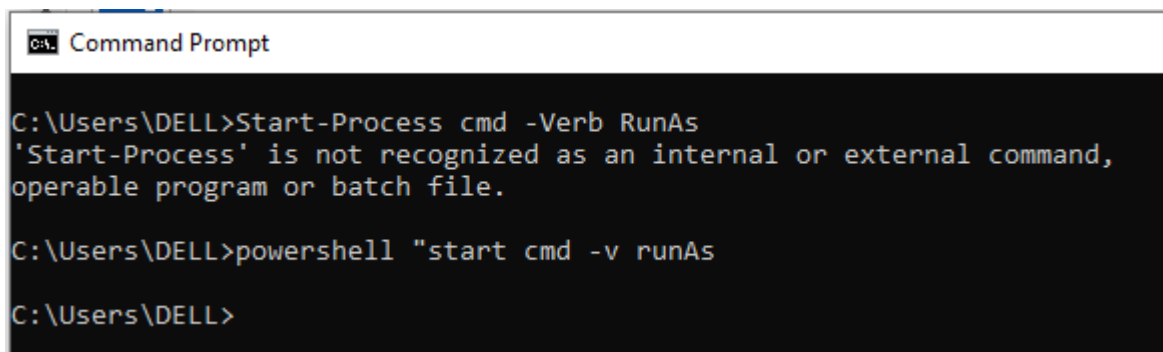


Command-line hacking

on a

Windows operating system

->powershell start cmd -v runAs – Run the Command Prompt as an Administrator:



```
CA: Command Prompt

C:\Users\DELL>Start-Process cmd -Verb RunAs
'Start-Process' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\DELL>powershell "start cmd -v runAs

C:\Users\DELL>
```

Entering this command opens another command prompt window as an administrator:

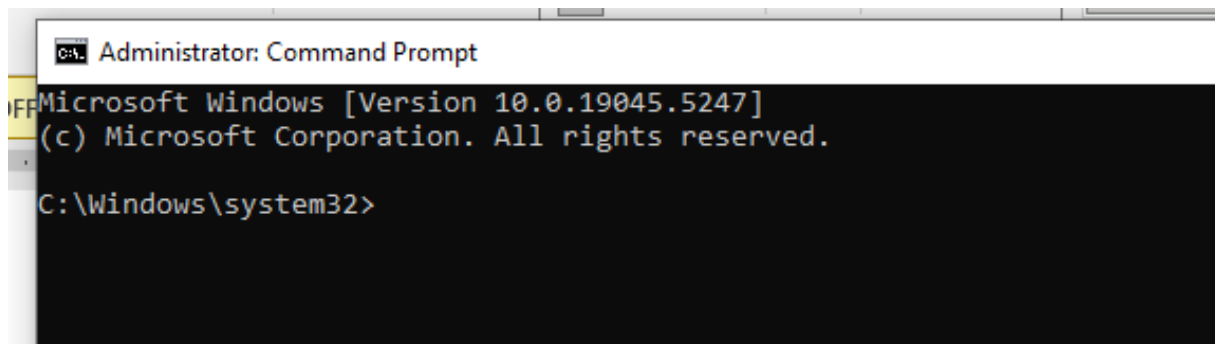
[1] title: The title command in Windows Command Prompt is used to set a custom title for the command prompt window. This can be helpful when you have multiple command prompt windows open and want to differentiate between them.

Original window title:

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

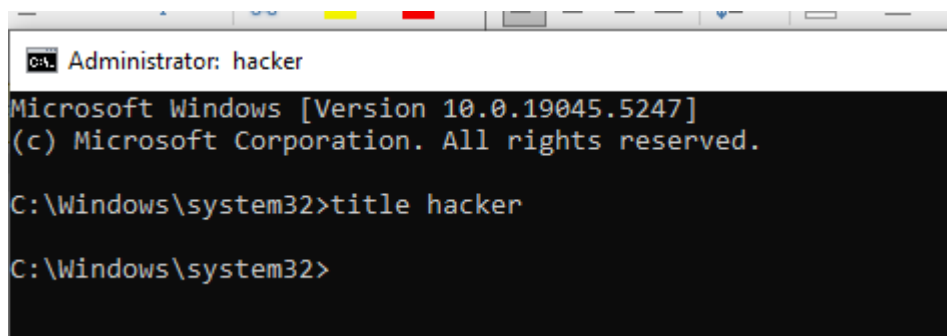
Topic :- Command-line hacking on a Windows operating system



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

After executing title command:



```
Administrator: hacker
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

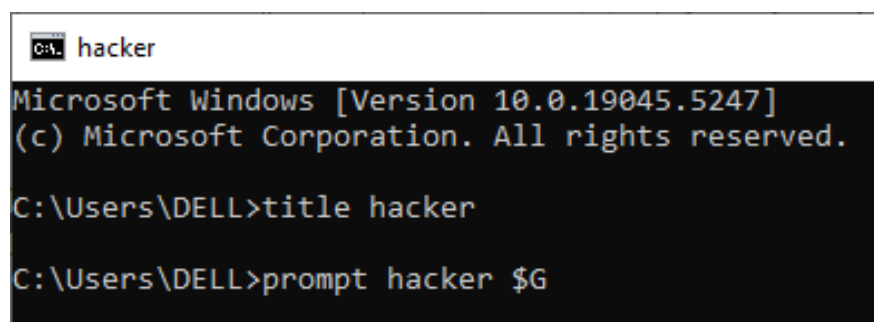
C:\Windows\system32>title hacker

C:\Windows\system32>
```

[2] prompt: The prompt command in Windows Command Prompt is used to customize the appearance of the command prompt text displayed before the cursor. This is useful for personalization or to provide more information in the command prompt interface.

Common Special Codes:

- `$P` : Current drive and path.
- `$G` : Greater-than sign (>).
- `$L` : Less-than sign (<).
- `$N` : Current drive.
- `$D` : Current date.
- `$T` : Current time.
- `$V` : Windows version number.
- `$H` : Backspace (erases previous character).
- `$E` : Escape character (ASCII 27).
- `$` : Dollar sign (\$).
- `$_` : Carriage return and line feed (new line).



```
C:\ hacker
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

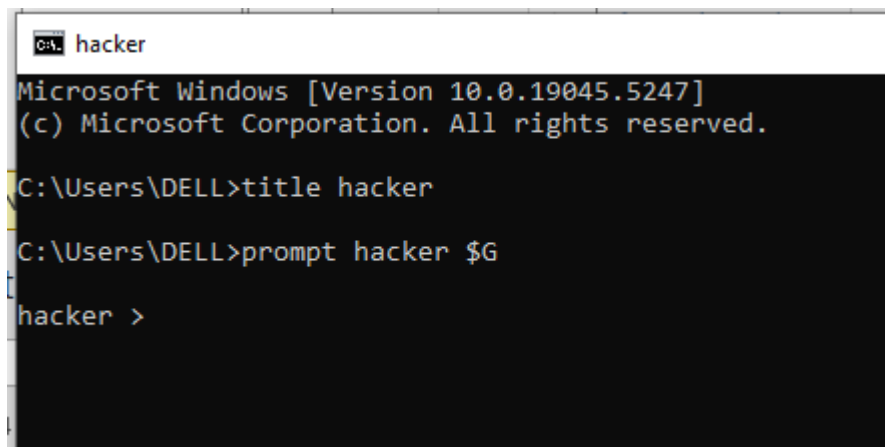
C:\Users\DELL>title hacker
C:\Users\DELL>prompt hacker $G
```

