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 primary purpose of vulnerability scanning is to identify security weaknesses and potential vulnerabilities in a system or network to prevent exploitation.

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

   CVSS (Common Vulnerability Scoring System) is a framework for assessing the severity of security vulnerabilities.

   The major difference between CVSS 2.0 and 3.0 is that CVSS 3.0 provides a more detailed, including Scope, User Interaction, and enhanced definitions for better risk assessment.

4. __Vulnerability____ type of scanning involves the use of tools like Nessus and OpenVAS.
5. What is the first step in a vulnerability assessment?

   The first step in vulnerability assessment is asset identification and enumeration,

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

   CVE (Common Vulnerabilities and Exposures) is a list of publicly disclosed security vulnerabilities with unique identifiers. The NVD (National Vulnerability Database) is a comprehensive database that enriches CVE entries with additional details and severity scores

7. OpenVAS stands for ____Open Vulnerability Assessment System Vulnerability Assessment System.

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

9. 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.

10. Security Information and Event Management (SIEM) systems often aggregate log data from diverse sources, and advanced SIEM platforms leverage Correlation Rules and Behavioral Analytics to identify sophisticated attack patterns.

11. The vulnerability scanning technique that involves sending crafted packets to identify open ports is known as Port scanning.
12. What does CVSS stand for?

    Common Vulnerability Scoring System.

13. The database that maintains a list of known vulnerabilities is called a database.
14. Describe the key features of the Common Vulnerability Scoring System (CVSS).

    Base Metrics: Assess the exploitability and impact of Vunerability.
    Temporal Metrics: Evalute the current state of the vulnerability.
    Environmental Metrics: Adjust e base and temporal metrics according to the specific environment wher the vulnerability exists.
    Score Calculation: Provides a numerical score and qualitative rating (e.g., Low, Medium, High, Critical) to indicate the severity of the Vulnerability.

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

    CVSS contributes to the prioritization of vulnerabilities by providing a standardized score that quantifies the severity of a vulnerability, allowing organizations to rank and address the most critical vulnerabilities first based on their potential impact and exploitability.

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

17. List three best practices for effective vulnerability management.

- **Regular Scanning:** Continuously perform vulnerability scans to identify new vulnerabilities and changes in the network environment.
- **Patch Management:** Timely apply patches and updates to address identified vulnerabilities.
- **Risk Assessment:** Prioritize vulnerabilities based on their severity, impact, and exploitability to allocate resources effectively.

18. 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 its unique identifiers to cross-reference and track vulnerabilities, leverage available details for assessment and remediation, and incorporate CVE data into automated scanning tools.

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

20. 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.

21. The Least Privilege Principle dictates that users and systems should have the minimum level of access necessary to perform their functions.

22. Explain the difference between automated and manual vulnerability scanning.

    Automated vulnerability scanning uses tools to quickly identify vulnerabilities based on predefined tests and signatures, while manual vulnerability scanning involves hands-on assessment by security experts to uncover vulnerabilities that automated tools may miss, providing a more nuanced evaluation.

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

24. 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 to perform advanced network scanning tasks, such as detecting specific vulnerabilities, gathering detailed information, and automating complex scanning processes.

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

Nessus is known for its extensive plugin library and ease of use, offering a wide range of vulnerability checks and a user-friendly interface. **OpenVAS** is open-source and provides a robust set of scanning features with frequent updates but may require more manual configuration and management.

26. Explain the role of Qualys in vulnerability management.

Qualys plays a role in vulnerability management by providing cloud-based security and compliance solutions, including vulnerability scanning, assessment, and management tools that help organizations identify, prioritize, and remediate vulnerabilities across their IT infrastructure.

27. The _OWASP Top Ten list is a critical resource for web application security.

28. What is the OWASP Top Ten?

The **OWASP Top Ten** is a list published by the Open Web Application Security Project that identifies the ten most critical web application security risks, providing a framework for understanding and mitigating common threats.

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

Vulnerability assessments can improve the security of web applications by identifying weaknesses in the application's code, configuration, and deployment, allowing for timely remediation and strengthening defenses against potential attacks.

30. __Burp Suite_ is a widely used vulnerability scanner for assessing web applications.

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

The focus of vulnerability analysis for mobile applications includes assessing issues related to insecure data storage, inadequate encryption, improper authentication, and other flaws specific to mobile platforms.

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

33. 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 reviews**, **firmware analysis**, and **penetration testing** to identify weaknesses and security gaps.

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

It is important to conduct vulnerability analysis on network devices to ensure they are secure from potential attacks, maintain the integrity of network infrastructure, and protect sensitive data and systems from being compromised.

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 malware, a technique involving embedded code in seemingly benign files.

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

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

- **Identification:** Detect and document the vulnerability.
- **Assessment:** Evaluate the severity and impact of the vulnerability.
- **Reporting:** Communicate the findings to relevant stakeholders with details and recommendations.
- **Remediation:** Collaborate on fixing the vulnerability.
- **Verification:** Confirm that the vulnerability has been effectively addressed.

38. Define SQL injection and write an example of SQL 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' --' AND password = 'password';`

39. How do exploitation frameworks assist in vulnerability analysis?

- Exploitation frameworks assist in vulnerability analysis by providing tools and methods to simulate attacks on discovered vulnerabilities, allowing analysts to assess the potential impact and effectiveness of security controls.

40. What is the primary function of OpenVAS?

The primary function of **OpenVAS** is to perform comprehensive vulnerability scanning and assessment to identify security weaknesses in 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.

- **Authorization:** Ensure you have permission to test the systems.
- **Data Protection:** Handle sensitive data responsibly and securely.
- **Disclosure:** Report vulnerabilities to the appropriate parties without causing harm.

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

Reporting and remediation are significant in the vulnerability management process as they ensure that vulnerabilities are not only identified but also addressed and fixed, reducing the risk of exploitation.

44. 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.
45. Case studies in vulnerability analysis often highlight __lessons learned__ from realworld scenarios.

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

    Case studies are important in learning about vulnerability analysis because they provide practical examples and insights into how vulnerabilities are exploited and managed in real-world situations.

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

    Case studies can improve your approach to vulnerability analysis by offering concrete examples of vulnerabilities and their impacts, helping you to better understand and anticipate potential issues.
48. Describe a scenario where comprehensive vulnerability analysis would be critical.

    A scenario where comprehensive vulnerability analysis would be critical is during a major software release or a security audit of a financial institution, where thorough testing is essential to protect sensitive data and ensure compliance with regulations.

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

    Lateral movement refers to the techniques attackers use to move from one system to another within a network to expand their access and achieve their goals. It is done to gain deeper access, access sensitive data, or maintain persistence.

50. During the practical on vulnerability analysis, students may use tools like __Nessus or OpenVAS_ to assess system security.

51. 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, allowing students to apply theoretical knowledge in real-world scenarios and develop practical skills.

52. 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 interact directly with tools and techniques, gaining firsthand experience in identifying and addressing vulnerabilities.

53. What are the key components of a comprehensive vulnerability analysis report?
    - **Executive Summary:** Overview of findings and risks.
    - **Detailed Findings:** Description of vulnerabilities and their impact.
    - **Risk Assessment:** Evaluation of severity and risk.
    - **Recommendations:** Suggested remediation steps.
    - **Supporting Evidence:** Proof of findings and test results.

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

55. 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, analyzing, and mitigating vulnerabilities in a controlled environment.

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.

- **Brute Force Attack:** Trying all possible combinations until the correct one is found.
- **Dictionary Attack:** Using a list of common passwords or phrases to guess the password.