**4. TCP scanning using NMAP**

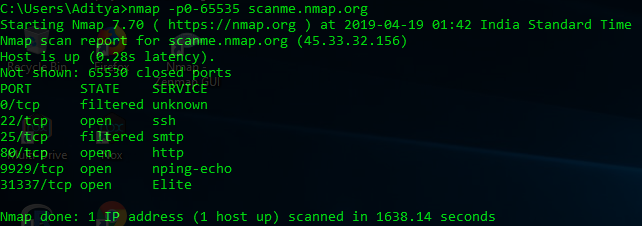
**How To Scan All TCP and UDP Ports with Nmap?**

Nmap is very useful and popular tool used to scan ports. Nmap by default scans most popular 1000 ports. We may need to change the port range and protocol type to all while scanning with nmap.

**Scan All TCP Ports with Range**

We can specify the port range with the -p option. As we know TCP port numbers are between 0 and 65535 . We will use –p 0-65535 as option in order to scan all TCP ports. We do not specify the TCP protocol because default protocol for nmap port scan is TCP.

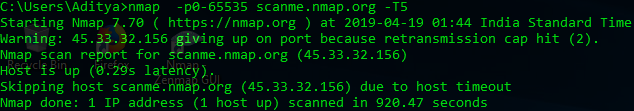
* nmap –p 0-65535 scanme.nmap.org



**Faster Scan For All Ports**

If we are scanning all ports this will take a lot of time. If the situation is not critical we can use faster scan with -T5 parameter. This is the fastest  scan level for nmap. This option can be used for UDP scans too.

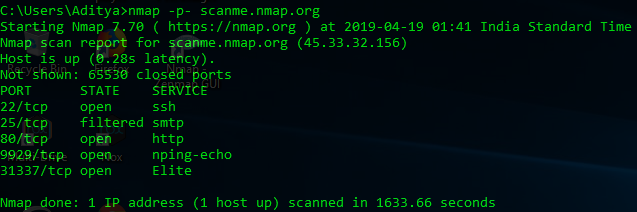
* nmap -p 0-65535 scame.nmap.org –T5



**Scan All TCP Ports**

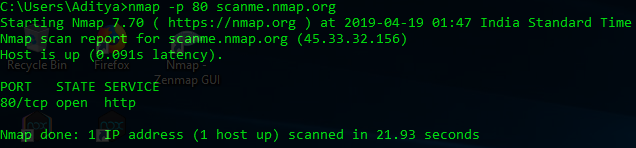
Another way to specify all TCP ports is dash. We can use -p- which is more practical then port range specification.

