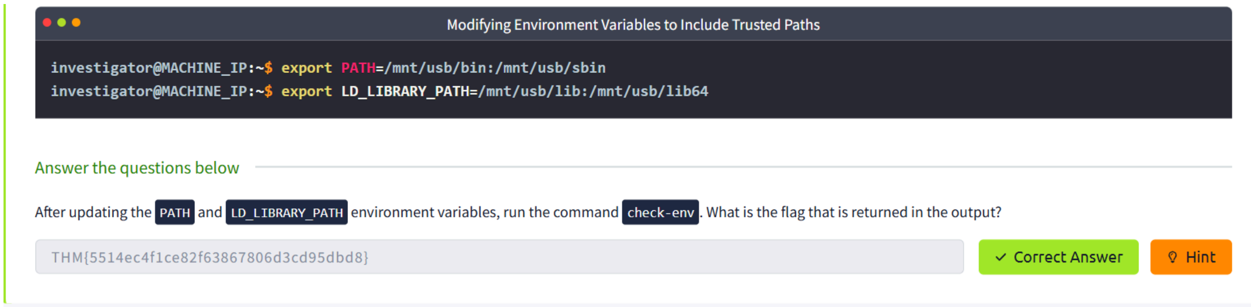
Name: Ram Haygrev S　　　　　　　　Roll No : 231901039

EX 8: Perform rootkit detection and removal using rkhunter tool.

AIM:

To learn about rootkit detection and rkhunter tool.

PROBLEMS:



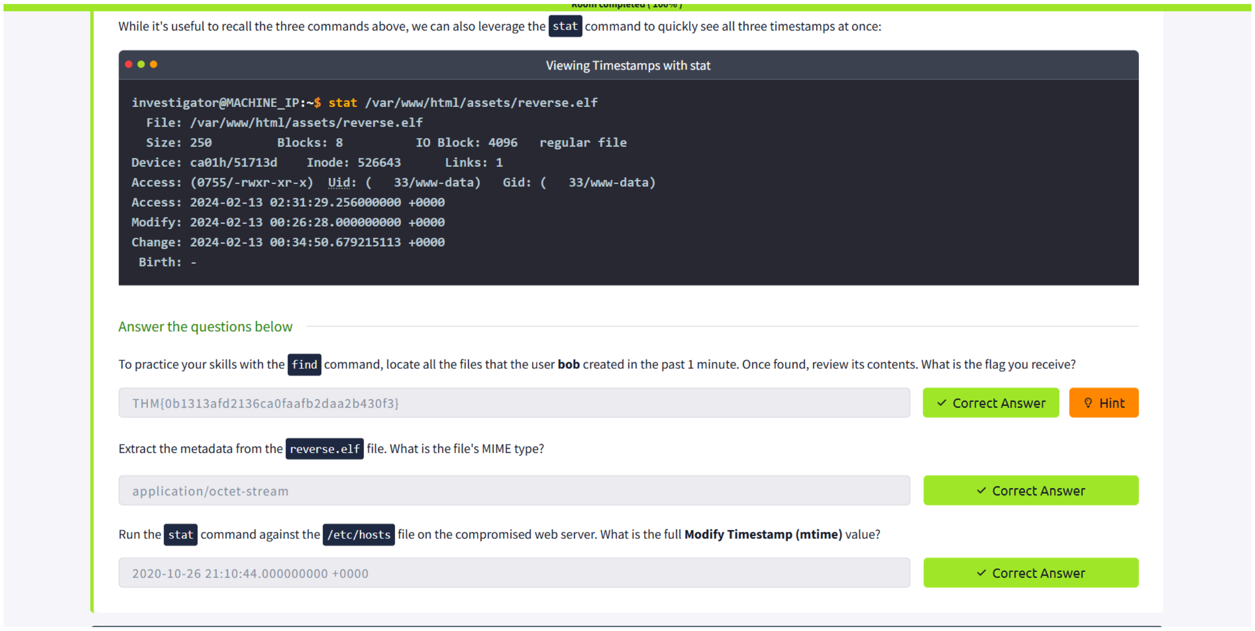
Modifying Environment Variables to Include Trusted Paths

```
investigator@MACHINE_IP:~$ export PATH=/mnt/usb/bin:/mnt/usb/sbin
investigator@MACHINE_IP:~$ export LD_LIBRARY_PATH=/mnt/usb/lib:/mnt/usb/lib64
```

Answer the questions below

After updating the `PATH` and `LD_LIBRARY_PATH` environment variables, run the command `check-env`. What is the flag that is returned in the output?

THM{5514ec4f1ce82f63867806d3cd95dbd8}



While it's useful to recall the three commands above, we can also leverage the `stat` command to quickly see all three timestamps at once:

Viewing Timestamps with stat

```
investigator@MACHINE_IP:~$ stat /var/www/html/assets/reverse.elf
  File: /var/www/html/assets/reverse.elf
  Size: 250         Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 526643      Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (   33/www-data)   Gid: (   33/www-data)
Access: 2024-02-13 02:31:29.256000000 +0000
Modify: 2024-02-13 00:26:28.000000000 +0000
Change: 2024-02-13 00:34:50.679215113 +0000
 Birth: -
```

Answer the questions below

To practice your skills with the `find` command, locate all the files that the user **bob** created in the past 1 minute. Once found, review its contents. What is the flag you receive?

