1: Which of the following is a punishable offense under the Information Technology Act, 2000 (India)?

A) Sending spam emails
B) Unauthorized access to computer systems
C) Encrypting personal data
D) Creating strong passwords

Answer: B) Unauthorized access to computer systems

2: Under the Information Technology Act, 2000, what is the punishment for hacking (Section 66)?

A) Imprisonment up to 6 months and/or fine up to ₹1 lakh
B) Imprisonment up to 3 years and/or fine up to ₹2 lakh
C) Imprisonment up to 5 years and/or fine up to ₹5 lakh
D) No punishment specified

Answer: B) Imprisonment up to 3 years and/or fine up to ₹2 lakh

3: Which of the following is considered cyber terrorism under the Information Technology Act, 2000?

A) Creating and spreading malware
B) Attacking critical infrastructure with intent to cause harm to national security
C) Making false claims online
D) Stalking someone online

Answer: B) Attacking critical infrastructure with intent to cause harm to national security

4: What is the penalty for sending offensive messages through communication services, etc., under Section 66A of the Information Technology Act (before it was struck down by the Supreme Court in 2015)?

A) Imprisonment up to 1 year and/or fine
B) Imprisonment up to 3 years and/or fine
C) Imprisonment up to 5 years and/or fine
D) No penalty

Answer: B) Imprisonment up to 3 years and/or fine (Note: Section 66A was struck down by the Supreme Court in 2015)

5: What is the maximum penalty for cyberstalking under the Information Technology Act, 2000?

A) Imprisonment for up to 1 year and/or fine up to ₹1 lakh
B) Imprisonment for up to 3 years and/or fine up to ₹5 lakh
C) Imprisonment for up to 5 years and/or fine up to ₹10 lakh
D) Imprisonment for up to 2 years and/or fine up to ₹2 lakh

Answer: B) Imprisonment for up to 3 years and/or fine up to ₹5 lakh

6: Under the Information Technology Act, 2000, what is the penalty for sending offensive or obscene emails?

A) Imprisonment up to 1 year and/or fine
B) Imprisonment up to 3 years and/or fine up to ₹2 lakh
C) Imprisonment up to 5 years and/or fine up to ₹5 lakh
D) No penalty

Answer: B) Imprisonment up to 3 years and/or fine up to ₹2 lakh

7: What is the penalty for identity theft under Section 66C of the Information Technology Act?

A) Imprisonment up to 2 years and/or fine up to ₹1 lakh
B) Imprisonment up to 3 years and/or fine up to ₹2 lakh
C) Imprisonment up to 5 years and/or fine up to ₹10 lakh
D) Imprisonment up to 1 year and/or fine up to ₹50,000

Answer: B) Imprisonment up to 3 years and/or fine up to ₹2 lakh

8: Under the Information Technology Act, 2000, what is the penalty for publishing or transmitting obscene material in electronic form (Section 67)?

A) Imprisonment up to 3 years and/or fine up to ₹5 lakh
B) Imprisonment up to 1 year and/or fine
C) Imprisonment up to 5 years and/or fine up to ₹10 lakh
D) No penalty

Answer: A) Imprisonment up to 3 years and/or fine up to ₹5 lakh

9: Which of the following actions is punishable under Section 43 of the Information Technology Act?

A) Data theft
B) Sending spam emails
C) Tampering with the computer source code
D) All of the above

Answer: D) All of the above

10: Under the Information Technology Act, 2000, what is the penalty for cyber fraud under Section 66D?

A) Imprisonment up to 1 year and/or fine up to ₹1 lakh
B) Imprisonment up to 3 years and/or fine up to ₹5 lakh
C) Imprisonment up to 5 years and/or fine up to ₹10 lakh
D) Imprisonment up to 7 years and/or fine up to ₹15 lakh

Answer: B) Imprisonment up to 3 years and/or fine up to ₹5 lakh

11: Which of the following is the primary purpose of the ISO/IEC 27001 standard?

A) To protect the physical security of data centers
B) To establish requirements for an Information Security Management System (ISMS)
C) To regulate the use of encryption technologies
D) To provide guidelines for software development security

Answer: B) To establish requirements for an Information Security Management System (ISMS)

12: Which of the following is a core principle of the General Data Protection Regulation (GDPR)?

A) Data minimization
B) Mandatory data encryption for all data types
C) Data retention for 10 years
D) Only government agencies can process personal data

Answer: A) Data minimization

13: The Payment Card Industry Data Security Standard (PCI DSS) is designed to protect which of the following?

