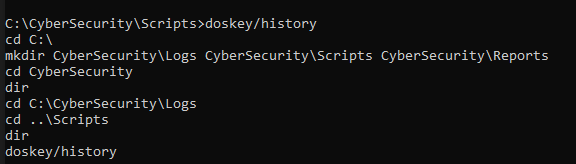
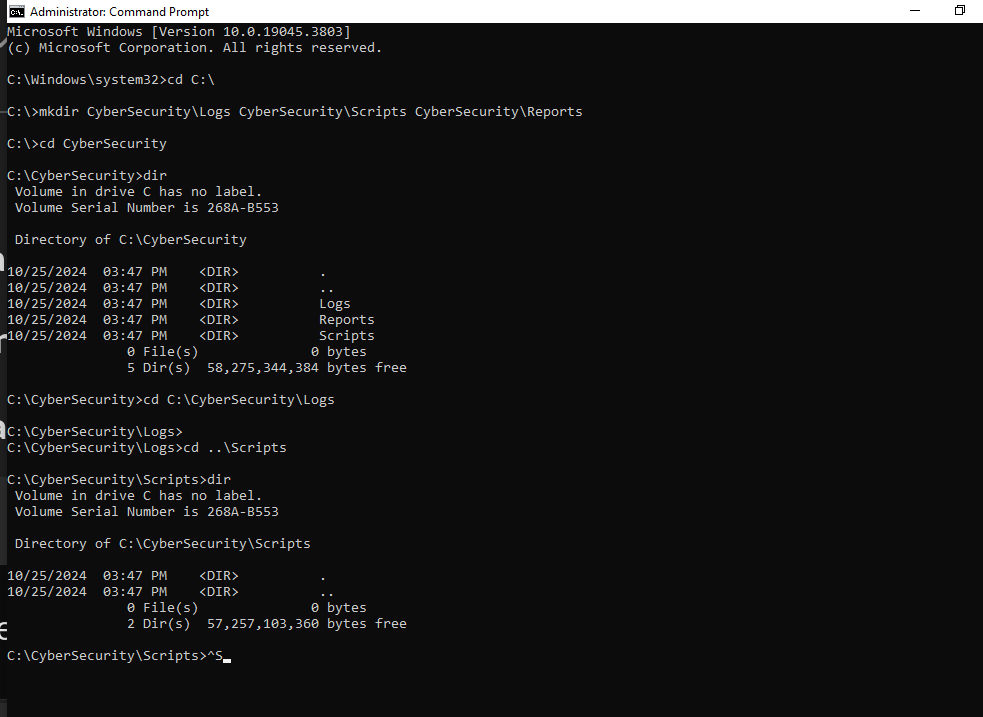
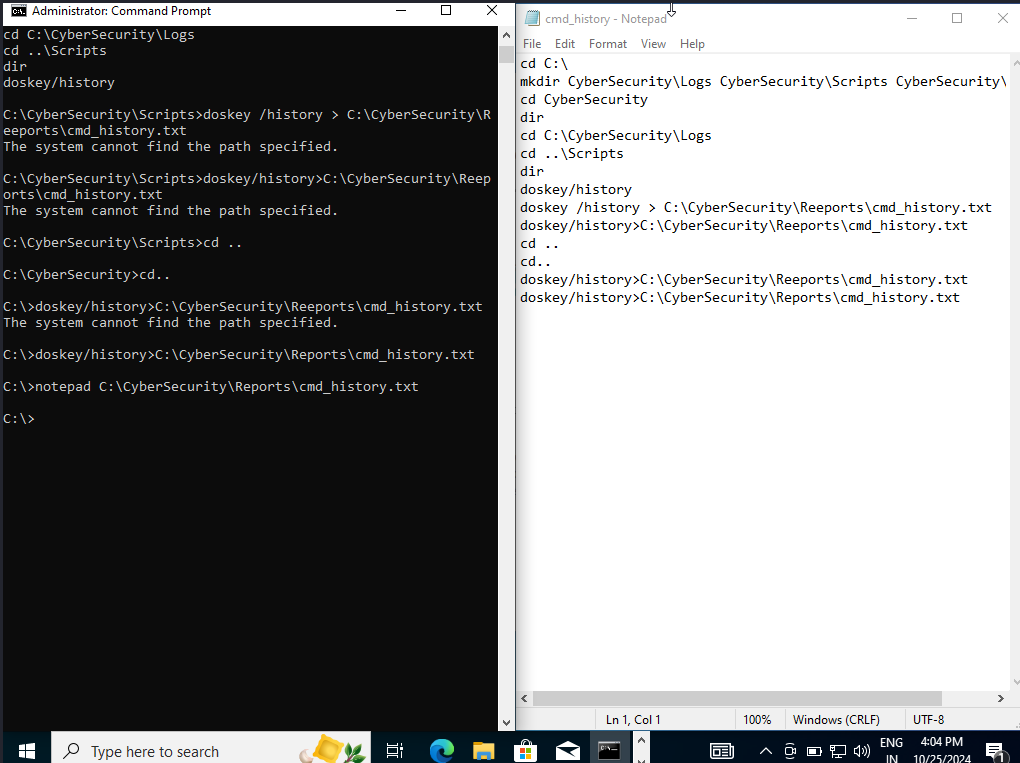
Assignment : Windows CMD

# Part 1: System Navigation and Basic Commands

Task 1.1: Directory Navigation and History :



**Commands and Explanations:**

1. **cd C:\**

**Purpose:** Navigated to the root of the C: drive. This command set the starting point for creating the directory structure.

1. **mkdir CyberSecurity\Logs CyberSecurity\Scripts CyberSecurity\Reports**

**Purpose:** Created a folder called CyberSecurity under C:\, with subfolders Logs, Scripts, and Reports. This structure supports organized storage for different types of files.

1. **cd CyberSecurity**

**Purpose:** Entered the CyberSecurity folder from the root directory to confirm its contents and prepare for further navigation.

1. **dir**

**Purpose:** Listed the contents of CyberSecurity, showing the presence of Logs, Scripts, and Reports subdirectories. This confirmed successful creation of the directory structure.

1. **cd C:\CyberSecurity\Logs (Absolute Path)**

**Purpose:** Used an absolute path to navigate directly to the Logs folder. Absolute paths specify the full path from the root, allowing quick access regardless of the current directory.

1. **cd ..\Scripts (Relative Path)**

**Purpose:** Used a relative path to move up one level from Logs to CyberSecurity and then down into Scripts. Relative paths make navigation efficient by referencing nearby directories.

1. **doskey /history**

**Purpose:** Displayed the history of commands used during the session. This feature is useful for tracking command usage and workflow.

1. **doskey /history > C:\CyberSecurity\Reports\cmd\_history.txt**

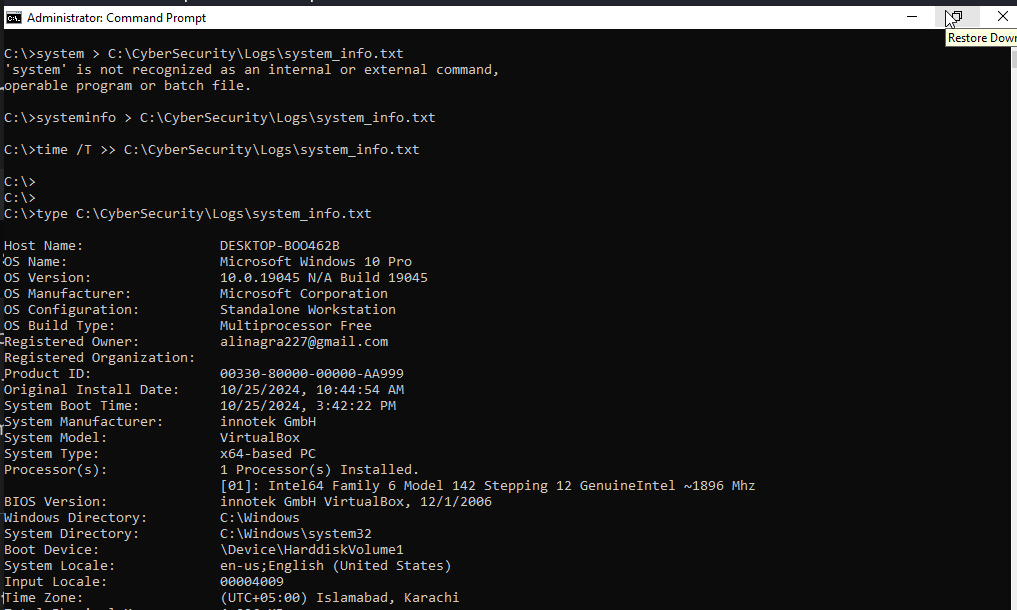
**Purpose:** Redirected the command history output to a text file named cmd\_history.txt in the Reports folder, creating a record of all commands run during this session for future reference.

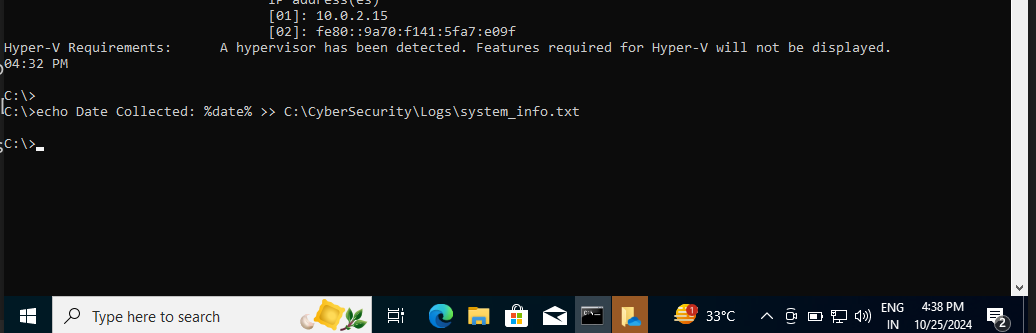
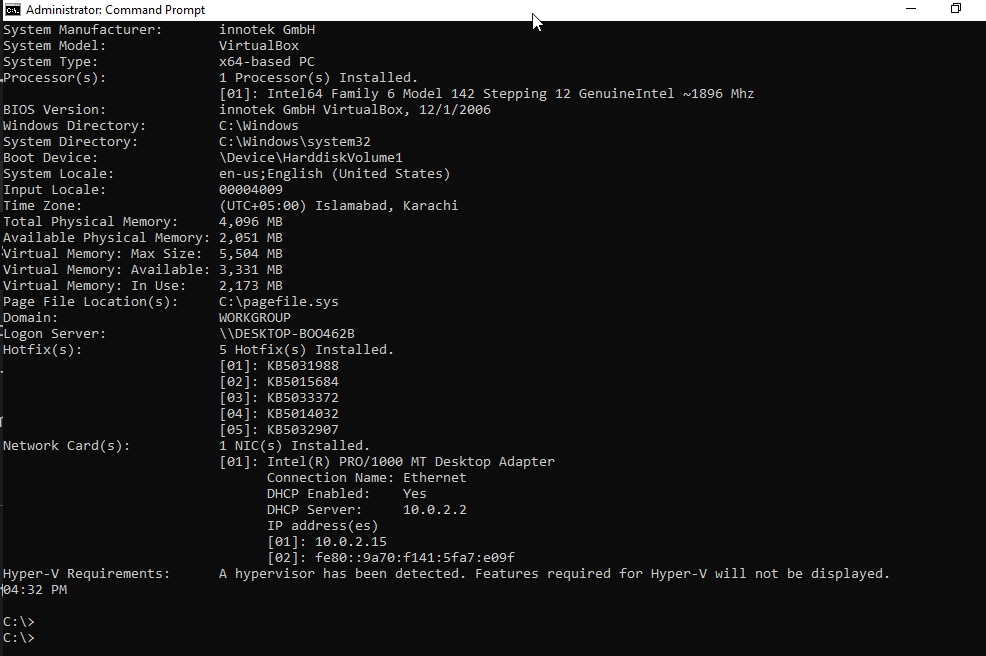
1. **notepad C:\CyberSecurity\Reports\cmd\_history.txt**

**Purpose:** Opened cmd\_history.txt in Notepad to verify the file was successfully created and contained the command history.

# Part 2: File and Directory Management

**Task 2.1: File Creation and Manipulation:**

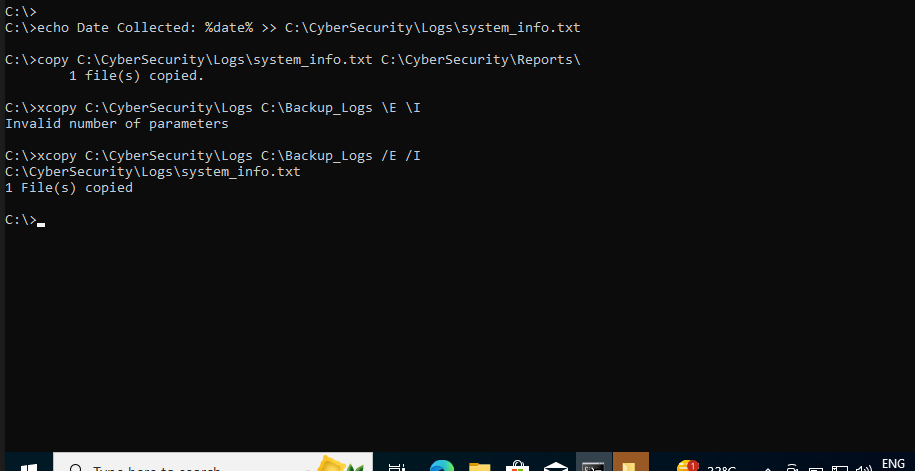




**Commands and Explanations:**

1. **systeminfo > C:\CyberSecurity\Logs\system\_info.txt**
   1. **Purpose:** Collected detailed system information (computer name, OS, etc.) and saved it to a file named system\_info.txt in the Logs directory.
   2. **Explanation:** The systeminfo command retrieves system details, and > saves this output to a text file.
2. **time /T >> C:\CyberSecurity\Logs\system\_info.txt**
   1. **Purpose:** Appended the current time to system\_info.txt.
   2. **Explanation:** The time /T command outputs only the time without prompting, and >> appends this time to the file.
3. **type C:\CyberSecurity\Logs\system\_info.txt**
   1. **Purpose:** Displayed the contents of system\_info.txt in the CMD window.
   2. **Explanation:** The type command outputs the contents of the file, allowing us to confirm the information is correctly recorded.
4. **echo Date Collected: %date% >> C:\CyberSecurity\Logs\system\_info.txt**
   1. **Purpose:** Added a line with the current date to indicate when the data was collected.
   2. **Explanation:** The echo command outputs text, and %date% provides the current date. The >> operator appends this date to system\_info.txt.

**Task 2.2: File and Directory Operations:**

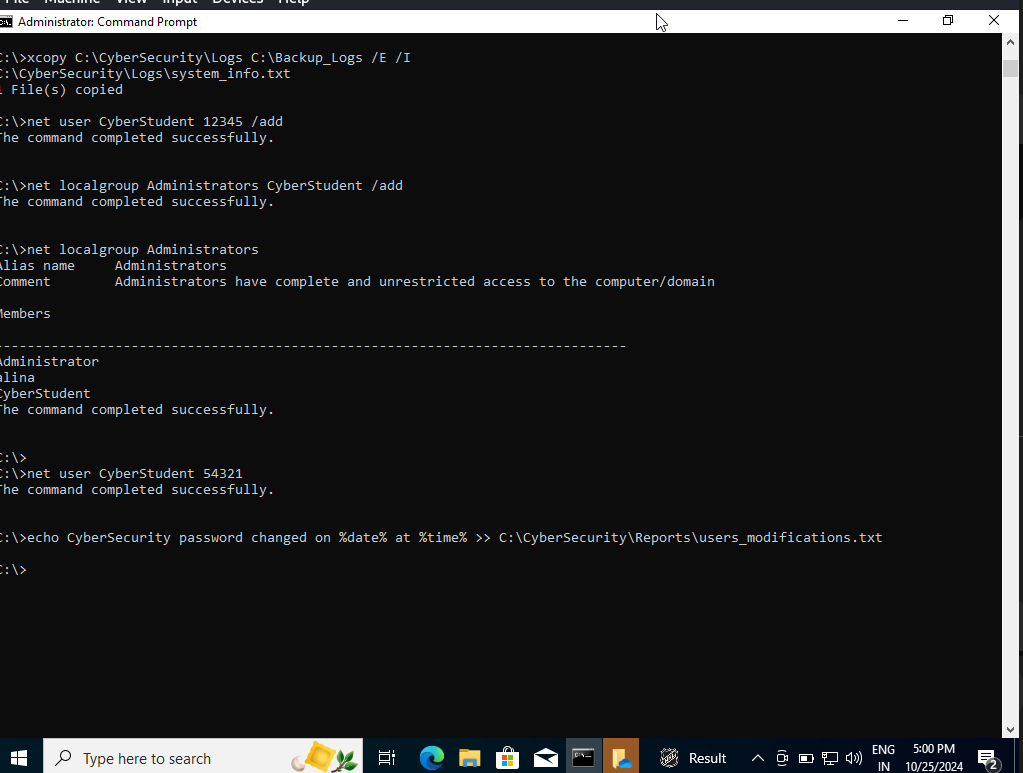


**Commands and Explanations:**

1. **copy C:\CyberSecurity\Logs\system\_info.txt C:\CyberSecurity\Reports\**
   1. **Purpose:** Duplicated the system\_info.txt file from the Logs directory to the Reports directory.
   2. **Explanation:** The copy command makes a copy of the file in a specified location, resulting in system\_info.txt existing in both Logs and Reports.
2. **xcopy C:\CyberSecurity\Logs C:\Backup\_Logs /E /I**
   1. **Purpose:** Copied the entire Logs directory, including all files and subdirectories, to a new directory called Backup\_Logs at the root of C:.
   2. **Explanation:**
      1. /E includes all subdirectories (even if empty).
      2. /I specifies that Backup\_Logs is the destination directory, preventing prompts.

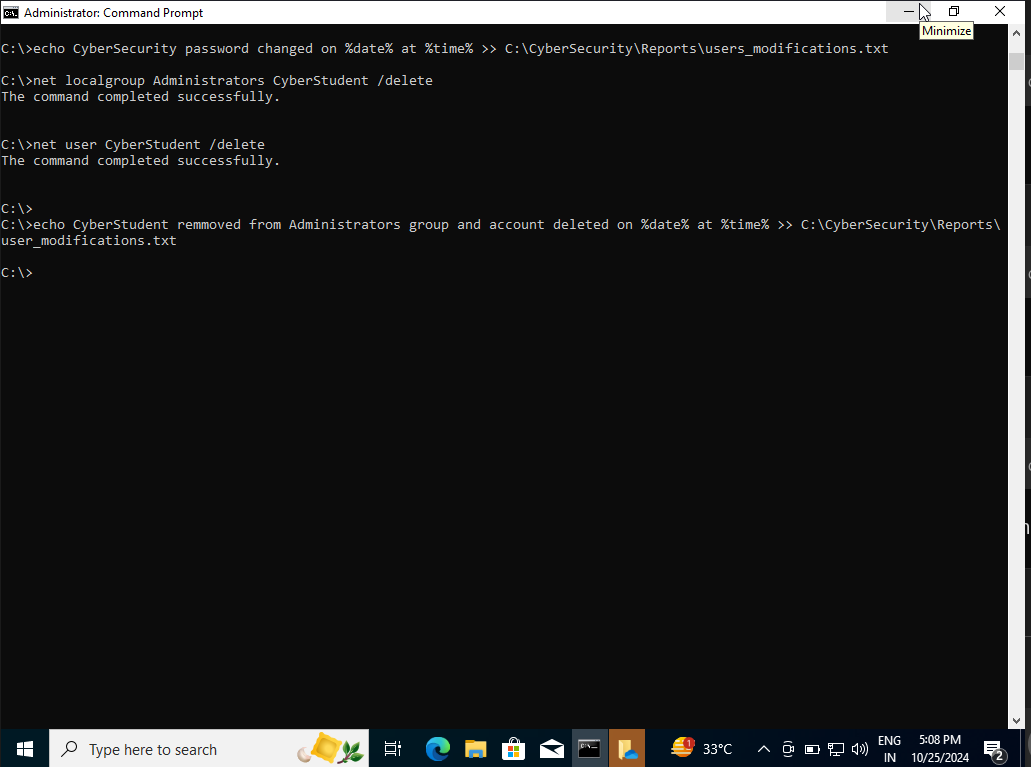
# Part 3: User and Group Management

**Task 3.1: User Creation and Modification :**

**Commands and Explanations:**

1. **net user CyberStudent your\_password\_here /add**
   1. **Purpose:** Created a new user account named CyberStudent with a specified password.
   2. **Explanation:** The net user command with /add is used to create user accounts in CMD.
2. **net localgroup Administrators CyberStudent /add**
   1. **Purpose:** Added CyberStudent to the Administrators group to grant administrative privileges.
   2. **Explanation:** The net localgroup command manages group memberships, and /add adds the user to the specified group.
3. **net localgroup Administrators**
   1. **Purpose:** Displayed the members of the Administrators group to confirm CyberStudent's membership.
   2. **Explanation:** This command lists all current members, verifying changes.
4. **net user CyberStudent new\_password\_here**
   1. **Purpose:** Changed the password for CyberStudent.
   2. **Explanation:** This command lets you update passwords for existing accounts.
5. **echo CyberStudent password changed on %date% at %time% >> C:\CyberSecurity\Reports\user\_modifications.txt**
   1. **Purpose:** Logged the password change in a text file named user\_modifications.txt.
   2. **Explanation:** The echo command appends a timestamped note to document the change.

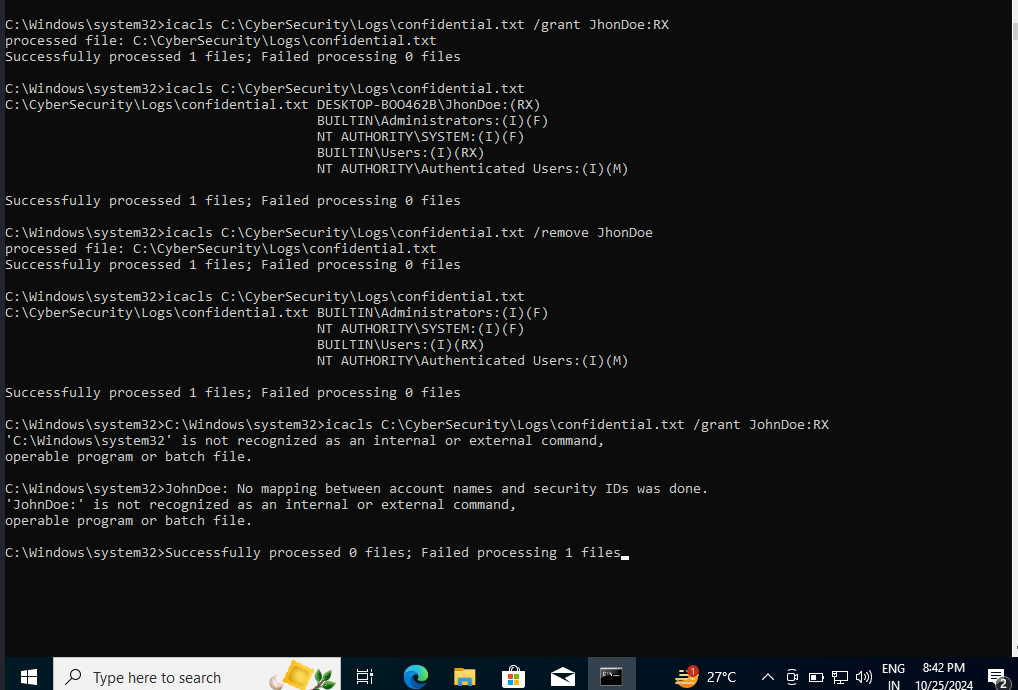
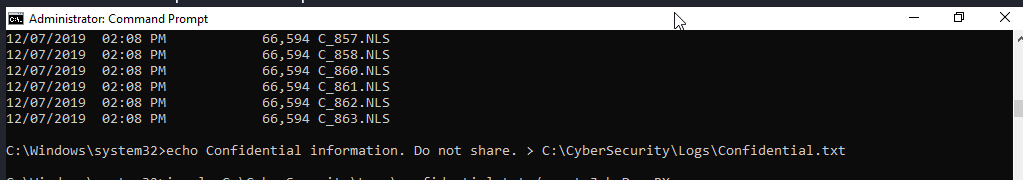
**Task 3.2: User and Group Cleanup:**

**Commands and Explanations:**

1. **net localgroup Administrators CyberStudent /delete**
   1. **Purpose:** Removed the CyberStudent account from the Administrators group.
   2. **Explanation:** This command revokes the administrative privileges of the user, effectively cleaning up group membership.
2. **net user CyberStudent /delete**
   1. **Purpose:** Deleted the CyberStudent user account from the system.
   2. **Explanation:** This command permanently removes the specified user account, completing the cleanup process.
3. **echo CyberStudent removed from Administrators group and account deleted on %date% at %time% >> C:\CyberSecurity\Reports\user\_modifications.txt**
   1. **Purpose:** Documented the cleanup actions in the user\_modifications.txt file.
   2. **Explanation:** The command appends a timestamped record of the actions taken, ensuring that there is a clear log of changes made.

## Part 4: File Permissions and Security :

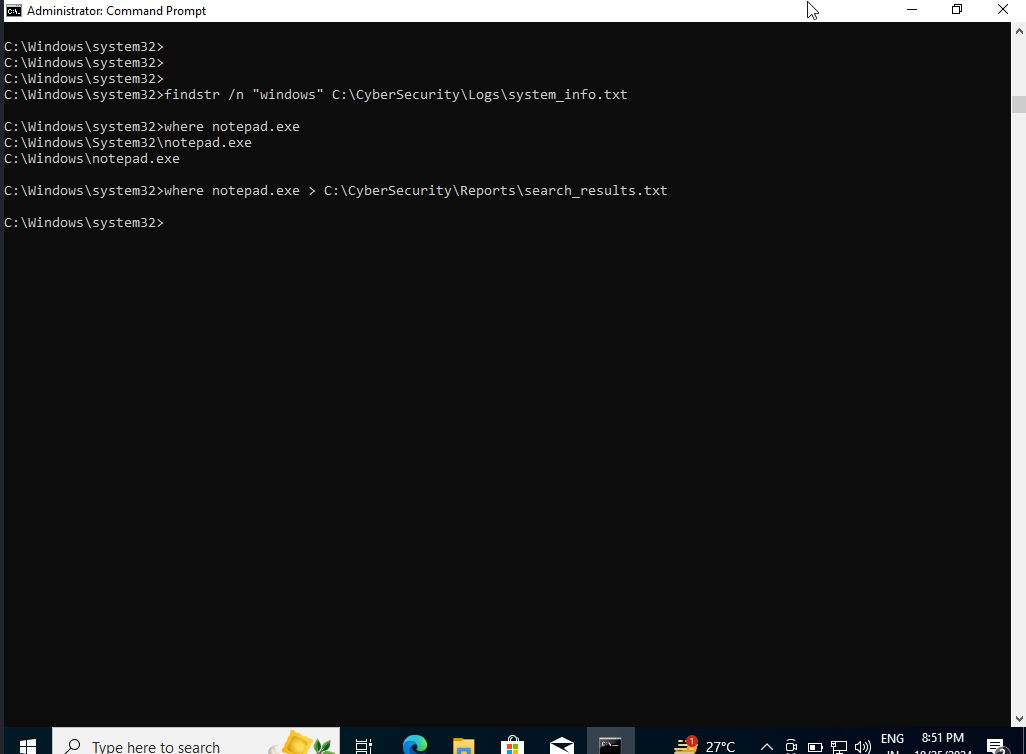
**Task 4.1: Permissions Handling with icacls:**

**Commands and Explanations:**

1. **net user JohnDoe your\_password /add**
   1. **Purpose:** Created the user JohnDoe, necessary for assigning permissions.
   2. **Explanation:** This command resolved the error related to mapping user account names by ensuring the user existed.
2. **icacls C:\CyberSecurity\Logs\confidential.txt /grant JohnDoe:RX**
   1. **Purpose:** Granted Read and Execute permissions on confidential.txt to JohnDoe.
   2. **Explanation:** The icacls command with /grant assigned specified permissions to the newly created user.
3. **icacls C:\CyberSecurity\Logs\confidential.txt**
   1. **Purpose:** Verified that JohnDoe had RX permissions on confidential.txt.
   2. **Explanation:** Displaying permissions confirmed that the task was completed successfully.

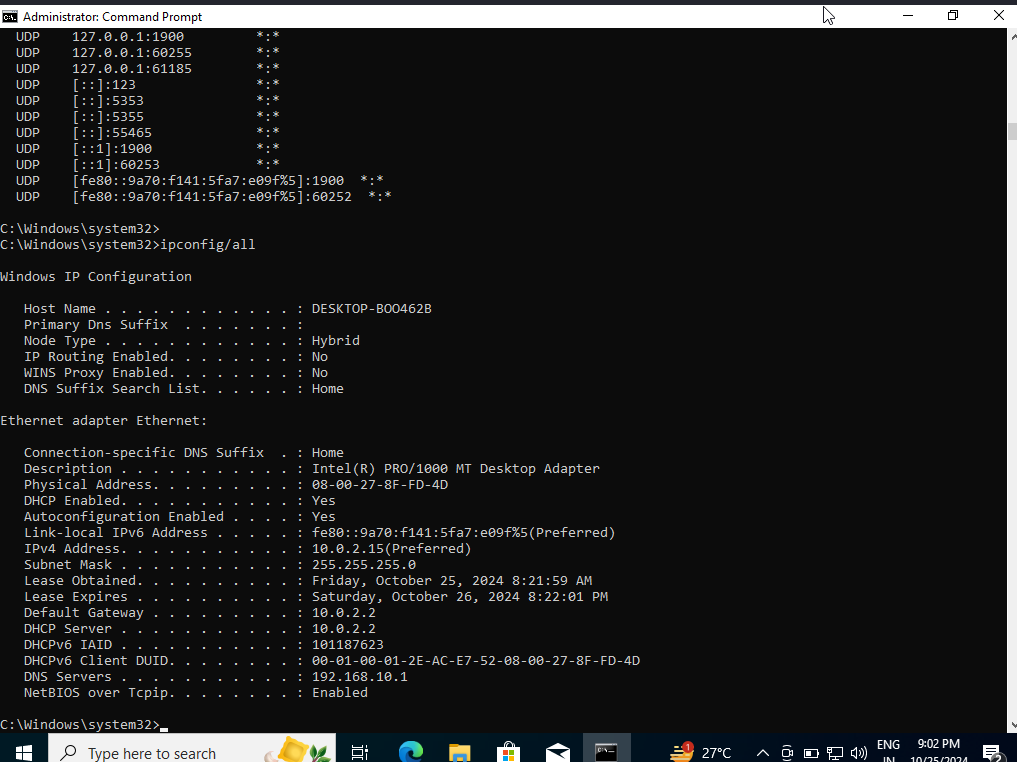
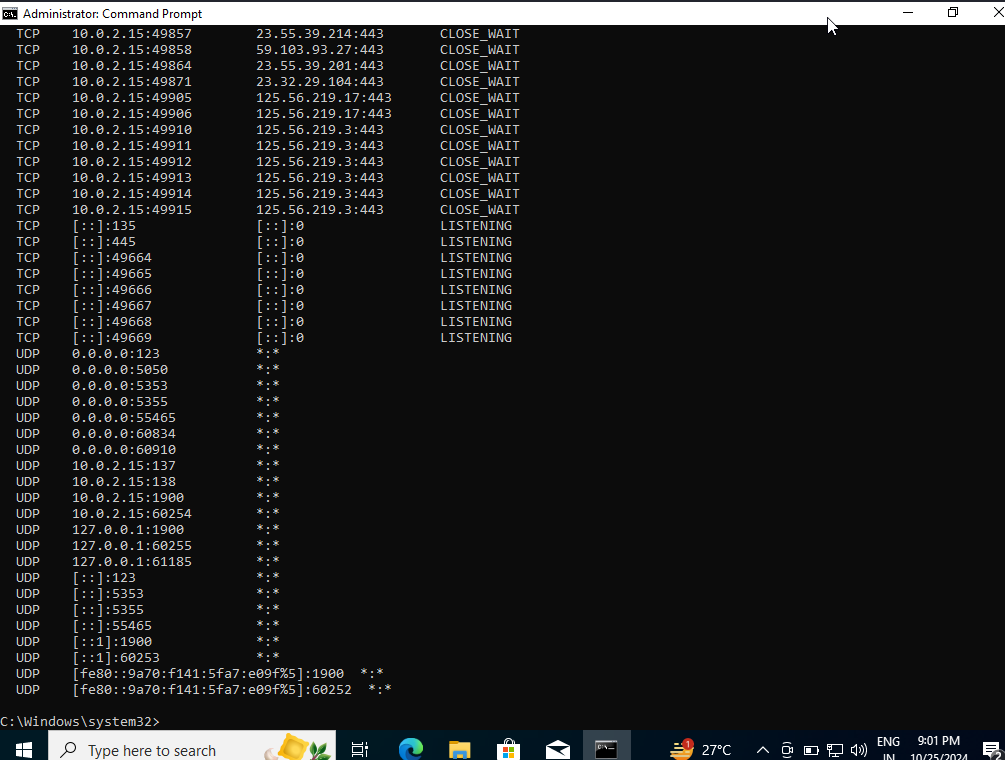
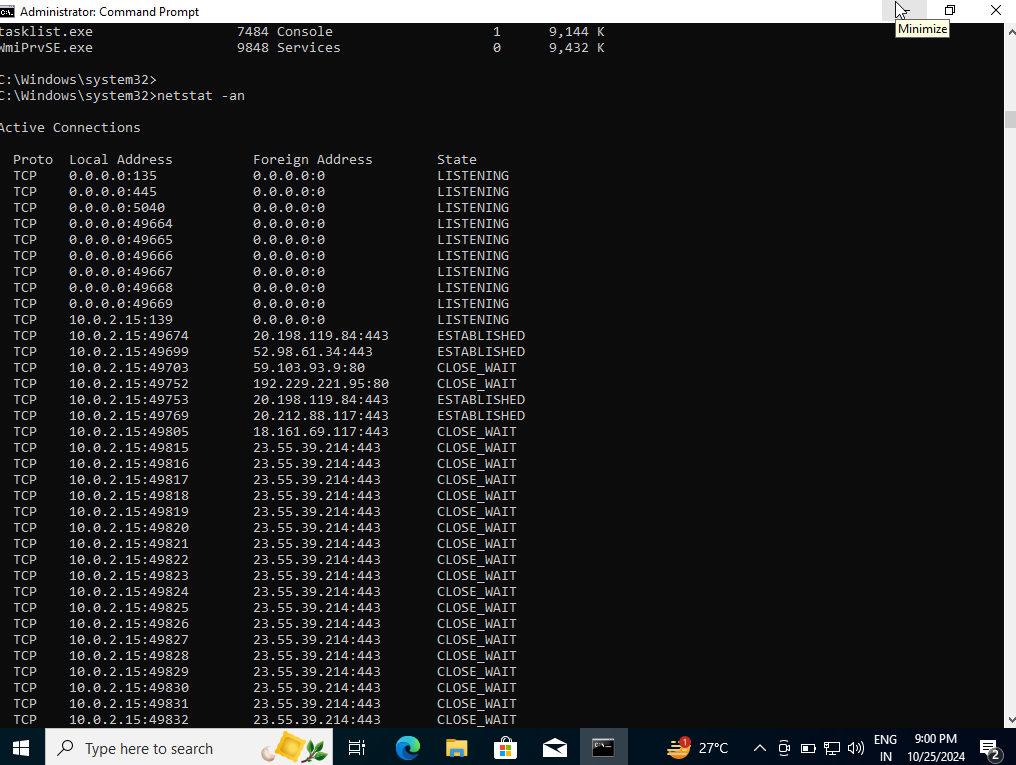
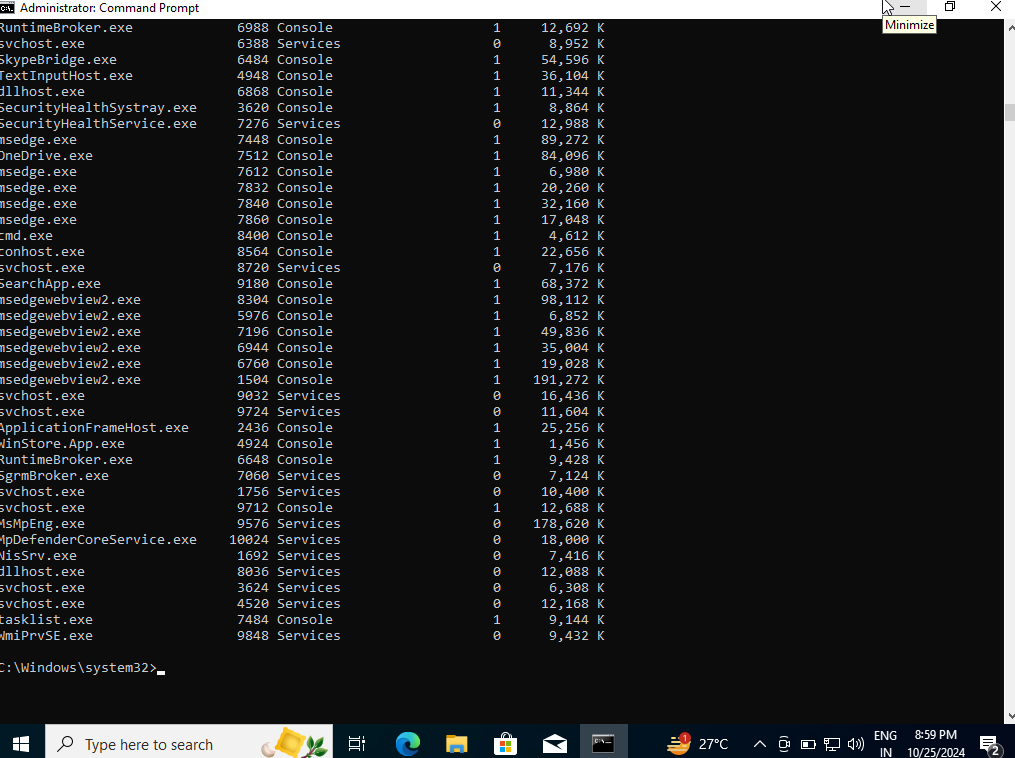
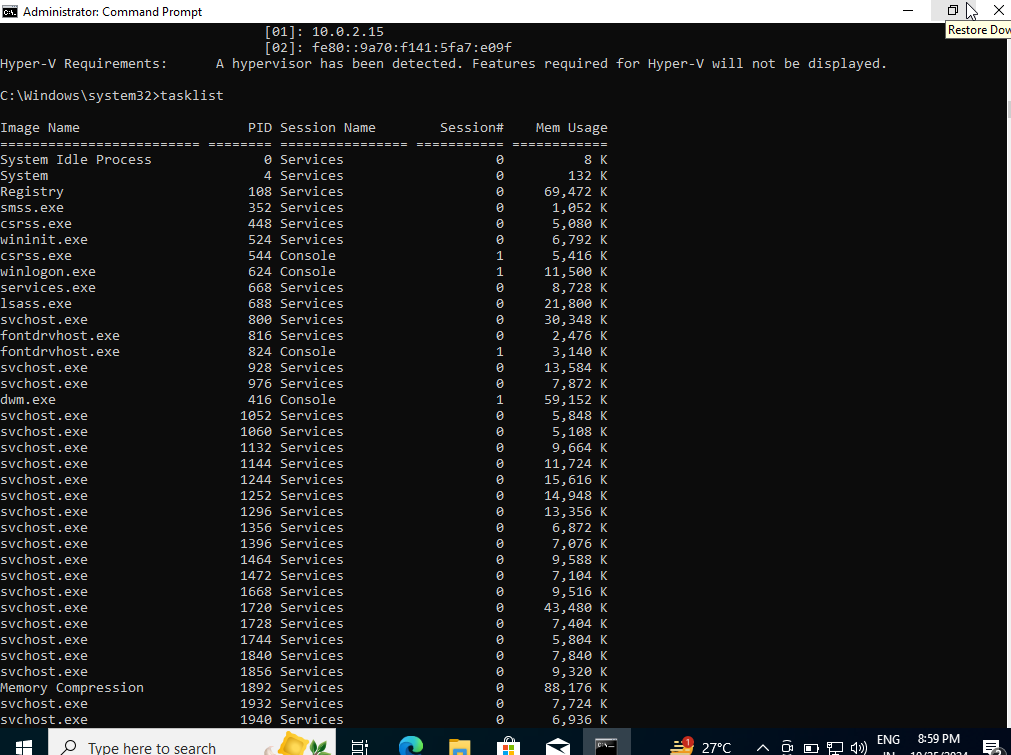
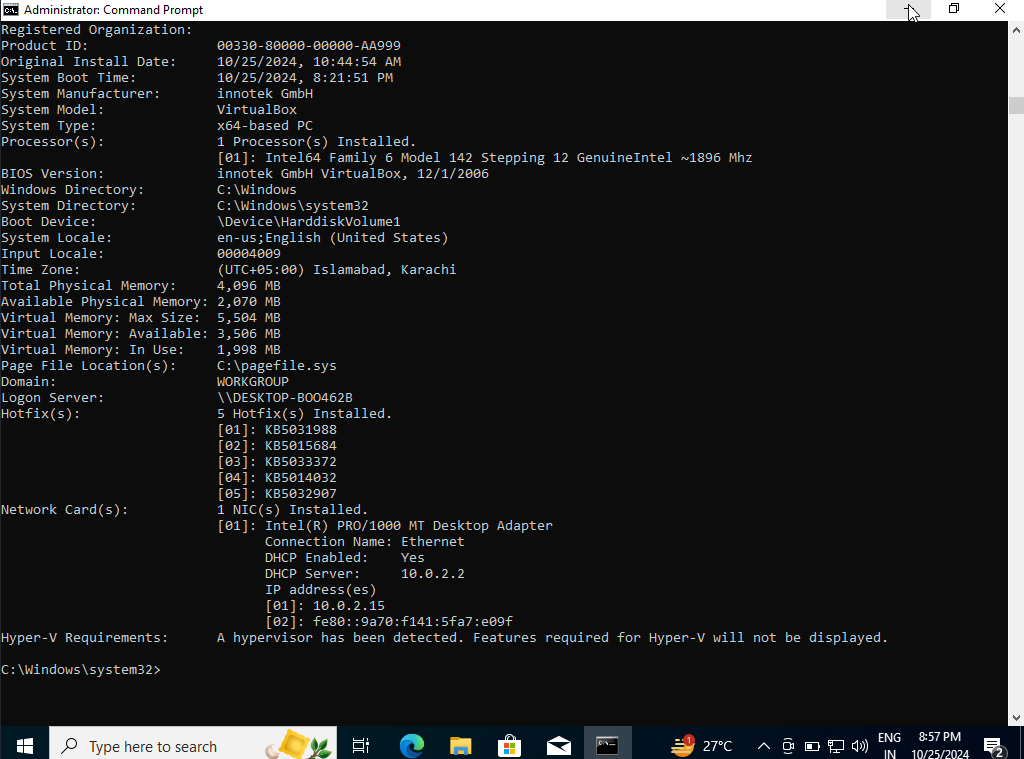
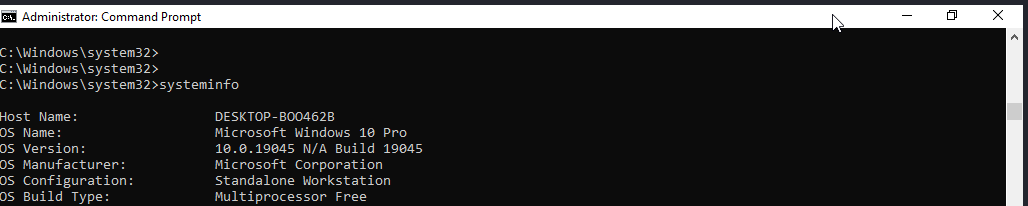
# Part 5: Advanced CMD Commands:

**Task 5.1: File and Content Search :**

**Commands and Explanations:**

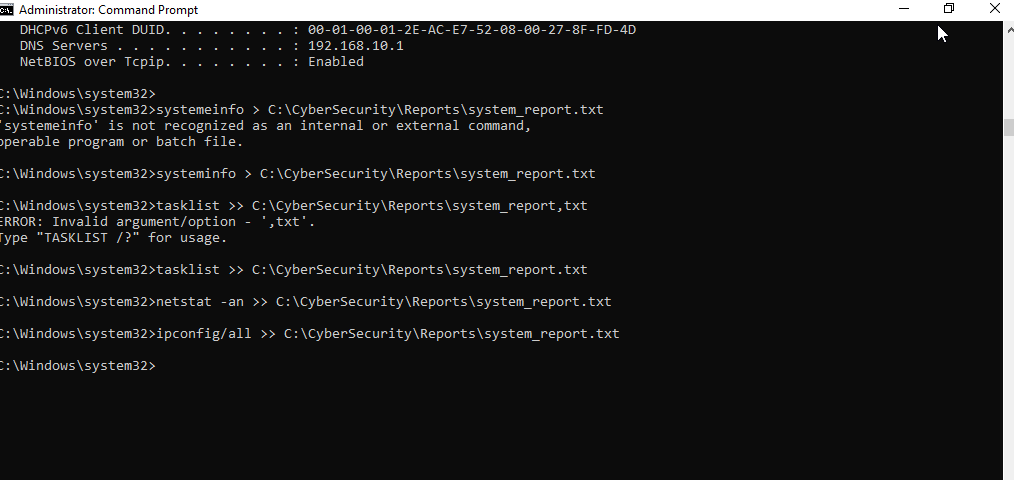
1. **findstr /n "Windows" C:\CyberSecurity\Logs\system\_info.txt**
   1. **Purpose:** Searched for the word "Windows" in system\_info.txt, displaying the line number where it appeared.
   2. **Explanation:** The findstr command with /n option shows each occurrence along with its line number, making it easy to locate specific information.
2. **where notepad.exe**
   1. **Purpose:** Located the path of the notepad.exe executable.
   2. **Explanation:** The where command finds the full path of executables in the system path, useful for identifying file locations.
3. **where notepad.exe > C:\CyberSecurity\Reports\search\_results.txt**
   1. **Purpose:** Saved the path of notepad.exe in search\_results.txt for documentation.
   2. **Explanation:** Redirecting output with > saved the path directly to the specified file, ensuring results were stored for future reference.

**Task 5.2: Gather System Information:**

**Commands and Explanations:**

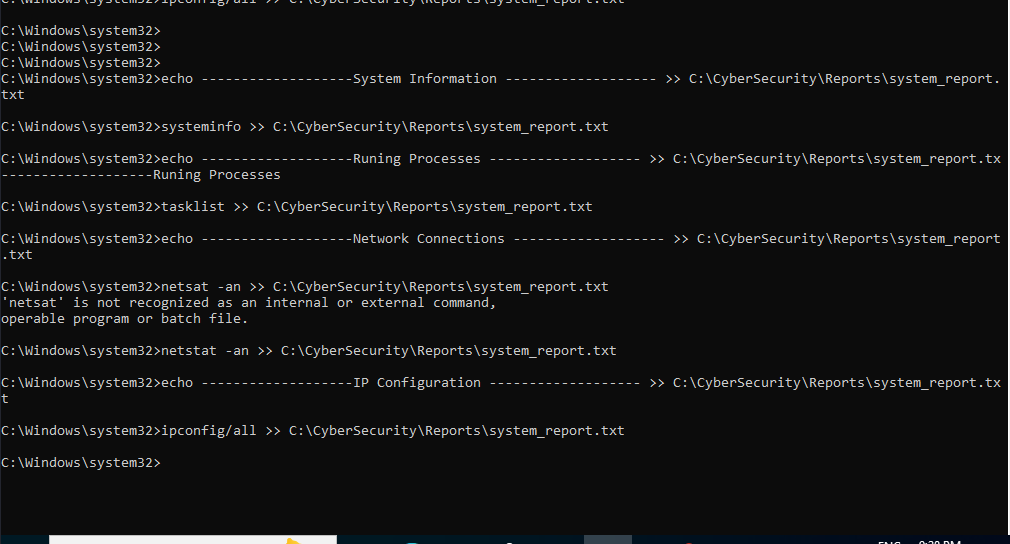
1. **systeminfo**
   1. **Purpose:** Displays detailed information about the system, including OS, manufacturer, model, and memory.
   2. **Explanation:** Helps understand the overall system specs and OS environment.
2. **tasklist**
   1. **Purpose:** Lists all currently running processes and their details, such as memory usage and process ID.
   2. **Explanation:** Useful for monitoring active tasks and managing system resources.
3. **netstat -an**
   1. **Purpose:** Shows all active network connections and listening ports.
   2. **Explanation:** Provides insight into network activity, helping diagnose network-related issues or security concerns.
4. **ipconfig /all**
   1. **Purpose:** Displays detailed IP configuration for all network adapters, including IP addresses and DNS information.
   2. **Explanation:** Useful for troubleshooting network configurations and viewing complete adapter details.

**Task 5.3: Create a System Report:**

**Commands and Explanations:**

1. **systeminfo > C:\CyberSecurity\Reports\system\_report.txt**
   1. **Purpose:** Captures detailed system specifications and saves them to system\_report.txt.
   2. **Explanation:** The > operator creates the file and saves systeminfo output as the first entry in the report.
2. **tasklist >> C:\CyberSecurity\Reports\system\_report.txt**
   1. **Purpose:** Appends a list of active processes to system\_report.txt.
   2. **Explanation:** The >> operator appends without overwriting, so tasklist results follow the systeminfo output.
3. **netstat -an >> C:\CyberSecurity\Reports\system\_report.txt**
   1. **Purpose:** Adds network connection data to the report file.
   2. **Explanation:** Continuing to use >>, netstat output is appended to document network activity.
4. **ipconfig /all >> C:\CyberSecurity\Reports\system\_report.txt**
   1. **Purpose:** Appends IP configuration information to the report.
   2. **Explanation:** Appending ipconfig details completes the comprehensive system report.

**Task 5.4: Organize the Report:**



## **Commands and Explanations:**

* Command: echo ------------------- System Information ------------------- >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Appends a header to denote the start of the system information section.

Explanation: The echo command outputs a line of text, helping to distinguish this section in the report.

* Command: systeminfo >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Appends detailed system information to the report.

Explanation: Captures important specifications about the computer.

* Command: echo ------------------- Running Processes ------------------- >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Marks the section for running processes.

Explanation: Clearly labels the upcoming data for easier navigation.

* Command: tasklist >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Appends a list of currently running processes.

Explanation: Provides details about active tasks on the system.

* Command: echo ------------------- Network Connections ------------------- >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Introduces the section displaying network connection data.

Explanation: Helps organize the output for easy identification.

* Command: netstat -an >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Appends the current network connections and listening ports.

Explanation: Valuable for monitoring network activity.

* Command: echo ------------------- IP Configuration ------------------- >> C:\CyberSecurity\Reports\system\_report.txt

Purpose: Designates the section for IP configuration details.

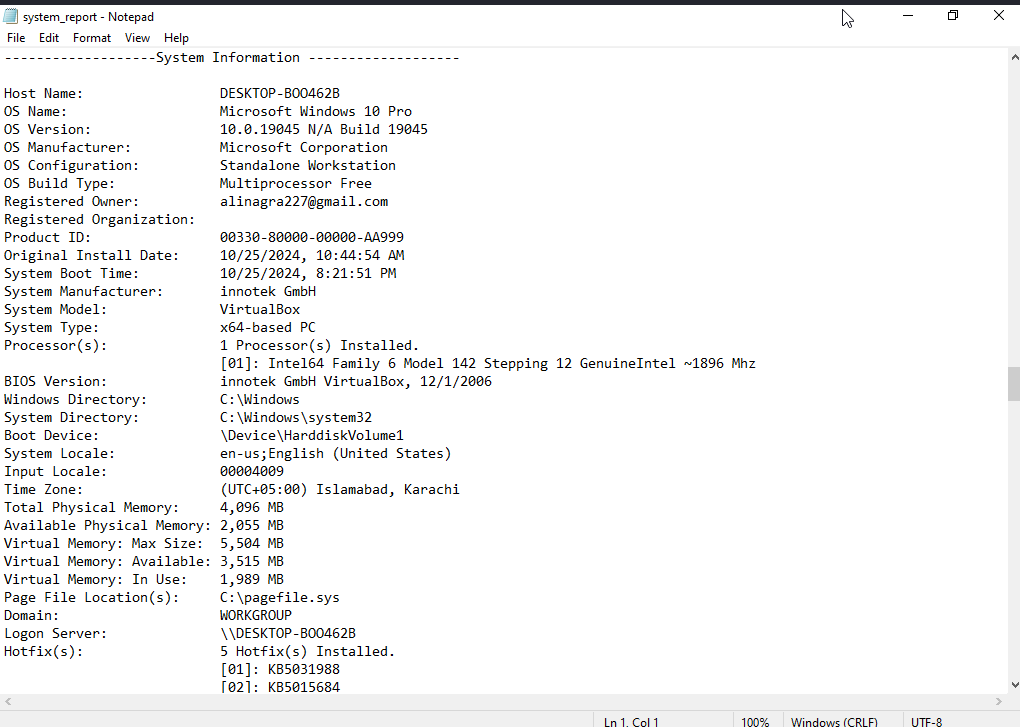
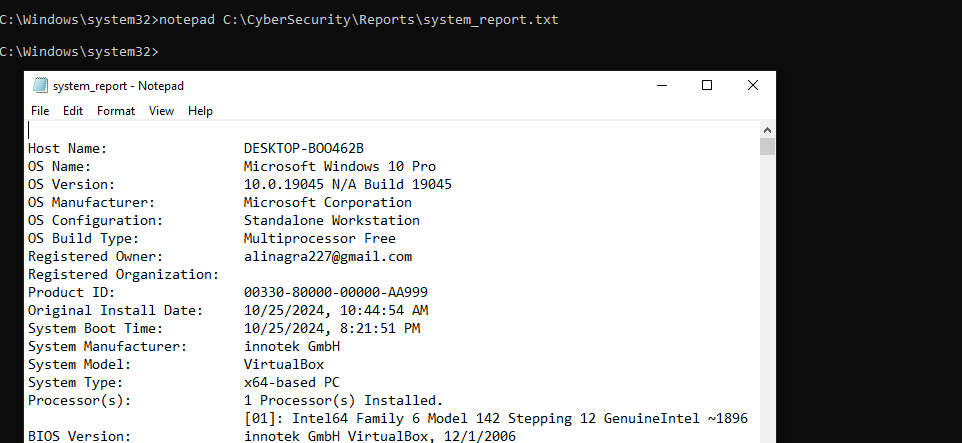
Explanation: Improves clarity and organization in the report.

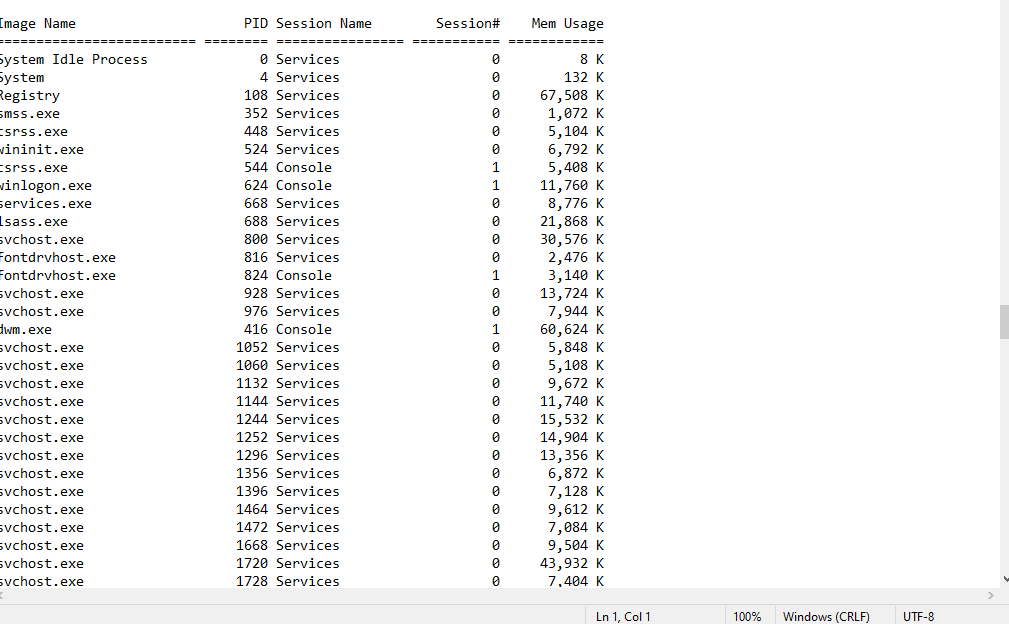
* Command: ipconfig /all >> C:\CyberSecurity\Reports\system\_report.txt

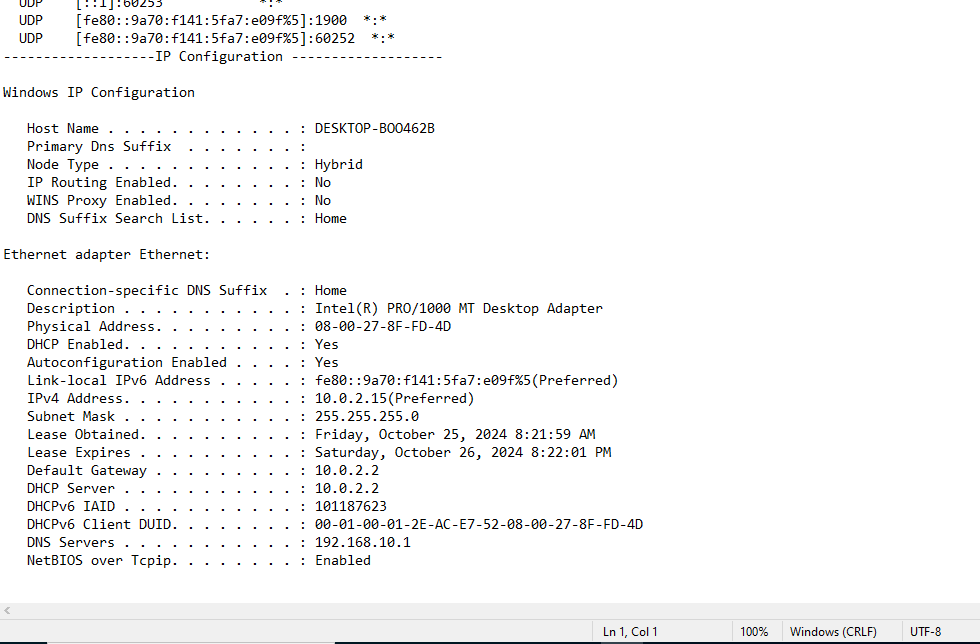
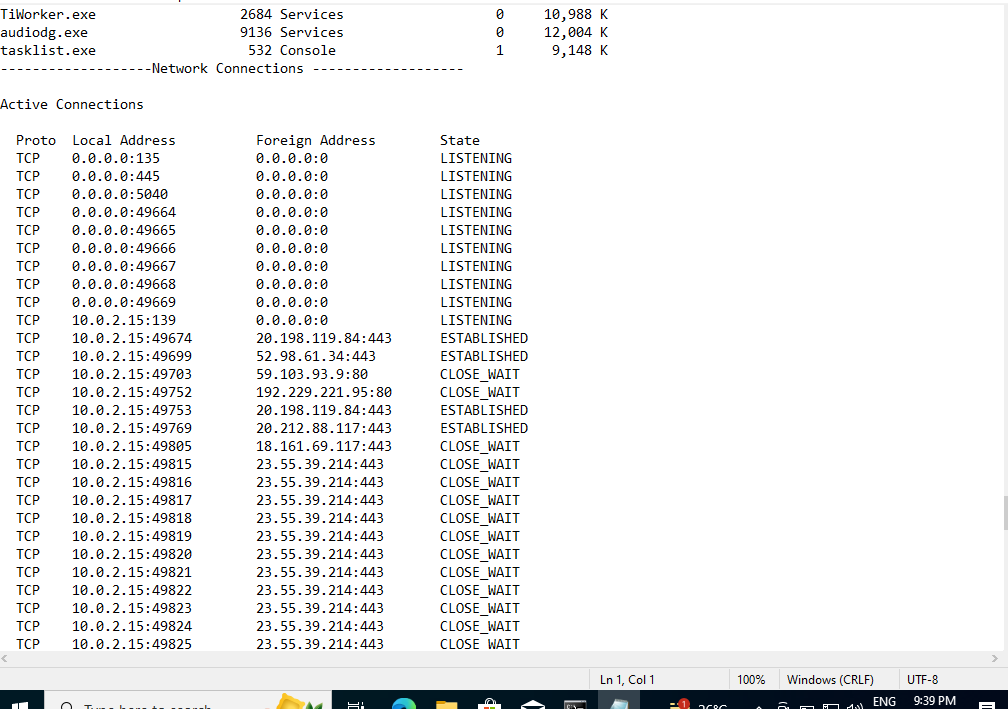
Purpose: Appends detailed IP configuration information.

Explanation: Completes the report with crucial network settings.

**Task 5.5: Review the Report :**





**Open the File in Notepad:**

* **Command:**

**notepad C:\CyberSecurity\Reports\system\_report.txt**

* 1. **Purpose:** Launches Notepad to view the contents of system\_report.txt.
  2. **Explanation:** This command opens the specified file in Notepad, allowing you to visually inspect the report.

1. **Review the Contents:**
   1. **What to Check:**
      1. Ensure each section is clearly separated with the appropriate headers.
      2. Verify that the outputs from systeminfo, tasklist, netstat -an, and ipconfig /all are present and complete.
      3. Look for any formatting issues or missing information that may need correction.
2. **Close Notepad:**
   1. After reviewing, simply close the Notepad application once you have completed your inspection.

### Brief Explanation of Task

In this task, the objective is to validate the contents of system\_report.txt by opening it in a text editor. The review process involves checking for accuracy in the captured data from various system commands, ensuring proper organization, and confirming that all relevant information is included. This step is crucial to maintain the integrity of the report, which serves as a reference for system specifications, active processes, network connections, and IP configurations.