THM{0b1313afd2136ca0faafb2daa2b430f3}

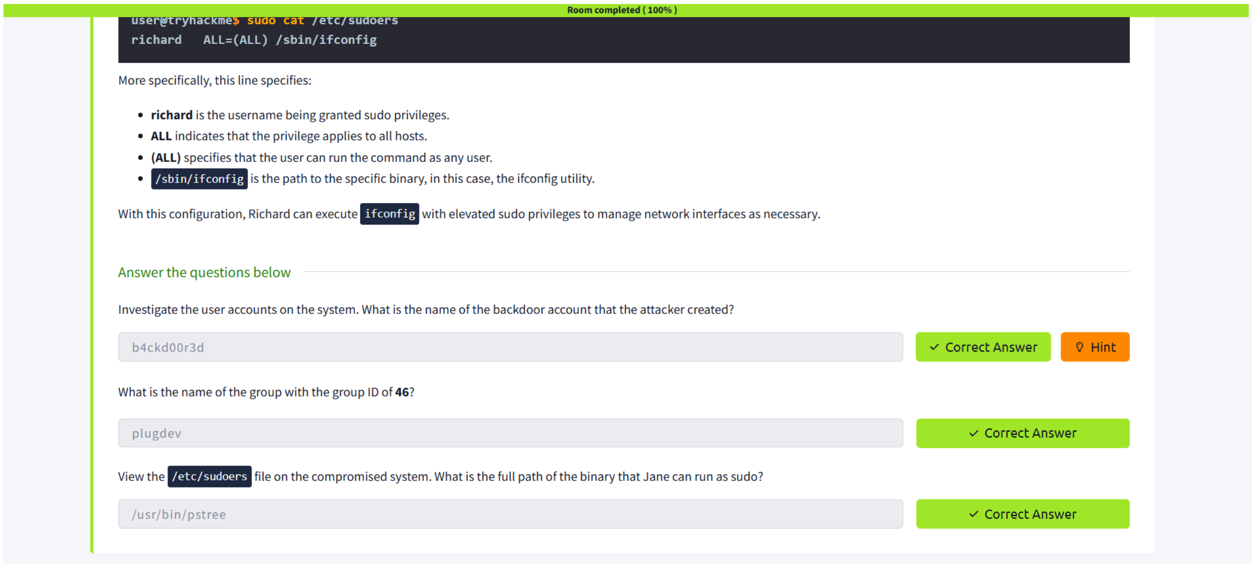
Extract the metadata from the `reverse.elf` file. What is the file's MIME type?

application/octet-stream

Run the `stat` command against the `/etc/hosts` file on the compromised web server. What is the full **Modify Timestamp (mtime)** value?

2020-10-26 21:10:44.000000000 +0000

Name: Ram Haygrev S Roll No : 231901039



```
user@tryhackme$ sudo cat /etc/sudoers
richard    ALL=(ALL) /sbin/ifconfig
```

More specifically, this line specifies:

- **richard** is the username being granted sudo privileges.
- **ALL** indicates that the privilege applies to all hosts.
- **(ALL)** specifies that the user can run the command as any user.
- `/sbin/ifconfig` is the path to the specific binary, in this case, the ifconfig utility.

With this configuration, Richard can execute `ifconfig` with elevated sudo privileges to manage network interfaces as necessary.

Answer the questions below

Investigate the user accounts on the system. What is the name of the backdoor account that the attacker created?

