1. Most network threats originate from which of the following?
   a. inside the company
   b. script kiddies
   c. back doors
   d. industrial spies

2. 2. What are some of the reasons for network attacks?
   a. industrial espionage
   b. revenge
   c. financial gain
   d. all of the above

3. The capability to prevent one participant in an electronic transaction from denying that it performed an action is called .
   a. plausible deniability
   b. integrity
   c. nonrepudiation
   d. undeniability

4. Servers with outside access to the public should be located on . (Choose all that apply.)
   a. their own subnet
   b. a DMZ
   c. an internal LAN
   d. a network perimeter

5. Packet filters can block or allow transmission of packets based on which of the following criteria? (Choose all that apply.)
   a. port number
   b. open ports
   c. time of access attempts
   d. IP address

6. An attacker who causes harm to systems in support of some principle is categorized as which of the following?
   a. cracker
   b. hacker
   c. industrial spy
   d. cyberterrorist

7. An IP address combined with a TCP/IP port number is called which of the following?
   a. network address
   b. socket
   c. script
   d. port ID

8. Firewall enforcement of policies is handled primarily through setting up packet-filtering rules, a set of which is contained in the .
   a. routing table
   b. rule base

c. access control list
d. packet filter

9. Name four goals of network security.

nonrepudiation, confidentiality, integrity, availability

10. An uninterruptible power supply is a component of security.
a. virtual
b. auditing
c. physical
d. password

11. The Stuxnet worm was designed to .
a. shut down Internet DNS servers
b. disrupt computer-controlled industrial operations
c. steal financial information
d. be used by script kiddies

12. A packet-filtering device evaluates data in the payload and compares it with a predefined set of rules. True or False?

13. Which of the following malware is designed to replicate itself? (Choose all that apply.)
a. worm
b. virus
c. Trojan horse
d. SYN flood

14. In a restrictive firewall policy, what is the starting point for developing a rule base?
a. allow all traffic
b. block all traffic except specified types
c. allow all traffic except specified types
d. block all traffic

15. In an IDPS, specific indications of a possible attack are called.
a. signatures
b. signals
c. true positives
d. alerts

16. What advantages does IPv6 have over IPv4? (Choose all that apply.)
a. IPv6 uses DHCP for its configuration settings.
b. IPv6 uses a 128-bit address space.
c. IPv4 cannot support IPsec.
d. IPv6 incorporates IPsec.

17. A Class C address has a first octet decimal range of to .
a. 172, 191
b. 191, 224
c. 192, 239
d. 192, 223

18. Which of the following is a method of hiding internal host IP addresses? (Choose all that apply.)
    a. Network Address Translation (NAT)
    b. configuring the computer to insert a fake source IP address into outgoing messages
    c. proxy servers
    d. setting up software firewalls on all internal hosts.

19. The Class A address 127.0.0.1 is used for which of the following?
    a. broadcasting to all hosts on a subnet
    b. testing the local TCP/IP software implementation
    c. experimentation
    d. testing the local NIC

20. Why is UDP considered unreliable?
    a. The header does not contain a checksum.
    b. The data is transmitted in clear text.
    c. It is connectionless.
    d. Routers typically drop a large number of UDP packets.

21. In CIDR notation, the IP address and subnet mask 191.9.205.22 255.255.192.0 are written as .
    a. 191.9.205.22/19
    b. 191.9.205.22/18
    c. 191.9.205.22/17
    d. 191.9.205.22/16

22. How do routers handle packets that are too large to pass through because of frame size limitations?
    a. Routers drop packets that are too large.
    b. Routers bounce packets back to the sender to be resized.
    c. Routers adjust their MTUs to accommodate the oversized packet.
    d. Routers break packets into smaller pieces called fragments.

23. Which of the following is an IPv6 protocol? (Choose all that apply.)
    a. Multicast Listening Detection
    b. IGMPv6
    c. Multicast Listener Discovery
    d. Neighbor Discovery

24. A DNS server translates to .
    a. encrypted IP addresses, clear text
    b. IP addresses, MAC addresses
    c. FQDNs, IP addresses
    d. static addresses, DHCP

25. Why is fragmentation considered a security risk?
    a. Fragments numbered 0 contain port information.
    b. Fragments numbered 1 or higher are passed through filters.

c. Fragmented packets cannot be assembled.
d. Fragmentation is frequently used.

