Ex: 8

# NMAP to discover Live hosts using nmap scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform

Aim:-

This equipment outlines the processes that Nmap takes before port-scanning to find which systems are online. This stage is Critical since attempting to port scan offline systems will merely waste time and create unneeded network noise.

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

1) ARP scan: This scan uses ARP requests to discover live hosts 2) 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 two scanners introduced:

1. arp scan
2. masscan

Nmap (Network Map) - 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:

1. Enumerate targets
2. Discover live hosts
3. Reverse-DNS lookup
4. Scan ports
5. Detect versions
6. Detect OS
7. Traceroute
8. Scripts
9. Write o/p

Result:

Thus the above program is executed successfully.