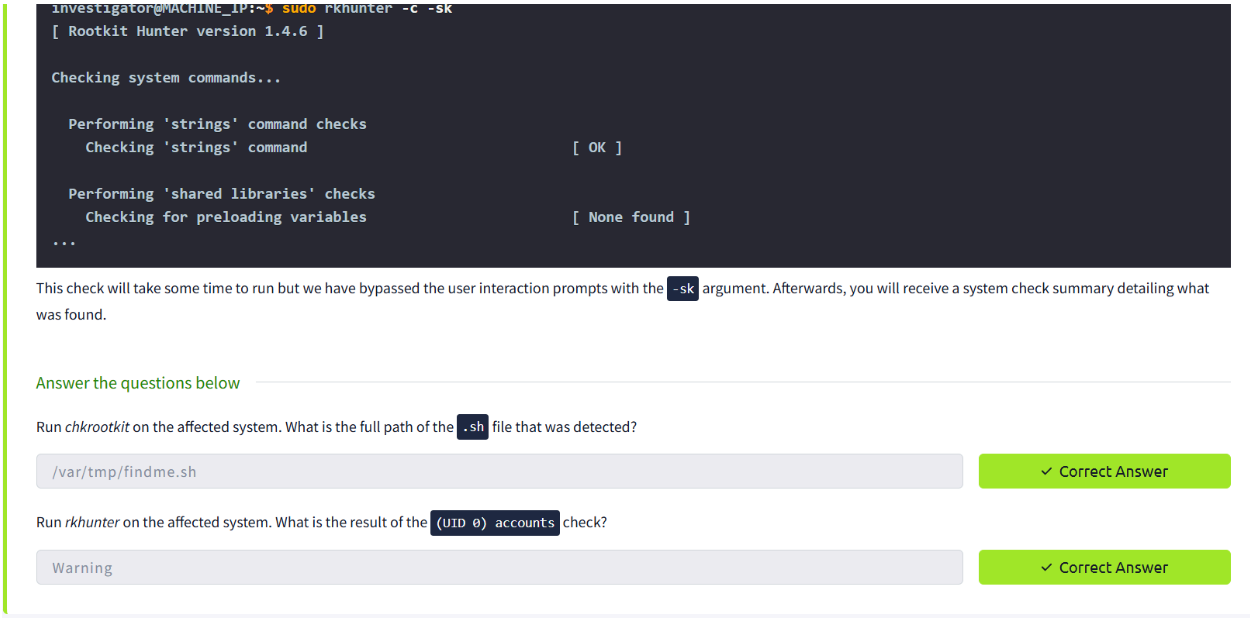
b4ckd00r3d

What is the name of the group with the group ID of **46**?

plugdev

View the `/etc/sudoers` file on the compromised system. What is the full path of the binary that Jane can run as sudo?

/usr/bin/pstree



```
investigator@MACHINE_IP:~$ sudo rkhunter -c -sk
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                           [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                    [ None found ]
...
```

This check will take some time to run but we have bypassed the user interaction prompts with the `-sk` argument. Afterwards, you will receive a system check summary detailing what was found.

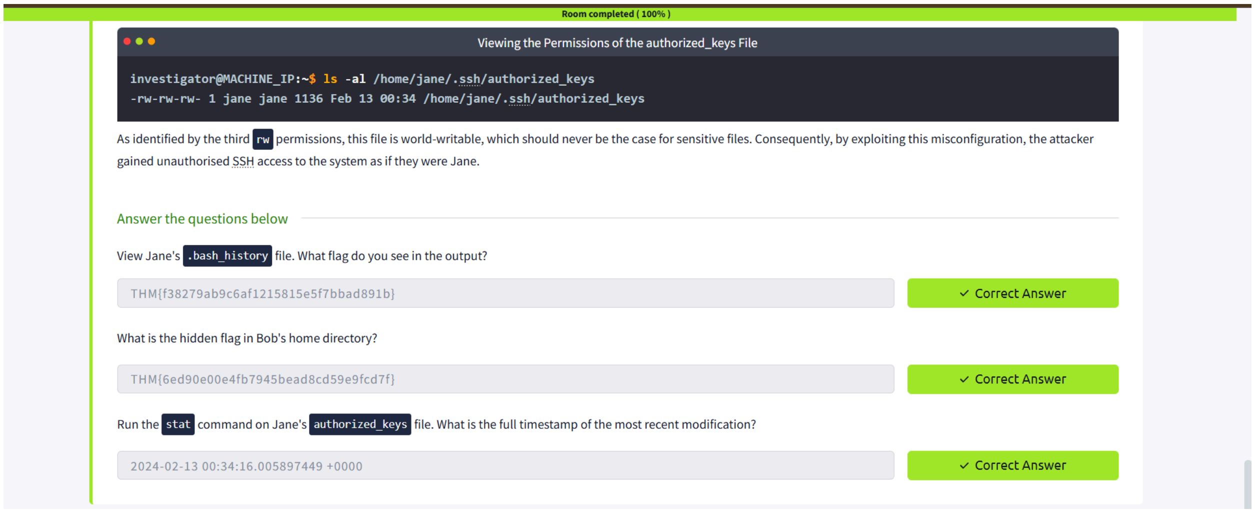
Answer the questions below

Run *chkrootkit* on the affected system. What is the full path of the `.sh` file that was detected?

/var/tmp/findme.sh

Run *rkhunter* on the affected system. What is the result of the `(UID 0) accounts` check?

Warning



```
investigator@MACHINE_IP:~$ ls -al /home/jane/.ssh/authorized_keys
-rw-rw-rw- 1 jane jane 1136 Feb 13 00:34 /home/jane/.ssh/authorized_keys
```

As identified by the third `rw` permissions, this file is world-writable, which should never be the case for sensitive files. Consequently, by exploiting this misconfiguration, the attacker gained unauthorised SSH access to the system as if they were Jane.

Answer the questions below

View Jane's `.bash_history` file. What flag do you see in the output?

THM{f38279ab9c6af1215815e5f7bbad891b}

What is the hidden flag in Bob's home directory?

THM{6ed90e00e4fb7945bead8cd59e9fcd7f}

Run the `stat` command on Jane's `authorized_keys` file. What is the full timestamp of the most recent modification?

2024-02-13 00:34:16.005897449 +0000

Result: Hence the experiment was done successfully