

11.09.25

## Experiment - 8,

Aim: To discover Live hosts using Nmap Scans on the toy Hack Me platform.com

This experiment outlines the process 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 unwanted 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 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

A Nmap scan usually goes through steps like  
in figure

below :

1. Enumerate targets
2. Discover Live hosts
3. Reverse DNS
4. Scan port
5. Detect version
6. Detect OS
7. Trace Route

8. Scripts

9. Write output



output



TCP/IP Packet	
TCP Header	
Source Port	Destination Port
Sequence Number	Window Size
Checksum	Options
TCP Trailer	
IP Header	
Version	Header Length
Type of Service	Total Length
Identification	Flags
Fragment Offset	Time to Live
Protocol	Source Address
Destination Address	
IP Trailer	

Handwritten notes in the right margin, including "12/12/2020" and other illegible text.

Handwritten notes in the middle section, including "The network is a local area network (LAN) and is used for communication between devices connected to the same network." and "The network is a local area network (LAN) and is used for communication between devices connected to the same network."

Result:

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