EC-Council

codered
FROM EC-COUNCIL

Module 18

NETWORK LOGS MONITORING AND ANALYSIS

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Module 18:
Network Logs Monitoring and Analysis

LAB SCENARIO

Extensive monitoring and analysis of network logs is critical to enhance the security of an organization. This helps identify and respond to threats quickly and protect the network assets from various attacks. Proper network log monitoring and analysis help reduce the frequency of attacks by proactively responding to threats.

A security professional must have the required knowledge to monitor network logs and further analyze them for any malicious or suspicious activity within the local network.

LAB OBJECTIVE

The objective of this lab is to provide expert knowledge in monitor and analyze network logs. This includes knowledge of the following tasks:

- Configure, view and analyze system logs using Windows Event Viewer
- View and analyze event logs of Windows and Linux system

OVERVIEW OF LOGS MONITORING AND ANALYSIS

Logs are a collection of information/data on events generated in the form of an audit trail by the various components of an information system such as network, applications, operating system (OS), service, etc. A log can provide an indication that something may have gone wrong and can help security professionals in analyzing and detecting issues.

A proper analysis of log data enables actionable information to be identified, which helps the security professional in detecting and monitoring potential security breaches, internal misuse of information, operational issues, and other long-term issues. It also helps validate whether the end-user has followed all documented protocols to detect fraudulent activities and policy violations. It is also useful for internal investigations, security auditing and forensic analysis, determination of operational trends, and implementation of baselines.

LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to monitor network logs. The recommended labs that will assist you in learning the monitoring and analyzing network logs include the following:

01 Configure, View, and Analyze Windows Event Logs

02 View and Analyze Windows Logs

03 View and Analyze Linux Logs

Note: Turn on **PfSense Firewall** virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: **CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS**

Windows OS tracks various events, activities, and functions through logs.

LAB SCENARIO

A security professional should be aware of the logging mechanism in Windows OS, where the logs are stored, the configuration needed to log a specific type of incident, and the format of logs among others. In this lab task, you will audit the Windows event, where the audit shows the success or failure of specific security events.

LAB OBJECTIVE

The objective of this lab is to learn how to configure, view, and analyze Windows security logs.

OVERVIEW OF WINDOWS EVENT LOGS

Windows event logs include critical information such as log-on failures, log tampering, failed attempts to access files, etc. They also warn about upcoming system issues and protect the system from unexpected disasters. In addition to this, these event logs may also describe an attempt by a user to compromise the system or an unsanctioned configuration change. Thus, these event logs need to be monitored and analyzed to identify network vulnerabilities, security breaches, and threats from intruders.

These event logs enable security professionals to protect a network against internal threats and vulnerabilities. Windows Event Viewer is the most common way to monitor and analyze Windows event logs.

LAB TASKS

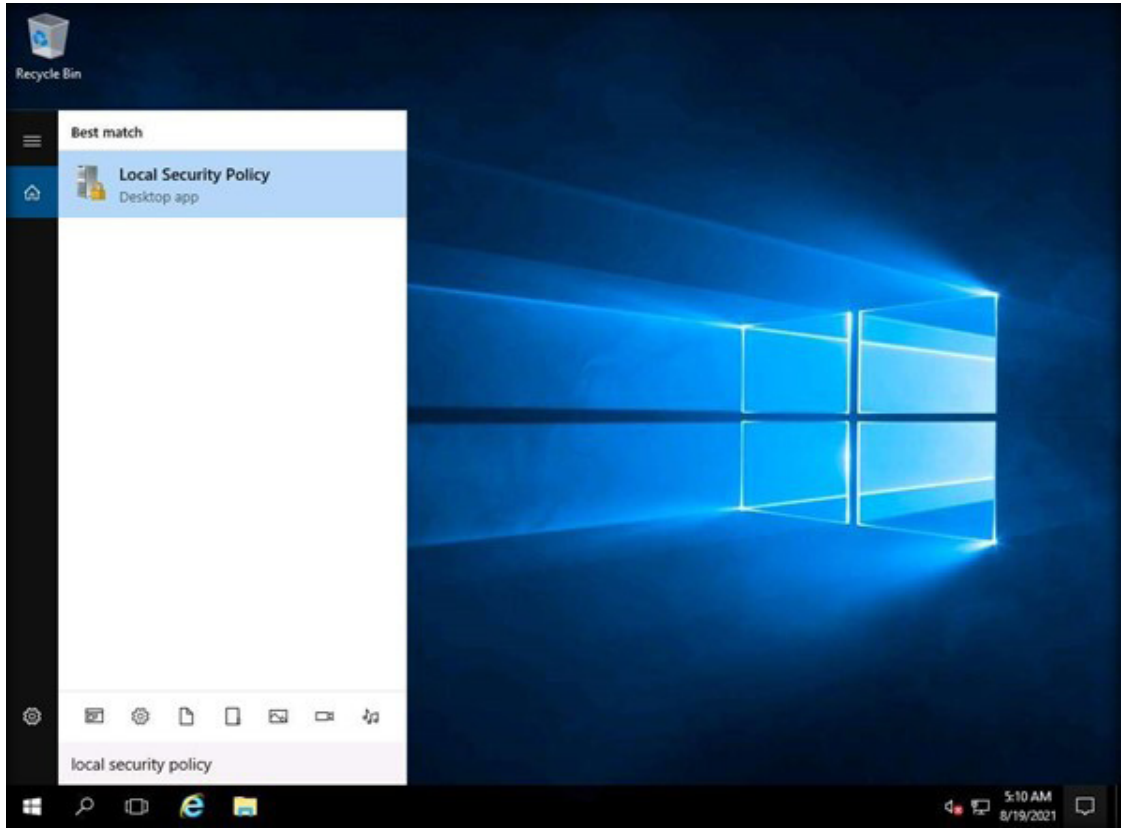
Note: Ensure that **PfSense Firewall** virtual machine is running.

EXERCISE 1: CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

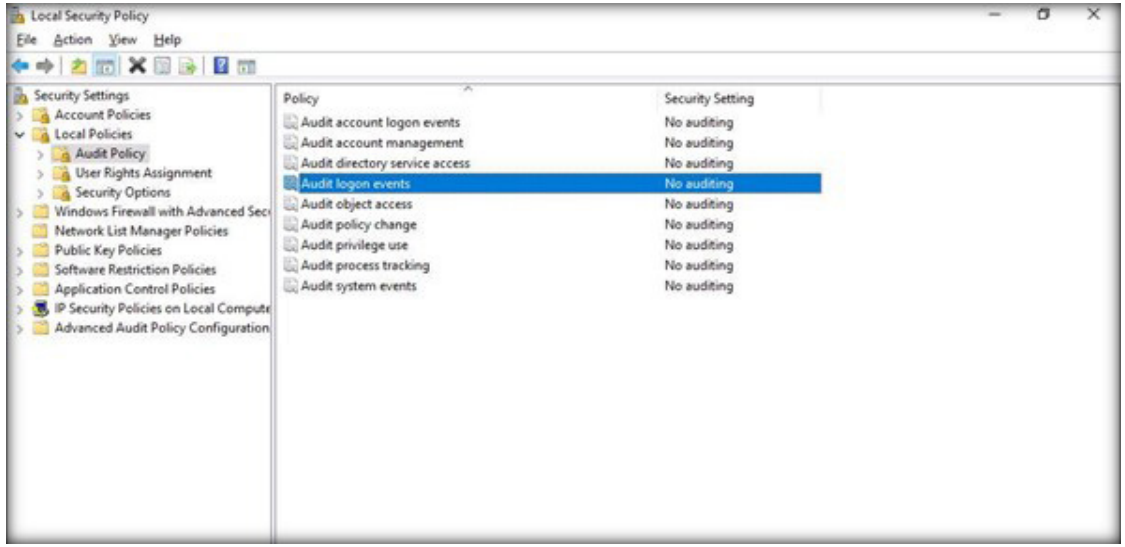
1. Turn on the **Web Server** virtual machine.

