

# Certificate

This is to certify that the practical report entitled

**“Practical File for M.Sc. Cyber Security”**

is submitted by

**Name: Dhrumil Soni**  
**Enrollment No: IU2554520008**  
**Class: M.Sc. Cyber Security**

under the guidance of  
**Prof. Varsha Patel**

**Academic Year: 2025–2026**

# TABLE OF CONTENTS

Practical No. 2 . . . . . 1

## Practical No. 2

Date: 14/Jul/2025

# Basic Commands For Powershell

## 1. Command: cd

**Description:** Changes the current directory.

### Screenshot

```
C:\Users\cyber-2>cd Downloads
C:\Users\cyber-2\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 7C89-8193

Directory of C:\Users\cyber-2\Downloads

11-07-2025  15:19          <DIR>          .
11-07-2025  15:06          <DIR>          ..
08-07-2025  14:44    1,474,385,344 android-studio-2025.1.1.13-windows.exe
11-07-2025  15:19      11,031,936 ChromeSetup.exe
11-07-2025  15:20         602 debug.log
03-07-2025  14:08    4,478,939,136 kali-linux-2025.2-installer-amd64.iso
09-07-2025  11:09    3,536,624,451 kali-linux-2025.2-vmware-amd64.7z
11-07-2025  12:12      429,579 Mahir Patel - Lab Manual (1).docx
11-07-2025  12:12      429,579 Mahir Patel - Lab Manual (2).docx
11-07-2025  12:12      429,579 Mahir Patel - Lab Manual.docx
               8 File(s)  9,502,270,206 bytes
               2 Dir(s)  23,642,808,320 bytes free

C:\Users\cyber-2\Downloads>
```

Figure 1: Output of cd command

## 2. Command: dir

**Description:** Lists the contents of a directory.

## Screenshot

```
C:\Users\cyber-2>dir
Volume in drive C has no label.
Volume Serial Number is 7CB9-8193

Directory of C:\Users\cyber-2

11-07-2025  15:06    <DIR>        .
08-07-2025  14:45    <DIR>        ..
08-07-2025  14:47    <DIR>        .android
03-07-2025  11:13    <DIR>        Contacts
11-07-2025  15:20    <DIR>        Desktop
03-07-2025  14:11    <DIR>        Documents
11-07-2025  15:19    <DIR>        Downloads
03-07-2025  11:13    <DIR>        Favorites
03-07-2025  11:13    <DIR>        Links
03-07-2025  11:13    <DIR>        Music
03-07-2025  11:14    <DIR>        OneDrive
07-07-2025  12:28    <DIR>        Pictures
03-07-2025  11:13    <DIR>        Saved Games
03-07-2025  11:13    <DIR>        Searches
11-07-2025  11:12    <DIR>        Videos
               0 File(s)              0 bytes
               15 Dir(s)  23,651,864,576 bytes free

C:\Users\cyber-2>
```

Figure 2: Output of dir command

## 3. Command: mkdir

**Description:** Creates a new directory.

## Screenshot

```
C:\Users\cyber-2\Downloads>mkdir Dhruvil

C:\Users\cyber-2\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 7CB9-8193

Directory of C:\Users\cyber-2\Downloads

14-07-2025  11:32    <DIR>        .
11-07-2025  15:06    <DIR>        ..
08-07-2025  14:44    1,470,385,344 android-studio-2025.1.1.13-windows.exe
11-07-2025  15:19    11,031,936 ChromeSetup.exe
11-07-2025  15:20    602 debug.log
14-07-2025  11:32    <DIR>        Dhruvil
03-07-2025  14:08    4,478,939,136 kali-linux-2025.2-installer-amd64.iso
09-07-2025  11:09    3,536,624,451 kali-linux-2025.2-vmware-amd64.7z
11-07-2025  12:12    429,579 Mahir Patel - Lab Manual (1).docx
11-07-2025  12:19    429,579 Mahir Patel - Lab Manual (2).docx
11-07-2025  12:12    429,579 Mahir Patel - Lab Manual.docx
               8 File(s)    9,502,270,286 bytes
               3 Dir(s)  23,642,312,704 bytes free

C:\Users\cyber-2\Downloads>
```