A) Intellectual property
B) Payment card data
C) Employee personal data
D) Secure software coding practices

Answer: B) Payment card data

14: Which of the following best describes the purpose of the NIST Cybersecurity Framework?

A) To provide a guideline for physical security in government facilities
B) To help organizations identify, assess, and manage cybersecurity risks
C) To mandate specific cybersecurity technologies for financial institutions
D) To standardize password requirements across all industries

Answer: B) To help organizations identify, assess, and manage cybersecurity risks

15: Which standard defines the best practices for securing critical infrastructure in the U.S.?

A) ISO/IEC 27001
B) NIST SP 800-53
C) HIPAA
D) NIST Cybersecurity Framework

Answer: B) NIST SP 800-53

16: Under the Health Insurance Portability and Accountability Act (HIPAA), what is the main focus of the Security Rule?

A) Preventing data loss due to cyberattacks
B) Ensuring the confidentiality, integrity, and availability of electronic health information
C) Encrypting all medical records
D) Mandating the use of strong passwords for healthcare professionals

Answer: B) Ensuring the confidentiality, integrity, and availability of electronic health information

17: Which of the following is a key requirement of the SOC 2 (Service Organization Control 2) framework?

A) Encrypting all business emails
B) Maintaining confidentiality of data and implementing strong access controls
C) Ensuring businesses must adopt multi-factor authentication
D) Implementing an enterprise-wide firewall

Answer: B) Maintaining confidentiality of data and implementing strong access controls

18: What is the primary purpose of the Sarbanes-Oxley Act (SOX) in relation to cybersecurity?

A) To mandate the use of firewalls
B) To protect financial information and enforce the accuracy of corporate disclosures
C) To regulate software updates for businesses
D) To define cybercrime laws

Answer: B) To protect financial information and enforce the accuracy of corporate disclosures

19: Which of the following frameworks is specifically designed to improve cybersecurity in the U.S. federal government?

A) NIST Cybersecurity Framework
B) ISO/IEC 27001
C) GDPR
D) PCI DSS

Answer: A) NIST Cybersecurity Framework

20: What is the primary focus of the COBIT (Control Objectives for Information and Related Technologies) framework?

A) Enhancing IT governance and management practices
B) Protecting personal data in healthcare
C) Providing a standardized approach to software testing
D) Protecting payment card information

Answer: A) Enhancing IT governance and management practices

21: What is the primary objective of digital forensics?

A) To protect networks from external attacks
B) To analyze and preserve digital evidence for legal and investigative purposes
C) To recover lost or deleted files from a hard drive
D) To monitor network traffic for malicious activities

Answer: B) To analyze and preserve digital evidence for legal and investigative purposes

22: Which of the following is NOT a key principle of digital forensics?

A) Integrity of the evidence must be maintained
B) All evidence should be analyzed directly from the original device
C) Documentation of each step taken during the investigation is essential
D) Evidence should be duplicated (imaged) before analysis

Answer: B) All evidence should be analyzed directly from the original device

23: In digital forensics, what is a "write blocker" used for?

A) To prevent unauthorized access to a system
B) To ensure that data is not modified during the analysis
C) To block the transfer of sensitive data
D) To recover deleted data from hard drives

Answer: B) To ensure that data is not modified during the analysis

24: What is the first step in a digital forensics investigation?

A) Analyzing the evidence
B) Acquiring the evidence
C) Presenting findings in court
D) Documenting the incident timeline

Answer: B) Acquiring the evidence

25: Which of the following tools is commonly used for creating forensic disk images?

A) FTK Imager
B) Wireshark
C) Kali Linux
D) Metasploit

Answer: A) FTK Imager

26: What is "data carving" in digital forensics?

A) Analyzing the structure of file systems
B) Recovering fragmented data by identifying patterns within unallocated space
C) Extracting encrypted data from a storage device
D) Writing data securely to a forensic evidence disk

Answer: B) Recovering fragmented data by identifying patterns within unallocated space

27: In a digital forensics investigation, what is the significance of "chain of custody"?

A) It ensures that the evidence has been analyzed by certified professionals
B) It maintains a record of everyone who has handled the evidence, preserving its integrity
C) It helps to identify patterns of cybercrime across multiple cases
D) It validates the accuracy of the analysis performed on the evidence

Answer: B) It maintains a record of everyone who has handled the evidence, preserving its integrity

28: Which of the following is the primary method of obtaining evidence from a powered-on system during a live forensics investigation?

