# 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

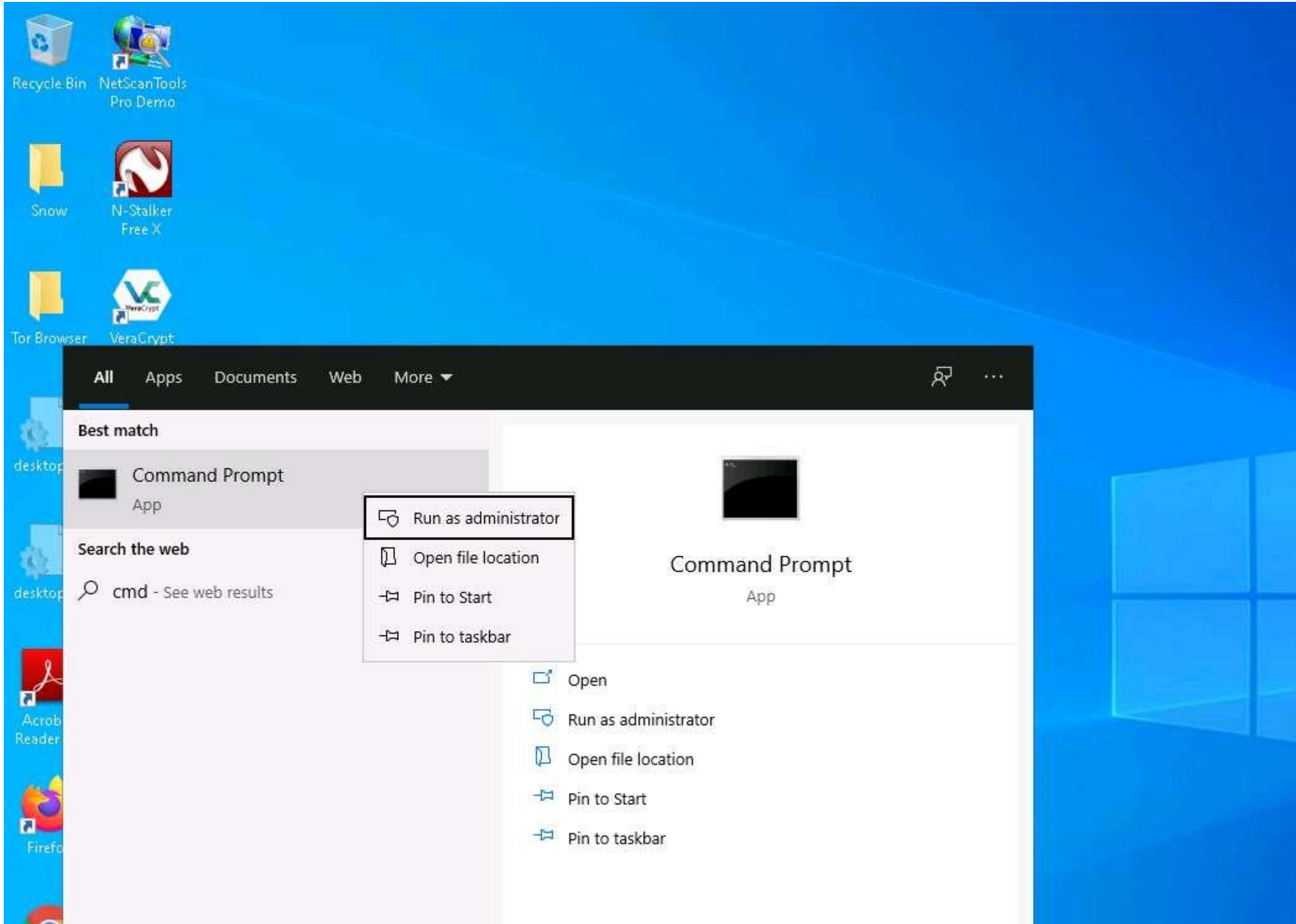
## Task 1: View, Enable, and Clear Audit Policies using Auditpol

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 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**.


