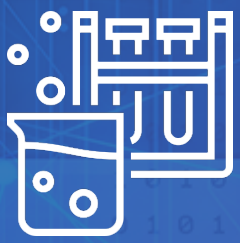
Lab Assignment



Cybersecurity Professional Program

Digital Forensics &
Incident Response

Log Analysis

DFIR-09-L3
Manipulate Log Files

Lab Objective

Acquire a better understanding of how an attacker can erase tracks.

Lab Mission

Modify and delete logs in Linux and Windows machines.

Lab Duration

20–35 minutes

Requirements

- Knowledge of event log filtering and structure
- Working knowledge of Linux commands

Resources

- VirtualBox
- SIFT VM (password: **forensics**)
- Windows 10 VM

Textbook References

- Chapter 9: Log Analysis
    - Section 3: Log Analysis
    - Section 4: Linux Logs
    - Section 6: Log Attacks

Lab Task 1: Modify and Delete Linux Logs

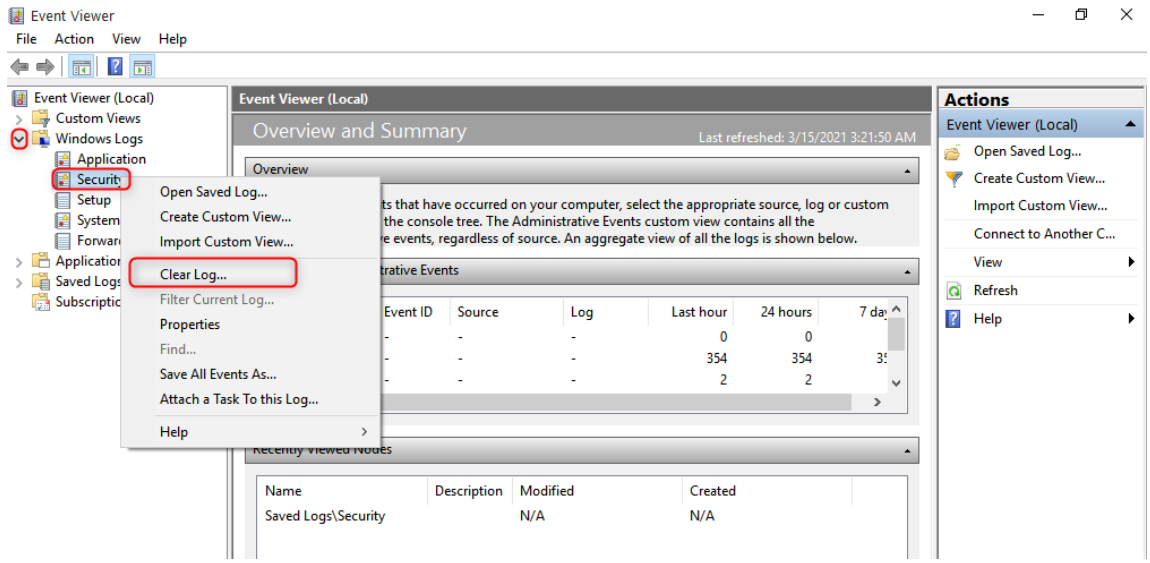
In this task, you will change Linux log data.

1. Start the SIFT VM and try to log in twice with an incorrect password (to generate a log). Then, log in using the correct password.
2. Use ***cat*** to check the content of the ***auth.log*** file found in ***/var/log/auth.log***. Do you see the failed login events?
3. To modify the ***auth.log*** file, you need to use an editor (like nano) and change one of the failed login usernames to **toor** instead of **sansforensics**. Do this, then read the file with ***cat*** again. Do you see that the log changed?
4. Use the ***sed*** command to replace all references to the logged-in username with the name you chose in the previous step. The format that is to be used is ***sed -I 's/[old-text]/[new-text]/g' [path]***. For example, ***sed -i 's/dave/john/'g /var/log/auth.log***. Verify with ***cat*** that the changes were made to the log.

Lab Task 2: Delete Windows Logs Without a Trace

In this task, you will remove the logs saved on the Windows machine and prevent investigators from tracking your actions.

1. Log into the Windows 10 VM.
2. Open the Event Viewer and check the number of security logs in the system.
3. Disable the event log service by opening ***services.msc*** and going to the startup drop-down to disable it. Then, restart the machine.
4. Move all files from ***C:\windows\System32\winevt\Logs to C:\Temp*** (create a directory called ***Temp***) and enable the Windows Event Log service. In the Event Viewer, check the number of logs. Are all the logs there?
5. Start the Event Log service backup by going again to the ***services.msc*** and setting the startup type drop down to ***Manual***.
6. In the Event Viewer security logs, do you see a message that the logs were cleared?
7. In Event Viewer, delete all security logs by right-clicking on the security icon and selecting ***Clear Log…***. Is there an indication that the logs were cleared?



Hints

Lab Task 1

- To search for failed login attempts in the ***auth.log*** file, you can use both ***cat*** and ***grep*** as follows (***cat*** was introduced in LNX-02):
  cat /var/log/auth.log | grep "authentication failure"
- To search for a specific string in a file using nano, press ***Ctrl + W*** and input the string.
- To use ***sed*** to change words in a log file, run the following command structure:
  sudo ssed -i 's/old-text/new-text/g' /var/log/auth.log

Lab Task 2

- To access the Event Viewer, click **Start** and search for **Event Viewer** or run the command ***eventvwr.msc*** in the **Run** window.
- In Event Viewer, to see how many events are logged in the security logs, click **Windows Logs**.
- Another way to access services is through the administrative tools in the Control Panel.
- To stop the **Event Log** service, open **Run**, type **services.msc**, and search for Windows Event Log. Open the properties of the service and change the startup type to ***Disabled***.
- To restart the **Event Log** service, open **Run**, type **services.msc**, and search for Windows Event Log. Open the properties of the service, change the startup type to ***Manual***, and click **Start**.
- To find an event that indicates that a log was cleared in the Event Viewer, filter by the relevant ID.