C|EH Certified Ethical Hacker

EC-Council

MODULE 05

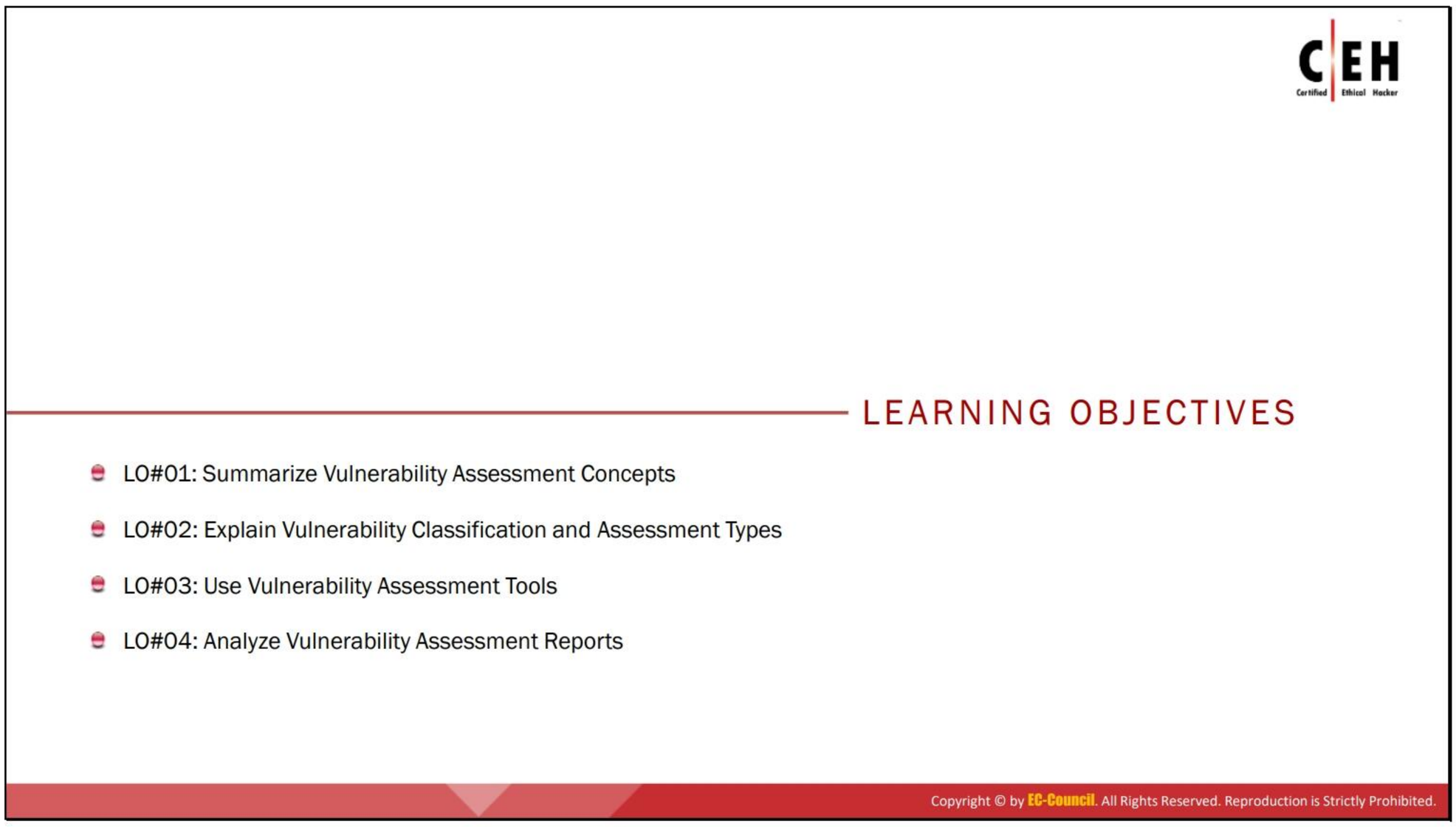
VULNERABILITY ANALYSIS



EC-COUNCIL OFFICIAL CURRICULA

This page is intentionally left blank.

https://t.me/learningnets



Learning Objectives

In today's world, organizations depend heavily on information technology for protecting vital information. This information is associated with areas of finance, research and development, personnel, legality, and security. Vulnerability assessments scan networks for known security weaknesses.

Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by attackers to further exploit that target network.

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute a vulnerability assessment.

This module starts with an introduction to vulnerability assessment concepts. It also discusses the various vulnerability scoring systems, vulnerability databases, vulnerability management life cycle, and various approaches and tools used to perform vulnerability assessments. This module will provide knowledge about the tools and techniques used by attackers to perform a quality vulnerability analysis. It concludes with an analysis of the vulnerability assessment reports that help an ethical hacker to fix the identified vulnerabilities.

At the end of this module, you will be able to:

- Understand vulnerability, vulnerability research, vulnerability assessment, and vulnerability scoring systems

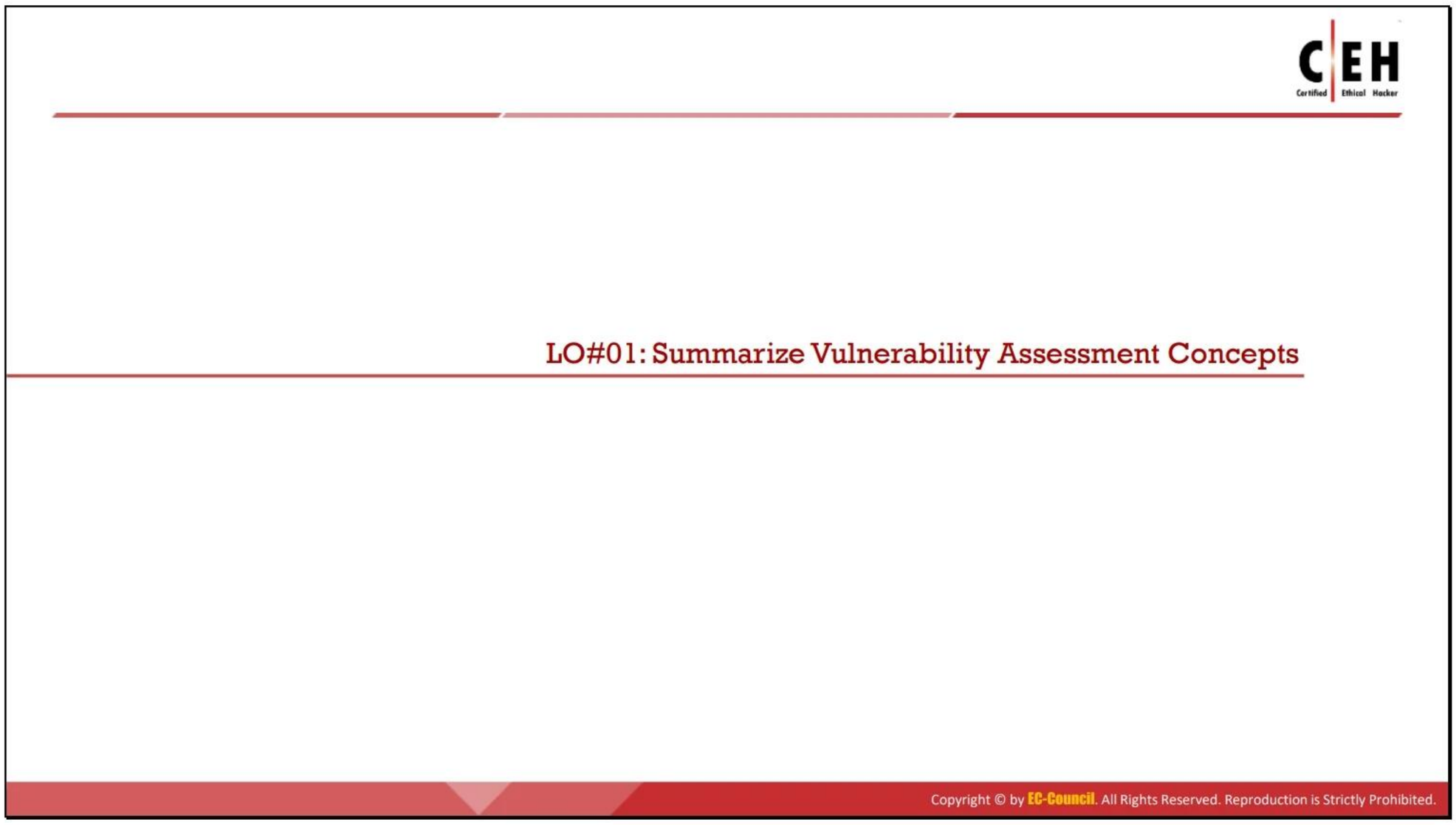
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Describe the vulnerability management life cycle (vulnerability assessment phases)
- Understand various types of vulnerabilities and vulnerability assessment techniques
- Understand different approaches to vulnerability assessment solutions
- Describe different characteristics of good vulnerability assessment solutions
- Explain different types of vulnerability assessment tools and the criteria for choosing them
- Use various vulnerability assessment tools
- Generate and analyze vulnerability assessment reports

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

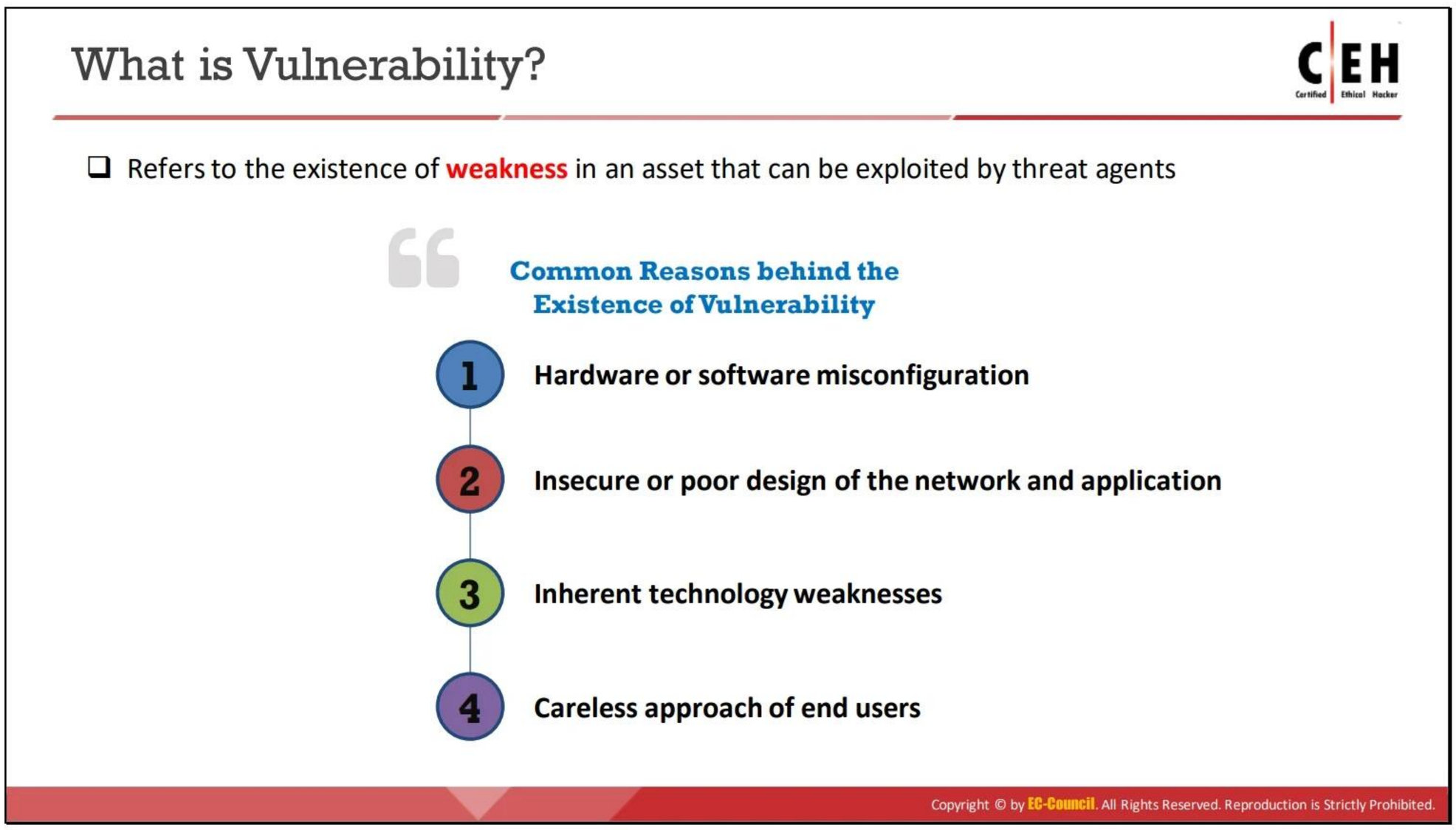


Vulnerability Assessment Concepts

This section provides an overview of vulnerability and its examples, vulnerability assessment, vulnerability scoring systems, vulnerability databases, and the vulnerability assessment lifecycle.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



What is Vulnerability?

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication. There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources.

Common Reasons for the Existence of Vulnerabilities

- **Hardware or software misconfiguration**

  The insecure configuration of the hardware or software in a network can lead to security loopholes. For example, a misconfiguration or the use of an unencrypted protocol may lead to network intrusions, resulting in the leakage of sensitive information. While a misconfiguration of hardware may allow attackers to obtain access to the network or system, a misconfiguration of software may allow attackers to obtain access to applications and data.

- **Insecure or poor design of network and application**

  An improper and insecure design of a network may make it susceptible to various threats and potential data loss. For example, if firewalls, IDS, and virtual private network (VPN) technologies are not implemented securely, they can expose the network to numerous threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Inherent technology weaknesses**

  If the hardware or software is not capable of defending the network against certain types of attacks, the network will be vulnerable to those attacks. Certain hardware, applications, or web browsers tend to be prone to attacks such as DoS or man-in-the-middle attacks. For example, systems running old versions of web browsers are prone to distributed attacks. If systems are not updated, a small Trojan attack can force the user to scan and clean the entire storage in the machine, which often leads to data loss.

- **End-user carelessness**

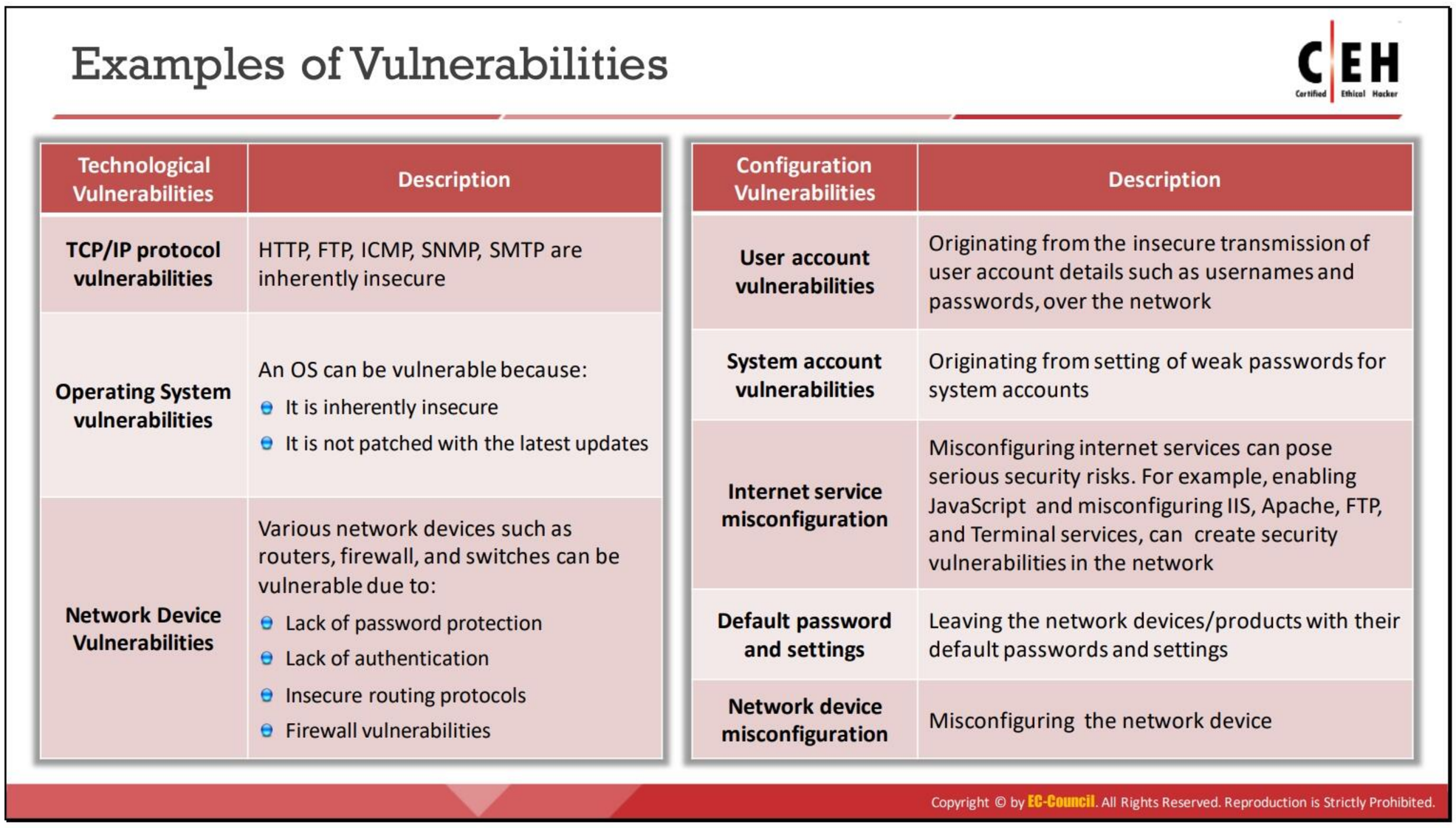
  End-user carelessness considerably impacts network security. Human behavior is fairly susceptible to various types of attacks and can be exploited to effect serious outcomes, including data loss and information leakage. Intruders can obtain sensitive information through various social engineering techniques. The sharing of account information or login credentials by users with potentially malicious entities can lead to the loss of data or exploitation of the information. Connecting systems to an insecure network can also lead to attacks from third parties.

- **Intentional end-user acts**

  Ex-employees who continue to have access to shared drives can misuse them by revealing the company's sensitive information. Such an act is called an intentional end-user act and can lead to heavy data and financial losses for the company.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Examples of Vulnerabilities

The following tables summarize examples of technological and configuration vulnerabilities:

Technological Vulnerabilities	Description
TCP/IP protocol vulnerabilities	▪ HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	▪ An OS can be vulnerable because: ○ It is inherently insecure ○ It is not patched with the latest updates
Network Device Vulnerabilities	▪ Various network devices such as routers, firewall, and switches can be vulnerable due to: ○ Lack of password protection ○ Lack of authentication ○ Insecure routing protocols ○ Firewall vulnerabilities

Table 5.1: Technological Vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

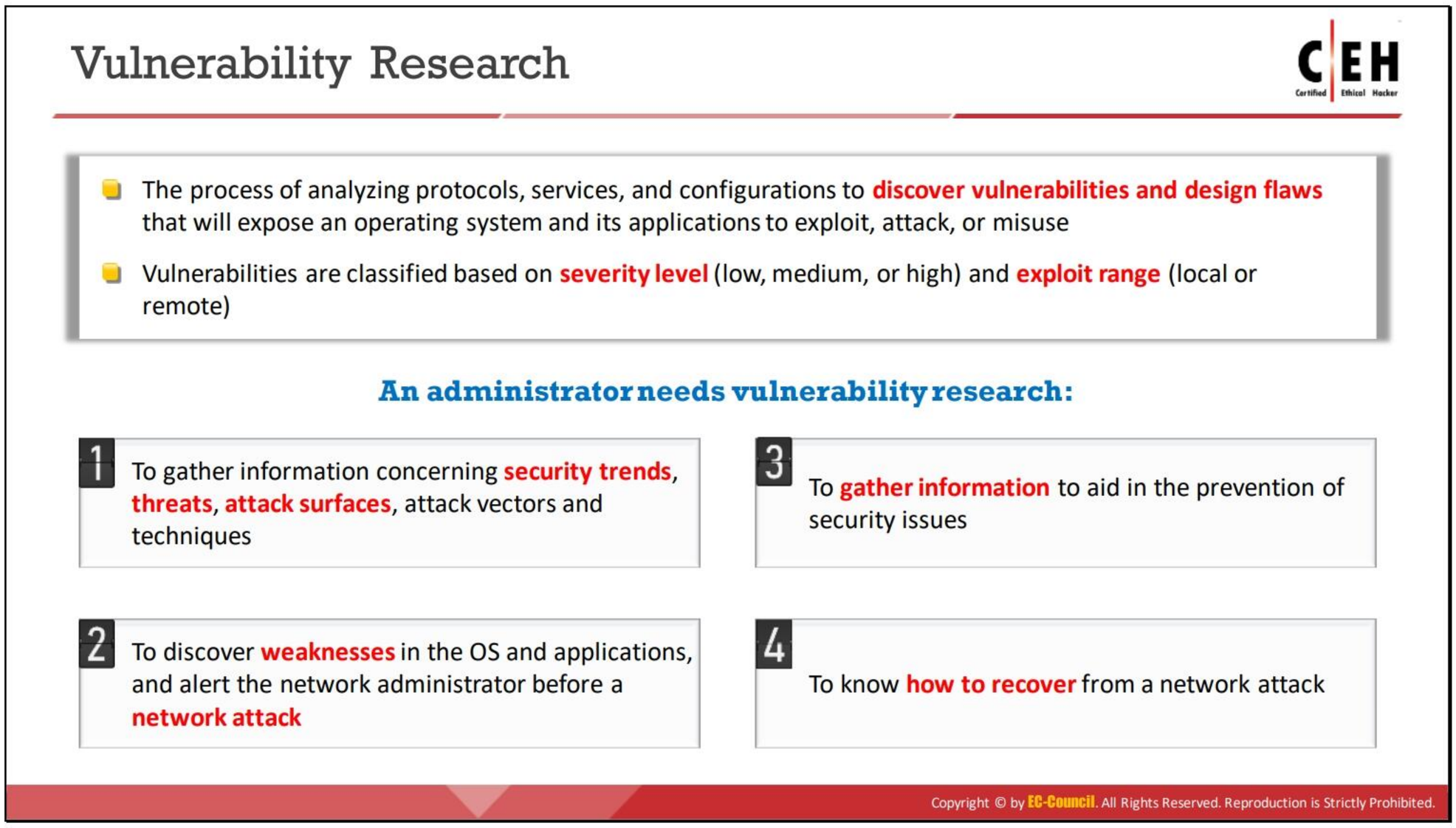
https://t.me/learningnets

Configuration Vulnerabilities	Description
User account vulnerabilities	▪ Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	▪ Originating from setting of weak passwords for system accounts
Internet service misconfiguration	▪ Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	▪ Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	▪ Misconfiguring the network device

Table 5.2: Configuration Vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Vulnerability Research

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

An administrator needs vulnerability research:

- To gather information about security trends, newly discovered threats, attack surfaces, attack vectors and techniques
- To find weaknesses in the OS and applications and alert the network administrator before a network attack
- To understand information that helps prevent security problems
- To know how to recover from a network attack

An ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits to stay one step ahead of attackers through vulnerability research, which includes:

