

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.

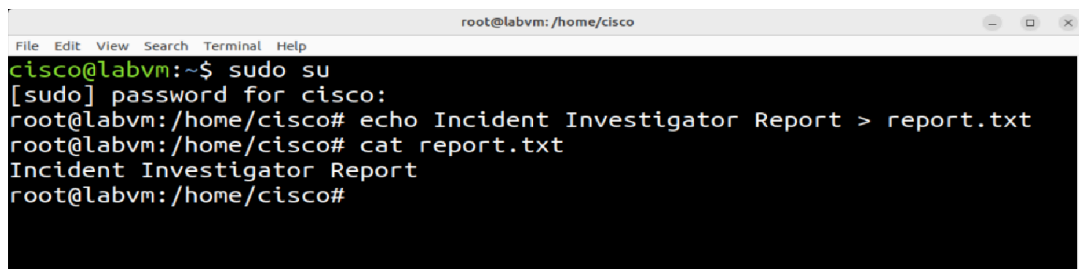
Step 1: Open a terminal window in the CSE-LABVM.

- 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.
- 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.

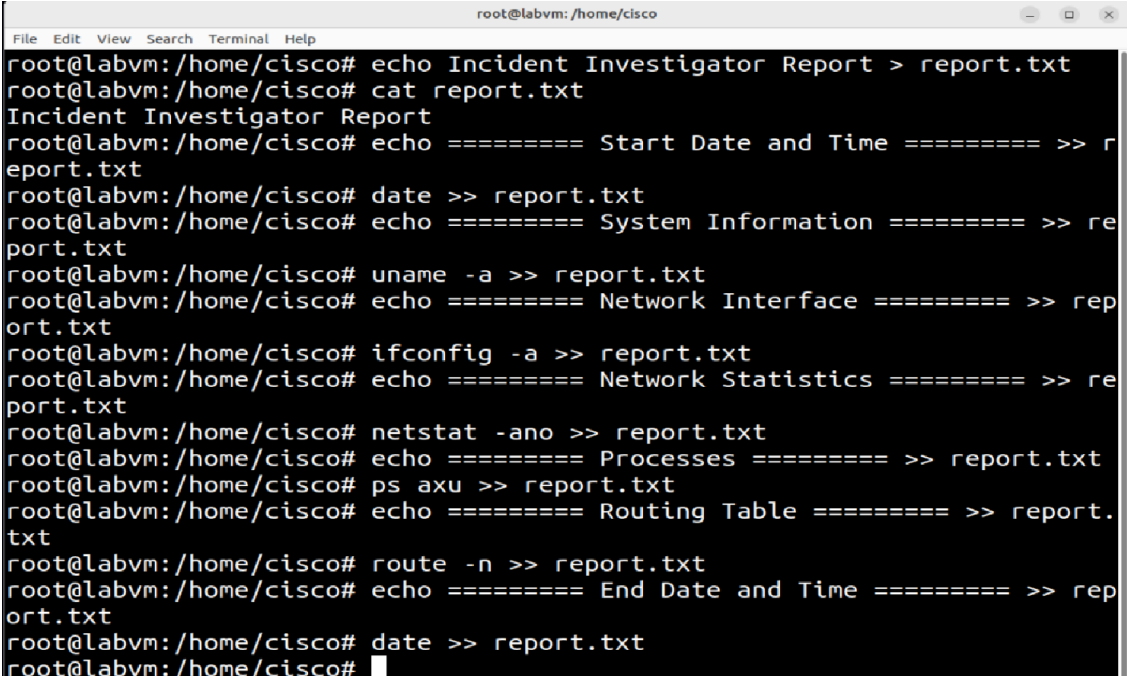


```
root@labvm: /home/cisco
File Edit View Search Terminal Help
cisco@labvm:~$ sudo su
[sudo] password for cisco:
root@labvm:/home/cisco# echo Incident Investigator Report > report.txt
root@labvm:/home/cisco# cat report.txt
Incident Investigator Report
root@labvm:/home/cisco#
```

- 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.

- d. Enter the `uname` command to print system information. Use the `-a` option to append all system information to the **report.txt** file.
- e. Enter the `ifconfig -a` command and append all network interface information to the **report.txt** file.
- 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.
- 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.
- 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.
- i. Enter the `date` command and append the date and timestamp to the end of the file to complete the report.

