CORVIT
Reaching end to end

LEARN RISE SHINE
NAVTTC

CEH based TEST
National Vocational and Technical Training Commission

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

Ans :The primary purpose of vulnerability scanning is to identify security weaknesses.

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

Ans :CVSS stands for Common Vulnerability Scoring System & major difference is the increased focus on user interaction, scope, and environmental factors in CVSS 3.0.

- **<u>Network </u>**type of scanning involves the use of tools like Nessus and OpenVAS.

- What is the first step in a vulnerability assessment?

Ans :The first step in a vulnerability assessment is asset identification.

- Define CVE and write about any CVE database that you know?

Ans : CVE stands for Common Vulnerabilities and Exposures. A well-known CVE database is the MITRE CVE database.

- OpenVAS stands for **Open Vulnerability Assessment System** Vulnerability Assessment System.
- The process of identifying vulnerabilities without automated tools is known as **Manual**______vulnerability assessment.

- Which automated scanner is known for its ability to detect a wide range of vulnerabilities with minimal configuration?
  Ans : Nessus is known for its ability to detect a wide range of vulnerabilities with minimal configuration.__________________________
  ____
- Security Information and Event Management (SIEM) systems often aggregate logdata from diverse sources, and advanced SIEM platforms leverage Correlation Rules and **Machine Learning** to identify sophisticated attack patterns.

- The vulnerability scanning technique that involves sending crafted packets to

  identify open ports is known as **Syn scanning**
- What does CVSS stand for?

Ans :Common Vulnerability Scoring System

scanning.

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

Ans :Metrics for assessing the severity of vulnerabilities based on exploitability, impact, and the environment.

- How does CVSS contribute to the prioritization of vulnerabilities?

Ans : By providing a standardized scoring system that helps in determining the criticality of vulnerabilities.

- **Vulnerability or CVE**_ databases are essential for keeping up-to-date with the latestvulnerabilities.

- List three best practices for effective vulnerability management.

Ans :Regular scanning, timely patching, and continuous monitoring.

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

Ans: By mapping discovered vulnerabilities to CVE IDs for easier tracking and remediation.

- Defense in Depth involves layering multiple security controls throughout an organization's IT environment to ensure that if one layer fails,**others will provide protection**.

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

- Explain the difference between automated and manual vulnerability scanning.

Ans:Automated scanning uses tools for efficiency, while manual scanning involves human analysis for deeper insights.

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

Ans :By allowing users to write scripts for custom scanning tasks.

- Compare and contrast Nessus and OpenVAS as vulnerability scanners.

Ans: Nessus is commercial with a broader range of plugins, while OpenVAS is open-source and free to use.

- Explain the role of Qualys in vulnerability management.

Ans : To provide cloud-based security and compliance solutions for vulnerability assessment, monitoring, and remediation.

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

Ans : A list of the most critical web application security risks.

- How can vulnerability assessments improve the security of web applications?

Ans :By identifying and addressing weaknesses before they can be exploited.

- _**Nessus**________is a widely used vulnerability scanner for assessing web applications.
- What is the focus of vulnerability analysis for mobile applications?

Ans:Identifying security weaknesses in the app's code, data storage, and communication.

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

- What are the common techniques used in vulnerability analysis for network devices?

Ans :Port scanning, configuration reviews, and firmware analysis

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

Ans: To ensure that they are not entry points for attackers.

- 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 _**phishing**____, a technique involving embedded code in seemingly benign files.
- Vulnerability analysis of network devices often focuses on **misconfigurations**_, configurations, and firmware.
- What are the typical steps involved in the reporting of vulnerabilities?

Ans: Identification, documentation, analysis, and reporting to the responsible parties.

- Define SQL injection and write an example of SQL injection?

Ans: SQL injection is a code injection technique used to attack data-driven applications by inserting malicious SQL statements into an entry field for execution.
Example: '; DROP TABLE Users; --

- How do exploitation frameworks assist in vulnerability analysis?

Ans: By Providing tools to test and exploit discovered vulnerabilities.

- What is the primary function of OpenVAS?

Ans: To perform comprehensive vulnerability scanning and management.

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

Ans : It includes responsible disclosure, ensuring no harm, and respecting privacy.

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

Ans: Use for ensures vulnerabilities are documented, prioritized, and addressed to enhance security.

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

- Why are case studies important in learning about vulnerability analysis?

Ans: Because they provide real-world examples and insights into how vulnerabilities are exploited and mitigated.

- How can case studies improve your approach to vulnerability analysis?

Ans : Can improve by offering practical lessons and strategies that can be applied in similar situations.

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

Ans : It would be critical is before launching a new system to ensure it is secure from potential attacks.

- Define lateral movement and why it's done?

Ans : Lateral movement is a technique used by attackers to move deeper into a network after compromising one system to reach critical assets.

- During the practical on vulnerability analysis, students may use tools like **Nmap** to assess system security.
- What is the purpose of practical exercises in a vulnerability analysis course?

Ans : To provide hands-on experience in identifying and addressing vulnerabilities.

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

Ans : By allowing learners to apply theoretical knowledge in real-world scenarios.

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

Ans : Findings, risk ratings, remediation recommendations, and executive summary.

- A well-conducted vulnerability analysis should lead to effective _**mitigation**_____ of discovered vulnerabilities.

- What is the goal of a practical vulnerability analysis session?

Ans: Goal is to identify and address security weaknesses in a controlled environment.

- _**Ethical**__________hacking is the practice of exploiting vulnerabilities in systems to gain unauthorized access.

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

Ans : Brute force and dictionary attacks.