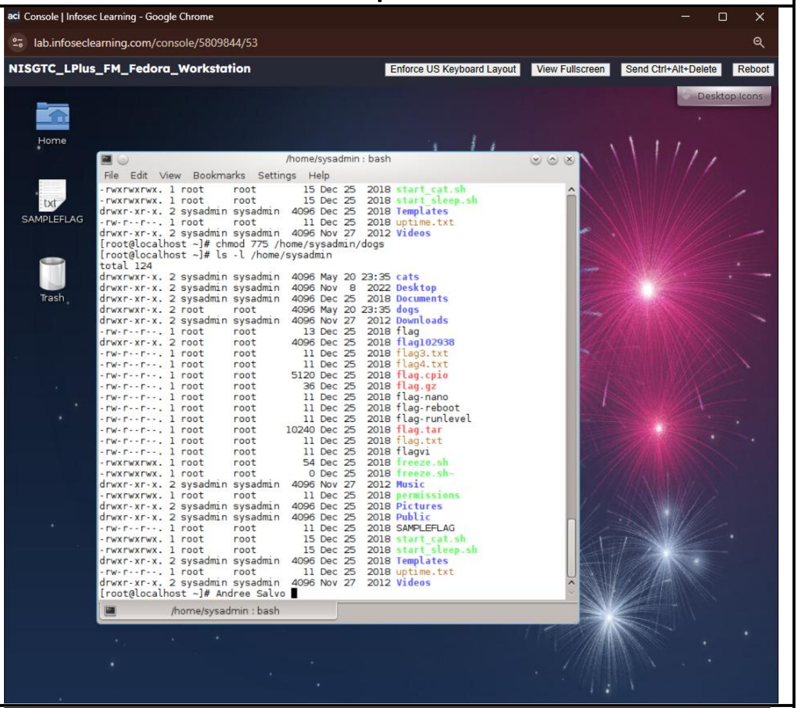
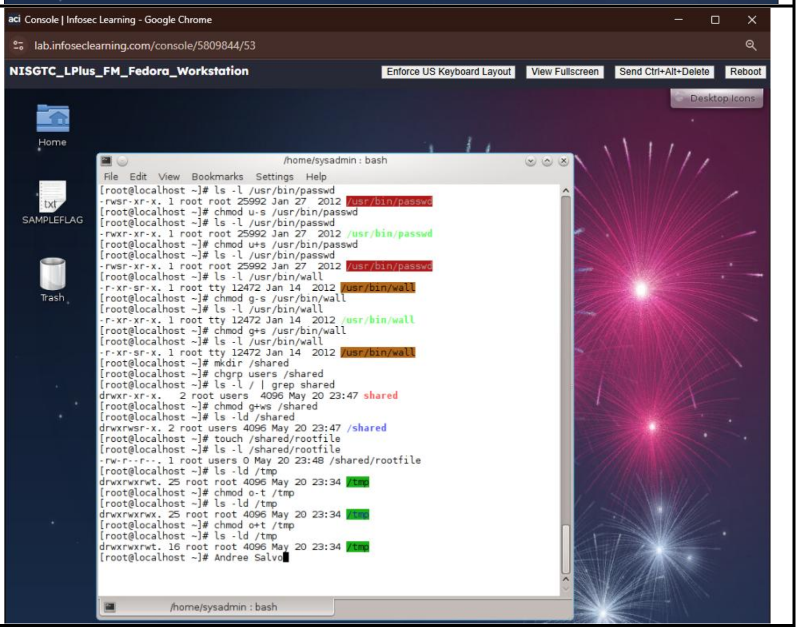
2025

4-2 Lab Worksheet

Andree Salvo
Southern New Hampshire University
CYB 230
Instructor: Joshua Brogdon