A screenshot of a terminal window titled 'root@labvm: /home/cisco'. The terminal shows a series of commands being executed to create and populate a file named 'report.txt'. The commands include: 'echo Incident Investigator Report > report.txt', 'cat report.txt', 'echo ===== Start Date and Time ===== >> report.txt', 'date >> report.txt', 'echo ===== System Information ===== >> report.txt', 'uname -a >> report.txt', 'echo ===== Network Interface ===== >> report.txt', 'ifconfig -a >> report.txt', 'echo ===== Network Statistics ===== >> report.txt', 'netstat -ano >> report.txt', 'echo ===== Processes ===== >> report.txt', 'ps axu >> report.txt', 'echo ===== Routing Table ===== >> report.txt', 'route -n >> report.txt', 'echo ===== End Date and Time ===== >> report.txt', and 'date >> report.txt'. The prompt 'root@labvm: /home/cisco#' is visible at the end of each line.

```
root@labvm: /home/cisco# echo Incident Investigator Report > report.txt
root@labvm: /home/cisco# cat report.txt
Incident Investigator Report
root@labvm: /home/cisco# echo ===== Start Date and Time ===== >> report.txt
root@labvm: /home/cisco# date >> report.txt
root@labvm: /home/cisco# echo ===== System Information ===== >> report.txt
root@labvm: /home/cisco# uname -a >> report.txt
root@labvm: /home/cisco# echo ===== Network Interface ===== >> report.txt
root@labvm: /home/cisco# ifconfig -a >> report.txt
root@labvm: /home/cisco# echo ===== Network Statistics ===== >> report.txt
root@labvm: /home/cisco# netstat -ano >> report.txt
root@labvm: /home/cisco# echo ===== Processes ===== >> report.txt
root@labvm: /home/cisco# ps axu >> report.txt
root@labvm: /home/cisco# echo ===== Routing Table ===== >> report.txt
root@labvm: /home/cisco# route -n >> report.txt
root@labvm: /home/cisco# echo ===== End Date and Time ===== >> report.txt
root@labvm: /home/cisco# date >> report.txt
root@labvm: /home/cisco#
```

- 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
File Edit View Search Terminal Help
Incident Investigator Report
===== Start Date and Time =====
Mon Jan 13 09:23:25 PM UTC 2025
===== 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 Interface =====
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.6 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 2806:2f0:53e0:326:a00:27ff:fe55:4407 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fe55:4407 prefixlen 64 scopeid 0x20<link>
    inet6 2806:2f0:53e0:326::3 prefixlen 128 scopeid 0x0<global>
    ether 08:00:27:55:44:07 txqueuelen 1000 (Ethernet)
    RX packets 79076 bytes 57533243 (57.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48743 bytes 7239910 (7.2 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 7235 bytes 847195 (847.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7235 bytes 847195 (847.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

===== Network Statistics =====
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:21            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN      off (0.00/0/0)
```

...

```
cisco      28039  0.0  3.1 2419456 63340 ?      Sl  20:31  0:00 /usr/lib/firefox/firefox -
contentproc -isForBrowser -prefsHandle 0 -prefsLen 38705 -prefMapHandle 1 -prefMapSize 256562
-jsInitHandle 2 -jsInitLen 234660 -parentBuildID 20241121140525 -sandboxReporter 3 -chrootCL
ient 4 -ipcHandle 5 -initialChannelId {9a5a1804-a456-4062-89f3-7d74f0c613cb} -parentPid 1812
-crashReporter 6 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja
-appDir /usr/lib/firefox/browser 48 tab
cisco      28088  0.0  3.1 2419456 63452 ?      Sl  20:31  0:01 /usr/lib/firefox/firefox -
contentproc -isForBrowser -prefsHandle 0 -prefsLen 38705 -prefMapHandle 1 -prefMapSize 256562
-jsInitHandle 2 -jsInitLen 234660 -parentBuildID 20241121140525 -sandboxReporter 3 -chrootCL
ient 4 -ipcHandle 5 -initialChannelId {4f75e386-35fb-4de2-a691-844698debb03} -parentPid 1812
-crashReporter 6 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja
-appDir /usr/lib/firefox/browser 49 tab
root       28290  0.0  0.0  0 0 ?      I  20:34  0:00 [kworker/u4:2-events_power
_efficient]
root       28776  0.0  0.0  0 0 ?      I  20:55  0:00 [kworker/1:1-events]
root       28777  0.0  0.0  0 0 ?      I  20:55  0:01 [kworker/0:1-events]
root       28924  0.0  0.0  0 0 ?      I  21:02  0:00 [kworker/1:2-events]
cisco      28987  0.5  2.4 897364 50504 ?      Sl  21:02  0:08 mate-terminal
cisco      29018  0.0  0.2  8668 5280 pts/3  Ss  21:02  0:00 bash
root       29118  0.0  0.3 11660 6088 pts/3  S+  21:05  0:00 sudo su
root       29121  0.0  0.0 11660  932 pts/4  Ss  21:05  0:00 sudo su
root       29122  0.0  0.2 10196 4392 pts/4  S  21:05  0:00 su
root       29123  0.0  0.2  7636 4292 pts/4  S  21:05  0:00 bash
root       29629  0.0  0.0  0 0 ?      I  21:07  0:00 [kworker/u4:3-events_unbou
nd]
root       30085  0.0  0.0  0 0 ?      I  21:12  0:00 [kworker/0:2-events]
root       30366  0.0  0.1 10072 3488 pts/4  R+  21:27  0:00 ps aux

