DISCOVER LIVE HOSTS USING NMAP SCANS

AIM:

To Discover Live Hosts Using Nmap Scans

This experiment outlines the processes that Nmap takes before portscanning to find which systems are online. This stage is critical since attempting to port-scan offline systems will merely waste time & create unneeded network noise.

The Following is the information that will be covered in an attempt to discover live hosts:

1) ARP scan:
   Uses ARP request to discover live host

2) ICMP scan:
   Uses ICMP request to discover live host

3) TCP/UDP ping scan:
   This scan sends packets to TCP ports & UDP ports to determine live hosts.

There will be two scanners introduced:

→ Arp-scan
→ masscan

Nmap:

It is a well-known tool for mapping networks, locating live hosts, & detecting running services.
Nmap's scripting engine can be used to extend its capabilities, such as fingerprinting services & exploiting flaws.

The scans typically follow the steps represented in the image below, but several are optional & are conditional on the "command line".

OPTIONS PROVIDED PRIOR TO SCAN:

→ Enumerate Targets
→ Discover Live Host
→ Reverse DNS lookup
→ Scan Ports
→ Detect versions
→ Detect OS
→ Traceroute
→ Scripts
→ Write output

CONCLUSION:

We can use several forms of "Port" scanning to get a certain result.

eg) MS windows blocks ICMP requests, which may not be very beneficial if we know the "target" is using it, but it's still good idea to utilize it if they are using another type of machine.

RESULT:

NMap discovery of Live Host on Try hack me was implemented successfully.