NAMA : IK-RARS’JATI PRAMESTI
NIM : 2141762003
KELAS : SIB-4C

Lab - Gather System Information After an Incident

Objectives

- Collect system information after an incident has occurred.
- View logs for potential intrusions.

Background / Scenario

When an incident occurs in an organization, people responsible must know how to respond. An organization needs to develop an incident response plan and put together a Computer Security Incident Response Team (CSIRT) to manage the response. In this lab, you will gather system information and review logs after an incident has occurred. Doing these tasks immediately after the incident is important because any data residing in RAM will be gone when the system is shut down.

Required Resources

PC with the **CSE-LABVM** installed in VirtualBox

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

a. Launch the **CSE-LABVM**.

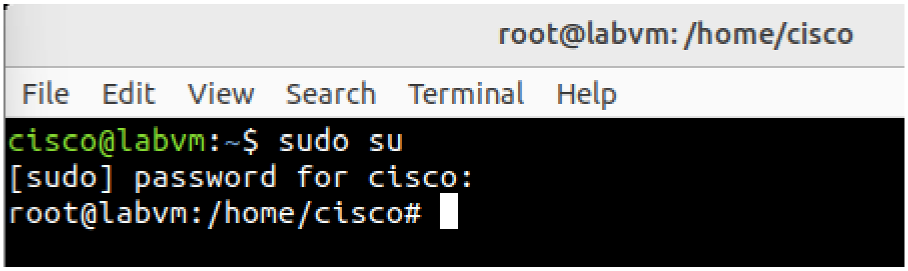
b. Double-click the **Terminal** icon to open a terminal.

Step 2: Collect volatile information of the compromised system.

In this step, you will create a file called **report.txt** that includes a variety of system information that can be used for incident analysis. This report can then be transferred to a USB drive, emailed, or uploaded to a cloud server to preserve the information. Then the system can be taken down.

a. Switch to the root user with the **sudo su** command. Enter **password** as the root password.

```
cisco@labvm:~$ sudo su
[sudo] password for cisco: password
root@labvm:/home/cisco#
```

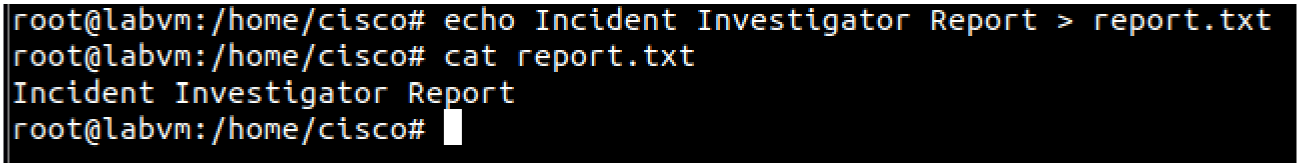


```
cisco@labvm:~$ sudo su
[sudo] password for cisco:
root@labvm:/home/cisco#
```

b. Enter the **echo** command, and then specify a heading for a newly created file named **report.txt**. Enter the **cat** command to review the new file.

```
root@labvm:/home/cisco# echo Incident Investigator Report > report.txt
root@labvm:/home/cisco# cat report.txt
Incident Investigator Report
root@labvm:/home/cisco#
```

NAMA : IK-RARS’JATI PRAMESTI
NIM : 2141762003
KELAS : SIB-4C

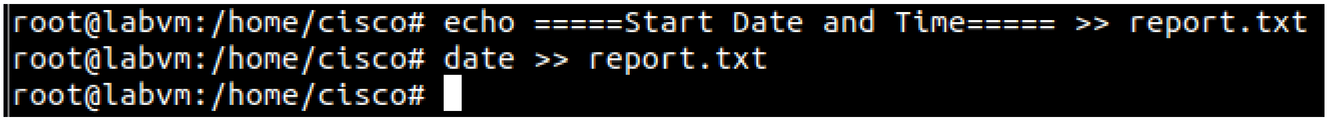


```
root@labvm:/home/cisco# echo Incident Investigator Report > report.txt
root@labvm:/home/cisco# cat report.txt
Incident Investigator Report
root@labvm:/home/cisco# 
```

c. Enter the **date** command and redirect the date and timestamp to the **report.txt** file. Be sure to use the double angle brackets (**>>**) to append to the **report.txt** file. Otherwise, you will replace the previous content.

Note: To better document the content stored in report.txt, use the **echo** command to add a subheading as shown here for **Start Date and Time**. Each substep will specify a subheading for you to append before you gather information.