After executing command prompt will be change

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system



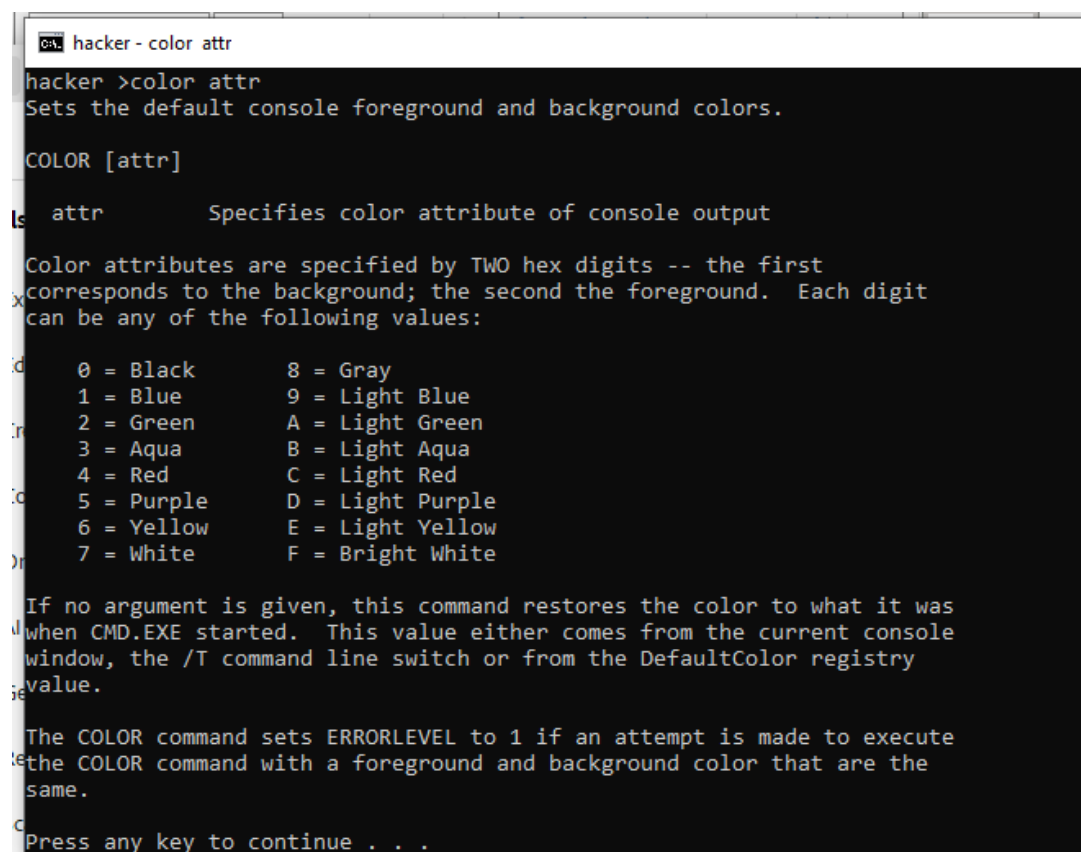
```
C:\> hacker
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>title hacker

C:\Users\DELL>prompt hacker $G

hacker >
```

[3]color: The color command in Windows Command Prompt is used to change the background and text colors of the Command Prompt window. This can be useful for improving readability or personalizing your terminal.



```
hacker - color attr
hacker >color attr
Sets the default console foreground and background colors.

COLOR [attr]

attr          Specifies color attribute of console output

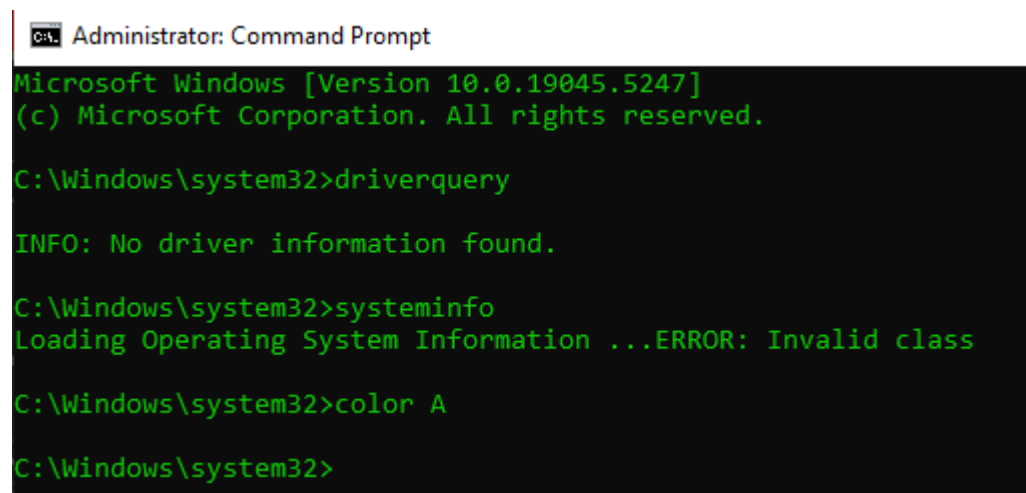
Color attributes are specified by TWO hex digits -- the first
corresponds to the background; the second the foreground. Each digit
can be any of the following values:

    0 = Black      8 = Gray
    1 = Blue       9 = Light Blue
    2 = Green      A = Light Green
    3 = Aqua       B = Light Aqua
    4 = Red        C = Light Red
    5 = Purple     D = Light Purple
    6 = Yellow     E = Light Yellow
    7 = White      F = Bright White

If no argument is given, this command restores the color to what it was
when CMD.EXE started. This value either comes from the current console
window, the /T command line switch or from the DefaultColor registry
value.

The COLOR command sets ERRORLEVEL to 1 if an attempt is made to execute
the COLOR command with a foreground and background color that are the
same.

Press any key to continue . . .
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>driverquery

INFO: No driver information found.

C:\Windows\system32>systeminfo
Loading Operating System Information ...ERROR: Invalid class

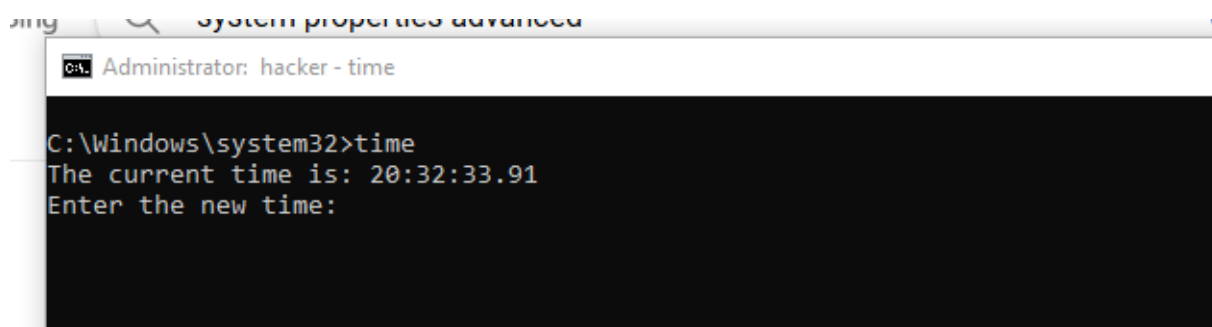
C:\Windows\system32>color A

C:\Windows\system32>
```

[4] cls: The cls command in Windows Command Prompt is used to **clear the screen** by removing all previously executed commands and their output from the current Command Prompt window. It does not close the Command Prompt or affect the current working directory or session state.

```
C:\Users\DELL\Desktop>cls
```

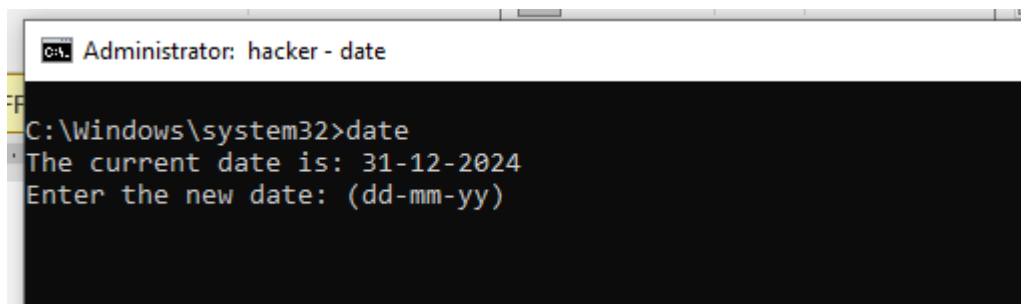
[5] time: The time command in Windows Command Prompt is used to **display or set the system time**. This command allows you to view the current system time or update it manually.



