

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

Lab Objectives

- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell

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

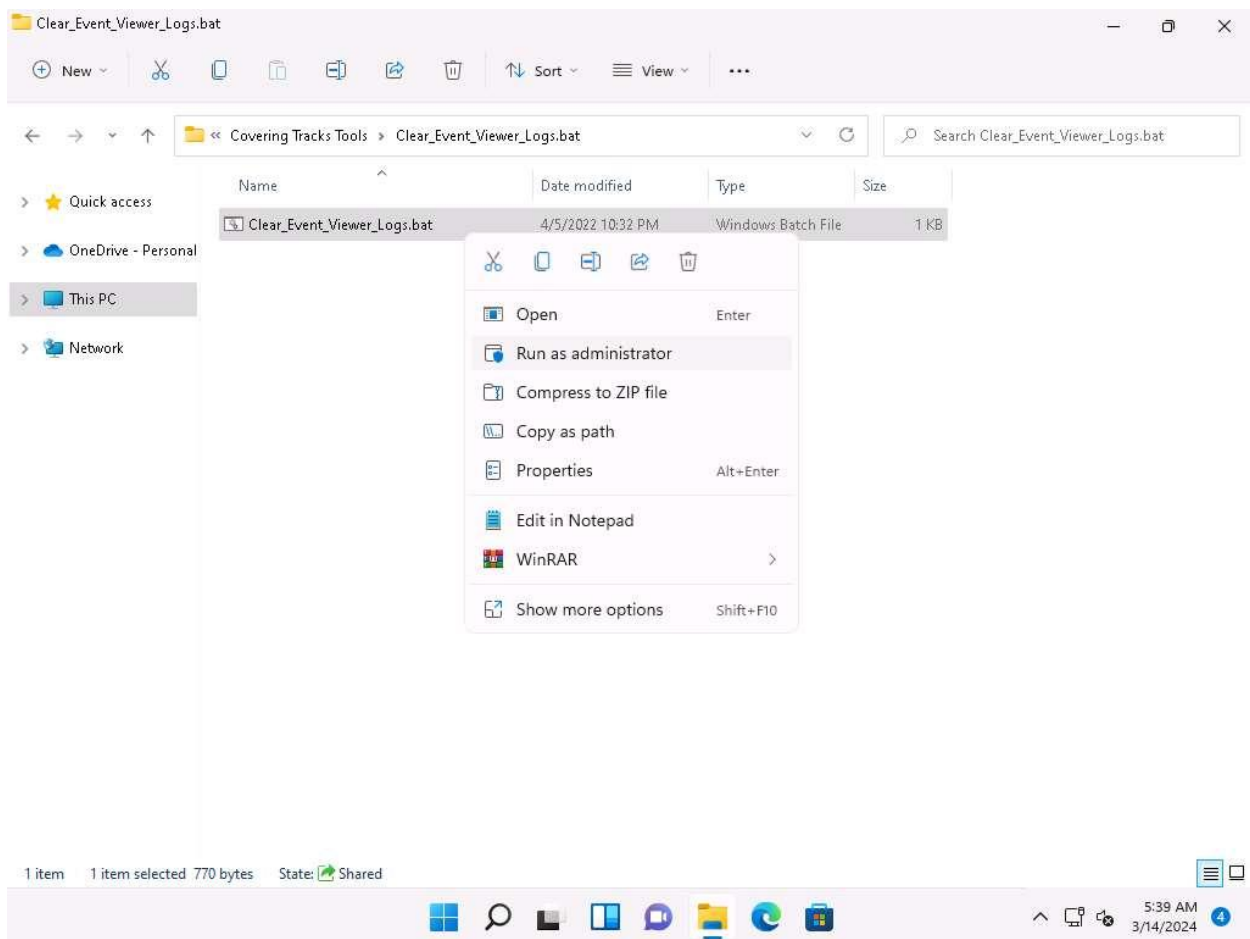
- **Disabling Windows Functionality:** Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Task 1: 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.

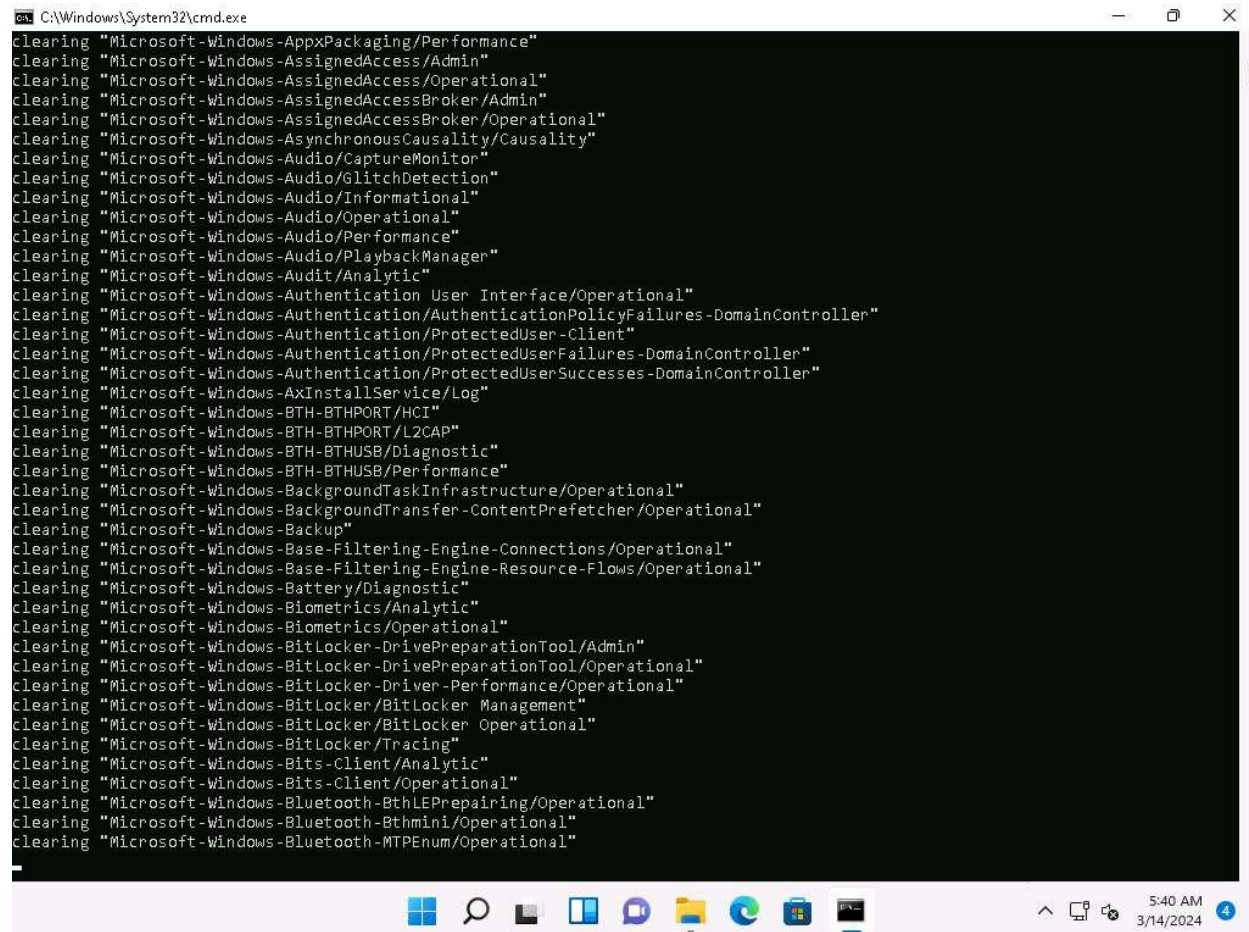
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.



2. The **User Account Control** pop-up appears; click **Yes**.
3. 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.

[more...](#)



```
C:\Windows\System32\cmd.exe
clearing "Microsoft-Windows-AppxPackaging/Performance"
clearing "Microsoft-Windows-AssignedAccess/Admin"
clearing "Microsoft-Windows-AssignedAccess/Operational"
clearing "Microsoft-Windows-AssignedAccessBroker/Admin"
clearing "Microsoft-Windows-AssignedAccessBroker/Operational"
clearing "Microsoft-Windows-AsynchronousCausality/Causality"
clearing "Microsoft-Windows-Audio/CaptureMonitor"
clearing "Microsoft-Windows-Audio/GlitchDetection"
clearing "Microsoft-Windows-Audio/Informational"
clearing "Microsoft-Windows-Audio/Operational"
clearing "Microsoft-Windows-Audio/Performance"
clearing "Microsoft-Windows-Audio/PlaybackManager"
clearing "Microsoft-Windows-Audit/Analytic"
clearing "Microsoft-Windows-Authentication User Interface/Operational"
clearing "Microsoft-Windows-Authentication/AuthenticationPolicyFailures-DomainController"
clearing "Microsoft-Windows-Authentication/ProtectedUser-Client"
clearing "Microsoft-Windows-Authentication/ProtectedUserFailures-DomainController"
clearing "Microsoft-Windows-Authentication/ProtectedUserSuccesses-DomainController"
clearing "Microsoft-Windows-AxInstallService/Log"
clearing "Microsoft-Windows-BTH-BTHPORT/HCI"
clearing "Microsoft-Windows-BTH-BTHPORT/L2CAP"
clearing "Microsoft-Windows-BTH-BTHUSB/Diagnostic"
clearing "Microsoft-Windows-BTH-BTHUSB/Performance"
clearing "Microsoft-Windows-BackgroundTaskInfrastructure/Operational"
clearing "Microsoft-Windows-BackgroundTransfer-ContentPrefetcher/Operational"
clearing "Microsoft-Windows-Backup"
clearing "Microsoft-Windows-Base-Filtering-Engine-Connections/Operational"
clearing "Microsoft-Windows-Base-Filtering-Engine-Resource-Flows/Operational"
clearing "Microsoft-Windows-Battery/Diagnostic"
clearing "Microsoft-Windows-Biometrics/Analytic"
clearing "Microsoft-Windows-Biometrics/Operational"
clearing "Microsoft-Windows-BitLocker-DrivePreparationTool/Admin"
clearing "Microsoft-Windows-BitLocker-DrivePreparationTool/Operational"
clearing "Microsoft-Windows-BitLocker-Driver-Performance/Operational"
clearing "Microsoft-Windows-BitLocker/BitLocker Management"
clearing "Microsoft-Windows-BitLocker/BitLocker Operational"
clearing "Microsoft-Windows-BitLocker/Tracing"
clearing "Microsoft-Windows-Bits-Client/Analytic"
clearing "Microsoft-Windows-Bits-Client/Operational"
clearing "Microsoft-Windows-Bluetooth-BthLEPrepairing/Operational"
clearing "Microsoft-Windows-Bluetooth-Bthmini/Operational"
clearing "Microsoft-Windows-Bluetooth-MTPEnum/Operational"
```

4. In the Windows search type **cmd** the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
5. The **User Account Control** pop-up appears; click **Yes**.
6. A **Command Prompt** window with **Administrator** privileges appears. Run **wevtutil el** command to display a list of event logs.

el | enum-logs lists event log names.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>wevtutil cl
AMSI/Debug
AirSpaceChannel
Analytic
Application
DebugChannel
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
General Logging
HardwareEvents
IHM_DebugChannel
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Intel-iaLPSS2-GPIO2/Debug
Intel-iaLPSS2-GPIO2/Performance
Intel-iaLPSS2-I2C/Debug
Intel-iaLPSS2-I2C/Performance
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceMFT
MF_MediaFoundationDeviceProxy
MF_MediaFoundationFrameServer
MediaFoundationVideoProc
MediaFoundationVideoProcD3D
MediaFoundationAsyncWrapper
MediaFoundationContentProtection
MediaFoundationDS
MediaFoundationDeviceProxy
MediaFoundationMP4
MediaFoundationMediaEngine
MediaFoundationPerformance
MediaFoundationPerformanceCore
MediaFoundationPipeline
MediaFoundationPlatform
MediaFoundationSrcPrefetch
Microsoft-AppV-Client-Streamingux/Debug
```

7. Now, run **wevtutil cl [log_name]** command (here, we are clearing **system** logs) 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.

```
Select Administrator: Command Prompt
Navigator
Network Isolation Operational
OAlerts
OSK_SoftKeyboard_Channel
OfficeChannel
OfficeDebugChannel
OpenSSH/Admin
OpenSSH/Debug
OpenSSH/Operational
Physical_Keyboard_Manager_Channel
PlayReadyPerformanceChannel
RTWorkQueueExtended
RTWorkQueueTheading
SMSApi
Security
Setup
SmbWmiAnalytic
System
SystemEventsBroker
TabletPC_InputPanel_Channel
TabletPC_InputPanel_Channel/IHM
TimeBroker
UIManager_Channel
Uac/Debug
WINDOWS_KS_CHANNEL
WINDOWS_MFH264Enc_CHANNEL
WINDOWS_MP4SDECD_CHANNEL
WINDOWS_MSMPG2ADEC_CHANNEL
WINDOWS_MSMPG2VDEC_CHANNEL
WINDOWS_VC1ENC_CHANNEL
WINDOWS_WMPHOTO_CHANNEL
WINDOWS_wmvdecod_CHANNEL
WMPSetup
WMPSyncEngine
Windows_Networking_Vpn_Plugin_Platform/Operational
Windows_Networking_Vpn_Plugin_Platform/OperationalVerbose
Windows_PowerShell
WordChannel
muxencode

C:\Windows\system32>wevtutil cl system

C:\Windows\system32>
```

8. 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.

9. In **Command Prompt**, run **cipher /w:[Drive or Folder or File Location]** command to overwrite 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.

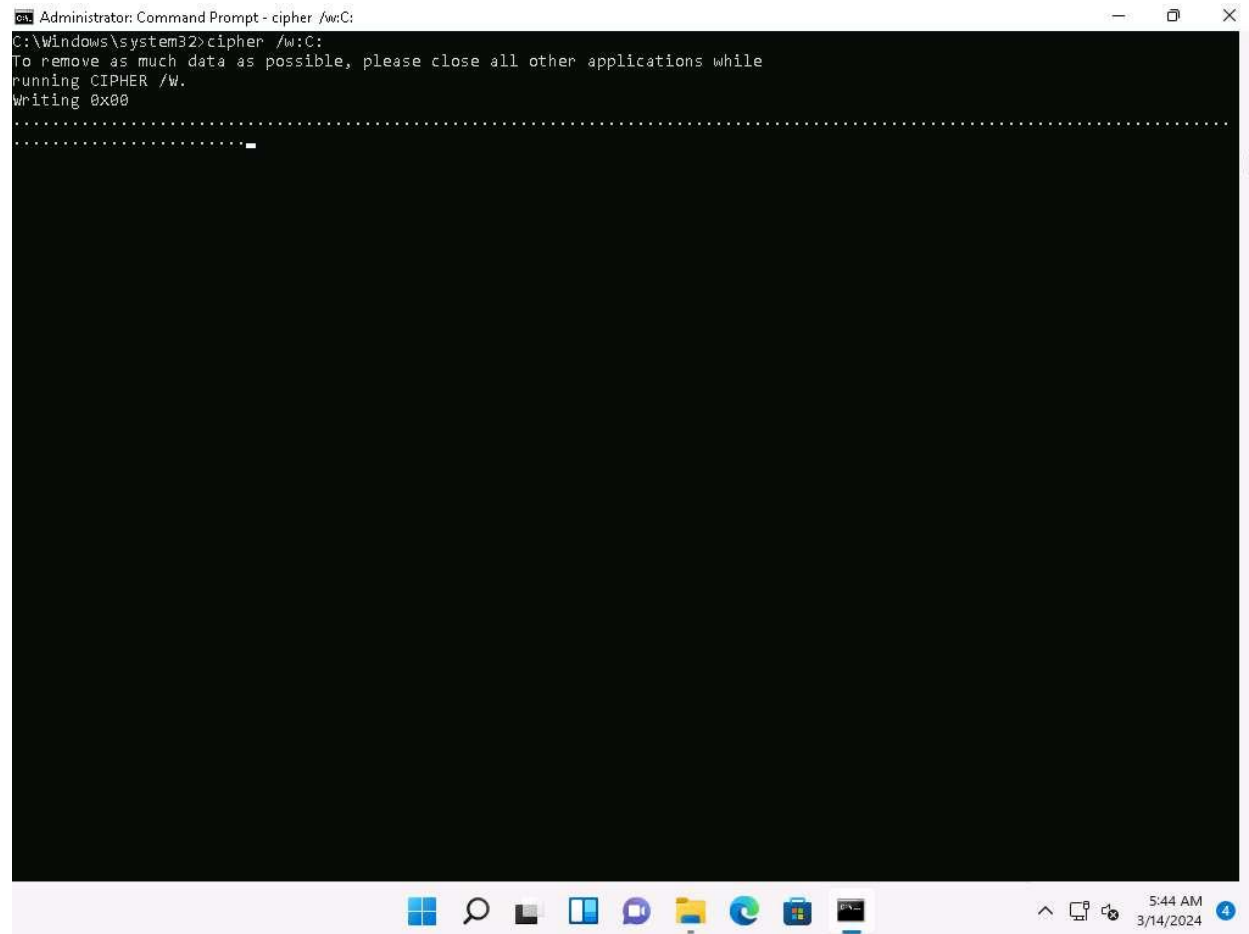
10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

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.

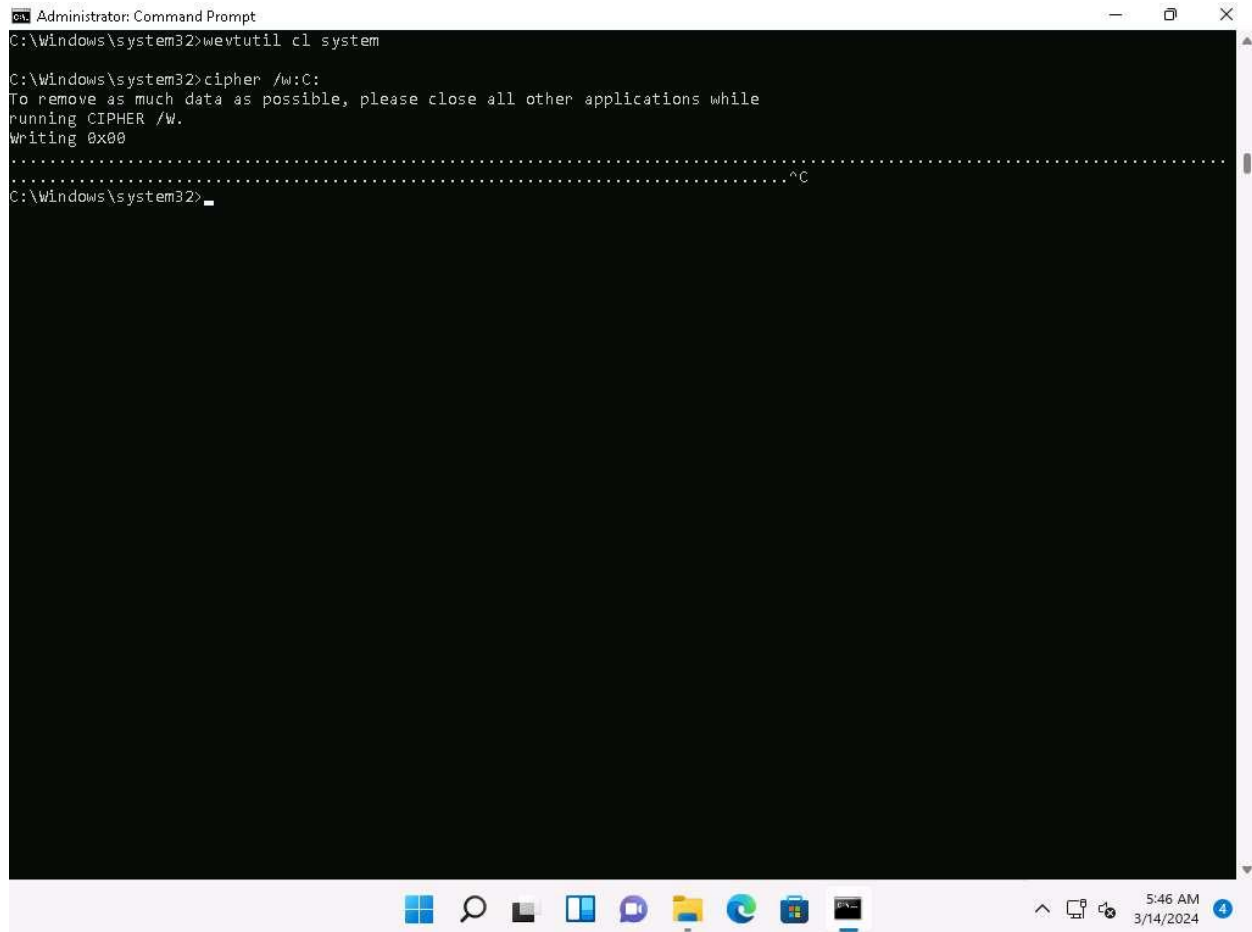
[more...](#)

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt - cipher /w:C:". The command prompt shows the command "C:\windows\system32>cipher /w:C:" and the following output: "To remove as much data as possible, please close all other applications while running CIPHER /W." followed by "Writing 0x00". Below this, there is a long line of dots representing progress, with a small white block at the end. The taskbar at the bottom shows various application icons and the system clock indicating 5:44 AM on 3/14/2024.

```
Administrator: Command Prompt - cipher /w:C:
C:\windows\system32>cipher /w:C:
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....
.....
```

11. Press **ctrl+c** in the command prompt to stop the encryption.

The time taken to overwrite the deleted file, folder or drive depends upon its size.



```
Administrator: Command Prompt
C:\Windows\system32>wevtutil cl system

C:\Windows\system32>cipher /w:C:
To remove as much data as possible, please close all other applications while
running CIPHER /w.
Writing 0x00
.....^C
C:\Windows\system32>
```

12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).

13. Close all open windows and document all the acquired information.

Question 6.4.1.1

In the Windows 11 machine, use various Windows utilities such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher to clear system logs. Which wevtutil command will clear all system logs (enter the complete command as the answer)?

Task 2: 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.

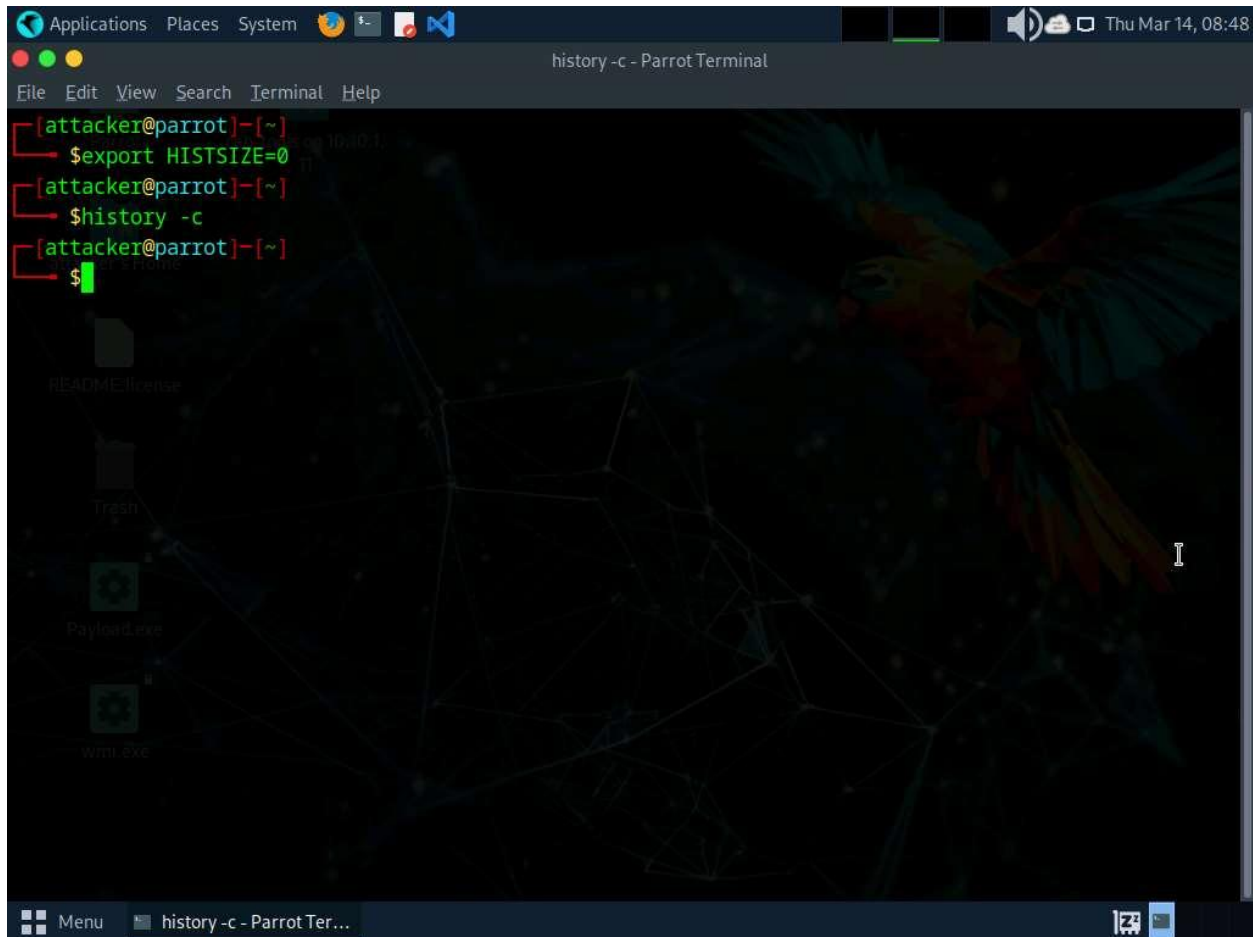
Here, we will clear the Linux machine event logs using the BASH shell.

1. Click [Parrot Security](#) to switch to the **Parrot Security** machine.
2. Open a Terminal window and run **export HISTSIZE=0** command to disable the BASH shell from saving the history.

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

3. In the **Terminal** window, run **history -c** command to clear the stored history.

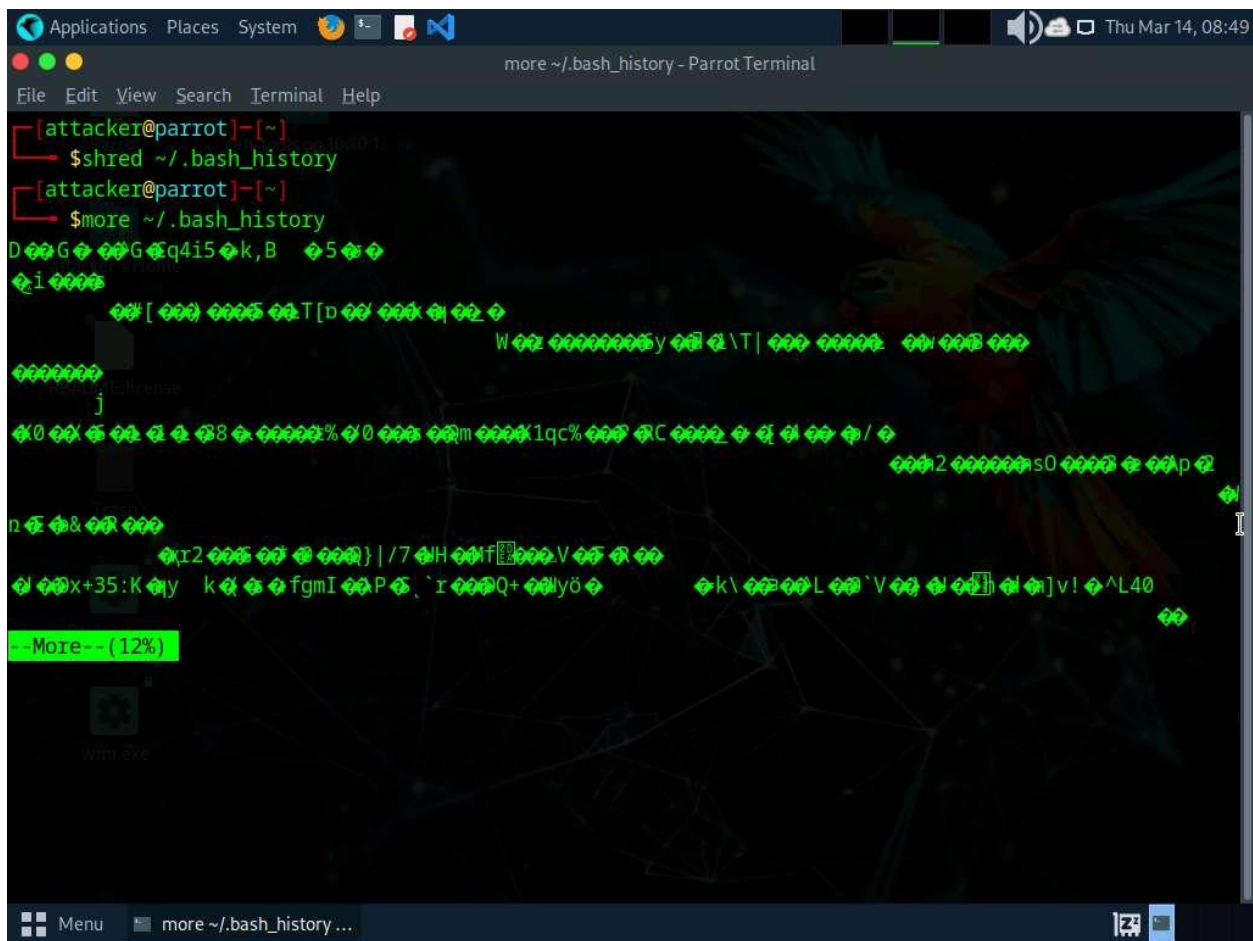
This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.

A screenshot of a terminal window titled "history -c - Parrot Terminal". The terminal shows a user prompt "[attacker@parrot]~" followed by the command "\$export HISTSIZE=0", another prompt "[attacker@parrot]~", and then "\$history -c". The final prompt is "[attacker@parrot]~" followed by a dollar sign "\$" and a cursor. The background of the terminal is a dark theme with a parrot illustration on the right and a network diagram on the left. The desktop environment is visible in the background with icons for "README.license", "Trash", "Payload.exe", and "wmi.exe". The top of the window shows a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The bottom of the window shows a taskbar with a "Menu" button and a window title "history -c - Parrot Ter...".

4. 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.
5. Run **shred ~/.bash_history** command 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.

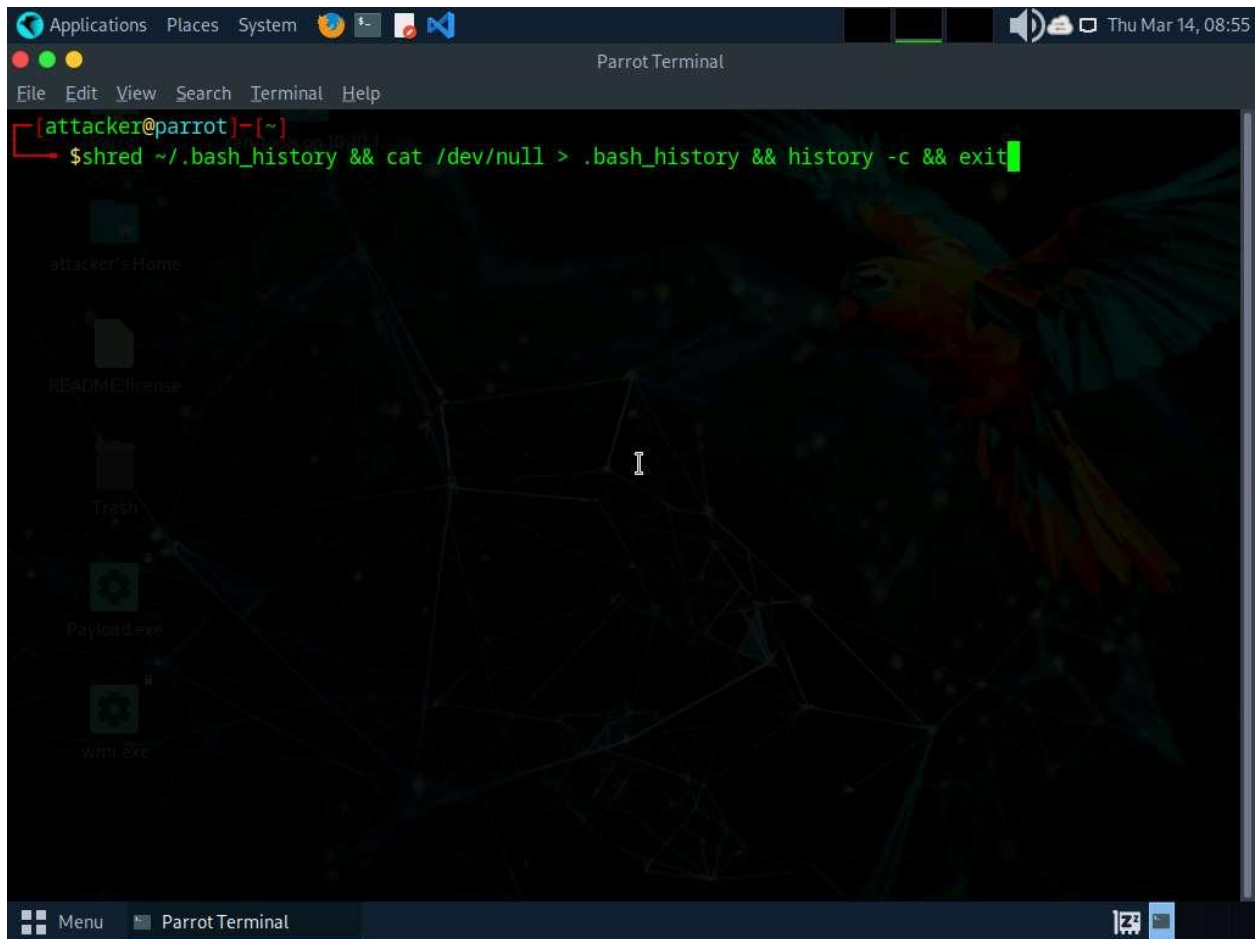
6. Now, run **more ~/.bash_history** command to view the shredded history content, as shown in the screenshot.



7. Type **ctrl+z** to stop viewing the shredded history content.

The time taken for shredding history file depends on the size of the file.

8. 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**.



9. 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.
10. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
11. Close all open windows and document all the acquired information.

Question 6.4.2.1

In the Parrot Security machine, clear the Linux machine event logs using the Bash shell. Which command will disable the Bash shell from saving the history?