

# Using nmap

nmap, which is short for Network Mapper, is a Linux based utility that, as its name suggests, maps a network. It can perform network scans to identify what services a host is running, determining the operating system it is using as well as the applications it may have running. Other information includes IP addresses, MAC addresses as well as an identification of the host firewall type a device may be using. nmap is a powerful tool that can be used by network admins but may also be leveraged by malicious users as well. In this exercise, you will examine how nmap functions.

To get a better understanding of this technology, please refer to your course material or use your preferred search engine to research this topic in more detail.

## Learning Outcomes

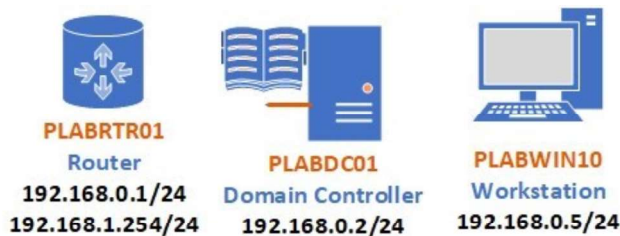
After completing this exercise, you will be able to:

- Examine hosts using nmap

## Your Devices

You will be using the following devices in this lab. Please make sure these are powered on before proceeding.

- **PLABDC01** (Domain Controller)
- **PLABWIN10** (Workstation)
- **PLABRTR01** (Router)



## Task 1 - Explore Working of nmap

To use nmap to determine the operating systems in use by hosts on the network,

perform the following steps.

### Step 1

Switch to **PLABRTR01** and, if it has not already been done, maximize the terminal window for ease of use. Clear the contents of the terminal window by typing the following command and pressing **Enter**:

```
clear
```

Begin by installing nmap on **PLABRTR01** by typing the following command and then pressing **Enter**:

```
sudo apt install nmap
```

When prompted, type **y** and press **Enter**.

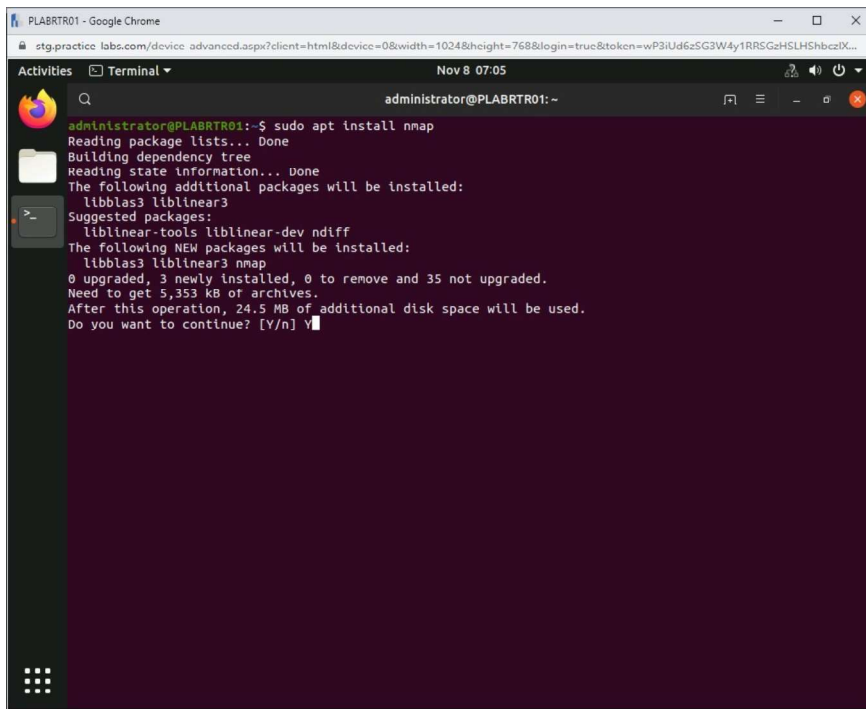


Figure 6.1 Screenshot of the PLABTR01 desktop: administrator@PLABTR01 window is displayed showing the nmap tool being installed.

## Step 2

Once the installation is complete, scan the **PLABWIN10** device by typing the following command and then pressing **Enter**:

```
nmap 192.168.0.5
```

You may receive a response stating that the host seems down. If this is received, please type:

```
nmap -Pn 192.168.0.5
```

*If the command takes up to a minute to complete, you can press **Enter** to get a status report of the operation that includes the estimated time remaining.*

Once the operation is complete, the report appears listing open and closed ports on the device as well as the amount of time the scan took.

