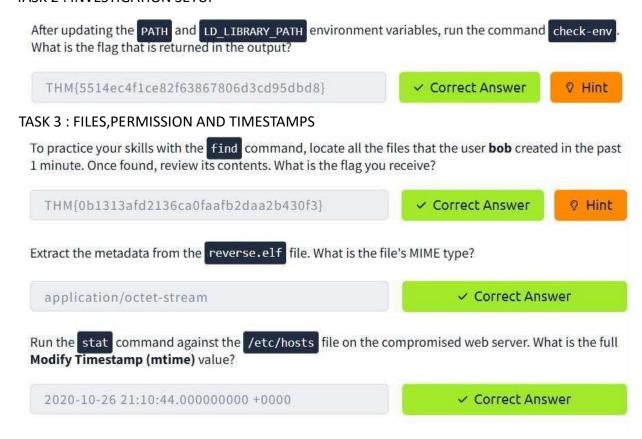
## **USING RKHUNTER TOOL**

## AIM:

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

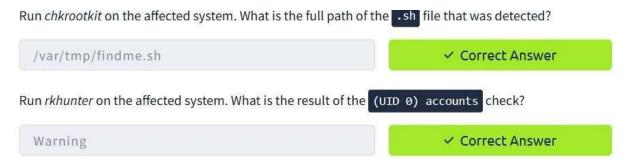
## **TASK 2: INVESTIGATION SETUP**



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 Correct Answer O Hint What is the name of the group with the group ID of 46? ✓ Correct Answer plugdev View the /etc/sudoers file on the compromised system. What is the full path of the binary that Jane can run as sudo? ✓ Correct Answer /usr/bin/pstree TASK 5: USER DIRECTORIES AND FILES View Jane's .bash history file. What flag do you see in the output? ✓ Correct Answer THM[f38279ab9c6af1215815e5f7bbad891b] What is the hidden flag in Bob's home directory? THM[6ed90e00e4fb7945bead8cd59e9fcd7f] ✓ Correct Answer 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 ✓ Correct Answer 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 ✓ Correct Answer What is the md5sum of the binary that the attacker created to escalate privileges to root? ✓ Correct Answer 7063c3930affe123baecd3b340f1ad2c

TASK 7: ROOTKITS



## CONCLUSION:

Rootkit detection and removal using rkhunter tool is successfully performed.