Cybersecurity

Multiple-Choice Quiz

1. Which of the following best defines cybersecurity?
A. Protecting computers from hardware failures
B. Protecting systems, networks, and data from digital attacks
C. Installing antivirus software only
D. Monitoring network traffic exclusively

2. What is phishing?
A. A method of data encryption
B. Sending fraudulent emails to obtain sensitive information
C. A type of firewall
D. A programming language

3. Which of these is a strong password?
A. password123
B. 12345678
C. S!8eR@2xYqP
D. qwerty

4. What does two-factor authentication (2FA) provide?
A. Single-step login
B. Only password protection
C. An additional layer of security beyond a password
D. Encryption of data in transit

5. Which type of malware locks files and demands payment?
A. Virus
B. Trojan
C. Ransomware
D. Worm

6. What is a firewall primarily used for?
A. Encrypting data
B. Blocking unauthorized network access
C. Creating passwords
D. Scanning for malware

7. SQL injection is an attack that targets which part of a system?
A. Network routers
B. Databases
C. User interfaces
D. Physical servers

8. What does the principle of least privilege mean?
A. Users have admin access by default
B. Users have minimal access needed to perform their tasks
C. Firewalls block all incoming traffic
D. Passwords never expire

9. Which of the following is an example of social engineering?
A. Virus infection
B. Someone pretending to be IT staff to steal login credentials
C. Brute-force attack
D. Keylogging software

10. Which encryption method uses two keys: public and private?
A. Symmetric encryption
B. Asymmetric encryption
C. Hashing
D. Steganography

11. A zero-day vulnerability refers to:
A. A vulnerability fixed immediately
B. A flaw unknown to software developers
C. A virus with zero impact
D. A phishing email

12. What is a VPN used for?
A. To increase internet speed
B. To create a secure, encrypted connection over the internet
C. To install antivirus
D. To track user activity

13. Which of the following is a common sign of malware infection?
A. Slow computer performance
B. Pop-up ads
C. Frequent crashes
D. All of the above

14. What does a brute-force attack involve?
A. Guessing passwords using automated attempts
B. Exploiting software bugs
C. Sending spam emails
D. Installing firewalls

15. Which of the following is a common form of phishing?
A. Clicking on a suspicious email link
B. Using encrypted email
C. Updating antivirus software

D. Scanning a QR code from a trusted source

16. What is the main purpose of a honeypot in cybersecurity?
A. Encrypt sensitive files
B. Detect and divert attackers
C. Install antivirus
D. Perform regular backups

17. Cross-site scripting (XSS) attacks target:
A. Network routers
B. Web applications
C. Physical security
D. Hardware firmware

18. Which of the following is an example of multi-factor authentication?
A. Password only
B. Password + fingerprint scan
C. Password + username
D. Password + email address

19. What is a Denial-of-Service (DoS) attack?
A. Stealing sensitive data
B. Making a service unavailable to users
C. Installing ransomware
D. Creating a phishing page

20. Which of the following is considered sensitive personal data?
A. Social Security number
B. Email address
C. Public blog posts
D. General website URL

21. Which protocol is commonly used to secure web traffic?
A. HTTP
B. HTTPS
C. FTP
D. SMTP

22. Which type of malware disguises itself as legitimate software?
A. Worm
B. Trojan
C. Ransomware
D. Adware

23. What is the purpose of a digital certificate?
A. To track browsing activity

B. To verify the authenticity of a website or user
C. To speed up internet connections
D. To block malware

24. Which of these is considered a strong security practice?
A. Using the same password for multiple accounts
B. Regularly updating software
C. Sharing passwords over email
D. Disabling firewalls

25. A botnet is:
A. A type of firewall
B. A network of infected devices controlled remotely
C. A virus scanner
D. A data encryption method

26. What does the CIA triad stand for in cybersecurity?
A. Control, Integrity, Access
B. Confidentiality, Integrity, Availability
C. Cryptography, Intelligence, Authentication
D. Connection, Identification, Authorization

27. Which of the following is an example of a physical security measure?
A. Antivirus software
B. Locked server room
C. Password-protected accounts
D. VPN

