1. **What is the primary purpose of a firewall in network security?**
   - **A. Encrypting data**
   - **B. Monitoring network traffic**
   - **C. Controlling access to network resources**
   - **D. Detecting malware**

2. **What type of attack involves intercepting and modifying communication between two parties?**
   - **A. Phishing**
   - **B. Man-in-the-middle**
   - **C. DDoS**
   - **D. Brute force**

3. **Which of the following encryption algorithms is symmetric?**
   - **A. RSA**
   - **B. AES**
   - **C. Diffie-Hellman**
   - **D. ECC**

4. **What is the primary purpose of a VPN (Virtual Private Network)?**
   - **A. Anonymize browsing**
   - **B. Secure communication over public networks**
   - **C. Filter out malicious content**
   - **D. Monitor network traffic**

5. **Which of the following is a secure protocol for transferring files?**
   - **A. FTP**
   - **B. SFTP**
   - **C. TFTP**
   - **D. SNMP**

6. **Which of the following is NOT a type of access control?**
   - **A. DAC**
   - **B. MAC**
   - **C. RBAC**
   - **D. HAC**

7. **What is the primary purpose of an Intrusion Detection System (IDS)?**
   - **A. Encrypting data**
   - **B. Monitoring and alerting on potential security breaches**
   - **C. Controlling access to network resources**
   - **D. Detecting malware**

8. **Which of the following is a form of social engineering?**
   - **A. SQL injection**
   - **B. DDoS**
   - **C. Phishing**
   - **D. Cross-site scripting**

9. **What type of vulnerability assessment actively attempts to exploit vulnerabilities?**
   - **A. Passive scanning**
   - **B. Active scanning**
   - **C. Penetration testing**
   - **D. Baseline reporting**

10. **What is the primary purpose of a digital signature?**
    - **A. Ensure confidentiality**
    - **B. Verify sender identity and data integrity**
    - **C. Encrypt data**
    - **D. Authenticate users**

11. **Which of the following is a common method for securely erasing data on a hard drive?**
    - **A. Overwriting**
    - **B. Degaussing**
    - **C. Shredding**
    - **D. All of the above**

12. Which of the following best describes a risk assessment?

- **A. A method for identifying vulnerabilities in a system**
- **B. A process for prioritizing risks based on likelihood and impact**
- **C. A framework for managing risks**
- **D. A tool for quantifying risks**

13. Which of the following is a type of biometric authentication?

- **A. Password**
- **B. Smart card**
- **C. Fingerprint scan**
- **D. PIN**

14. Which of the following is a public key infrastructure (PKI) component?

- **A. Certificate authority (CA)**
- **B. Intrusion detection system (IDS)**
- **C. VPN**
- **D. Firewall**

15. What is a zero-day vulnerability?

- **A. A vulnerability that is known but unpatched**
- **B. A vulnerability that is unknown and unpatched**
- **C. A vulnerability that has been patched**
- **D. A vulnerability that is actively being exploited**

16. What type of malware typically spreads itself through network connections?

- **A. Worm**
- **B. Virus**
- **C. Trojan**
- **D. Spyware**

17. Which of the following best describes a honeypot?

- **A. A decoy system used to attract and detect attackers**
- **B. A type of firewall**
- **C. A secure storage location for sensitive data**
- **D. A tool for scanning network vulnerabilities**

18. What is the primary purpose of a Security Information and Event Management (SIEM) system?

- **A. Encrypting data**
- **B. Centralizing and analyzing log data from various sources**
- **C. Controlling access to network resources**
- **D. Detecting malware**

19. Which of the following is a type of physical security control?

- **A. Firewall**
- **B. Intrusion detection system (IDS)**
- **C. Mantrap**
- **D. Security policy**

20. What does the principle of least privilege (POLP) dictate?

- **A. Users should only have the permissions necessary to perform their job functions**
- **B. Users should have full access to all systems and resources**
- **C. Users should share login credentials to streamline work processes**
- **D. Users should have different levels of access based on seniority**

21. Which of the following is an example of a security incident?

- **A. Software malfunction**
- **B. Unauthorized access to sensitive data**
- **C. Hardware failure**
- **D. Scheduled system maintenance**

22. What is the primary purpose of a Data Loss Prevention (DLP) solution?

- **A. Detecting and preventing unauthorized data transfers**
- **B. Encrypting data at rest and in transit**
- **C. Monitoring network traffic**
- **D. Scanning for malware**