* nmap -p- scame.nmap.org



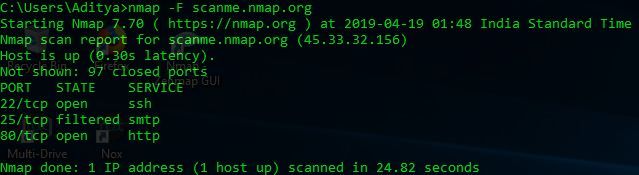
**Scan a single Port**

* nmap -p 80 scanme.nmap.org

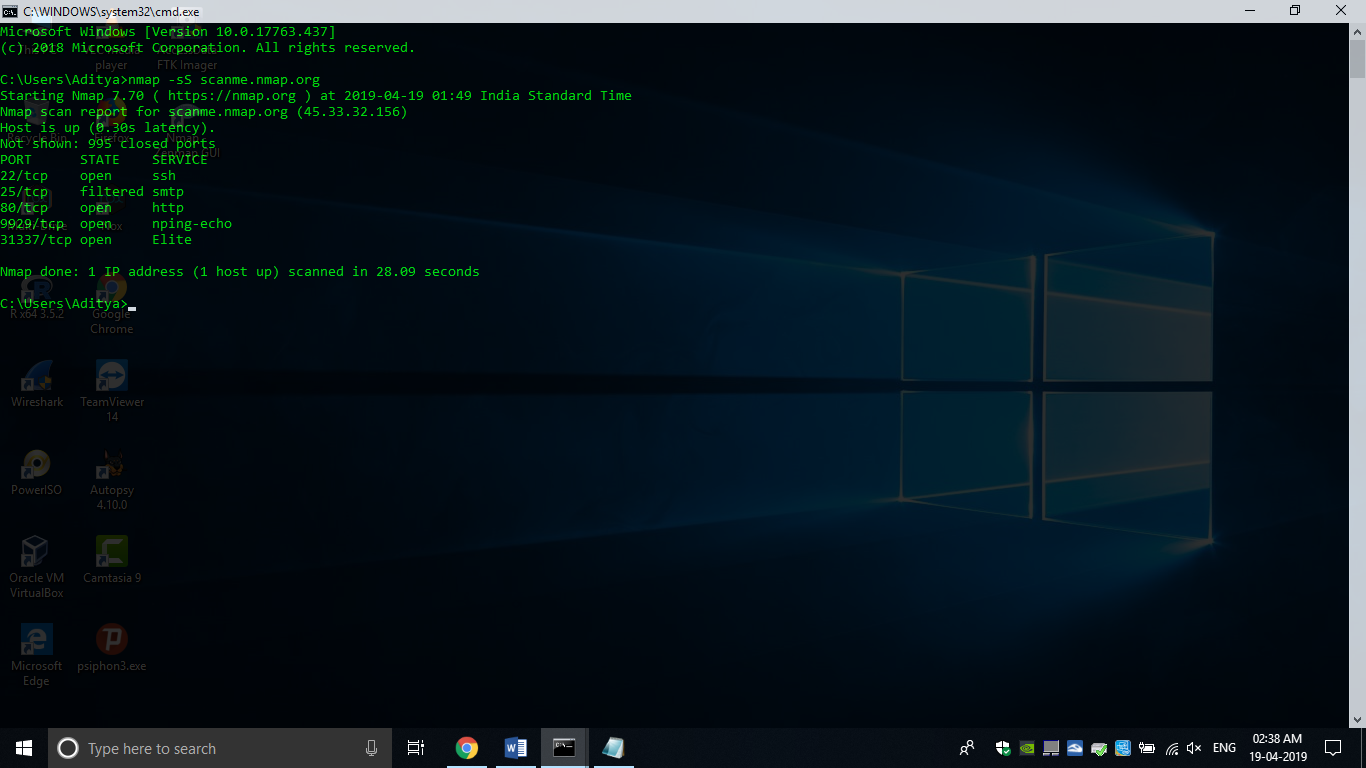


**Scan 100 most common ports (Fast)**

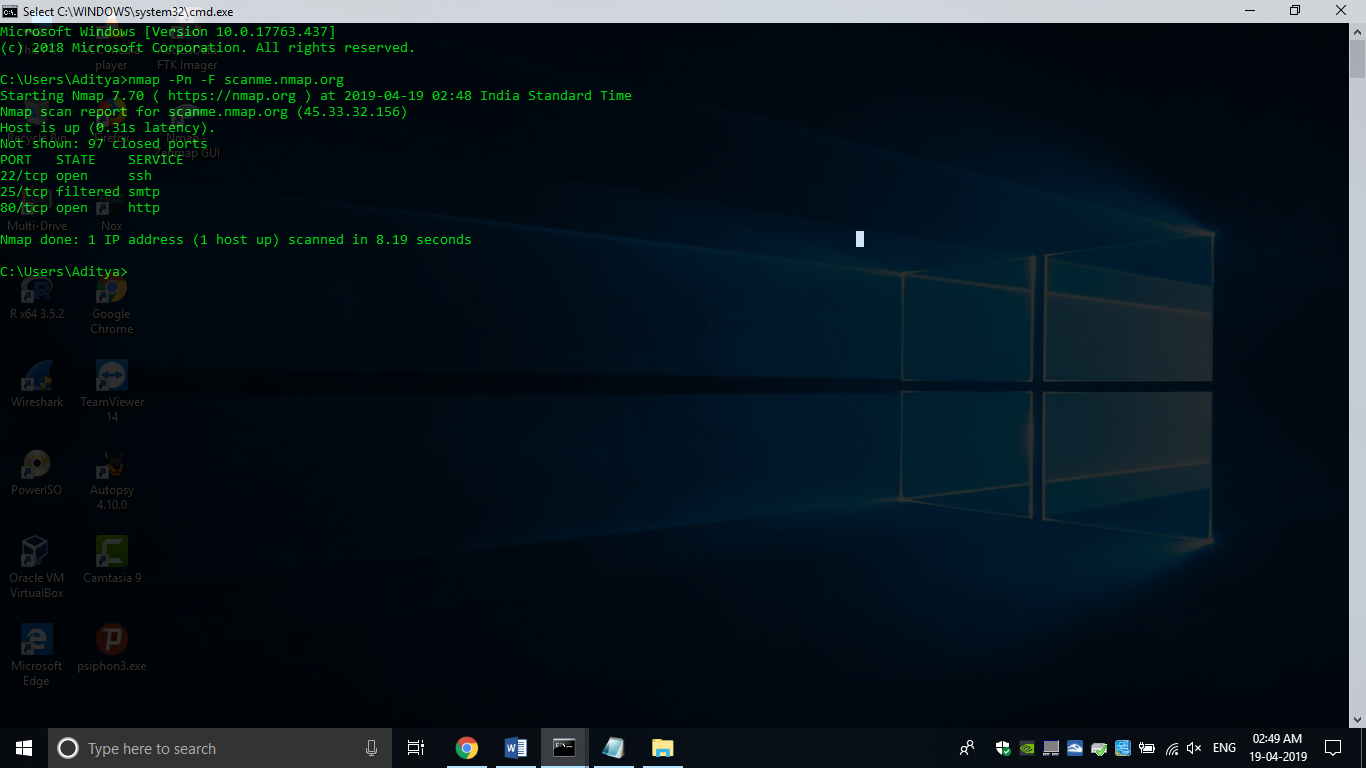
* nmap -F scanme.nmap.org



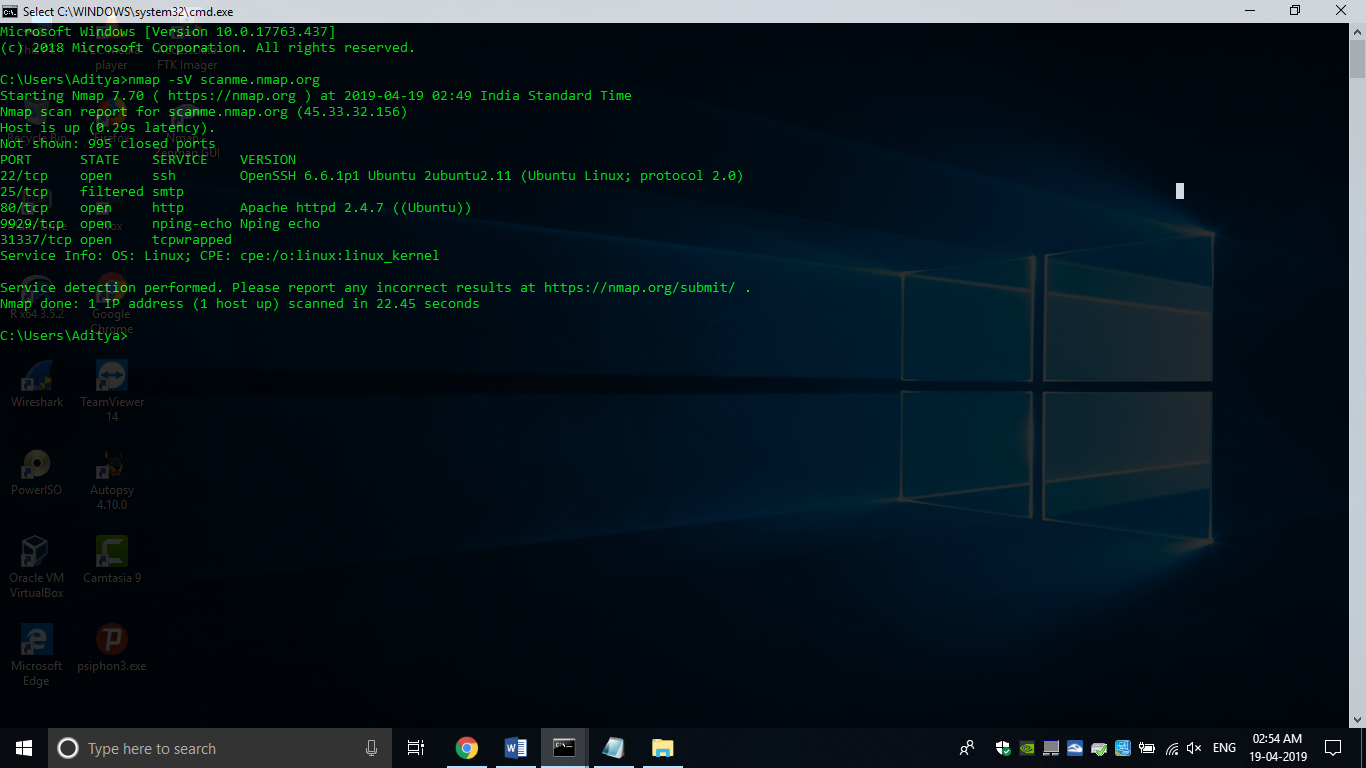