Figure 3: Output of mkdir command

## 4. Command: rmdir

**Description:** Deletes a directory (folder).

## Screenshot

```
PS C:\Users\cyber-2\Downloads> rmdir .\Demo\  
PS C:\Users\cyber-2\Downloads> dir  
  
Directory: C:\Users\cyber-2\Downloads  
  
Mode                LastWriteTime         Length Name  
----                -  
d-----          14-07-2025      11:43             Dhrumil  
-a-----          08-07-2025      14:44 1474385344 android-studio-2025.1.1.13-windows.exe  
-a-----          11-07-2025      15:19 11031936 ChromeSetup.exe  
-a-----          11-07-2025      15:28      602 debug.log  
-a-----          03-07-2025      14:08 4478939136 kali-linux-2025.2-installer-amd64.iso  
-a-----          09-07-2025      11:09 3536624451 kali-linux-2025.2-vmware-amd64.7z  
-a-----          11-07-2025      12:12 429579 Mahir Patel - Lab Manual (1).docx  
-a-----          11-07-2025      12:19 429579 Mahir Patel - Lab Manual (2).docx  
-a-----          11-07-2025      12:12 429579 Mahir Patel - Lab Manual.docx  
  
PS C:\Users\cyber-2\Downloads> |
```

Figure 4: Output of rmdir command

## 5. Command: copy

**Description:** Copies files from one location to another.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhrumil> copy .\xyz.txt abc.txt  
PS C:\Users\cyber-2\Downloads\Dhrumil> dir  
  
Directory: C:\Users\cyber-2\Downloads\Dhrumil  
  
Mode                LastWriteTime         Length Name  
----                -  
-a-----          14-07-2025      11:42           0 abc.txt  
-a-----          14-07-2025      11:42           0 xyz.txt  
  
PS C:\Users\cyber-2\Downloads\Dhrumil> |
```

Figure 5: Output of copy command

## 6. Command: rename

**Description:** Renames a file or directory.

## Screenshot

```
C:\Users\cyber-2\Downloads\Dhrumil>ren xyz.txt abc.txt

C:\Users\cyber-2\Downloads\Dhrumil>dir
Volume in drive C has no label.
Volume Serial Number is 7C89-8193

Directory of C:\Users\cyber-2\Downloads\Dhrumil

14-07-2025  11:39    <DIR>          .
14-07-2025  11:32    <DIR>          ..
14-07-2025  11:33                0 abc.txt
               1 File(s)                0 bytes
               2 Dir(s)  23,648,243,712 bytes free

C:\Users\cyber-2\Downloads\Dhrumil>
```

Figure 6: Output of rename command

## 7. Command: del

**Description:** Deletes one or more files.

## Screenshot

```
C:\Users\cyber-2\Downloads\Dhrumil>del abc.txt

C:\Users\cyber-2\Downloads\Dhrumil>dir
Volume in drive C has no label.
Volume Serial Number is 7C89-8193

Directory of C:\Users\cyber-2\Downloads\Dhrumil

14-07-2025  11:40    <DIR>          .
14-07-2025  11:32    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  23,644,577,792 bytes free

C:\Users\cyber-2\Downloads\Dhrumil>
```

Figure 7: Output of del command

## 8. Command: help

**Description:** Displays help information about available commands.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Ohrumil> help kill

NAME
    Stop-Process

SYNTAX
    Stop-Process [-Id] <int[]> [-PassThru] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]
    Stop-Process -Name <string[]> [-PassThru] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]
    Stop-Process [-InputObject] <Process[]> [-PassThru] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]

ALIASES
    stop
    kill

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
    -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
    -- To view the Help topic for this cmdlet online, type: "Get-Help Stop-Process -Online" or
       go to https://go.microsoft.com/fwlink/?LinkID=113012.

PS C:\Users\cyber-2\Downloads\Ohrumil> |
```