CYB 230 Module 4-2 Lab Worksheet

Lab: Working With Files

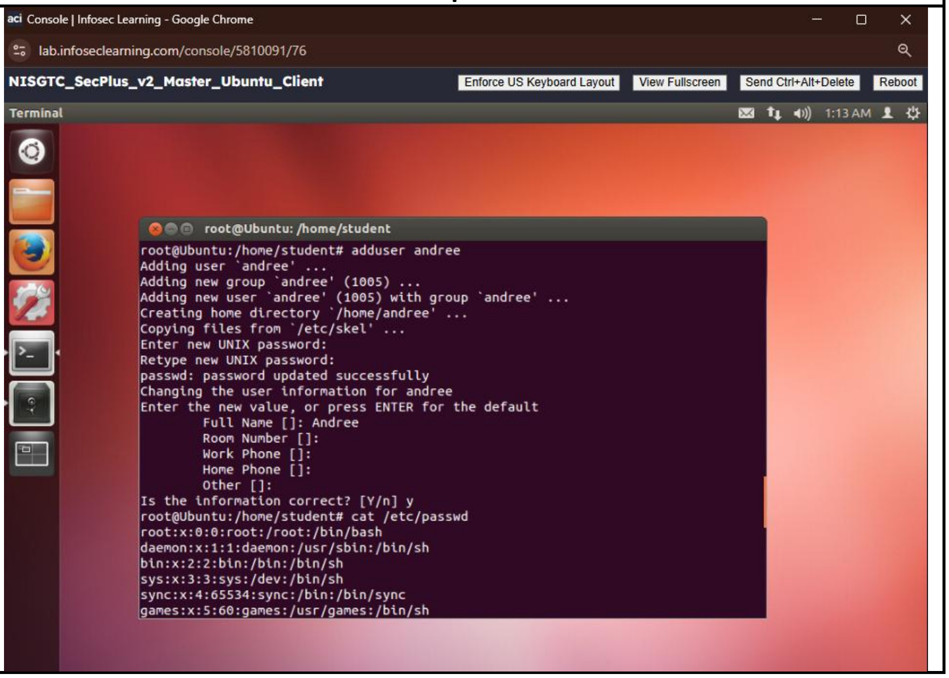
Prompt	Response
In the lab section “Using Chmod to Change Permissions,” insert your name at the command line below the ending output and include it in your screenshot.	
In the lab section “Setting Special Permissions,” insert your name at the command line below the ending output and include it in your screenshot.	

```
-rwxrwxrwx. 1 root     root        15 Dec 25  2018 start_cat.sh
-rwxrwxrwx. 1 root     root        15 Dec 25  2018 start_sleep.sh
drwxr-xr-x. 2 sysadmin sysadmin  4096 Dec 25  2018 Templates
-rw-r--r--. 1 root     root        11 Dec 25  2018 uptime.txt
drwxr-xr-x. 2 sysadmin sysadmin  4096 Nov 27  2012 Videos
[root@localhost ~]# chmod 775 /home/sysadmin/dogs
[root@localhost ~]# ls -l /home/sysadmin
total 124
drwxrwxr-x. 2 sysadmin sysadmin  4096 May 20 23:35 cats
drwxr-xr-x. 2 sysadmin sysadmin  4096 Nov  8  2022 Desktop
drwxr-xr-x. 2 sysadmin sysadmin  4096 Dec 25  2018 Documents
drwxrwxr-x. 2 root     root      4096 May 20 23:35 dogs
drwxr-xr-x. 2 sysadmin sysadmin  4096 Nov 27  2012 Downloads
-rw-r--r--. 1 root     root        13 Dec 25  2018 flag
drwxr-xr-x. 2 root     root      4096 Dec 25  2018 flag102938
-rw-r--r--. 1 root     root        11 Dec 25  2018 flag3.txt
-rw-r--r--. 1 root     root        11 Dec 25  2018 flag4.txt
-rw-r--r--. 1 root     root      5120 Dec 25  2018 flag.cpio
-rw-r--r--. 1 root     root        36 Dec 25  2018 flag.gz
-rw-r--r--. 1 root     root        11 Dec 25  2018 flag-nano
-rw-r--r--. 1 root     root        11 Dec 25  2018 flag-reboot
-rw-r--r--. 1 root     root        11 Dec 25  2018 flag-runlevel
-rw-r--r--. 1 root     root     10240 Dec 25  2018 flag.tar
-rw-r--r--. 1 root     root        11 Dec 25  2018 flag.txt
-rw-r--r--. 1 root     root        11 Dec 25  2018 flagvi
-rwxrwxrwx. 1 root     root        54 Dec 25  2018 freeze.sh
-rwxrwxrwx. 1 root     root         0 Dec 25  2018 freeze.sh~
drwxr-xr-x. 2 sysadmin sysadmin  4096 Nov 27  2012 Music
-rwxrwxrwx. 1 root     root        11 Dec 25  2018 permissions
