Lab 4: Clear Logs to Hide the Evidence of Compromise

**Lab Scenario**

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester’s last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable,or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This lab will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

**Lab Objectives**

* View, enable, and clear audit policies using Auditpol
* Clear Windows machine logs using various utilities
* Clear Linux machine logs using the BASH shell
* Clear Windows machine logs using CCleaner

**Overview of Clearing Logs**

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

* **Disable Auditing**: Disable the auditing features of the target system
* **Clearing Logs**: Clears and deletes the system log entries corresponding to security compromise activities
* **Manipulating Logs**: Manipulate logs in such a way that an intruder will not be caught in illegal actions
* **Covering Tracks on the Network**: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
* **Covering Tracks on the OS**: Use NTFS streams to hide and cover malicious files in the target system
* **Deleting Files**: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
* **Disabling Windows Functionality**: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

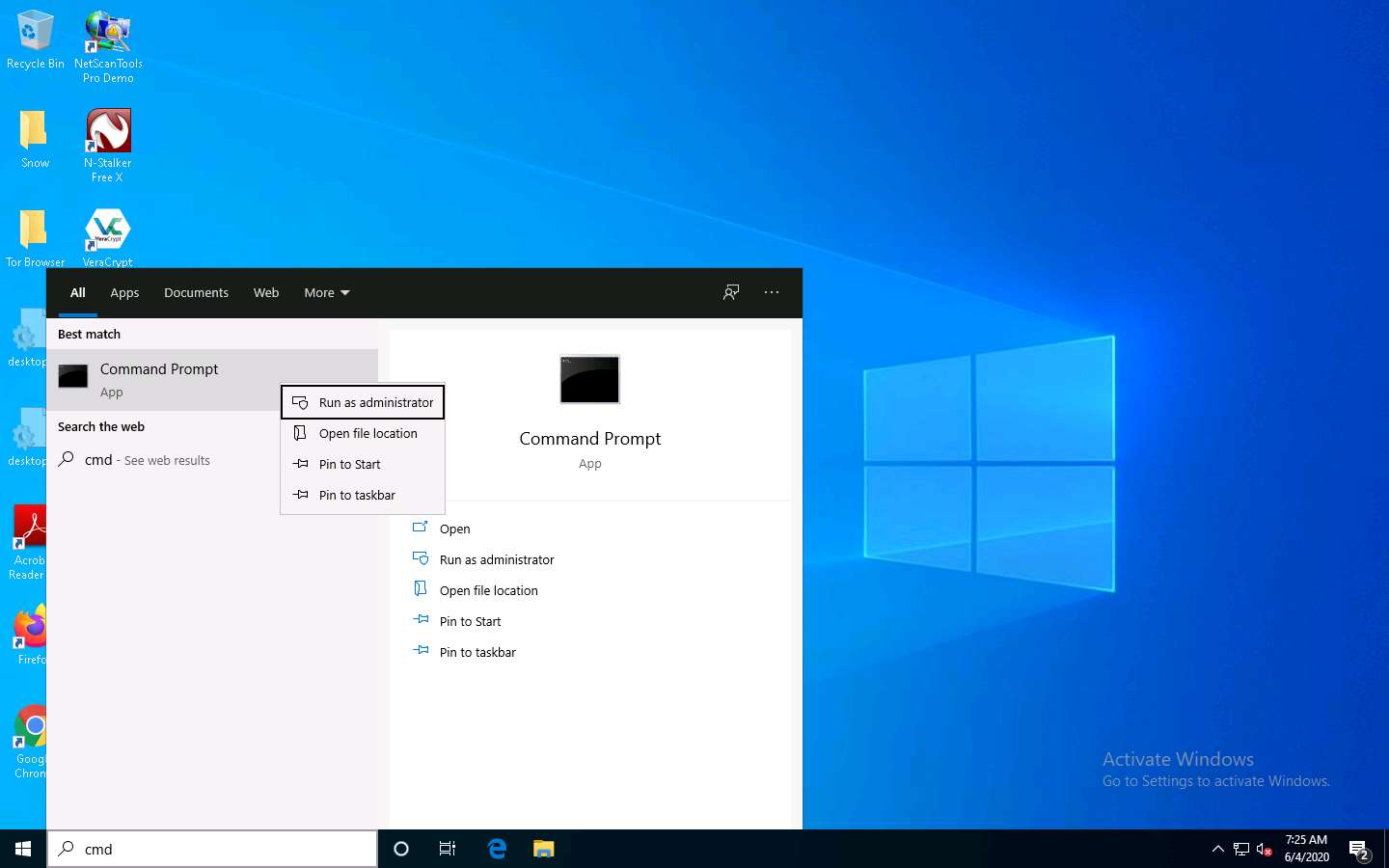
Task 1: View, Enable, and Clear Audit Policies using Auditpol

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

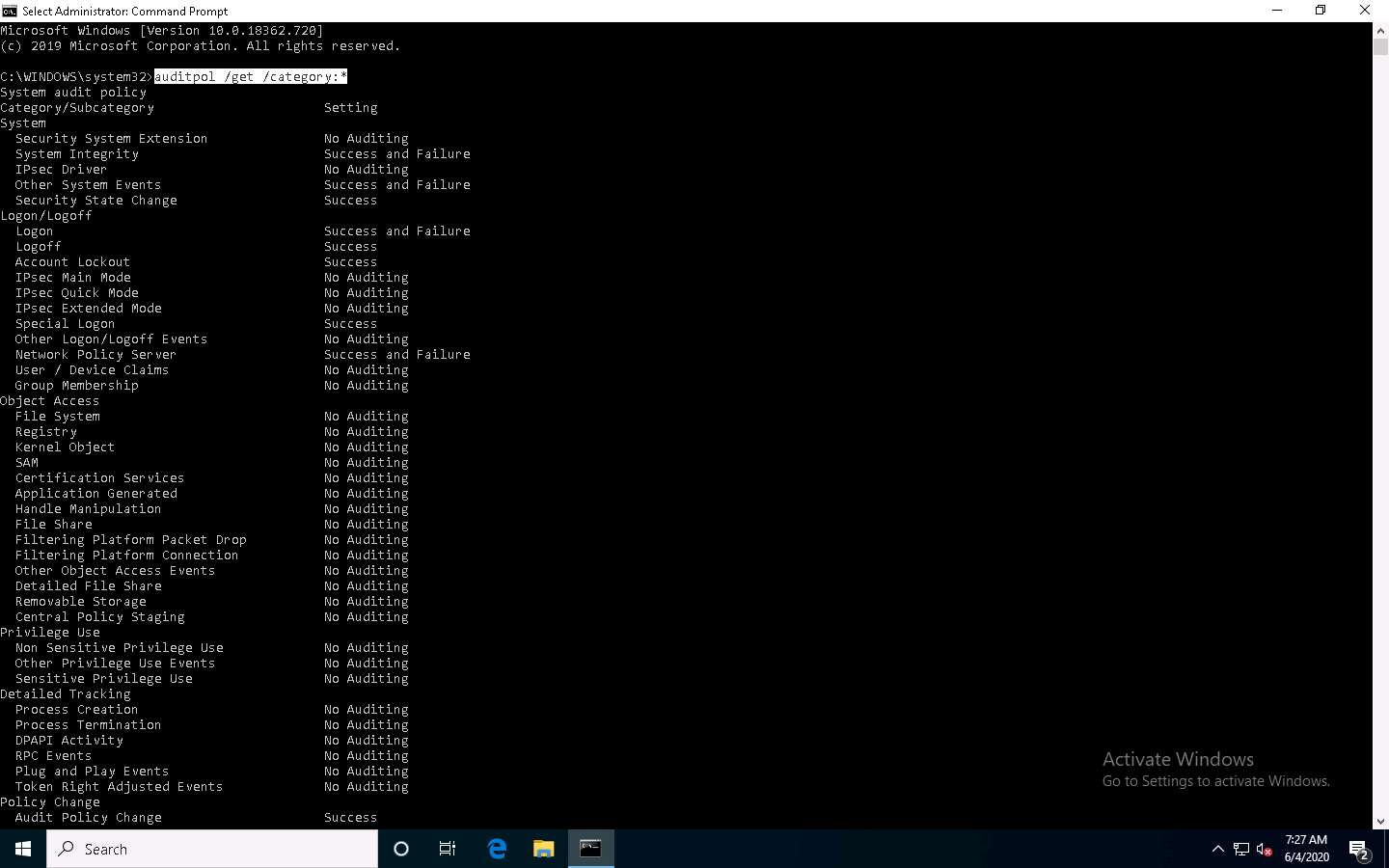
In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

Here, we will use Auditpol to view, enable, and clear audit policies.

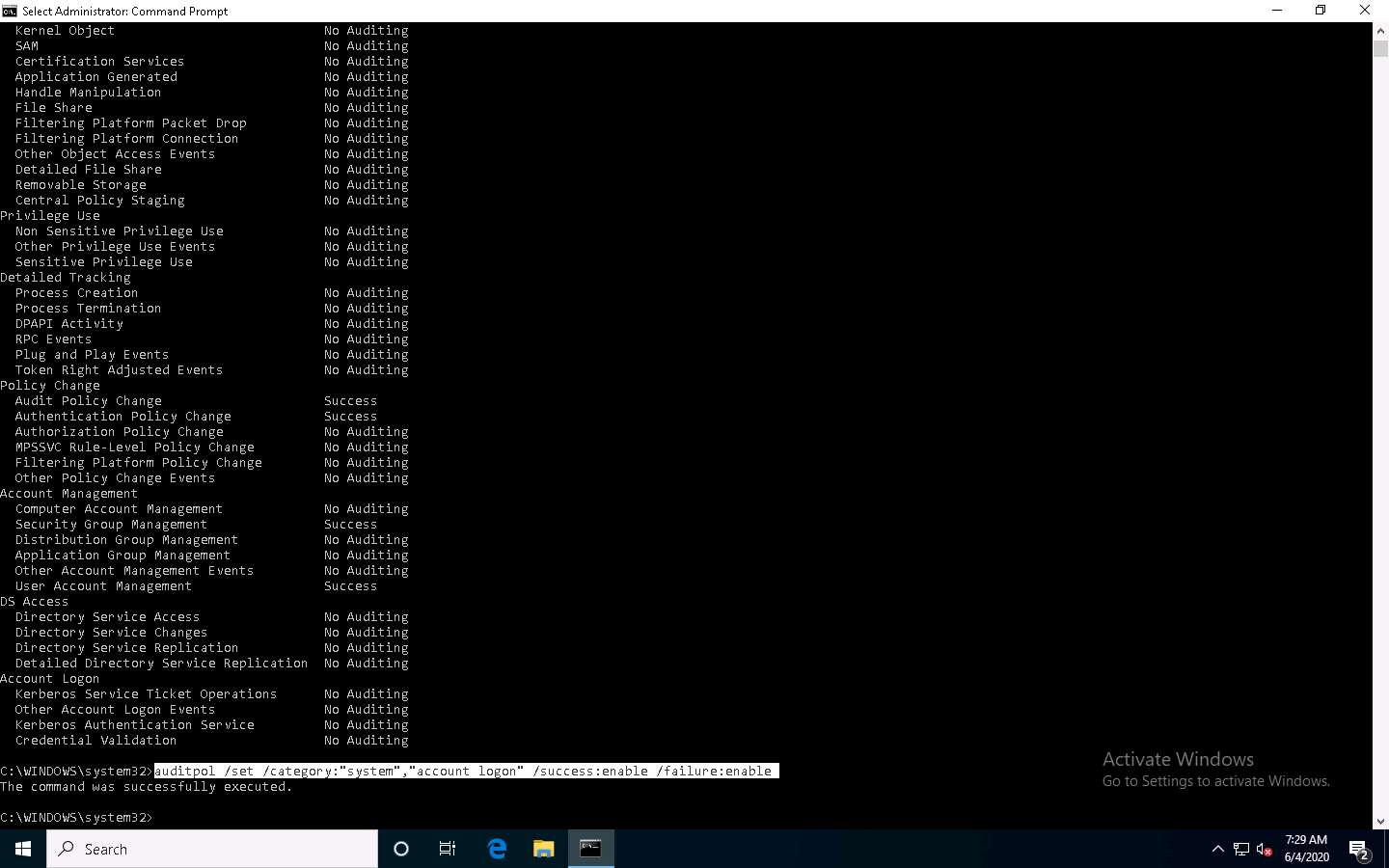
1. Click [Windows 10](https://labclient.labondemand.com/Instructions/9b2812b4-0c87-4fbc-be85-97032f9e7824?rc=10) to switch to the **Windows 10** machine.
2. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
3. The **User Account Control** pop-up appears; click **Yes**.



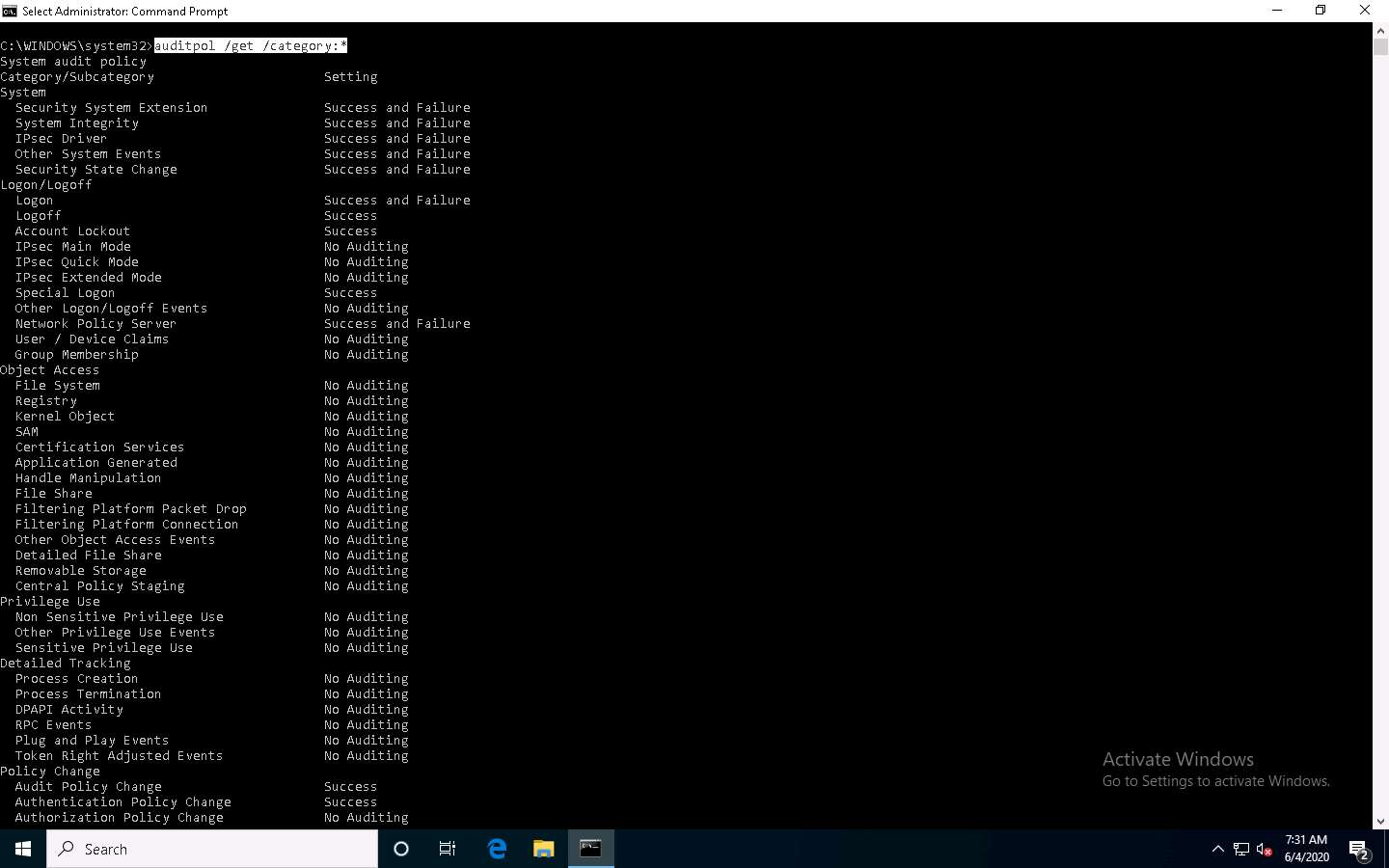
1. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:\*** and press **Enter** to view all the audit policies.



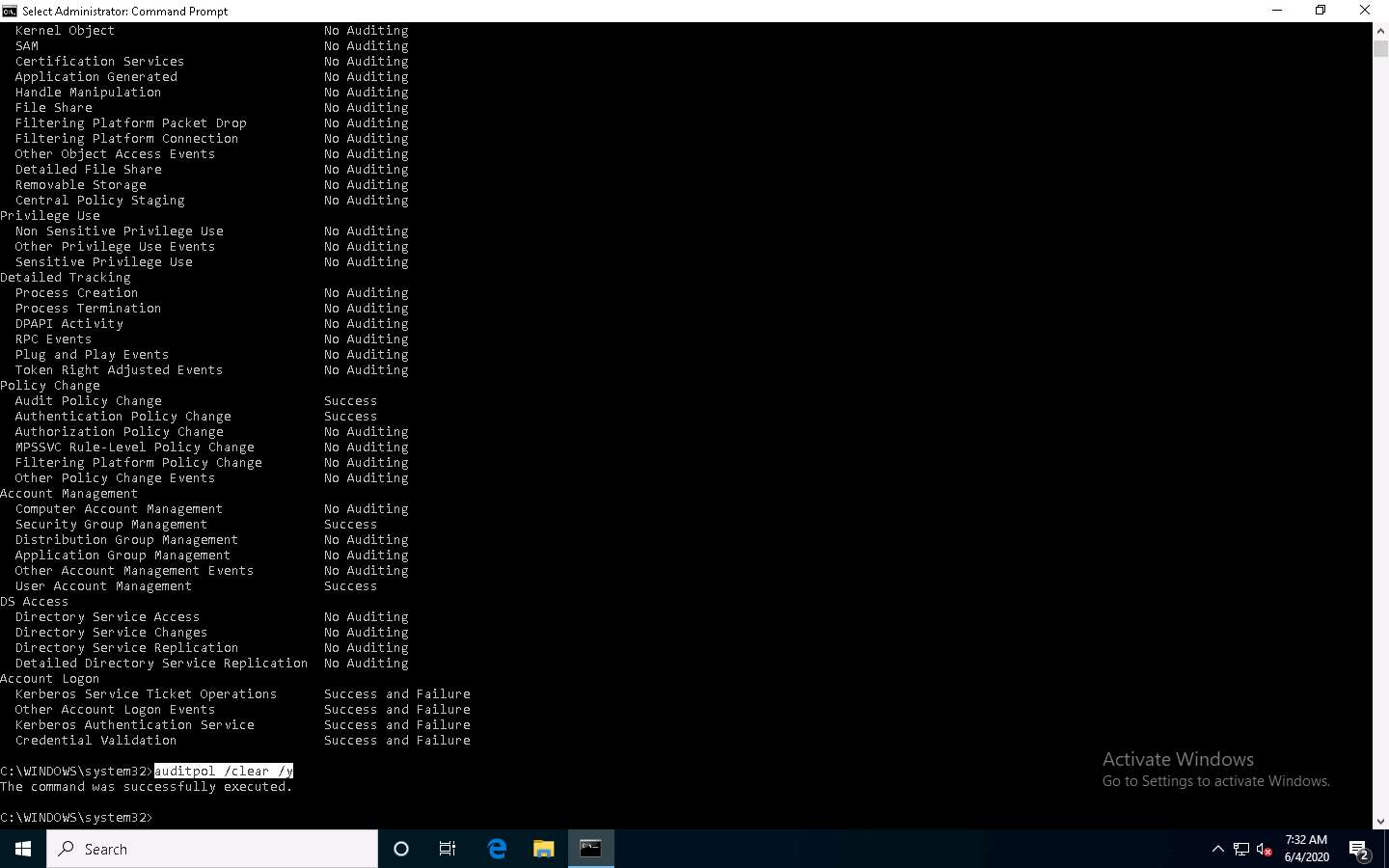
1. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.



1. Type **auditpol /get /category:\*** and press **Enter** to check whether the audit policies are enabled.



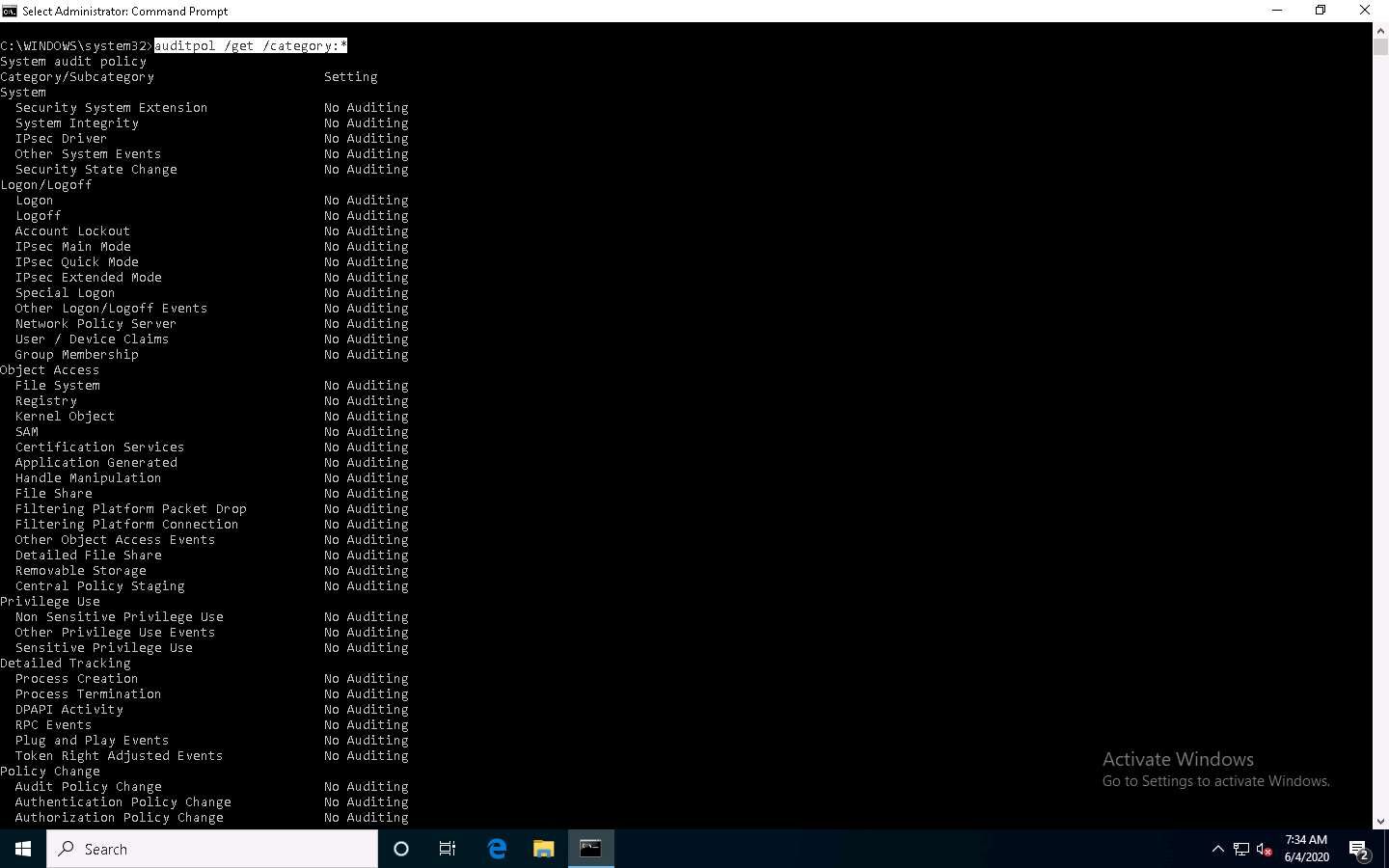
1. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.



1. Type **auditpol /get /category:\*** and press **Enter** to check whether the audit policies are cleared.

**No Auditing** indicates that the system is not logging audit policies.

For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.



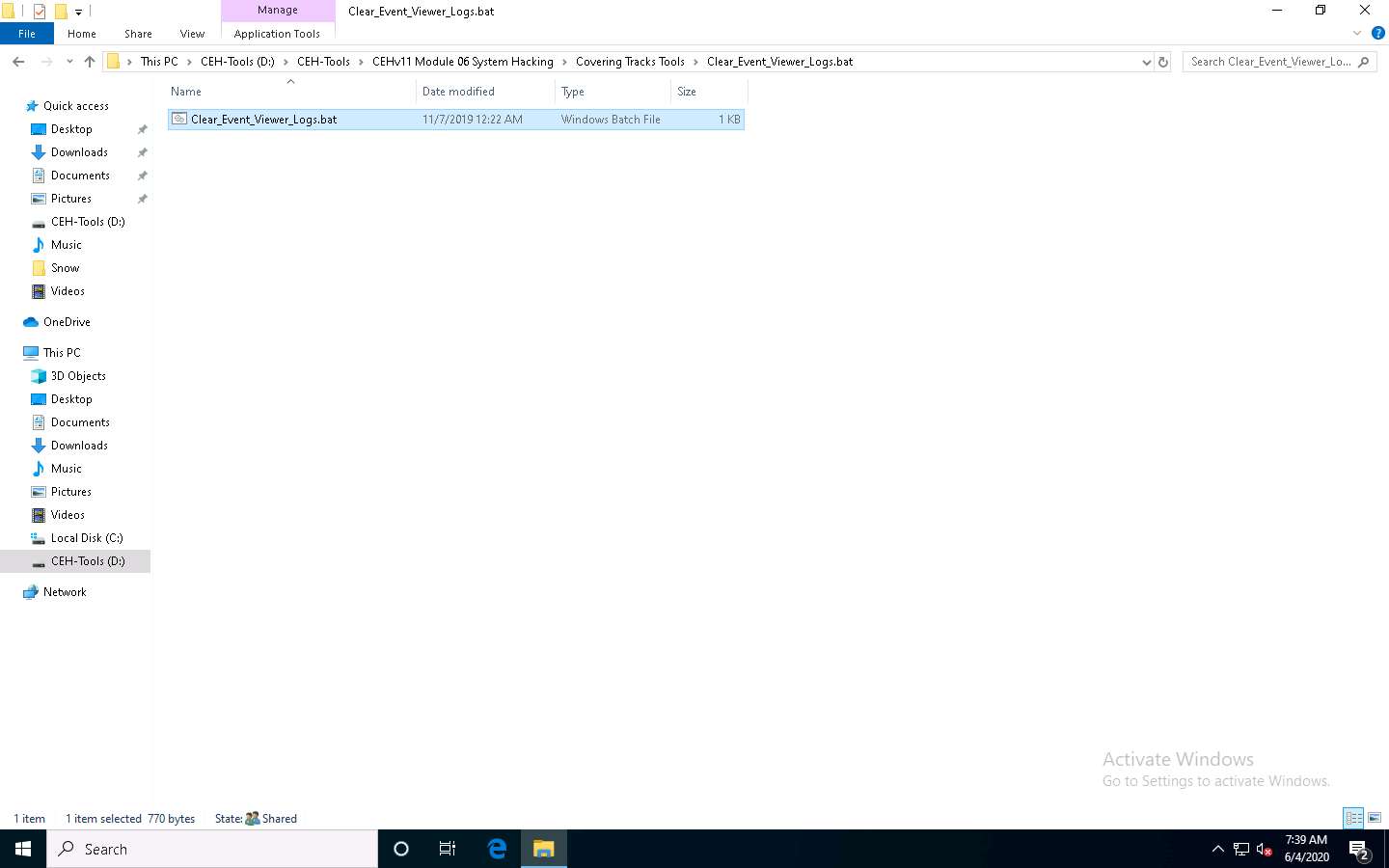
1. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
2. Close all open windows and document all the acquired information.

Task 2: Clear Windows Machine Logs using Various Utilities

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

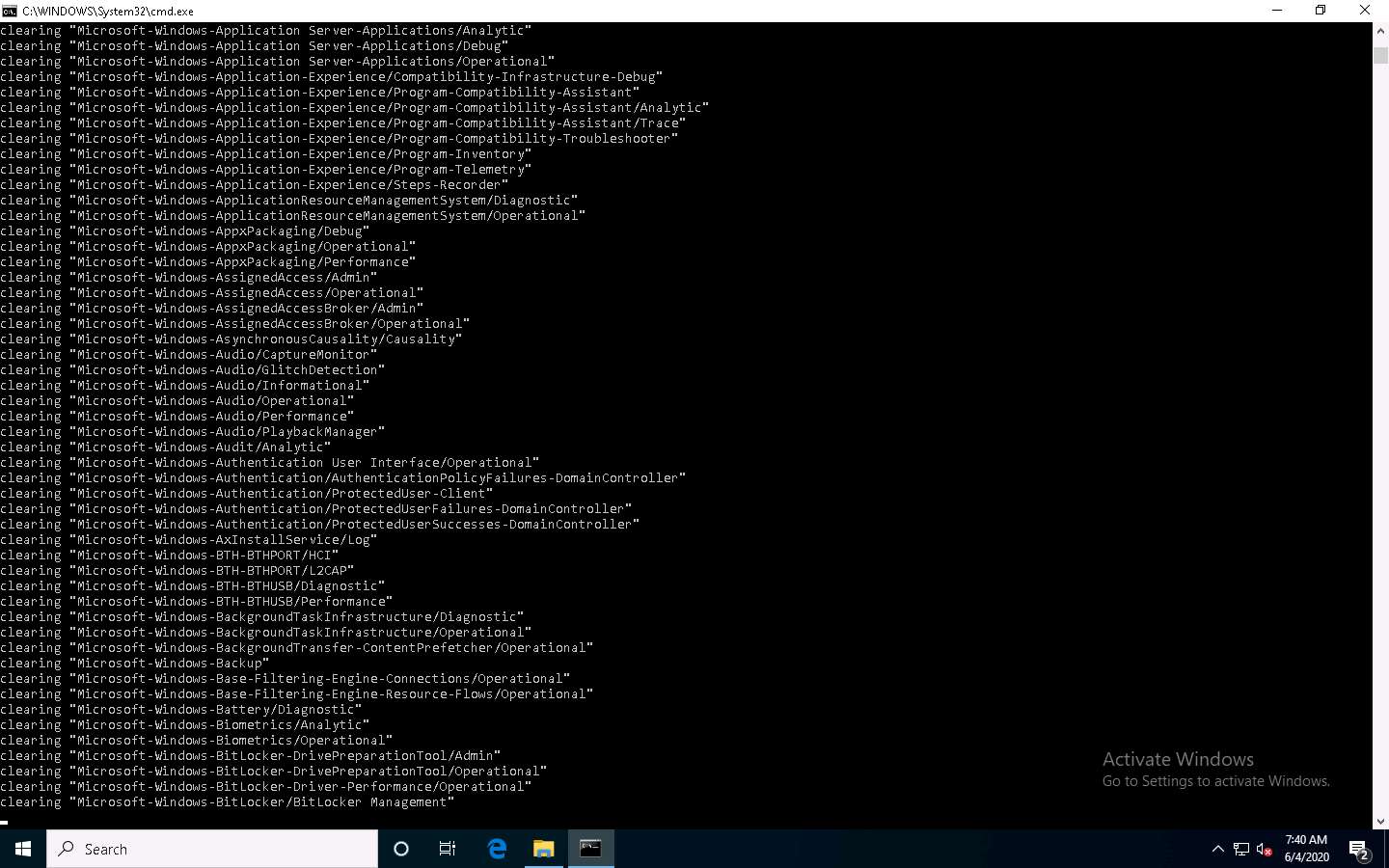
There are various Windows utilities that can be used to clear system logs such as Clear\_Event\_Viewer\_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

1. In the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear\_Event\_Viewer\_Logs.bat**. Right-click **Clear\_Event\_Viewer\_Logs.bat** and click **Run as administrator**.



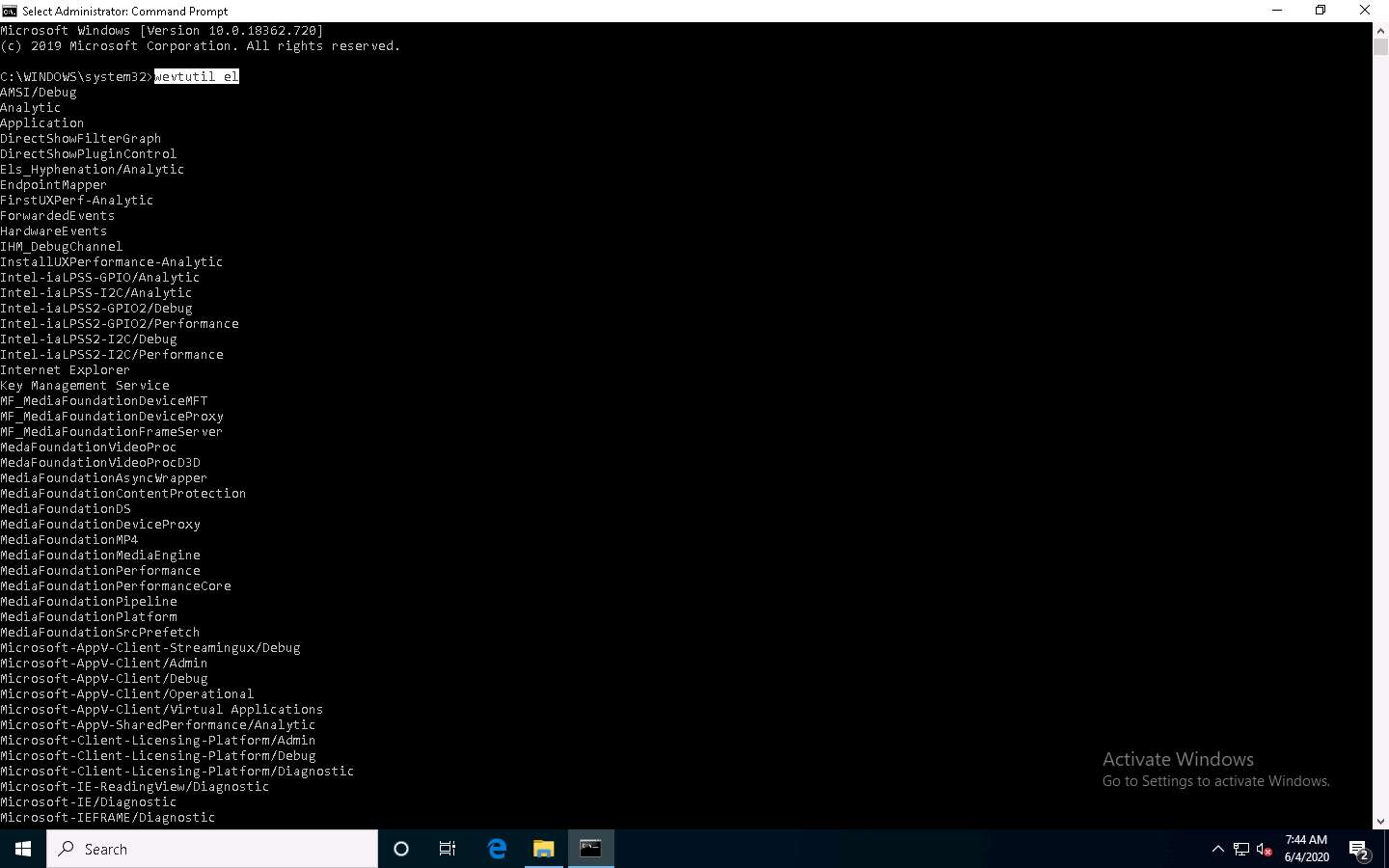
1. The **User Account Control** pop-up appears; click **Yes**.
2. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

Clear\_Event\_Viewer\_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.



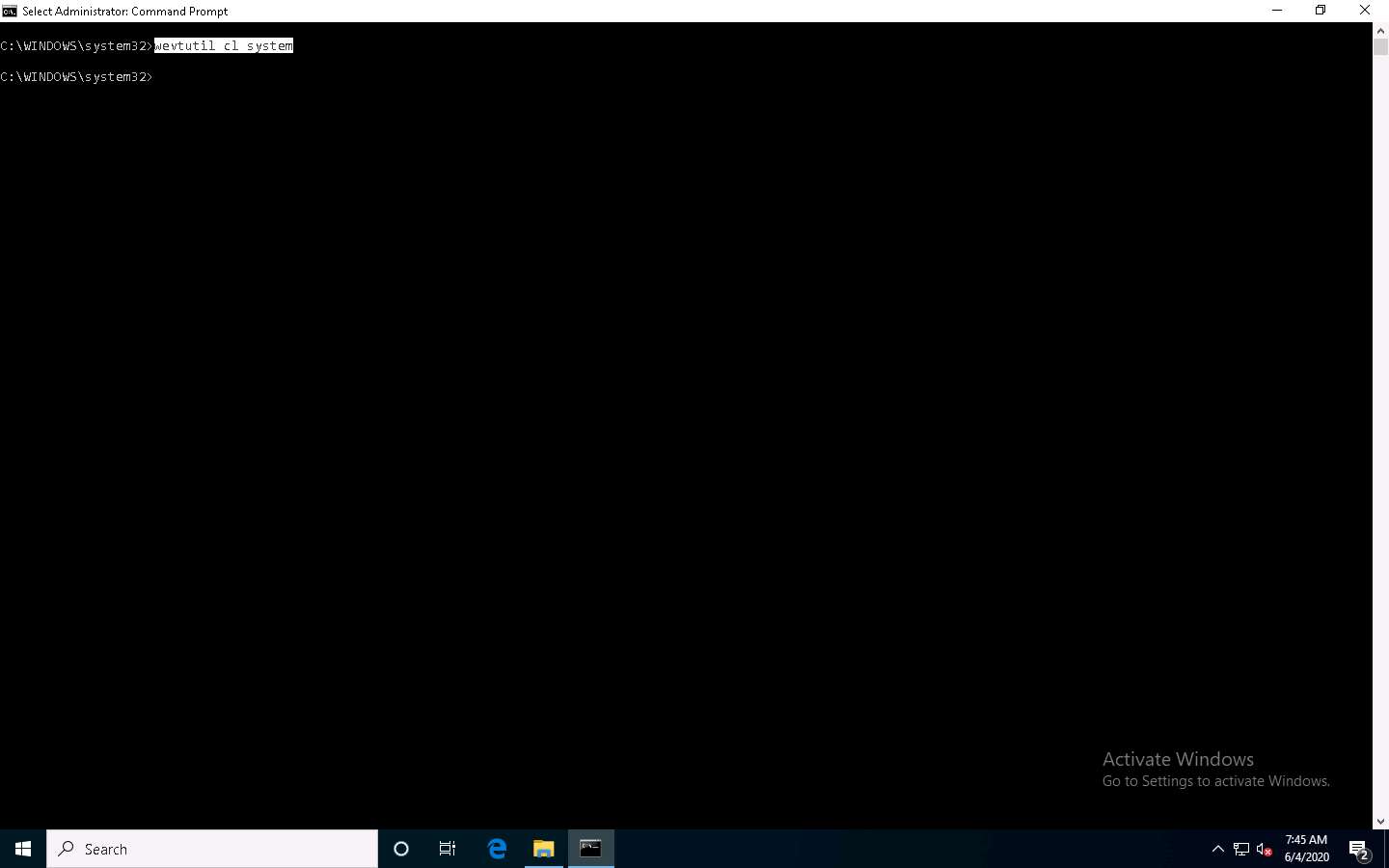
1. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

**el | enum-logs** lists event log names.



1. Now, type **wevtutil cl [log\_name]** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

**cl | clear-log**: clears a log, **log\_name** is the name of the log to clear, and ex: is the system, application, and security.



1. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application, security**).

wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

1. In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to deleted files in a specific drive, folder, or file.

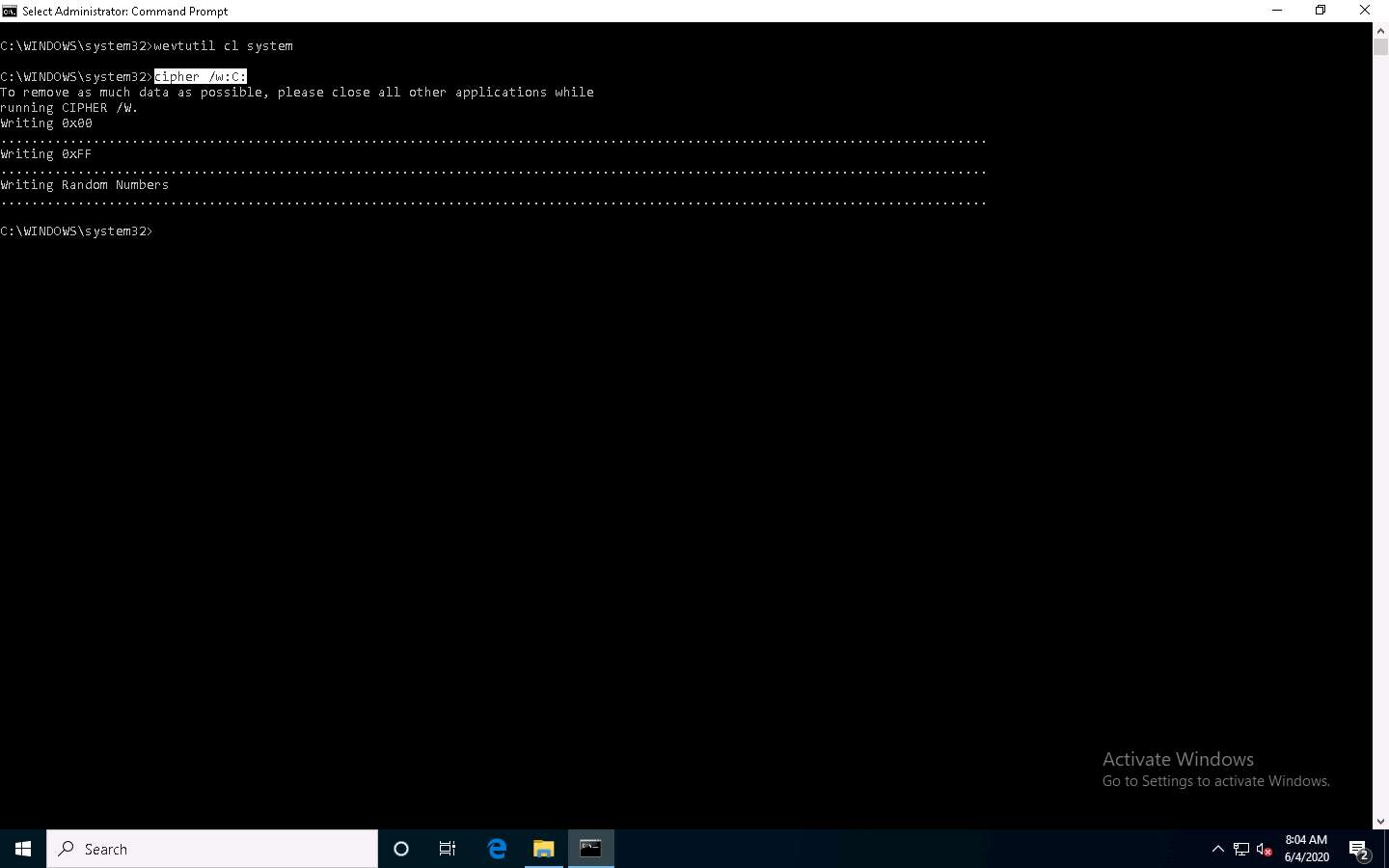
Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

1. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

[more...](https://labclient.labondemand.com/Instructions/9b2812b4-0c87-4fbc-be85-97032f9e7824?rc=10)



1. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear\_Event\_Viewer\_Logs.bat, wevtutil, and Cipher).
2. Close all open windows and document all the acquired information.

Task 3: Clear Linux Machine Logs using the BASH Shell

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the more ~/.bash\_history command. This feature of BASH is a problem for hackers, as investigators could use the bash\_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Here, we will clear the Linux machine event logs using the BASH shell.

1. Click [Parrot Security](https://labclient.labondemand.com/Instructions/9b2812b4-0c87-4fbc-be85-97032f9e7824?rc=10) to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Background pattern

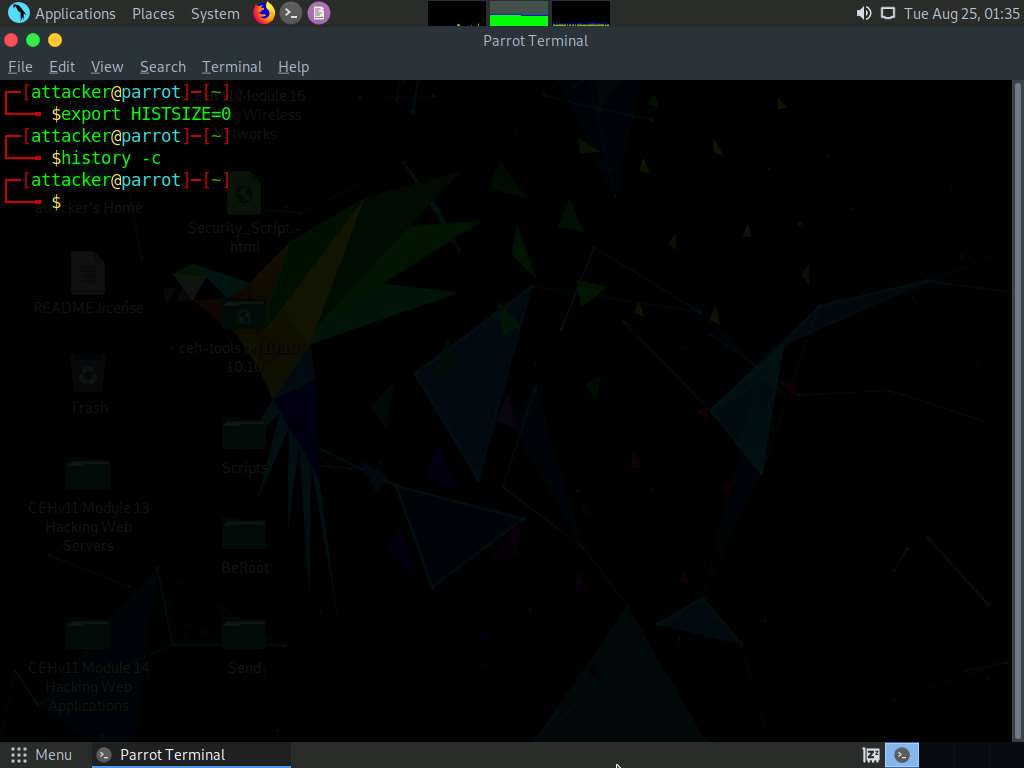
Description automatically generated with medium confidence

1. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

**HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

1. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

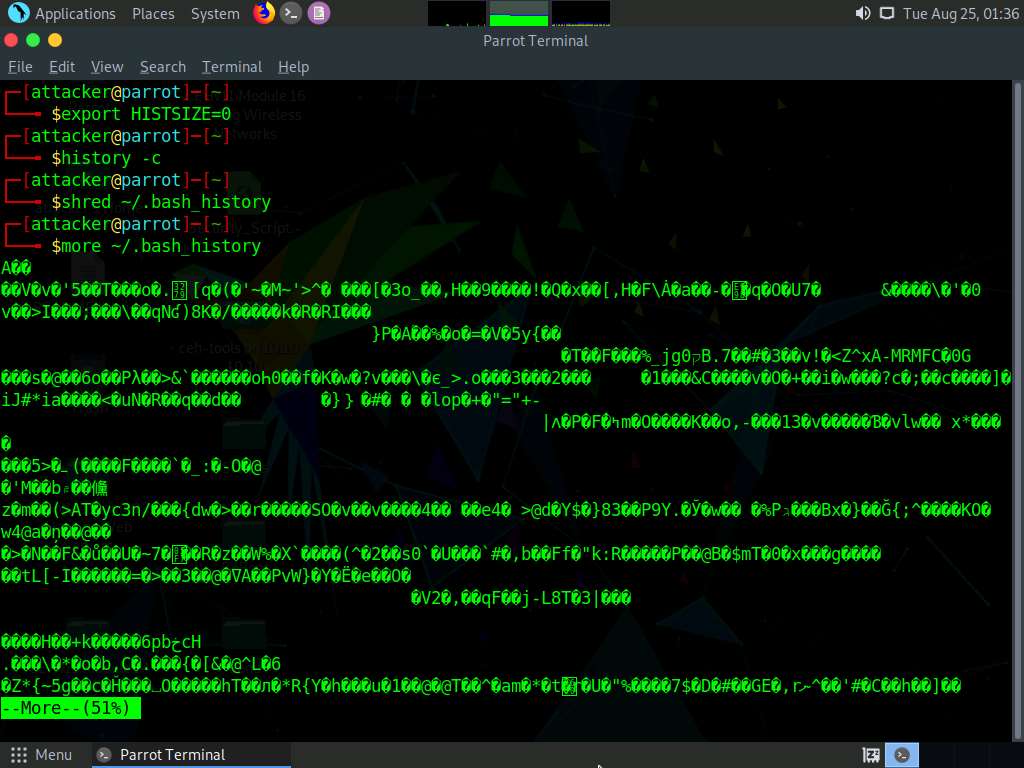
This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



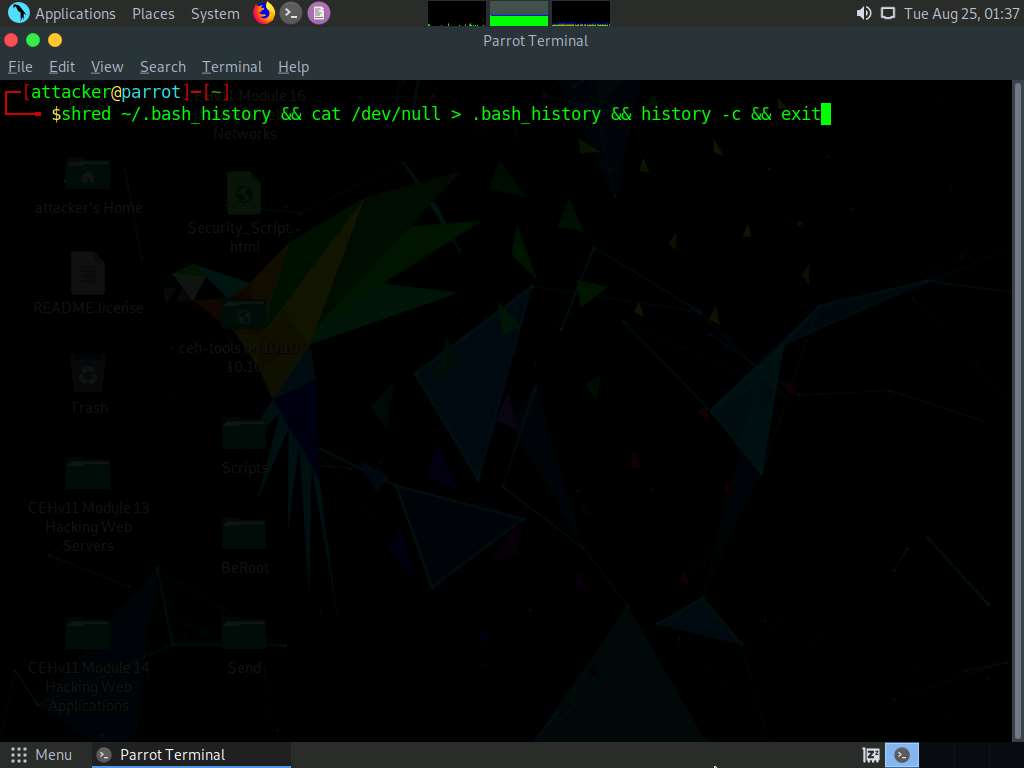
1. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.
2. Type **shred ~/.bash\_history** and press **Enter** to shred the history file, making its content unreadable.

This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

1. Now, type **more ~/.bash\_history** and press **Enter** to view the shredded history content, as shown in the screenshot.



1. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash\_history && cat /dev/null > .bash\_history && history -c && exit**.



1. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.
2. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
3. Close all open windows and document all the acquired information.

Task 4: Clear Windows Machine Logs using CCleaner

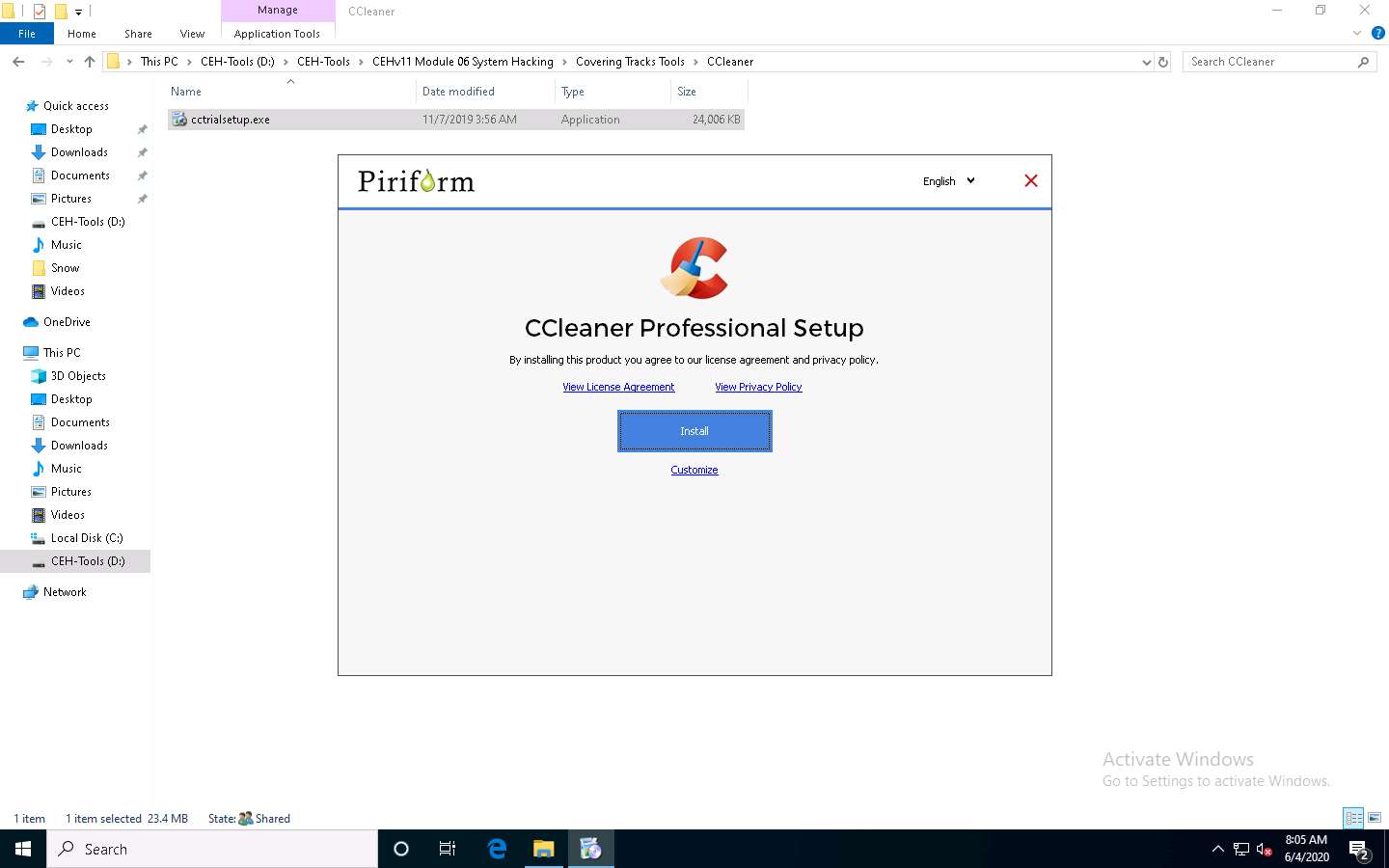
CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks.

Here, we will use CCleaner to clear the system logs of the Windows machine.

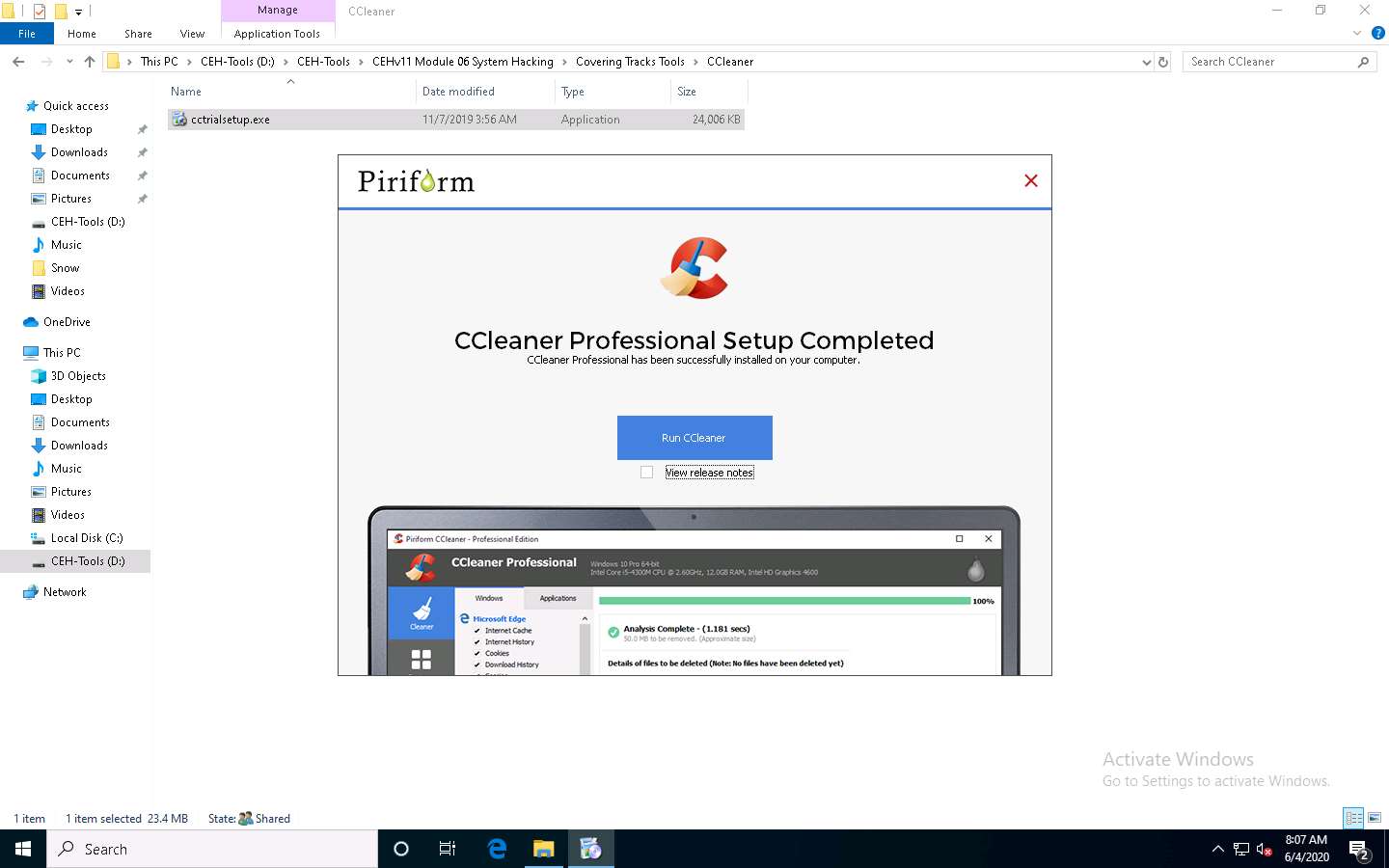
1. Click [Windows 10](https://labclient.labondemand.com/Instructions/9b2812b4-0c87-4fbc-be85-97032f9e7824?rc=10) to switch to the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **cctrialsetup.exe**.

If a **User Account Control** pop-up appears, click **Yes**.

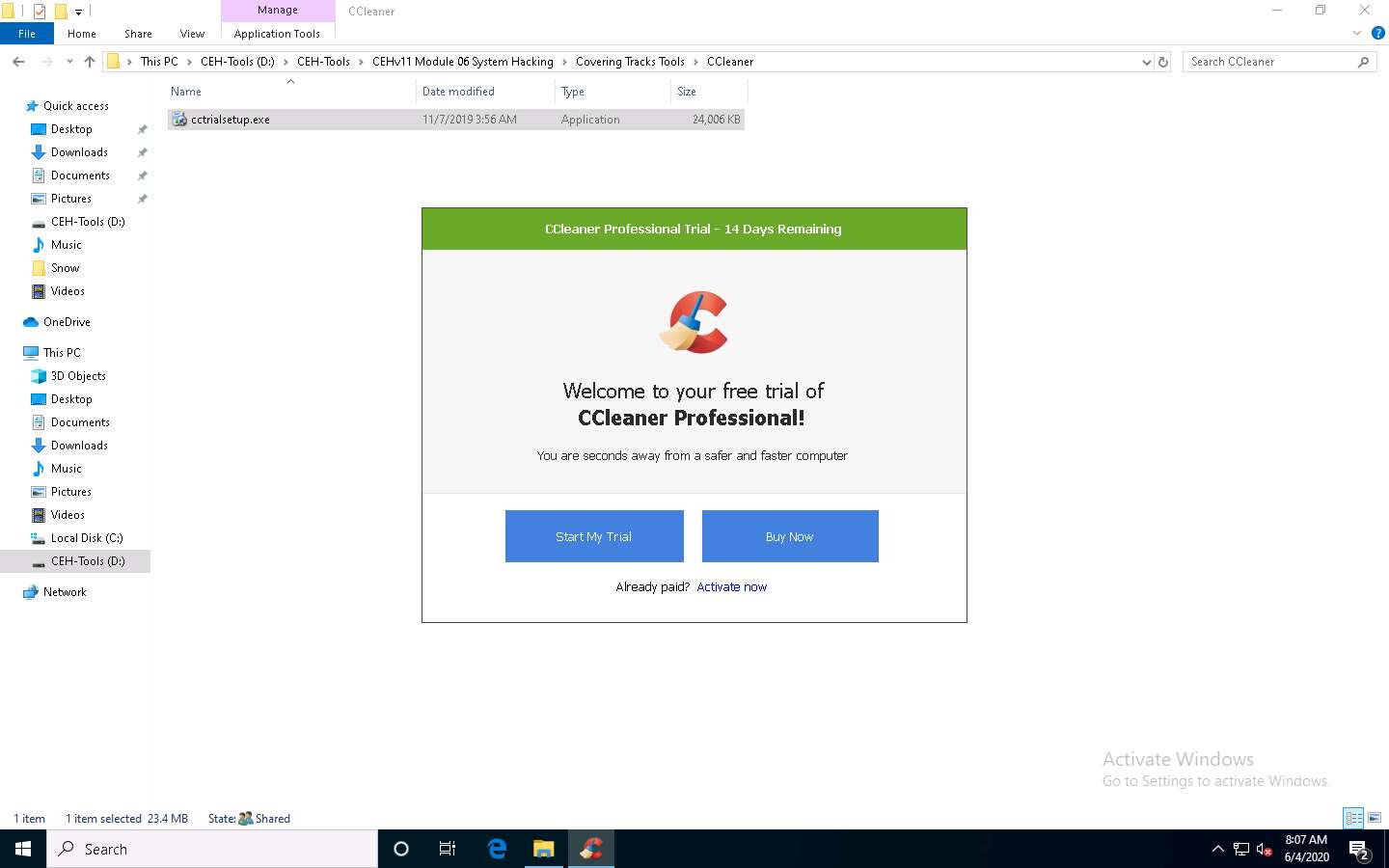
1. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.



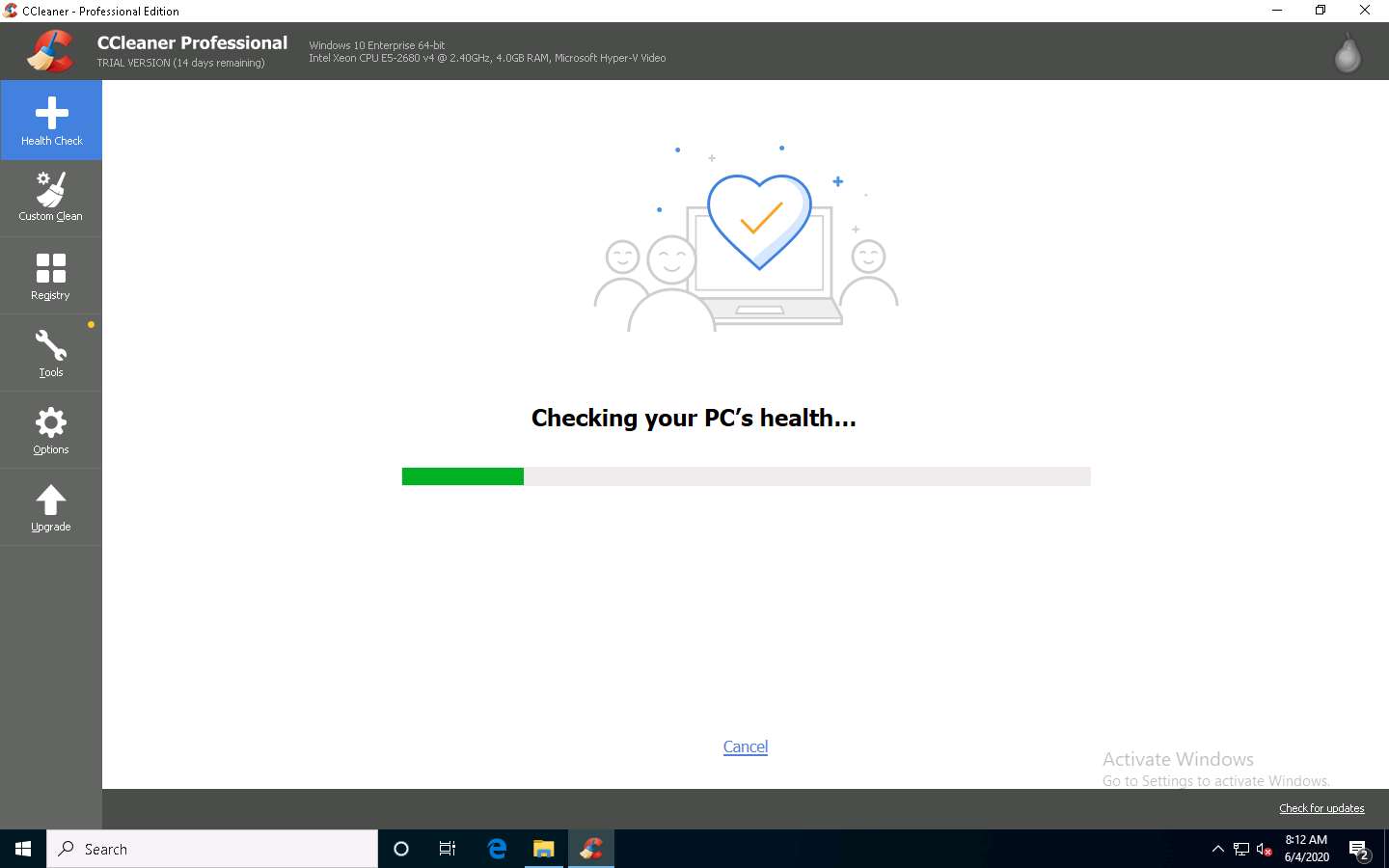
1. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.



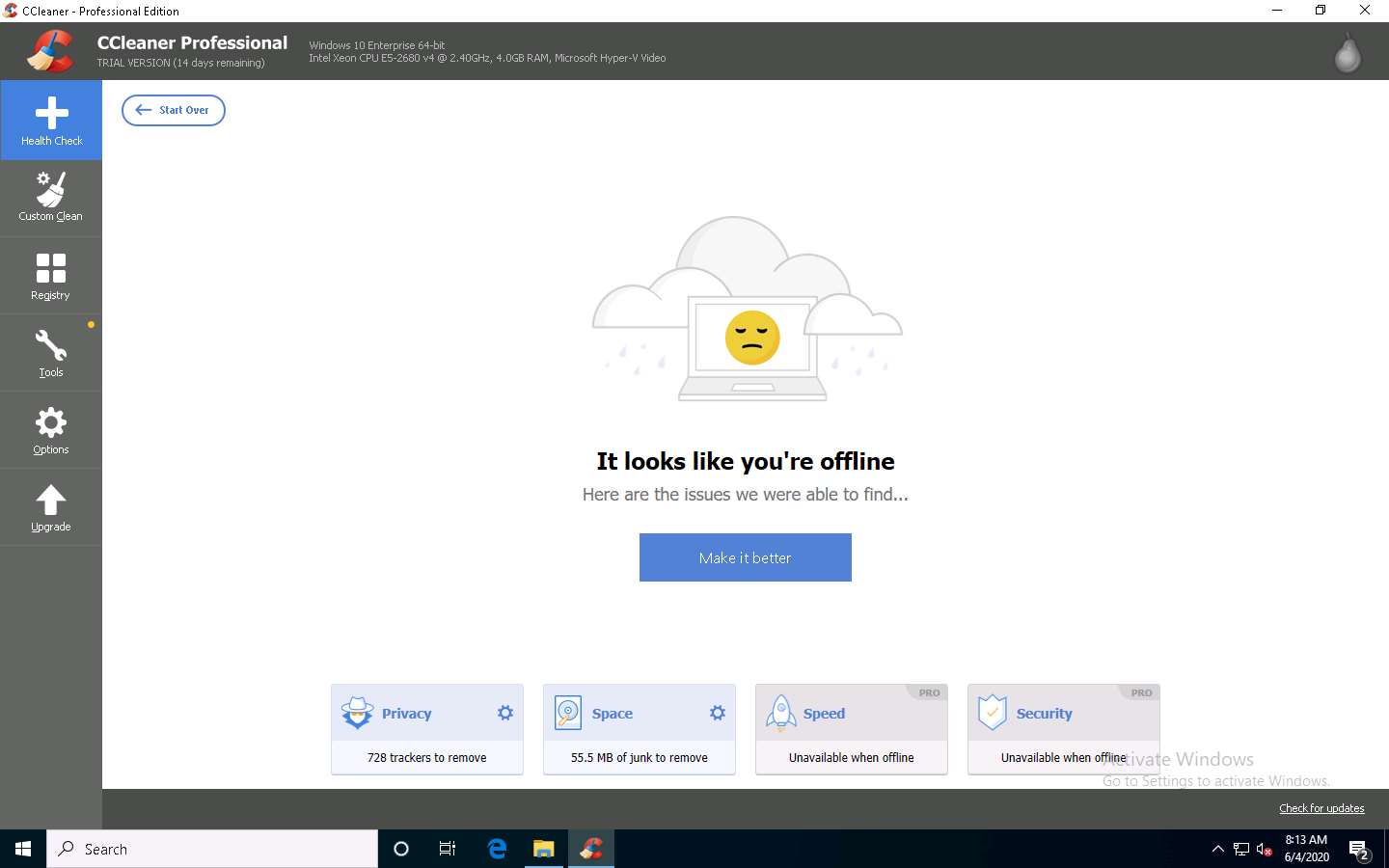
1. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.



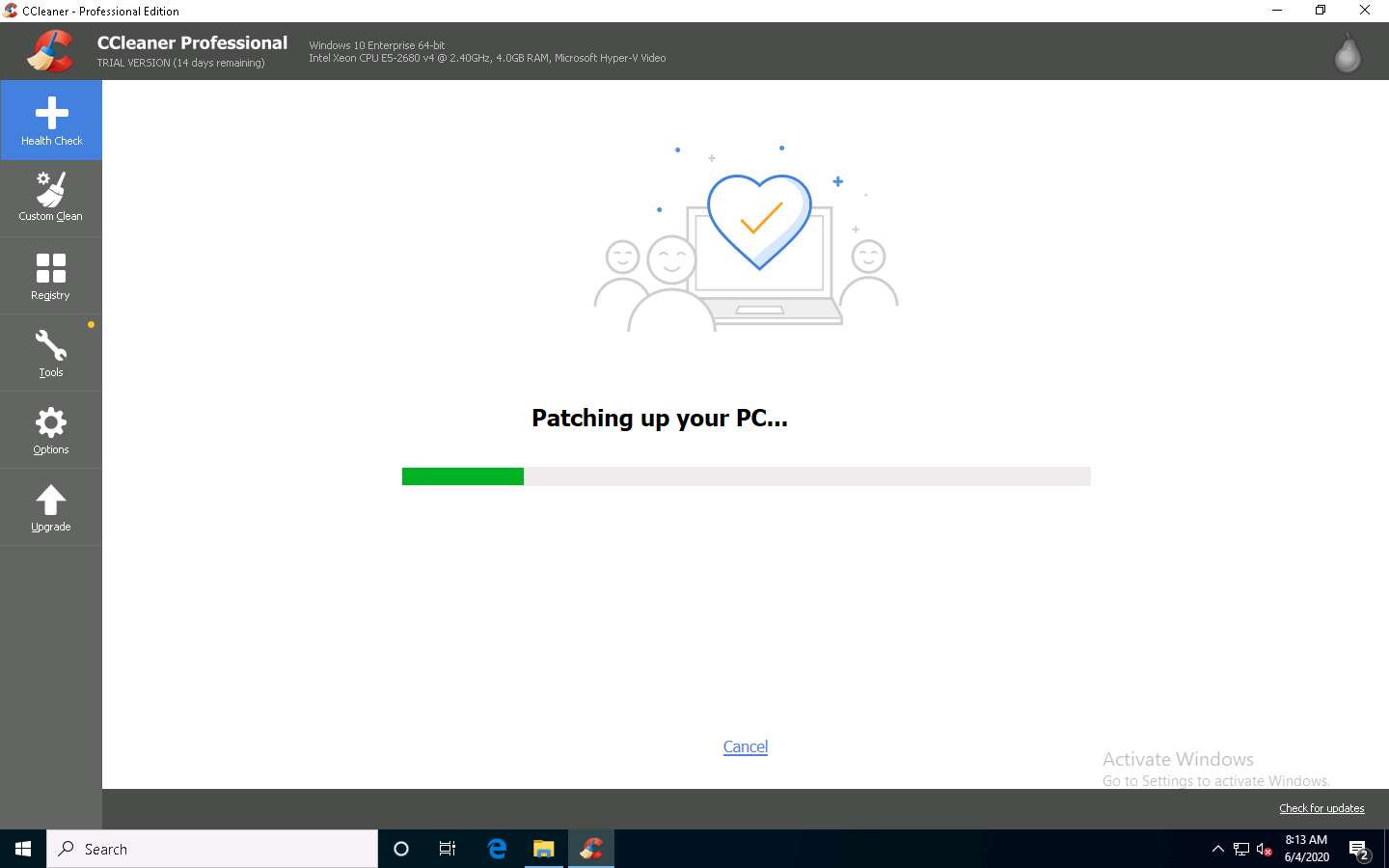
1. The **CCleaner - Professional Edition** window appears along with the **CCleaner Professional** window asking **Would you like to try our shiny new feature?** close it.
2. Click **Next** button until it gets changed to Get Started, click the **Get Started** button and **Checking your PC's health…** message appears.



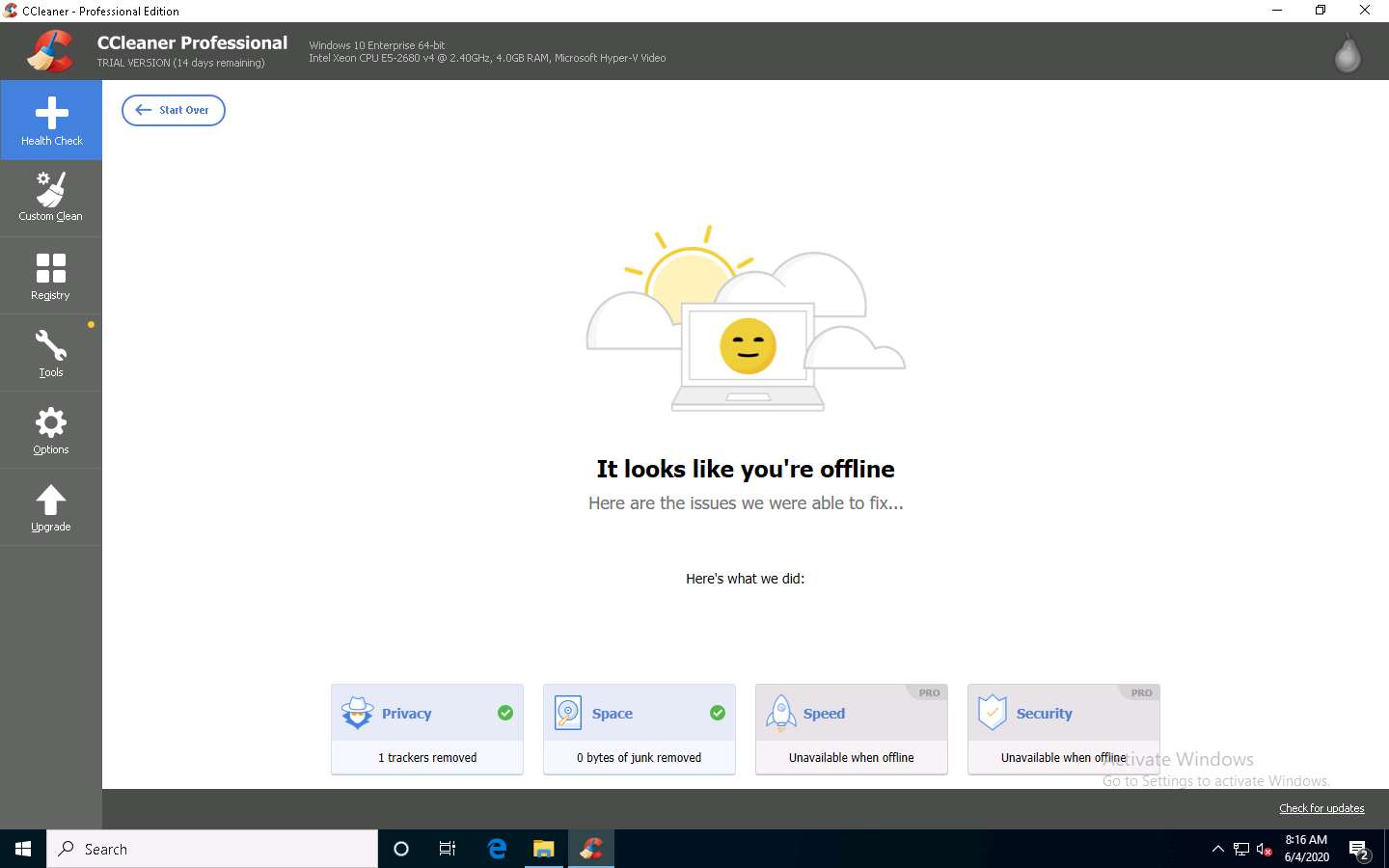
1. After the completion of scan, click **Make it better** button to proceed.



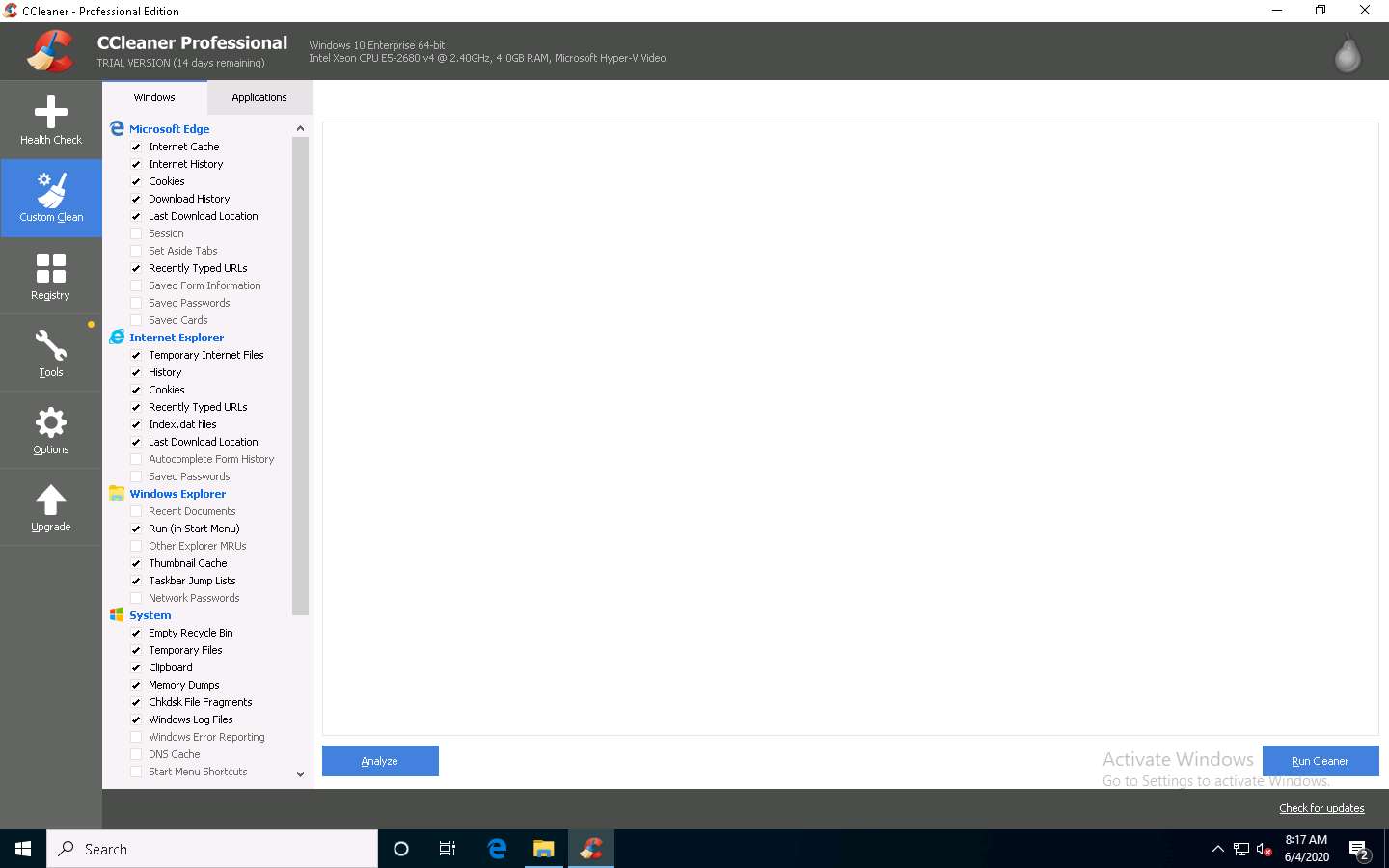
1. **Patching up your PC…** message aapears, wait for it to compete.



1. After the cleaning completes, **It looks like you're offline** message appears, as shown in the screenshot.



1. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.



1. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
2. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
3. You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.
4. Close all open windows and document all the acquired information.