Introduction of information security systems cis4385

1. Which if the following IPv6 address type is assigned to multiple interfaces but packets will only be delivered to one? a. Multicast b. Anycast c. Unicast d. Broadcast Grade: 1 User Responses: b. Anycast Feedback: a. An anycast address is assigned to a group of interfaces on multiple nodes. Packets are delivered to the “ first” interface only. 2. Routers operate at which OSI layer? a. Physical b. Transport c. Network d. Session Grade: 1 User Responses: c. Network Feedback: a. Routers operate at the network layer making routing decisions based on IP addresses. 3. Which of the following is NOT a private IPv4 address?

Choose all that apply. a. 192. 168. 5. 60 b. 172. 25. 6. 4 c. 10. 0. 6. 5 d. 26. 68. 6. 1 Grade: 1 User Responses: d. 26. 68. 6. 1 Feedback: a. The private IP address ranges are as follows. IP Class Assigned Range Class A 10. 0. 0. 0-10. 255. 255. 255 Class B 172. 16. 0. 0-172. 31. 255. 255 Class C 192. 168. 0. 0-192. 168. 255. 255 4. What is a server that evaluates Internet requests from LAN devices against a set called? a. Proxy b. Firewall c. Load balancer d. NAT server Grade: 1 User Responses: a. Proxy Feedback: a. A server that evaluates Internet requests from LAN devices against a set of rules is called a proxy server.

NAT servers perform private to public address translation; load balancers manage traffic between cluster hosts; and a firewall filters traffic based on access control lists. 5. Which type of device maintains awareness of the status of connections, thereby preventing IP spoofing attacks? a. Stateless packet filtering firewall b. Stateful packet filtering firewall c. NAT filter d. Application-level gateway Grade: 1 User Responses: b. Stateful packet filtering firewall Feedback: a. A stateful packet filtering firewall is one that

monitors the state of each connection by examining the header of each packet.

A stateless packet filtering firewall does not do this. NAT filters perform only private-to-public address translation. An application-level gateway provides protection to a specific application such as FTP. 6. Which of the following firewall services works at the session layer of the OSI model? a. Application layer gateway b. Stateful filtering c. NAT d. Circuit-level gateway Grade: 0 User Responses: c. NAT Feedback: a. Circuit-level gateways work at the Session Layer of the OSI model and apply security mechanisms when a TCP or UDP connection is established; they act as a go between for the Transport and Application Layers in TCP/IP.

After the connection has been made, packets can flow between the hosts without further checking. Circuit-level gateways hide information about the private network, but they do not filter individual packets. 7. Which of the following are the two main functions of a proxy server? a. Caching of web pages b. NAT c. Domain authentication d. DHCP Grade: 1 User Responses: a. Caching of web pages, c. Domain authentication Feedback: a. A proxy server secures a network by keeping machines behind it anonymous; it does this through the use of NAT. It also improves web performance by caching web pages from servers on the Internet for a set amount of time. b. A proxy server secures a network by keeping machines behind it anonymous; it does this through the use of NAT. It also improves web performance by caching web pages from servers on the Internet for a set amount of time. 8. Which of the following devices can detect but not prevent attacks across the entire network? a. NIDS b. Host-based IDS c. NIPS d. Protocol Analyzer Grade: 1

User Responses: a. NIDS Feedback: a. Network Intrusion Detection Systems (NIDS) detect but do not prevent attacks across the entire network. Host-based IDS can protect only the host on which it is installed.

Network Intrusion Protection Systems (NIPS) can detect and prevent attacks across the entire network. A Protocol Analyzer can capture traffic but not act upon it. 9. When a NIPs blocks legitimate traffic, what is it known as? a. False negative b. True negative c. False positive d. True positive Grade: 1 User Responses: c. False positive Feedback: a. A blocking of traffic is a positive action, and when it is in response to legitimate traffic, it is considered a false action; thus it is a false positive. A false negative would be when an action is NOT taken on traffic that is not legitimate.

The other two options are normal actions; a true negative is the allowing of legitimate traffic, whereas a true positive is the blocking of illegitimate traffic. 10. Which of the following types of NIPS reacts to actions that deviate from a baseline? a. Signature-based b. Heuristic c. Anomaly-based d. Bit blocker Grade: 1 User Responses: c. Anomaly-based Feedback: a. Anomaly-based NIPS recognizes traffic that is unusual and reports it. Signature-based NIPs are configured with the signatures of attacks. Heuristics looks for patterns in the traffic, whereas bit blocker is a not a type of NIPs. 1. Which of the following systems attempt to stop the leakage of confidential data, often concentrating on communications? a. DHCP b. DNS c. DLP d. STP Grade: 1 User Responses: c. DLP Feedback: a. Data loss prevention (DLP) systems are designed to protect data by way of content inspection. They are meant to stop the leakage of confidential data, often concentrating on communications. As such, they are often also referred to as data leak

prevention (DLP) devices, information leak prevention (ILP) devices, and extrusion prevention systems.

Regardless, they are intended to be used to keep data from leaking past a computer system or network and into unwanted hands. 12. When a company buys fire insurance they are _____ risk. a. accepting b. avoiding c. transferring d. reducing Grade: 1 User Responses: c. transferring Feedback: a. It is possible to transfer some risk to a third-party. An example of risk transference (also known as risk sharing) would be an organization that purchases insurance for a group of servers in a datacenter.

The organization still takes on the risk of losing data in the case of server failure, theft, and disaster, but transfers the risk of losing the money those servers are worth in the case they are lost. 13. Which of the following processes block external files that use JavaScript or images from loading into the browser? a. URL filtering b. Content filtering c. Malware inspection d. Blacklists Grade: 1 User Responses: b. Content filtering Feedback: a. Content filtering is a process that blocks external files that use JavaScript or images from loading into the browser. URL filtering blocks pages based on the URL.