Figure 8: Output of help command

## 9. Command: calc

**Description:** Opens the Windows calculator application.

## Screenshot

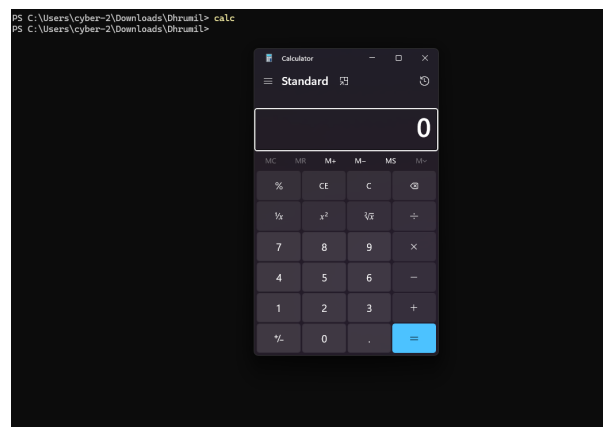


Figure 9: Output of calc command

## 10. Command: whoami

**Description:** Displays the current user and domain.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> whoami
drona2\cyber-2
PS C:\Users\cyber-2\Downloads\Dhruvil> |
```

Figure 10: Output of whoami command

# Advanced PowerShell Commands

## 11. Command: arp

**Description:** Displays the ARP cache, which maps IP addresses to MAC addresses.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> arp -a

Interface: 192.168.133.1 --- 0x2
Internet Address      Physical Address      Type
-----
192.168.133.254       00-50-56-e6-2a-62     dynamic
192.168.133.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.10.15.12 --- 0x9
Internet Address      Physical Address      Type
-----
10.10.15.1            3c-fa-38-88-8e-10     dynamic
10.10.15.6            c8-1f-d6-49-29-84     dynamic
10.10.15.16           00-60-e8-9c-d7-37     dynamic
10.10.15.17           00-60-e8-9c-e5-d5     dynamic
10.10.15.19           00-60-e8-9c-de-25     dynamic
10.10.15.62           7c-57-58-d9-6e-0b     dynamic
10.10.15.65           e0-73-e7-b9-f4-97     dynamic
10.10.15.70           e0-73-e7-b7-aa-9f     dynamic
10.10.15.255          ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.118.1 --- 0x10
Internet Address      Physical Address      Type
-----
192.168.118.254       00-50-56-e4-05-ce     dynamic
192.168.118.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

PS C:\Users\cyber-2\Downloads\Dhruvil> |
```

Figure 11: Output of arp command

## 12. Command: gpresult

**Description:** Displays the Resultant Set of Policy (RSOP) information.



## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> gpresult /r
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.9
© Microsoft Corporation. All rights reserved.
Created on 18-07-2025 at 12:18:51

GPO data for DROMA2\Cyber-2 on DROMA_2_D_002 : Logging Mode

OS Configuration: Member Workstation
OS Version: 10.0.22H31
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\cyber-2
Connected over a slow link?: No

COMPUTER SETTINGS
-----
C:\DROMA_2_D_002\Computer\DC=DROMA2,DC=CYBER,DC=COM
Last time Group Policy was applied: 18-07-2025 at 12:16:31
Group Policy was applied from: DROMA2\CYBER.DROMA2.CYBER.COM
Group Policy slow link threshold: 500 kbps
Domain Name: DROMA2
Domain Type: Windows 2008 or later

Applied Group Policy Objects
-----
N/A

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups
-----
BUILTIN\Administrators
Everyone
BUILTIN\Users
```

Figure 12: Output of gpresult command

## 13. Command: gpupdate

**Description:** Applies new Group Policy settings.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\cyber-2\Downloads\Dhruvil> |
```

