BY: KARAN JOE MATHEW D

DEPARTMENT: CSBS

REG NO: 210421244026

MAIL: dkaranjoemathew.csbs2021@citchennai.net

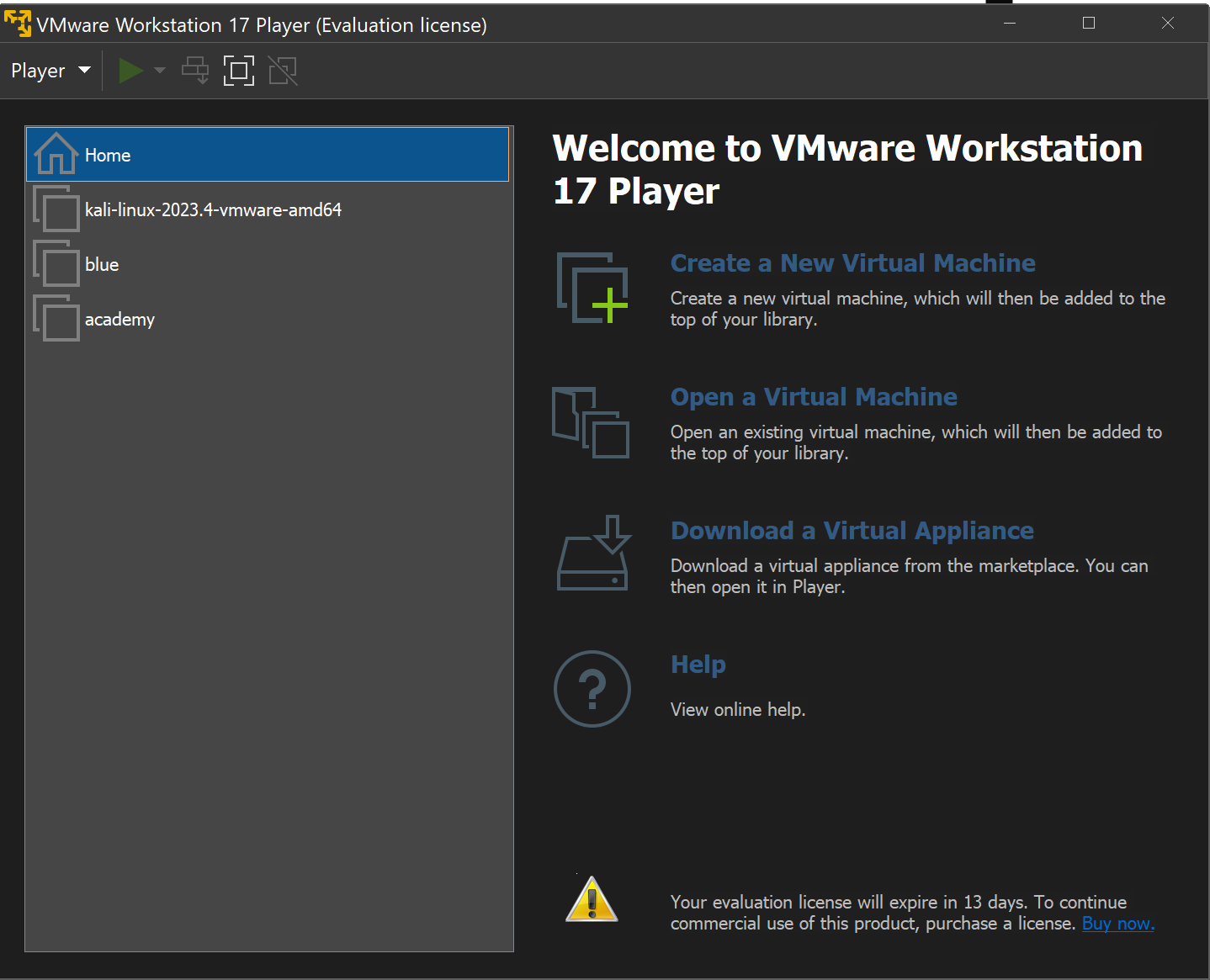
VAPT and SIEM Process

Documentation

**DOCUMENTATION**

Documentation for VAPT (Vulnerability Assessment and Penetration Testing) of a web server and SIEM (Security Information and Event Management) application typically involves detailing the processes, tools, methodologies, and findings related to assessing and testing the security posture of these systems.

**CONFIGURING ACADEMY:**



First, we need to configure the Academy device to make it connect to the local area network and with the internet.

**GETTING IP OF ACADEMY:**

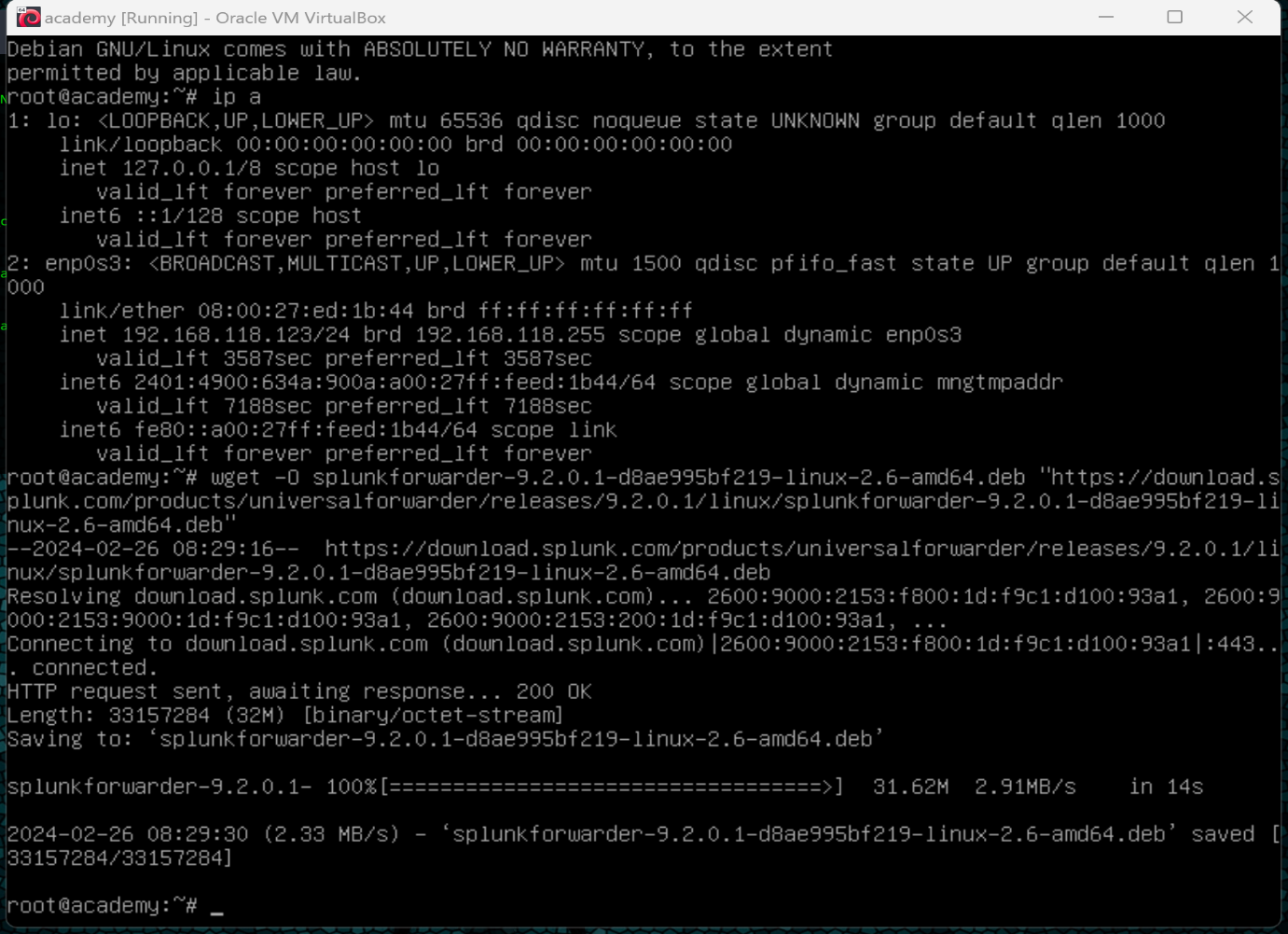
• It initiates the IP assignment from local ‘DHCP’ server using ‘ARP’ protocol.