- Discovering the system design faults and weaknesses that might allow attackers to compromise a system
- Staying updated about new products and technologies and reading news related to current exploits
- Checking underground hacking web sites (Deep and Dark websites) for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

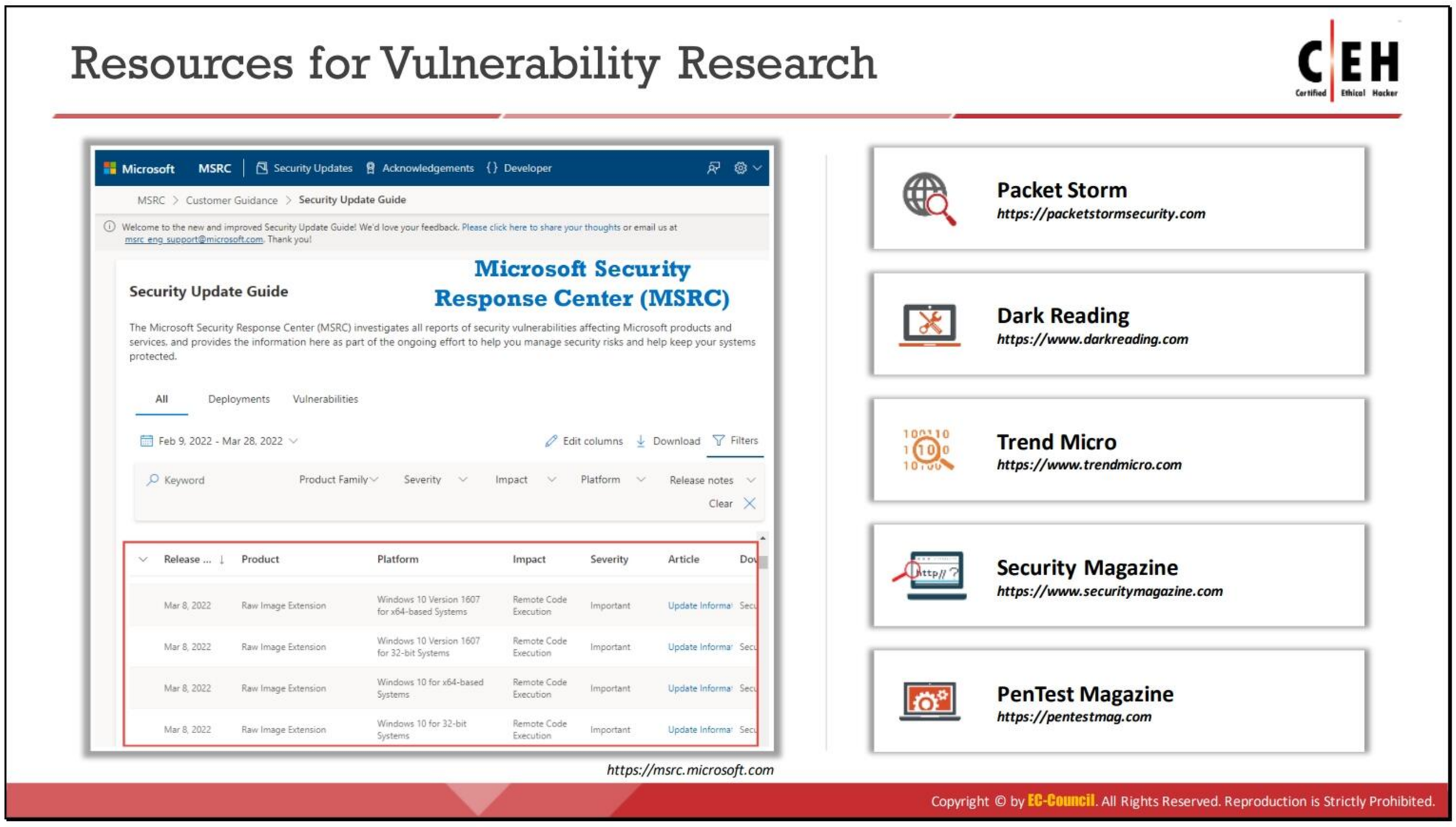
Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high)
- Exploit range (local or remote)

Ethical hackers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to find vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Resources for Vulnerability Research

The following are some of the websites used to perform vulnerability research.

- **Microsoft Security Response Center (MSRC)**

  Source: *https://msrc.microsoft.com*

  The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and it provides information as part of an ongoing effort to help security professionals manage security risks and keep organizational systems protected.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

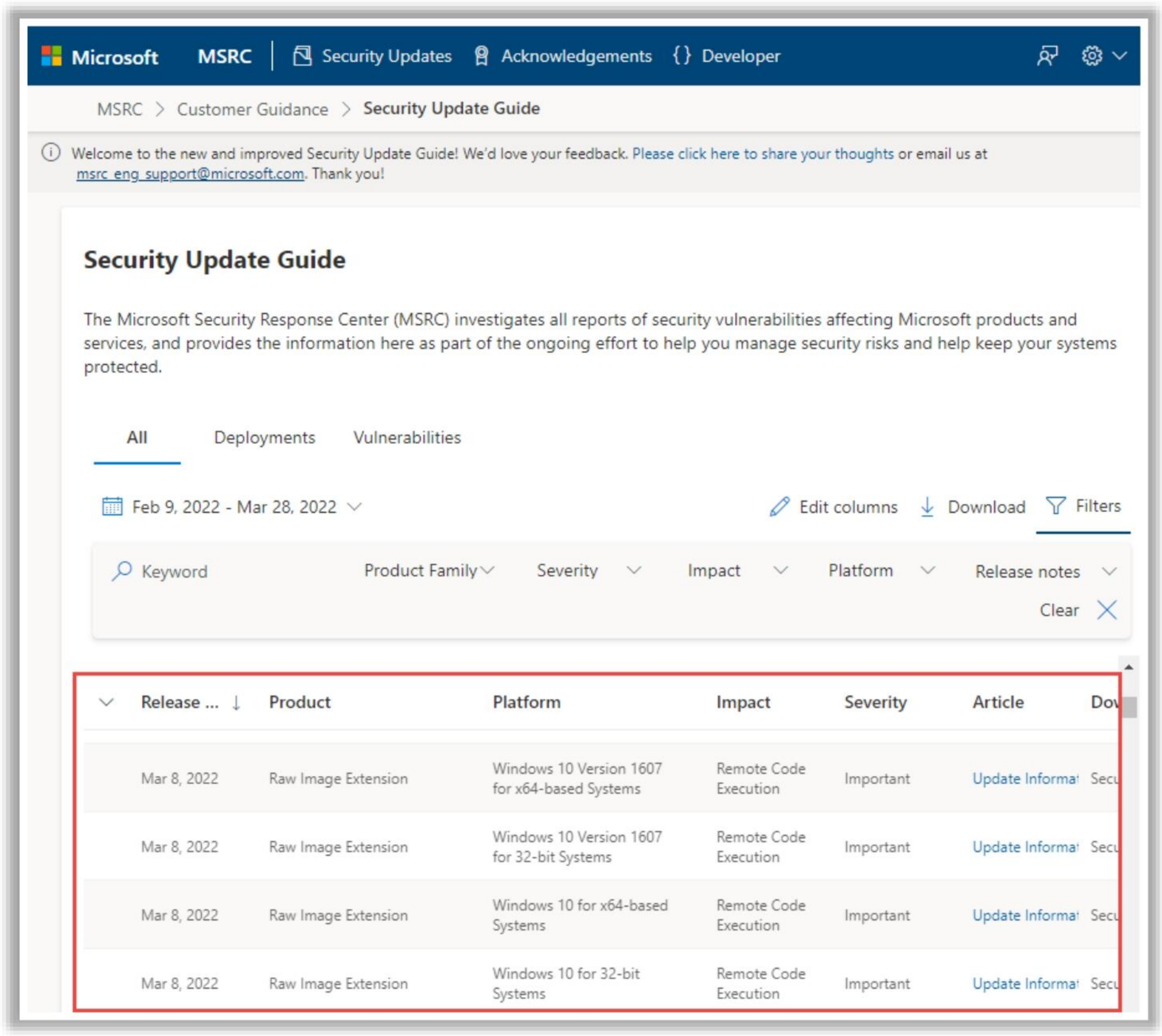
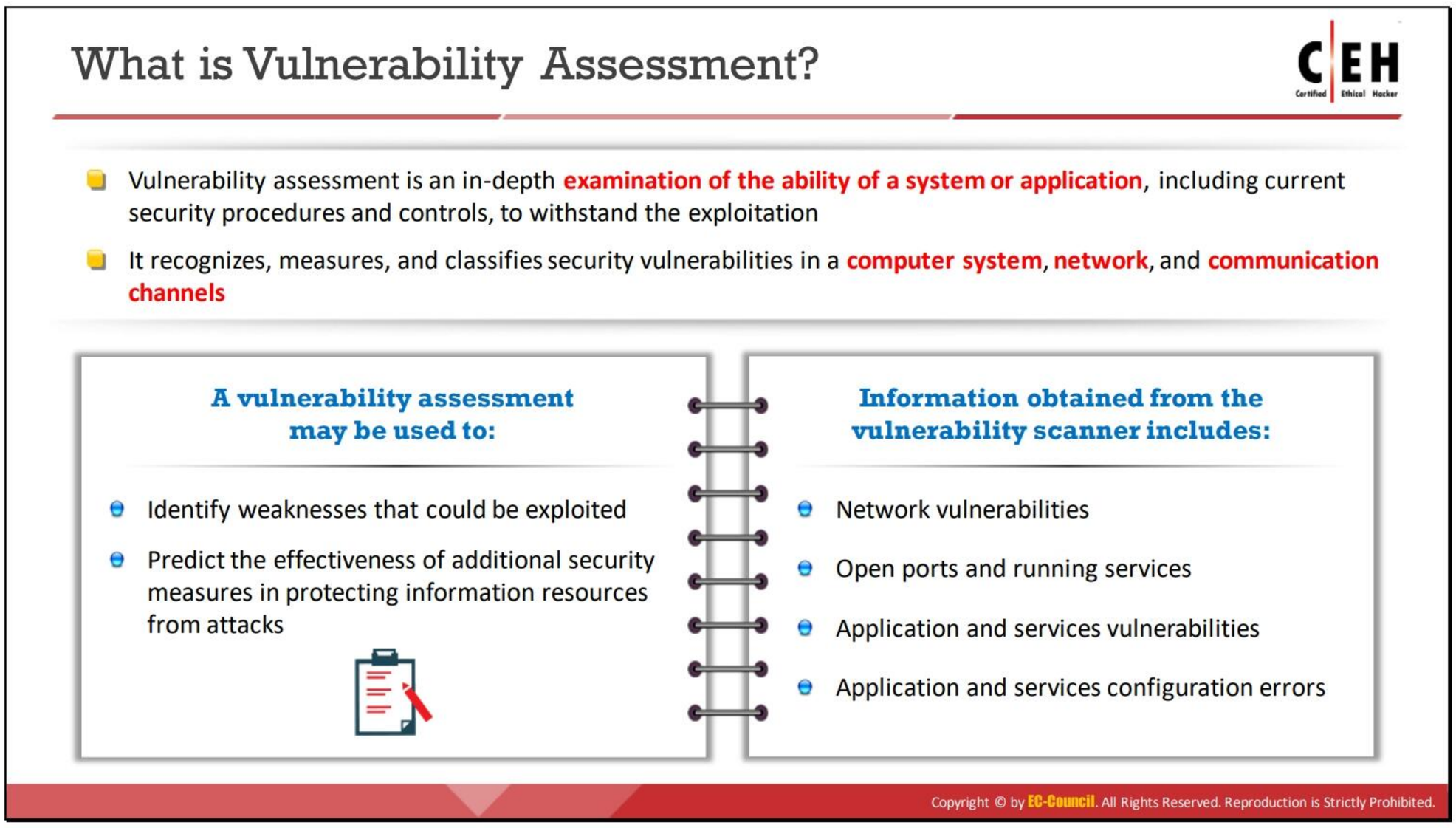


Figure 5.1: Screenshot of Microsoft Security Response Center (MSRC)

- Packet Storm (*https://packetstormsecurity.com*)
- Dark Reading (*https://www.darkreading.com*)
- Trend Micro (*https://www.trendmicro.com*)
- Security Magazine (*https://www.securitymagazine.com*)
- PenTest Magazine (*https://pentestmag.com*)
- SC Magazine (*https://www.scmagazine.com*)
- Exploit Database (*https://www.exploit-db.com*)
- Help Net Security (*https://www.helpnetsecurity.com*)
- HackerStorm (*http://www.hackerstorm.co.uk*)
- Computerworld (*https://www.computerworld.com*)
- D'Crypt (*https://www.d-crypt.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



What is Vulnerability Assessment?

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

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 attack

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Errors in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities
- EOL/EOS software information
- Missing patches and hotfixes
- Weak network configurations and misconfigured or risky ports
- Help to verify the inventory of all devices on the network

There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

  Example: An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities.

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weaknesses but does not provide a path for directly combating attacks.

  Example: An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown.

Attackers scan for vulnerabilities using tools such as Nessus Professional, Qualys, GFI LanGuard, and OpenVAS.

Limitations of Vulnerability Assessment

The following are some of the limitations of vulnerability assessment:

- Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time.
- Vulnerability scanning software must be updated when new vulnerabilities are discovered or when improvements are made to the software being used.
- Software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it.
- Vulnerability assessment does not measure the strength of security controls.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed.
- Human judgment is required to analyze the data after scanning and identifying false positives and false negatives.
- Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations.
- Vulnerability assessment reports are not always easy to understand and assess for risk factors and triage response.
- Vulnerability scanning tools have a narrow focus and do not cover attack vectors such as social engineering.
- Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior.

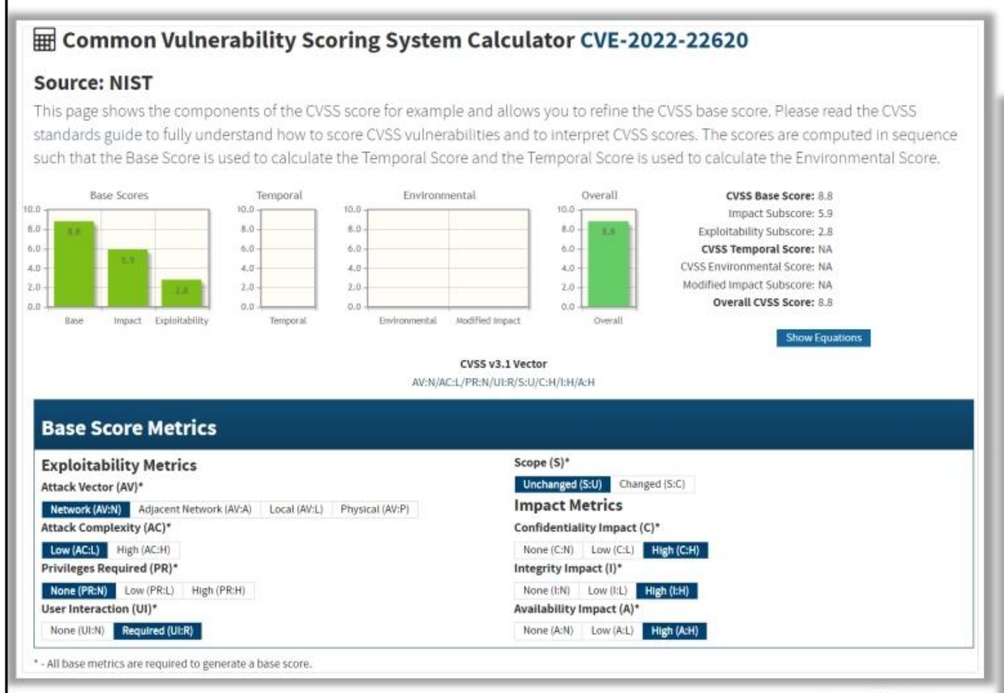
The methodology used may have an impact on the test results. For example, vulnerability scanning software that runs in the security context of the domain administrator will yield different results from software that runs in the security context of an authenticated or non-authenticated user. Similarly, diverse vulnerability scanning software packages differently assess security and have unique features. This can influence the assessment results.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

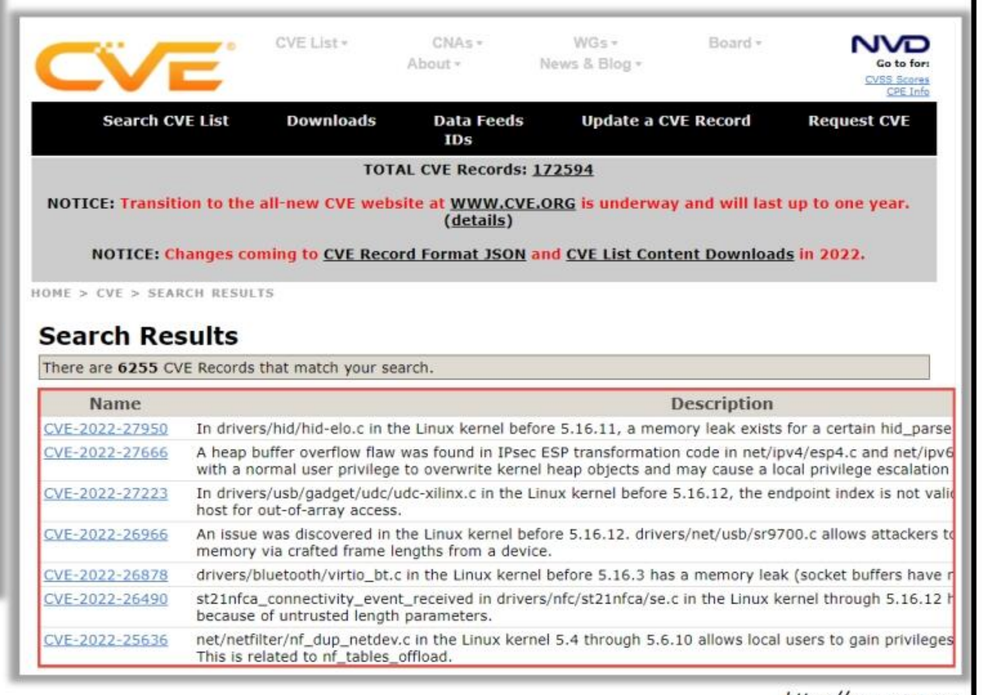
Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)



https://nvd.nist.gov

Common Vulnerabilities and Exposures (CVE)

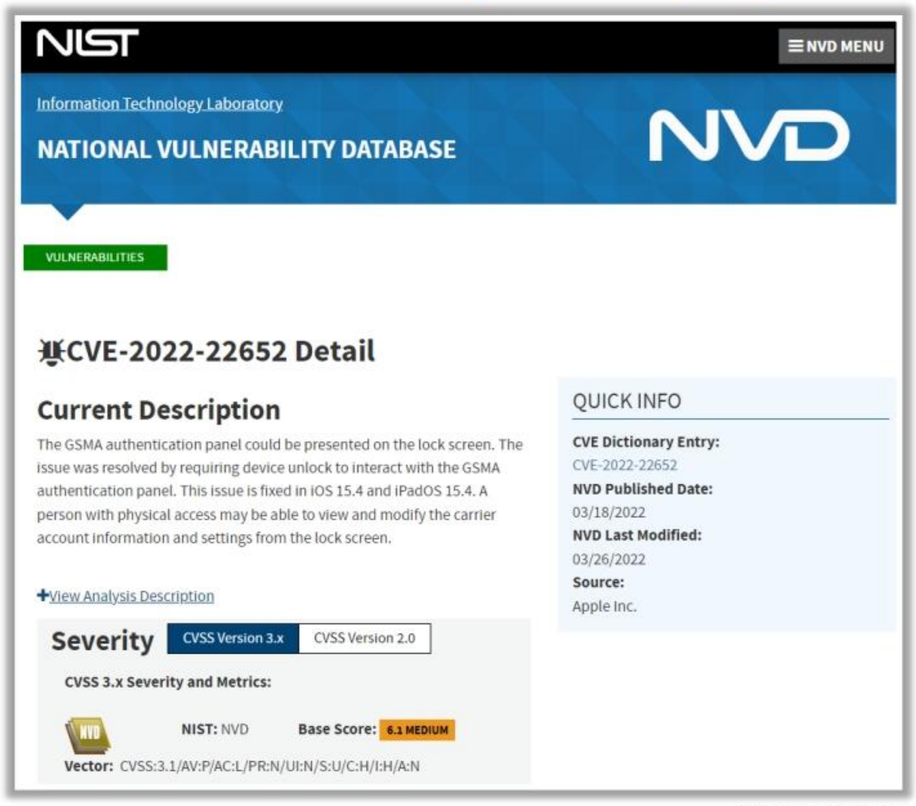


https://www.cve.org

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

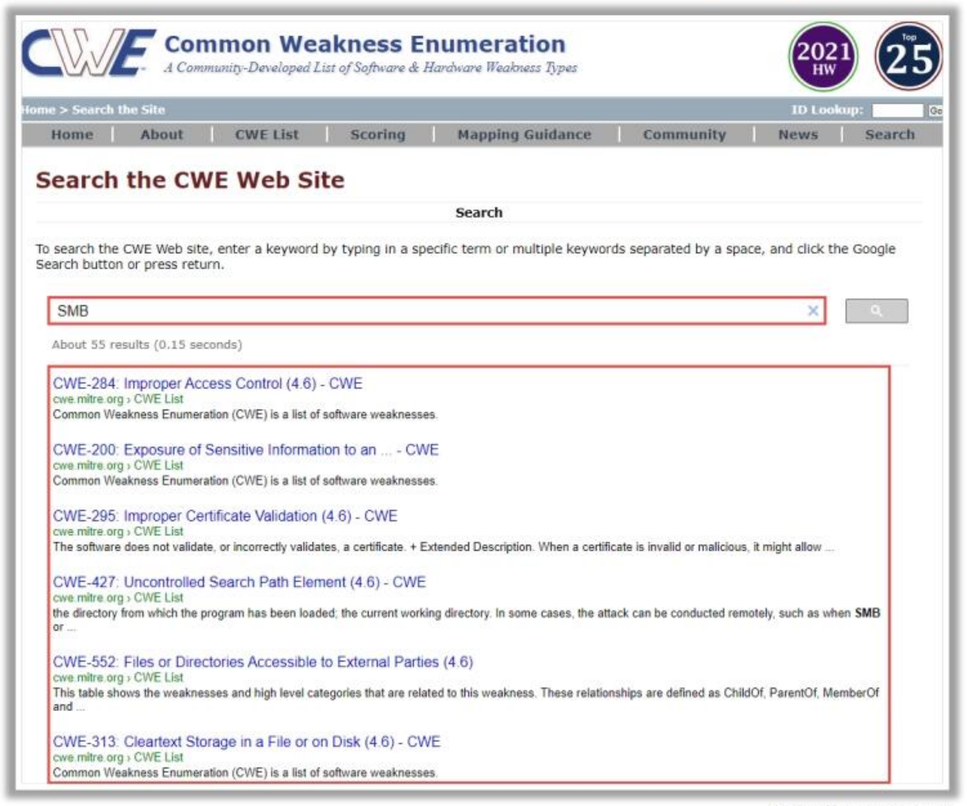
Vulnerability Scoring Systems and Databases (Cont'd)

National Vulnerability Database (NVD)



https://nvd.nist.gov

Common Weakness Enumeration (CWE)



https://cwe.mitre.org

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

Vulnerability Scoring Systems and Databases

Due to the growing severity of cyber-attacks, vulnerability research has become critical as it helps to mitigate the chance of attacks. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that can be exploited by attackers. Vulnerability scoring systems and vulnerability databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

risk associated with identified vulnerabilities. Vulnerability databases collect and maintain information about various vulnerabilities present in information systems.

