LINUX PRIVILEDGE ESCALATION

EXP.NO: 6 **DATE: 04-03-2025**

AIM:

The primary aim of the Linux Privilege Escalation is to equip learners with the knowledge and hands-on experience necessary to identify and exploit privilege escalation vulnerabilities in Linux systems. This is crucial for understanding how attackers gain elevated access and how to secure systems against such threats.

OBJECTIVES:

1. Understand Privilege Escalation Concepts:

- Learn the difference between vertical and horizontal privilege escalation and their impact on system security.
- Understand the typical attack vectors and misconfigurations that lead to privilege escalation.

2. Enumerate System Information:

- Develop skills to systematically gather information about the system, users, environment variables, services, and installed software to identify potential escalation paths.

3. Identify Common Vulnerabilities and Misconfigurations:

- Recognize common privilege escalation techniques, including:
- Exploiting SUID/SGID binaries.
- Abusing sudo permissions and misconfigured sudoers files.
- Kernel exploits for outdated or vulnerable kernels.
- Exploiting cron jobs and writable scripts.
- Leveraging environmental variables, PATH misconfigurations, and world-writable files.

4. Hands-on Exploitation Techniques:

- Gain practical experience in exploiting these vulnerabilities to escalate privileges on Linux systems in a controlled environment.

5. Utilize Enumeration and Exploitation Tools:

- Learn how to use tools like LinPEAS, Linux Exploit Suggester, GTFOBins, and custom scripts to automate the enumeration and privilege escalation process.

6. Post-Exploitation and Persistence Techniques:

- Understand what attackers can do after gaining root access, including establishing persistence, creating backdoors, and covering tracks.

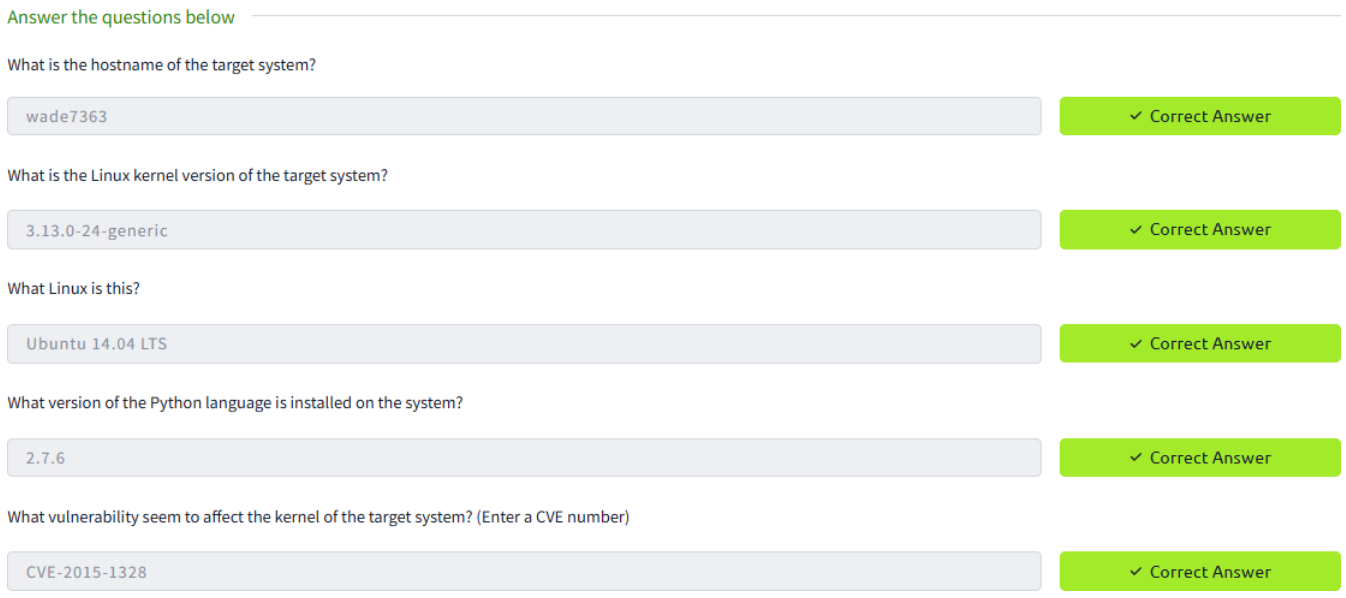
7. Mitigation and Hardening Strategies:

- Learn how to secure Linux systems by identifying and mitigating privilege escalation vulnerabilities.
- Understand best practices for system hardening and monitoring to prevent privilege escalation attacks.

8. Apply Knowledge in Real-World Scenarios:

- Engage in practical exercises and real-world simulations to apply privilege escalation techniques and improve problem-solving skills in ethical hacking and penetration testing contexts.

OUTPUT:



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$2.sUUDsOLIpXKxcr$eImtgFExyr2ls4jsghdD3DHLHHP9X50Iv.jNmwo/BJpphrPRJWjelWEz2HH.joV14aDEwW1c3CahzB1uaqe ✓ 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

RESULT:

After completing this exercise, the technical knowledge and practical skills to identify, exploit, and mitigate privilege escalation vulnerabilities in Linux systems—an essential component of ethical hacking, penetration testing, and system administration is learned.