**can using TCP SYN scan (default)**

* ****nmap –sS scanme.nmap.org

**Scan selected ports - ignore discovery**

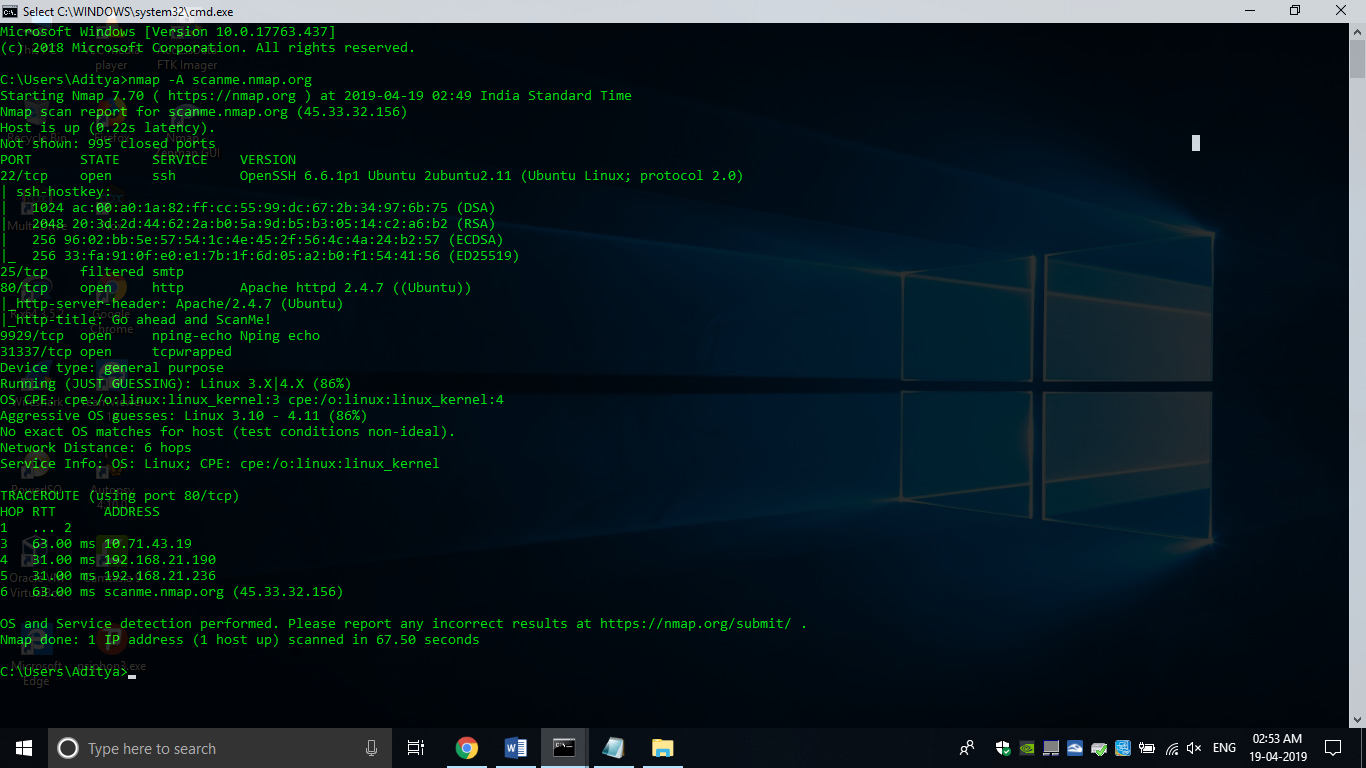
* nmap -Pn -F scanme.nmap.org

**Standard service detection**

* nmap -sV scanme.nmap.org

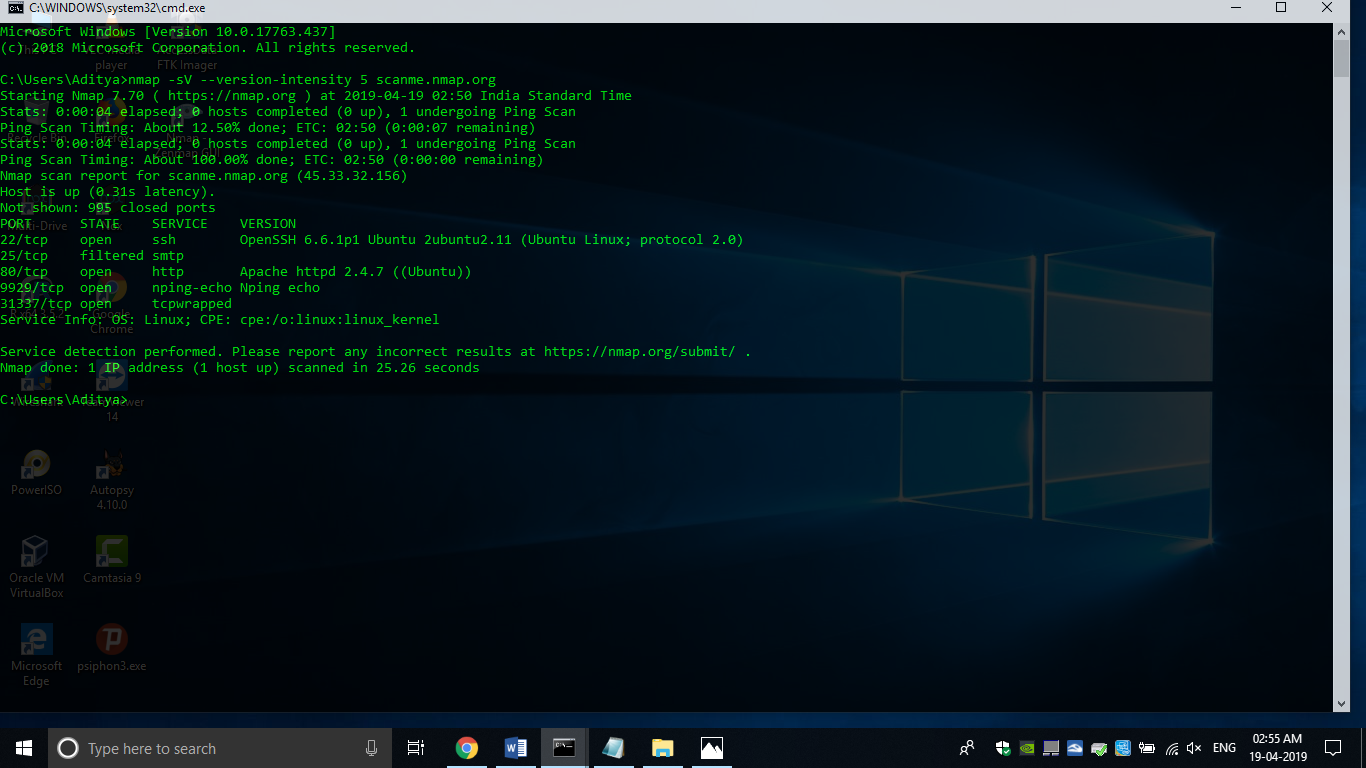
