18/9/25

Experiment 8

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 unneeded 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

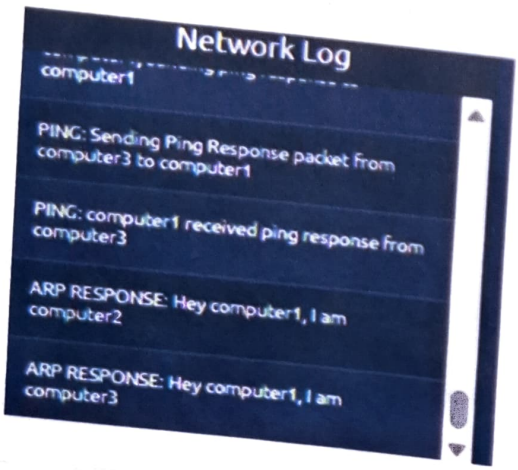
There will be two scanners introduced

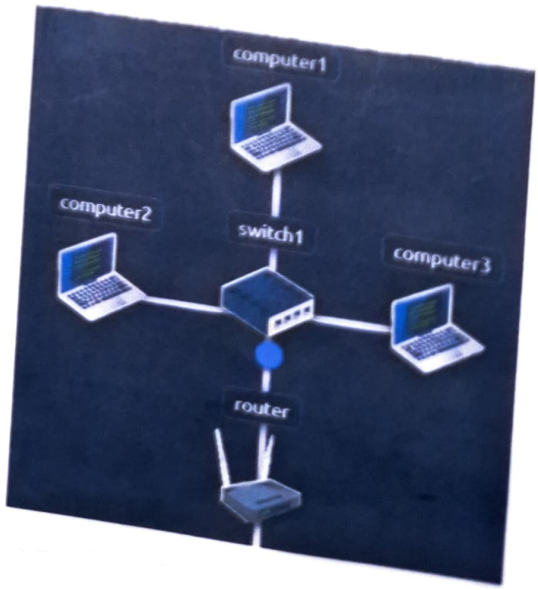
1) arp-scan

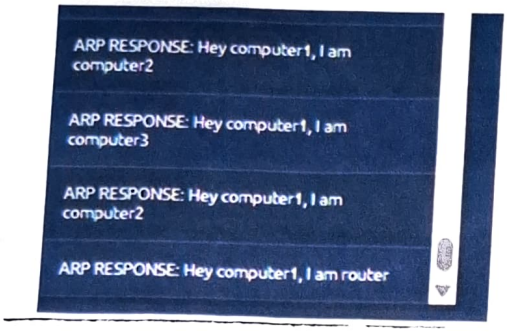
2) Masscan.

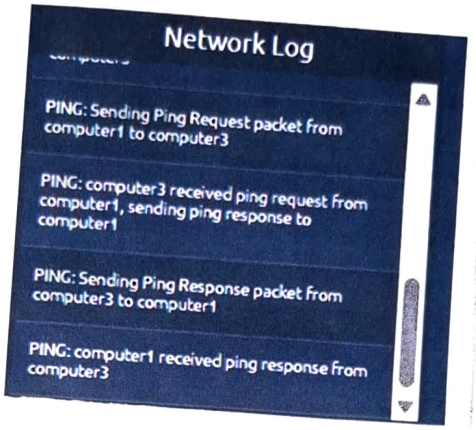
Nmap - It is a well-known tool for mapping networks, locating live hosts and detecting running services

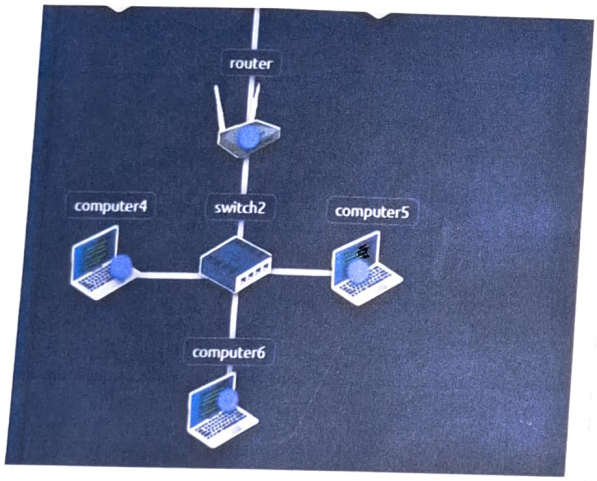
The scans typically follow the steps represented in the image below, but several are optional and are conditional on the command-line options. provided prior to the scan.

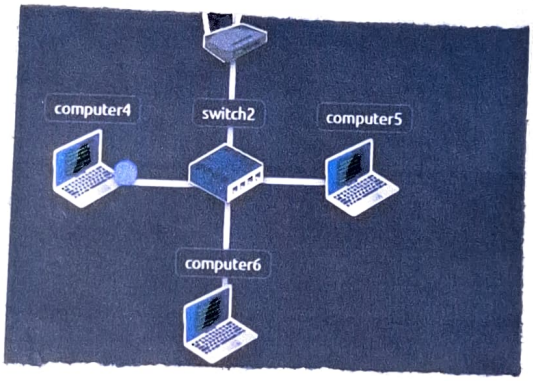


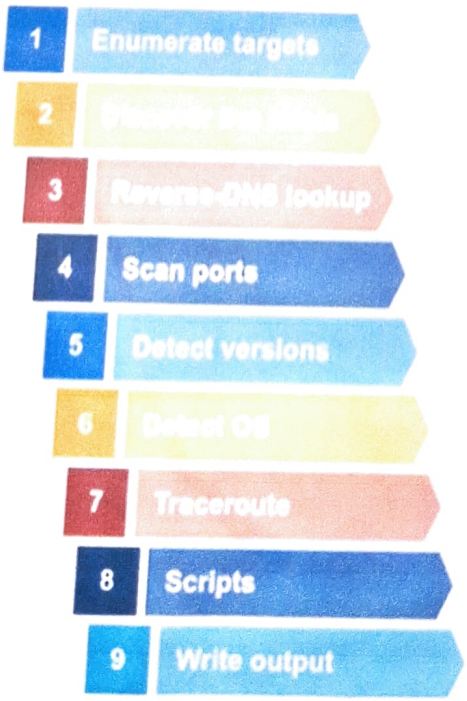












Result :-

Thus the above experiment is completed sucessfully