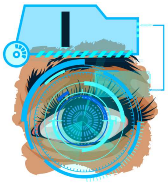
Jr Penetration Tester > Network Security > Nmap Live Host Discovery



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

Task 3 ✓ Enumerating Targets

Task 4 ✓ Discovering Live Hosts

Task 5 ✓ Nmap Host Discovery Using ARP

How would you know which hosts are up and running? It is essential to avoid wasting our time port-scanning an offline host or an IP address not in use. There are various ways to discover online hosts. When no host discovery options are provided, Nmap follows the following approaches to discover live hosts:

1. When a *privileged* user tries to scan targets on a local network (Ethernet), Nmap uses *ARP requests*. A privileged user is `root` or a user who belongs to `sudoers` and can run `sudo` .
2. When a *privileged* user tries to scan targets outside the local network, Nmap uses ICMP echo requests, TCP ACK (Acknowledge) to port 80, TCP SYN (Synchronize) to port 443, and ICMP timestamp request.
3. When an *unprivileged* user tries to scan targets outside the local network, Nmap resorts to a TCP 3-way handshake by sending SYN packets to ports 80 and 443

`nmap -sn TARGETS` . Let's dig deeper to gain a solid understanding of the different techniques used.

ARP scan is possible only if you are on the same subnet as the target systems. On an Ethernet (802.3) and WiFi (802.11), you need to know the MAC address of any system before you can

Room completed (100%)

communicate with it. The MAC address is necessary for the link-layer header; the header contains the source MAC address and the destination MAC address among other fields. To get the MAC address, the OS sends an ARP query. A host that replies to ARP queries is up. The ARP query only works if the target is on the same subnet as yourself, i.e., on the same Ethernet/WiFi. You should expect to see many ARP queries generated during a Nmap scan of a local network. If you want Nmap only to perform an ARP scan without port-scanning, you can use `nmap -PR -sn TARGETS` , where `-PR` indicates that you only want an ARP scan. The following example shows Nmap using ARP for host discovery without any port scanning. We run `nmap -PR -sn MACHINE_IP/24` to discover all the live systems on the same subnet as our target machine.

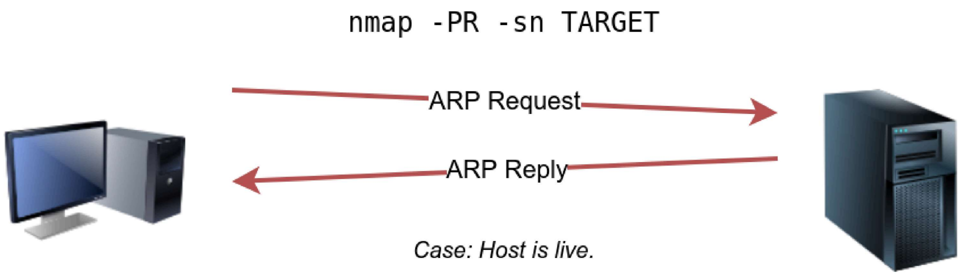
Pentester Terminal

```
pentester@TryHackMe$ sudo nmap -PR -sn 10.10.210.6/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 07:12 BST
Nmap scan report for ip-10-10-210-75.eu-west-1.compute.internal
(10.10.210.75)
Host is up (0.00013s latency).
MAC Address: 02:83:75:3A:F2:89 (Unknown)
Nmap scan report for ip-10-10-210-100.eu-west-1.compute.internal
(10.10.210.100)
Host is up (-0.100s latency).
MAC Address: 02:63:D0:1B:2D:CD (Unknown)
Nmap scan report for ip-10-10-210-165.eu-west-1.compute.internal
```