23. What type of attack involves overwhelming a target system with traffic or requests?

- **A. Man-in-the-middle**
- **B. DDoS**
- **C. Brute force**
- **D. Phishing**

24. Which of the following is a best practice for secure password management?

- **A. Use of complex, unique passwords for each account**
- **B. Sharing passwords with trusted colleagues**
- **C. Writing passwords on sticky notes for easy access**
- **D. Using the same password for all accounts**

25. What type of attack involves an attacker sending malformed or malicious data to a target application?

- **A. Buffer overflow**
- **B. SQL injection**
- **C. Cross-site scripting (XSS)**
- **D. Brute force**

26. Which security concept ensures that data is only accessible to authorized users?

- **A. Confidentiality**
- **B. Integrity**
- **C. Availability**
- **D. Non-repudiation**

27. What type of backup strategy involves creating a copy of only the data that has changed since the last full backup?

- **A. Incremental backup**
- **B. Differential backup**
- **C. Full backup**
- **D. Snapshot backup**

28. Which of the following is a secure email protocol that encrypts both messages and attachments?

- **A. SMTP**
- **B. IMAP**
- **C. POP3**
- **D. S/MIME**

29. Which of the following is a type of hardware-based security technology that isolates and protects sensitive data on a device?

- **A. HSM**
- **B. TPM**
- **C. BIOS**
- **D. UTM**

30. What type of attack involves an attacker sending unsolicited messages to a large number of recipients?

- **A. DDoS**
- **B. Brute force**
- **C. Spam**
- **D. Phishing**

31. What is the primary purpose of two-factor authentication (2FA)?

- **A. Increase security by requiring two different authentication methods**
- **B. Encrypt data in transit**
- **C. Monitor network traffic**
- **D. Detect malware**

32. Which of the following is an example of a network segmentation technique?

- **A. DMZ**
- **B. VLAN**
- **C. Subnetting**
- **D. All of the above**

33. Which type of cryptography uses two keys, one for encryption and one for decryption?

- **A. Symmetric-key cryptography**
- **B. Asymmetric-key cryptography**
- **C. Hash function**
- **D. Digital signature**

34. What is the primary purpose of a Security Operations Center (SOC)?

- **A. Encrypt data**
- **B. Monitor and respond to security incidents**
- **C. Control access to network resources**
- **D. Detect malware**

35. Which of the following is an example of a wireless security protocol?

- **A. WEP**
- **B. WPA2**
- **C. WPA3**
- **D. All of the above**

36. What is the primary purpose of a Network Access Control (NAC) system?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Control access to network resources based on device compliance**
- **D. Detect malware**

37. Which type of malware typically requires user interaction to execute and spread?

- **A. Worm**
- **B. Virus**
- **C. Trojan**
- **D. Ransomware**

38. Which of the following is a common method for detecting a rootkit?

- **A. Signature-based detection**
- **B. Heuristic analysis**
- **C. Behavior monitoring**
- **D. All of the above**

39. What is the primary purpose of a patch management process?

- **A. Detect and prevent unauthorized data transfers**
- **B. Encrypt data at rest and in transit**
- **C. Maintain system security and stability by applying updates**
- **D. Scan for malware**

40. Which type of security testing involves a tester with limited knowledge of the target system?

- **A. White box testing**
- **B. Gray box testing**
- **C. Black box testing**
- **D. Red team testing**

41. What is the primary purpose of an incident response plan?

- **A. Detect security incidents**
- **B. Provide a structured approach for managing security incidents**
- **C. Prevent security incidents**
- **D. Recover from security incidents**

42. Which of the following is an example of a security control that provides redundancy?

- **A. Firewall**
- **B. Intrusion detection system (IDS)**
- **C. Backup generator**
- **D. VPN**

43. What is the primary purpose of a port scanner?

- **A. Encrypt data**
- **B. Identify open network ports and services**
- **C. Control access to network resources**
- **D. Detect malware**

44. What type of disaster recovery strategy involves running systems and applications at a secondary site after a disaster?

