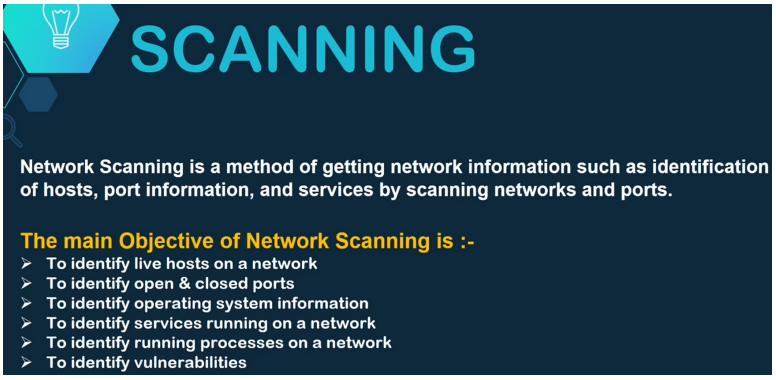
Network Scanning Complete

- `SCANNING`
- `TCP COMMUNICATION`
- `SCANNING TECHNIQUES`
- `WIRESHARK`
- `SCANNING TOOLS`
- `EVASION TECHNIQUES`
- `NMAP SCRIPTING`

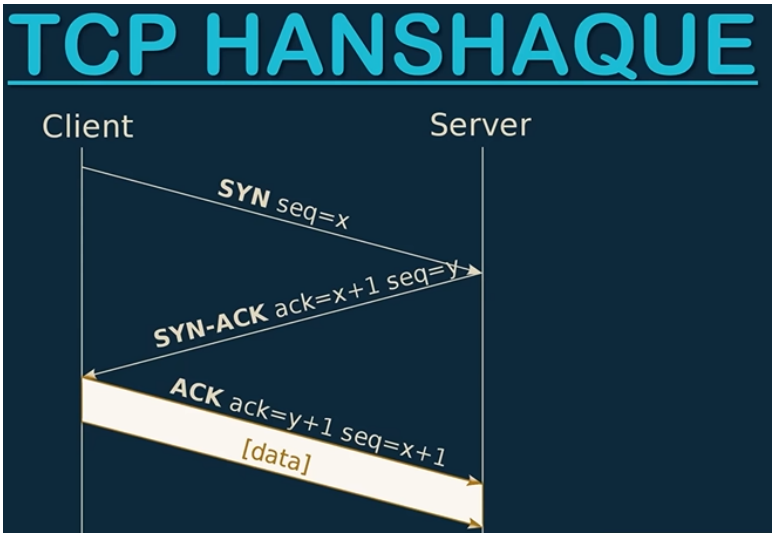


TCP and UDP

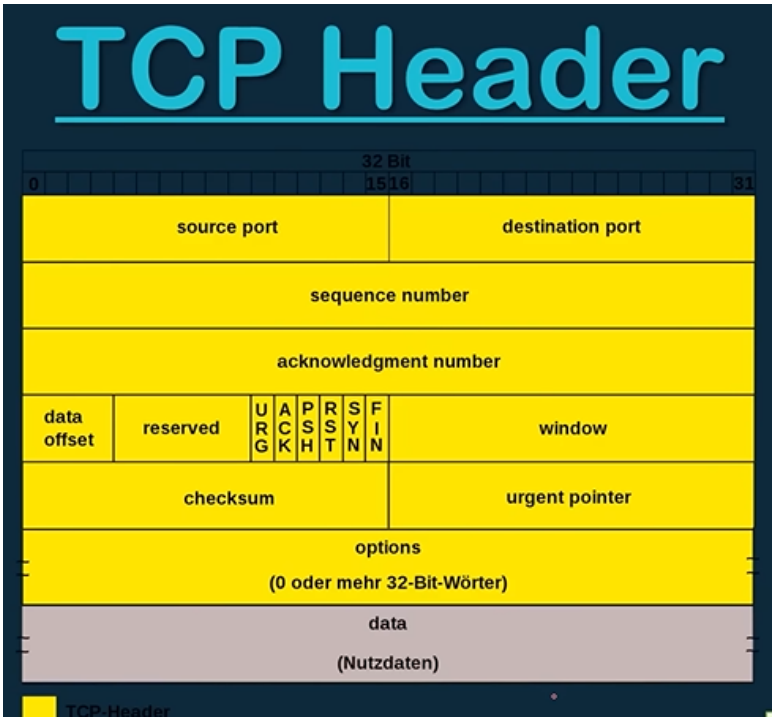
- **TCP** - Transmission Control Protocol
- **UDP** - User Datagram Protocol

TCP is connection oriented – once a connection is established, data can be sent bidirectional.
UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using **UDP**.

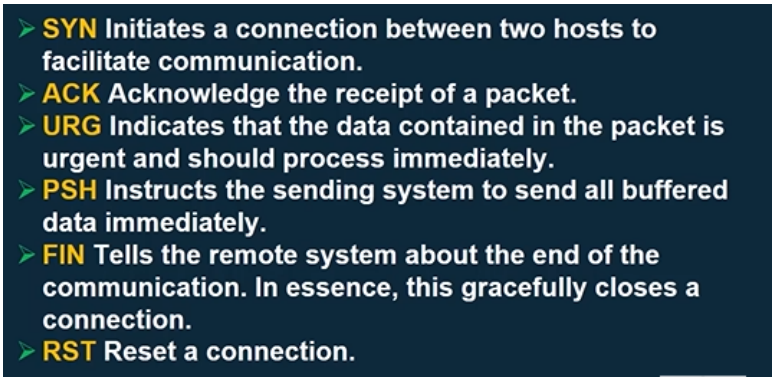
TCP HANSHAQUE



TCP Header



TCP FLAGS



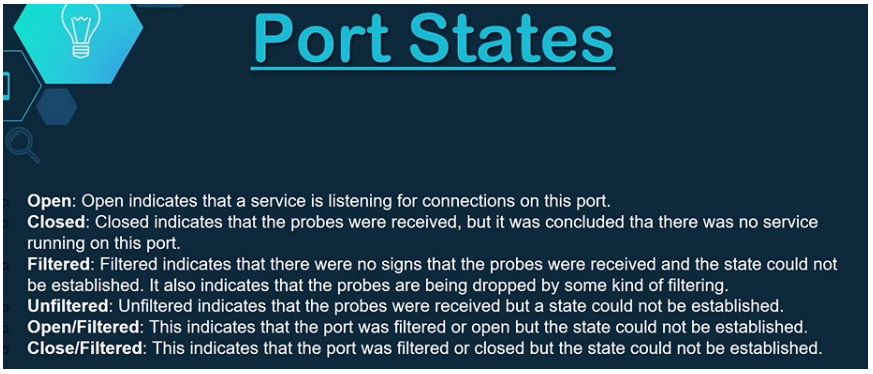

```
First Rule check the connection on/off Target


┌──(hacking㉿windows)-[~]
└─$ ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=64 time=10.7 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=64 time=4.33 ms
^C
--- 192.168.1.102 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002m
rtt min/avg/max/mdev = 4.332/7.517/10.702/3.185 ms


┌──(root㉿windows)-[/home/hacking]          #check through nma
└─# nmap -sn 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 09:4
Nmap scan report for 192.168.1.102
Host is up (0.080s latency).
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