A) Data carving
B) Memory dump
C) Hard disk imaging
D) Full system encryption

Answer: B) Memory dump

29: What type of evidence is typically examined during a digital forensics investigation on a mobile device?

A) Call logs and SMS messages
B) Only text files stored in the device
C) Network traffic logs
D) Hardware components

Answer: A) Call logs and SMS messages

30: In a digital forensics investigation, what is the role of "hashing"?

A) To encrypt the digital evidence
B) To create a unique identifier (hash value) for the evidence to ensure integrity
C) To speed up the analysis process by categorizing data
D) To recover deleted data from a storage device

Answer: B) To create a unique identifier (hash value) for the evidence to ensure integrity

31: What is the primary purpose of a Virtual Private Network (VPN)?

A) To improve internet speed by reducing latency
B) To encrypt data and protect online privacy while using public networks
C) To block malware from entering a network
D) To detect and respond to cyber threats in real-time

Answer: B) To encrypt data and protect online privacy while using public networks

32: Which of the following protocols is commonly used by VPNs for secure communication?

A) HTTP
B) FTP
C) IPsec
D) SMTP

Answer: C) IPsec

33: What is the main advantage of using a VPN for remote access?

A) It provides high-speed internet access
B) It allows secure connections to a private network over the internet
C) It eliminates the need for firewalls
D) It reduces the amount of data usage

Answer: B) It allows secure connections to a private network over the internet

34: Which of the following is a disadvantage of using a VPN?

A) It can increase internet speed due to encryption overhead
B) It can lead to reduced network performance due to encryption overhead
C) It prevents all forms of cyberattacks
D) It makes devices immune to malware

Answer: B) It can lead to reduced network performance due to encryption overhead

35: What does the term "tunneling" refer to in the context of VPNs?

A) The process of separating internet traffic from local network traffic
B) The method used to encrypt the data being sent over the VPN
C) The technique of compressing data to increase VPN speed
D) The way a VPN creates a private, secure connection over a public network

Answer: D) The way a VPN creates a private, secure connection over a public network

36: Which of the following types of VPNs is used by organizations to allow employees to securely access the corporate network remotely?

A) Site-to-Site VPN
B) Client-to-Site VPN
C) Peer-to-Peer VPN
D) Mesh VPN

Answer: B) Client-to-Site VPN

37: What is the function of a VPN "kill switch"?

A) It detects and prevents data leakage from the VPN connection
B) It automatically terminates the VPN connection if the connection is lost to protect the data
C) It prevents unauthorized devices from connecting to the VPN
D) It improves the encryption strength of the VPN connection

Answer: B) It automatically terminates the VPN connection if the connection is lost to protect the data

38: Which of the following is a common VPN protocol used to ensure security through encryption?

A) HTTP
B) PPTP
C) TCP/IP
D) DNS

Answer: B) PPTP

39: Which of the following is a potential risk associated with free VPN services?

A) Increased encryption overhead
B) Slower internet speeds due to high server demand
C) The potential for the provider to log and sell user data
D) All of the above

Answer: D) All of the above

40: Which type of VPN is typically used to securely connect two or more networks, such as connecting an office to a branch office?

A) Site-to-Site VPN
B) Client-to-Site VPN
C) Peer-to-Peer VPN
D) Hybrid VPN

Answer: A) Site-to-Site VPN

41. What does IPsec stand for?

a) Internet Protection Security
b) Internet Protocol Security
c) Internet Packet Security
d) Internal Protocol Security
Answer: b) Internet Protocol Security

42. Which protocol is used by IPsec to provide confidentiality?

a) AH (Authentication Header)
b) ESP (Encapsulating Security Payload)
c) ICMP (Internet Control Message Protocol)
d) TCP (Transmission Control Protocol)
Answer: b) ESP (Encapsulating Security Payload)

43. Which of the following is NOT a mode of IPsec operation?

a) Transport mode
b) Tunnel mode
c) Gateway mode
d) None of the above
Answer: c) Gateway mode

44. What is the primary purpose of the Authentication Header (AH) in IPsec?

a) To provide data encryption
b) To ensure integrity and authentication
c) To compress data packets

d) To improve network speed
Answer: b) To ensure integrity and authentication

45. Which protocol does IPsec use for key exchange?

a) HTTPS
b) ISAKMP (Internet Security Association and Key Management Protocol)
c) SSL
d) FTP
Answer: b) ISAKMP

46. What is the default port number for Internet Key Exchange (IKE) used in IPsec?

a) 80
b) 500
c) 443
d) 22
Answer: b) 500

47. In which layer of the OSI model does IPsec operate?

a) Application layer
b) Transport layer
c) Network layer
d) Data link layer
Answer: c) Network layer

48. Which of the following is true about IPsec Transport Mode?

a) The entire IP packet is encrypted.
b) Only the payload of the IP packet is encrypted.
c) It creates a new IP header.
d) It requires a tunnel to be established.
Answer: b) Only the payload of the IP packet is encrypted.