===== Routing Table =====
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.100.1 0.0.0.0 UG 100 0 0 enp0s3
192.168.100.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
192.168.100.1 0.0.0.0 255.255.255.255 UH 100 0 0 enp0s3

===== End Date and Time =====
Mon Jan 13 09:29:29 PM UTC 2025
(END)
```

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
 - `bttmp.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
```

File Edit View Search Terminal Help

```
Jan 13 21:05:11 labvm sudo: cisco : TTY=pts/3 ; PWD=/home/cisco ; USER=root ;  
COMMAND=/usr/bin/su  
Jan 13 21:05:11 labvm sudo: pam_unix(sudo:session): session opened for user root  
(uid=0) by (uid=1001)  
Jan 13 21:05:11 labvm su: (to root) root on pts/4  
Jan 13 21:05:11 labvm su: pam_unix(su:session): session opened for user root(uid=  
=0) by cisco(uid=0)  
Jan 13 21:17:01 labvm CRON[30164]: pam_unix(cron:session): session opened for us  
er root(uid=0) by (uid=0)  
Jan 13 21:17:01 labvm CRON[30164]: pam_unix(cron:session): session closed for us  
er root  
Jan 13 21:30:01 labvm CRON[30411]: pam_unix(cron:session): session opened for us  
er root(uid=0) by (uid=0)  
Jan 13 21:30:01 labvm CRON[30411]: pam_unix(cron:session): session closed for us  
er root  
  
~  
  
~  
  
~  
  
~  
  
~  
  
~  
  
(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 `btm` log file shows failed login attempts. Your output will be different.

```
root@labvm:/home/cisco
File Edit View Search Terminal Help
root@labvm:/home/cisco# last -f /var/log/btmp
btmp begins Fri Jan 3 21:24:53 2025
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 pts/6 127.0.0.1 Wed Jan 8 21:43 - 21:45 (00:02)
cisco pts/6 localhost Wed Jan 8 21:24 - 21:26 (00:02)
analyst pts/5 127.0.0.1 Fri Dec 27 16:11 - 16:27 (00:16)
analyst pts/5 localhost Fri Dec 27 15:55 - 16:00 (00:05)
analyst tty10 :3 Thu Dec 26 21:55 gone - no logout
joe tty9 :2 Mon Dec 16 22:29 gone - no logout
jenny tty8 :1 Mon Dec 16 22:18 gone - no logout
cisco tty7 :0 Fri Dec 6 22:25 gone - no logout
reboot system boot 5.15.0-60-generi Fri Dec 6 22:24 still running
analyst tty7 :0 Wed Dec 4 22:36 - 22:24 (1+23:48)
reboot system boot 5.15.0-60-generi Wed Dec 4 16:33 - 22:24 (2+05:50)
reboot tty7 :0 Wed Dec 4 22:29 - crash (-5:56)
reboot system boot 5.15.0-60-generi Wed Dec 4 16:28 - 22:24 (2+05:55)
analyst tty7 :0 Wed Dec 4 22:25 - crash (-5:56)
reboot system boot 5.15.0-60-generi Wed Dec 4 16:24 - 22:24 (2+05:59)
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
root@labvm:/home/cisco#
```

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

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