EX NO: 8 PERFORM ROOTKIT DETECTION AND REMOVAL ROLL NO: 231901058

DATE: 14.04.2025 USING RKHUNTER TOOL NAME: UDAYA SANKAR C

AIM:

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

TASK 2: INVESTIGATION SETUP

application/octet-stream



TASK 3: FILES, PERMISSION AND TIMESTAMPS

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?

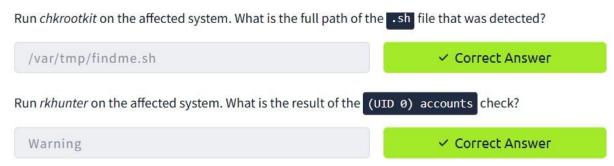
Run the stat command against the /etc/hosts file on the compromised web server. What is the full Modify Timestamp (mtime) value?

✓ Correct Answer

TASK 4: USERS AND GROUPS

Investigate the user accounts on the system. What is the name of the backdoor account that the attacker created? Correct Answer b4ckd00r3d ∀ 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? ✓ Correct Answer THM[6ed90e00e4fb7945bead8cd59e9fcd7f] Run the stat command on Jane's authorized keys file. What is the full timestamp of the most recent modification? ✓ Correct Answer 2024-02-13 00:34:16.005897449 +0000 TASK 6: BINARIES AND EXECUTABLES Run the debsums utility on the compromised host to check only configuration files. Which file came back as altered? ✓ Correct Answer /etc/sudoers 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.