28. Keylogging is a type of:
A. Malware
B. Encryption
C. Firewall
D. Network protocol

29. Which attack involves intercepting and altering communication between two parties?
A. Man-in-the-Middle (MITM)
B. SQL injection
C. Phishing
D. Brute-force attack

30. What is the purpose of patch management?
A. To track network traffic
B. To install antivirus software
C. To update software and fix security vulnerabilities
D. To create user accounts

31. Which of the following is an example of a network attack?
A. Shoulder surfing
B. Man-in-the-Middle
C. Social engineering
D. Phishing

32. What is the main purpose of hashing?
A. Encrypting data to make it reversible
B. Creating a unique fingerprint for data
C. Blocking unauthorized access
D. Capturing keystrokes

33. Which of the following is an example of two-factor authentication?
A. Username and password
B. Password and security question
C. Password and one-time code sent via SMS
D. Email and username

34. What is ransomware primarily designed to do?
A. Spy on users
B. Encrypt files and demand a ransom
C. Steal passwords silently
D. Delete system logs

35. Which cybersecurity practice helps reduce the risk of social engineering?
A. Using antivirus software
B. Employee security training
C. Installing a firewall
D. Encrypting emails

36. What is spear phishing?
A. A phishing attack targeting a specific individual or organization
B. Random spam emails
C. Malware that replicates itself
D. A type of firewall

37. Which of the following is a major benefit of endpoint security?
A. Protects physical offices
B. Secures individual devices like computers and smartphones
C. Encrypts all network traffic
D. Creates backups automatically

38. Which of these is an example of insider threat?
A. Hacker from another country
B. Employee stealing sensitive company data

C. Virus infection from email
D. Phishing attack

39. Which of the following protocols is used for secure email transmission?
A. SMTP
B. IMAP
C. POP3
D. SMTPS

40. What is a common method to prevent SQL injection attacks?
A. Using input validation and prepared statements
B. Installing antivirus software
C. Encrypting network traffic
D. Using strong passwords

41. What is a common use of intrusion detection systems (IDS)?
A. Encrypting network traffic
B. Detecting suspicious or malicious activity on a network
C. Creating backups
D. Managing passwords

42. What does the term “patch” refer to in cybersecurity?
A. A type of malware
B. A software update that fixes vulnerabilities or bugs
C. A network protocol
D. A firewall rule

43. Which of the following is NOT a type of malware?
A. Virus
B. Worm
C. Trojan
D. VPN

44. What is the primary goal of data encryption?
A. To compress files
B. To make data unreadable to unauthorized users
C. To monitor network traffic
D. To delete old data

45. Which type of attack targets the weakest link: the user?
A. Malware injection
B. Social engineering
C. DDoS
D. Man-in-the-Middle

46. What is a key difference between a virus and a worm?

A. Viruses self-replicate, worms do not
B. Worms self-replicate without user action, viruses require user action
C. Worms only affect websites
D. Viruses only affect networks

47. Which of these is a common indicator of a phishing email?
A. Email from a known contact with correct spelling
B. Email requesting sensitive information urgently
C. Email with only plain text
D. Email confirming a package delivery you ordered

48. What is the main purpose of network segmentation?
A. To increase network speed
B. To divide a network into smaller parts for security and efficiency
C. To block malware automatically
D. To encrypt data

49. Which of the following is considered an advanced persistent threat (APT)?
A. One-time malware infection
B. Long-term, targeted cyber attack by skilled attackers
C. Spam email campaign
D. Accidental data loss

50. What does the term “cyber hygiene” refer to?
A. Physical cleaning of computers
B. Regular practices to maintain secure systems and prevent cyber threats
C. Installing multiple antivirus programs
D. Using strong passwords only

51. Which cybersecurity principle involves verifying the identity of a user or system?
A. Authentication
B. Authorization
C. Encryption
D. Integrity

52. Which of the following is an example of ransomware behavior?
A. Stealing browsing history
B. Encrypting files and demanding payment for decryption
C. Redirecting web traffic
D. Monitoring network packets