**Detect OS and Services**

* nmap -A scanme.nmap.org



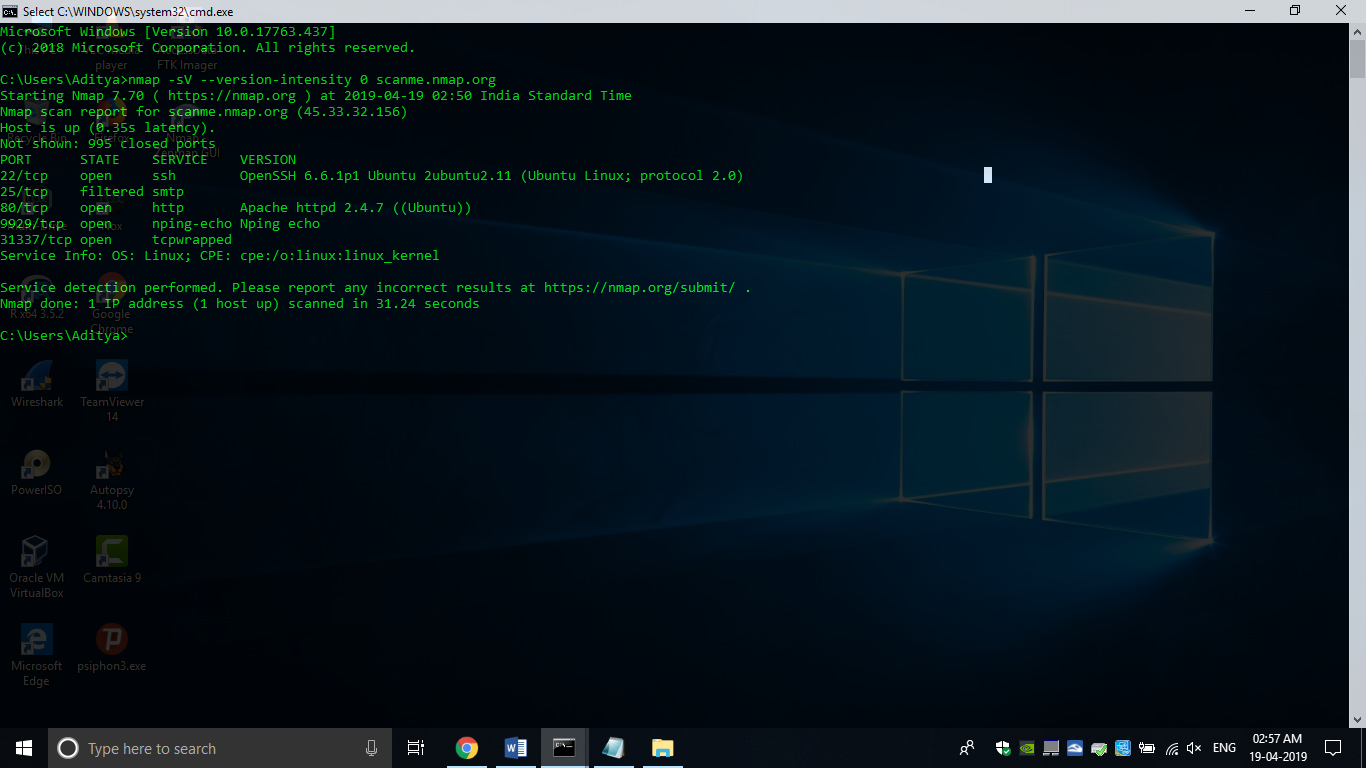
**More aggressive Service Detection**

* nmap -sV --version-intensity 5 scanme.nmap.org



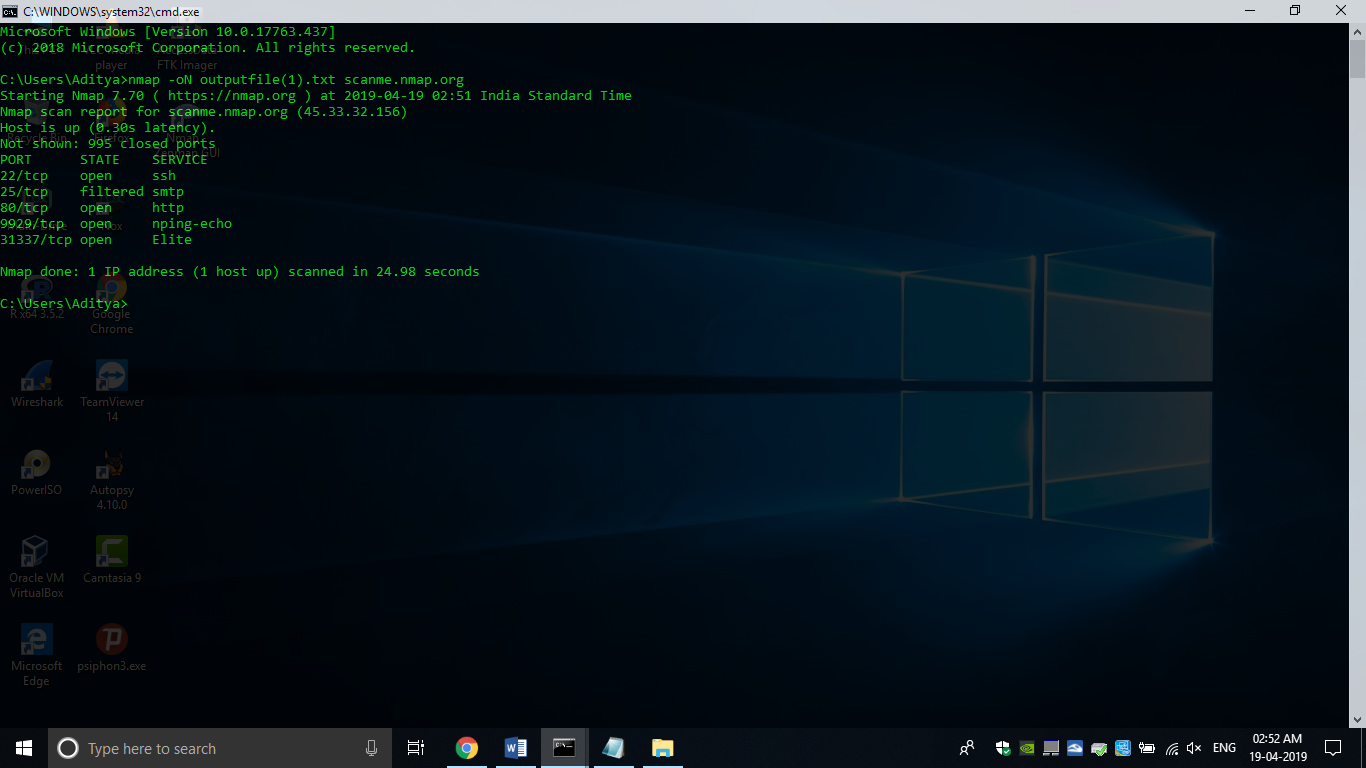
**Lighter banner grabbing detection**

* nmap -sV --version-intensity 0 scanme.nmap.org

