Exp No: 8
Date: 17.9.2025

Experiment on outliving the processes in NMAP, before port scanning to find system.

AIM:

To attempt to port scan offline systems and recognize the waste time and created unneeded network (because it is active recon).

The ARP scan:

This scan uses ARP requests to discover live hosts.

ICMP scan:

This scan uses ICMP requests to identify live hosts.

TCP/UDP Ping scan:

This scan sends packets to TCP ports and UDP ports to determine live hosts

There will be 2 scanners introduced

1) arp-scan
2) nmap

NMAP (network mapper) It is a well known tool for mapping networks, locating live hosts and detecting running services NMAP's scripting engine can be used to extend its capabilities such as fingerprinting services and exploiting

flaws. 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.

step 1: Enumerate the targets

step 2: Discover live hosts.

step 3: Reverse DNS lookup

step 4: scan ports

step 5: Detect versions

step 6: Detect OS

step 7: Traceroute

step 8: scripts.

step 9: write output.

Result: Hence the experiment on outliving the processes in the NMAP port scanning is done successfully.