Jawahar Education Societys Annasaheb Chudaman Patil College of Engineering, Kharghar, Navi Mumbai

DOP: / /2023 **DOS: / /2023**

Experiment No: 09

Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.

Theory:

🔷Nmap:

Nmap, short for Network Mapper, is a free and open-source tool used for vulnerability checking, port scanning and, of course, network mapping. Despite being created back in 1997, Nmap remains the gold standard against which all other similar tools, either commercial or open source, are judged.

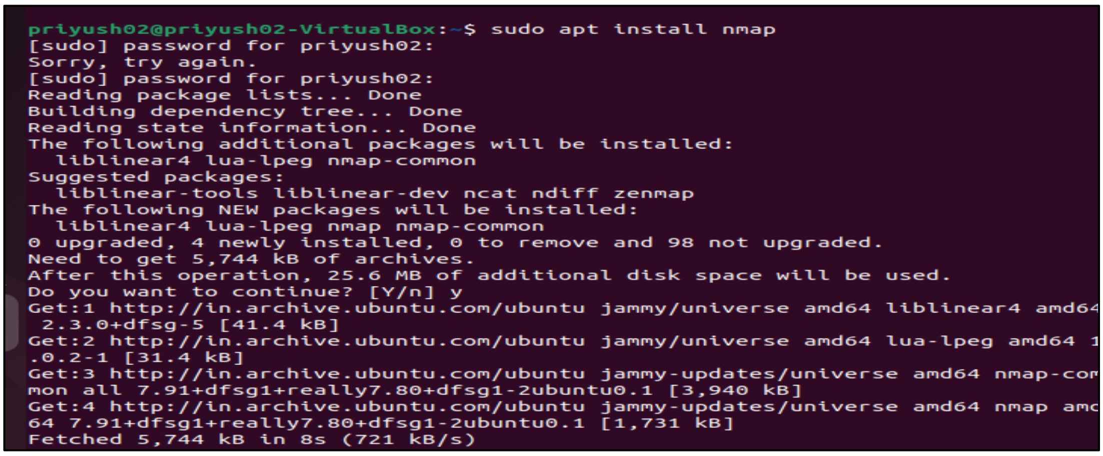
Nmap has maintained its pre-eminence because of the large community of developers and coders who help to maintain and update it. The Nmap community reports that the tool, which anyone can get for free, is downloaded several thousand times every week.

Because of its flexible, open-source code base, it can be modified to work within most customized or heavily specialized environments. There are distributions of Nmap specific to Windows, Mac and Linux environments, but Nmap also supports less popular or older operating systems like Solaris, AIX or AmigaOS. The source code is available in C, C++, Perl and Python.

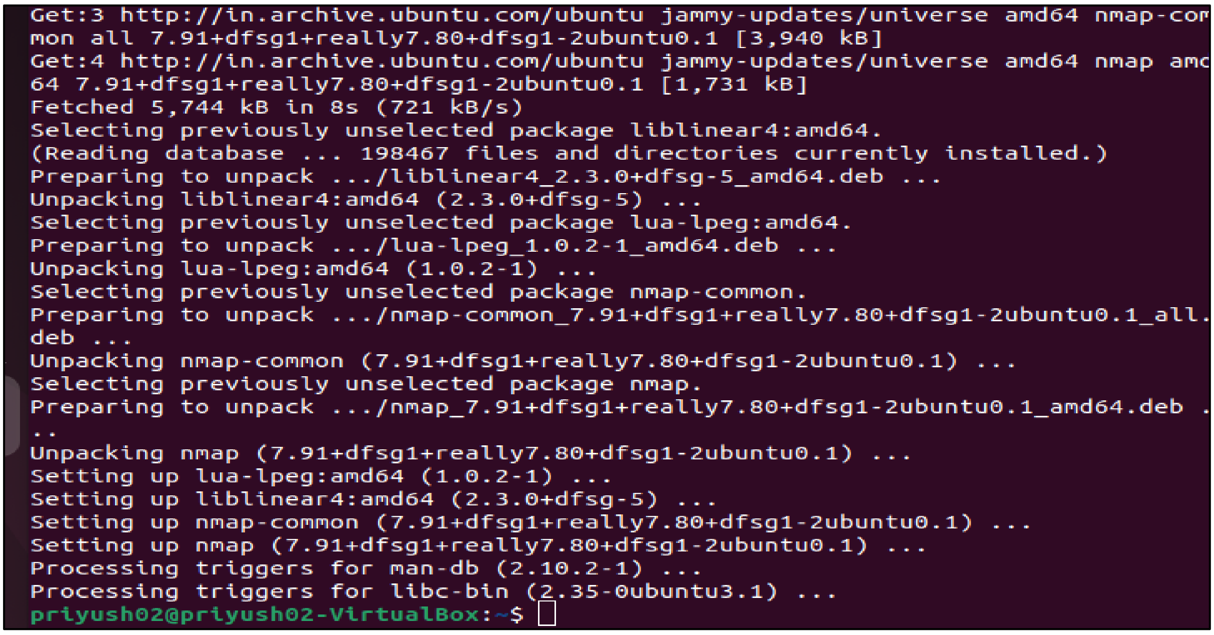
🔷Nmap features include:

- **Host Discovery** – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- **Port Scanning** – Enumerating the open ports on one or more target hosts.
- **Version Detection** – Interrogating listening network services listening on remote devices to determine the application name and version number.
- **OS Detection** – Remotely determining the operating system and some hardware characteristics of network devices.

The installation of **nmap:> sudo apt-get install nmap**



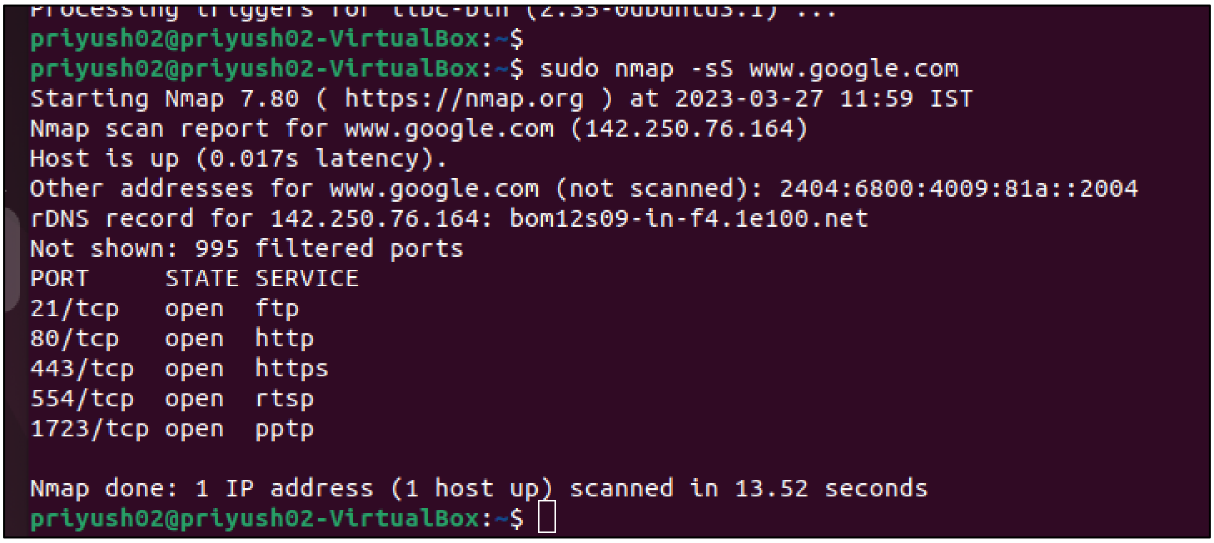
```
priyush02@priyush02-VirtualBox:~$ sudo apt install nmap
[sudo] password for priyush02:
Sorry, try again.
[sudo] password for priyush02:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  liblinear4 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  liblinear4 lua-lpeg nmap nmap-common
0 upgraded, 4 newly installed, 0 to remove and 98 not upgraded.
Need to get 5,744 kB of archives.
After this operation, 25.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 liblinear4 amd64
 2.3.0+dfsg-5 [41.4 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1
.0.2-1 [31.4 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap-com
mon all 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [3,940 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap amc
64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1,731 kB]
Fetched 5,744 kB in 8s (721 kB/s)
```



```
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap-com
mon all 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [3,940 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap amd
64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1,731 kB]
Fetched 5,744 kB in 8s (721 kB/s)
Selecting previously unselected package liblinear4:amd64.
(Reading database ... 198467 files and directories currently installed.)
Preparing to unpack .../liblinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_all.
deb ...
Unpacking nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_amd64.deb .
..
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
priyush02@priyush02-VirtualBox:~$
```

