The labs in this section cover basic commands/tools that can be used to connect to an existing WiFi network, create WiFi networks of different types of security schemes and bypass the MAC filter.

What will you learn?

- Connecting to WiFi networks using wpa_supplicant
- Creating WiFi networks to lure devices
- Bypassing MAC filter based access control

References:

1. Hosapd and wpa_supplicant? (https://w1.fi/)
2. Example hostapd.conf (https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf)
3. Example supplicant.conf (https://w1.fi/cgit/hostap/plain/wpa_supplicant/wpa_supplicant.conf)
4. Using WPA_supplicant to connect to WiFi (https://www.linuxbabe.com/command-line/ubuntu-server-16-04-wifi-wpa-supplicant)

Labs Covered:

- Hostapd: WEP Honeypot
  In this lab, you will learn to create a WiFi network with WEP security scheme for a given SSID using the Hostapd tool. This same technique is used to create the WiFi honeypots to lure a probing/non-probing client.

- Hostapd: WPA-PSK Honeypot
  In this lab, you will learn to create a WiFi network with WPA-PSK security scheme for a given SSID using the Hostapd tool. This same technique is used to create the WiFi honeypots to lure a probing/non-probing client.

- Hostapd: WPA2-PSK Honeypot
  In this lab, you will learn to create a WiFi network with WPA2-PSK security scheme for a given SSID using the Hostapd tool. This same technique is used to create the WiFi honeypots to lure a probing/non-probing client.

- WPA Supplicant: WEP Network
  In this lab, you will learn to connect a WiFi interface to a given WEP security scheme based WIFi network using the wpa_supplicant utility. This same technique is used by the Linux network manager to connect to the network.

- WPA Supplicant: WPA-PSK Network
  In this lab, you will learn to connect a WiFi interface to a given WPA-PSK security scheme based WIFi network using the wpa_supplicant utility. This same technique is used by the Linux network manager to connect to the network.

- WPA Supplicant: WPA2-PSK Network
  In this lab, you will learn to connect a WiFi interface to a given WPA2-PSK security scheme based WIFi network using the wpa_supplicant utility. This same technique is used by the Linux network manager to connect to the network.

- Bypassing MAC Filter
  In this lab, you will learn to change the MAC address of a WiFi interface, to evade the MAC filtering based access control deployed on a WiFi network.

- WPA Supplicant: WPA Enterprise

- Hostapd: Enhanced Open Honeypot
  In this lab, you will learn to create a WiFi network with WPA3-OWE security scheme for a given SSID using the Hostapd tool. This same technique is used to create the WiFi honeypots to lure a probing/non-probing client.

- WPA Supplicant: Enhanced Open
  In this lab, you will learn to connect a WiFi interface to a given WPA3-OWE security scheme based WIFi network using the wpa_supplicant utility. This same technique is used by the Linux network manager to connect to the network.

- Hostapd: WPA3-SAE Honeypot
  In this lab, you will learn to create a WiFi network with WPA3-SAE security scheme for a given SSID using the Hostapd tool. This same technique is used to create the WiFi honeypots to lure a probing/non-probing client.

- WPA Supplicant: WPA3-SAE
  In this lab, you will learn to connect a WiFi interface to a given WPA3-SAE security scheme based WIFi network using the wpa_supplicant utility. This same technique is used by the Linux network manager to connect to the network.

Hostapd: WEP Honeypot

Start

Hostapd: WPA-PSK Honeypot

Start

Hostapd: WPA2-PSK Honeypot

Start

WPA Supplicant: WEP Network

Start

WPA Supplicant: WPA-PSK Network

Start

WPA Supplicant: WPA2-PSK Network

Start

Bypassing MAC Filter

Start

WPA Supplicant: WPA Enterprise

Start