NAME: ADWAIT S PURAO

UID: 2021300101

BATCH: B2

AIM: Network Scanning using Open-Source Tools - NMAP

EXPERIMENT NO.: 10

THEORY:

What is Nmap and why do you need it on your network?

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.

What is Zenmap?

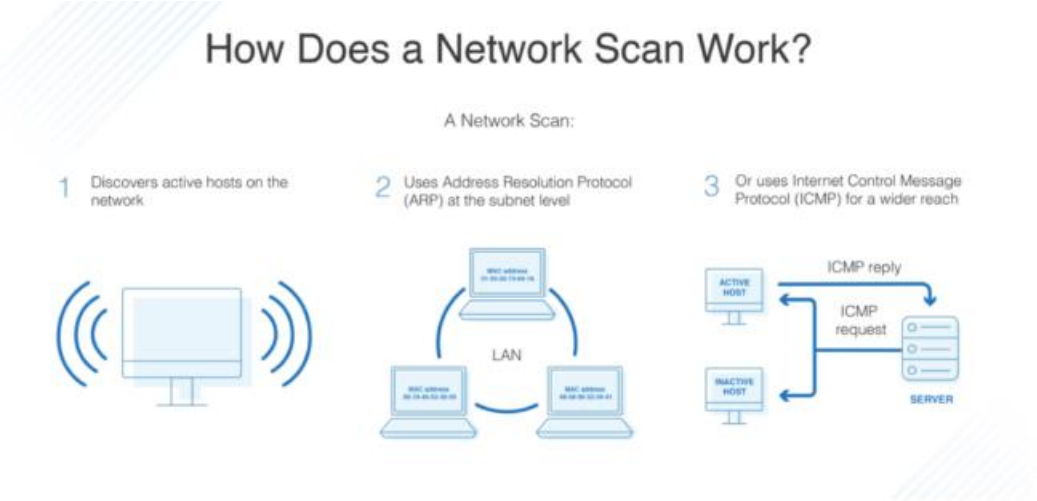
To deploy Nmap, users originally had to have some advanced programming skills, or at least know their way around console commands or non-graphical interfaces. That changed recently with the introduction of the Zenmap tool for Nmap, which adds a graphical interface that makes launching the program and analysing the returned output it generates much more accessible.

Zenmap was created to allow beginners to use the tool. Like Nmap, Zenmap is free, and the source code is both open and available to anyone who wants to use or modify it.

Here are some of the capabilities that are enabled by Zenmap: Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan

results can be compared with one another to see how they differ. And the results of recent scans can be stored in a searchable database.

How does Nmap work?



The heart of Nmap is port scanning. How it works is that users designate a list of targets on a network that they want to learn information about. Users don't need to identify specific targets, which is good because most administrators don't have a complete picture of everything that is using the potentially thousands of ports on their network. Instead, they compile a range of ports to scan.

It's also possible to scan all network ports, although that would potentially take a lot of time and eat up quite a bit of available bandwidth. Plus, depending on the type of passive defences that are in use on the network, such a massive port scan would likely trigger security alerts. As such, most people use Nmap in more limited deployments or divide different parts of their network up for scheduled scanning over time.

In addition to setting up a range targets to be scanned, users can also control the depth of each scan. For example, a light or limited scan might return information about which ports are open and which have been closed by firewall settings. More detailed scans could additionally capture information about what kind of devices are using those ports, the operating systems they are running and even the services that are active on them. Nmap can also discover deeper information, like the version of those discovered services. That makes it a perfect tool for finding vulnerabilities or assisting with patch management efforts.

Controlling the scans used to require console commands, which of course means that some training was required. But the new Zenmap graphical interface makes it easy for just about everyone to tell Nmap what they want it to discover, with or without formal training. Meanwhile, professionals can continue to use the console commands they always have, making it a useful tool for both experts and novices alike.

Is Nmap a security risk?

While one could make the argument that Nmap is a perfect hacking tool, many of the deeper scan activities require root access and privileges. Someone from outside can't just point Nmap at a target network they don't have permission to access and have it magically uncover vulnerabilities for them to exploit. Not only that, but the attempt would likely trigger a critical security alert by any defensive or network monitoring tools.

That is not to say that Nmap could not be dangerous in the wrong hands, especially if deployed by a turncoat system administrator or someone using stolen credentials. This was demonstrated in the 2016 Oliver Stone movie *Snowden* (another film that featured Nmap) about the accused traitor Edward Snowden.

What does Nmap do?

When used properly, Nmap can be invaluable for both optimizing and protecting networks and information. All of the return data sent back by ports scanned using Nmap is collected and complied by the program. Based on that information, there are several key activities that most people use the tool to help accomplish. They include:

Network Mapping: This is the core reason why Nmap was created and remains one of the top uses. Called host discovery, Nmap will identify the types of devices actively using scanned ports. This includes servers, routers, switches and other devices. Users can also see how those devices are connected, and how they link together to form a network map.

Port Rules Discovery: Nmap can easily tell, even with a low-level scan, if a port is open or closed by something like a firewall. In fact, many IT professionals use Nmap to check their work when programming firewalls. They can see if their policies are having the desired effect, and if their firewalls are working properly.

Shadow IT Hunting: Because Nmap discovers the type and location of devices on a network, it can be used to identity things that should not be there at all. These devices are called shadow IT because their presence on a network isn't officially authorized, or sometimes may be intentionally hidden. Shadow IT can be dangerous because such devices are not part of a security audit or program. For example, if someone secretly places an Xbox game server on a corporate network, not only will that potentially drain bandwidth, but could act as a springboard for an attack, especially if it's not maintained with all the latest security patches.

Operating System Detection: Nmap can discover the types of operating systems running on discovered devices in a process called OS fingerprinting. This generally returns information about the name of the vendor of the device (Dell, HP, etc.) and the operating system. With a deeper Nmap scan, you can even discover things like the patch level of the OS and the estimated uptime of the device.

Service Discovery: The ability to discover services elevates Nmap above the level of a common mapping tool. Instead of simply discovering that a device exists, users can trigger a deeper scan in order to find out what roles discovered devices are performing. This includes identifying if they are acting as mail server, a web server, a database repository, a storage device or almost anything else. Depending on the scan, Nmap can also report on which specific applications are running, and what version of those applications are being used.