• After that we get the private IP ADDRESS for our machine. (eg:172.16.3.113)

• Next, we need to install the ‘SPLUNK UNIVERSAL FORWARDER’ in our machine.

• It is done by using the ‘wget’ tool which is available in the Academy machine.

• The below image shows how it is done using the tool.



**Installing and Configuring Splunk Universal Forwarder:**

dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb

- Set up the Splunk Home directory:

export SPLUNK\_HOME="/opt/splunkforwarder"

mkdir $SPLUNK\_HOME

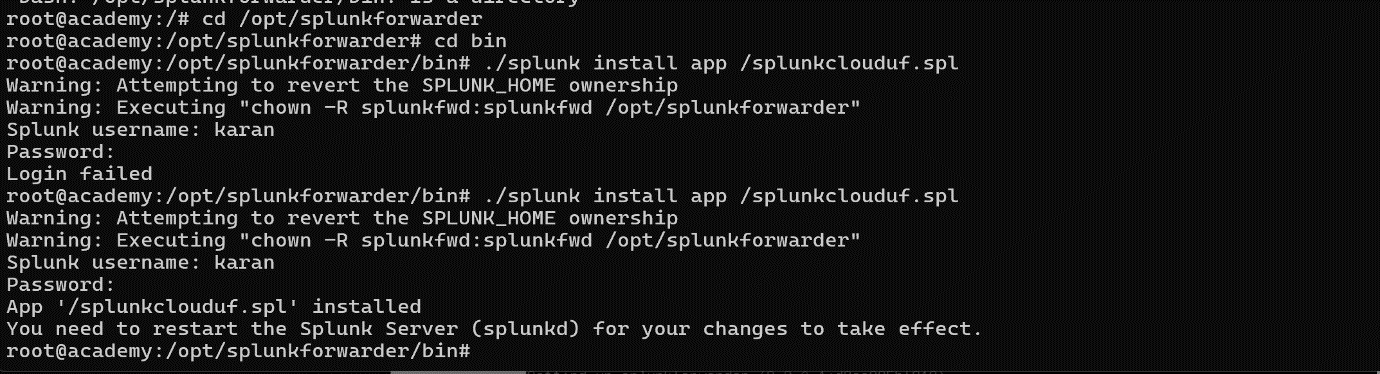
- Install Splunk Forwarder and start it:

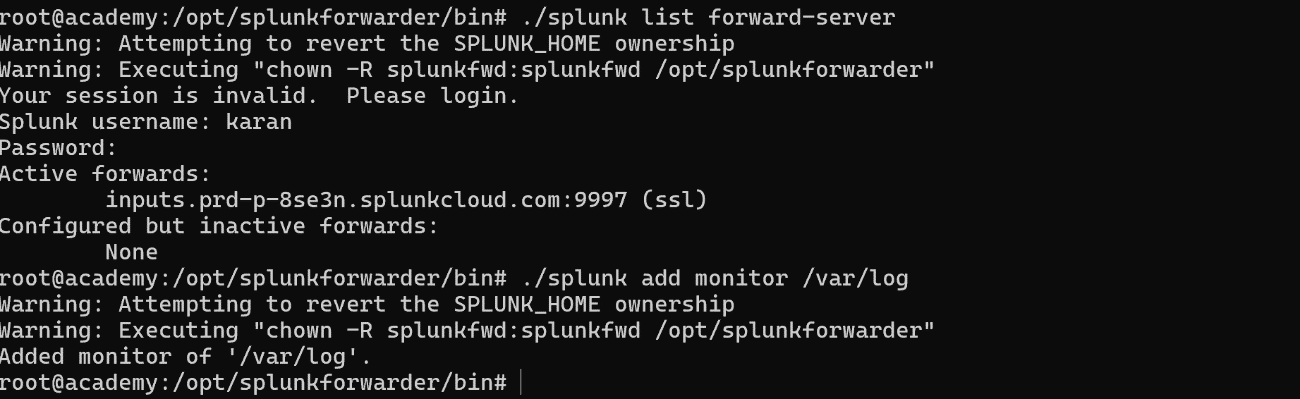
$SPLUNK\_HOME/bin/splunk start --accept-license

