**Practical No. 3**

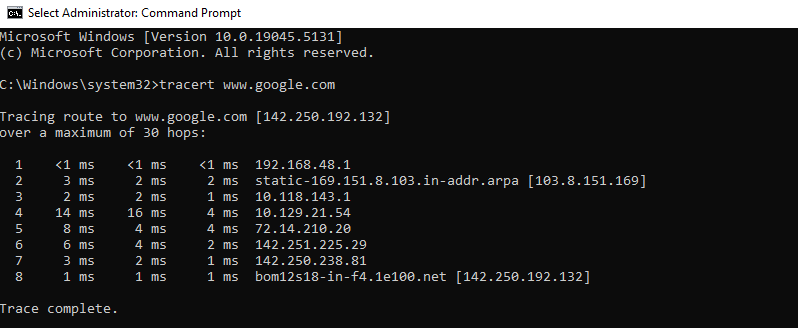
**Networking Commands**

**Aim:** Using TraceRoute , ping , ifconfig , netstat command.

**Steps:-**

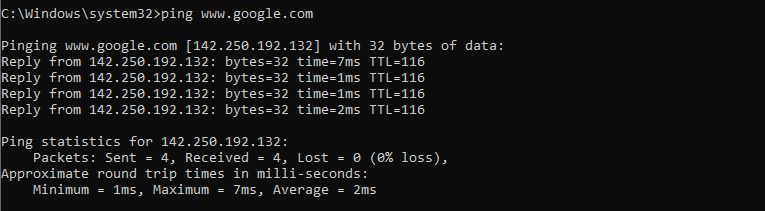
1. Open your cmd with administrator privelage.
2. Type the following commands:-
3. tracert [www.google.com](http://www.google.com)

The tracert command traces the path data packets take from your computer to a destination, showing each intermediate router along the way. It provides details on the time it takes for each hop, helping diagnose network performance issues like latency or routing problems.



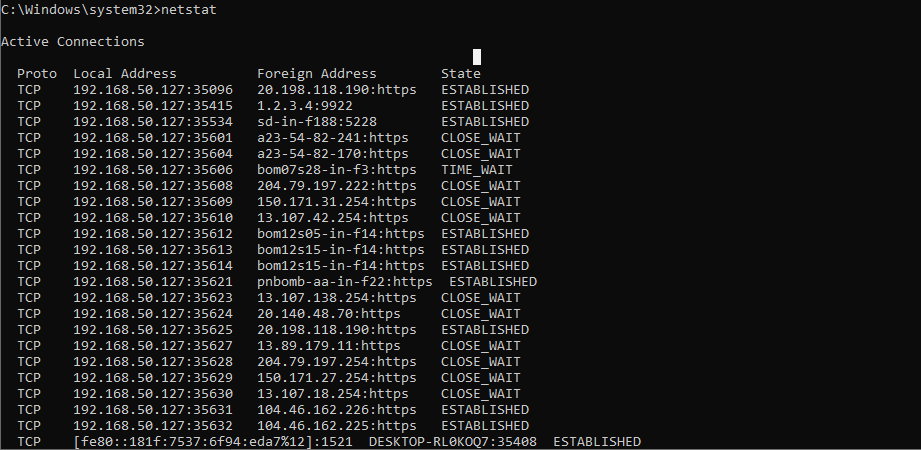
1. ping [www.google.com](http://www.google.com)

The ping command checks if a computer or website is reachable by sending small "test" messages. It then measures how long it takes for the message to go there and back, helping you see if there are any network delays or problems.



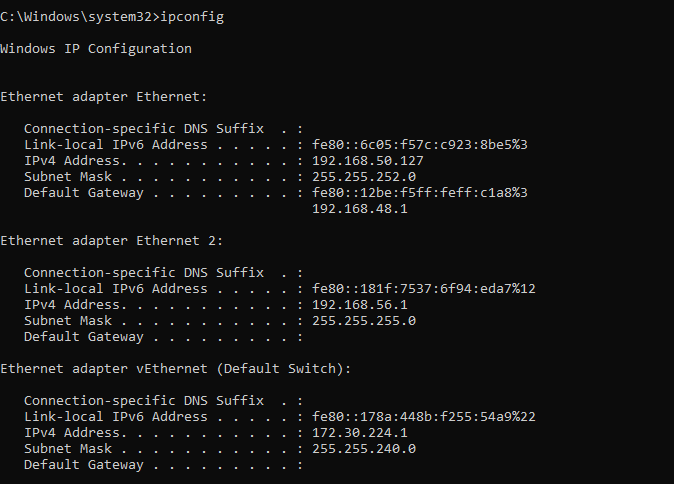
1. netstat

The netstat command shows active network connections on your computer, including open ports, connected devices, and network statistics. It helps you monitor and troubleshoot network activity by displaying information like which programs are using the network and their connection status.



1. ipconfig

The ipconfig command displays the current network configuration of your computer, including your IP address, subnet mask, and default gateway. It's useful for troubleshooting network issues and checking your device's network settings.



**Practical No. 4**

**Nmap Scanner**

**Aim:** Using Nmap scanner to perform port scanning of various forms – ACK , SYN , FIN , NULL , XMAS.

**Description:**

The Nmap (Network Mapper) command is a network scanning tool used to discover devices and services on a computer network. It can identify open ports, detect running services, and provide security information, helping with network security assessments and troubleshooting.