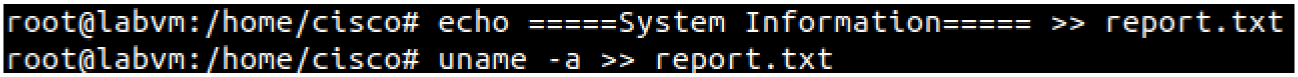
```
root@labvm:/home/cisco# echo =====Start Date and Time===== >> report.txt
root@labvm:/home/cisco# date >> report.txt
```



```
root@labvm:/home/cisco# echo =====Start Date and Time===== >> report.txt
root@labvm:/home/cisco# date >> report.txt
root@labvm:/home/cisco# 
```

d. Enter the **uname** command to print system information. Use the **-a** option to append all system information to the **report.txt** file.

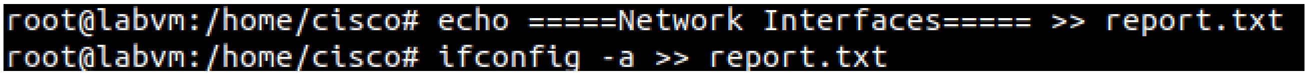
```
root@labvm:/home/cisco# echo =====System Information===== >> report.txt
root@labvm:/home/cisco# uname -a >> report.txt
```



```
root@labvm:/home/cisco# echo =====System Information===== >> report.txt
root@labvm:/home/cisco# uname -a >> report.txt
```

e. Enter the **ifconfig -a** command and append all network interface information to the **report.txt** file.

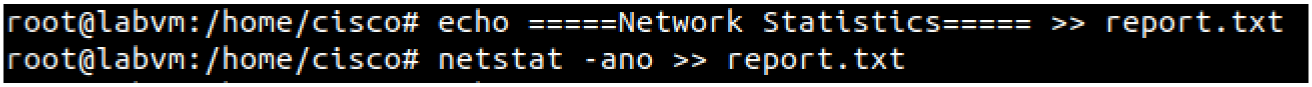
```
root@labvm:/home/cisco# echo =====Network Interfaces===== >> report.txt
root@labvm:/home/cisco# ifconfig -a >> report.txt
```



```
root@labvm:/home/cisco# echo =====Network Interfaces===== >> report.txt
root@labvm:/home/cisco# ifconfig -a >> report.txt
```

f. The **netstat** command can collect all the network statistics. Enter the command with the options **-ano** to collect data on all sockets (**-a**), IP addresses instead of domain names (**-n**), and information related to networking times (**-o**). Append the output to the **report.txt** file.

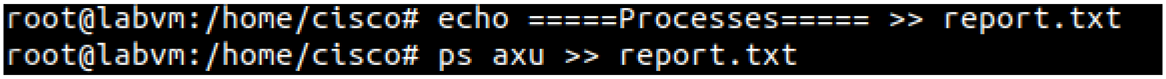
```
root@labvm:/home/cisco# echo =====Network Statistics===== >> report.txt
root@labvm:/home/cisco# netstat -ano >> report.txt
```



```
root@labvm:/home/cisco# echo =====Network Statistics===== >> report.txt
root@labvm:/home/cisco# netstat -ano >> report.txt
```

g. The **ps** command reports a snapshot of the current processes running on the system. Enter the command with the options **-axu** to list every process running on the system (**-a** and **-x**) and in a user-oriented format (**-u**). Append the output to the **report.txt** file.

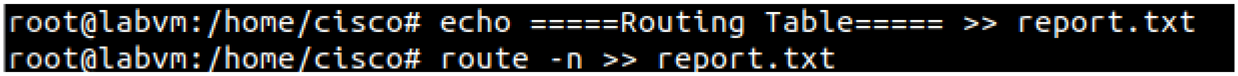
```
root@labvm:/home/cisco# echo =====Processes===== >> report.txt
root@labvm:/home/cisco# ps axu >> report.txt
```



```
root@labvm:/home/cisco# echo =====Processes===== >> report.txt
root@labvm:/home/cisco# ps axu >> report.txt
```

h. The route command lists the routing table currently used by the system. Enter the command with the option **-n** to list IP addresses instead of trying to determine host names. Append the output to the **report.txt** file.