◆nmap -sS for TCP SYN Scan:

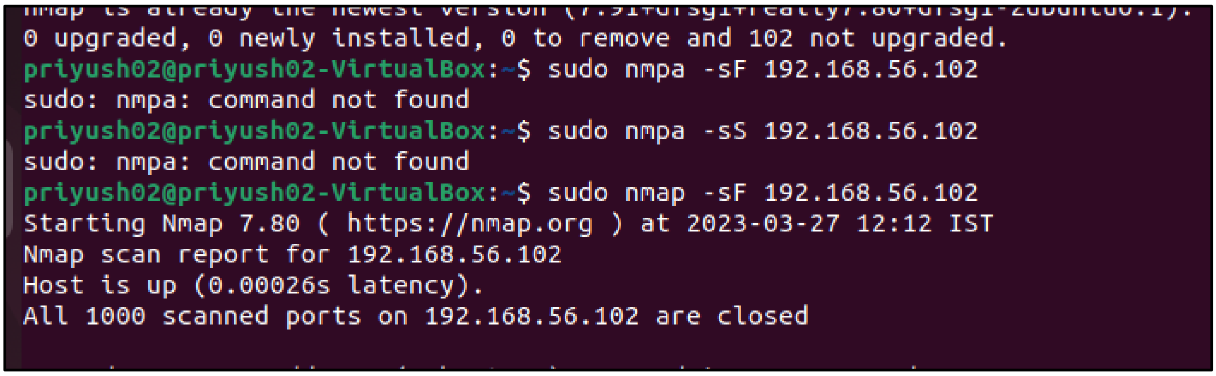
It is required privilege access and identifies TCP ports. TCP SYN Scan is a standard method for detecting open ports without going through the Three-way Handshake process. When an open port is spotted, the TCP handshake is reset before accomplishment. Hence this scanning is also called Half Open scanning.



```
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
priyush02@priyush02-VirtualBox:~$
priyush02@priyush02-VirtualBox:~$ sudo nmap -sS www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 11:59 IST
Nmap scan report for www.google.com (142.250.76.164)
Host is up (0.017s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:81a::2004
rDNS record for 142.250.76.164: bom12s09-in-f4.1e100.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 13.52 seconds
priyush02@priyush02-VirtualBox:~$
```

◆nmap -sF for FIN Scan:

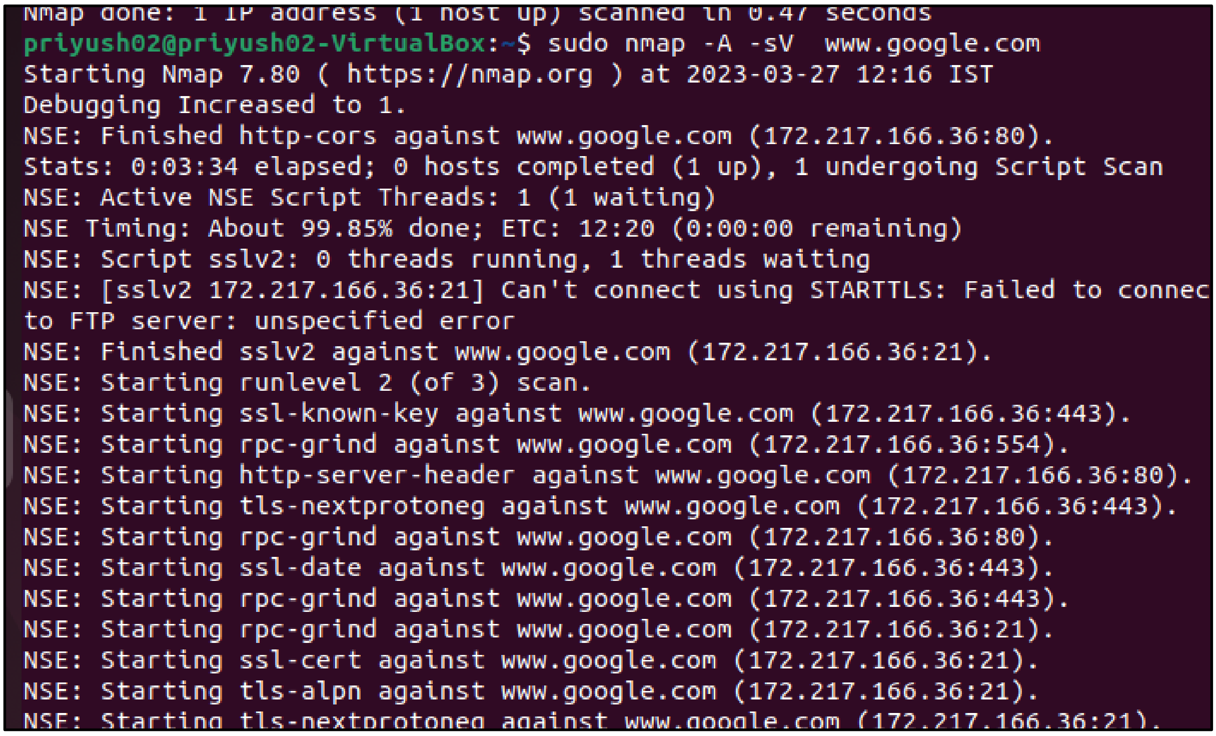
FIN scan transmits packets with a FIN flag to the target machine; therefore, these frames are abnormal as they are sent to the destination before the Three-way handshaking process can be completed. If there is no active TCP session, then the port is formally closed. If the destination machine's port is closed then the RST packet in the FIN Scan response is reversed.



```
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 102 not upgraded.
priyush02@priyush02-VirtualBox:~$ sudo nmpa -sF 192.168.56.102
sudo: nmpa: command not found
priyush02@priyush02-VirtualBox:~$ sudo nmpa -sS 192.168.56.102
sudo: nmpa: command not found
priyush02@priyush02-VirtualBox:~$ sudo nmap -sF 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:12 IST
Nmap scan report for 192.168.56.102
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.56.102 are closed
```

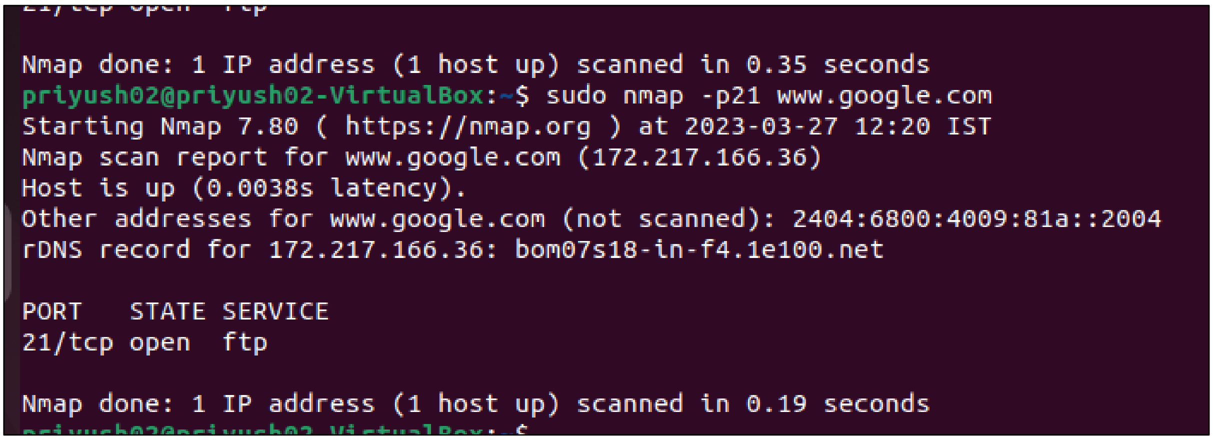
🔷sV (Version detection):