Following are some of the vulnerability scoring systems and databases:

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Weakness Enumeration (CWE)

Common Vulnerability Scoring System (CVSS)

Source: *https://www.first.org*, *https://nvd.nist.gov*

The CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The quantitative model of the system ensures repeatable and accurate measurement while enabling users to view the underlying vulnerability characteristics that were used to generate the scores. Thus, the CVSS is well-suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are the prioritization of vulnerability remediation activities and calculation of the severity of vulnerabilities discovered in a system. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

The CVSS helps capture the principal characteristics of a vulnerability and produces a numerical score to reflect its severity. This numerical score can thereafter be translated into a qualitative representation (such as low, medium, high, or critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS assessment consists of the following three metrics for measuring vulnerabilities.

- **Base Metric**: It represents the inherent qualities of a vulnerability.
- **Temporal Metric**: It represents the features that continue to change during the lifetime of the vulnerability.
- **Environmental Metric:** It represents vulnerabilities that are based on a particular environment or implementation.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

The metric ranges from 1 to 10, with 10 being the most severe. The CVSS score is calculated and generated by a vector string that represents the numerical score for each group in the form of a block of text. The CVSS calculator ranks security vulnerabilities and provides the user with information on the overall severity and risks related to the vulnerability.

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Table 5.3: CVSS v3.0 ratings

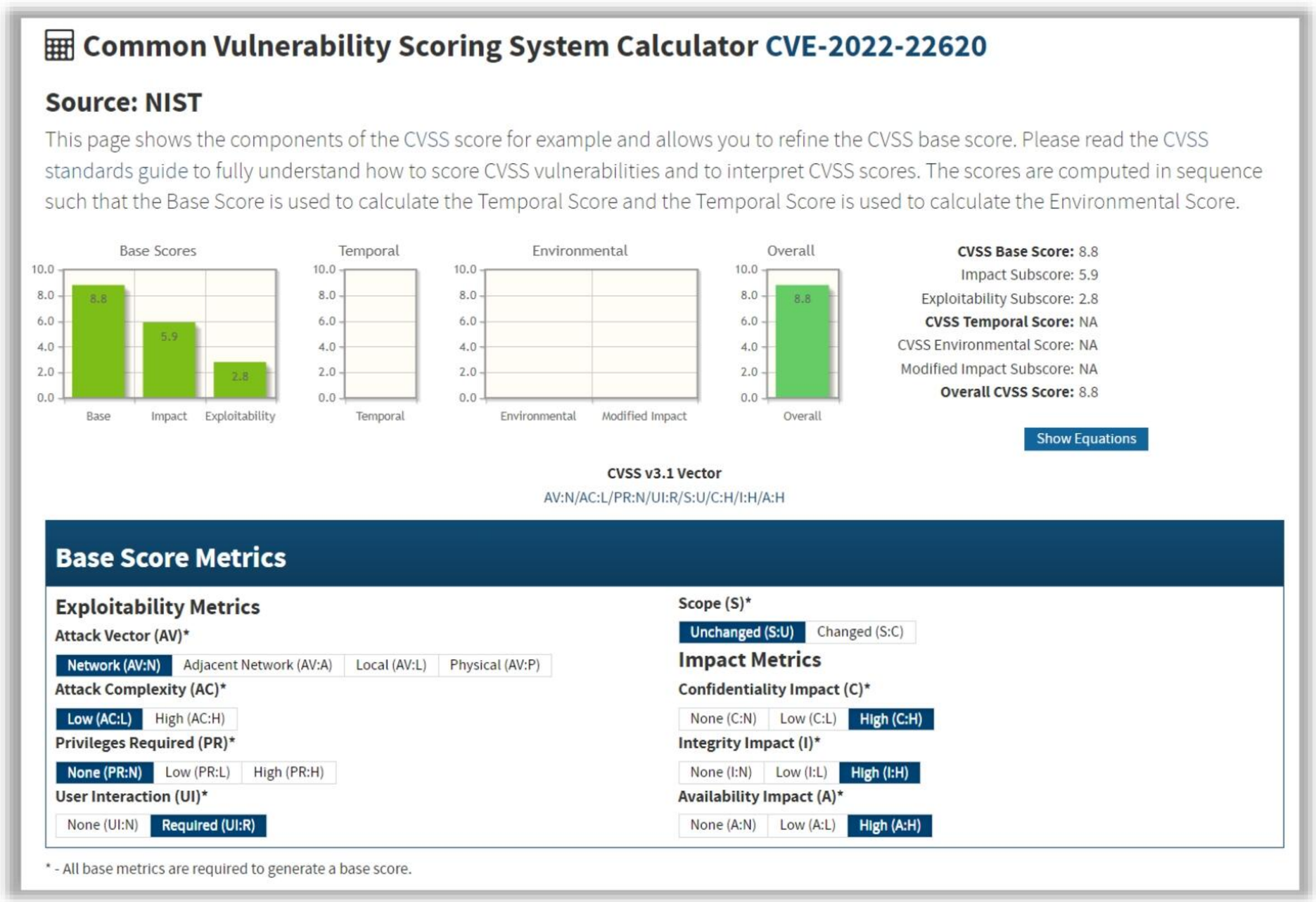


Figure 5.2: CVSS Calculator Version 3.1

Common Vulnerabilities and Exposures (CVE)

Source: *https://www.cve.org*

CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. The use of CVE Identifiers, or "CVE IDs," which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when discussing or sharing information about a unique software or firmware

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

vulnerability. CVE provides a baseline for tool evaluation and enables data exchange for cybersecurity automation. CVE IDs provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

What CVE is:

- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- A method for disparate databases and tools to "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for the public to download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and the numerous products and services that include CVE

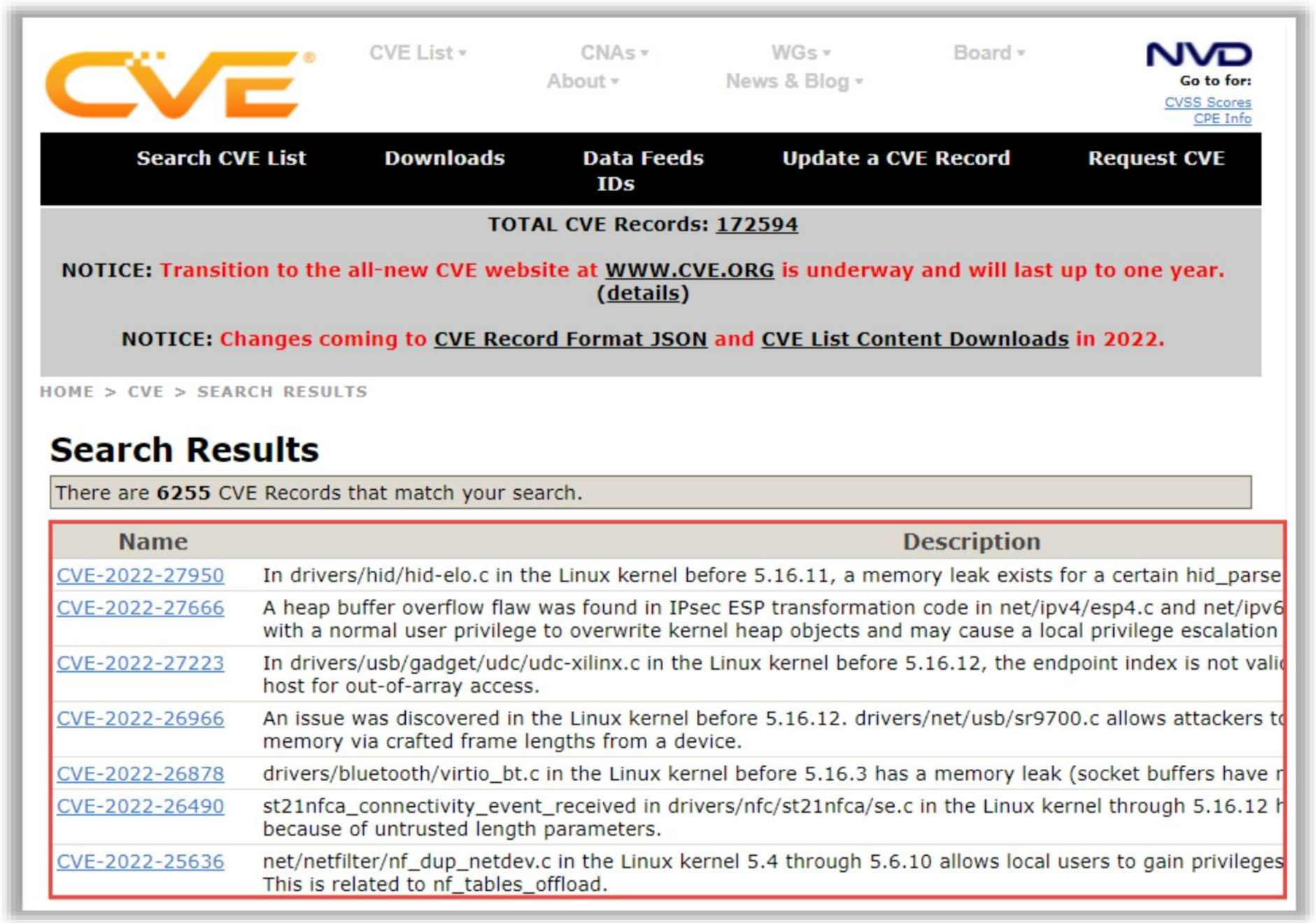


Figure 5.3: Common Vulnerabilities and Exposures (CVE)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

National Vulnerability Database (NVD)

Source: *https://nvd.nist.gov*

The NVD is the U.S. government repository of standards-based vulnerability management data. It uses the Security Content Automation Protocol (SCAP). Such data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

The NVD performs an analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with the analysis of CVEs by aggregating data points from the description, references supplied, and any supplemental data that are publicly available. This analysis results in association impact metrics (Common Vulnerability Scoring System – CVSS), vulnerability types (Common Weakness Enumeration — CWE), and applicability statements (Common Platform Enumeration — CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing; it relies on vendors, third party security researchers, and vulnerability coordinators to provide information that is used to assign these attributes.

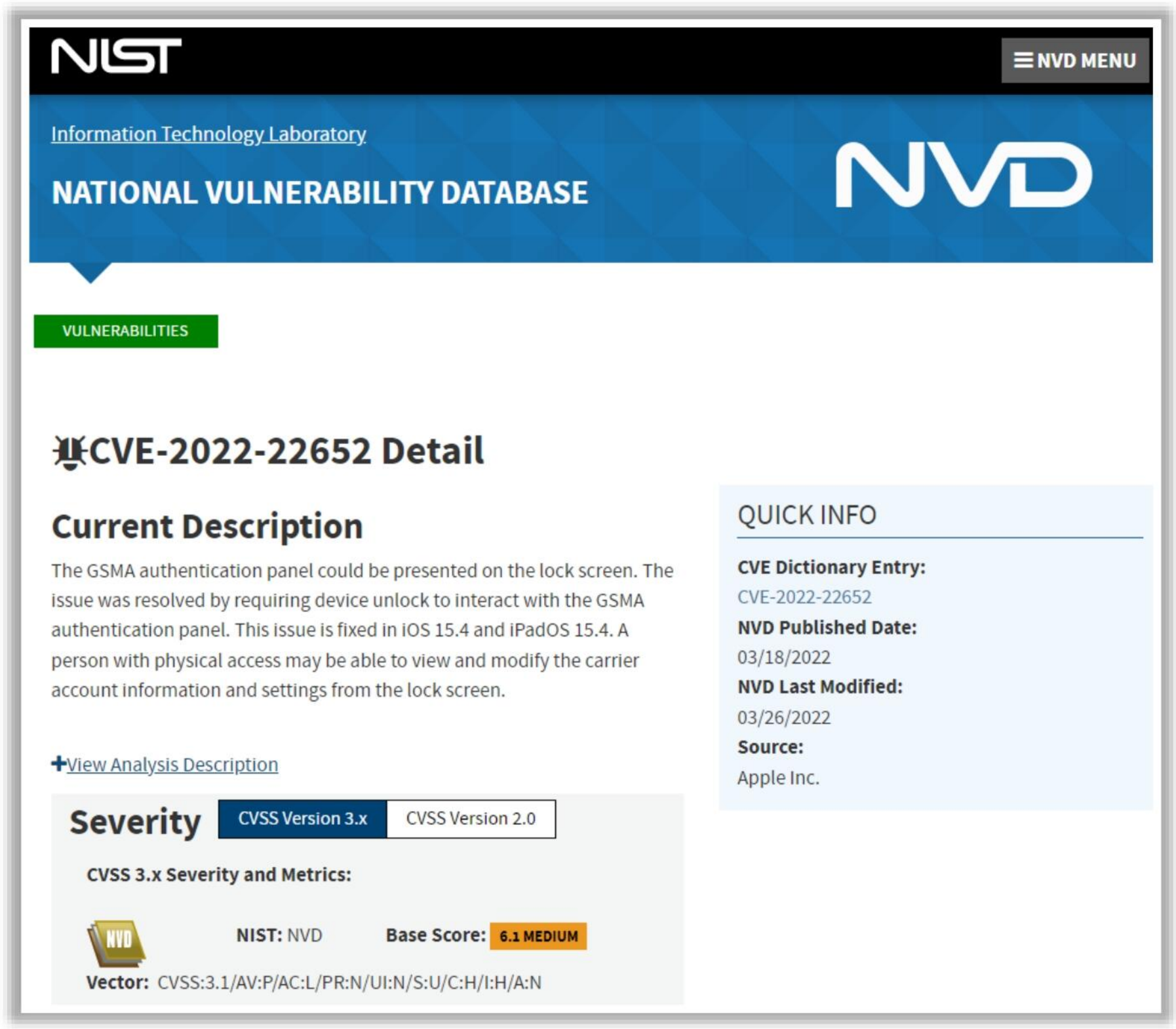


Figure 5.4: Screenshot showing CVE details in the National Vulnerability Database (NVD)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Common Weakness Enumeration (CWE)

Source: *https://cwe.mitre.org*

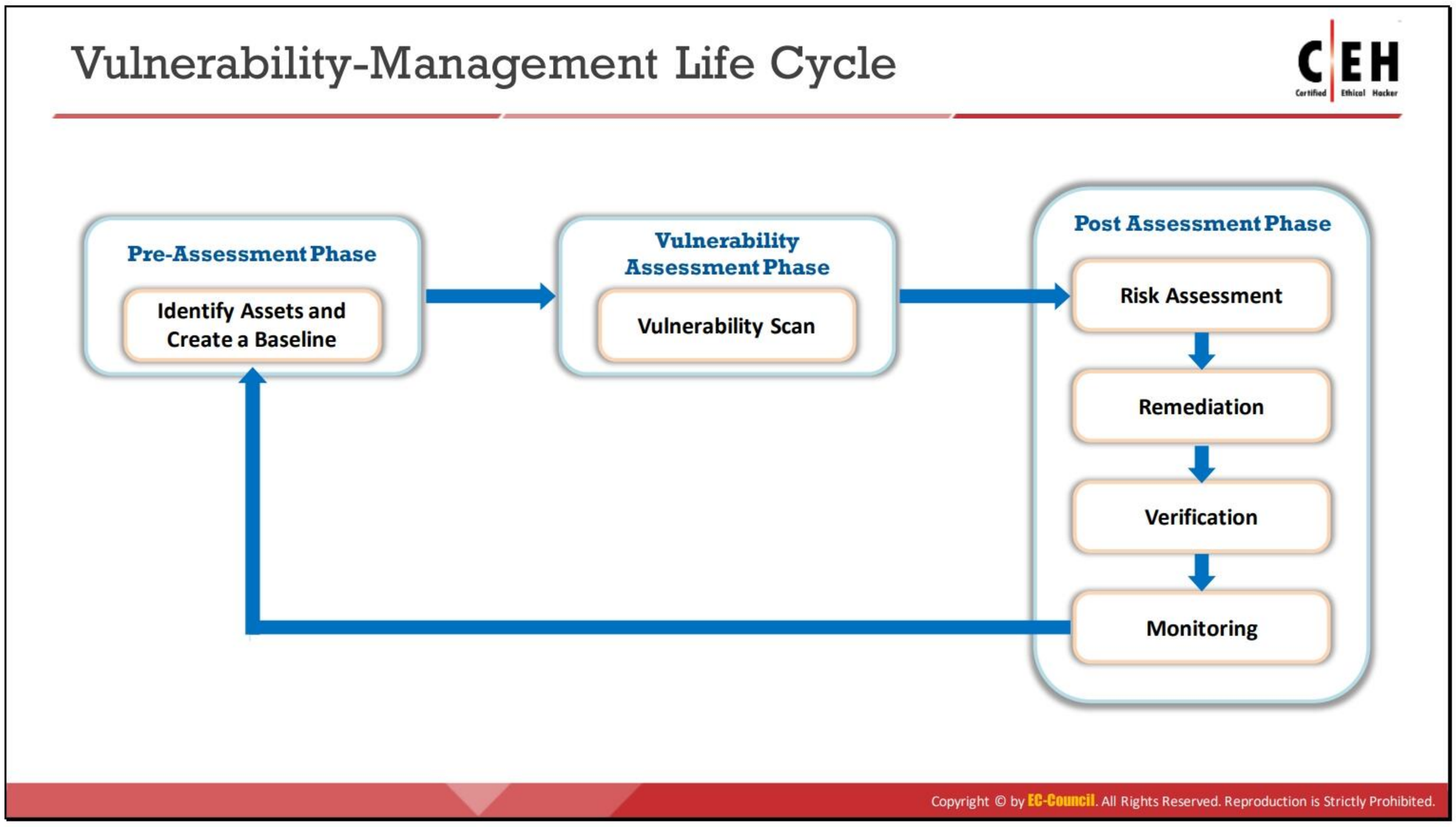
Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security. The latest version 3.2 of the CWE standard was released in January 2019. It has over 600 categories of weaknesses, which gives CWE the ability to be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. It also has an advanced search technique where attackers can search and view weaknesses based on research concepts, development concepts, and architectural concepts.



Figure 5.5: Screenshot showing CWE results for SMB query

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Vulnerability-Management Life Cycle

The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are identified. The implementation of a vulnerability management lifecycle helps gain a strategic perspective regarding possible cybersecurity threats and renders insecure computing environments more resilient to attacks.

Vulnerability management should be implemented in every organization as it evaluates and controls the risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system.

Organizations should maintain a proper vulnerability management program to ensure overall information security. Vulnerability management provides the best results when it is implemented in a sequence of well-organized phases.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

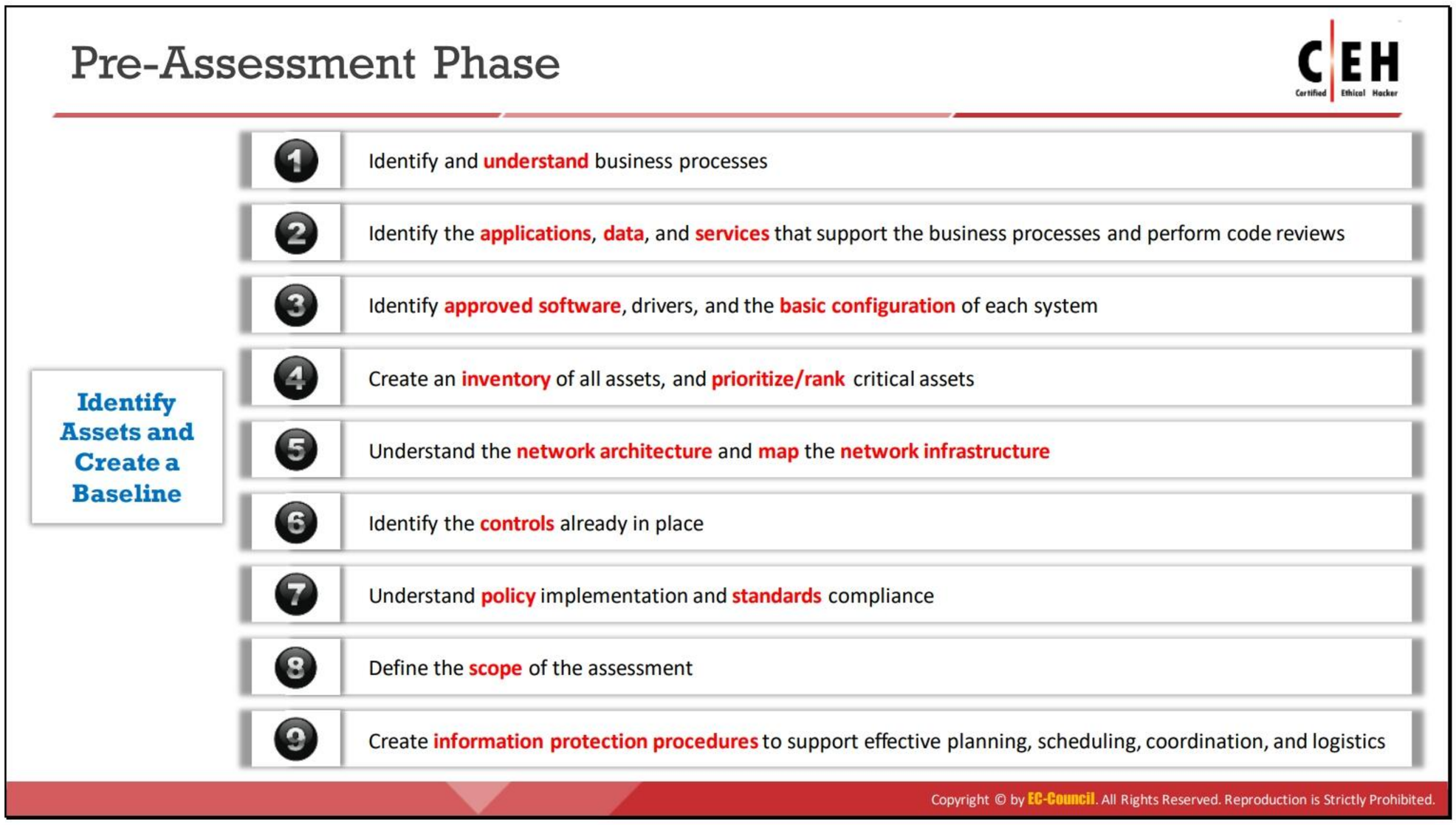
https://t.me/learningnets

The phases involved in vulnerability management are:

- **Pre-Assessment Phase**
  - Identify Assets and Create a Baseline
- **Vulnerability Assessment Phase**
  - Vulnerability Scan
- **Post Assessment Phase**
  - Risk Assessment
  - Remediation
  - Verification
  - Monitoring

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Pre-Assessment Phase

Identify Assets and Create a Baseline

The pre-assessment phase is a preparatory phase, which involves defining policies and standards, clarifying the scope of the assessment, designing appropriate information protection procedures, and identifying and prioritizing critical assets to create a good baseline for vulnerability management and to define the risk based on the criticality and value of each system. This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration of each system in order to develop and maintain a system baseline.