```
Firewall bypass check the host up/down
ARP ADDress = Address Resolution protocol

┌──(root㉿windows)-[/home/hacking]
└─# arp -e
Address                  HWtype  HWaddress           Flags Ma
```

```
_gateway                 ether   0c:xxxxxxxxxxxxxx   C
192.168.1.102            ether   d8:xxxxxxxxxxxxxx   C


──(root㉿windows)-[/home/hacking]
└─# sudo nmap -sn 192.168.1.101 -PR
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 09:4
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

```
# check the (Hub) pass packet point to point - using Tracerua

──(root㉿windows)-[/home/hacking]
└─# nmap -sn --traceroute google.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 09:5
Nmap scan report for google.com (142.250.183.142)
Host is up (0.071s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:
rDNS record for 142.250.183.142: bom07s31-in-f14.1e100.net

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   3.51 ms  192.168.1.1
2   4.56 ms  192.168.0.1
3   44.34 ms 106.208.190.65
4   ... 6
7   67.82 ms 72.14.213.254
8   65.36 ms 216.239.47.175
9   64.74 ms 142.250.214.113
10  61.18 ms bom07s31-in-f14.1e100.net (142.250.183.142)

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds


# DNS Address change / DNS Resolution on/off

──(root㉿windows)-[/home/hacking]
```

```
└─# nmap google.com --dns-server 1.1.1.1


──(root㉿windows)-[/home/hacking]
└─# nmap -n facebook.com          # name Resolution cut in th

──(root㉿windows)-[/home/hacking]
└─# nmap -Pn facebook.com         # ping scan off
```




```
# port scan 80 -http

──(root㉿windows)-[/home/hacking]
└─# nmap -p 80 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:0
Nmap scan report for 192.168.1.102
Host is up (0.099s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 21 192.168.1.102
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:0
Nmap scan report for 192.168.1.102
Host is up (0.12s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
-------------------------------------------------------------
 # multiple port scan
┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 21,80,22 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:0
Nmap scan report for 192.168.1.102
Host is up (0.045s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
22/tcp open   ssh
80/tcp open   http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
-------------------------------------------------------------
#   range scan
┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 1-1000 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:0
Nmap scan report for 192.168.1.102
Host is up (0.0065s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
-----------------------------------------------------------
 # All port scan 65535
┌──(root㉿windows)-[/home/hacking]
└─# nmap -p- 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:0
Nmap scan report for 192.168.1.102
Host is up (0.0047s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

```
# only TCP ports scan

──(root㉿windows)-[/home/hacking]
└─# nmap -sT 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:1
Nmap scan report for 192.168.1.102
Host is up (0.57s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)


# Only UDP port Scan

┌──(root㉿windows)-[/home/hacking]
└─# nmap -sU 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:1
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoin
```

```
UDP Scan Timing: About 7.27% done; ETC: 10:29 (0:13:37 remain
Nmap scan report for 192.168.1.102
Host is up (0.091s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
5353/udp open|filtered zeroconf
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 1093.56 second

Time tacking
```

```
# Scan IP address / Target Domain

──(root㉿windows)-[/home/hacking]
└─# nmap certifiedhacker.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:1
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.39s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 984 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
```

```
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
5432/tcp open  postgresql
Nmap done: 1 IP address (1 host up) scanned in 5.18 seconds

# multiple ip address scan
┌──(root㉿windows)-[/home/hacking]
└─# nmap 192.168.1.102,130,131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:2
Nmap scan report for 192.168.1.102
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Nmap done: 3 IP addresses (1 host up) scanned in 2.35 seconds

# range ip address scan

┌──(root㉿windows)-[/home/hacking]
└─# nmap 192.168.1.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:2
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 0C:xxxxxxxxxxxxx (D-Link International)

Nmap scan report for 192.168.1.100
Host is up (0.00075s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states
Not shown: 1000 filtered tcp ports (no-response)
```

```
MAC Address: 34:xxxxxxxxxxxxxx (AzureWave Technology)

Nmap scan report for 192.168.1.102
Host is up (0.010s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap scan report for 192.168.1.101
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (4 hosts up) scanned in 7.44 seco


# List of Host and ip address

┌──(root㉿windows)-[/home/hacking]
└─# nmap -iL iplist.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:3
Nmap scan report for 192.168.1.102
Host is up (0.0092s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap scan report for 192.168.1.1
Host is up (0.0043s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
```

```
MAC Address: 0C:xxxxxxxxxxxxxx (D-Link International)

Nmap scan report for 192.168.0.1
Host is up (0.013s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 3 IP addresses (3 hosts up) scanned in 1.23 second

# All ip address scan in ex... in the internet (Not scan this

──(root㉿windows)-[/home/hacking]
└─# nmap -iR
```

```
# Protocol scan like ssh,telnet,smpt etc

┌──(root㉿windows)-[/home/hacking]
└─# nmap -p ssh 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:3
Nmap scan report for 192.168.1.102
Host is up (0.092s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

```
# Change enterface Eth0/Wlan0

──(root㉿windows)-[/home/hacking]
└─# nmap -e eth0 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:3
Nmap scan report for 192.168.1.102
Host is up (0.0079s latency).
```

