

CEH based TEST

National Vocational and Technical Training Commission

1. **A** port **scan is performed to detect open ports on a system.**
2. **What is the primary purpose of vulnerability scanning?**

\_ The primary reason of the vulnerability scanning is also in the identification of the security weaknesses or vulnerabilities that can be exploited by the attackers.

This process can assist organizations in uncovering and have corrections on probable security threats that can be exploited.

1. **What is CVSS and what is the major difference between CVSS 2.0 and CVSS 3.0?**

CVSS is a mode that is normally applied in the assessment of the severity of vulnerabilities. It assigns a numerical risk and impact score so that organisations can assess where to allocate their effort.

Main Differences between CVSS 2. 0 and CVSS 3. 0:

Scoring Metrics:

CVSS 2. 0: It employs three metrics groups which include; Base, Temporal and; Environmental to determine the score.

CVSS 3. 0: Introduces new cleaner and more granular measurements: the changes in the Base metric group: for example, the addition of ‘Scope’ measuring whether a vulnerability impacts many systems or components.

1. Vulnerability **type of scanning involves the use of tools like Nessus and OpenVAS.**
2. **What is the first step in a vulnerability assessment?**

The first step in a vulnerability assessment is, as the name suggests, asset identification.

1. **Define CVE and write about any CVE database that you know?**

CVE is an identifier of publicly known information security vulnerabilities, drawn up according to international standards.

CVE Database Example: NVD is the most commonly used database that contains information about CVEs with the possibility of scoring them by their severity and impact.

1. **OpenVAS stands for** Open **Vulnerability Assessment System.**
2. **The process of identifying vulnerabilities without automated tools is known** as manual **vulnerability assessment.**

1. **Which automated scanner is known for its ability to detect a wide range of vulnerabilities with minimal configuration?**

Nessus is the well-known, free and open-sourced automated scanner which offers top performance in terms of quickly discovering as many vulnerabilities as possible with little or no configuration at all.

1. **Security Information and Event Management (SIEM) systems often aggregate log data from diverse sources, and advanced SIEM platforms leverage Correlation Rules and machine learning** **to identify sophisticated attack patterns.**

1. **The vulnerability scanning technique that involves sending crafted packets to identify open ports is known as port scanning.**
2. **What does CVSS stand for?**

**CVSS** stands for **Common Vulnerability Scoring System.**

1. **The database that maintains a list of known vulnerabilities is called a** **vulnerability database.**
2. **Describe the key features of the Common Vulnerability Scoring System (CVSS).**

Base Metrics: Some of the key internal characteristics include:

Temporal Metrics: What modern threat to existence looks like at the moment.

Environmental Metrics: Environment-specific adjustments.

Score: Numerical severity rating.

1. **How does CVSS contribute to the prioritization of vulnerabilities?**

CVSS also enables vendors to define a numerical value in order to underline the severity of the problem so that the organizations can easily identify which of the problems is the most important and requires immediate attention.

1. Vulnerability databases **databases are essential for keeping up-to-date with the latest vulnerabilities.**

1. **List three best practices for effective vulnerability management.**

* Regular Scanning
* Prioritization
* Patch Management

1. **How can a vulnerability database like CVE be integrated into an organization’s vulnerability management program?**

* Automate Alerts
* Cross-Reference Data
* Update Tools

**19**.**Defense in Depth involves layering multiple security controls throughout an organization’s IT environment to ensure that if one layer fails**,

Defense in Depth works such that when the lower layers of security have been breached, the higher ones still come into play.

1. **Threat Intelligence Integration involves incorporating real-time information about current and emerging** threats **into an organization’s security operations to better anticipate and defend against potential attacks.**
2. **The Least Privilege Principle dictates that users and systems should have the** **minimum** **level of access necessary to perform their functions.**

1. **Explain the difference between automated and manual vulnerability scanning.**

Automated Scanning: Chosen tools will be those which allow taking actions quickly, thereby requiring the least time from the user.

Manual Scanning: Engages parameters the hands-on analysis and employs the virtue of an expert view.

1. **Nmap's** Nmap Scripting **Engine (NSE) is used for advanced vulnerability scanning.**
2. **How does the Nmap Scripting Engine (NSE) enhance the capabilities of Nmap?**

NSE brings additional features to Nmap through scripted sessions for the specific detection of vulnerabilities, as well as more precise scanning.

1. **Compare and contrast Nessus and OpenVAS as vulnerability scanners.**

Nessus: Paid, often, easy, experts.

OpenVAS: Gratis, open source, broad functionality, people.

