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 and report security vulnerabilities in systems, networks and applications.

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

CVSS stands for Common Vulnerability Scoring System. It is a standardized framework for assessing the severity of security vulnerabilities.

The major difference between CVSS 2.0 and 3.0 is that, CVSS 3.0 provides more accurate scoring system.

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

Asset Discovery and Inventory is the first step in vulnerability assessment

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

CVE stands for Common Vulnerabilities and Exposures. It is a standardized system for identifying and cataloging publicly known cybersecurity vulnerabilities and exposures.

A CVE database I know is:
Exploit Database: A collection of exploits and vulnerabilities, including CVE identifiers, often with proof-of-concept code.

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?

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 Port scanning.

12. What does CVSS stand for?

CVSS stands for Common Vulnerability Scoring System

13. The database that maintains a list of known vulnerabilities is called a Vulnerability Database/ CVE Database.

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

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

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

CVSS contributes to the prioritization of vulnerabilities by providing a standardized and quantifiable measure of their severity.

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

17. List three best practices for effective vulnerability management.

1) Regular Scanning and Assessment
2)Prioritization and Risk Assessment
3)Timely Remediation and Patch Management

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

1) Automating Scans: Use CVE data in vulnerability scanners for up-to-date detection.
2) Prioritizing Risks: Use CVSS scores from CVE to assess and prioritize vulnerabilities.
3) Guiding Remediation: Reference CVE entries to identify patches and track fixes.

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

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 minimum level of access necessary to perform their functions.

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

Automated vulnerability scanning uses tools, while Manual vulnerability scanning involves human experts

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?

NSE enhances Nmap by enabling custom scripts for advanced vulnerability detection, detailed service information, and automation of complex scanning tasks.

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

Nessus is a commercial scanner with extensive features, frequent updates, and a user-friendly interface, while OpenVAS is an open-source tool that is free and flexible but may require more manual configuration and has slower updates.

26. Explain the role of Qualys in vulnerability management.

Qualys offers cloud-based vulnerability management with automated scanning, risk assessment, and compliance features to help organizations identify and address security vulnerabilities

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 of the ten most critical web application security risks
29. How can vulnerability assessments improve the security of web applications?

Vulnerability assessments improve web application security by identifying and prioritizing weaknesses, enabling focused remediation, and enhancing overall defenses.

30. OWASP Zap 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 is on identifying security flaws specific to mobile environments, such as insecure data storage and inadequate encryption.

32. Mobile application vulnerabilities can often be linked to Code 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, vulnerability scanning, configuration review, and penetration testing.

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

Conducting vulnerability analysis on network devices is important to identify and address security weaknesses that could be exploited by attackers, prevent unauthorized access, and protect sensitive data and network integrity.

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 Spear Phishing, a technique involving embedded code in seemingly benign files.

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

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

Typical steps in reporting vulnerabilities include discovery, assessment, reporting to stakeholders, recommending remediation, verification, and documentation.

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

SQL injection is a security vulnerability that occurs when an attacker inserts malicious SQL code into a query, allowing them to manipulate the database.

Example: ' OR 1 = 1 -- -

39. How do exploitation frameworks assist in vulnerability analysis?

Exploitation frameworks assist in vulnerability analysis by providing tools and modules to simulate attacks, identify and validate vulnerabilities, and assess the impact of exploiting these weaknesses in a controlled environment.

40. What is the primary function of OpenVAS?

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

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

42. Discuss the ethical considerations involved in vulnerability analysis.

Ethical considerations in vulnerability analysis include obtaining proper authorization before testing, ensuring the confidentiality of discovered vulnerabilities, and responsibly disclosing findings to avoid exploitation.

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

Reporting and remediation are crucial in vulnerability management as they ensure identified vulnerabilities are communicated to relevant stakeholders and addressed promptly, reducing the risk of exploitation and enhancing overall security.

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?

Case studies are important in learning about vulnerability analysis because they provide real-world examples of how vulnerabilities were exploited, the impact of those exploits, and effective strategies for detection, prevention, and response.

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

Case studies improve vulnerability analysis by providing real-world examples, highlighting best practices, identifying common pitfalls, and enhancing overall learning.

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

Comprehensive vulnerability analysis is critical during a major system overhaul or upgrade to ensure that newly integrated components are secure and do not introduce new vulnerabilities, protecting the organization from potential attacks.

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

Lateral movement is the technique used by attackers to move within a network after gaining initial access, aiming to find and exploit additional systems or data. It's done to escalate privileges, access more valuable information, and maintain persistence within the network.

50. During the practical on vulnerability analysis, students may use tools like Nessus 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 in identifying, assessing, and addressing security vulnerabilities, reinforcing theoretical knowledge through real-world applications and simulations.

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 learners to apply theoretical concepts in real scenarios, develop problem-solving skills, and gain experience with tools and techniques used in actual security assessments.

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

Key components of a comprehensive vulnerability analysis report include an executive summary, detailed vulnerability findings, risk assessment, recommended remediation actions, and a conclusion with follow-up steps.

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, assessing, and addressing security vulnerabilities to reinforce theoretical knowledge and develop practical skills.

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.

1) Brute-Force Attack

2) Dictionary Attack