Install the credentials file from splunk cloud in the /bin

Use the command ./splunk list forward-server to check the active forwards

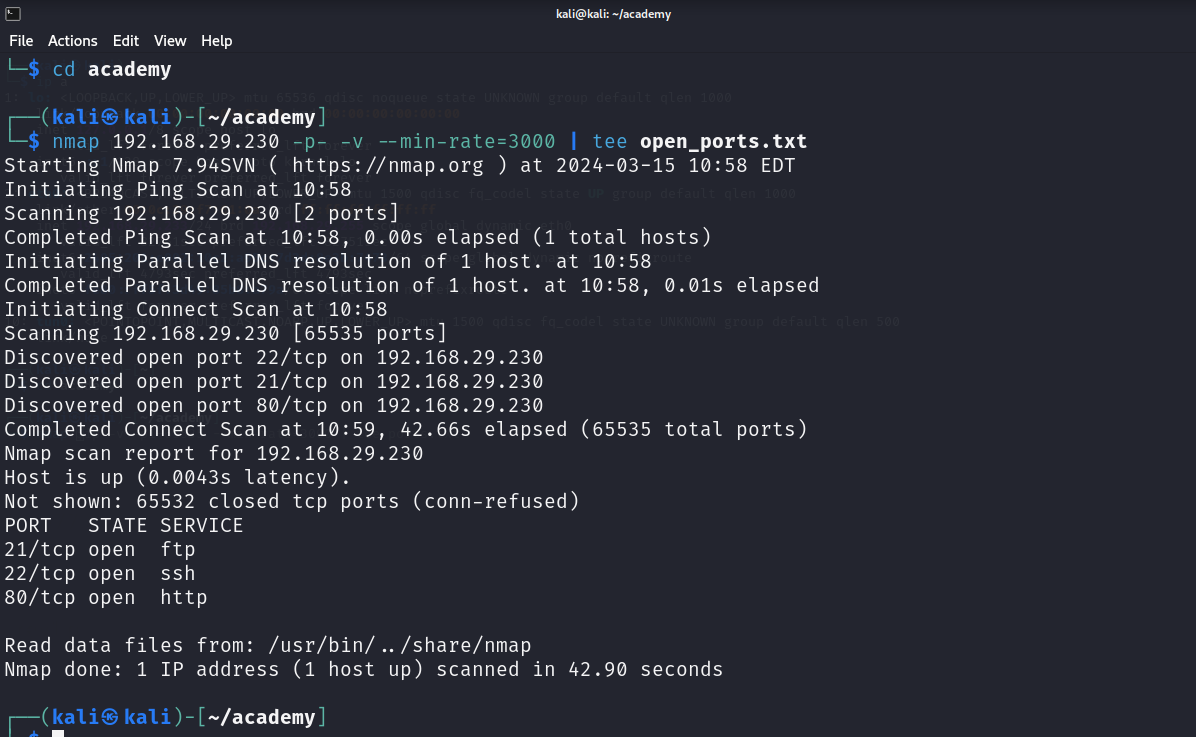
Add the files to monitor by the splunk cloud by using the command ./splunk add monitor /var/log