- **A. Cold site**
- **B. Warm site**
- **C. Hot site**
- **D. Mobile site**

45. What is the primary purpose of an antivirus software?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Control access to network resources**
- **D. Detect and remove malware**

46. Which type of attack involves exploiting a vulnerability in a system or application before the developer can fix it?

- **A. Brute force**
- **B. DDoS**
- **C. Zero-day exploit**
- **D. Man-in-the-middle**

47. What is the primary purpose of a password manager?

- **A. Encrypt data**
- **B. Store and manage user passwords securely**
- **C. Control access to network resources**
- **D. Detect malware**

48. Which of the following is a type of secure web communication protocol?

- **A. HTTP**
- **B. FTP**
- **C. HTTPS**
- **D. Telnet**

49. What type of attack involves an attacker repeatedly attempting to guess a user's login credentials?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Phishing**

50. What type of security control is a security policy?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

51. Which of the following best describes an Information Security Management System (ISMS)?

- **A. A hardware device for securing data**
- **B. A software tool for detecting security incidents**
- **C. A framework for managing and protecting information assets**
- **D. A set of guidelines for responding to security incidents**

52. Which of the following is an example of a physical access control?

- **A. Encryption**
- **B. Antivirus software**
- **C. Keycard lock**
- **D. Firewall**

53. What type of security control is an intrusion prevention system (IPS)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

54. Which of the following is a best practice for securing wireless networks?

- **A. Using weak encryption protocols**
- **B. Disabling SSID broadcasting**
- **C. Allowing open guest networks**
- **D. Not using a pre-shared key**

55. What is the primary purpose of a vulnerability scanner?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Identify potential security weaknesses in systems and networks**
- **D. Detect malware**

56. Which of the following is an example of a cloud computing deployment model?

- **A. Public cloud**
- **B. Private cloud**
- **C. Hybrid cloud**
- **D. All of the above**

57. Which type of authentication factor category does a fingerprint scanner belong to?

- **A. Something you know**
- **B. Something you have**
- **C. Something you are**
- **D. Somewhere you are**

58. What type of security control is a security awareness training program?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

59. Which of the following is an example of a network security monitoring tool?

- **A. HIDS**
- **B. NIDS**
- **C. DLP**
- **D. All of the above**

60. What type of attack involves an attacker gaining unauthorized access to a system by exploiting a vulnerability?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Exploit**

61. What type of malware is designed to encrypt a victim's files and demand a ransom for decryption?

- **A. Worm**
- **B. Virus**
- **C. Trojan**
- **D. Ransomware**

62. Which of the following is a standard for securely exchanging authentication and authorization data between parties?

- **A. OAuth**
- **B. SAML**
- **C. OpenID Connect**
- **D. All of the above**

63. What is the primary purpose of a data classification policy?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Control access to network resources**
- **D. Identify and protect sensitive data based on its value and risk**

64. Which of the following is a type of security control that deters attackers by increasing the perceived effort or risk of an attack?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

65. What type of security testing involves a tester with full knowledge of the target system?

- **A. White box testing**
- **B. Gray box testing**
- **C. Black box testing**
- **D. Red team testing**

66. What is the primary purpose of a business continuity plan (BCP)?

- **A. Detect security incidents**
- **B. Ensure the continued operation of an organization during and after a disruptive event**
- **C. Prevent security incidents**
- **D. Recover from security incidents**

67. Which of the following is a type of encryption algorithm that provides both authentication and encryption?

- **A. RSA**
- **B. AES-GCM**
- **C. DES**
- **D. 3DES**

68. What type of attack involves the unauthorized use of a user's session identifier to gain access to their account?

- **A. Session hijacking**
- **B. Brute force**
- **C. DDoS**
- **D. Phishing**

69. What type of network security device combines multiple security functions into a single appliance?

- **A. Intrusion Detection System (IDS)**
- **B. Firewall**
- **C. Unified Threat Management (UTM)**
- **D. Data Loss Prevention (DLP)**

70. What is the primary purpose of a key management system?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Control access to network resources**
- **D. Securely generate, store, and manage cryptographic keys**

71. Which of the following is an example of a secure remote access technology?

- **A. Remote Desktop Protocol (RDP)**
- **B. Secure Shell (SSH)**
- **C. Telnet**
- **D. Virtual Network Computing (VNC)**

72. What type of cybersecurity incident involves an attacker exploiting a web application to send malicious code to a user's browser?