49. Which component of IPsec is responsible for ensuring that data has not been tampered

a) Authentication Header (AH)
b) Encapsulating Security Payload (ESP)
c) Internet Key Exchange (IKE)
d) Datagram Transport Layer Security (DTLS)
Answer: a) Authentication Header (AH)

50. What is the purpose of Security Associations (SA) in IPsec?

a) To define the algorithms and keys for secure communication
b) To establish user identities
c) To block unauthorized IP addresses
d) To monitor network traffic
Answer: a) To define the algorithms and keys for secure communication

51. What is the primary purpose of an Intrusion Detection System (IDS)?

a) To prevent unauthorized access
b) To detect unauthorized access or abnormal activity
c) To block malicious IPs
d) To encrypt sensitive data
Answer: b) To detect unauthorized access or abnormal activity

52. Which of the following is NOT a type of IDS?

a) Host-based IDS (HIDS)
b) Network-based IDS (NIDS)
c) Application-based IDS (AIDS)
d) Cloud-based IDS
Answer: d) Cloud-based IDS

53. Which IDS detects intrusions by comparing activity against known patterns?

a) Anomaly-based IDS
b) Signature-based IDS
c) Behavioral-based IDS
d) Hybrid-based IDS
Answer: b) Signature-based IDS

54. What is a key limitation of signature-based IDS?

a) It generates too many false positives.
b) It cannot detect new or unknown threats.
c) It requires no updates.
d) It cannot monitor network traffic.
Answer: b) It cannot detect new or unknown threats.

55. Anomaly-based IDS identifies intrusions by:

a) Matching predefined rules
b) Detecting deviations from normal behavior
c) Encrypting all traffic

d) Blocking all unauthorized traffic
Answer: b) Detecting deviations from normal behavior

56. Which of the following is an example of a hybrid IDS?

a) IDS that combines host-based and network-based detection
b) IDS that integrates both signature and anomaly detection
c) IDS that blocks all unauthorized access
d) IDS that uses machine learning exclusively
Answer: b) IDS that integrates both signature and anomaly detection

57. What is the main difference between an IDS and an Intrusion Prevention System (IPS)?

a) IDS can block malicious activity, while IPS cannot.
b) IPS can block malicious activity, while IDS cannot.
c) IDS operates at the application layer, while IPS operates at the transport layer.
d) There is no difference; they are the same.
Answer: b) IPS can block malicious activity, while IDS cannot.

58. Which of the following is an open-source IDS?

a) McAfee IDS
b) Snort
c) Norton IDS
d) Cisco Secure IDS
Answer: b) Snort

59. What is a false positive in the context of intrusion detection?

a) A legitimate action flagged as an intrusion
b) A successful intrusion that goes undetected
c) An intrusion detected by the wrong system
d) A malicious action that bypasses the IDS
Answer: a) A legitimate action flagged as an intrusion

60. Which type of IDS monitors a single host for suspicious activity?
a) Network-based IDS (NIDS)
b) Host-based IDS (HIDS)
c) Anomaly-based IDS
d) Cloud-based IDS
Answer: b) Host-based IDS (HIDS)

61. Which protocol is commonly used to secure communication over the web?
a) HTTP
b) FTP
c) HTTPS
d) SMTP
Answer: c) HTTPS

62. What is the purpose of a web application firewall (WAF)?
a) To encrypt web traffic
b) To monitor and block malicious web traffic
c) To scan web applications for vulnerabilities
d) To block IP addresses
Answer: b) To monitor and block malicious web traffic

63. What is Cross-Site Scripting (XSS)?
a) A method to encrypt web data
b) A vulnerability that allows injecting malicious scripts into web pages
c) A protocol for secure file transfer
d) A tool to monitor network traffic
Answer: b) A vulnerability that allows injecting malicious scripts into web pages

64. Which method prevents SQL injection attacks?
a) Using firewalls
b) Using parameterized queries
c) Encrypting data at rest
d) Disabling JavaScript
Answer: b) Using parameterized queries