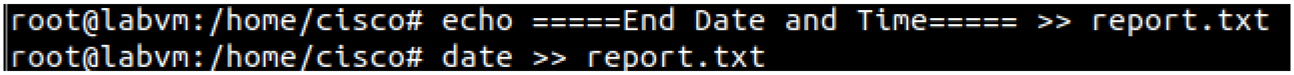
```
root@labvm:/home/cisco# echo =====Routing Table===== >> report.txt
root@labvm:/home/cisco# route -n >> report.txt
```



```
root@labvm:/home/cisco# echo =====Routing Table===== >> report.txt
root@labvm:/home/cisco# route -n >> report.txt
```

i. Enter the **date** command and append the date and timestamp to the end of the file to complete the report.

```
root@labvm:/home/cisco# echo =====End Date and Time===== >> report.txt
root@labvm:/home/cisco# date >> report.txt
```



```
root@labvm:/home/cisco# echo =====End Date and Time===== >> report.txt
root@labvm:/home/cisco# date >> report.txt
```

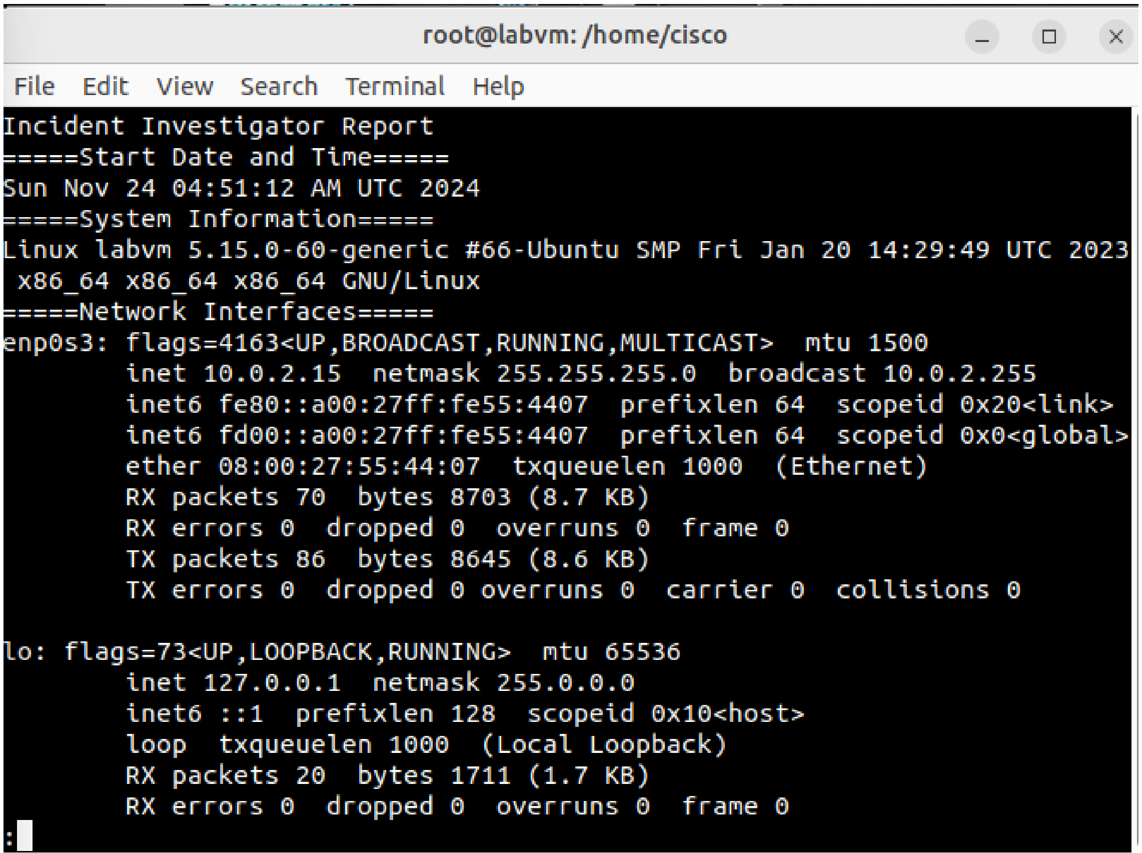
j. Use the **cat** command and pipe the output to the **less** command to view **report.txt** one page or line at a time. Press the **spacebar** to scroll down by page or press **Enter** to scroll down by a single line. Type **q** when finished.

```
root@labvm:/home/cisco# cat report.txt | less
Incident Investigator Report
=====Start Date and Time=====
Wed 24 Mar 2021 05:06:53 PM UTC
=====System Information=====
Linux labvm 5.4.0-67-generic #75-Ubuntu SMP Fri Feb 19 18:03:38 UTC 2021 x86_64
x86_64 x86_64 GNU/Linux
=====Network Interfaces=====
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:feb5:4bb0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b5:4b:b0  txqueuelen 1000  (Ethernet)
        RX packets 47719  bytes 36618515 (36.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31406  bytes 3590109 (3.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2292  bytes 244651 (244.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2292  bytes 244651 (244.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

=====Network Statistics=====
Active Internet connections (servers and established)
<output omitted>
unix  3      [ ]         STREAM     CONNECTED     22100
unix  3      [ ]         STREAM     CONNECTED     18249
=====Processes=====
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.5 101896 10768 ?        Ss   Mar23   0:03 /sbin/init
root           2  0.0  0.0      0     0 ?        S    Mar23   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Mar23   0:00 [rcu_gp]
<output omitted>
root        5319  0.0  0.0      0     0 ?        I    16:31   0:00 [kworker/0:2-
events]
root        5490  0.0  0.1  11492  3332 pts/1    R+   17:06   0:00 ps axu
=====Routing Table=====
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
```

