*Experiment No:4* VU1F1415033

***Aim:*** To study installation & commands of nmap.

***Theory:***

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

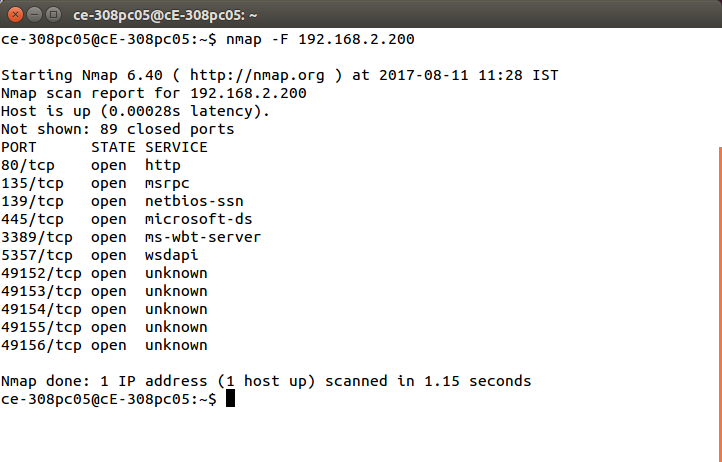
* ***Sudo nmap -sP 192.168.2.200***

Runs a ping scan on network

**

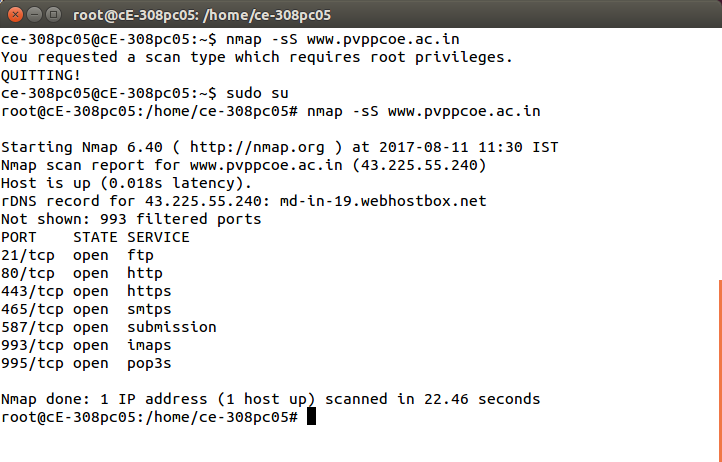
* ***Nmap -F 192.168.2.200***

Runs a Fast Scan

**

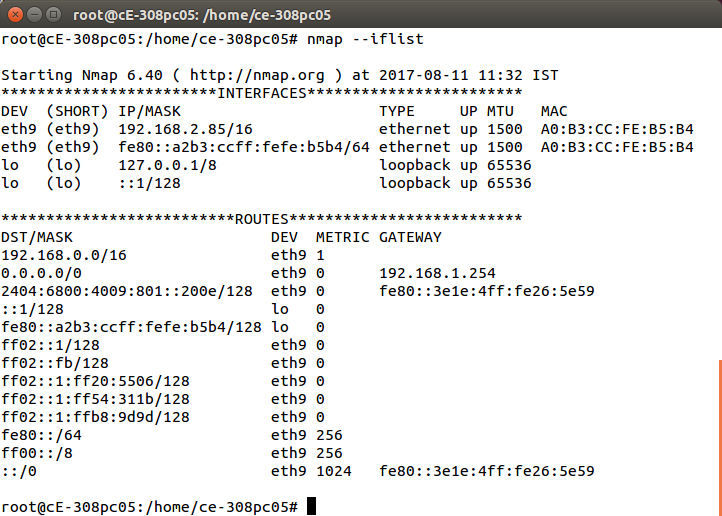
* ***Nmap -sS*** [***www.pvppcoe.ac.in***](http://www.pvppcoe.ac.in)

Runs a TCP SYN scan

**

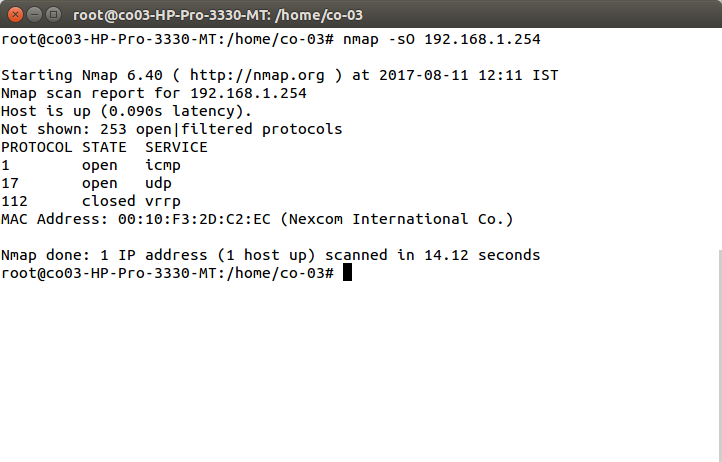
* ***Nmap --iflist***

This command is used for detailing nmap interface list.

