Nmap – tcp and port scanning

1. Open https://nmap.org/download.html, click on OS for which you want to download
2. Then install that downloaded exe file.

TCP Scanning

Run this command in linux/unix

Nmap –sT –p21 192.168.117.134

-s – scan

-T – tcp scan

-p21 – given port number 21

Then ip address – target machine

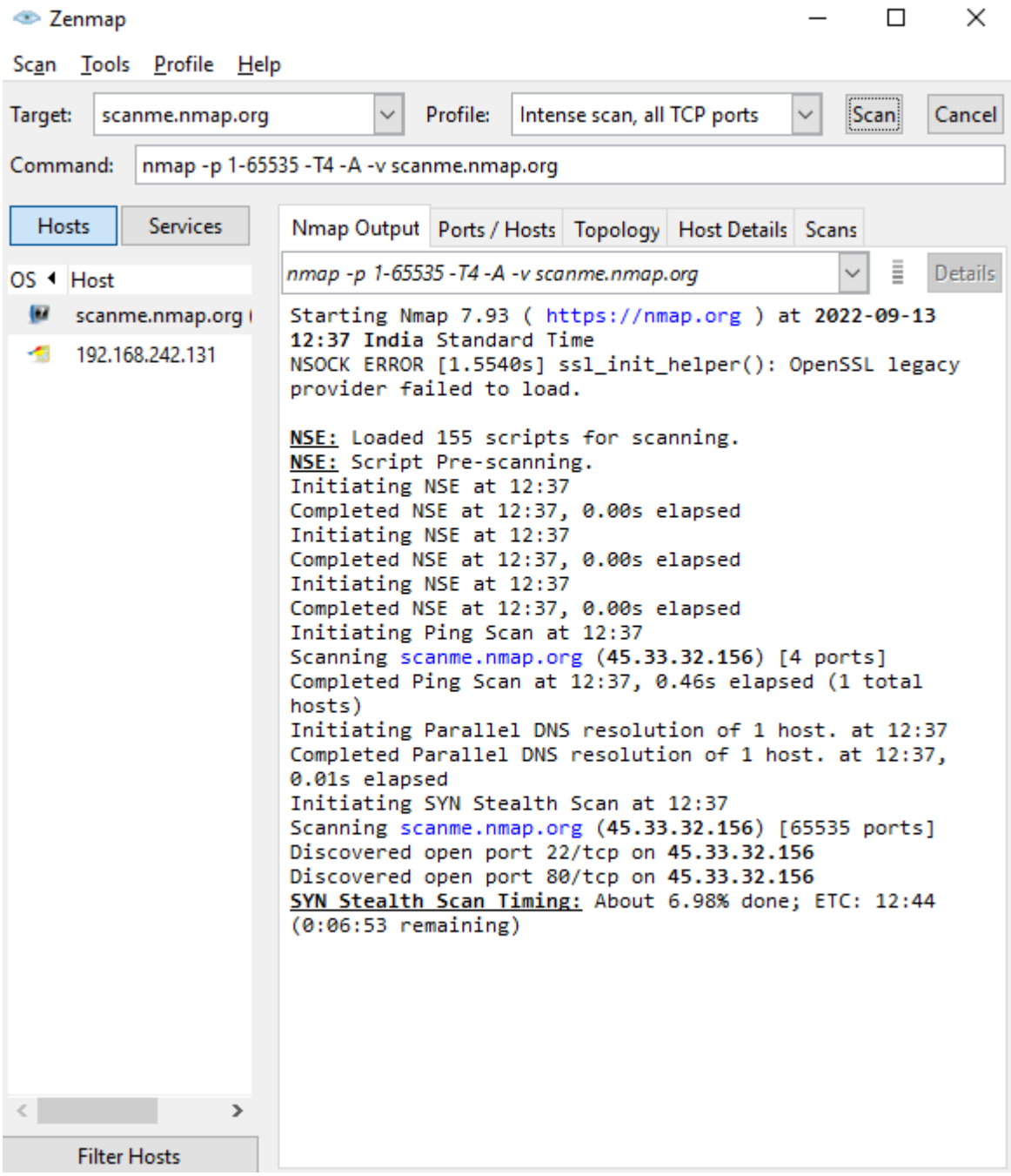
Output shows that port 21 is open and ftp service is running on that.

Now examine this in wireshark.

