|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. The current Bluetooth version is Bluetooth 6.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | 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 | |

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

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

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

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

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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) | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |
| --- |
| 41. Describe a piconet. |

|  |
| --- |
| 42. Discuss how to prevent bluesnarfing. |

|  |
| --- |
| 43. List and describe the major parts of an access point. |

|  |
| --- |
| 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? |

|  |
| --- |
| 45. Discuss the different types of interference one might encounter using wireless devices. |

|  |
| --- |
| 46. What are the four types of packets used by EAP? |

|  |
| --- |
| 47. Explain why it is important to be able to control the power level at which the WLAN transmits. |

|  |
| --- |
| 48. What is the Message Integrity Check (MIC) within WPA used for? |

|  |
| --- |
| 49. How does the WPA Temporal Key Integrity Protocol encryption technology operate? |

|  |
| --- |
| 50. What is the most common type of wireless access control? |