**

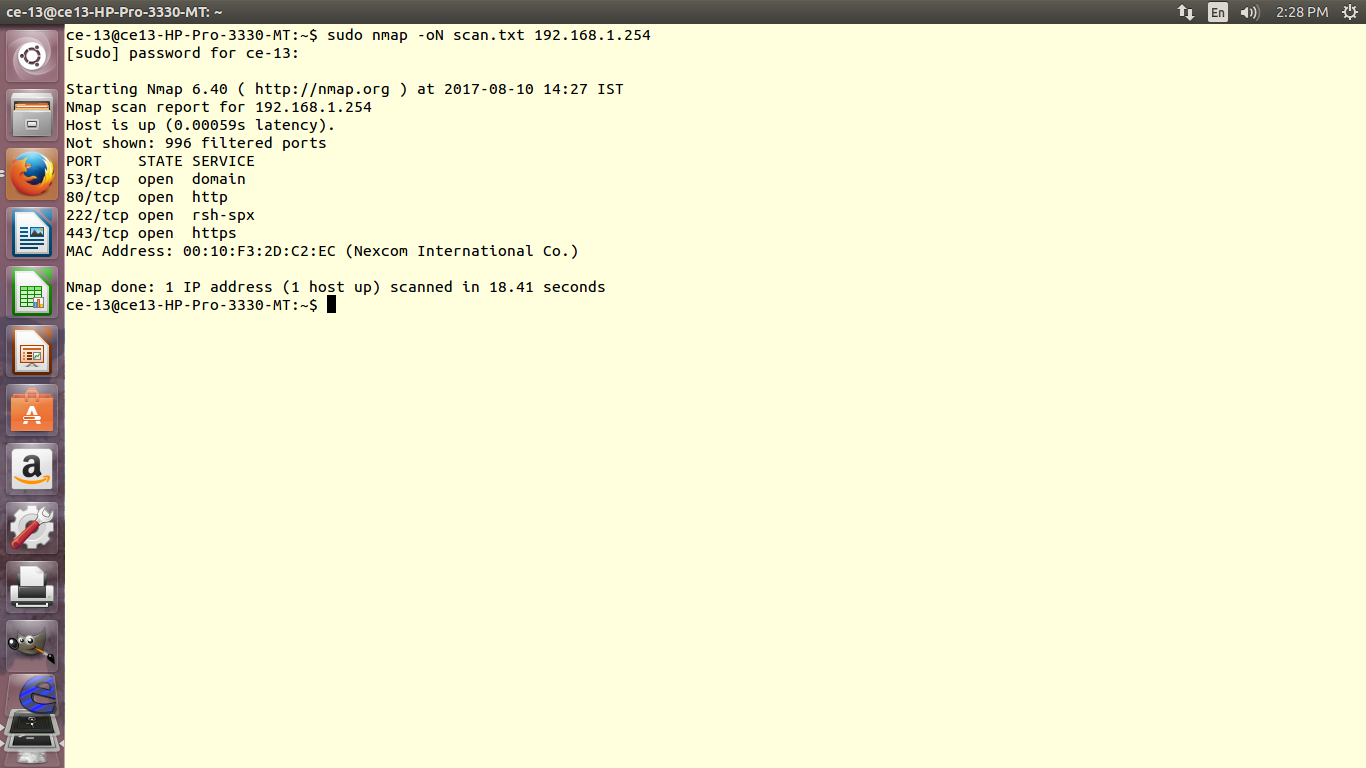
* ***Nmap -sO 192.168.1.254***

Runs ip protocol scan