Vulnerability Scanning: Nmap is not a dedicated vulnerability scanning tool in that it does not maintain a database of known vulnerabilities or any kind of artificial intelligence that could identify potential threats. However, organizations that regularly ingest security information from threat feeds or other sources can use Nmap to check their susceptibility to specific threats.

For example, if a newly uncovered vulnerability only affects a certain application or service running an older version of the software, Nmap can be used to check to see if any programs currently operating on network assets meet those conditions. If anything is found, then presumably IT teams could prioritize getting those systems patched as quickly as possible to eliminate the vulnerability before an attacker could discover the same thing.

What is the future of Nmap?

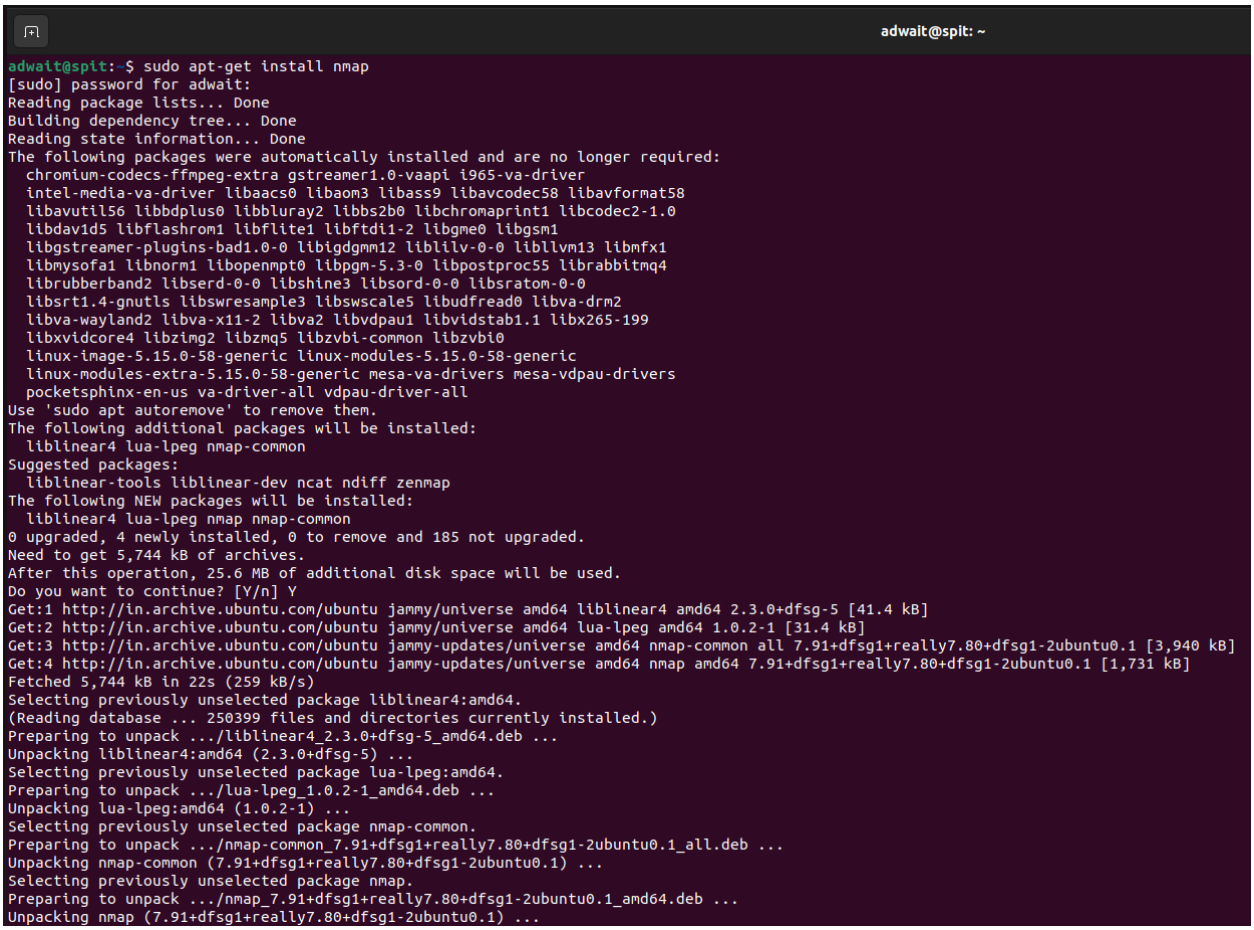
Although the Nmap tool is 25 years old, it continues to evolve. Like other seemingly ancient technologies such as Ethernet or Spanning Tree, it is well maintained by an active community of experts that keep it relevant and up to date. And in the case of Nmap, that community includes its very active creator, who still goes by his Fyodor guise online.

