# EXPERIMENT NO 08

CLASS: TE CMPN A PID: 182027

NAME: REBECCA DIAS ROLL NO. : 19

**Aim:** Download and install nmap. Use it with different options to scan open ports perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.

**Theory**

**a) What is Port Scanning?What is port scanning?**

* Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.
* This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.
* The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user’s device.
* After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

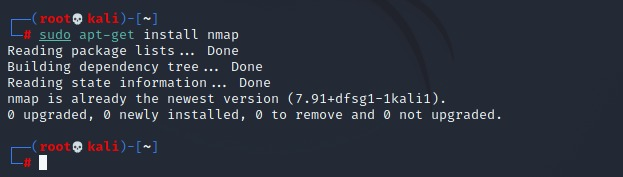
**b) What is Nmap?**

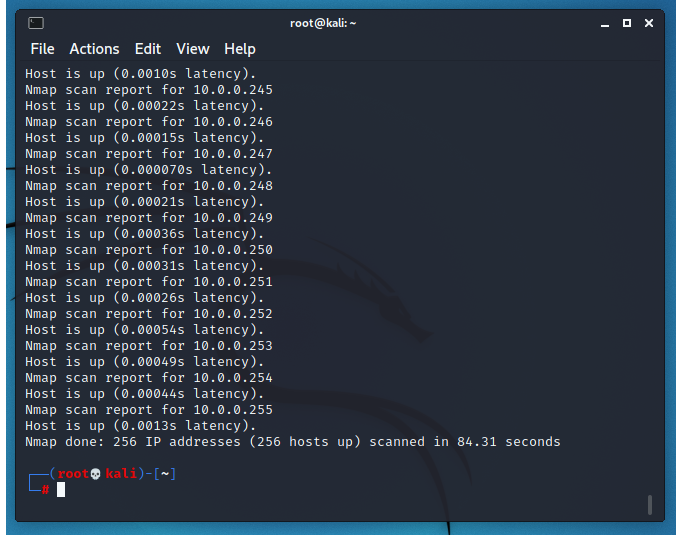
* Nmap ("Network Mapper") is a free and open source ([license](https://nmap.org/npsl/)) utility for network discovery and security auditing.
* Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service 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.
* Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in [twelve movies](https://nmap.org/movies/), including [The Matrix Reloaded](https://nmap.org/movies/#matrix), [Die Hard 4](https://nmap.org/movies/#diehard4), [Girl With the Dragon Tattoo](https://nmap.org/movies/#gwtdt), and [The Bourne Ultimatum](https://nmap.org/movies/#bourne).

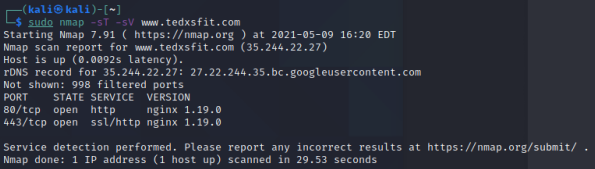
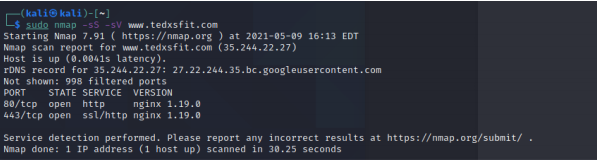
**c) Advantages of Nmap**

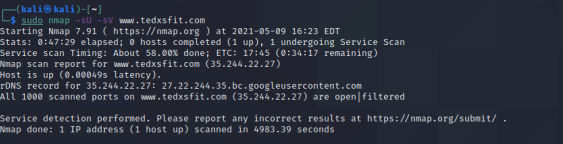
* It can be used for auditing the Network system as it can detect the new servers.
* It can search subdomain and [Domain Name system queries](https://www.educba.com/what-are-the-types-of-dns-servers/)
* With the help of the Nmap scripting engine (NSE), interaction can be made with the target host.
* It can determine the nature of the service that the host is performing, like whether the host is a mail service or a web server or so on

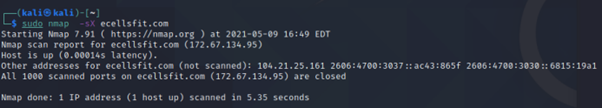
**d) Perform Various scan as follows**

****

**Ping scan:**

**TCP Port scan:**

**UDP Port scan:**

**Xmas Scan:**

**Conclusion**:

In this experiment we learnt to implement the different port scans using nmap tool on a linux environment. We learnt to use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.