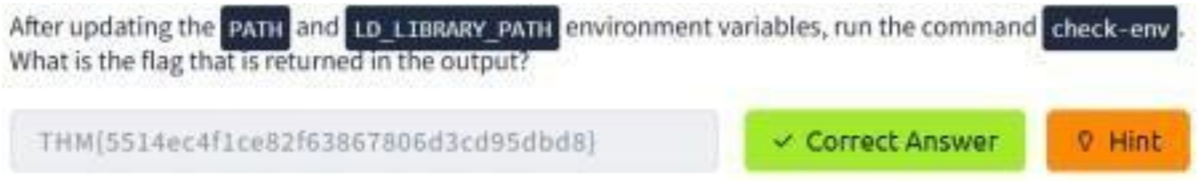
EX NO : 8 PERFORM ROOTKIT DETECTION AND REMOVAL USING RKHUNTER Tool **Date:6-4-25**

231901016 **Jose Mugilan D**

AIM:

Perform real-time file system analysis on a Linux system to identify an attacker's artefacts.

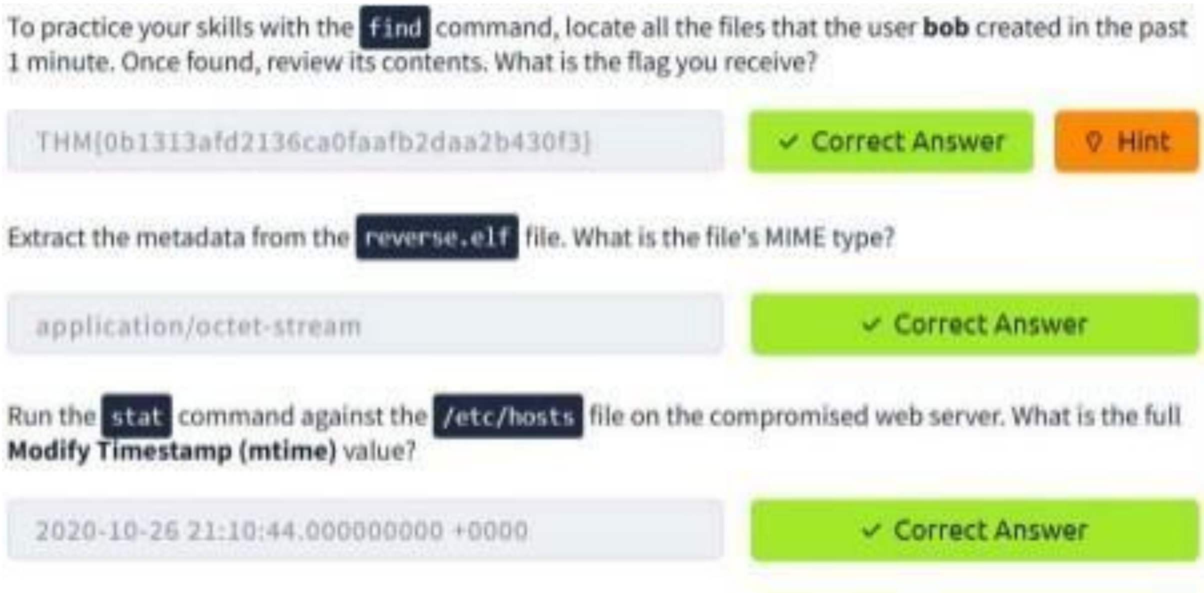
TASK 2 : INVESTIGATION SETUP



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}

TASK 3 : FILES,PERMISSION AND TIMESTAMPS



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}

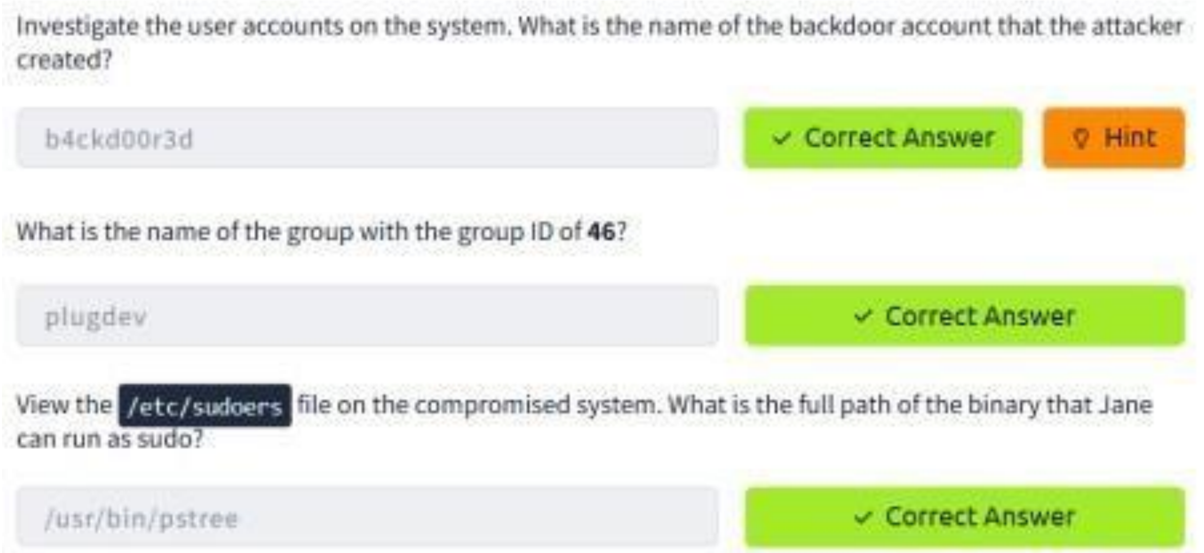
Extract the metadata from the `reverse.elf` file. What is the file's MIME type?