Malware inspection looks for malware based on a signature file, and blacklists are items to be denied by spam filters. 14. Which of the following actions should NOT be taken for the default account on a network device? a. Delete it. b. Change the password. c. Disable it. d. Leave it as is. Grade: 1 User Responses: d. Leave it as is. Feedback: a. The default account has a well-known username and password, so it should be either deleted or disabled, or at a minimum its password should be changed. 15. Firewall rules

are typically based in all but which of the following? a. IP addresses b. MAC addresses c. Port numbers . Content type Grade: 1 User Responses: d. Content type Feedback: a. Firewall rules are typically based on IP addresses, MAC addresses, or port numbers, but they cannot filter for content. 16. Which of the following is the target of a double tagging attack? a. VPNs b. VLANs c. Collision domains d. DMZs Grade: 1 User Responses: b. VLANs Feedback: a. A double tagging attack can enable the attacker to view traffic from multiple VLANs. 17. A network created to allow access to resources from the Internet, while maintaining separation from the internal network is called a _____? a. VPN b. VLAN c. Honeypot d. DMZ Grade: 1

User Responses: d. DMZ Feedback: a. When talking about computer security, a Demilitarized Zone (DMZ) is a special area of the network (sometimes referred to as a subnetwork) that houses servers which host information accessed by clients or other networks on the Internet, but which does not allow access to the internal network. 18. How can access to the remote management of a router be protected? a. Content filtering b. ACLs c. Firewalls d. IPS Grade: 0 User Responses: c. Firewalls Feedback: a. Remote access to a router is usually done via Telnet or SSH. The port used (vty line) can be secured using an access control list.

The other options can all be used to help protect routers but not access the remote management function. 19. You need to allow access from your network to all web sites. What port numbers should be opened in the firewall? Choose all that apply. a. 25 b. 443 c. 80 d. 119 e. 22 f. 23 Grade: 1 User Responses: c. 80 Feedback: a. HTTP and HTTPS are the two services you need to allow access to use ports 80 and 443 respectively. 20. Which of

the following mitigation techniques can prevent MAC flooding? a. Secure VLANs b. Prevent ICMP responses c. 802. 1x d. 802. 1q Grade: 1 User Responses: c. 802. 1x Feedback: a.

MAC flooding, which involves overwhelming the memory of the switch with MAC frames sourced from different MAC addresses, can be prevented by requiring authentication on each port through 802. 1x. Secure VLANs cannot prevent this because the frames don’t need to enter a VLAN to cause the problem. ICMP is at Layer 3, these frames are at Layer 2, and 802. 1q is a VLAN tagging protocol that does not prevent frames from entering the switch through access ports. 21. Which of the following attacks cannot be mitigated with a flood guard? a. Smurf attack b. Fraggle c. Teardrop attack d. Session theft Grade: 1 User Responses: d.

Session theft Feedback: a. The smurf, fraggle, and teardrop attacks all involve sending a flood of packets to a device, using different types of malformed packets. A session theft attack is when a session cookie is stolen and used to authenticate to a server. 22. Loop protection is designed to address problems that occur with which device? a. Switch b. Hub c. Router d. Firewall Grade: 0 User Responses: b. Hub Feedback: a. Loops occur when switches have redundant connections causing a loop. Loop guard (or loop protection) can prevent loops on the switch. 23. When creating an ACL which of the following statements is NOT true? a.

The order of the rules is important for proper functioning b. You must include a deny all statement at the end of the rule set for proper functioning c. The more specific rules should be placed at the beginning of the rule list d. Once

created, the ACL must be applied to an interface Grade: 1 User Responses: b. You must include a deny all statement at the end of the rule set for proper functioning Feedback: a. There is an implied deny all statement at the end of each ACL and it is not required to include one. 24. Which of the following is an example of insecure network bridging in a LAN? a. Laptop connected to a hotspot and an ad hoc network . Laptop connected to a wireless network and the wired LAN at the same time c. Router connected to two subnets d. PC connected with two NIC to the same LAN Grade: 1 User Responses: b. Laptop connected to a wireless network and the wired LAN at the same time Feedback: a. When a laptop connects to a wireless network and the wired LAN at the same time, it can create a bridge between the two allowing access to the LAN. The other scenarios do not create a security problem for the LAN. 25. When the administrator creates a rule on the firewall to prevent FTP traffic, this is a type of _____rule. . implicit deny b. implicit allow c. explicit deny d. explicit allow Grade: 1 User Responses: c. explicit deny Feedback: a. When traffic is specified to be prevented, it is an explicit deny. When it is denied simply because it was not specifically allowed, that is an implicit deny. 26. Network Access Control (NAC) is an example of_____. a. role-based management b. rules-based management c. port-based access d. application layer filtering Grade: 1 User Responses: b. rules-based management Feedback: a. Network Access Control (NAC) uses rules by which connections to a network are governed.

Computers attempting to connect to a network are denied access unless they comply with rules including levels of antivirus protection, system updates, and so on—effectively weeding out those who would perpetuate

malicious attacks. 27. What type of device is required for communication between VLANs? a. Hub b. Switch c. Router d. Firewall Grade: 1 User Responses: c. Router Feedback: a. Hosts in different VLANs are also in different subnets and routing must be performed for them to communicate. 28. Which of the following would be least likely to be placed in the DMZ? a. Web server b. DNS server c. Domain controller d. FTP server

Grade: 1 User Responses: c. Domain controller Feedback: a. All the options except a domain controller are often placed in the DMZ so they are accessible to the outside world. A DC however is sensitive and should NOT be placed in the DMZ. 29. Subnetting a network creates segmentation at which layer of the OSI model? a. Layer 1 b. Layer 2 c. Layer 3 d. Layer 4 Grade: 1 User Responses: c. Layer 3 Feedback: a. Subnetting a network creates segmentation using IP addresses, which is Layer 3. 30. What service is required to represent multiple private IP addresses with a single public IP address? a. NAT b. DHCP c. DNS d. DLP Grade: 0