- **A. SQL injection**
- **B. Cross-site scripting (XSS)**
- **C. CSRF**
- **D. Buffer overflow**

73. What is the primary purpose of a digital certificate?

- **A. Encrypt data**
- **B. Verify the identity of an entity and establish trust**
- **C. Control access to network resources**
- **D. Detect malware**

74. Which of the following is a best practice for managing vendor risks?

- **A. Assessing vendors' security controls and practices**
- **B. Providing vendors with unrestricted access to systems and data**
- **C. Ignoring vendor risks**
- **D. Relying solely on the vendor's reputation**

75. Which of the following is an example of an Information Security Framework?

- **A. NIST Cybersecurity Framework**
- **B. ISO/IEC 27001**
- **C. CIS Critical Security Controls**
- **D. All of the above**

76. Which of the following is an example of an email security best practice?

- **A. Disabling email filtering**
- **B. Using digital signatures**
- **C. Opening all email attachments**
- **D. Trusting all email links**

77. What type of security testing involves a simulated attack on an organization's systems to assess their security posture?

- **A. White box testing**
- **B. Gray box testing**
- **C. Black box testing**
- **D. Red team testing**

78. Which of the following is an example of a host-based intrusion detection system (HIDS)?

- **A. Snort**
- **B. OSSEC**
- **C. Suricata**
- **D. Bro**

79. What type of biometric authentication method involves analyzing a user's typing rhythm and patterns?

- **A. Fingerprint recognition**
- **B. Iris recognition**
- **C. Voice recognition**
- **D. Keystroke dynamics**

80. Which of the following is an example of a network-based intrusion detection system (NIDS)?

- **A. Snort**
- **B. OSSEC**
- **C. Suricata**
- **D. Bro**

81. What is the primary purpose of a Security Information and Event Management (SIEM) system?

- **A. Encrypt data**
- **B. Aggregate, analyze, and correlate security event data from multiple sources**
- **C. Control access to network resources**
- **D. Detect malware**

82. Which type of security control involves creating a baseline of normal system behavior and alerting when deviations occur?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

83. What type of security control is a firewall?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

84. What is the primary purpose of a risk assessment?

- **A. Encrypt data**
- **B. Identify and evaluate potential risks and vulnerabilities**
- **C. Control access to network resources**
- **D. Detect malware**

85. Which of the following is an example of a secure file transfer protocol?

- **A. FTP**
- **B. TFTP**
- **C. SFTP**
- **D. SCP**

86. What type of attack involves an attacker intercepting and altering communication between two parties without their knowledge?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Phishing**

87. Which of the following is a type of incident that typically triggers the activation of a disaster recovery plan?

- **A. Hardware failure**
- **B. Natural disaster**
- **C. Cyberattack**
- **D. All of the above**

88. What is the primary purpose of a demilitarized zone (DMZ) in a network architecture?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Create a buffer zone between an organization's internal network and the internet**
- **D. Detect malware**

89. Which type of security control is a security camera?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

90. What type of malware often disguises itself as legitimate software or is included in legitimate software that has been tampered with?

- **A. Worm**
- **B. Virus**
- **C. Trojan**
- **D. Ransomware**

91. Which of the following is an example of an encryption key exchange protocol?

- **A. RSA**
- **B. Diffie-Hellman**
- **C. AES**
- **D. Blowfish**

92. What is the primary purpose of a honeypot?

- **A. Encrypt data**
- **B. Attract and monitor attackers to gain insights and improve security**
- **C. Control access to network resources**
- **D. Detect malware**

93. What type of security control is a user awareness training program?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

94. Which type of attack involves an attacker flooding a network with malformed packets?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Fragmentation attack**

95. What type of security control is an audit log?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

96. Which of the following is an example of a data loss prevention (DLP) solution?

- **A. Digital Rights Management (DRM)**
- **B. Encryption**
- **C. Network monitoring**
- **D. All of the above**

97. What is the primary purpose of a secure software development lifecycle (SDLC) process?

- **A. Encrypt data**
- **B. Monitor network traffic**
- **C. Ensure that security is integrated throughout the software development process**
- **D. Detect malware**

98. What type of security control is a security policy?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

99. Which of the following is an example of a mobile device management (MDM) solution?

- **A. Apple Configurator**
- **B. Microsoft Intune**
- **C. MobileIron**
- **D. All of the above**

100. What is the primary purpose of a network intrusion detection system (NIDS)?

- **A. Encrypt data**
- **B. Monitor network traffic for signs of malicious activity**
- **C. Control access to network resources**
- **D. Detect malware**

