

## 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.

Learn > Linux File System Analysis

## Linux File System Analysis

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

📖 Easy ⌚ 60 min

🔗 Share your achievement

🏠 Start AttackBox ▼

📖 Help ▼

🔖 Save Room

👍 571 🗨

⚙️ Options ▼

Room completed ( 100% )

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]

✓ Correct Answer

🔑 Hint

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]

✓ Correct Answer

🔑 Hint

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

application/octet-stream

✓ Correct Answer

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

✓ Correct Answer

Answer the questions below

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

THM[f38279ab9c6af1215015e5f7bbad891b]

✓ Correct Answer

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

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.