**

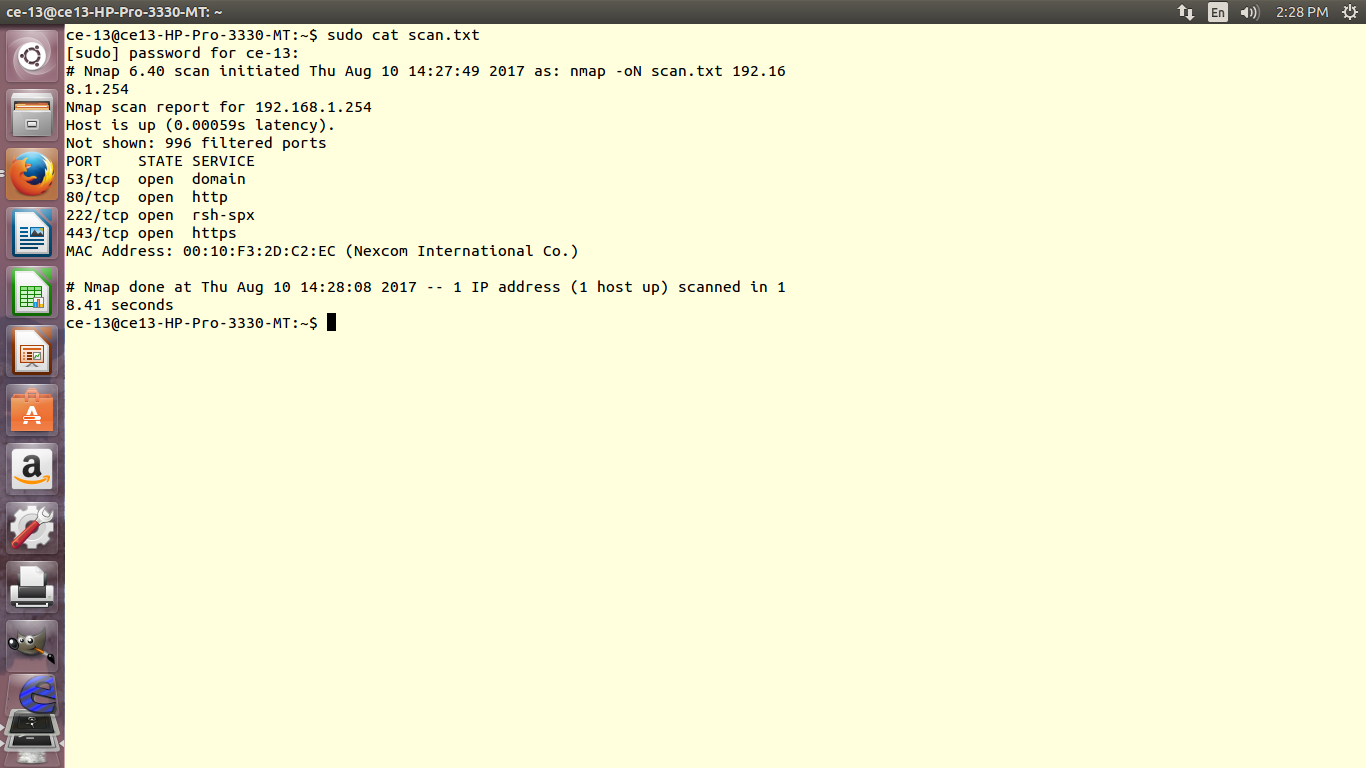
* ***Nmap -oN scan.txt 192.168.2.1/24***