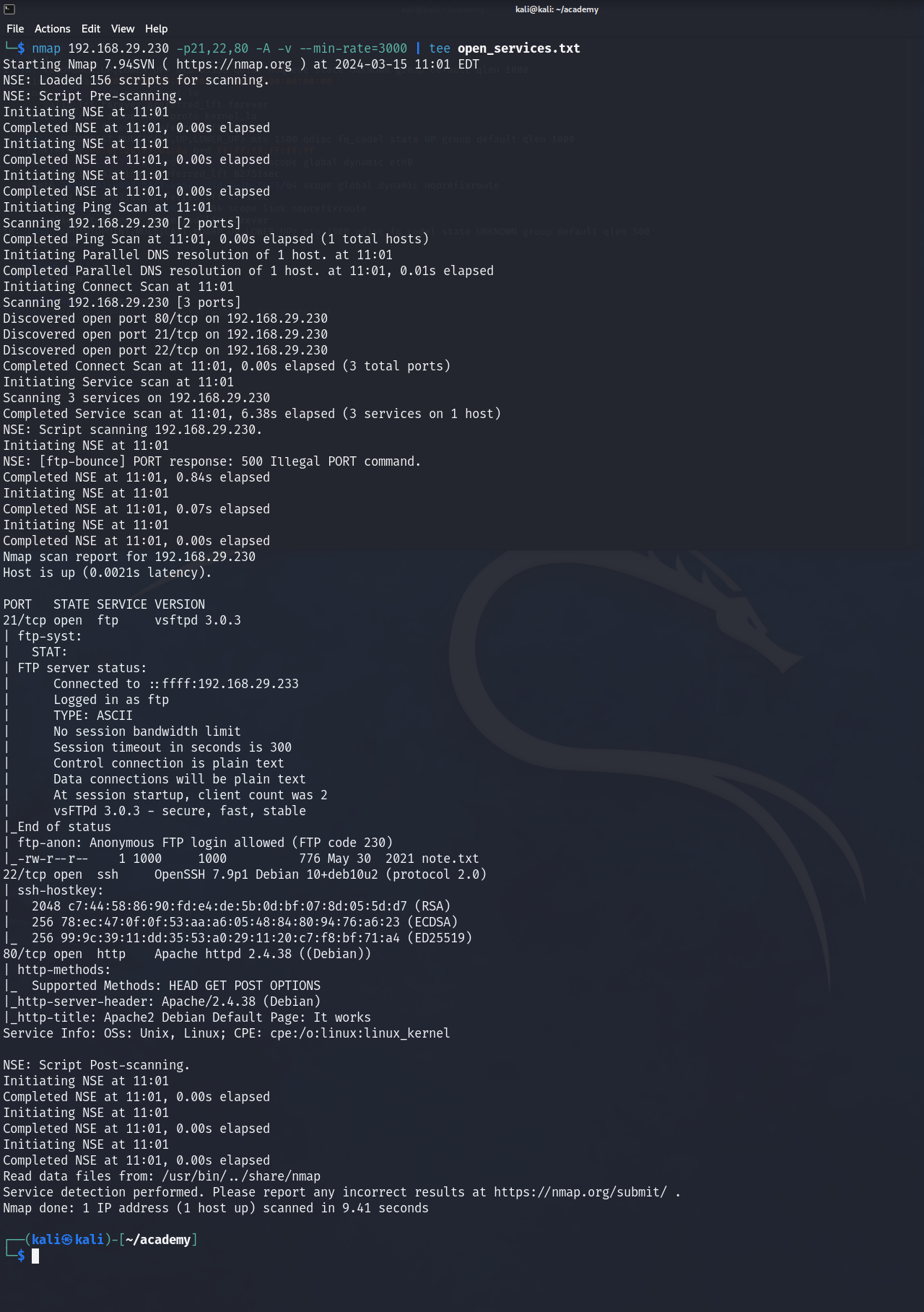


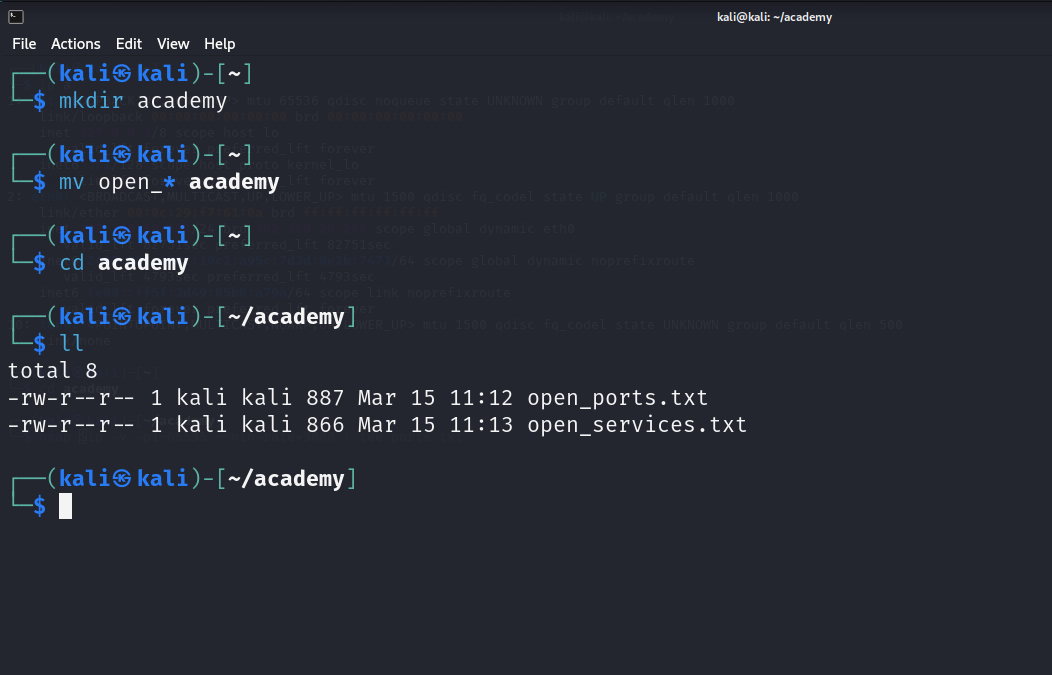


**Check for open ports and Services:**

* nmap 192.168.29.230 -p- -v --min-rate=3000 | tee open\_ports.txt
* nmap 192.168.29.230 -p21,22,80 -A -v --min-rate=3000 | tee open\_services.txt
* mkdir academy
* $mv open\_\* academy
* cd academy
* ftp 192.168.29.230



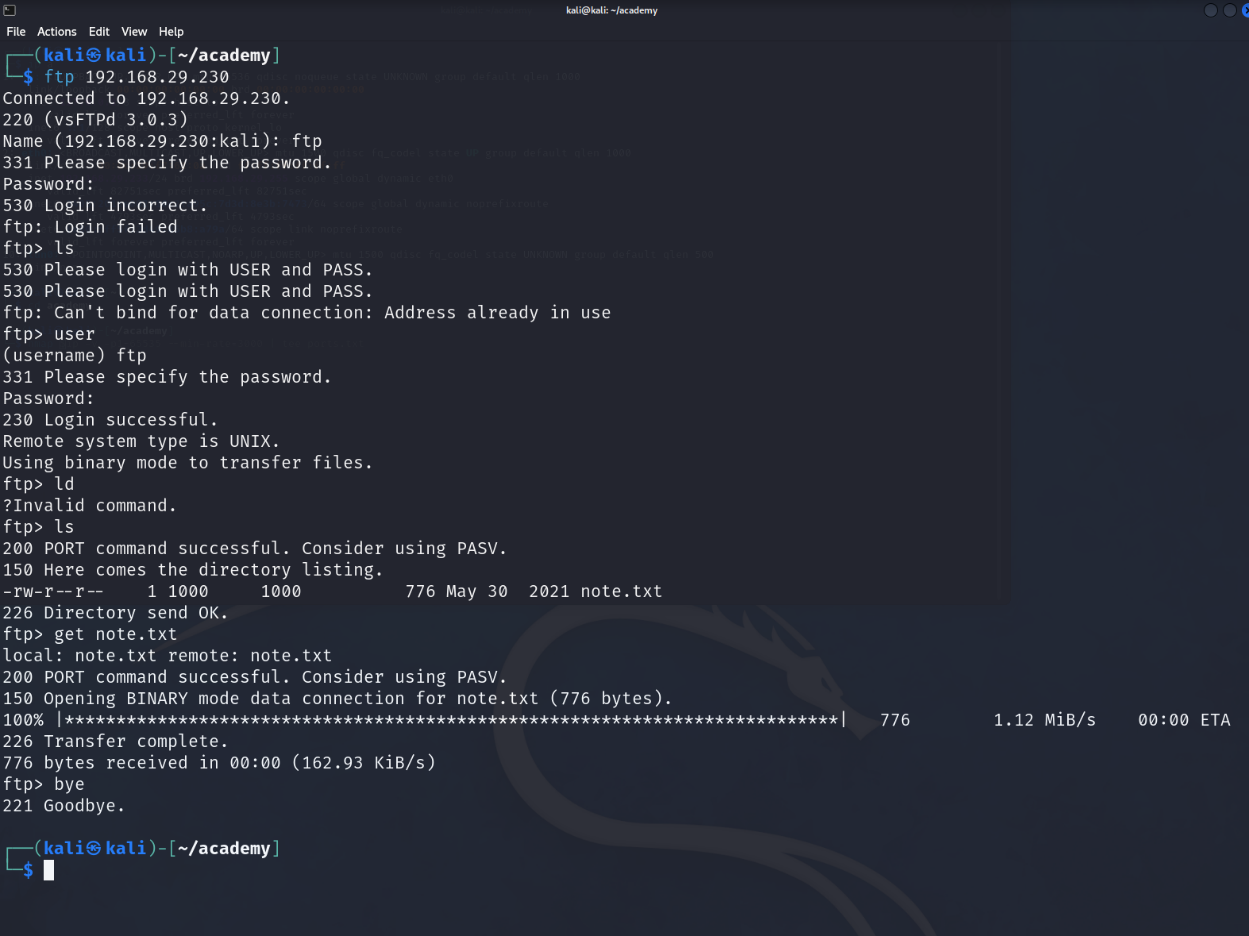




This step involves creating a directory and moving the open\_\*academy and also installing ftp if that doesn’t exist.

