**Vidyavardhini’s College of Engineering & Technology** Department of Computer Engineering Academic Year : 2025-26



Name of the Student: Neha Gupta

Class and Div and Roll No: TE-1/49

Experiment No.4

Perform network discovery using discovery tools

Date of Performance: 29/07/2025

Date of Submission: 05/08/2025

**Vidyavardhini’s College of Engineering & Technology** Department of Computer Engineering Academic Year : 2025-26



**Experiment No 4**

**Aim: Perform network discovery using discovery tools (eg. Nmap, mrtg)**

**Theory:**

1. To install NMAP on Ubuntu, run the command: sudo apt-get install nmap

2. After that open terminal and write nmap --version

3. Type nmap <ip address> and nmap <url>.

4. Next we will perform nmap operation on list of IP addresses.

For that we need to type nmap and all the ip addresses eg. nmap 115.96.26.154,115.96.26.153, 115.96.26.152, 115.96.26.151

You will get details regarding the IP addresses passed.

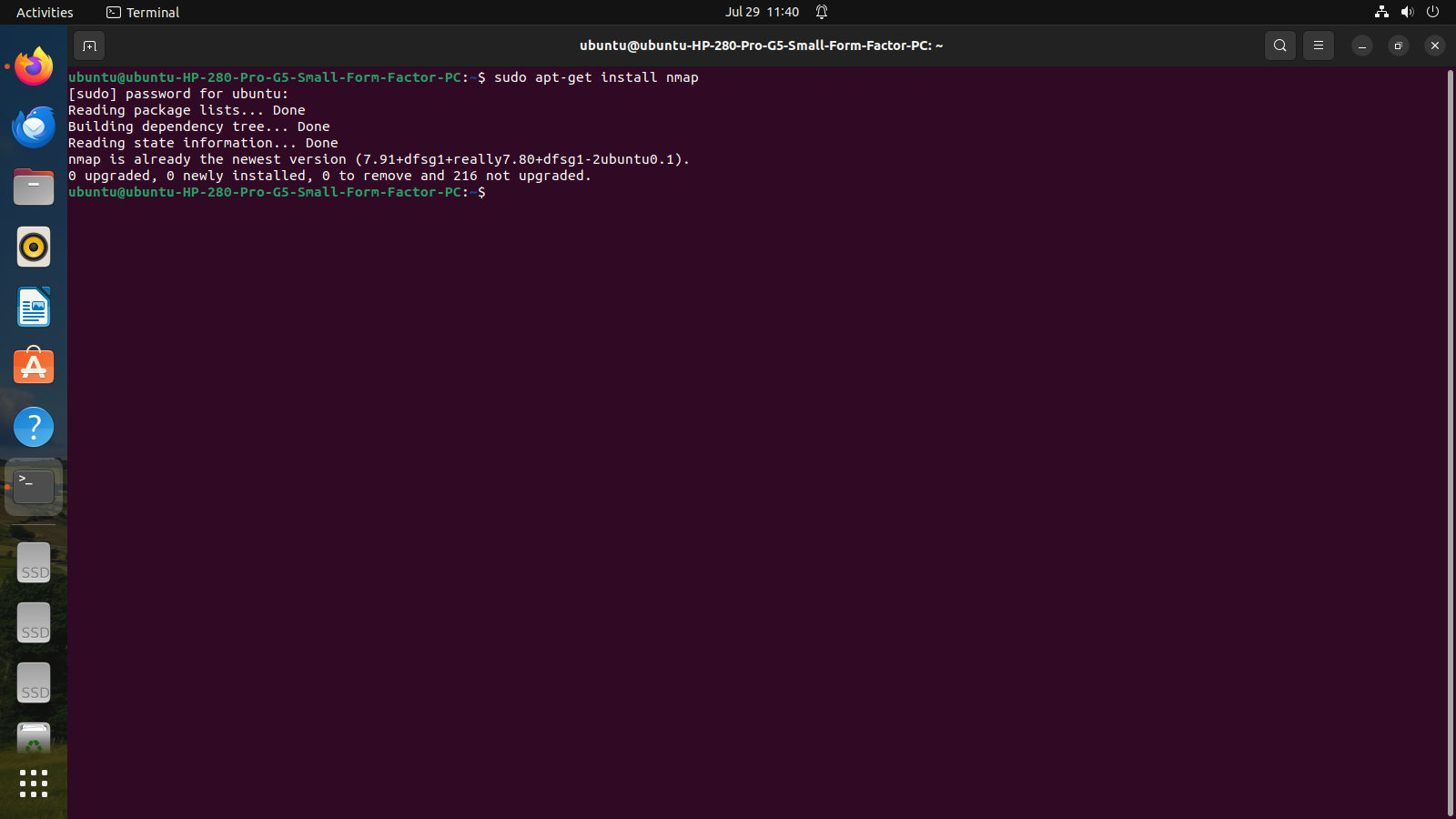
We can also give range of IP Addresses

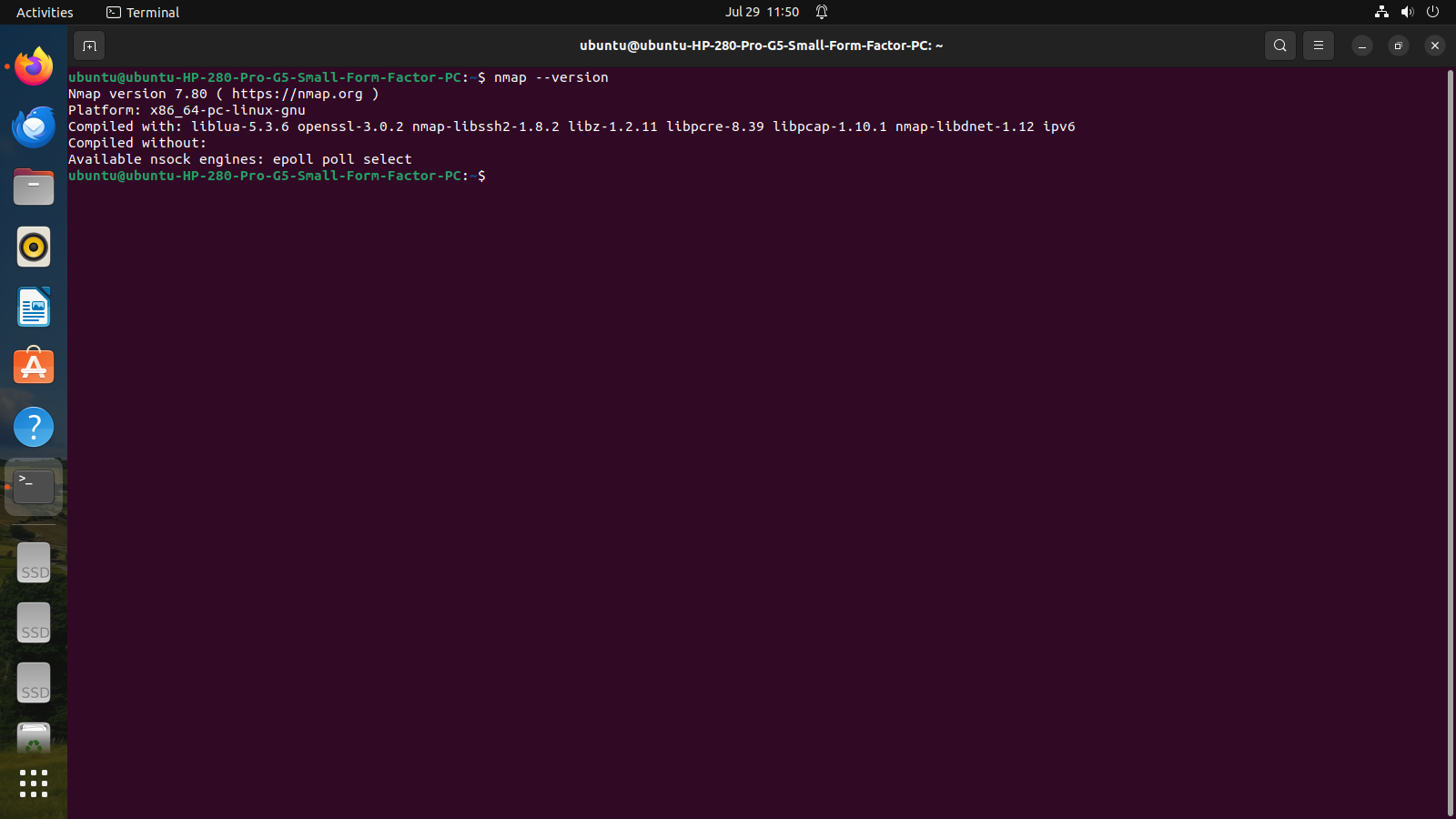
It can be done by typing 56.78.29.10-30.