The following are the steps involved in creating a baseline:

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes and perform code reviews
3. Identify the approved software, drivers, and basic configuration of each system
4. Create an inventory of all assets, and prioritize or rank the critical assets
5. Understand the network architecture and map the network infrastructure
6. Identify the controls already in place
7. Understand policy implementation and practice standard compliance with business processes
8. Define the scope of the assessment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

9. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

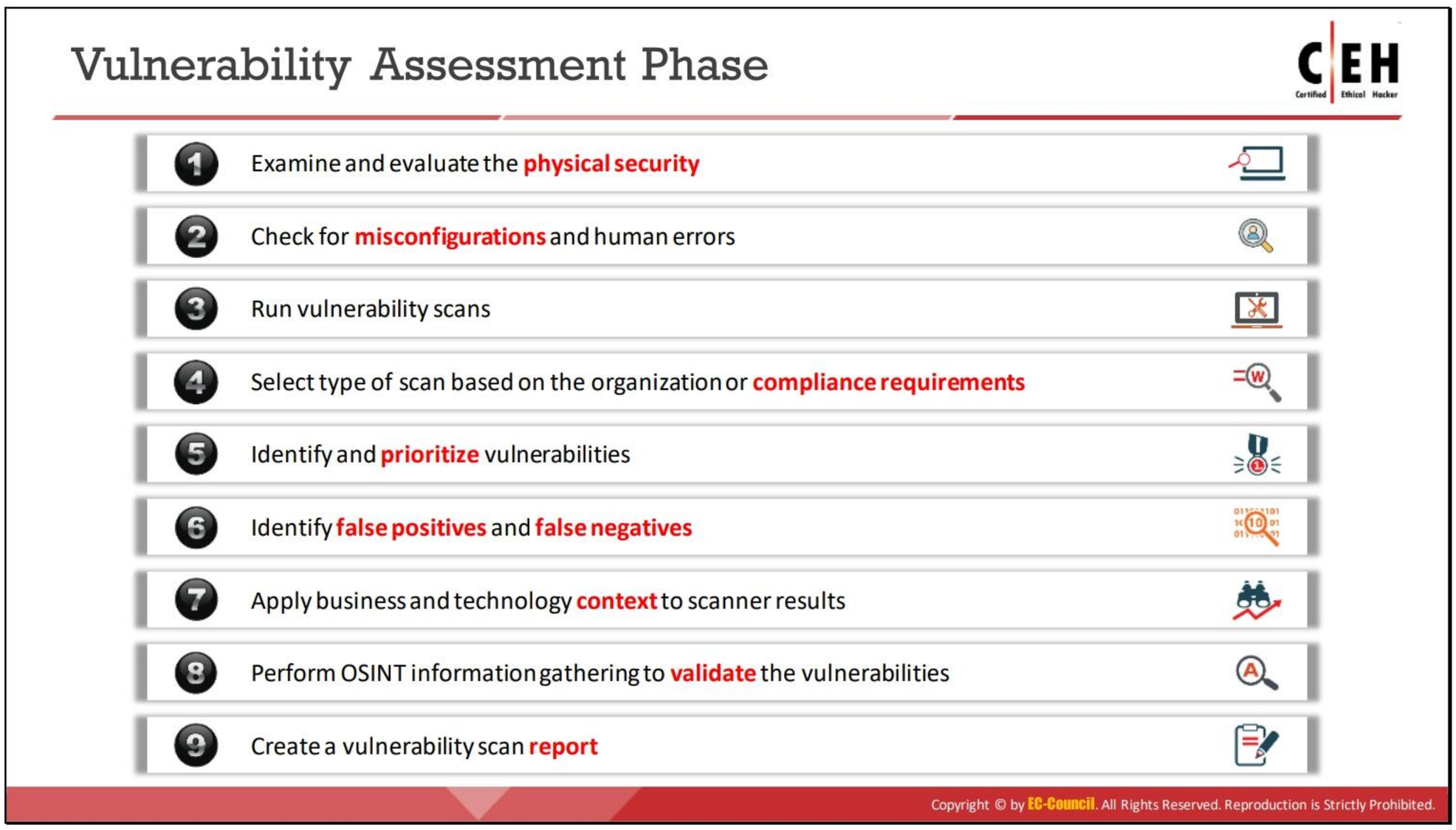
Classify the identified assets according to the business needs. Classification helps to identify the high business risks in an organization. Prioritize the rated assets based on the impact of their failure and their reliability in the business.

Prioritization helps:

- Evaluate and decide a solution for the consequence of the assets failing
- Examine the risk tolerance level
- Organize methods for prioritizing the assets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Vulnerability Assessment Phase

This phase is very crucial in vulnerability management. The vulnerability assessment phase refers to identifying vulnerabilities in the organization's infrastructure, including the operating system, web applications, and web server. It helps identify the category and criticality of the vulnerability in an organization and minimizes the level of risk. The ultimate goal of vulnerability scanning is to scan, examine, evaluate, and report the vulnerabilities in the organization's information system. Vulnerability scans can also be performed on applicable compliance templates to assess the organization's Infrastructure weaknesses against the respective compliance guidelines.

The assessment phase involves examining the architecture of the network, evaluating threats to the environment, performing penetration testing, examining and evaluating physical security, analyzing physical assets, assessing operational security, observing policies and procedures, and assessing the infrastructure's interdependencies.

Steps involved in the assessment phase:

1. Examine and evaluate the physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Select the type of scan based on the organization or compliance requirements
5. Identify and prioritize vulnerabilities
6. Identify false positives and false negatives
7. Apply the business and technology context to scanner results

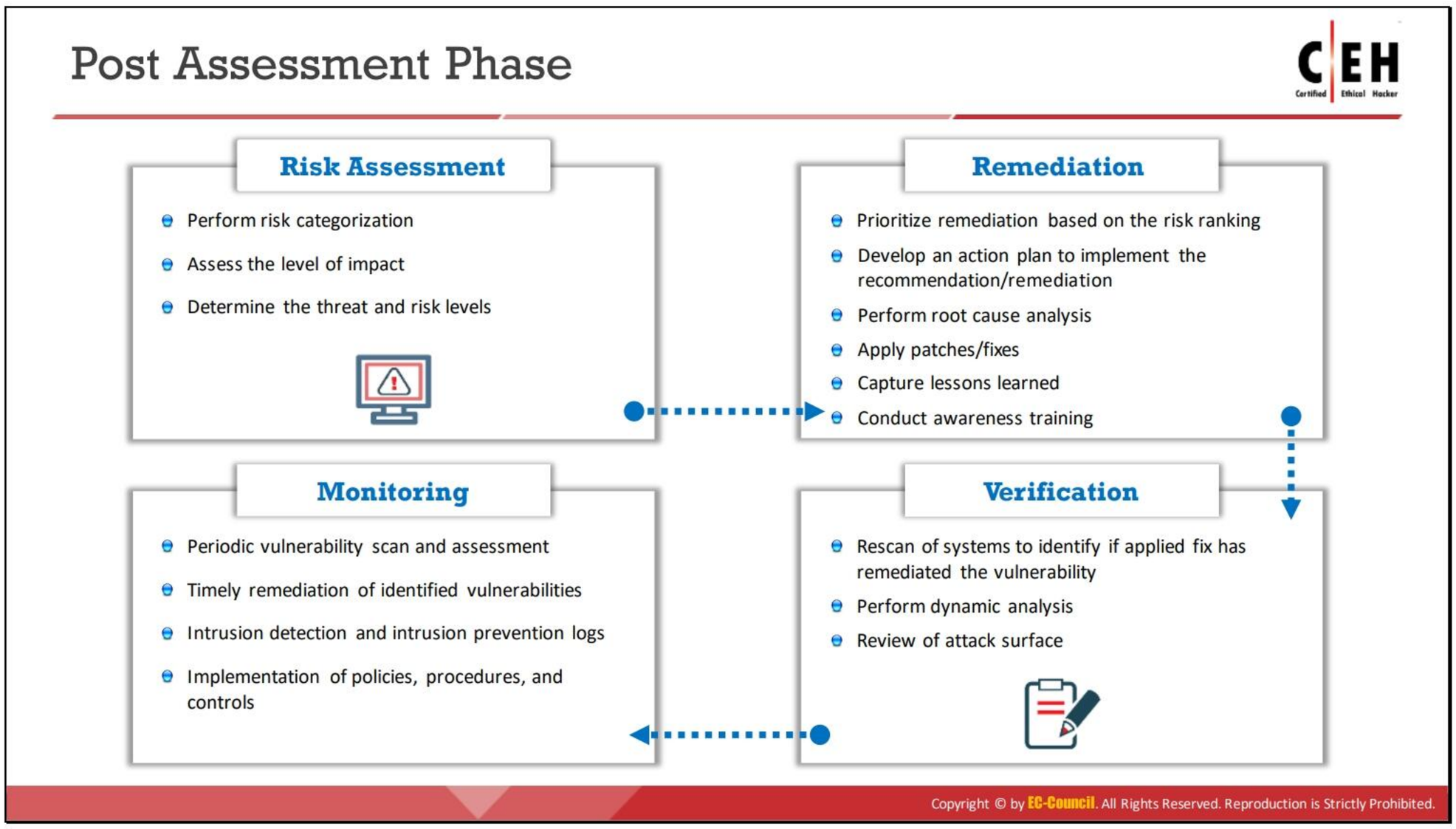
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

8. Perform OSINT information gathering to validate the vulnerabilities
9. Create a vulnerability scan report

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Post Assessment Phase

The post-assessment phase, also known as the recommendation phase, is performed after and based on risk assessment. Risk characterization is categorized by key criteria, which helps prioritize the list of recommendations.

The tasks performed in the post-assessment phase include:

- Creating a priority list for assessment recommendations based on the impact analysis
- Developing an action plan to implement the proposed remediation
- Capturing lessons learned to improve the complete process in the future
- Conducting training for employees

Post assessment includes risk assessment, remediation, verification, and monitoring.

- **Risk Assessment**

  In the risk assessment phase, risks are identified, characterized, and classified along with the techniques used to control or reduce their impact. It is an important step toward identifying the security weaknesses in the IT architecture of an organization.

  In this phase, all serious uncertainties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. Remediation is planned based on the determined risk level. For example, vulnerabilities ranked high-risk are targeted first to decrease the chances of exploitation that would adversely impact the organization.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

The tasks performed in the risk assessment phase include:

- Perform risk categorization based on risk ranking (for example, critical, high, medium, and low)
- Assess the level of impact
- Determine the threat and risk levels

- **Remediation**

  Remediation is the process of applying fixes on vulnerable systems in order to mitigate or reduce the impact and severity of vulnerabilities. These include steps like evaluating vulnerabilities, locating risks, and designing responses for vulnerabilities. It is important for the remediation process to be specific, measurable, attainable, relevant, and time-bound.

  This phase is initiated after the successful implementation of the baseline and assessment steps.

  The tasks performed in the remediation phase include:

  - Prioritize remediation based on the risk ranking
  - Develop an action plan to implement the recommendation or remediation
  - Perform a root-cause analysis
  - Apply patches and fixes
  - Capture lessons learned
  - Conduct awareness training
  - Perform exception handling and risk acceptance for the vulnerabilities that cannot be remediated

- **Verification**

  In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets. This phase includes the verification of the remedies used to mitigate risks. It provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not. Verification can be performed by using various means such as ticketing systems, scanners, and reports.

  The tasks performed in the verification phase include:

  - Rescanning the systems to identify if an applied fix is effective in remediating the vulnerability
  - Performing dynamic analysis
  - Reviewing the attack surface

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Monitoring**

  Organizations need to perform regular monitoring to maintain system security. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved. As per security best practices, all phases of vulnerability management must be performed regularly.

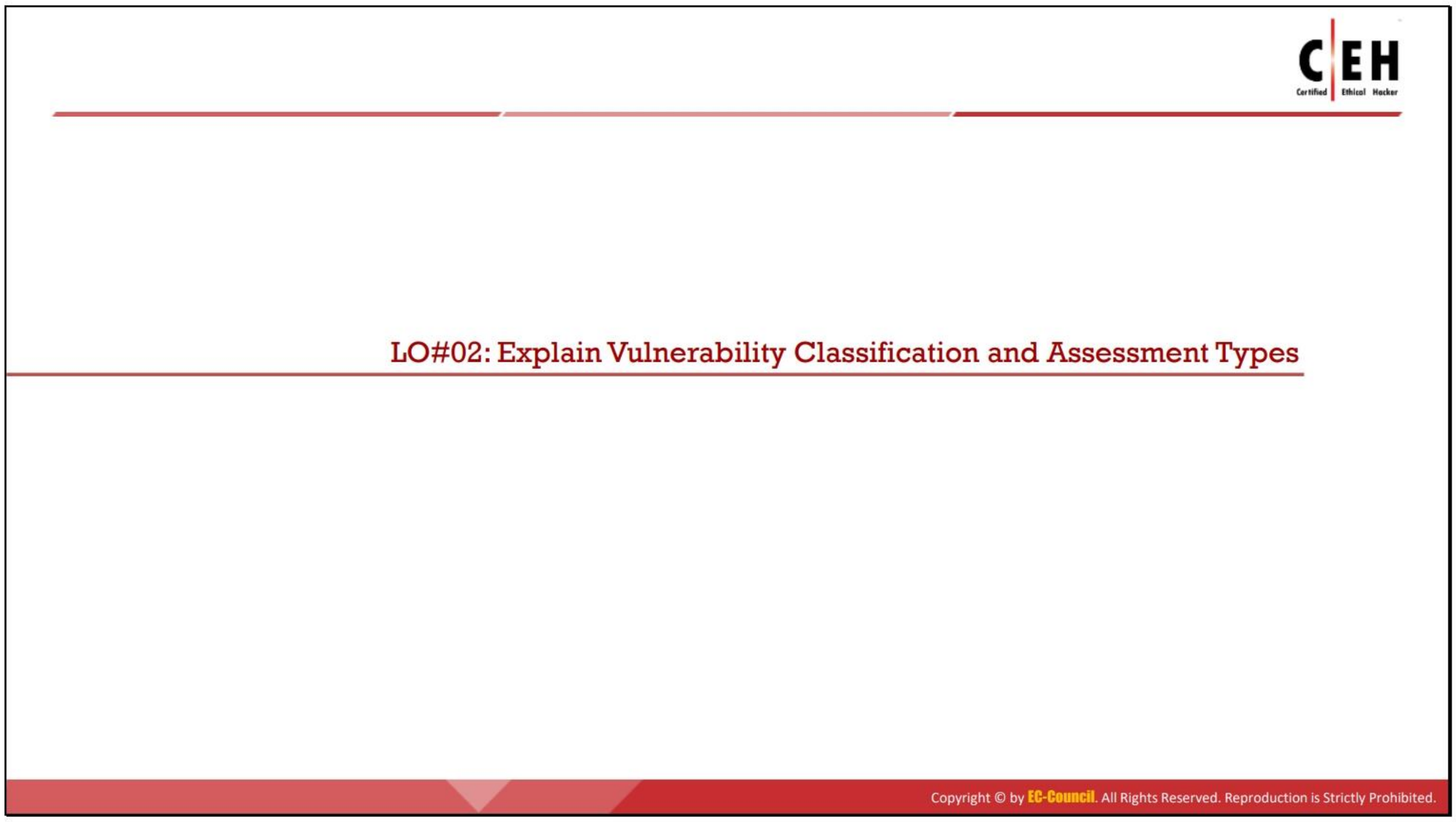
  This phase performs incident monitoring using tools such as IDS/IPS, SIEM, and firewalls. It implements continuous security monitoring to thwart ever-evolving threats.

  The tasks performed in the monitoring phase include:

  - Periodic vulnerability scan and assessment
  - Timely remediation of identified vulnerabilities
  - Monitoring intrusion detection and intrusion prevention logs
  - Implementing policies, procedures, and controls

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Vulnerability Classification and Assessment Types

Any vulnerability that is present in a system can be hazardous and can cause severe damage to the organization. It is important for ethical hackers to have knowledge about various types of vulnerabilities that they can employ, along with various vulnerability assessment techniques. This section in the module discusses the various types of vulnerabilities and vulnerability assessments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Vulnerability Classification

Vulnerability Type	Description	Examples
Misconfigurations/Weak Configurations	• Misconfiguration is the most common vulnerability and is mainly caused by human error • It allows attackers to **break into a network** and gain unauthorized access to systems	**Network Misconfigurations** • Insecure protocols, open ports and services, errors, and weak encryption **Host Misconfigurations** • Open permissions and unsecured root accounts
Application Flaws	• Application flaws are vulnerabilities in applications that are exploited by attackers • Flawed applications pose security threats such as **data tampering** and **unauthorized access** to configuration stores	• Buffer overflows, memory leaks, resource exhaustion, integer overflows, null pointer/object dereference, DLL injection, race conditions, improper input handling, and improper error handling
Poor Patch Management	• Software vendors provide patches that **prevent exploitations** and reduce the probability of threats exploiting a specific vulnerability • Unpatched software can make an application, server, or device **vulnerable to various attacks**	• Unpatched servers, unpatched firmware, unpatched OS, and unpatched applications
Design Flaws	• Logical flaws in the functionality of the system are exploited by the attackers to **bypass the detection mechanism** and acquire access to a secure system	• Incorrect encryption and poor validation of data
Third-Party Risks	• Third-party services can have access to privileged systems and applications, through which financial information, customer and employee data, and processes in the enterprise's supply chain can be compromised	• Vendor management, supply-chain risks, outsourced code development, data storage, and cloud-based vs. on-premises risks

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

Vulnerability Classification (Cont'd)

Vulnerability Type	Description
Default Installations/Default Configurations	• Failing to change the default settings while deploying software or hardware allows the attacker to **guess the settings** to break into the system
Operating System Flaws	• Owing to OS vulnerabilities, applications such as **Trojans**, **worms**, and **viruses** pose threats
Default Passwords	• Manufacturers provide users with default passwords to **access the device** during its initial set-up, which users must change for future use • When users **forget to update the passwords** and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute-force and dictionary attacks
Zero-Day Vulnerabilities	• These are unknown vulnerabilities in software/hardware that are **exposed but not yet patched** • These vulnerabilities are exploited by the attackers before being acknowledged and patched by the software developers or security analysts
Legacy Platform Vulnerabilities	• Legacy platform vulnerabilities are caused by **obsolete** or **familiar code** • Legacy platforms are usually **not supported** when patching technical assets such as smartphones, computers, IoT devices, OSes, applications, databases, firewalls, IDSes, or other network components • This type of vulnerabilities can cause costly data breaches for organizations
System Sprawl/Undocumented Assets	• The system sprawl vulnerability arises within an organizational network because of an **increased number of system or server connections** without proper documentation or an understanding of their maintenance • These assets are often neglected over time, making them susceptible to attacks
Improper Certificate and Key Management	• Improper certificate and key management may lead to many vulnerabilities that allow attackers to perform **password cracking** and **data exfiltration** attacks • Storing or retaining legacy or **outdated keys** also poses major threats to organizations

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

Vulnerability Classification

Vulnerabilities present in a system or network are classified into the following categories:

Misconfigurations/Weak Configurations

Misconfiguration is the most common vulnerability and is mainly caused by human error. It allows attackers to break into a network and gain unauthorized access to systems. Misconfigurations may occur both intentionally and unintentionally, and they affect web

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

servers, application platforms, databases, and networks. Attackers can detect misconfigurations through various scanning techniques and then exploit backend systems. Therefore, administrators must change the default configuration of devices and optimize device security.

- **Network Misconfigurations**

  Frequent changes to network and security devices are inevitable and essential for business improvement. However, administrators should ensure that all network components are configured appropriately because any loops in the implemented changes can cause adverse effects on the network such as performance degradation, service outage, and network intrusions. The following are some examples of weak network configurations.

  - **Insecure Protocols**

    Insecure protocols transmit information or data in plaintext without implementing any encryption techniques to secure the data. The use of vulnerable protocols causes authentication and integrity issues because attackers can leverage the unencrypted files or data transmission and tamper with the data in transit. Attackers can also gain remote access to the vulnerable system once they capture the credentials being shared in plaintext. This vulnerability can be avoided by removing devices operating on insecure protocols and deploying a centralized master node to update protocols.

  - **Open Ports and Services**

    User communications with an application or service can be achieved through TCP or UDP port numbers, which accept and transmit the information in the form of packets. The source and destination addresses can be identified through the unique IP addresses assigned to them. In addition to these, many ports operate in a network for specific services. Servers often operate with some open ports, but all open ports are not dangerous, unless they are misconfigured, unpatched, or implemented with poor security rules. However, the open ports must be limited and used only for important services. Leaving ports open for unnecessary services can invite new threats to the network. Open ports and services may lead to the loss of data or Denial-of-Service (DoS) attacks and allow attackers to perform further attacks on other connected devices. Administrators must continuously check for unnecessary or insecure ports and services to reduce the risk to the network.

  - **Errors**

    Improper configuration of applications or services can generate error reports while loading pages. Such error reports can provide detailed information to attackers searching for security flaws, application vulnerabilities, programming faults, or other exploits. Using outdated software can also generate security errors, which can be susceptible to remote attacks using techniques such as code injection to manipulate the application. To prevent this vulnerability, skilled programming practices need to

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

be adopted in such a manner that the application does not disclose critical information that could help attackers exploit the application server.

- **Weak Encryption**

  Implementing proper encryption methods can secure the data being transmitted across a network and the data saved on storage devices. The encrypted files can be accessed only with the corresponding decrypted key held by the client or application. Weak encryption can allow attackers to perform man-in-the-middle attacks, sniff the traffic to modify data, and then masquerade as the legitimate service to communicate with the end users with false information. The following are some causes of weak encryption:

  - Using a weak encryption algorithm
  - Key generation with guessable credentials
  - Insecure key distribution

- **Host Misconfigurations**

  Attackers can exploit configuration flaws in the host server to manipulate the resources and gain remote administrator access. The debugging functions could be activated, and unknown users may gain administrative permissions. These vulnerabilities may allow attackers to evade authentication mechanisms and access critical information, possibly with elevated privileges. The following are some examples of weak host configuration.

  - **Open Permissions**

    Granting unnecessary permissions to a user or group of users to access applications or files can lead to security issues such as data leakage or corruption of system functionality. Managing permissions is a complicated task, where administrators or users can potentially make mistakes such as allowing unknown guests to read and write critical files. An attacker can also perform privilege escalation by using unnecessarily created accounts to access unprotected files or to run commands on the operating system (OS).

  - **Unsecured Root Accounts**

    Using manufacturer-allotted default administrative account credentials for the database or applications can lead to system security issues. Failing to implement a secure password privacy policy can allow attackers to guess the credentials using different brute-force techniques.

Application Flaws

Application flaws are vulnerabilities in applications that are exploited by attackers. Applications should be secured using the validation and authorization of the user. Flawed applications pose security threats such as data tampering and unauthorized access to configuration stores. If applications are not secured, sensitive information may be lost or corrupted. Hence, developers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

must understand the anatomy of common security vulnerabilities and develop highly secure applications by providing proper user validation and authorization.

The following are some of the application flaws that can be exploited by attackers.

- **Buffer Overflows**

  Buffer overflows are common software vulnerabilities resulting from coding errors that allow attackers to gain access to the target system. In a buffer overflow attack, the attacker undermines the functioning of programs and attempts to take control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause of this vulnerability. The buffer cannot handle data beyond its limit, causing the flow of data to adjacent memory locations and overwriting their data values. When a buffer overflow occurs, systems often crash, become unstable, or show erratic program behavior.