26. Which of the following is used for one-to-many communication, in which a single host can send packets to a group of recipients?
a. multicast
b. unicast
c. anycast
d. netcast

27. The number of TCP segments that can be sent before an acknowledgement must be received is determined by the .
a. sequence number
b. sliding window size
c. transmission rate
d. port number in use for the session

28. When one host wants to initiate a TCP session with another host, it sends a packet with the flag set.
a. SYN
b. ACK
c. RST
d. FIN

29. An ICMPv6 header is indicated by a Next Header value of .
a. 60
b. 54
c. 58
d. 22

30. Compressing the IPv6 address 1080:0:0:0:8:800:200C:417A results in which of the following?
a. 1080::8:8:::2::C:417A
b. 1080::8:800:200C:417A
c. 1080::8:8::::20:C:417A
d. :1080::8:800:200C:417A

31. Security devices on a network process digital information, such as text files and Web pages, in the same way. However, which of the following pieces of information might they handle differently?
a. protocols
b. TCP/IP headers
c. attack signatures
d. port numbers

32. Which of the following is an example of a multiple-packet attack?
a. a fragment
b. an ICMP flood
c. a false Internet time stamp
d. a packet with SYN/FIN/ACK flags set

33. What is the purpose of the 4-byte acknowledgement number in a TCP header?
    a. It acknowledges receipt of the previous packet in the sequence.
    b. It acknowledges that a connection has been made.
    c. It verifies that the source and destination IP addresses are correct.
    d. It acknowledges the ID number the packet is using.

34. Which of the following is the correct order in which TCP flags appear during the initiation of a normal connection?
    a. SYN, ACK, FIN, RST
    b. SYN, PSH, ACK, RST
    c. SYN, SYN/ACK, ACK
    d. SYN, PSH, ACK, FIN

35. Which protocol uses one port number to establish a connection and a different port number to transfer data?
    a. TCP/IP
    b. FTP
    c. HTTP
    d. ICMP

36. Which of the following is an example of a reconnaissance traffic signature?
    a. Trojan program
    b. ping sweep
    c. denial of service
    d. Ping of Death

37. Which program keeps track of services and ports made available through Remote Procedure Calls?
    a. Network Information System
    b. Network File System
    c. Network File Sharing
    d. portmapper

38. To avoid attacks that use advanced evasion techniques, such as path obfuscation, CGI scripts, and packet injection, you must do which of the following? (Choose all that apply.)
    a. Watch your log files closely.
    b. Install additional IDPS sensors.
    c. Keep your anti-adware software updated.
    d. Keep your IDPS signature files updated.

39. Which of the following features distinguishes IPv6 from IPv4?
    a. IPv6 fragmentation occurs on IPv6-compliant routers.
    b. IPv4 is unfragmentable.
    c. IPv6 fragmentation occurs only at the source node.
    d. The IPv4 maximum fragment size is larger than its IPv6 counterpart

40. Consider the following statements:
    A: Dynamic routing protocols decrease network security.
    B: Static routing protocols conserve network bandwidth.
    a. Statement A is true, and statement B is false.

b. Statement A is false, and statement B is true.
c. Statement A is true, and statement B is true.
d. Statement A is false, and statement B is false.

41. A packet has a destination Data Link layer address of FF-FF-FF-FF-FF-FF.
a. Any router that receives this packet forwards it to the default route interface.
b. Any nonrouting device drops this packet.
c. Network hosts send this packet to their default gateway.
d. Network hosts process this packet to see if it is of interest.

42. Which of the following addresses are valid IPv6 addresses? (Choose all that apply.)
a. fe80::a02a:64b0:27a9:c73b
b. fe80:cd5c::f40f:9eea:7580
c. fe80::bef2:6cbe::678:1879
d. fe80:c693:bef2:6cbe:678:1879

43. Which of the following features are typical of dynamic routing protocols? (Choose all that apply.)
a. increased administrative effort
b. faster convergence
c. decreased processor load
d. increased network traffic.

