Experiment on outlining the processes in NMAI

Before Port Scanning Red Online System

**Aim:**

To attempt to port scan offline system and recognises the wastes time and the created connected network

**The ARP Scan!**

This scan uses ARP requests to discover like hosts

**ICMP Scan:**

This scan uses ICMP requests to identify live host 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 (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. The scans typically follow the step represented in the image below, but several are optional and or conditional on the command-line options provided prior to the scan.

Step : 1   enumerates   the   targets

Step : 2   Discover   live   hosts

Step : 3   Reverse   DNS   Lookup

Step : 4   Scans ports

Step : 5   Detect   versions

Step : 6   Detect   OS

Step : 7   Traceroute

Step : 8   run   scripts

Step : 9   writes   output

**Result**

     Hence the 1st experiment on referring the processes in NMAP port Scanning is done Successfully.