

Lab Question 1: Network Scanning, Sniffing, and Identification in Windows and Linux

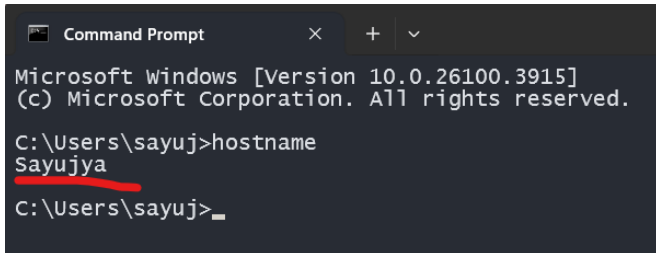
- Create a detailed lab report by researching and executing the following network-related commands in the Command Prompt (CMD). For each command, provide the purpose, the syntax, the output, and include screenshots of the results in your report. Use the commands below as a guideline:

Check computer name and username

Command: hostname

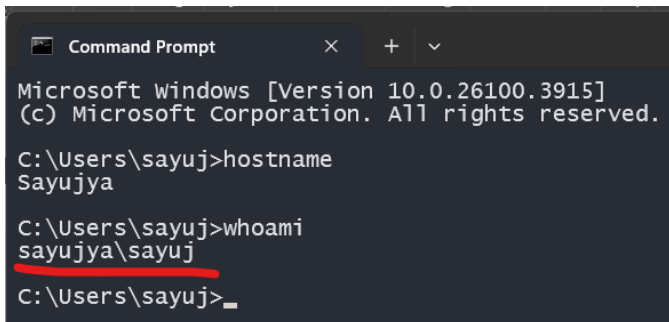
Command: whoami

Objective : Check computer name and username



```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sayuj>hostname
Sayujya
C:\Users\sayuj>
```



```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

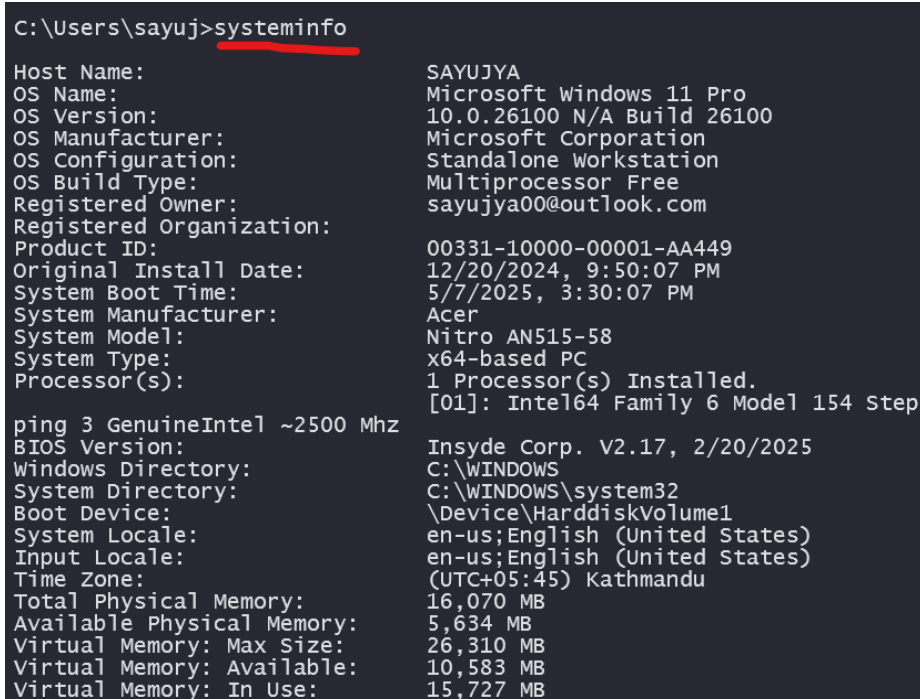
C:\Users\sayuj>hostname
Sayujya

C:\Users\sayuj>whoami
sayujya\sayuj
C:\Users\sayuj>
```

Detailed system info (OS, processor, BIOS, etc.):