101. Which of the following is an example of a network access control (NAC) solution?

- **A. Cisco ISE**
- **B. Microsoft Intune**
- **C. MobileIron**
- **D. Apple Configurator**

102. What type of security control is a backup and restore solution?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

103. What is the primary purpose of a digital signature?

- **A. Encrypt data**
- **B. Verify the integrity and authenticity of a message or document**
- **C. Control access to network resources**
- **D. Detect malware**

104. Which type of attack involves an attacker sending unsolicited messages to a large number of recipients, often for the purpose of spreading malware or phishing?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Spam**

105. Which of the following is a type of network segmentation used to isolate different types of network traffic?

- **A. Subnetting**
- **B. VLAN**
- **C. DMZ**
- **D. All of the above**

106. What type of security control is an intrusion detection system (IDS)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

107. What is the primary purpose of an incident response plan (IRP)?

- **A. Encrypt data**
- **B. Prepare for, respond to, and recover from security incidents**
- **C. Control access to network resources**
- **D. Detect malware**

108. Which of the following is an example of a secure communication protocol for remote administration?

- **A. Telnet**
- **B. RDP**
- **C. SSH**
- **D. VNC**

109. What type of security control involves restricting access to sensitive information based on a user's role or job function?

- **A. Access control**
- **B. Role-based access control (RBAC)**
- **C. Discretionary access control (DAC)**
- **D. Mandatory access control (MAC)**

110. Which type of attack involves an attacker attempting to gain unauthorized access to an account by guessing or cracking the password?

- **A. Password attack**
- **B. Brute force**
- **A. DDoS**
- **B. Phishing**

111. What is the primary purpose of an endpoint protection platform (EPP)?

- **A. Encrypt data**
- **B. Monitor, detect, and prevent threats on endpoints**
- **C. Control access to network resources**
- **D. Detect malware**

112. Which of the following is an example of a secure email protocol?

- **A. SMTP**
- **B. IMAP**
- **C. POP3**
- **D. STARTTLS**

113. What is the primary purpose of a threat intelligence platform?

- **A. Encrypt data**
- **B. Collect, analyze, and share threat information to improve security defenses**
- **C. Control access to network resources**
- **D. Detect malware**

114. Which type of security control is a secure coding guideline?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

115. What type of attack involves an attacker exploiting a DNS server to redirect traffic to a malicious site?

- **A. Man-in-the-middle**
- **B. DNS poisoning**
- **C. DDoS**
- **D. Phishing**

116. Which of the following is an example of a secure password hashing algorithm?

- **A. MD5**
- **B. SHA-1**
- **C. bcrypt**
- **D. DES**

117. What is the primary purpose of a security operations center (SOC)?

- **A. Encrypt data**
- **B. Monitor, detect, and respond to security incidents**
- **C. Control access to network resources**
- **D. Detect malware**

118. What type of security control is a firewall rule?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

119. Which of the following is an example of a secure voice communication protocol?

- **A. H.323**
- **B. SIP**
- **C. RTP**
- **D. SRTP**

120. What is the primary purpose of a web application firewall (WAF)?

- **A. Encrypt data**
- **B. Protect web applications from attacks and vulnerabilities**
- **C. Control access to network resources**
- **D. Detect malware**

121. Which type of security control involves the implementation of physical barriers to prevent unauthorized access to a facility?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

122. What type of security control is a security group in a cloud environment?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

123. Which of the following is an example of a zero-day vulnerability?

- **A. A vulnerability that has been publicly disclosed but not yet patched by the vendor**
- **B. A vulnerability that has been known for more than 30 days**
- **C. A vulnerability that is actively being exploited before the vendor is aware of its existence**
- **D. A vulnerability that has been patched by the vendor**

124. What is the primary purpose of a virtual private network (VPN)?

- **A. Encrypt data**
- **B. Create a secure, encrypted connection over a public network**
- **C. Control access to network resources**
- **D. Detect malware**

125. Which of the following is an example of a defense-in-depth security strategy?

- **A. Implementing a single layer of security controls**
- **B. Relying solely on a firewall for security**
- **C. Implementing multiple layers of security controls to protect against a variety of threats**
- **D. Focusing on perimeter security only**

126. What type of security control is multi-factor authentication (MFA)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

