CORVIT
Reaching end to end

LEARN RISE SHINE
NAVTTC

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?

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 (Common Vulnerability Scoring System) assesses the severity of security vulnerabilities

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 a vulnerability assessment is to determine the assets that need to be protected.

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

CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed information security flaws.

i know exploit DB

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

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

Nessus is an automated scanner known for its ability

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?

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).

key features of the Common Vulnerability Scoring System (CVSS) is Exploitability, Scope, and Impact

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

This helps organizations assess and prioritize which vulnerabilities to address first based on their risk level

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

17. List three best practices for effective vulnerability management.

Prioritization,Verification and Reporting.

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

can be integrated into an organization's vulnerability management program by using CVE IDs for tracking, automating alerts, and enhancing risk assessment.

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 still provide protection

20. Threat Intelligence Integration involves incorporating real-time information about current and emerging ______threat__________ 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 for fast, systematic detection of vulnerabilities, while manual vulnerability scanning involves detailed, human-driven analysis for deeper context and complex issues.

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?

by allowing users to write and execute custom scripts for advanced scanning tasks, such as vulnerability detection, service enumeration, and exploitation.

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

Nessus is a widely used commercial vulnerability scanner known for its comprehensive coverage and frequent updates, while OpenVAS is an open-source alternative that offers a robust scanning framework but may have fewer updates and support compared to Nessus.

26. Explain the role of Qualys in vulnerability management.

Qualys provides cloud-based vulnerability management solutions that include continuous scanning, asset management, and threat intelligence to help organizations identify and address security risks.

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 that identifies and prioritizes the ten most critical web application security risks, providing guidelines

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

by identifying and addressing weaknesses, helping to prevent exploits and reduce the risk of breaches.

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 for mobile applications is on identifying security flaws specific to mobile platforms, such as insecure data storage and weak authentication.

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

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

port scanning, configuration review, and vulnerability scanning.

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

identify and mitigate security weaknesses

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, assessment, documentation, notification, and tracking.

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

SQL Injection is a type of attack where an attacker inserts or manipulates SQL queries in a web application's input fields to execute unauthorized commands on the database. For example:

```
SELECT * FROM users WHERE username = 'admin' AND password = ''; --
```

39. How do exploitation frameworks assist in vulnerability analysis?

Exploitation frameworks assist in vulnerability analysis by providing tools and modules to simulate attacks, test the effectiveness of security controls, and assess the real-world impact of discovered vulnerabilities.

40. What is the primary function of OpenVAS?

The primary function of OpenVAS is to provide a comprehensive open-source vulnerability scanning and management solution to identify and assess security vulnerabilities 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.

Ethical considerations in vulnerability analysis include obtaining proper authorization before testing, ensuring minimal disruption to systems, protecting sensitive data, and reporting findings responsibly to help improve security without causing harm.

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

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 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 offer **real-world examples** and insights into how vulnerabilities are exploited and mitigated.

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 Nessus 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 remediation of discovered vulnerabilities.

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

to identify, assess, and remediate security weaknesses in systems using real-world tools and techniques to improve overall security posture.

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 and dictionary attacks.