The screenshot shows a Windows window titled "System properties advanced" with a search bar. Overlaid on this is a command prompt window titled "Administrator: hacker - time". The command prompt shows the following text:

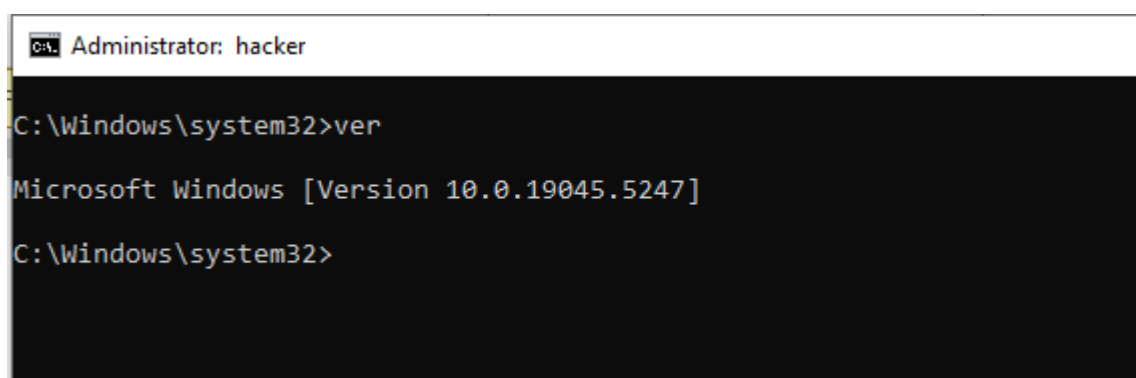
```
C:\Windows\system32>time  
The current time is: 20:32:33.91  
Enter the new time:
```

[6] **date**: The date command in Windows Command Prompt is used to **display or set the system date**. This allows you to view the current system date or change it manually.

A screenshot of a Windows Command Prompt window titled "Administrator: hacker - date". The prompt shows the command "C:\Windows\system32>date" being entered. The output displays "The current date is: 31-12-2024" followed by a prompt "Enter the new date: (dd-mm-yy)".

```
Administrator: hacker - date
C:\Windows\system32>date
The current date is: 31-12-2024
Enter the new date: (dd-mm-yy)
```

[7] **ver**: The ver command in Windows Command Prompt is used to **display the operating system version**. It's a simple command to check the version of Windows currently running on your system.

A screenshot of a Windows Command Prompt window titled "Administrator: hacker". The prompt shows the command "C:\Windows\system32>ver" being entered. The output displays "Microsoft Windows [Version 10.0.19045.5247]" followed by the prompt "C:\Windows\system32>".

```
Administrator: hacker
C:\Windows\system32>ver
Microsoft Windows [Version 10.0.19045.5247]
C:\Windows\system32>
```

[8] chdir or cd – Changes the Current Working Directory to the Specified Directory:

Command Prompt

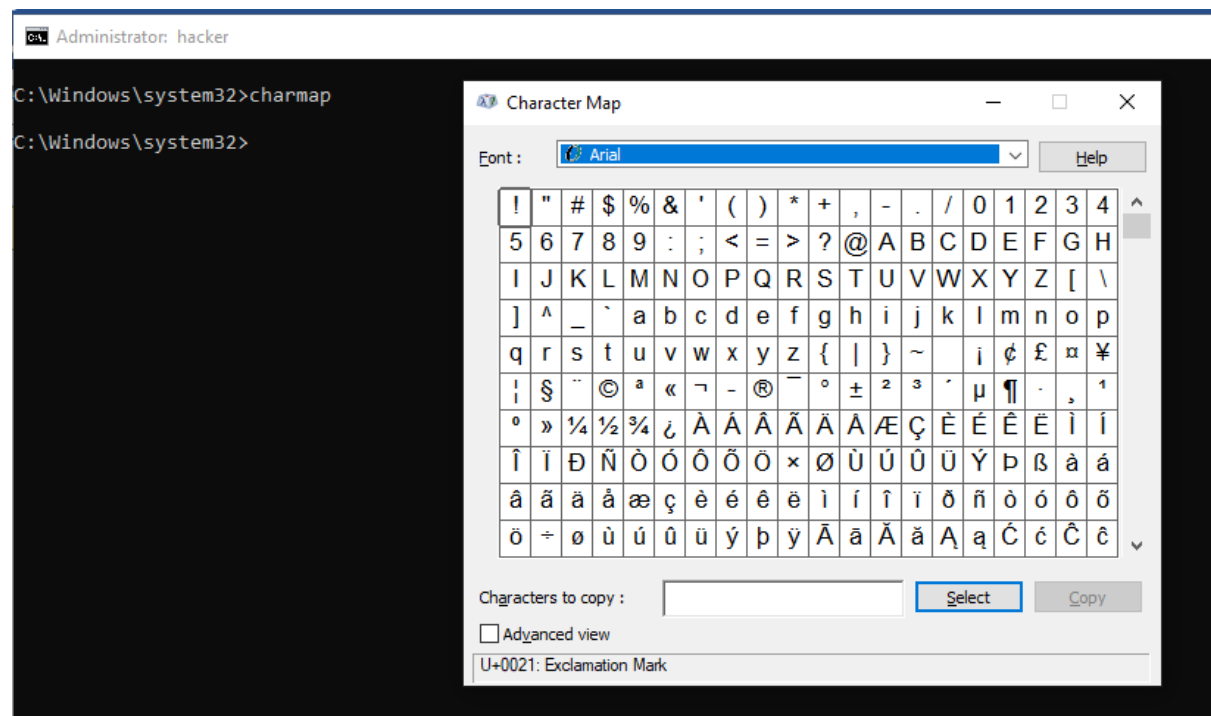
```
C:\Users\DELL>cd Desktop  
C:\Users\DELL\Desktop>cd..  
C:\Users\DELL>
```

[6] hostname: The hostname command in Windows Command Prompt is used to **display the name of the current computer** or the **hostname** of the system.

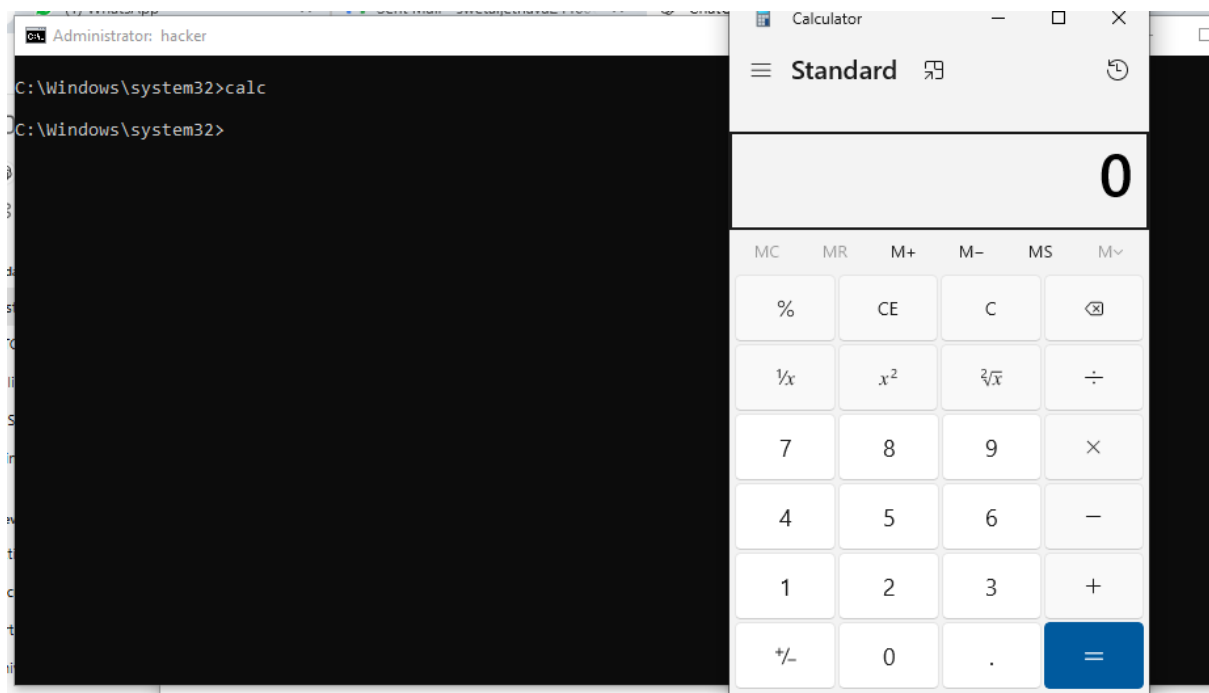
Administrator: hacker

```
C:\Windows\system32>hostname  
DESKTOP-4DDA VIC  
C:\Windows\system32>
```


[9]charmap: The charmap command in Windows is used to **open the Character Map application**, which allows you to view and select special characters, symbols, and letters that are not available on your standard keyboard.