65. What does Content Security Policy (CSP) aim to mitigate?

a) DDoS attacks
b) XSS attacks
c) SQL injection
d) Malware distribution
Answer: b) XSS attacks

66. Which of the following methods is effective against brute force attacks on web applications?

a) Implementing CAPTCHA
b) Disabling cookies
c) Using HTTP instead of HTTPS
d) Blocking all users from accessing the site
Answer: a) Implementing CAPTCHA

67. What is the purpose of Secure Sockets Layer (SSL) or Transport Layer Security (TLS)?

a) To block unauthorized IPs
b) To encrypt data transmitted between client and server
c) To prevent phishing attacks
d) To detect malware on the server
Answer: b) To encrypt data transmitted between client and server

68. What is a common method to prevent session hijacking?

a) Using strong passwords
b) Implementing session timeout and secure cookies
c) Disabling JavaScript
d) Using HTTP instead of HTTPS
Answer: b) Implementing session timeout and secure cookies

69. Which HTTP header helps protect against clickjacking attacks?

a) X-Content-Type-Options
b) X-Frame-Options
c) Strict-Transport-Security
d) Content-Security-Policy
Answer: b) X-Frame-Options

70. What is Two-Factor Authentication (2FA) primarily used for?

a) Encrypting sensitive data
b) Adding an additional layer of security for user authentication
c) Preventing SQL injection attacks
d) Blocking phishing emails
Answer: b) Adding an additional layer of security for user authentication

71. What does SSL stand for in cybersecurity?

a) Secure Software Layer
b) Secure Sockets Layer
c) Simple Secure Layer
d) System Security Layer
Answer: b) Secure Sockets Layer

72. Which protocol is the successor to SSL?

a) HTTPS
b) TLS (Transport Layer Security)
c) SSH (Secure Shell)
d) IPSec
Answer: b) TLS (Transport Layer Security)

73. Which version of SSL is considered insecure and no longer used?

a) SSL 1.0
b) SSL 2.0
c) SSL 3.0
d) All of the above
Answer: d) All of the above

74. What is the primary purpose of SSL/TLS protocols?

a) To prevent DDoS attacks
b) To encrypt data transmitted between client and server
c) To monitor network traffic
d) To block malware
Answer: b) To encrypt data transmitted between client and server

75. Which type of encryption does SSL/TLS use?

a) Symmetric encryption only
b) Asymmetric encryption only
c) Both symmetric and asymmetric encryption
d) Hashing only
Answer: c) Both symmetric and asymmetric encryption

76. Which port is commonly used by HTTPS that utilizes SSL/TLS?

a) 80
b) 443
c) 22
d) 8080
Answer: b) 443

77. What is a digital certificate in the context of SSL/TLS?

a) A document used to encrypt user passwords
b) A file that verifies the identity of a website or server
c) A tool to block malicious traffic

d) A protocol for encrypting files
Answer: b) A file that verifies the identity of a website or server

78. Which component of SSL/TLS ensures data integrity?

a) Encryption algorithms
b) Digital signatures
c) Hash functions
d) Secure keys
Answer: c) Hash functions

79. What is the purpose of the SSL/TLS handshake?

a) To initiate a secure file transfer
b) To establish a secure connection between client and server
c) To authenticate the user's identity
d) To encrypt stored data
Answer: b) To establish a secure connection between client and server

80. Which of the following is an attack targeting SSL/TLS protocols?

a) Man-in-the-Middle (MITM) attack
b) SQL injection
c) Cross-Site Scripting (XSS)
d) Buffer overflow
Answer: a) Man-in-the-Middle (MITM) attack

81. What does TLS stand for?

a) Transport Layer Security
b) Transmission Layer System
c) Trusted Layer Security
d) Transport Log System
Answer: a) Transport Layer Security

82. TLS is a successor to which protocol?

a) SSH
b) IPSec
c) SSL (Secure Sockets Layer)
d) HTTPS
Answer: c) SSL (Secure Sockets Layer)

83. What is the primary purpose of the TLS protocol?

a) To secure stored data
b) To encrypt data during transmission over the network
c) To monitor unauthorized access
d) To authenticate users locally
Answer: b) To encrypt data during transmission over the network

84. Which layer of the OSI model does TLS operate on?

a) Application layer
b) Transport layer
c) Network layer
d) Data link layer
Answer: b) Transport layer

