

NAME: KOMAL MAHESH CHITNIS

MOODLE ID: 20102068

ROLL NO. 26

DIV: A

EXPERIMENT NO. 7

```
komalchitnis02@komal-virtual-machine: ~  
$ sudo apt-get install nmap  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  libblas3 liblinear4 lua-lpeg nmap-common  
Suggested packages:  
  liblinear-tools liblinear-dev ncat ndiff zenmap  
The following NEW packages will be installed:  
  libblas3 liblinear4 lua-lpeg nmap nmap-common  
0 upgraded, 5 newly installed, 0 to remove and 95 not upgraded.  
Need to get 5,553 kB of archives.  
After this operation, 26.3 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1build1 [142 kB]  
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-3build1 [41.7 kB]  
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]  
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap-common all 7.80+dfsg1-2build1 [3,676 kB]  
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap amd64 7.80+dfsg1-2build1 [1,662 kB]  
Fetched 5,553 kB in 12s (449 kB/s)  
Selecting previously unselected package libblas3:amd64.  
(Reading database ... 186032 files and directories currently installed.)  
Preparing to unpack .../libblas3_3.9.0-1build1_amd64.deb ...  
Unpacking libblas3:amd64 (3.9.0-1build1) ...  
Selecting previously unselected package liblinear4:amd64.  
Preparing to unpack .../liblinear4_2.3.0+dfsg-3build1_amd64.deb ...  
Unpacking liblinear4:amd64 (2.3.0+dfsg-3build1) ...  
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_7.80+dfsg1-2build1_all.deb ...  
Unpacking nmap-common (7.80+dfsg1-2build1) ...  
Selecting previously unselected package nmap.  
Preparing to unpack .../nmap_7.80+dfsg1-2build1_amd64.deb ...  
Unpacking nmap (7.80+dfsg1-2build1) ...  
Setting up lua-lpeg:amd64 (1.0.2-1) ...  
Setting up libblas3:amd64 (3.9.0-1build1) ...  
update-alternatives: using /usr/lib/x86_64-linux-gnu/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode  
Setting up nmap-common (7.80+dfsg1-2build1) ...  
Setting up liblinear4:amd64 (2.3.0+dfsg-3build1) ...  
Setting up nmap (7.80+dfsg1-2build1) ...  
Processing triggers for man-db (2.9.1-1) ...  
Processing triggers for libc-bin (2.31-0ubuntu9.7) ...
```

```
komalchitnis02@komal-virtual-machine: ~  
$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.71.130 netmask 255.255.255.0 broadcast 192.168.71.255  
    inet6 fe80::c3bf:a2fb:e9c1:4e4e prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:5f:14:45 txqueuelen 1000 (Ethernet)  
    RX packets 9837 bytes 13456362 (13.4 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3061 bytes 305656 (305.6 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 429 bytes 43650 (43.6 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 429 bytes 43650 (43.6 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
komalchitnis02@komal-virtual-machine:~$ nmap -C  
komalchitnis02@komal-virtual-machine:~$ nmap 192.168.71.130  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:35 IST  
Nmap scan report for komal-virtual-machine (192.168.71.130)  
Host is up (0.00020s latency).  
All 1000 scanned ports on komal-virtual-machine (192.168.71.130) are closed  
  
Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds  
komalchitnis02@komal-virtual-machine:~$ nmap -v 192.168.71.130  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:36 IST  
Initiating Ping Scan at 13:36  
Scanning 192.168.71.130 [2 ports]  
Completed Ping Scan at 13:36, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 13:36  
Completed Parallel DNS resolution of 1 host. at 13:36, 4.06s elapsed  
Initiating Connect Scan at 13:36  
Scanning komal-virtual-machine (192.168.71.130) [1000 ports]  
Completed Connect Scan at 13:36, 0.03s elapsed (1000 total ports)  
Nmap scan report for komal-virtual-machine (192.168.71.130)  
Host is up (0.00021s latency).  
All 1000 scanned ports on komal-virtual-machine (192.168.71.130) are closed  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
```

```
komalchitnis02@komal-virtual-machine:~$ sudo nmap -o 192.168.71.130
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:37 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
komalchitnis02@komal-virtual-machine:~$ sudo nmap -O 192.168.71.130
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:38 IST
Nmap scan report for komal-virtual-machine (192.168.71.130)
Host is up (0.00015s latency).
All 1000 scanned ports on komal-virtual-machine (192.168.71.130) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.97 seconds
```

```
komalchitnis02@komal-virtual-machine:~$ sudo nmap -sV 192.168.71.130
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:39 IST
Nmap scan report for komal-virtual-machine (192.168.71.130)
Host is up (0.000090s latency).
All 1000 scanned ports on komal-virtual-machine (192.168.71.130) are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
komalchitnis02@komal-virtual-machine:~$ sudo nmap -sA 192.168.71.130
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:41 IST
Nmap scan report for komal-virtual-machine (192.168.71.130)
Host is up (0.000060s latency).
All 1000 scanned ports on komal-virtual-machine (192.168.71.130) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds
komalchitnis02@komal-virtual-machine:~$ sudo nmap -sA 192.168.99.2
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:42 IST
Nmap scan report for 192.168.99.2
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.99.2 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
komalchitnis02@komal-virtual-machine:~$ sudo nmap -sP 192.168.3.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:43 IST
Nmap scan report for 192.168.3.0
Host is up (0.00038s latency).
Nmap scan report for 192.168.3.1
Host is up (0.00023s latency).
Nmap scan report for 192.168.3.2
Host is up (1.4s latency).
Nmap scan report for 192.168.3.3
Host is up (0.00027s latency).
Nmap scan report for 192.168.3.4
Host is up (0.00028s latency).
Nmap scan report for 192.168.3.5
Host is up (0.55s latency).
Nmap scan report for 192.168.3.6
Host is up (0.00024s latency).
Nmap scan report for 192.168.3.7
Host is up (0.00026s latency).
Nmap scan report for 192.168.3.8
Host is up (0.00056s latency).
Nmap scan report for 192.168.3.9
Host is up (0.00036s latency).
Nmap scan report for 192.168.3.10
Host is up (0.00028s latency).
Nmap scan report for 192.168.3.11
Host is up (0.00032s latency).
Nmap scan report for 192.168.3.12
```

```
Host is up (0.00033s latency).
Nmap scan report for 192.168.3.245
Host is up (0.00025s latency).
Nmap scan report for 192.168.3.246
Host is up (0.00059s latency).
Nmap scan report for 192.168.3.247
Host is up (0.00063s latency).
Nmap scan report for 192.168.3.248
Host is up (0.00028s latency).
Nmap scan report for 192.168.3.249
Host is up (0.00030s latency).
Nmap scan report for 192.168.3.250
Host is up (0.12s latency).
Nmap scan report for 192.168.3.251
Host is up (0.00028s latency).
Nmap scan report for 192.168.3.252
Host is up (0.00028s latency).
Nmap scan report for 192.168.3.253
Host is up (0.00025s latency).
Nmap scan report for 192.168.3.254
Host is up (0.00028s latency).
Nmap scan report for 192.168.3.255
Host is up (0.00052s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 97.67 seconds
komalchitnis02@komal-virtual-machine:~$ sudo nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:45 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).

komalchitnis02@komal-virtual-machine:~$ sudo nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:47 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).

komalchitnis02@komal-virtual-machine:~$ sudo nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 13:50 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (3.3s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
443/tcp   open      https
514/tcp   filtered  shell
9929/tcp  open      nping-echo
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 225.86 seconds
komalchitnis02@komal-virtual-machine:~$
```