CORVIT
Reaching end to end

NAVTTC
LEARN RISE SHINE

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 find cybersecurity weakness in a network, device, or system. After the vulnerability scanning, vulnerability assessment report is generated based on which organization plan security defences.

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 method for assessing the severity of computer system security vulnerabilities. CVSS score ranges from 0 to 10, with 10 being the most severe.CVSS v3.0 provides a more comprehensive and accurate assessment of vulnerability severity compared to CVSS v2.0

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?

Perform vulnerability scanning

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

CVE stands for Common Vulnerabilities and Exposures. It is a publicly available list of known vulnerabilities and exposures. Similarly, National Vulnerability Database (NVD) is a comprehensive database of known vulnerabilities maintained by the National Institute of Standards and Technology (NIST).

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?

nmap

10. Security Information and Event Management (SIEM) systems often aggregate log data from diverse sources, and advanced SIEM platforms leverage Correlation Rules and User and Entity Behavior Analytics (UEBA) 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).

CVSS provides support for: Base Metrics: These metrics represent the intrinsic characteristics of a vulnerability
Threat Metrics: These metrics reflect the characteristics that may change over time
Environmental Metrics: These metrics account for the unique characteristics of a user's environment
Supplemental Metrics: These metrics provide additional context about the vulnerability

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

CVSS contributes to the prioritization of vulnerabilities through its standardized scoring system, which helps organizations assess and rank vulnerabilities based on their severity and potential impact

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

17. List three best practices for effective vulnerability management.

1) Continuous Asset Discovery and Inventory; 2) Prioritize Vulnerabilities Based on Risk; 3) Regular Scanning and Remediation

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

Through SIEM 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 are in place to provide backup protection against potential threats.

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 offers speed, efficiency, and cost-effectiveness for identifying common vulnerabilities, manual scanning provides deeper insights and the ability to detect complex security issues. Organizations often benefit from a combination of both methods

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?

Nmap Scripting Engine (NSE) significantly enhances the capabilities of Nmap by allowing users to automate and customize network scanning tasks through the use of scripts

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

OpenVAS is an open-source tool available for free, making it an attractive option for organizations with limited budgets.Nessus offers both a free version (Nessus Essentials) with limited functionality and commercial versions with advanced features, which come at a cost.

26. Explain the role of Qualys in vulnerability management.

Qualys plays a crucial role in vulnerability management by providing a comprehensive, cloud-based platform designed to continuously identify, assess, and remediate vulnerabilities across an organization IT environment

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

28. What is the OWASP Top Ten? Open Web Application Security Project

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

by identifying the security weaknesses

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 is to identify potential security weaknesses and risks that could be exploited by attackers

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

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

Port Scanning, Version Scanning, Vulnerability Signature Matching, Fuzzing

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

It helps to get: Identification of Security Flaws, Risk Mitigation, Compliance Requirements, Enhanced Incident Response, Continuous Monitoring and Improvement

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

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

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

Identify the Vulnerability, Verify and Reproduce the Vulnerability, Determine the Affected Party, Prepare the Vulnerability Report, Submit the Vulnerability Report, Engage in Responsible Disclosure

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

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. An attacker could exploit this by entering the following: Username: admin' OR '1'='1 and Password: anything

39. How do exploitation frameworks assist in vulnerability analysis?

Exploitation frameworks, such as Metasploit, play a crucial role in vulnerability analysis by providing a structured environment to test and validate security vulnerabilities.

40. What is the primary function of OpenVAS?

The primary function of OpenVAS is to perform comprehensive vulnerability scanning and management. It helps identify security issues such as misconfigurations, outdated software, and weak passwords that could b

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

42. Discuss the ethical considerations involved in vulnerability analysis.

Vulnerability analysis, especially in the context of cybersecurity and research, involves several ethical considerations to ensure that the process is conducted responsibly and ethically

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

Together, reporting and remediation form a comprehensive approach to vulnerability management. Reporting ensures that vulnerabilities are identified, documented, and prioritized, while remediation focuses on addressing these vulnerabilities to mitigate risks and improve 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?

By providing detailed, real-world examples, case studies enhance understanding, improve skills, and offer valuable lessons that can be applied to future vulnerability analysis efforts. They are a powerful tool for continuous learning and improvement in the field of cybersecurity

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

Case studies provide real-world examples and lessons learned, helping you understand effective strategies and common pitfalls in vulnerability analysis. They enhance critical thinking and decision-making skills by presenting practical scenarios.

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

A comprehensive vulnerability analysis is critical when a financial institution upgrades its online banking system to ensure no security gaps could be exploited by cybercriminals.
This protects sensitive customer data and maintains trust in the institution's security measures.

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

Lateral movement in cybersecurity refers to the techniques attackers use to move through a network after gaining initial access. This allows them to explore the network, escalate privileges, and access sensitive data or system

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

Practical exercises in a vulnerability analysis course provide hands-on experience in identifying and mitigating vulnerabilities, helping students apply theory to real-world scenarios and learn to use relevant tools.

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

A hands-on practical approach enhances understanding by letting students apply theory, gain real-world experience, and develop problem-solving skills with actual tools.

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

A comprehensive vulnerability analysis report includes an **executive summary** of key findings, detailed **vulnerability descriptions**, **technical evidence**, a **risk assessment**, **remediation recommendations**, and a **conclusion** on overall security posture.

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, enabling participants to apply theoretical knowledge and develop practical skills in a real-world context

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