- **Memory Leaks**

  A memory leak or resource leak is an unintended class of memory consumption that occurs when a programmer fails to erase an assigned block of memory when no longer required. It is caused by exceptional circumstances, flaw conditions, and uncertainty over which portion of code is responsible for freeing memory. These conditions depend on application consequences in cases such as such as short-lived user-land applications, long-lived user-land applications, and kernel-land processes. A memory leak results in software reliability–related concerns and encourages a malicious actor to take control over the compromised system to perform attacks such as DoS to crash the system, inject malicious code to change application behavior, and hijack the program's control flow. Tools such as Valgrind, which is compatible with the Unix/Linux environment, track memory leaks and display the status of the software environment.

- **Resource Exhaustion**

  A resource exhaustion attack damages the server by sending multiple resource requests from different locations to exploit software bugs or errors, thereby hanging the system and server or causing a system crash. In software applications, memory management has an error of memory leaks that can be exploited easily by remote attackers. It is similar to a DoS attack in that it can compromise or exhaust the resources available for a system in the network. Owing to design or code errors, any interaction or connection established between the client and server can waste resources or consume more resources than required.

- **Integer Overflows**

  An integer overflow occurs when an arithmetic function generates and attempts to store an integer value larger than the maximum value that the allocated memory space can store. These overflow conditions may lead to undesirable behavior of the software. Failure to discover an overflow condition beforehand can cause security and reliability issues in the program. Alongside yielding inaccurate results and causing software instability, integer overflows can also lead to buffer overflows and open doors for

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

attackers to manipulate values, eventually leading to random or malicious code execution.

- **Null Pointer/Object Dereference**

  Also known as a null reference, a null pointer is a value stored to represent that the pointer is not designated to any valid object; it also indicates invalid memory location. The majority of null-pointer issues lead to common software reliability issues, but once an attacker deliberately triggers a null-pointer dereference, they might be able to use the resulting exception to evade the security logic and make the application disclose debugging details that can help in devising strategies for subsequent attacks. Programs generally utilize these null pointers to indicate a condition such as the last point of unspecified length and incompetence to perform some operations; this type of null-pointer usage is comparable to the nullable types and no value in the option type. A null-pointer dereference can prevent a program from execution or crash the program and cause it to exit.

- **DLL Injection**

  When an application runs third-party code or untrusted code that loads an assembly or DLL file, an attacker may exploit this vulnerability to inject a malicious DLL into the current running process and execute malicious code. Furthermore, loading DLL files without specifying the complete path of the file location may allow attackers to create a malicious DLL and place it in a location that precedes the path of the legitimate DLL file. Consequently, the application executes the malicious DLL. To prevent such vulnerabilities, programmers must never load untrusted DLLs from user input and must always invoke DLLs by specifying the full path of the file location.

- **Race Conditions**

  A race condition is an undesirable incident that occurs when a software or system program depends on the execution of processes in a sequence and on the timing of the programs. This condition occurs when a system that handles events in a sequential format is coerced to perform multiple operations simultaneously. The condition results in the improper execution of a program or software bugs. A typical race condition occurs when multiple threads depend on a shared resource. Most race conditions impact the security associated with the system. An attacker can perform DoS or privilege escalation attacks by accessing the shared resource of a trusted process.

  - **Time of Check/Time of Use**

    The time of check or time of use (TOC/TOU) is a software error that occurs because of the race condition that occurs after checking the state of particular segment of the system at a specific time and before the time of using the checking results. In simple terms, it is defined as the change in system state from the time of checking for a prediction to the time of acting on the prediction. It is a timing vulnerability that occurs when the system grants access permission to a resource request. For example, when a user wishes to transfer an amount from one account to another, a

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

risk of an attack exists in the middle of the transaction between the TOC and TOU, i.e., from the time of checking whether the required amount is available to the time of transferring that amount.

- **Improper Input Handling**

  Input handling is defined as the verification of application functionalities such as validation, filtering, sanitizing, encryption, and decryption of input data. Failure in verifying the input data results in vulnerabilities. Input validation is mandatory to ensure the integrity of incoming data by checking and comparing the data with the type of expected data. Data originating from both trusted and untrusted sources have the risk of being corrupted by attackers using techniques such as SQL injection, cross-site scripting, and buffer overflow. Implementing both client-side and server-side validation ensures effective data authentication.

- **Improper Error Handling**

  Improper error handling occurs when an attacker exploits the security system by utilizing error information. Most web applications or servers disclose detailed information about errors such as database dumps and stack traces. They can also generate detailed errors that include information about the system condition such as system call failure, timeouts, exceptions, and data availability, which can help an attacker analyze and attack the system. Fail-open is one of the security issues caused by improper error handling. Fail-open is defined as the granting of access after a system has failed or denied access.

Poor Patch Management

A patch is a small piece of software designed to fix problems, security vulnerabilities, and bugs as well as improve the usability or performance of a computer program or its supporting data. Software vendors provide patches that prevent exploitations and reduce the probability of threats exploiting a specific vulnerability. Unpatched software can make an application, server, or device vulnerable to various attacks. The following are some examples of poor patch management.

- **Unpatched Servers**

  Servers are an essential component of the infrastructure of any organization. There have been several cases where organizations ran unpatched and misconfigured servers that compromised the security and integrity of the data in their system. Hackers search for these vulnerabilities in servers and exploit them. These unpatched servers serve as a hub for attackers or an entry point into the network. This can lead to the exposure of private data, financial loss, and discontinuation of operations. Updating software regularly and maintaining systems properly by patching and fixing bugs can help in mitigating the vulnerabilities caused by unpatched servers.

- **Unpatched Firmware**

  Unpatched firmware may lead to vulnerabilities through which an attacker can easily enter a corporate network and steal critical information or damage critical resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Firmware vulnerabilities allow attackers to inject malicious code, infect legitimate updates, delete data stored on the hard drive, or even control the system hardware from a remote location in some cases. To mitigate such vulnerabilities, security professionals must regularly check and update the firmware.

- **Unpatched OS**

  Attackers use systems having unpatched OSes as the origin of an infection vector to infect other systems or devices connected to the same network. Attackers scan for systems having unpatched OSes and use those systems for spreading malware to other systems connected to the network. If an attacker identifies a vulnerability in an OS kernel file or shared library, they can exploit this vulnerability in an attempt to perform privilege escalation using malware that gains system- or root-level access. Security professionals must enable the auto-update feature to update OSes automatically and regularly.

- **Unpatched Applications**

  Unpatched application vulnerabilities allow attackers to inject and run malicious code by exploiting a known software bug. Generally, no software or applications are flawless. Software vendors frequently release patches to resolve identified vulnerabilities. Unpatched applications pave the way for attackers to exploit and compromise the security of systems and software. Therefore, it is important for organizations to apply vulnerability patches and upgrade applications on a regular basis.

Design Flaws

Vulnerabilities due to design flaws are universal to all operating devices and systems. Design vulnerabilities such as incorrect encryption or the poor validation of data refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.

Third-Party Risks

A third party can become another potential threat to enterprises. Third-party services or products can have access to privileged systems and applications, through which financial information, customer and employee data, and processes in the enterprise's supply chain can be compromised. The third party may be trustworthy, but enterprises usually do not check if they maintain appropriate standards and security measures; eventually, they can become a threat for the enterprise network. Major third-party risks include identity theft, intellectual property theft, data breaches, implantation of file-less malware, and network intrusions. An organization should be aware of third-party risks and run real-time, continuous risk management processes within the environment. The following are different types of risks associated with third-party dependency.

- **Vendor management:** It is the activity of selecting suppliers and assessing the risks of third-party services and products. It includes all the essential programs and processes required for an organization to handle and manage operations and communications with its third-party vendors. Organizations often depend on third-party vendors to save

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

expenses, fend off market rivalry, increase productivity, and gain higher profits with lower effort. However, if the third-party vendor is not trusted or fails to follow the required standards, it can pose risks to the organization's data or information. The organization may need to face all the consequences in case of a breach. The best approach to discover risks associated with the third party include employing best vendor management practices alongside enforcing third-party vendor risk management systems.

- **System integration**: It is a process of employing third-party services or hiring third-party vendors to run business operations. When a third party hosts the services or performs software development for the company, the system integrators need full access to the systems/application. As the integrators work from inside the company, they can easily evade firewalls and security solutions and install malware or spyware in the network. The integrators can also employ port scanning techniques to obtain data packets directly from the network. Organizations need to oversee the operations of third-party vendors and the progress of projects.
- **Lack of vendor support**: Organizations often depend on third-party vendors to manage the security of systems inside a network. In such cases, the vendors are entrusted with discovering and fixing issues before they get exploited, and they become members within the working environment of the organization. As they deal with complex network infrastructure, insufficient knowledge in handling security systems or identifying risks can open avenues for new cyber-attacks. Vendors should be adept in finding issues and should be encouraged to maintain a high quality of work and keep systems secure and updated.

- **Supply-chain risks**: The majority of network devices and systems in an organization are often purchased from a third party. The use of such equipment in each segment along the supply chain can potentially pose security risks due to improper maintenance or configuration. Proper security controls must be implemented for the equipment/devices or software that organizations purchase or borrow from a third party. For instance, the software or hardware purchased from a third party may not be properly sanitized. In such cases, malware concealed inside the previously provisioned equipment can infect the new systems deployed in the organization and spread to all other devices connected to the network.
- **Outsourced code development**: In some cases, enterprises do not have all the resources required for developing products inside their environment. In such cases, organizations hire contract-based third parties to develop products or software. In such cases, organizations should establish a secure environment for the third-party designers to develop and assess the code being built. Organizations should also determine where the code needs to be stored and place appropriate security controls to the storage space because the code can be stolen to develop similar projects. After the coding process is completed, the product requires thorough testing, and developers should ensure that unauthorized access to the application resources is prevented. It is also important to ensure that resources being accessed by the application are stored in a

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

protected environment and that data are encrypted before being transmitted over the network.

- **Data storage**: With the emergence of cloud technology, organizations are storing large amounts of data in third-party storage spaces, where vendors may also have access to organizations' data. Therefore, the data should be frequently inspected for security concerns to protect sensitive information related to customers, employees, or users. Organizations should insist that appropriate security controls be implemented and integrity be maintained for the data stored in the third-party storage. Data transmission should be performed with encryption and through a secure channel.
- **Cloud-based vs. on-premises risks:** As organizations are migrating their business infrastructure to cloud environments, storage and data exposure issues often arise in third-party storage locations. On the other hand, businesses running in an on-premises environment may also have issues such as weak security configurations, application or software vulnerabilities, and vendor issues that can emerge from network devices such as firewalls, switches, and routers, which are placed within the organization's infrastructure. Proper configuration and encryption are the main solutions for both environments. In the context of cloud security, the cloud provider has the sole responsibility of securing the cloud; however, the client should also be aware of the best practices to use cloud services in a secure manner.

Default Installations/Default Configurations

Default installations are usually user-friendly — especially when the device is being used for the first time when the primary concern is the usability of the device rather than the device's security. In some cases, infected devices may not contain any valuable information, but are connected to networks or systems that have confidential information that would result in a data breach. Failing to change the default settings while deploying the software or hardware allows the attacker to guess the settings to break into the system.

Systems or devices with default configurations, if connected to the production or corporate network, enable attackers to perform advanced persistent attacks. These systems allow attackers to gain information about the target OS and other vulnerabilities existing in the target network. Based on the identified vulnerabilities, attackers may perform further attacks. When connecting a system or device to a network, it is important to disable unnecessary components and services associated with the default configuration.

Operating System Flaws

Due to vulnerabilities in the operating systems, applications such as Trojans, worms, and viruses pose threats. These attacks use malicious code, script, or unwanted software, which results in the loss of sensitive information and control of computer operations. Timely patching of the OS, installing minimal software applications, and using applications with firewall capabilities are essential steps that an administrator must take to protect the OS from attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Default Passwords

Manufacturers provide users with default passwords to access the device during its initial set-up, which users must change for future use. When users forget to update the passwords and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute force and dictionary attacks. Attackers exploit this vulnerability to obtain access to the system. Passwords should be kept confidential; failing to protect the confidentiality of a password allows the system to be easily compromised.

Zero-Day Vulnerabilities

Zero-day vulnerabilities are unknown vulnerabilities in software/hardware that are exposed but not yet patched. These Vulnerabilities are exploited by the attackers before being acknowledged and patched by the software developers or security analysts. Zero-day vulnerabilities are one of the major cyber-threats that continuously expose the vulnerable systems until they get patched.

Legacy Platform Vulnerabilities

Legacy platform vulnerabilities are caused by obsolete or familiar codes. Legacy platforms are usually not supported when patching technical assets such as smartphones, computers, IoT devices, OSes, applications, databases, firewalls, intrusion detection systems (IDSs), or other network components. This type of vulnerabilities could cause costly data breaches for organizations. Legacy systems can be secured using other security controls, rather than by fixing them. Another possible solution is to segregate these systems from the network so that attackers cannot gain physical access to them.

System Sprawl/Undocumented Assets

The system sprawl vulnerability arises within an organization network because of an increased number of system or server connections without proper documentation or the understanding of their maintenance. These assets are often neglected over time, making them susceptible to attacks. It could also lead to expensive maintenance because each vulnerable asset will be included in the maintenance cost each time effective maintenance is required or the latest hardware or software upgrades need to be scheduled. Additionally, undocumented assets do not support multiplexed database backups or quick multi-streaming, thereby forcing IT teams to choose between fast backups and capacity optimization.

Improper Certificate and Key Management

Improper certificate and key management may lead to many vulnerabilities that allow attackers to perform password cracking and data exfiltration attacks. Keys stored on servers are vulnerable to attacks. Security professionals need to ensure that keys are stored in an encrypted format and are decrypted only in a protected secure environment. Storing or retaining legacy or outdated keys also poses major threats to organizations. Private keys used with certificates must be stored in a highly secured environment; otherwise, an unauthorized individual can intercept the keys and gain access to confidential data or critical systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Types of Vulnerability Assessment

Assessment Type	Description
Active Assessment	Uses a **network scanner** to find hosts, services, and vulnerabilities
Passive Assessment	Used to **sniff the network traffic** to discover present active systems, network services, applications, and vulnerabilities present
External Assessment	**Assesses the network** from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world
Internal Assessment	Scans the **internal infrastructure** to discover exploits and vulnerabilities
Host-based Assessment	Conducts a **configuration-level check** to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise
Network-based Assessment	Determines possible **network security attacks** that may occur on the organization's system
Application Assessment	Tests and analyzes all elements of the **web infrastructure** for any **misconfiguration**, **outdated content**, or **known vulnerabilities**

Assessment Type	Description
Database Assessment	Focuses on testing databases, such as **MYSQL**, **MSSQL**, **ORACLE**, **POSTGRESQL**, etc., for the presence of **data exposure** or **injection** type vulnerabilities
Wireless Network Assessment	Determines the vulnerabilities in the organization's **wireless networks**
Distributed Assessment	Assesses the **distributed organization assets**, such as client and server applications, simultaneously through appropriate synchronization techniques
Credentialed Assessment	Assesses the network by **obtaining the credentials** of all machines present in the network
Non-Credentialed Assessment	Assesses the network without acquiring **any credentials** of the assets present in the enterprise network
Manual Assessment	In this type of assessment, the ethical hacker **manually** assesses the **vulnerabilities**, **vulnerability ranking**, **vulnerability score**, etc.
Automated Assessment	In this type of assessment, the ethical hacker employs various **vulnerability assessment tools**, such as **Nessus**, **Qualys**, **GFI LanGuard**, etc.

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

Types of Vulnerability Assessment

Given below are the different types of vulnerability assessments:

- **Active Assessment**

  A type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network. Active network scanners can reduce the intrusiveness of the checks they perform.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

- **External Assessment**

  External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall.

  The following are some of the possible steps in performing an external assessment:

  - Determine a set of rules for firewall and router configurations for the external network
  - Check whether the external server devices and network devices are mapped
  - Identify open ports and related services on the external network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Examine the patch levels on the server and external network devices
- Review detection systems such as IDS, firewalls, and application-layer protection systems
- Get information on DNS zones
- Scan the external network through a variety of proprietary tools available on the Internet
- Examine Web applications such as e-commerce and shopping cart software for vulnerabilities

- **Internal Assessment**

  An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some of the possible steps in performing an internal assessment:

  - Specify the open ports and related services on network devices, servers, and systems
  - Check the router configurations and firewall rule sets
  - List the internal vulnerabilities of the operating system and server
  - Scan for any trojans that may be present in the internal environment
  - Check the patch levels on the organization's internal network devices, servers, and systems
  - Check for the existence of malware, spyware, and virus activity and document them
  - Evaluate the physical security
  - Identify and review the remote management process and events
  - Assess the file-sharing mechanisms (for example, NFS and SMB/CIFS shares)
  - Examine the antivirus implementation and events

- **Host-based Assessment**

  Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.

- **Network-based Assessment**

  Network assessments determine the possible network security attacks that may occur on an organization's system. These assessments discover network resources and map the ports and services running to various areas on the network. It evaluates the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewalls and network scanners, such as Nessus. These scanners identify open ports, recognize the services running on those ports, and detect vulnerabilities associated with these services. These assessments help organizations identify points of entry and attack into a network since they follow the path and approach of the hacker. They help organizations determine how systems are vulnerable to Internet and intranet attacks, and how an attacker can gain access to important information. A typical network assessment conducts the following tests on a network:

- Checks the network topologies for inappropriate firewall configuration
- Examines the router filtering rules
- Identifies inappropriately configured database servers
- Tests individual services and protocols such as HTTP, SNMP, and FTP
- Reviews HTML source code for unnecessary information
- Performs bounds checking on variables

- **Application Assessment**

  An application assessment focuses on transactional Web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the webserver infrastructure for any misconfiguration, outdated content, or known vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Database Assessment**

  A database assessment is any assessment focused on testing the databases for the presence of any misconfiguration or known vulnerabilities. These assessments mainly concentrate on testing various database technologies like MYSQL, MSSQL, ORACLE, and POSTGRESQL to identify data exposure or injection type vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Wireless Network Assessment**

  Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Distributed Assessment**

  This type of assessment, employed by organizations that possess assets like servers and clients at different locations, involves simultaneously assessing the distributed organization assets, such as client and server applications, using appropriate synchronization techniques. Synchronization plays a critical role in this type of assessment. By synchronizing the test runs together, all the separate assets situated at multiple locations can be tested at the same time.

- **Credentialed Assessment**

  Credentialed assessment is also called authenticated assessment. In this type of assessment, the ethical hacker possesses the credentials of all machines present in the assessed network. The chances of finding vulnerabilities related to operating systems and applications are higher in credential assessment than in non-credential assessment. This type of assessment is challenging since it is highly unclear who owns particular assets in large enterprises, and even when the ethical hacker identifies the actual owners of the assets, accessing the credentials of these assets is highly tricky since the asset owners generally do not share such confidential information. Also, even if the ethical hacker successfully acquires all required credentials, maintaining the password list is a huge task since there can be issues with things like changed passwords, typing errors, and administrative privileges. Although it is the best way of assessing a target enterprise network for vulnerabilities and is highly reliable, it is a complex assessment that is challenging.

- **Non-Credentialed Assessment**

  Non-credentialed assessment, also called unauthenticated assessment, provides a quick overview of weaknesses by analyzing the network services that are exposed by the host. Since it is a non-credential assessment, an ethical hacker does not require any credentials for the assets to perform their assessments. This type of assessment generates a brief report regarding vulnerabilities; however, it is not reliable because it does not provide deeper insight into the OS and application vulnerabilities that are not exposed by the host to the network. This assessment is also incapable of detecting the vulnerabilities that are potentially covered by firewalls. It is prone to false-positive outputs and is not reliably effective as compared to credential-based assessment.

- **Manual Assessment**

  After performing footprinting and network scanning and obtaining crucial information, if the ethical hacker performs manual research for exploring the vulnerabilities or weaknesses, they manually rank the vulnerabilities and score them by referring to vulnerability scoring standards like CVSS and vulnerability databases like CVE and CWE. Such assessment is considered to be manual.

- **Automated Assessment**

  An assessment where an ethical hacker uses vulnerability assessment tools such as Nessus Professional, Qualys, or GFI LanGuard to perform a vulnerability assessment of

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

the target is called an automated assessment. Unlike manual assessments, in this type of assessment, the ethical hacker does not perform footprinting and network scanning. They employ automated tools that can perform all such activities and are also capable of identifying weaknesses and CVSS scores, acquiring critical CVE/CWE information related to the vulnerability, and suggesting remediation strategies.

- **Cloud-based Assessment**

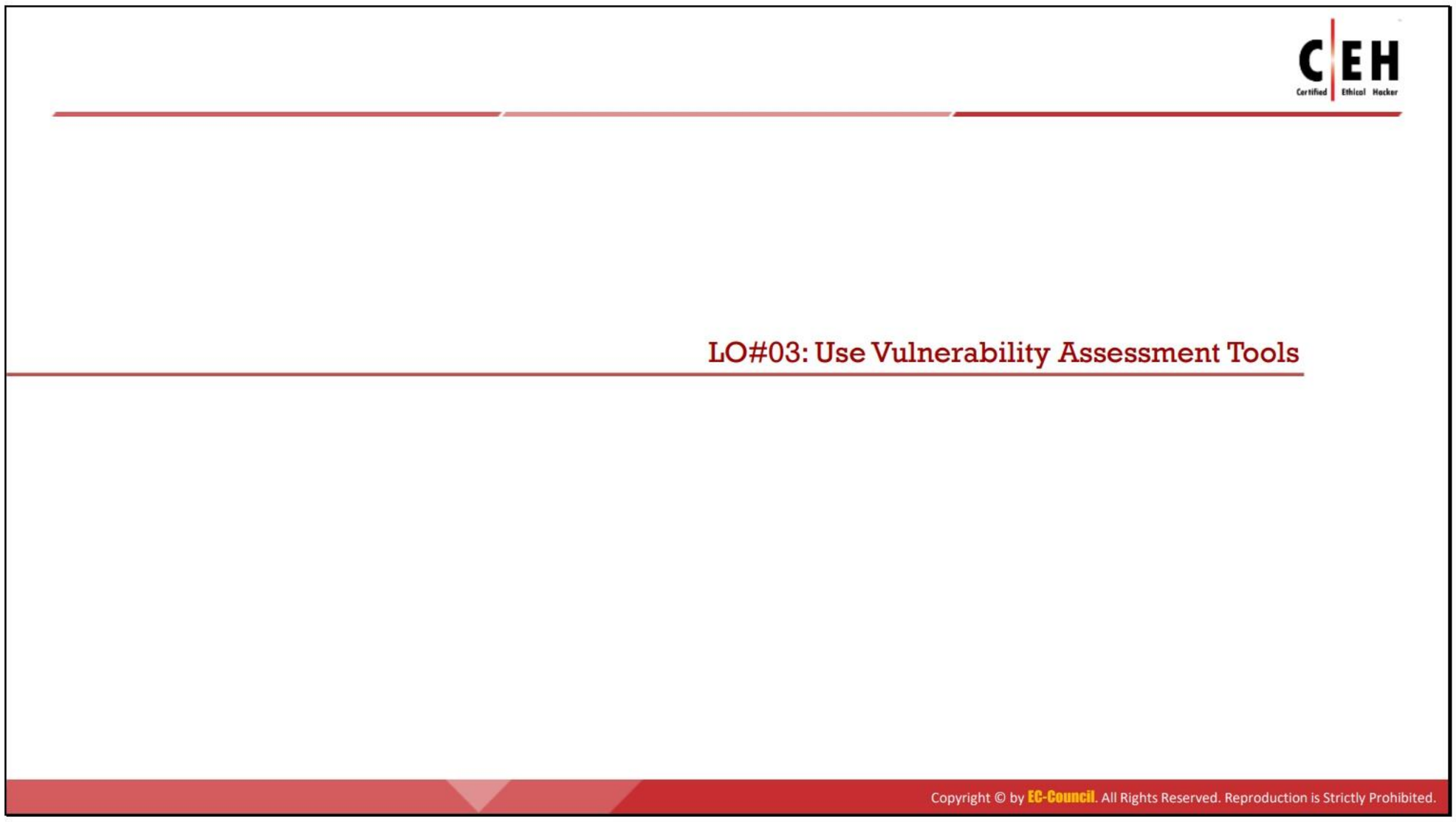
  This type of assessment focuses on evaluating overall security of the cloud infrastructure according to the cloud service provider's best practices or guidelines. This assessment involves identifying cloud infrastructure vulnerabilities and mitigating them through access control mechanisms and proper security measures complying with the standards. This type of assessment is frequently performed to identify the risks associated with the assets deployed over the cloud. It also assists security professionals to detect weak entry points on the cloud, through which the attackers can make their way into the organization's network.