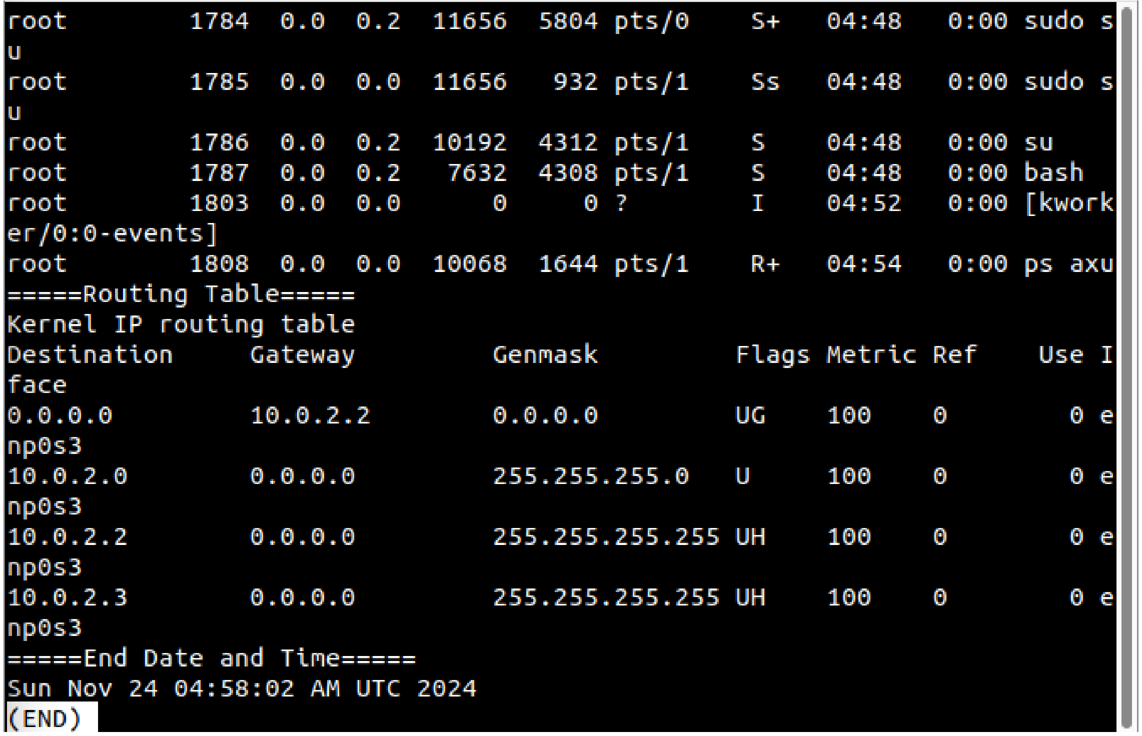
NAMA : IK-RARS’JATI PRAMESTI
NIM : 2141762003
KELAS : SIB-4C

```
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
10.0.2.2        0.0.0.0         255.255.255.255 UH    100    0        0 enp0s3
=====End Date and Time=====
Wed 24 Mar 2021 05:06:53 PM UTC
(END) q
root@labvm:/home/cisco#
```



```
Incident Investigator Report
=====Start Date and Time=====
Sun Nov 24 04:51:12 AM UTC 2024
=====System Information=====
Linux labvm 5.15.0-60-generic #66-Ubuntu SMP Fri Jan 20 14:29:49 UTC 2023
 x86_64 x86_64 x86_64 GNU/Linux
=====Network Interfaces=====
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe55:4407  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::a00:27ff:fe55:4407  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:55:44:07  txqueuelen 1000  (Ethernet)
        RX packets 70  bytes 8703 (8.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 8645 (8.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1711 (1.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
:
```



```
root        1784  0.0  0.2  11656  5804 pts/0    S+   04:48   0:00 sudo s
u
root        1785  0.0  0.0  11656   932 pts/1    Ss   04:48   0:00 sudo s
u
root        1786  0.0  0.2  10192  4312 pts/1    S    04:48   0:00 su
root        1787  0.0  0.2   7632  4308 pts/1    S    04:48   0:00 bash
root        1803  0.0  0.0      0     0 ?        I    04:52   0:00 [kwork
er/0:0-events]
root        1808  0.0  0.0  10068  1644 pts/1    R+   04:54   0:00 ps axu
=====Routing Table=====
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use I
face
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 e
np0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 e
np0s3
10.0.2.2        0.0.0.0         255.255.255.255 UH    100    0        0 e
np0s3
10.0.2.3        0.0.0.0         255.255.255.255 UH    100    0        0 e
np0s3
=====End Date and Time=====
Sun Nov 24 04:58:02 AM UTC 2024
(END)
```