85. Which encryption techniques does TLS use?

a) Symmetric encryption only
b) Asymmetric encryption only
c) Both symmetric and asymmetric encryption
d) Hashing only
Answer: c) Both symmetric and asymmetric encryption

86. Which port is typically associated with TLS-secured HTTPS?

a) 22
b) 80
c) 443
d) 8080
Answer: c) 443

87. What is a key feature of the TLS handshake process?

a) Verifies the server's identity using a digital certificate
b) Encrypts data stored in a database
c) Establishes a direct connection without encryption
d) Detects malware on the server
Answer: a) Verifies the server's identity using a digital certificate

88. Which algorithm is commonly used in TLS for key exchange?

a) RSA
b) AES
c) MD5

d) DES
Answer: a) RSA

89. What does Perfect Forward Secrecy (PFS) in TLS ensure?

a) That encrypted data remains secure even if private keys are compromised
b) That only the client is authenticated
c) That data is stored securely on the server
d) That symmetric encryption keys never expire
Answer: a) That encrypted data remains secure even if private keys are compromised

90. What is the role of the Certificate Authority (CA) in TLS?

a) To issue and validate digital certificates
b) To encrypt data at rest
c) To monitor network traffic
d) To secure databases
Answer: a) To issue and validate digital certificates

91. What does HTTPS stand for?

a) Hypertext Transfer Protocol Secure
b) Hypertext Transfer Protocol Simple
c) Hypertext Transmission Protocol Secure
d) Hypertext Transfer Packet Secure
Answer: a) Hypertext Transfer Protocol Secure

92. Which protocol does HTTPS use to secure data transmission?

a) SSL/TLS
b) FTP
c) SSH
d) IPSec
Answer: a) SSL/TLS

93. What is the default port for HTTPS?

a) 80
b) 443
c) 22
d) 8080
Answer: b) 443

94. What is the primary difference between HTTP and HTTPS?

a) HTTPS is faster than HTTP.
b) HTTPS encrypts data, while HTTP does not.
c) HTTPS uses a different IP address than HTTP.
d) HTTP can only be used for websites, while HTTPS is for email.
Answer: b) HTTPS encrypts data, while HTTP does not.

95. Which cryptographic methods are used in HTTPS?

a) Only symmetric encryption
b) Only asymmetric encryption
c) Both symmetric and asymmetric encryption
d) Hashing only
Answer: c) Both symmetric and asymmetric encryption

96. Which of the following ensures the authenticity of an HTTPS website?

a) Secure Socket Layer (SSL) certificate
b) Firewall rules
c) Encryption keys
d) Network Address Translation (NAT)
Answer: a) Secure Socket Layer (SSL) certificate

97. What role does a Certificate Authority (CA) play in HTTPS?

a) It issues and verifies digital certificates for websites.
b) It encrypts data at rest.
c) It monitors HTTPS traffic.
d) It blocks unauthorized access to websites.
Answer: a) It issues and verifies digital certificates for websites.

98. Which type of attack does HTTPS help prevent?

a) Man-in-the-Middle (MITM) attacks
b) Denial of Service (DoS) attacks
c) Phishing attacks
d) Ransomware attacks
Answer: a) Man-in-the-Middle (MITM) attacks

99. What happens if an HTTPS certificate is invalid or expired?

a) The browser shows a warning about the site's security.
b) The website becomes inaccessible.
c) The browser encrypts data with default keys.
d) The browser ignores it and continues to load the site.
Answer: a) The browser shows a warning about the site's security.

100. Which HTTPS component ensures data integrity during transmission?

a) Hashing algorithms
b) Symmetric encryption
c) Asymmetric encryption
d) IP address verification
Answer: a) Hashing algorithms

101. What is Nikto primarily used for?

a) Penetration testing on wireless networks
b) Scanning web servers for vulnerabilities
c) Encrypting web traffic
d) Managing firewalls
Answer: b) Scanning web servers for vulnerabilities

102. Which of the following is true about Nikto?

a) It is a commercial tool.
b) It focuses on scanning for malware.
c) It is an open-source web server scanner.
d) It scans for SQL injection vulnerabilities only.
Answer: c) It is an open-source web server scanner.