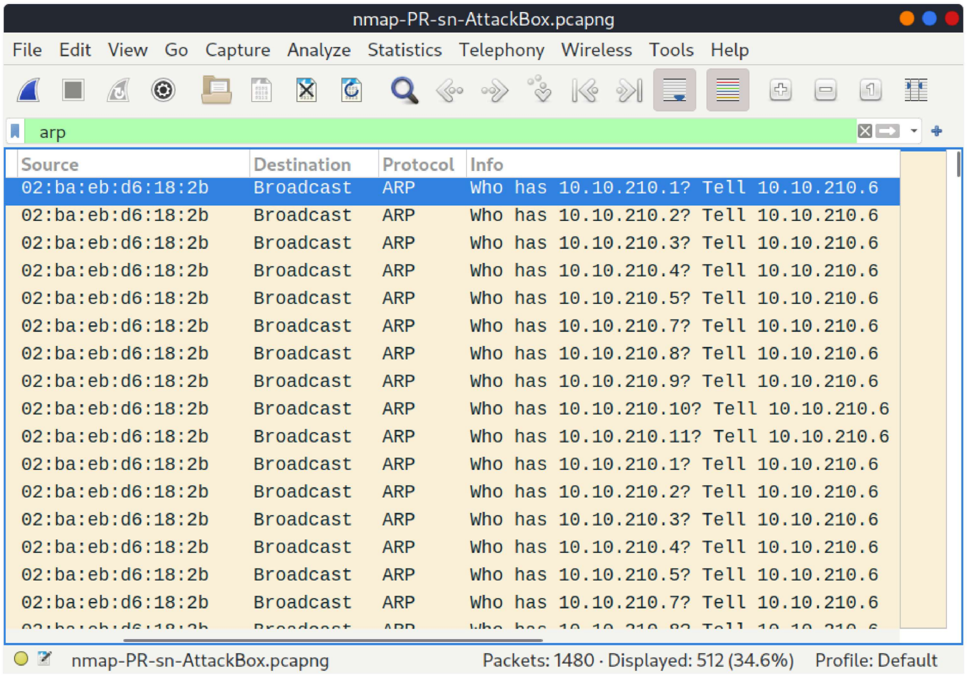
```
(10.10.210.165)
Host is up (0.00025s latency).
MAC Address: 02:59:79:4F:17:B7 (Unknown)
Nmap scan report for ip-10-10-210-6.eu-west-1.compute.internal
(10.10.210.6)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.12 seconds
```

In this case, the AttackBox had the IP address 10.10.210.6, and it used ARP requests to discover the live hosts on the same subnet. ARP scan works, as shown in the figure below. Nmap sends ARP requests to all the target computers, and those online should send an ARP reply back.



Case: Host is live.

If we look at the packets generated using a tool such as tcpdump or Wireshark, we will see network traffic similar to the figure below. In the figure below, Wireshark displays the source MAC address, destination MAC address, protocol, and query related to each ARP request. The source address is the MAC address of our AttackBox, while the destination is the broadcast address as we don't know the MAC address of the target. However, we see the target's IP address, which appears in the Info column. In the figure, we can see that we are requesting the MAC addresses of all the IP addresses on the subnet, starting with `10.10.210.1` . The host with the IP address we are asking about will send an ARP reply with its MAC address, and that's how we will know that it is online.


nmap-PR-sn-AttackBox.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

Source	Destination	Protocol	Info
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6

nmap-PR-sn-AttackBox.pcapng Packets: 1480 · Displayed: 512 (34.6%) Profile: Default

Talking about ARP scans, we should mention a scanner built around ARP queries: `arp-scan` ; it provides many options to customize your scan. Visit the arp-scan wiki for detailed information. One popular choice is `arp-scan --localnet` or simply `arp-scan -l` . This command will send ARP queries to all valid IP addresses on your local networks. Moreover, if your system has more than one interface and you are interested in discovering the live hosts on one of them, you can specify the interface using `-I` . For instance, `sudo arp-scan -I eth0 -l` will send ARP queries for all valid IP addresses on the `eth0` interface.

Note that `arp-scan` is not installed on the AttackBox; however, it can be installed using `apt install arp-scan` .