NAMA : IK-RARS'JATI PRAMESTI
NIM : 2141762003
KELAS : SIB-4C

Step 3: Analyze different log files and learn their importance.

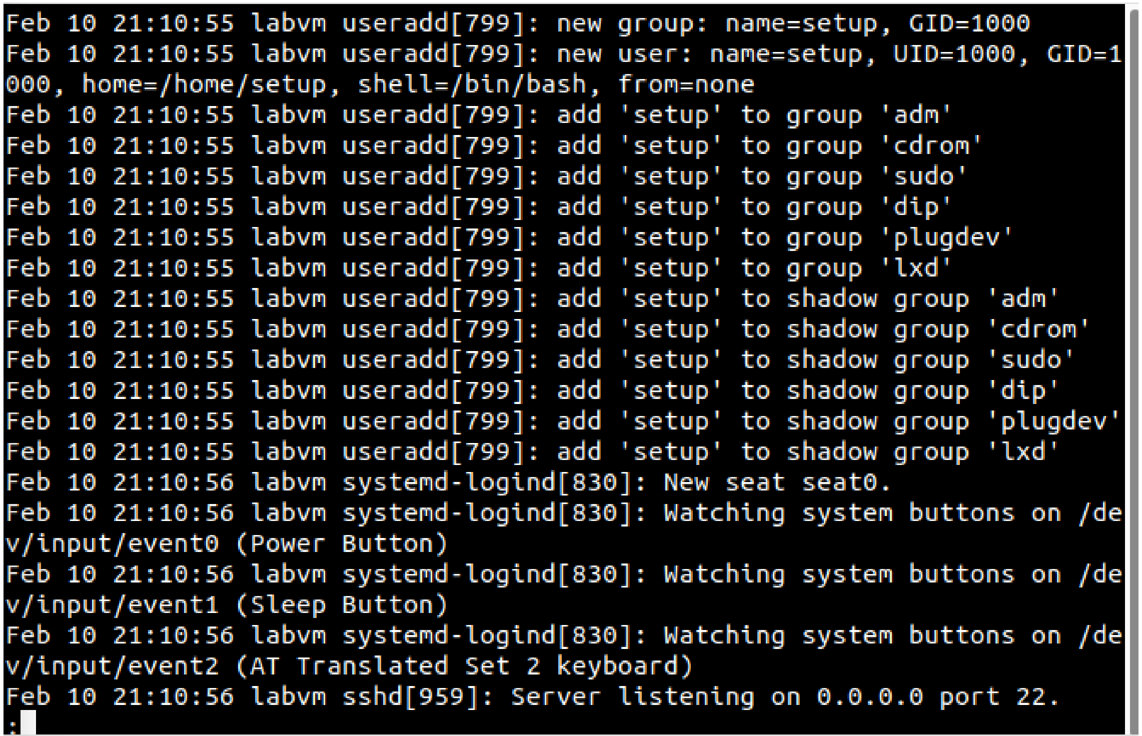
In addition to capturing information stored in RAM, the system also maintains a variety of logs that you should review after an incident. These log files can also be appended to your **report.txt** file or stored separately off the system in the event the system needs to be wiped. Logs of particular interest include, but are not limited to, the following:

- auth.log - logs system authorization information
- btmp.log - logs failed login attempts
- wtmp.log - logs who is currently logged into the system

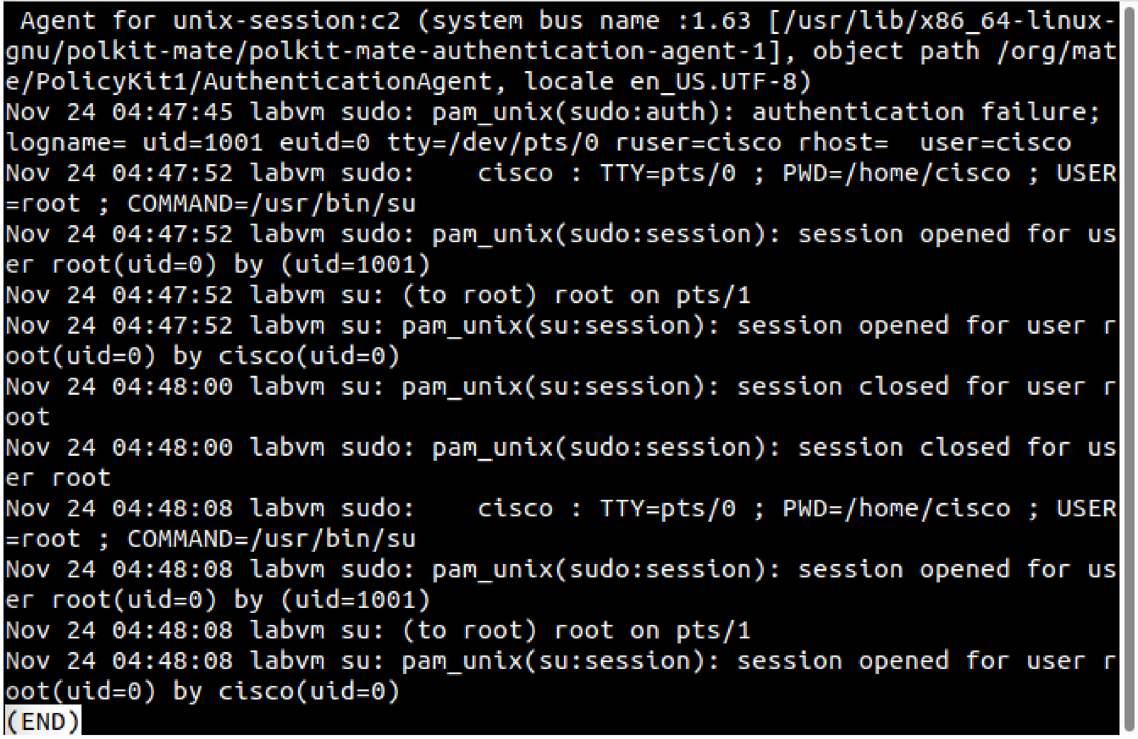
a. Use the **cat** command to view the auth.log and pipe it to the **less** command. Press the **spacebar** to scroll down by page or press **Enter** to scroll down by a single line. Type **q** when finished. Your output will be different.

```
root@labvm:/home/cisco# cat /var/log/auth.log | less
Mar 18 21:43:57 labvm sshd[375]: Server listening on 0.0.0.0 port 22.
Mar 18 21:43:57 labvm sshd[375]: Server listening on :: port 22.
Mar 18 21:43:57 labvm systemd-logind[366]: New seat seat0.
Mar 18 21:43:57 labvm systemd-logind[366]: Watching system buttons on
/dev/input/event0 (Power Button)
Mar 18 21:43:57 labvm systemd-logind[366]: Watching system buttons on
/dev/input/event1 (Sleep Button)
Mar 18 21:43:57 labvm systemd-logind[366]: Watching system buttons on
/dev/input/event2 (AT Translated Set 2 keyboard)
Mar 18 21:43:59 labvm sshd[408]: error: kex_exchange_identification: Connection
closed by remote host
Mar 18 21:43:59 labvm sshd[407]: Accepted password for cisco from 10.0.2.2 port
57067 ssh2
Mar 18 21:43:59 labvm sshd[407]: pam_unix(sshd:session): session opened for user
cisco by (uid=0)
Mar 18 21:43:59 labvm systemd-logind[366]: New session 1 of user cisco.
<output omitted>
(END) q
root@labvm:/home/cisco#
```