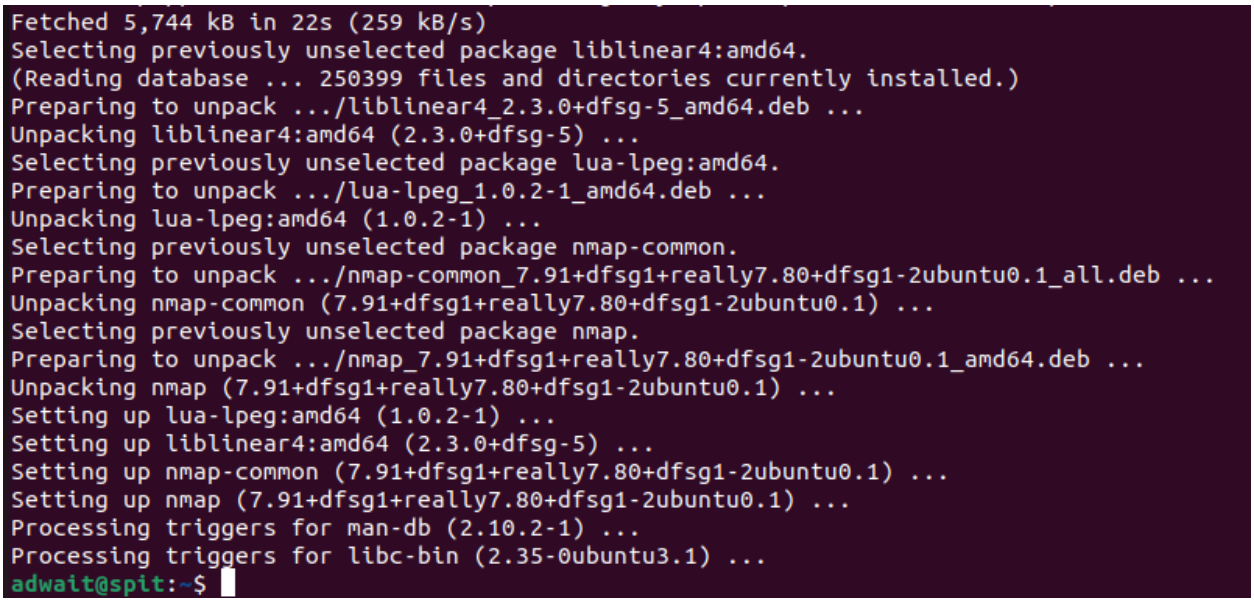
Other advancements like the new Zenmap tool make it even more useful, especially for those who don't like working with console or command lines. The graphical interface for Zenmap allows users to quickly set up targets and configure desired scans with just a few clicks. That will help Nmap find an even bigger user base.

And finally, while there are many other tools these days that can perform similar functions, none of them have the proven track record of Nmap. Not only that, but Nmap has always been completely free and ready to download. Because of all of these factors, it's almost a sure thing that Nmap will be just as useful and relevant over the next 25 years as it has been for past quarter century.

Screenshots:

• Installing NMAP


adwait@spit: ~
adwait@spit:~$ sudo apt-get install nmap
[sudo] password for adwait:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58
libavutil56 libbdplus0 libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0
libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1
libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1
libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4
librubberband2 libserd-0-0 libshine3 libsord-0-0 libsratom-0-0
libsrt1.4-gnutls libswresample3 libswscale5 libudfread0 libva-drm2
libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199
libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
linux-image-5.15.0-58-generic linux-modules-5.15.0-58-generic
linux-modules-extra-5.15.0-58-generic mesa-va-drivers mesa-vdpau-drivers
pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
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 185 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-common 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 amd64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1,731 kB]
Fetched 5,744 kB in 22s (259 kB/s)
Selecting previously unselected package liblinear4:amd64.
(Reading database ... 250399 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) ...


Fetched 5,744 kB in 22s (259 kB/s)
Selecting previously unselected package liblinear4:amd64.
(Reading database ... 250399 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) ...
adwait@spit:~$

• Single

```
adwait@spit:~$ sudo nmap 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 18:01 IST
Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.38 seconds
adwait@spit:~$
```

• Server name

```
adwait@spit:~$ sudo nmap spit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 18:03 IST
Nmap scan report for spit.ac.in (127.0.1.1)
Host is up (0.0000020s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
adwait@spit:~$
```

• 2-3 addresses

```
adwait@spit:~$ sudo nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 18:04 IST
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.2
Host is up (0.0030s latency).
All 1000 scanned ports on 192.168.1.2 are filtered

Nmap scan report for 192.168.1.3
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.1.3 are filtered

Nmap done: 3 IP addresses (3 hosts up) scanned in 29.09 seconds
adwait@spit:~$
```

• Range of IP Addresses

```
adwait@spit:~$ sudo nmap 192.168.1.1,2,3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 18:06 IST
Nmap scan report for 192.168.1.1
Host is up (0.0049s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.2
Host is up (0.0027s latency).
All 1000 scanned ports on 192.168.1.2 are filtered

Nmap scan report for 192.168.1.3
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.1.3 are filtered

Nmap done: 3 IP addresses (3 hosts up) scanned in 27.97 seconds
adwait@spit:~$
```

• Range of IP address

```
adwait@spit:~$ sudo nmap 192.168.1.1-20
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 18:08 IST
Nmap scan report for 192.168.1.1
Host is up (0.0093s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.2
Host is up (0.0064s latency).
All 1000 scanned ports on 192.168.1.2 are filtered

Nmap scan report for 192.168.1.3
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.1.3 are filtered

Nmap scan report for 192.168.1.4
Host is up (0.0094s latency).
All 1000 scanned ports on 192.168.1.4 are filtered

Nmap scan report for 192.168.1.5
Host is up (0.11s latency).
All 1000 scanned ports on 192.168.1.5 are filtered

Nmap scan report for 192.168.1.6
Host is up (0.019s latency).
All 1000 scanned ports on 192.168.1.6 are filtered

Nmap scan report for 192.168.1.7
Host is up (0.0061s latency).
All 1000 scanned ports on 192.168.1.7 are filtered

Nmap scan report for 192.168.1.8
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.8 are filtered

Nmap scan report for 192.168.1.9
Host is up (0.0065s latency).
All 1000 scanned ports on 192.168.1.9 are filtered

Nmap scan report for 192.168.1.10
Host is up (0.0080s latency).
All 1000 scanned ports on 192.168.1.10 are filtered

Nmap scan report for 192.168.1.11
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.1.11 are filtered

Nmap scan report for 192.168.1.12
Host is up (0.0093s latency).
```

```
All 1000 scanned ports on 192.168.1.9 are filtered

Nmap scan report for 192.168.1.10
Host is up (0.0080s latency).
All 1000 scanned ports on 192.168.1.10 are filtered

Nmap scan report for 192.168.1.11
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.1.11 are filtered

Nmap scan report for 192.168.1.12
Host is up (0.0093s latency).
All 1000 scanned ports on 192.168.1.12 are filtered

Nmap scan report for 192.168.1.13
Host is up (0.0092s latency).
All 1000 scanned ports on 192.168.1.13 are filtered

Nmap scan report for 192.168.1.14
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.1.14 are filtered

Nmap scan report for 192.168.1.15
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.15 are filtered

Nmap scan report for 192.168.1.16
Host is up (0.0080s latency).
All 1000 scanned ports on 192.168.1.16 are filtered

Nmap scan report for 192.168.1.17
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.17 are filtered

Nmap scan report for 192.168.1.18
Host is up (0.021s latency).
All 1000 scanned ports on 192.168.1.18 are filtered

Nmap scan report for 192.168.1.19
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.19 are filtered

Nmap scan report for 192.168.1.20
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.1.20 are filtered

Nmap done: 20 IP addresses (20 hosts up) scanned in 291.81 seconds
adwait@spit:~$
```

