

Live Cracking

This section covers the live attack/cracking labs for personal networks protected by personal WiFi security schemes such as WEP, WPA-PSK and WPA2-PSK. An emulated WiFi environment and monitor mode capable wlan0 is provided to users.

What will you learn?

- Understanding how WEP Cracking works and recovering secret WEP key
- 4-way handshake and WPA/WPA2-PSK passphrase cracking

References:

- 1. WEP in depth (https://www.pentesteracademy.com/video?id=489)
- 2. How WEP cracking works (https://www.pentesteracademy.com/video?id=490)
- 3. How does WPA-PSK work? (https://www.pentesteracademy.com/video?id=489)
- 4. Cracking WPA-PSK secret passphrase (https://www.pentesteracademy.com/video?id=497)

Labs Covered:

• Pivoting over WiFi: WEP

In this lab, you will learn to attack a WEP protected WiFi network operating in the vicinity and retrieve WEP key. A non-exhaustive list of activities to be covered includes:

- Use airodump-ng to capture traffic
- Use aireplay-ng to replay the ARP packets to increase the frame count
- Use aircrack-ng to recover the WEP key
- Connect to the network using wpa_supplicant (with recovered WEP key)
- Obtain IP address using dhclient
- Perform Nmap scan to discover the machine on the LAN side of the router.

• Live Cracking: WPA-PSK

In this lab, you will learn to attack a WPA-PSK protected WiFi network operating in the vicinity and retrieve the secret passphrase. A non-exhaustive list of activities to be covered includes:

- Use airodump-ng to locate the network and capture traffic
- Use aireplay-ng to launch deauth attack and disconnect the client to capture the 4-way handshake
- Use aircrack-ng to launch a dictionary attack and recover the secret passphrase

Live Cracking: WPA2-PSK

In this lab, you will learn to attack a WPA2-PSK protected WiFi network operating in the vicinity and retrieve the secret passphrase. A non-exhaustive list of activities to be covered includes:

- Use airodump-ng to locate the network and capture traffic
- Use aireplay-ng to launch deauth attack and disconnect the client to capture the 4-way handshake
- Use aircrack-ng to launch dictionary attack and recover the secret passphrase

AP-less WPA2-PSK Cracking

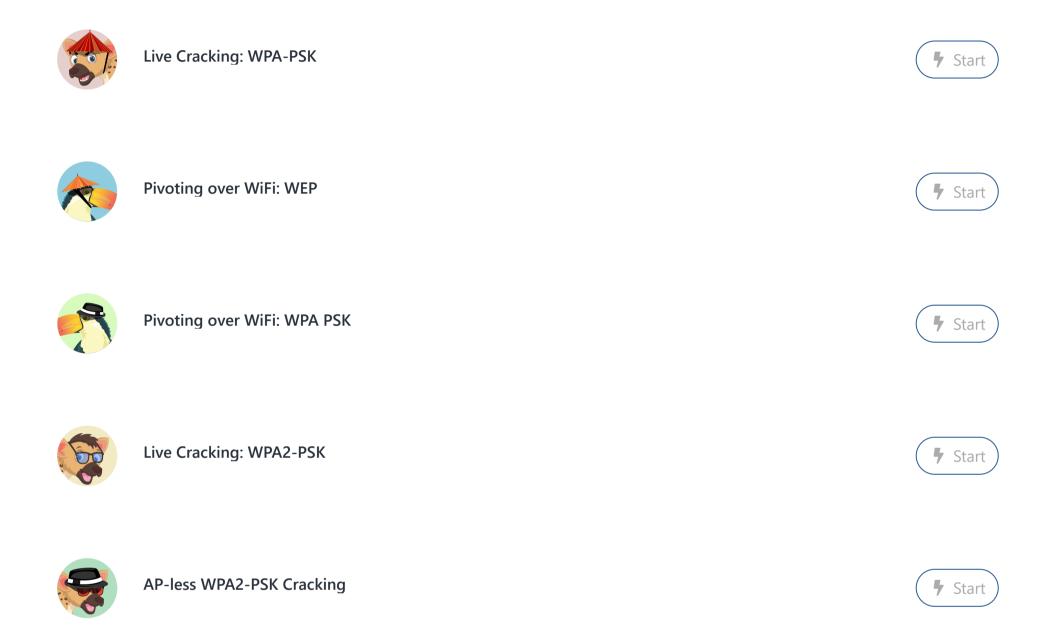
In this lab, you will learn to attack a WPA2-PSK protected WiFi network that is not operating in the vicinity but a device that has used that network is. Perform honeypot attack and retrieve the secret passphrase for that network. A non-exhaustive list of activities to be covered includes:

- Use airodump-ng to observe the probe requests
- Use airodump-ng to capture traffic
- Use Hostapd to create a WPA2-PSK with the same SSID name as the SSID name appearing in probe requests

• Pivoting over WiFi: WPA PSK

In this lab, you will learn to attack a WPA-PSK protected WiFi network operating in the vicinity and retrieve a secret passphrase. A non-exhaustive list of activities to be covered includes:

- Use airodump-ng to locate the network and capture traffic
- Use aireplay-ng to launch deauth attack and disconnect the client to capture the 4-way handshake
- Use aircrack-ng to launch dictionary attack and recover the secret passphrase
- Connect to the network using wpa_supplicant (with a recovered passphrase)
- Obtain IP address using dhclient
- Perform Nmap scan to discover the machine on the LAN side of the router.



<u>Privacy Policy</u> <u>ToS</u>

Copyright © 2018-2019. All right reserved.