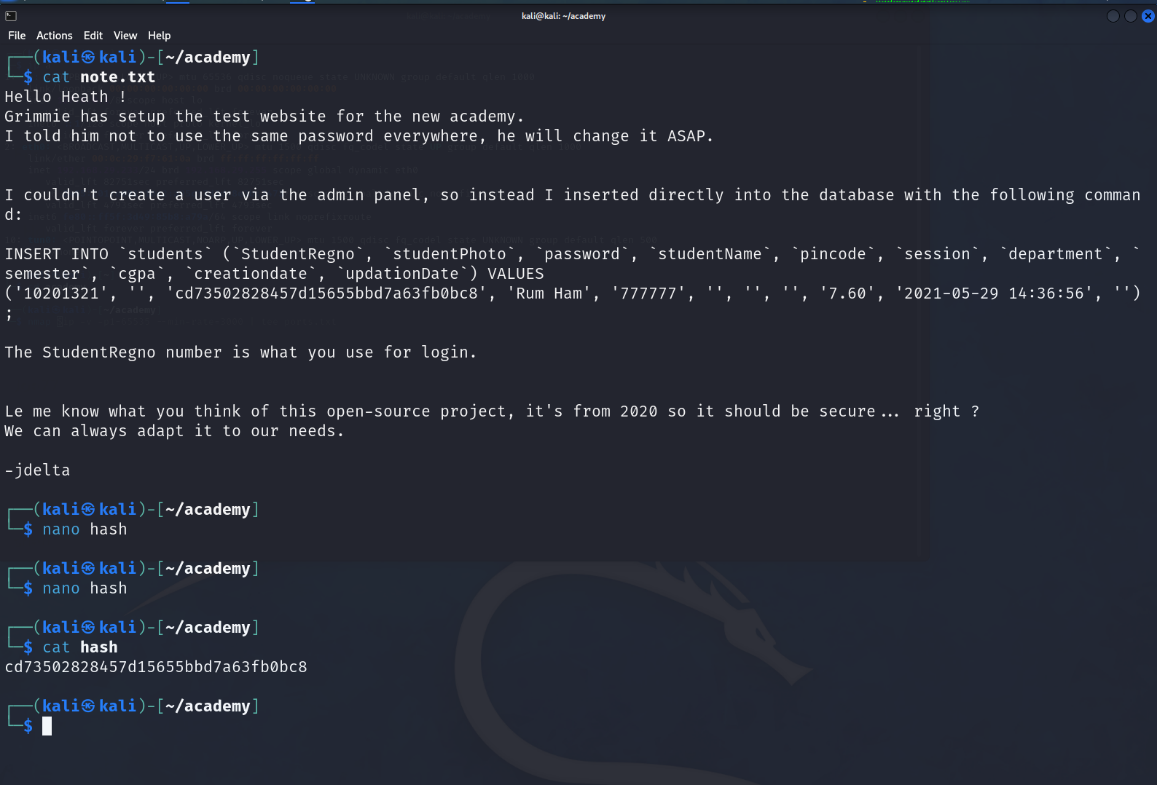
This enables ftp and includes setup and configuration and connecting the ip of academy to ftp.

The ip of academy can be seen by using the command ip a.



The next step involves creating an user login in ftp .

This requires to specify the password and then the login will be successful.



In this we store the value in the text file named note.txt and open a text editor.

We will have hash value and login credentials in that file.

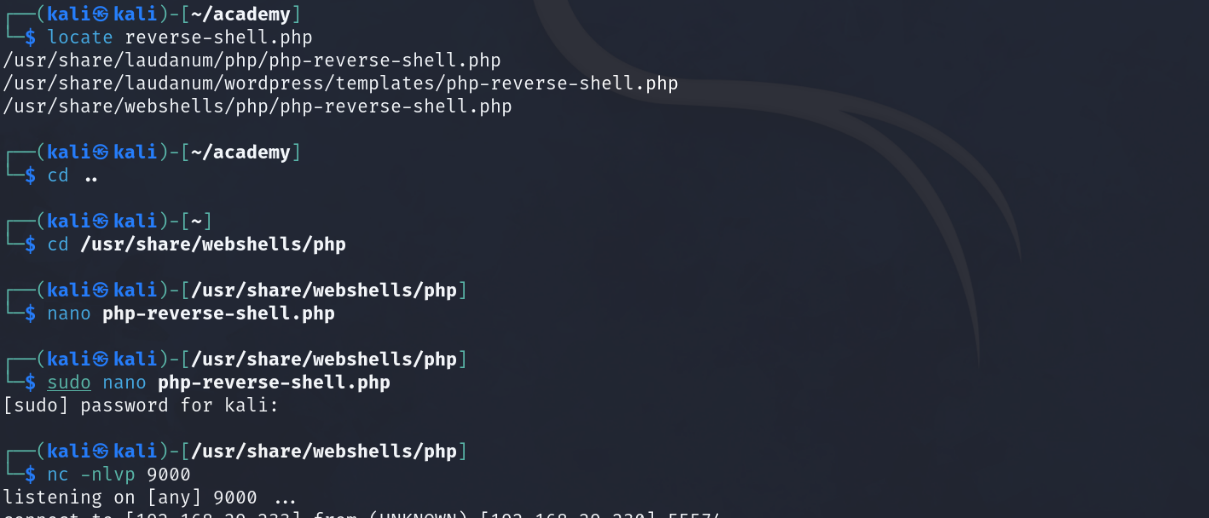
Use the cat command to display the values of login and hash values

I used the MD5 hash decrypter to convert the hash into readable format and thus the decrypted value is “ student “.



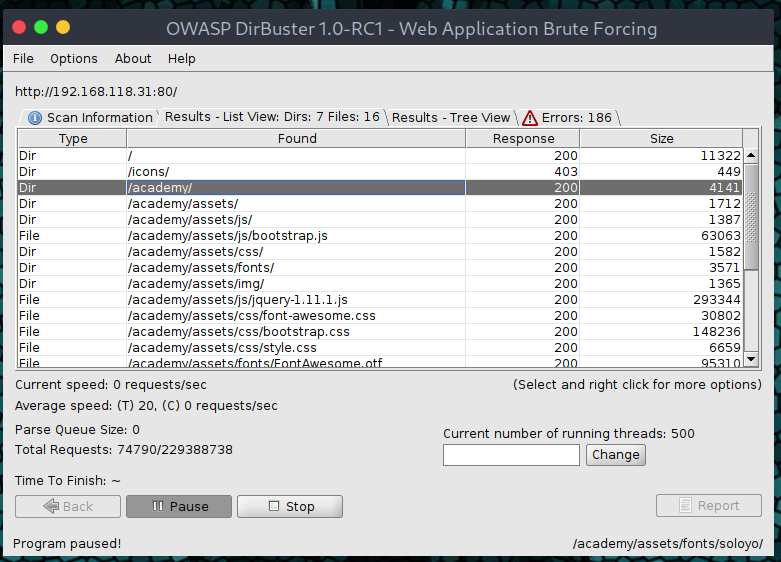
Thus we got the password as student and login id as 10201321.

We use this password for login.



