Labs

< back to dashboard

Nmap Essentials 101 ♥ EXPIRED

Perform reconnaissance with nmap to reveal hidden secrets

`15-45 Minutes` `250 Points` `2/10 Difficulty`

Start Stop

✓ You have already completed this exercise.

Mission Statement | Verify Flags | Solution

Nmap ("Network Mapper") is a network reconnaissance tool that helps you discover live hosts and open ports on a network.
It is one of the most widely used tools by System Administrators and Penetrations Testers alike. Where SysAdmins use it for managing devices on a network, penetration testers use it to gather information about a network to further use it for possible exploitation into the network.

Being an active scanner, Nmap is often detected and blocked by firewalls. But to begin with the network scanner tool, we will be using a real-world scenario without a firewall blocking our scans.

This lab will help you learn:

1. How to scan open ports on a server
2. How to identify running service and its version
3. How to scan an entire sub-network and find live hosts.

Complete the following challenges to acquire the general Nmap recon skills:

1. Which service is running on port 22 for IP `10.1.3.2`
2. Identify server running Samba on port 445
3. What is the version of Redis running on server `10.1.3.9`
4. Redis server is running on which port number?
5. Identify the server running on port 8090 and Retrieve Flag using curl from user-agent headers

Note:
This lab is an environment dedicated to you exclusively. That means this environment is never shared with any other student. So, no downtime or connection drops you would've faced in a shared-server