Chapter 7

1. Which of the following TCP/IP protocols do not relate to security?
2. **IP**
3. SNMP
4. HTTPS
5. FTP
6. Aideen sent an email to her supervisor explaining the Domain Name System Security Extensions (DNSSEC). Which of the following statements would Aideen have NOT included in her email?
7. It is fully supported in BIND9.
8. It adds additional resource records.
9. It adds message header information.
10. **It can prevent a DNS transfer attack**.
11. What is the recommended secure protocol for voice and video applications?
12. **Secure Real-time Transport Protocol (SRTP)**
13. Hypertext Transport Protocol Secure (HTTPS)
14. Network Time Protocol (NTP)
15. Secure/Multipurpose Internet Mail Extensions (S/MIME)
16. Which type of log can provide details regarding requests for specific files on a system?
17. audit log
18. **event log**
19. access log
20. SysFile log
21. Which type of device log contains the most beneficial security data?
22. **firewall log**
23. email log
24. switch log
25. router log
26. Which type of cloud is offered to specific organizations that have common concerns?
27. public cloud
28. hybrid cloud
29. private cloud
30. **community cloud**
31. Which of these is NOT correct about an SSL accelerator?
32. It can be a separate hardware card that inserts into a web server
33. It can be a separate hardware module
34. It should reside between the user’s device and the web servers
35. **It can only handle the SSL protocol.**
36. Catriona needed to monitor network traffic. She did not have the resources to install an additional device on the network. Which of the following solutions would meet her needs?
37. Network tap
38. **Port mirroring**
39. Aggregation switch
40. Correlation engine
41. Which version of Simple Network Management Protocol (SNMP) is considered the most secure?
42. SNMPv2
43. **SNMPv3**
44. SNMPv4
45. SNMPv5
46. Which Domain Name System (DNS) attack replaces a fraudulent IP address for a symbolic name?
47. DNS replay
48. DNS masking
49. **DNS poisoning**
50. DNS forwarding
51. Which of these is the most secure protocol for transferring files?
52. FTPS
53. TCP
54. **SFTP**
55. FTP
56. Which of the following can be used to prevent a buffer overflow attack?
57. **DEP**
58. FIM
59. VPN
60. DNS
61. Which of the following is NOT a service model in cloud computing?
62. Software as a Service (SaaS)
63. **Hardware as a Service (HaaS)**
64. Platform as a Service (PaaS)
65. Infrastructure as a Service (IaaS)
66. Eachna is showing a new security intern the log file from a firewall. Which of the following entries would she tell him do not need to be investigated?
67. suspicious outbound connections
68. IP addresses that are being rejected and dropped
69. **successful logins**
70. IP addresses that are being rejected and dropped
71. Which type of hypervisor does not run on an underlying operating system?
72. **Type I**
73. Type II
74. Type III
75. Type IV
76. Which application stores the user’s desktop inside a virtual machine that resides on a server and is accessible from multiple locations?
77. Application cell
78. Container
79. VDE
80. **VDI**
81. Kyle asked his supervisor which type of computing model was used when the enterprise first started. She explained that the organization purchased all the hardware and software necessary to run the company. What type of model was she describing to Kyle?
82. Virtual services
83. Off-premises
84. **On-premises**
85. Hosted services
86. DNSSEC adds additional \_\_\_\_\_ and message header information, which can be used to verify that the requested data has not been altered in transmission.
87. **resource records**
88. field flags
89. hash sequences
90. zone transfers
91. What functions of a switch does a software defined network separate?
92. Host and virtual
93. **Control plane and physical plane**
94. RAM and hard drive
95. Network level and resource level
96. Which of the following is NOT a security concern of virtualized environments?
97. Virtual machines must be protected from both the outside world and from other virtual machines on the same physical computer.
98. Physical security appliances are not always designed to protect virtual systems.
99. **Virtual servers are less expensive than their physical counterparts**.
100. Live migration can immediately move one virtualized server to another hypervisor.