Recycle Bin
NetScanTools Pro Demo
Snow
N-Stalker Free X
Tor Browser
VeraCrypt
All
Apps
Documents
Web
More
Best match
Command Prompt
App
Search the web
cmd - See web results
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar

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

Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
```

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

Select Administrator: Command Prompt

```
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     Success
  Authentication Policy Change            Success
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             No Auditing
  Security Group Management               Success
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing
  User Account Management                 Success
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
```

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

Select Administrator: Command Prompt

```
C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
```

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

Select Administrator: Command Prompt

```
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     Success
  Authentication Policy Change            Success
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             No Auditing
  Security Group Management               Success
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing
  User Account Management                 Success
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
```

8. 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.

Select Administrator: Command Prompt

```
C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   No Auditing
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
```

9. ☐ This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
10. ☐ 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**.

Manage

Clear_Event_Viewer_Logs.bat

File | Home | Share | View | Application Tools

This PC > CEH-Tools (D:) > CEH-Tools > CEHv11 Module 06 System Hacking > Covering Tracks Tools > Clear_Event_Viewer_Logs.bat

- Quick access
  - Desktop
  - Downloads
  - Documents
  - Pictures
  - CEH-Tools (D:)
  - Music
  - Snow
  - Videos
- OneDrive
- This PC
  - 3D Objects
  - Desktop
  - Documents
  - Downloads
  - Music
  - Pictures
  - Videos
  - Local Disk (C:)
  - CEH-Tools (D:)
- Network

| Name | Date modified | Type | Size |
|---|---|---|---|
| Clear_Event_Viewer_Logs.bat | 11/7/2019 12:22 AM | Windows Batch File | 1 KB |

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.

C:\WINDOWS\System32\cmd.exe

```
clearing "Microsoft-Windows-Application Server-Applications/Analytic"
clearing "Microsoft-Windows-Application Server-Applications/Debug"
clearing "Microsoft-Windows-Application Server-Applications/Operational"
clearing "Microsoft-Windows-Application-Experience/Compatibility-Infrastructure-Debug"
clearing "Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant"
clearing "Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant/Analytic"
clearing "Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant/Trace"
clearing "Microsoft-Windows-Application-Experience/Program-Compatibility-Troubleshooter"
clearing "Microsoft-Windows-Application-Experience/Program-Inventory"
clearing "Microsoft-Windows-Application-Experience/Program-Telemetry"
clearing "Microsoft-Windows-Application-Experience/Steps-Recorder"
clearing "Microsoft-Windows-ApplicationResourceManagementSystem/Diagnostic"
clearing "Microsoft-Windows-ApplicationResourceManagementSystem/Operational"
clearing "Microsoft-Windows-AppxPackaging/Debug"
clearing "Microsoft-Windows-AppxPackaging/Operational"
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/Diagnostic"
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"
```

4. ☐ 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**.
5. ☐ The **User Account Control** pop-up appears; click **Yes**.
6. ☐ 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.

Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wevtutil el
AMSI/Debug
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
HardwareEvents
IHM_DebugChannel
InstallUXPerformance-Analytic
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
MedaFoundationVideoProc
MedaFoundationVideoProcD3D
MediaFoundationAsyncWrapper
MediaFoundationContentProtection
MediaFoundationDS
MediaFoundationDeviceProxy
MediaFoundationMP4
MediaFoundationMediaEngine
MediaFoundationPerformance
MediaFoundationPerformanceCore
MediaFoundationPipeline
MediaFoundationPlatform
MediaFoundationSrcPrefetch
Microsoft-AppV-Client-Streamingux/Debug
Microsoft-AppV-Client/Admin
Microsoft-AppV-Client/Debug
Microsoft-AppV-Client/Operational
Microsoft-AppV-Client/Virtual Applications
```

7. 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.

Select Administrator: Command Prompt

```
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**, 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.

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...

Select 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
.................................................................................................................
Writing 0xFF
.................................................................................................................
Writing Random Numbers
.................................................................................................................

C:\WINDOWS\system32>
```

11. ☐ This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
12. ☐ Close all open windows and document all the acquired information.

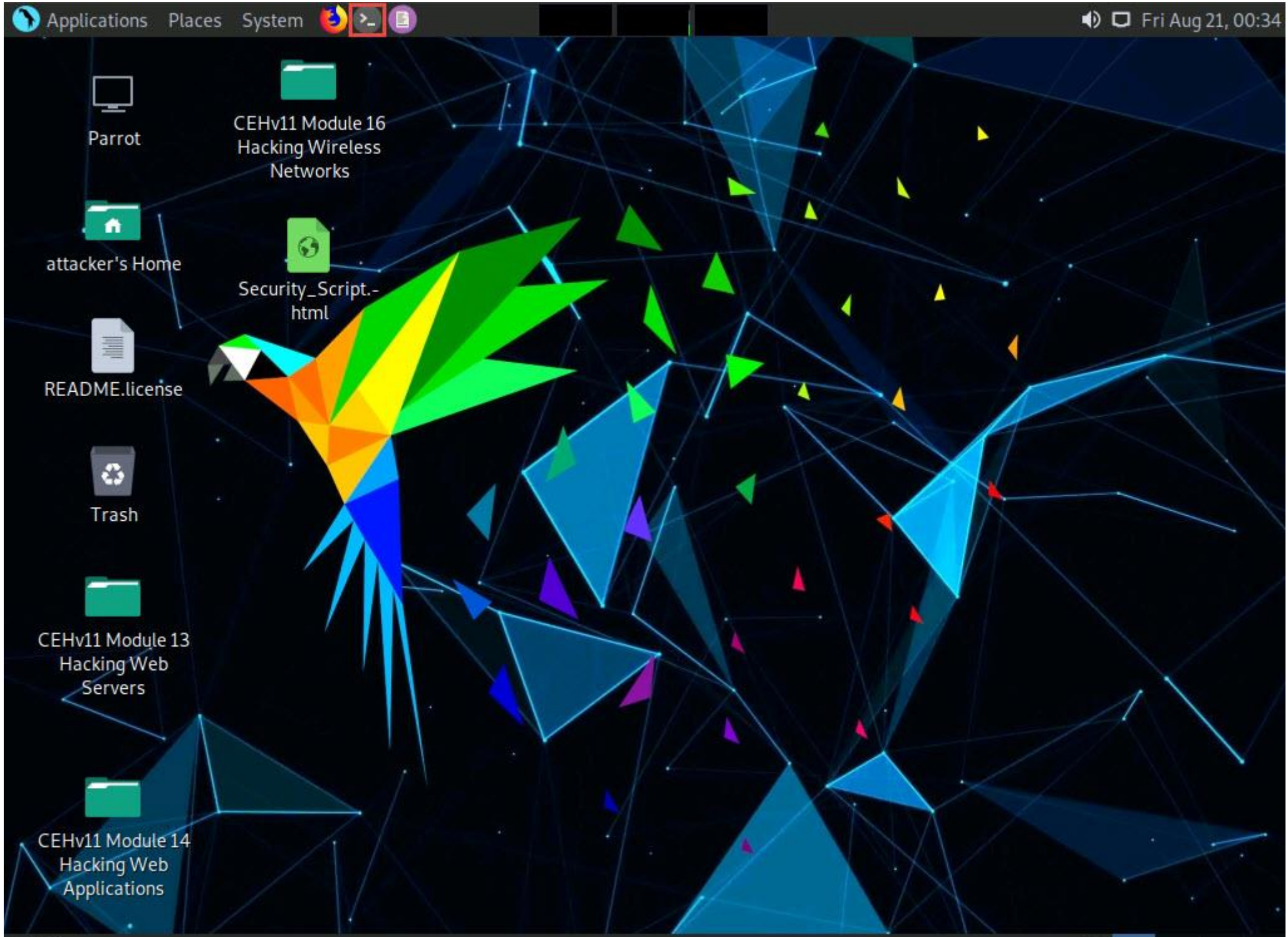
---

## 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 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.


Applications
Places
System
Fri Aug 21, 00:34
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

3. 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.

4. 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.

