QUESTIONS

1. Which of the following is *not* true regarding SSIDs?
   - **A.** The SSID is broadcast by APs in the network, unless otherwise configured.
   - **B.** If the SSID changes, all clients must update to the new SSID to communicate.
   - **C.** Turning off the SSID broadcast ensures only authorized clients, who know the SSID, can connect.
   - **D.** The SSID serves to identify wireless networks.
   - **E.** SSIDs are case sensitive.
2. Amanda is war driving and plans to use PrismStumbler. She wants to use the information gathered in a GPS mapping software application. Which of the following is the best choice to interface with PrismStumbler?
   - **A.** GPSDrive
   - **B.** GPSMap
   - **C.** WinPcap
   - **D.** Microsoft Mappoint
3. Which of the following tools would be used in a blackjacking attack?
   - **A.** Aircrack
   - **B.** BBCrack
   - **C.** BBProxy
   - **D.** Paros Proxy
4. Which of the following uses a 48-bit initialization vector? (Choose all that apply.)
   - **A.** WEP
   - **B.** WPA
   - **C.** WPA2
   - **D.** WEP2
5. Which of the following are true statements? (Choose all that apply.)
   - **A.** WEP uses shared key encryption with TKIP.
   - **B.** WEP uses shared key encryption with RC4.
   - **C.** WPA2 uses shared key encryption with RC4.
   - **D.** WPA2 uses TKIP and AES encryption.
6. Which of the following best describes the "evil twin" wireless hacking attack?
   - **A.** An attacker sets up a client machine using the same MAC as an authorized user.
   - **B.** An attacker connects using the same username and password as an authorized user.

C. An attacker sets up an access point inside the network range for clients to connect to.

D. An attacker sets up an authentication server on the wireless network.

7. Brad is responsible for wireless security in his organization. He has turned off SSID broadcasting, enabled MAC filtering, and instituted wireless encryption. While strolling around the area, he notices an employee using an HP laptop, and the organization purchases only Dell systems for employees. After reviewing access logs and site survey information, Brad determines there appears to be no rogue access points in the area, and all connection attempts in wireless appear to be valid. There are no obvious signs of an attack. Which of the following best describes the successful connection attempt by the employee on the HP laptop?

A. The employee has brute-forced the encryption.

B. The employee has spoofed a legitimate MAC address.

C. The laptop choice is irrelevant, as long as the OUI is the same.

D. An evil twin attack is in place.

8. During an outbrief of a pen test, you share successes your team has had against the target's wireless network. The client asks for an explanation of the results, stating directional antennas for the access points were strategically placed to provide coverage for the building instead of omnidirectional antennas. Which of the following statements provides the correct response?

A. Positioning and types of antennas are irrelevant.

B. Directional antennas provide only for weak encryption of signal.

C. Positioning of the antennas is irrelevant unless 802.11n is the standard chosen.

D. Wireless signals can be detected from miles away; therefore, this step alone will not secure the network.

9. An attacker is attempting to crack a WEP code to gain access to the network. After enabling monitor mode on wlan0 and creating a monitoring interface (mon 0), she types this command:

```
aireplay –ng -0 0 –a 0A:00:2B:40:70:80 –c mon0
```

What is she trying to accomplish?

A. Gain access to the WEP access code by examining the response to deauthentication packets, which contain the WEP code

B. Use deauthentication packets to generate lots of network traffic

C. Determine the BSSID of the access point

D. Discover the cloaked SSID of the network

10. Which wireless standard works at 54Mbps on a frequency range of 2.4GHz?
    - **A.** 802.11a
    - **B.** 802.11b
    - **C.** 802.11g
    - **D.** 802.11n
11. The team has discovered an access point configured with WEP encryption. What is needed to perform a fake authentication to the AP in an effort to crack WEP? Choose all that apply.
    - **A.** A captured authentication packet
    - **B.** The IP address of the AP
    - **C.** The MAC address of the AP
    - **D.** The SSID
12. Which of the tools listed here is a passive discovery tool?
    - **A.** Aircrack
    - **B.** Kismet
    - **C.** NetStumbler
    - **D.** Netsniff
13. You have discovered an access point using WEP for encryption purposes. Which of the following is the best choice for uncovering the network key?
    - **A.** NetStumbler
    - **B.** Aircrack
    - **C.** John the Ripper
    - **D.** Kismet
14. Which of the following statements are true regarding TKIP? (Choose all that apply.)
    - **A.** Temporal Key Integrity Protocol forces a key change every 10,000 packets.
    - **B.** Temporal Key Integrity Protocol ensures keys do not change during a session.
    - **C.** Temporal Key Integrity Protocol is an integral part of WEP.
    - **D.** Temporal Key Integrity Protocol is an integral part of WPA.
15. Regarding SSIDs, which of the following are true statements? (Choose all that apply.)
    - **A.** SSIDs are always 32 characters in length.
    - **B.** SSIDs can be up to 32 characters in length.
    - **C.** Turning off broadcasting prevents discovery of the SSID.