53. What is the main difference between symmetric and asymmetric encryption?
A. Symmetric uses two keys, asymmetric uses one key

B. Symmetric uses one key for both encryption and decryption, asymmetric uses two keys
C. Symmetric is slower than asymmetric
D. Asymmetric cannot encrypt files

54. Which of the following is a best practice for password management?
A. Writing passwords on sticky notes
B. Using a password manager
C. Using “password123” for all accounts
D. Sharing passwords with coworkers

55. Which type of attack floods a system with traffic to make it unavailable?
A. Phishing
B. Denial-of-Service (DoS)
C. SQL Injection
D. Keylogging

56. Which security measure ensures data cannot be read if intercepted?
A. Authentication
B. Encryption
C. Patching
D. Firewalls

57. What is the main risk of using public Wi-Fi without protection?
A. Slow internet speed
B. Interception of sensitive data by attackers
C. Automatic software updates
D. VPN malfunction

58. Which of the following is NOT considered a form of malware?
A. Trojan
B. Worm
C. Antivirus
D. Ransomware

59. Which type of security threat targets Internet of Things (IoT) devices?
A. Botnets
B. Keylogging
C. SQL Injection
D. Firewall bypass

60. What is the role of an incident response plan?
A. To prevent all cyber attacks
B. To provide steps to respond to and recover from security incidents
C. To encrypt all company data
D. To block unauthorized websites

61. What is cloud security primarily concerned with?
A. Securing physical offices
B. Protecting data, applications, and services in cloud environments
C. Installing antivirus on all laptops
D. Encrypting email only

62. Which of the following is a key risk in cloud computing?
A. Malware only on local devices
B. Data breaches due to misconfigured storage
C. Keyboard logging
D. USB malware

63. What is multi-factor authentication (MFA)?
A. Logging in with username only
B. Using more than one form of verification to confirm identity
C. Installing multiple antivirus programs
D. Encrypting data twice

64. Which of the following is a cybersecurity compliance standard for protecting health data?
A. GDPR
B. HIPAA
C. PCI-DSS
D. ISO 27001

65. What is the purpose of threat intelligence?
A. To slow down networks
B. To collect, analyze, and share information about potential threats
C. To encrypt all emails
D. To install antivirus

66. Which of the following best describes a Distributed Denial-of-Service (DDoS) attack?
A. One attacker targeting a single server
B. Multiple systems overwhelming a target server or network
C. Malware infection
D. Social engineering

67. What is the primary purpose of mobile device management (MDM)?
A. To manage physical servers
B. To secure and control mobile devices used in an organization
C. To encrypt websites
D. To block phishing emails

68. Which of these is a secure way to dispose of sensitive data?

A. Deleting files and leaving the recycle bin full
B. Physical destruction or secure data wiping
C. Compressing files
D. Moving files to another folder

69. Which of the following is an example of a software vulnerability?
A. Strong password
B. Buffer overflow
C. VPN connection
D. Firewall

70. What is the main goal of penetration testing?
A. Encrypt data
B. Test a system's security by simulating attacks
C. Monitor network traffic
D. Create firewalls

71. Which of these is considered an advanced malware technique?
A. File compression
B. Polymorphic malware that changes its code to avoid detection
C. Using strong passwords
D. Updating software regularly

72. What is the purpose of data loss prevention (DLP) systems?
A. Encrypt all outgoing emails automatically
B. Prevent sensitive data from leaving the organization
C. Install antivirus software
D. Monitor web traffic only

73. Which of the following is a security risk associated with Bring Your Own Device (BYOD) policies?
A. Faster network speeds
B. Unmanaged devices increasing vulnerability to attacks
C. Easier software updates
D. Reduced malware exposure

74. What is a common cybersecurity challenge with IoT devices?
A. They always have strong security
B. Limited processing power can prevent robust security measures
C. They cannot connect to networks
D. They cannot be compromised

75. What is a common use of a security information and event management (SIEM) system?
A. Encrypt files automatically
B. Collect and analyze security data for threat detection