drwxr-xr-x. 2 sysadmin sysadmin  4096 Dec 25  2018 Pictures
drwxr-xr-x. 2 sysadmin sysadmin  4096 Dec 25  2018 Public
-rw-r--r--. 1 root     root        11 Dec 25  2018 SAMPLEFLAG
-rwxrwxrwx. 1 root     root        15 Dec 25  2018 start_cat.sh
-rwxrwxrwx. 1 root     root        15 Dec 25  2018 start_sleep.sh
drwxr-xr-x. 2 sysadmin sysadmin  4096 Dec 25  2018 Templates
-rw-r--r--. 1 root     root        11 Dec 25  2018 uptime.txt
drwxr-xr-x. 2 sysadmin sysadmin  4096 Nov 27  2012 Videos
[root@localhost ~]# Andree Salvo
```

```
[root@localhost ~]# ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 25992 Jan 27  2012 /usr/bin/passwd
[root@localhost ~]# chmod u-s /usr/bin/passwd
[root@localhost ~]# ls -l /usr/bin/passwd
-rwxr-xr-x. 1 root root 25992 Jan 27  2012 /usr/bin/passwd
[root@localhost ~]# chmod u+s /usr/bin/passwd
[root@localhost ~]# ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 25992 Jan 27  2012 /usr/bin/passwd
[root@localhost ~]# ls -l /usr/bin/wall
-r-xr-sr-x. 1 root tty 12472 Jan 14  2012 /usr/bin/wall
[root@localhost ~]# chmod g-s /usr/bin/wall
[root@localhost ~]# ls -l /usr/bin/wall
-r-xr-xr-x. 1 root tty 12472 Jan 14  2012 /usr/bin/wall
[root@localhost ~]# chmod g+s /usr/bin/wall
[root@localhost ~]# ls -l /usr/bin/wall
-r-xr-sr-x. 1 root tty 12472 Jan 14  2012 /usr/bin/wall
[root@localhost ~]# mkdir /shared
[root@localhost ~]# chgrp users /shared
[root@localhost ~]# ls -l / | grep shared
drwxr-xr-x.   2 root users  4096 May 20 23:47 shared
[root@localhost ~]# chmod g+ws /shared
[root@localhost ~]# ls -ld /shared
drwxrwsr-x. 2 root users 4096 May 20 23:47 /shared
[root@localhost ~]# touch /shared/rootfile
[root@localhost ~]# ls -l /shared/rootfile
-rw-r--r--. 1 root users 0 May 20 23:48 /shared/rootfile
[root@localhost ~]# ls -ld /tmp
drwxrwxrwt. 25 root root 4096 May 20 23:34 /tmp
[root@localhost ~]# chmod o-t /tmp
[root@localhost ~]# ls -ld /tmp
drwxrwxrwx. 25 root root 4096 May 20 23:34 /tmp
[root@localhost ~]# chmod o+t /tmp
[root@localhost ~]# ls -ld /tmp
drwxrwxrwt. 16 root root 4096 May 20 23:34 /tmp
[root@localhost ~]# Andree Salvo
```