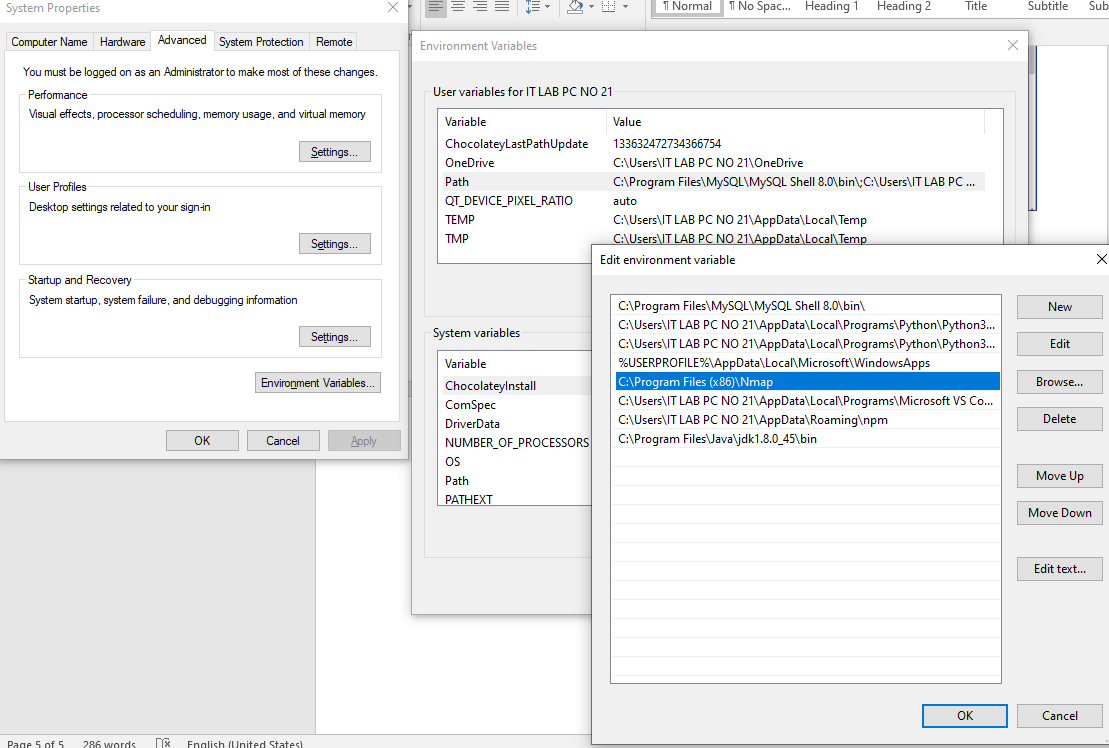
**Steps:**

1. Download and install Nmap , DL link:

https://nmap.org/dist/nmap-7.95-setup.exe



1. Set path for Nmap from any window.
2. Do the all set path steps properly.



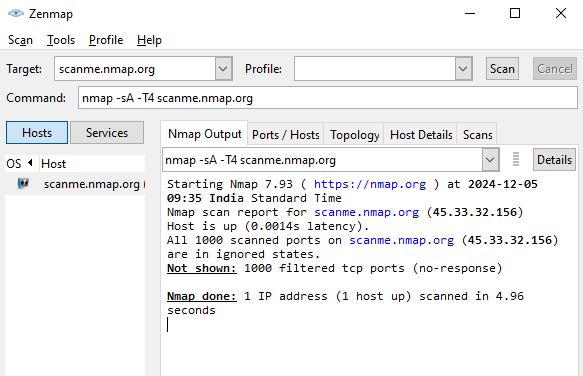
1. Open Zenmap GUI from desktop.

**Theory:**

1. ACK -sA (TCP ACK scan):

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

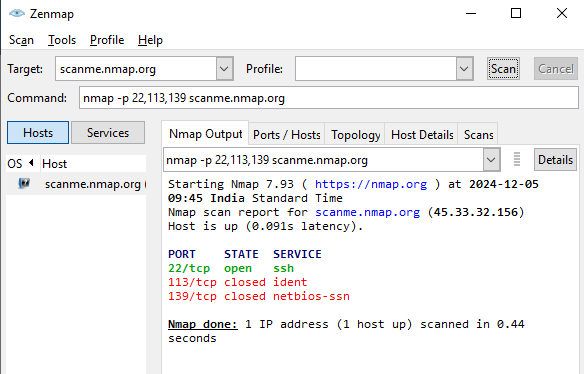
**Command:** nmap -sA -T4 scanme.nmap.org



1. SYN (Stealth) Scan (-sS):

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

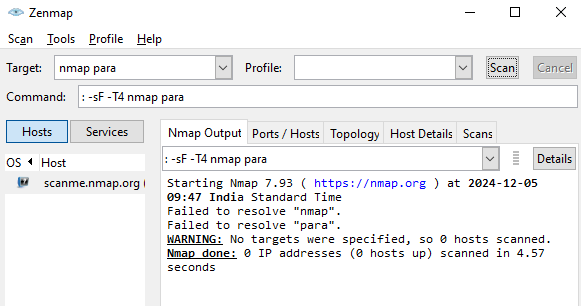
**Command:** nmap -p22,113,139 scanme.nmap.org



1. FIN Scan (-sF):

Sets just the TCP FIN bit.

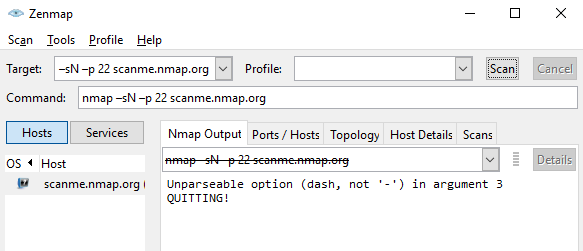
**Command:** nmap -sF -T4 para.



1. NULL Scan (-sN):

Does not set any bits (TCP flag header is 0)

**Command:** nmap –sN –p 22 scanme.nmap.org



1. XMAS Scan (-sX):

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

**Command:** nmap -sX -T4 scanme.nmap.org