127. Which of the following is an example of a cloud deployment model?

- **A. Public cloud**
- **B. Private cloud**
- **C. Hybrid cloud**
- **D. All of the above**

128. What type of attack involves an attacker intercepting and forwarding network traffic between two parties?

- **A. Man-in-the-middle**
- **B. Replay attack**
- **C. DDoS**
- **D. Phishing**

129. Which of the following is an example of an IT governance framework?

- **A. NIST Cybersecurity Framework**
- **B. ISO/IEC 27001**
- **C. COBIT**
- **D. ITIL**

130. What is the primary purpose of a vulnerability assessment?

- **A. Encrypt data**
- **B. Identify, quantify, and prioritize vulnerabilities in an organization's systems**
- **C. Control access to network resources**
- **D. Detect malware**

131. Which type of security control is a security awareness training program?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

132. What type of security control is a secure boot process?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

133. Which of the following is an example of a network monitoring tool?

- **A. Wireshark**
- **B. Nmap**
- **C. Nessus**
- **D. Metasploit**

134. What is the primary purpose of a security policy?

- **A. Encrypt data**
- **B. Define an organization's security requirements, expectations, and responsibilities**
- **C. Control access to network resources**
- **D. Detect malware**

135. Which of the following is an example of a secure coding best practice?

- **A. Input validation**
- **B. Hardcoding passwords**
- **C. Using deprecated functions**
- **D. Ignoring error handling**

136. What type of security control is an antivirus software?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

137. What is the primary purpose of a data classification policy?

- **A. Encrypt data**
- **B. Organize and protect data according to its sensitivity and value**
- **C. Control access to network resources**
- **D. Detect malware**

138. Which of the following is an example of a network vulnerability scanner?

- **A. Wireshark**
- **B. Nmap**
- **C. Nessus**
- **D. Metasploit**

139. What type of security control is a security incident and event management (SIEM) system?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

140. What type of attack involves an attacker flooding a network with an excessive amount of traffic, overwhelming its resources and causing a denial of service?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Phishing**

141. What is the primary purpose of a digital forensics investigation?

- **A. Encrypt data**
- **B. Collect, preserve, analyze, and present digital evidence in a legally admissible manner**
- **C. Control access to network resources**
- **D. Detect malware**

142. Which of the following is an example of a host-based firewall?

- **A. pfSense**
- **B. Windows Defender Firewall**
- **C. Cisco ASA**
- **D. Fortinet FortiGate**

143. What is the primary purpose of an identity and access management (IAM) system?

- **A. Encrypt data**
- **B. Manage and control user access to resources and data within an organization**
- **C. Monitor network traffic**
- **D. Detect malware**

144. Which type of security control is a log analysis tool?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

145. What type of attack involves an attacker encrypting a victim's data and demanding payment in exchange for the decryption key?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Ransomware**

146. Which of the following is an example of a secure wireless communication protocol?

- **A. WEP**
- **B. WPA**
- **C. WPA2**
- **D. WPA3**

147. What is the primary purpose of a certificate authority (CA)?

- **A. Encrypt data**
- **B. Issue and manage digital certificates for secure communication**
- **C. Control access to network resources**
- **D. Detect malware**

148. Which type of security control is a data loss prevention (DLP) solution?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

149. What type of security control is a network segmentation?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

150. Which of the following is an example of a social engineering attack?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Phishing**

151. What type of security control is a biometric authentication system?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

152. Which of the following is an example of a privacy-enhancing technology?

- **A. Tor**
- **B. VPN**
- **C. HTTPS**
- **D. All of the above**

153. What type of attack involves an attacker sending a large number of SYN packets to a target system, causing it to allocate resources for connections that will never be completed?

- **A. Man-in-the-middle**
- **B. SYN flood**
- **C. DDoS**
- **D. Phishing**

154. Which of the following is an example of a risk management framework?

- **A. NIST SP 800-37**
- **B. ISO/IEC 27005**
- **C. FAIR**
- **D. All of the above**

155. What is the primary purpose of a firewall?

- **A. Encrypt data**
- **B. Control incoming and outgoing network traffic based on predetermined rules**
- **C. Monitor network traffic**
- **D. Detect malware**

156. Which type of security control is a patch management system?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

157. What type of security control is a password policy?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **E. Preventative**