Prompt	Response
Implementing the sticky bit on the directory can stop people from accidentally deleting files that they don’t own. How can this technique be used to implement the concept of least privilege, and how can it be used to assure file availability?	Using a sticky bit like "/tmp" makes it so that only the file owners, directory owners, or root users can delete or rename files. This helps enforce the least privilege by making sure users can only access their own files, not someone else’s. It can also help keep important or shared files safe.

Lab: Permissions, Users, and Groups in Linux

<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>After completing the lab section “Adding Groups, Users, and Passwords,” <b>repeat the steps to</b> add another user using your first name. Provide a screenshot of the <b>cat etc/passwd</b> command when you are done.</td><td>
aci Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/5810091/76
NISGTC_SecPlus_v2_Master_Ubuntu_Client
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Terminal
1:13 AM
root@Ubuntu: /home/student
<pre>
root@Ubuntu:/home/student# adduser andree
Adding user `andree' ...
Adding new group `andree' (1005) ...
Adding new user `andree' (1005) with group `andree' ...
Creating home directory `/home/andree' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for andree
Enter the new value, or press ENTER for the default
        Full Name []: Andree
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@Ubuntu:/home/student# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
</pre></td></tr>
</table>

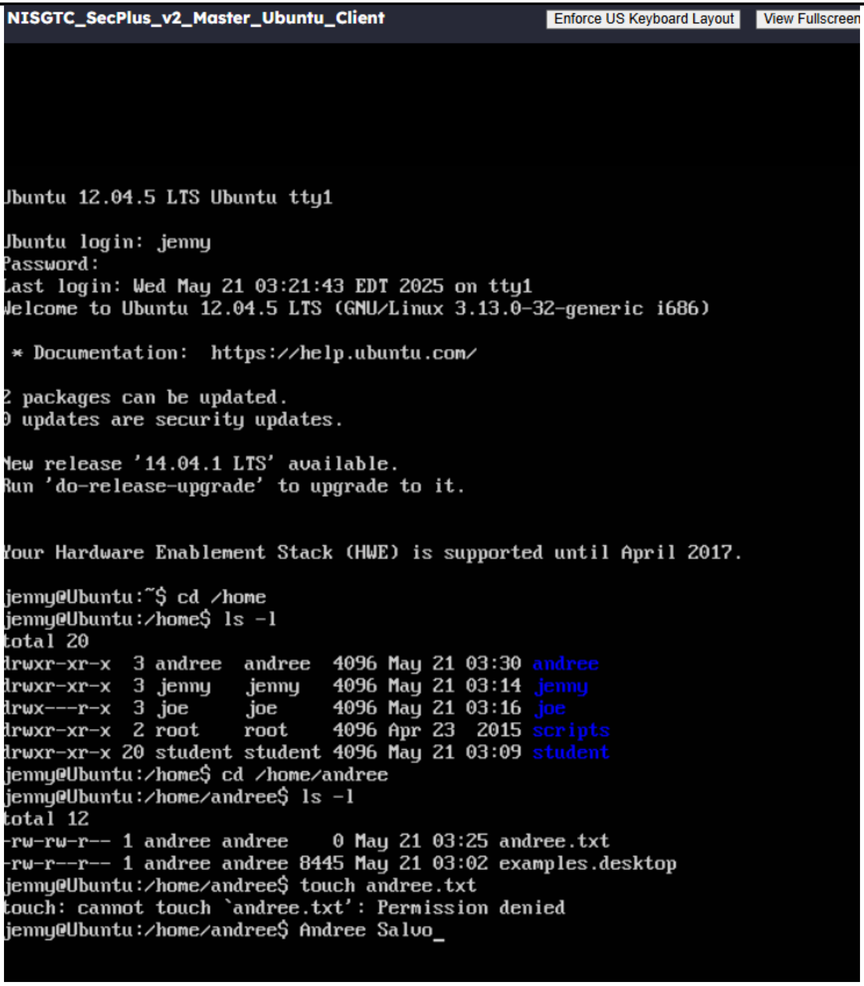
<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr>
<td>

After completing the lab section “Absolute Permission,” repeat the process using your first name as the text file. Provide a screenshot of the output.

Note: By default, some computer systems use the key sequence **Ctrl+Alt+F1** to access a shortcut for other programs such as the Intel Graphics Control Panel. If this is the case, you will need to change the key sequence from the default to complete this step.

To exit the tty1 or tty2 window, use the key sequence **Ctrl+Alt+F7**.

</td>
<td>



NISGTC_SecPlus_v2_Master_Ubuntu_Client
Enforce US Keyboard Layout
View Fullscreen

