CEH based TEST
National Vocational and Technical Training Commission

1. **A Port Scanner** scan is performed to detect open ports on a system.

2. What is the primary purpose of vulnerability scanning?

ANSWER: To **identify and assess potential security weaknesses or vulnerabilities** in systems, applications, or networks, allowing organizations to address these issues before they can be exploited by attackers.

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

ANSWER: CVSS (Common Vulnerability Scoring System) is a framework used to rate the severity of security vulnerabilities. The major difference between CVSS 2.0 and CVSS 3.0 is that **CVSS 3.0 includes additional metrics** such as environmental metrics, which allow for more accurate and context-aware scoring, making it more flexible and comprehensive compared to CVSS 2.0.

4. **Authenticated Scans:** type of scanning involves the use of tools like Nessus and OpenVAS.

5. What is the first step in a vulnerability assessment?

ANSWER: The first step in a vulnerability assessment is **asset identification and prioritization**, where the systems, applications, and data that need to be protected are identified and prioritized based on their importance to the organization.

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

ANSWER: CVE (Common Vulnerabilities and Exposures) is a list of publicly disclosed cybersecurity vulnerabilities and exposures. The **NVD (National Vulnerability Database)** is a CVE database maintained by the National Institute of Standards and Technology (NIST). It provides detailed information on each CVE entry, including severity scores, impact ratings, and mitigation advice.

7. OpenVAS stands for **Open** Vulnerability Assessment System.

8. The process of identifying vulnerabilities without automated tools is known as **manual** vulnerability assessment.

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

   ANSWER: The automated scanner known for its ability to detect a wide range of vulnerabilities with minimal configuration is **Nessus**.

10. 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.

11. The vulnerability scanning technique that involves sending crafted packets to identify open ports is known as **TCP SYN** scanning.

12. What does CVSS stand for?

    ANSWSER: Common Vulnerability Scoring System.

13. The database that maintains a list of known vulnerabilities is called a **CVE (Common Vulnerabilities and Exposures) database**.

14. Describe the key features of the Common Vulnerability Scoring System (CVSS).

ANSWER: Key features of the **Common Vulnerability Scoring System (CVSS)** include:

- **Base score**: Reflects the inherent severity of the vulnerability.
- **Temporal score**: Adjusts the base score based on the current environment and exploitability.
- **Environmental score**: Customizes the score based on the user's specific environment.

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

ANSWER: By providing a standardized scoring system that helps organizations assess the severity of vulnerabilities and prioritize remediation efforts based on their potential impact.

16. **VULNERABILITY** databases are essential for keeping up-to-date with the latest vulnerabilities.

17. List three best practices for effective vulnerability management.

    ANSWER: 1. Regular Scanning 2. Patch Management 3. Prioritization

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

    ANSWER: A vulnerability database like CVE can be integrated into an organization's vulnerability management program by:

- **Automated Tools Integration**: Using tools like Nessus or Qualys that reference CVE entries for identifying and tracking vulnerabilities.
- **Patch Management**: Leveraging CVE data to prioritize patching and updates based on the severity of vulnerabilities.
- **Reporting and Compliance**: Incorporating CVE references into vulnerability reports and ensuring compliance with industry standards.

19. Defense in Depth involves layering multiple security controls throughout an organization's IT environment to ensure that if one layer fails, **others remain to protect the system**.

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

22. Explain the difference between automated and manual vulnerability scanning.
    - **Automated Scanning**: Uses tools to quickly scan systems for known vulnerabilities, offering speed and coverage.
    - **Manual Scanning**: Involves human analysis to identify complex vulnerabilities that automated tools might miss, such as logic flaws.

23. Nmap's **SCRIPTING** Engine (NSE) is used for advanced vulnerability scanning.

24. How does the Nmap Scripting Engine (NSE) enhance the capabilities of Nmap?

ANSWER: The Nmap Scripting Engine (NSE) enhances the capabilities of Nmap by:

- **Custom Scripts**: Allowing users to write custom scripts to automate a wide range of tasks from vulnerability scanning to network discovery.
- **Extensive Library**: Providing a large library of pre-written scripts for specific scanning tasks.

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

ANSWER: Nessus vs. OpenVAS:

- **Nessus**: A commercial product known for its extensive vulnerability coverage, regular updates, and intuitive interface.
- **OpenVAS**: An open-source alternative, offering a wide range of features but requiring more configuration and maintenance.

26. Explain the role of Qualys in vulnerability management.

ANSWER: The role of **Qualys** in vulnerability management:

- **Cloud-based Platform**: Qualys provides a comprehensive suite of tools for vulnerability scanning, compliance management, and continuous monitoring.
- **Automation**: It automates the process of identifying, prioritizing, and remediating vulnerabilities across an organization's assets.

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

ANSWER: The **OWASP Top Ten** is a list of the most critical security risks to web applications, updated regularly by the Open Web Application Security Project.

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

ANSWER: Vulnerability assessments improve the security of web applications by:

- **Identifying Weaknesses**: Highlighting flaws that could be exploited by attackers.
- **Providing Recommendations**: Offering actionable steps to mitigate identified vulnerabilities.

30. **OWASP ZAP** is a widely used vulnerability scanner for assessing web applications.

31. What is the focus of vulnerability analysis for mobile applications?

ANSWER: The focus of vulnerability analysis for mobile applications:

- **Data Security**: Ensuring that sensitive data is protected in transit and at rest.
- **Authentication**: Verifying the implementation of secure authentication mechanisms.