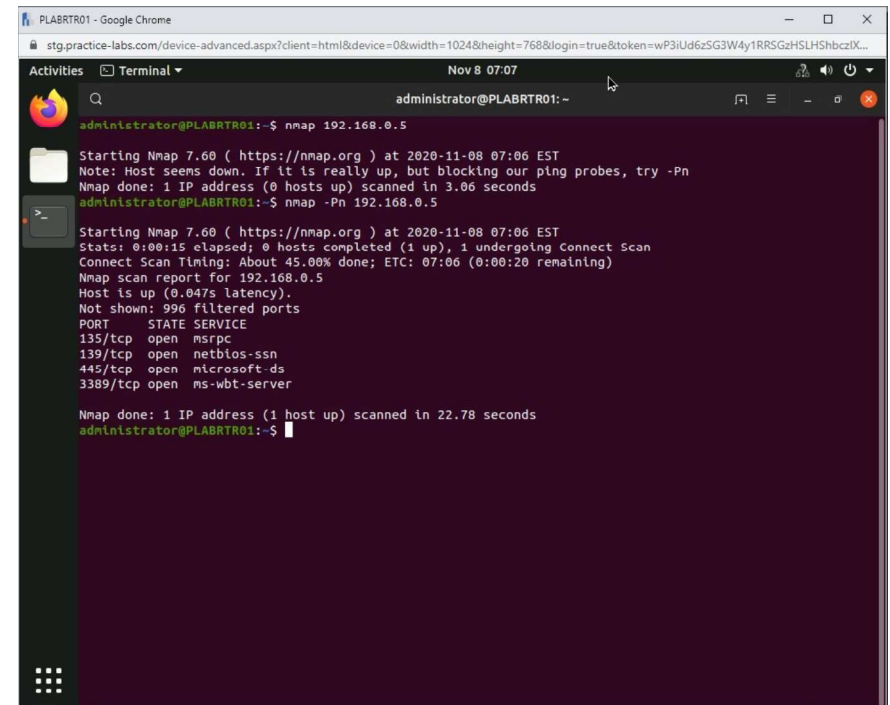


Figure 6.2 Screenshot of the PLABTR01 desktop: administrator@PLABTR01 window is displayed listing scan results for the specified device.

## Step 3

To list information about the operating system on **PLABWIN10**, a procedure also known as OS fingerprinting, issue the following command and press **Enter**.

```
sudo nmap -O 192.168.0.5
```

The parameter -O is the uppercase letter O as in OSI.

*Note that this command requires root privileges and that is why it must be preceded by the **sudo** keyword. Enter a password of **Passw0rd** if you are requested for one. Once again, this operation may take up to a minute to complete.*

Notice that the output lists information concerning the OS version including build numbers and service pack information.

