Corvit CEH Based Test Solution

Submitted by: M Zeeshan Zafar

Submitted to: M Bilal

1. **A network/SYN scan is performed to detect open ports on a system.**
2. **What is the primary purpose of vulnerability scanning?**
   - To identify security weaknesses in a system or network before attackers can exploit them.
3. **What is CVSS and what is the major difference between CVSS 2.0 and CVSS 3.0?**
   - **CVSS**: Common Vulnerability Scoring System.
   - **Difference**: CVSS 3.0 provides more granularity in the scoring metrics and includes environmental and temporal metrics that are more detailed compared to CVSS 2.0.
4. **Active type of scanning involves the use of tools like Nessus and OpenVAS.**
5. **What is the first step in a vulnerability assessment?**
   - Identifying and defining the assets and scope of the assessment.
6. **Define CVE and write about any CVE database that you know.**
   - **CVE**: Common Vulnerabilities and Exposures. It is a list of publicly known cybersecurity vulnerabilities.
   - **CVE Database**: Maintained by MITRE, it provides a reference-method for publicly known information-security vulnerabilities and exposures.
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?**
   - **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 and Analytics to identify sophisticated attack patterns.**

11. **The vulnerability scanning technique that involves sending crafted packets to identify open ports is known as TCP 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 database**.
14. **Describe the key features of the Common Vulnerability Scoring System (CVSS).**

- CVSS provides a standardized way to assess the severity of computer system security vulnerabilities, combining three metric groups: Base, Temporal, and Environmental to calculate a score reflecting the severity of a vulnerability.

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

- CVSS scores help organizations prioritize vulnerabilities based on their severity, impact, and exploitability, enabling more efficient resource allocation for remediation.

16. **CVE/Vulnerability databases are essential for keeping up-to-date with the latest vulnerabilities.**
17. **List three best practices for effective vulnerability management.**

- Regular vulnerability scanning and patching.
- Implementing security controls and monitoring.
- Conducting periodic security assessments and audits.

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

- By using CVE identifiers to track vulnerabilities in systems, allowing for consistent reporting, tracking, and remediation prioritization.

19. **Defense in Depth involves layering multiple security controls throughout an organization's IT environment to ensure that if one layer fails, others will prevent or mitigate an 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 minimal level of access necessary to perform their functions.**
22. **Explain the difference between automated and manual vulnerability scanning.**

- **Automated scanning** uses tools to quickly scan systems for vulnerabilities, while **manual scanning** involves human analysis to identify more complex vulnerabilities that tools may miss.

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 allows users to write scripts for customized scanning, enhancing Nmap's ability to detect specific vulnerabilities and perform complex network tasks.

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

- **Nessus**: Commercial, regularly updated, with extensive plugin support.
- **OpenVAS**: Open-source, community-supported, suitable for organizations preferring open solutions.

26. **Explain the role of Qualys in vulnerability management.**

- Qualys provides cloud-based solutions for vulnerability management, allowing organizations to detect and manage vulnerabilities across their IT assets.

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

- A standard awareness document for developers and web application security, representing a broad consensus about the most critical security risks to web applications.

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

- By identifying and mitigating security flaws, ensuring compliance with security standards, and reducing the risk of exploitation.

30. **OWASP ZAP is a widely used vulnerability scanner for assessing web applications (Burpsuite is a framework, not scanner).**
31. **What is the focus of vulnerability analysis for mobile applications?**

- Protecting sensitive data, ensuring secure communication, and preventing unauthorized access.

32. **Mobile application vulnerabilities can often be linked to insecure coding OR software flaws.**
33. **What are the common techniques used in vulnerability analysis for network devices?**

- Configuration reviews, firmware analysis, and network protocol testing.

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

- To ensure network security by identifying potential vulnerabilities that could be exploited to compromise the entire network.

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/watermarking , a technique involving embedded code in seemingly benign files.**
36. **Vulnerability analysis of network devices often focuses on hardware, weak passwords, configurations, and firmware.**

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

- Identifying the vulnerability, documenting its details, assessing its impact, and reporting to relevant stakeholders.

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

- **SQL Injection**: A code injection technique that exploits vulnerabilities in an application's software by injecting malicious SQL code into a query.
- **Example**: ' OR '1'='1' --.

39. **How do exploitation frameworks assist in vulnerability analysis?**

- By providing tools and scripts to automate the exploitation of identified vulnerabilities, allowing for easier testing and validation of security controls.

40. **What is the primary function of OpenVAS?**

- To perform comprehensive vulnerability scanning and management for network security assessments.

41. **Exploitation frameworks like Metasploit are used to simulate attacks on discovered vulnerabilities.**
42. **Discuss the ethical considerations involved in vulnerability analysis.**

- Ensuring that the analysis does not cause harm, obtaining proper authorization, respecting privacy, and disclosing findings responsibly.

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

- Accurate reporting enables organizations to understand vulnerabilities and take timely action, while remediation helps in mitigating risks and improving security posture.

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 real-world examples of vulnerabilities, their impact, and effective remediation strategies, enhancing learning through practical scenarios.

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

- By learning from real incidents, identifying common mistakes, and applying best practices to avoid similar issues.

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

- In a financial institution handling sensitive customer data, comprehensive analysis is vital to prevent data breaches and ensure compliance with regulations.

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

- **Lateral Movement**: The technique attackers use to move within a network after gaining initial access, to find and access additional systems or 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?**

- To provide hands-on experience, reinforcing theoretical knowledge and enhancing skills in identifying and mitigating vulnerabilities.

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

- By allowing learners to directly interact with tools and scenarios, gaining experience in identifying and resolving real-world vulnerabilities.

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

- Executive summary, identified vulnerabilities, risk assessments, recommendations, and remediation steps.

54. **A well-conducted vulnerability analysis should lead to effective mitigation/ remediation of discovered vulnerabilities.**
55. **What is the goal of a practical vulnerability analysis session?**

- To develop skills in identifying, analyzing, and mitigating vulnerabilities through hands-on practice.

56. **Black Hat 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**