2. Log in with the credentials **Administrator** and **admin@123**.

3. Click on the **Search Windows** icon and type **"local security policy"** in the search textbox, and press then **Enter** button.



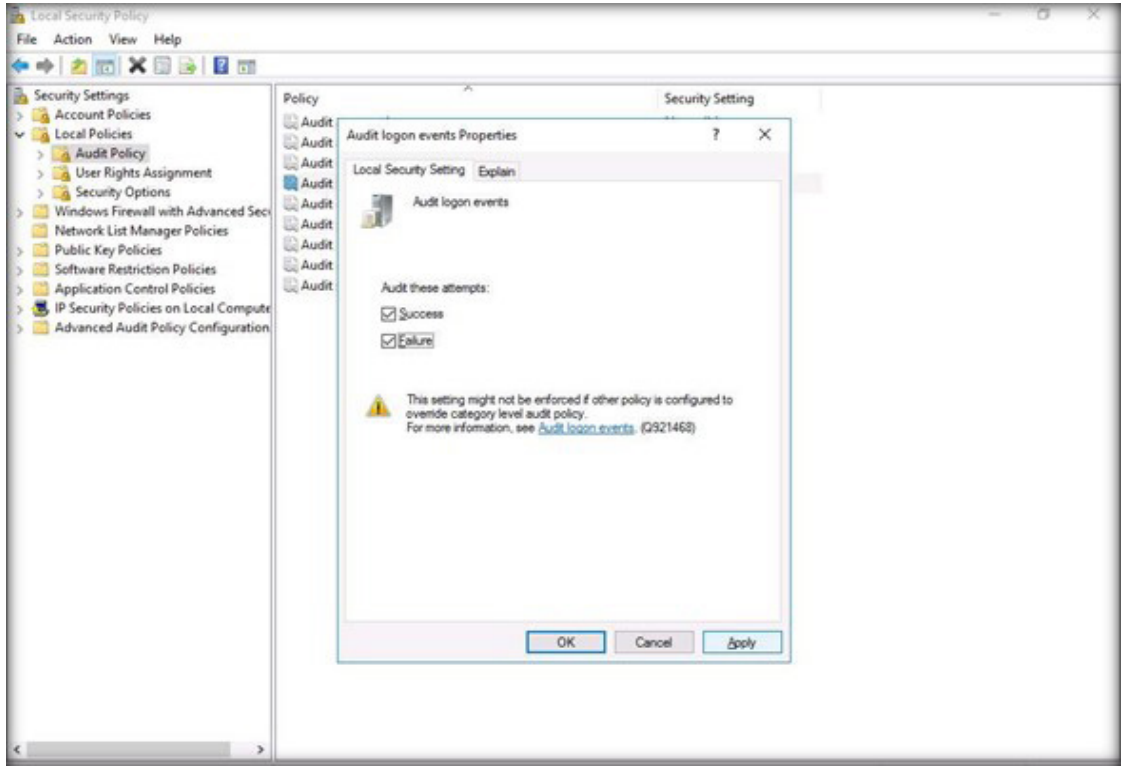
4. The **Local Security Policy** window will open. In the left pane, expand **Local Policies** and click on **Audit Policy**. Then, double-click on **Audit logon events** in the right pane.



EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

5. The **Audit logon events Properties** window will appear. Check **Success** and **Failure**, then click on **Apply** and **OK**.



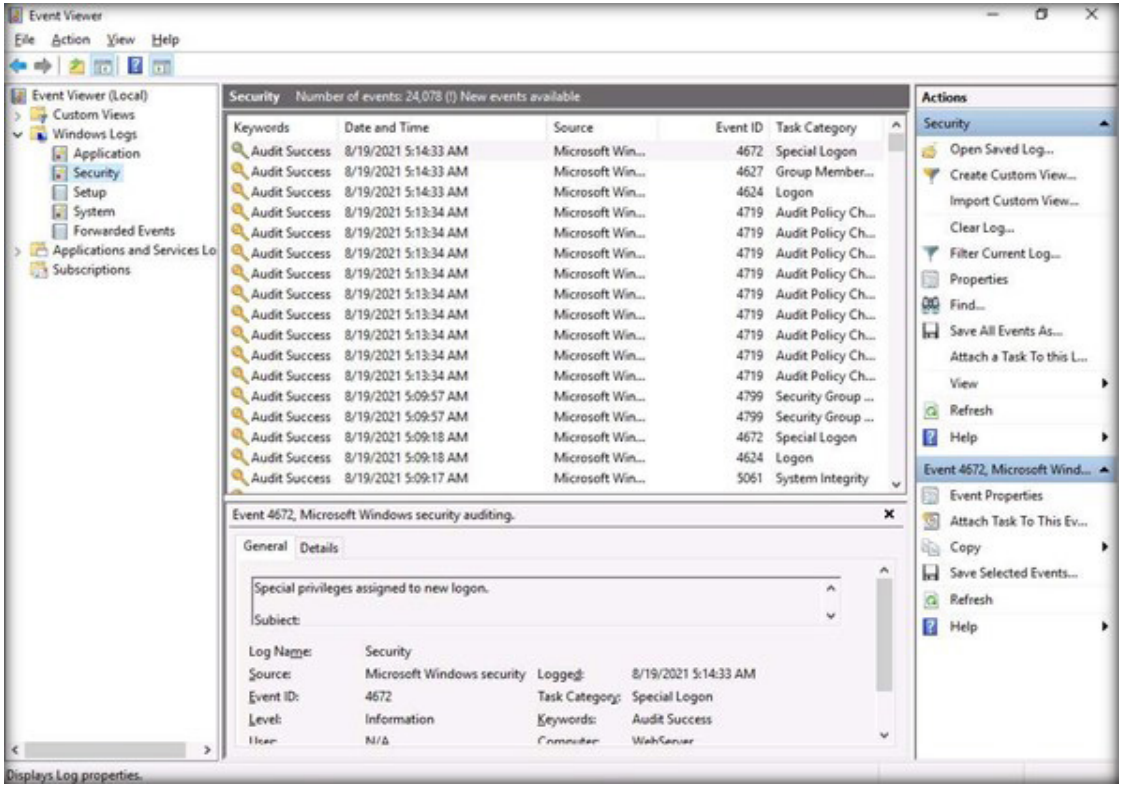
6. Close the **Local Security Policy** window.