Figure 13: Output of gpupdate command

## 14. Command: getmac

**Description:** Displays the MAC address of the system's network interfaces.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Ohrumil> getmac

Physical Address      Transport Name
-----
00-68-EB-9C-EE-93    \Device\NPF{77067346-CF61-4029-A318-CD7818E19328}
00-50-56-C9-00-01    \Device\NPF{863A728C-1434-444A-B597-2C2817E33312}
00-50-56-C9-00-08    \Device\NPF{E4C5E2DF-9E2E-4711-872B-A2280F4A6C50}
PS C:\Users\cyber-2\Downloads\Ohrumil> |
```

Figure 14: Output of getmac command

## 15. Command: ipconfig

**Description:** Displays all current TCP/IP network configuration values.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Ohrumil> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8628:4f05:f27c:c50a%9
    IPv4 Address. . . . . : 10.10.15.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.15.1

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8ecf:ffad:1ad9:d03a%2
    IPv4 Address. . . . . : 192.168.133.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::379b:b8f4:ad5c:f910%16
    IPv4 Address. . . . . : 192.168.118.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
PS C:\Users\cyber-2\Downloads\Ohrumil> |
```

Figure 15: Output of ipconfig command

## 16. Command: net

**Description:** Used to manage network resources like shares and users.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> net user
User accounts for \\DRODA_2_D_002
-----
Administrator      DefaultAccount      Guest
TI_infra            WDAGUtilityAccount
The command completed successfully.
PS C:\Users\cyber-2\Downloads\Dhruvil> |
```

Figure 16: Output of net command

## 17. Command: netstat

**Description:** Displays active network connections and listening ports.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> netstat
Active Connections
Proto Local Address          Foreign Address         State
TCP    10.10.15.12:55293      4.213.25.240:https      ESTABLISHED
TCP    10.10.15.12:55538      ec2-3-108-140-32:https  ESTABLISHED
TCP    10.10.15.12:55633      sd-in-f188:https       ESTABLISHED
TCP    10.10.15.12:55777      a23-1-241-97:https     ESTABLISHED
TCP    10.10.15.12:55842      211:https              ESTABLISHED
TCP    10.10.15.12:55863      218:https              ESTABLISHED
TCP    10.10.15.12:55911      90:https               TIME_WAIT
TCP    10.10.15.12:56041      1:https                ESTABLISHED
TCP    10.10.15.12:56079      173:https              TIME_WAIT
TCP    10.10.15.12:56085      a23-1-241-107:https    CLOSE_WAIT
TCP    10.10.15.12:56089      1:https                TIME_WAIT
TCP    10.10.15.12:56094      a23-1-241-96:https     CLOSE_WAIT
TCP    10.10.15.12:56102      40.104.66.130:https    ESTABLISHED
TCP    10.10.15.12:56109      40.104.66.162:https    ESTABLISHED
TCP    10.10.15.12:56110      40.104.66.162:https    ESTABLISHED
TCP    10.10.15.12:56121      151.101.66.132:https   ESTABLISHED
TCP    10.10.15.12:56123      66:https               ESTABLISHED
TCP    10.10.15.12:56144      13.107.246.254:https   CLOSE_WAIT
TCP    10.10.15.12:56163      69:https               ESTABLISHED
TCP    10.10.15.12:56170      a23-217-111-90:https   CLOSE_WAIT
TCP    10.10.15.12:56172      40.99.31.162:https     ESTABLISHED
PS C:\Users\cyber-2\Downloads\Dhruvil> |
```