3: Read list of hosts/networks from a file (IPv4):

• The -iL option allows you to read the list of target systems using a text file. This is useful to scan many hosts/networks.

```
adwait@spit:~$ cat > /tmp/test.txt
192.168.1.0
^C
adwait@spit:~$ sudo nmap -iL /tmp/test.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 18:16 IST
Nmap scan report for 192.168.1.0
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.1.0 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
adwait@spit:~$
```

4: Excluding hosts/networks (IPv4):

When scanning many hosts/networks you can exclude hosts from a scan:

```
adwait@spit:~$ sudo nmap 192.168.1.0/24 --exclude 192.168.1.5
[sudo] password for adwait:
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-26 20:03 IST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 1.96% done; ETC: 20:04 (0:01:40 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 6.86% done; ETC: 20:04 (0:01:35 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 10.78% done; ETC: 20:04 (0:01:31 remaining)
Nmap done: 255 IP addresses (0 hosts up) scanned in 103.74 seconds
```

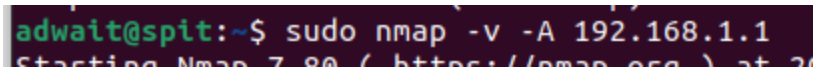
5: Turn on OS and version detection scanning script (IPv4):

```
adwait@spit:~$ sudo nmap -A 192.168.1.254
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:15 IST
Nmap scan report for 192.168.1.254
Host is up (0.0032s latency).
All 1000 scanned ports on 192.168.1.254 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   3.48 ms _gateway (10.0.2.2)
2   3.54 ms 192.168.1.254

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 7.54 seconds
```


adwait@spit:~$ sudo nmap -v -A 192.168.1.1

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:17 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating Ping Scan at 22:17
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 22:17, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:17
Completed Parallel DNS resolution of 1 host. at 22:17, 0.01s elapsed
Initiating SYN Stealth Scan at 22:17
Scanning 192.168.1.1 [1000 ports]
Completed SYN Stealth Scan at 22:17, 4.12s elapsed (1000 total ports)
Initiating Service scan at 22:17
Initiating OS detection (try #1) against 192.168.1.1
Retrying OS detection (try #2) against 192.168.1.1
Initiating Traceroute at 22:17
Completed Traceroute at 22:17, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 22:17
Completed Parallel DNS resolution of 2 hosts. at 22:17, 0.02s elapsed
NSE: Script scanning 192.168.1.1.
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.1.1 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.19 ms _gateway (10.0.2.2)
2   2.55 ms 192.168.1.1

NSE: Script Post-scanning.
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
```

```
TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.19 ms _gateway (10.0.2.2)
2   2.55 ms 192.168.1.1

NSE: Script Post-scanning.
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Initiating NSE at 22:17
Completed NSE at 22:17, 0.00s elapsed
Read data files from: /usr/bin/../share/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 7.51 seconds
           Raw packets sent: 2053 (94.624KB) | Rcvd: 18 (736B)
adwait@spit:~$
```

6: Find out if a host/network is protected by a firewall:

```
adwait@spit:~$ sudo nmap -sA 192.168.1.254
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:21 IST
Nmap scan report for 192.168.1.254
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.1.254 are unfiltered
```

```
adwait@spit:~$ sudo nmap -sA spit.ac.in
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:22 IST
Nmap scan report for spit.ac.in (127.0.1.1)
Host is up (0.0000020s latency).
All 1000 scanned ports on spit.ac.in (127.0.1.1) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

7: Scan a host when protected by the firewall

```
adwait@spit:~$ sudo nmap -PN 192.168.1.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-26 20:11 IST
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.00% done; ETC: 20:14 (0:00:08 remaining)
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 202.84 seconds
```

