Security+[SY0–601] Lab Walkthrough

Lab 2 — Nmap

Hassen Hannachi

June 7, 2025

Contents

List of Figures

1 Introduction

Nmap (Network Mapper) is one of the most common tools used among hackers and system administrators. It is used to scan a host, which can be a server, pc, network, etc. When running an Nmap scan, the goal is usually to discover various pieces of information about a target system or network. Examples of such information include: the devices that are connected to a network, the ports that are open on a device, the services that are running on these ports, whether the device is up, and whether there is a firewall protecting the device, among others.

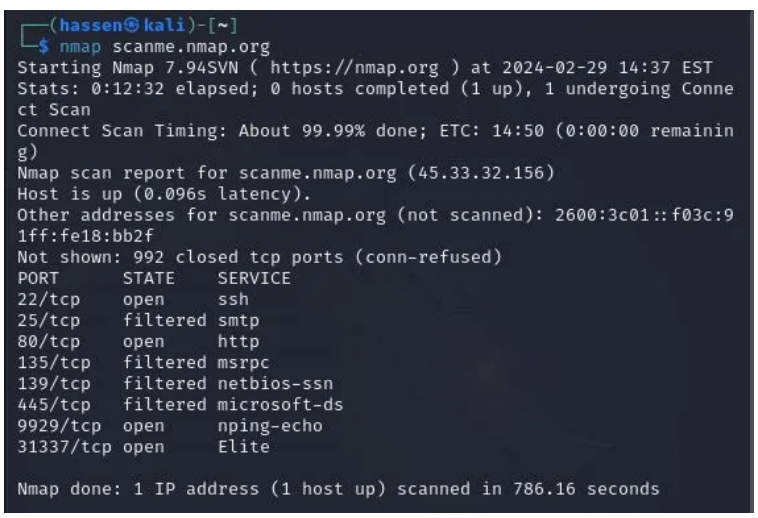
2 Environment Setup

Please follow these labs to get hands-on experience for CompTIA Security+ exam [SY0–601]. All the labs use free tools. I STRONGLY suggest you use a virtual machine[1] such as VMware or Virtualbox for these labs to avoid exposing your home PC or laptop. [2]

3 Lab Walkthrough

3.1 Task 1

Nmap comes pre-installed in Kali Linux. Just open a terminal, type "***nmap scanme.nmap.org***"[3] without the inverted commas. This will initiate a scan of the target and will attempt to determine which ***ports are open*** and what ***services are open*** on these ports.



```
┌──(hassen㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 14:37 EST
Stats: 0:12:32 elapsed; 0 hosts completed (1 up), 1 undergoing Conne
ct Scan
Connect Scan Timing: About 99.99% done; ETC: 14:50 (0:00:00 remainin
g)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.096s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:9
1ff:fe18:bb2f
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 786.16 seconds
```

Figure 1: Scan scanme.nmap.org

[1] You can use Kali Linux in a virtual machine for the purpose of this lab.

[2] NEVER configure these labs at work using your employers' PCs.

[3] This site has been developed by Nmap for the purpose of scanning. Never scan any site, system, or network without prior permission from the owner.

As we can see from the scan results, there are 4 ports open, and there are different services running on each port. The scan we just performed, however, is a very basic scan and will only scan the top 1000 ports for basic information. In the next step, we will run a more advanced scan.

3.2 Task 2

In this step, we will be scanning the same target, scanme.nmap.org, but with a more advanced scan. Let's say we want to determine the versions for the services running on each port, so that we can determine if they are out of date and potentially vulnerable to exploitation. We also want to determine the operating system of the webserver running the target site. We will run the following scan to determine this information:

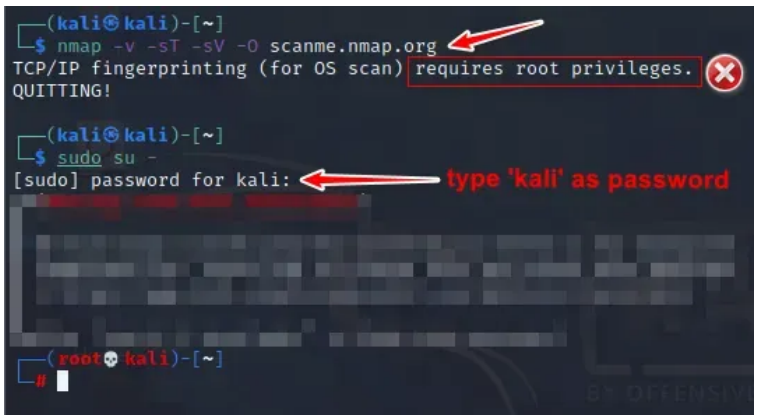


Figure 2: Nmap advanced scan

Oops! You must be root before doing this type of scan. Type "sudo" and re-enter nmap command with desired parameters. The line in the terminal will be like the following:

sudo nmap -v -sT -sV -O scanme.nmap.org

When asked for the password, type "***kali***" without inverted commas.

