

# Cybersecurity

## Multiple-Choice Quiz with Answers and Explanations

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

Answer: B

Explanation: Cybersecurity is the practice of protecting systems, networks, and data from unauthorized access, attacks, damage, or theft. While antivirus software and monitoring help, cybersecurity is broader.

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

Answer: B

Explanation: Phishing involves tricking users into revealing personal information like passwords or credit card numbers, often through deceptive emails or websites.

3. Which of these is a strong password?

- A. password123
- B. 12345678
- C. S!8eR@2xYqP
- D. qwerty

Answer: C

Explanation: Strong passwords are long, random, and include letters (upper/lower), numbers, and symbols. "S!8eR@2xYqP" is complex and hard to guess.

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

Answer: C

Explanation: 2FA requires two forms of verification (e.g., password + SMS code), making unauthorized access much harder.

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

Answer: C

Explanation: Ransomware encrypts files or locks a system and demands a ransom to restore access.

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

Answer: B

Explanation: A firewall monitors incoming and outgoing network traffic and blocks unauthorized connections to protect the network.

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

Answer: B

Explanation: SQL injection exploits vulnerabilities in database query inputs to manipulate or steal data.

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

Answer: B

Explanation: Limiting users to only the permissions necessary reduces the risk of accidental or malicious data exposure.

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

Answer: B

Explanation: Social engineering manipulates people into divulging confidential information rather than exploiting software.

10. Which encryption method uses two keys: public and private?

- A. Symmetric encryption
- B. Asymmetric encryption
- C. Hashing
- D. Steganography

Answer: B

Explanation: Asymmetric encryption uses a public key for encryption and a private key for decryption, enabling secure communication.

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

Answer: B

Explanation: Zero-day vulnerabilities are security flaws unknown to the vendor, leaving systems exposed until patched.

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

Answer: B

Explanation: VPNs protect data in transit by encrypting the connection, hiding IP addresses, and securing online communications.

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

Answer: D

Explanation: Malware can cause multiple issues, including slow performance, unexpected pop-ups, and system crashes.

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

Answer: A

Explanation: Brute-force attacks systematically try all possible passwords until the correct one is found.

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

Answer: A

Explanation: Phishing often uses deceptive emails to trick users into clicking malicious links or providing sensitive info.

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

Answer: B

Explanation: Honeypots are decoy systems designed to attract attackers and study their methods without harming real systems.

17. Cross-site scripting (XSS) attacks target:

- A. Network routers
- B. Web applications
- C. Physical security
- D. Hardware firmware

Answer: B

Explanation: XSS attacks inject malicious scripts into web pages, affecting users who visit those pages.

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

Answer: B

Explanation: Multi-factor authentication requires two or more different factors (something you know + something you have/are).

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

Answer: B

Explanation: DoS attacks overwhelm systems or networks to disrupt legitimate access, often using excessive traffic.

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

Answer: A

Explanation: Sensitive personal data includes information that can uniquely identify a person or be misused for identity theft.

That completes Questions 1–20 with answers and explanations.

I can continue with Questions 21–100 in the next batch, keeping the same structure, covering malware, attacks, network security, cryptography, social engineering, and cybersecurity best practices.

Do you want me to continue straight through with the next 20 questions?

yes

Perfect! Here's Part 2: Questions 21–40 of the cybersecurity quiz, with answers and explanations.

Cybersecurity Quiz: Questions 21–40

21. Which protocol is commonly used to secure web traffic?

- A. HTTP
- B. HTTPS
- C. FTP
- D. SMTP

Answer: B

Explanation: HTTPS uses SSL/TLS to encrypt data between a web browser and server, securing communications.

22. Which type of malware disguises itself as legitimate software?

- A. Worm
- B. Trojan
- C. Ransomware
- D. Adware

Answer: B

Explanation: Trojans appear harmless but contain malicious code that can steal data or damage systems.

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

Answer: B

Explanation: Digital certificates confirm that a public key belongs to a verified entity, enabling secure communications.

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

Answer: B

Explanation: Keeping software updated ensures known vulnerabilities are patched, reducing the risk of exploits.

