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?

ANS: The purpose of scanning is to get the vulnerabilities in our system and network.

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

ANS:CVSS stand for Common Vulnerability Scoring System .The main difference between CVSS 2.0 and CVSS 3.0 is that CVSS 3.0 get more comprehensive scoring system according to the severity of the vulnerability .

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?

ANS: The first step is to determine the resources to be protected.

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

ANS:CVE (Common Vulnerabilities and Exposures) is a reference system for publicly known information-security vulnerabilities and exposures.The CVE database is Exploitdb .

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?

Answer: 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?

Answer: Common Vulnerability Scoring System

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

ANS:Exploitdb

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

Answer: CVSS provides a method for rating the severity of security vulnerabilities. Key features help in determining the urgency of a vulnerability in different contexts.

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

Answer: By providing a numerical score that helps organizations assess the risk level and determine which vulnerabilities need immediate attention.

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

17.List three best practices for effective vulnerability management.

Regularly update and patch systems.

Conduct frequent vulnerability scans.

Prioritize vulnerabilities based on risk assessment.

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

vulnerability management program?

Answer: A vulnerability database like CVE can be integrated by using it to identify known vulnerabilities in systems, allowing for automated scanning and reporting, and assisting in the process.

19.Defense in Depth involves layering multiple security controls throughout an

organization's IT environment to ensure that if one layer fails, **.others will still 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.

Automated vulnerability scanning uses tools to scan systems quickly and efficiently with minimal human intervention FOREXAMPLE: openvas,nessus,nmap**, while manual vulnerability scanning involves human analysts who manually check systems for vulnerabilities, often providing more in-depth analysis but at a slower pace.**

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?

Answer: The Nmap Scripting Engine (NSE) enhances Nmap by allowing users to write scripts to automate a wide range of tasks.

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

Answer: Nessus is a commercial vulnerability scanner and easy to use, while OpenVAS is an open-source alternative that give similar functionality but may require more manual configuration and maintained data.

26.Explain the role of Qualys in vulnerability management.

Answer: Qualys is a cloud-based platform that offers vulnerability management, including continuous monitoring, scanning, and reporting, helping organizations maintain a secure IT environment.

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

28.What is the OWASP Top Ten?

Answer: The OWASP Top Ten is a list of the most critical security risks to web applications, published by the Open Web Application Security Project (OWASP) to guide developers and security professionals in improving web security.

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

Answer: Vulnerability assessments can improve the security of web applications by identifying and addressing security weaknesses in the system to avoid attackers.

30.**Burp Suite** is a widely used vulnerability scanner for assessing web applications.

31.What is the focus of vulnerability analysis for mobile applications?

Answer: The focus of vulnerability analysis for mobile applications includes identifying security flaws related to data storage, transmission, authentication, and the use of third-party libraries or APIs.

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

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

Answer: Common techniques include configuration review, firmware analysis, and network protocol analysis to identify weaknesses in network devices.

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

Answer: It is important to conduct vulnerability analysis on network devices because they are critical to the overall security of the network, and vulnerabilities in these devices can be exploited to gain unauthorized access or disrupt network services.

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** a technique involving embedded code in seemingly benign files.

36.Vulnerability analysis of network devices often focuses on ,**patch management** configurations, and firmware.

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

ANS:Identification and documentation of the vulnerability.

Assessment of the vulnerability's impact and risk.

Notification of the appropriate stakeholders.

Recommendation of remediation steps.

Verification of the remediation.

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

Answer: SQL injection is a code injection technique that exploits vulnerabilities in an application's software by inserting malicious SQL code into a query. Example: ' OR '1'='1' --.

39.How do exploitation frameworks assist in vulnerability analysis?

Answer: Exploitation frameworks, such as Metasploit, assist in vulnerability analysis by providing tools and scripts to simulate attacks, validate vulnerabilities, and assess the potential impact of exploitation.

40.What is the primary function of OpenVAS?

Answer: The primary function of OpenVAS is to conduct comprehensive vulnerability scanning and assessment for identifying and mitigating security risks 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.

- **Answer: Ethical considerations include obtaining proper authorization before conducting tests, ensuring that the analysis does not cause harm or disruption, respecting privacy, and responsibly disclosing vulnerabilities to prevent exploitation.**

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

- **Answer:** Reporting and remediation are critical as they ensure that identified vulnerabilities are communicated to the appropriate parties and addressed promptly to prevent potential security breaches.

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 learned **from real-world scenarios**

46.Why are case studies important in learning about vulnerability analysis?

- **Answer:** Case studies are important because they provide practical insights and real-world examples of how vulnerabilities are discovered, exploited, and remediated, helping learners understand the

application of theoretical concepts.

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

- **Answer:** Case studies can improve your approach by offering lessons from real incidents, showing effective and ineffective strategies, and providing context for applying best practices in vulnerability management.

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

- **Answer:** A scenario where comprehensive vulnerability analysis would be critical is in the security assessment of a financial institution's network, where failure to identify and remediate vulnerabilities could lead to significant financial loss and reputational damage.

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

- **Answer:** Lateral movement is the technique used by attackers to move deeper into a network by compromising multiple systems, often to reach high-value targets or sensitive data after gaining initial access.

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?

- **Answer: The purpose is to provide hands-on experience, allowing students to apply theoretical knowledge, learn the use of tools, and develop skills necessary to conduct real-world vulnerability assessments.**

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

Answer: A hands-on practical approach enhances understanding by allowing students to directly interact with tools, observe the impact of vulnerabilities, and experiment with different techniques, leading to a deeper and more practical knowledge of vulnerability analysis.

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

Answer: Key components include an executive summary, detailed findings, risk assessment, recommendations, remediation steps, and verification procedures.

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

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

Answer: The goal is to identify, understand, and mitigate vulnerabilities in a controlled environment to prepare students for real-world scenarios.

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.

Answer:

1. **Brute force attack**
2. **Dictionary attack**