C. Monitor physical security only
D. Replace antivirus software

76. Which of the following is an example of endpoint security?
A. Firewall
B. Antivirus installed on laptops and desktops
C. VPN
D. Cloud storage

77. What is the purpose of network access control (NAC)?
A. To encrypt files
B. To restrict access to a network based on security policies
C. To block email spam
D. To monitor website traffic

78. Which of the following best describes ransomware-as-a-service (RaaS)?
A. A security tool for encrypting data
B. A business model where attackers rent ransomware tools to launch attacks
C. A type of firewall
D. An antivirus subscription service

79. Which of the following is considered a critical step in vulnerability management?
A. Only updating antivirus
B. Identifying, assessing, and remediating vulnerabilities
C. Ignoring minor patches
D. Using default passwords

80. What is a honeynet?
A. A single decoy computer
B. A network of decoy systems designed to attract and analyze attackers
C. A type of antivirus
D. A secure VPN network

81. Which of the following is a sign of a compromised system?
A. Slow performance
B. Unexpected pop-ups
C. Unauthorized file changes
D. All of the above

82. What is the main purpose of a Security Operations Center (SOC)?
A. Install firewalls
B. Monitor, detect, and respond to security incidents
C. Encrypt all company data
D. Manage user passwords

83. What does “pharming” refer to?
A. Infecting crops with malware
B. Redirecting users to malicious websites without their knowledge
C. Sending spam emails
D. Encrypting files for ransom

84. What is the purpose of a cybersecurity audit?
A. To test system speed
B. To evaluate security policies, controls, and compliance
C. To encrypt all network traffic
D. To install antivirus software

85. Which of the following is a common cloud security measure?
A. Multi-factor authentication (MFA)
B. Encrypting data in transit and at rest
C. Regular access reviews
D. All of the above

86. Which type of malware can spread without user interaction?
A. Trojan
B. Worm
C. Adware
D. Ransomware

87. Which is the main purpose of threat modeling?
A. To encrypt files
B. To identify potential threats and design mitigations
C. To monitor employee behavior
D. To install firewalls

88. What is a common characteristic of Advanced Persistent Threats (APTs)?
A. Short-term, random attacks
B. Long-term, targeted, and stealthy attacks
C. Only occur via email
D. Cannot steal sensitive data

89. Which of the following is a cybersecurity framework?
A. NIST Cybersecurity Framework
B. HTTP
C. TCP/IP
D. SQL

90. Which type of attack exploits vulnerabilities in a web application to steal data or execute commands?
A. SQL injection
B. DDoS

C. Phishing
D. Keylogging

91. Which security measure helps prevent data exfiltration over the network?
A. Firewall
B. Data Loss Prevention (DLP)
C. Antivirus software
D. Password complexity

92. Which type of attack uses multiple devices to overwhelm a system?
A. DDoS
B. MITM
C. Phishing
D. Spyware

93. Which of the following is a best practice for securing APIs?
A. Using weak authentication
B. Validating input and output data
C. Leaving endpoints public
D. Ignoring logging

94. What is the primary goal of ethical hacking?
A. Steal sensitive data
B. Test systems for vulnerabilities with permission to improve security
C. Deploy ransomware
D. Monitor employees

95. Which of the following is a common risk of shadow IT?
A. Unauthorized applications bypassing security controls
B. Faster network connections
C. Improved compliance
D. Increased encryption

96. What is the purpose of network segmentation in security?
A. To increase malware exposure
B. To isolate critical systems and limit lateral movement
C. To slow down users
D. To encrypt data

97. Which type of malware records user activities, including keystrokes and browsing?
A. Ransomware
B. Keylogger
C. Worm
D. Adware

98. Which practice helps mitigate phishing attacks?
A. Regular employee training
B. Using multi-factor authentication
C. Email filtering solutions
D. All of the above

99. Which emerging threat involves AI-generated content to deceive users?
A. Spear phishing
B. Deepfake attacks
C. DDoS
D. SQL injection

100. What is the first step in responding to a cybersecurity incident?
A. Recovering backups immediately
B. Identification and detection of the incident
C. Installing a firewall
D. Encrypting all files