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?

   The primary purpose of vulnerability scanning in cybersecurity is to identify weaknesses or security holes in a system or network.

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. The major difference between CVSS 2.0 and CVSS 3.0 is that CVSS 3.0 includes enhancements such as increased granularity in scoring, a focus on exploitability and impact metrics, and a more consistent scoring approach compared to 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?

The first step in a vulnerability assessment in cybersecurity is "preparation." It involves defining the scope, goals, and objectives of the assessment.

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

CVE stands for Common Vulnerabilities and Exposures. One popular CVE database is the National Vulnerability Database (NVD) maintained by NIST in the US.

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?

Ans: **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 **SYN** scanning.

12. What does CVSS stand for?

    Common Vulnerability Scoring System

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

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

    CVSS provides a numerical score to rate the severity of security vulnerabilities based on exploitability, impact, and complexity.

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

    CVSS gives a number to show how bad a security issue is. This helps decide which problems need fixing first to make things safer online.

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

17. List three best practices for effective vulnerability management.

- Keeping software up-to-date,
- Using strong passwords,
- Being cautious about clicking on unknown links or emails.

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

    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, **others can still protect the system.**

20. Threat Intelligence Integration involves incorporating real-time information about current and emerging **Threads** 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 to scan for vulnerabilities quickly, while manual scanning involves human experts conducting in-depth assessments for security gaps.

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?

The Nmap Scripting Engine (NSE) boosts Nmap's abilities by allowing customized scripts to automate tasks and perform advanced security checks.

25. Compare and contrast Nessus and OpenVAS as vulnerability scanners.
    - **Nessus: user-friendly, extensive database.**
    - **OpenVAS: open-source, customizable.**

26. Explain the role of Qualys in vulnerability management.

Qualys helps manage vulnerabilities by offering cloud-based solutions for monitoring and fixing security issues in IT systems.

27. The **OWASP** Top Ten list is a critical resource for web application security.
28. What is the OWASP Top Ten?

List of the most critical security risks to web applications, created to raise awareness and promote best practices.

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

To Identifying and addressing weaknesses that could be exploited by attackers, thereby reducing the risk of breaches.

---

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

To identifying security flaws in app code, data storage, and communication mechanisms.

---

32. Mobile application vulnerabilities can often be linked to **Poor Code** flaws.

33. What are the common techniques used in vulnerability analysis for network devices?
    - **Port scanning,**
    - **Firmware analysis,**
    - **Configuration auditing.**

34. Why is it important to conduct vulnerability analysis on network devices?
    these devices are critical to the overall security of a network, and vulnerabilities in them can lead to significant breaches.

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 **authentication mechanisms**, configurations, and firmware.

37. What are the typical steps involved in the reporting of vulnerabilities?
    - **identification,**
    - **documentation,**
    - **impact assessment,**
    - **notification of relevant stakeholders.**

38. Define SQL injection and write an example of SQL injection?
    SQL injection is a type of attack where an attacker inserts malicious SQL code into a query to manipulate the database, for example: `SELECT * FROM users WHERE username = 'admin'--' AND password = 'password';`.

39. How do exploitation frameworks assist in vulnerability analysis?
    Providing tools to simulate real-world attacks, allowing security teams to test the effectiveness of their defenses.

40. What is the primary function of OpenVAS?
    Perform comprehensive vulnerability scanning and management.

41. Exploitation frameworks like **Metasploit** are used to simulate attacks on discovered vulnerabilities.
42. Discuss the ethical considerations involved in vulnerability analysis.
    Obtaining proper authorization, ensuring privacy, and avoiding harm while conducting assessments.

43. What is the significance of reporting and remediation in the vulnerability management process?
    It ensures vulnerabilities are documented, prioritized, and addressed to reduce the risk of exploitation.

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?
    They provide practical insights and examples of how vulnerabilities were identified and mitigated in real situations.

47. How can case studies improve your approach to vulnerability analysis?
    Offering lessons on effective strategies, common pitfalls, and innovative solutions used by others.

48. Describe a scenario where comprehensive vulnerability analysis would be critical.
    Before the deployment of a new network infrastructure to ensure all potential security risks are identified and mitigated.

49. Define lateral movement and why it's done?
    Lateral movement is the process where attackers move through a network to gain access to additional systems or data after initially compromising a single point.

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?
    Provide hands-on experience in identifying and addressing security vulnerabilities.

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

    Allowing students to apply theoretical knowledge to real-world scenarios, thereby reinforcing learning.

____

____

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

    An executive summary, detailed findings, risk assessment, and remediation recommendations.

____

____

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

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

Apply theoretical knowledge in a hands-on environment to identify, analyze, and mitigate security vulnerabilities.

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**
- **Dictionary attacks**.