‹ Dashboard

OFFLINE CRACKING
Personal Networks

Offline Cracking

Personal WiFi network security schemes are the ones usually deployed at home or in personal spaces. Examples of such schemes include WEP, WPA-PSK, WPA2-PSK. This section covers the offline cracking labs for personal networks. A traffic capture PCAP is provided to the user along with the required tools.

What will you learn?

- Understanding how WEP Cracking works and recovering secret WEP key
- The 4-way handshake and WPA-PSK passphrase cracking
- Unconventional attack to crack the passphrase

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:

- WEP Cracking
  In this lab, you will learn to use Aircrack-ng to crack a WiFi network with WEP security scheme using the packets present in a provided PCAP. A sufficient number of packets are present in the packet capture, so the WEP scheme can be cracked easily.

- WEP Cracking Advanced
  In this lab, you will learn to use Python script to crack a WiFi network with WEP security scheme using the packets present in a provided PCAP. A sufficient number of packets are not present in the packet capture, so the conventional cracking method of WEP cracking won't work. However, the dictionary attack can still be launched.

- WPA PSK Cracking
  In this lab, you will learn to use aircrack-ng to launch a dictionary attack and recover the secret passphrase for a WPA-PSK protected WiFi network. All information required to launch an attack (i.e. SSID, BSSID, client MAC, 4-way handshake) is present in the PCAP file.

- WPA2 PSK Cracking
  In this lab, you will learn to use aircrack-ng to launch a dictionary attack and recover the secret passphrase for a WPA2-PSK protected WiFi network. All information required to launch an attack (i.e. SSID, BSSID, client MAC, 4-way handshake) is present in the PCAP file.

- WPA2 PSK Cracking II
  In this lab, you will learn to use aircrack-ng to launch a dictionary attack and recover the secret passphrase for a WPA2-PSK protected WiFi network. All information required to launch an attack (i.e. SSID, BSSID, client MAC, 4-way handshake) is present in the PCAP file.

- WPA PSK Cracking III
  In this lab, you will learn to use aircrack-ng to launch a dictionary attack and recover the secret passphrase for a WPA-PSK protected WiFi network. However, the information required to launch the attack (i.e. SSID, BSSID, client MAC, handshake) is distributed in two PCAP files.