User Responses: a. NAT Feedback: a. Network Address Translation (NAT) is required to represent multiple private IP addresses with a single public IP address. The specific form of NAT required to represent multiple private IP addresses with a single public IP address is called Port Address Translation (PAT). 31. Which of the following is NOT a remote access protocol? a. MS-CHAP b. CHAP c. LDAP d. PAP Grade: 1 User Responses: c. LDAP Feedback: a. Lightweight Directory Access Protocol is used for accessing directory services such as Active Directory. It is not used in remote access. All other options are remote access protocols. 2. Which of the following devices are susceptible to war dialing? a. Modems b. Firewalls c. Content filters d. Load balancers

Grade: 0 User Responses: a. Modems Feedback: a. Any devices that accept phone calls such as modems or PBX systems with remote phone access are susceptible to war dialing. 33. When computers are not allowed to connect to the network without proper security patches and virus updates, the network is using a form of _____. a. PAT b. DAC c. NAC d. DMZ Grade: 0 User Responses: d. DMZ Feedback: a. Network Access Control (NAC) uses rules by which connections to a network are governed.

Computers attempting to connect to a network are denied access unless they comply with rules including levels of antivirus protection, system updates, and so on—effectively weeding out those who would perpetuate malicious attacks. 34. Which of the following items do not need to be changed on a new router to ensure secure router management? a. IP address b. Administrator name c. Administrator password d. IOS version Grade: 1 User Responses: d. IOS version Feedback: a. All the options except the IOS version can be set to defaults from the factory and should be changed because they are well known. 5. Which of the following is NOT an example of cloud computing? a. SaaS b. IaaS c. PaaS d. BaaS Grade: 1 User Responses: d. BaaS Feedback: a. Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are all forms of cloud computing. 36. On which concept is cloud computing based? a. load balancing b. virtualization c. RAID d. DLP Grade: 1 User Responses: b. virtualization Feedback: a. All forms of cloud computing use virtualization. 37. A three legged perimeter is a form of _____. a. VPN b. DMZ c. NAT d. ACL Grade: 1 User Responses: b. DMZ Feedback: a.

A three-legged perimeter is a firewall or server with three NICs: one pointed to the LAN, one to the Internet, and one to the DMZ. 38. Which of the following is NOT a benefit provided by subnetting? a. It increases security by compartmentalizing the network. b. It is a more efficient use of IP address space. c. It reduces broadcast traffic and collisions. d. It eases administration of the network. Grade: 1 User Responses: d. It eases administration of the network. Feedback: a. Subnetting provides a number of benefits but easing administration is not one of them. 39. Which of the following is the result of implementing VLANs? . Larger broadcast domains b. Smaller collision domains c. Smaller broadcast domains d. Larger collision domains Grade: 1 User Responses: c. Smaller broadcast domains Feedback: a. VLANs break up the network into subnets and as such result in smaller broadcast domains. 40. Which of the following services helps conserve public IP addresses? a. NAT b. DHCP c. DNS d. SLIP Grade: 0 User Responses: c. DNS Feedback: a. By allowing the use of private IP addresses inside each network and by representing those groups of private IP addresses with a single public IP address, public IP addresses are conserved by NAT. 41.

Which of the following remote access protocols are used with VPNs? Choose all that apply. a. PPTP b. PPP c. L2TP d. SLIP Grade: 1 User Responses: c. L2TP, d. SLIP Feedback: a. Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling protocol (L2TP) are used with VPNs. PPP and SLIP are used for dial-up. /b. Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling protocol (L2TP) are used with VPNs. PPP and SLIP are used for dial-up. 42. Which of the following security protocols operates at the network layer of the

OSI model? a. IPSec b. SSH c. SSL d. TLS Grade: 1 User Responses: a. IPSec Feedback: a.

One of the key features of IPSec is its operation at the network layer enabling it to protect any type of communication operating at the upper layers of the OSI model. 43. Which of the following are components of SNMP? Choose all that apply. a. NMS b. IPSec c. Agent d. CARP Grade: 1 User Responses: b. IPSec, c. Agent Feedback: a. The three components of SNMP are a network management system (NMS), agent software, and the managed device, where the agent software operates. /b. The three components of SNMP are a network management system (NMS), agent software, and the managed device, where the agent software operates. 44.

SSL is designed as a secure replacement for which of the following? a. PPP b. Telnet c. TLS d. SSH Grade: 0 User Responses: d. SSH Feedback: a. SSL is designed as a secure replacement for Telnet, which transmits in clear text. 45. Which of the following protocols supersedes SSL? a. SSH b. TLS c. S/MIME d. EAP Grade: 0 User Responses: a. SSH Feedback: a. TLS 1. 2, the latest version, is used when establishing an HTTPS connection and supersedes SSLv3. 46. The operation of which of the following protocols makes the SYN flood attack possible? a. IPX/SPX b. AppleTalk c. TCP/IP d. RIP Grade: 1 User Responses: c. TCP/IP Feedback: a.

TCP/IP uses a three-way handshake for its connection, and the SYN flood attack attempts to take advantage of the operation of this connection operation. 47. Which of the following provides secure web access? a. SFTP b. HTTP c. HTTPS d. SSH Grade: 1 User Responses: c. HTTPS Feedback: a.

HTTPS uses port 443 and is the standard for secure web access. 48. SCP is a secure copy protocol that uses the port of which other protocol for transfers? a. HTTPS b. SSH c. SSL d. FTPS Grade: 0 User Responses: d. FTPS Feedback: a. Secure copy (SCP) is another example of a protocol that uses another protocol (and its corresponding port).