44. Consider the following statements:
A: Supernetting reduces the number of routes in routing tables.
B: Variable length subnet masks allow routers to determine whether an address is public or private.
a. Statement A is true, and statement B is false.
b. Statement A is false, and statement B is true.
c. Statement A is true, and statement B is true.
d. Statement A is false, and statement B is false

45. All Cisco access control lists require .
a. at least one permit statement
b. at least one deny statement
c. either a source or destination IP address in each access control entry
d. a deny all statement as the last access control entry

46. Which of the following parameters can you find in a standard access control list? (Choose all that apply.)
a. source IP address
b. destination IP address
c. source port number
d. destination MAC address

47. Which of the following IP addresses would be filtered by an access control entry that contained the IP address and inverse mask specification of 12.96.115.77 0.15.255.255? (Choose all that apply.)
a. 21.48.200.9

b. 12.104.146.190
c. 12.111.115.77
d. 12.113.84.3

48. Which of the following packet elements can be filtered by a named ACL? (Choose all that apply.)
a. TCP flags
b. noninitial fragments
c. destination ports
d. source IP addresses

49. Cisco encryption type 7 is the strongest encryption method available on the router. True or False?

50. To configure a router using a telephone connection, you would connect to the port.
a. CON
b. AUX
c. TTY
d. VTY

51. To enable SSH on a Cisco router, you should .
a. run the command ssh enable rsa
b. run the command crypto key zeroize rsa
c. create RSA keys
d. install SSHv3

52. Which of the following are routing protocols? (Choose all that apply.)
a. EIGRP
b. ARP
c. MAC
d. RIP

53. Protocols that guide a router's decisions on packet forwarding based on the current condition of the network are .
a. link-state protocols
b. static protocols
c. the most secure routing protocols
d. routed protocols

54. Consider the following statements:
A: An ACL can be applied only to one router interface.
B: An ACL can apply only to one routed protocol.
C: An ACL can filter packets traveling in only one direction.
a. Statements A and C are correct.
b. Statements A and C are incorrect.
c. Statement A is correct, and statement B is false.
d. Statement A is false, and statement B is correct

55. Define cryptographic primitives.

Modular mathematical functions that perform one task reliably. They form the basic building blocks of modern cryptography.

56. Which of the following is used as a cryptographic primitive? (Choose all that apply.)
    a. pseudorandom number generators
    b. hashing functions
    c. Feistel networks
    d. side channels

57. Why are cryptographically secure pseudorandom number generators so important to cryptography?

    Cryptographic primitives used to generate sequence of numbers that approximate random values.

58. What is the block size in the AES implementation of Rijndael?
    a. 128 or 256 bits
    b. 128, 192, or 256 bits
    c. variable
    d. 128 bits

59. Which of the following issues public and private key pairs?
    a. certificate publisher
    b. certification authority
    c. certificate revocation list
    d. certificate store

60. Which of the following is used to check whether a certificate is still valid?
    a. certificate revocation list
    b. certification authority
    c. certificate publisher
    d. registration authority

61. Which of the following is a symmetric algorithm that is not considered safe for encryption use?
    a. AES
    b. Diffie-Hellman
    c. DES
    d. RSA

62. In digital signatures, which of the following values is compared to verify a message's integrity?
    a. public key
    b. message digest
    c. private key
    d. certificate

63. When using symmetric and asymmetric algorithms to encrypt the same amount of data, which of the following statements is correct?
    a. The symmetric algorithm encrypts data faster than the asymmetric algorithm.
    b. The asymmetric algorithm encrypts data faster than the symmetric algorithm.
    c. The symmetric and asymmetric algorithms work at the same speed to encrypt data.
    d. The faster an asymmetric algorithm works, the stronger its encryption.

64. Which of the following combines a hashed message authentication code with a shared secret key, processes each half of the input data with different hashing algorithms, and recombines them with an XOR function?
    a. SSL
    b. SSH
    c. TLS
    d. WPA

65. Which of the following is a reason that IPsec has become the standard protocol for tunneled communication? (Choose all that apply.)
    a. IPsec is fast and supported universally.
    b. IPsec supports IPv4 and IPv6.
    c. IPsec is implemented at Layer 2.
    d. IPsec can encrypt the entire packet.

66. Which of the following components enables IPsec to use Diffie-Hellman to create keys?
    a. Internet Key Exchange
    b. Internet Security Association Key Management Protocol
    c. Oakley
    d. IPsec driver

67. Authentication Header verifies the integrity of TCP/IP packets by signing them with a digital signature. True or False?

68. In tunnel mode, Encapsulating Security Payload encrypts which of the following?
    a. packet header
    b. data
    c. both the header and the data
    d. neither the header nor the data

69. Which of the following attacks might have the potential to exploit AES?
    a. PRNG
    b. visual cryptanalysis
    c. chosen ciphertext
    d. XSL

70. In which of the following situations would a wireless network be an effective alternative?
    a. a business that occupies temporary space
    b. a network with employees who travel
    c. an older building with no wiring
    d. all of the above

71. Wireless communication emits which types of EM radiation? (Choose all that apply.)
    a. gamma rays
    b. infrared radiation
    c. ultraviolet light
    d. radio frequency waves

72. The maximum departure of a wave from its undisturbed state is called which of the following?
    a. frequency
    b. wavelength
    c. amplitude
    d. hertz

73. All types of electromagnetic radiation are collectively called which of the following?
    a. EM spectrum
    b. EM field
    c. light spectrum
    d. visible light spectrum.

