Linux Privilege Escalation

EX.NO-06

DATE: 26-03-2025

AIM:

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

PROCEDURE:

- 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
- Task 9 Privilege Escalation: Cron Jobs
- Task 10 Privilege Escalation: PATH
- Task 11 Privilege Escalation: NFS
- Task 12 Capstone Challenge

Task 1 Introduction :

Answer the questions below

Read the above.

No answer needed   ✓ Correct Answer

Task 2 What is Privilege Escalation? :

Answer the questions below

Read the above.

No answer needed   ✓ Correct Answer

Task 3 Enumeration :

Answer the questions below

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 :

Answer the questions below

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

No answer needed   ✓ Correct Answer

Task 5 Privilege Escalation: Kernel Exploits :

Answer the questions below

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 :

Answer the questions below

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$2.sUUDsOLIpXKxcr$eImtgFExyr2ls4jsghdD3DHLHHP9X50Iv.jNmwo/BJpphrPRJWjelWEz2HH.joV14aDEwW1c3Cahzl | ✓ Correct Answer |

Task 7 Privilege Escalation: SUID :

Answer the questions below

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 :

Answer the questions below

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 :

Answer the questions below

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 :

Answer the questions below

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 :

Answer the questions below

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 :

Answer the questions below

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 the Linux Privilege Escalation is completed using tryhackme platform.