# **Topic I - Introduction to Commands prompt**

# **Open CMD**

* Search for "cmd" in the Start menu and open it.

# **Show Current Directory**

* cd

# **Change Directory**

* cd [path]
* Example: - cd C:\Users

# **Move Up One Directory**

* cd ..

# **List Files and Folders in the Current Directory**

* dir

# **Clear the Screen**

* cls

# **Open a Specific Drive**

* [drive\_letter]:
* Example: - D:

# **Create a New Directory**

* mkdir [folder\_name]
* **Example:** mkdir MyFolder

# **Remove Directory with Files & Folders**

* rd [folder\_name] /S
* **Example:** rd MyFolder /S

# **Delete a Directory**

* rmdir [folder\_name]
* **Example:** rmdir MyFolder

# **Exit Command Prompt**

* exit

# **Topic II - Basic Files and Folders Operations - Create Copy Move and Delete Commands**

# **Change Directory**

* cd [path]
* Example: cd C:\Users

# **Rename File**

* ren [old.format] [new.format]
* Example: ren old.txt new.txt

# **Copy File**

* copy [file-name] (Path where you want to paste)
* Example: copy one.txt "C:\Users\Mahrus Ali\Desktop"

# **Move File**

* move [file-name] (Path where you want to paste)
* Example: move one.txt "C:\Users\Mahrus Ali\Desktop"

# **Delete Single File**

* del [file.format]
* Example: del one.txt

# **Delete Multiple Files**

* del \*.format
* Example: del \*.txt

# **Create File with Text**

* echo [text] > [file-name]
* Example: echo This is a sample text > file.txt

# **Append Text to File**

* echo [text] >> [file-name]
* Example: echo This is also crazy sample text >> file.txt

# **Create File and Input Text from Console**

* copy con [file-name]
* Example: copy con example.txt

# **Topic III -Managing Tasks and Services using CMD – Start & Stop Commands**

# **List Running Processes**

* tasklist
* Example: tasklist

# **Terminate Task by PID**

* taskkill /PID [PID]
* Example: taskkill /PID 1234

# **Forcibly Terminate Task by PID**

* taskkill /PID [PID] /F
* Example: taskkill /PID 1234 /F

# **List Installed Device Drivers**

* driverquery
* Example: driverquery

# **List Running Services**

* net start
* Example: net start

# **Stop Running Service**

* net stop "service-name"
* Example: net stop "Print Spooler"

# **Start Service**

* net start "service-name"
* Example: net start "Print Spooler"

# **Check Disk**

* chkdsk [drive:]
* Example: chkdsk C:

# **Scan and Repair System Files**

* sfc /scannow
* Example: sfc /scannow

# **Shutdown Computer**

* shutdown /s /t 0
* Example: shutdown /s /t 0

# **Display Services in Each Process**

* tasklist /svc
* Example: tasklist /svc

# **Query Service Information**

* sc query
* Example: sc query

# **Topic IV - Getting Information using WMIC commands in CMD**

# **Initialize WMIC Command**

* **wmic**
* **Example: wmic**

# **Query CPU Information**

* **cpu**
* **Example: wmic:root\cli> cpu**

# **Exit WMIC Environment**

* **quit**
* **Example: wmic:root\cli> quit**

**Here are 15 additional WMIC commands related to system management**

# **Query BIOS Information**

* **bios**
* **Example: wmic:root\cli> bios**

# **Query Operating System Information**

* **os**
* **Example: wmic:root\cli> os**

# **Query Disk Drive Information**

* **diskdrive**
* **Example: wmic:root\cli> diskdrive**

# **Query Memory Information**

* **memorychip**
* **Example: wmic:root\cli> memorychip**

# **Query Network Adapter Information**

* **nic**
* **Example: wmic:root\cli> nic**

# **Query Processes**

* **process**
* **Example: wmic:root\cli> process**

# **Query User Accounts**

* **useraccount**
* **Example: wmic:root\cli> useraccount**

# **Query Installed Software**

* **product**
* **Example: wmic:root\cli> product**

# **Query Services**

* **service**
* **Example: wmic:root\cli> service**

# **Query Logical Disks**

* **logicaldisk**
* **Example: wmic:root\cli> logicaldisk**

# **Query Sound Devices**

* **sounddev**
* **Example: wmic:root\cli> sounddev**

# **Query Printers**

* **printer**
* **Example: wmic:root\cli> printer**

# **Query Startup Programs**

* **startup**
* **Example: wmic:root\cli> startup**

# **Query Environment Variables**

* **environment**
* **Example: wmic:root\cli> environment**

# **Query Shared Folders**

* **share**
* **Example: wmic:root\cli> share**

# **Query Network Protocols**

* **netprotocol**
* **Example: wmic:root\cli> netprotocol**

# **Topic V - Information Gathering using CMD - Collecting system info**

# **Retrieve Name and Version of Installed Software Products**

* product get name, version
* Example: wmic:root\cli> product get name, version

# **Retrieve Size and Model of Disk Drives**

* diskdrive get size, model
* Example: wmic:root\cli> diskdrive get size, model

# **Retrieve Operating System Name and Version**

* os get name, version
* Example: wmic:root\cli> os get name, version

# **Retrieve Computer System Information**

* computersystem get name, manufacturer, model
* Example: wmic:root\cli> computersystem get name, manufacturer, model

# **Retrieve BIOS Name and Version**

* bios get name, version
* Example: wmic:root\cli> bios get name, version

# **Retrieve Network Adapter Information**

* nic get name, macaddress
* Example: wmic:root\cli> nic get name, macaddress

# **Retrieve Logical Disk Information**

* logicaldisk get name, filesystem, freespace
* Example: wmic:root\cli> logicaldisk get name, filesystem, freespace

# **List Installed Windows Updates (QFE)**

* qfe list
* Example: wmic:root\cli> qfe list

# **List Startup Programs**

* startup list full
* Example: wmic:root\cli> startup list full

# **List User Accounts with Brief Information**

* useraccount list brief
* Example: wmic:root\cli> useraccount list brief

# **Terminate Process by Name**

* wmic process where name="process.exe" call terminate
* Example: wmic process where name="notepad.exe" call terminate

# **Topic VI - Hiding & Encrypting Files using CMD - AES Encryption cipher & attrib**

# **Change File Attributes**

* attrib +h +r +s file.png
* Description: Changes the attributes of a file to hidden, read-only, and system.
* Explanation:
  + +h: Sets the hidden attribute, making the file invisible in the default directory view.
  + +r: Sets the read-only attribute, preventing the file from being modified.
  + +s: Sets the system attribute, marking the file as a system file.
* Example: attrib +h +r +s file.png

# **Remove File Attributes**

* attrib -h -r -s file.png
* Description: Removes the hidden, read-only, and system attributes from a file.
* Explanation:
  + -h: Removes the hidden attribute.
  + -r: Removes the read-only attribute.
  + -s: Removes the system attribute.
* Example: attrib -h -r -s file.png

# **Encrypt File**

* cipher /e file.format
* Description: Encrypts the specified file(s) or directory.
* Explanation:
  + /e: Encrypts the specified files or directories.
* Example: cipher /e file.txt

# **Decrypt File**

* cipher /d file.format
* Description: Decrypts the specified file(s) or directory.
* Explanation:
  + /d: Decrypts the specified files or directories.
* Example: cipher /d file.txt

# **Display Encryption Information**

* cipher /c
* Description: Displays information about the encryption of a file or directory.
* Explanation:
  + /c: Displays the current encryption state of the specified files.
* Example: cipher /c file.txt

# **Display/Modify File Extension Associations**

* assoc .format
* Description: Displays or modifies file extension associations.
* Explanation:
  + This command is used to associate a file extension with a specific program.
* Example to display current association: assoc .txt
* Example to associate .txt with Notepad: assoc .txt=txtfile

Additional Related Commands:

# **Display/Change File Attributes**

* attrib
* Description: Displays or changes file attributes.
* Example: attrib file.txt

# **Create New File Encryption Key**

* cipher /k
* Description: Creates a new file encryption key for the user running the cipher command.
* Example: cipher /k

# **Encrypt Files in Directory**

* cipher /s:directory
* Description: Performs the encryption operation on all files in the specified directory and its subdirectories.
* Example: cipher /e /s:C:\Users\Mahrus Ali\Documents

# **Display All Associations**

* assoc
* Description: Displays or modifies file extension associations.
* Example to display all associations: assoc

# **Display/Modify File Types**

* ftype
* Description: Displays or modifies file types that have been assigned file extension associations.
* Example: ftype txtfile="C:\Windows\System32\NOTEPAD.EXE" "%1"

# **Class VII - User Management using CMD – Adding & Deleting Resetting users**

# **Add a New User**

* Description: To add a user
* Syntax: net user [username] [password] /add
* Example: -
  + - net user mahrus123 password123 /add

# **Assign the User to Administrators Group**

* Description: To give administrative rights
* Syntax: net localgroup administrators [username] /add
* Example: -
  + - net localgroup administrators mahrus123 /add

# **Delete a User**

* Description: To remove a user
* Syntax: net user [username] /delete
* Example: -
  + - net user mahrus123 /delete

# **Reset User Password**

* Description: To reset a password
* Syntax: net user [username] [newpassword]
* Example: -
  + - net user mahrus123 newpassword321

# **List All Users**

* Description: To view all users on the system
* Syntax: net user
* Example: -
  + - net user

# **Disable a User Account**

* Description: To disable a user
* Syntax: net user [username] /active:no
* Example: -
  + - net user mahrus123 /active:no

# **Enable a User Account**

* Description: To re-enable a user
* Syntax: net user [username] /active:yes
* Example: -
  + - net user mahrus123 /active:yes

# **Users Info**

* Description: To get users information
* Syntax: net user "user-name"
* Example: -
  + - net user "Mahrus Ali"

# **Topic 08 - Creating Exporting Files through \_ Create\_ Export \_ Read Files via CUI**

# **Export Full System Information**

* + Use the "systeminfo" command:
  + Example:-
  + systeminfo > systeminfo.txt

This saves all system details (e.g., OS, memory, processor) to a file named "systeminfo.txt".

# **Export Specific System Information**

* + Export details about network configuration:
  + Example:-
  + ipconfig > networkinfo.txt
  + Export detailed network adapter configuration:
  + Example:-
  + ipconfig /all > fullnetworkinfo.txt

# **Export Disk and Volume Information**

* Save disk drive information:
* Example:-
  + wmic diskdrive get > diskinfo.txt
* Save volume information:
* Example:-
  + wmic volume get > volumeinfo.txt

# **Export List of Installed Software**

* + - Use "wmic" to get installed programs:
    - Example:-
  + wmic product get name,version > installed\_programs.txt

# **Export Running Processes**

* + - Save a list of running processes:
    - Example:-
  + tasklist > running\_processes.txt