

Ex.no: 6

Roll no: 231901004

DATE: 09.04.2025

DEMONSTRATE LINUX PRIVILEGE ESCALATION

AIM:

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

The screenshot displays the TryHackMe interface for the 'Linux Privilege Escalation' room. The header includes the TryHackMe logo, navigation links (Dashboard, Learn, Compete, Other), and user options (Access Machines, Go Premium, 0). The room title 'Linux Privilege Escalation' is prominently displayed, along with a description: 'Learn the fundamentals of Linux privilege escalation. From enumeration to exploitation, get hands-on with over 8 different privilege escalation techniques.' The difficulty is 'Medium' and the estimated time is '50 min'. Below this, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', and 'Options'. A progress bar indicates 'Room completed (100%)'. The main content area lists eight tasks, each with a green checkmark indicating completion:

- Task 1: Introduction
- Task 2: What is Privilege Escalation?
- Task 3: Enumeration
- Task 4: Automated Enumeration Tools
- Task 5: Privilege Escalation: Kernel Exploits
- Task 6: Privilege Escalation: Sudo
- Task 7: Privilege Escalation: SUID
- Task 8: Privilege Escalation: Capabilities

What is the hostname of the target system?

wade7363

✓ Correct Answer

What is the Linux kernel version of the target system?

3.13.0-24-generic

✓ Correct Answer

What Linux is this?

Ubuntu 14.04 LTS

✓ Correct Answer

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

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

No answer needed

✓ Correct Answer

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

✓ Correct Answer

How many programs can the user "karen" run on the target system with sudo rights?

3

✓ Correct Answer

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

✓ Correct Answer

What is the hash of frank's password?

\$6\$2.sUUDsOLIpXKxcr\$eImtgFExyr2ls4jsghdD3DHL

✓ Correct Answer

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

gerryconway

✓ Correct Answer

What is the password of user2?

Password1

✓ Correct Answer

What is the content of the flag3.txt file?

THM-3847834

✓ Correct Answer

Complete the task described above on the target system

No answer needed

✓ Correct Answer

How many binaries have set capabilities?

6

✓ Correct Answer

What other binary can be used through its capabilities?

view

✓ Correct Answer

What is the content of the flag4.txt file?

THM-9349843

✓ Correct Answer

How many user-defined cron jobs can you see on the target system?

4

✓ Correct Answer

What is the content of the flag5.txt file?

THM-383000283

✓ Correct Answer

What is Matt's password?

123456

✓ Correct Answer

What is the odd folder you have write access for?

/home/murdoch

✓ Correct Answer

💡 Hint

Exploit the \$PATH vulnerability to read the content of the flag6.txt file.

No answer needed

✓ Correct Answer

💡 Hint

What is the content of the flag6.txt file?

THM-736628929

✓ Correct Answer

How many mountable shares can you identify on the target system?

3

✓ Correct Answer

How many shares have the "no_root_squash" option enabled?

3

✓ Correct Answer

Gain a root shell on the target system

No answer needed

✓ Correct Answer

What is the content of the flag7.txt file?

THM-89384012

✓ Correct Answer

What is the content of the flag1.txt file?

THM-42828719920544

✓ Correct Answer

What is the content of the flag2.txt file?

THM-168824782390238

✓ Correct Answer

Result:

Thus, Tryhackme platform demonstrate linux privilege escalation task is successfully executed.