Command: Systeminfo

Objective: Displays OS version, manufacturer, boot time, RAM, domain, etc



```
C:\Users\sayuj>systeminfo

Host Name: SAYUJYA
OS Name: Microsoft Windows 11 Pro
OS Version: 10.0.26100 N/A Build 26100
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: sayujya00@outlook.com
Registered Organization:
Product ID: 00331-10000-00001-AA449
Original Install Date: 12/20/2024, 9:50:07 PM
System Boot Time: 5/7/2025, 3:30:07 PM
System Manufacturer: Acer
System Model: Nitro AN515-58
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 154 Step
ping 3 GenuineIntel ~2500 Mhz
BIOS Version: Insyde Corp. V2.17, 2/20/2025
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC+05:45) Kathmandu
Total Physical Memory: 16,070 MB
Available Physical Memory: 5,634 MB
Virtual Memory: Max Size: 26,310 MB
Virtual Memory: Available: 10,583 MB
Virtual Memory: In Use: 15,727 MB
```

```
Command Prompt
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sayuj>hostname
Sayujya

C:\Users\sayuj>whoami
sayujya\sayuj

C:\Users\sayuj>systeminfo

Host Name: SAYUJYA
OS Name: Microsoft Windows 11 Pro
OS Version: 10.0.26100 N/A Build 26100
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: sayujya00@outlook.com
Registered Organization:
Product ID: 00331-10000-00001-AA449
Original Install Date: 12/20/2024, 9:50:07 PM
System Boot Time: 5/7/2025, 3:30:07 PM
System Manufacturer: Acer
System Model: Nitro AN515-58
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 154 Step
ping 3 GenuineIntel ~2500 Mhz
BIOS Version: Insyde Corp. V2.17, 2/20/2025
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
```

Network Information-View IP address, gateway, DNS:

Objective: To display the current network configuration details of all network adapters on a Windows machine. This includes: IP address ; Subnet mask ;Default gateway ; DNS server ; MAC address.

Command: ipconfig

Options:

- **/?:** Display this help message
- **/all:** Display full configuration information.
- **/release:** Release the IPv4 address for the specified adapter.
- **/release6:** Release the IPv6 address for the specified adapter.
- **/renew:** Renew the IPv4 address for the specified adapter.
- **/renew6:** Renew the IPv6 address for the specified adapter.
- **/flushdns:** Purges the DNS Resolver cache.
- **/registerdns:** Refreshes all DHCP leases and re-registers DNS names
- **/displaydns:** Display the contents of the DNS Resolver Cache.
- **/showclassid:** Displays all the dhcp class IDs allowed for adapter.
- **/setclassid:** Modifies the dhcp class id.
- **/showclassid6:** Displays all the IPv6 DHCP class IDs allowed for adapter.
- **/setclassid6:** Modifies the IPv6 DHCP class id.

Used For:

- Check if the PC has an IP address assigned
- Identify network issues (e.g., no gateway = no internet)
- View DNS configuration

```
C:\Users\sayuj>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : Sayujya
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet
Adapter
Physical Address. . . . . : 0A-00-27-00-00-06
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::607:c9cf:c416:1d91%6(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 772407335
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-F0-B8-4A-40-C2-BA-14-20-C3
NetBIOS over Tcpip. . . . . : Enabled
```

Wireless LAN adapter Local Area Connection* 9:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
```

```
C:\Users\sayuj>ipconfig /?
```

USAGE:

```
ipconfig [/allcompartments] [/? | /all |
/renew [adapter] | /release [adapter] |
/renew6 [adapter] | /release6 [adapter] |
/flushdns | /displaydns | /registerdns |
/showclassid adapter |
/setclassid adapter [classid] |
/showclassid6 adapter |
/setclassid6 adapter [classid] ]
```

where

adapter Connection name
 (wildcard characters * and ? allowed, see examples)

Options:

/?	Display this help message
/all	Display full configuration information.
/release	Release the IPv4 address for the specified adapter
/release6	Release the IPv6 address for the specified adapter
/renew	Renew the IPv4 address for the specified adapter.
/renew6	Renew the IPv6 address for the specified adapter.
/flushdns	Purges the DNS Resolver cache.
/registerdns	Refreshes all DHCP leases and re-registers DNS names
/displaydns	Display the contents of the DNS Resolver Cache.
/showclassid	Displays all the dhcp class IDs allowed for adapter.
/setclassid	Modifies the dhcp class id.
/showclassid6	Displays all the IPv6 DHCP class IDs allowed for adapter.
/setclassid6	Modifies the IPv6 DHCP class id.

Command: ping <hostname/IP>

Objective: Tests network connectivity to another host.

