

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?

* Vulnerability scanning aims to detect security flaws in a system or network. This enables organizations to fix these weaknesses before they can be exploited by attackers.

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

* CVSS 3.0 introduces additional metrics like “Exploit Code Maturity” and “Remediation Level” for a more detailed assessment. It also revises the scoring calculations to better reflect the real-world impact of vulnerabilities.

1. \_\_**Network 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 “identifying and defining the scope” of the assessment. This involves determining which systems, networks or applications will be evaluated for vulnerabilities.

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

* **CVE** is a standardized list of known security vulnerabilities.**National Vulnerability Database (NVD)** is the well-known database of CVE which is maintained by the U.S. government.



1. OpenVAS stands for \_Open\_ Vulnerability Assessment System.

1. 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 known for its ability to detect a wide range of vulnerabilities with minimal configuration.

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).

* Key features of the Common Vulnerability Scoring System (CVSS) include **a base score** that measures the severity of a vulnerability and **temporal and environmental scores** that assess the impact over time and in specific environments.

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

* CVSS include **a base score** that measures the severity of a vulnerability and **temporal and environmental scores** that assess the impact over time and in specific environments.

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

1. List three best practices for effective vulnerability management.

* Regular scanning for vulnerabilities, prioritizing based on risk and timely remediation of identified issues are the best practices of EVM.

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

* A vulnerability database like CVE can be integrated into an organization’s vulnerability management program by using it to identify known vulnerabilities in systems, applying CVE information to assess risk and guiding remediation efforts.

19.Defense in Depth involves layering multiple security controls throughout an organization’s IT environment to ensure that if one layer fails, \_**other layers will still provide protection\_**.

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 vulnerability scanning uses software tools to systematically identify vulnerabilities, while manual vulnerability scanning involves human analysis and expertise to find vulnerabilities

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

* The Nmap Scripting Engine (NSE) enhances the capabilities of Nmap by allowing users to write and execute custom scripts for advanced network discovery and vulnerability scanning.

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

* Nessus and OpenVAS are both vulnerability scanners but differ in licensing (Nessus is commercial, while OpenVAS is open-source) and features (Nessus often has more frequent updates and a broader plugin library).

1. Explain the role of Qualys in vulnerability management.

* Qualys provides cloud-based vulnerability management and security solutions, including continuous scanning and reporting on vulnerabilities to help organizations manage and mitigate risks.

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 is a list of the most critical security risks to web applications, updated regularly to reflect the current threat landscape.

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

* Vulnerability assessments improve the security of web applications by identifying and addressing weaknesses before they can be exploited, reducing the risk of data breaches and other attacks.

1. \_Burp Suite\_is a widely used vulnerability scanner for assessing web applications.
2. What is the focus of vulnerability analysis for mobile applications?

* The focus of vulnerability analysis for mobile applications includes identifying and addressing issues such as insecure data storage, improper implementation of authentication and vulnerabilities in app communication.

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, configuration review and firmware analysis are the common techniques.

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

* Conducting vulnerability analysis on network devices is important to identify and remediate security flaws that could be exploited to gain unauthorized access or disrupt network operations.

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?

* The typical steps involved in the reporting of vulnerabilities include discovery, classification, impact assessment, recommendations and remediation verification.

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

* **SQL injection** is a vulnerability that allows attackers to execute arbitrary SQL code on a database. For example: SELECT \* FROM users WHERE username = 'admin' OR '1'='1';.

1. How do exploitation frameworks assist in vulnerability analysis?

* Exploitation frameworks assist in vulnerability analysis by providing tools and techniques to simulate attacks, test defenses, and validate the effectiveness of security measures.

1. What is the primary function of OpenVAS?

* The primary function of OpenVAS is to **perform comprehensive network vulnerability assessments** to identify and report security weaknesses.

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

* Ethical considerations in vulnerability analysis include **obtaining proper authorization**, **handling sensitive information responsibly** and **reporting findings responsibly** to avoid unintended harm.

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

* Reporting and remediation are crucial in the vulnerability management process as they help **address** discovered vulnerabilities and ensure **security improvements** are implemented effectively.

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 in learning about vulnerability analysis because they provide **real-world examples** of vulnerabilities, their impacts and how they were addressed, which helps in understanding practical applications.

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

* Case studies improve your approach to vulnerability analysis by offering **insights into effective practices**, **common pitfalls** and **successful strategies** used in addressing vulnerabilities.

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

* Comprehensive vulnerability analysis is critical in **high-risk environments**, such as financial institutions or critical infrastructure, where security breaches could have severe consequences.

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

* **Lateral movement** refers to the technique of moving within a network after an initial breach to gain access to additional systems or 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?

* The purpose of practical exercises in a vulnerability analysis course is to provide hands-on experience with real-world tools and techniques, enhancing understanding and skills in identifying and mitigating vulnerabilities.

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

* A hands-on practical approach enhances understanding of vulnerability analysis by allowing students to apply theoretical knowledge, experience real-world scenarios and develop practical skills in identifying and addressing vulnerabilities.

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

* **vulnerability details**, **risk assessment**, **recommendations** and **remediation status**.

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

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

* The goal of a practical vulnerability analysis session is to provide **hands-on experience** with tools and techniques used to identify and address security vulnerabilities effectively.

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

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

* Brute-force attacks and dictionary attacks.