8/9/25

Practical-8.

Aim:

To discover Live Hosts Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe platform. Room Link:

https://tryhackme.com/room/nmapo1

This experiment outlines the process that Nmap takes before port-scanning to find which systems are online. This stage is critical since attempting to portscan offline systems will merely waste time and create unneeded network noise (because it is active recon)

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 / ~~SCTP~~ UDP ping scan
This scan sends packets to TCP ports and UDP ports to determine live hosts.

3. ICMP scan
This scan uses ICMP requests to identify live hosts.

There will be two 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. Nmaps scripting engine can be used to extend its capabilities, such as fingerprinting services 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 Output

Hence!

The discovery of live host Nmap was on try Hacleme performed successfully 9/10/23