74. Frequency is defined as which of the following?
    a. the distance between repeating units of a wave
    b. the number of times an event occurs in a specified period
    c. a method of transporting energy without physical movement of material
    d. radiation spreading out as it moves

75. The distance between midpoints of a wave is called which of the following?
    a. frequency
    b. wavelength
    c. amplitude
    d. hertz

76. What type of infrared transmission relies on reflected light?

    diffused IR transmission

77. Infrared wireless is extremely fast, can travel long distances, and is not susceptible to interference. True or False?

78. Which of the following is a common type of signal loss? (Choose all that apply.)
    a. deletion
    b. diffraction
    c. deflection
    d. scattering

79. Refraction occurs when the RF signal is dispersed by small objects, such as raindrops or foliage. True or False?

80. Which of the following is used to provide a relative measurement of RF power?
    a. milliwatts
    b. decibels
    c. watts
    d. 10s and 3s rules of RF math

81. Why is digital modulation superior to analog modulation? (Choose all that apply.)
    a. It makes more efficient use of bandwidth.
    b. It has fewer interference problems.

c. Error correction is more compatible with other digital systems.
d. Less power is required to transmit.

82. Which of the following is considered an advantage of spread spectrum over narrowband wireless transmission? (Choose all that apply.)
a. increased security
b. decreased susceptibility to interference
c. requires less power to reach the same amplitude
d. does not require a chipping code

83. Radio waves striking an antenna create infrared radiation. True or False?

84. IEEE 802.11ac is expected to support a bandwidth of .
a. 54 Mbps
b. 102 Mbps
c. 512 Mbps
d. 1000 Mbps.

85. What function does an SSID serve on a wireless network?
a. identifies an access point's location
b. monitors a station's connection properties
c. identifies the network name
d. encrypts network traffic

86. Which of the following OSI layers is the most important in a wireless network? (Choose all that apply.)
a. Physical
b. Network
c. Session
d. Data Link

87. Which of the following frames carries TCP/IP packets in a wireless network?
a. management
b. data
c. control
d. MAC

88. What is the purpose of a beacon frame?
a. An AP sends it to determine whether to allow a device to enter the network.
b. It advertises services or information about the wireless network.
c. It aids in establishing and maintaining communication.
d. It assists in delivering frames that contain data.

89. Which of the following is the process of listening on each available channel for an AP's beacon?
a. surfing
b. monitoring
c. scanning
d. probing

90. The IEEE 802.11 standard provides which of the following authentication methods? (Choose all that apply.)
    a. asymmetric
    b. shared key
    c. open system
    d. closed system.

91. A station can be authenticated without being associated. True or False?

92. Which is the most secure wireless implementation?
    a. WPA2-TKIP Personal
    b. WPA-TKIP Enterprise
    c. WPA2-AES Personal
    d. WPA-EAP Enterprise

93. Which authentication method does WPA2 Enterprise Security use?
    a. preshared key
    b. 802.1x
    c. EAP
    d. AES

94. Even though 802.11 wireless devices can hold up to four keys simultaneously, they have to use the same one to communicate with each other. True or False?

95. A site survey helps accomplish which of the following? (Choose all that apply.)
    a. determining placement of stations
    b. evaluating what type of antennas to use
    c. identifying where APs should be placed
    d. determining where data should be stored

96. Having an abundance of APs in a wireless network improves security. True or False?

97. Which of the following default settings should you change before connecting a device? (Choose all that apply.)
    a. SSID
    b. channel
    c. port address
    d. MAC address

98. WPA2 uses which of the following for encryption?
    a. LEAP
    b. EAP
    c. AES
    d. EAS

99. Which control frame gives a station permission to transmit?
    a. RTS
    b. CTS
    c. AES
    d. ACK

100. How can data gained from intrusion detection improve network security? (Choose all that apply.)
a. It can help prevent future attacks.
b. It can route traffic more efficiently.
c. It can shield IP addresses on the network.
d. It can help determine how to respond to security incidents.