7. To view the events, right-click on the **Start** icon and then on **Event Viewer** to open it.

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

8. Expand **Windows Logs** in the left pane and click on **Security**. This will list the audit logs entries.

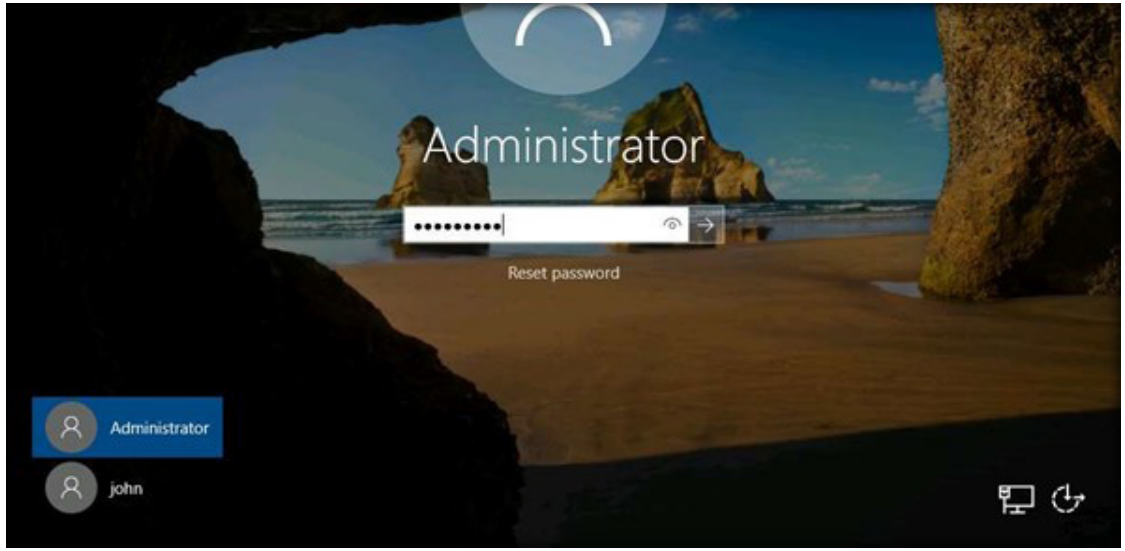


9. Close the **Event Viewer** window. **Sign out** and try to log in to the **Web Server** machine twice/thrice using invalid passwords to generate logs related to failed login attempts.

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

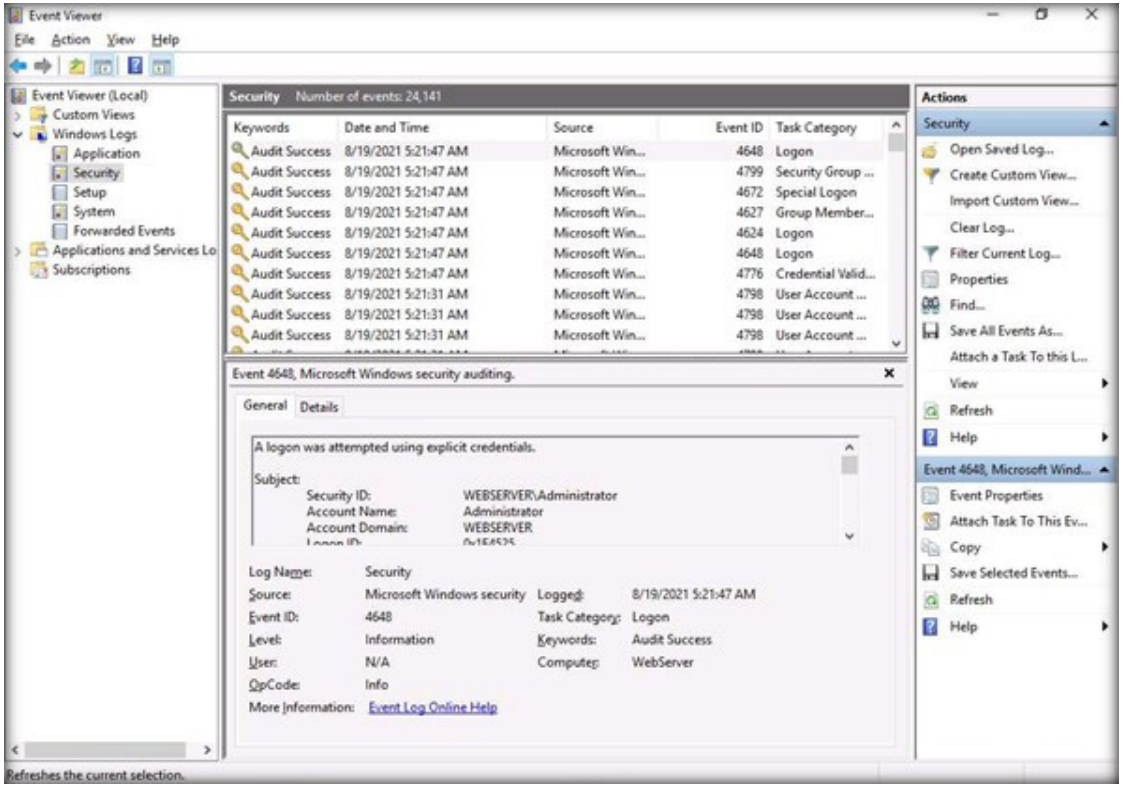
10. Now, sign into **Web Server** with the credentials **Administrator** and **admin@123**.



11. To view the events, right-click on the **Start** icon and then on **Event Viewer** to open it.
    Note: If the **network** screen appears, click **Yes**.

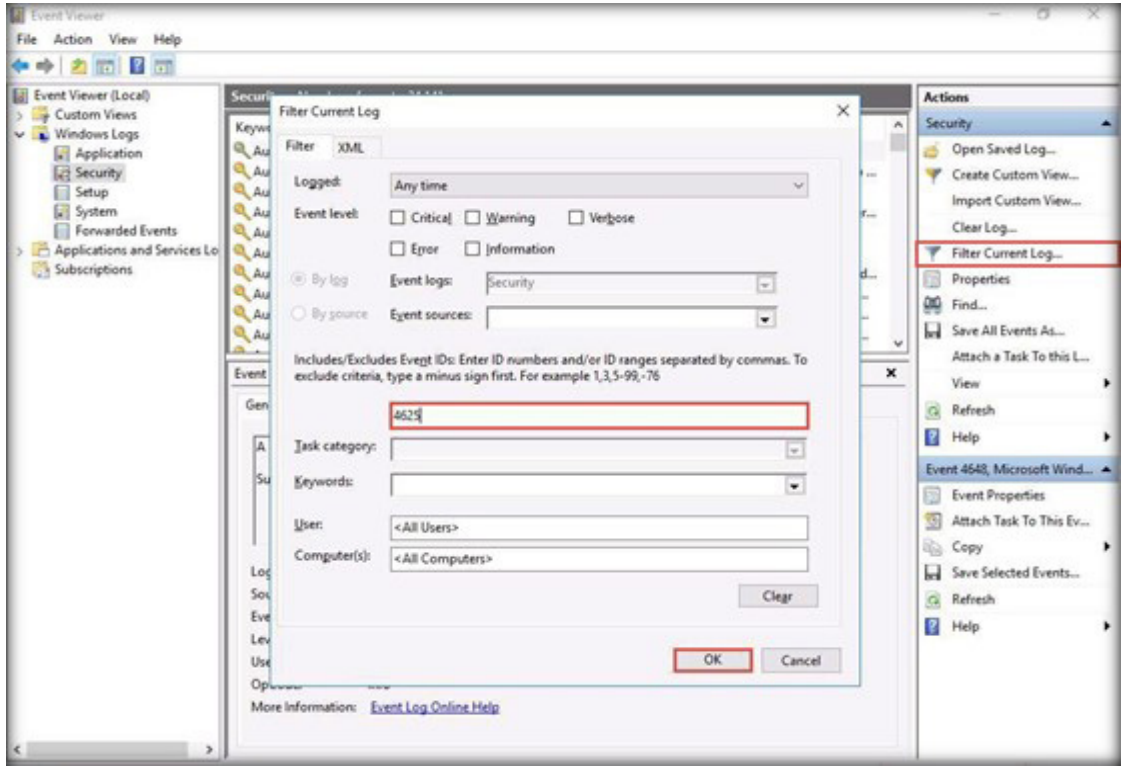
12. Expand **Windows Logs** in the left pane and click on **Security**. This will list the audit logs entries.

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS



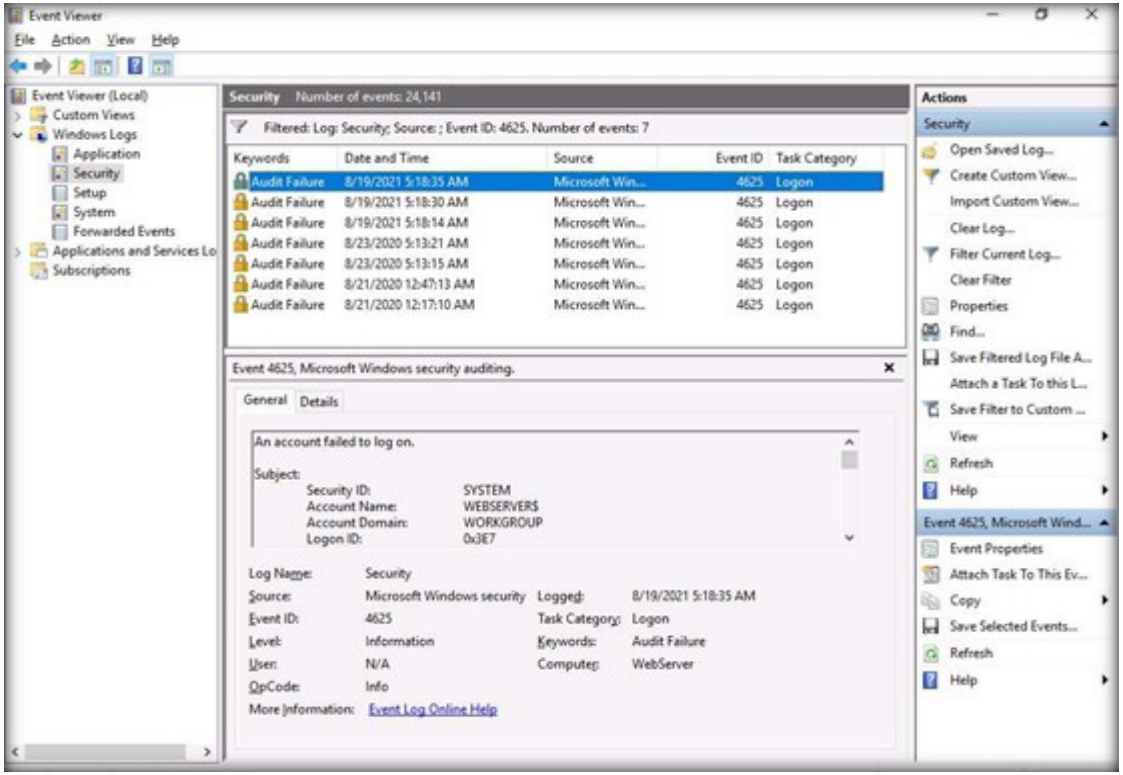
13. To view the login failure events, click on **Filter Current Log...** in the right pane and search for event ID **4625** to filter logs related to failed login attempts. Then, click **OK**.

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS



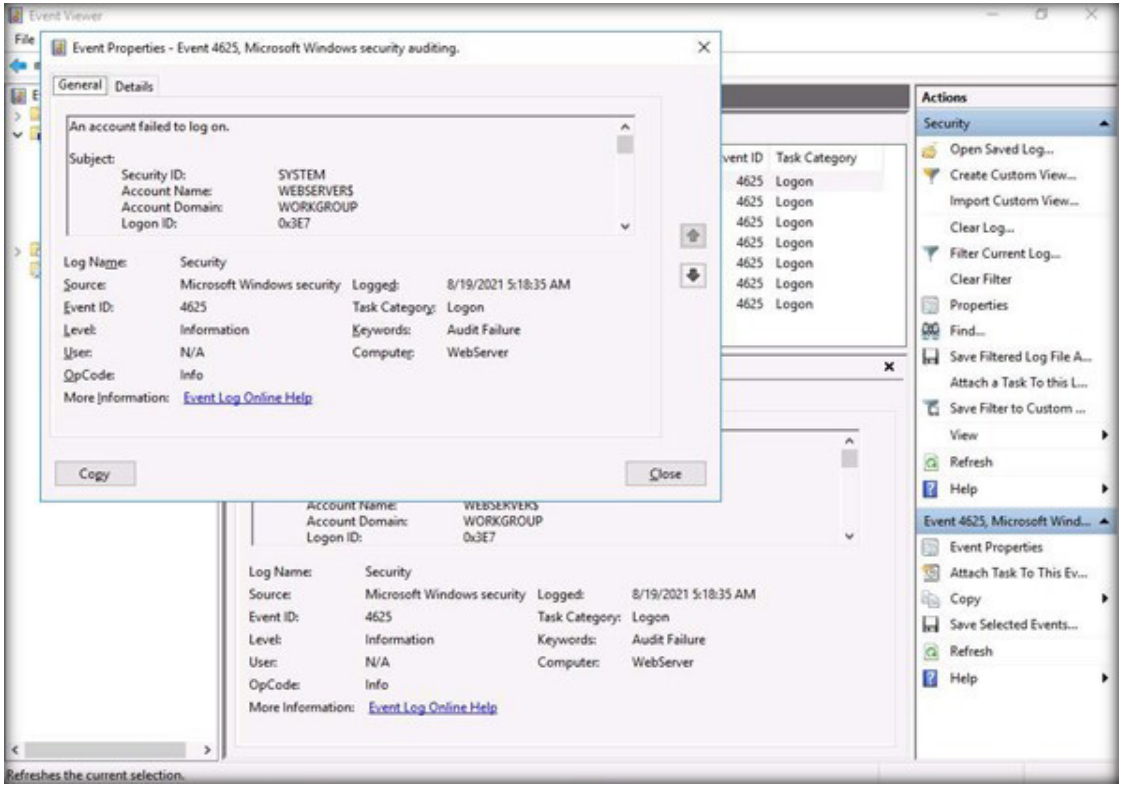
EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS

14. The entries of all **Audit Failure logs** will be listed, as shown in the screenshot below.



15. Double-click on one of the entries to **view** its details.

EXERCISE 1:
CONFIGURE, VIEW, AND ANALYZE WINDOWS EVENT LOGS



16. This concludes the demonstration showing how to configure, view and analyze Windows Event Logs.

17. Close all open windows.

18. Turn off the **Web Server** virtual machine.

EXERCISE 2: **VIEW AND ANALYZE WINDOWS LOGS**

Windows OS tracks various events, activities, and functions through logs.

LAB SCENARIO

A security professional should be aware of the path where event logs are stored, apart from being familiar with the format of logs, types of logs and categories of severity levels, in order to examine them for any malicious activities such as unauthorized access, data theft, deletion of sensitive information, etc.

LAB OBJECTIVE

The objective of this lab is to learn how to view and analyze Windows event logs.

OVERVIEW OF WINDOWS LOGS

Windows event logging service collects events from multiple sources and keeps them in a single location known as Windows event log. These logs act as the primary source of evidence for all important actions/activities on a Windows system. Windows event log contains logs of system, security, and application notifications that are monitored and analyzed by security professionals to detect issues in the system.

Based on their severity levels, events are categorized into five types:

- **Error**: This type of event describes a significant problem such as loss of data or functionality.
- **Warning**: This type of event is of less importance but may describe a possible future problem.
- **Information**: This type of event indicates the successful operation of an application, driver, or service.
- **Success Audit**: This type of event is recorded when any successfully audited security access attempt is detected.
- **Failure Audit**: This type of event is recorded when any unsuccessful audited security access attempt is detected.

LAB TASKS

Note: Ensure that **PfSense Firewall** virtual machine is running.

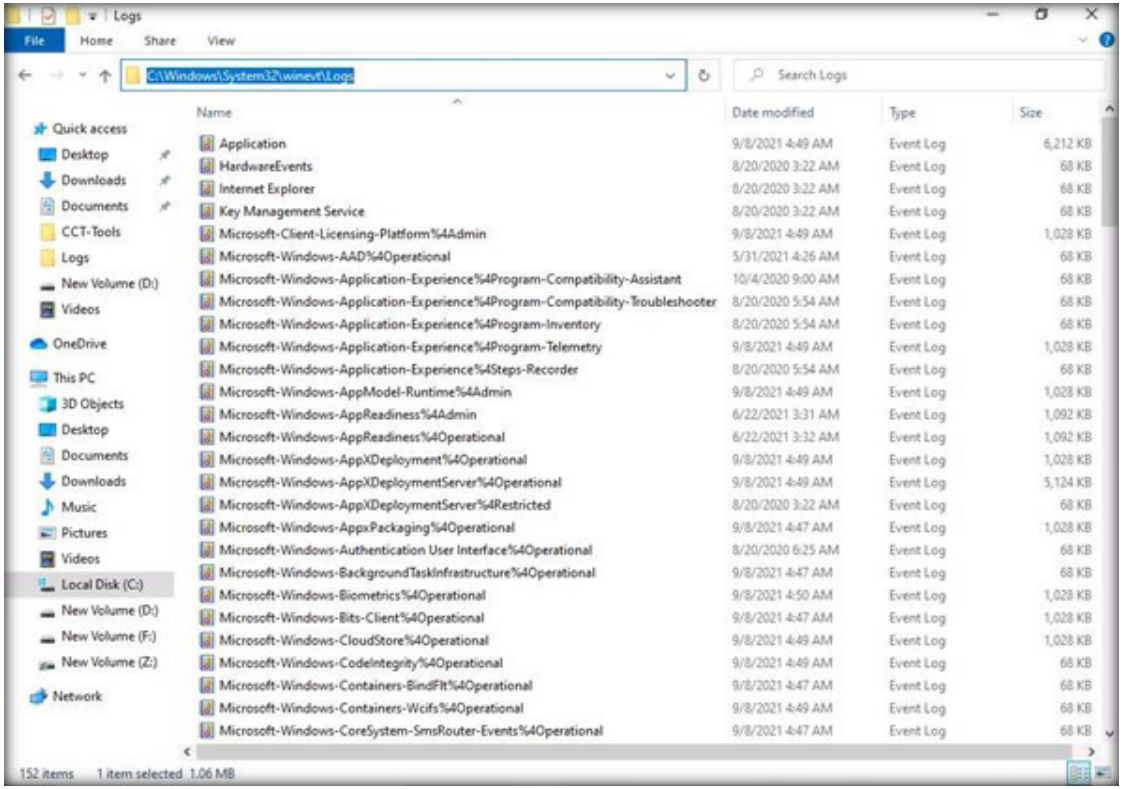
1. Turn on the **Admin Machine-1** virtual machine.

2. Log in with the credentials **Admin** and **admin@123**.
   Note: If a network screen appears, click **Yes**.

3. Open **File Explorer** and navigate to **C:\Windows\System32\winevt\Logs** to view the system logs.

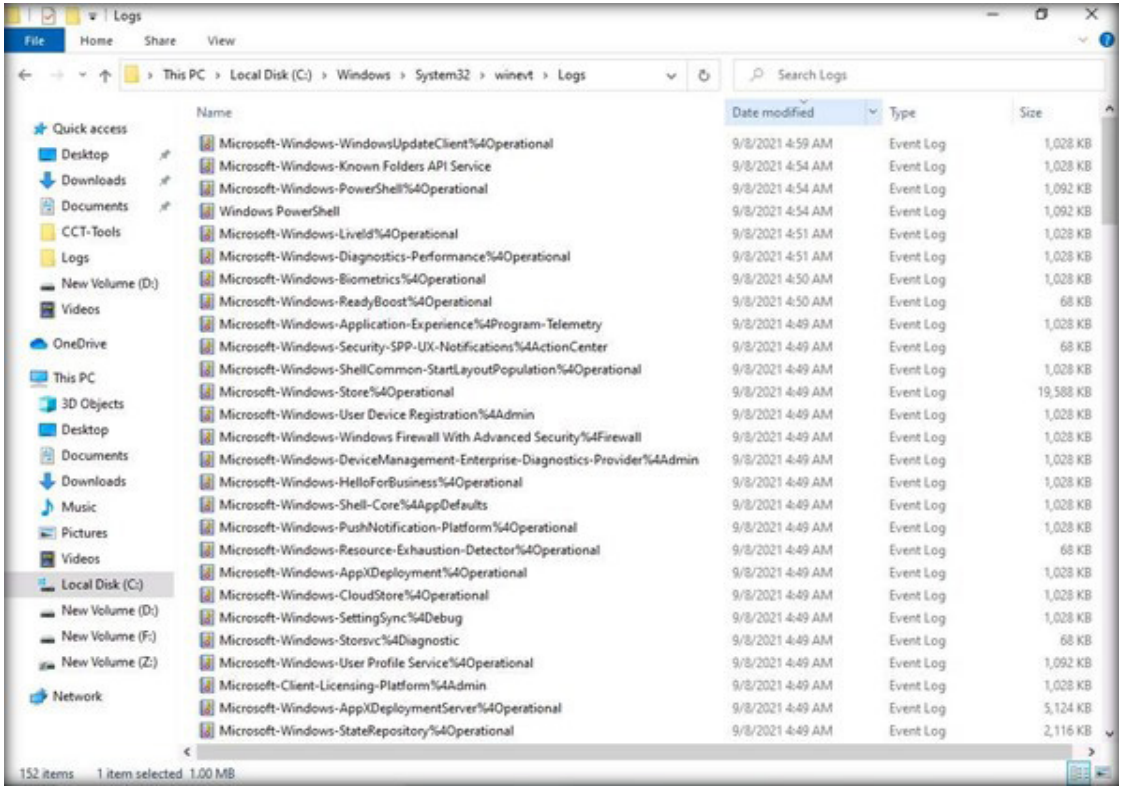
4. You can observe the event logs captured within the system, as shown in the screenshot below.
   Note: Databases related to the system are stored in a file named **System.evtx**, the databases related to security are stored in a file named **Security.evtx**, and the databases related to applications are stored in a file named **Application.evtx**.

EXERCISE 2: VIEW AND ANALYZE WINDOWS LOGS



EXERCISE 2:
VIEW AND ANALYZE
WINDOWS LOGS

5. You can click on the **Date modified** column to sort the event logs with the latest event on the top, as shown in the screenshot below.



6. Now, double-click on any log (here, **Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall**) to view a detailed information about the captured event.

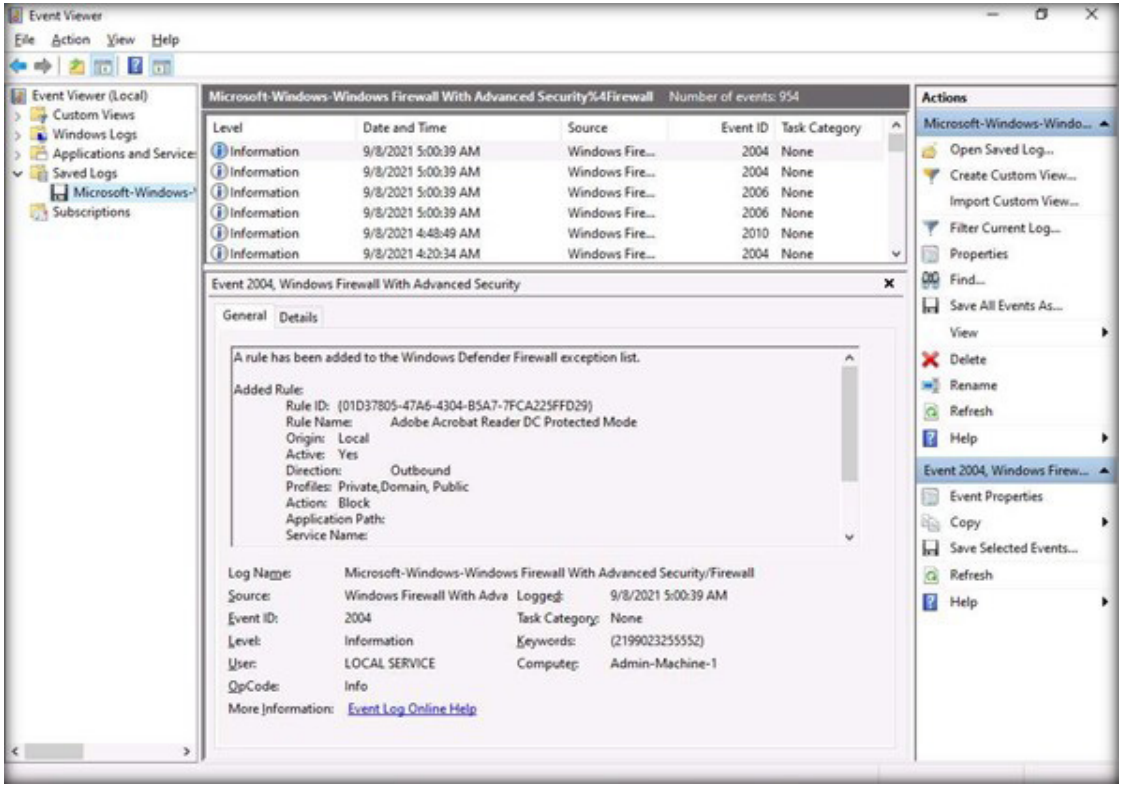
7. An **Event Viewer** window appears, displaying the information about the selected event. The event is categorized as **Information**, as shown in the screenshot below.

Note: The **Number of events** might vary in your lab environment.

The information about the event displayed in the Preview pane is described below:

- **Log Name**: The type of Windows log.
- **Source**: Source is the cause responsible for the event raised by either an individual or a system or a program.
- **Event ID**: The type of event that has occurred.
- **Level**: Event level is divided into five types: Error, Warning, Information, Success Audit, and Failure Audit.
- **User**: User responsible and who logged on to the computer at the instance of the event.
- **Logged**: The timestamp of the event.
- **Task category**: Primarily used in case for a security log that classifies an event based on the event source.
- **Keyword**: Unique number of the event.
- **Computer**: The name assigned to the computer where the event occurred.

EXERCISE 2: VIEW AND ANALYZE WINDOWS LOGS



8. You can further navigate to the **Details** tab to view information such as Provider, Event ID, Level, Task, and TimeCreated.

9. This concludes the demonstration showing how to view and analyze Windows event logs.

10. Close all open windows.

11. Turn off the **Admin Machine-1** virtual machine.

EXERCISE 3: **VIEW AND ANALYZE LINUX LOGS**

Linux logs are a record of any activity or event in a Linux-based OS.

LAB SCENARIO

Log files should be monitored to predict any upcoming issues before they actually occur. However, monitoring and analyzing all log files to determine which file contains the required information can be cumbersome. Therefore, to make the process a little simpler, a few critical Linux log files are introduced here; they should be monitored effectively to gather all essential information.

A security professional should be aware of the logging mechanism of Linux OS, and where the logs are stored. In this lab task, you will view and analyze the Linux event logs.

LAB OBJECTIVE

The objective of this lab is to learn how to view and analyze Linux event logs.

OVERVIEW OF LINUX LOGS

Linux logs include messages on just about everything, including system, kernel, package managers, boot processes, Xorg, Apache, and MySQL. These log files are useful for troubleshooting any security issue. They help in monitor and analyze security threats and vulnerabilities and remediate them as soon as possible. They also help in tracking the communication between systems and networks.

LAB TASKS

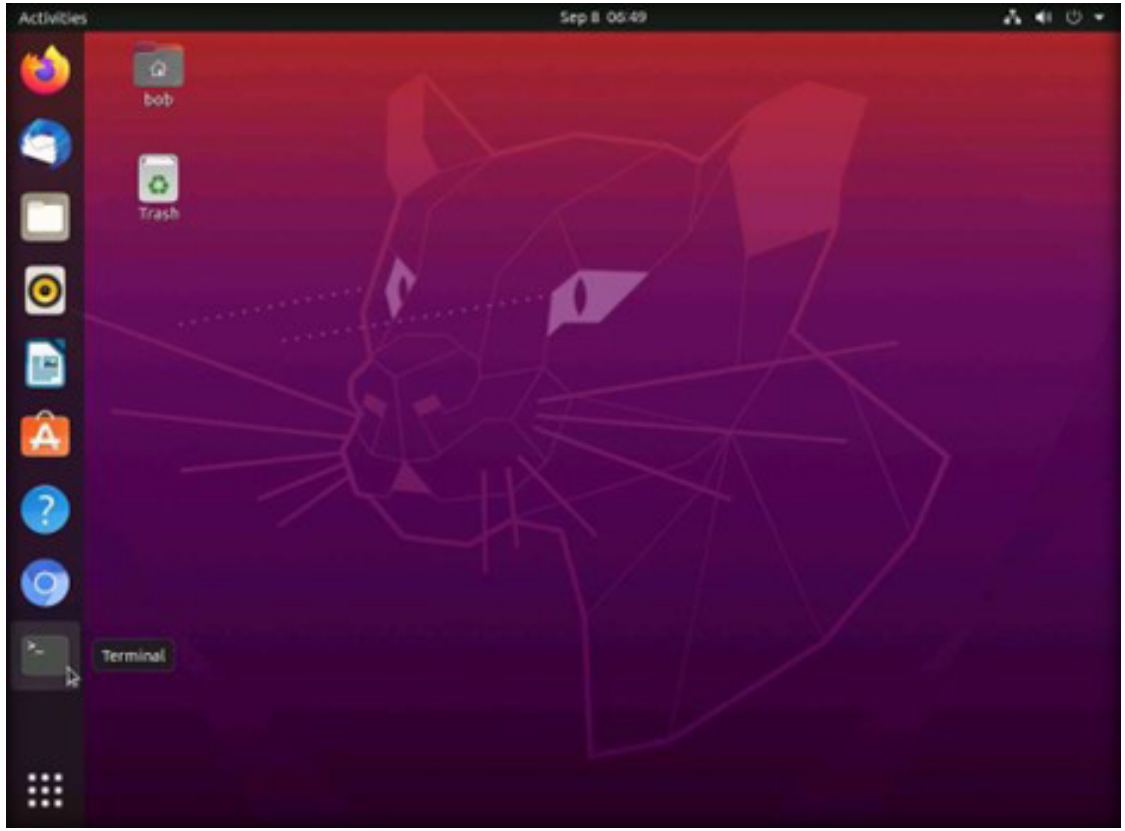
Note: Ensure that **PfSense Firewall** virtual machine is running.

EXERCISE 3: VIEW AND ANALYZE LINUX LOGS

1. Turn on the **Attacker Machine-1** virtual machine.

2. Click to select **Bob** account. In the **Password** field, type **user@123** and press **Enter** to sign in.

3. In the left pane, scroll down under **Activities** list and click on the terminal icon to open a **Terminal** window.



4. In the **Terminal** window, type **sudo su** and press **Enter** to use the terminal as a superuser.
   Note: In the **[sudo] password for bob** field, enter **user@123** and press **Enter**.

5. Type **cd /var/log** and press **Enter** to navigate to the /var/log location.
   Note: In Linux machines, event logs are located in the **/var/log** directory and subdirectory in plain ASCII text format. These system and service log files provide information about OS-specific or service-specific issues.

6. Type **ls** and press **Enter** to view the event logs in the **/log** directory.

7. You can observe the event log files appear, as shown in the screenshot below.

EXERCISE 3: VIEW AND ANALYZE LINUX LOGS

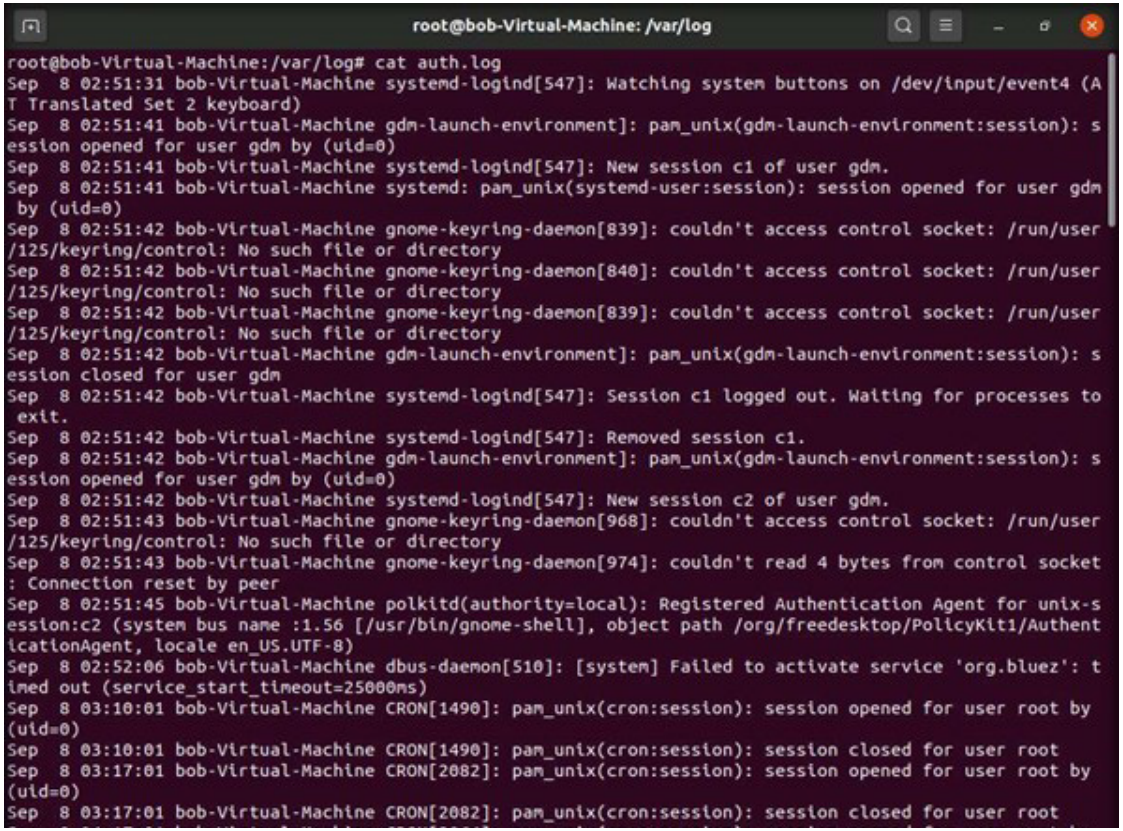
EXERCISE 3:
VIEW AND ANALYZE
LINUX LOGS

8. Now, we will open an event log to view its content.

9. Type **cat auth.log** and press **Enter** to view authentication related event logs.

   Note: **auth.log** file contains authentication logs, including both successful and unsuccessful user login attempts as well as authentication techniques. This file is beneficial if you want to examine brute-force attacks and other vulnerabilities related to user authorization.

10. The content of log file appears, displaying information on authentication with respect to time and date, as shown in the screenshot below.



EXERCISE 3:
VIEW AND ANALYZE
LINUX LOGS

11. Now, type **cat boot.log** and press **Enter** to view boot related logs.

    Note: **boot.log** file stores all information related to system booting. The booting messages are sent by system initialization script, **/etc/init.d/bootmisc.sh**, to this log file. This file is helpful when trying to troubleshoot problems related to improper shutdowns, booting failures, or unplanned reboots. By checking this file, the time span of a system downtime because of an unexpected shutdown can be determined.

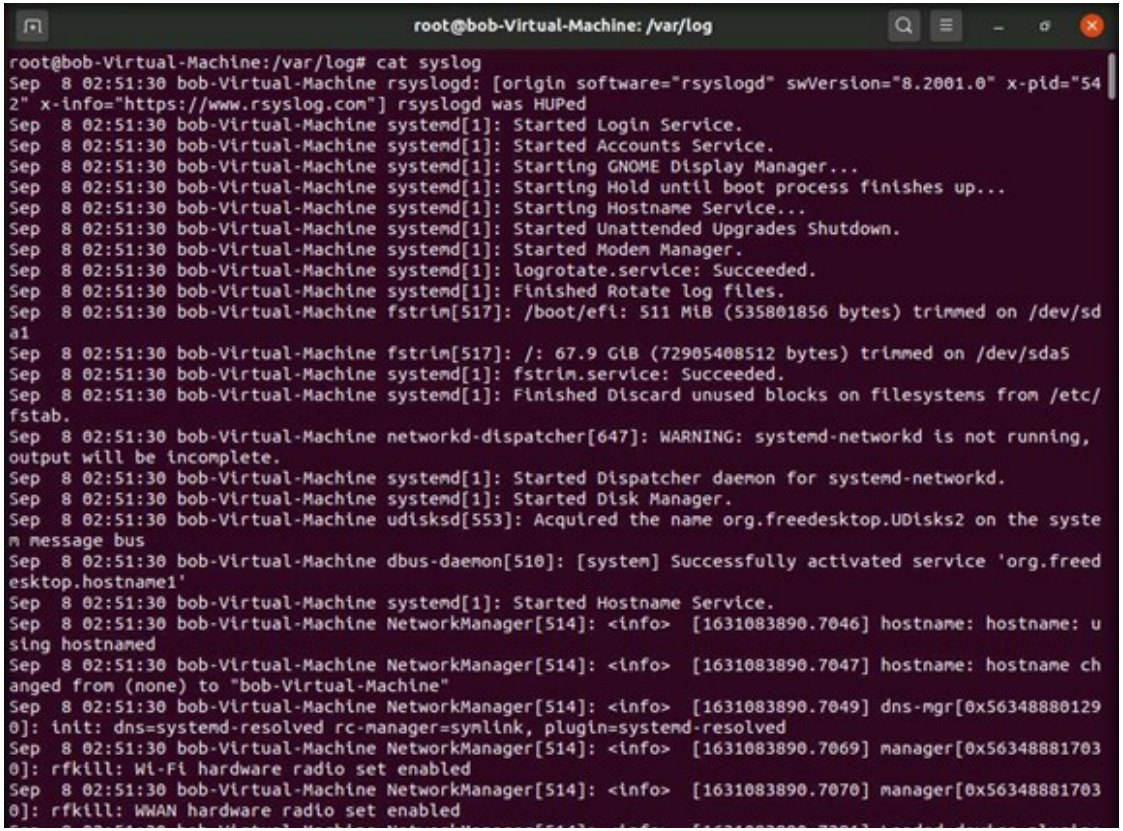
12. The content of log file appears, displaying the status of system processes, as shown in the screenshot below.

EXERCISE 3:
VIEW AND ANALYZE
LINUX LOGS

13. Type **cat syslog** and press **Enter** to view the file containing general messages and system-related information.

    Note: **syslog** or **message** stores all informational and noncritical messages across the global system such as system error messages, system startups, and shutdowns, change in the network configuration, etc. It can also log several things such as mail, cron, daemon, kern, auth, etc.

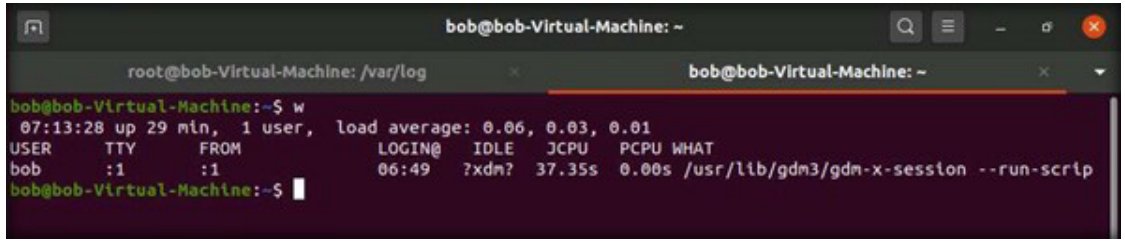
14. The content of log file appears, displaying information related running processes, as shown in the screenshot below.



15. Similarly, you can explore other log files to assess system security.

16. Now, open another **Terminal** window by clicking the ( ) icon from the top-left corner of the **Terminal** window.

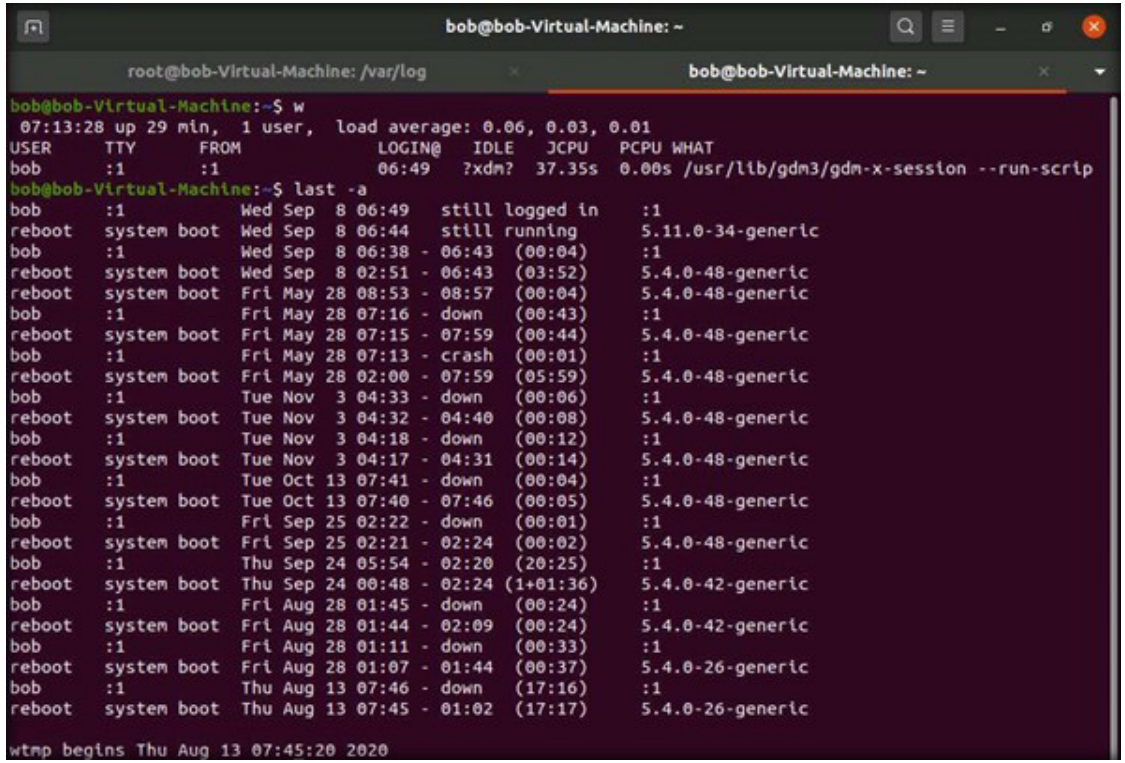
17. A new **Terminal** appears in another tab. Type **w** and press **Enter** to display the time for which the machine has been up since login.



EXERCISE 3:
VIEW AND ANALYZE
LINUX LOGS

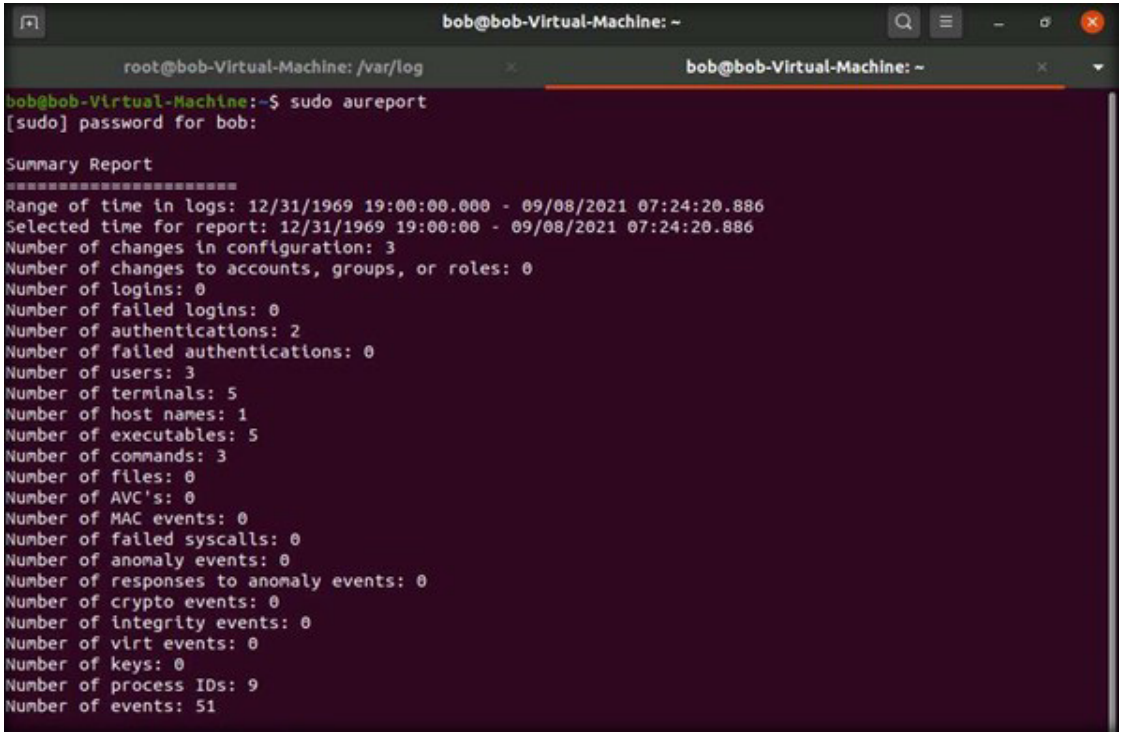
EXERCISE 3:
VIEW AND ANALYZE
LINUX LOGS

18. Type **last -a** and press **Enter** to gather the details of last login sessions.



19. Type **sudo aureport** and press **Enter** to fetch the details of all login attempts made to the system.

20. In the **[sudo] password for bob** field, enter **user@123** and press **Enter**.
    Note: The password you enter will not be visible.



21. This concludes the demonstration showing how to view and analyze system logs in Linux machine.

22. Close all open windows.

23. Turn off **Attacker Machine-1** and **PfSense Firewall** virtual machines.


EC-Council