- **Mobile Application Assessment**

  Mobile application assessment aims at protecting the privacy of data across mobile applications and APIs. It is a must-have security practice for every organization that hosts publicly accessible applications. This type of assessment involves examining source code and internal security controls of mobile applications. Security professionals need to perform this type of assessment to evaluate and improve the overall application's strength against known and future threats to protect sensitive data. An effective assessment can minimize risks and assists in incorporating appropriate security controls to increase the safety of mobile applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Vulnerability Assessment Tools

Vulnerability assessment solutions are important tools for information security management as they identify all potential security weaknesses before an attacker can exploit them. There are different approaches and solutions available to perform a vulnerability assessment. Selecting an appropriate assessment approach plays a major role in mitigating the threats that an organization faces.

This section outlines the various approaches, solutions, and tools used to perform a vulnerability assessment.

Comparing Approaches to Vulnerability Assessment

There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and inference-based assessment.

- **Product-Based Solutions**

  Product-based solutions are installed in the organization's internal network. They are installed either on a private or non-routable space or in the Internet-addressable portion of an organization's network. If they are installed on a private network (behind the firewall), they cannot always detect outside attacks.

- **Service-Based Solutions**

  Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can audit the network from the outside.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Tree-Based Assessment**

  In a tree-based assessment, the auditor selects different strategies for each machine or component of the information system. For example, the administrator selects a scanner for servers running Windows, databases, and web services but uses a different scanner for Linux servers. This approach relies on the administrator to provide a starting piece of intelligence, and then to start scanning continuously without incorporating any information found at the time of scanning.

- **Inference-Based Assessment**

  In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

Characteristics of a Good Vulnerability Assessment Solution

Organizations need to select a proper and suitable vulnerability assessment solution to detect, assess, and protect their critical IT assets from various internal and external threats.

The characteristics of a good vulnerability assessment solution are as follows:

- Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
- Uses a well-organized inference-based approach for testing
- Automatically scans and checks against continuously updated databases
- Creates brief, actionable, customizable reports, including reports of vulnerabilities by severity level, and trend analysis
- Supports multiple networks
- Suggests appropriate remedies and workarounds to correct vulnerabilities
- Imitates the outside view of attackers to gain its objective

Working of Vulnerability Scanning Solutions

Any organization needs to handle and process large volumes of data to conduct business. These large volumes of data contain privileged information of that particular organization. Attackers try to identify vulnerabilities that they can exploit, and then use these to gain access to critical data for illegal purposes. Vulnerability analysis analyzes and detects risk-prone areas in the organizational network. This analysis uses various tools and reports on the vulnerabilities present in the network.

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

- **Locating nodes**: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Performing service and OS discovery on them**: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services along with the operating system on the target systems.
- **Testing those services and OS for known vulnerabilities**: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

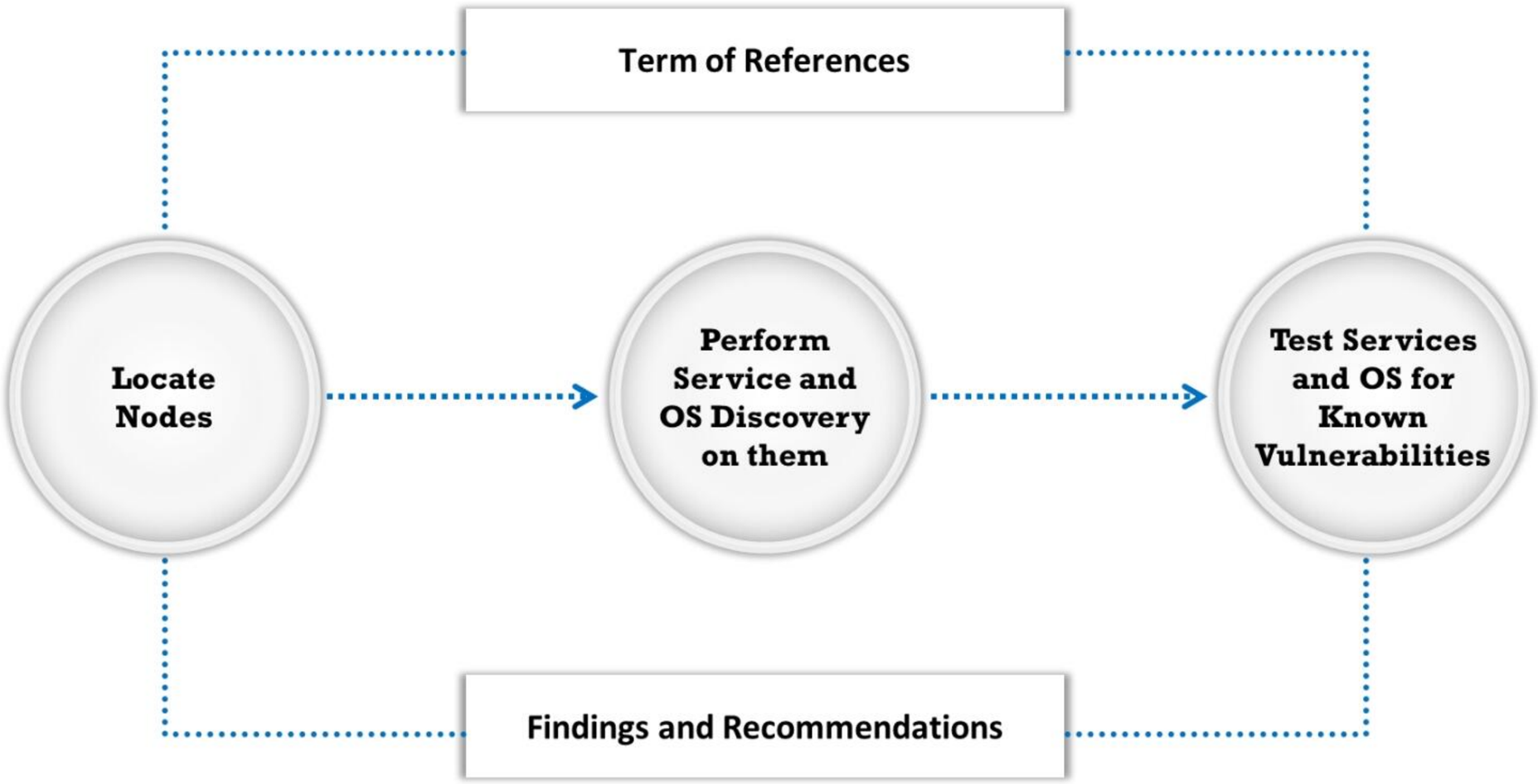


Figure 5.6: The working of vulnerability scanning solutions

Types of Vulnerability Assessment Tools

There are six types of vulnerability assessment tools: host-based vulnerability assessment tools, application-layer vulnerability assessment tools, depth assessment tools, scope assessment tools, active and passive tools, and location and data-examination tools.

- **Host-Based Vulnerability Assessment Tools**

  The host-based scanning tools are appropriate for servers that run various applications, such as the Web, critical files, databases, directories, and remote accesses. These host-based scanners can detect high levels of vulnerabilities and provide required information about the fixes (patches). A host-based vulnerability assessment tool identifies the OS running on a particular host computer and tests it for known deficiencies. It also searches for common applications and services.

- **Depth Assessment Tools**

  Depth assessment tools are used to discover and identify previously unknown vulnerabilities in a system. Generally, tools such as fuzzers, which provide arbitrary input to a system's interface, are used to identify vulnerabilities to an unstable depth. Many of these tools use a set of vulnerability signatures to test whether a product is resistant to a known vulnerability or not.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Application-Layer Vulnerability Assessment Tools**

  Application-layer vulnerability assessment tools are designed to serve the needs of all kinds of operating system types and applications. Various resources pose a variety of security threats and are identified by the tools designed for that purpose. Observing system vulnerabilities through the Internet using an external router, firewall, or webserver is called an external vulnerability assessment. These vulnerabilities could be external DoS/DDoS threats, network data interception, or other issues. The analyst performs a vulnerability assessment and notes vulnerable resources. The network vulnerability information is updated regularly into the tools. Application-layer vulnerability assessment tools are directed towards web servers or databases.

- **Scope Assessment Tools**

  Scope assessment tools provide an assessment of the security by testing vulnerabilities in the applications and operating system. These tools provide standard controls and a reporting interface that allows the user to select a suitable scan. These tools generate a standard report based on the information found. Some assessment tools are designed to test a specific application or application type for vulnerability.

- **Active and Passive Tools**

  Active scanners perform vulnerability checks on the network functions that consume resources on the network. The main advantage of the active scanner is that the system administrator or IT manager has good control of the timing and the parameters of vulnerability scans. This scanner cannot be used for critical operating systems because it uses system resources that affect the processing of other tasks.

  Passive scanners are those that do not considerably affect system resources, as they only observe system data and perform data processing on a separate analysis machine. A passive scanner first receives system data that provide complete information on the processes that are running and then assesses that data against a set of rules.

- **Location and Data Examination Tools**

  Listed below are some of the location and data examination tools:

  - **Network-Based Scanner:** Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
  - **Agent-Based Scanner:** Agent-based scanners reside on a single machine but can scan several machines on the same network.
  - **Proxy Scanner:** Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
  - **Cluster scanner:** Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Choosing a Vulnerability Assessment Tool

Vendor-designed vulnerability assessment tools can be used to test a host or application for vulnerabilities. There are several available vulnerability assessment tools that include port scanners, vulnerability scanners, and OS vulnerability assessment scanners. Organizations must choose appropriate tools based on their test requirements.

Choose the tools that best satisfy the following requirements:

- Tools must be capable of testing anywhere from dozens to 30,000 different vulnerabilities, depending on the product
- The selected tool should have a sound database of vulnerabilities and frequently updated attack signatures
- Pick a tool that matches the environment and expertise
- Make sure to regularly update the scan engine to ensure the tool is aware of the latest known vulnerabilities
- Verify that the chosen vulnerability assessment tool has accurate network mapping, application mapping, and penetration tests. Not all tools can find the protocols running and analyze a network's performance.
- Ensure that the tool has several regularly updated vulnerability scripts for the platforms you are scanning
- Make sure that any patches are applied; failing to do so might lead to false positives
- Find out how many reports are returned, what information they contain, and whether they are exportable
- Check whether the tool has different levels of penetration to stop lockups
- The maintenance costs of tools can be offset by effectively using them
- Ensure that the vulnerability assessment tool can run its scans quickly and accurately
- Ensure that the tool can perform scans using multiple protocols
- Verify that the tool can understand and analyze the network topology to perform the assessment
- Bandwidth limitations are a major concern when dealing with large networks. Ensure the vulnerability assessment tool has high bandwidth allocation
- Ensure that the vulnerability assessment tool possess excellent query throttling features
- Ensure that the tool can also assess fragile systems and non-traditional assets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Criteria for Choosing a Vulnerability Assessment Tool

The criteria to follow when choosing or purchasing any vulnerability assessment tool are as follows:

- **Types of vulnerabilities being assessed**: The most important information at the time of evaluating any tool is to find out how many types of vulnerabilities it will discover.
- **Testing capability of scanning**: The vulnerability assessment tool must have the capacity to execute the entire selected test and must scan all the systems selected for scanning.
- **Ability to provide accurate reports**: The ability to prepare an accurate report is essential. Vulnerability reports should be short, clear, and should provide an easy method to mitigate the discovered vulnerability.
- **Efficient and accurate scanning**: Two essential aspects of scanner performance are how much time it takes for a single host and what resources are required, and the loss of services at the time of scanning. It is important to ensure accuracy and to be aware of the accuracy of the results.
- **Capability to perform a smart search**: How clever they are at the time of scanning is also a key factor in judging any vulnerability assessment tool.
- **Functionality for writing its own tests**: When a signature is not present for a recently found vulnerability, it is helpful if the vulnerability scanning tool allows the use of user-developed tests.
- **Test run scheduling**: It is important to be able to do test-run scheduling as it allows users to perform scanning when traffic on the network is light.

Best Practices for Selecting Vulnerability Assessment Tools

Some of the best practices that can be adopted for selecting vulnerability assessment tools are:

- Vulnerability assessment tools are used to secure and protect the organization's system or network. Ensure that they do not damage the network or system while running.
- Before using any vulnerability assessment tools, it is important to understand their function and to decide what information is needed before starting
- Security mechanisms for accessing from within and from outside the network are somewhat different, so decide the location for the scan based on the desired information
- At the time of scanning, enable logging and ensure that all outcomes and methodologies are annotated every time a scan is performed on any computer
- Users should frequently scan their systems for vulnerabilities and regularly monitor them for vulnerabilities and exploits

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Vulnerability Assessment Tools: Qualys Vulnerability Management

- A cloud-based service that offers immediate global visibility into IT system areas that might be **vulnerable to the latest Internet threats** and how to protect them
- Aids in the continuous **identification of threats and monitoring of unexpected changes** in a network before they become breaches

Qualys.

Qualys

Vulnerability Scorecard Report December 25

Vulnerability Scorecard Report_system_PO_displayedAll
Source Business Unit
Operating System All

Print Download

Results

Vulnerability Distribution by Severity Level



Level 5 37,210 65%
Level 4 58,268 38%
Level 3 47,317 21%
Level 2 17,768 18%
Level 1 2,413 5%

Vulnerability Distribution by Type



Confirmed 37,210 76%
Potential 58,268 24%

Asset Groups		Severities by Levels					Vulnerability Type			Hosts w/Vuln Levels 5,4,3		Vulnerability Status				Vulnerability Age by Days		
Title	Hosts	Level 5	Level 4	Level 3	Level 2	Level 1	Confirmed	Potential	IG	Total	%	New	Active	Fixed	ReOpen	> 30	> 60	> 90
The subnet	73	1783	1880	1783	1783	1783	7986	777	777	112	89%	80	80	80	80	0	0	8763
RSA Demo	28	1125	1282	1125	1125	1125	5289	203	203	62	100%	80	80	80	80	0	0	5494
Windows Systems	10	844	92	844	844	844	3076	56	56	28	100%	80	80	80	80	0	0	3132
AIX 5&6 (Chiharu)	1	0	0	0	0	0	257	15	15	12	100%	80	80	80	80	0	0	6
Empty	1	0	0	0	0	0	11	2	2	1	0	80	80	80	80	0	0	13

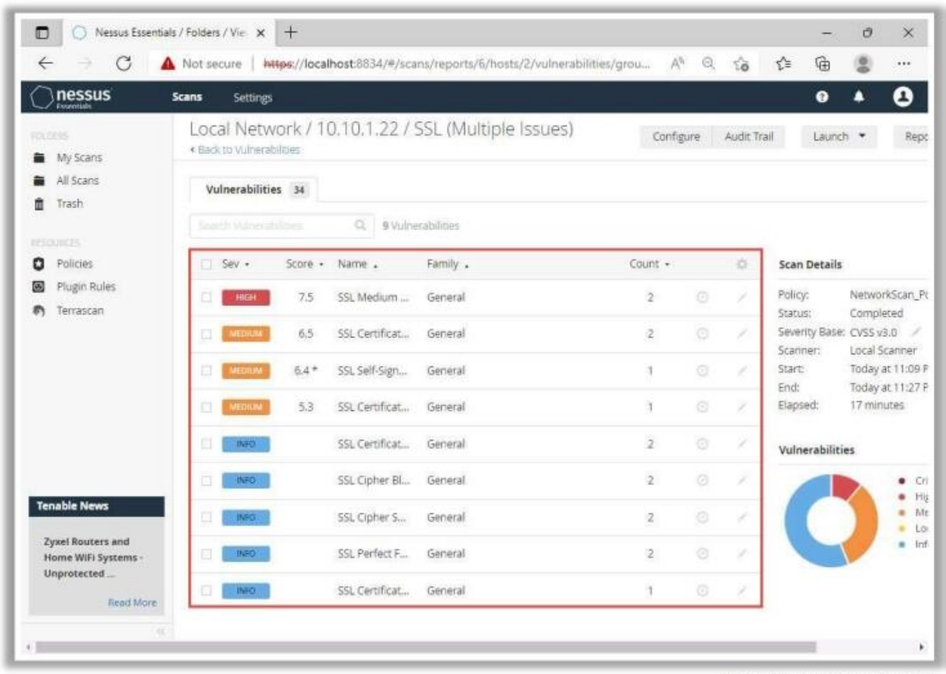
https://www.qualys.com

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

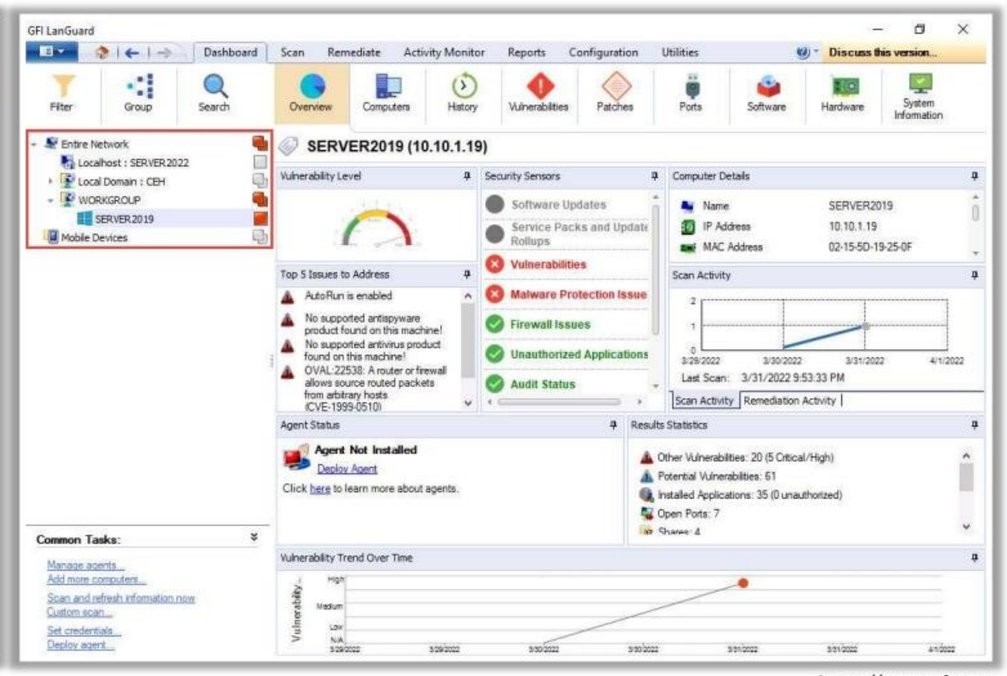
Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional — An assessment solution for **identifying the vulnerabilities**, **configuration issues**, and **malware**

GFI LanGuard — Scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices



https://www.tenable.com



https://www.gfi.com

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

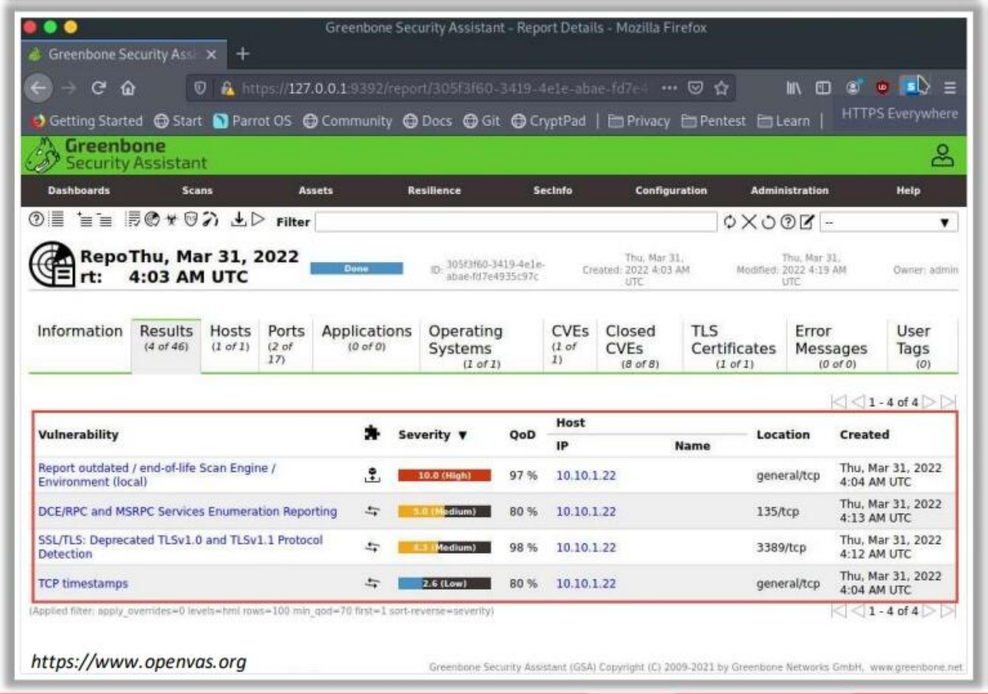
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Vulnerability Assessment Tools: OpenVAS and Nikto

OpenVAS

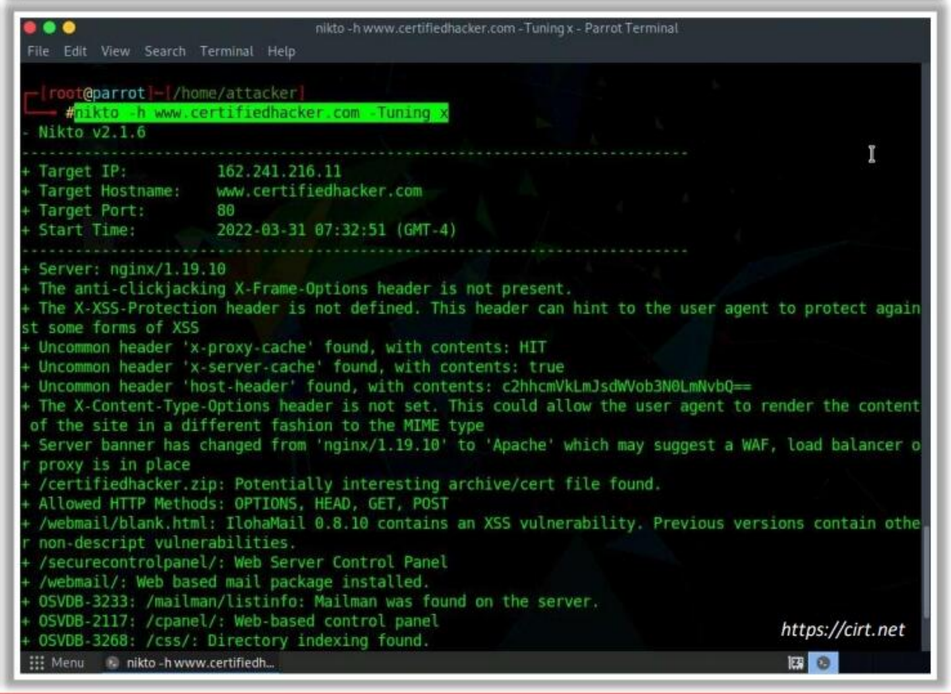
A framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**



https://www.openvas.org

Nikto

A **web server assessment tool** that examines a web server to discover potential problems and security vulnerabilities



https://cirt.net

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

Other Vulnerability Assessment Tools

- **Qualys FreeScan** — *https://www.qualys.com*
- **Acunetix Web Vulnerability Scanner** — *https://www.acunetix.com*
- **Nexpose** — *https://www.rapid7.com*
- **Network Security Scanner** — *https://www.beyondtrust.com*
- **SAINT** — *https://www.carson-saint.com*
- **beSECURE (AVDS)** — *https://www.beyondsecurity.com*
- **Core Impact Pro** — *https://www.coresecurity.com*
- **N-Stalker Web Application Security Scanner** — *https://www.nstalker.com*
- **ManageEngine Vulnerability Manager Plus** — *https://www.manageengine.com*
- **Nipper Studio** — *https://www.titania.com*

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

Vulnerability Assessment Tools

An attacker performs vulnerability scanning to identify security loopholes in the target network that they can exploit to launch attacks. Security analysts can use vulnerability assessment tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Network vulnerability scanners help to analyze and identify vulnerabilities in the target network or network resources by using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

The following are some of the most effective vulnerability assessment tools:

- **Qualys Vulnerability Management**

  Source: *https://www.qualys.com*

  Qualys VM is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.

