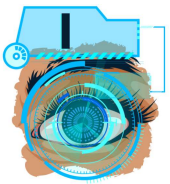
Jr Penetration Tester > Network Security > Nmap Live Host Discovery



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

Show Split View | Start AttackBox | Help | Save Room

3754 | Options

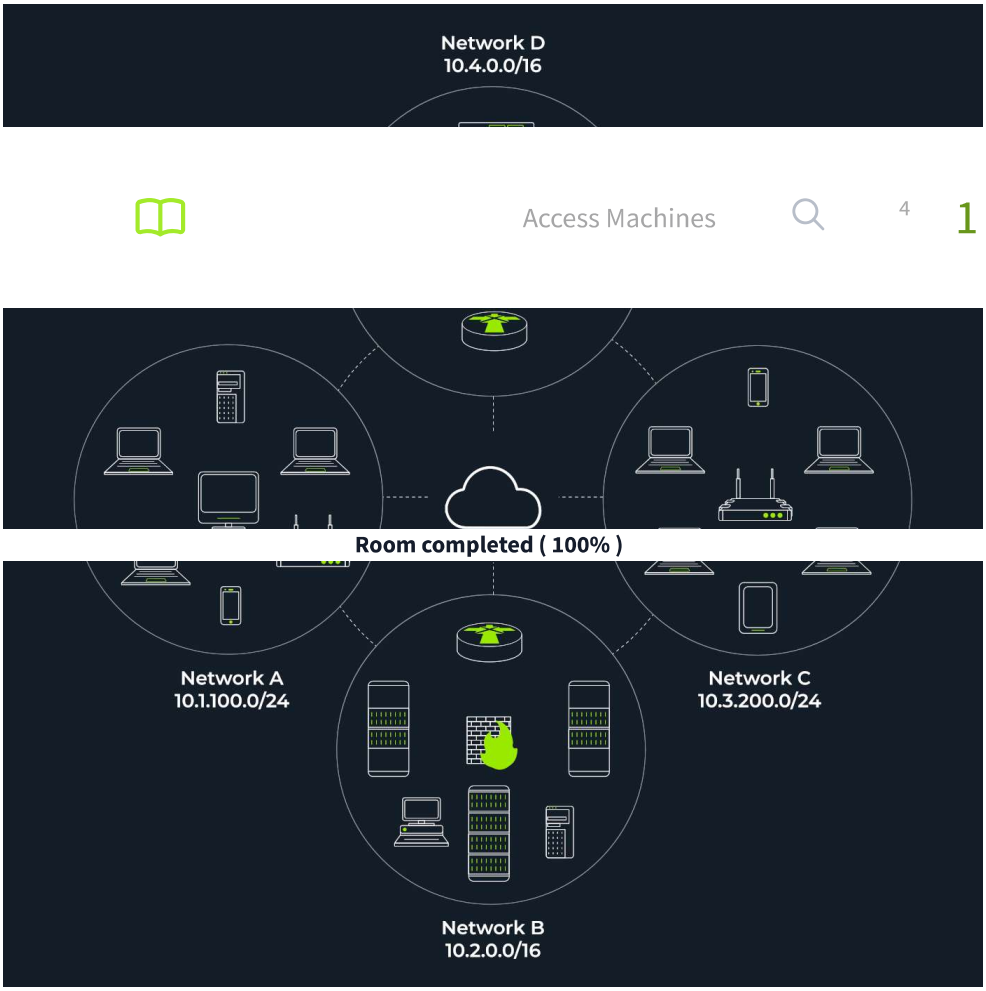
Task 1 Introduction

Task 2 Subnetworks

View Site

Let's review a couple of terms before we move on to the main tasks. A *network segment* is a group of computers connected using a shared medium. For instance, the medium can be the Ethernet switch or WiFi access point. In an IP network, a *subnetwork* is usually the equivalent of one or more network segments connected together and configured to use the same router. The network segment refers to a physical connection, while a subnetwork refers to a logical connection.

In the following network diagram, we have four network segments or subnetworks. Generally speaking, your system would be connected to one of these network segments/subnetworks. A subnetwork, or simply a subnet, has its own IP address range and is connected to a more extensive network via a router. There might be a firewall enforcing security policies depending on each network.



The figure above shows two types of subnets:

- Subnets with `/16`, which means that the subnet mask can be written as `255.255.0.0`. This subnet can have around 65 thousand hosts.
- Subnets with `/24`, which indicates that the subnet mask can be expressed as `255.255.255.0`. This subnet can have around 250 hosts.

You might want to refer to Task 2 in the Intro to LAN room if you need to learn more about subnetting.

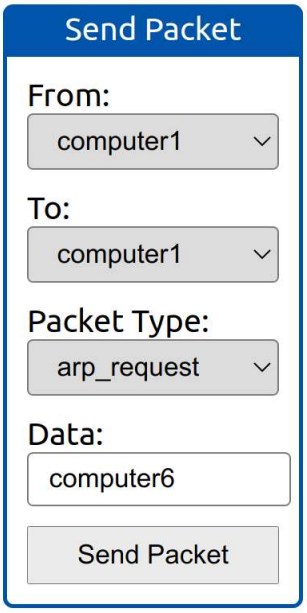
As part of active reconnaissance, we want to discover more information about a group of hosts or about a subnet. If you are connected to the same subnet, you would expect your scanner to rely on ARP (Address Resolution Protocol) queries to discover live hosts. An ARP query aims to get the hardware address (MAC address) so that communication over the link-layer becomes possible; however, we can use this to infer that the host is online. (We revisit link-layer in Task 4.)

If you are in Network A, you can use ARP only to discover the devices within that subnet (10.1.100.0/24). Suppose you are connected to a subnet different from the subnet of the target system(s). In that case, all packets generated by your scanner will be routed via the default gateway (router) to reach the systems on another subnet; however, the ARP queries won't be routed and hence cannot cross the subnet router. ARP is a link-layer protocol, and ARP packets are bound to their subnet.

Click on the "View Site" button to start the network simulator. We will use this simulator to answer the questions in tasks 2, 4, and 5.

Answer the questions below

Send a packet with the following:



- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

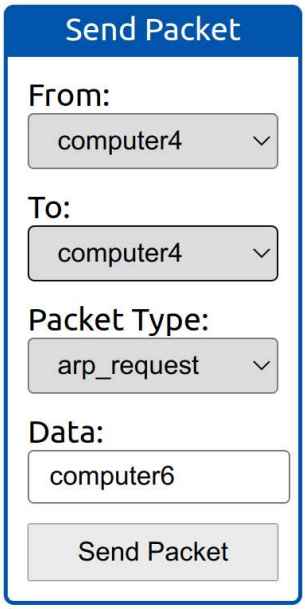
How many devices can see the ARP Request?

4 ✓ Correct Answer Hint

Did computer6 receive the ARP Request? (Y/N)

N ✓ Correct Answer

Send a packet with the following:



- From computer4
- To computer4 (to indicate it is broadcast)
- Packet Type: “ARP Request”
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4 ✓ Correct Answer Hint

Did computer6 reply to the ARP Request? (Y/N)

Y ✓ Correct Answer

Task 3 Enumerating Targets

Task 4 Discovering Live Hosts

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