Sure! Here’s a set of 100 multiple-choice questions (MCQs) on network penetration testing, covering various vulnerabilities. The correct answers are bolded for your convenience.

MCQs on Network Penetration Testing

1. What is the primary goal of penetration testing?
- a) To break into systems
- **b) To identify vulnerabilities**
- c) To create new security policies
- d) To patch software

2. Which of the following is a common tool used in penetration testing?
- a) Microsoft Word
- **b) Metasploit**
- c) Adobe Photoshop
- d) Google Chrome

3. What does the acronym OWASP stand for?
- **a) Open Web Application Security Project**
- b) Online Web Application Security Protocol
- c) Open Web Applications Security Program
- d) Online Web Application Safety Project

4. Which type of attack involves intercepting and altering communication between two parties?
- a) Phishing
- **b) Man-in-the-Middle (MitM)**
- c) Denial of Service (DoS)
- d) SQL Injection

5. What vulnerability is commonly associated with unvalidated input?
 - **a) SQL Injection**
 - b) Cross-Site Scripting (XSS)
 - c) Buffer Overflow
 - d) Denial of Service

6. Which protocol is primarily used for secure communication over a computer network?
 - a) HTTP
 - **b) HTTPS**
 - c) FTP
 - d) SMTP

7. What is a common method for gaining unauthorized access to a network?
 - a) Password expiration
 - b) Encryption
 - **c) Social Engineering**
 - d) Data loss prevention

8. A vulnerability that allows an attacker to execute arbitrary code is known as:
 - a) Cross-Site Scripting
 - **b) Remote Code Execution (RCE)**
 - c) Denial of Service
 - d) Man-in-the-Middle

9. Which type of testing assesses security from an outsider's perspective?
 - **a) External Penetration Testing**
 - b) Internal Penetration Testing
 - c) Application Penetration Testing

- d) Automated Penetration Testing

10. What does the acronym DDoS stand for?
- a) Data Delivery Over Security
- b) Distributed Data Over Service
- **c) Distributed Denial of Service**
- d) Dynamic Denial of Security

11. A common risk associated with wireless networks is:
- a) Lack of bandwidth
- b) Data redundancy
- **c) Eavesdropping**
- d) Network speed

12. Which of the following is a security standard for payment card transactions?
- **a) PCI-DSS**
- b) ISO 27001
- c) HIPAA
- d) GDPR

13. Which attack targets the availability of a service?
- a) Man-in-the-Middle
- b) SQL Injection
- **c) Denial of Service**
- d) Cross-Site Scripting

14. What is the main purpose of a firewall?
- a) To encrypt data

- b) To monitor user activity
- **c) To block unauthorized access**
- d) To back up data

15. What does the term "phishing" refer to?
- **a) Deceptive attempts to obtain sensitive information**
- b) Injecting malicious code into a website
- c) A technique to brute-force passwords
- d) Scanning networks for open ports

16. Which type of testing focuses on the security of web applications?
- a) Network Penetration Testing
- **b) Web Application Penetration Testing**
- c) Wireless Penetration Testing
- d) System Penetration Testing

17. The process of scanning a network for vulnerabilities is known as:
- a) Exploitation
- b) Reporting
- **c) Scanning**
- d) Reconnaissance

18. What is a common tool for network scanning?
- a) Wireshark
- b) Nmap
- **c) Nessus**
- d) Burp Suite

19. SQL Injection primarily affects which type of system?
  - **a) Databases**
  - b) File servers
  - c) Web servers
  - d) Mail servers

20. Which of the following is a common type of malware?
  - a) Firewall
  - b) VPN
  - **c) Trojan Horse**
  - d) Router

21. What is the first step in the penetration testing process?
  - a) Scanning
  - b) Reporting
  - **c) Planning**
  - d) Exploitation

22. What is the purpose of a vulnerability assessment?
  - **a) To identify and prioritize vulnerabilities**
  - b) To exploit vulnerabilities
  - c) To monitor network traffic
  - d) To patch software

23. Cross-Site Scripting (XSS) vulnerabilities allow attackers to:
  - a) Access files on the server
  - **b) Inject malicious scripts into web pages**
  - c) Overload a server
  - d) Bypass authentication