103. What does w3af stand for?

a) Web Application Audit Framework
b) Web Application Attack and Audit Framework
c) Website Automated Attack Framework
d) Web Attack Application Framework
Answer: b) Web Application Attack and Audit Framework

104. Which programming language is w3af written in?

a) Python
b) Java
c) C++
d) Ruby
Answer: a) Python

105. What type of vulnerabilities can Nikto detect?

a) Outdated software and misconfigurations
b) Password breaches
c) Wireless network attacks
d) Buffer overflows in operating systems
Answer: a) Outdated software and misconfigurations

106. Which of the following features is provided by w3af?

a) Exploitation of identified vulnerabilities
b) Traffic encryption
c) Secure coding recommendations
d) Blocking malicious IPs in real-time
Answer: a) Exploitation of identified vulnerabilities

107. How does Nikto handle scanning for web vulnerabilities?

a) It performs brute force attacks on web servers.
b) It checks web servers against a database of known vulnerabilities.
c) It encrypts web traffic to secure connections.
d) It blocks unauthorized users.
Answer: b) It checks web servers against a database of known vulnerabilities.

108. Which of the following is a limitation of Nikto?

a) It cannot detect outdated server software.
b) It generates many false positives.
c) It performs scans that are easily detectable by intrusion detection systems (IDS).
d) It cannot scan web servers with HTTPS.
Answer: c) It performs scans that are easily detectable by intrusion detection systems (IDS).

109. What is the primary difference between Nikto and w3af?

a) Nikto focuses on web server scanning, while w3af focuses on web application vulnerabilities.
b) Nikto is commercial, and w3af is open source.
c) w3af is used only for network security, while Nikto is used for web security.
d) Both are identical in functionality.
Answer: a) Nikto focuses on web server scanning, while w3af focuses on web application vulnerabilities.

110. Which of the following is an advantage of using w3af?

a) It has a graphical user interface (GUI) for easier usability.
b) It provides real-time blocking of malicious traffic.
c) It focuses only on database security.
d) It is designed exclusively for mobile application testing.
Answer: a) It has a graphical user interface (GUI) for easier usability.

111. What is the primary function of the curl utility?

a) Encrypt files
b) Interact with URLs and transfer data
c) Manage firewalls
d) Monitor system logs
Answer: b) Interact with URLs and transfer data

112. Which protocol is NOT supported by curl?

a) HTTP
b) FTP
c) SMTP
d) SNMP
Answer: d) SNMP

113. What is the primary purpose of OpenSSL in cybersecurity?

a) To create secure tunnels for encrypted communication
b) To generate and manage SSL/TLS certificates
c) To perform vulnerability scanning
d) To encrypt files only
Answer: b) To generate and manage SSL/TLS certificates

114. Which of the following is a function of stunnel?

a) Encrypting plain TCP connections
b) Monitoring network traffic
c) Scanning web applications for vulnerabilities
d) Generating encryption keys
Answer: a) Encrypting plain TCP connections

115. What is the command to download a file using curl?

a) curl -d
b) curl -u
c) curl -o
d) curl -x
Answer: c) curl -o

116. Which command in OpenSSL is used to generate a private key?

a) openssl genrsa
b) openssl req
c) openssl enc
d) openssl pkcs12
Answer: a) openssl genrsa

117. What does the stunnel utility primarily rely on for encryption?

a) SSH keys
b) SSL/TLS protocols
c) Symmetric encryption only
d) IPsec tunneling
Answer: b) SSL/TLS protocols

118. Which curl option allows you to include custom HTTP headers in your request?

a) -d
b) -H
c) -k
d) -s
Answer: b) -H

119. How does OpenSSL verify the authenticity of an SSL certificate?

a) By hashing the certificate's public key
b) By checking it against a Certificate Authority (CA)
c) By decrypting it with a private key
d) By comparing the certificate to a pre-shared key
Answer: b) By checking it against a Certificate Authority (CA)

120. What is the primary use case of stunnel in cybersecurity?

a) Setting up secure VPNs
b) Encrypting plaintext protocols like HTTP or SMTP
c) Scanning for outdated software
d) Monitoring unauthorized access
Answer: b) Encrypting plaintext protocols like HTTP or SMTP

121. What is the primary purpose of Zed Attack Proxy (ZAP)?

a) To perform denial-of-service attacks
b) To test and identify security vulnerabilities in web applications
c) To scan for malware in web servers
d) To monitor network traffic
Answer: b) To test and identify security vulnerabilities in web applications

122. Which of the following is a feature of ZAP?

a) Automated scanners for common vulnerabilities
b) Custom rule creation for specific attacks
c) Passive and active scanning for security issues
d) All of the above
Answer: d) All of the above