Figure 17: Output of netstat command

## 18. Command: pathping

**Description:** Combines ping and tracertr to find network issues.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\DhruMil> pathping geeksforgeeks.org
Tracing route to geeksforgeeks.org [34.218.62.116]
over a maximum of 30 hops:
 0  DROMA_2_D_002.DROMA2.CYBER.COM [10.10.15.12]
 1  10.10.15.1
 2  47.247.92.185
 3  47.247.146.25
 4  * * *
Computing statistics for 75 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0      Lost/Sent = Pct  Lost/Sent = Pct  Address
 0      0/ 100 = 0%      0/ 100 = 0%      DROMA_2_D_002.DROMA2.CYBER.COM [10.10.15.12]
 1      1ms          0/ 100 = 0%      0/ 100 = 0%      10.10.15.1
 2      1ms          0/ 100 = 0%      0/ 100 = 0%      47.247.92.185
 3      1ms          0/ 100 = 0%      0/ 100 = 0%      47.247.146.25
Trace complete.
PS C:\Users\cyber-2\Downloads\DhruMil> |
```

Figure 18: Output of pathping command

## 19. Command: ping

**Description:** Sends ICMP echo requests to test network connectivity.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\DhruMil> ping google.com

Pinging google.com [142.250.67.238] with 32 bytes of data:
Reply from 142.250.67.238: bytes=32 time=10ms TTL=118
Reply from 142.250.67.238: bytes=32 time=10ms TTL=118
Reply from 142.250.67.238: bytes=32 time=10ms TTL=118
Reply from 142.250.67.238: bytes=32 time=10ms TTL=118

Ping statistics for 142.250.67.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms
PS C:\Users\cyber-2\Downloads\DhruMil> |
```

