This section covers popular WiFi security tools. Each tool is installed in the lab along with other supporting files/environment.

What will you learn?

- Attack automation with wifite
- Analyzing traffic on CLI with termshark
- WiFi attacks with bettercap and MDK4
- Attacking enterprise networks using EAPHammer
- Plotting airodump-ng scan results with scan visualizer

References:

1. Wifite (https://github.com/derv82/wifite)
2. termshark (https://termshark.io/)
3. bettercap (https://github.com/bettercap/bettercap)
4. MDK4 (https://github.com/aircrack-ng/mdk4)
5. EAPHammer (https://github.com/s0lst1c3/eaphammer)
6. Airodump-ng scan visualizer (https://www.pentesteracademy.com/course?id=18)

Labs Covered:

- Tool: Wifite
  In this lab, you will learn to use the Wifite to automatically attack a WPA2-PSKprotected WiFi network and recover its secret passphrase.

- Tool: Termshark
  In this lab, you will learn to use the Termshark TUI (terminal UI) tool to open a PCAP file and check/analyze the captured packets.

- Tool: Bettercap
  In this lab, you will learn to use the Bettercap tool to open a PCAP file and perform WiFi recon to locate nearby WiFi networks/clients.

- Tool: MDK4
  In this lab, you will learn to use the MDK4 tool to perform beacon flood. As the beacon flood is being performed in an emulated environment, it will need to be verified using airodump-ng.

- Tool: EAPHammer
  In this lab, you will learn to use the EAPHammer tool to perform honeypot based attacks on a WPA-Enterprise network, lure a client and steal the user's credentials.

Tool: Wifite

Start

Tool: Termshark

Start