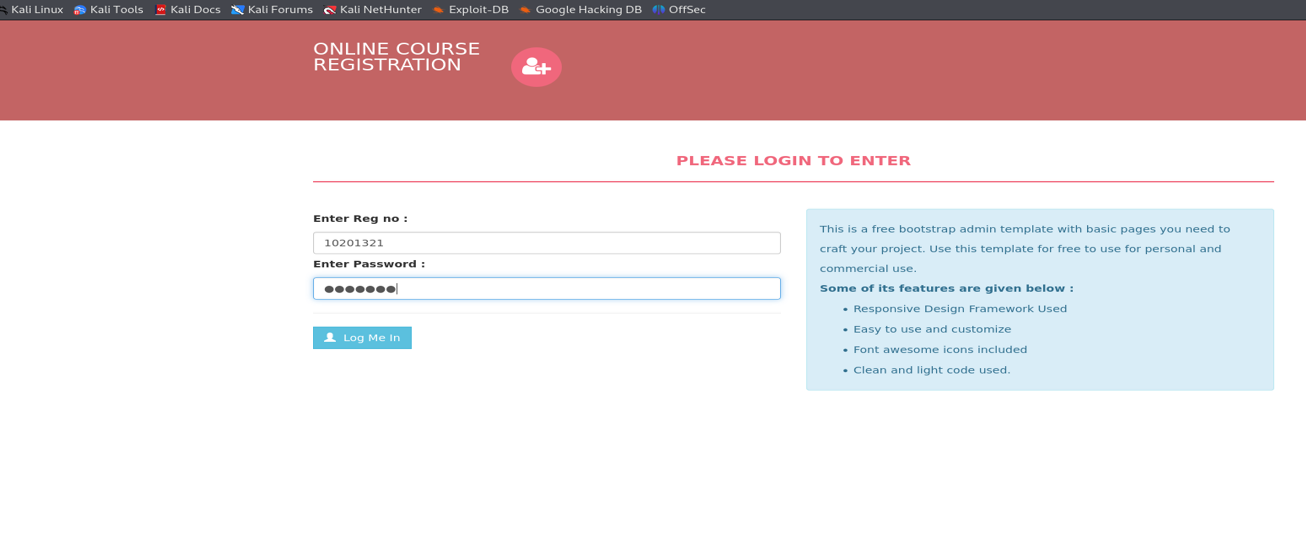
Now we need to open the dirbuster application in the parrot os.

And enter the ip of the parrot machine in the dirbuster and maximise the speed and click start.



Now find the academy file and right click on the file.

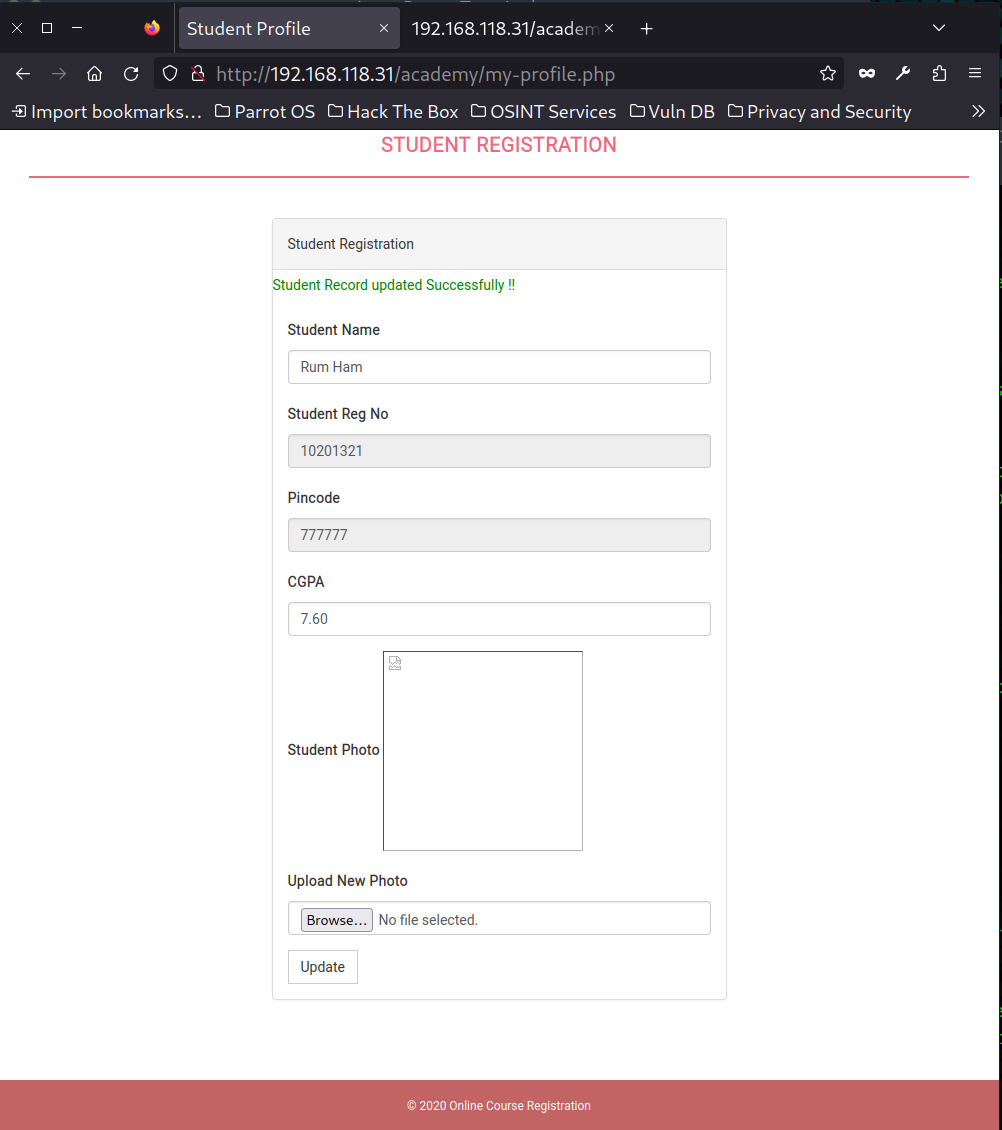
Once done it will show an option called open in browser, this will open the webpage in browser.



Now I use the login credentials to login to the account.

The vulnerability found here is they failed to add the file type restrictions thus we try to upload an executable php file to implement reverse shell.

It is also important to give execution permission to the php file using the command “ chmod +x filename.php “



**Upload the rev php file**

**nc -lvnp 12345(any port number)** - This command is used to set up a listener on a specific port for receiving incoming network connections.

We have **www-data, grimmie and root.**

There are two types of privilege escalation:

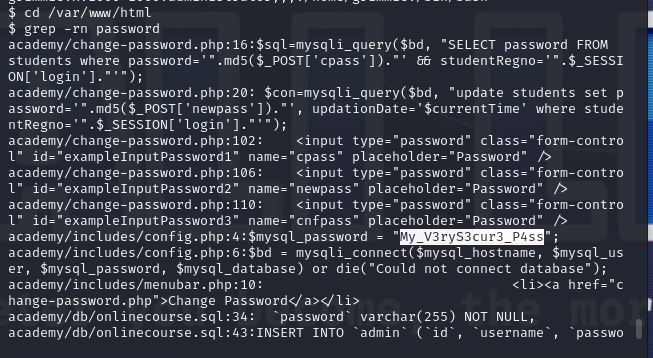
* **Horizontal privilege escalation:** gains access of similar users or groups.
* **Vertical privilege escalation:** gains access of higher authority users.

