

2.9.2025

EXP No: 8

Experiment on outlining the process in NMAP before port scanning to find online system.

AIM:

To attempt to port scan offline system and recognize the waste time and the created unneeded network noise (because it is active scanner)

The ARP scan uses ARP requests to discover live hosts.

ICMP scan: This scan uses ARP 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) masscan

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 exploring flows. The scans typically follow the steps represented in the image below, but 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 outputting the processes in NMAP port scanning is completed successfully.