VULNERABILITY ASSESSMENT

AND

PENETRATION TESTING



[madisettysaibhavitha.cse2021@citchennai.net](mailto:madisettysaibhavitha.cse2021@citchennai.net) 210421104095

Copyright

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission.

1. Vulnerability Assessment and Penetration Testing

1.1 Introduction

1.2 Objective

1.3 Requirements

2. High level summary

3. Methodologies

4. Download the Academy

4.1 Open the Academy in VM Ware

4.2 IP Address of Academy

4.3 IP Address of kali

4.4 Download Splunk forwarder

4.5 IP Address of windows

5. Service Enumeration

5.1 Creating a Directory

5.2 FTP Server

5.2.1 MD5 Conversion

5.3 Installation of secLists

5.3.1 WFUZZ command

5.3.2 php reverse

5.4 Login page

6. Reverse Shell Generator

7. Privilege Escalation

7.1 Horizontal Escalation

7.1.1 Access the Grimmie

7.2 Vertical Escalation

VULNERABILITY ASSESSMENT AND PENETRATION TESTING:

* 1. Introduction -

A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage. Using a risk-based approach, vulnerability assessments may target different layers of technology, the most common being host-, network-, and application-layer assessments. Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system.

1.2 Objective -

The objective of this assessment is to perform vulnerability assessment and penetration testing. This report helps you to understand that how to go through all the steps and to identify, analyze, and prioritize vulnerabilities within a system, network, or organization in order to assess potential risks and weaknesses, enabling informed decision-making for the implementation of effective security measures and risk mitigation strategy.

1.3 Requirements -

The main requirement to do this is of the following:

* VM ware WorkStation named Academy
* Splunk cloud platform and also forwarder
* VM ware WorkStation named Kali

1. HIGH LEVEL SUMMARY :

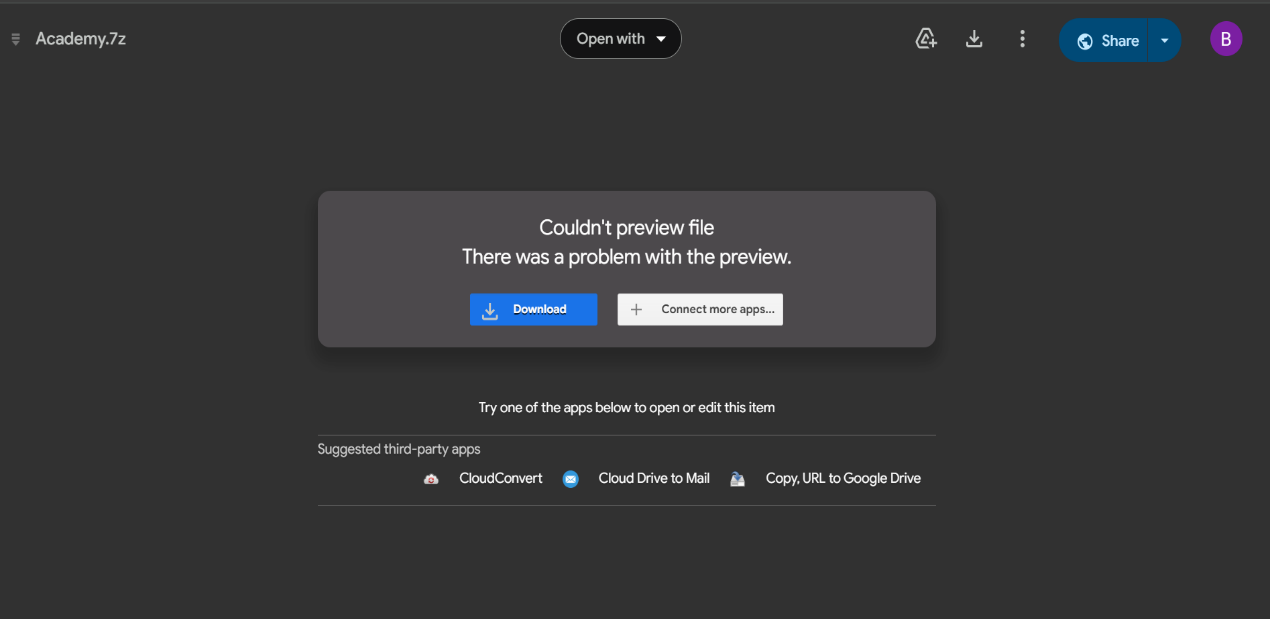
When performing the attacks, we are able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, we had administrative level access to multiple systems. The systems were successfully exploited and access granted. Alternatively , we must use Cloud instance to get log for that security purposes.