It uses SSH and ultimately uses port 22 to transfer data. 49. Which of the following protocols is abused when a ping flood occurs? a. SNMP b. IGMP c. ICMP d. EIGRP Grade: 0 User Responses: a. SNMP Feedback: a. Ping floods use ICMP echo request packets aimed at the target. 50. Which of the following security mechanisms are built into IPv6? a. IPSec b. SSL c. HTTPS d. EAP Grade: 1 User Responses: a. IPSec Feedback: a. IPv6 has IPSec support built in. 51. What method is used by SSL to obtain and validate certificates? a. SPI b. PKI c. TLS d. EAP Grade: 1 User Responses: b. PKI Feedback: a.

SSL and TLS use a public Key Infrastructure (PKI) to obtain and validate certificates. 52. What port number does FTPS use to protect the transmission? a. 21 b. 88 c. 443 d. 445 Grade: 0 User Responses: a. 21 Feedback: a. FTPS uses SSL or TLS over port 443 to make a secure connection. 53. Which of the following protocols uses port 22, normally used by SSH, to make a secure connection? a. FTPS b. SCP c. SFTP d. SSL Grade: 0 User Responses: b. SCP Feedback: a. Secure FTP (SFTP) uses port 22, the port for SSH, which is why it is also sometimes called SSH FTP. 54. Which protocol uses ports 161 and 162? a. SMTP b. IMAP4 . SNMP d. IGMP Grade: 0 User Responses: a. SMTP Feedback: a. SNMP is used to collect information about and make changes to devices on the network. It uses ports 161 and 162. 55. Which protocol uses the same port as HTTPS? a. SCP b. FTPS c. SFTP

d. IMAP4 Grade: 0 User Responses: c. SFTP Feedback: a. FTP secure (FTPS) uses port 443, which is also used by HTTPS. 56. Which protocol uses port 69? a. SCP b. FTPS c. TFTP d. IMAP4 Grade: 1 User Responses: c. TFTP Feedback: a. TFTP uses port 69. 57. What port number is used by Telnet? a. 80 b. 443 c. 21 d. 23 Grade: 1 User Responses: d. 23 Feedback: a. Port 23 is used by Telnet. 8. Which port does HTTP use? a. 80 b. 443 c. 21 d. 23 Grade: 0 User Responses: b. 443 Feedback: a. HTTP uses port 80. 59. Which port does SCP use to transfer data? a. 80 b. 22 c. 21 d. 23 Grade: 0 User Responses: c. 21 Feedback: a. SCP uses SSH and thus port 22 to transfer data. 60. Which protocol uses port 443? a. HTTPS b. FTPS c. TFTP d. IMAP4 Grade: 1 User Responses: a. HTTPS Feedback: a. HTTPS uses port 443. 61. Which two protocols use port 22? a. HTTPS b. FTPS c. SSH d. SCP Grade: 2 User Responses: c. SSH, d. SCP Feedback: a. SCP uses SSH and thus port 22 to transfer data, so both protocols use this port. b. SCP uses SSH and thus port 22 to transfer data, so both protocols use this port. 62. Which ports does the NetBIOS protocol uses? Choose all that apply. a. 138 b. 139 c. 137 d. 140 Grade: 3 User Responses: a. 138, b. 139, c. 137 Feedback: a. The NetBIOS protocol uses ports 137 through 139. /b. The NetBIOS protocol uses ports 137 through 139. /c. The NetBIOS protocol uses ports 137 through 139. 63. What protocol uses port 53? a. HTTPS b. FTPS c. SSH d. DNS Grade: 0 User Responses: b. FTPS Feedback: a. DNS uses port 53. 64. Which port number does RDP use? a. 3389 b. 1723 c. 1701 d. 140 Grade: 1

User Responses: a. 3389 Feedback: a. Port 3389 is used for Remote Desktop (RDP). 65. What protocol uses port 25? a. HTTPS b. SMTP c. SSH d. DNS Grade: 1 User Responses: b. SMTP Feedback: a. SMTP uses port 25. 66.

Which of the following statements is true regarding WPA and WPA2? (Choose all that apply.) a. WPA uses 256-bit encryption. b. WPA2 uses 128-bit encryption. c. WPA uses TKIP. d. WPA2 uses AES. Grade: 2 User Responses: c. WPA uses TKIP. , d. WPA2 uses AES. Feedback: a. WPA uses TKIP 128-bit encryption, whereas WPA2 uses 256-bit AES. /b. WPA uses TKIP 128-bit encryption, whereas WPA2 uses 256-bit AES. 67.

Which statement is NOT true with regard to WPA2? a. Uses AES encryption b. Meets requirements of 802. 11i c. Uses TKIP encryption d. Uses 256 bit encryption Grade: 1 User Responses: c. Uses TKIP encryption Feedback: a. WPA uses TKIP but WPA2 uses AES. 68. Which of the following is the security provided in the original 802. 11 standard? a. WPA b. WPA2 c. WEP d. CCMP Grade: 1 User Responses: c. WEP Feedback: a. Wired Equivalent Privacy (WEP) is the security provided in the original 802. 11 standard. 69. What is the authentication system that calls for a supplicant, authenticator, and authentication server called? . EAP b. WPA c. WPA2 d. WEP Grade: 1 User Responses: a. EAP Feedback: a. Extensible Authentication Protocol (EAP) is an authentication system that calls for a supplicant, authenticator, and authentication server. 70. Which of the following implementations of EAP requires certificates on the client and the server? a. EAP-FAST b. EAP-TTLS c. PEAP d. EAP-TLS Grade: 1 User Responses: d. EAP-TLS Feedback: a. EAP-TLS requires certificates on the client and the server. 71. Which of the following versions of EAP is Cisco proprietary? a. LEAP b. EAP-TTLS c. PEAP d. EAP-TLS Grade: 1 User Responses: a. LEAP

Feedback: a. Lightweight EAP is a version that works only on Cisco devices unless the device is from a partner that participates in the Cisco Compatible

Extensions program. 72. Why are MAC filters not effective in preventing access to the WLAN? a. The MAC addresses of allowed devices are contained in the beacon frames sent by the AP. b. The MAC addresses of allowed devices are contained in any frames sent by the allowed device. c. The administrative effort to maintain the MAC list is prohibitive. d. If the user changes his MAC address, the filter will disallow entry. Grade: 1 User Responses: b.