Applications Places System Tue Aug 25, 01:35

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $export HISTSIZE=0
┌─[attacker@parrot]─[~]
└──╼ $history -c
┌─[attacker@parrot]─[~]
└──╼ $
```

5. 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.
6. 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.

7. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

Applications Places System Tue Aug 25, 01:36

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $export HISTSIZE=0
┌─[attacker@parrot]─[~]
└──╼ $history -c
┌─[attacker@parrot]─[~]
└──╼ $shred ~/.bash_history
┌─[attacker@parrot]─[~]
└──╼ $more ~/.bash_history
A►►
►►V►v►'5►►T►►►o►.[q►(►'~►M~'>^► ►►►[►3o_►►,H►►9►►►►!►Q►x►►[,H►F\Ȧ►a►►-►►q►O►U7►      &►►►►\►'►0
v►►>I►►►;►►►\►►qNǵ)8K►/►►►►►k►R►RI►►►
                                        }P►A►►%►o►=►V►5y{►►
                                                                  ►T►►F►►►%_jg0┐B.7►►#►3►►v!►<Z^xA-MRMFC►0G
►►►s►@►►6o►►Pλ►►>&`►►►►►►oh0►►f►K►w►?v►►►\►ϵ_>.o►►►3►►►2►►►     ►1►►►&C►►►►v►O►+►►i►w►►►?c►;►►c►►►►]►
iJ#*ia►►►►<►uN►R►►q►►d►►        ►}} ►►# ► ►lop►+►"="+-
                                                                  |∧►P►F►ꜟm►O►►►►K►►o,-►►►13►v►►►►►B►vlw►► x*►►►
►
►►►5>►_(►►►►F►►►►`►_:►-O►@
►'M►►b►►►儘
z►m►►(>AT►yc3n/►►►{dw►>►►r►►►►►S0►v►►v►►►►4►► ►►e4► >@d►Y$►}83►►P9Y.►Ÿ►w►► ►%P►►►Bx►}►►Ğ{;^►►►►K0►
w4@a►n►►@►►
►>►N►►F&►ů►►U►~7►►►R►z►►W%►X`►►►►(^►2►►s0`►U►►►`#►,b►►Ff►"k:R►►►►►P►►@B►$mT►0►x►►►g►►►►
►►tL[-I►►►►►►=►>►►3►►@►►∇A►►PvW}►Y►Ë►e►►O►
                                        ►V2►,►►qF►►j-L8T►3|►►►

►►►►H►►+k►►►►►6pb►cH
.►►►\►*►o►b,C►.►►►{►[&►►@^L►6
►Z*{~5g►►c►Ĥ►►►_O►►►►►hT►►л►*R{Y►h►►►u►1►►@►►@T►►^►am►*►t►►►U►"%►►►►7$►D►#►►GE►,r~^►►'#►C►►h►►]►►
--More--(51%)
```

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**.

Applications Places System Tue Aug 25, 01:37

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $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.

---

## 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 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**.

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

File Home Share View Manage Application Tools CCleaner

This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 06 System Hacking › Covering Tracks Tools › CCleaner

| Name | Date modified | Type | Size |
|---|---|---|---|
| cctrialsetup.exe | 11/7/2019 3:56 AM | Application | 24,006 KB |

Quick access
- Desktop
- Downloads
- Documents
- Pictures
- CEH-Tools (D:)
- Music
- Snow
- Videos

OneDrive

This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- CEH-Tools (D:)

Network

Piriform

English

# CCleaner Professional Setup

By installing this product you agree to our license agreement and privacy policy.

View License Agreement  View Privacy Policy

Install

Customize

3. ☐ **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.

File Home Share View | Manage Application Tools | CCleaner

This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 06 System Hacking › Covering Tracks Tools › CCleaner

| Name | Date modified | Type | Size |
|---|---|---|---|
| cctrialsetup.exe | 11/7/2019 3:56 AM | Application | 24,006 KB |

Quick access
- Desktop
- Downloads
- Documents
- Pictures
- CEH-Tools (D:)
- Music
- Snow
- Videos

OneDrive

This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- CEH-Tools (D:)

Network

Piriform

CCleaner Professional Setup Completed

CCleaner Professional has been successfully installed on your computer.

