EX NO : 8 PERFORM ROOTKIT DETECTION AND REMOVAL ROLL NO : 231901027

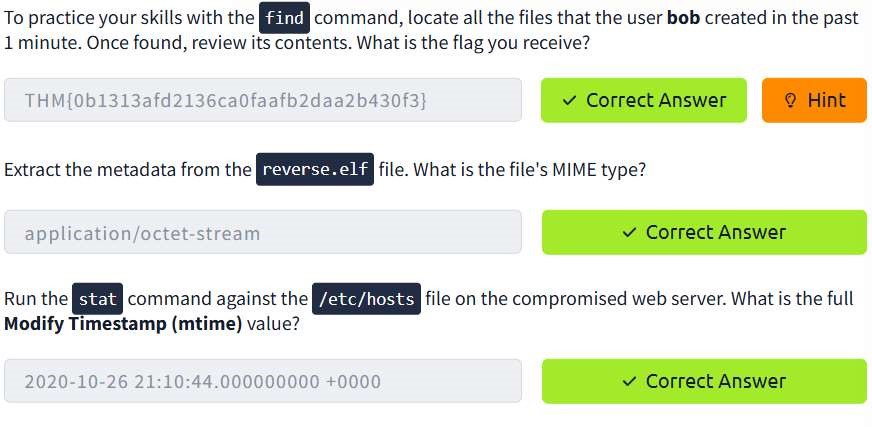
DATE : 14.04.2025 USING RKHUNTER TOOL

AIM:

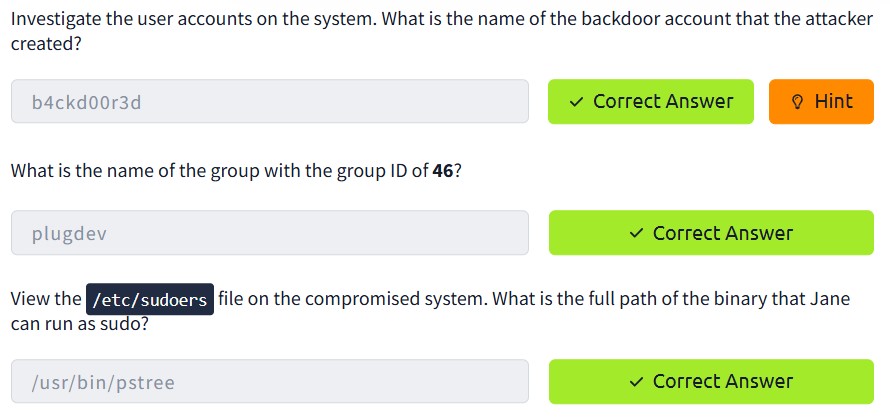
Perform real-time file system analysis on a Linux system to identify an attacker's artefacts. TASK 2 : INVESTIGATION SETUP



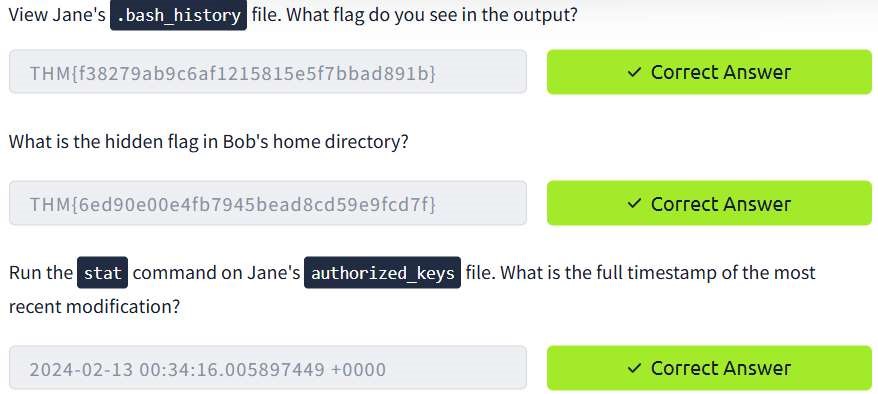
TASK 3 : FILES,PERMISSION AND TIMESTAMPS



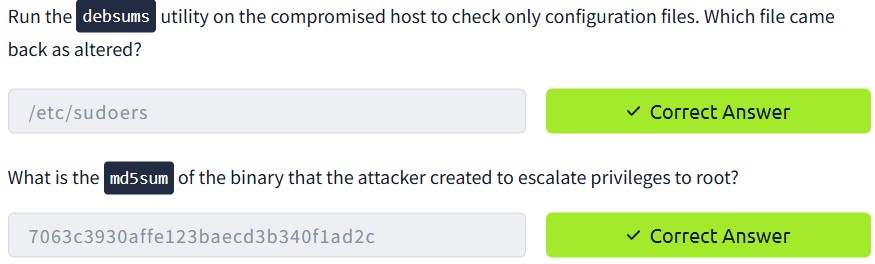
TASK 4 : USERS AND GROUPS



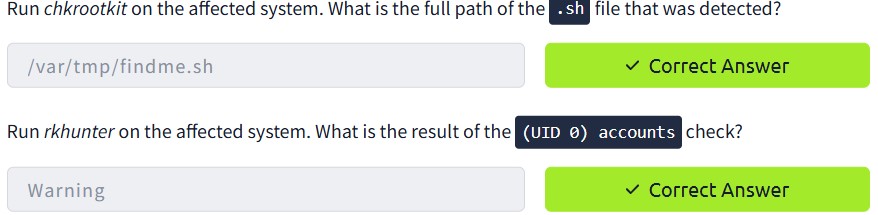
TASK 5 : USER DIRECTORIES AND FILES



TASK 6 : BINARIES AND EXECUTABLES



TASK 7 : ROOTKITS



CONCLUSION :

Rootkit detection and removal using rkhunter tool is successfully performed.