EXPERIMENT : 8
Date: 17.09.25

EXPERIMENT ON OUTLINING THE PROCESSOR IN NMAP BEFORE POST SCANNING TO FIND OUTLINING SYSTEM.

AIM:

To attempt to port scan offline systems and recognize the waste time and the 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 request to identify live hosts.

TCP/UDP ping Scan:

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

There will be 2 scanners introduced:

1) arp_scan
2) Mass can.

NMAP (network mapper) It is a well known tool for mapping network, 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:

Step1: Enumerate the targets.

Step2: Discover live host

Step3: Reverse DNS lookup

Step4: Scan ports

Step5: Detect versions.

Step6: Detect os

Step7: Traceroute

Step8: Script

Step9: write output.

Result:

Hence the experiment on outlining the process in NMAP port scaning is done successfully