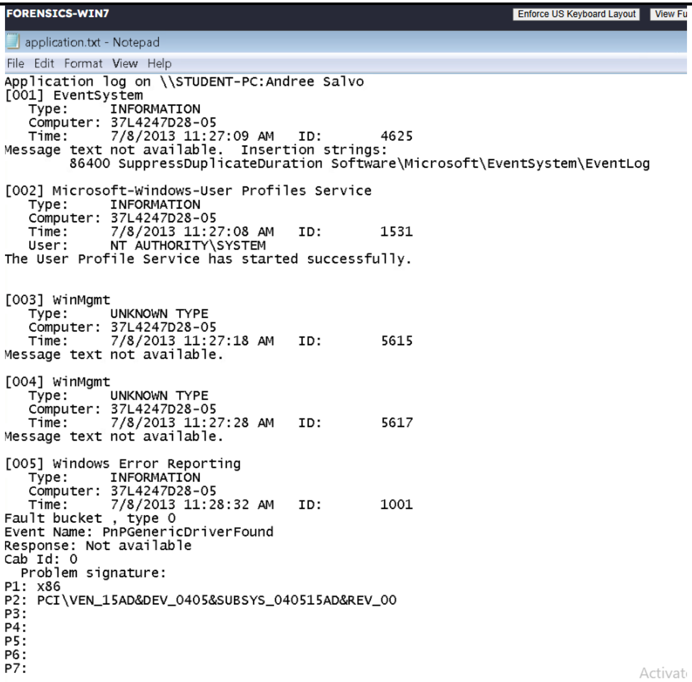
```
Jbuntu 12.04.5 LTS Ubuntu tty1

Jbuntu login: jenny
Password:
Last login: Wed May 21 03:21:43 EDT 2025 on tty1
Jelcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

2 packages can be updated.
0 updates are security updates.

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Your Hardware Enablement Stack (HWE) is supported until April 2017.

jenny@Ubuntu:~$ cd /home
jenny@Ubuntu:/home$ ls -l
total 20
drwxr-xr-x  3 andree  andree  4096 May 21 03:30 andree
drwxr-xr-x  3 jenny   jenny   4096 May 21 03:14 jenny
drwx---r-x  3 joe     joe     4096 May 21 03:16 joe
drwxr-xr-x  2 root    root    4096 Apr 23  2015 scripts
drwxr-xr-x 20 student student 4096 May 21 03:09 student
jenny@Ubuntu:/home$ cd /home/andree
jenny@Ubuntu:/home/andree$ ls -l
total 12
-rw-rw-r-- 1 andree andree    0 May 21 03:25 andree.txt
-rw-r--r-- 1 andree andree 8445 May 21 03:02 examples.desktop
jenny@Ubuntu:/home/andree$ touch andree.txt
touch: cannot touch `andree.txt': Permission denied
jenny@Ubuntu:/home/andree$ Andree Salvo_
```

</td>
</tr>
</table>

Prompt	Response
Using the **chmod** command, which commands would you use to set the following permissions to a file called **Answers.txt**? (Provide the one line used at the command line for each bulleted item.) • User (read and write), group (execute) other (execute) • User (read, write, execute), group (read and execute) other (write and execute) • User (write), group (read) other (none)	- Chmod 611 > rw- --x –x - Chmod 753 > rwx-r-x-wx - Chmod 240 > -w-r-- ---

Lab: Log Analysis

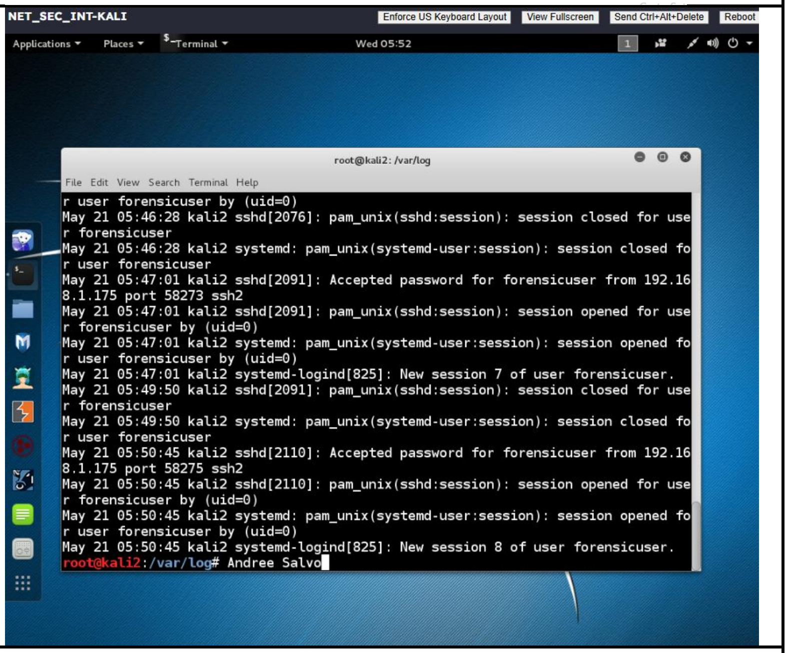
<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>In the lab section “Examining Windows Event Logs, IIs Logs, and Scheduled Tasks,” add your name as the top line of the file and then take a screenshot.</td><td>