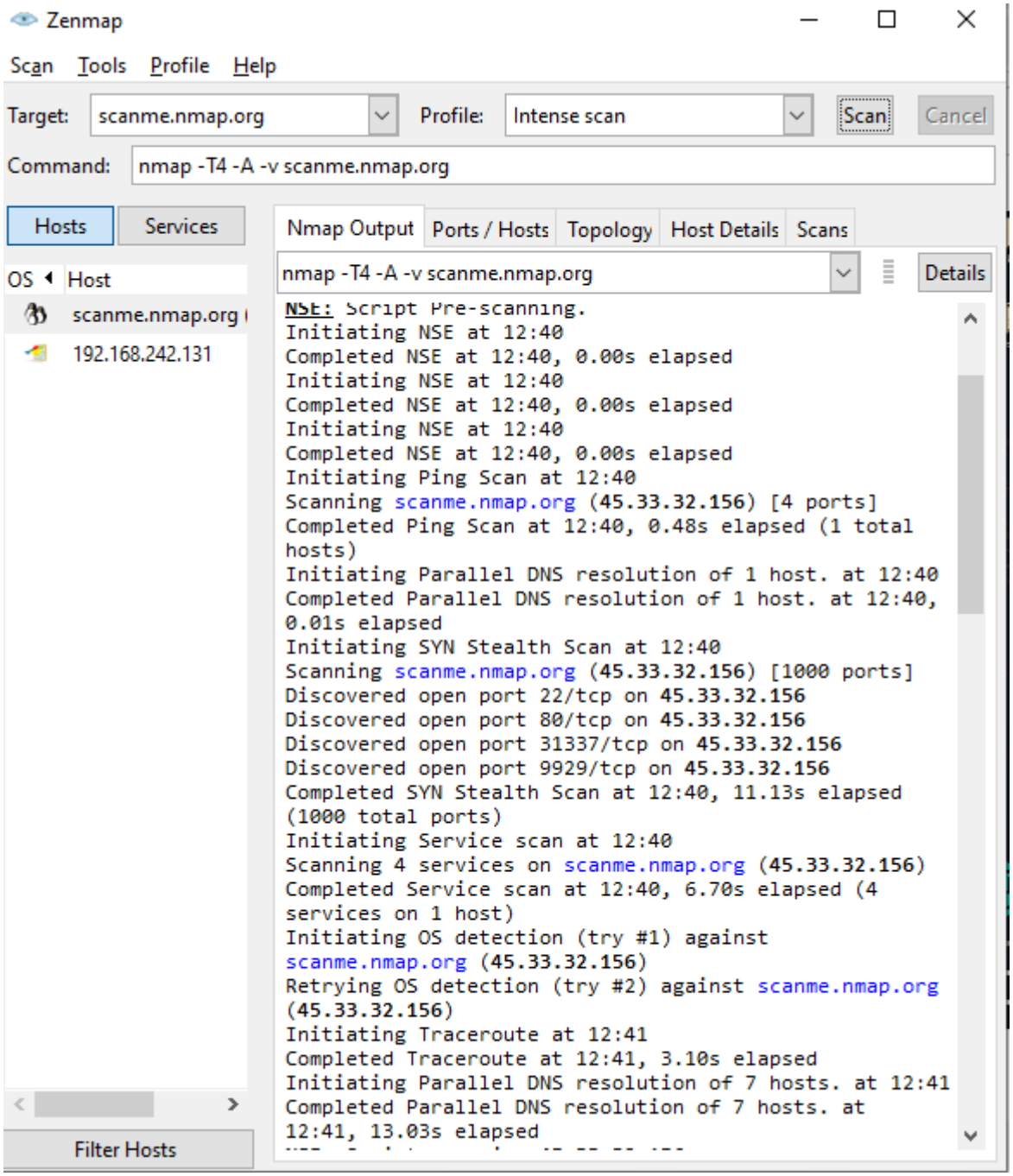
Open wireshark and then run this command again so we can see 3 way tcp handshake. So it is clear that someone is scanning my system. Some one is performing port scanning so we should block it.

https://www.youtube.com/watch?v=pytnN9YBTdU

tcp scan on scanme.nmap.org



Intense scans



Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

192.168.242.131

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v scanme.nmap.org Details

```
Initiating NSE at 12:41
Completed NSE at 12:41, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu
2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac00a01a82ffcc5599dc672b34976b75 (DSA)
|   2048 203d2d44622ab05a9db5b30514c2a6b2 (RSA)
|   256 9602bb5e57541c4e452f564c4a24b257 (ECDSA)
|_  256 33fa910fe0e17b1f6d05a2b0f1544156 (ED25519)
80/tcp    open     http         Apache httpd 2.4.7
((Ubuntu))
|_http-title: Go ahead and ScanMe!
|_http-favicon: Nmap Project
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.7 (Ubuntu)
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Device type: general purpose
Running (JUST GUESSING): Linux 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:5.0
Aggressive OS guesses: Linux 5.0 (91%), Linux 5.0 -
5.4 (86%)
No exact OS matches for host (test conditions non-
ideal).
Uptime guess: 49.663 days (since Mon Jul 25 20:46:58
2022)
```

