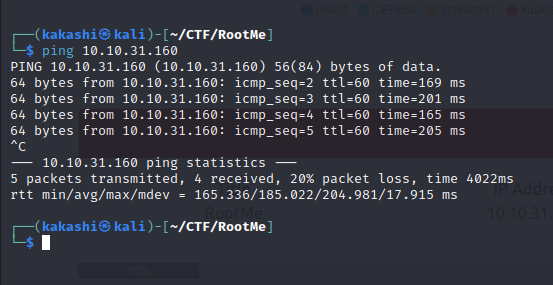
CTF Writeups

Try Hack Me

Rootme

Step 1: Deploy the Machine and check the Connectivity with the target System.



Step 2: Ping command is success, let’s start start information gathering about the target machine by doing **nmap** tool to check for open ports and the version of the service running in that port.

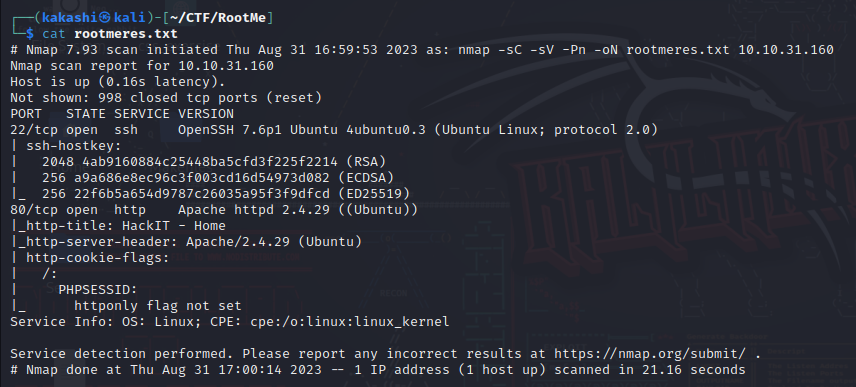
sudo nmap -sC -sV -Pn -oN rootmeres.txt 10.10.31.160