The MAC addresses of allowed devices are contained in any frames sent by the allowed device. Feedback: a. The MAC addresses of allowed devices are contained in any frames sent by the allowed device and can be seen by those using wireless protocol analyzers. The MAC address can then be spoofed for entry. 73. Which of the following frame types contain the SSID? (Choose all that apply.) a. Beacon frames b. Data frames c. Association frames d. Authentication frames Grade: 3 User Responses: b. Data frames, c. Association frames, d. Authentication frames Feedback: a. The SSID is contained in all frames.

If the SSID is hidden, it is removed only from the beacon frames. /b. The SSID is contained in all frames. If the SSID is hidden, it is removed only from the beacon frames. /c. The SSID is contained in all frames. If the SSID is hidden, it is removed only from the beacon frames. 74. TKIP was designed to correct the shortcomings of which of the following? a. EAP b. WPA c. WEP d. WPA2 Grade: 1 User Responses: c. WEP Feedback: a. TKIP was designed to correct the shortcomings of WEP. It was a temporary solution for use until the 802. 1x standard was completed. 75. Which of the following encryption protocols is used with WPA2? . TKIP b. CCMP c. WEP d. DES Grade: 1 User Responses:

b. CCMP Feedback: a. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is the encryption protocol used with WPA2. It addresses the vulnerabilities of TKIP and meets requirements of IEEE 802. 11i. 76. Which antenna types would be best for shaping the signal away from the front of the building for security purposes while still providing coverage in the other part of the building? (Choose all that apply.) a. Yagi b. Omni c. Parabolic dish d. Semidirectional Grade: 2 User Responses: a. Yagi, d. Semidirectional Feedback: a.

You can use a yagi antenna, which is a type of semidirectional antenna, to shape the coverage area as called for in the scenario. /b. You can use a yagi antenna, which is a type of semidirectional antenna, to shape the coverage area as called for in the scenario. 77. How can you keep the existing radiation pattern of the antenna while reducing the coverage area? a. Increase the power of the transmitter. b. Decrease the power of the transmitter. c. Change the polarity of the antenna. d. Remove one of the attenuators from the line. Grade: 1 User Responses: b. Decrease the power of the transmitter.

Feedback: a. Reducing the power level maintains the radiation pattern while making the area of radiation smaller. 78. What organization created WPA? a. FCC b. Wi-Fi Alliance c. IEEE d. ISO Grade: 1 User Responses: b. Wi-Fi Alliance Feedback: a. The Wi-Fi Alliance created WPA to address the weaknesses of WEP. 79. To which standard is WPA2 designed to adhere? a. 802. 16 b. 802. 11f c. 802. 11i d. 802. 11e Grade: 1 User Responses: c. 802. 11i Feedback: a. WPA2 is designed to adhere to the 802. 11i security standard. 80. Which of

the following is the weakest form of security? a. TKIP b. WPA c. WEP d. EAP Grade: 1

User Responses: c. WEP Feedback: a. WEP is the weakest form of security. It has been cracked and is not suitable for Enterprise WLANs. 81. A _____ attack intercepts all data between a client and a server. a. DDoS b. Man-in-the-middle c. Replay d. Smurf Grade: 1 User Responses: b. Man-in-the-middle Feedback: a. Man-in-the-middle is a type of active interception. If successful, all communications now go through the MITM attacking computer. 82. When a group of compromised systems attack a single target it is a called a _____ attack. a. DDoS b. Man-in-the middle c. Replay d. Smurf Grade: 1

User Responses: a. DDoS Feedback: a. A distributed denial-of-service attack occurs when a group of compromised systems launches a DDoS attack on a single target. 83. When valid data transmissions are maliciously or fraudulently repeated, it is called a _____ attack. a. DDoS b. man-in-the middle c. replay d. smurf Grade: 1 User Responses: c. replay Feedback: a. When valid data transmissions are maliciously or fraudulently repeated, it is a called a replay attack. 84. What attack sends large amounts of ICMP echoes, broadcasting the ICMP echo requests to every computer on its network or subnetwork? a.

DDoS b. Man-in-the middle c. Replay d. Smurf Grade: 1 User Responses: d. Smurf Feedback: a. A smurf attack sends large amounts of ICMP echoes, broadcasting the ICMP echo requests to every computer on its network or subnetwork. The ICMP request is sent to a broadcast address. When all hosts

receive the ICMP broadcast request, these host send ICMP replies to the source address, which has been set to the address of the target. 85. Changing your MAC address to that of another host is called _____. a. spear phishing b. spoofing c. pharming d. vishing Grade: 1 User Responses: b. spoofing Feedback: a.

Spoofing is when an attacker tails the IP or MAC address of another computer. 86. Which of the following is more an aggravation than an attack? a. Spear phishing b. Spoofing c. Spam d. Vishing Grade: 1 User Responses: c. Spam Feedback: a. Spam or unwanted email is more an aggravation than an attack. 87. Which of the following uses instant messaging as its vehicle? a. Spim b. Spoofing c. Phishing d. Vishing Grade: 1 User Responses: a. Spim Feedback: a. Spam Over Instant Messaging (SPIM) uses IM to deliver the spam. 88. When VoIP phone calls are used in the pursuit of social engineering, it is called_____. a. spim b. poofing c. phishing d. vishing Grade: 1 User Responses: d. vishing Feedback: a. Vishing is phishing performed with VoIP calls, which are harder to trace than regular calls. 89. What type of attack is an advanced scan that tries to get around firewalls and look for open ports? a. DDoS b. Man-in-the-middle c. Xmas attack d. Smurf Grade: 1 User Responses: c. Xmas attack Feedback: a. Usually using Nmap, the Xmas attack is an advanced scan that tries to get around firewalls and look for open ports. 90. _____ is when an attacker redirects one website’s traffic to another bogus and possibly malicious website. a.

