CEH based TEST
National Vocational and Technical Training Commission

1. **Nmap** scan is performed to detect open ports on a system.
2. What is the primary purpose of vulnerability scanning?

**To protect the organization from breaches and the exposure of sensitive data**

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

**CVSS 3.0 is more granular and flexible than CVSS 2.0.**

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

**identifying assets and defining the assessment scope**.

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

**A unique identifier for publicly known cybersecurity vulnerabilities. NVD (National Vulnerability Database)**

OpenVAS stands for **Open Vulnerability Assessment System**

7. _____ Vulnerability Assessment System.
8. The process of identifying vulnerabilities without automated tools is known as **penetration testing** 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 **analytics** to identify sophisticated attack patterns.

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

12. What does CVSS stand for?
**Common Vulnerability Scoring System**

13. The database that maintains a list of known vulnerabilities is called a **Vulnerability database**.

14. Describe the key features of the Common Vulnerability Scoring System (CVSS).
**CVSS features Base, Temporal, and Environmental metrics,**

15. How does CVSS contribute to the prioritization of vulnerabilities?
**CVSS scores help prioritize vulnerabilities based on their severity and impact.**

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 Timely patching Risk prioritization**

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

**Use CVE data to identify, assess, and prioritize vulnerabilities within the organization's system.**

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

organization's IT environment to ensure that if one layer fails, **Another layer can still provide protection.**

_____.

20. Threat Intelligence Integration involves incorporating real-time information about current and emerging **Threat intelligence** 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 scanning** uses software tools to identify vulnerabilities, while **manual scanning** involves human analysts manually assessing systems for weaknesses.

23. Nmap's **Script** Engine (NSE) is used for advanced vulnerability scanning.
24. How does the Nmap Scripting Engine (NSE) enhance the capabilities of Nmap?
**enabling it to run scripts for various tasks, making it a more versatile and powerful tool for network scanning and security assessment.**

25. Compare and contrast Nessus and OpenVAS as vulnerability scanners.
**Nessus:** Commercial, feature-rich, and regularly updated. **OpenVAS:** Free, open-source, with community-driven updates and fewer features.

26. Explain the role of Qualys in vulnerability management.
**Qualys** provides cloud-based vulnerability management, scanning, and continuous monitoring for identifying and managing risks.

27. The **OWASP** Top Ten list is a critical resource for web application security.
28. What is the OWASP Top Ten? **A list of the top ten web application security risks**.
29. How can vulnerability assessments improve the security of web applications?
**Vulnerability assessments identify weaknesses, enabling timely fixes and reducing risks in web applications.**

30. **Effective** is a widely used vulnerability scanner for assessing web applications.
31. What is the focus of vulnerability analysis for mobile applications?
**he focus is on identifying security flaws specific to mobile platforms and app interactions.**

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 include port scanning, network mapping, and vulnerability scanning tools.**

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

**It identifies security weaknesses, prevents breaches, and ensures network integrity and protection.**

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 **social engineering**, 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, assessment, documentation, communication, and tracking of remediation efforts.**

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

**SQL injection is exploiting a vulnerability to execute arbitrary SQL commands. Example:** `'; DROP TABLE users;--`

39. How do exploitation frameworks assist in vulnerability analysis?

**They simulate attacks to test and validate vulnerabilities and assess their impact**.

40. What is the primary function of OpenVAS?

**OpenVAS is used for vulnerability scanning and assessment to identify security issues.**

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

**Ensure permission, avoid causing harm, report responsibly, and respect privacy and confidentiality.**

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

**Reporting highlights issues, while remediation fixes them, reducing risk and improving security.**

44. Zero Trust Architecture operates on the principle of " **never**_____, 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?

**They provide practical insights, illustrate real-world impacts, and guide effective security measures.**

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

**They offer examples of past mistakes and successes, informing better strategies and practices.**

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

**Analyzing a financial institution's systems before a major merger to ensure security integration.**

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

**Lateral movement involves moving within a network to access other systems after initial compromise, often to gain further access or escalate privileges.**

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?

**To provide hands-on experience, apply theoretical knowledge, and develop practical skills in vulnerability assessment.**

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

**t allows students to experience real-world scenarios, test theories, and develop practical problem-solving skills.**

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

Executive summary, vulnerability details, risk assessment, impact analysis, and remediation recommendations.

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?
o apply techniques, identify real vulnerabilities, and develop effective remediation strategies.

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.
Name two commonly used password-cracking techniques. • **Brute force**

1. • **Dictionary attack**