ZenMap Enumerate a Network

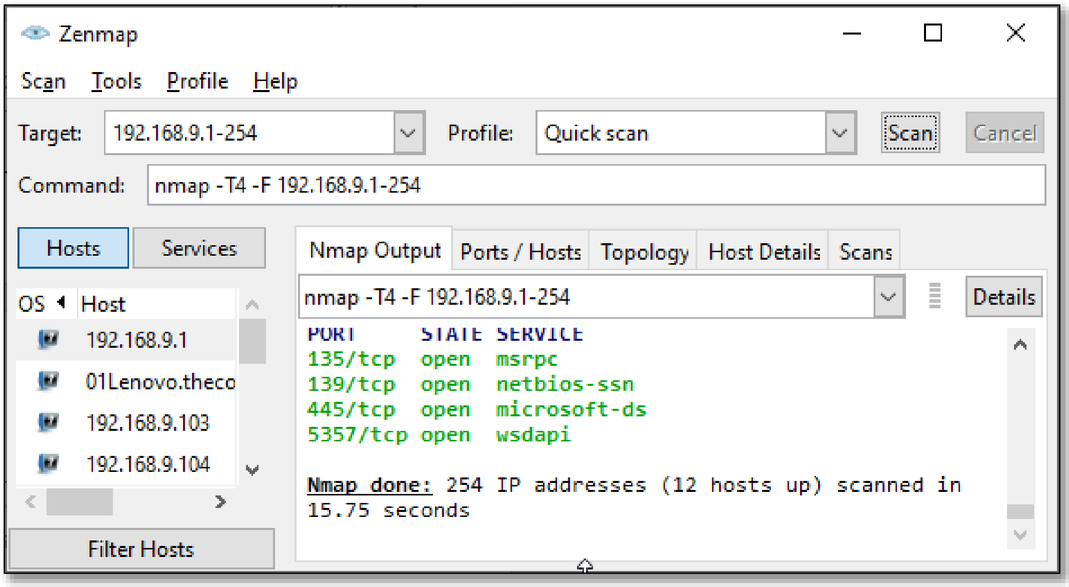
Time required: 30 minutes

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

Several programs are available to assist in detecting, identifying, and monitoring the devices on your network. One of the simpler and most popular tools is Nmap. Nmap was originally designed for Linux as a command-line only utility but has since been expanded for compatibility on several other OSs and is now available in GUI form. In this activity, you will use the GUI version of Nmap for Windows, which is called Zenmap.



Target: 192.168.9.1-254

Profile: Quick scan

Command: nmap -T4 -F 192.168.9.1-254

```
nmap -T4 -F 192.168.9.1-254
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 254 IP addresses (12 hosts up) scanned in
15.75 seconds
```

Install Zenmap

NOTE: This lab can be safely done on your local computer. If you do decide to do this lab on a Virtual Machine, make sure you are using the Bridged Adapter to connect to your local network.

1. Go to www.nmap.org and go to **Download → Windows**
2. At the time of this writing, the download was underneath Microsoft Windows binaries, “Latest release self-installer”.
3. Download and install Nmap. Use default settings throughout the installation process.

Scan Local Computer

1. Open the Zenmap program. Start with a quick scan of your local computer.
2. In the Target field, enter **localhost**. In the Profile field, select **Quick scan plus**. Click **Scan**.
3. **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.

Scan Local Network

NOTE: 192.168.56.1 is not a valid IP address. It is the address of the virtual network adapter for VirtualBox.

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.

1. Open a Command Prompt window and enter the command **ipconfig /all**
2. Find your IPv4 address and write it down if necessary.
3. **Insert a screenshot of your ipconfig results:**

Click or tap here to enter text.

4. Go back to **Zenmap**.
5. In the **Target** field, type in the IP address range for your local network’s IP address range. Replace the final block of digits in your IPv4 address with 1-254. For example,

if your IPv4 address is 192.168.1.106, you would enter 192.168.1.1-254 in the Target field.

6. Choose **Quick scan plus** → click **Scan**.

7. 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.

8. **Insert a screenshot of your scan results:**

Click or tap here to enter text.

9. Scroll through the output and answer the following questions:

10. **How many IP addresses were scanned? How many hosts are up?**

Click or tap here to enter text.

11. **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.

12. 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.

Assignment Submission

Attach this completed document to the assignment in Blackboard.