101. Which of the following IDPS results is the cause of greatest concern?
a. true positives
b. true negatives
c. false positives
d. false negatives

102. An IDPS management server performs which of the following functions?
a. monitoring inbound and outbound traffic
b. modifying state information
c. storing and analyzing sensor data
d. providing an IDPS interface

103. Which of the following is an IDPS detection capability you can customize? (Choose all that apply.)
a. blacklists
b. signatures
c. state tables
d. thresholds

104. Misuse-based detection is based on which feature of network traffic?
a. user profiles
b. normal traffic
c. signatures
d. user accounts

105. An anomaly-based IDPS can be circumvented in which of the following ways?
a. new attacks
b. changes in user habits
c. changes in published signatures
d. minor changes in attack methods that do not match known signatures

106. A signature-detection IDPS can be circumvented in which of the following ways?
a. changes in attack methods
b. a stolen user account
c. making traffic appear normal
d. attacks made during the IDPS training period

107. Which intrusion detection method can begin protecting a network immediately after installation?

signature detection

108. Which intrusion detection method is almost impossible for intruders to test before attempting an attack?
anomaly detection

109. Which IDPS activity could detect a DoS attack?
a. protocol state tracking
b. signature detection
c. traffic monitoring
d. IP packet reassembly

110. What type of IDPS should you use if your main concern is preventing known attacks?
a. signature-based IDPS
b. network-based IDPS
c. host-based IDPS
d. anomaly-based IDPS

111. An HIDPS can detect an intrusion attempt that targets the entire network, such as a port scan on a range of computers. True or False? False. NIDPS

112. What preventive responses can an IDPS make to a possible attack? (Choose all that apply.)
a. prevents malicious code from running
b. drops the suspicious packet
c. allows, reset, alarm
d. reset all network connections

113. Which of the following is almost inevitable and should be expected after installing an IDPS? (Choose all that apply.)
a. false negatives
b. huge log files
c. signatures that become outdated
d. false positives

114. How can an inline sensor be positioned to reduce the load on a perimeter security device, such as a firewall or router?
a. Place the sensor inside the security perimeter.
b. Replace the firewall or router with the sensor.
c. Position the sensor outside the security perimeter.
d. Add another firewall or router.

115. A firewall can do which of the following? (Choose all that apply.)
a. Screen traffic for viruses.
b. Determine what user is sending transmissions.
c. Filter traffic based on rules.
d. Provide a layer of protection for the network.

116. A firewall is an effective stand-alone security solution. True or False?

117. Stateless packet filters allow or block packets based on which of the following?
a. status of the connection
b. information in protocol headers

c. state table
d. packets that have been handled previously

118. Which of the following is an advantage of using a software firewall rather than a hardware firewall?
a. throughput
b. reliability
c. cost
d. availability.

119. Which of the following is an advantage of using a hardware firewall rather than a software firewall? (Choose all that apply.)
a. scalability
b. cost
c. ease of maintenance
d. increased throughput

120. Almost every type of firewall depends on what configurable feature for its effectiveness?
a. network connection
b. state table
c. rule base
d. management console

121. Where should you place the most important rules in a rule base?
a. in the connection log file
b. at the bottom of the rule base
c. in the state table
d. at the top of the rule base

122. Which of the following is a guideline for developing a firewall rule base? (Choose all that apply.)
a. The rule base should restrict all Internet access.
b. The rule base should restrict access to ports and subnets on the internal network from the Internet.
c. The rule base should be as detailed as possible.
d. The rule base should not interfere with application traffic.

123. A firewall policy does which of the following? (Choose all that apply.)
a. describes how employees can use the firewall
b. identifies and mitigates risks
c. explains how the firewall is set up, managed, and updated
d. specifies how the firewall should handle application traffic

124. A rule base should end with a(n) rule.
a. reject
b. allow
c. cleanup
d. block

125. When you request a Web page, which port does the Web server use to send you the page?
a. 80
b. 443
c. one higher than 1023
d. one lower than 1023

126. Stateless packet filters are more secure than stateful packet filters because they do not contain a state table that can be exploited by an attacker. True or False?