```
C:\Users\sayuj>ping sxc.edu.np

Pinging sxc.edu.np [103.90.87.172] with 32 bytes of data:
Reply from 103.90.87.172: bytes=32 time=4ms TTL=56
Reply from 103.90.87.172: bytes=32 time=17ms TTL=56
Reply from 103.90.87.172: bytes=32 time=3ms TTL=56
Reply from 103.90.87.172: bytes=32 time=3ms TTL=56

Ping statistics for 103.90.87.172:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 17ms, Average = 6ms
```

Command: ping /?

Objective: To view all ping command options (help menu) in Windows Command Prompt

```
C:\Users\sayuj>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
    -t                Ping the specified host until stopped.
                       To see statistics and continue - type Control-Break;
                       To stop - type Control-C.
    -a                Resolve addresses to hostnames.
    -n count           Number of echo requests to send.
    -l size            Send buffer size.
    -f                Set Don't Fragment flag in packet (IPv4-only).
    -i TTL             Time To Live.
    -v TOS             Type Of Service (IPv4-only. This setting has been depre
cated
P                     and has no effect on the type of service field in the I
P
                       Header).
    -r count           Record route for count hops (IPv4-only).
    -s count           Timestamp for count hops (IPv4-only).
    -j host-list       Loose source route along host-list (IPv4-only).
    -k host-list       Strict source route along host-list (IPv4-only).
    -w timeout         Timeout in milliseconds to wait for each reply.
    -R                Use routing header to test reverse route also (IPv6-onl
y).
                       Per RFC 5095 the use of this routing header has been
                       deprecated. Some systems may drop echo requests if
                       this header is used.
    -S srcaddr         Source address to use.
    -c compartment     Routing compartment identifier.
    -p                Ping a Hyper-V Network Virtualization provider address.
    -4                Force using IPV4.
    -6                Force using IPV6.
```

Command: ping youtube.com -t

Note: For stop/break the request use command: press at a time “ctrl+c” in your keyboard.

```

C:\Users\sayuj>ping sxc.edu.np -t
Pinging sxc.edu.np [103.90.87.172] with 32 bytes of data:
Reply from 103.90.87.172: bytes=32 time=4ms TTL=56
Reply from 103.90.87.172: bytes=32 time=4ms TTL=56
Reply from 103.90.87.172: bytes=32 time=4ms TTL=56
Reply from 103.90.87.172: bytes=32 time=4ms TTL=56
Reply from 103.90.87.172: bytes=32 time=3ms TTL=56
Reply from 103.90.87.172: bytes=32 time=3ms TTL=56

Ping statistics for 103.90.87.172:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms
Control-C
^C
C:\Users\sayuj>_

```

Example Scenario:

- You're troubleshooting a slow internet connection.
- Run ping google.com -t to see if any packet loss or high latency occurs.
- Use ping google.com -l 1500 to check if large packets are being dropped.
- Use ping google.com -4 and -6 to test if the issue is with IPv4 or IPv6.

Command and their Use Case/When to Use

ping <IP>: To test if a device or website is reachable (e.g., ping 8.8.8.8 to check internet connection).

ping <IP> -t: To monitor network stability over time, useful for spotting intermittent connection drops.

ping <IP> -n <X>: To send a specific number of pings for controlled testing (e.g., test 10 responses with -n 10).

ping <IP> -l <X>: To test network packet handling or MTU size issues by sending larger or smaller packets.

ping <IP> -4: To ensure the ping uses an IPv4 address, especially in dual-stack networks (IPv4 + IPv6).

ping <IP> -6: To test IPv6 connectivity on networks where IPv6 is used or being configured.

User and Computer Details:

List all users on the system:

Command: net user

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user

User accounts for \\SAYUJYA

-----
Administrator          DefaultAccount          Guest
sayuj                   WDAGUtilityAccount
The command completed successfully.

```

Command: net user sayuj

In cybersecurity, knowing User and Computer Details through command-line tools is essential for multiple tasks, such as monitoring, incident response, auditing, and securing systems. Here's how these commands are used in a cybersecurity context:

User and Computer Detail Commands (with Cybersecurity Uses)

Command	Use in Cybersecurity
whoami	Shows the currently logged-in user — useful to verify privilege level (e.g., admin vs standard).
net user	Lists all user accounts on the system — used to detect unauthorized or suspicious users .
net user <username>	Checks details like password policies, account status, and login info — helps audit user configurations .
hostname	Identifies the machine name — important for tracking incidents across multiple systems.
echo %username%	Quickly displays the current user — helpful in batch scripting and automation.
systeminfo	Provides OS, BIOS, and update info — used to check patch levels and vulnerabilities .
wmic computersystem get name,username	Shows currently logged-in user and computer name — useful for tracking active sessions .
set	Lists environment variables — can reveal paths and configurations useful to attackers or defenders.

```

C:\Windows\System32>net user sayuj
User name                sayuj
Full Name                 SAYUJYA SATYAL
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        11/22/2023 11:35:08 PM
Password expires         Never
Password changeable      11/22/2023 11:35:08 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

Local Group Memberships  *Administrators      *ORA_ASMDBA
                        *ORA_DBA                *ORA_Oradb21Home1_SYSB
                        *ORA_Oradb21Home1_SYSD*ORA_Oradb21Home1_SYSK
                        *Users
Global Group memberships *None
The command completed successfully.

