Experiment No. – 3				
Date of Performance:				
Date of Submission:				
Program Execution/ formation/ correction/ ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 3
Network Discovery tools

3.1Aim: Perform network discovery using discovery tools like NMAP.

3.2Course Outcome: To understand the flow and methodology of an attack.

3.3 Learning Objectives: Network discovery using NMAP.

3.4 Requirement: Kali Linux

3.5 Related Theory:

Nmap ("Network Mapper") is an open-source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key to that information is the "interesting ports table". That

table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.
In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

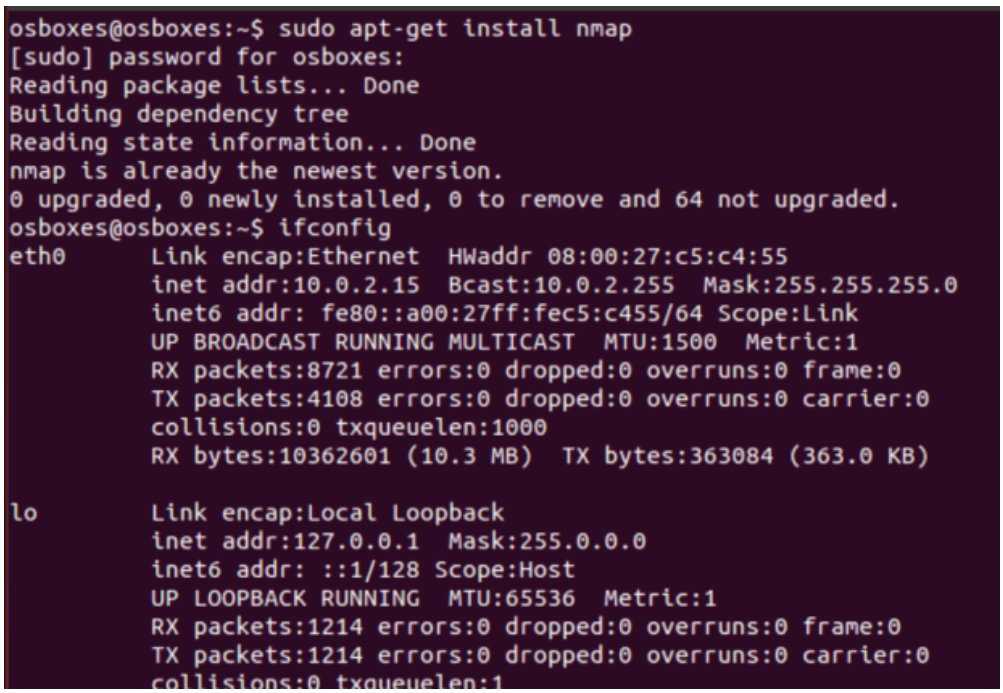


Figure 3.1 Installing nmap

```
osboxes@osboxes:~$ nmap shahandanchor.com

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-14 01:59 EDT
Nmap scan report for shahandanchor.com (192.96.210.12)
Host is up (0.27s latency).
rDNS record for 192.96.210.12: iis1.cloudsector.net
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 23.01 seconds
osboxes@osboxes:~$ nmap 10.0.2.15 10.0.2.2 10.0.2.20

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-14 02:00 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00038s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 3 IP addresses (1 host up) scanned in 1.43 seconds
osboxes@osboxes:~$ nmap 10.0.2.*
```

Figure 3.2 Running nmap

```
Nmap done: 5 IP addresses (3 hosts up) scanned in 6.00 seconds
osboxes@osboxes:~$ nmap -A 10.0.2.15

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-14 02:04 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00037s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http://nmap
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.27 seconds
osboxes@osboxes:~$ sudo nmap -O 10.0.2.15

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-14 02:04 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000037s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
```

Figure 3.3 Running nmap in different modes

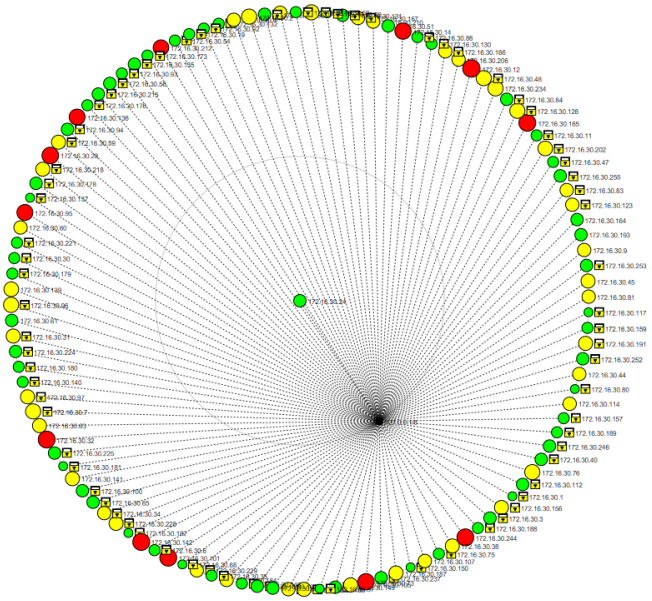
```
osboxes@osboxes:~$ nmap -st 10.0.2.15
nmap: option '-st' is ambiguous; possibilities: '--stylesheet' '--stats-every
--stats_every'
Nmap 6.40 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

Figure 3.4 Running nmap in different modes

3.6 Command Listing and Output:

```
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.239.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 11:19 IST
Nmap scan report for 192.168.239.1
Host is up (0.00048s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
113/tcp  closed ident
8010/tcp closed xmpp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.18
OS details: Linux 2.6.18
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   ...
2   0.31 ms 192.168.239.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.239.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 11:19 IST
Nmap scan report for 192.168.239.1
Host is up (0.00048s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
113/tcp  closed ident
8010/tcp closed xmpp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.18
OS details: Linux 2.6.18
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   ...
2   0.31 ms 192.168.239.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```



3.7 Conclusion:

……

……

……

……

……

……

3.8 Questions:

1. # 192.100.1.1/24 nmap -sp This command is used to perform _____scan.
2. The command for a ping scan is: _____
3. nmap -p 80,443 192.168.1.100 In this command, the number 80 denotes the _____.