**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

1. After that open terminal and write

nmap --version

1. Type nmap <ip address> and nmap <url>.
2. 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

1. Now let’s perform nmap using file

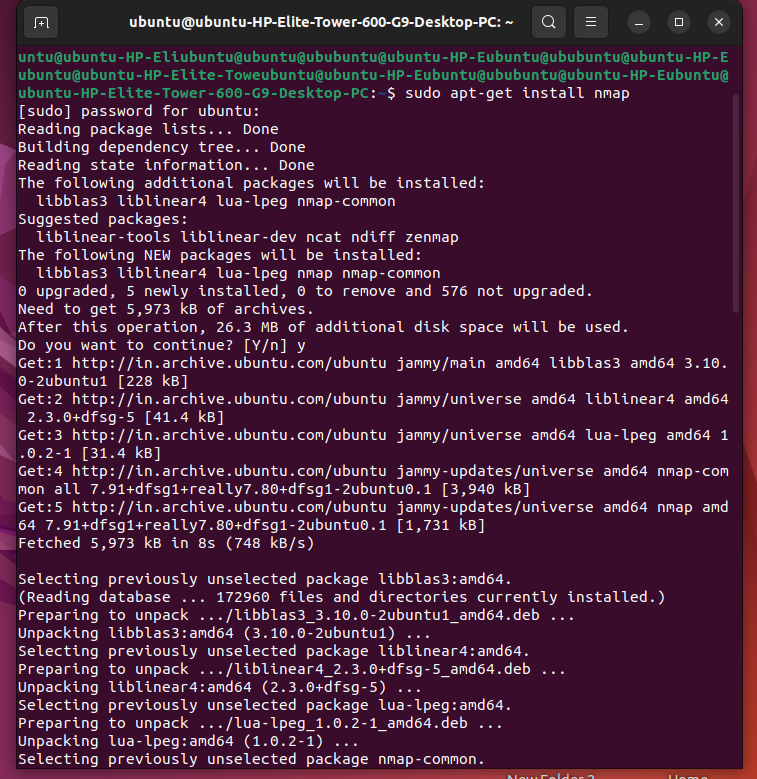
Create a text file and in that paste ip address one below another

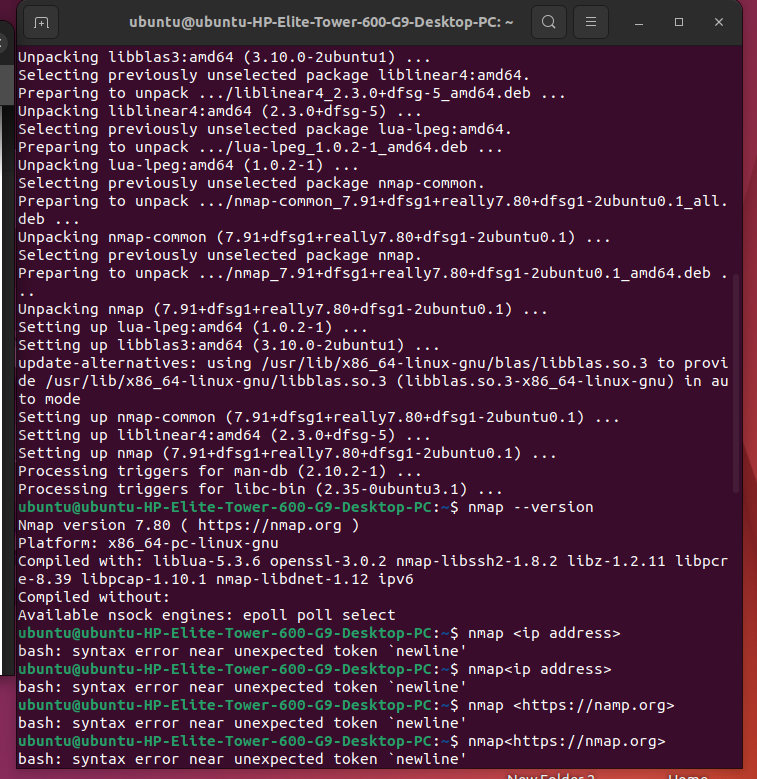
Save the file and run nmap -iL filename.txt command.

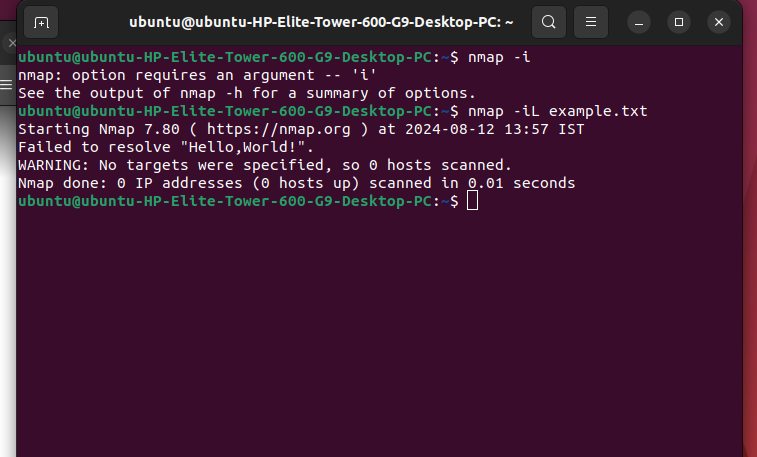
After a few minutes you will be able to see all available details of the sites mentioned .

**Output:**

IP and URL address:







**Conclusion:**

Nmap efficiently gathered detailed information on specified IP addresses and URLs, revealing open ports, services, and vulnerabilities. It proved to be a versatile tool for network discovery, useful for network administration and security auditing.