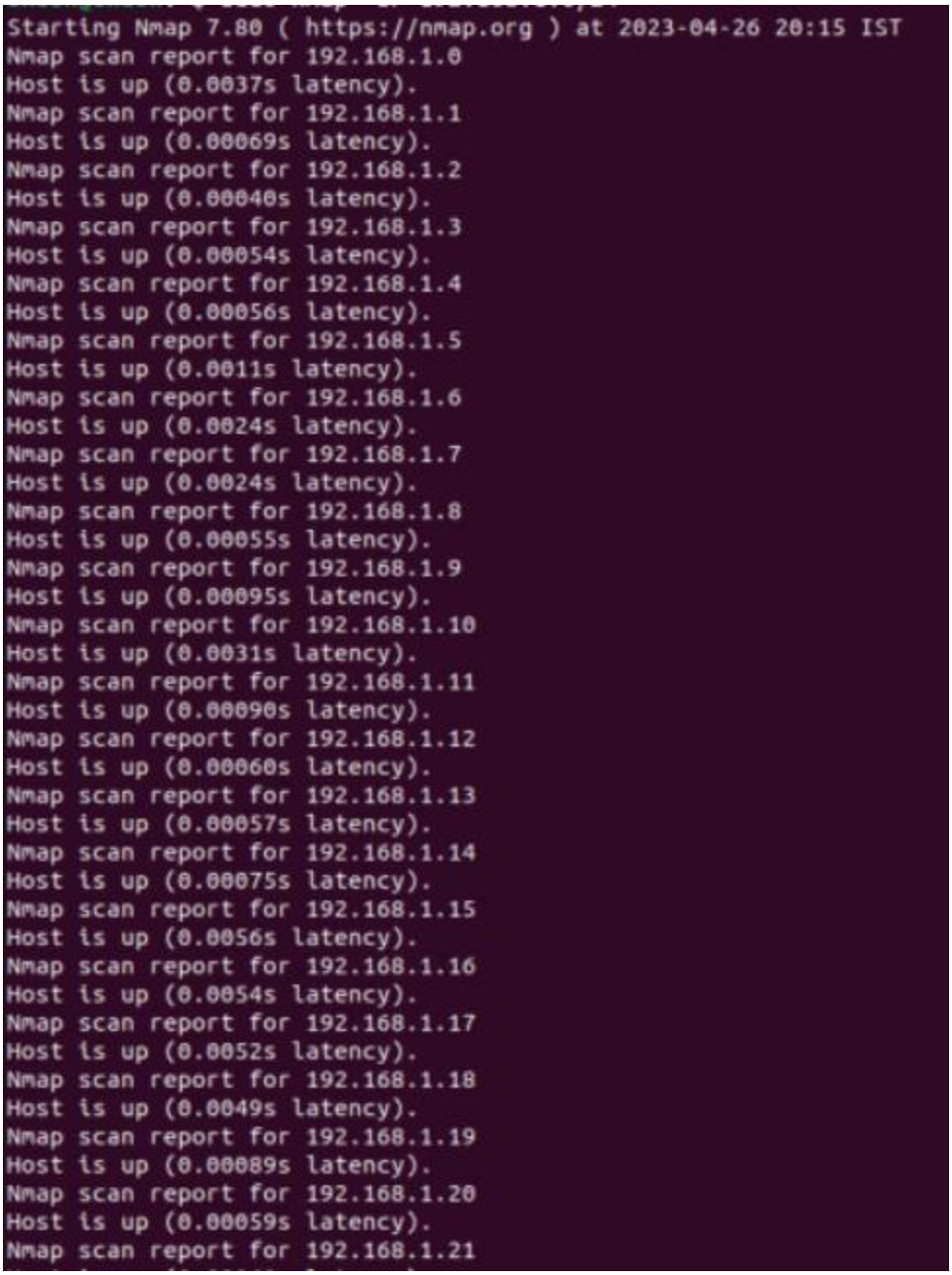
```
adwait@spit:~$ sudo nmap -PN spit.ac.in
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:25 IST
Nmap scan report for spit.ac.in (127.0.1.1)
Host is up (0.0000020s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

8: Scan a network and find out which servers and devices are up and running

```
adwait@spit:~$ sudo nmap -sP 192.168.1.0/24
```


Starting Nmap 7.80 (https://nmap.org) at 2023-04-26 20:15 IST
Nmap scan report for 192.168.1.0
Host is up (0.0037s latency).
Nmap scan report for 192.168.1.1
Host is up (0.00069s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00040s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00054s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00056s latency).
Nmap scan report for 192.168.1.5
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.6
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.7
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00055s latency).
Nmap scan report for 192.168.1.9
Host is up (0.00095s latency).
Nmap scan report for 192.168.1.10
Host is up (0.0031s latency).
Nmap scan report for 192.168.1.11
Host is up (0.00090s latency).
Nmap scan report for 192.168.1.12
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.13
Host is up (0.00057s latency).
Nmap scan report for 192.168.1.14
Host is up (0.00075s latency).
Nmap scan report for 192.168.1.15
Host is up (0.0056s latency).
Nmap scan report for 192.168.1.16
Host is up (0.0054s latency).
Nmap scan report for 192.168.1.17
Host is up (0.0052s latency).
Nmap scan report for 192.168.1.18
Host is up (0.0049s latency).
Nmap scan report for 192.168.1.19
Host is up (0.00089s latency).
Nmap scan report for 192.168.1.20
Host is up (0.00059s latency).
Nmap scan report for 192.168.1.21

```
Host is up (0.00025s latency).
Nmap scan report for 192.168.1.235
Host is up (0.00090s latency).
Nmap scan report for 192.168.1.236
Host is up (0.00056s latency).
Nmap scan report for 192.168.1.237
Host is up (0.00028s latency).
Nmap scan report for 192.168.1.238
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.239
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.240
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.241
Host is up (0.00026s latency).
Nmap scan report for 192.168.1.242
Host is up (0.00073s latency).
Nmap scan report for 192.168.1.243
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.244
Host is up (0.0018s latency).
Nmap scan report for 192.168.1.245
Host is up (0.00078s latency).
Nmap scan report for 192.168.1.246
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.247
Host is up (0.00059s latency).
Nmap scan report for 192.168.1.248
Host is up (0.00028s latency).
Nmap scan report for 192.168.1.249
Host is up (0.0014s latency).
Nmap scan report for 192.168.1.250
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.251
Host is up (0.0019s latency).
Nmap scan report for 192.168.1.252
Host is up (0.00061s latency).
Nmap scan report for 192.168.1.253
Host is up (0.00080s latency).
Nmap scan report for 192.168.1.254
Host is up (0.0026s latency).
Nmap scan report for 192.168.1.255
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 53.33 second
```

9: How to perform a fast scan?

```
adwait@spit:~$ sudo nmap -F 192.168.1.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:29 IST
Nmap scan report for 192.168.1.1
Host is up (0.0014s latency).
All 100 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

10: Display the reason a port is in a particular state

```
adwait@spit:~$ sudo nmap --reason 192.168.1.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:30 IST
Nmap scan report for 192.168.1.1
Host is up, received reset ttl 255 (0.0017s latency).
All 1000 scanned ports on 192.168.1.1 are filtered because of 1000 no-responses

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds
```

```
adwait@spit:~$ sudo nmap --reason spit.ac.in
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:31 IST
Nmap scan report for spit.ac.in (127.0.1.1)
Host is up, received localhost-response (0.0000020s latency).
Not shown: 997 closed ports
Reason: 997 resets
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
25/tcp open  smtp    syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

11: Only show open (or possibly open) ports

```
adwait@spit:~$ sudo nmap --open 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:33 IST
Nmap done: 1 IP address (1 host up) scanned in 4.28 seconds
```

```
adwait@spit:~$ sudo nmap --open spit.ac.in
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:33 IST
Nmap scan report for spit.ac.in (127.0.1.1)
Host is up (0.0000020s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