Figure 19: Output of ping command

## 20. Command: route print

**Description:** Displays the routing table on the system.

## Screenshot

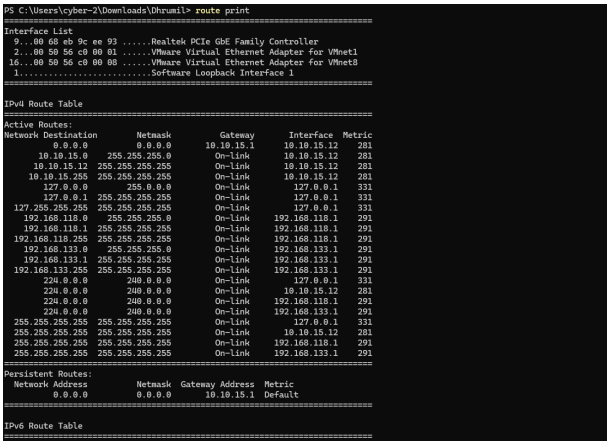


Figure 20: Output of route print command

## 21. Command: systeminfo

**Description:** Provides detailed configuration info about the system.

## Screenshot

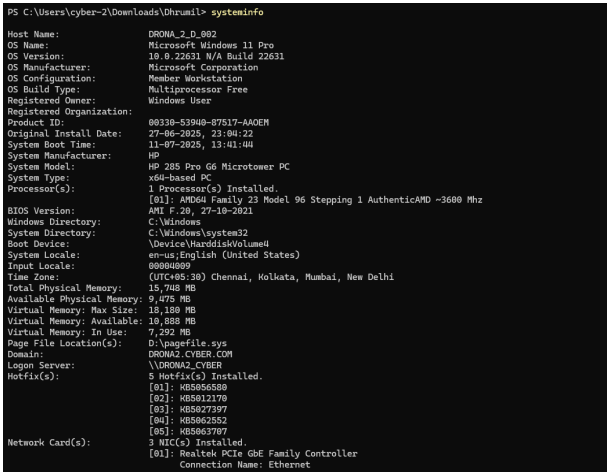


Figure 21: Output of systeminfo command

## 22. Command: tasklist

**Description:** Displays a list of currently running processes.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	7,764 K
Secure System	172	Services	0	47,844 K
Registry	212	Services	0	28,976 K
smss.exe	704	Services	0	1,292 K
csrss.exe	960	Services	0	5,772 K
wininit.exe	732	Services	0	7,512 K
services.exe	1148	Services	0	18,884 K
lsass.exe	1284	Services	0	4,336 K
lsass.exe	1212	Services	0	38,972 K
svchost.exe	1340	Services	0	31,076 K
fontdrvhost.exe	1396	Services	0	4,368 K
svchost.exe	1488	Services	0	16,392 K
svchost.exe	1532	Services	0	11,392 K
svchost.exe	1644	Services	0	5,508 K
svchost.exe	1648	Services	0	43,896 K
svchost.exe	1772	Services	0	7,956 K
svchost.exe	1788	Services	0	9,184 K
svchost.exe	1788	Services	0	18,576 K
svchost.exe	1796	Services	0	9,764 K
svchost.exe	1812	Services	0	7,748 K
svchost.exe	1922	Services	0	9,768 K
svchost.exe	1988	Services	0	18,344 K
svchost.exe	1988	Services	0	6,088 K
svchost.exe	1744	Services	0	19,688 K
svchost.exe	2152	Services	0	20,328 K
svchost.exe	2396	Services	0	17,276 K
svchost.exe	2552	Services	0	11,624 K
svchost.exe	2672	Services	0	5,836 K
svchost.exe	2684	Services	0	21,716 K
amd64msrpc.exe	2692	Services	0	7,984 K
alg.exe	2704	Services	0	7,268 K
svchost.exe	2796	Services	0	12,540 K
svchost.exe	2888	Services	0	11,376 K
svchost.exe	3008	Services	0	6,768 K

Figure 22: Output of tasklist command

## 23. Command: tracert

**Description:** Traces the route packets take to a destination.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhruvil> tracert geeksforgeeks.org
Tracing route to geeksforgeeks.org [34.218.62.116]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  10.10.15.1
  1  1 ms  1 ms  1 ms  47.247.92.185
  2  1 ms  1 ms  1 ms  47.247.146.25
  3  *  *  *  Request timed out.
  4  *  *  *  Request timed out.
  5  34 ms  34 ms  34 ms  172.16.5.85
  6  33 ms  33 ms  95 ms  172.16.5.85
  7  35 ms  34 ms  35 ms  103.198.140.170
  8  251 ms  251 ms  251 ms  49.45.4.85
  9  251 ms  251 ms  251 ms  49.45.4.85
 10  *  *  *  Request timed out.
 11  *  *  *  Request timed out.
 12  *  *  *  Request timed out.
PS C:\Users\cyber-2\Downloads\Dhruvil> |
```

Figure 23: Output of tracert command

## 24. Command: powercfg

**Description:** Manages the power settings and configurations on a system.

## Screenshot

```
PS C:\Users\cyber-2\Downloads\Dhrumil> powercfg /list

Existing Power Schemes (* Active)

Power Scheme GUID: 381b4222-f694-41f0-9685-ff5bb260df2e (Balanced) *
Power Scheme GUID: 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c (High performance)
Power Scheme GUID: a1841388-3541-4fab-bc81-f71556f20b4a (Power saver)
PS C:\Users\cyber-2\Downloads\Dhrumil>
```

Figure 24: Output of powercfg command

## 25. Command: regedit

**Description:** Opens the Windows Registry Editor.

## Screenshot

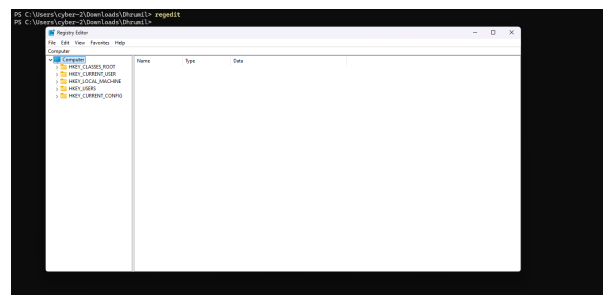


Figure 25: Output of regedit command

## Conclusion

This practical helped us understand and use both basic and advanced PowerShell commands. Basic commands allowed file and folder management, while advanced commands provided tools for system and network monitoring. Overall, it improved our skills in handling administrative tasks using PowerShell.