Output scan in normal text file

******

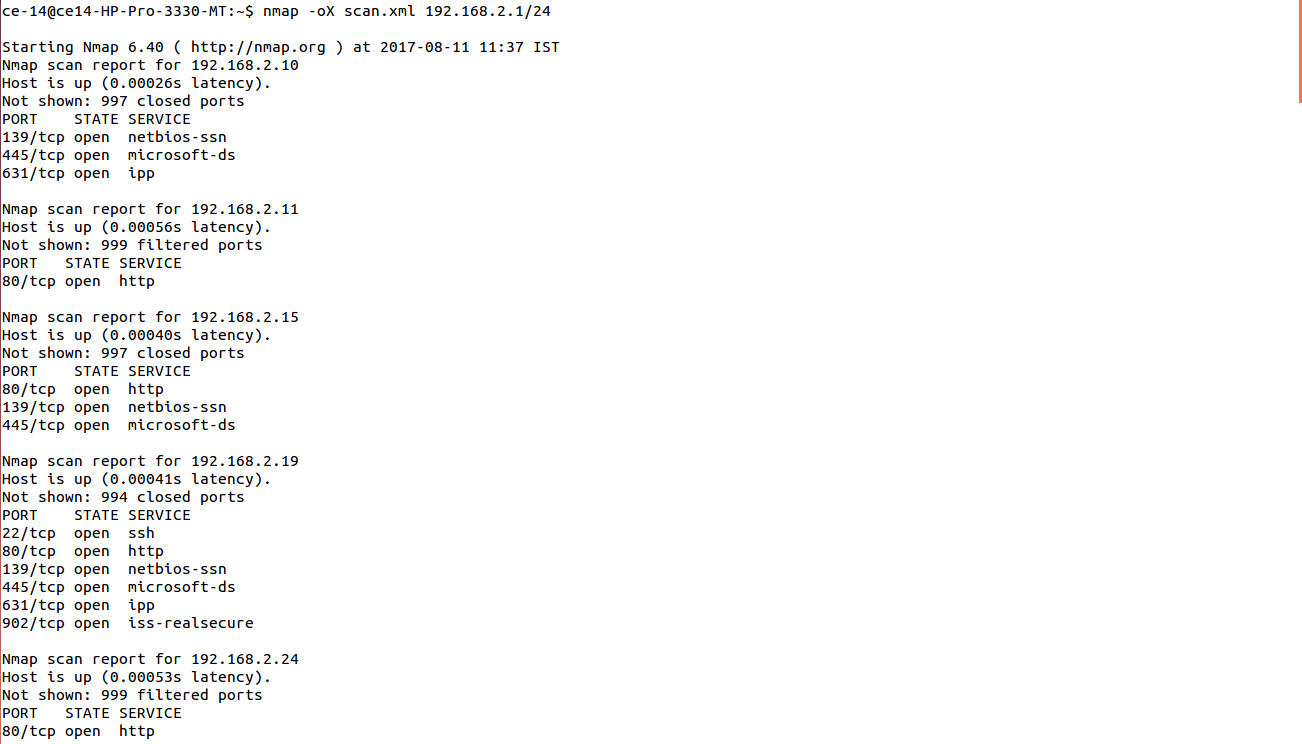
* ***Cat scan.txt***

Display content of scan.txt

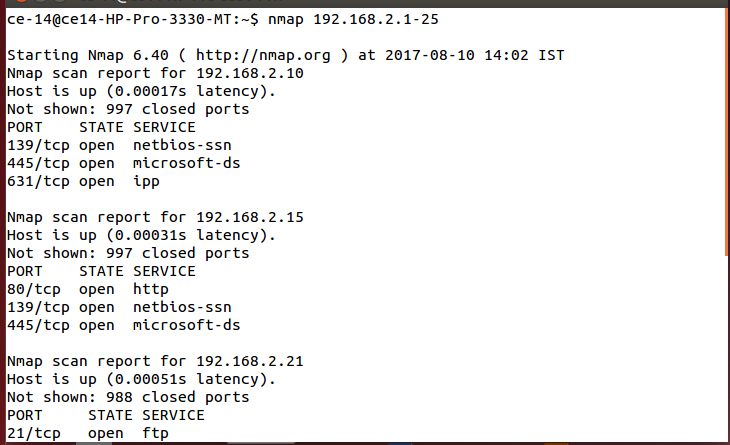
******

* ***Nmap -oX scan.xml 192.168.2.1/24***

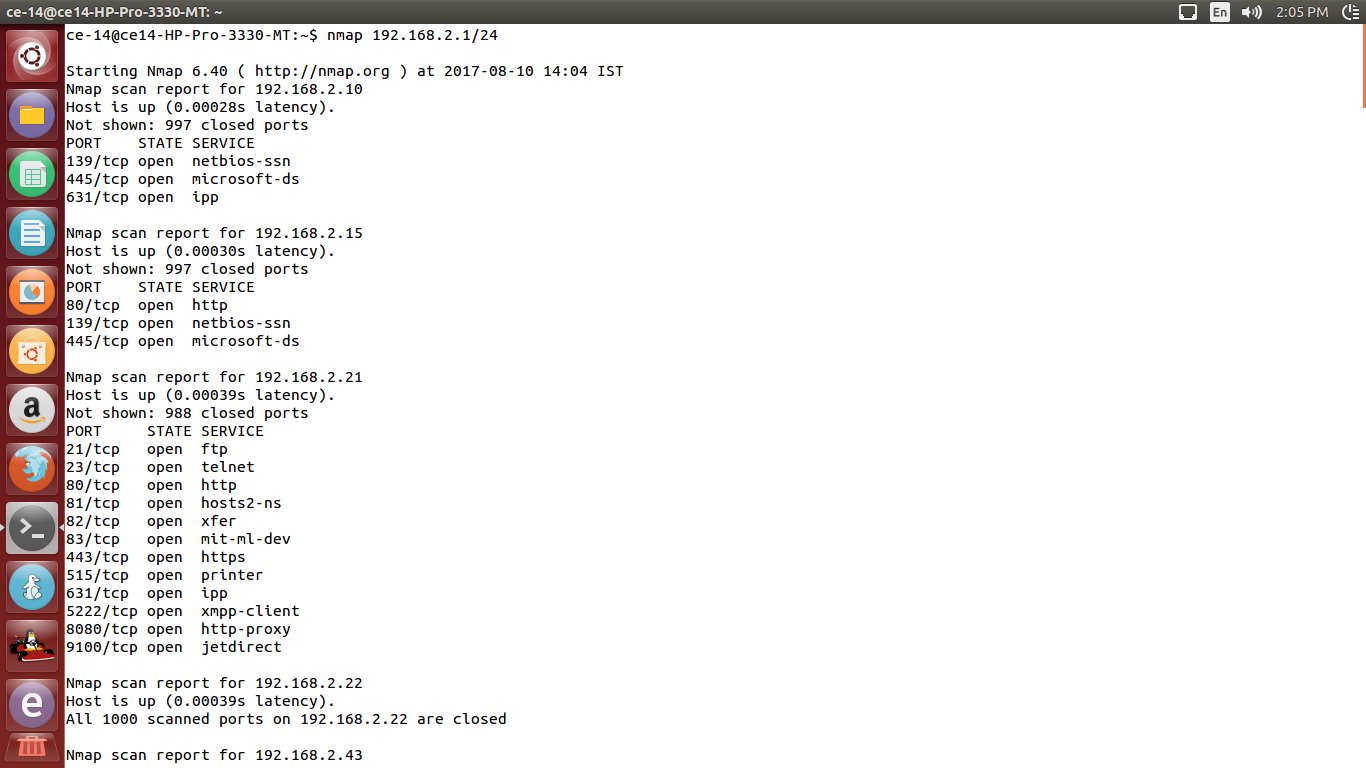
Output Scan to XML File

******

* **Nmap 192.168.2.1-25**

