|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. The current Bluetooth version is Bluetooth 6.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. In a bluesnooping attack, the attacker copies emails, calendars, contact lists, cell phone pictures, or videos by connecting to the Bluetooth device without the owner's knowledge or permission.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. Near field communication (NFC) is a set of standards used to establish communication between devices in very close proximity.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. RFID is commonly used to transmit information between networked computers.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. In ad hoc mode, devices can only communicate between themselves and cannot connect to another network.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. RF signals can be picked up from an open or mis-configured AP.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. RF signal "noise" that creates interference and prevents communications from occurring is called signal blocking.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. The MAC address is a unique 64-bit number that is "burned" into the network interface card adapter when it is manufactured.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |
| 9. Wired Equivalent Privacy (WEP) is an IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmitted wireless information.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. For IEEE WLANs, the maximum transmit power is 200 milliwatts (mW).   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. Bluetooth is an example of what type of technology below?   |  |  |  | | --- | --- | --- | |  | a. | Small Area Network | |  | b. | Private Area Network | |  | c. | Personal Area Network | |  | d. | Limited Area Network |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. What is the maximum range of most Bluetooth 5 devices?   |  |  |  | | --- | --- | --- | |  | a. | 200 ft | |  | b. | 60 meters | |  | c. | 150 meters | |  | d. | 800 ft |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What type of radio frequency transmissions are used by Bluetooth devices?   |  |  |  | | --- | --- | --- | |  | a. | single-range radio | |  | b. | long-range radio | |  | c. | short-range radio | |  | d. | ultra-short-range radio |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. Slave devices that are connected to a piconet and are sending transmissions are known as what?   |  |  |  | | --- | --- | --- | |  | a. | active slave | |  | b. | passive slaves | |  | c. | parked slaves | |  | d. | neutral slaves |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Piconets in which connections exist between different piconets are known as which of the following terms?   |  |  |  | | --- | --- | --- | |  | a. | broadnet | |  | b. | honeynet | |  | c. | boundnet | |  | d. | scatternet |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. What term below is used to describe an attack that sends unsolicited messages to Bluetooth enabled devices?   |  |  |  | | --- | --- | --- | |  | a. | Bluesnarfing | |  | b. | Bluejacking | |  | c. | Bluecracking | |  | d. | Bluetalking |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. A Bluetooth attack in which the attacker accesses unauthorized information from a wireless device using a Bluetooth connection, is known as which of the following terms?   |  |  |  | | --- | --- | --- | |  | a. | Bluejacking | |  | b. | Bluecracking | |  | c. | Bluesnarfing | |  | d. | Bluetalking |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. What device acts like a wireless base station in a network, acting as a bridge between wireless and wired networks?   |  |  |  | | --- | --- | --- | |  | a. | access Point | |  | b. | endpoint | |  | c. | WMM | |  | d. | ad-hoc peer |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. An access point that is unauthorized and allows an attacker to bypass network security configurations is considered to be what type of access point?   |  |  |  | | --- | --- | --- | |  | a. | random | |  | b. | sanctioned | |  | c. | rogue | |  | d. | legitimate |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. What type of access point is configured by an attacker in such a manner that it mimics an authorized access point?   |  |  |  | | --- | --- | --- | |  | a. | active twin | |  | b. | authorized twin | |  | c. | internal replica | |  | d. | evil twin |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. What is the maximum number of characters that can exist within a SSID name?   |  |  |  | | --- | --- | --- | |  | a. | 10 | |  | b. | 12 | |  | c. | 26 | |  | d. | 32 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. The Temporal Key Integrity Protocol (TKIP) encryption technology uses a MIC value that is what length?   |  |  |  | | --- | --- | --- | |  | a. | 24 bits | |  | b. | 32 bits | |  | c. | 48 bits | |  | d. | 64 bits |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Which encryption protocol below is used in the WPA2 standard?   |  |  |  | | --- | --- | --- | |  | a. | AES-CCMP | |  | b. | AES-CTR | |  | c. | AES-TKIP | |  | d. | AES-SCMP |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. Which of the following choices is not one of the four types of packets used by EAP?   |  |  |  | | --- | --- | --- | |  | a. | Request | |  | b. | Response | |  | c. | Success | |  | d. | Error |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Which option below is responsible for the issuing of EAP request packets?   |  |  |  | | --- | --- | --- | |  | a. | supplicant | |  | b. | authenticator | |  | c. | authentication server | |  | d. | proxy |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. Select the EAP protocol supported by WPA2 Enterprise that securely tunnels any credential form for authentication using TLS.   |  |  |  | | --- | --- | --- | |  | a. | EAP-MSCHAPv2 | |  | b. | EAP-AKA | |  | c. | EAP-FAST | |  | d. | EAP-TLS |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Select the EAP protocol that uses digital certificates for authentication?   |  |  |  | | --- | --- | --- | |  | a. | EAP-MSCHAPv2 | |  | b. | EAP-AKA | |  | c. | EAP-FAST | |  | d. | EAP-TLS |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. Which EAP protocol creates an encrypted channel between the client authentication server and the client, and uses Microsoft Windows logins and passwords?   |  |  |  | | --- | --- | --- | |  | a. | TKIP | |  | b. | LEAP | |  | c. | PEAP | |  | d. | ICMP |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What technology uses a standard web browser to provide information, and gives the wireless user the opportunity to agree to a policy or present valid login credentials, providing a higher degree of security?   |  |  |  | | --- | --- | --- | |  | a. | captive portal AP | |  | b. | gateway access point | |  | c. | wireless device probe | |  | d. | AUP access point |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. When using AES-CCMP, the AES-256 bit key requires how many rounds?   |  |  |  | | --- | --- | --- | |  | a. | 4 | |  | b. | 10 | |  | c. | 13 | |  | d. | 15 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. Where does the supplicant send identity information?   |  |  |  | | --- | --- | --- | |  | a. | client | |  | b. | second supplicant | |  | c. | authenticator | |  | d. | certificate authority |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. Select the device that is designed to exclusively monitor the RF frequency for network transmissions?   |  |  |  | | --- | --- | --- | |  | a. | access point probe | |  | b. | dedicated probe | |  | c. | WAP | |  | d. | wireless device probe |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What encryption protocol is used for WPA2?   |  |  |  | | --- | --- | --- | |  | a. | TKIP | |  | b. | TKIP MIC | |  | c. | CCMP | |  | d. | CBC-MAC |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What is the maximum transmission power for IEEE WLANs?   |  |  |  | | --- | --- | --- | |  | a. | 100 milliwatts (mW) | |  | b. | 200 milliwatts (mW) | |  | c. | 400 milliwatts (mW) | |  | d. | 500 milliwatts (mW) |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What specific feature on an AP controls how much of the spectrum is available to transfer data?   |  |  |  | | --- | --- | --- | |  | a. | channel width | |  | b. | channel variance | |  | c. | channel selection | |  | d. | channel frequency limit |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which direction do access point antennas radiate their signals and where should they be located?   |  |  |  | | --- | --- | --- | |  | a. | two direction and centrally located | |  | b. | four directions and asymmetrically located | |  | c. | all directions and asymmetrically located | |  | d. | all directions and centrally located |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. What type of survey can help a network administrator make decisions about bands, channels, and widths when installing new access points?   |  |  |  | | --- | --- | --- | |  | a. | wireless | |  | b. | site | |  | c. | frequency | |  | d. | architectural |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following self-contained APs are autonomous, or independent, because they are separate from other network devices and even other autonomous APs?   |  |  |  | | --- | --- | --- | |  | a. | fat APs | |  | b. | single APs | |  | c. | thin APs | |  | d. | super APs |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is the most secure form of IEEE 802.1x authentication?   |  |  |  | | --- | --- | --- | |  | a. | approved authentication | |  | b. | authenticator-based authentication | |  | c. | spectrum-based authentication | |  | d. | certificate-based authentication |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Authentication for WPA Personal is accomplished by using what type of key?   |  |  |  | | --- | --- | --- | |  | a. | IV | |  | b. | PSK | |  | c. | TKIP | |  | d. | MIC |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |
| --- | --- | --- |
| 41. Describe a piconet.   |  |  | | --- | --- | | *ANSWER:* | When two Bluetooth devices come within range of each other, they automatically connect with one another. One device is the master and controls all of the wireless traffic. The other device is known as a slave, which takes commands from the master. Slave devices that are connected to the piconet and are sending transmissions are known as active slaves; devices that are connected but are not actively participating are called parked slaves. | |

