1. Which of the following threats is/are examples of unauthorized network extensions in wireless-network security?

2. A criminal opens an unauthorized hotspot in a coffee shop and traps unsophisticated users of wireless communications into connecting to the rogue address. The criminal can thus trick the users into providing their credentials for access to the Internet or to restricted network resources. This kind of attack is called a ____

3. The server responsible for brokering the authentication and authorization of a user requesting access to a wireless access point generally uses ____

4. Which of the following is an example of a nonmalicious internal rogue WAP?

5. What does the acronym TKIP refer to in discussions of wireless networks?

6. Which of the following wireless security protocols is LEAST recommended?

7. Which of the following is/are (a) functional benefit(s) of wireless networking?

8. [A] major advantage[s] of wireless networking is/are that ____

9. Which of the following is an example of a malicious internal rogue WAP?

10. What technology uses IEEE 802.11 standards?

11. Which of the following is an example of a malicious external rogue WAP?

12. To reduce the likelihood of physical damage, wireless access points can be ____

13. Which of the following roles is/are included in IEEE 802.1X?

14. What does the acronym EAP mean in discussion of wireless security?

15. Which of the following threats is/are examples of unauthorized network extensions in wireless-network security?

16. What does the acronym _WEP_ mean in discussions of networking?

17. What is the family of wireless LAN standards developed by the IEEE?

18. In which decade were IEEE 802.11 standards first developed?

19. Which of the following threats can be enabled by rogue WAPs?

20. The IEEE released the 802.11i standard which is also called the ____

21. What does the acronym RADIUS mean in discussions of wireless security?

22. A unique identifier used by a client to establish connectivity to a particular wireless network is a(n) ____

23. What does the acronym _VLAN_ mean in discussions of information technology?

24. An attacker sets up a rogue RADIUS server that a victim connects to wirelessly. The fake server send a fixed RADIUS challenge that causes the victim's system to return an encrypted hash to the fixed challenge. This hashed password is then decrypted using brute-force dictionary-based cryptanalysis so that the criminal can retrieve the cleartext password. This attack is known as a ____

25. The process of accepting a client connection and allocating resources for it is called ____

26. Which of the following features is/are included in IEEE 802.1X?

27. Which of the following threats is/are examples of unauthorized network extensions in wireless-network security?