24. Which of the following is NOT a type of social engineering attack?

- a) Phishing
- **b) SQL Injection**
- c) Pretexting
- d) Baiting

25. What tool can be used to capture and analyze network traffic?

- a) Nmap
- **b) Wireshark**
- c) Metasploit
- d) Nessus

26. Which of the following is a common result of a successful SQL Injection attack?

- a) Network slowdown
- **b) Unauthorized data access**
- c) Service interruption
- d) Denied user access

27. What is a key aspect of a good password policy?

- a) Short passwords
- **b) Complexity and length**
- c) No expiration
- d) Shared passwords

28. What does the acronym IDS stand for?

- a) Internet Detection System
- **b) Intrusion Detection System**
- c) Internet Defense System

  - d) Intrusion Data System

29. What type of vulnerability allows an attacker to execute code on a system without permission?
  - **a) Remote Code Execution**
  - b) Directory Traversal
  - c) Cross-Site Request Forgery
  - d) SQL Injection

30. What is the main purpose of a penetration test report?
  - a) To list all software used
  - **b) To provide findings and recommendations**
  - c) To document network architecture
  - d) To record user activities

31. What is the most common method of gaining unauthorized access to a network?
  - a) Malware
  - b) Brute-force attacks
  - **c) Weak passwords**
  - d) Exploiting vulnerabilities

32. What type of vulnerability is often found in web applications that fail to validate user input?
  - **a) Cross-Site Scripting**
  - b) SQL Injection
  - c) Buffer Overflow
  - d) Denial of Service

33. Which of the following is an example of a denial-of-service attack?
  - **a) Flooding a server with traffic**

- b) Accessing unauthorized files
- c) Capturing login credentials
- d) Exploiting software vulnerabilities

34. What does the term "exploit" refer to in penetration testing?
- a) A successful attack
- b) A software tool
- **c) Code that takes advantage of a vulnerability**
- d) A network scanning method

35. What type of attack uses a fake website to collect user credentials?
- **a) Phishing**
- b) Spoofing
- c) Keylogging
- d) DDoS

36. What is the main purpose of encryption in data security?
- a) To increase speed
- **b) To protect data confidentiality**
- c) To ensure data integrity
- d) To provide redundancy

37. What does a honeypot do?
- a) Backs up data
- b) Monitors network traffic
- **c) Attracts attackers to study their methods**
- d) Encrypts sensitive data

38. What type of vulnerability is associated with buffer overflow?
  - a) Denial of Service
  - b) Cross-Site Scripting
  - **c) Memory corruption**
  - d) SQL Injection

39. Which of the following is a strong password policy?
  - a) Passwords should be easily memorable
  - **b) Passwords should be at least 12 characters long and include numbers and symbols**
  - c) Passwords can be reused
  - d) Passwords should be written down

40. What does the term "black box testing" refer to?
  - a) Testing with prior knowledge of the system
  - **b) Testing without any prior knowledge of the system**
  - c) Testing conducted by an internal team
  - d) Testing using automated tools only

41. Which of the following is an effective way to prevent SQL Injection?
  - **a) Use prepared statements and parameterized queries**
  - b) Allow user

input
  - c) Disable all database connections
  - d) Use plain text queries

42. What does the acronym VPN stand for?
  - **a) Virtual Private Network**

  - b) Virtual Protected Network
  - c) Variable Private Network
  - d) Verified Protected Network

43. What is the function of a network scanner?
  - **a) To discover devices and services on a network**
  - b) To encrypt data
  - c) To monitor network speed
  - d) To filter incoming traffic

44. What is the primary risk of using outdated software?
  - a) Increased costs
  - b) Reduced functionality
  - **c) Increased vulnerability to attacks**
  - d) Compatibility issues

45. Which of the following is a common form of authentication?
  - a) IP Address
  - **b) Password**
  - c) MAC Address
  - d) DNS

46. What is the purpose of a penetration test?
  - **a) To find and fix security weaknesses**
  - b) To ensure compliance with laws
  - c) To install software updates
  - d) To monitor user behavior

47. Which of the following vulnerabilities can lead to data leakage?
  - a) Buffer Overflow
  - **b) Insecure Direct Object References**
  - c) SQL Injection
  - d) Denial of Service

48. What does the term "social engineering" refer to?
  - a) Analyzing social media data
  - **b) Manipulating people to gain confidential information**
  - c) Engineering social networks
  - d) Using algorithms for social trends

49. Which of the following is a common port for HTTPS traffic?
  - a) 80
  - **b) 443**
  - c) 21
  - d) 25

50. What is a primary characteristic of a Trojan horse?
  - a) It replicates itself
  - **b) It disguises itself as legitimate software**
  - c) It disrupts service
  - d) It encrypts data

