

ompleted

AIM:-

This exp outlines the processes that Nmap takes before port scanning to find which systems are online. This stage is critical since attempting to port-scan offline systems will merely waste time and create unwanted network noise.

The following is the information that will be covered in an attempt to discover live hosts.

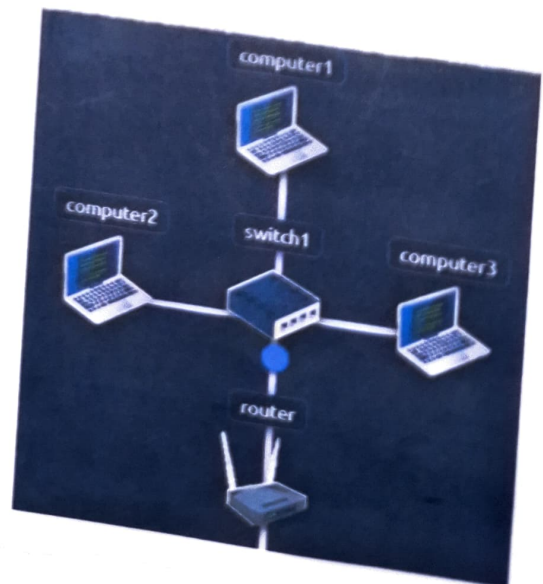
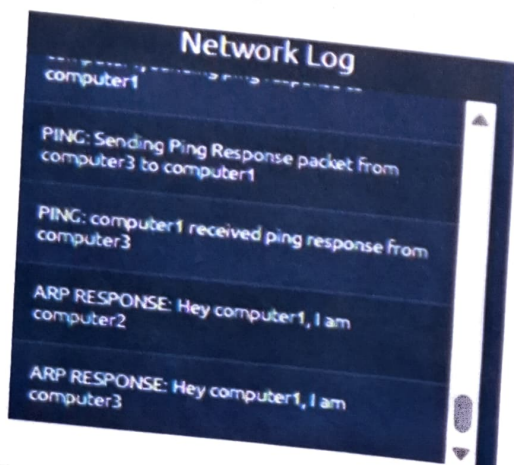
- 1) ARP scan: This scan uses ARP req to discover live hosts.
- 2) ICMP scan: This scan uses ICMP req to identify live hosts.
- 3) TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

There will be two scanners introduced

- 1) arp-scan
- 2) masscan.

Nmap - It is a well-known tool for mapping networks, locating live hosts and detecting running services.

The scans typically follow the steps represented in the image below, but several are optional and are conditional on the command-line options provided prior to the scan.



duced

l for  
hosts,

steps

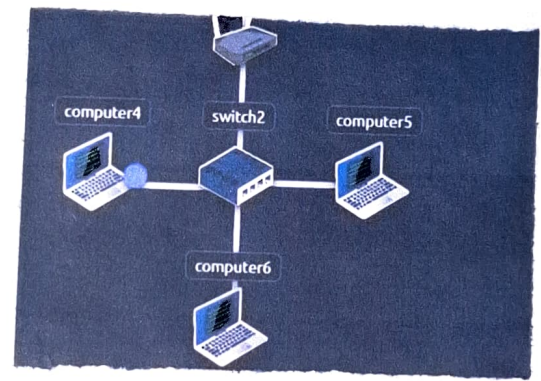
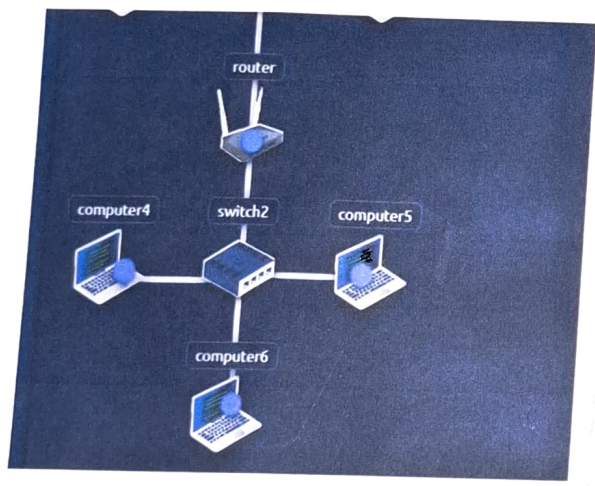
re

time

```
ARP RESPONSE: Hey computer1, I am computer2
ARP RESPONSE: Hey computer1, I am computer3
ARP RESPONSE: Hey computer1, I am computer2
ARP RESPONSE: Hey computer1, I am router
```

### Network Log

```
PING: Sending Ping Request packet from computer1 to computer3
PING: computer3 received ping request from computer1, sending ping response to computer1
PING: Sending Ping Response packet from computer3 to computer1
PING: computer1 received ping response from computer3
```



- 1 Enumerate targets
- 2 Discover the hosts
- 3 Reverse-DNS lookup
- 4 Scan ports
- 5 Detect versions
- 6 Detect OS
- 7 Traceroute
- 8 Scripts
- 9 Write output

18/10

Result:

Thus the above experiment is completed successfully