**EXPERIMENT – 05**

**AIM** – **To implement different commands using 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 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, Sun OS, 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. Binaries are available for those who do not wish to compile Nmap from source.

**Steps**:

1. Start the nmap tool in the terminal by writing the command sudo nmap.
2. To Scan a System with Hostname and IP address write the command in the terminal sudo nmap google.com or give the IP address of the desired target.
3. We can use -v command to get more detailed information about the remote machines.
4. Nmap also have the feature to scan multiple hosts at a time. Command used: sudo nmap <multiple IP addresses of different websites>.
5. Nmap can also be used to identify hostnames of the given IP’s by using the command sudo nmap -sL <Random IP Adress>.
6. Nmap also have a command -A which indicates Aggressive it will let Us Know The Extra Information’s like OS Detection (-O), version detection, script scanning (-sC), and traceroute (–traceroute) even it provides a lot of valuable information About The Host.
7. Implement all the above mentioned commands in the Kali Linux Terminal.