DDoS b. Pharming c. Xmas attack d. Smurf Grade: 1 User Responses: b. Pharming Feedback: a. Host files and vulnerable DNS software can also be victims of pharming attacks. Pharming is when an attacker redirects one

website’s traffic to another bogus and possibly malicious website. Pharming can be prevented by carefully monitoring DNS configurations and host files. 91. _____ is when a person that is not normally authorized to a server manages to get administrative permissions to resources. a. Whaling b. Pharming c. Spear phishing d. Privilege escalation Grade: 1 User Responses: d. Privilege escalation Feedback: a.

Privilege escalation is when a person that is not normally authorized to a server manages to get administrative permissions to resources. 92. Which problem is the most difficult to contend with? a. Malicious insider threat b. Fraggle attack c. Distributed denial-of-service d. Whaling Grade: 1 User Responses: a. Malicious insider threat Feedback: a. Because the attacker already is inside the network with company knowledge, a malicious insider threat is the most difficult to contend with. 93. What type of attack can DNS poisoning lead to? a. Whaling b. Pharming c. Spear phishing d. Privilege escalation Grade: 0

User Responses: c. Spear phishing Feedback: a. Pharming attacks lead users from a legitimate website to a malicious twin. The easiest way to do this is to poison the DNS cache so that the DNS server sends them to the malicious site. 94. Strong input validation can help prevent _____. a. bluesnarfing b. SQL injection c. session highjacking d. header manipulation Grade: 0 User Responses: c. session highjacking Feedback: a. SQL injection attacks user input in web forms that is not correctly filtered. This can be prevented with input validations. 95. LDAP injection is an attack on _____servers. . SQL b. directory c. web d. email Grade: 1 User

Responses: b. directory Feedback: a. Lightweight Directory Access Protocol is

a protocol used to maintain a directory of information such as user accounts or other types of objects. 96. XML injection can be prevented with _____. a. IDS b. IPS c. input validation d. complex passwords Grade: 0 User Responses: d. complex passwords Feedback: a. The best way to protect against this (and all code injection techniques for that matter) is to incorporate strong input validation. 97. The .. / attack is also known as _____. a. irectory traversal b. SQL injection c. session highjacking d. header manipulation Grade: 1 User Responses: a. directory traversal Feedback: a. Directory traversal, or the .. / (dot dot slash) attack is a method to access unauthorized parent (or worse, root) directories. 98. _____ is when commands and command syntax are entered into an application or OS. a. Directory traversal b. Command injection c. Command highjacking d. Code manipulation Grade: 1 User Responses: b. Command injection Feedback: a. Command injection is when commands and command syntax are entered into an application or OS. 99.

Buffer overflows operate against the _____ of the computer. a. NIC b. disk c. CPU d. memory Grade: 1 User Responses: d. memory Feedback: a. A buffer overflow is when a process stores data outside of the memory that the developer intended. 100. What is the difference between an XSS and XSRF attack? a. The XSS attack exploits the trust a user’s browser has in a website, whereas the XSFR attack exploits the trust that a website has in a user’s browser. b. The XSFR attack exploits the trust a user’s browser has in a website, whereas the XSS attack exploits the trust that a website has in a user’s browser. . The XSS attack creates a buffer overflow on the website, whereas the XSFR attack creates a buffer overflow on the client. d. The XSS

attack creates a buffer overflow on the client, whereas the XSFR attack creates a buffer overflow on the website. Grade: 1 User Responses: a. The XSS attack exploits the trust a user’s browser has in a website, whereas the XSFR attack exploits the trust that a website has in a user’s browser. Feedback: a. The XSS attack exploits the trust a user’s browser has in a website. The converse of this: the XSRF attack exploits the trust that a website has in a user’s browser.

In this attack (also known as a one-click attack), the user’s browser is compromised and transmits unauthorized commands to the website. 101. _____ are placed by programmers, knowingly or inadvertently, to bypass normal authentication and other security mechanisms in place. a. Landing spots b. Backdoors c. Hotspots d. Code heels Grade: 1 User Responses: b. Backdoors Feedback: a. Backdoors are placed by programmers, knowingly or inadvertently, to bypass normal authentication and other security mechanisms in place. 102. An XSS attack is also called a(n) _____ attack. a. Zero day b. Command injection . Xmas d. Cross site scripting Grade: 1 User Responses: d. Cross site scripting Feedback: a. XSS attacks, also called cross site scripting attacks, exploit the trust a user’s browser has in a website through code injection, often in webforms. 103. _____can be used by spyware and can track people without their permission. a. MAC addresses b. Cookies c. IP addresses d. Attachments Grade: 1 User Responses: b. Cookies Feedback: a. Cookies are text files placed on the client computer that store information about it, which could include your computer’s browsing habits and possibly user credentials. 104.

