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 main aim of vulnerability scanning is to find security flaws and weaknesses in a system or network, so that these problems may be solved by organizations before they are exploited by attackers.

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

CVSS is a framework used to evaluate the extent of severity of security vulnerabilities. CVSS 3.0 enhances CVSS 2.0 by introducing additional metrics and improved scoring criteria for better vulnerability evaluations.

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 is the first step in a vulnerability assessment to determine which systems, applications, and data need to be evaluated for vulnerabilities.

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

A system to identify and name publicly known cybersecurity vulnerabilities is known as CVE. With respect to this, the National Vulnerability Database (NVD) offers extensive information together with severity scores for these vulnerabilities.

7. OpenVAS stands for Open Vulnerability Assessment System 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?

With minimum configuration, Nessus becomes a tool which is capable of detecting many vulnerabilities.

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 CVE database.

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

* Standardized scoring system (0-10) for vulnerability severity.
* Considers exploitability, remediation status, and impact.
* Provides Base, Temporal, and Environmental scores for comprehensive assessment

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

By providing a numerical score that reflects the severity of each vulnerability, allowing organizations to focus on the most critical issues first.

16. CVE 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, and continuous monitoring of systems

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

Automating the import of CVE data into security tools and using it to prioritize and remediate vulnerabilities

19. Defense in Depth involves layering multiple security controls throughout an organization's IT environment to ensure that if one layer fails, other security controls remain in place to mitigate the attack.

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: Uses tools like Nessus or OpenVAS, is faster and efficient for large networks but has limited scope and customization. Manual: Involves penetration testing and code review, is more thorough and can identify complex vulnerabilities, but is time-consuming and requires skilled personnel.

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's Scripting Engine (NSE) adds numerous capabilities because it allows users to write their own programs or perform them using scripts in order to achieve automation and get detailed reports on the services available and any vulnerabilities present in the network.

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

Nessus is known for its extensive plugin library, low false positive rate, and ease of use, making it suitable for enterprises. OpenVAS is an open-source tool offering customizable scanning options and is more budget-friendly, ideal for smaller security teams

26. Explain the role of Qualys in vulnerability management.

Qualys provides cloud-based vulnerability management solutions that automate scanning, continuous monitoring, and detailed reporting. This helps organizations identify, assess, and remediate security vulnerabilities effectively.

27. The _____OWASP_____ 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?

by identifying weaknesses and potential entry points, allowing for remediation before attackers can exploit them.

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

identifying flaws specific to mobile environments, such as insecure data storage, improper implementation of security controls, and issues with app permissions

32. Mobile application vulnerabilities can often be linked to _____insecure coding_____ flaws.

question no 28 answer: The OWASP Top Ten is a list of the most critical security risks to web applications, providing guidelines and best practices for mitigating these risks.

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

port scanning, network mapping, and configuration review

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

to identify and address potential security weaknesses, preventing unauthorized access and reducing risk

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, classification, risk assessment, and communication

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

SQL injection is a type of attack where malicious SQL queries are inserted into input fields to manipulate the database e.g OR '1'='1

39. How do exploitation frameworks assist in vulnerability analysis?

by providing tools and scripts to simulate attacks, allowing for testing and validation of vulnerabilities

40. What is the primary function of OpenVAS?

automated vulnerability scanning

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 ensuring consent from stakeholders, avoiding unauthorized access, and responsibly disclosing vulnerabilities to prevent misuse

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

document vulnerabilities, track mitigation efforts, and ensure that security weaknesses are addressed effectively

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.

_____

_____