127. A socket is a combination of a(n) and a(n) .
a. NetBIOS name, port number
b. port number, MAC address
c. MAC address, IP address
d. IP address, port number

128. The Windows RPC service works like the UNIX service.
a. mountd
b. Portmapper
c. QOTD
d. INFS

129. Which port is used for name/address resolution?
a. 20
b. 53
c. 80
d. 110

……chap 10 – 14……

130. A DMZ is .
a. a trusted network
b. a semitrusted network
c. an untrusted network
d. not actually a network

131. A screening router would be an appropriate choice for meeting the security needs of a _____?
a. small office network
b. home network
c. DMZ
d. none of the above

132. Which of the following computers is likely to be found in a DMZ? (Choose all that apply.)
a. e-mail server
b. domain controller
c. Web server
d. customer information database

133. Which of the following issues should you consider in firewall design? (Choose all that apply.)
a. fault tolerance
b. log size
c. authorization
d. load balancing

134. A proxy server . (Choose all that apply.)
a. is designed to improve Web access
b. is the same as a reverse firewall
c. uses fewer system resources than a software firewall
d. can filter Application layer content

135. What is the main problem with using a screening router?
a. The router can be configured incorrectly.
b. The router might not provide an adequate screen.
c. The router cannot be used with a firewall.
d. The router alone cannot stop many types of attacks.

136. What enables servers in a server farm to work together to handle requests?
a. a router
b. a switch
c. a networking hub
d. load-balancing software

137. For which of the following reasons would you consider creating a protected subnet within an already protected internal network? (Choose all that apply.)
a. to protect customer information
b. to protect management servers
c. to protect the company's reputation
d. to protect Web servers.

138. A corporation with several branch offices has decided to maintain multiple firewalls, one to protect each branch office's network. What is the most efficient way to maintain these firewalls?
a. Use a centralized security workstation.
b. Send information about the security policy to each network administrator.
c. Set up remote desktop management software.
d. Broadcast configuration instructions periodically by e-mail.

139. Which of the following functions can a bastion host perform? (Choose all that apply.)
a. FTP server
b. e-mail server
c. security management server
d. domain controller

140. Which of the following can hide internal IP addresses from the Internet? (Choose all that apply.)
a. packet filters
b. NAT

c. proxy servers
d. state tables

141. Hardening a bastion host involves which of the following measures? (Choose all that apply.)
a. disabling unnecessary services
b. removing unnecessary accounts
c. installing current patches
d. all of the above

142. To isolate all external Web requests to a specific Web server on the DMZ, it would be best to use many-to-one NAT. True or False?

143. A bastion host is usually located on the internal network. True or False?

144. In a Cisco ASA 5505 firewall, security level 100 is the least secure level. True or False?

145. What client-side issues do you need to consider when planning a VPN deployment? (Choose all that apply.)
a. whether to require the client to use a firewall
b. the organization's current growth rate
c. how policies should be enforced on the client computer
d. the cost of equipment that employees need to buy.

146. In a mesh topology, all participants in the VPN have with one another.
a. tunnels
b. SAs
c. static routes
d. trusts

147. What is a main disadvantage of mesh VPNs?
a. They are not reliable.
b. There is a lack of confidentiality among peers.
c. They are difficult to enlarge or change.
d. The equipment must be the same at all sites.

148. Putting a VPN on the firewall has which of the following disadvantages? (Choose all that apply.)
a. There are more computers to manage.
b. Only one server controls security, so any configuration errors leave the network open to attack.
c. Internet access and VPN traffic compete for resources on the server.
d. VPN traffic is not encrypted.

149. A VPN server configured to receive PPTP traffic listens for incoming connections on port and needs to receive GRE traffic identified by protocol ID .
a. UDP 1443, 17
b. TCP 1723, 47
c. UDP 3349, 443
d. UDP 1723, 47.

150. Which protocols and ports must be allowed to pass when you are using L2TP and IPsec? (Choose all that apply.)
a. protocol ID 50
b. UDP 500
c. TCP 50
d. protocol ID 1701.

151. AH uses protocol ID .
a. 50
b. 171
c. 500
d. 51

152. The VPN connection through which data passes from one endpoint to another is called a(n) .
a. gateway
b. extranet
c. tunnel
d. transport

153. A group of authentication and encryption settings that two computers negotiate to set up a secure VPN connection is called which of the following?
a. protocol
b. Security Association (SA)
c. handshake
d. key exchange

154. What makes a VPN a cost-effective option?
a. Computers can use the same hardware and software.
b. It requires no administrative configuration to set up or maintain.
c. Many VPN applications are available as shareware or freeware.
d. VPNs use public Internet and ISP connections.

155. IPsec provides for what security activity to take place before data is encrypted or transmitted?
a. encapsulation
b. authentication
c. establishment of a Security Association (SA)
d. application of security policy settings.

156. Which of the following is an advantage of using a star VPN configuration?
a. It is easier to increase the VPN's size.
b. Fewer VPN hardware or software devices are required.
c. Only the VPN server at the center or "hub" needs to be updated.
d. All participants can communicate with all other participants.