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

192.168.242.131

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v scanme.nmap.org Details

```
2022)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   7.00 ms   192.168.242.69
2   ... 3
4   31.00 ms  123.63.86.122
5   41.00 ms  182.19.106.200
6   ...
7   153.00 ms gtt-as3257-gw.mrx.cw.net (195.2.29.158)
8   291.00 ms ae3.cr5-sjc1.ip4.gtt.net (89.149.180.38)
9   287.00 ms ip4.gtt.net (208.116.213.134)
10  288.00 ms if-2-6.csw5-fnc1.linode.com
(173.230.159.71)
11  288.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 12:41
Completed NSE at 12:41, 0.00s elapsed
Initiating NSE at 12:41
Completed NSE at 12:41, 0.00s elapsed
Initiating NSE at 12:41
Completed NSE at 12:41, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 60.08
seconds
           Raw packets sent: 1165 (54.380KB) | Rcvd:
1111 (45.472KB)
```

Nmap with turmux

How to scan a Website with Nmap Termux :

To **scan a Website** you must have permissions Else it can cause you Trouble, Nmap allows you to Scan there Test website so, in this post, we will use that website, you just have to type Nmap and then the site name you can **paste the below command** in the termux **to scan the Nmap test website.**
nmap Scanme.nmap.org

```
$ nmap Scanme.nmap.org
```

Output :

You can see that we got an **IP-Adress of the website** in the second line as well as we can see the **latency is 0.24 Seconds.**and we can also **see all the open port of the website.**

```
$ nmap Scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 202
0-10-09 23:22 IST
Nmap scan report for Scanme.nmap.org (45.33.32
.156)
Host is up (0.24s latency).
Other addresses for Scanme.nmap.org (not scann
ed): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
50300/tcp filtered unknown

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

Scan your Local Network with Nmap Termux :

If You just wanna **scan your Local network (Your Intire subnet)**and **know How many devices are connected with your Wifi** then you can use this command. This command will give you a **list of all Devices in the network** as well as you **all the open ports** of those devices.
nmap 192.168.1.1/24

```
$ nmap 192.168.1.1/24
```

Output :

Now you can see in the below picture, **I have 2 devices in my network.** and you can also see **all the open ports**. The 192.168.1.202 **Host is up** and the **latency is 0.0025s.** If you have multiple devices on your network then it will show you a list of all the Devices.

```
$ nmap 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap
.org ) at 2020-10-09 23:24 IST
Nmap scan report for 192.168.1.1
Host is up (0.0088s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.1.20
2
Host is up (0.0094s latency).
All 1000 scanned ports on 192.168
.1.202 are closed

Nmap done: 256 IP addresses (2 ho
sts up) scanned in 12.79 seconds
```

Aggressive scan using Nmap Termux :

In the above Local Network scan, It won't show you detailed information but if you want to **see every possible detail** then you can use **-A argument in the command.** I am just gonna use the above command with -A argument.
nmap -A 192.168.1.1/24

```
$ nmap -A 192.168.1.1/24
```

Output :

Now you can see **Its showing iBall Baton I Login** as well as it is showing the **URL of the login page**. This is just my local network that's why you are unable to see anything interesting but if are scanning any website then it can surely give you some extra data.

```
$ nmap -A 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2
020-10-09 23:28 IST
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    GoAhead WebServer
| http-title: iBall Baton | LOGIN
|_Requested resource was http://192.168.1.1/
login.html

Nmap scan report for 192.168.1.202
Host is up (0.0042s latency).
All 1000 scanned ports on 192.168.1.202 are
closed

Service detection performed. Please report a
ny incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 256 IP addresses (2 hosts up) sca
nned in 21.53 seconds
```

Scan a Single port in Nmap Termux :

If you just wanna **scan a Single Port of a Particular Ip address** then you can do that using the below command. Here I am scanning the entire **network for the port 80** but you can put a single IP and it will work Perfectly. The advantage of scanning a single port is that it will **save you some extra time** especially when you are in a hurry.

nmap -p 80 192.168.1.1/24

```
$ nmap -p 80 192.168.1.1/24
```

Output :

Here you can see that Nmap is checking for **port 80 only** but on my entire network.

