WiFi Pivoting refers to the approach where the attacker first gets access to the WiFi network and then attacks the machines on the wired LAN. This section covers attacks on the WPA enterprise network including the PEAP Relay attack. In each lab, the user has to first get access to the protected WiFi network and then target the machines running on the wired LAN side of the network.

What will you learn?

- Attacking WPA Enterprise networks with hostapd-mana and asleap
- Performing PEAP-Relay attack

References:

1. Hostapd Mana (https://github.com/sensepost/hostapd-mana)
2. WPA Sycophant (https://github.com/sensepost/wpa_sycophant)
3. PEAP-Relay attack blog (https://sensepost.com/blog/2019/peap-relay-attacks-with-wpa_sycophant/)
4. PEAP-Relay attack talk (https://www.youtube.com/watch?v=eYsGyvGxlpI&feature=youtu.be)

Labs Covered:

- Pivoting over WiFi: WPA Enterprise
  In this lab, you will learn to attack a WPA-Enterprise (TTLS-PAP) protected WiFi network operating in the vicinity, obtain the username/password of a user and use it to access the network. A non-exhaustive list of activities to be covered includes:
  - Use airodump-ng to locate the network
  - Create an evil twin for WPA-Enterprise network operating in the vicinity using EAPHammer
  - Use aireplay-ng to launch deauth attack and disconnect the client
  - Connect to the network using wpa_supplicant (with recovered username, password and network scheme information)
  - Obtain IP address using dhclient
  - Perform Nmap scan to discover the machine on the LAN side of the router.

- Pivoting over WiFi: PEAP Relay
  In this lab, you will learn to attack a WPA-Enterprise (PEAP-MSCHAPv2) protected WiFi network operating in the vicinity and use PEAP Relay attack to obtain access to the network. A non-exhaustive list of activities to be covered includes:
  - Use airodump-ng to locate the network
  - Create an evil twin for WPA-Enterprise network operating in the vicinity using Hostapd-mana
  - Ready PEAP Relay setup by starting WPA sycophant
  - Use aireplay-ng to launch deauth attack and disconnect the client
  - Observe the PEAP relay in action. WPA sycophant will replay the PEAP challenge-response and connect to the network
  - Perform Nmap scan to discover the machine on the LAN side of the router.

Pivoting over WiFi: WPA Enterprise

Starting..