D. SSIDs are part of every packet header from the AP.

E. SSIDs provide important security for the network.

F. Multiple SSIDs are needed to move between APs within an ESS.

16. You are discussing WEP cracking with a junior pen test team member. Which of the following are true statements regarding the initialization vectors? (Choose all that apply.)

A. IVs are 32 bits in length.

B. IVs are 24 bits in length.

C. IVs get reused frequently.

D. IVs are sent in clear text.

E. IVs are encrypted during transmission.

F. IVs are used once per encryption session.

17. A pen test member has configured a wireless access point with the same SSID as the target organization's SSID and has set it up inside a closet in the building. After some time, clients begin connecting to his access point. Which of the following statements are true regarding this attack? (Choose all that apply.)

A. The rogue access point may be discovered by security personnel using NetStumbler.

B. The rogue access point may be discovered by security personnel using NetSurveyor.

C. The rogue access point may be discovered by security personnel using Kismet.

D. The rogue access point may be discovered by security personnel using Aircrack.

E. The rogue access point may be discovered by security personnel using ToneLoc.

18. A pen test member is running the airsnarf tool from a Linux laptop. What is she attempting to do?

A. MAC flooding against an AP on the network

B. Denial-of-service attacks against APs on the network

C. Cracking network encryption codes from the WEP AP

D. Stealing usernames and passwords from an AP

19. What frequency does Bluetooth operate in?

A. 2.4–2.48GHz

B. 2.5GHz

C. 2.5–5GHz

D. 5GHz

20. Which of the following is true regarding wireless network architecture?
    A. The service area provided by a single AP is known as an ESS.
    B. The service area provided by a single AP is known as a BSSID.
    C. The service area provided by multiple APs acting within the same network is known as an ESS.
    D. The service area provided by multiple APs acting within the same network is known as an ESSID.
21. A pen tester boosts the signal reception capabilities of a laptop. She then drives from building to building in the target organization's campus searching for wireless access points. What attack is she performing?
    A. War chalking
    B. War walking
    C. War driving
    D. War moving
22. You are examining the physical configuration of a target's wireless network. You notice on the site survey that omnidirectional antenna access points are located in the corners of the building. Which of the following statements are true regarding this configuration? (Choose all that apply.)
    A. The site may be vulnerable to sniffing from locations outside the building.
    B. The site is not vulnerable to sniffing from locations outside the building.
    C. The use of dipole antennas may improve the security of the site.
    D. The use of directional antennas may improve the security of the site.
23. Which of the following is a true statement regarding wireless security?
    A. WPA2 is a better encryption choice than WEP.
    B. WEP is a better encryption choice than WPA2.
    C. Cloaking the SSID and implementing MAC filtering eliminate the need for encryption.
    D. Increasing the length of the SSID to its maximum increases security for the system.
24. A pen test colleague is attempting to use a wireless connection inside the target's building. On his Linux laptop he types the following commands:

```
ifconfig wlan0 down
ifconfig wlan0 hw ether 0A:0B:0C:1A:1B:1C
ifconfig wlan0 up
```

What is the most likely reason for this action?

A. Port security is enabled on the access point.

B. The SSID is cloaked from the access point.

C. MAC filtering is enabled on the access point.

D. Weak signaling is frustrating connectivity to the access point.

25. An individual attempts to make a call using his cell phone; however, it seems unresponsive. After a few minutes' effort, he turns it off and turns it on again. During his next phone call, the phone disconnects and becomes unresponsive again. Which Bluetooth attack is underway?

A. Bluesmacking

B. Bluejacking

C. Bluesniffing

D. Bluesnarfing

26. Which wireless standard achieves high data rate speeds by implementing MIMO antenna technology?

A. 802.11b

B. 802.11g

C. 802.11n

D. 802.16