158. Which of the following is an example of a network traffic analysis tool?

- **A. Wireshark**
- **B. Nmap**
- **C. Nessus**
- **D. Metasploit**

159. What is the primary purpose of a business continuity plan (BCP)?

- **A. Encrypt data**
- **B. Ensure the continued operation of an organization during and after a disruption or disaster**
- **C. Control access to network resources**
- **D. Detect malware**

160. Which of the following is an example of a cybersecurity framework?

- **A. NIST Cybersecurity Framework**
- **B. ISO/IEC 27001**
- **C. CIS Critical Security Controls**
- **D. All of the above**

161. What type of security control is a host-based intrusion detection system (HIDS)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

162. What is the primary purpose of a security information and event management (SIEM) system?

- **A. Encrypt data**
- **B. Aggregate, analyze, and correlate log data from various sources to detect and respond to security incidents**
- **C. Control access to network resources**
- **D. Detect malware**

163. Which of the following is an example of a cloud access security broker (CASB)?

- **A. Microsoft Cloud App Security**
- **B. McAfee MVISION Cloud**
- **C. Netskope**
- **E. All of the above**

164. What type of security control is a secure software development lifecycle (SDLC) process?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

165. Which type of attack involves an attacker compromising a legitimate website to serve malicious content or exploit user vulnerabilities?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Watering hole**

166. What is the primary purpose of a public key infrastructure (PKI)?

- **A. Manage and distribute public and private cryptographic keys for secure communication**
- **B. Detect and prevent network intrusions**
- **C. Control access to network resources**
- **E. Detect malware**

167. Which of the following is an example of a secure file transfer protocol?

- **A. FTP**
- **B. TFTP**
- **C. SFTP**
- **D. SCP**

168. What type of security control is a log retention policy?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

169. Which type of security control is a user access review?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

170. What is the primary purpose of a data encryption standard (DES)?

- **A. Provide symmetric-key encryption for secure communication**
- **B. Detect and prevent network intrusions**
- **C. Control access to network resources**
- **D. Detect malware**

171. Which of the following is an example of a cryptographic hash function?

- **A. AES**
- **B. RSA**
- **C. SHA-256**
- **D. 3DES**

172. What type of security control is a network intrusion detection system (NIDS)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

173. What is the primary purpose of a key management system?

- **A. Generate, store, distribute, and revoke cryptographic keys**
- **B. Detect and prevent network intrusions**
- **C. Control access to network resources**
- **D. Detect malware**

174. Which of the following is an example of a secure web communication protocol?

- **A. HTTP**
- **B. HTTPS**
- **C. FTP**
- **D. SSH**

175. What type of security control is a hardware security module (HSM)?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

176. Which of the following is an example of a containerization technology?

- **A. Docker**
- **B. Kubernetes**
- **C. OpenStack**
- **D. VMware**

177. What type of attack involves an attacker sending a large number of ICMP echo request packets to a target system, causing it to respond with an equal number of echo reply packets, overwhelming its resources?

- **A. Ping flood**
- **B. SYN flood**
- **C. DDoS**
- **D. Phishing**

178. Which of the following is an example of a secure email communication protocol?

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

179. What is the primary purpose of a threat intelligence platform?

- **A. Encrypt data**
- **B. Collect, analyze, and share threat intelligence data for improved security decision-making**
- **C. Control access to network resources**
- **D. Detect malware**

180. Which type of security control is an intrusion prevention system (IPS)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

181. What type of security control is an information security policy?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

182. Which of the following is an example of a network scanning tool?

- **A. Wireshark**
- **B. Nmap**
- **C. Nessus**
- **D. Metasploit**

183. What is the primary purpose of a disaster recovery plan (DRP)?

- **A. Encrypt data**
- **B. Define the procedures for restoring an organization's critical systems and data after a disruption or disaster**
- **C. Control access to network resources**
- **D. Detect malware**

184. Which of the following is an example of a mobile device management (MDM) solution?

- **A. AirWatch**
- **B. MobileIron**
- **C. Microsoft Intune**
- **D. All of the above**

185. What type of security control is an intrusion detection system (IDS)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

186. What is the primary purpose of a risk assessment?

- **A. Encrypt data**
- **B. Identify and evaluate the potential impact of threats and vulnerabilities to an organization's assets**
- **C. Control access to network resources**
- **D. Detect malware**

