GHARDA FOUNDATION

GHARDA FOUNDATION'S
GHARDA INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

GIT GHARDA INSTITUTE OF TECHNOLOGY

Evaluation Sheet

Class: T.E Computer Engineering **Sem:** VI

Subject: Cryptography and System Security

Experiment No: 11

Date:

Title of Experiment: Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.

Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	12	
2	Oral	2	
3	Timely Submission	1	
	Total	15	

Signature of Subject Teacher
[Vijesh M.Nair]

Output –

```
student@student-HP-Desktop-Pro-G1-MT:~$ sudo apt-get install nmap
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  gir1.2-goa-1.0
Use 'sudo apt autoremove' to remove it.
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 124 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 3.9.0-1bu
ild1 [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+dfsg
1-2build1 [1,662 kB]
Fetched 5,553 kB in 25s (219 kB/s)
```

```
student@student-HP-Desktop-Pro-G1-MT:~$ nmap -sP 192.168.12.93/22
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:24 IST
Nmap scan report for 192.168.12.10
Host is up (0.16s latency).
Nmap scan report for 192.168.12.25
Host is up (0.68s latency).
Nmap scan report for 192.168.12.37
Host is up (0.088s latency).
Nmap scan report for 192.168.12.42
Host is up (0.90s latency).
Nmap scan report for 192.168.12.91
Host is up (2.9s latency).
Nmap scan report for 192.168.12.111
Host is up (1.6s latency).
Nmap scan report for 192.168.12.169
Host is up (0.036s latency).
Nmap scan report for 192.168.12.207
Host is up (0.60s latency).
Nmap scan report for 192.168.13.37
```

```
student@student-HP-Desktop-Pro-G1-MT:~$ sudo nmap -sS www.google.co.in
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:32 IST
Nmap scan report for www.google.co.in (142.250.194.163)
Host is up (0.0059s latency).
Other addresses for www.google.co.in (not scanned): 2404:6800:4002:823::2003
rDNS record for 142.250.194.163: del12s06-in-f3.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 72.47 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ sudo nmap -o 192.168.12.93
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:36 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ sudo nmap -A -sV www.google.co.in
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:37 IST
Failed to resolve "www.google.co.in".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 15.34 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ sudo nmap -sO 192.168.12.93
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:39 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.49 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ sudo nmap -A 192.168.12.93
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:39 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.81 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ nmap -p 8090 192.168.8.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:40 IST
Nmap scan report for _gateway (192.168.8.1)
Host is up (0.0050s latency).

PORT     STATE SERVICE
8090/tcp open  opsmessaging

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

```
student@student-HP-Desktop-Pro-G1-MT:~$ nmap -p 8090 192.168.8.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:40 IST
Nmap scan report for _gateway (192.168.8.1)
Host is up (0.0050s latency).

PORT     STATE SERVICE
8090/tcp open  opsmessaging

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ nmap -p 80,8090 192.168.8.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:40 IST
Nmap scan report for 192.168.8.1
Host is up (0.0012s latency).

PORT     STATE SERVICE
80/tcp   open  http
8090/tcp open  opsmessaging

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
student@student-HP-Desktop-Pro-G1-MT:~$ nmap --top-ports 80 192.168.8.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:42 IST
Nmap scan report for _gateway (192.168.8.1)
Host is up (0.0080s latency).
Not shown: 76 filtered ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
3128/tcp open  squid-http

Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds
```

```
student@student-HP-Desktop-Pro-G1-MT:~$ nmap -iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-11 15:42 IST
************************INTERFACES************************
DEV    (SHORT)  IP/MASK                       TYPE     UP MTU   MAC
lo     (lo)     127.0.0.1/8                   loopback up 65536
lo     (lo)     ::1/128                       loopback up 65536
enp3s0 (enp3s0) 192.168.15.71/21              ethernet up 1500  C4:65:16:11:22:34
enp3s0 (enp3s0) fd80::8279:f772:74a1:a58c/64 ethernet up 1500  C4:65:16:11:22:34
enp3s0 (enp3s0) fe80::834c:f167:2232:6c68/64 ethernet up 1500  C4:65:16:11:22:34
enp3s0 (enp3s0) fd80::2dd7:e3ae:e044:1f3c/64 ethernet up 1500  C4:65:16:11:22:34

**************************ROUTES**************************
DST/MASK                      DEV    METRIC GATEWAY
192.168.8.0/21                enp3s0 100
169.254.0.0/16                enp3s0 1000
0.0.0.0/0                     enp3s0 100    192.168.8.1
::1/128                       lo     0
fd80::2dd7:e3ae:e044:1f3c/128 enp3s0 0
fd80::8279:f772:74a1:a58c/128 enp3s0 0
fe80::834c:f167:2232:6c68/128 enp3s0 0
::1/128                       lo     256
fd80::/64                     enp3s0 100
fe80::/64                     enp3s0 100
ff00::/8                      enp3s0 256
::/0                          enp3s0 20100  fe80::1
```