[10]calc: The calc command in Windows is used to **open the Calculator application**. It allows you to quickly access the built-in calculator for performing basic and scientific calculations.



Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

[11] dir: The dir command in Windows Command Prompt is used to **display a list of files and directories** in the specified directory or the current directory if no directory is specified. It's useful for viewing the contents of a folder or drive.

```
Command Prompt

C:\Users\DELL>dir
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

Directory of C:\Users\DELL

01-01-2025  16:51    <DIR>          .
01-01-2025  16:51    <DIR>          ..
20-08-2023  19:48             1,376 .bash_history
17-02-2024  14:44    <DIR>          .config
20-12-2024  21:14    <DIR>          .icesoft
15-02-2023  05:02    <DIR>          .ms-ad
20-12-2024  21:10    <DIR>          .openjfx
20-12-2024  21:18      20,341 .pdfbox.cache
02-01-2025  14:58    <DIR>          .VirtualBox
29-12-2024  20:31    <DIR>          .zenmap
24-01-2024  12:29      41,588 2021abcpending.xlsx
22-03-2023  19:07    <DIR>          3D Objects
17-06-2023  22:27    <DIR>          abc
14-02-2023  07:34    <DIR>          Contacts
02-01-2025  16:58    <DIR>          Desktop
02-09-2024  13:16    <DIR>          Documents
01-01-2025  23:04    <DIR>          Downloads
14-02-2023  07:34    <DIR>          Favorites
14-02-2023  07:34    <DIR>          Links
14-02-2023  07:34    <DIR>          Music
14-02-2023  07:38    <DIR>          OneDrive
15-02-2023  10:52    <DIR>          Oracle
20-10-2024  15:59    <DIR>          Pictures
```

[12] del: The del command in Windows Command Prompt is used to **delete one or more files**. It allows you to remove files from the file system permanently

(unless the file is in the Recycle Bin or protected in some way).

```
C:\Users\DELL\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

Directory of C:\Users\DELL\Desktop

02-01-2025  19:49    <DIR>          .
02-01-2025  19:49    <DIR>          ..
25-11-2024  22:31    <DIR>          ANSHUL DATA
31-12-2024  22:20             348 ASSESSMENT-PASSWORD.txt
02-01-2025  19:49    <DIR>          cmddel
29-12-2024  16:21    <DIR>          college data
18-12-2024  08:36    <DIR>          CSF TOOLS
30-05-2014  14:22    <DIR>          DISK1
28-12-2024  09:59    <DIR>          FIP PRESENTAION-SJ
30-12-2024  19:51    <DIR>          MICRO TEACHING PPT
14-02-2023  07:34             2,348 Microsoft Edge.lnk
02-01-2025  16:57             15,281 misplace issue application.docx
04-12-2024  15:24    <DIR>          Sem -1 Templates
11-12-2024  16:40             2,388 Sweta - Chrome.lnk
13-07-2024  11:50    <DIR>          UGC
               4 File(s)                20,365 bytes
              11 Dir(s)  21,373,751,296 bytes free

C:\Users\DELL\Desktop>del cmddel
C:\Users\DELL\Desktop\cmddel\*, Are you sure (Y/N)? y
```

[13] **attrib +h +s +r folder_name – Hides a Folder**

You can hide a folder right from the command line by typing in `attrib +h +s +r folder_name` and then pressing

ENTER.

```
Directory of C:\Users\DELL\Desktop

02-01-2025  19:50    <DIR>        .
02-01-2025  19:50    <DIR>        ..
25-11-2024  22:31    <DIR>        ANSHUL DATA
31-12-2024  22:20                348 ASSESSMENT-PASSWORD.txt
02-01-2025  19:49    <DIR>        cmddel
29-12-2024  16:21    <DIR>        college data
18-12-2024  08:36    <DIR>        CSF TOOLS
30-05-2014  14:22    <DIR>        DISK1
28-12-2024  09:59    <DIR>        FIP PRESENTAION-SJ
02-01-2025  19:50    <DIR>        hidefld
30-12-2024  19:51    <DIR>        MICRO TEACHING PPT
14-02-2023  07:34                2,348 Microsoft Edge.lnk
02-01-2025  16:57                15,281 misplace issue application.docx
04-12-2024  15:24    <DIR>        Sem -1 Templates
11-12-2024  16:40                2,388 Sweta - Chrome.lnk
13-07-2024  11:50    <DIR>        UGC
               4 File(s)                20,365 bytes
               12 Dir(s)  21,369,315,328 bytes free

C:\Users\DELL\Desktop>attrib +h +s +r hidefld

C:\Users\DELL\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

Directory of C:\Users\DELL\Desktop

02-01-2025  19:50    <DIR>        .
02-01-2025  19:50    <DIR>        ..
25-11-2024  22:31    <DIR>        ANSHUL DATA
31-12-2024  22:20                348 ASSESSMENT-PASSWORD.txt
02-01-2025  19:49    <DIR>        cmddel
29-12-2024  16:21    <DIR>        college data
18-12-2024  08:36    <DIR>        CSF TOOLS
30-05-2014  14:22    <DIR>        DISK1
28-12-2024  09:59    <DIR>        FIP PRESENTAION-SJ
30-12-2024  19:51    <DIR>        MICRO TEACHING PPT
14-02-2023  07:34                2,348 Microsoft Edge.lnk
02-01-2025  16:57                15,281 misplace issue application.docx
04-12-2024  15:24    <DIR>        Sem -1 Templates
```

To show the folder again, execute the command – attrib -h -s -r folder_name.

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

```
C:\Users\DELL\Desktop>attrib -h -s -r hidefld

C:\Users\DELL\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

Directory of C:\Users\DELL\Desktop

02-01-2025  19:50    <DIR>          .
02-01-2025  19:50    <DIR>          ..
25-11-2024  22:31    <DIR>          ANSHUL DATA
31-12-2024  22:20             348 ASSESSMENT-PASSWORD.txt
02-01-2025  19:49    <DIR>          cmddel
29-12-2024  16:21    <DIR>          college data
18-12-2024  08:36    <DIR>          CSF TOOLS
30-05-2014  14:22    <DIR>          DISK1
28-12-2024  09:59    <DIR>          FIP PRESENTAION-SJ
02-01-2025  19:50    <DIR>          hidefld
30-12-2024  19:51    <DIR>          MICRO TEACHING PPT
14-02-2023  07:34             2,348 Microsoft Edge.lnk
02-01-2025  16:57             15,281 misplace issue application.docx
04-12-2024  15:24    <DIR>          Sem -1 Templates
11-12-2024  16:40             2,388 Sweta - Chrome.lnk
13-07-2024  11:50    <DIR>          UGC
               4 File(s)                20,365 bytes
              12 Dir(s)  21,369,151,488 bytes free
```

[14]echo: The echo command in Windows Command Prompt is used to **display a message or output to the screen**. It can also be used to **enable or disable the command echoing** (displaying commands as they are executed in batch scripts).

```
C:\Users\DELL\Desktop>echo "Hello Parul Students!"  
"Hello Parul Students!"  
  
C:\Users\DELL\Desktop>
```

[15] mkdir: The mkdir (or md) command in Windows Command Prompt is used to **create a new directory (folder)** at the specified location.

