

EX.No:08      Perform rootkit detection and removal using rkhunter tool      DATE:14/04/2025

NAME: M.A.MADHESH

ROLL.NO:231901029

AIM:

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

The screenshot shows the TryHackMe interface for the 'Linux File System Analysis' room. The top navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other'. The room title 'Linux File System Analysis' is prominently displayed, along with a description: 'Perform real-time file system analysis on a Linux system to identify an attacker's artefacts.' The difficulty is marked as 'Easy' and the estimated time is '60 min'. A progress bar at the top indicates 'Room completed (100%)'. Below this, a list of tasks is shown, all marked as completed with green checkmarks:

- 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

## Task 02: Investigation Setup

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

## Task 03: Files, Permissions, and Timestamps

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

## Task 04: User and Groups

Answer the questions below

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

b4ckd00r3d

✓ Correct Answer

🔍 Hint

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

plugdev

✓ Correct Answer

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

✓ Correct Answer

## Task 05: User Directories and Files

Answer the questions below

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

THM{f38279ab9c6af1215815e5f7bbad891b}

✓ 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

## Task 06: Binaries and Executables

Answer the questions below

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

## Task 07: RootKits

Answer the questions below

Run `chkrootkit` on the affected system. What is the full path of the `.sh` file that was detected?

/var/tmp/findme.sh

✓ Correct Answer

Run `rkhunter` on the affected system. What is the result of the `(UID 0) accounts` check?

Warning

✓ Correct Answer

