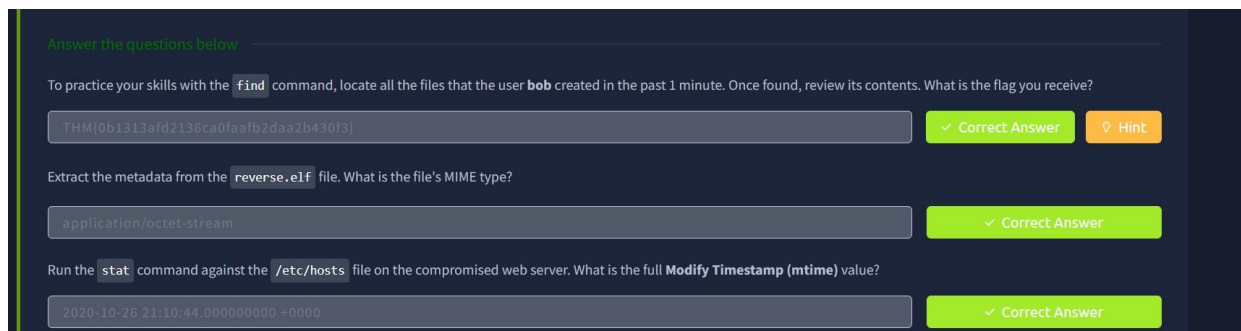
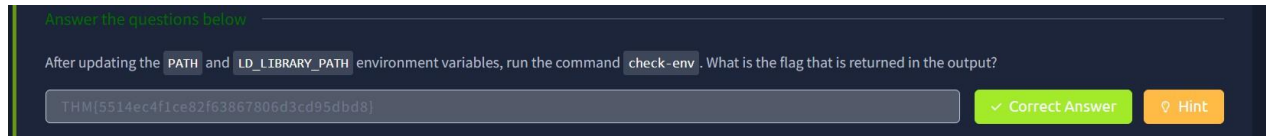


## EXERCISE 8

## Perform rootkit detection and removal using rkhunter tool

## AIM:

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



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?

`7063c3930affe123baecd3b340f1ad2c` ✓ Correct Answer

Room completed (100%)

- Task 1 ✓ Introduction
- Task 2 ✓ Investigation Setup
- Task 3 ✓ Files, Permissions, and Timestamps
- Task 4 ✓ Users and Groups
- Task 5 ✓ User Directories and Files
- Task 6 ✓ Binaries and Executables
- Task 7 ✓ Rootkits
- Task 8 ✓ Conclusion

## RESULT:

Identified malicious files, unauthorized modifications, and suspicious activities in the file system logs.