|  |  |  |
| --- | --- | --- |
| 42. Discuss how to prevent bluesnarfing.   |  |  | | --- | --- | | *ANSWER:* | To prevent bluesnarfing, Bluetooth devices should be turned off when not being used or when in a room with unknown people. Another option is to set Bluetooth on the device as undiscoverable, which keeps Bluetooth turned on, yet it cannot be detected by another device.42 | |

|  |  |  |
| --- | --- | --- |
| 43. List and describe the major parts of an access point.   |  |  | | --- | --- | | *ANSWER:* | An access point (AP) consists of three major parts: An antenna and a radio transmitter/receiver to send and receive wireless signals Special bridging software to interface wireless devices to other devices A wired network interface that allows it to connect by cable to a standard wired network. | |

|  |  |  |
| --- | --- | --- |
| 44. What technique can an attacker use to search for unprotected home wireless signals from an automobile or on foot using a portable computing device?   |  |  | | --- | --- | | *ANSWER:* | An attacker can use the war driving technique to identify unprotected home wireless networks. | |

|  |  |  |
| --- | --- | --- |
| 45. Discuss the different types of interference one might encounter using wireless devices.   |  |  | | --- | --- | | *ANSWER:* | Because wireless devices operate using RF signals, there is the potential for two types of signal interference. The wireless device may itself be the source of interference for other devices, and signals from other devices can disrupt wireless transmissions. Several types of devices transmit a radio signal that can cause incidental interference with a WLAN. These devices include microwave ovens, elevator motors, photocopying machines, certain types of outdoor lighting systems, theft protection devices, cordless telephones, microwave ovens, and Bluetooth devices. These may cause errors or completely prevent transmission between a wireless device and an AP. | |

|  |  |  |
| --- | --- | --- |
| 46. What are the four types of packets used by EAP?   |  |  | | --- | --- | | *ANSWER:* | EAP uses four types of packets: request, response, success, and failure. | |

|  |  |  |
| --- | --- | --- |
| 47. Explain why it is important to be able to control the power level at which the WLAN transmits.   |  |  | | --- | --- | | *ANSWER:* | Another security feature on some APs is the ability to adjust the level of power at which the WLAN transmits. On devices with that feature, the power can be adjusted so that less of the signal leaves the premises and reaches outsiders. | |

|  |  |  |
| --- | --- | --- |
| 48. What is the Message Integrity Check (MIC) within WPA used for?   |  |  | | --- | --- | | *ANSWER:* | The Message Integrity Check (MIC) is used to prevent an attacker from conducting active or passive man-in-the-middle attacks by capturing, altering, and resending data packets. | |

|  |  |  |
| --- | --- | --- |
| 49. How does the WPA Temporal Key Integrity Protocol encryption technology operate?   |  |  | | --- | --- | | *ANSWER:* | TKIP functions as a "wrapper" around WEP by adding an additional layer of security but preserving WEP's basic functionality. TKIP's enhancements are in three basic areas: the required key length is increased from 64 bits to 128 bits (making it harder to break), the IV is increased from 24 bits to 48 bits (effectively eliminating collisions), and a unique "base key" is created for each wireless device using a master key derived in the authentication process along with the sender's unique MAC address. | |

|  |  |  |
| --- | --- | --- |
| 50. What is the most common type of wireless access control?   |  |  | | --- | --- | | *ANSWER:* | Media Access Control (MAC) address filtering is the most common type of wireless access control. | |