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

TASK 4 : USERS AND GROUPS



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

b4ckd00r3d

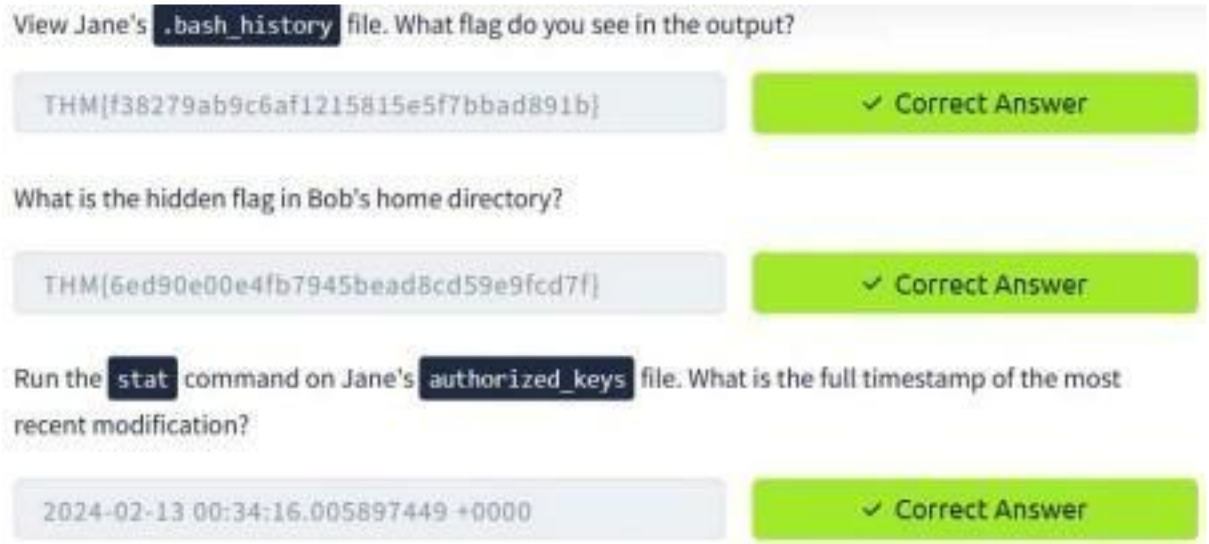
What is the name of the group with the group ID of **46**?

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

TASK 5 : USER DIRECTORIES AND FILES



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

THM{f38279ab9c6af1215815e5f7bbad891b}

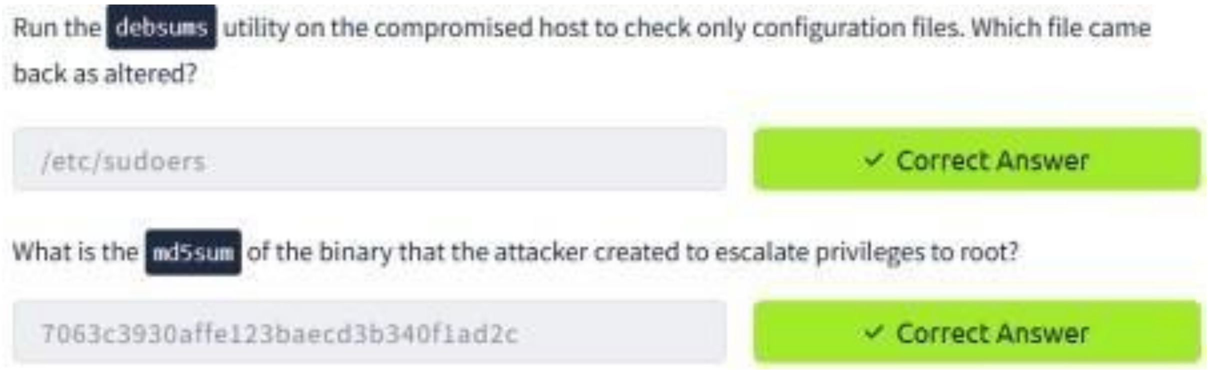
What is the hidden flag in Bob's home directory?

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

TASK 6 : BINARIES AND EXECUTABLES



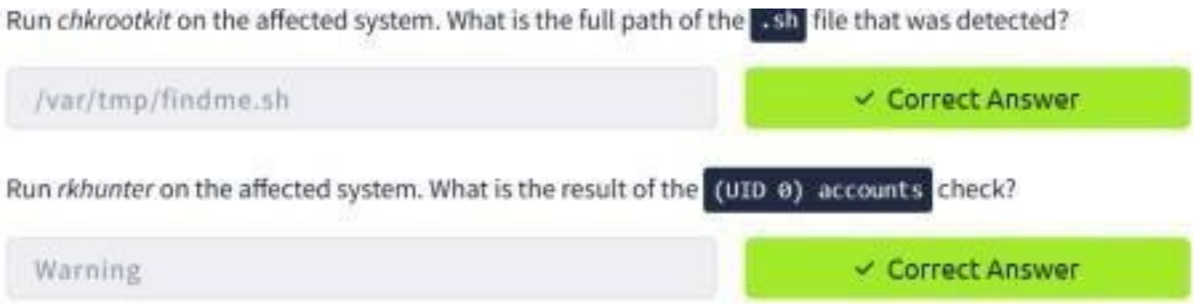
Run the `debsums` utility on the compromised host to check only configuration files. Which file came back as altered?

/etc/sudoers

What is the `md5sum` of the binary that the attacker created to escalate privileges to root?

7063c3930affe123baecd3b340f1ad2c

TASK 7 : ROOTKITS



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

CONCLUSION :

Rootkit detection and removal using rkhunter tool is successfully performed.