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

Answer: B

Explanation: Botnets are networks of compromised devices used for malicious purposes like DoS attacks or spamming.

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

Answer: B

Explanation: The CIA triad is a fundamental model for cybersecurity, focusing on protecting data confidentiality, integrity, and availability.

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

Answer: B

Explanation: Physical security protects hardware and facilities from unauthorized access, theft, or damage.

28. Keylogging is a type of:

- A. Malware
- B. Encryption
- C. Firewall
- D. Network protocol

Answer: A

Explanation: Keyloggers record keystrokes to capture sensitive information like passwords.

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

Answer: A

Explanation: MITM attacks intercept communications and may alter data without the users' knowledge.

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

Answer: C

Explanation: Patch management ensures systems are up-to-date, fixing vulnerabilities that could be exploited by attackers.

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

Answer: B

Explanation: Network attacks target the flow of data, and MITM attacks specifically intercept communications over networks.

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

Answer: B

Explanation: Hashing produces a fixed-length value (hash) from data, which is typically irreversible and used for integrity verification.

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

Answer: C

Explanation: Two-factor authentication requires something you know (password) and something you have (one-time code), improving security.

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

Answer: B

Explanation: Ransomware locks data or systems, making them inaccessible until a ransom is paid.

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

Answer: B

Explanation: Training employees to recognize phishing, scams, and other manipulations is critical to prevent social engineering attacks.

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

Answer: A

Explanation: Spear phishing is personalized phishing targeting specific individuals, often using gathered personal information.

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

Answer: B

Explanation: Endpoint security protects devices connected to the network from malware, unauthorized access, and other threats.

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

Answer: B

Explanation: Insider threats involve individuals within an organization abusing access privileges to harm the organization intentionally or accidentally.

39. Which of the following protocols is used for secure email transmission?

- A. SMTP
- B. IMAP
- C. POP3
- D. SMTPS

Answer: D

Explanation: SMTPS (SMTP Secure) encrypts email during transmission, protecting content from interception.

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

Answer: A

Explanation: Input validation and parameterized queries prevent attackers from inserting malicious SQL into database queries.

That completes Questions 21–40.

I can continue with Questions 41–60, which will include more advanced topics like cloud security, IoT threats, incident response, and more.

Shall I proceed with the next 20 questions?

yes

Great! Here's Part 3: Questions 41–60 of the cybersecurity quiz, with answers and explanations.

Cybersecurity Quiz: Questions 41–60

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

Answer: B

Explanation: IDS monitors network or system activity for signs of attacks or policy violations and alerts administrators.

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

Answer: B

Explanation: Patches are updates released by software vendors to correct security flaws or improve functionality.

43. Which of the following is NOT a type of malware?

- A. Virus
- B. Worm
- C. Trojan
- D. VPN

Answer: D

Explanation: VPNs (Virtual Private Networks) are security tools, not malware. Viruses, worms, and trojans are all types of malicious software.

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

Answer: B

Explanation: Encryption converts data into a coded format that can only be read by someone with the correct decryption key.

45. Which type of attack targets the weakest link: the user?

- A. Malware injection
- B. Social engineering
- C. DDoS
- D. Man-in-the-Middle

Answer: B

Explanation: Social engineering exploits human behavior rather than technical vulnerabilities, often tricking users into revealing information.

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

Answer: B

Explanation: Worms can spread automatically through networks, while viruses typically require a user to execute an infected file.

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

Answer: B

Explanation: Phishing emails often create urgency or fear to trick users into revealing sensitive information or clicking malicious links.

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

Answer: B

Explanation: Network segmentation isolates critical systems, reducing the impact of breaches and limiting lateral movement by attackers.

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

Answer: B

Explanation: APTs are sustained, sophisticated attacks aimed at stealing sensitive data over an extended period.

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

Answer: B

Explanation: Cyber hygiene involves routine security measures such as updates, backups, and safe online behavior to reduce vulnerabilities.