1. **Explain the role of Qualys in vulnerability management.**

Qualys’ is a constant vulnerability scanner and assessment tool available on a cloud platform.

1. **The** OWASP **Top Ten list is a critical resource for web application security.**
2. **What is the OWASP Top Ten?**

The OWASP Top Ten presents the ten most significant Web application vulnerability categories.

1. **How can vulnerability assessments improve the security of web applications?**

Vulnerability test involves examination of the flaws with aim to rectify to improve the protective measures of web applications.

1. BURP SUITE **is a widely used vulnerability scanner for assessing web applications.**
2. **What is the focus of vulnerability analysis for mobile applications?**

It is concentrated on such mobile-specific vulnerabilities as ineffective data protection and wrong permissions.

**32**.**Mobile application vulnerabilities can often be linked to coding flaws.**

1. **What are the common techniques used in vulnerability analysis for network devices?**

 Port Scanning

 Network Mapping

 Service Enumeration

 Configuration Review

 Exploit Testing

1. **Why is it important to conduct vulnerability analysis on network devices?**

It’s important to identify and fix weaknesses to prevent attacks and ensure network security.

1. **In the Kill Chain Model, the Exploit phase may involve the use of zero-day vulnerabilities, which are unknown to the public and are often exploited through** malware**, a technique involving embedded code in seemingly benign files.**
2. **Vulnerability analysis of network devices often focuses on**  services **configurations, and firmware.**
3. **What are the typical steps involved in the reporting of vulnerabilities?**

* Discovery
* Assessment
* Documentation
* Reporting
* Remediation
* Follow-Up

1. **Define SQL injection and write an example of SQL injection?**

SQL injection allows attackers to execute arbitrary SQL through user input.

Example: ' OR '1'='1 used to bypass login

1. **How do exploitation frameworks assist in vulnerability analysis?**

Exploitation frameworks are used to automate the process of exploiting the discovered vulnerabilities so as to validate and test their impact.

1. **What is the primary function of OpenVAS?**

The primary function of OpenVAS is to perform comprehensive vulnerability scanning and assessment.

1. **Exploitation frameworks like** **Metasploit are used to simulate attacks on discovered vulnerabilities.**
2. **Discuss the ethical considerations involved in vulnerability analysis**.

Authorization: Get permission before testing.

Confidentiality: Protect sensitive data.

Impact: Minimize system disruption.

Reporting: Disclose responsibly.

Compliance: Follow legal requirements.

1. .**What is the significance of reporting and remediation in the vulnerability management process?**

Reporting: Provides visibility into vulnerabilities, enabling informed decision-making.

Remediation: Addresses and fixes vulnerabilities to reduce risk and enhance security

1. **Zero Trust Architecture operates on the principle of "** never trust, always verify, **always verify," meaning that every access request is subjected to strict verification regardless of its origin.**
2. **Case studies in vulnerability analysis often highlight** lessons learned **from realworld scenarios.**

1. **Why are case studies important in learning about vulnerability analysis?**

Case studies are important because they provide practical examples, illustrate real-world impacts, and offer insights into effective strategies and common pitfalls in vulnerability analysis

1. **How can case studies improve your approach to vulnerability analysis?**

Case studies provide real-world examples and insights, helping to refine and enhance vulnerability analysis practices.

1. **Describe a scenario where comprehensive vulnerability analysis would be critical.**

A major software update requires comprehensive vulnerability analysis to prevent potential exploits and ensure system integrity.

1. **Define lateral movement and why it's done?**

Lateral movement is moving through a network to exploit additional systems, aiming to gain broader access or find valuable data.

1. **During the practical on vulnerability analysis, students may use tools like Nessus\_ to assess system security.**
2. **What is the purpose of practical exercises in a vulnerability analysis course?**

Practical exercises provide hands-on experience and skill development for real-world vulnerability assessment.

1. **Explain how a hands-on practical approach enhances understanding of vulnerability analysis.**

A hands-on practical approach enhances understanding by allowing learners to apply concepts in real scenarios, gaining direct experience and solving real problems.

1. **What are the key components of a comprehensive vulnerability analysis report?**

* Executive Summary
* Vulnerability Details
* Risk Assessment
* Recommendations
* Remediation Plan
* Appendices

54.A well-conducted vulnerability analysis should lead to effective \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of discovered vulnerabilities.

1. What is the goal of a practical vulnerability analysis session?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ hacking is the practice of exploiting vulnerabilities in systems to gain unauthorized access.

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ cracking tools are used to recover lost or stolen passwords.
2. Name two commonly used password-cracking techniques.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_