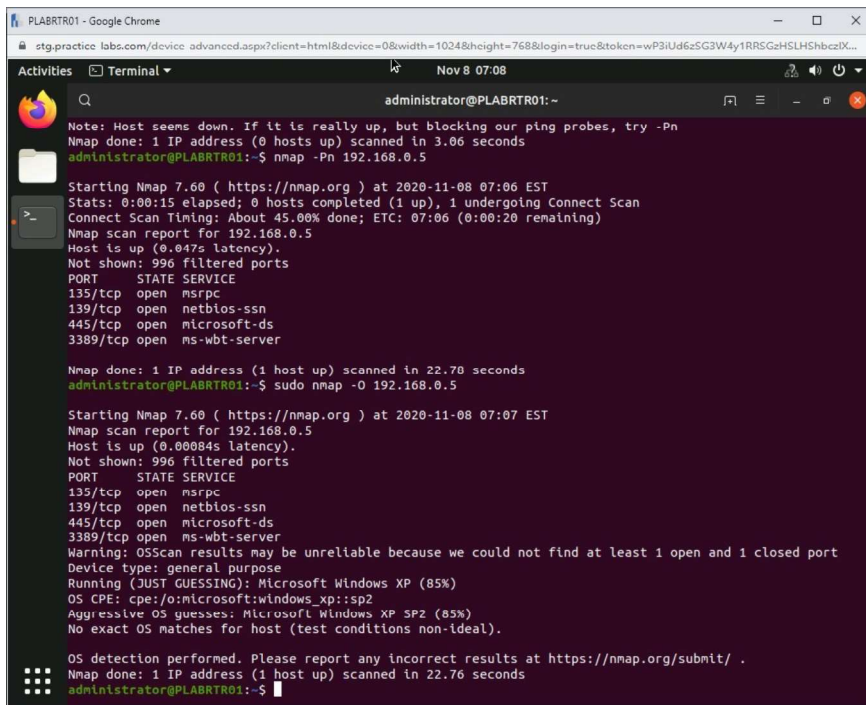
## Step 4

To perform a more aggressive scan of specific services and their parameters that may be running on **PLABWIN10**, issue the following command and press **Enter**.

```
sudo nmap -sV 192.168.0.5
```

You may need to scroll through the output to examine it more closely. Notice that in this output, for every open port, there is a more detailed description of the application running on it including the service name and its version.

You may also notice that additional service is running which returned data but is not recognized by the nmap utility. You are given a set of data known as a fingerprint that you are asked to submit to the nmap public repository. This is a good example of how users participate in the advancement and development of open source software.



```
PLABTR01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=wP3iUd6zSG3W4y1RRSGzHSLHShbczIX...
Nov 8 07:08
administrator@PLABTR01: ~
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
administrator@PLABTR01:~$ nmap -Pn 192.168.0.5

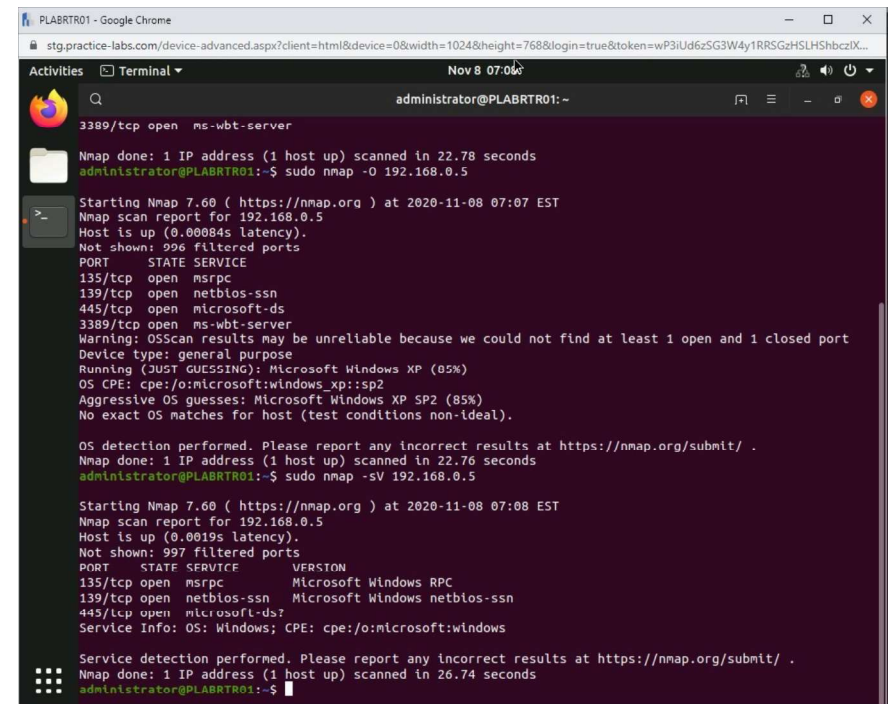
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-08 07:06 EST
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 45.00% done; ETC: 07:06 (0:00:20 remaining)
Nmap scan report for 192.168.0.5
Host is up (0.047s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 22.70 seconds
administrator@PLABTR01:~$ sudo nmap -O 192.168.0.5

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-08 07:07 EST
Nmap scan report for 192.168.0.5
Host is up (0.00084s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.76 seconds
administrator@PLABTR01:~$
```

Figure 6.3 Screenshot of the PLABTR01 desktop: administrator@PLABTR01 window is displayed listing OS fingerprinting results for the specified device.



```
PLABTR01 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=wP3iUd6zSG3W4y1RRSGzHSLHShbczIX...
Nov 8 07:08
administrator@PLABTR01: ~
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 22.78 seconds
administrator@PLABTR01:~$ sudo nmap -O 192.168.0.5

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-08 07:07 EST
Nmap scan report for 192.168.0.5
Host is up (0.00084s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.76 seconds
administrator@PLABTR01:~$ sudo nmap -sV 192.168.0.5

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-08 07:08 EST
Nmap scan report for 192.168.0.5
Host is up (0.0019s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.74 seconds
administrator@PLABTR01:~$
```

Figure 6.4 Screenshot of the PLABRTR01 desktop:  
administrator@PLABRTR01 window is displayed listing details of services running on the system.