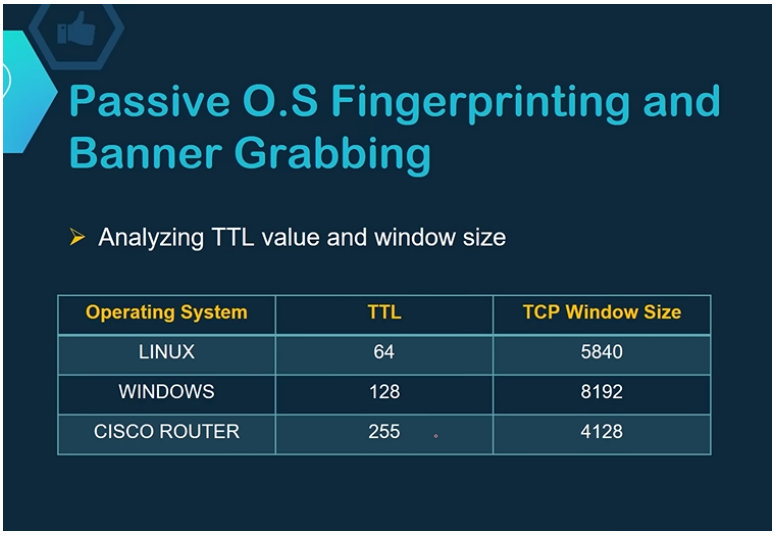
```
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

```
# Versions scan

──(root㉿windows)-[/home/hacking]
└─# nmap -sV 192.168.1.102 -p 22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:3
Nmap scan report for 192.168.1.102
Host is up (0.092s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Debian 3 (protocol 2.0)
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect resu
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds

──(root㉿windows)-[/home/hacking]
└─# nmap -sV 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:3
Nmap scan report for 192.168.1.102
Host is up (0.0045s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
22/tcp open  ssh        OpenSSH 9.6p1 Debian 3 (protocol 2.0)
53/tcp open  tcpwrapped
80/tcp open  http       Apache httpd 2.4.58 ((Debian))
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect resu
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds

------------------------------------------------------------
──(root㉿windows)-[/home/hacking]
└─# nmap -sV --version-intensity 9 -p 22 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:4
Nmap scan report for 192.168.1.102
Host is up (0.047s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Debian 3 (protocol 2.0)
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect resu
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

```
# operating system Ditect

──(root㉿windows)-[/home/hacking]
└─# nmap -O 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:4
Nmap scan report for 192.168.1.102
Host is up (0.0080s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Device type: phone
Running: Google Android 5.X|6.X|7.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:
/o:google:android:7 cpe:/o:linux:linux_kernel:3
```

```
OS details: Android 5.0 - 7.0 (Linux 3.4 - 3.10)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results a
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds

┌──(root㉿windows)-[/home/hacking]
└─# nmap -O --osscan-guess 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 10:4
Nmap scan report for 192.168.1.102
Host is up (0.0074s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)
Device type: phone
Running: Google Android 5.X|6.X|7.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6
cpe:/o:google:android:7 cpe:/o:linux:linux_kernel:3
OS details: Android 5.0 - 7.0 (Linux 3.4 - 3.10)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 2.02 seconds
```




```
# TTL value analyst to find the OS running in the Target mach

──(root㉿windows)-[/home/hacking]
└─# ping 192.168.0.76
PING 192.168.0.76 (192.168.0.76) 56(84) bytes of data.
64 bytes from 192.168.0.76: icmp_seq=1 ttl=64 time=77.1 ms
64 bytes from 192.168.0.76: icmp_seq=2 ttl=64 time=89.8 ms
^C
--- 192.168.0.76 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003m
rtt min/avg/max/mdev = 77.067/83.439/89.811/6.372 ms

TTL VALUE = 64 = Linux
TTL VALUE = 60 aprox = MAC apple
------------------------------------------------------------

──(root㉿windows)-[/home/hacking]
└─# ping 192.168.0.76

PING 192.168.0.76 (192.168.0.76) 56(84) bytes of data.
64 bytes from 192.168.0.76: icmp_seq=1 ttl=128 time=176 ms
64 bytes from 192.168.0.76: icmp_seq=2 ttl=128 time=120 ms

TTL VALUE = 128 = windows Running
```

```
------------------------------------------------------------
```

```
# IPv6 Scan

──(root㉿windows)-[/home/hacking]
└─# nmap -6 41526615516617
```

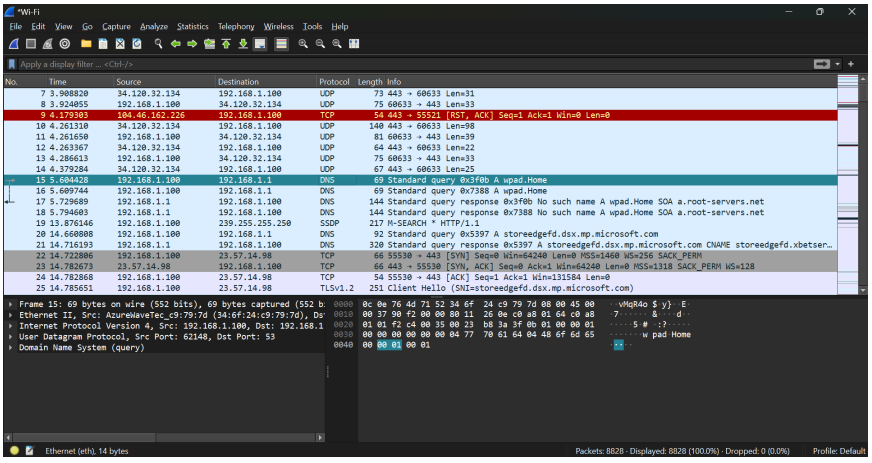
```
# aggressive Scan
Nmap has a special flag to activate aggressive detection, nam
Aggressive mode enables OS detection ( -O ), version detectio
script scanning ( -sC ), and traceroute ( --traceroute ).

──(root㉿windows)-[/home/hacking]
└─# nmap -A 192.168.0.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:3
Nmap scan report for 192.168.0.76
Host is up (0.014s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
22/tcp open  ssh        OpenSSH 9.6p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
|   256 f6:9c:d1:0f:4a:f5:79:bd:8a:c5:00:21:ed:9d:6a:56 (ECDS
|_  256 c4:69:86:59:8d:32:2f:e2:ff:ec:8d:c9:95:54:f1:dd (ED25
53/tcp open  tcpwrapped
80/tcp open  http       Apache httpd 2.4.58 ((Debian))
|_http-server-header: Apache/2.4.58 (Debian)
|_http-title: Log in to WifiLock using your Google Facebook Tw
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Device type: phone
Running: Google Android 5.X|6.X|7.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6
cpe:/o:google:android:7 cpe:/o:linux:linux_kernel:3
OS details: Android 5.0 - 7.0 (Linux 3.4 - 3.10)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   14.17 ms 192.168.0.76

OS and Service detection performed. Please report any incorre
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.48 seconds
```

```
Security Devices in Network Like
Firewall -
IDS - intrusion detection system
IPS - intrusion prevention system
Antvires-

Security Devices Bypass
# Firewall off
──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.0.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:4
Nmap scan report for 192.168.0.76
Host is up (0.17s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds

# Firewall bypass Not -Pn
──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.0.51 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:4
Nmap scan report for LAPTOP-HIT6CD6V (192.168.0.51)
Host is up (0.080s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 34:xxxxxxxxxxxxx (AzureWave Technology)
```