187. Which of the following is an example of a virtual private network (VPN) protocol?

- **A. PPTP**
- **B. L2TP**
- **C. IPSec**
- **D. All of the above**

188. What type of security control is an incident response plan?

- **A. Physical**
- **B. Technical**
- **C. Administrative**
- **D. Preventative**

189. Which type of attack involves an attacker using multiple systems to target a single system with a flood of network packets?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. Distributed denial of service (DDoS)**
- **D. Phishing**

190. What is the primary purpose of an authentication, authorization, and accounting (AAA) system?

- **A. Ensure that users are who they claim to be, grant appropriate access, and track user activities**
- **B. Detect and prevent network intrusions**
- **C. Control access to network resources**
- **D. Detect malware**

191. Which of the following is an example of a secure shell (SSH) client?

- **A. PuTTY**
- **B. WinSCP**
- **C. FileZilla**
- **D. All of the above**

192. What type of security control is a security operations center (SOC)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

193. What is the primary purpose of a honeypot?

- **A. Encrypt data**
- **B. Attract and observe attackers to gain insight into their tactics, techniques, and procedures**
- **C. Control access to network resources**
- **D. Detect malware**

194. Which of the following is an example of a network access control (NAC) solution?

- **A. Cisco ISE**
- **B. Forescout CounterACT**
- **C. Aruba ClearPass**
- **D. All of the above**

195. What type of security control is an asset management system?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

196. What is the primary purpose of a secure socket layer (SSL) certificate?

- **A. Encrypt data and authenticate the identity of a website**
- **B. Detect and prevent network intrusions**
- **C. Control access to network resources**
- **D. Detect malware**

197. Which of the following is an example of a symmetric encryption algorithm?

- **A. RSA**
- **B. Diffie-Hellman**
- **C. AES**
- **D. ElGamal**

198. What type of security control is a web application firewall (WAF)?

- **A. Preventative**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

199. Which type of attack involves an attacker attempting to gain unauthorized access to a system by trying every possible combination of characters until the correct password is found?

- **A. Man-in-the-middle**
- **B. Brute force**
- **C. DDoS**
- **D. Phishing**

200. What is the primary purpose of a demilitarized zone (DMZ)?

- **A. Encrypt data**
- **B. Separate an organization's internal network from the internet while allowing specific services to be accessible**
- **C. Control access to network resources**
- **D. Detect malware**

1. C	51. C	101.A	151.A
2. B	52. C	102.C	152.D
3. B	53. A	103.B	153.B
4. B	54. B	104.D	154.D
5. B	55. C	105.D	155.B
6. D	56. D	106.B	156.C
7. B	57. C	107.B	157.C
8. C	58. C	108.C	158.A
9. C	59. D	109.B	159.B
10. B	60. D	110.B	160.D
11. D	61. D	111.B	161.B
12. B	62. D	112.D	162.B
13. C	63. D	113.B	163.D
14. A	64. D	114.D	164.D
15. B	65. A	115.B	165.D
16. A	66. B	116.C	166.A
17. A	67. B	117.B	167.C
18. B	68. A	118.A	168.C
19. C	69. C	119.D	169.B
20. A	70. D	120.B	170.A
21. B	71. B	121.A	171.C
22. A	72. B	122.A	172.B
23. B	73. B	123.C	173.A
24. A	74. A	124.B	174.B
25. A	75. D	125.C	175.D
26. A	76. B	126.A	176.A
27. A	77. D	127.D	177.A
28. D	78. B	128.A	178.D
29. B	79. D	129.C	179.B
30. C	80. A	130.B	180.A
31. A	81. B	131.C	181.C
32. D	82. B	132.A	182.B
33. B	83. A	133.A	183.B
34. B	84. B	134.B	184.D
35. D	85. C	135.A	185.B
36. C	86. A	136.C	186.B
37. B	87. D	137.B	187.D
38. D	88. C	138.C	188.C
39. C	89. A	139.B	189.C
40. B	90. C	140.C	190.A
41. B	91. B	141.B	191.D
42. C	92. B	142.B	192.B
43. B	93. A	143.B	193.B
44. C	94. D	144.B	194.D
45. D	95. B	145.D	195.A
46. C	96. D	146.D	196.A
47. B	97. C	147.B	197.C
48. C	98. C	148.A	198.A
49. B	99. D	149.A	199.B
50. C	100.B	150.D	200.B