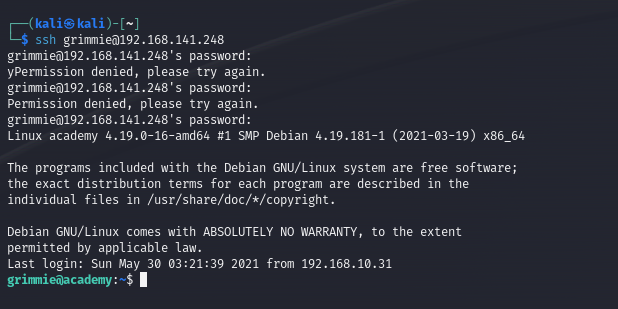
**www-data to grimmie** ---🡪 Horizontal privilege escalation.

**grimmie to root** ----🡪 Vertical privilege escalation.

Horizontal privilege escalation in our task is done by performing ssh (www-data to grimmie)

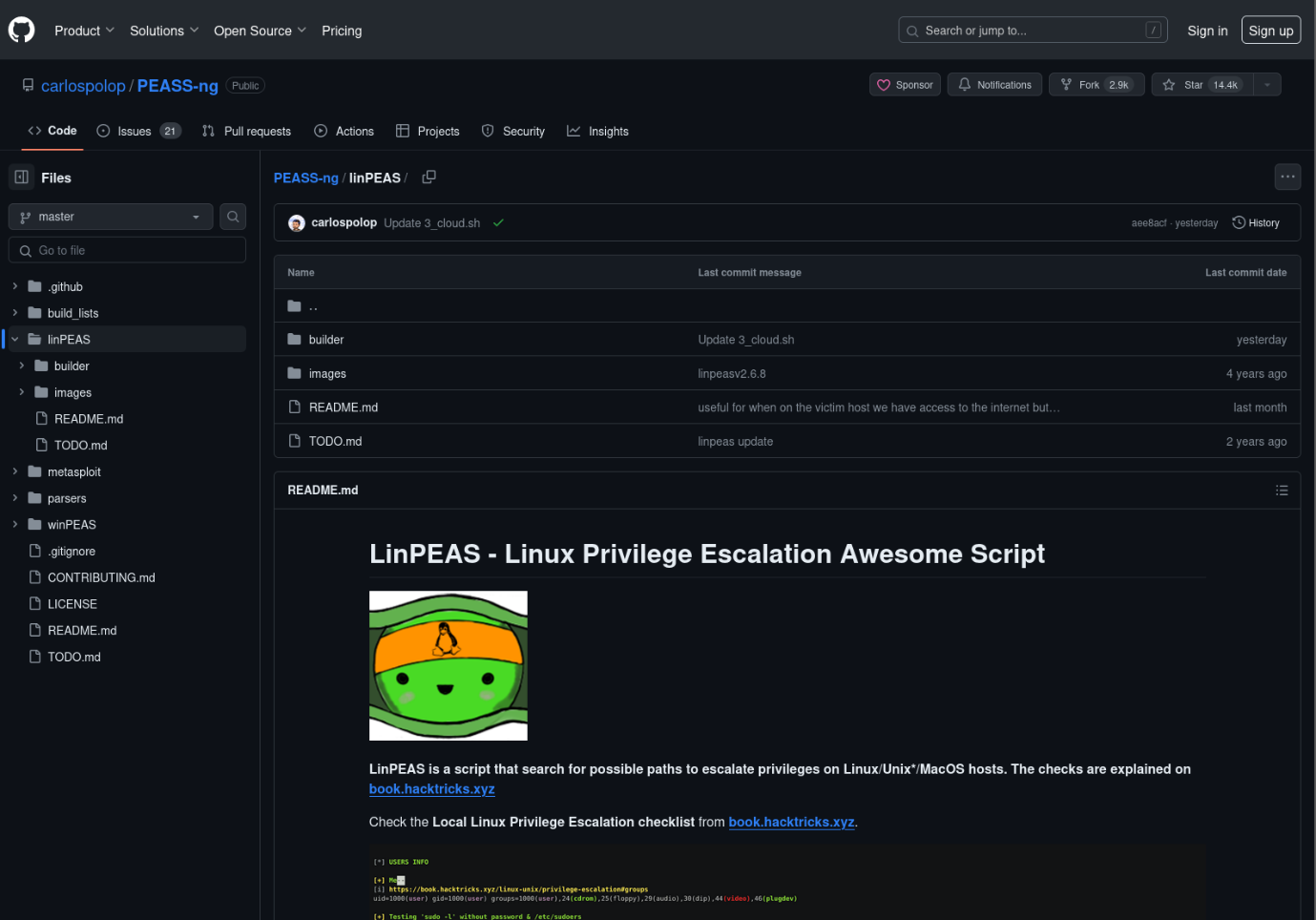
Grimmie’s password – **My\_V3ryS3cur3\_P4ss**





**Linpeas:**

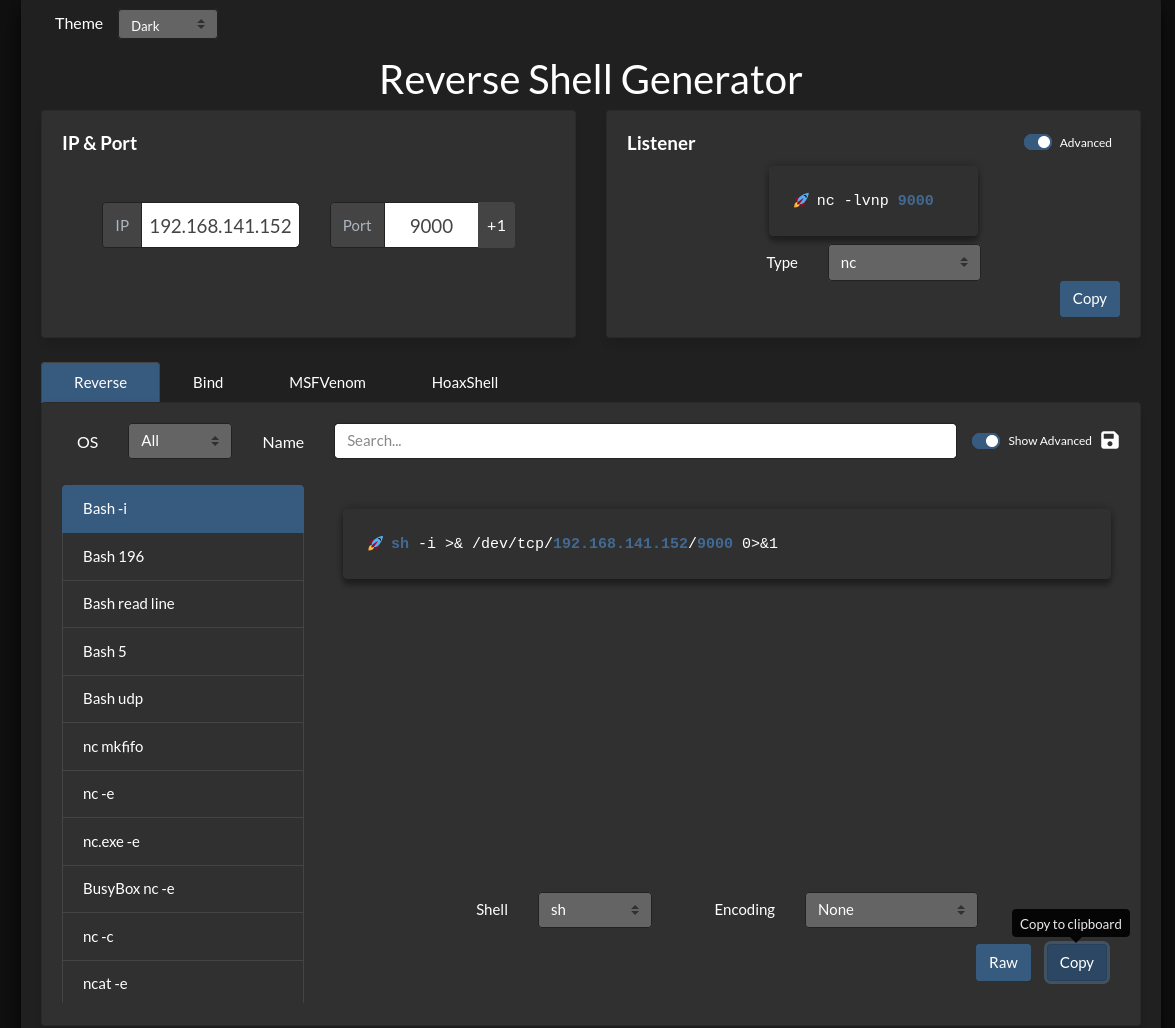
* Search for linpeas in browser in github
* Select the releases page

