Chapter 6 Review Questions

1. Isabella is a security support manager for a large enterprise. In a recent meeting, she was asked which of the standard networking devices already present on the network could be configured to supplement the specific network security hardware devices that were recently purchased. Which of these standard networking devices would Isabella recommend?
2. router
3. hub
4. virtual private network
5. SIEM device
6. Ximena noticed that Sofia had created a network bridge on her new laptop between the unsecured wireless network and the organization’s secure intranet. Ximena explained to Sofia the problem associated with setting up the bridge. What did Ximena tell Sofia?
7. A bridge will block packets between two different types of networks.
8. A bridge cannot be used on any Internet connection.
9. A bridge would block packets from reaching the Internet.
10. A bridge could permit access to the secure wired network from the unsecured wireless network
11. Which of these would NOTbe a filtering mechanism found in a firewall ACL rule?
12. source address
13. direction
14. date
15. protocol
16. Which of the following devices can identify the application that send packets and then make decisions about filtering based on it?
17. Internet content filter
18. application-based firewall
19. reverse proxy
20. web security gateway
21. Which function does an Internet content filter NOT perform?
22. intrusion detection
23. URL filtering
24. malware inspection
25. content inspection
26. How does network address translation (NAT) improve security?
27. It filters based on protocol.
28. It discards unsolicited packets.
29. It masks the IP address of the NAT device.
30. NATs do not improve security.
31. Francisco was asked by a student intern to explain the danger of a MAC flooding attack on a switch. What would Francisco say?
32. Once the MAC address table is full the switch functions like a network hub.
33. A MAC flooding attack with filter to the local host computer’s MAC-to-IP address tables and prevent these hosts from reaching the network.
34. In a defense of a MAC flooding attack network routers will freeze and not permit any incoming traffic.
35. A MAC flooding attack will prevent load balances from identifying the correct VIP of the servers.
36. Which device is easiest for an attacker to take advantage of to capture and analyze packets?
37. router
38. hub
39. switch
40. load balancer
41. Sebastian was explaining to his supervisor why the enterprise needed to implement port security. His supervisor asked what security action a flood guard could do when a MAC flooding attack occurred. Which of the following was NOT an answer that was given by Sebastian?
42. Ignore the new MAC addresses while allowing normal traffic from the single pre-approved MAC address
43. Cause the device to enter a fail-open mode.
44. Record new MAC addresses up to a specific limit
45. Block the port entirely
46. Which statement regarding a demilitarized zone (DMZ) is NOT true?
47. It can be configured to have one or two firewalls.
48. It typically includes an email or web server.
49. It provides an extra degree of security.
50. It contains servers that are used only by internal network users.
51. Which statement about network address translation (NAT) is true?
52. It substitutes MAC addresses for IP addresses.
53. It can be stateful or stateless.
54. It can be found only on core routers.
55. It removes private addresses when the packet leaves the network.
56. Which of these is NOT used in scheduling a load balancer?
57. The IP address of the destination packet
58. Data within the application message itself
59. Round-robin
60. Affinity
61. In which of the following configurations are all the load balancers always active?
62. Active-active
63. Active-passive
64. Passive-active-passive
65. Active-load-passive-load
66. Which device intercepts internal user requests and then processes those requests on behalf of the users?
67. Forward proxy server
68. Reverse proxy server
69. Host detection server
70. Intrusion prevention device
71. Raul was asked to configure the VPN to preserve bandwidth. Which configuration would he choose?
72. Split tunnel
73. Full tunnel
74. Narrow tunnel
75. Wide tunnel
76. Which device watches for attacks and sounds an alert only when one occurs?
77. firewall
78. network intrusion detection system (NIDS)
79. network intrusion prevention system (NIPS)
80. proxy intrusion device
81. Which of the following is a multipurpose security device?
82. Hardware security module
83. Unified Threat Management (UTM)
84. Media gateway
85. Intrusion Detection/Prevention (ID/P)
86. Which of the following CANNOT be used to hide information about the internal network?
87. network address translation (NAT)
88. a protocol analyzer
89. a subnetter
90. a proxy server
91. What is the difference between a network intrusion detection system (NIDS) and a network intrusion prevention system (NIPS)?
92. A NIDS provides more valuable information about attacks.
93. There is no difference; a NIDS and a NIPS are equal.
94. A NIPS can take actions more quickly to combat an attack.
95. A NIPS is much slower because it uses protocol analysis.
96. Which is the most secure type of firewall?
97. stateless packet filtering
98. stateful packet filtering
99. network intrusion detection system replay
100. reverse proxy analysis