CEH based TEST

National Vocational and Technical Training Commission

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

7. OpenVAS stands for _____ Vulnerability Assessment System.
8. The process of identifying vulnerabilities without automated tools is known as _____ vulnerability assessment.

9. Which automated scanner 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 _____ to identify sophisticated attack patterns.

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

_____

_____

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

_____

_____

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

_____

_____

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

17. List three best practices for effective vulnerability management.

_____

_____

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

_____

_____

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

20. Threat Intelligence Integration involves incorporating real-time information about current and emerging _____ 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 _____ level of access necessary to perform their functions.

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

_____

_____

23. Nmap's _____ Engine (NSE) is used for advanced vulnerability scanning.
24. How does the Nmap Scripting Engine (NSE) enhance the capabilities of Nmap?

_____

_____

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

_____

_____

26. Explain the role of Qualys in vulnerability management.

_____

_____

27. The _____ Top Ten list is a critical resource for web application security.
28. What is the OWASP Top Ten?
29. How can vulnerability assessments improve the security of web applications?

_____

_____

30. _____ is a widely used vulnerability scanner for assessing web applications.
31. What is the focus of vulnerability analysis for mobile applications?

_____

_____

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

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

_____

_____

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

_____

_____

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 _____, a technique involving embedded code in seemingly benign files.
36. Vulnerability analysis of network devices often focuses on _____, configurations, and firmware.
37. What are the typical steps involved in the reporting of vulnerabilities?

_____

_____

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

_____

_____

39. How do exploitation frameworks assist in vulnerability analysis?

_____

_____

40. What is the primary function of OpenVAS?

_____

_____

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

_____

_____

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

_____

_____

44. Zero Trust Architecture operates on the principle of "_____, always verify," meaning that every access request is subjected to strict verification regardless of its origin.
45. Case studies in vulnerability analysis often highlight _____ from real-world scenarios.

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

_____

_____

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

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

_____

_____

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

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

58. Name two commonly used password-cracking techniques.

_____

_____