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

```
C:\Users\DELL\Desktop>mkdir mycmdfolder

C:\Users\DELL\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

Directory of C:\Users\DELL\Desktop

02-01-2025  20:00    <DIR>          .
02-01-2025  20:00    <DIR>          ..
25-11-2024  22:31    <DIR>          ANSHUL DATA
31-12-2024  22:20           348 ASSESSMENT-PASSWORD.txt
02-01-2025  19:49    <DIR>          cmddel
29-12-2024  16:21    <DIR>          college data
18-12-2024  08:36    <DIR>          CSF TOOLS
30-05-2014  14:22    <DIR>          DISK1
28-12-2024  09:59    <DIR>          FIP PRESENTAION-SJ
02-01-2025  19:50    <DIR>          hidefld
30-12-2024  19:51    <DIR>          MICRO TEACHING PPT
14-02-2023  07:34           2,348 Microsoft Edge.lnk
02-01-2025  16:57          15,281 misplace issue application.docx
02-01-2025  20:00    <DIR>          mycmdfolder
04-12-2024  15:24    <DIR>          Sem -1 Templates
11-12-2024  16:40           2,388 Sweta - Chrome.lnk
13-07-2024  11:50    <DIR>          UGC
               4 File(s)              20,365 bytes
              13 Dir(s)  21,368,291,328 bytes free
```

[16]rmdir: The rmdir (or rd) command in Windows Command Prompt is used to **remove (delete) a**

directory. The directory must be empty for it to be removed by this command.

```
C:\Users\DELL\Desktop>rmdir mycmdfolder

C:\Users\DELL\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

Directory of C:\Users\DELL\Desktop

02-01-2025  20:00    <DIR>          .
02-01-2025  20:00    <DIR>          ..
25-11-2024  22:31    <DIR>          ANSHUL DATA
31-12-2024  22:20             348 ASSESSMENT-PASSWORD.txt
02-01-2025  19:49    <DIR>          cmddel
29-12-2024  16:21    <DIR>          college data
18-12-2024  08:36    <DIR>          CSF TOOLS
30-05-2014  14:22    <DIR>          DISK1
28-12-2024  09:59    <DIR>          FIP PRESENTAION-SJ
02-01-2025  19:50    <DIR>          hidefld
30-12-2024  19:51    <DIR>          MICRO TEACHING PPT
14-02-2023  07:34             2,348 Microsoft Edge.lnk
02-01-2025  16:57             15,281 misplace issue application.docx
04-12-2024  15:24    <DIR>          Sem -1 Templates
11-12-2024  16:40             2,388 Sweta - Chrome.lnk
13-07-2024  11:50    <DIR>          UGC
               4 File(s)                20,365 bytes
              12 Dir(s)  21,368,225,792 bytes free
```

[17]tree: The tree command in Windows Command Prompt is used to **display a graphical representation of the directory structure** of a specified drive or directory. It shows the hierarchy of folders and subfolders in a tree-like format, which can be useful for visualizing folder structures.

```
Administrator: hacker
C:\Windows\system32>tree
```

Output of command:

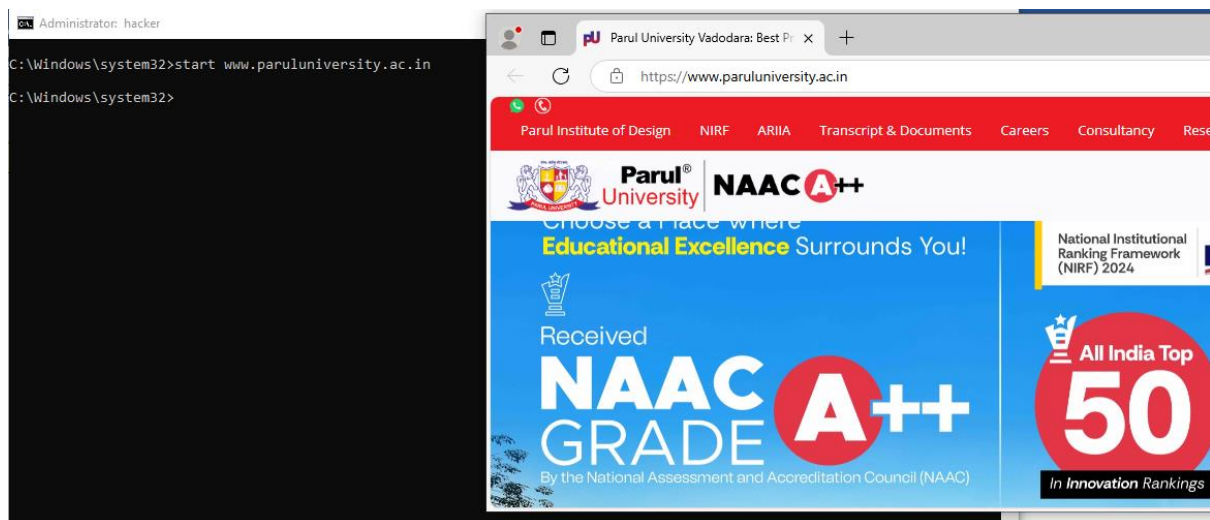
```
Administrator: hacker
Engines
├── SR
│   └── en-US
└── TTS
SpeechUX
└── en-US
Speech_OneCore
├── common
│   └── en-US
├── Engines
│   ├── SR
│   └── TTS
└── VoiceActivation
    └── en-US
spool
├── drivers
│   ├── ARM64
│   ├── color
│   ├── IA64
│   ├── W32X86
│   │   ├── 3
│   │   └── PCC
│   ├── WIN40
│   └── x64
│       ├── 3
│       │   └── en-US
│       ├── PCC
│       ├── {0150DE4E-E4DE-49FC-8E65-E96BC0A72059}
│       ├── {084BF8DE-63B1-47E0-902B-064A66AB75C7}
│       └── {0BEAA5FE-588E-4852-BF38-6F03662F03E4}
```

Parul Institute of Computer Application

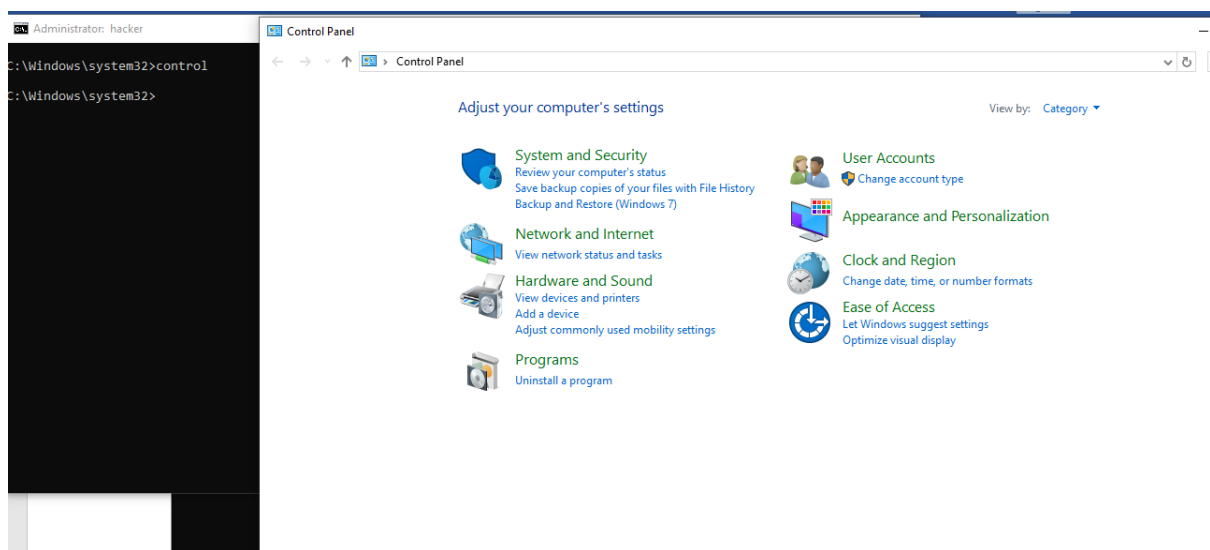
Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

[18]start: The start command in Windows Command Prompt is used to **start a program, command, or open a new command window**. It can be used to run programs in a new window or open files and folders.



[19]control: The control command in Windows Command Prompt is used to **open the Control Panel** or specific applets and settings from the Control Panel directly via the command line. It provides a quick way to access various system settings and tools without navigating through the graphical interface.



[20] firewall.cpl : The firewall.cpl command in Windows is used to **open the Windows Firewall settings** in the Control Panel. It provides a graphical interface for managing the firewall, including enabling or disabling the firewall, configuring inbound and outbound rules, and adjusting other security settings.



[21]sfc: The sfc (System File Checker) command in Windows is a **utility to scan and repair corrupted or missing system files**. It is used to restore critical system files that may be damaged or modified, ensuring the stability and functionality of the operating system.