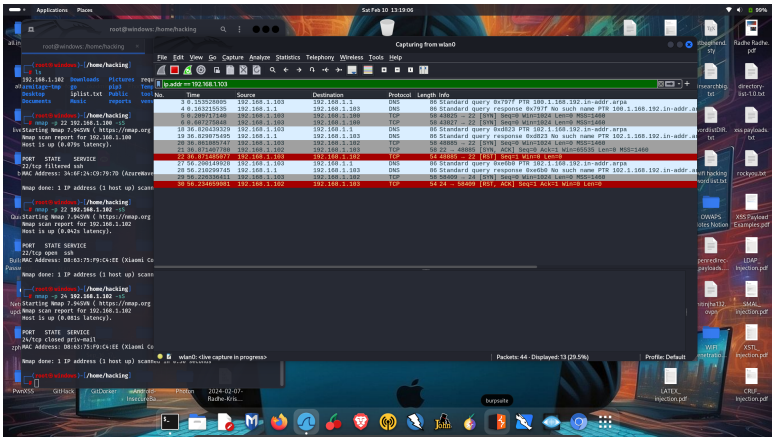
```
Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
```

```
Wireshark

Source Ip ---------->>>  Destination
- Capture options
- save file open
- save the capture file
- deleted options
- Reload options
- Find the packet
```

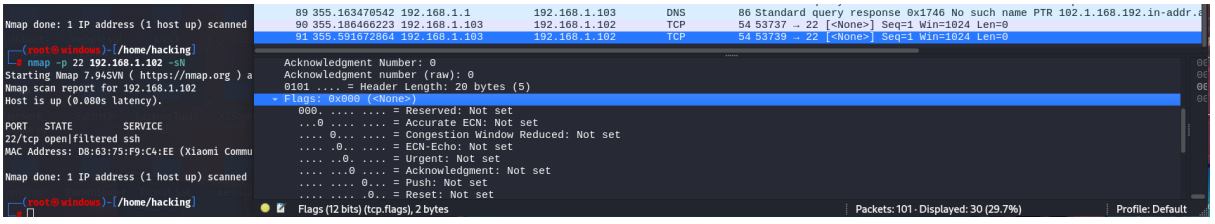



```
Port Open or Not check with Wireshark

┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.1.100 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:1
Nmap scan report for 192.168.1.100
Host is up (0.079s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 34:xxxxxxxxxxxxxx (AzureWave Technology)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
------------------------------------------------------------
┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.1.102 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:1
Nmap scan report for 192.168.1.102
Host is up (0.042s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
------------------------------------------------------------
┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 24 192.168.1.102 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:1
Nmap scan report for 192.168.1.102
Host is up (0.081s latency).

PORT   STATE  SERVICE
24/tcp closed priv-mail
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

┌──(root㉿windows)-[/home/hacking]


See the packet send and R... Wireshark
```

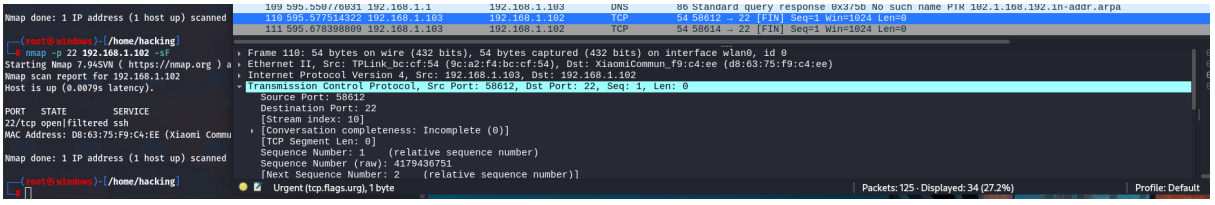


```
NUL scan

┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.1.102 -sN
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:2
Nmap scan report for 192.168.1.102
Host is up (0.080s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```




```
FIN SCAN
┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.1.102 -sF
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:2
Nmap scan report for 192.168.1.102
Host is up (0.0079s latency).
```

```
PORT   STATE          SERVICE
22/tcp open|filtered ssh
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```



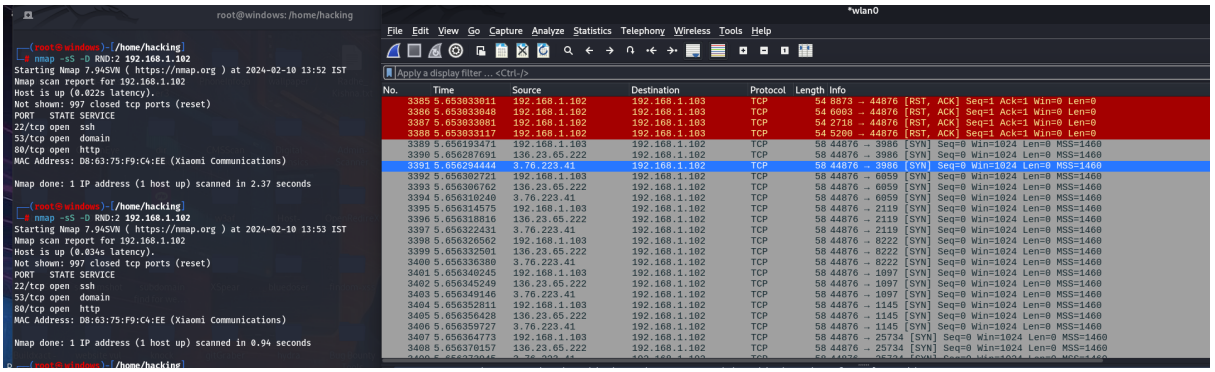

```
Timing and Performance scan NMap
(0-5)

──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 192.168.1.102 -T2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:4
Nmap scan report for 192.168.1.102
Host is up (0.099s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds

┌──(root㉿windows)-[/home/hacking]
└─# nmap 192.168.1.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:4
Nmap scan report for 192.168.1.102
Host is up (0.022s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

```
Mac address spoofing

┌──(root㉿windows)-[/home/hacking]
└─# nmap --spoof-mac 0 -p 22 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:4
Spoofing MAC address 6B:46:E7:E7:C3:72 (No registered vendor)
Nmap scan report for 192.168.1.102
Host is up (0.011s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