- -v (Verbose)

  Verbose output gives more detailed scan progress and results.

- -sT (TCP Connect Scan)

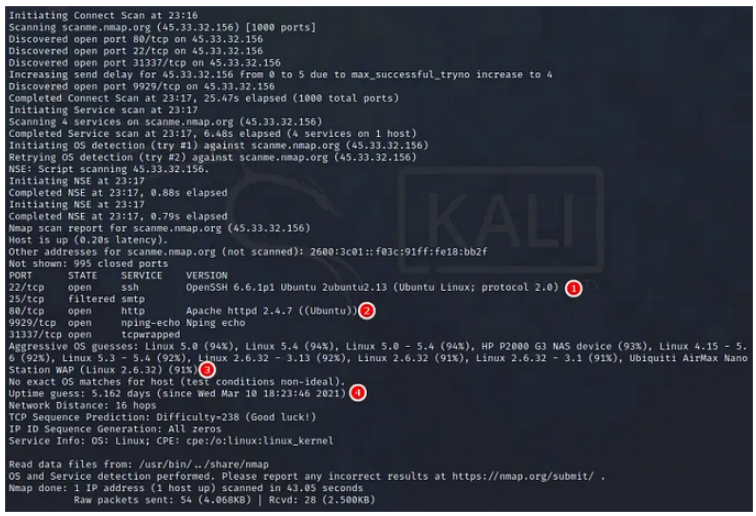
  Performs a TCP connect scan (the "three-way handshake").

- -sV (Service Version Detection)

  Probes open ports to determine what service is running and its version.

The results from our scan show us the exact versions of software running on each open port. Note, if there was a firewall protecting this webserver, we may be unable to see this information. We can also determine with relatively high accuracy the version of the operating system running on the web server.

An easier way to perform a full scan on a target is to use the ***-A*** flag, which will scan a target using the ***-sS***, ***-sV*** , and ***-O*** flags.



```
Initiating Connect Scan at 23:16
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to max_successful_tryno increase to 4
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 23:17, 25.47s elapsed (1000 total ports)
Initiating Service scan at 23:17
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 23:17, 6.48s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.88s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.79s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) 1
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu)) 2
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 5.0 (94%), Linux 5.4 (94%), Linux 5.0 - 5.4 (94%), HP P2000 G3 NAS device (93%), Linux 4.15 - 5.
6 (92%), Linux 5.3 - 5.4 (92%), Linux 2.6.32 - 3.13 (92%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.1 (91%), Ubiquiti AirMax Nano
Station WAP (Linux 2.6.32) (91%) 3
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 5.162 days (since Wed Mar 10 18:23:46 2021) 4
Network Distance: 16 hops
TCP Sequence Prediction: Difficulty=238 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.05 seconds
           Raw packets sent: 54 (4.068KB) | Rcvd: 28 (2.500KB)
```

Figure 3: Nmap advanced scan result

- -A (Aggressive Scan)

  Enables OS detection, version detection, script scanning, and traceroute. Great for in-depth analysis but noisy

- -sS – (TCP SYN Scan)

  Performs a TCP connect scan (the "three-way handshake").

- -sV (Service Version Detection)

  Identifies what services are running on open ports and tries to determine their versions.

- -O (Operating System Detection)

  Attempts to determine the OS and kernel of the target machine using TCP/IP fingerprinting.

3.3 Task 3

Try scanning the same target with a number of different flags. Visit the following site to see the different scans you can run against targets, as well as the different outputs different flags will provide.

4 Conclusion

Nmap is a powerful and essential tool for cybersecurity professionals. It plays a key role in the reconnaissance and vulnerability identification stages of the cybersecurity kill chain

References

[1] Namp: A Beginner's Guide to Network Mapping and Security

[2] Nmap Port Scanning Options.