-sC script scan

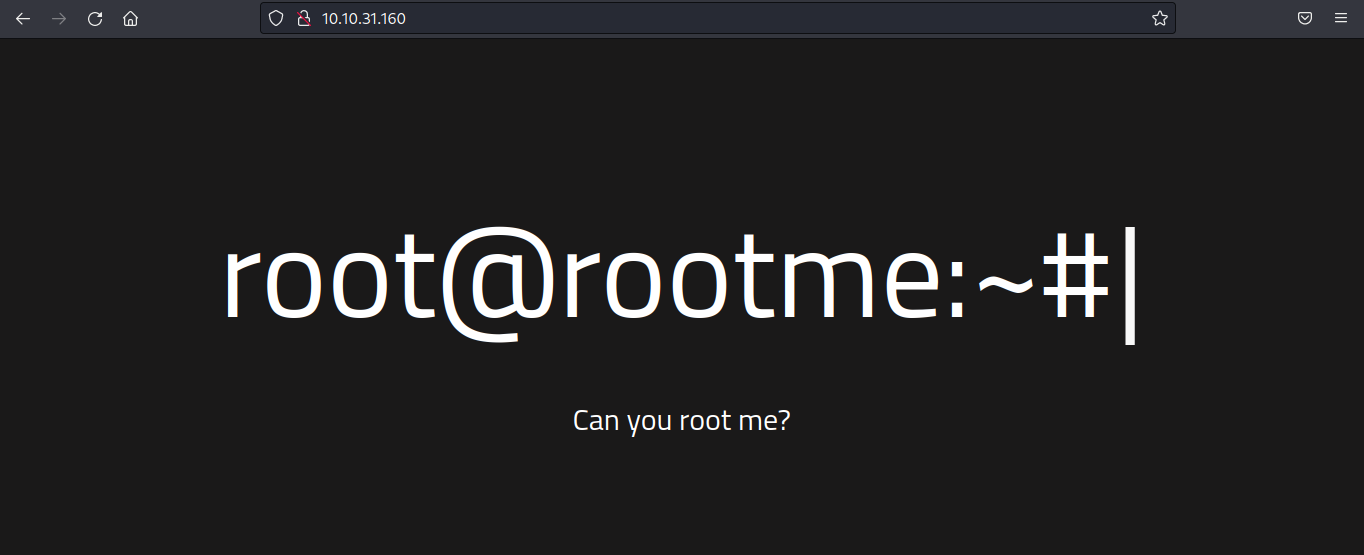
-sV version Scan

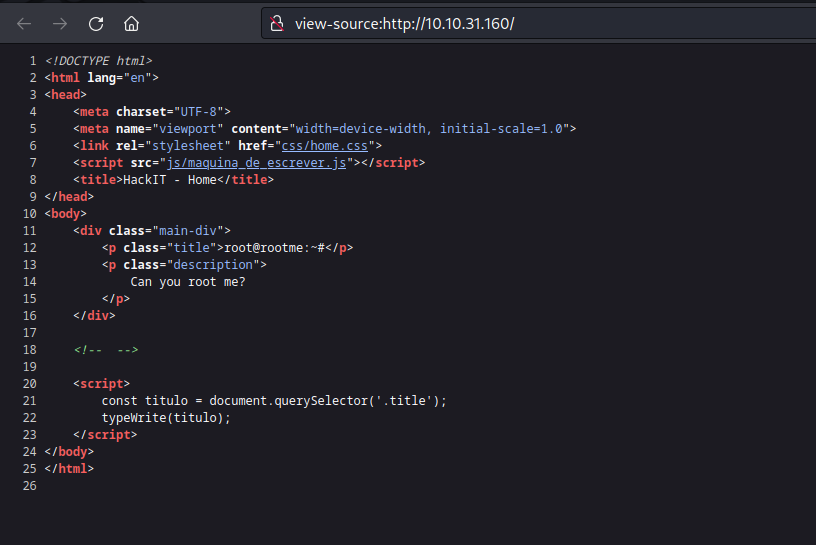
-Pn Dont ping

-oN save the output in the file.



We found that port 22(ssh) and port 80(http) is open. For SSH we need username and password, The only option we have is to check port 80.





After inspecting both website and page source we doen’t find sufficient information.

Step 3: Directory Enumeration

Tool: **gobuster**

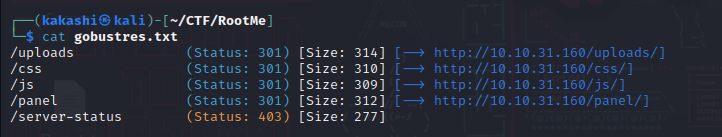
Gobuster dir -u 10.10.31.160 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o gobustres.txt

dir means directory in our case we are doing directory enumeration to find whether there are any hidden directories

