

Nama : Sasmita Rachmawati

Absen : 15

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.

- Launch the **CSE-LABVM**.
- Double-click the **Terminal** icon to open a terminal.

Step 2: Collect volatile information of the compromised system.

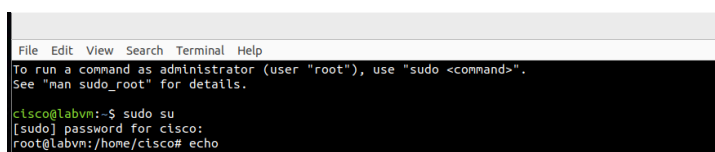
In this step, you will create a file called **report.txt** that includes a variety of system information that can be used for incident analysis. This report can then be transferred to a USB drive, emailed, or uploaded to a cloud server to preserve the information. Then the system can be taken down.

- 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#
```



```
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

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

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#
```

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

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
```

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
uname -a: command not found
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 Statistic=====>>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
0.0.0.0	10.0.2.2	0.0.0.0	UG	100	0	0	enp0s3

```
10.0.2.2    0.0.0.0    255.255.255.255 UH  100  0    0 enp0s3
```

Wed 24 Mar 2021 05:06:53 PM UTC

(END) **q**

```
root@labvm:/home/cisco#
```

```
root@labvm:/home/cisco# cat report.txt | less
```

```

File Edit View Search Terminal Help
Incident Investigator Report
Reporter Date and Time:
Fri Nov 7 10:43:56 AM UTC 2024
Network System Information:
Linux labvm-1.x86_64-generic #40-Ubuntu SMP Fri Jan 7 04:19:49 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
=====Network Interface=====
ensd3sl flags=43BUP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet 10.0.2.15 network 255.255.255.0 broadcast 10.0.2.255
ether f8bb:1ad0:2fff:f655:440f prefilterlen 64 scoped backglobal
TX packets 67 bytes 6782 (c.7 kb)
RX errors 0 dropped 0 overruns 0 frame 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
-----
lo flags=73UP,LOOPBACK,RUNNING mtu 65536
inet 127.0.0.1 network 255.0.0.0
ether ::::: prefilterlen 3284 scoped backhost+
loop txqueuelen 1000 (Local Loopback)
RX packets 30 bytes 2404 (c.4 kb)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 30 bytes 2404 (c.4 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 0.0.0.0:* LISTEN off (0.00/0/0)
tcp 0 0 0.0.0.0:22 LISTEN off (0.00/0/0)
tcp 0 0 0.127.0.0:22 LISTEN off (0.00/0/0)
udp 0 0 0.0.0.0:3301 LISTEN off (0.00/0/0)
udp 0 0 *:223 LISTEN off (0.00/0/0)
udp 0 0 *:223 LISTEN off (0.00/0/0)
udp 0 0 0.0.0.0:21559551 ESTABLISHED off (0.00/0/0)
udp 0 0 0.0.0.0:81031 ESTABLISHED off (0.00/0/0)
udp 0 0 0.127.0.0:3113 ESTABLISHED off (0.00/0/0)
udp 0 0 0.0.0.0:2155108 ESTABLISHED off (0.00/0/0)
udp 0 0 0.10.0.2:21541038 ESTABLISHED off (0.00/0/0)
udp 0 0 0.0.0.0:2151123 ESTABLISHED off (0.00/0/0)
udp 0 0 0.127.0.0:21123 ESTABLISHED off (0.00/0/0)
udp 0 0 0.0.0.0:81123 ESTABLISHED off (0.00/0/0)
udp 0 0 0.0.0.0:81353 ESTABLISHED off (0.00/0/0)
udp 0 0 0 FDB8:1AD0:2FFF:F655:123:123:1111 off (0.00/0/0)
udp 0 0 0 FDB8:1AD0:2FFF:F655:123:123:1111 off (0.00/0/0)
udp 0 0 0 FDB8:1AD0:2FFF:F655:123:123:1111 off (0.00/0/0)
udp 0 0 0 :1123 off (0.00/0/0)
udp 0 0 0 :1123 off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ] DGRAM LISTENING 21830 /tmp/.ICE-unix/1134
unix 2 [ ] STREAM LISTENING 21841 /run/user/1001/systemd/notify
unix 2 [ ] STREAM LISTENING 21847 /run/user/1001/bos
unix 2 [ ] STREAM LISTENING 21849 /run/user/1001/gnupg/gpg-agent-browser
unix 2 [ ] STREAM LISTENING 21853 /run/user/1001/gnupg/gpg-agent-writer
unix 2 [ ] STREAM LISTENING 21853 /run/user/1001/gnupg/gpg-agent-x11
unix 2 [ ] STREAM LISTENING 21877 /tmp/.X11-unix/R0
unix 2 [ ] STREAM LISTENING 21855 /run/user/1001/gnupg/gpg-agent-sch
unix 2 [ ] STREAM LISTENING 21857 /run/user/1001/gnupg/gpg-agent
unix 2 [ ] STREAM LISTENING 21859 /run/user/1001/gnupg/gpg-agent
unix 2 [ ] STREAM LISTENING 21861 /run/user/1001/polkit/native
unix 2 [ ] STREAM LISTENING 21912 /run/user/1001/dbusconf/socket
unix 3 [ ] DGRAM CONNECTED 16710 /run/systemd/notify
unix 2 [ ] STREAM LISTENING 16712 /run/systemd/tlsync
unix 2 [ ] STREAM LISTENING 16715 /run/systemd/userdb-to-systemd-dynamicuser
unix 2 [ ] STREAM LISTENING 16716 /run/systemd/journal/routing
unix 2 [ ] STREAM LISTENING 16721 /run/systemd/frack.progress
unix 17 [ ] DGRAM CONNECTED 10757 /run/systemd/journal/send-log

```



```
btcp begins Fri Feb 10 21:00:02 2023
```

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
```

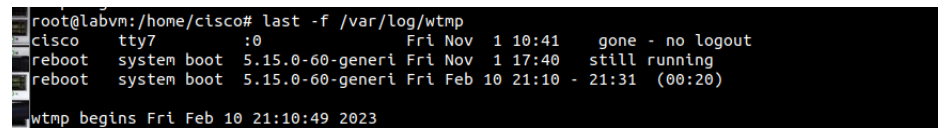
```
cisco  tty7      :0          Tue Mar 23 19:38  gone - no logout
```

```
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          Fri Nov  1 10:41  gone - no logout
reboot  system boot  5.15.0-60-generi Fri Nov  1 17:40  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:~$
```