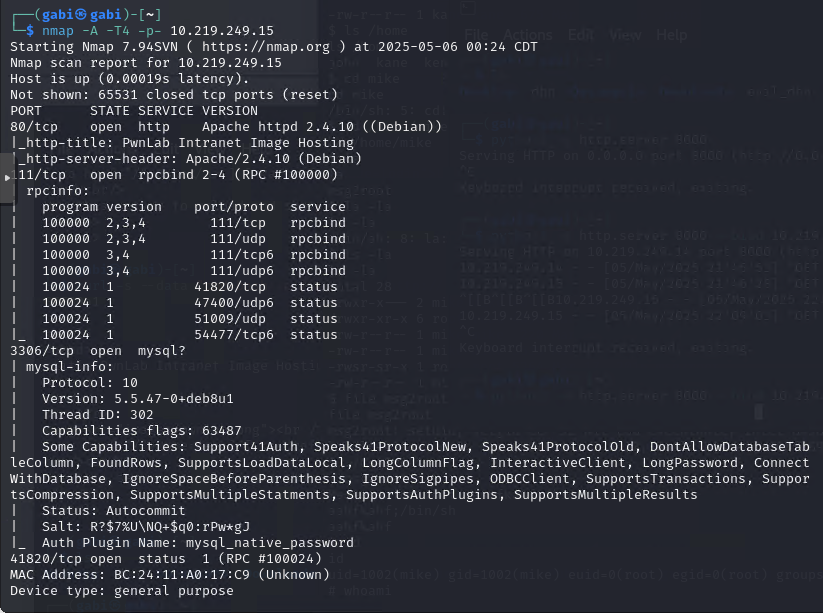
Pwnlab:init - Writeout

**Perform nmap on target**

To start, when setting up the VM it gives you an IP address.

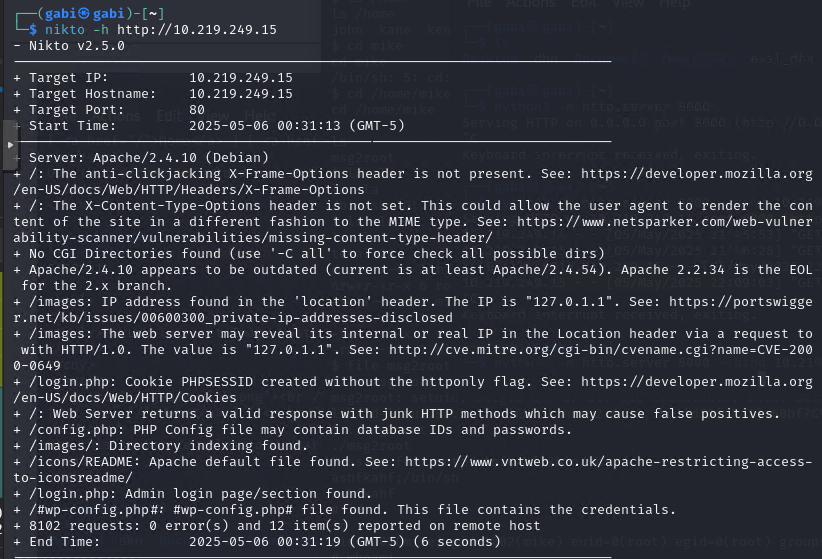
Perform a *nmap* with parameters: *-A* which allows the detection of OS, the version, script scanning, and traceroute; *-T4* indicates the time to send packets from 0-6, the lowest number is the slowest but better because it could evade some firewalls.



Notice: port 80 http is open, port 111 rcpbind is open, port 3306 mysql.

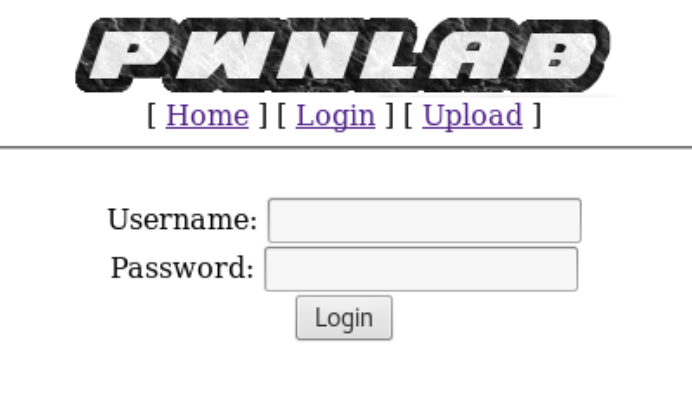
**Perform nikto**

Perform *nikto -h http://IP* to analyze the vulnerabilities of web service. Notice a service based on PHP, a config.php site that contains possible id’s and passwords, a login available for updating pictures.

