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 check the system or web application have any vulnerable patches that can be exploited and result in gain unauthorized access of the system

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

CVSS attempts to assign severity scores to vulnerabilities.

4. Many 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 is information gathering

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

Each CVE entry provides a unique identifier (CVE ID) for a specific vulnerability or exposure, making it easier for organizations and security tools to share and reference information about cybersecurity issues. Shodan is also the CVE database

7. OpenVAS stands for open source 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?
Nessus

10. Security Information and Event Management (SIEM) systems often aggregate log data from diverse sources, and advanced SIEM platforms leverage Correlation Rules and Anomaly Detection to identify sophisticated attack patterns.

11. The vulnerability scanning technique that involves sending crafted packets to identify open ports is known as Port Scanning scanning.
12. What does CVSS stand for?
common vulnerabily scoring system

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

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

16. Vulnerability databases 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, other layers will continue to provide protection.

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.

Utilizes various tools and techniques but involves human input for analysis. and in automated Utilizes specialized software such as Nessus, OpenVAS, or Qualys to perform scans.

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?

NSE scripts are written in the Lua programming language and can be used to perform detailed vulnerability assessments on discovered services.

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

26. Explain the role of Qualys in vulnerability management.

27. The owasp top ten 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?

it is use to identify the vulnerablities in system first you will obviously identify then you treat the vulnerablity

30. owasp zap 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 Development flaws.

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

1- network scanning and vulnerablity scannning

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 spear-phishing emails, a technique involving embedded code in seemingly benign files.
36. Vulnerability analysis of network devices often focuses on network services, 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?

this attack is carried on website through their login pages to again unauthorized admin access
this use standard query language to reshape the query like to comment out the query etc Username: admin Password: ' OR '1'='1

39. How do exploitation frameworks assist in vulnerability analysis?

40. What is the primary function of OpenVAS?

The primary function of OpenVAS (Open Vulnerability Assessment System) is to perform vulnerability scanning and assessment

41. Exploitation frameworks like metasploit 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?

reporting is not so significant but remediation is very significant beacuse how you take care of of vulnerablity is remediation

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 lesson learnt 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 provide real-world examples and practical insights into how vulnerabilities are discovered, exploited, and mitigated.

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

Case studies improve your approach to vulnerability analysis by offering real-world examples and practical insights that refine detection, assessment, and remediation techniques.

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 secure sensitive customer data from potential cyberattacks.

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

The technique used by cyber attacker to move through the networks and search for key data and assets that ultimately the target of hacker campaign.

50. During the practical on vulnerability analysis, students may use tools like ZAP 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.

A hands-on practical approach enhances understanding of vulnerability analysis by allowing direct interaction with systems, tools,

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

1- methods used for analysis
2- Savernity of vulnerablity
3- how to comeup with solution

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

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

To have an idea that where we can gain acces of the system by using the paches that are vulnerable

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

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

58. Name two commonly used password-cracking techniques.

1- Brute force cracking 2- Dictionary Attack