EX NO: 6 DEMONSTRATE LINUX PRIVILEGE ESCALATION NAME: vishwanath M DATE:

2.4.2025 ROLL NO: 231901062

AIM:

Learn the fundamentals of Linux privilege escalation. From enumeration to exploitation, get hands-on with over 8 different privilege escalation techniques.

TASK 2: WHAT IS PRIVILEGE ESCALATION?

Read the above. Correct Answer No answer needed **TASK 3: ENUMERATION** What is the hostname of the target system? wade7363 ✓ Correct Answer What is the Linux kernel version of the target system? Correct Answer 3.13.0-24-generic What Linux is this? Correct Answer Ubuntu 14.04 LTS What version of the Python language is installed on the system? 2.7.6 Correct Answer What vulnerability seem to affect the kernel of the target system? (Enter a CVE number) CVE-2015-1328 Correct Answer TASK 4: AUTOMATED ENUMERATION TOOLS Install and try a few automated enumeration tools on your local Linux distribution Correct Answer No answer needed

TASK 5 : PRIVILEGE ESCALATION : KERNEL EXPLOITS find and use the appropriate kernel exploit to gain root privileges on the target system. No answer needed Correct Answer Hint What is the content of the flag1.txt file? THM-28392872729920 TASK 6 : PRIVILEGE ESCALATION : SUDO How many programs can the user "karen" run on the target system with sudo rights?

What is the content of the flag2.txt file?

THM-402028394

Correct Answer

How would you use Nmap to spawn a root shell if your user had sudo rights on nmap?

sudo nmap --interactive

Variety Correct Answer

What is the hash of frank's password?

\$6\$2.sUUDsOLIpXKxcr\$eImtgFExyr2ls4jsghdD3DHLI

Correct Answer

gerryconway

Correct Answer

What is the password of user2?

Password1

Correct Answer

TASK 7: PRIVILEGE ESCALATION: SUID

Which user shares the name of a great comic book writer?

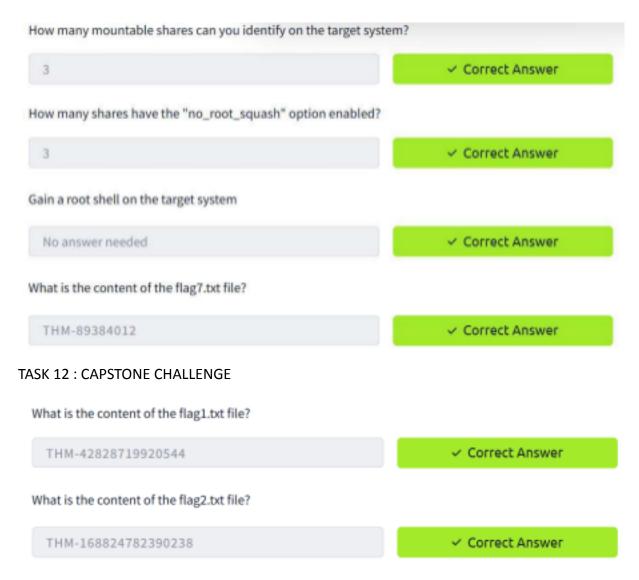
TASK 8: PRIVILEGE ESCALATION: CAPABILITIES

What is the content of the flag3.txt file?

THM-3847834 Correct Answer

Complete the task described above on the target system Correct Answer No answer needed How many binaries have set capabilities? Correct Answer 6 What other binary can be used through its capabilities? Correct Answer view What is the content of the flag4.txt file? THM-9349843 Correct Answer TASK 9: PRIVILEGE ESCALATION: CRON JOBS How many user-defined cron jobs can you see on the target system? Correct Answer What is the content of the flag5.txt file? Correct Answer THM-383000283 What is Matt's password? 123456 Correct Answer TASK 10: PRIVILEGE ESCALATION: PATH What is the odd folder you have write access for? Correct Answer ♥ Hint /home/murdoch Exploit the \$PATH vulnerability to read the content of the flag6.txt file. Correct Answer No answer needed ♥ Hint What is the content of the flag6.txt file? THM-736628929 Correct Answer

TASK 11: PRIVILEGE ESCALATION: NFS



CONCLUSION:

Tryhackme platform demonstrate linux privilege escalation task is successfully executed.