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

```
Administrator: hacker
C:\Windows\system32>firewall.cpl
C:\Windows\system32>sfc
Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (C) Microsoft Corporation. All rights reserved.

Scans the integrity of all protected system files and replaces incorrect versions with
correct Microsoft versions.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]
[/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory> [/OFFLOGFILE=<log file path>]]

/SCANNOW      Scans integrity of all protected system files and repairs files with
              problems when possible.
/VERIFYONLY   Scans integrity of all protected system files. No repair operation is
              performed.
/SCANFILE     Scans integrity of the referenced file, repairs file if problems are
              identified. Specify full path <file>
/VERIFYFILE   Verifies the integrity of the file with full path <file>. No repair
              operation is performed.
/OFFBOOTDIR   For offline repair, specify the location of the offline boot directory
/OFFWINDIR    For offline repair, specify the location of the offline windows directory
/OFFLOGFILE   For offline repair, optionally enable logging by specifying a log file path

e.g.

sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt
sfc /VERIFYONLY

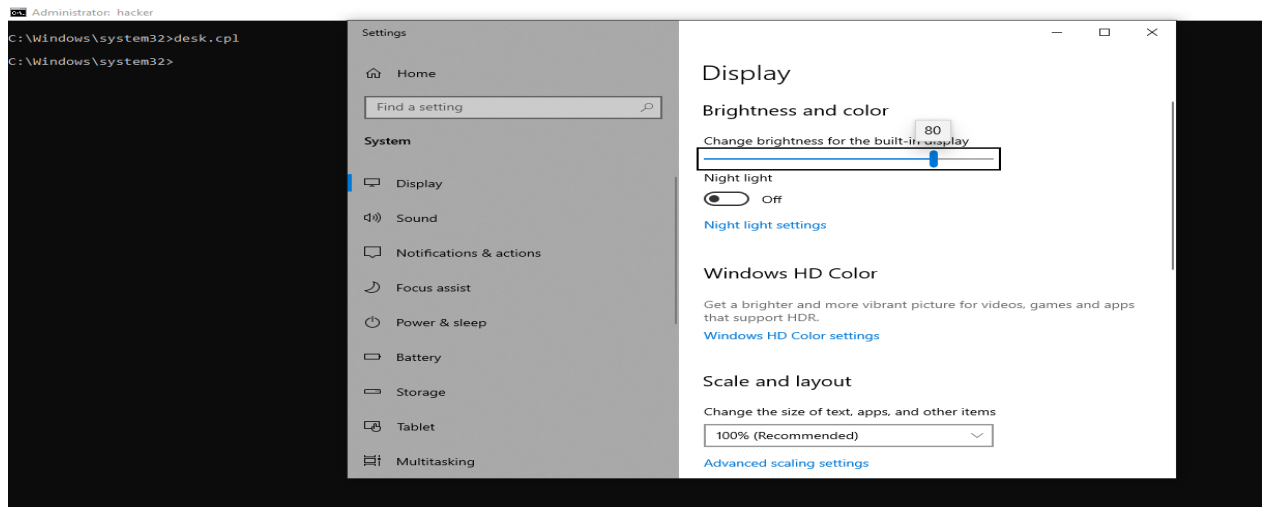
C:\Windows\system32>
```

[22] desk.cpl : The desk.cpl command in Windows is used to **open the Display Properties** window, where you can manage settings related to screen resolution, display orientation, and other display-related configurations. This command is typically used in older versions of Windows (such as Windows XP and earlier) to quickly access display settings via the command line.

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

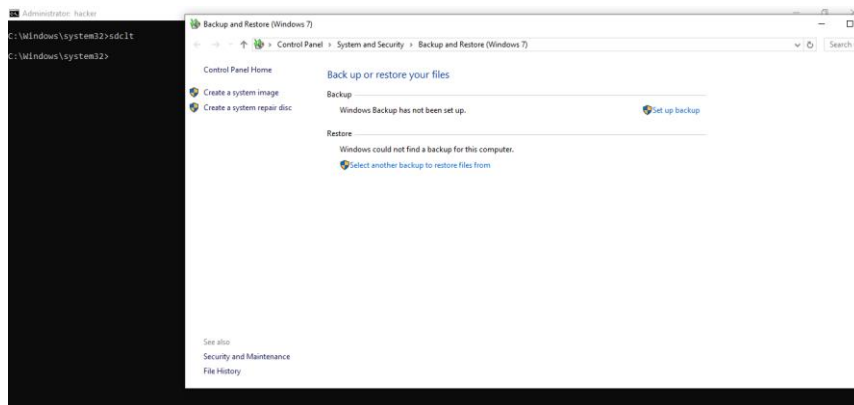


[23]sdclt : The sdclt command in Windows is used to **open the "Backup and Restore" utility**. This utility allows users to create backups of their system and restore files from previously created backups. It provides an interface for setting up system backups, recovering files, and managing backup settings.

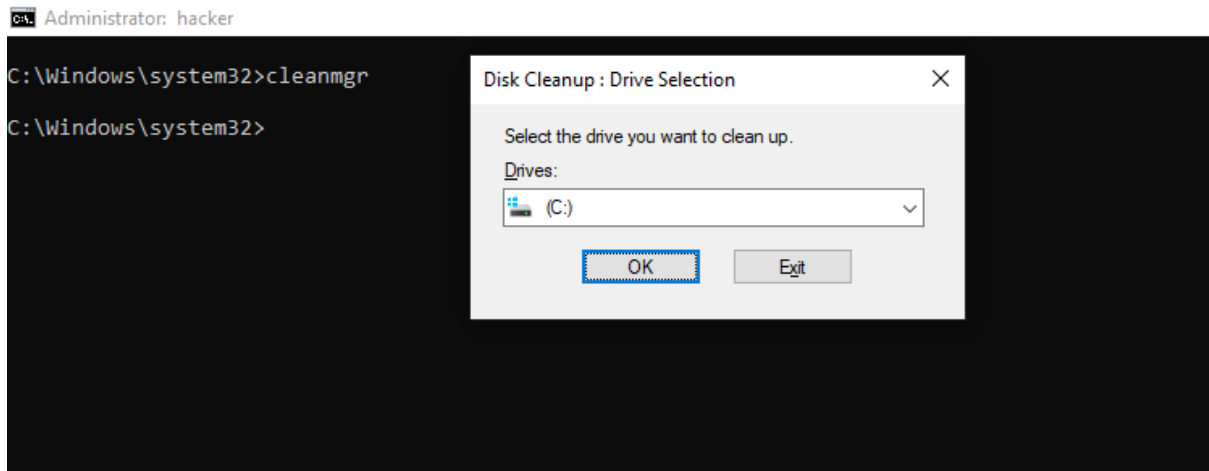
Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system



[24]cleanmgr : The cleanmgr command in Windows is used to **open the Disk Cleanup utility**, which helps users free up space on their hard drives by removing unnecessary files such as temporary files, system files, and cached files.



[25]vol: The vol command in Windows is used to **display the volume label and serial number** of a specified drive. It shows basic information about a drive's file system, which includes the volume label (if assigned) and the unique serial number assigned to the drive.

```
C:\Windows\system32>vol
Volume in drive C has no label.
Volume Serial Number is 124B-F2CB

C:\Windows\system32>vol D:
Volume in drive D is New Volume
Volume Serial Number is DEA0-1930

C:\Windows\system32>
```

[26]ftype: The ftype command in Windows is used to **display or modify file types** that are associated with particular programs or applications. It allows you to

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

manage the file associations and the program that opens a file type (extension).

The ftype command can be used to view and change the file type associations, which define how Windows handles various types of files based on their extension.

```
Administrator: hacker
C:\Windows\system32>ftype
Access.ACCDAExtension.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
Access.ACCDFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
Access.ACCDFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.ACCDFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.ACCDFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
Access.ACCDFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.Application.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.BlankDatabaseTemplate.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /NEWDB "%1"
Access.BlankProjectTemplate.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /NEWDB "%1"
Access.Extension.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
Access.MDBFile=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.MDEFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.Project.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.ShortCut.DataAccessPage.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenDataAccessPage "%1"]
Access.ShortCut.Diagram.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenDiagram "%1"]
Access.ShortCut.Form.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenForm "%1"]
Access.ShortCut.Function.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /SHELLSYSTEM [OpenFunction "%1"]
Access.ShortCut.Macro.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [ShellOpenMacro "%1"]
Access.ShortCut.Module.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenModule "%1"]
Access.ShortCut.Query.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenQuery "%1"]
Access.ShortCut.Report.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenReport "%1", 2]
Access.ShortCut.StoredProcedure.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenStoredProcedure "%1"]
Access.ShortCut.Table.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenTable "%1"]
Access.ShortCut.View.1=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP /SHELLSYSTEM [OpenView "%1"]
Access.UriLink.16=C:\Program Files\Microsoft Office\Root\Office16\protocolhandler.exe "%1"
Access.WebApplicationReference.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1" %2 %3 %4 %5 %6 %7 %8 %9
Access.WizardDataFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
Access.WizardUserDataFile.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
Access.Workgroup.16=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE /NOSTARTUP "%1"
accesshtmlfile=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE
accesshtmltemplate=C:\Program Files\Microsoft Office\Root\Office16\MSACCESS.EXE
acrobat=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe /u "%1"
Acrobat.aau=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.acrobatsecuritysettings.1=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.Document.DC=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.FDFDoc=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.pdfxml.1=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.RMFFile=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.XDPDoc=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.XPDFDoc=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe "%1"
Acrobat.ZB18=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe /u "%1"
Acrobat.ZB18=C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe /u "%1"
```

