EX NO: 6 DEMONSTRATE LINUX PRIVILEGE ESCALATION NAME: NAVEEN CH

DATE: 2.04.2025 ROLL NO: 231901020

Aim:

To learn the fundamentals of Linux privilege escalation. From enumeration to exploitation, practice over 8 different privilege escalation techniques.

Procedure:

- 1. Task 1 Introduction
- 2. Task 2 What is Privilege Escalation?
- 3. Task 3 Enumeration Techniques
- 4. Task 4 Use Automated Enumeration Tools
- 5. Task 5 Kernel Exploits
- 6. Task 6 Sudo Exploits
- 7. Task 7 SUID Exploits
- 8. **Task 8** Exploiting Capabilities
- 9. **Task 9** Cron Job Exploits
- 10. Task 10 PATH Variable Exploits
- 11. Task 11 NFS Exploits
- 12. Task 12 Capstone Challenge to apply all techniques

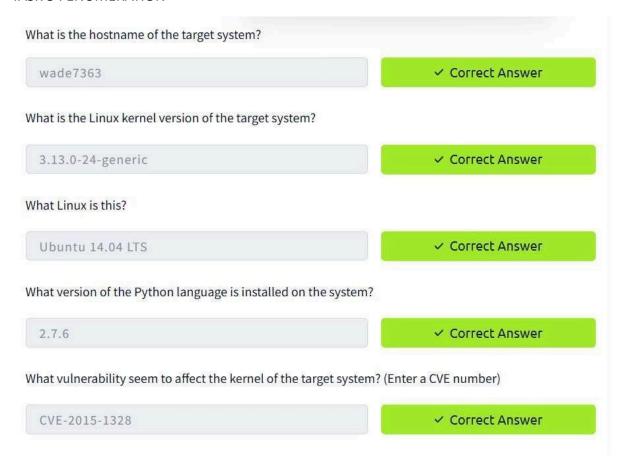
TASK 2: WHAT IS PRIVILEGE ESCALATION?

Read the above.

No answer needed

✓ Correct Answer

TASK 3: ENUMERATION



TASK 4: AUTOMATED ENUMERATION TOOLS

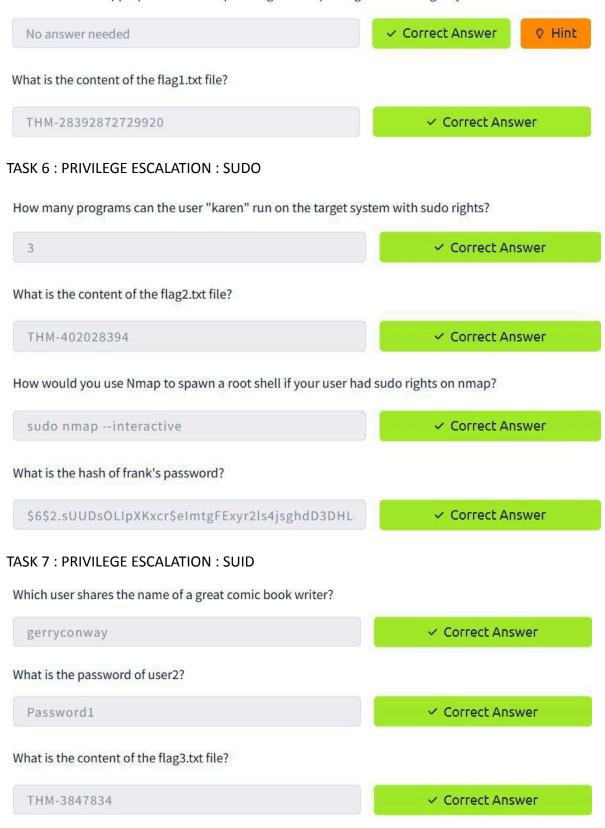
Install and try a few automated enumeration tools on your local Linux distribution

No answer needed

Correct Answer

TASK 5: PRIVILEGE ESCALATION: KERNEL EXPLOITS

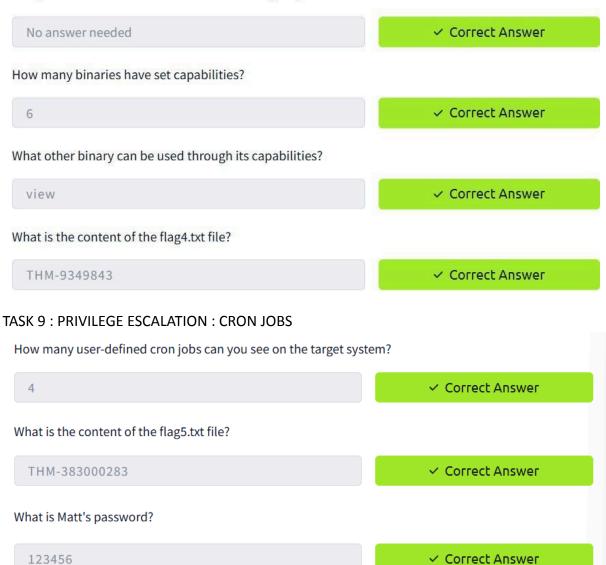
find and use the appropriate kernel exploit to gain root privileges on the target system.



TASK 8: PRIVILEGE ESCALATION: CAPABILITIES

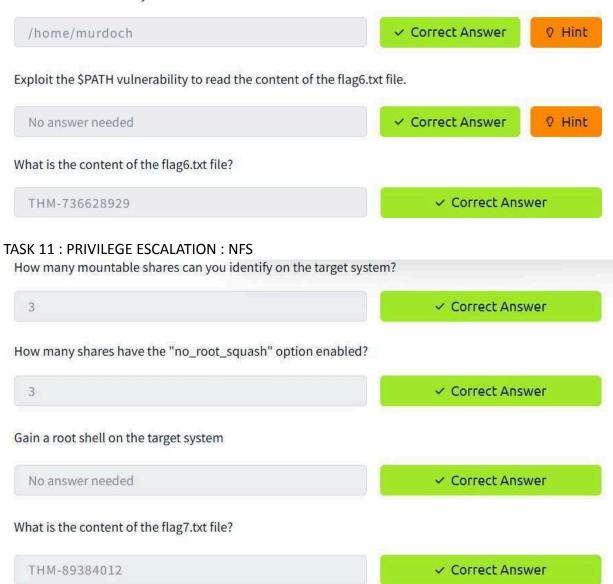
123456

Complete the task described above on the target system



TASK 10: PRIVILEGE ESCALATION: PATH

What is the odd folder you have write access for?



TASK 12 : CAPSTONE CHALLENGE

What is the content of the flag1.txt file?



Result:

Tryhackme platform demonstrate linux privilege escalation task is successfully executed.