13.1.6 Wireless Hacking Facts

With wireless networking, an attacker need only be in relatively close proximity to present a threat. To mitigate and eliminate attacks on your wireless network, it is important to understand the most common types of attacks you can expect, as well as the methodology and tools hackers use.

This lesson covers the following topics:

- Types of wireless attacks
- Wi-Fi discovery
- Wi-Fi discovery tools
- Global Positioning System mapping
- Wireless traffic analysis
- Wireless network cards

Types of Wireless Attacks

The following table lists many of the common types of attacks a wireless network administrator can expect from a hacker.

Wireless Attack Type	Description
Wardriving	Wardriving is when a hacker, using a laptop or smartphone, drives around and searches for wireless networks to attempt to break into. Although wardriving is defined as using a car for this purpose, any means of transportation can be used, such as biking, walking, and jogging. These are then referred to as warbiking, warwalking, and warjogging.
MAC spoofing	A media access control (MAC) address is a number that uniquely identifies a network interface card. This number is stored on the card in a read-only memory area. Since each network card has a unique MAC address, wireless network managers can create a list of legitimate MAC addresses and then allow only devices with listed MAC addresses to access the wireless network. However, many network drivers allow the MAC address to be changed. A hacker can use a packet analyzer tool, sometimes referred to as a sniffing tool, to obtain the legitimate MAC addresses. Then the hacker changes the MAC address on the driver to match one of the legitimate addresses being used and obtain access to the network.
Rogue access points and unauthorized association	A rogue access point is an unauthorized access point that has been set up in a company. These are sometimes set up by employees to bypass existing restrictions on the company's authorized access points. Rogue and unauthorized access points can also be installed by a hacker who has gained physical access to the building. A hacker can configure an extremely compact and powerful hardware device called a Raspberry Pi as an access point. A hacker can also use software-only access points called soft access points. Rogue access points can also be set up in close proximity to where users access the internet. The intent is that users will inadvertently connect to rogue access points. This is known as unauthorized association.
Access point misconfiguration	Wireless attacks are often successful simply because a network administrator doesn’t properly configure the access points. This is known as access point misconfiguration. The misconfiguration of the access point typically happens when the proper security steps not have been fully implemented, opening a wireless network to potential hackers.
Ad hoc networks	An ad hoc network is a network that has been established without using a pre-existing infrastructure, such as a router in a wired network or an access point in a managed wireless network. Instead, the devices participating in an ad hoc network communicate with each other directly. Ad hoc networks are often used because they can be cheaper to build. Unfortunately, most ad hoc networks offer minimal security against unwanted incoming connections. For example, ad hoc devices cannot disable SSID broadcasts like infrastructure mode devices can. Therefore, attackers generally have little difficulty connecting to an ad hoc device if they get within signal range.
Client mis-association	The basic idea behind a mis-association attack is to get a user or client to unintentionally connect to an unauthorized access point instead of the authorized one they intended to use. This can be achieved in many ways. For example, when a client connects to an access point, usually, there is an option to save the Service Set Identifier (SSID) of that access point. The device will automatically connect to a saved access point whenever that access point is available.

	Although this is convenient, it also opens the door for an attacker. A hacker can create and advertise an access point using the same SSID. Since the attacker's access point has the same name as the authorized access point and provides access to the internet, victims are not typically aware that they are accessing a different wireless network. Once a client connects to the unauthorized access point, the hacker is able to use tools that are easily available on the internet to steal valuable corporate data.
Promiscuous client	A promiscuous client is often used in conjunction with many of the other types of attacks. A hacker uses advanced technology to set up and advertise the promiscuous client using an extremely strong signal. Since most users are looking for the strongest signal, a promiscuous client's strong signal is almost irresistible. Blinded by the great connection being offered, mobile users often forget to consider that they may be opening themselves up to an attack.
Jamming attacks	Wi-Fi jamming is the deliberate use of radio noise or signals in an attempt to block or interfere with authorized wireless communications. Hackers can perform jamming attacks by analyzing the spectrum used by a wireless network and then transmitting a powerful signal to interfere with communication on the discovered frequency. While jamming is taking place, users can't connect to login because the 802.11 protocol is based on a collision avoidance algorithm that requires a period of silence before a device is allowed to transmit. In addition, those who were already connected will lose their connection.