[27]set: The set command in Windows is used to **set or display environment variables** in the command line or in batch scripts. Environment variables are used to

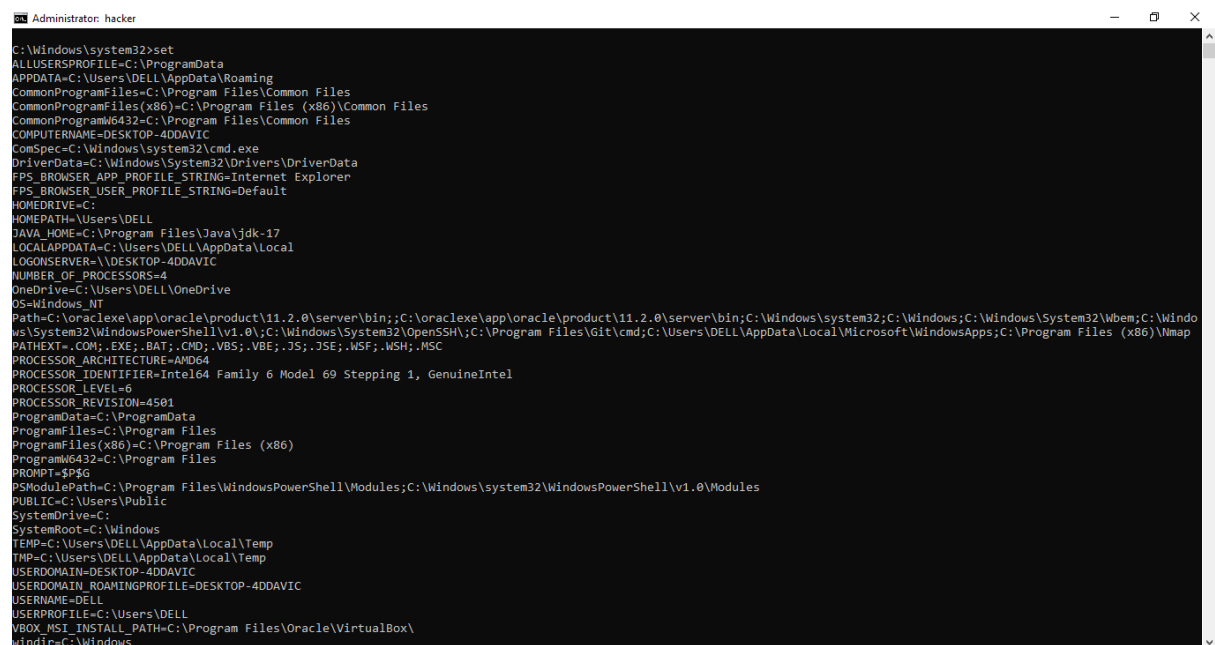
Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

store system-wide settings that can affect the behavior of the operating system or applications.

The set command can either be used to display the current environment variables or to create/modify custom environment variables for the current session.



```
Administrator: hacker
C:\Windows\system32>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\DELL\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-4DDA6IC
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
FPS_BROWSER_USER_PROFILE_STRING=Default
HOMEDRIVE=C:
HOMEPATH=\Users\DELL
JAVA_HOME=C:\Program Files\Java\jdk-17
LOCALAPPDATA=C:\Users\DELL\AppData\Local
LOGONSERVER=\\DESKTOP-4DDA6IC
NUMBER_OF_PROCESSORS=4
OneDrive=C:\Users\DELL\OneDrive
OS=Windows_NT
Path=C:\oraclexe\app\oracle\product\11.2.0\server\bin;;C:\oraclexe\app\oracle\product\11.2.0\server\bin;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\Git\cmd;C:\Users\DELL\AppData\Local\Microsoft\WindowsApps;C:\Program Files (x86)\Nmap
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 69 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4501
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$PSG
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\DELL\AppData\Local\Temp
TMP=C:\Users\DELL\AppData\Local\Temp
USERDOMAIN=DESKTOP-4DDA6IC
USERDOMAIN_ROAMINGPROFILE=DESKTOP-4DDA6IC
USERNAME=DELL
USERPROFILE=C:\Users\DELL
VBOX_MSI_INSTALL_PATH=C:\Program Files\Oracle\VirtualBox\
windir=C:\Windows
```

[28]ipconfig: The ipconfig command in Windows is used to **display and manage network configuration settings** for all active network interfaces on your computer. It provides detailed information about the network adapter, such as the IP address, subnet mask, default gateway, and DNS servers.

You can also use ipconfig to refresh network settings, release and renew IP addresses, and more.

```
C:\Windows\system32>ipconfig
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix  . : home.local
IPv4 Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

[29] `ipconfig /all` : The `ipconfig /all` command in Windows is used to **display detailed information** about the network configuration for all network interfaces on the system. It provides a comprehensive list of all active and inactive network adapters, along with their settings, such as IP addresses, MAC addresses, DNS servers, and more.

This command is especially useful for troubleshooting network issues or verifying network configuration details.

What it Displays:

When you run `ipconfig /all`, you get detailed information for each network interface (including Ethernet adapters, Wi-Fi, and virtual adapters) on the computer. The output typically includes:

1. **Host Name:** The name of the computer.
2. **DNS Suffix:** The DNS domain name suffix.
3. **Adapter Description:** The name of the network adapter (e.g., Realtek Ethernet adapter).
4. **Physical Address (MAC Address):** The unique hardware address for the network adapter.

5. **DHCP Enabled:** Whether Dynamic Host Configuration Protocol (DHCP) is enabled (assigns IP addresses dynamically).
6. **IPv4 Address:** The computer's assigned IPv4 address.
7. **IPv6 Address:** The computer's assigned IPv6 address (if applicable).
8. **Subnet Mask:** The network's subnet mask.
9. **Default Gateway:** The IP address of the default gateway, typically the router.
10. **DNS Servers:** The DNS servers used by the computer to resolve domain names.
11. **Lease Obtained and Lease Expires:** The dates and times for DHCP lease assignment, if DHCP is enabled.

```
C:\Windows\system32>ipconfig /all
```

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

```
Windows IP Configuration

Host Name . . . . . : MyComputer
Primary Dns Suffix . . . . . : home.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : home.local
   Description . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . : XX-XX-XX-XX-XX-XX
   DHCP Enabled. . . . . : Yes
   IPv4 Address. . . . . : 192.168.1.2(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
   DNS Servers . . . . . : 8.8.8.8
```

[30]netstat : The netstat (Network Statistics) command in Windows is used to **display active network connections** and network statistics for your computer. It provides information about the current network connections, open ports, routing tables, and network interface statistics.

The netstat command is helpful for monitoring network activity, troubleshooting connection issues, and finding open ports or services running on your machine.

```
C:\Windows\system32>netstat

Active Connections

Proto Local Address          Foreign Address         State
```


[31]nslookup: The nslookup command in Windows is a **network diagnostic tool** used to query the Domain Name System (DNS) and obtain information about domain names, IP addresses, and DNS records. It allows you to perform DNS lookups, troubleshoot DNS-related issues, and check the configuration of DNS servers.

```
C:\Windows\system32>nslookup www.paruluniversity.ac.in
Server:    UnKnown
Address:   192.168.0.1

Non-authoritative answer:
Name:      paruluniversity.ac.in
Address:   34.131.228.21
Aliases:   www.paruluniversity.ac.in
```

[32]route -h : The route -h command is used in Windows to display the **help** information for the route command, which is used to display or modify the routing table of a computer. The routing table is a set of rules that determines where network traffic is directed. This command is useful for network configuration and troubleshooting.