Which of the following attachments is the riskiest to open? a.. exe b.. pdf c.. doc d.. txt Grade: 1 User Responses: a.. exe Feedback: a. A . exe or executable file is one that contains a program that will do something, perhaps malicious to the computer. 105. Stolen cookies can be used to launch a(n) _____. a. XSS attack b. SQL injection c. session highjack d. header manipulation Grade: 1 User Responses: c. session highjack Feedback: a. Session cookies authenticate you to a server and can be used to highjack your session. 106. Header manipulation alters information in _____ headers. a. LDAP b. file c. HTTP . SQL Grade: 1 User Responses: c. HTTP Feedback: a. Header manipulation alters information in HTTP headers and falsifies access. 107. An ActiveX control is an example of a(n) _____. a. cookie b. add-on c. cipher d. virus Grade: 1 User Responses: b. add-on Feedback: a. You can enable and disable add-on programs such as ActiveX controls in the Programs tab by clicking the Manage add-ons button in Internet Explorer. 108. When an attack targets an operating system vulnerability that is still unknown to the world in general, it is called a _____. a. P2P attack b. zero day attack c. whaling attack d. DDoS attack Grade: 1

User Responses: b. zero day attack Feedback: a. A zero day attack targets an operating system vulnerability that is still unknown to the world in general. 109. _____is a concept that refers to the monitoring of data in use, data in motion, and data at rest. a. DLP b. DHCP c. DEP d. DMS Grade: 1 User Responses: a. DLP Feedback: a. Data Loss Prevention (DLP) is a concept that refers to the monitoring of data in use, data in motion, and data at rest. It does this through content inspection and is designed to prevent

unauthorized use of data as well as prevent the leakage of data outside the computer (or network) that it resides. 10. Which form of DLP is typically installed in data centers or server rooms? a. Endpoint DLP b. Network DLP c. Storage DLP d. Comprehensive DLP Grade: 1 User Responses: c. Storage DLP Feedback: a. Storage DLP systems are typically installed in data centers or server rooms as software that inspect data at rest. 111. Which of the following is an example of drive encryption? a. AppLocker b. BitLocker c. Windows defender d. Trusted Platform Module Grade: 1 User Responses: b. BitLocker Feedback: a. To encrypt an entire hard disk, you need some kind of full disk encryption software.

Several are currently available on the market; one developed by Microsoft is called BitLocker. 112. The beauty of hardware-based encryption devices such as HSM (and TPM) is that it is _____ than software encryption. a. more difficult to crack b. easier to use than software encryption c. faster than software encryption d. can be used to calculate data other than encryption keys Grade: 1 User Responses: c. faster than software encryption Feedback: a. Hardware security modules (HSMs) are physical devices that act as secure cryptoprocessors.

This means that they are used for encryption during secure login/authentication processes, during digital signings of data, and for payment security systems. The beauty of hardware-based encryption devices such as HSM (and TPM) is that it is faster than software encryption. 113. A _____ is a chip residing on the motherboard that actually stores the encrypted keys. a. DLP b. DHCP c. DEP d. TPM Grade: 1 User Responses: d. TPM Feedback: a. A Trusted Platform Module (TPM) chip is one

residing on the motherboard that actually stores the encrypted keys. 114. Which of the following is NOT required to encrypt the entire disk in Windows?

Choose all that apply. a. TPM chip or USB key b. A hard drive with two volumes c. HSM Module d. Cryptoprocessor Grade: 2 User Responses: c. HSM Module, d. Cryptoprocessor Feedback: a. Hardware security modules (HSMs) are physical devices that act as secure cryptoprocessors; however, they are NOT a part of encrypting the entire disk in Windows. /b. Hardware security modules (HSMs) are physical devices that act as secure cryptoprocessors; however, they are NOT a part of encrypting the entire disk in Windows. 115. Probably the most important security concern with cloud computing is _____. . less secure connections b. loss of physical control of data c. weak authentication d. bug exploitation Grade: 1 User Responses: b. loss of physical control of data Feedback: a. Probably the most important security control concern is the physical control of data that is lost when an organization makes use of cloud computing. 116. Which of the following is NOT a solution to security issues surrounding cloud computing? a. Complex passwords b. Strong authentication methods c. Standardization of programming d. Multiple firewalls Grade: 1 User Responses: d. Multiple firewalls Feedback: a.

Solutions to these security issues include complex passwords, strong authentication methods, encryption, and standardization of programming. 117. Which form of DLP is typically installed on individual computers? a. Endpoint DLP b. Network DLP c. Storage DLP d. Comprehensive DLP Grade: 1 User Responses: a. Endpoint DLP Feedback: a. Endpoint DLP systems run on an individual computer and are usually software-based. They monitor data in

use such as email communications and can control what information flows between various users. 118. Where could you disable the use of removable media on a computer? a. Device manager . BIOS c. Control panel d. Programs and features Grade: 1 User Responses: b. BIOS Feedback: a. BIOS settings can be used to reduce the risk of infiltration including disabling removable media including the floppy drives and eSATA and USB ports. 119. What are two shortcomings of using BitLocker drive encryption? a. Weak encryption b. Expensive c. Performance suffers d. Shorter drive life Grade: 2 User Responses: c. Performance suffers, d. Shorter drive life Feedback: a. A drive encrypted with BitLocker usually suffers in performance compared to a nonencrypted drive and could have a shorter shelf life as well. /b.

A drive encrypted with BitLocker usually suffers in performance compared to a nonencrypted drive and could have a shorter shelf life as well. 120. Which form of DLP is typically installed on the perimeter of the network? a. Endpoint DLP b. Network DLP c. Storage DLP d. Comprehensive DLP Grade: 1 User Responses: b. Network DLP Feedback: a. Network DLP systems can be software or hardware solutions that are often installed on the perimeter of the network. They inspect data that is in motion. 121. Software as a service (SaaS) is a type of _____ computing. a. HSM b. cloud c. role-based d. TPM Grade: 1 User Responses: b. cloud

Feedback: a. Software as a Service (SaaS) is the most commonly used and recognized example of cloud computing. SaaS is when users access applications over the Internet that are provided by a third party. 122. Which form of DLP inspects ONLY data in motion? a. Endpoint DLP b. Network DLP c. Storage DLP d. Comprehensive DLP Grade: 1 User Responses: b. Network

DLP Feedback: a. Network DLP systems can be software or hardware solutions that are often installed on the perimeter of the network. They inspect data that is in motion. 123. Which of the following is NOT an example of cloud services? a. SaaS b. IaaS c. PaaS d. BaaS Grade: 1

User Responses: d. BaaS Feedback: a. Examples of cloud services include Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). 124. When an electronic control suffers an error, reports the error, and shuts down, it is called_____. a. Failopen b. Failsafe c. Failclose d. Failshut Grade: 1 User Responses: b. Failsafe Feedback: a. When the control fails and shuts down, it is a failsafe. When it fails and leaves a vulnerable system, it is a failopen. 125. What should be the first thing you check when an intrusion has been detected? a. Firewall logs b. Server logs c. Workstation logs d.

