11.09.25

Experiment - 8

Aim: To discover Live hosts using Nmap Scans on the tryHackMe platform room

This experiment outlines the process that Nmap takes before port scanning to find which systems are online. This stage is critical since attempting to pre-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:

There will be two scanners introduced

1. arp-scan
2. nmap

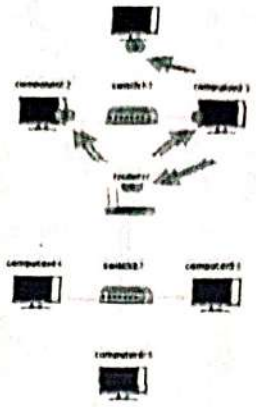
Nmap (network Mapper) - It is a well-known tool for mapping network. locating live hosts and detecting running services

Nmap's Scripting engine can be used to extend its capabilities such as fingerprinting services and exploiting flaws

A Nmap scan usually goes through steps, as in figure below:

1. Enumerate targets
2. Discover Live hosts
3. Reverse DNS
4. Scan port
5. Detect versions
6. Detect OS
7. Trace Route
8. Scripts
9. Write output

output



Result:

Thus we learnt how ARP, ICMP, TCP and UDP can detect the hosts by completing the tryHackMe room.