12: Show all packets sent and received

On address

```
adwait@spit:~$ sudo nmap --packet-trace 192.168.1.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:35 IST
SENT (0.0530s) ICMP [10.0.2.15 > 192.168.1.1 Echo request (type=8/code=0) id=18894 seq=0] IP [ttl=40 id=58850 iplen=28 ]
SENT (0.0532s) TCP 10.0.2.15:49440 > 192.168.1.1:443 S ttl=53 id=15139 iplen=44  seq=3350937487 win=1024 <mss 1460>
SENT (0.0533s) TCP 10.0.2.15:49440 > 192.168.1.1:80 A ttl=39 id=58784 iplen=40  seq=0 win=1024
SENT (0.0534s) ICMP [10.0.2.15 > 192.168.1.1 Timestamp request (type=13/code=0) id=37090 seq=0 orig=0 recv=0 trans=0] IP [ttl=39 id=63802 iplen=40 ]
RCVD (0.0546s) TCP 192.168.1.1:80 > 10.0.2.15:49440 R ttl=255 id=15434 iplen=40  seq=3350937487 win=0
NSOCK INFO [0.1120s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1120s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.1120s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
NSOCK INFO [0.1120s] nsock_write(): Write request for 42 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.1120s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.1120s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [0.1310s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.53:53] (77 bytes): .i..........1.1.168.192.in-addr.arpa.............Q............p.... ..:...Q.
NSOCK INFO [0.1320s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 34
NSOCK INFO [0.1320s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1320s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.1569s) TCP 10.0.2.15:49696 > 192.168.1.1:8080 S ttl=38 id=28289 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1570s) TCP 10.0.2.15:49696 > 192.168.1.1:445 S ttl=40 id=43307 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1571s) TCP 10.0.2.15:49696 > 192.168.1.1:199 S ttl=44 id=64758 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1572s) TCP 10.0.2.15:49696 > 192.168.1.1:139 S ttl=37 id=7655 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1573s) TCP 10.0.2.15:49696 > 192.168.1.1:1025 S ttl=41 id=43680 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1574s) TCP 10.0.2.15:49696 > 192.168.1.1:5900 S ttl=38 id=33770 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1575s) TCP 10.0.2.15:49696 > 192.168.1.1:53 S ttl=37 id=59000 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1576s) TCP 10.0.2.15:49696 > 192.168.1.1:1723 S ttl=52 id=9878 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1577s) TCP 10.0.2.15:49696 > 192.168.1.1:8888 S ttl=37 id=42957 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (0.1578s) TCP 10.0.2.15:49696 > 192.168.1.1:443 S ttl=44 id=49462 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.2699s) TCP 10.0.2.15:49697 > 192.168.1.1:443 S ttl=43 id=31471 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2700s) TCP 10.0.2.15:49697 > 192.168.1.1:8888 S ttl=53 id=64274 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2700s) TCP 10.0.2.15:49697 > 192.168.1.1:1723 S ttl=40 id=5205 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2704s) TCP 10.0.2.15:49697 > 192.168.1.1:53 S ttl=58 id=53174 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2707s) TCP 10.0.2.15:49697 > 192.168.1.1:5900 S ttl=40 id=39396 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2707s) TCP 10.0.2.15:49697 > 192.168.1.1:1025 S ttl=54 id=14613 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2708s) TCP 10.0.2.15:49697 > 192.168.1.1:139 S ttl=59 id=4359 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2709s) TCP 10.0.2.15:49697 > 192.168.1.1:199 S ttl=45 id=47911 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2709s) TCP 10.0.2.15:49697 > 192.168.1.1:445 S ttl=45 id=46128 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.2710s) TCP 10.0.2.15:49697 > 192.168.1.1:8080 S ttl=44 id=26200 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (1.3701s) TCP 10.0.2.15:49696 > 192.168.1.1:256 S ttl=43 id=17393 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3727s) TCP 10.0.2.15:49696 > 192.168.1.1:135 S ttl=46 id=10540 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3728s) TCP 10.0.2.15:49696 > 192.168.1.1:21 S ttl=55 id=15243 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3728s) TCP 10.0.2.15:49696 > 192.168.1.1:25 S ttl=54 id=63180 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3729s) TCP 10.0.2.15:49696 > 192.168.1.1:110 S ttl=48 id=58188 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3729s) TCP 10.0.2.15:49696 > 192.168.1.1:3389 S ttl=50 id=39939 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3729s) TCP 10.0.2.15:49696 > 192.168.1.1:554 S ttl=44 id=15266 iplen=44  seq=1362989577 win=1024 <mss 1460>
SENT (1.3730s) TCP 10.0.2.15:49696 > 192.168.1.1:993 S ttl=41 id=48425 iplen=44  seq=1362989577 win=1024 <mss 1460>
```

```
SENT (4.1188s) TCP 10.0.2.15:49697 > 192.168.1.1:2811 S ttl=51 id=9288 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1285s) TCP 10.0.2.15:49697 > 192.168.1.1:1099 S ttl=39 id=19742 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1286s) TCP 10.0.2.15:49697 > 192.168.1.1:8001 S ttl=42 id=42390 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1287s) TCP 10.0.2.15:49697 > 192.168.1.1:15003 S ttl=51 id=35326 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1288s) TCP 10.0.2.15:49697 > 192.168.1.1:3325 S ttl=47 id=3673 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1290s) TCP 10.0.2.15:49697 > 192.168.1.1:901 S ttl=50 id=52050 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1291s) TCP 10.0.2.15:49697 > 192.168.1.1:8099 S ttl=52 id=45532 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1292s) TCP 10.0.2.15:49697 > 192.168.1.1:12174 S ttl=37 id=15747 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1293s) TCP 10.0.2.15:49697 > 192.168.1.1:10001 S ttl=37 id=9613 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1293s) TCP 10.0.2.15:49697 > 192.168.1.1:49 S ttl=38 id=33132 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1294s) TCP 10.0.2.15:49697 > 192.168.1.1:711 S ttl=50 id=37602 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1295s) TCP 10.0.2.15:49697 > 192.168.1.1:987 S ttl=52 id=9795 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1296s) TCP 10.0.2.15:49697 > 192.168.1.1:1174 S ttl=37 id=23364 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1296s) TCP 10.0.2.15:49697 > 192.168.1.1:5718 S ttl=59 id=45043 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1297s) TCP 10.0.2.15:49697 > 192.168.1.1:34572 S ttl=51 id=51177 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1298s) TCP 10.0.2.15:49697 > 192.168.1.1:9102 S ttl=46 id=32370 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1298s) TCP 10.0.2.15:49697 > 192.168.1.1:32784 S ttl=38 id=60541 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1299s) TCP 10.0.2.15:49697 > 192.168.1.1:1077 S ttl=51 id=7197 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1299s) TCP 10.0.2.15:49697 > 192.168.1.1:3828 S ttl=50 id=15236 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1300s) TCP 10.0.2.15:49697 > 192.168.1.1:9103 S ttl=51 id=59244 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1300s) TCP 10.0.2.15:49697 > 192.168.1.1:3261 S ttl=57 id=7128 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1302s) TCP 10.0.2.15:49697 > 192.168.1.1:212 S ttl=53 id=37806 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1302s) TCP 10.0.2.15:49697 > 192.168.1.1:1114 S ttl=37 id=36092 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1303s) TCP 10.0.2.15:49697 > 192.168.1.1:1085 S ttl=43 id=29136 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1305s) TCP 10.0.2.15:49697 > 192.168.1.1:5822 S ttl=59 id=49864 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1306s) TCP 10.0.2.15:49697 > 192.168.1.1:2065 S ttl=42 id=7986 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1306s) TCP 10.0.2.15:49697 > 192.168.1.1:30951 S ttl=54 id=6538 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1307s) TCP 10.0.2.15:49697 > 192.168.1.1:5901 S ttl=42 id=2906 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1358s) TCP 10.0.2.15:49697 > 192.168.1.1:1051 S ttl=54 id=24807 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1873s) TCP 10.0.2.15:49697 > 192.168.1.1:5987 S ttl=58 id=62078 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1877s) TCP 10.0.2.15:49697 > 192.168.1.1:9929 S ttl=38 id=65214 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1880s) TCP 10.0.2.15:49697 > 192.168.1.1:1805 S ttl=55 id=54014 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1880s) TCP 10.0.2.15:49697 > 192.168.1.1:3390 S ttl=52 id=11494 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1882s) TCP 10.0.2.15:49697 > 192.168.1.1:340 S ttl=58 id=8477 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1882s) TCP 10.0.2.15:49697 > 192.168.1.1:11111 S ttl=37 id=60492 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1883s) TCP 10.0.2.15:49697 > 192.168.1.1:2366 S ttl=45 id=49230 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1914s) TCP 10.0.2.15:49697 > 192.168.1.1:3889 S ttl=46 id=25302 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1916s) TCP 10.0.2.15:49697 > 192.168.1.1:1149 S ttl=50 id=30047 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1917s) TCP 10.0.2.15:49697 > 192.168.1.1:8899 S ttl=45 id=11029 iplen=44  seq=1362924040 win=1024 <mss 1460>
SENT (4.1923s) TCP 10.0.2.15:49697 > 192.168.1.1:6389 S ttl=38 id=51767 iplen=44  seq=1362924040 win=1024 <mss 1460>
Nmap scan report for 192.168.1.1
Host is up (0.0028s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds
```