```

```

C:\Windows\System32>whoami
sayujya\sayuj

```

```

C:\Windows\System32>whoami
sayujya\sayuj

C:\Windows\System32>echo %username%
sayuj

C:\Windows\System32>wmic computersystem get name, username
Name      UserName
SAYUJYA   Sayujya\sayuj

```

Command to Create a New User (Windows CMD)

Syntax: net user Test test@123 /add

Test = New username

test@123 = Password (you can customize it)

/add = Tells Windows to add the user


```
C:\Windows\System32>net user Test test@123 /add  
The command completed successfully.  
  
C:\Windows\System32>net user Test test@123 /add  
The account already exists.  
  
More help is available by typing NET HELPMSG 2224.
```

To Make the User an Administrator

Command: net localgroup administrators Test /add

Objective: Adds the user to the Administrators group, giving them admin privileges

```
C:\Windows\System32>net localgroup administrators Test /add  
The command completed successfully.
```

Use Case: In cybersecurity, the command to create a new user and assign admin privileges has both defensive and offensive (ethical hacking or forensic) applications. Here's the purpose and use of these commands in cybersecurity:

Cybersecurity Uses of Creating a New User

1. For Lab & Audit Setup (Defensive Use)

- You create a user like Test to verify that a student or analyst is using their own system for lab work.
- Helps track user actions separately from the default system user.
- Used during forensic imaging or analysis, so the forensic examiner works in a separate user account.

2. For Privilege Escalation Testing (Offensive / Ethical Hacking Use)

- In penetration testing, attackers or ethical hackers may try to:
- Create a hidden admin user to maintain access.
- Escalate privileges by adding a user to the Administrators group.

3. For Incident Response & Recovery

- If a system is compromised and the main admin account is locked or damaged:
- An incident responder can create a new admin account to regain control.
- Quickly restore administrative access without reinstalling the OS.

Security Best Practice

- Audit all user creation and admin privilege changes using Event Viewer or logs.
- Disable or delete test/admin accounts like AnishBIM004 after the lab or incident is done.

To hide a user account from the Windows login screen (e.g., for legitimate administrative or forensic purposes), you can do it via the Windows Registry Editor using Command Prompt. This is sometimes used by system administrators or forensic analysts to keep a user account hidden from casual users.

Important: This should only be done on systems you own or have explicit permission to modify. Unauthorized hiding of users can be considered malicious behavior.

Steps to Hide a User Account in Windows via CMD

1. Open Command Prompt as Administrator
2. Run the following command:

Command:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v AnishBIM004 /t REG_DWORD /d 0 /f
```

- Test = The username you want to hide
- 0 = Hides the user from the login screen
- This modifies the Registry to hide the user under the UserList key.

Explanation of Each Flag & Component:

Part	Meaning
<code>reg add</code>	Adds a new registry key or value to the Windows Registry.
<code>"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList"</code>	This is the registry path . It tells Windows where to add the new entry. <ul style="list-style-type: none">◆ <code>HKLM</code> = HKEY_LOCAL_MACHINE (global to all users)◆ <code>SpecialAccounts\UserList</code> = A special section that controls whether user accounts appear on the login screen.
<code>/v AnishBIM004</code>	Specifies the name of the value (in this case, the username) being added to that registry location.
<code>/t REG_DWORD</code>	Specifies the type of value. <ul style="list-style-type: none">◆ <code>REG_DWORD</code> = A 32-bit number, used here to toggle visibility (0 or 1).
<code>/d 0</code>	The actual data or value you're setting. <ul style="list-style-type: none">◆ <code>0</code> = Hide the user from the login screen.◆ <code>1</code> = Show the user again.
<code>/f</code>	Force overwrite without asking for confirmation. Useful for scripts or automation.

Example Use Case (Cybersecurity):

- In a cybersecurity lab or forensic setting, an investigator might use this command to:
- Hide a local admin or forensic account so it doesn't show up to the suspect.
- Create a clean environment to observe behavior without interfering.

To Unhide the User Again:

Run the Command:

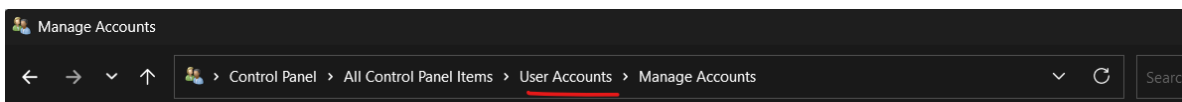
```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v AnishBIM004 /t REG_DWORD /d 1 /f
```

```
C:\Windows\System32>net user
```

User accounts for \\SAYUJYA

```
-----
Administrator          DefaultAccount          Guest
sayuj                   Test                   WDAGUtilityAccount
The command completed successfully.
```

