Experiment No:5

**Aim:** To study Nmap for port scanning

**Theory:**

Port scanning or scanning is when intruders collect information on the network services on the target network. Here, the intruder attempts to find open ports on the target system.

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.

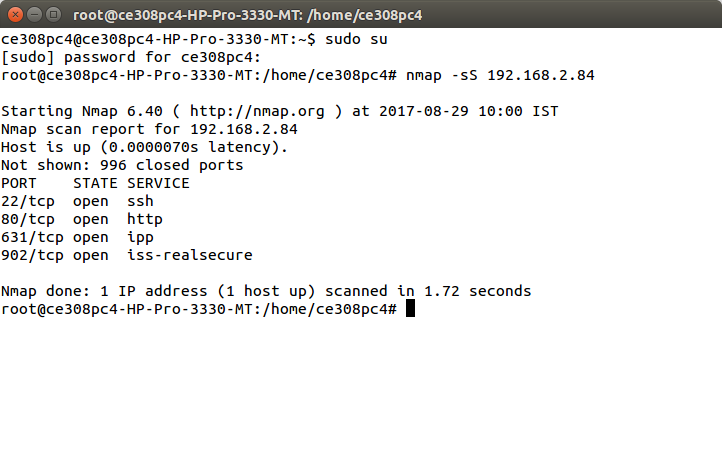
Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

NMAP is

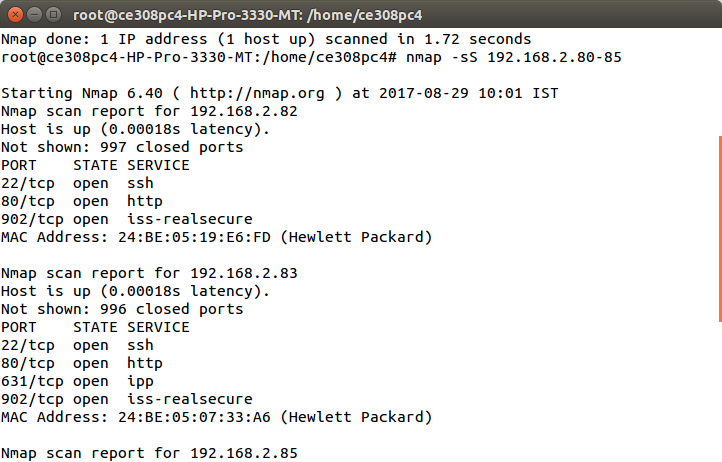
* **Flexible:** Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more.
* **Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
* **Portable:** Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, SunOS, Amiga, and more.
* **Easy:** While Nmap offers a rich set of advanced features for power users, you can start out as simply as “nmap -v -A targethost”. Both traditional command line and graphical (GUI) versions are available to suit your preference.
* **Free:** The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
* **Well Documented:** Significant effort has been put into comprehensive and up-to-date man pages, white papers, tutorials, and even a whole book.
* **Supported:** While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines.
* **Acclaimed:** Nmap has won numerous awards, including “Information Security Product of the Year” by Linux Journal, Info World and Code Talker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series.
* **Popular:** Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

**Input:**

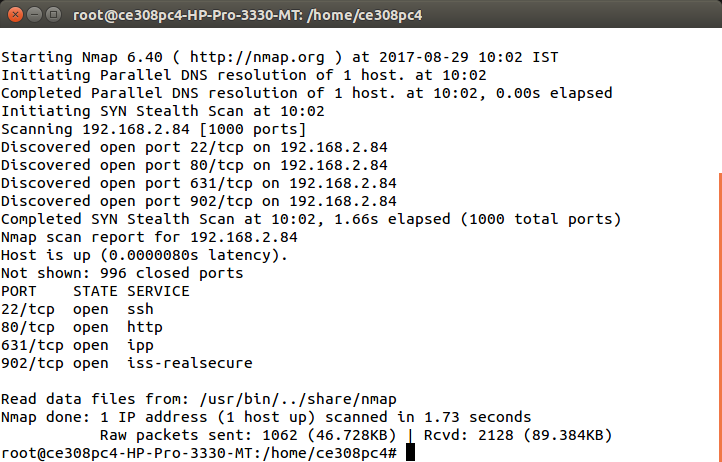
**nmap -sS 192.168.2.84**



**nmap -sS 192.168.2.80-85**



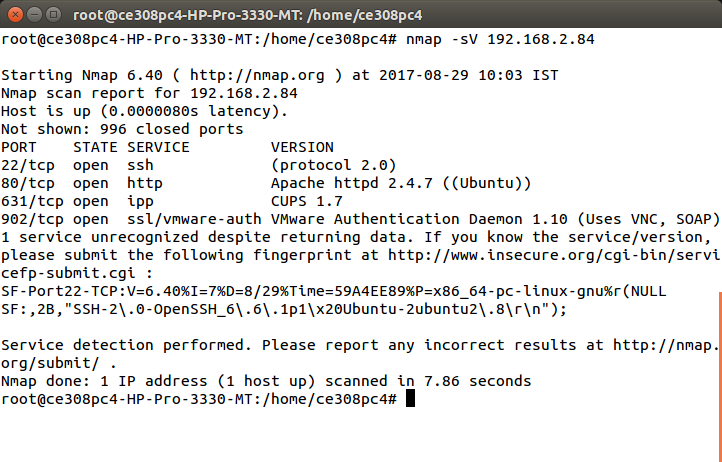
**Find Open ports on System: nmap -v 192.168.2.84**



**Find machines which are active in network: nmap -sP 192.168.2.80-85**



**Service and Version detection by nmap: nmap -sV 192.168.2.84**



**Find the version of software’s installed on the other system: nmap -A -T4 192.168.2.85**



**Conclusion:**

Hence, nmap tool is studied successfully.