```
C:\Windows\system32>route -h

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                                     [MASK netmask] [gateway] [METRIC metric] [IF interface]

-f          Clears the routing tables of all gateway entries.  If this is
            used in conjunction with one of the commands, the tables are
            cleared prior to running the command.

-p          When used with the ADD command, makes a route persistent across
            boots of the system.  By default, routes are not preserved
            when the system is restarted.  Ignored for all other commands,
            which always affect the appropriate persistent routes.

-4          Force using IPv4.

-6          Force using IPv6.

command     One of these:
            PRINT      Prints  a route
            ADD        Adds    a route
            DELETE     Deletes a route
            CHANGE     Modifies an existing route

destination Specifies the host.
MASK          Specifies that the next parameter is the 'netmask' value.
netmask       Specifies a subnet mask value for this route entry.
            If not specified, it defaults to 255.255.255.255.
gateway       Specifies gateway.
interface     the interface number for the specified route.
METRIC        specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS.  The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE.  Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed.  The '*' matches any string,
and '?' matches any one char.  Examples: 157.*.1, 157.*, 127.*, *224*.
```

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

```
C:\Windows\system32>route print
=====
Interface List
 8...20 47 47 cc 07 66 .....Realtek PCIe GBE Family Controller
16...0a 00 27 00 00 10 .....VirtualBox Host-Only Ethernet Adapter
11...b4 6d 83 16 79 76 .....Microsoft Wi-Fi Direct Virtual Adapter
10...b6 6d 83 16 79 75 .....Microsoft Wi-Fi Direct Virtual Adapter #2
18...b4 6d 83 16 79 75 .....Intel(R) Dual Band Wireless-AC 3160
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.0.1      192.168.0.110    50
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
192.168.0.0                 255.255.255.0    On-link          192.168.0.110    306
192.168.0.110              255.255.255.255  On-link          192.168.0.110    306
192.168.0.255              255.255.255.255  On-link          192.168.0.110    306
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          192.168.0.110    306
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          192.168.0.110    306
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
```

[33]arp: The arp command in Windows is used to **view and modify the Address Resolution Protocol (ARP)** cache. ARP is a protocol used to map a 32-bit IP address to a physical MAC address (Media Access Control address), which is necessary for devices to communicate over a local network.

The ARP cache is a table that stores the mappings of IP addresses to MAC addresses for devices within a local network, improving network communication efficiency. The arp command allows you to view this cache and perform actions like adding or deleting entries.

```
C:\Windows\system32>arp -a  
Interface: 192.168.56.1 --- 0x10
```

[34]tracert: The tracert command in Windows is used to trace the **route** that packets take from your computer to a destination host (such as a domain name or IP address) across a network, typically the Internet. It helps to identify the path taken by packets, including the intermediate routers, and can assist in diagnosing network connectivity issues or delays.

tracert stands for **Trace Route**, and it shows the list of routers (also known as hops) that a packet passes through on its way to the destination. It also provides the **round-trip time** (RTT) for each hop, helping you understand where delays or packet loss may be occurring in the network.

```
C:\Windows\system32>tracert google.com

Tracing route to google.com [142.250.192.110]
over a maximum of 30 hops:

  1    7 ms    1 ms    1 ms  192.168.0.1
  2    4 ms    2 ms    2 ms  10.100.0.1
  3    *       13 ms   10 ms  10.233.11.2
  4   12 ms   11 ms    9 ms  103.241.47.89
  5   12 ms  293 ms   39 ms  142.250.47.236
  6    9 ms   10 ms    9 ms  74.125.37.7
  7   13 ms   18 ms   13 ms  72.14.237.11
  8   10 ms   10 ms    9 ms  bom12s17-in-f14.1e100.net [142.250.192.110]

Trace complete.
```

[35]ping: The ping command in Windows is used to **test network connectivity** between your computer and a remote device, such as a server or another computer. It works by sending **ICMP Echo Request** packets to the target and waiting for **ICMP Echo Reply** packets. The command helps determine if a device on a network is reachable and how long it takes for data to travel between the source and destination.

```
C:\Windows\system32>ping google.com

Pinging google.com [142.250.192.110] with 32 bytes of data:
Reply from 142.250.192.110: bytes=32 time=12ms TTL=59
Reply from 142.250.192.110: bytes=32 time=24ms TTL=59
Reply from 142.250.192.110: bytes=32 time=9ms TTL=59
Reply from 142.250.192.110: bytes=32 time=9ms TTL=59

Ping statistics for 142.250.192.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 24ms, Average = 13ms
```

[36]ping -4: The ping -4 command in Windows is used to force the ping command to use **IPv4** (Internet Protocol version 4) when testing the network connectivity. This is helpful when the system supports both IPv4 and IPv6 but you want to explicitly use IPv4 for your test.

```
C:\Windows\system32>ping -4 google.com

Pinging google.com [142.250.192.110] with 32 bytes of data:
Reply from 142.250.192.110: bytes=32 time=9ms TTL=59
Reply from 142.250.192.110: bytes=32 time=9ms TTL=59
Reply from 142.250.192.110: bytes=32 time=9ms TTL=59
Reply from 142.250.192.110: bytes=32 time=12ms TTL=59

Ping statistics for 142.250.192.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 12ms, Average = 9ms
```

[37]nbtstat: The nbtstat command in Windows is used to display **NetBIOS over TCP/IP (NetBT)** statistics, which includes information about the NetBIOS name resolution and the NetBIOS name table. It helps in diagnosing network issues related to the NetBIOS protocol, which is commonly used in local area networks (LANs) for network file sharing and other services.

```
C:\Windows\system32>nbtstate -a selftarget_ip
```

[38] **assoc**: The **assoc** command in Windows is used to display or modify the **file extension associations**. It helps associate file extensions (such as .txt, .jpg, .docx, etc.) with specific programs that are used to open those files. This command allows you to manage which program opens a particular type of file based on its file extension.

```
hacker >assoc
.001=WinRAR
.386=vxdfile
.3g2=WMP11.AssocFile.3G2
.3ga=VLC.3ga
.3gp=WMP11.AssocFile.3GP
.3gp2=WMP11.AssocFile.3G2
.3gpp=WMP11.AssocFile.3GP
.5vw=wireshark-capture-file
.669=VLC.669
.7z=WinRAR
.a52=VLC.a52
.AAC=WMP11.AssocFile.ADTS
.aau=Acrobat.aau
.acdda=Access.ACCDAExtension.16
.acddb=Access.Application.16
.accdc=Access.ACCDCFile.16
.accde=Access.ACCDEFile.16
.accdr=Access.ACCDRFile.16
.accdt=Access.ACCDTFile.16
.accdu=Access.WizardUserDataFile.16
.accdw=Access.WebApplicationReference.16
.accft=Access.ACCFTFile.16
```


[39] powercfg help: The powercfg command in Windows is a powerful tool used to configure and manage power settings, such as sleep settings, power plans, and hibernation. It allows you to optimize the system's power usage and troubleshoot power-related issues.

```
hacker
hacker >powercfg
Invalid Parameters -- try "/" for help

hacker >powercfg help

POWERCFG /COMMAND [ARGUMENTS]

Description:
  Enables users to control power settings on a local system.

  For detailed command and option information, run "POWERCFG /? <COMMAND>"

Command List:
  /LIST, /L          Lists all power schemes.
  /QUERY, /Q         Displays the contents of a power scheme.
  /CHANGE, /X        Modifies a setting value in the current power scheme.
  /CHANGENAME        Modifies the name and description of a power scheme.
  /DUPLICATESCHEME   Duplicates a power scheme.
  /DELETE, /D        Deletes a power scheme.
  /DELETESSETTING    Deletes a power setting.
  /SETACTIVE, /S     Makes a power scheme active on the system.
  /GETACTIVESCHEME   Retrieves the currently active power scheme.
  /SETACVALUEINDEX   Sets the value associated with a power setting
                    while the system is powered by AC power.
  /SETDCVALUEINDEX   Sets the value associated with a power setting
                    while the system is powered by DC power.
  /IMPORT            Imports all power settings from a file.
  /EXPORT            Exports a power scheme to a file.
  /ALIASES           Displays all aliases and their corresponding GUIDs.
```

[40] exit & shutdown:

exit – Closes the Command Line

&

Parul Institute of Computer Application

Prepared By :- Prof. Sweta Jethava

Topic :- Command-line hacking on a Windows operating system

shutdown – Shuts down, Restarts, Hibernates, Sleeps the Computer