CEH based TEST

National Vocational and Technical Training Commission

1. A Port Scan scan is performed to detect open ports on a system.
2. What is the primary purpose of vulnerability scanning?

The purpose of vulnerability scanning is to identify security weaknesses in systems, networks, or applications.

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. Major dufference between these to is CVSS3.0 is better beacuse it has more details and new ways to measure the impact of a problem

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?

Information gathering

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 cybersecurity vulnerabilities and exposures that affect software and hardware systems. One well-known CVE database is the National Vulnerability Database (NVD)

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?

openvass

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?

CVSS stands for Common Vulnerability Scoring System

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

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

Base Metrics
Temporal Metrics
Environmental Metrics

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

CVSS provides a standardized score that helps prioritize vulnerabilities based on their severity and potential impact.

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

17. List three best practices for effective vulnerability management.

Regularly perform vulnerability scans.
Implement a robust patch management process.
Prioritize vulnerabilities based on risk.

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

By cross-referencing the vulnerabilities found in the scans against the CVE database, you can implement consistent and effective remediation processes.

19. Defense in Depth involves layering multiple security controls throughout an organization's IT environment to ensure that if one layer fails, another layer can help prevent a successful 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 vulnerability scanning is the process performed by tools that search for known vulnerabilities across a network at a quick pace. On the other hand, manual vulnerability scanning involves human analysis in finding less obvious or more complex vulnerabilities.

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?

This allows users to write scripts or just use predefined ones for advanced scanning, which automatizes many things. This makes Nmap even more versatile at detecting vulnerabilities.

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

Nessus is a commercial scanner with comprehensive plugins and regular updates. OpenVAS represents the alternative in open source and provides extensive scanning capability, but with more manual configuration.

26. Explain the role of Qualys in vulnerability management.

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 of the most critical web application security risks. It is published by the Open Web Application Security Project (OWASP)
29. How can vulnerability assessments improve the security of web applications?

identify and address security flaws to reduce the risk of breaches.

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

Identifying and mitigating security risks specific to mobile platforms, such as insecure data storage and improper platform usage.

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

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

Techniques include configuration reviews, firmware analysis, and network scanning to detect weaknesses in routers, switches, and firewalls.

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

Ensure network integrity and prevent attackers from exploiting weaknesses in critical 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 _____, a technique involving embedded code in seemingly benign files.
36. Vulnerability analysis of network devices often focuses on Protocols, configurations, and firmware.
37. What are the typical steps involved in the reporting of vulnerabilities?

Identifying, assessing, documenting, and reporting vulnerabilities with recommended remediation steps.

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

SQL injection injects malicious SQL queries into input fields to exploit vulnerabilities. Example: '" OR '1'='1' --".

39. How do exploitation frameworks assist in vulnerability analysis?

They automate exploit testing and help confirm vulnerabilities.

40. What is the primary function of OpenVAS?

OpenVAS is an open-source tool used for vulnerability scanning and management, identifying security weaknesses 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.

Some of the ethical considerations involve getting proper authorization before testing, making sure tests do not disrupt operations, and responsible disclosure of vulnerabilities to affected parties without undue exposure to risk.

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

It allows vulnerability reporting in identification to relevant stakeholders and informs them, while remediation is the actions taken to fix or mitigate identified risks, reducing the likelihood 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 examples from the wild on how vulnerabilities have been exploited and mitigated with practical insights and lessons learned to improve security practices.

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

~~Such training will help you polish your analysis techniques by reading experiences, examining other people's~~ mistakes and successes, and better prepare for problems one may encounter.

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

A new software application massively deployed in the enterprise network, and discovering vulnerabilities within it resulted in extensive data breaches or system failures.

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

Lateral movement refers to a technique attackers use after gaining an initial foothold to gain deeper entry into a network. This will help them to explore the network and escalate privileges to critical systems and data.

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

The students will receive hands-on experience in searching, analyzing, and mitigating vulnerabilities in real-life environments.

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

~~This would allow students to apply theoretical knowledge in practical situations and enable them~~ to acquire skills related to the identification and mitigation of security risk

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

The report is comprised of a vulnerability identification, risk assessment, impact analysis, recommended remediation steps, and summary of the findings.

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?

This course helps students develop the right skills and knowledge to identify and mitigate security vulnerabilities in various environments.

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 Attack