```
C:\Windows\System32>
```



Choose the user you would like to change



SAYUJYA SATYAL
sayujya00@outlook.com
Administrator
Password protected

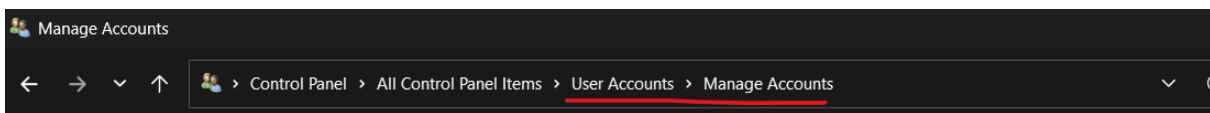
1



Test
Local Account
Administrator
Password protected

2

```
C:\Windows\System32>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v Test /t REG_DWORD /d 0 /f  
The operation completed successfully.
```



Choose the user you would like to change



SAYUJYA SATYAL
sayujya00@outlook.com
Administrator
Password protected

1

How to Log in to a Hidden User Account in Windows

Method 1: Manual Username Entry (Windows Login Screen)

1. On the login screen, press **Ctrl + Alt + Delete** (if required).
2. Click "**Other user**" or press **Esc** if your usual login options appear.
3. In the **username field**, manually type the hidden username (e.g., AnishBIM004).
4. Enter the password and press **Enter**.
Even though the account is hidden from the welcome screen, it can still be used by **manually typing the credentials**.

Method 2: Switch User (If Already Logged In)

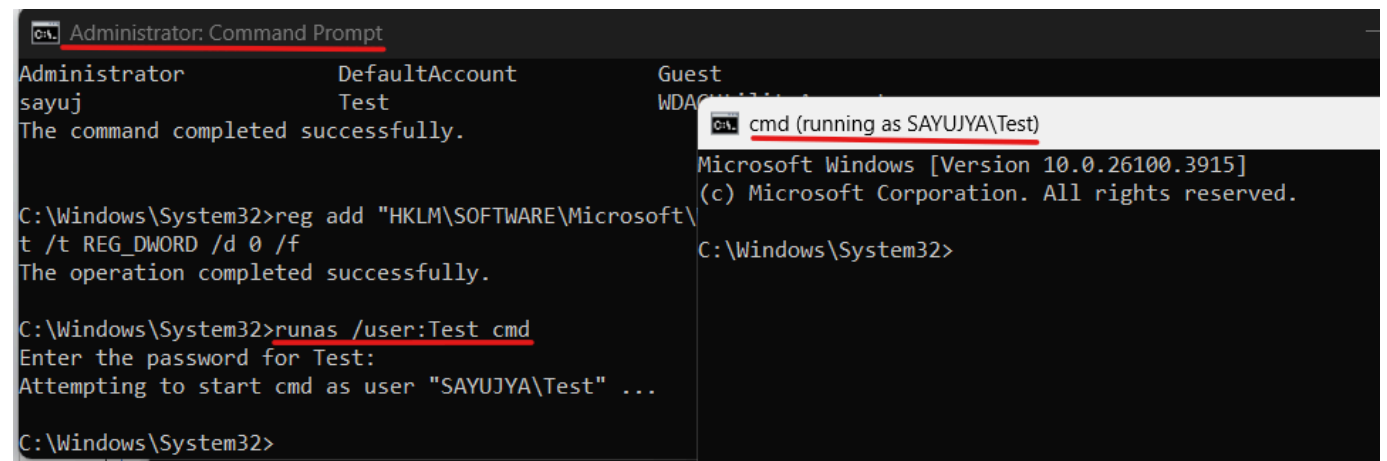
If you're logged in with another user:

1. Press **Ctrl + Alt + Delete** → choose "**Switch user**".
2. Now you'll get the manual login screen where you can type:
Username: AnishBIM004
Password: (whatever you set)

Method 3: Login via Command Line (RunAs)

- If you're inside another account and want to run something as the hidden user:
- Command: `runas /user:AnishBIM004 cmd`

Command: `runas /user:Test cmd`



```
Administrator: Command Prompt
Administrator      DefaultAccount      Guest
sayuj              Test                WDA
The command completed successfully.

C:\Windows\System32>reg add "HKLM\SOFTWARE\Microsoft\
t /t REG_DWORD /d 0 /f
The operation completed successfully.

C:\Windows\System32>runas /user:Test cmd
Enter the password for Test:
Attempting to start cmd as user "SAYUJYA\Test" ...