Run CCleaner

View release notes

Piriform CCleaner - Professional Edition

CCleaner Professional

Windows 10 Pro 64-bit
Intel Core i5-4300M CPU @ 2.60GHz, 12.0GB RAM, Intel HD Graphics 4600

Cleaner

Windows | Applications

Microsoft Edge
- Internet Cache
- Internet History
- Cookies
- Download History

100%

Analysis Complete - (1.181 secs)
50.0 MB to be removed. (Approximate size)

Details of files to be deleted (Note: No files have been deleted yet)

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

File Home Share View | Manage Application Tools | CCleaner

This PC › CEH-Tools (D:) › CEH-Tools › CEHv11 Module 06 System Hacking › Covering Tracks Tools › CCleaner

| Name | Date modified | Type | Size |
|---|---|---|---|
| cctrialsetup.exe | 11/7/2019 3:56 AM | Application | 24,006 KB |

Quick access
- Desktop
- Downloads
- Documents
- Pictures
- CEH-Tools (D:)
- Music
- Snow
- Videos

OneDrive

This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- CEH-Tools (D:)

Network

**CCleaner Professional Trial - 14 Days Remaining**

Welcome to your free trial of
**CCleaner Professional!**

You are seconds away from a safer and faster computer

Start My Trial | Buy Now

Already paid? Activate now

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

CCleaner - Professional Edition

**CCleaner Professional**
TRIAL VERSION (14 days remaining)

Windows 10 Enterprise 64-bit
Intel Xeon CPU E5-2680 v4 @ 2.40GHz, 4.0GB RAM, Microsoft Hyper-V Video

Health Check
Custom Clean
Registry
Tools
Options
Upgrade

**Checking your PC's health...**

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

CCleaner - Professional Edition

**CCleaner Professional**
TRIAL VERSION (14 days remaining)

Windows 10 Enterprise 64-bit
Intel Xeon CPU E5-2680 v4 @ 2.40GHz, 4.0GB RAM, Microsoft Hyper-V Video

Health Check
Custom Clean
Registry
Tools
Options
Upgrade

Start Over

## It looks like you're offline

Here are the issues we were able to find...

Make it better

Privacy | Space | Speed PRO

8. ☐ **Patching up your PC...** message aapears, wait for it to compete.

CCleaner - Professional Edition

**CCleaner Professional**
TRIAL VERSION (14 days remaining)

Windows 10 Enterprise 64-bit
Intel Xeon CPU E5-2680 v4 @ 2.40GHz, 4.0GB RAM, Microsoft Hyper-V Video

Health Check
Custom Clean
Registry
Tools
Options
Upgrade

**Patching up your PC...**

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

CCleaner - Professional Edition

**CCleaner Professional**
TRIAL VERSION (14 days remaining)

Windows 10 Enterprise 64-bit
Intel Xeon CPU E5-2680 v4 @ 2.40GHz, 4.0GB RAM, Microsoft Hyper-V Video

Health Check
Custom Clean
Registry
Tools
Options
Upgrade

Start Over

## It looks like you're offline

Here are the issues we were able to fix...

Here's what we did:

Privacy

Space

PRO
Speed

10. 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.

CCleaner - Professional Edition

**CCleaner Professional**
TRIAL VERSION (14 days remaining)

Windows 10 Enterprise 64-bit
Intel Xeon CPU E5-2680 v4 @ 2.40GHz, 4.0GB RAM, Microsoft Hyper-V Video

Health Check
Custom Clean
Registry
Tools
Options
Upgrade

Windows | Applications

**Microsoft Edge**
- [x] Internet Cache
- [x] Internet History
- [x] Cookies
- [x] Download History
- [x] Last Download Location
- [ ] Session
- [ ] Set Aside Tabs
- [x] Recently Typed URLs
- [ ] Saved Form Information
- [ ] Saved Passwords
- [ ] Saved Cards

**Internet Explorer**
- [x] Temporary Internet Files
- [x] History
- [x] Cookies
- [x] Recently Typed URLs
- [x] Index.dat files
- [x] Last Download Location
- [ ] Autocomplete Form History
- [ ] Saved Passwords

**Windows Explorer**
- [ ] Recent Documents
- [x] Run (in Start Menu)
- [ ] Other Explorer MRUs
- [x] Thumbnail Cache
- [x] Taskbar Jump Lists
- [ ] Network Passwords

**System**
- [x] Empty Recycle Bin
- [x] Temporary Files
- [x] Clipboard
- [x] Memory Dumps
- [x] Chkdsk File Fragments

11. ☐ 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.
12. ☐ This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. ☐ 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.
14. ☐ Close all open windows and document all the acquired information.