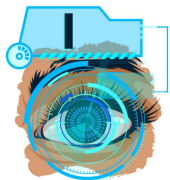Jr Penetration Tester > Network Security > Nmap Live Host Discovery

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 ▾ |

📖   Access Machines   🔍   4   1🔥   🫙

Task 2 ✅ Subnetworks   🗔   ▾

Room completed (100%)

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

You have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room. Any response from a host is an indication that it is online. Below is a quick summary of the command-line options for Nmap that we have covered.

Scan Type	Example Command
ARP Scan	`sudo nmap -PR -sn MACHINE_IP/24`
ICMP Echo Scan	`sudo nmap -PE -sn MACHINE_IP/24`
ICMP Timestamp Scan	`sudo nmap -PP -sn MACHINE_IP/24`
ICMP Address Mask Scan	`sudo nmap -PM -sn MACHINE_IP/24`
TCP SYN Ping Scan	`sudo nmap -PS22,80,443 -sn MACHINE_IP/30`
TCP ACK Ping Scan	`sudo nmap -PA22,80,443 -sn MACHINE_IP/30`
UDP Ping Scan	`sudo nmap -PU53,161,162 -sn MACHINE_IP/30`

Remember to add `-sn` if you are only interested in host discovery without port-scanning. Omitting `-sn` will let Nmap default to port-scanning the live hosts.

Option	Purpose
`-n`	no DNS lookup
`-R`	reverse-DNS lookup for all hosts
`-sn`	host discovery only

Answer the questions below

Ensure you have taken note of all the Nmap options explained in this room. To continue learning about Nmap, please join the room Nmap Basic Port Scans, which introduces the basic types of port scans.

No answer needed	✓ Correct Answer

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