C:\Windows\System32>
```

cmd (running as SAYUJYA\Test)

```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

What a Hidden Admin User Can Do (If Misused):

Action	Description
 Bypass monitoring	Operate without drawing attention since the user is hidden from the login screen.
 Install malicious software	Install keyloggers, remote access tools (RATs), or backdoors.
 Extract or change passwords	Use tools like <code>mimikatz</code> or access <code>Credential Manager</code> to steal saved credentials.
 Access all user files	As an admin, access all folders—even those of other users.
 Delete logs/traces	Clear event logs or manipulate log files to cover tracks.
 Disable security features	Turn off antivirus, firewall, UAC, or Windows Defender.
 Exfiltrate data	Upload confidential files to the internet or external drives.
 Create persistence	Add scheduled tasks, registry entries, or startup items to regain access later.
 Sniff network traffic	Install sniffers like Wireshark to capture network credentials or traffic.
 Impersonate other users	Add themselves to user groups or reset passwords to take over accounts.

Real-World Risk Example:

A rogue employee creates a hidden admin account before quitting. Months later, they log in remotely, access sensitive files, or sabotage systems—completely unnoticed, since their account doesn't appear on the login screen or in casual user management views.

From a Cybersecurity Training View: This scenario is often part of **Red Team exercises**, used to:

- Simulate insider threats.
- Train Blue Teams on detecting hidden persistence.
- Test incident response processes.

Defense Tip (Blue Team / Prevention):

- Monitor the registry key:
- `HKLM\...\Winlogon\SpecialAccounts\UserList`
- Regularly audit user accounts via:

- Regularly audit user accounts via:

```
cmd

net user
```

- Check for users in the **Administrators group**:

```
cmd

net localgroup administrators
```

- Use SIEM tools or Windows Event Logs to flag logins from unknown or hidden users.

Traceroute and Path Testing

Run tracert google.com.

- **Purpose:** Shows the path that packets take from your computer to a destination by listing all intermediate routers (hops).
- **Syntax:** tracert [hostname or IP address]

```
C:\Users\sayuj>tracert google.com
```

```
Tracing route to google.com [2404:6800:4009:831::200e]
over a maximum of 30 hops:
```

```
  1      2 ms      2 ms      2 ms  2404:7c00:44:3e41:72a5:6aff:fe7b:5cad
  2      3 ms      3 ms     21 ms  2404:7c00::10
  3      3 ms      2 ms      3 ms  2404:7c00:0:7::2
  4      4 ms      3 ms      3 ms  2404:7c00:0:6::2
  5     44 ms     44 ms     44 ms  2404:a800:3a00:2::279
  6     43 ms     43 ms     43 ms  2404:a800::92
  7     41 ms     41 ms     41 ms  2001:4860:1:1::674
  8     44 ms     44 ms     44 ms  2404:6800:8202:240::1
  9      *        *        *    Request timed out.
 10     52 ms      *        52 ms  2001:4860:0:1::8826
 11     51 ms     51 ms     51 ms  2001:4860::9:4001:b922
 12     66 ms     54 ms     55 ms  2001:4860::9:4002:d931
 13     51 ms     51 ms     51 ms  2001:4860:0:1::8711
 14     52 ms     51 ms     51 ms  2001:4860:0:1::5c07
 15     51 ms     51 ms     52 ms  bom12s21-in-x0e.1e100.net [2404:6800:4009:831::200e]
```

```
Trace complete.
```

Use pathping google.com.

- **Purpose:** Combines the functions of ping and tracert to show route and packet loss statistics for each hop.
- **Syntax:** pathping [hostname or IP address]

```
C:\Users\sayuj>pathping google.com

Tracing route to google.com [2404:6800:4009:831::200e]
over a maximum of 30 hops:
 0 Sayujya [2404:7c00:44:3e41:6da1:a895:8300:efc5]
 1 2404:7c00:44:3e41:72a5:6aff:fe7b:5cad
 2 2404:7c00::10
 3 2404:7c00:0:7::2
 4 2404:7c00:0:6::2
 5 2404:a800:3a00:2::279
 6 2404:a800::92
 7 2001:4860:1:1::674
 8 2404:6800:8202:240::1
 9 * * *

Computing statistics for 200 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
     RTT      Lost/Sent = Pct  Lost/Sent = Pct  Sayujya [2404:7c00:44:3e41:6da1:a895:8300:efc5]
 0      0ms      0/ 100 = 0%      0/ 100 = 0%      |
 1      2ms      0/ 100 = 0%      0/ 100 = 0%      | 2404:7c00:44:3e41:72a5:6aff:fe7b:5cad
 2      5ms      0/ 100 = 0%      0/ 100 = 0%      | 2404:7c00::10
 3      6ms      0/ 100 = 0%      0/ 100 = 0%      | 2404:7c00:0:7::2
 4      4ms      0/ 100 = 0%      0/ 100 = 0%      | 2404:7c00:0:6::2
 5     42ms      0/ 100 = 0%      0/ 100 = 0%      | 2404:a800:3a00:2::279
 6     51ms      0/ 100 = 0%      0/ 100 = 0%      | 2404:a800::92
 7     56ms      0/ 100 = 0%      0/ 100 = 0%      | 2001:4860:1:1::674
 8     ---     100/ 100 =100%   100/ 100 =100%   | 2404:6800:8202:240::1
Trace complete.
```