NAMA : IK-RARS’JATI PRAMESTI
NIM : 2141762003
KELAS : SIB-4C



```
Feb 10 21:10:55 labvm useradd[799]: new group: name=setup, GID=1000
Feb 10 21:10:55 labvm useradd[799]: new user: name=setup, UID=1000, GID=1
000, home=/home/setup, shell=/bin/bash, from=none
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to group 'adm'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to group 'cdrom'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to group 'sudo'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to group 'dip'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to group 'plugdev'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to group 'lxd'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to shadow group 'adm'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to shadow group 'cdrom'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to shadow group 'sudo'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to shadow group 'dip'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to shadow group 'plugdev'
Feb 10 21:10:55 labvm useradd[799]: add 'setup' to shadow group 'lxd'
Feb 10 21:10:56 labvm systemd-logind[830]: New seat seat0.
Feb 10 21:10:56 labvm systemd-logind[830]: Watching system buttons on /de
v/input/event0 (Power Button)
Feb 10 21:10:56 labvm systemd-logind[830]: Watching system buttons on /de
v/input/event1 (Sleep Button)
Feb 10 21:10:56 labvm systemd-logind[830]: Watching system buttons on /de
v/input/event2 (AT Translated Set 2 keyboard)
Feb 10 21:10:56 labvm sshd[959]: Server listening on 0.0.0.0 port 22.
:
```

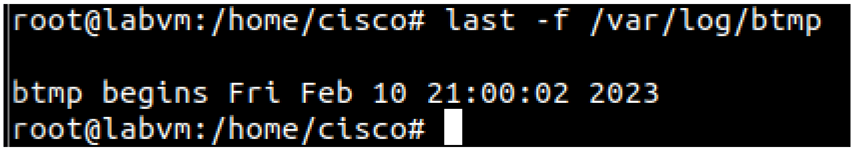


```
 Agent for unix-session:c2 (system bus name :1.63 [/usr/lib/x86_64-linux-
gnu/polkit-mate/polkit-mate-authentication-agent-1], object path /org/mat
e/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Nov 24 04:47:45 labvm sudo: pam_unix(sudo:auth): authentication failure;
logname= uid=1001 euid=0 tty=/dev/pts/0 ruser=cisco rhost=  user=cisco
Nov 24 04:47:52 labvm sudo:    cisco : TTY=pts/0 ; PWD=/home/cisco ; USER
=root ; COMMAND=/usr/bin/su
Nov 24 04:47:52 labvm sudo: pam_unix(sudo:session): session opened for us
er root(uid=0) by (uid=1001)
Nov 24 04:47:52 labvm su: (to root) root on pts/1
Nov 24 04:47:52 labvm su: pam_unix(su:session): session opened for user r
oot(uid=0) by cisco(uid=0)
Nov 24 04:48:00 labvm su: pam_unix(su:session): session closed for user r
oot
Nov 24 04:48:00 labvm sudo: pam_unix(sudo:session): session closed for us
er root
Nov 24 04:48:08 labvm sudo:    cisco : TTY=pts/0 ; PWD=/home/cisco ; USER
=root ; COMMAND=/usr/bin/su
Nov 24 04:48:08 labvm sudo: pam_unix(sudo:session): session opened for us
er root(uid=0) by (uid=1001)
Nov 24 04:48:08 labvm su: (to root) root on pts/1
Nov 24 04:48:08 labvm su: pam_unix(su:session): session opened for user r
oot(uid=0) by cisco(uid=0)
(END)
```

b. The **last** command shows a listing of last logged in users. Enter the command with the **-f** option to specify the log file. The **btmp** log file shows failed login attempts. Your output will be different.

```
root@labvm:/home/cisco# last -f /var/log/btmp
UNKNOWN  tty6                          Thu Mar 18 21:47    gone - no logout
UNKNOWN  tty4                          Thu Mar 18 21:47    gone - no logout
UNKNOWN  tty3                          Thu Mar 18 21:47    gone - no logout
cisco    tty1                          Thu Mar 18 21:47    gone - no logout
cisco    tty1                          Thu Mar 18 21:47 - 21:47  (00:00)
```

```
btmp begins Thu Mar 18 21:47:05 2021
root@labvm:/home/cisco#
```