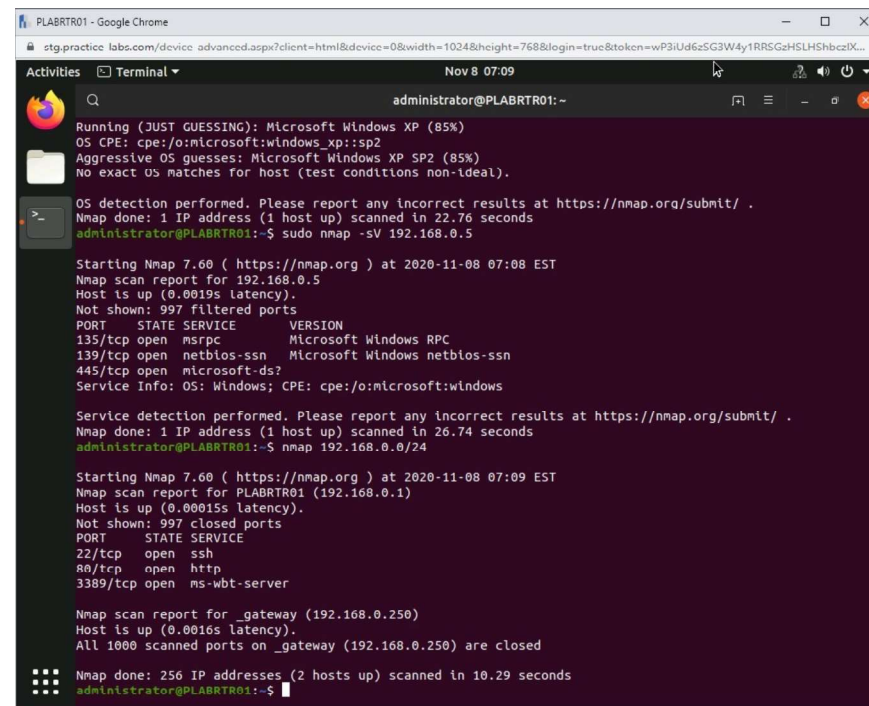
## Step 5

To scan the whole subnet using nmap, issue the following command and press **Enter**.

```
nmap 192.168.0.0/24
```

*Because the whole subnet is being scanned, this may take a little longer than the previous scans. Once again, you can press Enter to obtain a status report and the estimated time to completion of the process.*

Once the operation is complete, you can see the report stating the number of hosts found and scanned on the subnet.



The screenshot shows a terminal window on the PLABRTR01 desktop. The terminal displays the output of an nmap scan. It starts with a 'Running (JUST GUESSING): Microsoft Windows XP (85%)' message, followed by OS CPE and aggressive OS guesses. The scan is performed on 192.168.0.5. The output shows the scan starting at 2020-11-08 07:08 EST, with 1 IP address scanned in 22.76 seconds. The host is up, and 997 filtered ports are shown. The scan results for 192.168.0.5 are as follows:

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

The scan is then performed on the entire subnet 192.168.0.0/24. The output shows the scan starting at 2020-11-08 07:09 EST, with 256 IP addresses scanned in 10.29 seconds. The results show 2 hosts up: 192.168.0.1 (PLABRTR01) and 192.168.0.250 (gateway). The scan results for 192.168.0.1 are as follows:

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	
80/tcp	open	http	
3389/tcp	open	ms-wbt-server	

The scan results for the gateway (192.168.0.250) show all 1000 scanned ports are closed.

Figure 6.5 Screenshot of the PLABRTR01 desktop:  
administrator@PLABRTR01 window is displayed listing results of scanning the specified subnetwork on the system.

Scroll up to examine the output further. Notice the following:

- The process has also examined the host with IP address **192.168.0.1** which is the **PLABRTR01** device itself
- The output of the **192.168.0.250** device which is the gateway indicates that it has all its ports closed

Leave the devices you have powered on in their current state and proceed to the next exercise.