On Server:

```
adwait@spit:~$ sudo nmap --packet-trace spit.ac.in
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:37 IST
SENT (0.0559s) TCP 127.0.0.1:42527 > 127.0.1.1:21 S ttl=46 id=54560 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0560s) TCP 127.0.0.1:42527 > 127.0.1.1:143 S ttl=59 id=47290 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0561s) TCP 127.0.0.1:42527 > 127.0.1.1:993 S ttl=40 id=59691 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0561s) TCP 127.0.0.1:42527 > 127.0.1.1:53 S ttl=38 id=35583 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0561s) TCP 127.0.0.1:42527 > 127.0.1.1:8888 S ttl=58 id=35113 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0565s) TCP 127.0.0.1:42527 > 127.0.1.1:1025 S ttl=57 id=13718 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0567s) TCP 127.0.0.1:42527 > 127.0.1.1:22 S ttl=45 id=56692 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0567s) TCP 127.0.0.1:42527 > 127.0.1.1:23 S ttl=48 id=35211 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0568s) TCP 127.0.0.1:42527 > 127.0.1.1:3389 S ttl=57 id=15029 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0568s) TCP 127.0.0.1:42527 > 127.0.1.1:443 S ttl=47 id=5876 iplen=44  seq=3497412939 win=1024 <mss 1460>
RCVD (0.0559s) TCP 127.0.1.1:21 > 127.0.0.1:42527 SA ttl=64 id=0 iplen=44  seq=532952202 win=65495 <mss 65495>
RCVD (0.0560s) TCP 127.0.1.1:143 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0561s) TCP 127.0.1.1:993 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0561s) TCP 127.0.1.1:53 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0561s) TCP 127.0.1.1:8888 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0565s) TCP 127.0.1.1:1025 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0567s) TCP 127.0.1.1:22 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0567s) TCP 127.0.1.1:23 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0568s) TCP 127.0.1.1:3389 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0568s) TCP 127.0.1.1:443 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:111 S ttl=43 id=421 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:80 S ttl=53 id=14304 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:445 S ttl=42 id=60354 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:3306 S ttl=49 id=59176 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:135 S ttl=45 id=7945 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:995 S ttl=52 id=27637 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:110 S ttl=55 id=5319 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0572s) TCP 127.0.0.1:42527 > 127.0.1.1:256 S ttl=37 id=5129 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0573s) TCP 127.0.0.1:42527 > 127.0.1.1:199 S ttl=42 id=47526 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0573s) TCP 127.0.0.1:42527 > 127.0.1.1:1720 S ttl=47 id=46201 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0573s) TCP 127.0.0.1:42527 > 127.0.1.1:587 S ttl=53 id=23204 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0573s) TCP 127.0.0.1:42527 > 127.0.1.1:113 S ttl=49 id=51712 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0573s) TCP 127.0.0.1:42527 > 127.0.1.1:1723 S ttl=46 id=23449 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0573s) TCP 127.0.0.1:42527 > 127.0.1.1:8080 S ttl=47 id=41046 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0574s) TCP 127.0.0.1:42527 > 127.0.1.1:25 S ttl=45 id=16507 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0574s) TCP 127.0.0.1:42527 > 127.0.1.1:554 S ttl=49 id=52969 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0574s) TCP 127.0.0.1:42527 > 127.0.1.1:5900 S ttl=44 id=24002 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0575s) TCP 127.0.0.1:42527 > 127.0.1.1:139 S ttl=37 id=541 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0575s) TCP 127.0.0.1:42527 > 127.0.1.1:711 S ttl=53 id=38378 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0575s) TCP 127.0.0.1:42527 > 127.0.1.1:543 S ttl=54 id=30036 iplen=44  seq=3497412939 win=1024 <mss 1460>
RCVD (0.0572s) TCP 127.0.1.1:111 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0572s) TCP 127.0.1.1:80 > 127.0.0.1:42527 SA ttl=64 id=0 iplen=44  seq=4254093121 win=65495 <mss 65495>
RCVD (0.0572s) TCP 127.0.1.1:445 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0572s) TCP 127.0.1.1:3306 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0572s) TCP 127.0.1.1:135 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
```

```
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:3168 S ttl=59 id=4926 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:2383 S ttl=43 id=41581 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:3920 S ttl=54 id=4135 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:992 S ttl=46 id=45340 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:5102 S ttl=45 id=29564 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:720 S ttl=45 id=25836 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:8192 S ttl=37 id=16546 iplen=44  seq=3497412939 win=1024 <mss 1460>
SENT (0.0918s) TCP 127.0.0.1:42527 > 127.0.1.1:3128 S ttl=51 id=16559 iplen=44  seq=3497412939 win=1024 <mss 1460>
RCVD (0.0915s) TCP 127.0.1.1:32777 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:3017 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:4321 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:8009 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:4224 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:1417 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:2107 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:389 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:2190 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:31038 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:9011 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0916s) TCP 127.0.1.1:1027 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:5988 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:1947 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:843 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:2381 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:1244 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:1040 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:4567 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:3370 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0917s) TCP 127.0.1.1:9207 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:10215 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:3168 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:2383 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:3920 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:992 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:5102 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:720 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:8192 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.0918s) TCP 127.0.1.1:3128 > 127.0.0.1:42527 RA ttl=64 id=0 iplen=40  seq=0 win=0
Nmap scan report for spit.ac.in (127.0.1.1)
Host is up (0.0000020s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Web Server Scanning

