Ex No: 8

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

Aim:
To attempt the port scan offline systems and Recognizes the waste time & the created unneeded network (because it is active recon)

The ARP Scan:
This Scan uses ARP Requests to discover live hosts 3.

ICMP Scan:
This Scan uses ICMP Requests 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 2 Scanners introduced:
(1) arp-scan
(2) mass scan

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 follows 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: Trace Route
Step 8: Scripts
Step 9: Write output

Result:-
Hence the experiment on outlining the Processes in NMAP port Scanning is done Successfully.