# nmap --spoof-mac dell -p 22 192.168.1.102
```

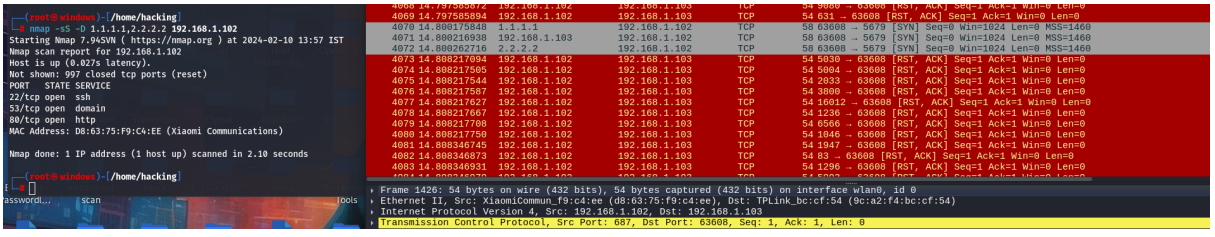
```
decoy scan nmap
you can use the IP address decoy technique to avoid detection

──(root㉿windows)-[/home/hacking]
└─# nmap -sS -D RND:2 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:5
Nmap scan report for 192.168.1.102
Host is up (0.034s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

See the packet the wireshark the diffirent ip

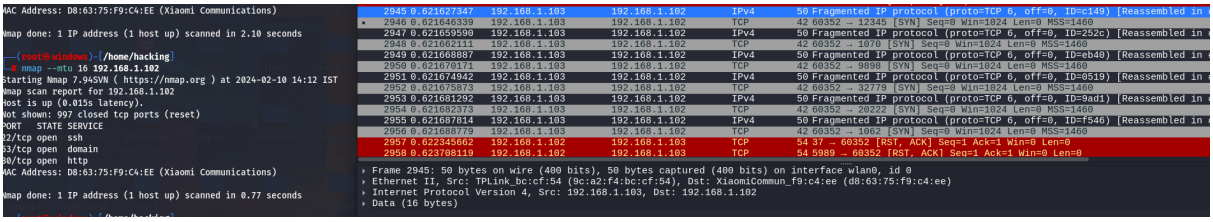


Set IP any

```
┌──(root㉿windows)-[/home/hacking]
└─# nmap -sS -D 1.1.1.1,2.2.2.2 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:5
Nmap scan report for 192.168.1.102
Host is up (0.027s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

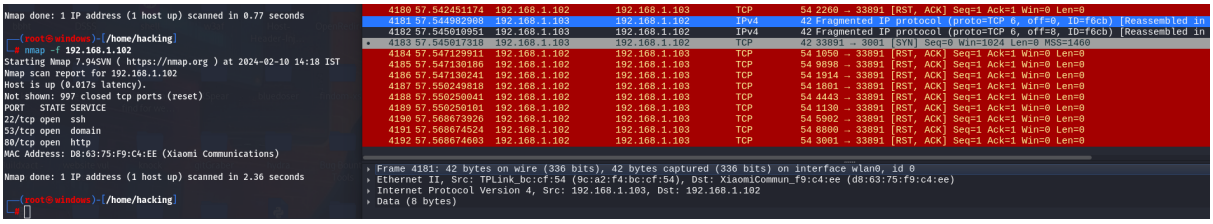


```
MTU - nmap mtu scan send crafted mtu size (8*)

──(root㉿windows)-[/home/hacking]
└─# nmap --mtu 16 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 14:1
Nmap scan report for 192.168.1.102
Host is up (0.015s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

See Wireshark
```




```
size def… 8

┌──(root㉿windows)-[/home/hacking]
└─# nmap -f 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 14:1
Nmap scan report for 192.168.1.102
Host is up (0.017s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxxx (Xiaomi Communications)
```

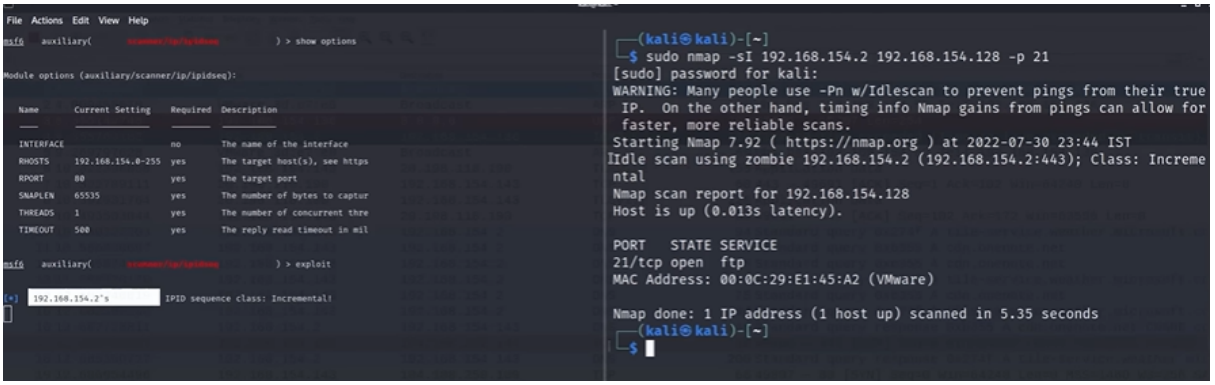
```
Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds


see the wireshark
Idle Zombie Scan Nmap:
```



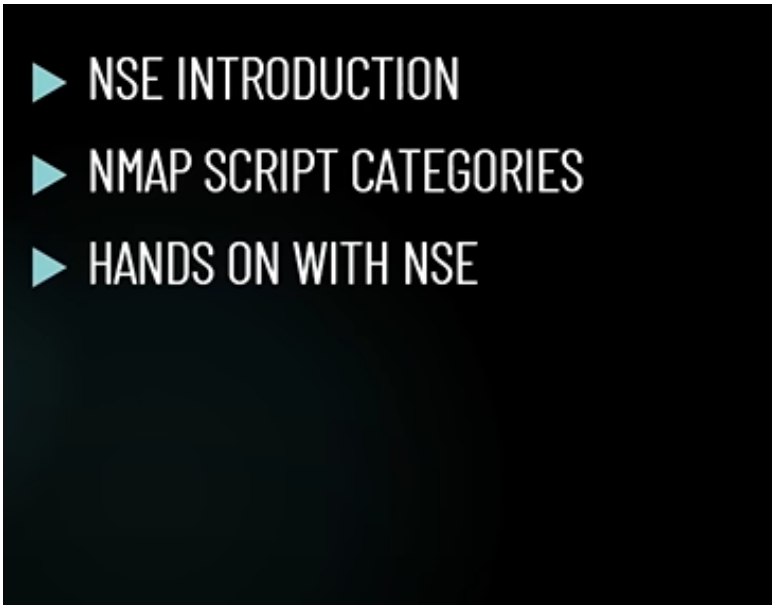