  Features:

  - **Agent-based detection**

    Also works with the Qualys Cloud Agents, extending its network coverage to unscannable assets.

  - **Constant monitoring and alerts**

    When VM is paired with Continuous Monitoring (CM), InfoSec teams are proactively alerted about potential threats, so problems can be tackled before they turn into breaches.

  - **Comprehensive coverage and visibility**

    Continuously scans and identifies vulnerabilities for protecting IT assets on-premises, in the cloud, and at mobile endpoints. Its executive dashboard displays an overview of the security posture and gives access to remediation details. VM generates custom, role-based reports for multiple stakeholders, including automatic security documentation for compliance auditors.

  - **VM for the perimeter-less world**

    As enterprises adopt cloud computing, mobility, and other disruptive technologies for digital transformation, Qualys VM offers next-generation vulnerability management for these hybrid IT environments whose traditional boundaries have been blurred.

  - **Discover forgotten devices and organize the host assets**

    Qualys can help quickly determine what is running in different parts of the network—from the perimeter and corporate network to virtualized machines and cloud services. It can also identify unexpected access points, web servers, and other devices that can expose the network to attack.

  - **Scan for vulnerabilities everywhere, accurately and efficiently**

    Scan systems anywhere from the same console, including the perimeter, the internal network, and cloud environments.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

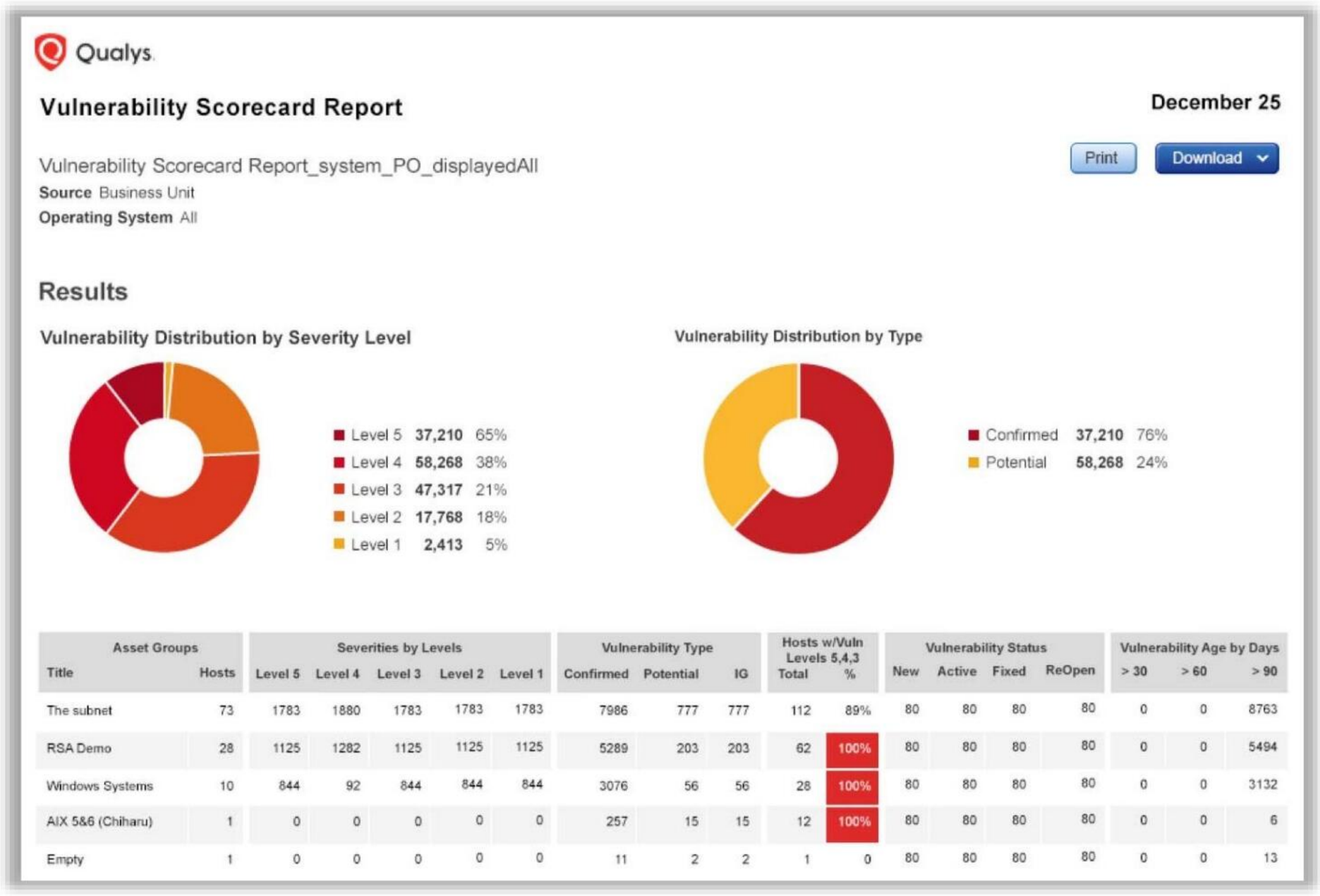
https://t.me/learningnets

- **Identify and prioritize risks**

  Qualys, using trend analysis, Zero-Day, and Patch impact predictions, can identify the highest business risks.

- **Remediate vulnerabilities**

  Qualys's ability to track vulnerability data across hosts and time produces interactive reports that provide a better understanding of the security of the network.



Asset Groups		Severities by Levels					Vulnerability Type			Hosts w/Vuln Levels 5,4,3		Vulnerability Status				Vulnerability Age by Days		
Title	Hosts	Level 5	Level 4	Level 3	Level 2	Level 1	Confirmed	Potential	IG	Total	%	New	Active	Fixed	ReOpen	> 30	> 60	> 90
The subnet	73	1783	1880	1783	1783	1783	7986	777	777	112	89%	80	80	80	80	0	0	8763
RSA Demo	28	1125	1282	1125	1125	1125	5289	203	203	62	100%	80	80	80	80	0	0	5494
Windows Systems	10	844	92	844	844	844	3076	56	56	28	100%	80	80	80	80	0	0	3132
AIX 5&6 (Chiharu)	1	0	0	0	0	0	257	15	15	12	100%	80	80	80	80	0	0	6
Empty	1	0	0	0	0	0	11	2	2	1	0	80	80	80	80	0	0	13

Figure 5.7: Vulnerability scanning using Qualys Vulnerability Management

- **Nessus Professional**

  Source: *https://www.tenable.com*

  Nessus Professional is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets and phones, web servers, and critical infrastructure.

  Nessus is the vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, and use wizards to easily and quickly create policies, schedule scans, and send results via email.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Features:

- High-speed asset discovery
- Vulnerability assessment
- Malware and Botnet detection
- Configuration and compliance auditing
- Scanning and auditing virtualized and cloud platforms

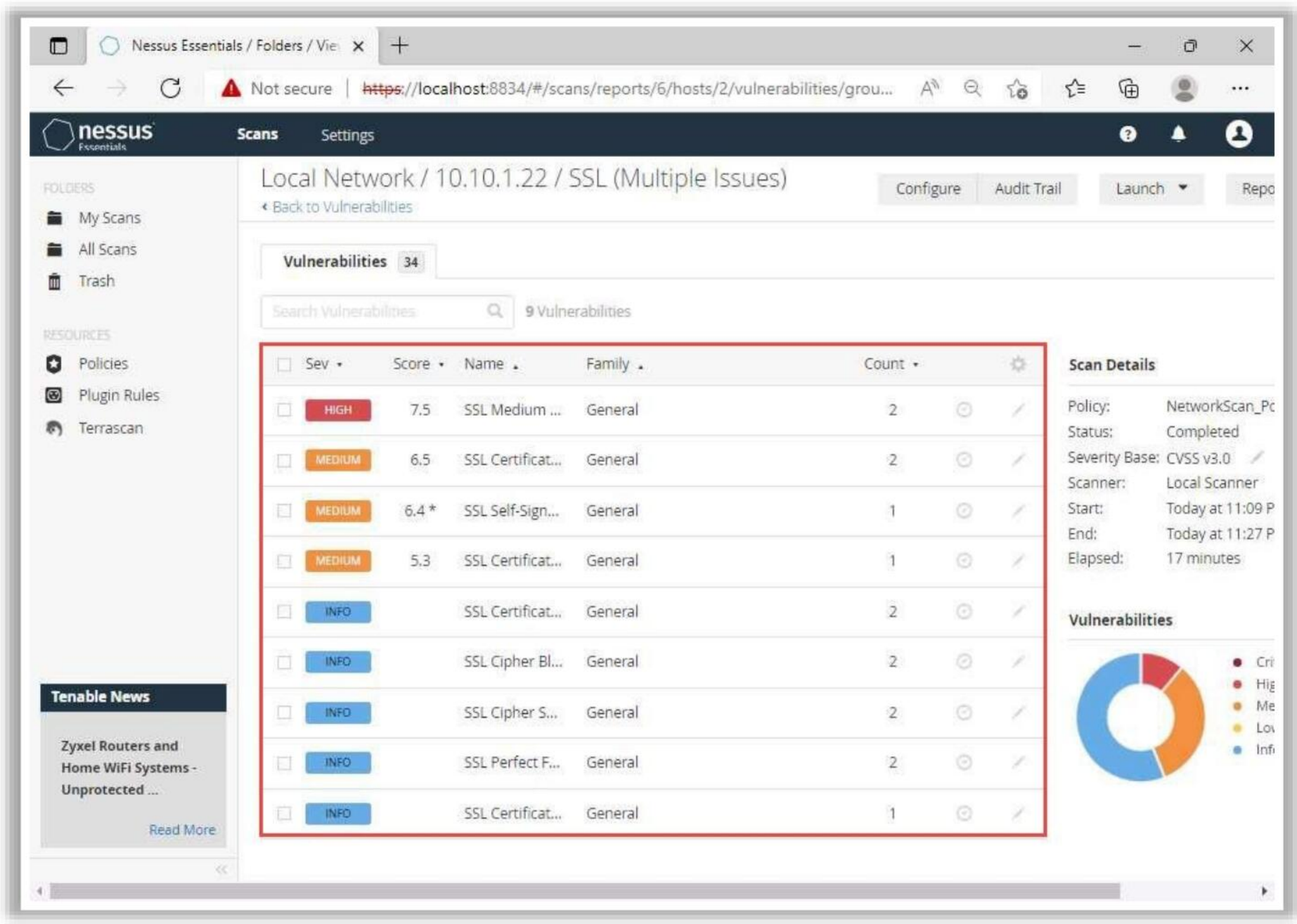


Figure 5.8: Vulnerability scanning using Nessus

- **GFI LanGuard**

  Source: *https://www.gfi.com*

  GFI LanGuard scans for, detects, assesses, and rectifies security vulnerabilities in a network and its connected devices. This is done with minimal administrative effort. It scans the operating systems, virtual environments, and installed applications through vulnerability check databases. It enables analysis of the state of network security, identifies risks, and offers solutions before the system can be compromised.

  Features:

  - Patch management for operating systems and third-party applications
  - Vulnerability assessment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- A Web reporting console
- Track latest vulnerabilities and missing updates
- Integration with security applications
- Network device vulnerability checks
- Network and software auditing
- Support for virtual environments

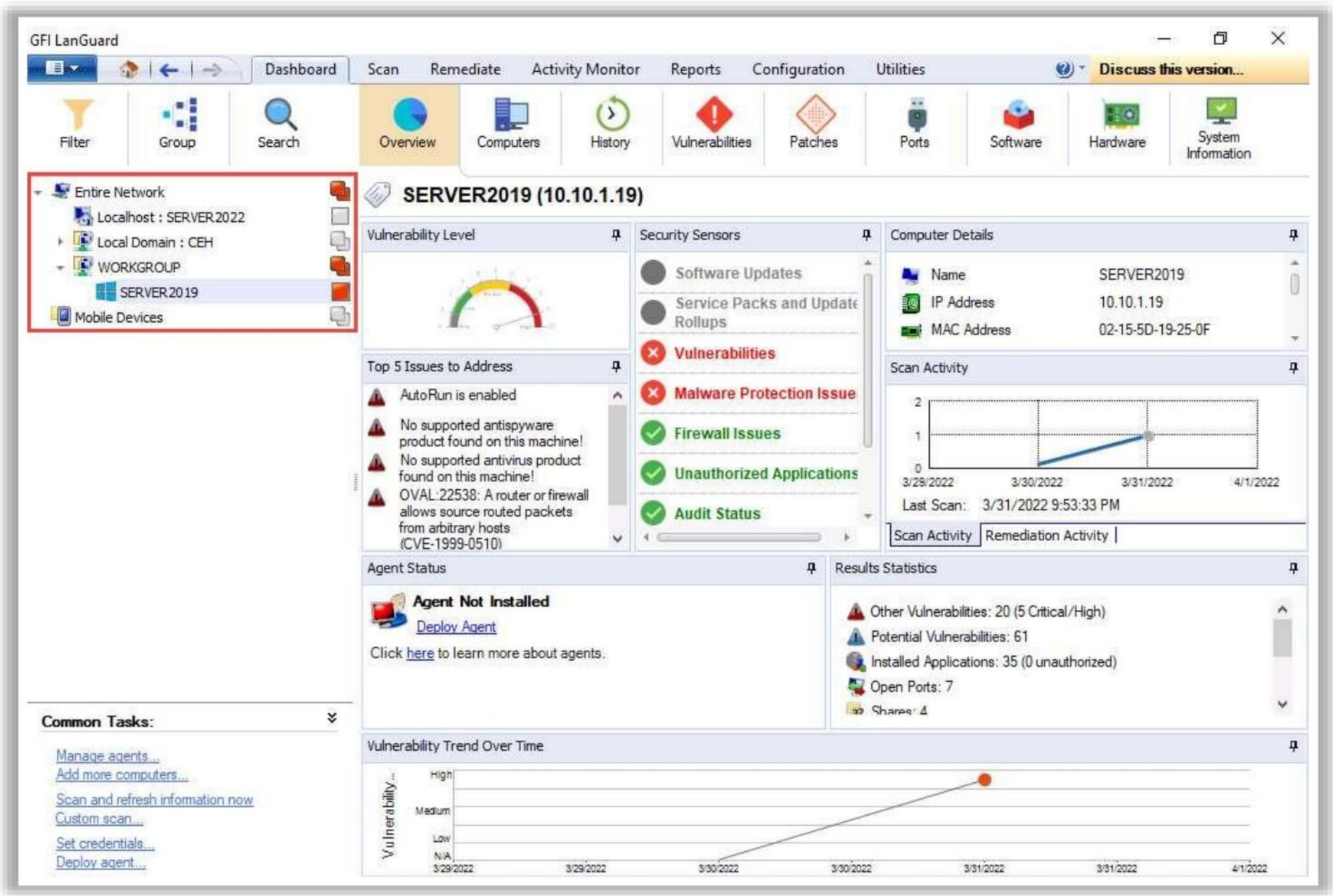


Figure 5.9: Vulnerability scanning using GFI LanGuard

- **OpenVAS**

  Source: *https://www.openvas.org*

  OpenVAS is a framework of several services and tools that offer a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Network's commercial vulnerability management solution, developments from which have been contributed to the open-source community since 2009.

  The actual security scanner is accompanied by a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

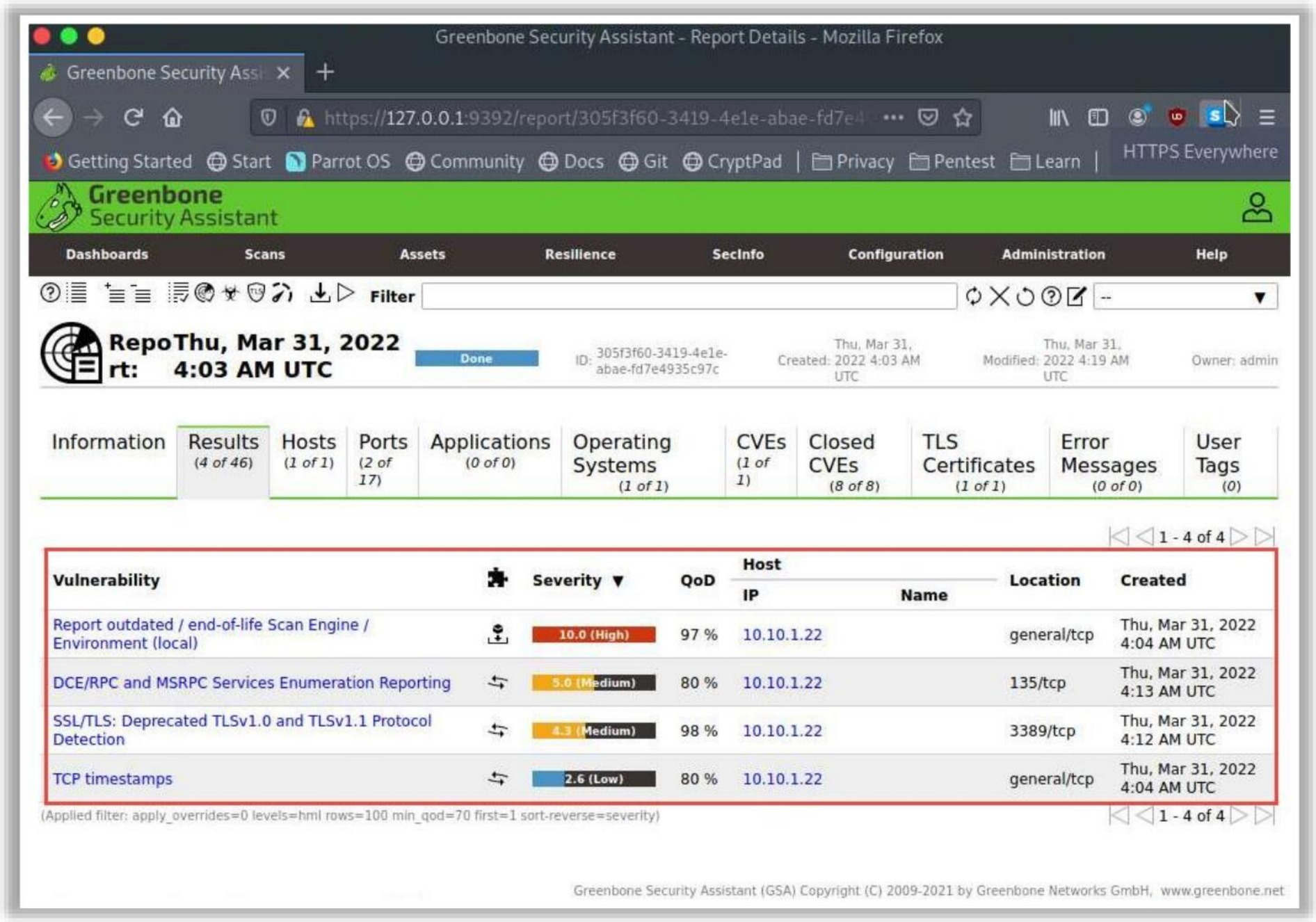


Figure 5.10: Vulnerability scanning using OpenVAS

- **Nikto**

  Source: *https://cirt.net*

  Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files or programs, checks for outdated versions of over 1250 servers, and checks for version specific problems on over 270 servers. It also looks at server configuration items such as the presence of multiple index files and the HTTP server options and will attempt to identify installed web servers and software.