In the example below, we scanned the subnet of the AttackBox using `arp-scan ATTACKBOX_IP/24` . Since we ran this scan at a time frame close to the previous one `nmap -PR -sn ATTACKBOX_IP/24` , we obtained the same three live targets.

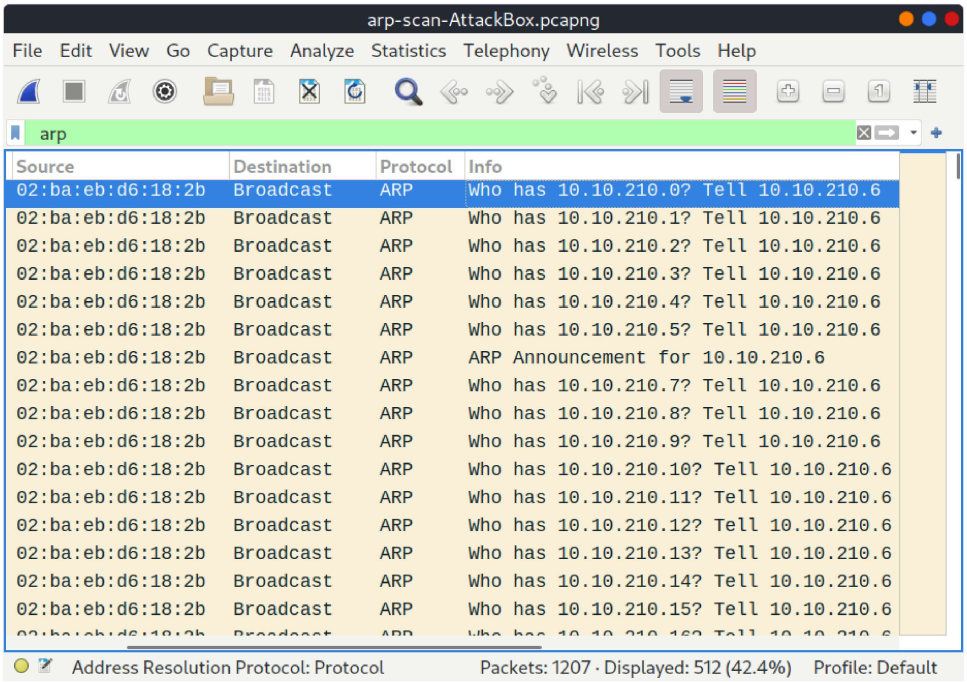
Pentester Terminal

```
pentester@TryHackMe$ sudo arp-scan 10.10.210.6/24
Interface: eth0, datalink type: EN10MB (Ethernet)
WARNING: host part of 10.10.210.6/24 is non-zero
Starting arp-scan 1.9 with 256 hosts (http://www.nta-
monitor.com/tools/arp-scan/)
10.10.210.75     02:83:75:3a:f2:89    (Unknown)
10.10.210.100    02:63:d0:1b:2d:cd    (Unknown)
```

```
10.10.210.165   02:59:79:4f:17:b7   (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.726 seconds (93.91
hosts/sec). 3 responded
```

Similarly, the command `arp-scan` will generate many ARP queries that we can see using tcpdump, Wireshark, or a similar tool. We can notice that the packet capture for `arp-scan` and `nmap -PR -sn` yield similar traffic patterns. Below is the Wireshark output.


arp-scan-AttackBox.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

Source	Destination	Protocol	Info
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.0? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	ARP Announcement for 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.12? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.13? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.14? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.15? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.16? Tell 10.10.210.6

Address Resolution Protocol: Protocol   Packets: 1207 · Displayed: 512 (42.4%)   Profile: Default

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

Answer the questions below

We will be sending broadcast ARP Requests packets with the following options:

- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: “ARP Request”
- Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

How many devices are you able to discover using ARP requests?

3 | ✓ Correct Answer

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