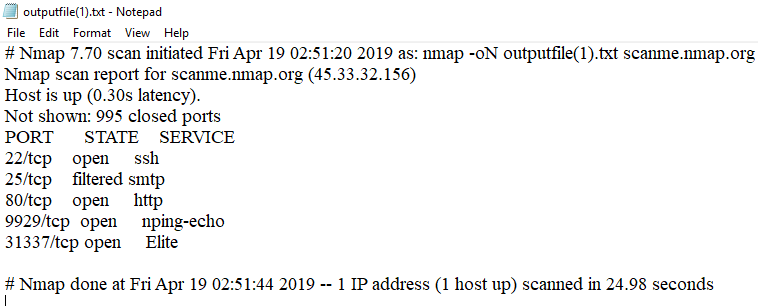


**Save default output to file**

* nmap -oN outputfile(1).txt scanme.nmap.org

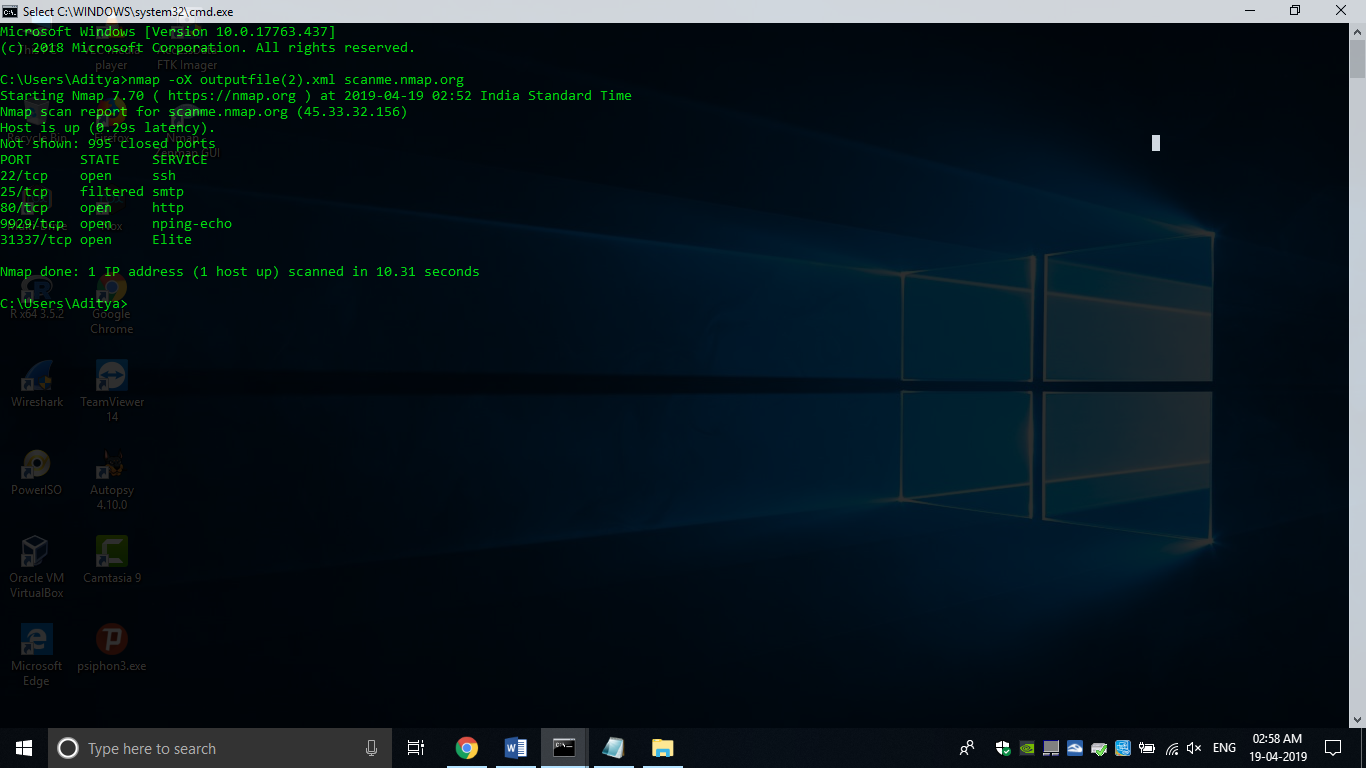


* Here, Text File

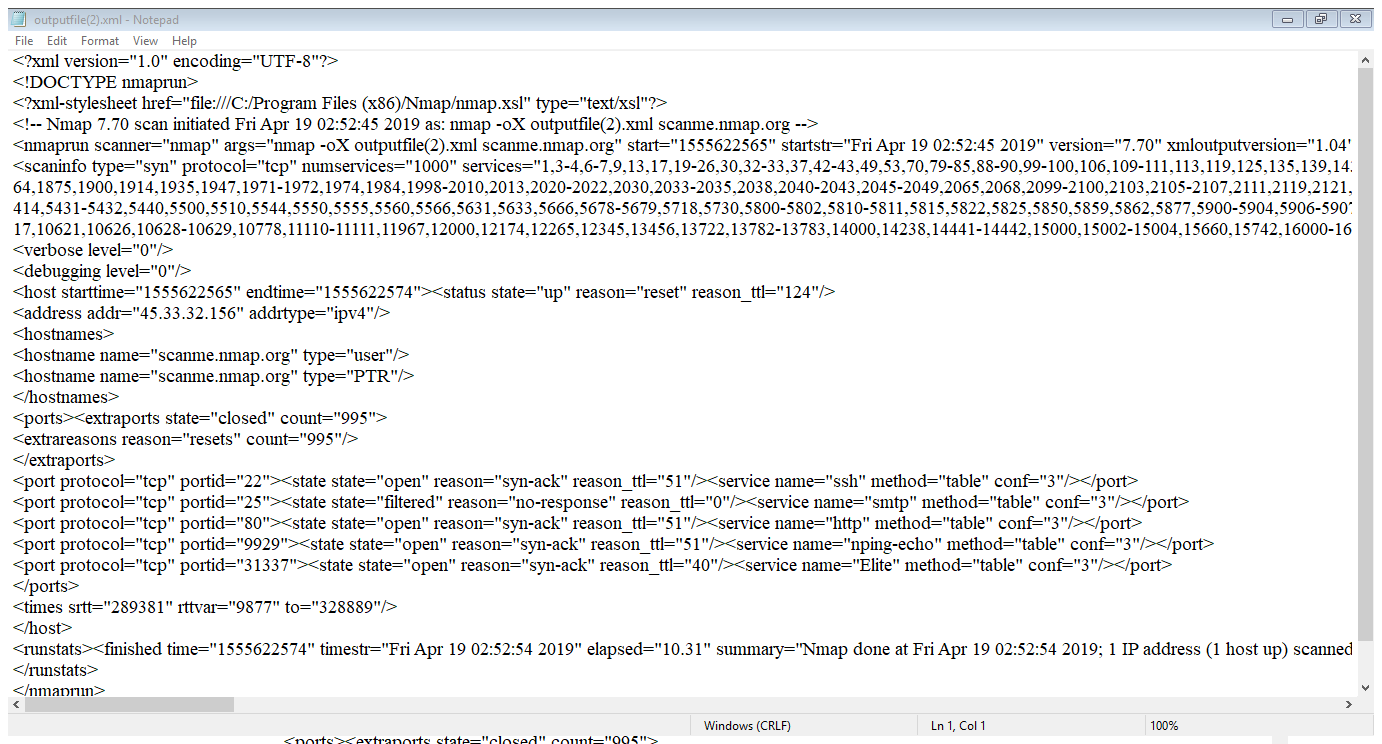


**Save results as XML**

* nmap -oX outputfile(2).xml scanme.nmap.org

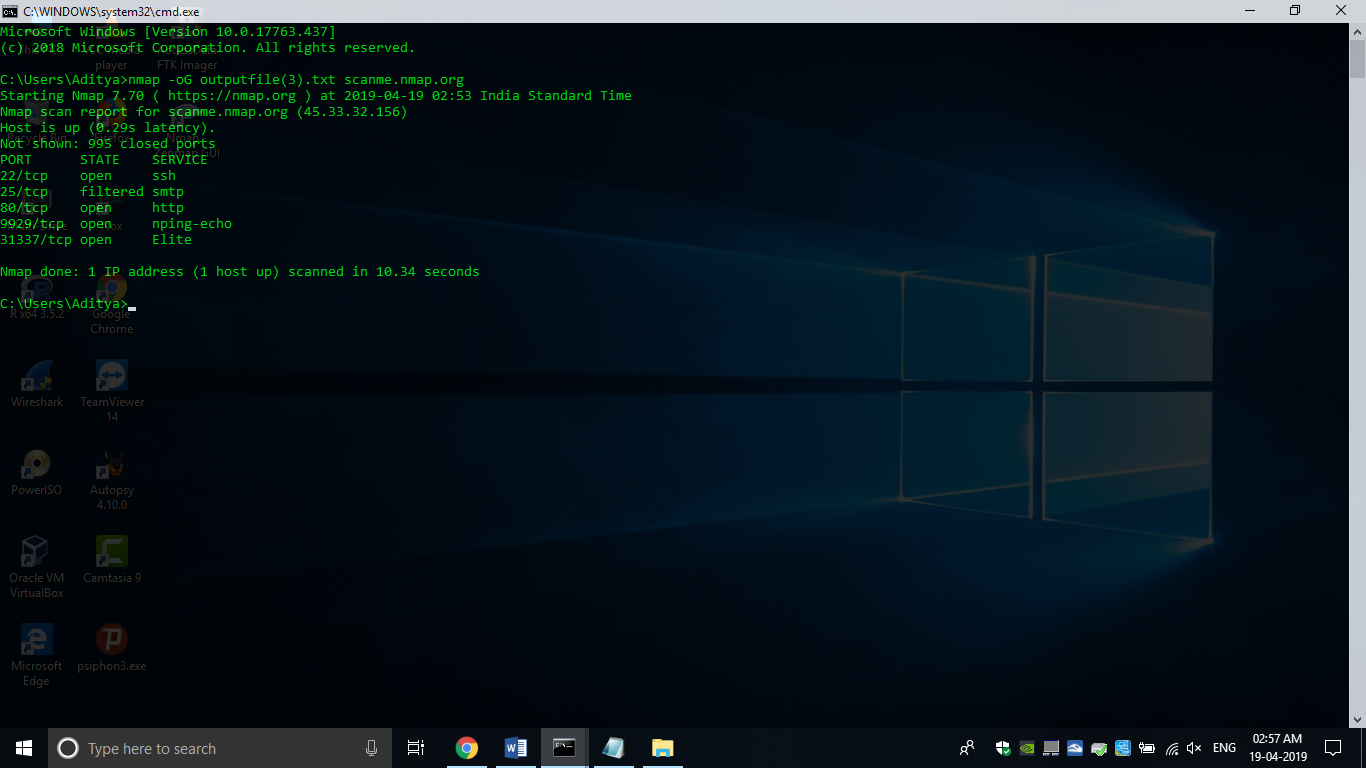


