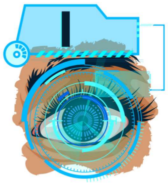
Jr Penetration Tester > Network Security > Nmap Live Host Discovery



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

3754 Options

Room completed (100%)

Task 1 Introduction

When we want to target a network, we want to find an efficient tool to help us handle repetitive tasks and answer the following questions:

1. Which systems are up?
2. What services are running on these systems?

The tool that we will rely on is Nmap. The first question about finding live computers is answered in this room. This room is the first in a series of four rooms dedicated to Nmap. The second question about discovering running services is answered in the next Nmap rooms that focus on port-scanning.

This room is the first of four in this Nmap series. These four rooms are also part of the Network Security module.

1. Nmap Live Host Discovery
2. Nmap Basic Port Scans

3. Nmap Advanced Port Scans
4. Nmap Post Port Scans

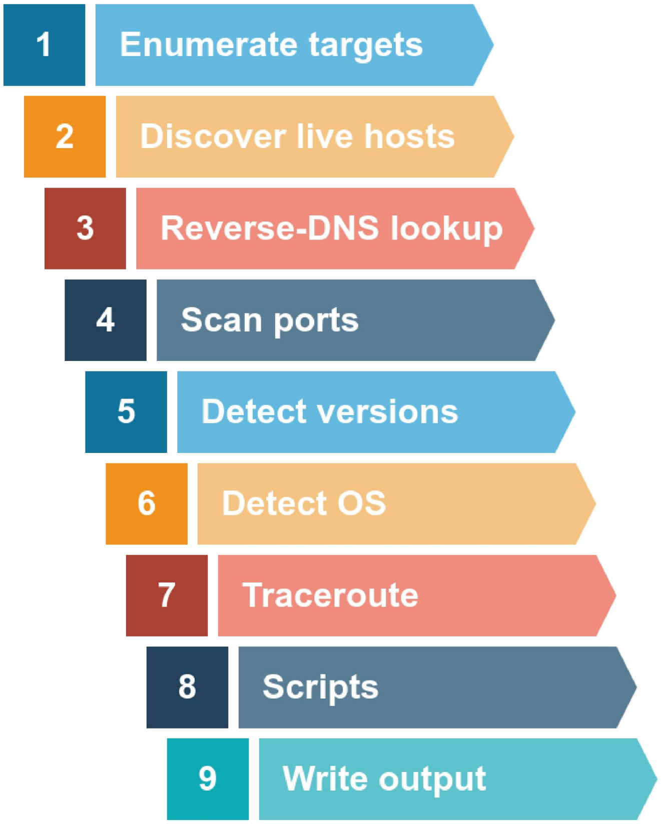
This room explains the steps that Nmap carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that Nmap uses to discover live hosts. In particular, we cover:

1. ARP scan: This scan uses ARP requests to discover live hosts
2. ICMP scan: This scan uses ICMP requests to identify live hosts
3. TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

We also introduce two scanners, `arp-scan` and `masscan`, and explain how they overlap with part of Nmap's host discovery.

As already mentioned, starting with this room, we will use Nmap to discover systems and services actively. Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under GPL license. Nmap is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services. Nmap's scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities. A Nmap scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.



Answer the questions below

Some of these questions will require the use of a static site to answer the task questions, while others require the use of the AttackBox and the target VM.

No answer needed

✓ Correct Answer

Task 2 ✓ Subnetworks

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