EXPNO: 8

24/9/25

NMAP to discover Live Hosts using Nmap scans (ARP, ICMP, TCP/UDP) on the Try Hack me platforms.

Aim:-

This experiment outlines the process that nmap takes before port scanning to find which system 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, arpscan

2, masian.

Nmap (networking Mappin) It is a well known tool for mapping networking, locating livehosts and deteting running services, Nmap's

scriptingengine 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 outputs.

Result: Thus the clone program is created sucesfully.