157. Because of an increase in the use of Web-based business applications, there has been an increase in ---based VPNs.
a. SSL
b. IPsec

c. L2TP
d. PPTP

158. Which of the following is not a best practice for VPN client management?
a. Enable split tunneling.
b. Disable FTP.
c. Disable Telnet.
d. Enable VPN quarantine.

159. Which of the following IP addresses is most likely to be the source IP address of an encapsulated VPN packet?
a. 150.80.26.59
b. 172.30.78.45
c. 11.17.5.210
d. 210.240.255.48.

160. The Internet backbone is connected to regional ISPs via which of the following?
a. POP ISPs
b. network service points
c. network access points
d. carrier network points

161. How many root servers are in the DNS infrastructure?
a. 10
b. 11
c. 13
d. 14

162. Attackers can exploit routing information updates to do which of the following? (Choose all that apply.)
a. Launch DoS attacks.
b. Poison DNS caches.
c. Use IP spoofing to intercept packets.
d. Launch man-in-the-middle attacks.

163. Attackers often use DNS cache poisoning to do which of the following?
a. Query systems on a network one by one.
b. Steer unsuspecting users to a server of their choice instead of the Web site where users intended to go.
c. Flood the network with packets and cause it to crash.
d. Install a virus on the network.

164. Which of the following is caused by a flaw in how a running process allocates memory to a variable?
a. unsecured cryptographic storage
b. buffer overflow
c. broken authentication
d. SQL injection

165. Which of the following is a common type of SQL injection attack? (Choose all that apply.)

a. Web form attack
b. browser executable attack
c. system tray attack
d. query string attack

166. In a SQL injection attack, which character is an attacker most likely to use?
a. asterisk
b. single quotation mark
c. exclamation mark
d. double quotation mark.

167. Which of the following attack methods target Web users? (Choose all that apply.)
a. social engineering
b. phishing
c. SQL injection
d. pharming.

168. What is a requirement for a successful file attachment attack?
a. The user must open the file attachment.
b. The user must reply to the e-mail that contains the attachment.
c. The user must delete the file attachment immediately.
d. The attachment must be an image file.

169. Which of the following factors enables attackers to program ActiveX controls to run malicious code on a user's Web browser? (Choose all that apply.)
a. ActiveX controls run in a sandbox that allows interaction with the OS.
b. ActiveX controls do not require user action to be activated.
c. ActiveX controls run automatically when the browser loads the Web page that contains them.
d. ActiveX controls have almost full access to the Windows OS.

170. A Web server can be hardened just by configuring the Web application correctly. True or False?

171. For optimum efficiency, configure a domain controller to function also as an IIS Web server. True or False?

172. When securing an Apache Web server, which of the following tasks is not necessary?
a. installing the latest Apache patches
b. disabling processing of server-side includes (SSIs)
c. deleting unneeded or default Apache files and sample code
d. creating a privileged user ID for the Apache Web User account with root access.

173. In a DNS zone transfer, what is actually transferred?
a. fully qualified domain names and IP addresses
b. usernames and passwords
c. server MAC addresses
d. UDP and ICMP messages

174. To keep log files organized, store them on the server you are monitoring. True or False?

175. Survivable Network Analysis begins with what assumption?
a. that you have laid the groundwork for a risk analysis
b. that your network will be attacked
c. that the probability of threats is increasing constantly
d. that an effective security policy can reduce risks to zero.

176. To determine the value of hardware and software you need to protect, which of the following approaches is easiest to use?
a. getting the most recent prices online
b. keeping records of purchase costs
c. using your experience and expertise
d. interviewing support personnel

177. When should an organization conduct a new round of risk analysis?
a. every month
b. every three months
c. as frequently as possible
d. when equipment or staff change significantly.

178. A risk analysis report should call attention to .
a. all identified risks
b. the most urgent risks
c. the newest risks
d. the risks that are easiest to manage.

179. The ultimate goal of a security policy is which of the following?
a. reducing the risks to zero
b. doing it right the first time so the policy does not have to be rewritten constantly
c. convincing management that the IT budget should be increased
d. none of the above.

180. What are the hardware, software, and informational resources you need to protect?
a. threats
b. tangibles
c. assets
d. business holdings.

181. Ensuring that databases remain accessible if primary systems go offline is known as .
a. fault tolerance
b. failover
c. redundancy
d. resiliency.