******

* ***Nmap 192.168.2.1/24***

******

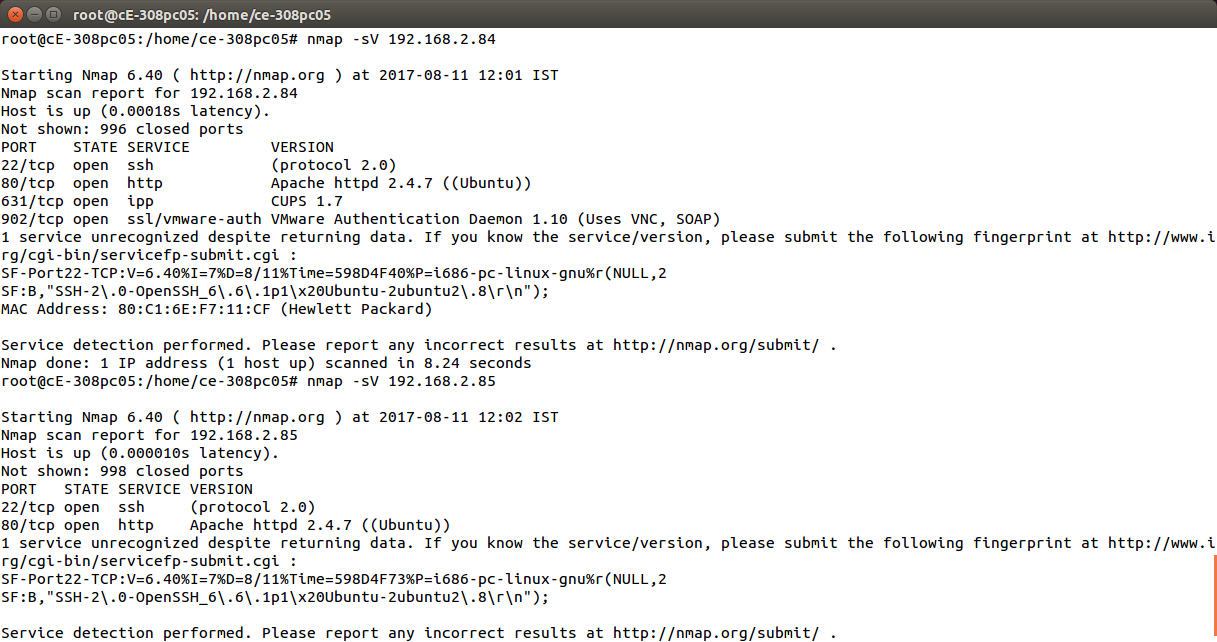
* ***Nmap -A 192.168.2.85***

Enable OS detection, version detection, script scanning, and traceroute

******

* ***Nmap -sV 192.168.2.85***

Probe open ports to determine service/version info

******

***Conclusion:*** Hence NMAP is installed and implemented.