Reconnaissance refers to the activity of finding/locating WiFi devices (APs and clients) present in the vicinity. It can also reveal information about the client device/owner and its behavior. The labs provided in this section provide the users with an emulated WiFi environment and monitor mode capable WiFi cards for sniffing. The objective is to use airodump-ng and other tools to find information about WiFi devices.

What will you learn?

- Sniffing WiFi traffic in monitor mode
- Locating WiFi networks and clients
- Broadcast/Directed probes and Preferred Network Lists

References:

1. Monitor mode (https://en.wikipedia.org/wiki/Monitor_mode)
2. Sniffing traffic with airodump-ng (https://www.aircrack-ng.org/doku.php?id=airodump-ng)
3. List of WiFi channels (https://en.wikipedia.org/wiki/List_of_WLAN_channels)
4. Tracking WiFi devices using frames (https://newatlas.com/wi-fi-track-smartphone-creepydol/28585/)

Labs Covered:

- WiFi Recon I

  In this lab, you will learn to interact with WiFi interfaces using CLI tools to perform recon. A non-exhaustive list of activities covered includes:
  - Enable different modes on WiFi interface using CLI tools
  - Scan the WiFi traffic to locate networks/clients of interest
  - Understand different terms like SSID, BSSID, client MAC, etc
  - Identify the security scheme of a network

- WiFi Recon II

  In this lab, you will learn to interact with WiFi interfaces using CLI tools and perform recon. A non-exhaustive list of activities to be covered includes:
  - Enable different modes on WiFi interface using CLI tools
  - Scan the WiFi traffic to locate networks/clients of interest
  - Understand different terms like SSID, BSSID, client MAC, etc
  - Identify the security scheme of a network
  - Learn to sniff traffic on both bands of WIFi

- Preferred Network List (PNL) Basics

  In this lab, you will learn to collect probe requests being sent out by devices and analyze those to deduce some information about the device owner. A non-exhaustive list of activities to be covered includes:
  - Scan the WiFi traffic to find probe requests and maintain the list
  - Learn about PNL and its significance

WiFi Recon I

Start