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

Answer: A

Explanation: Authentication ensures that the user or system is who they claim to be, typically via passwords, biometrics, or tokens.

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

Answer: B

Explanation: Ransomware encrypts files or systems and requests payment for the decryption key.

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

Answer: B

Explanation: Symmetric encryption uses the same key for both encryption and decryption, while asymmetric uses a public/private key pair.

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

Answer: B

Explanation: Password managers securely store and generate complex passwords, reducing the risk of reuse or theft.

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

Answer: B

Explanation: DoS attacks overwhelm system resources, preventing legitimate users from accessing services.

56. Which security measure ensures data cannot be read if intercepted?

- A. Authentication
- B. Encryption
- C. Patching
- D. Firewalls

Answer: B

Explanation: Encryption protects data in transit or storage, making it unreadable without the proper key.

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

Answer: B

Explanation: Public Wi-Fi is often unsecured, making it possible for attackers to intercept data like passwords and personal information.

58. Which of the following is NOT considered a form of malware?

- A. Trojan
- B. Worm
- C. Antivirus
- D. Ransomware

Answer: C

Explanation: Antivirus software protects against malware; Trojans, worms, and ransomware are all types of malware.

59. Which type of security threat targets Internet of Things (IoT) devices?

- A. Botnets
- B. Keylogging
- C. SQL Injection
- D. Firewall bypass

Answer: A

Explanation: IoT devices are often less secure, making them targets for botnets that exploit vulnerabilities for large-scale attacks.

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

Answer: B

Explanation: An incident response plan outlines procedures to detect, contain, and recover from cyber incidents efficiently.

That completes Questions 41–60.

The next set, Questions 61–80, will dive into cloud security, mobile security, threat intelligence, compliance, and emerging threats.

Ready for the next 20 questions?

yes

Perfect! Here's Part 4: Questions 61–80 of the cybersecurity quiz, with answers and explanations.

Cybersecurity Quiz: Questions 61–80

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

Answer: B

Explanation: Cloud security focuses on safeguarding data and services hosted in cloud platforms from unauthorized access, breaches, and data loss.

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

Answer: B

Explanation: Misconfigured cloud storage can expose sensitive data publicly, making it a common cloud security risk.

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

Answer: B

Explanation: MFA strengthens security by requiring two or more verification methods (e.g., password + fingerprint).

64. Which of the following is a cybersecurity compliance standard for protecting health data?

- A. GDPR
- B. HIPAA
- C. PCI-DSS
- D. ISO 27001

Answer: B

Explanation: HIPAA sets regulations for protecting personal health information (PHI) in the healthcare sector.

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

Answer: B

Explanation: Threat intelligence helps organizations proactively identify and mitigate cyber threats.

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

Answer: B

Explanation: DDoS attacks use many compromised devices to flood a system with traffic, causing disruption.

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

Answer: B

Explanation: MDM solutions enforce security policies, remotely manage devices, and protect sensitive data on mobile devices.

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

Answer: B

Explanation: Proper disposal ensures that sensitive data cannot be recovered, reducing the risk of data breaches.

69. Which of the following is an example of a software vulnerability?

- A. Strong password

- B. Buffer overflow
- C. VPN connection
- D. Firewall

Answer: B

Explanation: A buffer overflow is a flaw in software that can be exploited to execute malicious code or crash systems.

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

Answer: B

Explanation: Penetration testing identifies weaknesses in a system by mimicking real-world attack scenarios.

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

Answer: B

Explanation: Polymorphic malware modifies its code continuously to evade antivirus and detection mechanisms.

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

Answer: B

Explanation: DLP systems detect and block unauthorized attempts to transfer sensitive information outside the organization.

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

Answer: B

Explanation: BYOD introduces devices that may not meet organizational security standards, increasing the risk of breaches.

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

Answer: B

Explanation: Many IoT devices lack resources to implement strong security, making them vulnerable to attacks.

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

Answer: B

Explanation: SIEM systems provide centralized monitoring and analysis of security events to detect and respond to threats.

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

Answer: B

Explanation: Endpoint security focuses on protecting individual devices connected to the network from malware and unauthorized access.

