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?

__primarily used to identify and assess potential security weaknesses in a system, network, or application

____

______

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.It's a standardized framework used to measure the severity of IT vulnerabilities___

__ The major difference between CVSS 2.0 and CVSS 3.0 lies in their scoring methodologies and metrics____

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?

______ **Identifying assets** __

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

___ CVE (Common Vulnerabilities and Exposures) **is a publicly available database of known information security vulnerabilities_____**

___ MITRE's CVE Dictionary_____

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**__ 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 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).

____ **Standardization, Scoring methodology, Metrics, Environmental factors.** ____

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

______ **by providing a quantitative measure of their severity**____

16. __ **CVE (Common Vulnerabilities and Exposures)** _____ databases are essential for keeping up-to-date with the latest vulnerabilities.

17. List three best practices for effective vulnerability management.

_____ **Regular scanning, Prioritization, Patch management**.____

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

____ **Subscribe to CVE feeds, Integrate with scanning tool, Use for prioritization**.____

19.Defense in Depth involves layering multiple security controls throughout an organization's IT environment to ensure that if one layer fails, __ **another can 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 software tools to automatically identify vulnerabilities in systems and networks.** Manual vulnerability scanning **involves human experts manually testing systems for vulnerabilitie**s_____

23. Nmap's _ **Nmap Scripting Engine (NSE)__** _ Engine (NSE) is used for advanced vulnerability scanning.

24. How does the Nmap Scripting Engine (NSE) enhance the capabilities of Nmap?

____ **by providing a framework for creating and using scripts to perform specialized vulnerability scans and checks**__

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

_____ Nessus is known for its ease of use and extensive plugin library, while OpenVAS is highly customizable and often used in enterprise environments.__

26. Explain the role of Qualys in vulnerability management.

____ Qualys have features like Scalable scanning, Continuous monitoring, Patch management tools. ___

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

28. What is the OWASP Top Ten?

___ OWASP Top Ten is a standard awareness document that identifies the ten most critical web application security risks___

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

_____provide by Identifying security weaknesses, Helping prioritize, Providing insights into potential attack vectors_____

30. ___ **Acunetix____** is a widely used vulnerability scanner for assessing web applications.

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

___focus on the hacker not Gain unauthorized access to user data, Install malware on the user's device, Disrupt the normal operation of the application____

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

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

___common technique are Port scanning, Protocol analysis, vulnerability scanning. _____

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

____ because they are often a critical entry point for **attackers ___**

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 **___zero-day vulnerability____**, 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?
____steps are identifying vulnerabilities, Prioritizing vulnerabilities, Documenting vulnerabilities, Communicating findings___

38. Define SQL injection and write an example of SQL injection?
_____ SQL injection is a type of attack where malicious code is injected into an SQL query to manipulate the database
___e.g: ' OR 1=1 -- ___

39. How do exploitation frameworks assist in vulnerability analysis?
______ **by providing a set of tools and techniques that can be used to simulate attacks on discovered vulnerabilities**____

40. What is the primary function of OpenVAS?
______ identify and assess vulnerabilities ______

41. Exploitation frameworks like ___ **Metasploit**_____ are used to simulate attacks on discovered vulnerabilities.

42. Discuss the ethical considerations involved in vulnerability analysis.
______**ethical consideration are obtaining authorization, Avoiding unauthorized access, Minimizing impact, Reporting vulnerabilities responsibly.** ______

43.What is the significance of reporting and remediation in the vulnerability management process? **___ because they ensure that identified vulnerabilities are addressed in a timely manner**____

44. Zero Trust Architecture operates on the principle of "___ **"never trust, always verify,"** ___, always verify," meaning that every access request is subjected to strict verification regardless of its origin.

45. Case studies in vulnerability analysis often highlight **__ real-world examples**___ from realworld scenarios.

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

____ because they provide concrete examples **of how vulnerabilities can be exploited and the potential impact of such attacks**______

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

______ Providing insights into common attack vectors, Demonstrating the consequences of unpatched vulnerabilities. ______

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

_____ **before a major event or launch**______

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

_____ **Lateral** movement **refers to the ability of an attacker to move from one compromised system to another within a network. Attackers often use lateral movement to gain access to more sensitive 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 purpose of practical exercises in a vulnerability analysis course is to provide students with** hands-on experience **in identifying and assessing vulnerabilities**______

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

________hands-on practical are Providing practical experience, Building confidence.

______

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

___key components are Remediation recommendations, Executive summary_____

54.A well-conducted vulnerability analysis should lead to effective ___ **remediation**______ of discovered vulnerabilities.

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

____ **provide students with hands-on experience**

______

56. _**black hat hacking**________ hacking is the practice of exploiting vulnerabilities in systems to gain unauthorized access.

57. ___ **Password-cracking**_________ cracking tools are used to recover lost or stolen passwords.

58. Name two commonly used password-cracking techniques.

_____ **Brute force and Dictionary attacks**

____

______