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

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

ANSWER: Common techniques used in vulnerability analysis for network devices:

- **Firmware Analysis**: Checking for outdated or vulnerable firmware.
- **Configuration Review**: Ensuring devices are configured securely.
- **Port Scanning**: Identifying open ports that could be exploited.

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

ANSWER: It is important to conduct vulnerability analysis on network devices because:

- **Entry Points**: Network devices are often the first point of entry for attackers.
- **Impact**: Compromised devices can lead to a wider breach of the network.

35. 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.

36. Vulnerability analysis of network devices often focuses on **open ports**, configurations, and firmware.

37. What are the typical steps involved in the reporting of vulnerabilities?

ANSWER: The typical steps involved in the reporting of vulnerabilities:

- **Discovery**: Identifying and validating the vulnerability.
- **Documentation**: Recording details of the vulnerability, including impact and potential exploits.
- **Reporting**: Communicating the findings to relevant stakeholders, which may include the vendor or a public database.
- **Mitigation**: Suggesting or applying fixes or workarounds.
- **Verification**: Ensuring that the applied mitigations effectively address the vulnerability.

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

ANSWER: SQL Injection is a code injection technique where an attacker inserts malicious SQL statements into an input field, which are then executed by the database.

- Example: If a login form uses the query `SELECT * FROM users WHERE username = '$username' AND password = '$password'`, an attacker could input `username: admin' --` and `password: anything` to bypass authentication.

39. How do exploitation frameworks assist in vulnerability analysis?

ANSWER: Exploitation frameworks assist in vulnerability analysis by:

- **Automating Exploits**: Providing tools to exploit known vulnerabilities.
- **Validating Vulnerabilities**: Helping security professionals confirm the presence of a vulnerability.
- **Simulating Attacks**: Allowing security teams to understand how an attacker might exploit vulnerabilities.

40. What is the primary function of OpenVAS?

ANSWER: The primary function of **OpenVAS** is to perform comprehensive vulnerability scanning and management, identifying security issues across systems and networks.

41. Exploitation frameworks like **Metasploit** are used to simulate attacks on discovered vulnerabilities.

42. Discuss the ethical considerations involved in vulnerability analysis.

ANSWER: Ethical considerations in vulnerability analysis involve:

- **Permission**: Ensuring that the analysis is conducted with proper authorization.
- **Confidentiality**: Protecting sensitive data discovered during the analysis.
- **Responsibility**: Reporting vulnerabilities to the appropriate parties and not disclosing them to malicious actors.

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

ANSWER: The significance of reporting and remediation in the vulnerability management process:

- **Reporting**: Ensures that all stakeholders are aware of vulnerabilities and can take action.
- **Remediation**: Focuses on applying fixes to eliminate or mitigate the risks posed by vulnerabilities.

44. 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.
45. Case studies in vulnerability analysis often highlight **lessons learned** from real world scenarios.

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

ANSWER: Case studies are important in learning about vulnerability analysis because they provide:

- **Real-World Context**: Showing how vulnerabilities were exploited and remediated in actual situations.
- **Lessons Learned**: Offering insights into best practices and common pitfalls.

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

ANSWER: Case studies can improve your approach to vulnerability analysis by:

- **Learning from Mistakes**: Understanding how past vulnerabilities were handled helps avoid repeating the same mistakes.
- **Adopting Best Practices**: Gaining insights into successful strategies for identifying and mitigating vulnerabilities.

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

ANSWER: A scenario where comprehensive vulnerability analysis would be critical:

- **Critical Infrastructure**: In a power plant or financial institution, where a security breach could have severe consequences, thorough vulnerability analysis is essential to prevent catastrophic failures.

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

ANSWER: Lateral movement refers to the techniques used by attackers to move within a network after gaining initial access. It is done to access additional systems and data.

50. During the practical on vulnerability analysis, students may use tools like **NMAP** to assess system security.

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

ANSWER: The purpose of practical exercises in a vulnerability analysis course is to:

- **Apply Theoretical Knowledge**: Helping students practice and understand concepts in real-world scenarios.
- **Develop Skills**: Enhancing hands-on skills in identifying and mitigating vulnerabilities.

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

ANSWER: A hands-on practical approach enhances understanding of vulnerability analysis by:

- **Active Learning**: Engaging students in real-world scenarios to reinforce theoretical concepts.
- **Skill Building**: Providing the opportunity to develop and refine technical skills through practice

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

ANSWER: Key components of a comprehensive vulnerability analysis report:

- **Executive Summary**: An overview of findings and recommendations.
- **Detailed Findings**: In-depth analysis of each vulnerability discovered.
- **Risk Assessment**: Evaluation of the potential impact of the vulnerabilities.
- **Recommendations**: Suggested actions to remediate the identified vulnerabilities.
- **Appendices**: Supporting data, such as logs or screenshots.

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

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

ANSWER: The goal of a practical vulnerability analysis session is to:

- **Identify Vulnerabilities**: Find security weaknesses in systems.
- **Develop Mitigation Strategies**: Learn how to address and fix vulnerabilities.

56. **ETHICAL** hacking is the practice of exploiting vulnerabilities in systems to gain unauthorized access.

57. **PASSWORD** cracking tools are used to recover lost or stolen passwords.

58. Name two commonly used password-cracking techniques.

ANSWER: Two commonly used password-cracking techniques:

- **Brute Force**: Trying all possible combinations of characters until the correct password is found.
- **Dictionary Attack**: Using a pre-compiled list of possible passwords (a dictionary) to find the correct one.