Network Interface and Connections

Execute netstat -an and netstat -b

1. netstat -an

- **Purpose:** Displays all active network connections and listening ports in numerical form.
- **What It Shows:**
 - Active TCP and UDP connections
 - Local and foreign IP addresses
 - Port numbers
 - Connection states (e.g., LISTENING, ESTABLISHED)

```
C:\Users\sayuj>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1521	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1536	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1538	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1546	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1566	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1568	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5432	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:30518	0.0.0.0:0	LISTENING
TCP	0.0.0.0:44801	0.0.0.0:0	LISTENING
TCP	0.0.0.0:57621	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1558	127.0.0.1:1559	ESTABLISHED

2. netstat -b

- **Purpose:** Shows which executables (programs) are using which network connections/ports.
- **What It Shows:**
 - Similar to netstat -an, but with executable names for each connection.
 - Useful for identifying which applications are using the network.


```
C:\Windows\System32>netstat -b
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1562	Sayujya:1563	ESTABLISHED
[WUDFHost.exe]			
TCP	127.0.0.1:1563	Sayujya:1562	ESTABLISHED
[WUDFHost.exe]			
TCP	127.0.0.1:1569	Sayujya:1570	ESTABLISHED
[WUDFHost.exe]			
TCP	127.0.0.1:1570	Sayujya:1569	ESTABLISHED
[WUDFHost.exe]			
TCP	127.0.0.1:1576	Sayujya:1577	ESTABLISHED
[NVDIplay.Container.exe]			
TCP	127.0.0.1:1577	Sayujya:1576	ESTABLISHED
[NVDIplay.Container.exe]			
TCP	127.0.0.1:1608	Sayujya:1609	ESTABLISHED
[ipfsvc.exe]			
TCP	127.0.0.1:1609	Sayujya:1608	ESTABLISHED
[ipfsvc.exe]			
TCP	127.0.0.1:1640	Sayujya:40572	ESTABLISHED
[NVIDIA Web Helper.exe]			
TCP	127.0.0.1:40532	Sayujya:65001	ESTABLISHED
[nvcontainer.exe]			
TCP	127.0.0.1:40572	Sayujya:1640	ESTABLISHED
[NVIDIA Share.exe]			
TCP	127.0.0.1:61798	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61803	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61808	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61810	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61811	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61812	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61813	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61814	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61815	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61822	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61823	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61824	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61825	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61826	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61827	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:61828	Sayujya:49350	TIME_WAIT
TCP	127.0.0.1:65001	Sayujya:40532	ESTABLISHED
[nvcontainer.exe]			
TCP	192.168.101.4:44801	atadevice20:3a:eb:db:99:1c:56390	ESTABLISHED

Run netstat -e.

- **Purpose:** Displays Ethernet statistics, including:Bytes sent/received, Unicast/multicast packets, Error counts
- **What It Shows:**
 - Total network traffic since the last boot
 - Useful for performance monitoring or detecting abnormal activity

```
C:\Users\sayuj>netstat -e
Interface Statistics
```

	Received	Sent
Bytes	1826803403	1360330361
Unicast packets	33510101	32663426
Non-unicast packets	157725	48665
Discards	0	0
Errors	0	0
Unknown protocols	0	

Use route print.

- **Purpose:** Displays the current routing table of the system, showing how network traffic is routed.

```
C:\Users\sayuj>route print
=====
Interface List
18...40 c2 ba 14 20 c3 .....Killer E2600 Gigabit Ethernet Controller
6...0a 00 27 00 00 06 .....VirtualBox Host-Only Ethernet Adapter
3...a4 f9 33 a5 da 1c .....Microsoft Wi-Fi Direct Virtual Adapter
15...a6 f9 33 a5 da 1b .....Microsoft Wi-Fi Direct Virtual Adapter #2
12...5a 6f ed 84 db ef .....Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.8      35
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
169.254.0.0                255.255.0.0      On-link          169.254.214.206  281
169.254.214.206            255.255.255.255  On-link          169.254.214.206  281
169.254.255.255            255.255.255.255  On-link          169.254.214.206  281
192.168.1.0                255.255.255.0    On-link          192.168.1.8      291
192.168.1.8                255.255.255.255  On-link          192.168.1.8      291
192.168.1.255              255.255.255.255  On-link          192.168.1.8      291
192.168.56.0               255.255.255.0    On-link          192.168.56.1     281
192.168.56.1               255.255.255.255  On-link          192.168.56.1     281
192.168.56.255             255.255.255.255  On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link          169.254.214.206  281
224.0.0.0                  240.0.0.0        On-link          192.168.1.8      291
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.56.1     281
255.255.255.255            255.255.255.255  On-link          169.254.214.206  281
255.255.255.255            255.255.255.255  On-link          192.168.1.8      291
=====
Persistent Routes:
None
```

Wireless Network and Firewall

Run netsh wlan show profiles.