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

Answer: B

Explanation: NAC ensures that only devices meeting security requirements can access the network, reducing risk of compromise.

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

Answer: B

Explanation: RaaS allows less-skilled attackers to deploy ransomware by renting tools from more skilled cybercriminals.

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

Answer: B

Explanation: Vulnerability management involves a continuous cycle of identifying, prioritizing, and fixing security weaknesses.

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

Answer: B

Explanation: A honeynet is a collection of honeypots used to monitor attacker behavior across multiple systems for research and defense.

That completes Questions 61–80.

The final set, Questions 81–100, will cover advanced attacks, emerging cybersecurity trends, cloud threats, incident response, and best practices for organizations.

Shall I continue with the last 20 questions?

yes

Excellent! Here's Part 5: Questions 81–100, completing the 100-question cybersecurity quiz with answers and explanations.

Cybersecurity Quiz: Questions 81–100

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

Answer: D

Explanation: Malware or attacks can cause multiple symptoms including slow performance, pop-ups, or altered files.

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

Answer: B

Explanation: SOCs centralize cybersecurity monitoring and incident response for organizations.

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

Answer: B

Explanation: Pharming attacks manipulate DNS or website settings to redirect users to fraudulent sites to steal credentials.

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

Answer: B

Explanation: Audits assess whether security measures meet organizational standards and regulatory requirements.

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

Answer: D

Explanation: Cloud security combines MFA, encryption, and access control to protect sensitive data and resources.

86. Which type of malware can spread without user interaction?

- A. Trojan
- B. Worm
- C. Adware
- D. Ransomware

Answer: B

Explanation: Worms self-propagate across networks, while trojans and ransomware typically require user action.

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

Answer: B

Explanation: Threat modeling analyzes systems to anticipate possible attacks and plan countermeasures proactively.

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

Answer: B

Explanation: APTs involve sustained attacks, often targeting specific organizations or data over months or years.

89. Which of the following is a cybersecurity framework?

- A. NIST Cybersecurity Framework
- B. HTTP
- C. TCP/IP
- D. SQL

Answer: A

Explanation: The NIST framework provides guidelines for managing and reducing cybersecurity risks.

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

Answer: A

Explanation: SQL injection targets web application databases by injecting malicious queries to manipulate or steal data.

91. Which security measure helps prevent data exfiltration over the network?

- A. Firewall
- B. Data Loss Prevention (DLP)
- C. Antivirus software
- D. Password complexity

Answer: B

Explanation: DLP systems monitor and block unauthorized transfer of sensitive information.

92. Which type of attack uses multiple devices to overwhelm a system?

- A. DDoS
- B. MITM
- C. Phishing
- D. Spyware

Answer: A

Explanation: Distributed Denial-of-Service (DDoS) attacks use many compromised devices to flood a target, making it unavailable.

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

Answer: B

Explanation: Proper API security involves validating input, authenticating users, encrypting data, and monitoring usage.

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

Answer: B

Explanation: Ethical hackers identify and fix security weaknesses legally to prevent malicious attacks.

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

Answer: A

Explanation: Shadow IT refers to systems or apps used without IT approval, introducing security vulnerabilities.

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

Answer: B

Explanation: Segmentation reduces the risk of attackers moving freely through a network after compromising one system.

97. Which type of malware records user activities, including keystrokes and browsing?

- A. Ransomware
- B. Keylogger
- C. Worm
- D. Adware

Answer: B

Explanation: Keyloggers capture keystrokes to steal sensitive information such as passwords and financial data.

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

Answer: D

Explanation: A combination of awareness training, technical controls, and authentication reduces phishing risks.

99. Which emerging threat involves AI-generated content to deceive users?

- A. Spear phishing
- B. Deepfake attacks
- C. DDoS
- D. SQL injection

Answer: B

Explanation: Deepfakes use AI to create realistic fake audio or video to impersonate individuals, often for fraud or misinformation.

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

Answer: B

Explanation: Incident response begins with identifying and detecting the incident to understand its scope before containment and remediation.