vulnerability scanning techniques and penetration testing concepts in cybersecurity,

1. What is a vulnerability scan?

- A. A type of penetration test
- B. A process to identify security weaknesses in a system
- C. A method to secure network communication
- D. A technique to encrypt data at rest

Answer: B

2. Which of the following is NOT a common vulnerability scanning technique?

- A. Port scanning
- B. Patch management
- C. Password cracking
- D. Vulnerability assessment

Answer: B

3. What is the primary goal of a vulnerability scan?

- A. To exploit vulnerabilities in a system
- B. To identify security weaknesses
- C. To encrypt data in transit

- D. To secure network devices

Answer: B

4. Which of the following is a passive vulnerability scanning technique?

- A. Network-based vulnerability scan
- B. Host-based vulnerability scan
- C. Intrusive scan
- D. Packet sniffing

Answer: D

5. What is the difference between vulnerability scanning and penetration testing?

- A. Vulnerability scanning is manual, while penetration testing is automated
- B. Vulnerability scanning identifies weaknesses, while penetration testing attempts to exploit them
- C. Vulnerability scanning is only performed on networks, while penetration testing is only performed on hosts
- D. Vulnerability scanning is a subset of penetration testing

Answer: B

6. Which of the following is an active vulnerability scanning technique?

- A. Port scanning
- B. Packet sniffing
- C. Log analysis
- D. Intrusion detection

Answer: A

7. What is the purpose of penetration testing?

- A. To identify vulnerabilities in a system
- B. To exploit vulnerabilities to assess the impact
- C. To secure network communications
- D. To conduct regular security audits

Answer: B

8. Which of the following is NOT a phase of penetration testing?

- A. Planning
- B. Reconnaissance
- C. Post-exploitation
- D. Patching

Answer: D

9. What is the primary difference between black-box testing and white-box testing?

- A. Black-box testing is performed by internal testers, while white-box testing is performed by external testers

- B. Black-box testing is conducted with no prior knowledge of the system, while white-box testing is conducted with full knowledge

- C. Black-box testing is automated, while white-box testing is manual

- D. Black-box testing is faster than white-box testing

Answer: B

10. Which of the following is NOT a common penetration testing methodology?

- A. The Open Source Security Testing Methodology Manual (OSSTMM)

- B. The National Institute of Standards and Technology (NIST) Cybersecurity Framework

- C. The Penetration Testing Execution Standard (PTES)

- D. The Information Systems Security Assessment Framework (ISSAF)

Answer: B

11. What is the purpose of a vulnerability assessment?

- A. To identify security weaknesses and assess their impact
- B. To exploit vulnerabilities in a system
- C. To secure network communications
- D. To conduct regular security audits

Answer: A

12. Which of the following is a limitation of vulnerability scanning?

- A. It requires deep knowledge of system internals
- B. It may produce false positives and false negatives
- C. It can only be performed manually
- D. It is not effective for identifying network vulnerabilities

Answer: B

13. What is the goal of an authenticated vulnerability scan?

- A. To identify vulnerabilities in a system without authentication
- B. To exploit vulnerabilities in a system
- C. To identify vulnerabilities in a system with authentication
- D. To secure network communications

Answer: C

14. Which of the following is NOT a common vulnerability scanning tool?

- A. Nessus
- B. OpenVAS
- C. Metasploit
- D. QualysGuard

Answer: C

15. What is the purpose of a port scan in vulnerability scanning?

- A. To identify open ports on a system
- B. To encrypt data at rest
- C. To secure network communications
- D. To conduct regular security audits

Answer: A

16. What is the primary goal of penetration testing?

- A. To identify security weaknesses in a system
- B. To exploit vulnerabilities to assess the impact
- C. To secure network communications
- D. To conduct regular security audits

Answer: B

17. Which of the following is a limitation of vulnerability scanning?

- A. It cannot identify vulnerabilities in a system
- B. It may produce false positives and false negatives
- C. It can only be performed manually
- D. It is not effective for identifying network vulnerabilities

Answer: B

18. What is the purpose of a vulnerability assessment?

- A. To identify security weaknesses and assess their impact
- B. To exploit vulnerabilities in a system
- C. To secure network communications
- D. To conduct regular security audits

Answer: A

19. Which of the following is a limitation of vulnerability scanning?

- A. It requires deep knowledge of system internals
- B. It may produce false positives and false negatives
- C. It can only be performed manually
- D. It is not effective for identifying network vulnerabilities

Answer: B

20. What is the goal of an authenticated vulnerability scan?

- A. To identify vulnerabilities in a system without authentication
- B. To exploit vulnerabilities in a system
- C. To identify vulnerabilities in a system with authentication
- D. To secure network communications

Answer: C

21. Which of the following is NOT a common vulnerability scanning tool?

- A. Nessus
- B. OpenVAS
- C. Metasploit
- D. QualysGuard

Answer: C

22. What is the purpose of a port scan in vulnerability scanning?

- A. To identify open ports on a system
- B. To encrypt data at rest
- C. To secure network communications
- D. To conduct regular security audits

Answer: A

23. What is the primary goal of penetration testing?

- A. To identify security weaknesses in a system

- B. To exploit vulnerabilities to assess the impact

- C. To secure network communications

- D. To conduct regular security audits

Answer: B

24. Which of the following is a limitation of vulnerability scanning?

- A. It cannot identify vulnerabilities in a system

- B. It may produce false positives and false negatives

- C. It can only be performed manually

- D. It is not effective for identifying network vulnerabilities