****

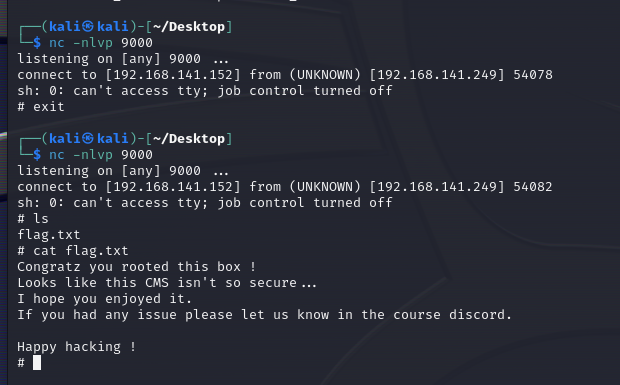
* Download the **linpeas.sh** as we use it for shell
* Copy the linpeas.sh file to lin.sh file and give the executable permission
* Copy this lin.sh file to the grimmie by using python webserver
* Change the permission for the lin.sh file and execute it

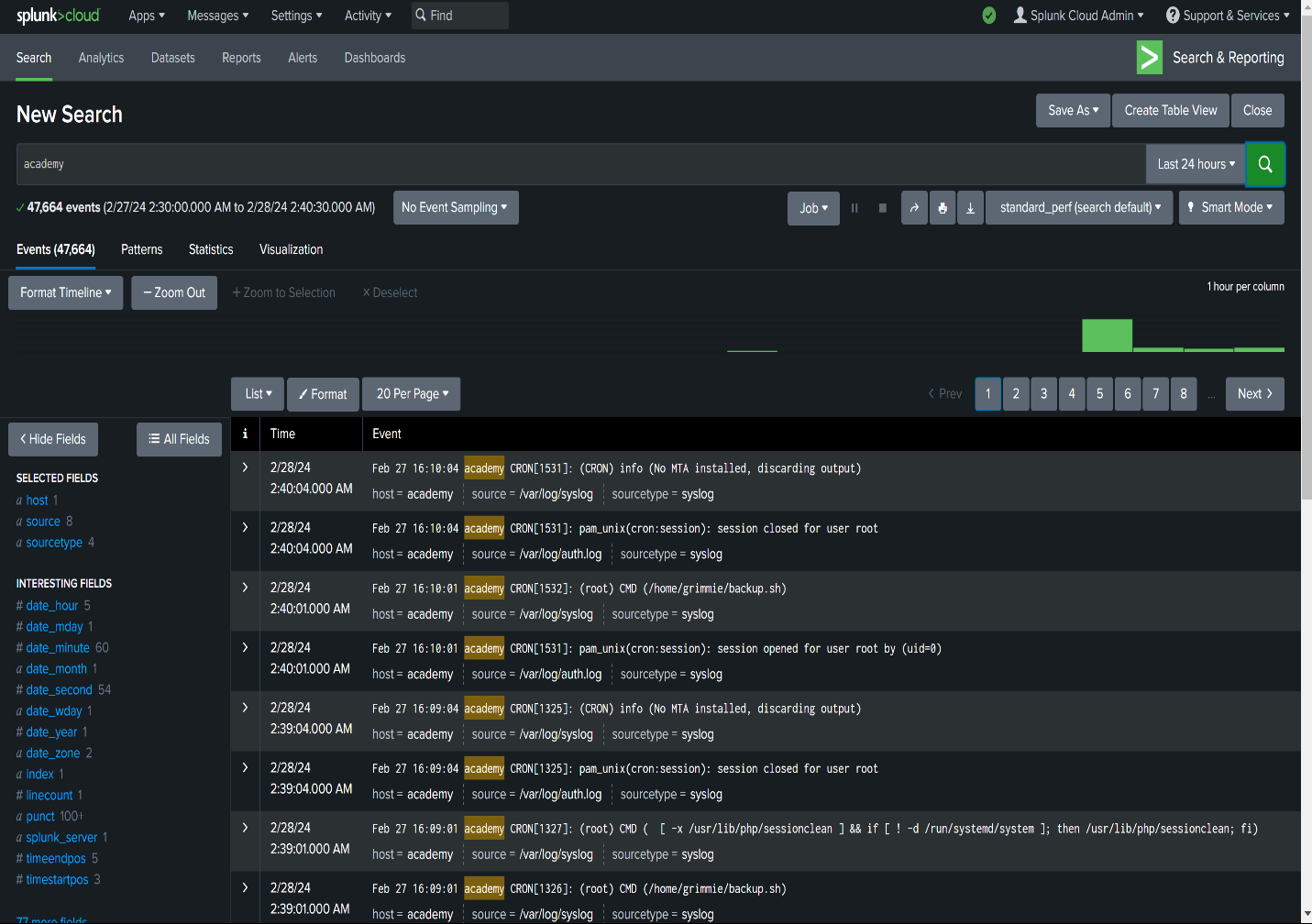
****

* In the backup.sh shell paste the reverse shell copied from the Reverse Shell Generator



* Now turn on the listener in the kali
* Once the user opens the file we get the access to the root
* We can also check the cloud instances and sources



****