123. What does SQLmap specialize in?

a) Cross-site scripting (XSS) vulnerabilities
b) SQL injection vulnerabilities
c) Buffer overflow vulnerabilities
d) Authentication bypass vulnerabilities
Answer: b) SQL injection vulnerabilities

124. How does SQLmap assist cybersecurity professionals?

a) By exploiting SQL injection vulnerabilities and extracting data from a database
b) By monitoring SQL traffic in real-time
c) By providing recommendations for secure SQL queries
d) By generating encrypted SQL keys
Answer: a) By exploiting SQL injection vulnerabilities and extracting data from a database

125. What is the primary use of DVWA (Damn Vulnerable Web Application)?

a) To provide a platform for testing web application security tools
b) To scan for vulnerabilities in enterprise-level applications
c) To learn and practice ethical hacking techniques
d) To monitor web application traffic
Answer: c) To learn and practice ethical hacking techniques

126. Which of the following vulnerabilities can be tested using DVWA?

a) SQL injection
b) Cross-Site Scripting (XSS)
c) Command injection
d) All of the above
Answer: d) All of the above

127. WebGoat is designed to help users understand and test which type of vulnerabilities?

a) Network-based vulnerabilities
b) Operating system vulnerabilities
c) Web application vulnerabilities
d) File system vulnerabilities
Answer: c) Web application vulnerabilities

128. What is the main feature of WebGoat?

a) It is an application for testing network traffic.
b) It is a vulnerable web application for learning security concepts.
c) It scans web applications for vulnerabilities automatically.
d) It provides secure coding guidelines for developers.
Answer: b) It is a vulnerable web application for learning security concepts.

129. Which of the following is a key feature of SQLmap?

a) Automated exploitation of SQL injection vulnerabilities
b) Password cracking for encrypted SQL databases
c) Buffer overflow detection in SQL queries
d) Generating secure SQL queries
Answer: a) Automated exploitation of SQL injection vulnerabilities

130. Which security testing tool is best suited for a beginner to practice web application security vulnerabilities?

a) ZAP
b) SQLmap
c) WebGoat
d) Burp Suite
Answer: c) WebGoat

131. What is the primary function of John the Ripper?

a) To scan for malware in password files
b) To crack password hashes using various algorithms
c) To monitor network traffic for stolen credentials
d) To encrypt passwords for secure storage
Answer: b) To crack password hashes using various algorithms

132. Which algorithm is supported by John the Ripper for password cracking?

a) MD5
b) SHA-1

c) DES
d) All of the above
Answer: d) All of the above

133. What is L0htcrack primarily used for?

a) Cracking encrypted emails
b) Cracking Windows password hashes
c) Brute-forcing login pages
d) Encrypting passwords
Answer: b) Cracking Windows password hashes

134. Which of the following is a feature of L0htcrack?

a) It supports GPU acceleration for faster password cracking.
b) It only works on Linux operating systems.
c) It provides encrypted communication for password recovery.
d) It automatically generates secure passwords.
Answer: a) It supports GPU acceleration for faster password cracking.

135. What is the main use of pwdump?

a) To dump password hashes from Windows systems
b) To generate complex passwords
c) To encrypt passwords for secure storage
d) To monitor password changes in real-time
Answer: a) To dump password hashes from Windows systems

136. What does HTC-Hydra primarily perform?

a) File integrity checking
b) Distributed denial-of-service (DDoS) attacks
c) Brute-force attacks on network services and web applications
d) Scanning for security vulnerabilities in networks
Answer: c) Brute-force attacks on network services and web applications

137. Which protocols does HTC-Hydra support for brute-force attacks?

a) HTTP
b) FTP
c) SSH
d) All of the above
Answer: d) All of the above

138. Which feature does John the Ripper offer for password cracking?

a) Dictionary-based attack
b) Rainbow table generation
c) Social engineering methods
d) Phishing attacks
Answer: a) Dictionary-based attack

139. What makes L0htcrack a preferred choice for password cracking in Windows

a) Its ability to recover passwords from encrypted files
b) Its specific optimization for Windows password hash formats
c) Its use of machine learning algorithms to predict passwords
d) Its ability to scan entire networks for vulnerable accounts
Answer: b) Its specific optimization for Windows password hash formats

140. What is the primary advantage of using HTC-Hydra for brute-force attacks?

a) It automatically generates password hashes
b) It can perform parallel attacks across multiple protocols
c) It encrypts the password database during attacks
d) It only works with HTTP-based protocols
Answer: b) It can perform parallel attacks across multiple protocols

---