The massive increase in WiFi devices in both enterprises and homes has made the WiFi aspect important for incident response. Most organizations store WiFi authentication/access logs and traffic captures in case of attacks and anomalies. These can later be analyzed to reconstruct the chain of events. In each lab in this section, the user is provided with a case scenario, WiFi traffic captures and other relevant information. The user has to use Wireshark and other tools to analyze the traffic and solve the scenarios.

What will you learn?

- Analyzing WiFi traffic using Wireshark
- Decrypting WiFi traffic in Wireshark
- Locating covert channels
- Understanding how to estimate/correlate physical distance from signal strength

References:

1. Received Signal Strength (https://en.wikipedia.org/wiki/Received_signal_strength_indication)
2. Decrypt WiFi traffic (https://wiki.wireshark.org/HowToDecrypt802.11)
3. Covert channel (https://en.wikipedia.org/wiki/Covert_channel)

Labs Covered:

- Dumb Assassin
  In this lab, you will learn to analyze the traffic of an unprotected/open WiFi network. A non-exhaustive list of activities to be covered includes:
  - Filtering traffic for specific devices
  - Filtering traffic for protocols of interest
  - Locating information of interest by going through shortlisted/filtered packets

- Backdoored System
  In this lab, you will learn to identify and locate a covert channel created over WiFi frames to exfiltrate information. A non-exhaustive list of activities to be covered includes:
  - Check different frames to look for anomalies
  - Read the information being transmitted and reconstruct the whole conversation/sequence

- Breach Investigation
  In this lab, you will learn to decrypt encrypted traffic using Wireshark and investigate a breach scenario. A non-exhaustive list of activities to be covered includes:
  - Filter the traffic of relevant devices
  - Use the provided secret passphrase to decrypt the encrypted traffic
  - Look for suspicious protocols and identify the suspect

- Private Investigator
  In this lab, you will learn to crack the passphrase, decrypt encrypted traffic using Wireshark and analyze the traffic to locate a communication channel. A non-exhaustive list of activities to be covered includes:
  - Filter the traffic of relevant devices
  - Crack the passphrase for a WPA2-PSK network using aircrack-ng
  - Use the provided secret passphrase to decrypt the encrypted traffic
  - Look for protocols that can be used to communicate with other parties and retrieve the messages transmitted

- WiFi Addict

- Analyze the WiFi frames sent by devices of interest
- Correlate that information with provided information with the case

Backdoored System

Start

Breach Investigation

Start

Dumb Assassin

Start

Private Investigator

Start

WiFi Addict

Start