

EX 6: Linux Privilege Escalation

Aim : To Learn about linux Privilege Escalation.

Tasks:

room completed (100%)

General Linux Commands

As we are in the Linux realm, familiarity with Linux commands, in general, will be very useful. Please spend some time getting comfortable with commands such as `find`, `locate`, `grep`, `cut`, `sort`, etc.

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

Although it looks simple, please remember that a failed kernel exploit can lead to a system crash. Make sure any potential outcome is acceptable within the scope of your penetration testing engagement before attempting a kernel exploit.

Research sources:

1. Based on your findings, you can use Google to search for an existing exploit code.
2. Sources such as <https://www.cvedetails.com/> can also be useful.
3. Another alternative would be to use a script like LES (Linux Exploit Suggester) but remember that these tools can generate false positives (report a kernel vulnerability that does not affect the target system) or false negatives (not report any kernel vulnerabilities although the kernel is vulnerable).

Hints/Notes:

1. Being too specific about the kernel version when searching for exploits on Google, Exploit-db, or searchsploit
2. Be sure you understand how the exploit code works BEFORE you launch it. Some exploit codes can make changes on the operating system that would make them unsecured in further use or make irreversible changes to the system, creating problems later. Of course, these may not be great concerns within a lab or CTF environment, but these are absolute no-nos during a real penetration testing engagement.
3. Some exploits may require further interaction once they are run. Read all comments and instructions provided with the exploit code.
4. You can transfer the exploit code from your machine to the target system using the `SimpleHTTPServer` Python module and `wget` respectively.

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

Room completed (100%)

```
root@debian:/home/user/ldpreload# whoami
root
root@debian:/home/user/ldpreload#
```

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.sUUDsOLlpXKxcr\$elmtgFExyr2ls4jsghdD3DHLHHP9X50lv.jNmwo/BjpphrPRJWjelWEz2HH.joV14aDEwW1c3CahzB1uaqe

✓ Correct Answer

The screenshot shows a web browser window with the URL `tryhackme.com/room/linprivesc`. The browser's address bar and tabs are visible at the top. The main content area displays a terminal window with the following output:

```
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:~$ whoami
user
user@debian:~$ su hacker
Password:
root@debian:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user# whoami
root
root@debian:/home/user#
```

Below the terminal, a message reads: "Now it's your turn to use the skills you were just taught to find a vulnerable binary."

Under the heading "Answer the questions below", there are three quiz questions, each with a text input field and a "Correct Answer" button:

- Question: "Which user shares the name of a great comic book writer?"
Answer: `gerryconway`
- Question: "What is the password of user2?"
Answer: `Password1`
- Question: "What is the content of the flag3.txt file?"
Answer: `THM-3847834`

At the bottom of the page, a list of tasks is shown, each with a green checkmark icon and a dropdown arrow:

- Task 8: Privilege Escalation: Capabilities
- Task 9: Privilege Escalation: Cron Jobs
- Task 10: Privilege Escalation: PATH

Result: Hence the tasks were completed successfully