  Features:

  - SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
  - A full HTTP proxy support
  - Checks for outdated server components
  - Saves reports in plain text, XML, HTML, NBE or CSV
  - A Template engine to easily customize reports
  - Scans multiple ports on a server, or multiple servers via input file
  - LibWhisker's IDS encoding techniques

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Identifies installed software via headers, favicons, and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Apache and cgiwrap username enumeration
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guesses credentials for authorization realms (including many default ID and password combinations)

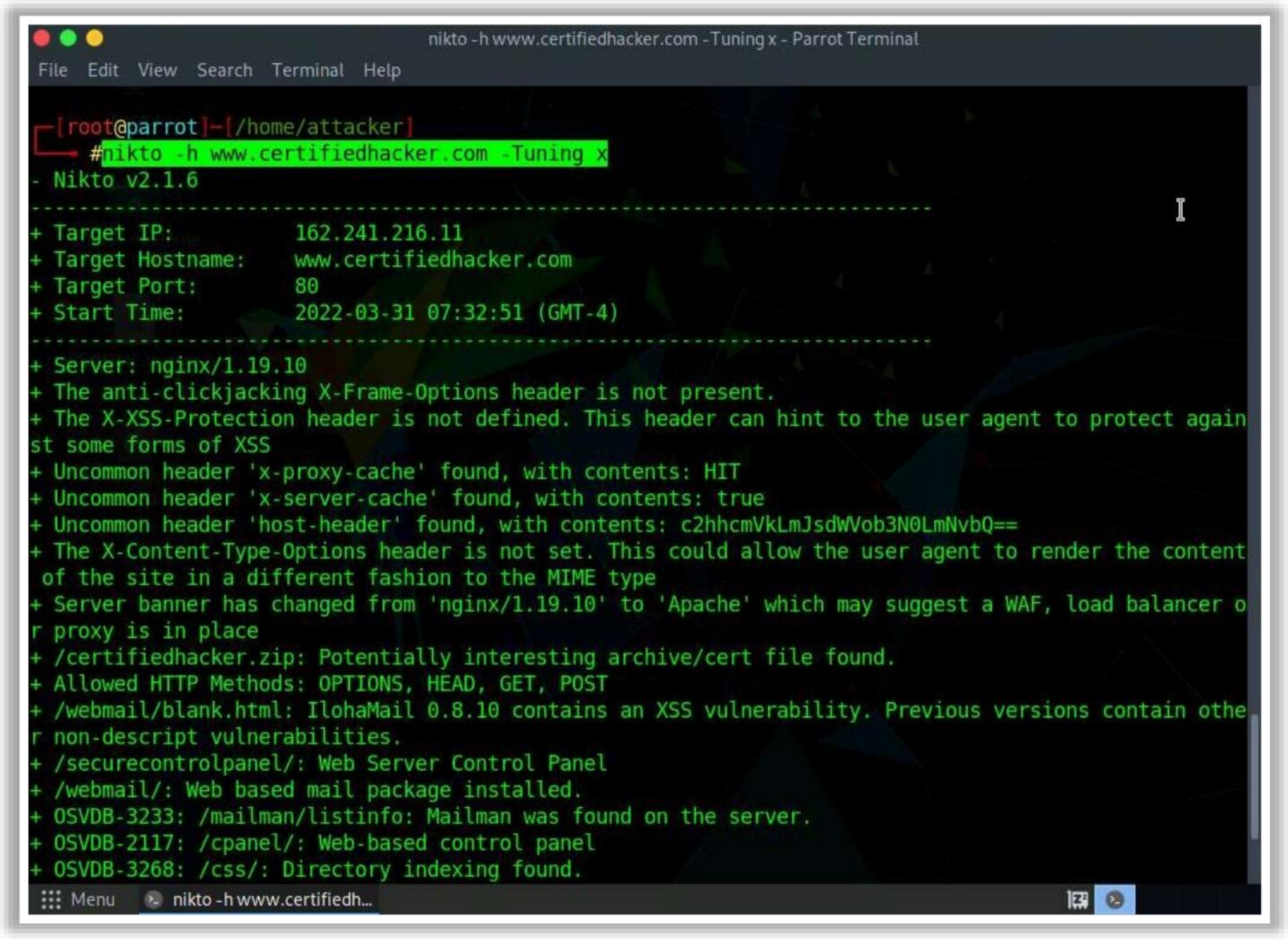


Figure 5.11: Screenshot of Nikto

Listed below are some of the additional vulnerability assessment tools:

- Qualys FreeScan (*https://www.qualys.com*)
- Acunetix Web Vulnerability Scanner (*https://www.acunetix.com*)
- Nexpose (*https://www.rapid7.com*)
- Network Security Scanner (*https://www.beyondtrust.com*)
- SAINT (*https://www.carson-saint.com*)
- beSECURE (AVDS) (*https://www.beyondsecurity.com*)
- Core Impact Pro (*https://www.coresecurity.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- N-Stalker Web Application Security Scanner (*https://www.nstalker.com*)
- ManageEngine Vulnerability Manager Plus (*https://www.manageengine.com*)
- Nipper Studio (*https://www.titania.com*)

Vulnerability Assessment Tools for Mobile

- **Vulners Scanner**

  Source: *https://vulners.com*

  Vulners scanner is an Android application that performs passive vulnerability detection based on a software version's fingerprint. Since this is a passive method of vulnerability assessment, this app can only be used to identify vulnerabilities; it is not effective in performing compliance checks.



Figure 5.12: Vulners Scanner — critical risk score

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

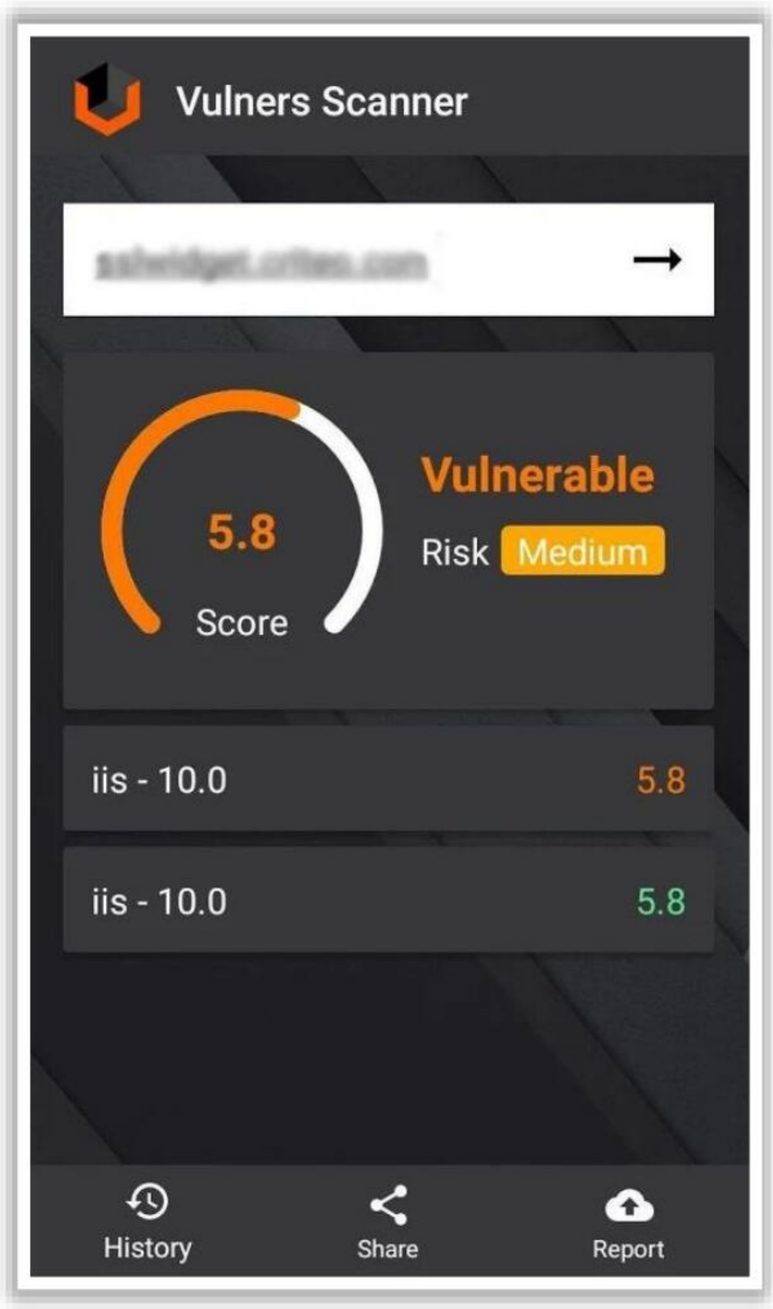


Figure 5.13: Vulners Scanner — medium risk score

- **SecurityMetrics Mobile**

  Source: *https://www.securitymetrics.com*

  SecurityMetrics Mobile is a mobile defense tool that helps to identify mobile device vulnerabilities to protect customers' sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, personal and business use, unwarranted app privileges, data and device storage, account data access, Bluetooth, Infrared (IR), Near-field communication (NFC), and SIM and SD cards.

  SecurityMetrics MobileScan complies with PCI SSC (Payment Card Industry Security Standards Council) guidelines to prevent mobile data theft. On completion of a scan, the report generated comprises a total risk score, a summary of discovered vulnerabilities, and recommendations on how to resolve threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

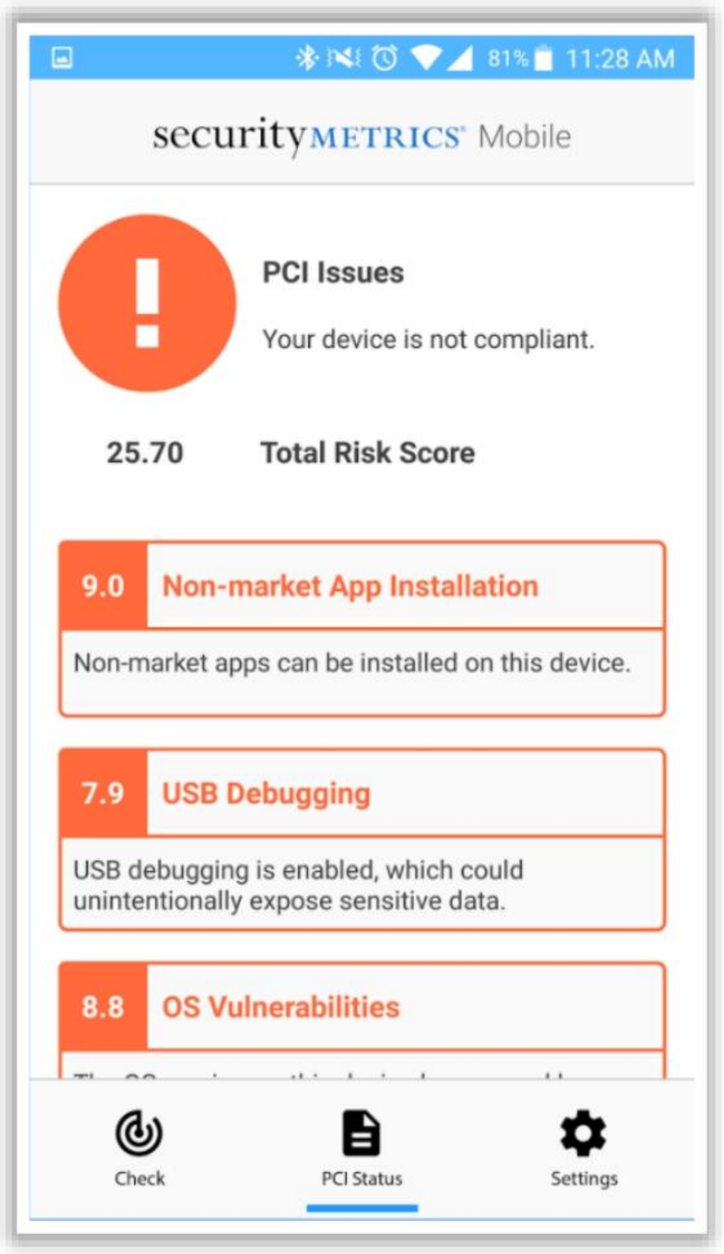


Figure 5.14: SecurityMetrics Mobile — Risk Score

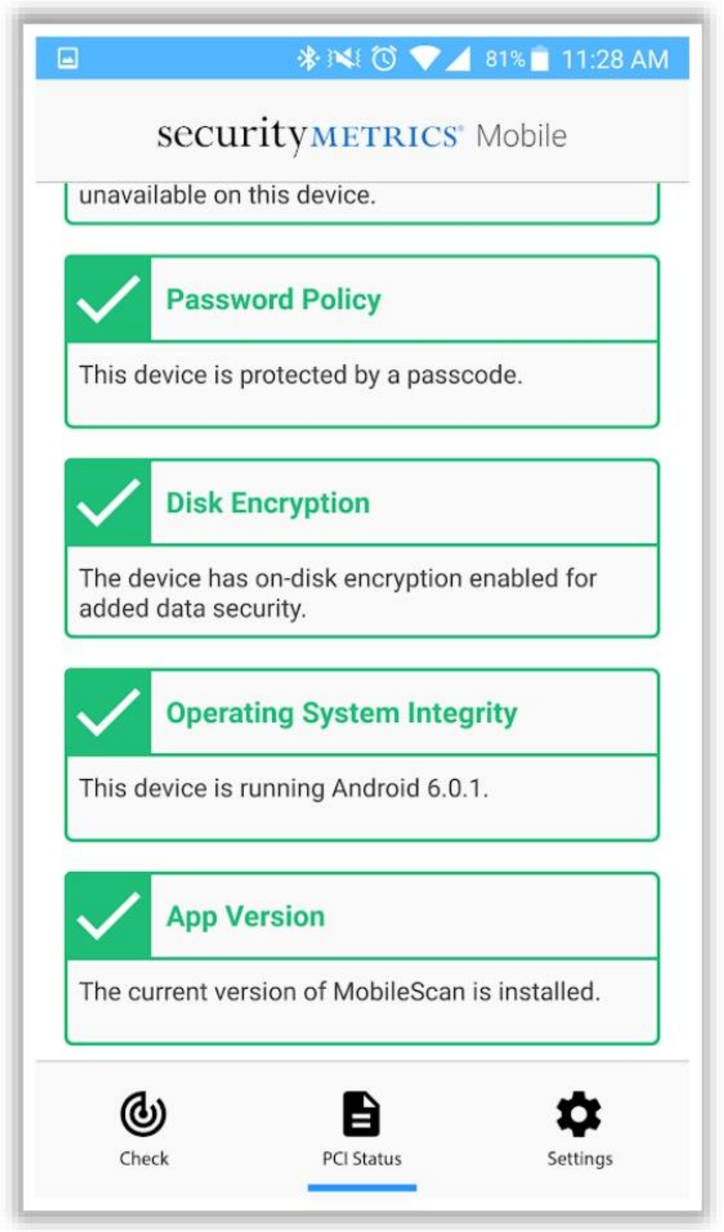


Figure 5.15: SecurityMetrics Mobile — result

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

LO#04: Analyze Vulnerability Assessment Reports

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

Vulnerability Assessment Reports

1. The vulnerability assessment report **discloses the risks detected after scanning** a network
2. The report **alerts the organization** of possible attacks and suggests **countermeasures**
3. Information available in the reports is used to fix **security flaws**



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

Vulnerability Assessment Reports

In the vulnerability assessment process, once all the phases are completed, the security team will review the results and process the information to prepare the final report. In this phase, the security team will try to disclose any identified vulnerabilities, document any variations and findings, and include all these in the final report along with remediation steps to mitigate the identified risks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

The vulnerability assessment report discloses the risks that are detected through scanning the network. Tools such as Nessus Professional, GFI LanGuard, and Qualys Vulnerability Management are used for vulnerability assessment. These tools provide a comprehensive assessment report in a specified format. The report alerts the organization to possible attacks and suggests countermeasures.

The report provides details of all the possible vulnerabilities with regard to the company's security policies. The vulnerabilities are categorized based on severity into three levels: High, Medium, and Low risk.

High-risk vulnerabilities are those that might allow unauthorized access to the network. These vulnerabilities must be rectified immediately before the network is compromised. The report describes different kinds of attacks that are possible given the organization's set of operating systems, network components, and protocols.

The vulnerability assessment report must include, but are not limited to, the following points:

- The vulnerability's name and its mapped CVE ID
- The date of discovery
- The score based on Common Vulnerabilities and Exposures (CVE) databases
- A detailed description of the vulnerability
- The impact of the vulnerability
- Details regarding the affected systems
- Details regarding the process needed to correct the vulnerability, including information patches, configuration fixes, and ports to be blocked.
- A proof of concept (PoC) of the vulnerability for the system (if possible)

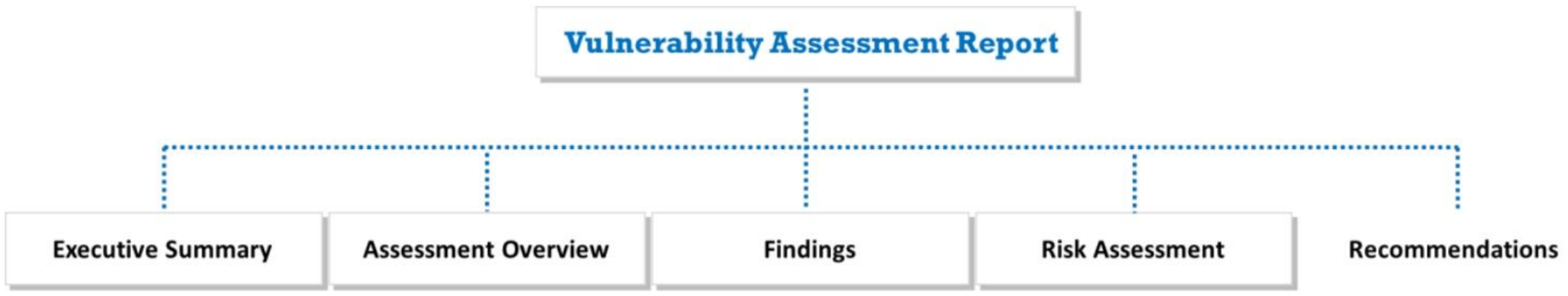
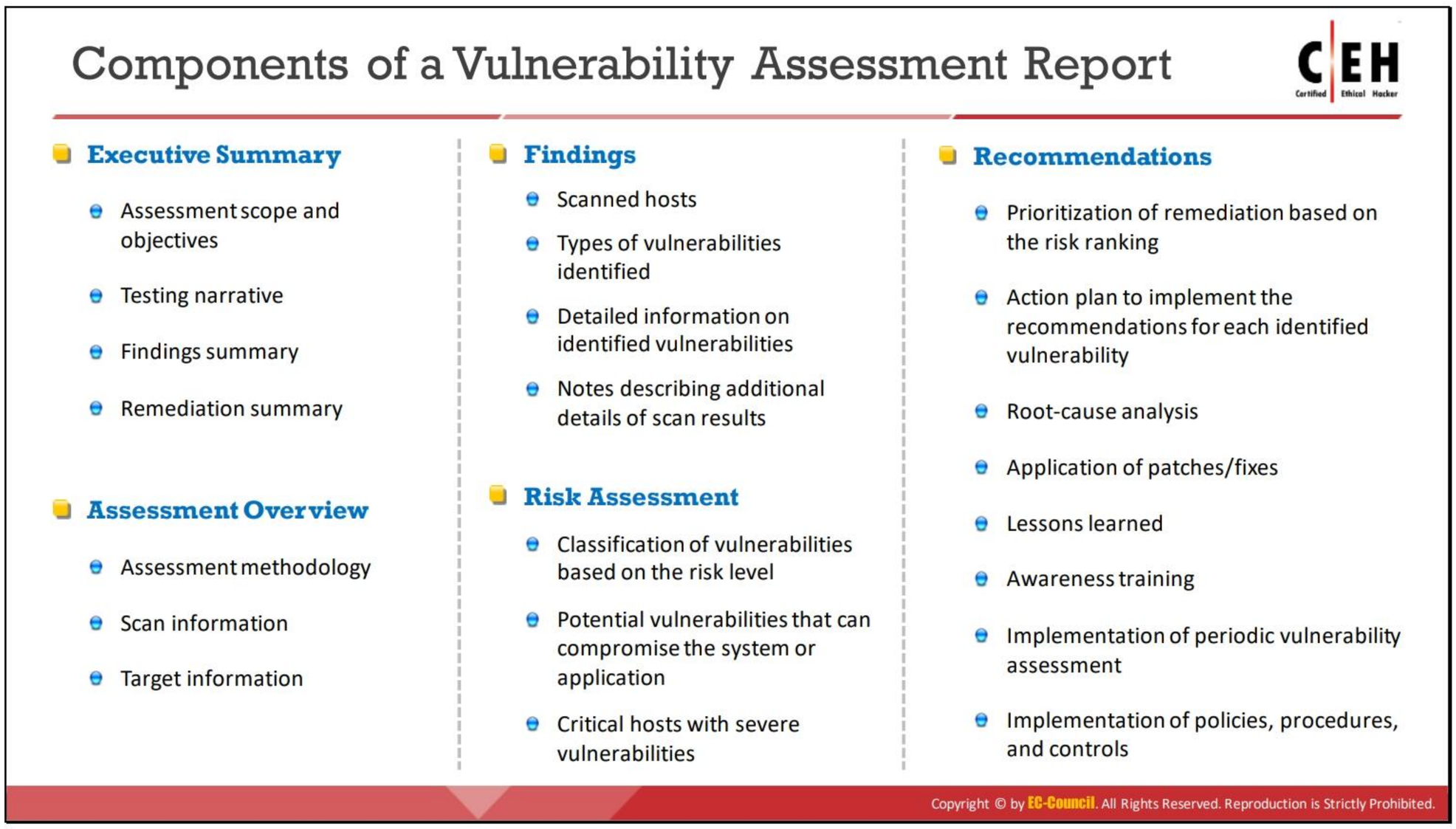


Figure 5.16: Components of a vulnerability assessment report

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Components of a Vulnerability Assessment Report

A vulnerability assessment report provides detailed information regarding the vulnerabilities found in the computing environment. The report helps organizations identify the security posture of computing systems (such as web servers, firewalls, routers, email, and file services) and provide solutions to reduce system failures. An ethical hacker must be careful when analyzing vulnerability assessment reports to avoid false positives.

The assessment report helps organizations take mitigation steps to avoid risk proactively by identifying, tracking, and eliminating security vulnerabilities.

Vulnerability assessment reports are classified into two types:

- Security vulnerability reports
- Security vulnerability summaries

Security Vulnerability Report

This is a combined report of all the scanned devices and servers in the organization's network.

The security vulnerability report includes the following details:

- Newly found vulnerabilities
- Open ports and detected services
- Suggestions for remediation
- Links to patches

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Security Vulnerability Summary

This report is produced for every device or server after scanning. It provides a summary of the scan result, which includes the following elements:

- Current security flaws
- Categories of vulnerabilities
- Newly detected security vulnerabilities
- Severity of vulnerabilities
- Resolved vulnerabilities

A vulnerability assessment report covers the following elements:

- **Executive Summary**
  - Assessment scope and objectives
    - Purpose of the vulnerability scanning
    - Scope of the scanning
  - Testing narrative
    - Operating systems upon which scanning is performed
    - IP addresses upon which scanning is performed
    - Types of scans performed
    - Date and time (Including start, end, and duration of scan)
  - Findings summary
    - Critical vulnerabilities identified (highlights based on risk level)
      - ✓ Number of vulnerabilities based on severity (graphical representation)
    - Identified operating systems
    - Performance of the systems and applications during the scan
    - Overall risk level
    - Critical issues that need to be addressed
  - Remediation summary
- **Assessment Overview**
  - Assessment methodology
  - Scan information: information such as the type of scan performed, tools used, versions, and the assets scanned.
  - Target information: Information about the target system's name and address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Findings**
  - Scanned hosts, including each host's detailed information
    - **<Node>**: Name and address of the host
    - <**OS>**: Operating system type
    - **<Date>**: Date of the test
    - **Vulnerable services:** Network services by their names and ports.
  - Types of vulnerabilities identified
  - Detailed information on identified vulnerabilities (including CVE ID, CVSS score, threat description, impact caused, remediation, and exploitability)
  - Notes describing additional details of scan results
- **Risk Assessment**
  - Classification of vulnerabilities based on the risk level: critical, high, moderate, or low
  - Potential vulnerabilities that can compromise the system or application
  - Critical hosts with severe vulnerabilities
- **Recommendations**
  - Prioritization of remediation based on the risk ranking
  - Action plan to implement the recommendations/remediation for each identified vulnerability
  - Root-cause analysis
  - Application of patches/fixes
  - Lessons learned
  - Awareness training
  - Implementation of periodic vulnerability assessment
  - Implementation of policies, procedures, and controls

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Module Summary



- In this module, we have discussed:
  - The definition of vulnerability research, vulnerability assessment, and vulnerability-management life cycle
  - The CVSS vulnerability scoring system and databases
  - Various types of vulnerabilities and vulnerability assessment techniques
  - Various vulnerability assessment solutions, along with their characteristics
  - Various tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool
  - We concluded with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning the network
- In the next module, we will discuss the methods attackers, as well as ethical hackers and pen testers, utilize to hack a system based on the information collected about a target of evaluation; for example, footprinting, scanning, enumeration, and vulnerability analysis phases

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

Module Summary

This module discussed vulnerability research, vulnerability assessment, and the vulnerability-management life cycle. It also discussed the CVSS vulnerability scoring system and databases and various types of vulnerabilities and vulnerability assessment techniques. It described various vulnerability assessment solutions along with their characteristics and described various vulnerability assessment tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool. Finally, this module ended with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning a network.

The next module will show how attackers, as well as ethical hackers and pen testers, attempt system hacking based on the information collected about a target in the footprinting, scanning, enumeration, and vulnerability analysis phases.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets