



# Module 18 **NETWORK LOGS** MONITORING AND ANALYSIS

## CERTIFIED CYBERSECURITY TECHNICIAN

Copyrights @ 2021 EC-Council International Ltd.





# INDEX

#### Module 18: Network Logs Monitoring and Analysis

Exercise 1: Configure, View, and Analyze Windows Event Logs	05
<b>Exercise 2:</b> View and Analyze Windows Logs	18
Exercise 3: View and Analyze Linux Logs	25





#### 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:



Configure, View, and Analyze Windows Event Logs



View and Analyze Windows Logs



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.







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.



Local Security Policy			-	σ	×
the Action Yiew Help					
<ul> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Security Options</li> <li>Windows Firewall with Advanced Second Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Control Policies</li> <li>Software Audit Policy Configuration</li> </ul>	Policy Audit account logon events Audit account management Audit directory service access Audit object access Audit policy change Audit policy change Audit process tracking Audit system events	Security Setting No auditing No auditing No auditing No auditing No auditing No auditing No auditing No auditing			



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



Security Settings p	~	Security Settin	ing	
Account Policies     Local Policies     Local Policies     Audit Policy     Government     Security Options     Windows Frewall with Advanced Sec     Network List Manager Policies     Public Key Policies     Software Restriction Policies     Application Control Policies     Ploscurity Policies on Local Compute     Advanced Audit Policy Configuration	vents Properties Setting Explan St logon events se attempts: set setting might not be enforced if ride category level audt policy. nore information, see <u>Audit logon</u>	? ther policy is configured to <u>overtia</u> . (2921468) Cancel <u>A</u> sc	×	





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.





W, AND

00



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.









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.



Event Viewer (Local)	Security Number		Actions				
<ul> <li>Gustom Views</li> <li>Windows Logs</li> <li>Application</li> </ul>	Keywords	Date and Time	Source	Event ID	Task Category	^	Security
	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4648	Logon		Open Saved Log
Security	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4799	Security Group		Treate Custom Vi
Setup	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4672	Special Logon		Incode Condense M
System	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4627	Group Member		Import Custom Vi
Forwarded Events	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4624	Logon		Clear Log
Applications and Services Lo	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4648	Logon		Filter Current Log
Subscriptions	Audit Success	8/19/2021 5:21:47 AM	Microsoft Win	4776	Credential Valid		Descention .
	Audit Success	8/19/2021 5:21:31 AM	Microsoft Win	4798	User Account		Propertes
	Audit Success	8/19/2021 5:21:31 AM	Microsoft Win	A 4798	User Account		Find_
	Q Audit Success	8/19/2021 5:21:31 AM	Microsoft Win	4798	User Account		Save All Events As
	a	A 10 A 10 A A A A A A A A A A A A A A A				~	Attach a Task To t
	Event 4648, Micros	View					
	General Details						G Refresh
							Helo
	A logon was at	tempted using explicit credentia	da,		^		
	Subject						Event 4648, Microsoft
	Securi	ity ID: WEBSERVI	R\Administrator				Event Properties
	Accou	unt Name: Administr	ator				Attach Tark To Th
	Accou	unt Domain: WEBSERVE	ER		~		
						1	Copy
	Log Name:	Security					Save Selected Eve
	Source:	Microsoft Windows security	y Logged: 8/1	19/2021 5:21:47 AM			G Refresh
	Event ID:	4648	Task Category: Lo	gon			E Hale
	Level	Information	Keywords: Au	dit Success		111	I meip
	User	N/A	Computer: We	ebServer			
	Orfode	Info	company in				
	Specide	into the contraction					
	More informatio	on: Event Log Unline Help					



W, AND

00



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**.

Event Viewer (Local)	Securi Filter Current L	og	×	Actions
<ul> <li>Windows Logs</li> <li>Application</li> <li>Security</li> <li>Setup</li> <li>System</li> <li>Forwarded Events</li> <li>Applications and Services Lo</li> <li>Subscriptions</li> </ul>	Keywe Au Au Au Au Au Au Au Au Au Au	Any time  Critical  Kyent logs:  Security  Egent sources:  Clagr  Clagr  Event Log Online Help	4. 	Create Custom Import Custom Clear Log  Create Custom Import Custom Clear Log  Friter Current L Sove All Events Attach a Task T View Refresh Help Event 4648, Microso Event Propertie Event Propertie Sove Selected I Refresh Help Help Help

14

EW, AND

00



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.



Event Propertie	es - Event 4625, Microsoft Wind	ows security auditing.		×			
General Details							Actions
An account fail Subject: Securi	ed to log on. tv ID: SYSTEM		, i	~	vent ID	Task Category	Security Open Saved Log Create Custom View
Accou Accou Logor	int Name: WEBSERV Int Domain: WORKGR/ ID: 0x3E7	WEBSERVERS WORKGROUP 0x3E7 V				Logon Logon Logon	Import Custom View. Clear Log
Log Name Source: Event ID: Level:	Security Microsoft Windows securit 4625 Information	y Loggeg: 8/19/2021 5 Task Category: Logon Keywords: Audit Failur	18:35 AM	•	4625 4625 4625	Logon Logon	Filter Current Log Clear Filter  Properties  Clear Find
User: OpCode: More Information	N/A Info m: <u>Event Log Online Help</u>	Computer WebServer				×	Attach a Task To this L
Cogy				Glose		î	Ci Refresh
	Acco	unt Name: WEBSER unt Domain: WORKGF n ID: 0x3E7	OUP			v	Event 4625, Microsoft Wine
	Log Name: Source: Event ID: Level: User: OpCode: More Informat	Security Microsoft Windows securi 4625 Information N/A Info on: <u>Event Log Online Help</u>	ty Logged: Task Category: Keywords: Computer:	8/19/2021 5:18:3 Logon Audit Failure WebServer	IS AM		Even Properties     Attach Task To This Ev     Copy     Save Selected Events     Refresh     Help





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.

19

ANAL





![](_page_20_Picture_1.jpeg)

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.

🕆 📕 > Th	is PC → Local Disk (C:) → Windows → System32 → winevt → Logs 🛛 🗸 Ö	,O Search Logs		
	Name	Date modified	Type	Size
A Quick access	Microsoft-Windows-WindowsUpdateClient%4Operational	9/8/2021 4:59 AM	Event Log	1.028
Desktop 📌	Microsoft-Windows-Known Folders API Service	9/8/2021 4:54 AM	Event Log	1,028
Downloads **	Microsoft-Windows-PowerShell%40perational	9/8/2021 4:54 AM	Event Log	1,092
🖹 Documents 🦽	Windows PowerShell	9/8/2021 4:54 AM	Event Log	1,092
CCT-Tools	Microsoft-Windows-Liveld%4Operational	9/8/2021 4:51 AM	Event Log	1,025
Logs	Microsoft-Windows-Diagnostics-Performance%40perational	9/8/2021 4:51 AM	Event Log	1,025
- New Volume (D)	Microsoft-Windows-Biometrics%40perational	9/8/2021 4:50 AM	Event Log	1,028
Videor	Microsoft-Windows-ReadyBoost%4Operational	9/8/2021 4:50 AM	Event Log	6
a videos	Microsoft-Windows-Application-Experience%4Program-Telemetry	9/8/2021 4:49 AM	Event Log	1,02
<ul> <li>OneDrive</li> </ul>	Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter	9/8/2021 4:49 AM	Event Log	6
This DC	Microsoft-Windows-ShellCommon-StartLayoutPopulation%4Operational	9/8/2021 4:49 AM	Event Log	1,02
ins PC	Microsoft-Windows-Store%40perational	9/8/2021 4:49 AM	Event Log	19,58
3D Objects	Microsoft-Windows-User Device Registration%4Admin	9/8/2021 4:49 AM	Event Log	1,02
Desktop	Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall	9/8/2021 4:49 AM	Event Log	1,02
Documents	Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin	9/8/2021 4:49 AM	Event Log	1,02
Downloads	Microsoft-Windows-HelloForBusiness%4Operational	9/8/2021 4:49 AM	Event Log	1,02
1 Music	Microsoft-Windows-Shell-Core%4AppDefaults	9/8/2021 4:49 AM	Event Log	1,02
E Pictures	Microsoft-Windows-PushNotification-Platform%4Operational	9/8/2021 4:49 AM	Event Log	1,02
Videos	Microsoft-Windows-Resource-Exhaustion-Detector%4Operational	9/8/2021 4:49 AM	Event Log	6
The sector sector	Microsoft-Windows-App)(Deployment%40perational	9/8/2021 4:49 AM	Event Log	1,02
Local Disk (C:)	Microsoft-Windows-CloudStore%4Operational	9/8/2021 4:49 AM	Event Log	1,02
<ul> <li>New Volume (D:)</li> </ul>	Microsoft-Windows-SettingSync%4Debug	9/8/2021 4:49 AM	Event Log	1,02
<ul> <li>New Volume (F:)</li> </ul>	Microsoft-Windows-Storsvc%4Diagnostic	9/8/2021 4:49 AM	Event Log	6
Im New Volume (Z:)	Microsoft-Windows-User Profile Service%40perational	9/8/2021 4:49 AM	Event Log	1,09
Alabarach	Microsoft-Client-Licensing-Platform%4Admin	9/8/2021 4:49 AM	Event Log	1,02
- rectwork	Microsoft-Windows-App//DeploymentServer%40perational	9/8/2021 4:49 AM	Event Log	5,12
	Microsoft-Windows-StateRepository%4Operational	9/8/2021 4:49 AM	Event Log	2,11

EXERCISE 2: VIEW AND ANALYZE WINDOWS LOGS

![](_page_21_Picture_1.jpeg)

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.

ANALYZI

ŝ

![](_page_22_Picture_1.jpeg)

![](_page_22_Picture_2.jpeg)

23

![](_page_23_Picture_1.jpeg)

- 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.

![](_page_24_Picture_1.jpeg)

## 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.

![](_page_25_Picture_0.jpeg)

![](_page_25_Picture_1.jpeg)

![](_page_25_Picture_2.jpeg)

- 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.

![](_page_25_Picture_5.jpeg)

![](_page_25_Picture_6.jpeg)

![](_page_26_Picture_0.jpeg)

![](_page_26_Picture_1.jpeg)

- 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 **Is** 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.

![](_page_27_Picture_1.jpeg)

![](_page_27_Picture_2.jpeg)

EXERCISE 3: VIEW AND ANALYZE LINUX LOGS

28

![](_page_28_Picture_0.jpeg)

NALY

![](_page_28_Picture_1.jpeg)

![](_page_28_Picture_2.jpeg)

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.

root@bob-Virtual-Machine:/ Sep 8 02:51:31 bob-Virtua T Translated Set 2 keyboar Sep 8 02:51:41 bob-Virtua	var/log# cat auth.log I-Machine systemd-log d) I-Machine gdm-launch- by (uid=0)	ind[547]: Watching syst	tem buttons on /d	ev/inpu	t/event	
Sep 8 02:51:31 Dob-Virtua T Translated Set 2 keyboar Sep 8 02:51:41 bob-Virtua	l-Machine systemd-log d) l-Machine gdm-launch- bv (uid=0)	ind[547]: Watching syst	tem buttons on /d	ev/inpu	t/event	
Sep 8 02:51:41 bob-Virtua	L-Machine gdm-launch-	environmentl: pam unix(				4 (A
	by (uid=0)		(gdm-launch-envir	onment:	session	): s
ssion opened for user gdm						
Sep 8 02:51:41 bob-Virtua	I-Machine systemd-log	Ind[547]: New session o	c1 of user gdm.			
by (uid=8)	t-machine systemu: pa	"_unix(systemd-user:ses	ssion): session o	peneo re	or user	ga
Sep 8 02:51:42 bob-Virtua	I-Machine gnome-keyri	ng-daemon[839]: couldn	't access control	socket	: /run/	use
/125/keyring/control: No s	uch file or directory					
Sep 8 02:51:42 bob-Virtua	l-Machine gnome-keyri	ng-daemon[840]: couldn'	't access control	socket	: /run/	use
/125/keyring/control: No s	uch file or directory				21 028-2-0	
<pre>sep 8 02:51:42 bob-Virtua /125/keyring/control: No.</pre>	-Machine gnome-keyri	ng-daemon[839]: Couldn'	t access control	socket	: /run/	use
Sen 8 02:51:42 hob-Virtua	-Machine odm-launch-	environmentl: nam unix	(odm-launch-envir	onment	session	1.
ession closed for user adm	c noenene gan council	enteronnene]: pan_onent	(gon council cirrer	onnenen		· ·
Sep 8 02:51:42 bob-Virtua	l-Machine systemd-log	ind[547]: Session c1 lo	ogged out. Waitin	g for p	rocesse	s 1
exit.						
Sep 8 02:51:42 bob-Virtua	I-Machine systemd-log	Ind[547]: Removed sessi	ion c1.			
sep 8 02:51:42 DoD-Virtua	by (uid-a)	environment]: pam_unix(	(gdm-launch-envir	onment:	session	):
Sep 8 02:51:42 bob-Virtua	L-Machine systemd-log	ind[547]: New session of	c2 of user odm.			
Sep 8 02:51:43 bob-Virtua	I-Machine gnome-keyri	ng-daemon[968]: couldn	't access control	socket	: /run/	us
125/keyring/control: No s	uch file or directory					
Sep 8 02:51:43 bob-Virtua	l-Machine gnome-keyri	ng-daemon[974]: couldn'	't read 4 bytes f	rom con	trol so	ck
: Connection reset by peer	weeks and back					
sep 8 02:51:45 DoD-Virtua	1 56 [/uss/bin/onom	nority=local): Register	red Authenticatio	n Agent	tor un	LX
icationAgent. locale en US	.UTF-8)	e-sherry, object path /	org/ireedeskcop/	FULLEYK	cci/Aut	ile
Sep 8 02:52:06 bob-Virtua	L-Machine dbus-daemon	[510]: [system] Failed	to activate serv	ice 'or	g.bluez	1:
imed out (service_start_ti	neout=25000ms)					
Sep 8 03:10:01 bob-Virtua	L-Machine CRON[1490]:	pam_unix(cron:session)	): session opened	for us	er root	b
(uid=0)						
Sep 8 03:10:01 bob-Virtua	L-Machine CRON[1490]:	pam_unix(cron:session)	): session closed	for us	er root	
(uid=0)	c-machine cRow[2082]:	pam_unix(cron:session)	): session opened	for us	er root	D
Sep 8 03:17:01 bob-Virtua	L-Machine CRON[2082]:	pam unix(cron:session)	): session closed	for us	er root	

![](_page_29_Picture_0.jpeg)

![](_page_29_Picture_1.jpeg)

#### 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.

![](_page_29_Picture_5.jpeg)

m	root@bob-Virtual-Machine: /var/log	Q	Ξ	-	ø	
root@b	ob-Virtual-Machine:/var/log# cat boot.log					
[ OK	] Started System Logging Service.					
[ OK	] Started LSB: Record successful boot for GRUB.					
[ OK	] Started LSB: automatic crash report generation.					
[ OK	] Reached target Host and Network Name Lookups.					
	Stopping CUPS Scheduler					
[ OK	] Stopped CUPS Scheduler.					
[ 0K	] Started CUPS Scheduler.					
[ OK	] Started Thermal Daemon Service.					
[ OK	] Started WPA supplicant.					
[ OK	] Started Avahi mDNS/DNS-SD Stack.					
[ OK	] Started Make remote CUPS printers available locally.					
[ OK	] Started Authorization Manager.					
-	Starting Modem Manager					
C OK	] Started Switcheroo Control Proxy service.					
L OK	] Started Network Manager.					
LOK	J Reached target Network.					
	Starting Network Manager Walt Online					
	Starting OpenVPN Service					
-	Starting Permit User Sessions					
UK OK	J Finished OpenVPN Service.					
	j Finished Permit User Sessions.					
L OK	J Started Login Service.					
L OK	Starting CNONE Dicelay Nanager					
	Starting unume Display Hanager					
	Starting Note and Carvica					
T OK	3 Started Hostandad Hostades Shutdown					
P OK	] Started Midden Manager					
r ok	J Finished Rotate log files					
F OK	] Finished Discard unused blocks on filesystems from /etc/fstab.					
r ok	1 Started Dispatcher daemon for systemd-networkd					
I OK	1 Started Disk Manager.					
r ok	] Started Hostname Service.					
	Starting Network Manager Script Dispatcher Service					
f ok	1 Started Network Manager Script Dispatcher Service.					
r ok	1 Finished Network Manager Wait Online.					

![](_page_30_Picture_1.jpeg)

![](_page_30_Picture_2.jpeg)

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

root@bob-Virtual-Machine:/var/log≢ cat syslog Sep 8 02:51:30 bob-Virtual-Machine rsyslogd: [origin software="rsyslogd" swVersion="8.2001.0" x-pid="54 2" x-info="https://www.rsyslog.com"] rsyslogd was HUPed Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Accounts Service. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Accounts Service. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Starting Hold until boot process finishes up Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Starting Hold until boot process finishes up Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Starting Hold until boot process finishes up Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Modem Manager. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Modem Manager. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Finished Rotate log files. Sep 8 02:51:30 bob-Virtual-Machine fstrim[517]: /boot/eft: 511 MLB (535801856 bytes) trimmed on /dev/sda 10 2:51:30 bob-Virtual-Machine fstrim[517]: /boot/eft: 511 MLB (535801856 bytes) trimmed on /dev/sda Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: finished Discard unused blocks on filesystems from /dev/sda Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Hostname Service. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Hostname Service. Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname: u sing hostnamed' Sep 8 02:51:30 bob-Vir</info>	Π	root@bob-Virtual-Machine: /var/log	Q = - • 😆
<pre>Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Starting GoMoMe Display Manager Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Starting Hold until boot process finishes up Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Started Unattended Upgrades Shutdown. Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Started Modem Manager. Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Finished Rotate.service: Succeeded. Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Finished Rotate log files. Sep 8 02:51:30 bob-Virtual-Machine fstrim[517]: /bot/efi: 511 MiB (535801856 bytes) trimmed on /dev/sda Sep 8 02:51:30 bob-Virtual-Machine fstrim[517]: /cot/efi: 511 MiB (535801856 bytes) trimmed on /dev/sda Sep 8 02:51:30 bob-Virtual-Machine fstrim[517]: /cot/efi: Succeeded. Sep 8 02:51:30 bob-Virtual-Machine system0[1]: finished Discard unused blocks on filesystems from /etc/ fstab. Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Started Dispatcher daenon for systemd-networkd is not running, output will be incomplete. Sep 8 02:51:30 bob-Virtual-Machine system0[1]: Started Dispatcher daenon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine udisksd[553]: Acquired the name org.freedesktop.UDIsks2 on the system sep 8 02:51:30 bob-Virtual-Machine dbus-daemon[510]: [system] Successfully activated service 'org.freed esktop.hostname1' Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname: u sing hostnamed Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname: u sing hostnamed Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348880129 0]: inti: dns-systemd-resolved rc-manager-syntik, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enab</info></info></info></info></info></pre>	root@bob-Virtua Sep 8 02:51:30 2" x-info="http Sep 8 02:51:30 Sep 8 02:51:30	l-Machine:/var/log# cat syslog bob-Virtual-Machine rsyslogd: [origin software="rsyslogd" swVersi s://www.rsyslog.com"] rsyslogd was HUPed bob-Virtual-Machine systemd[1]: Started Login Service. bob-Virtual-Machine systemd[1]: Started Accounts Service.	on="8.2001.0" x-pid="54
<pre>Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: logrotate.service: Succeeded. Sep 8 02:51:30 bob-Virtual-Machine fstrim[517]: /boot/efi: 511 MLB (535801856 bytes) trimmed on /dev/sda a1 Sep 8 02:51:30 bob-Virtual-Machine fstrim[517]: /: 67.9 GLB (72905408512 bytes) trimmed on /dev/sda Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: fstrim.service: Succeeded. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: finished Discard unused blocks on filesystems from /etc/ fstab. Sep 8 02:51:30 bob-Virtual-Machine networkd-dispatcher[647]: WARNING: systemd-networkd is not running, output will be incomplete. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine udisksd[553]: Acquired the name org.freedesktop.UDisks2 on the system message bus Sep 8 02:51:30 bob-Virtual-Machine dbus-daemon[510]: [system] Successfully activated service 'org.freed esktop.hostname1' Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Hostname Service. Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname: u sing hostnamed Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname ch anged from (none) to "bob-Virtual-Machine" Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348880129 0]: init: dns=systemd-resolved rc-manager=symlink, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348880129 0]: init: dns=systemd-resolved rc-manager=symlink, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7070] manager[0x56348881703 0]: rfkill: WiAN hardware radio set enabled</info></info></info></info></info></info></pre>	Sep 8 02:51:30 Sep 8 02:51:30 Sep 8 02:51:30 Sep 8 02:51:30 Sep 8 02:51:30	bob-Virtual-Machine systemd[1]: Starting Hold until boot process bob-Virtual-Machine systemd[1]: Starting Hostname Service bob-Virtual-Machine systemd[1]: Started Unattended Upgrades Shutd bob-Virtual-Machine systemd[1]: Started Modem Manager.	finishes up Iown.
<pre>Sep &amp; 02:51:30 bob-Virtual-Machine fstrim[57]: /: 67.9 GlB (72905408512 bytes) trimmed on /dev/sdas Sep &amp; 02:51:30 bob-Virtual-Machine systemd[1]: fstrim.service: Succeeded. Sep &amp; 02:51:30 bob-Virtual-Machine networkd-dispatcher[647]: WARNING: systemd-networkd is not running, output will be incomplete. Sep &amp; 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep &amp; 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep &amp; 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep &amp; 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep &amp; 02:51:30 bob-Virtual-Machine udisksd[553]: Acquired the name org.freedesktop.UDisks2 on the syste m message bus Sep &amp; 02:51:30 bob-Virtual-Machine dbus-daemon[510]: [system] Successfully activated service 'org.freed esktop.hostname1' Sep &amp; 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname: u sing hostnamed Sep &amp; 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname ch anged from (none) to "bob-Virtual-Machine" Sep &amp; 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname ch anged from (none) to "bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname ch anged from (none) to "bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348880129 0]: init: dns=systemd-resolved rc-manager=symlink, plugin=systemd-resolved Sep &amp; 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep &amp; 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-An hardware radio set enabled</info></info></info></info></info></info></info></pre>	Sep 8 02:51:30 Sep 8 02:51:30 Sep 8 02:51:30 a1	<pre>bob-Virtual-Machine systemd[1]: logrotate.service: Succeeded. bob-Virtual-Machine systemd[1]: Finished Rotate log files. bob-Virtual-Machine fstrim[517]: /boot/efi: 511 MiB (535801856 by bob-Virtual-Machine fstrim[517]: /boot/efi: 511 MiB (535801856 by)</pre>	tes) trimmed on /dev/sd
Sep 8 02:51:30 bob-Virtual-Machine networkd-dispatcher[647]: WARNING: systemd-networkd is not running, output will be incomplete. Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for systemd-networkd. Sep 8 02:51:30 bob-Virtual-Machine udisksd[553]: Acquired the name org.freedesktop.UDisks2 on the system message bus Sep 8 02:51:30 bob-Virtual-Machine dbus-daemon[510]: [system] Successfully activated service 'org.freed esktop.hostname1' Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Hostname Service. Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname: u sing hostnamed Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname ch anged from (none) to "bob-Virtual-Machine" Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348880129 0]: init: dns=systemd-resolved rc-manager=synlink, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7070] manager[0x56348881703 0]: rfkill: Wi-AN hardware radio set enabled</info></info></info></info></info>	Sep 8 02:51:30 Sep 8 02:51:30 Sep 8 02:51:30 fstab.	<pre>bob-Virtual-Machine fstrim[517]: /: 07.9 GLB (72905408512 bytes) bob-Virtual-Machine systemd[1]: fstrim.service: Succeeded. bob-Virtual-Machine systemd[1]: Finished Discard unused blocks or bob-Virtual-Machine systemd[1]: Finished Discard unused blocks or</pre>	trimmed on /dev/sdas
<pre>m message bus Sep 8 02:51:30 bob-Virtual-Machine dbus-daemon[510]: [system] Successfully activated service 'org.freed esktop.hostname1' Sep 8 02:51:30 bob-Virtual-Machine systemd[1]: Started Hostname Service. Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] hostname: hostname: u sing hostnamed Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname ch anged from (none) to "bob-Virtual-Machine" Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348880129 0]: init: dns=systemd-resolved rc-manager=symlink, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7070] manager[0x56348881703 0]: rfkill: WWAN hardware radio set enabled</info></info></info></info></info></pre>	Sep 8 02:51:30 output will be Sep 8 02:51:30 Sep 8 02:51:30 Sep 8 02:51:30	DOD-Virtual-Machine networkd-dispatcher[647]: WARNING: systemd-ne incomplete. ) bob-Virtual-Machine systemd[1]: Started Dispatcher daemon for sys ) bob-Virtual-Machine systemd[1]: Started Disk Manager. ) bob-Virtual-Machine udisksd[553]: Acquired the name org.freedeskt	tworkd is not running, temd-networkd. op.UDisks2 on the syste
Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7046] nostname: nostname: u sing hostnamed Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7047] hostname: hostname ch anged from (none) to "bob-Virtual-Machine" Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7049] dns-mgr[0x56348880129 0]: init: dns=systemd-resolved rc-manager=symlink, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7070] manager[0x56348881703 0]: rfkill: Wi-AN hardware radio set enabled</info></info></info></info></info>	m message bus Sep 8 02:51:30 esktop.hostname Sep 8 02:51:30	bob-Virtual-Machine dbus-daemon[510]: [system] Successfully activ 1' bob-Virtual-Machine systemd[1]: Started Hostname Service.	ated service 'org.freed
0]: init: dns=systemd-resolved rc-manager=symlink, plugin=systemd-resolved Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7069] manager[0x56348881703 0]: rfkill: Wi-Fi hardware radio set enabled Sep 8 02:51:30 bob-Virtual-Machine NetworkManager[514]: <info> [1631083890.7070] manager[0x56348881703 0]: rfkill: WWAN hardware radio set enabled</info></info>	sep 8 02:51:30 sing hostnamed Sep 8 02:51:30 anged from (non Sep 8 02:51:30	<pre>bob-virtual-Machine NetworkManager[514]: <info> [1631083890.7046 bob-virtual-Machine NetworkManager[514]: <info> [1631083890.7047 e) to "bob-virtual-Machine" bob-virtual-Machine NetworkManager[514]: <info> [1631883898.7849</info></info></info></pre>	) nostname: nostname: u ) hostname: hostname ch
0]: rfkill: WWAN hardware radio set enabled	0]: init: dns=s Sep 8 02:51:30 0]: rfkill: Wi- Sep 8 02:51:30	ystemd-resolved rc-manager=symlink, plugin=systemd-resolved ) bob-Virtual-Machine NetworkManager[514]; <info> [1631083890.7069 Fi hardware radio set enabled ) bob-Virtual-Machine NetworkManager[514]; <info></info></info>	] manager[0x56348881703
	0]: rfkill: WWA	N hardware radio set enabled	

![](_page_31_Picture_0.jpeg)

![](_page_31_Picture_1.jpeg)

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.

![](_page_31_Picture_5.jpeg)

![](_page_31_Picture_6.jpeg)

![](_page_32_Picture_1.jpeg)

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

Ē	1			bob@	bob-Virtual-I	Machine: ~	Q								
	root(	@bob-\	/irtual-	-Maci	hine	: /var/lo	g			bob@bob-Virtual-Mac	:hine: -				
bob@bob-	Virtual	-Macht	ne:-S	w					anna Shina						
07:13:2	28 up 29	min,	1 US	ser,	10	oad av	er	age: 0	.06, 0.03,	0.01					
USER	TTY	FRO	M			LOG	EN	a ID	LE JCPU	PCPU WHAT					
bob	:1	:1				86:	49	?xd	m? 37.35s	0.00s /usr/lib/gdm3/gdm-	x-ses	sion	61	un-sc	rip
bob@bob-	-Virtual	-Machi	ine:-\$	las	st	-a									
bob	:1		Wed	Sep	8	06:49		still	logged in	:1					
reboot	system	boot	Wed	Sep	8	86:44		still	running	5.11.0-34-generic					
bob	:1		Wed	Sep	8	06:38		06:43	(00:04)	:1					
reboot	system	boot	Wed	Sep	8	02:51		06:43	(03:52)	5.4.0-48-generic					
reboot	system	boot	Fri	May	28	08:53		08:57	(00:04)	5.4.0-48-generic					
bob	:1		Fri	May	28	07:16		down	(00:43)	:1					
reboot	system	boot	Fri	May	28	07:15		07:59	(00:44)	5.4.0-48-generic					
bob	:1		Fri	May	28	07:13		crash	(00:01)	:1					
reboot	system	boot	Fri	May	28	02:00		07:59	(05:59)	5.4.0-48-generic					
bob	:1		Tue	Nov	3	04:33		down	(00:06)	:1					
reboot	system	boot	Tue	Nov	3	04:32		04:40	(00:08)	5.4.0-48-generic					
bob	:1		Tue	Nov	3	04:18		down	(00:12)	:1					
reboot	system	boot	Tue	Nov	3	04:17		04:31	(00:14)	5.4.0-48-generic					
bob	:1		Tue	Oct	13	87:41		down	(00:04)	:1					
reboot	system	boot	Tue	Oct	13	07:40		07:46	(00:05)	5.4.0-48-generic					
bob	:1		Fri	Sep	25	02:22		down	(00:01)	:1					
reboot	system	boot	Fri	Sep	25	02:21		02:24	(00:02)	5.4.0-48-generic					
bob	:1		Thu	Sep	24	05:54		02:20	(20:25)	:1					
reboot	system	boot	Thu	Sep	24	00:48		02:24	(1+01:36)	5.4.0-42-generic					
bob	:1		Fri	Aug	28	01:45		down	(00:24)	:1					
reboot	system	boot	Fri	Aug	28	01:44		02:09	(00:24)	5.4.0-42-generic					
bob	:1		Fri	Aug	28	01:11		down	(00:33)	:1					
reboot	system	boot	Fri	Aug	28	01:07		01:44	(00:37)	5.4.0-26-generic					
bob	:1		Thu	Aug	13	07:46		down	(17:16)	:1					
reboot	system	boot	Thu	Aug	13	07:45		01:02	(17:17)	5.4.0-26-generic					
wtmp bec	ins Thu	Aug	3 07:	45:2	20 3	2020									

33

![](_page_33_Picture_0.jpeg)

ANALY

![](_page_33_Picture_1.jpeg)

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.

bob@bob-Virtual-Machine: ~ root@bob-Virtual-Machine: /var/log bob@bob-Virtual-Machine: ~ ob@bob-Virtual-Machine:-\$ sudo aureport [sudo] password for bob: Summary Report -----Range of time in logs: 12/31/1969 19:00:00.000 - 09/08/2021 07:24:20.886 Selected time for report: 12/31/1969 19:00:00 - 09/08/2021 07:24:20.886 lumber of changes in configuration: 3 Number of changes to accounts, groups, or roles: 0 Number of logins: 0 Number of failed logins: 0 Number of authentications: 2 umber of failed authentications: 0 Number of users: 3 Number of terminals: 5 Number of host names: 1 Number of executables: 5 Number of commands: 3 Number of files: 0 Number of AVC's: 0 Number of MAC events: 0 Number of failed syscalls: 0 Number of anomaly events: 0 Number of responses to anomaly events: 0 Number of crypto events: 0 Number of integrity events: 0 Number of virt events: 0 Number of keys: 0 Number of process IDs: 9 Number of events: 51

![](_page_34_Picture_0.jpeg)

![](_page_34_Picture_1.jpeg)

- 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.

# 1 10 1001 01010110

# **EC-COURCI**

override for onPageSgrglled(post

override fun onPageSelected(Usertion

b<u>Layout</u>.getTabAt(<u>selectedTab</u>) bLayout.<u>tabMode</u> = TabLayout.MODE\_FIXED bLayout.<u>tabGravity</u> = TabLayout.GRAVITY\_FIL bLayout.setupWithVic**O**P1(\*\*(0010Parts))