```
Zombie Scan Before find the vulnb... machine in the network u

msf6 > search idle ip

Matching Modules
================

   #  Name                              Disclosure Date  Rank    
   -  ----                              ---------------  ----    
   0  auxiliary/scanner/ip/ipidseq                       normal  


Interact with a module by name or index. For example info 0,
use auxiliary/scanner/ip/ipidseq

msf6 > use 0
msf6 auxiliary(scanner/ip/ipidseq) > show options

Module options (auxiliary/scanner/ip/ipidseq):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the inte
   RHOSTS                      yes       The target host(s),
   RPORT      80               yes       The target port
```

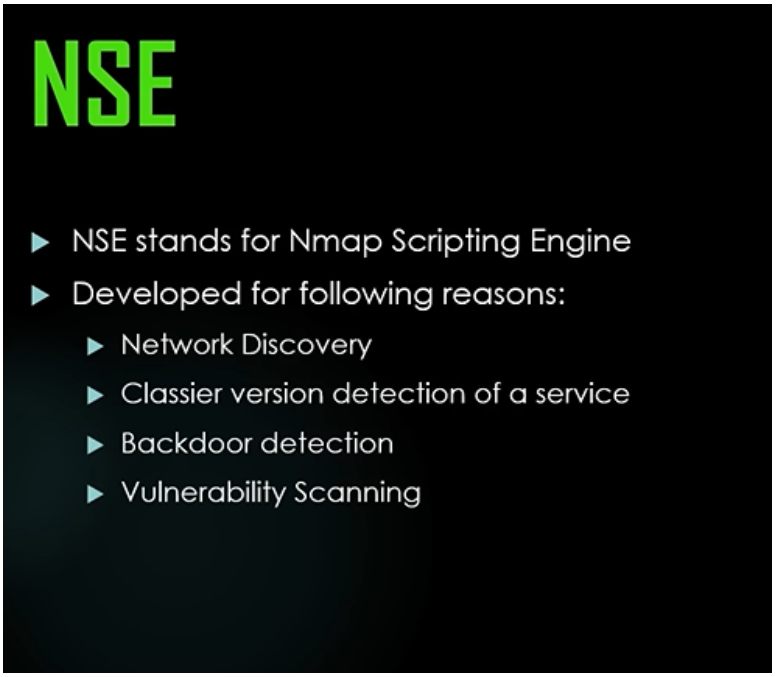
```
   SNAPLEN    65535            yes       The number of bytes
   THREADS    1                yes       The number of concur
   TIMEOUT    500              yes       The reply read timeo


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ip/ipidseq) > set rhosts 192.168.1.0-2
rhosts => 192.168.1.0-255
msf6 auxiliary(scanner/ip/ipidseq) > exploit

[*] 192.168.1.1's IPID sequence class: All zeros
[*] Error: 192.168.1.4: Timeout::ExitException execution expi
[*] Error: 192.168.1.9: Timeout::ExitException execution expi
[*] Error: 192.168.1.10: Timeout::ExitException execution exp
[*] Error: 192.168.1.11: Timeout::ExitException execution exp
[*] Error: 192.168.1.14: Timeout::ExitException execution exp
[*] Error: 192.168.1.17: Timeout::ExitException execution exp
[*] Error: 192.168.1.20: Timeout::ExitException execution exp
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

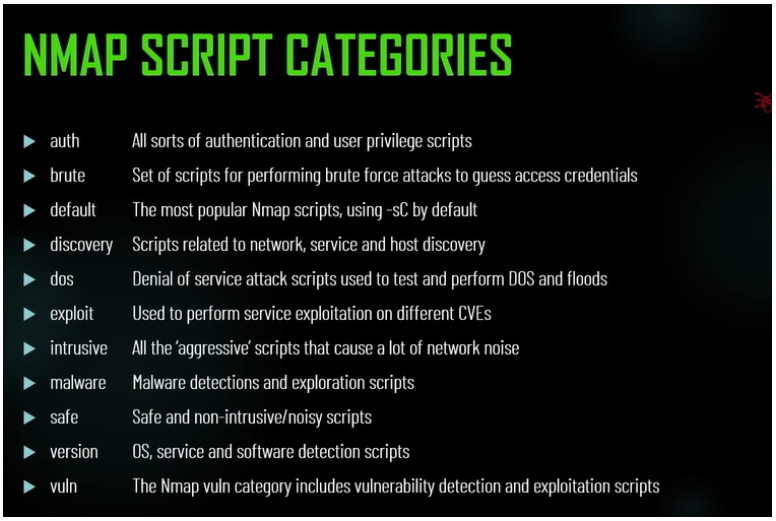
```
Zombie Scan
┌──(root㉿windows)-[/home/hacking]
└─# nmap -SI 192.168.1.1 192.168.1.102 -p 22
```



```
Source port Spoof

┌──(root㉿windows)-[/home/hacking]
└─# nmap --source-port 53 192.168.1.102 -p 22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 14:4
Nmap scan report for 192.168.1.102
Host is up (0.049s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```







Script locate path

```
┌──(root㉿windows)-[/home/hacking]
└─# ls /usr/share/nmap/scripts
acarsd-info.nse                         ip-geolocation-ipinfo
address-info.nse                        ip-geolocation-map-bi
afp-brute.nse                           ip-geolocation-map-go
afp-ls.nse                              ip-geolocation-map-km
afp-path-vuln.nse                       ip-geolocation-maxmin
afp-serverinfo.nse                      ip-https-discover.nse
```

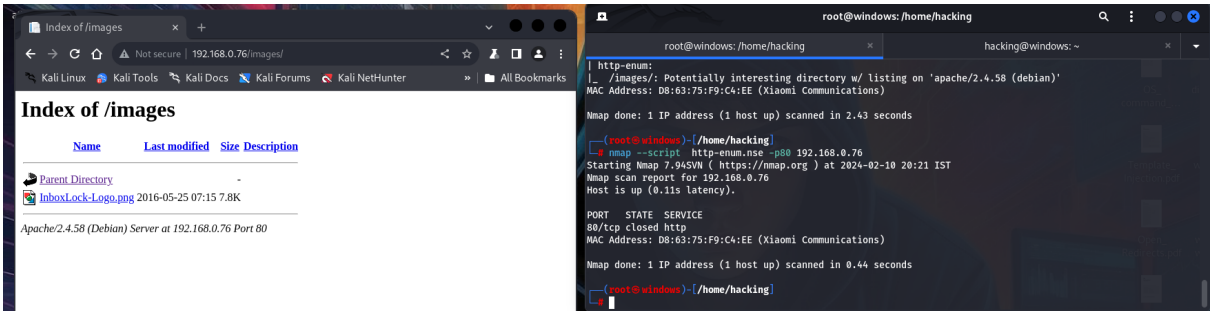
```
afp-showmount.nse                           ipidseq.nse
ajp-auth.nse                                ipmi-brute.nse
ajp-brute.nse                               ipmi-cipher-zero.nse
ajp-headers.nse                             ipmi-version.nse
.....................................................
.....................................................

┌──(root㉿windows)-[/home/hacking]
└─# sudo nmap --script-updatedb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 19:4
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.68 second


Find script
┌──(root㉿windows)-[/home/hacking]
└─# ls /usr/share/nmap/scripts | grep ssh
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse
```

```
Script use

──(root㉿windows)-[/home/hacking]
└─# nmap --script ssh-auth-methods.nse 192.168.0.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 20:0
Nmap scan report for 192.168.0.76
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
```

```
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds


┌──(root㉿windows)-[/home/hacking]
└─# nmap -p 22 --script ssh-auth-methods --script-args=root  1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 20:0
Nmap scan report for 192.168.0.76
Host is up (0.21s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

```
Directory find in the website using nse script
──(root㉿windows)-[/home/hacking]
└─# ls /usr/share/nmap/scripts | grep http

┌──(root㉿windows)-[/home/hacking]
└─# nmap --script http-enum.nse 192.168.0.76 -p80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 20:1
Nmap scan report for 192.168.0.76
Host is up (0.18s latency).

PORT   STATE SERVICE
```

```
80/tcp open  http
| http-enum:
|_  /images/: Potentially interesting directory w/ listing on
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds
```




```
Find the Email address and subdomain in the website -> http-g
This nse script run sudo/without sudo see the result both
┌──(root㉿windows)-[/home/hacking]
└─# nmap --script  http-grep.nse -p80 192.168.0.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 20:5
Nmap scan report for 192.168.0.76
Host is up (0.15s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

xyz@admin.com
tsghs@gsj.com
hsudgb@hdjdb.com

Nmap done: 1 IP address (1 host up) scanned in 16.40 seconds
```

```
Password crack ssh, telnet, FTP like
──(root㉿windows)-[/home/hacking]
└─# ls /usr/share/nmap/scripts | grep ftp
```

```
┌──(root㉿windows)-[/home/hacking]
└─# nmap --script ftp-brute.nse -p21 192.168.1.101 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 15:0
```

```
Check anon Login
──(hacking㉿windows)-[~]
└─$ nmap --script ftp-anon.nse -p21 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 15:3
Nmap scan report for 192.168.1.101
Host is up (0.0076s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 500 OOPS: socket

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

```
Multiple script run like Discovery all script run
Category = Discovery

┌──(root㉿windows)-[/home/hacking]
└─# nmap --script discovery 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 15:1
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to change
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-igmp-discovery:
|   192.168.1.1
|     Interface: wlan0
|     Version: 2
|     Group: 224.0.1.178
|     Description: IEEE IAPP
|   192.168.1.1
```

```
|     Interface: wlan0
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targe
| targets-ipv6-multicast-mld:
|   IP: fe80::a791:b4a2:942c:5eeb  MAC: 34:6f:24:c9:79:7d  IF
|   IP: fe80::da63:75ff:fef9:c4ee  MAC: d8:63:75:f9:c4:ee  IF
|   IP: fe80::e0e:76ff:fe4d:7152   MAC: 0c:0e:76:4d:71:52  IF
|
|_  Use --script-args=newtargets to add the results as target
| ipv6-multicast-mld-list:
|   fe80::da63:75ff:fef9:c4ee:
|     device: wlan0
|     mac: d8:63:75:f9:c4:ee
|     multicast_ips:
|       ff02::1:fff9:c4ee         (NDP Solicited-node)
|       ff02::1:ff29:e13e         (Solicited-Node Address)
|       ff02::1:ff29:e13e         (Solicited-Node Address)
|   fe80::e0e:76ff:fe4d:7152:
|     device: wlan0
|     mac: 0c:0e:76:4d:71:52
|     multicast_ips:
|       ff02::1:ff4d:7152         (NDP Solicited-node)
|   fe80::a791:b4a2:942c:5eeb:
|     device: wlan0
|     mac: 34:6f:24:c9:79:7d
|     multicast_ips:
|       ff02::1:ff2c:5eeb         (NDP Solicited-node)
|       ff02::1:ffe7:e443         (Solicited-Node Address)
|       ff02::1:ff26:294d         (Solicited-Node Address)
|       ff02::1:ffe7:e443         (Solicited-Node Address)
|_      ff02::1:ff26:294d         (Solicited-Node Address)
| targets-ipv6-multicast-invalid-dst:
|   IP: fe80::e0e:76ff:fe4d:7152   MAC: 0c:0e:76:4d:71:52  IF
|   IP: fe80::da63:75ff:fef9:c4ee  MAC: d8:63:75:f9:c4:ee  IF
|_  Use --script-args=newtargets to add the results as target
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Ro
```

```
| targets-ipv6-multicast-echo:
|   IP: fe80::e0e:76ff:fe4d:7152   MAC: 0c:0e:76:4d:71:52  IF
|   IP: fe80::da63:75ff:fef9:c4ee  MAC: d8:63:75:f9:c4:ee  IF
|_  Use --script-args=newtargets to add the results as target
Nmap scan report for 192.168.1.101
Host is up (0.018s latency).
Not shown: 996 closed tcp ports (reset)
Bug in http-security-headers: no string output.
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (12)
|   server_host_key_algorithms: (4)
|   encryption_algorithms: (6)
|   mac_algorithms: (10)
|_  compression_algorithms: (2)
| ssh-hostkey:
|   256 f6:9c:d1:0f:4a:f5:79:bd:8a:c5:00:21:ed:9d:6a:56 (ECDS
|_  256 c4:69:86:59:8d:32:2f:e2:ff:ec:8d:c9:95:54:f1:dd (ED25
|_banner: SSH-2.0-OpenSSH_9.6p1 Debian-3
53/tcp open  domain
|_dns-nsec3-enum: Can't determine domain for host 192.168.1.1
|_dns-nsec-enum: Can't determine domain for host 192.168.1.10
80/tcp open  http
|_http-chrono: Request times for /; avg: 297.88ms; min: 232.8
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 127.0.0.1
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; h

