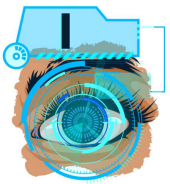
Jr Penetration Tester > Network Security > Nmap Live Host Discovery



Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

Medium 120 min

Access Machines 4 1

Task 1 Introduction

Room completed (100%)

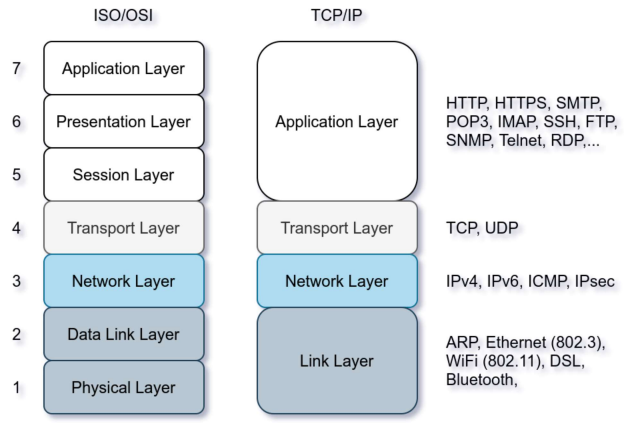
Task 2 Subnetworks

Task 3 Enumerating Targets

Task 4 Discovering Live Hosts

Let's revisit the TCP/IP layers shown in the figure next. We will leverage the protocols to discover the live hosts. Starting from bottom to top, we can use:

- ARP from Link Layer
- ICMP from Network Layer
- TCP from Transport Layer
- UDP from Transport Layer



Before we discuss how scanners can use each in detail, we will briefly review these four protocols. ARP has one purpose: sending a frame to the broadcast address on the network segment and asking the computer with a specific IP address to respond by providing its MAC (hardware) address.

ICMP has many types. ICMP ping uses Type 8 (Echo) and Type 0 (Echo Reply).

If you want to ping a system on the same subnet, an ARP query should precede the ICMP Echo.

Although TCP and UDP are transport layers, for network scanning purposes, a scanner can send a specially-crafted packet to common TCP or UDP ports to check whether the target will respond. This method is efficient, especially when ICMP Echo is blocked.

If you have closed the network simulator, click on the “View Site” button in Task 2 to display it again.

Answer the questions below

Send a packet with the following:

- From computer1
- To computer3
- Packet Type: “Ping Request”

What is the type of packet that computer1 sent before the ping?

ARP Request ✓ Correct Answer

What is the type of packet that computer1 received before being able to send the ping?

ARP Response ✓ Correct Answer

How many computers responded to the ping request?

1 ✓ Correct Answer

Send a packet with the following:

- From computer2
- To computer5
- Packet Type: “Ping Request”

What is the name of the first device that responded to the first ARP Request?

router ✓ Correct Answer

What is the name of the first device that responded to the second ARP Request?

computer5 ✓ Correct Answer

Send another Ping Request. Did it require new ARP Requests? (Y/N)

N ✓ Correct Answer

Task 5 Nmap Host Discovery Using ARP

Task 6 Nmap Host Discovery Using ICMP

Task 7 Nmap Host Discovery Using TCP and UDP

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

Created by

 tryhackme  strategos

Room Type	Users in Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	168,140	1064 days ago