-u means url

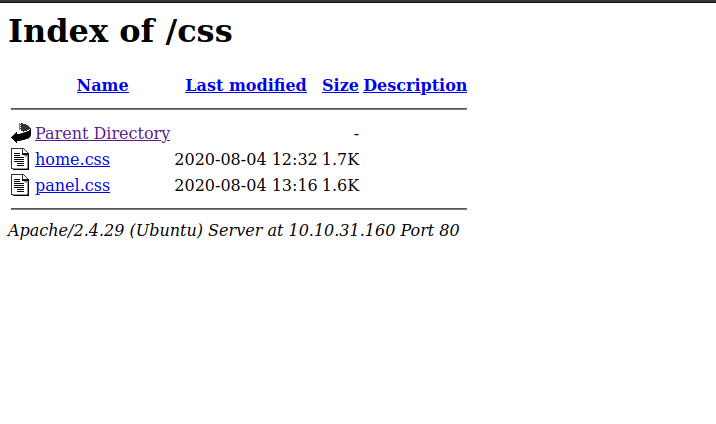
-w means wordlist

-o means output file

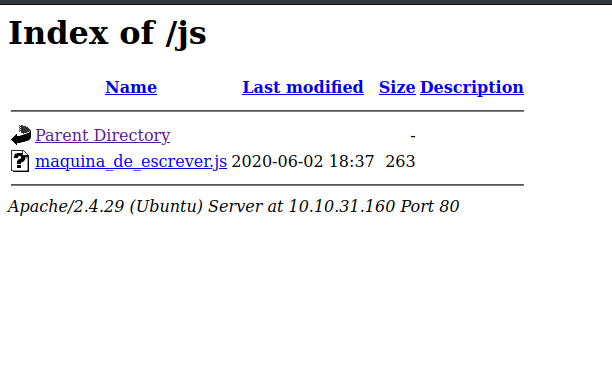


Step 4: Analyzing the directories found by the gobuster tool.

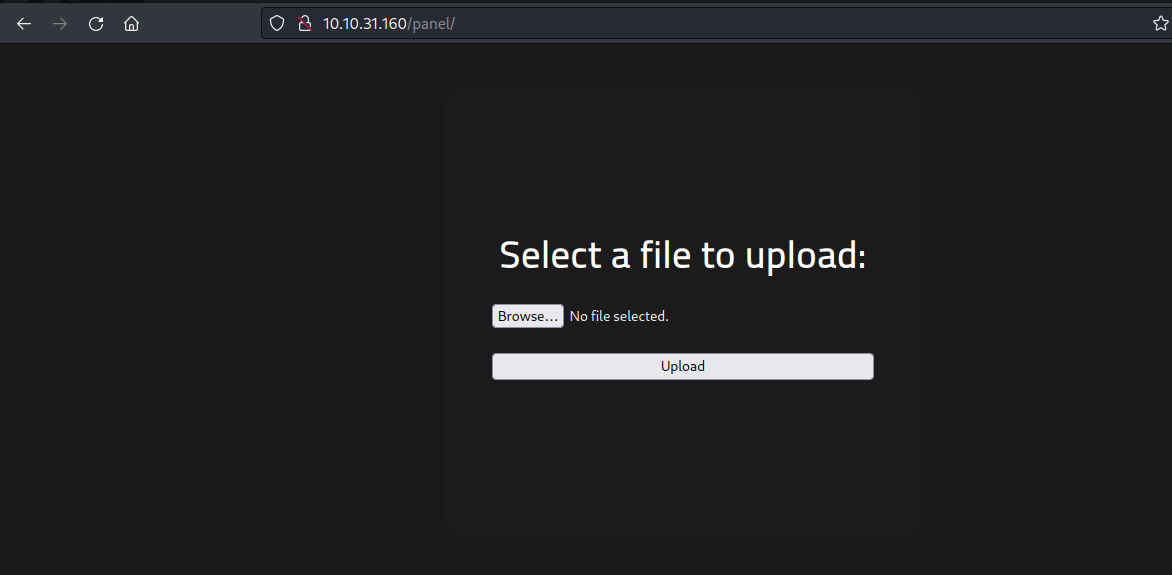
ip/css



ip/js



ip/panel



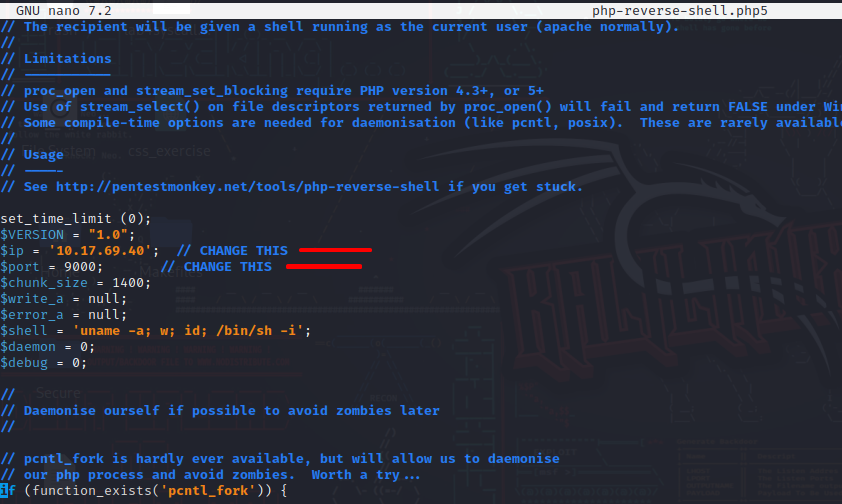
So the Hidden Directory is **/panel/.**

**Step 5:** We found a file upload section where we can upload our payload and get reverse shell access(**file Upload Vulnerability)**.

To Do that first we need to choose the reverse shell file, In this room we use php-reverse-shell developed by pentestmonkey.

Git clone the pentestmonkey php reverse shell to our rootme directory

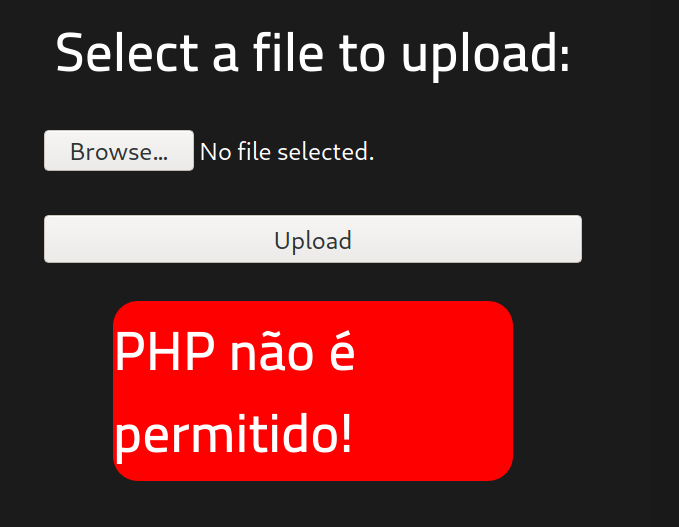
After cloning github open the php-reverse-shell file and update ip address and port for which we are going to listen the reverse shell using netcat



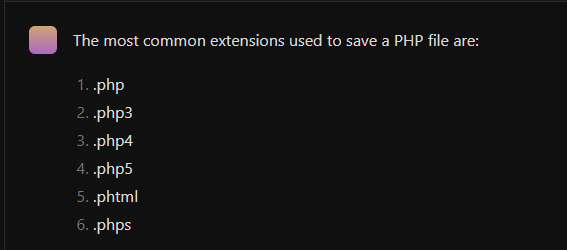
After Updating the ip address and port, save the file and change the mode of the file to executable.

chmod +x php-reverse-shell.php

Upload the payload file in the 10.10.31.160/panel page



This is showing a error like invalid file format. To Bypass this a easy method is to find what are all the available extension to save a php file.



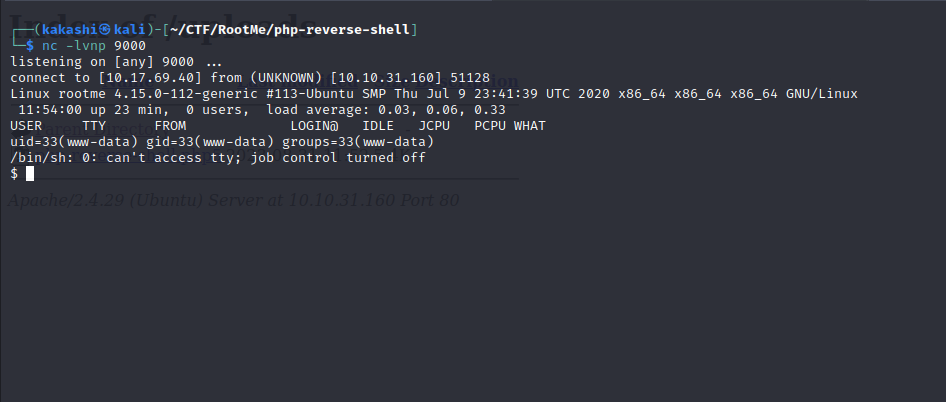
The above are the available php file extensions, luckily we got .php5 extension bypass the file validation and the file has been uploaded. We can view our payload in 10.10.31.160/uploads

**Step 6:** Gaining Shell

To activate the uploaded shell navigate to 10.10.31.160/uploads and double click the uploaded payload before clicking run the netcat command to listen to the incoming traffic.

nc -lvnp 9000

Now Double Click the payload. We got the shell.



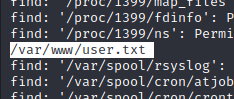
To find the user.txt flag run the following command to find it:

find / -type f -name user.txt

/ denotes entire file system

-type f denotes file

We found the user.txt flag in the /var/www directory

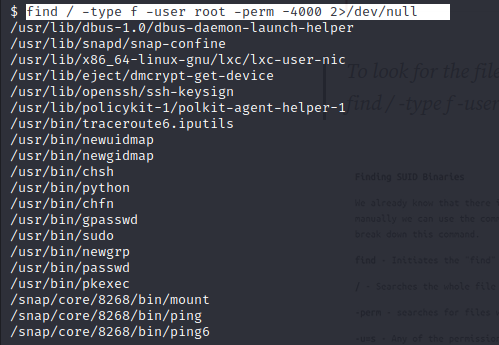


**Step 7:** Privilege Escalation

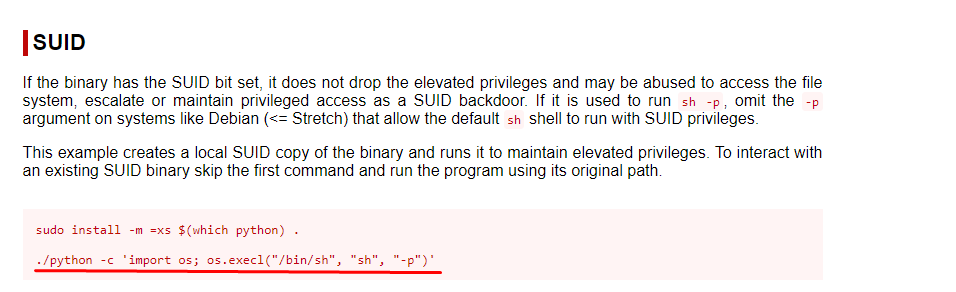
In order to find the root.txt flag we need root level privilege to access it, In this room they guide us with initial step to crack the privilege escalation.

The Below command helps us to identify the program which are running with suid=0 which means it will run the program with the owners name instead of the user who is running that command.

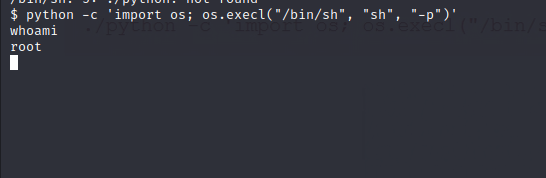
/usr/bin/python is something we can exploit, why i choose python is i run the same command in my kali linux machine, except python every other file matches, my guess they have added python especially for this rootme lab.

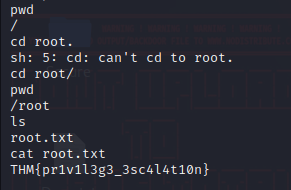


We Found that with python we can gain root privileges we can search for python PE in the GTFOBINS in there search python and navigate to suid column.



Run the Above python command to gain root shell.





Note: Consider linPEAS or EnumLinux.sh for privilege Escalation.