```
adwait@spit:~$ sudo apt-get install nikto
```

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
  intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58
  libavutil56 libbdplus0 libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0
  libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1
  libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1
  libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4
  librubberband2 libserd-0-0 libshine3 libsord-0-0 libsratom-0-0
  libsrt1.4-gnutls libswresample3 libswscale5 libudfread0 libva-drm2
  libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199
  libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
  linux-image-5.15.0-60-generic linux-modules-5.15.0-60-generic
  linux-modules-extra-5.15.0-60-generic mesa-va-drivers mesa-vdpau-drivers
  pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libwhisker2-perl
The following NEW packages will be installed:
  libwhisker2-perl nikto
0 upgraded, 2 newly installed, 0 to remove and 129 not upgraded.
Need to get 344 kB of archives.
After this operation, 2,207 kB 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 libwhisker2-perl all 2.5-1.2 [98.1 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/multiverse amd64 nikto all 1:2.1.5-3.1 [246 kB]
Fetched 344 kB in 2s (162 kB/s)
Selecting previously unselected package libwhisker2-perl.
(Reading database ... 280430 files and directories currently installed.)
Preparing to unpack .../libwhisker2-perl_2.5-1.2_all.deb ...
Unpacking libwhisker2-perl (2.5-1.2) ...
Selecting previously unselected package nikto.
Preparing to unpack .../nikto_1%3a2.1.5-3.1_all.deb ...
Unpacking nikto (1:2.1.5-3.1) ...
Setting up libwhisker2-perl (2.5-1.2) ...
Setting up nikto (1:2.1.5-3.1) ...
Processing triggers for man-db (2.10.2-1) ...
```

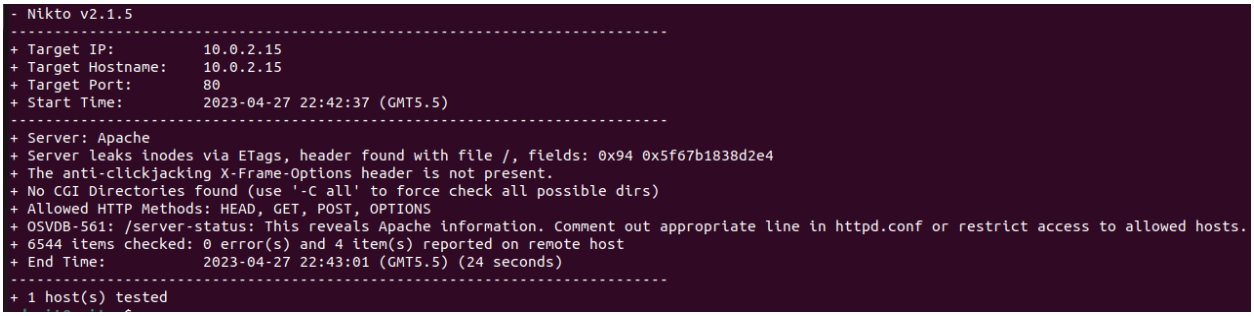
```
adwait@spit:~$ sudo nmap -sT -p80,443 192.168.56.101
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-27 22:41 IST
Nmap scan report for 192.168.56.101
Host is up (0.00080s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

```
adwait@spit:~$ nikto -h 10.0.2.15:80
```



Conclusion:

In the experiment, we gained a comprehensive understanding of the Nmap package and its capabilities. Nmap proved to be a valuable tool in scanning and analyzing networks by detecting the operating system, identifying open ports, and services running on the target system. We also learned about web scanning using nikto, which allowed us to identify potential security risks and vulnerabilities in web applications. Overall, this experience provided us with valuable hands-on experience in using Nmap and nikto, two powerful tools for network and web security professionals.