FORENSICS-WIN7
Enforce US Keyboard Layout
View Fu
application.txt - Notepad
File Edit Format View Help
Activat

```
Application log on \\STUDENT-PC:Andree Salvo
[001] EventSystem
   Type:      INFORMATION
   Computer: 37L4247D28-05
   Time:      7/8/2013 11:27:09 AM   ID:       4625
Message text not available.  Insertion strings:
        86400 SuppressDuplicateDuration Software\Microsoft\EventSystem\EventLog

[002] Microsoft-Windows-User Profiles Service
   Type:      INFORMATION
   Computer: 37L4247D28-05
   Time:      7/8/2013 11:27:08 AM   ID:       1531
   User:      NT AUTHORITY\SYSTEM
The User Profile Service has started successfully.


[003] WinMgmt
   Type:      UNKNOWN TYPE
   Computer: 37L4247D28-05
   Time:      7/8/2013 11:27:18 AM   ID:       5615
Message text not available.

[004] WinMgmt
   Type:      UNKNOWN TYPE
   Computer: 37L4247D28-05
   Time:      7/8/2013 11:27:28 AM   ID:       5617
Message text not available.

[005] Windows Error Reporting
   Type:      INFORMATION
   Computer: 37L4247D28-05
   Time:      7/8/2013 11:28:32 AM   ID:       1001
Fault bucket , type 0
Event Name: PnPGenericDriverFound
Response: Not available
Cab Id: 0
  Problem signature:
P1: x86
P2: PCI\VEN_15AD&DEV_0405&SUBSYS_040515AD&REV_00
P3:
P4:
P5:
P6:
P7:
```

</td></tr>
<tr><td>In the lab section “Examining Linux Log Files,” insert your name at the command line below the ending output and include it in your screenshot.</td><td>



```
r user forensicuser by (uid=0)
May 21 05:46:28 kali2 sshd[2076]: pam_unix(sshd:session): session closed for use
r forensicuser
May 21 05:46:28 kali2 systemd: pam_unix(systemd-user:session): session closed fo
r user forensicuser
May 21 05:47:01 kali2 sshd[2091]: Accepted password for forensicuser from 192.16
8.1.175 port 58273 ssh2
May 21 05:47:01 kali2 sshd[2091]: pam_unix(sshd:session): session opened for use
r forensicuser by (uid=0)
May 21 05:47:01 kali2 systemd: pam_unix(systemd-user:session): session opened fo
r user forensicuser by (uid=0)
May 21 05:47:01 kali2 systemd-logind[825]: New session 7 of user forensicuser.
May 21 05:49:50 kali2 sshd[2091]: pam_unix(sshd:session): session closed for use
r forensicuser
May 21 05:49:50 kali2 systemd: pam_unix(systemd-user:session): session closed fo
r user forensicuser
May 21 05:50:45 kali2 sshd[2110]: Accepted password for forensicuser from 192.16
8.1.175 port 58275 ssh2
May 21 05:50:45 kali2 sshd[2110]: pam_unix(sshd:session): session opened for use
r forensicuser by (uid=0)
May 21 05:50:45 kali2 systemd: pam_unix(systemd-user:session): session opened fo
r user forensicuser by (uid=0)
May 21 05:50:45 kali2 systemd-logind[825]: New session 8 of user forensicuser.
root@kali2:/var/log# Andree Salvo
```

</td></tr>
<tr><td>What is the importance of maintaining clean log files that are well formatted?</td><td>Maintaining clean log files makes it easier for us to spot issues, track system activity, and investigate any security breaches. When it comes to troubleshooting and understanding what happened and what went wrong.</td></tr>
</table>