****

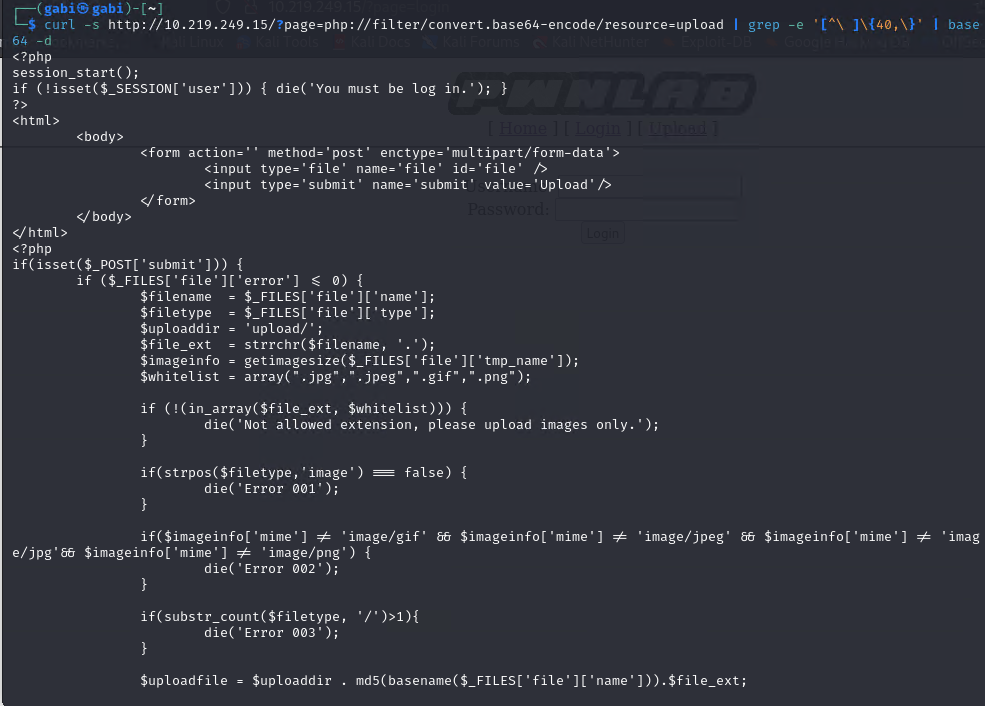
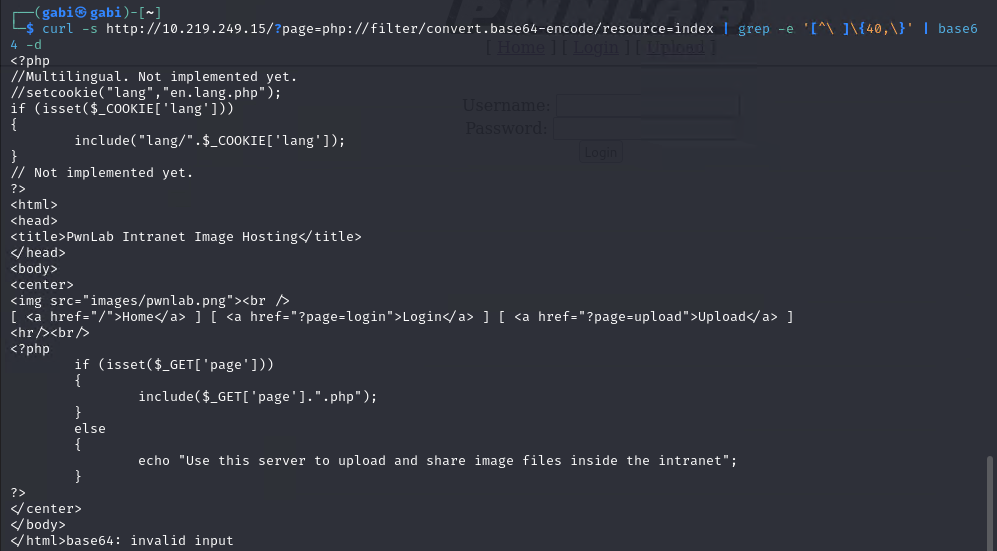
**Go to the web**

