Namp
we perform host discovery
host discoveyr
2 user for network scan

1. root user
2. local user

1.root

ICMP Eco Request
TCP Syn-443
TCP ACk -80

2.Local
Syn 443
Ack -80

Syntax

nmap IP/Subet(CIDR) |Port Number|Scan Type|Scan Timing |Output Types

exmaple namp 192.168.2.1/24

Ip range Target

1.Single IP nmap 10.1.2.1
2.Subnet Range namp 192.168.2.1/24
3.Ip Range nmap 192.168.10.20-6
4.Specific IP 10.1.2.1 192.168.10.20 10.2.2.12
5.Text File nmap -iL iplist.txt
6.Domain nmap facebook.com

port number

example nmap 10.1.2.1 -p

Scan Method
1.Single port scan method
nmap 10.0.2.1 -p[portnumber]

2.seq prot

```
   nmap 10.0.2.1 -p[10-50]
```

3.Distrubuted only

```
    nmap 10.0.2.1 -p80,22,21,8080
```

4.service specific

```
    nmap 10.0.2.1 -p[servicename]
```

5.protocol specific

```
  nmap 10.0.2.1 -p T:53
```

6.all port

```
 nmap 10.0.2.1 -p-
```

scan Type/Tech
TCP Connect scan-ST
TCP syn scan -ss
Fin scan-sf
xmas scan- sx
null scan -sn
ping scan-sp
udp scan-su
ack scan- sa

x -> y 22 port

Scan Status

1.Open
2.Close
3.Filtered
4.open|Filtered
5.Close|Filtered
6.Unfiltered