* Here, XML File in Notepad

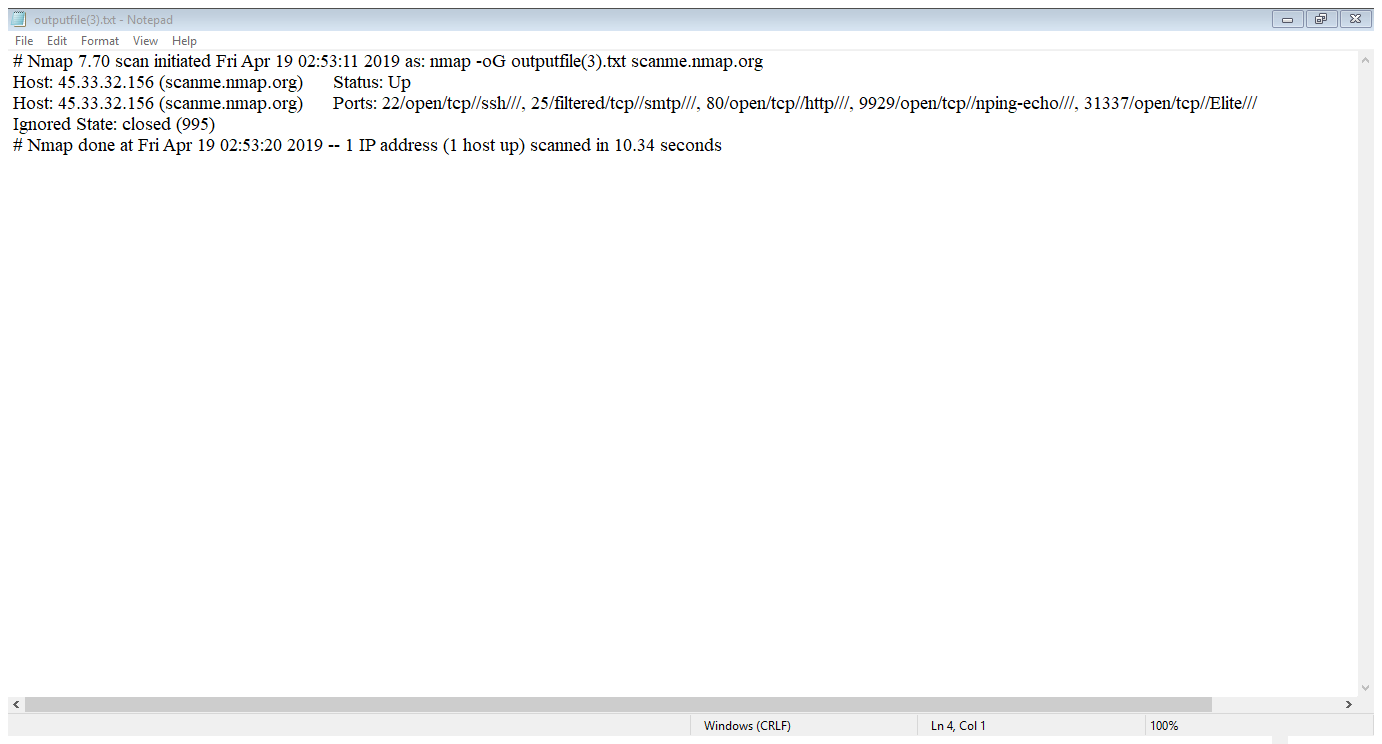


**Save results in a format for grep**

* nmap -oG outputfile(3).txt scanme.nmap.org

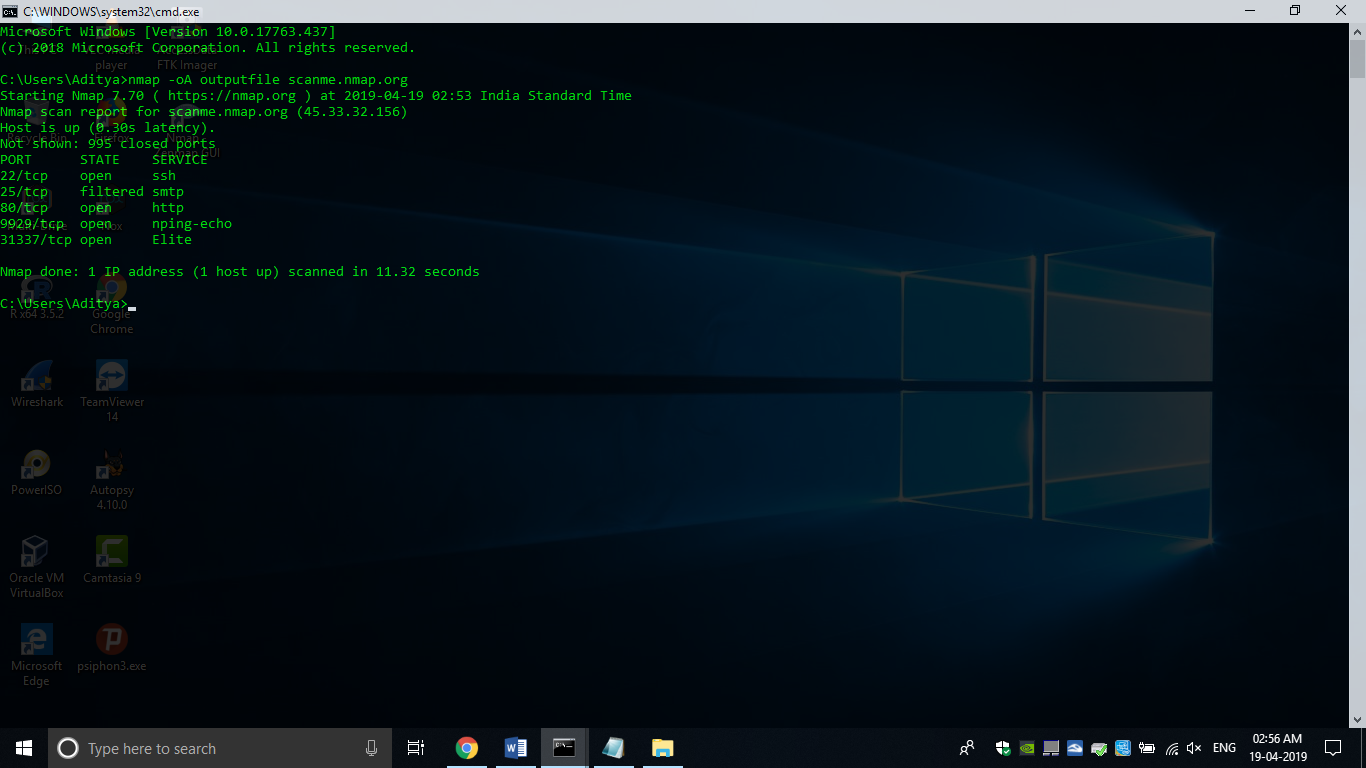


* Here, GRAP File output.txt

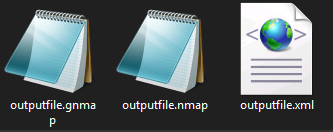


**Save in all formats**

* nmap -oA outputfile scanme.nmap.org



* Here, Three output file type



**Scan All UDP Ports with Range**

Nmap uses TCP as default protocol for port scan. We should explicitly specify the UDP protocol for UDP port scan. We will use same port range specification used in TCP. We will use -sU for UDP protocol specification.

* nmap -sU -p0-65535 scanme.nmap.org

**Scan All UDP Ports**

We will use -p- to specify all ports easily.

* nmap -sU -p- scanme.nmap.org

**Scan All TCP UDP Ports**

We can scan all UDP and TCP ports in a single command. We will use -sU for UDP and sT for TCP protocol.

* nmap -sU -sT -p0-65535 scanme.nmap.org