Introducing Nmap

- Nmap is a tool used for determining the hosts that are running and what services the hosts are running.
- Nmap is a free and open-source utility for network discovery and security auditing.
- Nmap supports all platform of OS like
- Linux/Unix
- Microsoft
- Mac

Primary Uses of Nmap

1. Determining open ports and services running in a host:
2. Determine the Operating System running on a host
3. Alter the source IP of the scan (One way is to use –S option)

Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices.

- The primary uses of Nmap can be broken into three core processes.

1. First, the program gives you detailed information on every IP active on your networks, and each IP can then be scanned.
2. Secondly, Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device.
3. Thirdly, Nmap has also become a valuable tool for users looking to protect personal and business websites.

- In order to use Nmap, you need to be familiar with command-line interfaces.

How To Install Nmap

- For Windows, Nmap comes with a custom installer (namp<version>setup.exe). Download and run this installer, and it automatically configures Nmap on your system.
- On Mac, Nmap also comes with a dedicated installer. Run the Nmap-<version>mpkg file to start this installer. On some recent versions of macOS, you might see a warning that Nmap is an “unidentified developer”, but you can ignore this warning.
- Linux users can either compile Nmap from source or use their chosen package manager. To use apt, for instance, you can run Nmap –version to check if Nmap is installed, and sudo apt-get install Nmap to install it.

The Options in Nmap

- Some of the Nmap options are explained below:

1. TCP Connect Scanning: Any host can issue a connect () system call to try and open an interesting port on a machine. If the port is open the call succeeds.

2. TCP SYN Scanning: The monitoring host attempts a three way hand shake but does not comple the third step, while negotiating a TCP connection. Once an acknowledgement is received from the target host, the connection is reset.

3. TCP FIN Scanning: FIN packets tend to be undetected by firewalls and packet filters. TCP property forces closed port to respond with a RST packet to a FIN packet. This property is used for scanning to determine the open and closed ports.

4. Fragmentation Scanning: The TCP header of the probe packet is spilt to smaller packets making it difficult for detection.

5. ICMP Port Unreachable Scanning: The scan uses the property of the closed port sending ICMP_port_unreachable error message for closed port for detection.