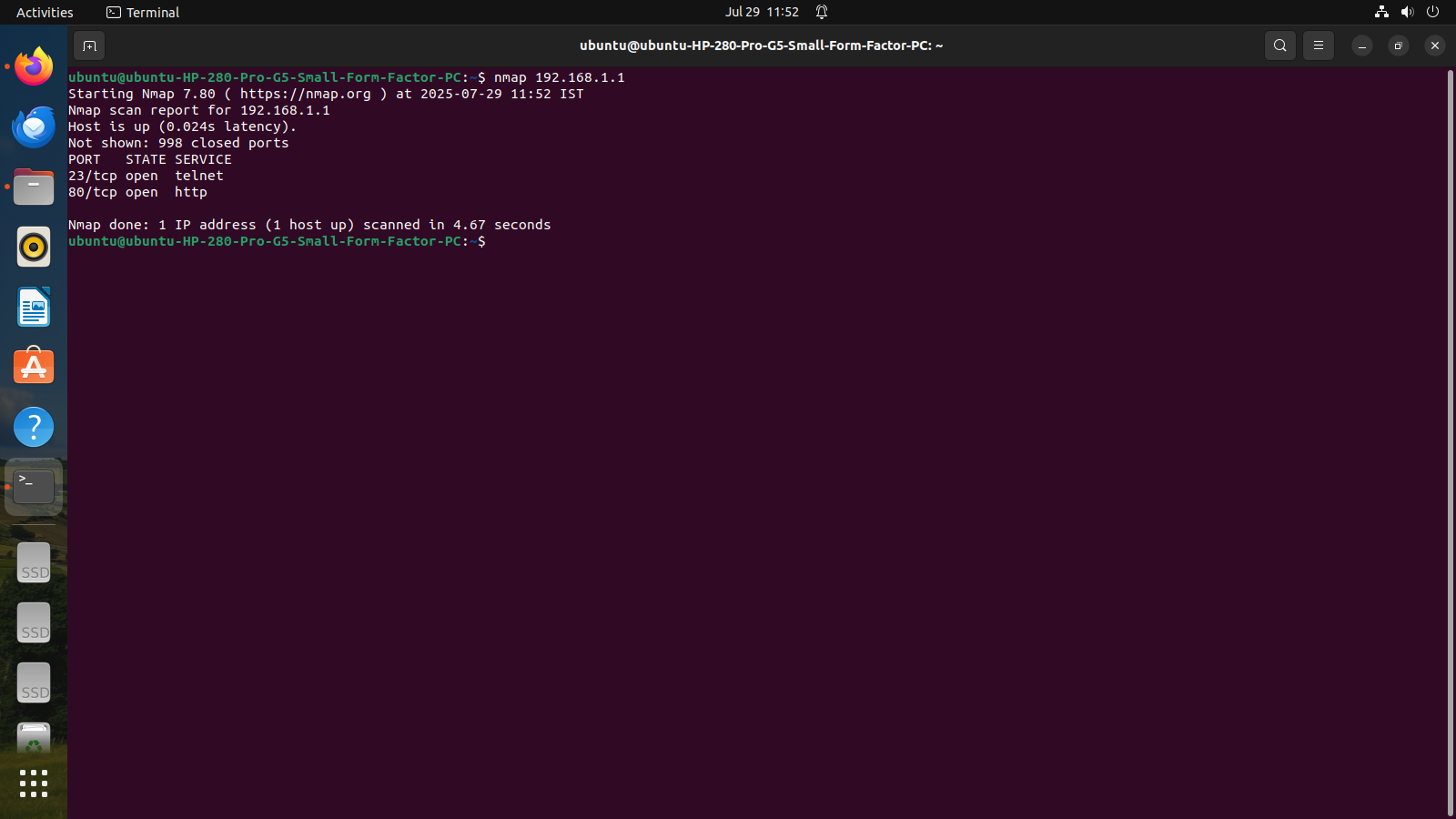
This example will perform nmap operation on 20 ip addresses 5. Now let’s perform nmap using file

Create a text file and in that paste ip address one below another Save the file and run nmap -iL filename.txt command.

After a few minutes you will be able to see all available details of the sites mentioned. **Output:** IP and URL address:







**Conclusion:**

Thus in this practical we have performed network discovery using discovery tool NMAP on Windows/Ubuntu operating system and got desired output.

**Questions:**

**1. What is Nmap?**

Nmap, short for Network Mapper, is an open-source tool used for network discovery and security auditing. It is designed to scan networks and identify what hosts are available, what services they are offering, and other characteristics.

**2. What is the primary purpose of network discovery?**

The primary purpose of network discovery is to identify devices and services on a network, map out the network topology, and gather information about the network's structure and operational status.

**3. Give a basic Nmap command to scan a single IP address.**

A basic Nmap command to scan a single IP address is:

*nmap [IP Address]*

For example, to scan an IP address like 192.168.1.1, you would use:

*nmap 192.168.1.1*

**4. Why is Nmap considered a security tool as well as a discovery tool?**

Nmap is considered both a security tool and a discovery tool because it can be used to identify vulnerabilities and security risks in a network (security tool) while also being capable of mapping networks and discovering devices and services (discovery tool).

**5. What are some precautions when using Nmap on a live network?**

Some precautions when using Nmap on a live network include:

* Obtain proper authorization before scanning to avoid legal issues and potential disruption of network services.
* Be cautious with aggressive scan options that could potentially disrupt network operations or overwhelm network devices.
* Use Nmap responsibly and ethically, respecting privacy and avoiding unauthorized access to systems