Nmap Enumerate a Network

Contents

Time required: 60 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Lab Description

Part of penetration testing or doing a security audit is to find out what devices are on the network.

NOTE: In VirtualBox, switch to a Bridged adapter. We will scan your local network. Only scan a network that you own or have permission to scan.

Windows Zenmap

There is a GUI version of nmap for Windows named Zenmap.

1. Go to www.nmap.org → Download and install Nmap for Windows.
2. Run Zenmap. In the **Target** field, enter **localhost**, in the **Profile** field, choose **Quick scan plus**. Click **Scan**.
3. **Insert a screenshot:**

Click or tap here to enter text.

4. Open a command prompt → Run **ipconfig**

Use this information to figure out your network Target. For example: If your IP address was 192.168.1.106, and your subnet mask is 255.255.255.0, then your network Target is 192.168.1.1-254.

Write this down. You will use your network address any time you see 192.168.1.1-254

NOTE: 192.168.56.1 is the VirtualBox IP. This is not your network IP.

5. Enter your network range in the Target field. Click **Scan**.
6. **Insert a screenshot of the completed scan:**

Click or tap here to enter text.

7. **How many IP addresses were scanned?**

Click or tap here to enter text.

8. **How many hosts are up?**

Click or tap here to enter text.

9. Choose a host with open ports reported, use the Ports/Hosts tab to list the ports and services.
10. **What type of information is available?**

Click or tap here to enter text.

11. Choose the host details tab.
12. **What type of information is available?**

Click or tap here to enter text.

13. **Can you figure out which machine is the one you are scanning from?**

Click or tap here to enter text.

14. **What other information is provided?**

Click or tap here to enter text.

15. **Insert a screenshot of the host details of one of your hosts.**

Click or tap here to enter text.

Kali Linux Nmap

Objective: Learn the basic commands and syntax of Nmap.

Description: In this activity, you're introduced to using Nmap for quick scans of a network.

NOTE: Make sure your Kali VM is attached to the Bridged Adapter.

In this example, the attack network IP addresses are 192.168.1.1 to 192.168.1.254. You would change this to your local network. Make sure to follow the rules of engagement, and don't perform port scanning on any systems other than your own network.

1. Run **ip a**

Use this information to figure out your network Target. For example: If your IP address was 192.168.1.106, and your subnet mask is 255.255.255.0, then your network Target is 192.168.1.1/24
Write this down.

2. Open a Terminal session.
3. Type **nmap -h | less** and press Enter to see all available Nmap commands.
4. After reviewing the parameters, write down three options that can be used with the Nmap command, and then press q to exit the help screen.

As you go through this lab, substitute your IP address range for 192.168.1.1/24

5. A ping scan: **sudo nmap -sn 192.168.1.1/24**
6. **Insert a screenshot of the completed scan:**

Click or tap here to enter text.

7. **How many IP addresses were scanned?**

Click or tap here to enter text.

8. **How many hosts are up?**

Click or tap here to enter text.

The scan we just completed is called a SYN scan. We are going to send invididual SYN packets to see what the response is.

A SYN packet is the first packet sent to initiate a conversations with another computer. If the host responds, we know that host is alive.

Substitute your networks gateway address for 192.168.1.1.

```
sudo nmap -sS -v 192.168.1.1
```

1. Press Enter.
2. What are the results of your SYN scan? Insert a screenshot of the results.

   Click or tap here to enter text.

3. Try sending a new SYN packet to any IP address in your network.
4. What are the results of this new scan? Do you see any differences? Is the host alive? If so, list them.
5. Insert a screenshot of the results.

   Click or tap here to enter text.

Nmap can scan through a range of IP addresses, so entering one IP address at a time isn't necessary.

6. To send a SYN packet to every IP address in your attack range, type

```
sudo nmap -sS -v 192.168.1.1/24
```

7. Press Enter.
8. To see the output in a format you can scroll, press the up arrow key, add the | less option to the end of the Nmap command, and press Enter. The command should look like this:

```
sudo nmap -sS -v 192.168.1.1/24 | less
```

   Insert a screenshot of the results.

   Click or tap here to enter text.

9. Scan **lab.wncc.net** on port 8080. Use the help command we used earlier to figure out how to scan only one port.
10. What are the results of the script scan?

Click or tap here to enter text.

Zenmap for Linux

1. Go to the Kali launch button → type in and run **Zenmap**. It will look and work exactly as the Windows version.
2. In the Target field, enter **localhost** (This is your local computer.)
3. In the Profile field, select **Quick scan**. Click **Scan**.
4. **Insert a screenshot:**

Click or tap here to enter text.

The scan will show a list of ports on your computer and the services assigned to them.

We will scan your local network and see how the output changes. This time you will target all IP addresses in the same range as your computer's IP address. The easiest way to do this is to first determine your computer's IP address.

5. Open a terminal and enter the command **ip a**. Find your IPv4 address and write it down if necessary.
6. **Insert a screenshot of your ipconfig results:**

Click or tap here to enter text.

7. Go back to **Zenmap**. In the **Target** field, type in the IP address range for your local network's IP address range that you wrote down earlier.
8. Click **Scan**.
9. This time the output shows information about other hosts on your network as well as the information you've already seen for your own computer.
10. **Insert a screenshot of your scan results:**

Click or tap here to enter text.

11. Scroll through the output and answer the following questions:
12. **How many IP addresses were scanned? How many hosts are up?**

Click or tap here to enter text.

13. **Compared with the information you saw earlier about your own computer, what different information is revealed about the other hosts?**

Click or tap here to enter text.

14. Find a host with open ports reported and list the ports and their services in your answer. **What other information is provided about that host?**

Click or tap here to enter text.

Attach this completed document to the assignment in Blackboard.

Assignment Submission

Attach this completed document to the assignment in Blackboard.