Enables version detection, as discussed above. Alternatively, we can use -A, which enables version detection among other things,



```
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
priyush02@priyush02-VirtualBox:~$ sudo nmap -A -sV  www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:16 IST
Debugging Increased to 1.
NSE: Finished http-cors against www.google.com (172.217.166.36:80).
Stats: 0:03:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 99.85% done; ETC: 12:20 (0:00:00 remaining)
NSE: Script sslv2: 0 threads running, 1 threads waiting
NSE: [sslv2 172.217.166.36:21] Can't connect using STARTTLS: Failed to connec
to FTP server: unspecified error
NSE: Finished sslv2 against www.google.com (172.217.166.36:21).
NSE: Starting runlevel 2 (of 3) scan.
NSE: Starting ssl-known-key against www.google.com (172.217.166.36:443).
NSE: Starting rpc-grind against www.google.com (172.217.166.36:554).
NSE: Starting http-server-header against www.google.com (172.217.166.36:80).
NSE: Starting tls-nextprotoneg against www.google.com (172.217.166.36:443).
NSE: Starting rpc-grind against www.google.com (172.217.166.36:80).
NSE: Starting ssl-date against www.google.com (172.217.166.36:443).
NSE: Starting rpc-grind against www.google.com (172.217.166.36:443).
NSE: Starting rpc-grind against www.google.com (172.217.166.36:21).
NSE: Starting ssl-cert against www.google.com (172.217.166.36:21).
NSE: Starting tls-alpn against www.google.com (172.217.166.36:21).
NSE: Starting tls-nextprotoneg against www.google.com (172.217.166.36:21).
```

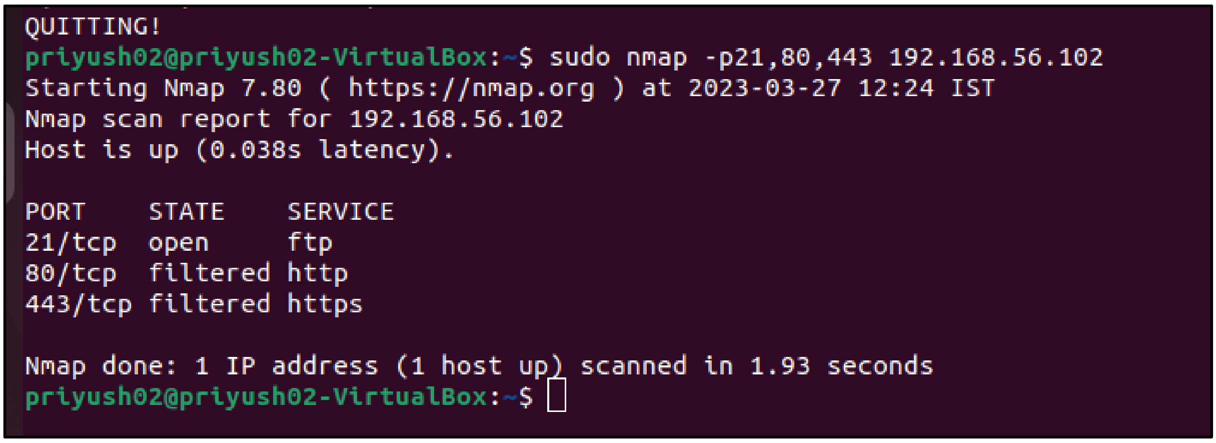
Multiple scan ports:



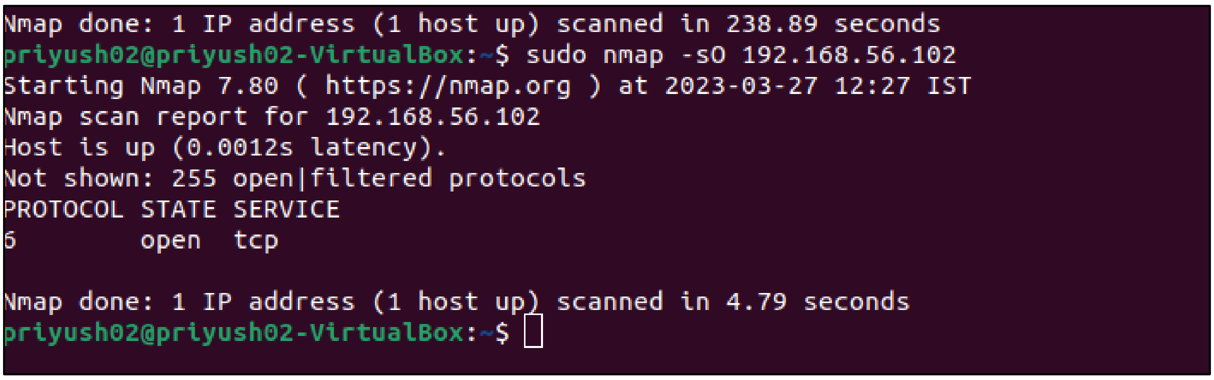
```
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
priyush02@priyush02-VirtualBox:~$ sudo nmap -p21 www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:20 IST
Nmap scan report for www.google.com (172.217.166.36)
Host is up (0.0038s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:81a::2004
rDNS record for 172.217.166.36: bom07s18-in-f4.1e100.net

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
priyush02@priyush02-VirtualBox:~$
```