```
$ nmap -p 80 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org
 ) at 2020-10-09 23:29 IST
Nmap scan report for 192.168.1.1
Host is up (0.031s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.1.201
Host is up (0.15s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 192.168.1.202
Host is up (0.0014s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 256 IP addresses (3 hosts
up) scanned in 4.55 seconds
```

Scan Multiple Port in Nmap Termux :

Do you know most of the time when you scan a Network and you find a device with open port 80 as well as 443 then it means that its a **WebServer**? So In the below command, I am gonna scan these two ports on my network, of course, I don't have a webserver running in my home so it won't show 443 port but if you scan it in a network where they have a webserver then it will show with this command.

nmap -p 80,443 192.168.1.1/24

```
$ nmap -p 80,443 192.168.1.1/24
```

Output :

In the below picture you can clearly see that it is **only checking for 2 port** and as the output, we can see in my routers Ip address port 80 is open but port 443 is not. And in my second device, Both ports are closed.

```
$ nmap -p 80,443 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.or
g ) at 2020-10-09 23:30 IST
Nmap scan report for 192.168.1.1
Host is up (0.057s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 192.168.1.202
Host is up (0.0015s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 256 IP addresses (2 hosts
 up) scanned in 4.21 seconds
```

Ping A Website or an IP-Address with Nmap in Termux :

If you Quickly wanna Check if a **Host is still up or not** then you can **do a Ping.** It will tell you the amount of time it took the Nmap to make a connection with the website or the Device.

nmap -sP 192.168.1.202

```
$ nmap -sP 192.168.1.202
```

You can also Type **Nmap -sP www.scanme.namp.org** and it will ping the google server and tell you latency.

Output :

You can see that the **latency is 0.02 seconds** and the **Host is still up.**

```
$ nmap -sP 192.168.1.202
Starting Nmap 7.80 ( https://n
map.org ) at 2020-10-09 23:31
IST
Nmap scan report for 192.168.1
.202
Host is up (0.0019s latency).
Nmap done: 1 IP address (1 hos
t up) scanned in 0.02 seconds
```

Perform a Quick Scan with Nmap in Termux:

If you just wanna do a **quick scan of the network** and you only wanna know **basic information** then you can use **-F Argument**. It is much faster than the normal scan.
nmap -F 192.168.1.1/24

```
$ nmap -F 192.168.1.1/24
```

Output :

Here you can see **I got the output much faster** and The **result is still good.**

```
$ nmap -F 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.or
g ) at 2020-10-09 23:32 IST
Nmap scan report for 192.168.1.1
Host is up (0.0059s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.1.202
Host is up (0.0030s latency).
All 100 scanned ports on 192.168.1.2
02 are closed

Nmap done: 256 IP addresses (2 hosts
 up) scanned in 3.63 seconds
```

Check Nmap Version in Termux :

If you wanna **check the Nmap Version** then you can type the below command.
nmap -V

```
$ nmap -V
```

Output :

Now you can see the **Nmap Version in the below picture.**

```
$ nmap -V
Nmap version 7.80 ( https://nmap.org )
Platform: aarch64-unknown-linux-android
Compiled with: liblua-5.3.5 openssl-1.1.1h
 libssh2-1.9.0 libz-1.2.11 libpcre-8.44 li
bpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Namp in klai linux with metasploitable

```
root@lucifer: ~
File  Actions  Edit  View  Help
┌──(root💀 lucifer)-[~]
└─# nmap 192.168.43.75
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-27 18:11 IST
Nmap scan report for 192.168.43.75
Host is up (0.00050s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
```

```
┌──(root💀 lucifer)-[~]
└─# nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-27 18:14 IST
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:14 (0:00:00 remaining)
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:14 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
554/tcp   open     rtsp
1723/tcp  open     pptp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 27.31 seconds
```

Namp to get details about services

```
┌──(root💀 lucifer)-[~]
└─# nmap -sV 192.168.43.75
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-27 18:17 IST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 18:17 (0:00:01 remaining)
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 18:17 (0:00:01 remaining)
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 18:17 (0:00:01 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 18:18 (0:00:02 remaining)
Nmap scan report for 192.168.43.75
Host is up (0.00046s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
```

To find operating system use capital O, it also gives details about MAC address.

```
┌──(root💀 lucifer)-[~]
└─# nmap -O 192.168.43.75
```

```
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:84:43:47 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.87 seconds
```

To scan entire network

```
networkchuck@voldemort:~$ nmap -sP 10.7.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 17:30 CDT
```

Stealth scan for port 80,443 for rang of ip 10.7.1.0 to 24

```
networkchuck@voldemort:~$ sudo nmap -sS -p 80,443 10.7.1.0/24
[sudo] password for networkchuck:
```

To find out vulnerability use nmap script

```
networkchuck@voldemort:~$ sudo nmap --script vuln 10.7.1.226
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 18:40 CDT
```