182. Which of the following technologies helps protect sensitive data even after it has been stolen from a secured medium?
a. virus protection
b. authentication
c. encryption
d. Spybot.

183. Which of the following sections of a security policy affects the most people in an organization?
a. incident handling policy
b. privileged access policy
c. acceptable use policy
d. remote access policy.

184. What is an escalation procedure? (Choose all that apply.)
a. It describes how network security can be improved in stages.
b. It describes how a virus can multiply and affect more assets.
c. It describes different levels of response based on incident severity.
d. It identifies employees who should be involved in the response.

185. Which of the following, if worded correctly, can protect companies from wrongful termination lawsuits?
a. nondisclosure clauses
b. acceptable use policies
c. penalty clauses
d. punitive clauses

186. A password policy might specify which of the following attributes for password selection?
a. length requirements
b. complexity requirements
c. frequency for changing passwords
d. all of the above.

187. Which of the following provides employees with formal instructions about the organization's security strategy?
a. acceptable use policy
b. risk assessment
c. strategy meeting
d. security user awareness program

188. If organizations have employees who connect remotely, which of the following security concerns should be considered?
a. the possibility of mobile devices being stolen
b. virus infections spreading from home and mobile systems to corporate systems
c. the use of updated, effective antivirus and firewall software on mobile devices or home systems that connect to the network
d. all of the above

189. A password policy should be established in the and enforced by whenever possible.
a. risk assessment process, management
b. company Web site, network administrators
c. security policy, software
d. company employee handbook, security guards.

190. Which of the following is a type of security audit? (Choose all that apply.)
a. automated

b. independent
c. centralized
d. operational

191. Why is it important to protect the confidentiality of information you gather through auditing? (Choose all that apply.)
a. Employee privacy could be compromised.
b. The information might become corrupted when you store it.
c. Intruders could discover passwords.
d. Viruses could infect it.

192. When should you follow the procedure for carrying out change shown in Figure 14-4?
a. when many employees will be affected by the change
b. when the change is needed urgently
c. whenever a change needs to be made to security configurations
d. when the change will have a substantial impact.

193. What is an auditing program in which current connections are scanned and alerts are generated after suspicious logon attempts?
a. social engineering
b. port scan
c. event monitoring
d. Tinkerbell program.

194. Which of the following employees has primary responsibilities that include maintaining and strengthening network defenses?
a. security incident response team leader
b. computer security manager
c. chief information officer
d. security auditor.

195. What is a realistic goal of ongoing security management? (Choose all that apply.)
a. blocking all suspicious packets
b. tracing all attacks
c. tracing as many intrusion attempts as possible
d. continually strengthening and modifying defenses.

196. Which of the following describes a goal of a security event management program? (Choose all that apply.)
a. consolidating events from multiple sources
b. responding to events as quickly as possible
c. conducting forensics to trace and prosecute offenders
d. managing IDPS signatures.

197. How can you gather information on a variety of security events and respond to it quickly?
a. Assemble a large response team.
b. Use distributed data collection.
c. Automate data collection and analysis.
d. Outsource security management.

198. Which of the following is an advantage of centralized data collection? (Choose all that apply.)
a. reduced traffic through network gateways
b. reduced administrative costs
c. reduced software and hardware costs
d. only one person needed to review data.

199. Why would you choose distributed data collection rather than centralized data collection?
a. to reduce traffic through gateways
b. to reduce the load on security managers
c. to reduce overall costs
d. to reduce hardware and software costs.

200. Before installing new signatures for an IDPS, what do you need to do?
a. Back up the IDPS.
b. Stop the IDPS.
c. Change passwords.
d. Double-check to verify whether new signatures are necessary.

201. What can happen if you change a security configuration too abruptly and without proper authorization? (Choose all that apply.)
a. Employees might ignore the change.
b. The change might surprise other security managers.
c. You might be flooded with protests from employees.
d. You could face disciplinary action.

202. The change management process might apply when which of the following occurs? (Choose all that apply.)
a. New password logon procedures are needed.
b. You need to block access to DMZ servers.
c. A new VPN gateway is installed.
d. You need to change a fragmentation rule in a packet filter.

203. Security auditing involves which of the following? (Choose all that apply.)
a. reviewing log files
b. reviewing hardware and software costs
c. testing defenses
d. rotating firewall logs

204. What is nonrepudiation?
a. the ability of a system to authenticate users
b. the ability to rely on information gained through a security audit
c. a legal defense used by employees whose privacy has allegedly been violated
d. the ability to validate transactions through electronic documentation