◆sO (IP protocol scan).

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn´t technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers



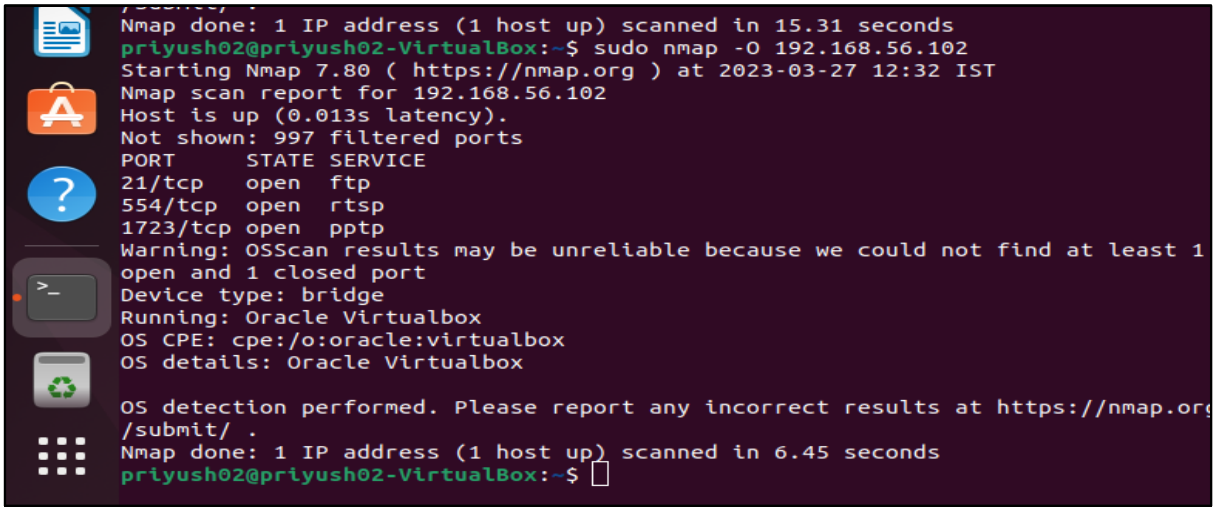
```
QUITTING!
priyush02@priyush02-VirtualBox:~$ sudo nmap -p21,80,443 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:24 IST
Nmap scan report for 192.168.56.102
Host is up (0.038s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
80/tcp   filtered http
443/tcp  filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
priyush02@priyush02-VirtualBox:~$ 
```



```
Nmap done: 1 IP address (1 host up) scanned in 238.89 seconds
priyush02@priyush02-VirtualBox:~$ sudo nmap -sO 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:27 IST
Nmap scan report for 192.168.56.102
Host is up (0.0012s latency).
Not shown: 255 open|filtered protocols
PROTOCOL STATE SERVICE
6        open  tcp

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
priyush02@priyush02-VirtualBox:~$ 
```

◆What is OS Fingerprinting?