- **Purpose:** This command lists all the Wi-Fi profiles saved on your system. It's useful for:
 - Identifying previously connected networks
 - Managing or deleting old/unused Wi-Fi profiles
 - Troubleshooting wireless connection issues

```
C:\Users\sayuj>netsh wlan show profiles
Profiles on interface Wi-Fi:
Group policy profiles (read only)
-----
<None>
User profiles
-----
All User Profile       : AyjuYaas
All User Profile       : UI
All User Profile       : The5GTwo
All User Profile       : mellowgarden_5
All User Profile       : burgerhouse44_2.4
All User Profile       : Juju cafe5G@ClassicTech
All User Profile       : juju cafe4@ClassicTech
All User Profile       : Meroma_restro
All User Profile       : St. Xavier
All User Profile       : ROJA-SHRESTHA05 6820
All User Profile       : Ojha Cyber
All User Profile       : 12345
All User Profile       : LCR
All User Profile       : Sultan
All User Profile       : SAYU
All User Profile       : Aq_5G
All User Profile       : H196A_A51C
All User Profile       : TP-LINK
All User Profile       : sherap@vianet_5G
All User Profile       : AdvancedCollege
All User Profile       : 1
```

Execute netsh wlan show profile [profile name]

- **Purpose:** This command retrieves details about a specific Wi-Fi profile. It helps with:
 - Checking the security type and settings

- Retrieving the saved Wi-Fi password (when using the key=clear flag)

```
C:\Users\sayuj>netsh wlan show profile name="St. Xavier"

Profile St. Xavier on interface Wi-Fi:
=====

Applied: All User Profile

Profile information
-----
    Version                : 1
    Type                   : Wireless LAN
    Name                   : St. Xavier
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
-----
    Number of SSIDs        : 1
    SSID name              : "St. Xavier"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension       : Not present

Security settings
-----
    Authentication         : Open
    Cipher                 : None
    Security key           : Absent
    Key Index              : 1

Cost settings
-----
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default
```

Use netsh advfirewall show allprofiles.

- **Purpose:** This command displays firewall settings for all network profiles (Domain, Private, and Public). It's useful for:
 - Verifying firewall status
 - Checking inbound/outbound rules
 - Ensuring your system is protected on all networks

Use netsh advfirewall show allprofiles.

- **Purpose:** This command displays firewall settings for all network profiles (Domain, Private, and Public). It's useful for:
 - Verifying firewall status
 - Checking inbound/outbound rules
 - Ensuring your system is protected on all networks

```
C:\Users\sayuj>netsh advfirewall show allprofiles
```

Domain Profile Settings:

```
-----  
State                                ON  
Firewall Policy                     BlockInbound,AllowOutbound  
LocalFirewallRules                  N/A (GPO-store only)  
LocalConSecRules                    N/A (GPO-store only)  
InboundUserNotification             Enable  
RemoteManagement                   Disable  
UnicastResponseToMulticast          Enable  
  
Logging:  
LogAllowedConnections               Disable  
LogDroppedConnections               Disable  
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewa  
log  
MaxFileSize                          4096
```

Private Profile Settings:

```
-----  
State                                ON  
Firewall Policy                     BlockInbound,AllowOutbound  
LocalFirewallRules                  N/A (GPO-store only)  
LocalConSecRules                    N/A (GPO-store only)  
InboundUserNotification             Enable  
RemoteManagement                   Disable  
UnicastResponseToMulticast          Enable  
  
Logging:  
LogAllowedConnections               Disable  
LogDroppedConnections               Disable  
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewa  
log  
MaxFileSize                          4096
```

Public Profile Settings:

```
-----  
State                                ON  
Firewall Policy                     BlockInbound,AllowOutbound  
LocalFirewallRules                  N/A (GPO-store only)  
LocalConSecRules                    N/A (GPO-store only)  
InboundUserNotification             Enable  
RemoteManagement                   Disable  
UnicastResponseToMulticast          Enable  
  
Logging:  
LogAllowedConnections               Disable  
LogDroppedConnections               Disable  
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewa
```