Homework Assignment: Chapter 10 – Wireless Network Attacks and Defenses

Answer each question in 3-5 sentences.

1. List and describe at least three types of wireless technologies mentioned in this chapter.
2. How do cellular networks provide Internet connectivity, and who is responsible for their security?
3. What is a Bluetooth piconet and how does it function?
4. Explain the difference between bluejacking and bluesnarfing.
5. Describe how Near Field Communication (NFC) works and name one vulnerability.
6. What are common defenses against NFC-based attacks?
7. What is RFID and why is it vulnerable to attacks like eavesdropping and cloning?
8. What is the role of an access point (AP) in a wireless local area network (WLAN)?
9. Compare the functions of autonomous (fat) APs and thin APs.
10. What is a rogue AP, and how does it threaten network security?
11. Explain what an evil twin AP is and how it is used in attacks.
12. What is RF jamming and how does it disrupt wireless networks?
13. Define a disassociation attack in the context of WLANs.
14. Why are consumer WLANs more vulnerable to attacks compared to enterprise WLANs?
15. What are the weaknesses of Wired Equivalent Privacy (WEP)?
16. Describe how Wi-Fi Protected Setup (WPS) can be exploited.
17. What is MAC address filtering and what makes it insecure?
18. Compare WPA Personal and WPA Enterprise authentication methods.
19. What security enhancements are introduced in WPA2 compared to WEP and WPA?
20. What role does the IEEE 802.1x standard play in WPA2-Enterprise?
21. Explain what Extensible Authentication Protocol (EAP) is and how PEAP simplifies deployment.
22. What are the main improvements introduced in WPA3?
23. What should be considered when performing a wireless site survey?
24. How can signal strength and spectrum selection enhance wireless security?
25. Describe how antenna placement can impact WLAN security.
26. What is rogue AP system detection and how does it work?