.....................................................
.....................................................
.....................................................
.....................................................
```

```
Telnet all script Run

┌──(root㉿windows)-[/home/hacking]
└─# nmap --script telnet* 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 15:3
Nmap scan report for 192.168.1.101
Host is up (0.020s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

```
wordpress plugins theams version Find
──(root㉿windows)-[/home/hacking]
└─# ls /usr/share/nmap/scripts | grep wordpress
http-wordpress-brute.nse
http-wordpress-enum.nse
http-wordpress-users.nse
```

```
Find SQL vuln URL in the Target
──(root㉿windows)-[/home/hacking]
└─# ls /usr/share/nmap/scripts | grep sql

──(root㉿windows)-[/home/hacking]
└─# nmap --script http-sql-injection.nse -p 80 testphp.vulnwe
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 15:4
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
```

```
Host is up (0.31s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.comp

PORT   STATE SERVICE
80/tcp open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://testphp.vulnweb.com:80/search.php?test=query%27%
|     http://testphp.vulnweb.com:80/search.php?test=query%27%
|     http://testphp.vulnweb.com:80/search.php?test=query%27%
|     http://testphp.vulnweb.com:80/search.php?test=query%27%
.............................................................
.............................................................
.............
```

```
Imp
Target website/ip check The cve vulnerability available
Vulscan Github load in script Database

┌──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap -sV --script=vulscan/vulscan.nse 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:0
Nmap scan report for 192.168.1.101
Host is up (0.016s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
21/tcp open  ftp?
| fingerprint-strings:
|   Help:
|_    421 There are too many connections from your internet a
22/tcp open  ssh        OpenSSH 9.6p1 Debian 3 (protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
-------------------------------------------------------------
-------------------------------------------------------------
-------------------------------------------------------------
```

https://github.com/scipag/vulscan

```
PHP version check on Target website

──(root㉿windows)-[/home/hacking/Desktop]
└─# ls /usr/share/nmap/scripts | grep php
http-cakephp-version.nse
http-phpmyadmin-dir-traversal.nse
http-phpself-xss.nse
http-php-version.nse

┌──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap --script http-php-version.nse -p 80 testphp.vulnweb.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:1
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.comp

PORT   STATE SERVICE
80/tcp open  http
|_http-php-version: Version from header x-powered-by: PHP/5.6
```

```
Vuln script = all vulnerability Acroding to This script

──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap --script vuln 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:1
Pre-scan script results:
| broadcast-avahi-dos:
```

```
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.101
Host is up (0.0072s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabiliti
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 127.0.0.1
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinho
|   Found the following indications of potential DOM based XS
-------------------------------------------------
-----------------------------------------------------
-----------------------------------------------------------
```

CVE -

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

https://cve.mitre.org/

```
All This types of script run *

┌──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap --script http-vuln* 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:2
Nmap scan report for 192.168.1.101
Host is up (0.019s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
```

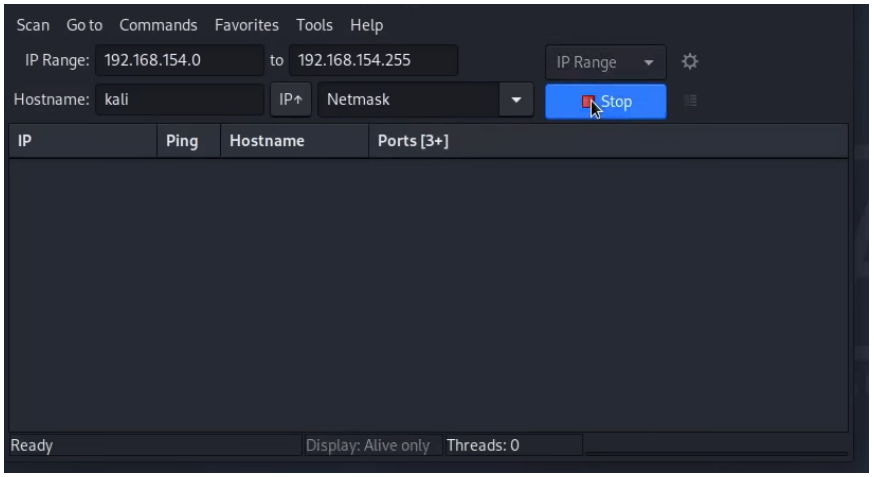
```
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)
```

```
Server location Find

──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap --script ip-geolocation-* facebook.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:2
NSE: [ip-geolocation-maxmind] You must specify a Maxmind data
NSE: [ip-geolocation-maxmind] Download the database from http
Nmap scan report for facebook.com (157.240.16.35)
Host is up (0.15s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f12
rDNS record for 157.240.16.35: edge-star-mini-shv-01-bom1.fac
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Host script results:
| ip-geolocation-geoplugin: coordinates: 19.0748, 72.8856
|_location: Maharashtra, India

Post-scan script results:
Bug in ip-geolocation-map-bing: no string output.
Bug in ip-geolocation-map-google: no string output.
Bug in ip-geolocation-map-kml: no string output.
Nmap done: 1 IP address (1 host up) scanned in 26.25 seconds
```

```
nmap script save report format
types - txt, xml

──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap -oN samplereport.txt 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:3
```

```
Nmap scan report for 192.168.1.101
Host is up (0.014s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

------------------------------------------------------------
Create report on xml formate


──(root㉿windows)-[/home/hacking/Desktop]
└─# nmap -oX report 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-11 16:4
Nmap scan report for 192.168.1.101
Host is up (0.021s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D8:xxxxxxxxxxxxx (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

```
Angry ip scan

Add range and see all ip scan and see the machine

https://angryip.org/
```




```
Zmap
What is the difference between ZMap and Nmap?
Nmap: Nmap is widely used for network inventory,
vulnerability assessment, and penetration testing on smaller
ZMap: ZMap is designed for large-scale internet-wide scans, d
enabling the analysis of a significant portion of the interne
```

```
Solarwinds network mapper:
What is SolarWinds network topology mapper?
SolarWinds Network Topology Mapper (NTM) shows nodes on your
indicates and updates status both for the nodes and the netwo
scalable maps with customizable icons.
```

`RAHUL-Nj`