Wireless Network Attacks

Wireless network attacks involve performing intrusive monitoring, packet capturing, and penetration tests on a wireless network. Given the rapid deployment of wireless network connectivity in both public and private places, the mobile user is under constant threat. Wireless networks may be compromised as a network access point into your IT infrastructure. Implementation of proper wireless networking security controls is the key to mitigate the risks, threats, and vulnerabilities that arise from wireless networks. Many different tactics are used by hackers and perpetrators as they attempt to penetrate and attack wireless networks.

Here is a summary of wireless network attacks:

Bluejacking—Hacking and gaining control of the Bluetooth wireless communication link between a user's earphone and smartphone device.

Bluesnarfing—Packet sniffing communications traffic between Bluetooth devices.

Evil twin—Faking an open or public wireless network to use a packet sniffer on any user who connects to it.

IV attack—Modifying the initialization vector of an encrypted IP packet in transmission in hopes of decrypting a common encryption key over time.

Jamming/interference—Sending radio frequencies in the same frequency as wireless network access points to jam and interfere with wireless communications and disrupting availability for legitimate users.

Near field communication attack—Intercepting, at close range (a few inches), communications between two mobile operating system devices.

Packet sniffing—Capturing IP packets off a wireless network and analyzing the TCP/IP packet data using a tool such as Wireshark®.

Replay attacks—Replaying an IP packet stream to fool a server into thinking you are authenticating to it.

Rogue access points—Using an unauthorized network device to offer wireless availability to unsuspecting users.

War chalking—Creating a map of the physical or geographic location of any wireless access points and networks.

War driving—Physically driving around neighborhoods or business complexes looking for wireless access points and networks that broadcast an open or public network connection.

In addition to these specific attacks, hackers may also attempt to exploit weaknesses in the wireless encryption method used by the target: WEP (Wireless Encryption Protocol), WPA (Wi-Fi Protected Assets), or WPS (Wi-Fi Protected Setup).