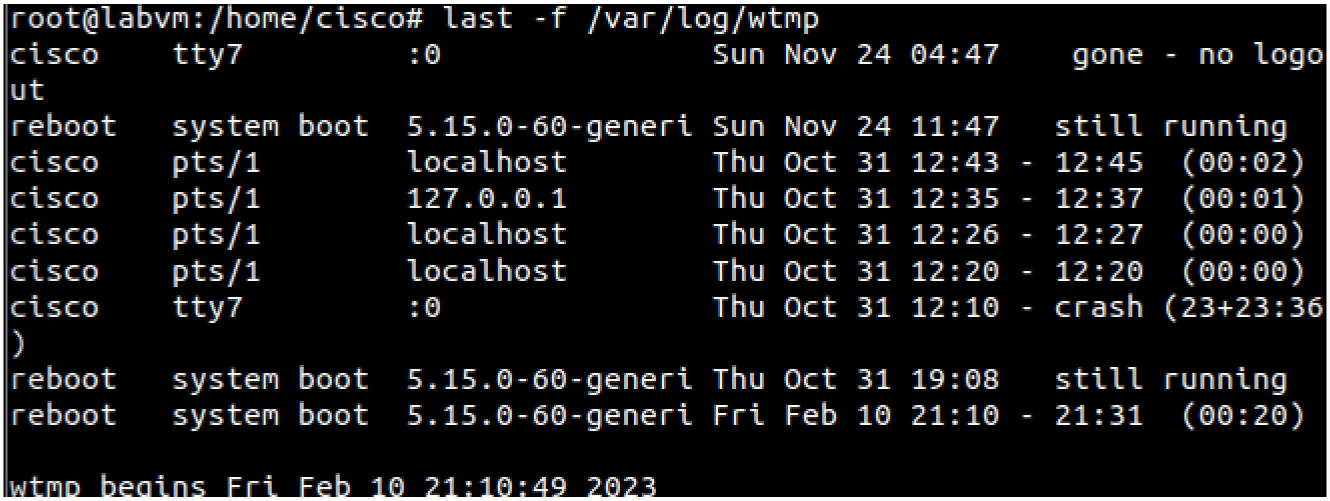
```
root@labvm:/home/cisco# last -f /var/log/btmp

btmp begins Fri Feb 10 21:00:02 2023
root@labvm:/home/cisco# 
```

c. Enter the **last** command again specifying the **wtmp** file to show who is currently connected to the system. Your output will be different.

```
root@labvm:/home/cisco# last -f /var/log/wtmp
cisco    tty7         :0                Tue Mar 23 19:38    gone - no logout
reboot   system boot  5.4.0-67-generic Tue Mar 23 14:38   still running
cisco    tty2                           Thu Mar 18 21:47 - 21:47  (00:00)
reboot   system boot  5.4.0-67-generic Thu Mar 18 21:43 - 22:02  (00:18)

wtmp begins Thu Mar 18 21:43:54 2021
```

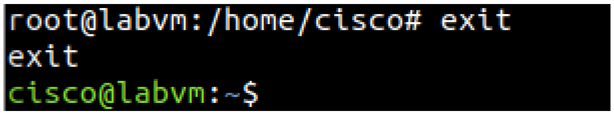


```
root@labvm:/home/cisco# last -f /var/log/wtmp
cisco    tty7         :0               Sun Nov 24 04:47    gone - no logo
ut
reboot   system boot  5.15.0-60-generi Sun Nov 24 11:47   still running
cisco    pts/1        localhost        Thu Oct 31 12:43 - 12:45  (00:02)
cisco    pts/1        127.0.0.1        Thu Oct 31 12:35 - 12:37  (00:01)
cisco    pts/1        localhost        Thu Oct 31 12:26 - 12:27  (00:00)
cisco    pts/1        localhost        Thu Oct 31 12:20 - 12:20  (00:00)
cisco    tty7         :0               Thu Oct 31 12:10 - crash (23+23:36
)
reboot   system boot  5.15.0-60-generi Thu Oct 31 19:08   still running
reboot   system boot  5.15.0-60-generi Fri Feb 10 21:10 - 21:31  (00:20)

wtmp begins Fri Feb 10 21:10:49 2023
```

d. Enter the **exit** command to switch back to the cisco user.

```
root@labvm:/home/cisco# exit
cisco@labvm:~$
```



```
root@labvm:/home/cisco# exit
exit
cisco@labvm:~$
```

End of document