Security patches Grade: 1 User Responses: a. Firewall logs Feedback: a. Logging is also important when it comes to a firewall. Firewall logs should be the first thing you check when an intrusion has been detected. You should know how to access the logs and how to read them. 126. Which log on a Windows server is where you could learn if Joe logged in today? a. Applications b. System c. Security d. DNS Grade: 1 User Responses: c. Security Feedback: a. The security log contains entries about logins and access to resources both successful and unsuccessful. 127. Which of the following is NOT an example of physical security? a. Mantraps b.

Security logs c. Video surveillance d. Hardware locks Grade: 1 User Responses: b. Security logs Feedback: a. Security logs track activities on the

network which is logical not physical security. 128. Which of the following is NOT a type of door lock? a. Cipher b. Keyed c. Cardkey d. Mantrap Grade: 1 User Responses: d. Mantrap Feedback: a. A mantrap is a two door system designed to prevent tailgating. 129. Which of the following is NOT an example of operating system hardening? a. Disabling unnecessary services b. Removing the NIC c. Protecting management interfaces d. Password protection Grade: 1 User Responses: b. Removing the NIC Feedback: a.

Hardening the system should not reduce its functionality, and removing the NIC would do that. 130. Which of the following standards is often referred to as port-based security? a. 802. 1x b. 802. 11 c. 802. 11n d. 802. 1 Grade: 1 User Responses: a. 802. 1x Feedback: a. 802. 1x enforces perimeter security by keeping the port of the station closed until authentication is complete. 131. In which type of monitoring is network traffic analyzed for predetermined attack patterns? a. Signature-based monitoring b. Anomaly-based monitoring c. Behavior-based monitoring d. Reactive-based monitoring Grade: 1 User Responses: a. Signature-based monitoring

Feedback: a. Network traffic is analyzed for predetermined attack patterns. These attack patterns are known as signatures. 132. A(n) _____ uses baseline reporting and other analyses to discover vulnerabilities and weaknesses in systems. a. NAT b. SPA c. SLA d. PSK Grade: 1 User Responses: b. SPA Feedback: a. The security posture can be defined as the risk level to which a system, or other technology element, is exposed. Security Posture Assessments (SPA) use baseline reporting and other analyses to discover vulnerabilities and weaknesses in systems. 133. Which of the following indicate a problem currently occurring? . Trends b. Baselines

c. Alarms d. Averts Grade: 1 User Responses: c. Alarms Feedback: a. Although alerts indicate an issue that MAY need attention, alarms indicate a problem currently occurring. 134. Which of the following are detection controls? (Choose all that apply.) a. IDS b. IPS c. Video cameras d. Security guard Grade: 2 User Responses: a. IDS, c. Video cameras Feedback: a. Detection controls, such as Intrusion Detection systems and video cameras record only activity; they do not prevent it. /b. Detection controls, such as Intrusion Detection systems and video cameras record only activity; they do not prevent it. 35. Which of the following is designed to prevent tailgating? a. Mantraps b. Security logs c. Video surveillance d. Hardware locks Grade: 1 User Responses: a. Mantraps Feedback: a. Mantraps use double doors to prevent tailgating. 136. Which of the following is a proximity reader? a. a security card that transmits the location of the holder b. a device that tracks how close an individual is c. a security card reader that can read the card from a distance d. a card reader that locks the door when the holder is a certain distance from the door Grade: 1 User Responses: c. security card reader that can read the card from a distance Feedback: a. These cards use radio waves to transmit to the reader. 137. By frequently updating systems and by employing other methods such as group policies and baselining, you _____ the systems. a. brace b. harden c. virtualize d. hardline Grade: 1 User Responses: b. harden Feedback: a. By frequently updating systems and by employing other methods such as group policies and baselining, you harden the system. 138. Installing service packs is a part of the _____ process. a. baselining b. hardening c. scaling . security templating Grade: 1 User Responses: b. hardening Feedback: a. Hardening the OS is accomplished through the use of service packs, patch management,

hotfixes, group policies, security templates, and configuration baselines. 139. _____ can be described as unauthorized WAPs that inadvertently enable access to secure networks. a. Rogue access points b. Evil twin c. War driver d. Phisher Grade: 1 User Responses: a. Rogue access points Feedback: a. Rogue access points can be described as unauthorized wireless access points/routers that enable access to secure networks.

They differ from an Evil twin in that an Evil twin is strategically placed for the purpose of accessing the network or performing a high jacking attack, whereas rogue access points generally may be placed by employees for their convenience. 140. Which wireless attacks include the introduction of radio interference? a. Rogue Access Point b. Evil twin c. War driver d. Bluesnarfing Grade: 1 User Responses: b. Evil twin Feedback: a. The evil twin attack includes jamming the network to cause the stations to associate with the evil twin AP. 141. When executing the Evil twin attack, what value must match on the Evil twin and the legitimate AP? . IP address b. SSID c. MAC address d. Admin password Grade: 1 User Responses: b. SSID Feedback: a. The Evil twin attack includes jamming the network to cause the stations to associate with the Evil twin AP. The stations will not roam to the Evil twin unless the SSID is the same as the legitimate AP. 142. _____ is when a person attempts to access a wireless network, usually while driving in a vehicle. a. War chalking b. Radiophishing c. War driving d. Bluesnarfing Grade: 1 User Responses: c. War driving Feedback: a. War driving is when a person attempts to access a wireless