51. What does the acronym CVE stand for?
  - **a) Common Vulnerabilities and Exposures**
  - b) Computer Virus Exploit
  - c) Common Vulnerability Evaluation
  - d) Cybersecurity Vulnerabilities and Exposures

52. A common method of gaining unauthorized access is:
- a) Updating software
- **b) Password cracking**
- c) Regular backups
- d) Using firewalls

53. Which of the following is a form of passive reconnaissance?
- **a) Gathering information from public sources**
- b) Scanning for open ports
- c) Exploiting known vulnerabilities
- d) Conducting social engineering

54. What is the purpose of an Intrusion Prevention System (IPS)?
- a) To log network traffic
- b) To encrypt data
- **c) To detect and prevent attacks**
- d) To backup data

55. What does the term "zero-day exploit" refer to?
- a) An exploit that has been patched
- **b) An exploit that targets a newly discovered vulnerability**
- c) An exploit that is widely known
- d) An exploit that is easy to detect

56. Which of the following is an example of credential stuffing?
- a) Phishing
- b) Keylogging
- **c) Using stolen credentials from one breach to access another account**

- d) Social engineering

57. What is the purpose of a security policy?
- a) To restrict access to data
- b) To outline procedures for employees
- **c) To define security measures and responsibilities**
- d) To monitor employee performance

58. Which attack method involves overwhelming a server with traffic?
- a) Phishing
- **b) Denial of Service (DoS)**
- c) SQL Injection
- d) Man-in-the-Middle

59. What does the term "patch management" refer to?
- **a) The process of applying updates to software**
- b) Monitoring network activity
- c) Backing up data
- d) Configuring firewalls

60. Which of the following is an example of an insider threat?
- a) An attacker from outside the organization
- **b) A disgruntled employee stealing data**
- c) A hacker exploiting software vulnerabilities
- d) A third-party vendor accessing sensitive data

61. What is the main function of a Digital Certificate?
- a) To encrypt data

  - **b) To verify the identity of a website**
  - c) To back up data
  - d) To monitor network traffic

62. Which of the following is an indication of a successful phishing attempt?
  - **a) Unusual account activity**
  - b) Increased network traffic
  - c) Slow internet speed
  - d) Software updates

63. What is the primary purpose of a honeynet?
  - a) To speed up network traffic
  - b) To back up sensitive data
  - **c) To attract and analyze attackers**
  - d) To monitor employee activity

64. Which of the following is NOT a common vulnerability scanning tool?
  - a) Nessus
  - b) OpenVAS
  - **c) Microsoft Excel**
  - d) Qualys

65. What type of testing is performed after a vulnerability has been identified?
  - a) Penetration Testing
  - **b) Remediation Testing**
  - c) Vulnerability Assessment
  - d) Compliance Testing

66. Which of the following is a secure method of transmitting data?
- a) FTP
- **b) SFTP**
- c) HTTP
- d) Telnet

67. What does the term "brute-force attack" refer to?
- a) Exploiting a vulnerability
- **b) Trying all possible combinations to guess a password**
- c) Phishing for credentials
- d) Social engineering

68. What is the primary goal of a red team in penetration testing?
- a) To improve systems
- **b) To simulate an attack**
- c) To assess compliance
- d) To monitor performance

69. What is the purpose of a web application firewall (WAF)?
- a) To encrypt web traffic
- **b) To filter and monitor HTTP traffic**
- c) To backup data
- d) To log network activity

70. Which of the following is an example of two-factor authentication (2FA)?
- a) Username and password
- **b) Password and a text message code**
- c) Username and security question
- d) Password and a security image

71. What is a common outcome of a successful phishing attack?
  - **a) Compromised user credentials**
  - b) Slower network speed
  - c) Denial of service
  - d) Data encryption

72. What does the term "data breach" refer to?
  - a) Losing internet connection
  - **b) Unauthorized access to sensitive data**
  - c) Deleting files accidentally
  - d) System downtime

73. Which of the following is a characteristic of ransomware?
  - a) It spreads through emails
  - b) It collects personal data
  - **c) It encrypts files and demands payment**
  - d) It slows down networks

74. What does a penetration test simulate?
  - a) A system backup
  - **b) A cyberattack**
  - c) User behavior
  - d) Network traffic

