 

CEH based TEST

National Vocational and Technical Training Commission

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

**Vulnerability scanning** is the process of identifying security weaknesses and

flaws in systems and software.

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

[The key difference is that CVSS 3.0 introduced a new metric called **Scope**, which accounts for vulnerabilities where the impacted component differs from the vulnerable component](https://nvd.nist.gov/vuln-metrics/cvss)

1. **vulnerability scanning** 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 to define the scope and objectives, identifying the assets and systems that need to be evaluated for potential vulnerabilities.

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

CVE (Common Vulnerabilities and Exposures) is a list of publicly disclosed cybersecurity vulnerabilities. NVD (National Vulnerability Database) is a data base of CVE.

1. OpenVAS stands for **Open Vulnerability Assessment Scanner** 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 an automated scanner known for its ability to detect a wide range of vulnerabilities with minimal configuration. It is widely used for network vulnerability assessments \_

\_

1. Security Information and Event Management (SIEM) systems often aggregate log data from diverse sources, and advanced SIEM platforms leverage Correlation

Rules and **Analytics** to identify sophisticated attack patterns.

1. The vulnerability scanning technique that involves sending crafted packets to

identify open ports is known as **port scanning** .

What does CVSS stand 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).

 **Severity Rating**: Assigns numerical scores based on exploitability and impact.

 **Metrics**: Includes base, temporal, and environmental metrics for comprehensive assessment.

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

CVSS scores help prioritize vulnerabilities based on severity.

1. **By providing a standardized rating,** \_ databases are essential for keeping up-to-date with the latest vulnerabilities.
2. List three best practices for effective vulnerability management.

1-**Regular Scanning** 2- **Prioritization**: 3- **Patch Management**:

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

vulnerability management program?

1. Defense in Depth involves layering multiple security controls throughout an

organization’s IT environment to ensure that if one layer fails, **others 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.
2. Nmap's Network Security Scanner Engine (NSE) is used for advanced vulnerability scanning.
3. 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 scripts for advanced network discovery, vulnerability detection, and exploitation, providing deeper insights beyond basic scanning.

1. Compare and contrast Nessus and OpenVAS as vulnerability scanners.
2. **Nessus** vs. **OpenVAS**:

* **Nessus**: Commercial tool with a user-friendly interface, extensive plugin library, and regular updates; known for its comprehensive vulnerability detection.
* **OpenVAS**: Open-source tool with a robust scanning engine and regular updates; lacks some advanced features and commercial support found in Nessus but is freely available.

1. **Nessus** vs. **OpenVAS**:

* **Nessus**: Commercial tool with a user-friendly interface, extensive plugin library, and regular updates; known for its comprehensive vulnerability detection.
* **OpenVAS**: Open-source tool with a robust scanning engine and regular updates; lacks some advanced features and commercial support found in Nessus but is freely available.

1. Explain the role of Ǫualys in vulnerability management.

**Qualys** plays a crucial role in vulnerability management by providing cloud-based security and compliance solutions that include continuous vulnerability scanning, assessment, and reporting, helping organizations identify and address security issues efficiently.

1. The OWASP Top Ten Top Ten list is a critical resource for web application security.
2. What is the OWASP Top Ten?
3. How can vulnerability assessments improve the security of web applications?
4. Burp Suite is a widely used vulnerability scanner for assessing web applications.
5. What is the focus of vulnerability analysis for mobile applications?

The focus of vulnerability analysis for mobile applications is to identify and address security weaknesses related to data storage, authentication, communication, and code execution, ensuring

1. Mobile application vulnerabilities can often be linked to **code flaws**. flaws.
2. What are the common techniques used in vulnerability analysis for network devices?

Common techniques used in vulnerability analysis for network devices include **port scanning**, **configuration review**, **firmware analysis**, and **vulnerability scanning**.

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

It is important to conduct vulnerability analysis on network devices to identify and address potential security weaknesses that could be exploited by attackers 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

malicious payloads , a technique involving embedded code in seemingly benign files.

1. Vulnerability analysis of network devices often focuses on **ports**, , configurations, and firmware.
2. What are the typical steps involved in the reporting of vulnerabilities?

 **Identification**: Discovering and documenting the vulnerability.

 **Assessment**: Evaluating the severity and impact.

 **Reporting**: Creating a detailed report with findings and recommendations.

 **Remediation**: Proposing and tracking fixes.

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

**SQL injection** is a type of attack where malicious SQL code is inserted into a query to manipulate or access a database. 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 scripts to test and exploit vulnerabilities, simulating real-world attacks to assess security weaknesses.

1. What is the primary function of OpenVAS?

The primary function of OpenVAS is to perform comprehensive vulnerability scanning and assessment to identify and report security issues within systems and networks.

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

It is important to conduct vulnerability analysis on network devices to identify and address potential security weaknesses that could be exploited by attackers to gain unauthorized access or disrupt network operations.

1. What is the significance of reporting and remediation in the vulnerability management process?
2. 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.
3. Case studies in vulnerability analysis often highlight **lessons learned** from real- world scenarios.
4. 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 and practical insights into how vulnerabilities are exploited and mitigated.

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

Case studies improve your approach to vulnerability analysis by showcasing effective strategies, common pitfalls, and lessons learned from actual incidents.

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

A scenario where comprehensive vulnerability analysis would be critical is in the security assessment of a financial institution's IT infrastructure to protect sensitive customer data.

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

Lateral movement is the technique of navigating within a network after initial access to expand control and gather more information; it’s done to access additional resources and escalate privileges

1. During the practical on vulnerability analysis, students may use tools like

Nmapto assess system security.

1. 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 in identifying, evaluating, and addressing vulnerabilities in real-world scenarios.

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 in a controlled environment, reinforcing learning through direct experience.

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

The key components of a comprehensive vulnerability analysis report include **vulnerability findings**, **risk assessment**, **recommendations**, and **remediation steps**.

1. A well-conducted vulnerability analysis should lead to effective **remediation** of discovered vulnerabilities.
2. What is the goal of a practical vulnerability analysis session?

The goal of a practical vulnerability analysis session is to provide hands-on experience in identifying, evaluating, and mitigating security vulnerabilities, enhancing understanding through real-world application and problem-solving.

4o mini

1. Ethical hacking hacking is the practice of exploiting vulnerabilities in systems to gain unauthorized access.
2. Password cracking cracking tools are used to recover lost or stolen passwords.
3. Name two commonly used password-cracking techniques.

Two commonly used password-cracking techniques are **brute-force attacks** and **dictionary attacks**.