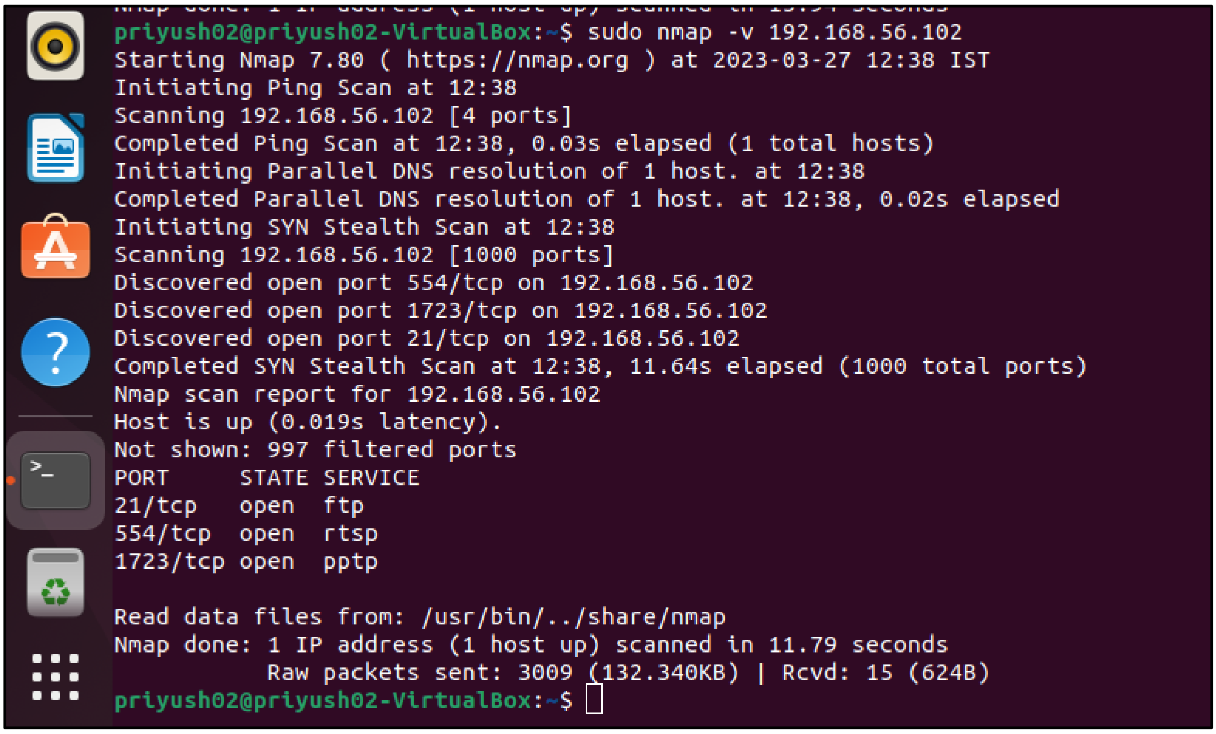
Operating System (OS) Fingerprinting is the process of analysing data packets which originate from a network in an attempt to glean intelligence to be used in later attacks. By detecting which operating system, a network operates on, hackers have an easier time targeting known vulnerabilities.



```
Nmap done: 1 IP address (1 host up) scanned in 15.31 seconds
priyush02@priyush02-VirtualBox:~$ sudo nmap -O 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:32 IST
Nmap scan report for 192.168.56.102
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
554/tcp  open  rtsp
1723/tcp open  pptp
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox

OS detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
priyush02@priyush02-VirtualBox:~$ 
```

◆Ping:

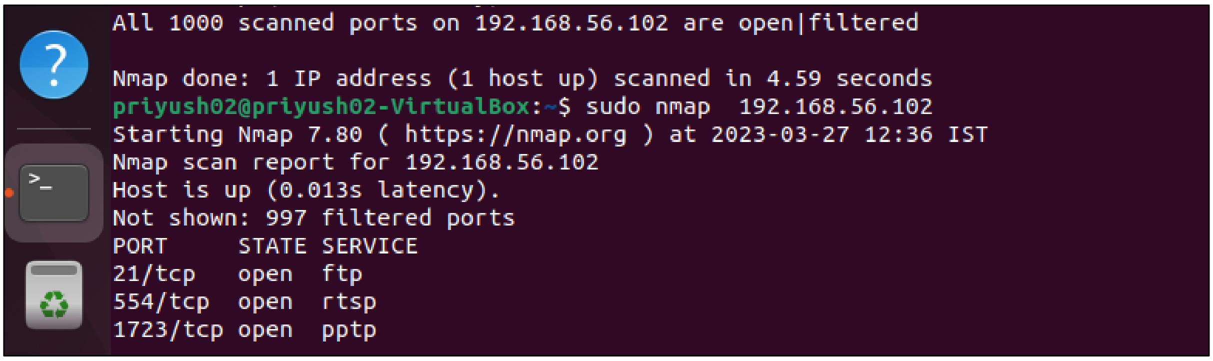
The Ping Scanner Tool sends ICMP ping packets to every IP address in any range of IPv4 addresses you specify. It looks for ICMP responses from active devices. This tool operates across any range of IPv4 addresses whether on your subnet or across the internet. It can also ping a list of IPv4 addresses that you need to ping. That list need not be contiguous, it can be random.



```
priyush02@priyush02-VirtualBox:~$ sudo nmap -v 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:38 IST
Initiating Ping Scan at 12:38
Scanning 192.168.56.102 [4 ports]
Completed Ping Scan at 12:38, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:38
Completed Parallel DNS resolution of 1 host. at 12:38, 0.02s elapsed
Initiating SYN Stealth Scan at 12:38
Scanning 192.168.56.102 [1000 ports]
Discovered open port 554/tcp on 192.168.56.102
Discovered open port 1723/tcp on 192.168.56.102
Discovered open port 21/tcp on 192.168.56.102
Completed SYN Stealth Scan at 12:38, 11.64s elapsed (1000 total ports)
Nmap scan report for 192.168.56.102
Host is up (0.019s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
554/tcp  open  rtsp
1723/tcp open  pptp

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
           Raw packets sent: 3009 (132.340KB) | Rcvd: 15 (624B)
priyush02@priyush02-VirtualBox:~$
```

◆What is this TCP Port Scan?

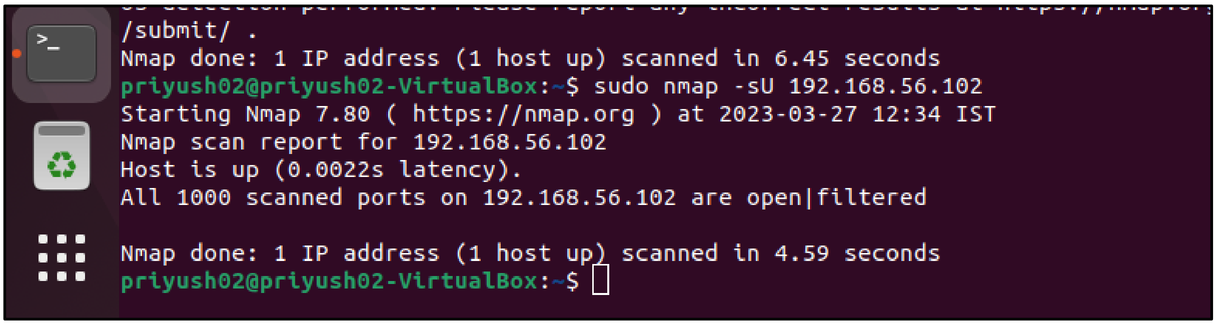
The TCP Port Scan will test an IP Address for common open ports. This technique of testing for listening services is known as a port scan. Try our advanced online port scanner that is able to scan any IP Address or IP range and all 65535 ports.



```
All 1000 scanned ports on 192.168.56.102 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds
priyush02@priyush02-VirtualBox:~$ sudo nmap  192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:36 IST
Nmap scan report for 192.168.56.102
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
554/tcp  open  rtsp
1723/tcp open  pptp
```

◆UDP scanning:

UDP scanning is a process in which we scan for the UDP services that are being deployed on the target system or are currently in a running state. UDP is a connectionless protocol, hence it is hard to probe as compared to TCP.



```
OS detection performed. Please report any incorrect results at https://nmap.or
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
priyush02@priyush02-VirtualBox:~$ sudo nmap -sU 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-27 12:34 IST
Nmap scan report for 192.168.56.102
Host is up (0.0022s latency).
All 1000 scanned ports on 192.168.56.102 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds
priyush02@priyush02-VirtualBox:~$ 
```

Conclusion:

Network scanning provides a wealth of information about the target network, which is valuable regardless of whether you're trying to attack the network or protect it from attack. While performing a basic scan is a simple matter, the network scanners covered in this experiment provide a wide array of options to tweak your scan to achieve the best results. Nmap is used to detect IP spoofing and port scanning.