Go to the IP address of the target. The address would be something like *http://10.219.249.15/?page=login.*

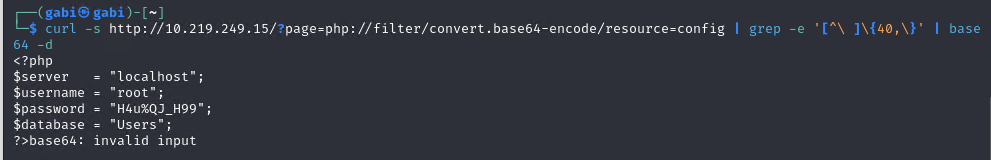


**PHP Filter**

By looking at the address and analyzing the *nikto*, one can assume that the website is vulnerable to local file inclusion (LFI). Perform an analysis of the site using php://filter with *source=index, upload, login, config.* Previously I ran the command without decoding and it gave me base64 encoding, on the following I added the base64 -d to decode the encoded text.



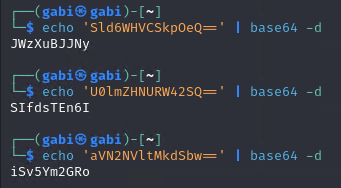
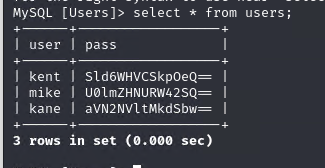
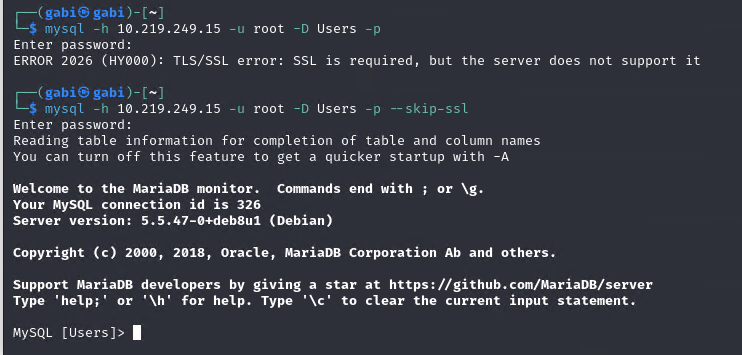




*Resource=config* gives credentials to mysql database with users.

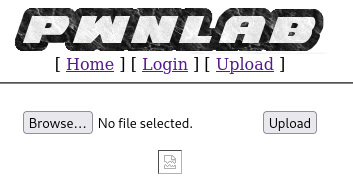
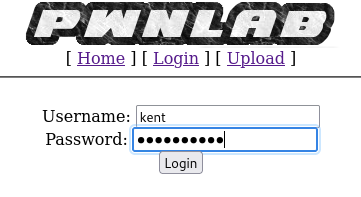
**Connect to mysql**

Proceed to connect to the database using the credentials obtained from config. I had trouble with SSL so I decided to ignore it. After accessing mysql, send a query to select all users and decode the given passwords.

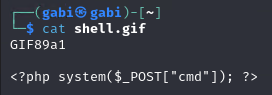
****

**Login with credentials**

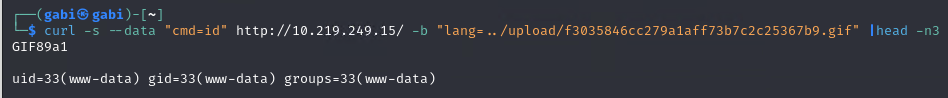
Login to the web with one of the users found in the database, I selected kent. After login in, we try uploading a file but it only allows pictures, gif, etc.



I created a shell gif that contains a valid GIF header and a line of code (payload) that executes any command via POST parameter “cmd”.

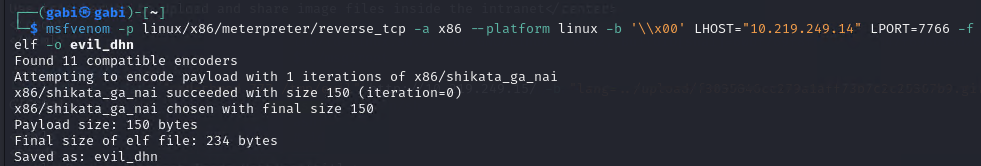


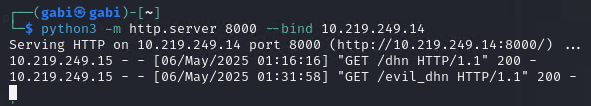
Select the path of the gif on the website and trigger the payload in upload shell.gid by using the “lang” cookie flag in the index.php.



**Create Meterpreter and start server**

Create a *meterpreter* and start server, as well as starting a server for the attacker’s machine (your machine). We created the *meterpreter* with *msfvenom,* setting payload, host to the local machines, and port number. This will write out to a file called evil\_dhn.





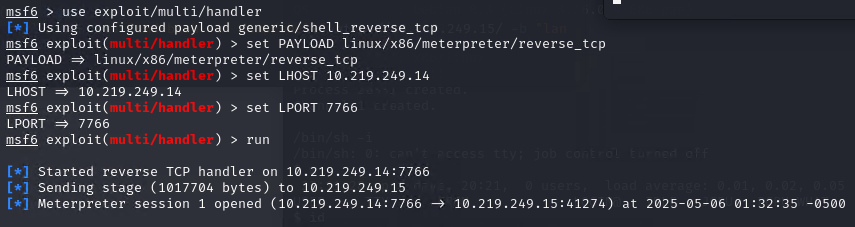
**Use webshell to download and execute meterpreter**

Send evil\_dhn file



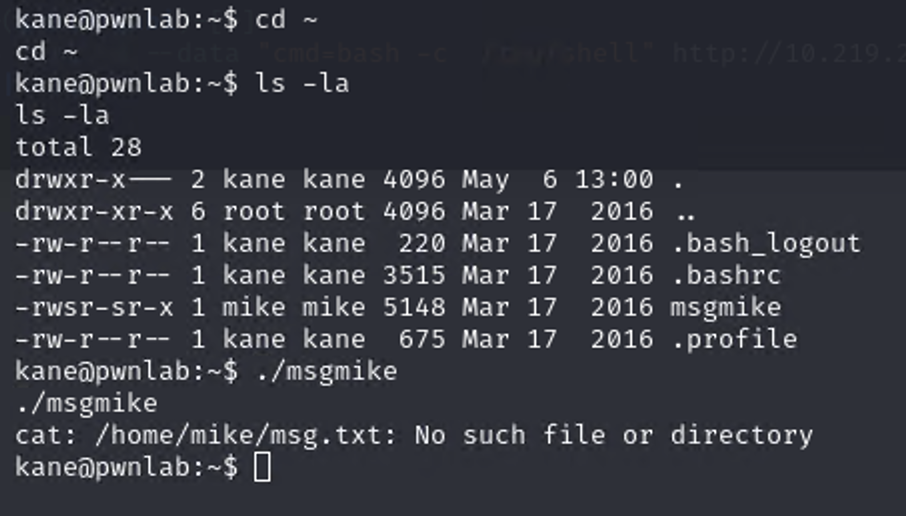
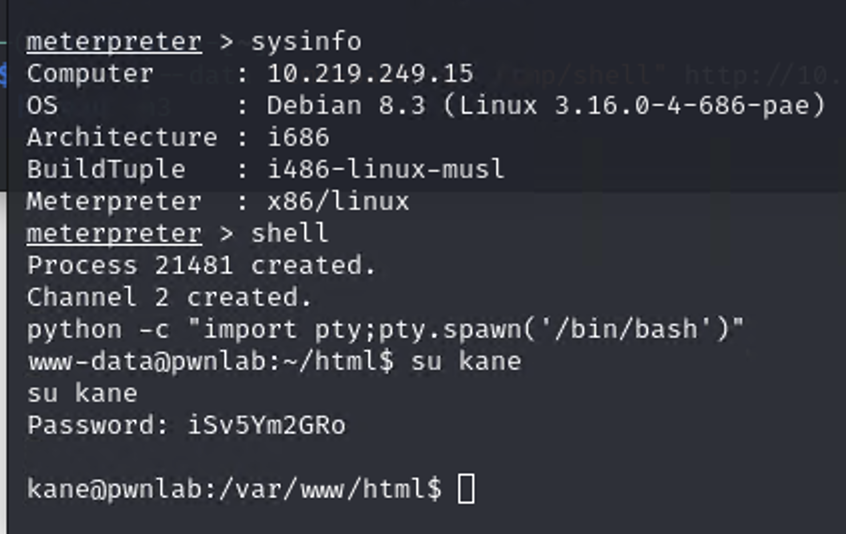
**Gather information**

Start *metasploid* and use the local host and port as set up previously in the msfvenom and you will obtain the reverse shell.



Gather information inside the shell. First look at the system information and you’ll realize you are inside the pwnlab (10.219.249.15). Then log in with one of the previous users and passwords, I used Kane.

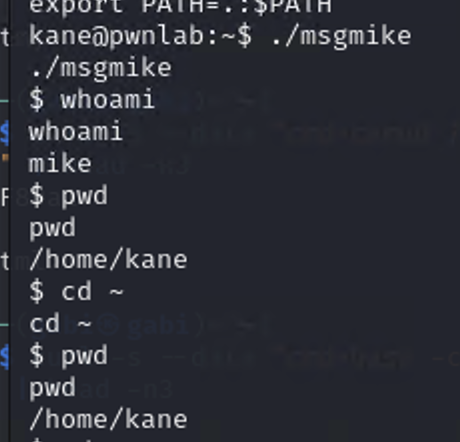
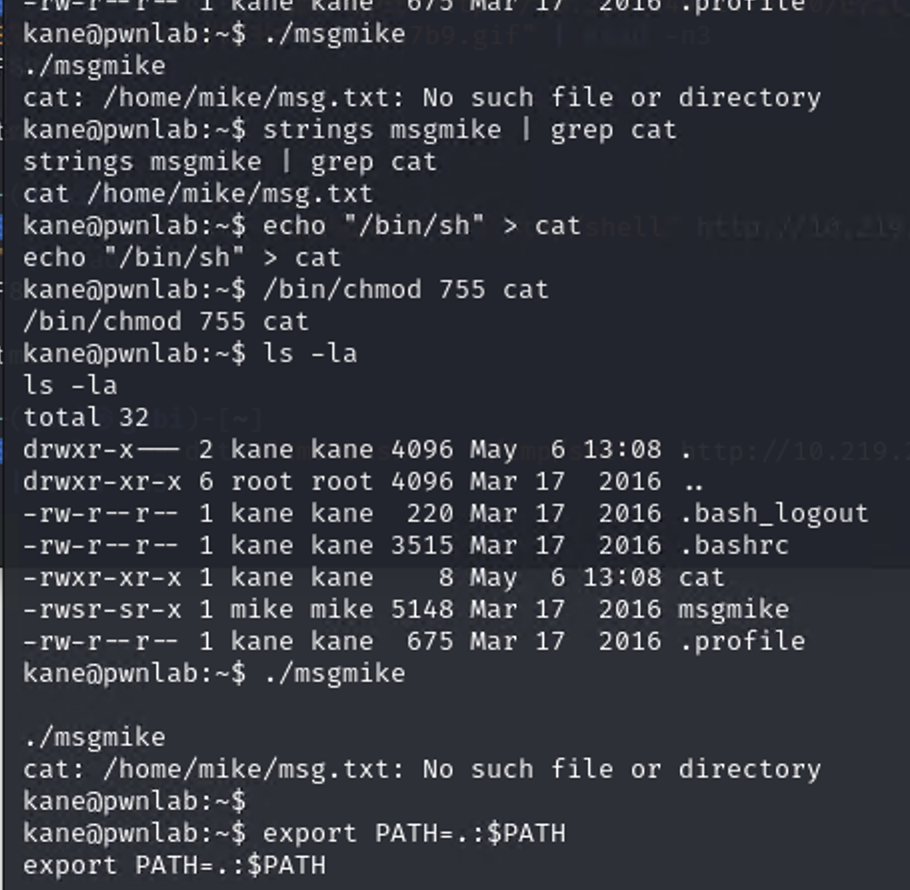
Some of the following steps are pretty straightforward like looking at where you're at, listing elements, navigating through paths, etc.



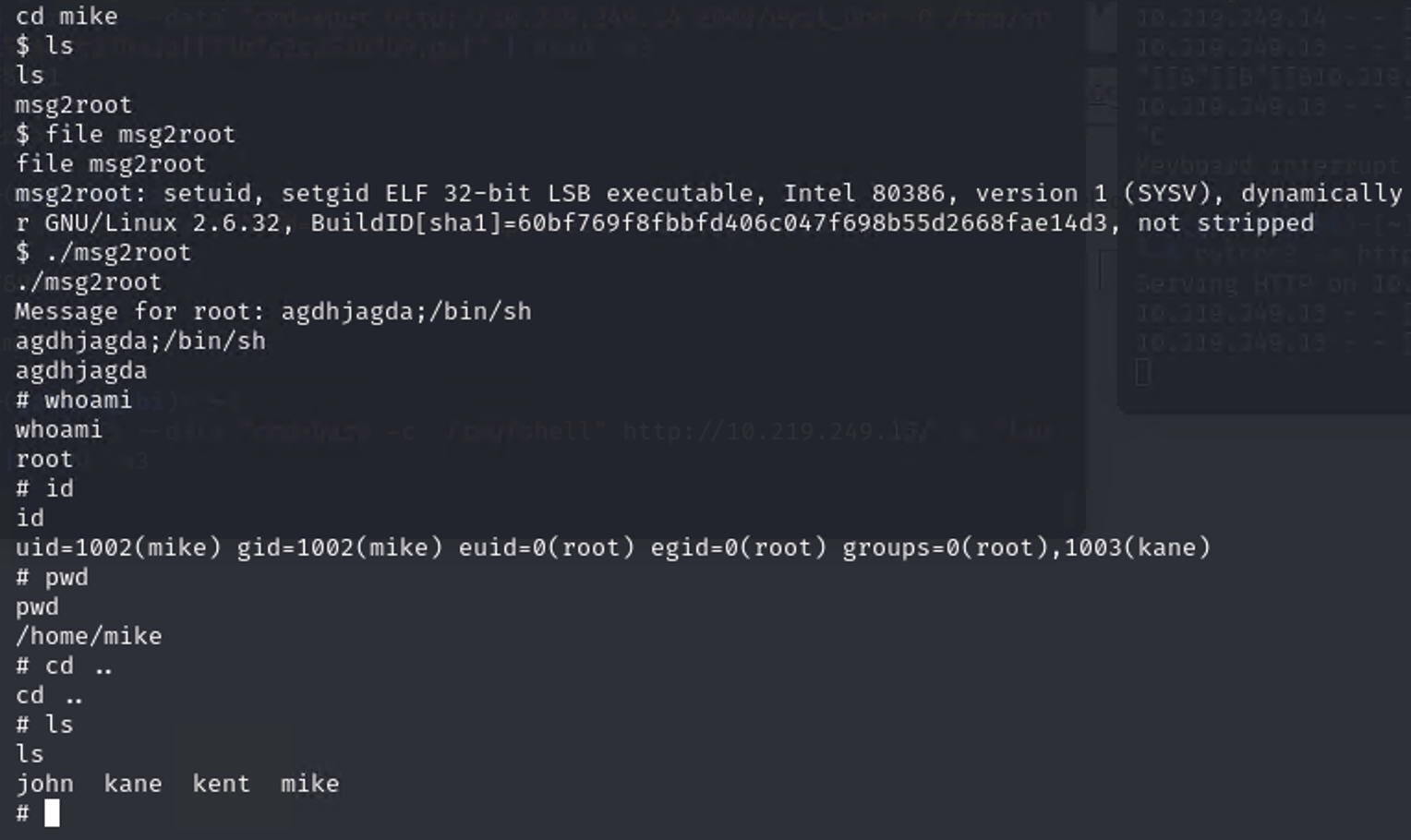
Notice that there is a *msgmike* file with SUID, but the moment we execute it we get an error message with an unclear path, insinuating that the path might be incomplete. When trying to execute this file, it shows that it is trying to *cat* a wrong path.

Then we overwrite a *cat* fale with ‘*/bin/sh*’ inside to use it for an attack and we change the permission to execute the *cat* file. Then we export PATH to our current directory, to let us run the *cat* malicious file.

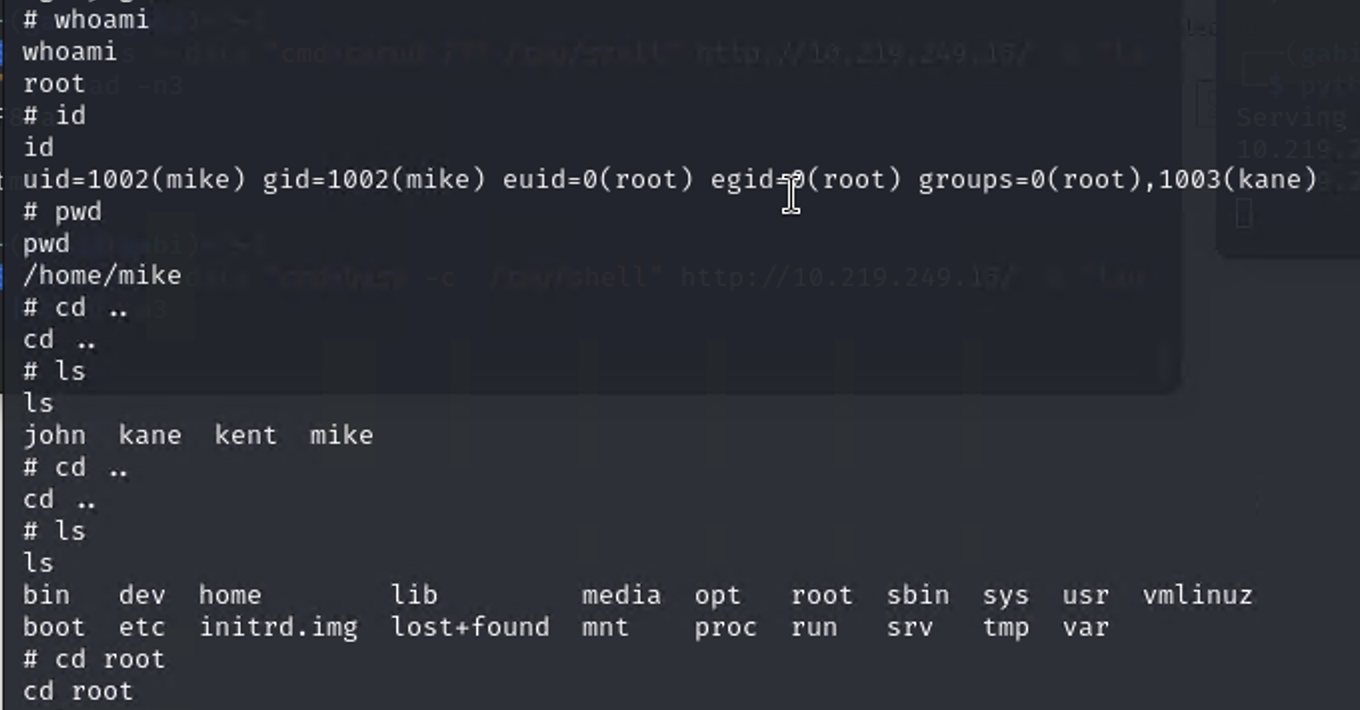
Then we execute the *./msgmike* and we become mike thanks to the SUID.



After navigating to *mike*, we do a file on the file we find in the directory, notice how that is another SUID (setuid) and if we run a string we’ll find “*/bin/echo %s >> /root/messages.txt*”. After writing anything we type ‘*;*’ to interrupt the echo execution and perform a privilege escalation with ‘/bin/sh’.



Got root access!!! Now navigate through the directories until you are in the root directory.



CATCH THE FLAG!!!!