75. What is the primary goal of threat modeling?
  - a) To patch software
  - **b) To identify potential threats and vulnerabilities**
  - c) To monitor user activity

- d) To analyze network performance

76. Which of the following is a common security framework?
  - a) ISO 9001
  - b) GDPR
  - **c) NIST Cybersecurity Framework**
  - d) HIPAA

77. What does the term "malware" encompass?
  - a) Only viruses
  - **b) All malicious software**
  - c) Only spyware
  - d) Only phishing tools

78. Which of the following is a method of securing wireless networks?
  - a) Open authentication
  - b) Weak encryption
  - **c) WPA2 encryption**
  - d) No password

79. What is the primary benefit of regular software updates?
  - a) Enhanced performance
  - **b) Fixing security vulnerabilities**
  - c) Adding new features
  - d) Increasing compatibility

80. Which of the following is a best practice for password management?
  - a) Reusing passwords

- **b) Using a password manager**
- c) Sharing passwords
- d) Storing passwords in plain text

81. What is a common use of port scanning?
- **a) To identify open ports on a network**
- b) To encrypt network traffic
- c) To log user activities
- d) To monitor bandwidth usage

82. What is the primary purpose of a security audit?
- a) To install updates
- **b) To assess the effectiveness of security measures**
- c) To analyze user behavior
- d) To monitor system performance

83. Which of the following is a risk of using public Wi-Fi?

- a) High speed
- b) Free access
- **c) Data interception**
- d) Wide accessibility

84. What does the term "data exfiltration" refer to?
- a) Data storage
- **b) Unauthorized transfer of data**
- c) Data backup

  - d) Data deletion

85. Which of the following is NOT a type of encryption?
  - a) Symmetric encryption
  - b) Asymmetric encryption
  - **c) Linear encryption**
  - d) Hashing

86. What is the main function of a SIEM system?
  - **a) To analyze security alerts in real-time**
  - b) To encrypt data
  - c) To monitor bandwidth
  - d) To back up data

87. What type of attack targets a user’s session on a website?
  - a) SQL Injection
  - **b) Session Hijacking**
  - c) Phishing
  - d) DDoS

88. Which of the following is a best practice for secure coding?
  - a) Allowing all user inputs
  - b) Using deprecated functions
  - **c) Validating and sanitizing inputs**
  - d) Hardcoding sensitive information

89. What is the primary risk of SQL Injection?
  - a) Network downtime

  - b) Data corruption
  - **c) Unauthorized data access**
  - d) Malware installation

90. Which of the following is a consequence of poor access control?
  - **a) Unauthorized data access**
  - b) Slower network speed
  - c) Increased costs
  - d) Better user experience

91. What does the term "black hat hacker" refer to?
  - a) Ethical hacker
  - **b) Malicious hacker**
  - c) Security researcher
  - d) Software developer

92. What is the purpose of a digital signature?
  - a) To encrypt data
  - **b) To verify the authenticity of a message**
  - c) To store data
  - d) To speed up transactions

93. Which of the following can be used to enhance network security?
  - a) Open ports
  - **b) Firewalls**
  - c) Weak passwords
  - d) Unpatched software

94. What does the term "red teaming" refer to?
- a) Compliance testing
- **b) Simulating an attack to test defenses**
- c) User training
- d) Network performance analysis

95. Which of the following is a type of denial-of-service attack?
- a) Eavesdropping
- **b) SYN flood**
- c) Phishing
- d) Keylogging

96. What is the primary function of a password hash?
- a) To store passwords in plain text
- **b) To securely store password representations**
- c) To encrypt sensitive data
- d) To create user accounts

97. What is a primary characteristic of a phishing attack?
- a) It is always successful
- **b) It attempts to trick users into revealing information**
- c) It is performed only by insiders
- d) It is a physical attack

98. What does the term "threat vector" refer to?
- **a) A method or pathway used by attackers**
- b) A security protocol
- c) A type of malware
- d) A software tool

99. Which of the following is an example of an advanced persistent threat (APT)?
  - **a) A long-term targeted attack**
  - b) A random attack
  - c) A denial-of-service attack
  - d) A phishing scam

100. What is the primary goal of data encryption?
  - a) To improve performance
  - **b) To protect data confidentiality**
  - c) To reduce storage space
  - d) To speed up access times

Feel free to study these questions, and let me know if you need any more help or clarification on any topics! Good luck with your quiz!