

**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

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

### 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.

No answer needed

✓ Correct Answer

💡 Hint

What is the content of the flag1.txt file?

THM-28392872729920

✓ Correct Answer

## TASK 6 : PRIVILEGE ESCALATION : SUDO

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\$elmtgFExyr2ls4jsghdD3DHL

✓ Correct Answer

## TASK 7 : PRIVILEGE ESCALATION : SUID

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

## TASK 8 : PRIVILEGE ESCALATION : CAPABILITIES

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

## TASK 9 : PRIVILEGE ESCALATION : CRON JOBS

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

## TASK 10 : PRIVILEGE ESCALATION : PATH

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

## TASK 11 : PRIVILEGE ESCALATION : NFS

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

## TASK 12 : CAPSTONE CHALLENGE

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:**

Tryhackme platform demonstrate linux privilege escalation task is successfully executed.