Wi-Fi Discovery

In addition to the different types of wireless attacks that you can expect to see, it is also important to understand some of the methods and tools hackers use to find any way possible to target and break into your wireless computers and networks. One of the first methods used is Wi-Fi discovery, also known as discovery and footprinting. Your network won't be hacked if it can't be found. As such, the first thing a hacker must do is find your network.

The hacker uses a process of discovery and footprinting to find the wireless network and obtain information that will help to breach it. Two of the most important things a hacker needs to break into a wireless network are the Basic Service Sets (BSS) and the Service Set ID (SSID). Both of these are provided by access points.

As described in the following table, the process of footprinting can be done either passively or actively.

Footprinting Process	Description
Passive footprinting	Uses some type of wireless listening device, known as a sniffer, to capture packets in an attempt to discover the critical information needed. As mentioned earlier, this is often done using the wardriving method, where the hacker drives around with wireless laptop and external Wi-Fi antenna, trying to locate wireless networks. Keep in mind that with passive footprinting, no attempt is made to connect with any of the access points or wireless clients. The hacker only collects the data.
Active footprinting	Allows a hacker to use information obtained using the passive technique to get a little more aggressive in the attack on the network. For example, a hacker may send packets to the access point using a discovered SSID or send a probing packet without the SSID. When a probing packet without an SSID is answered, it includes the BSS.

Wi-Fi Discovery Tools

When it comes to the actual process of discovering and mapping wireless networks, you have many tools to choose from. The follow table describes two.

Wi-Fi Discovery Tool	Description
inSSIDer Plus	inSSIDer Plus is a wireless network scanner application that runs on Microsoft Windows platforms and was developed by MetaGeek, LLC. With this tool, you can scan for wireless networks using your laptop's wireless adapter. When a network is found, its signal strength is displayed along with the channels the network is using. In addition, inSSIDer Plus lists other useful information about the network. MetaGeek also sells other software and devices such as the Wi-Spy DBx USB device that measures Wi-Fi and non-Wi-Fi activity in both the 2.4 GHz and 5GHz bands.
WiFi Explorer	WiFi Explorer (developed by Nuts About Nets) is another Wi-Fi scanning tool designed to run on mobile platforms, specifically Android phones and tablets. Since these types of devices have built-in 802.11 radio capabilities, you can install and use WiFi Explorer to collect information from nearby wireless access points. The data collected can be displayed and used in many beneficial, legitimate ways.

	Unfortunately, this tool can help hackers understand the relationship between access points, wireless network SSIDs, and client stations.

Global Positioning System Mapping

Another methodology used by hackers is Global Positioning System (GPS) mapping. GPS mapping uses the same tracking technology that is commonly used in cars and phones to guide you as you travel.

Using this satellite navigation system, several companies are now monitoring wireless traffic and often sell this information to other companies, typically for marketing purposes. However, a hacker can also obtain this information and use it to create a map with locations of known access points.

Some of these tools are freely available, while others must be purchased. For example, you or a hacker can find locations of wireless access points from the Wireless Geographic Logging Engine (WiGLE) site (https://wigle.net/). The WiGLE database stores information about wireless hotspots around the world. The unique thing about WiGLE is that the information comes from people who register and then upload information. Anyone can view this information at no cost.

Companies such as WeFi, NinthDecimal (formally JiWire), and OpenSignal typically charge a fee to map wireless networks.

Wireless Traffic Analysis

After a hacker has identified the network, penetration often begins by using some sort of wireless traffic analysis. The analysis is typically performed before committing actual attacks on the wireless network.

Hackers use wireless sniffing tools such as Wireshark, SteelCentral Packet Analyzer, CommView for Wi-Fi, and OmniPeek Enterprise to obtain information. This type of analysis usually provides client information and may reveal vulnerabilities.

Wireless Network Cards

Much of what has been described in regard to wireless traffic discovery and analysis is dependent on using a network interface card that is capable of capturing the desired information. For example, capturing and displaying wireless data with Wireshark may require that the wireless card support promiscuous mode like the older AirPcap cards.

As an alternative, you may need to purchase a WIFI USB device, such as the Acrylic WiFi USB device that will perform some of the function of a promiscuous card. Before selecting an applicable card, spend some time researching cards on the internet. Make sure to consider the type of operating system the card uses, the architecture (such as PCMCIA or USB), and other important features such as transmitting or injecting packets into the network.
