 

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 purpose of Vulnerability Scanning is to find the Gap, weakness and flaws on the system for security purpose.

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

CVSS is a standardized framework used to assess the severity of security vulnerabilities in software systems. The major difference between CVSS 2.0 and CVSS 3.0 is Scope and Impact Assessment

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 **defining the scope**

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

CVE provides unique identifiers for publicly known security vulnerabilities and exposures in software and hardware. CVE-2024-3400 known CVE

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** \_

\_

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

1. What does CVSS stand for?

PORT scanning.

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, **Temporal Metrics**: Environmental Metrics

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

**By providing a standardized severity score**

1. **CVE and NVD** \_ databases are essential for keeping up-to-date with the latest vulnerabilities.
2. List three best practices for effective vulnerability management.

1-Patch Management 2-Regular scanning and monitor 3-**Prioritize and Remediate:**

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

vulnerability management program?

Via risk assessment , scanning , patch management and incident response

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

organization’s IT environment to ensure that if one layer fails, additional layers of protection remain in place. .

1. Threat Intelligence Integration involves incorporating real-time information about current and emerging Threat 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 use different s/w or program while In manual we use command manually to check the vulnerability.

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?

By providing In-Depth Analysis, Automating Advanced Task and save time.

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

Nessus offers a polished, regularly updated experience but at a cost, while OpenVAS is a free, customizable tool with a steeper learning curve.

1. Explain the role of Ǫualys in vulnerability management.

Qualys enhances vulnerability management by providing robust, scalable tools for identifying, assessing, and addressing security vulnerabilities efficiently

1. The OWASP Top Ten list is a critical resource for web application security.
2. What is the OWASP Top Ten?  
   Critical resource for web application security
3. How can vulnerability assessments improve the security of web applications?

vulnerability assessments are essential for proactively managing and mitigating security risks in web applications

1. OWASP ZAP (Zed Attack Proxy) is a widely used vulnerability scanner for assessing web applications.
2. What is the focus of vulnerability analysis for mobile applications?

Provide security, data protection, secure code , input validation and **Platform-Specific Risks:**

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

Port scanning, n/w mapping, configure review , firm and traffic analysis

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

vulnerability analysis is crucial for maintaining a secure and resilient network environmen

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

spear-phishing , a technique involving embedded code in seemingly benign files.

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

Discovery ,validation , documentation follow up and reporting,

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

**SQL Injection** is a vulnerability where an attacker inserts malicious SQL code into an input field to manipulate database queries

e.g : SELECT \* FROM users WHERE username = '' OR '1'='1' AND password = '';

1. How do exploitation frameworks assist in vulnerability analysis?

Exploitation frameworks automate the process of testing and demonstrating vulnerabilities by providing tools to exploit them. They help verify vulnerabilities, assess their impact, and streamline reporting

1. What is the primary function of OpenVAS?

The primary function of OpenVAS is to perform comprehensive vulnerability scanning and assessment. It identifies security weaknesses in systems and networks by scanning for known vulnerabilities and providing detailed reports and recommendations for remediation

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 and protecting sensitive information to avoid unauthorized access or damage. Additionally, responsible disclosure practices should be followed to ensure vulnerabilities are reported and remediated before public release

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

**Reporting** provides detailed information on identified vulnerabilities, enabling organizations to understand and prioritize risks. **Remediation** involves addressing and fixing these vulnerabilities to reduce security risks and improve overall protection

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 real- world scenarios.
3. Why are case studies important in learning about vulnerability analysis?

Case studies are important in vulnerability analysis because they provide real-world examples, highlight lessons learned, and enhance understanding of effective mitigation strategies

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

Case studies improve vulnerability analysis by providing real-world examples, showcasing best practices, and identifying common pitfalls

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

A comprehensive vulnerability analysis is critical when a financial institution upgrades its systems to protect sensitive data, ensure regulatory compliance, and prevent security breaches.

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

\*\*Lateral movement\*\* is the technique attackers use to navigate through a network to access additional systems and data. It’s done to expand access, find valuable targets, and evade detection.

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

**Nessus**, **OpenVAS**, or **OWASP ZAP** to assess system security.

1. What is the purpose of practical exercises in a vulnerability analysis course?

Practical exercises in a vulnerability analysis course provide hands-on experience in identifying and mitigating vulnerabilities, helping students apply theory to real-world scenarios and learn to use relevant tools.

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

A hands-on practical approach enhances understanding by letting students apply theory, gain real-world experience, and develop problem-solving skills with actual tools.

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

A comprehensive vulnerability analysis report includes an \*\*executive summary\*\* of key findings, detailed \*\*vulnerability descriptions\*\*, \*\*technical evidence\*\*, a \*\*risk assessment\*\*, \*\*remediation recommendations\*\*, and a \*\*conclusion\*\* on overall security posture.

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, assessing, and addressing security vulnerabilities, enabling participants to apply theoretical knowledge and develop practical skills in a real-world context.

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

Brute force and dictionary