3.METHODOLOGIES:

We have utilized a widely approach to perform penetration testing that is effective in testing the academy login page is secure. Below is a breakout of how we have able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

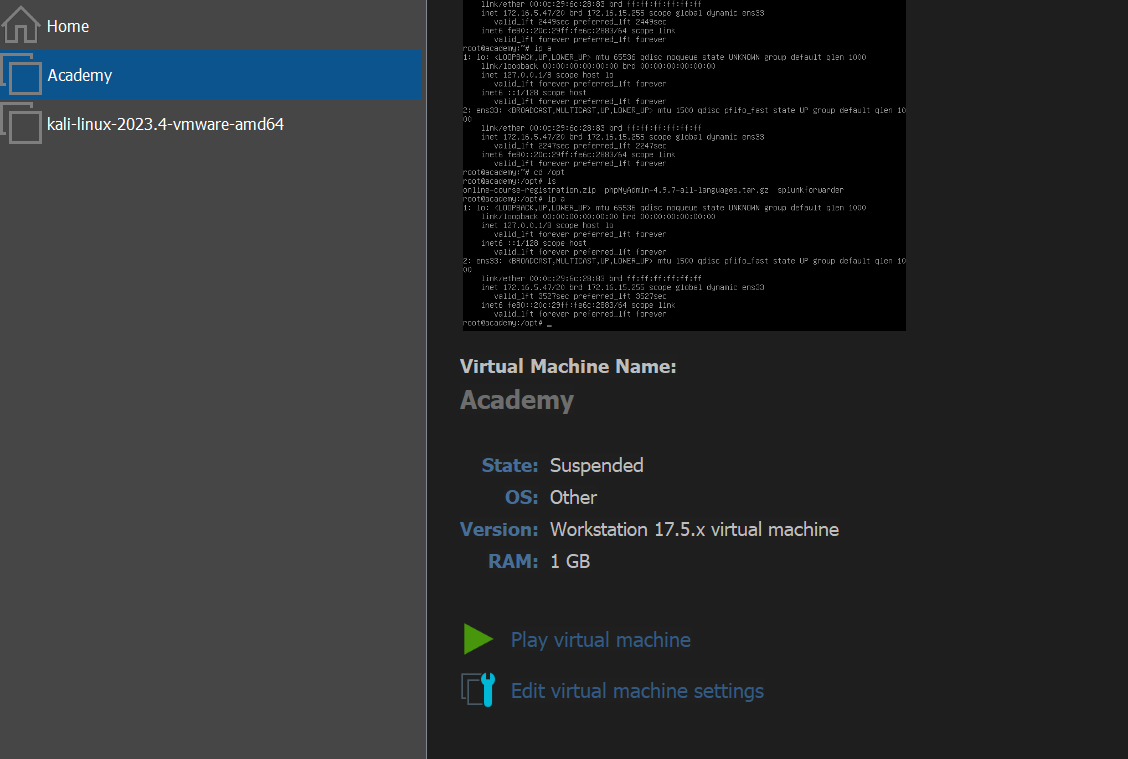
There are 5 steps to perform this task :

* Reconnaissance (Information gathering)
* Service Enumeration
* Gaining Access
* Maintaining Access
* House Cleaning
* 4.Download the Academy:



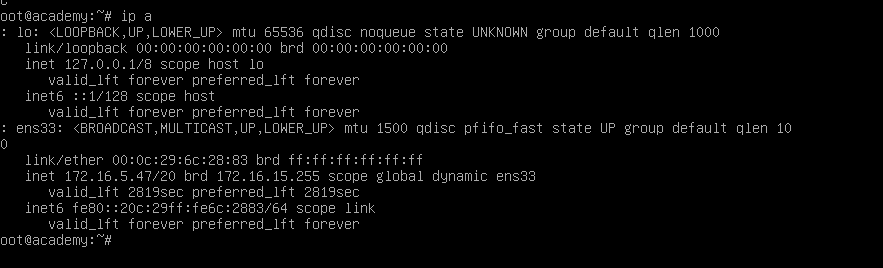
Here we have downloaded the Zip file named Academy and Extracted it into a VM Ware. Then we have opened the Academy in the VM ware and choose the path in the D Drive and imported further.

4.1 Open the Academy in VM Ware:



4.2 IP Address of Academy:



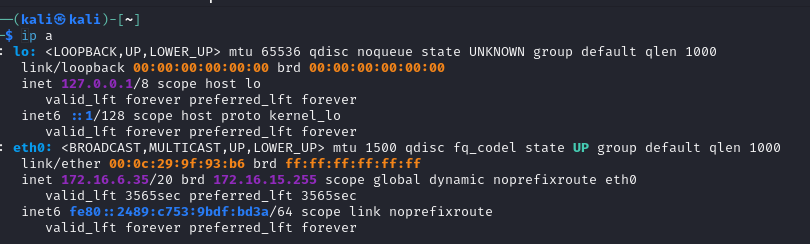


Here first we have gained access to login the academy and started finding the ip address of the academy. To find the ip address we have used two commands. Dhclient is used to provide the ip address from DHCP server.

4.3 IP address of Kali:

Now we need to configure the ip address of kali . Through this ip address , we will attack the Academy machine .In kali , we will use the command named ip a .

Ip address of kali:

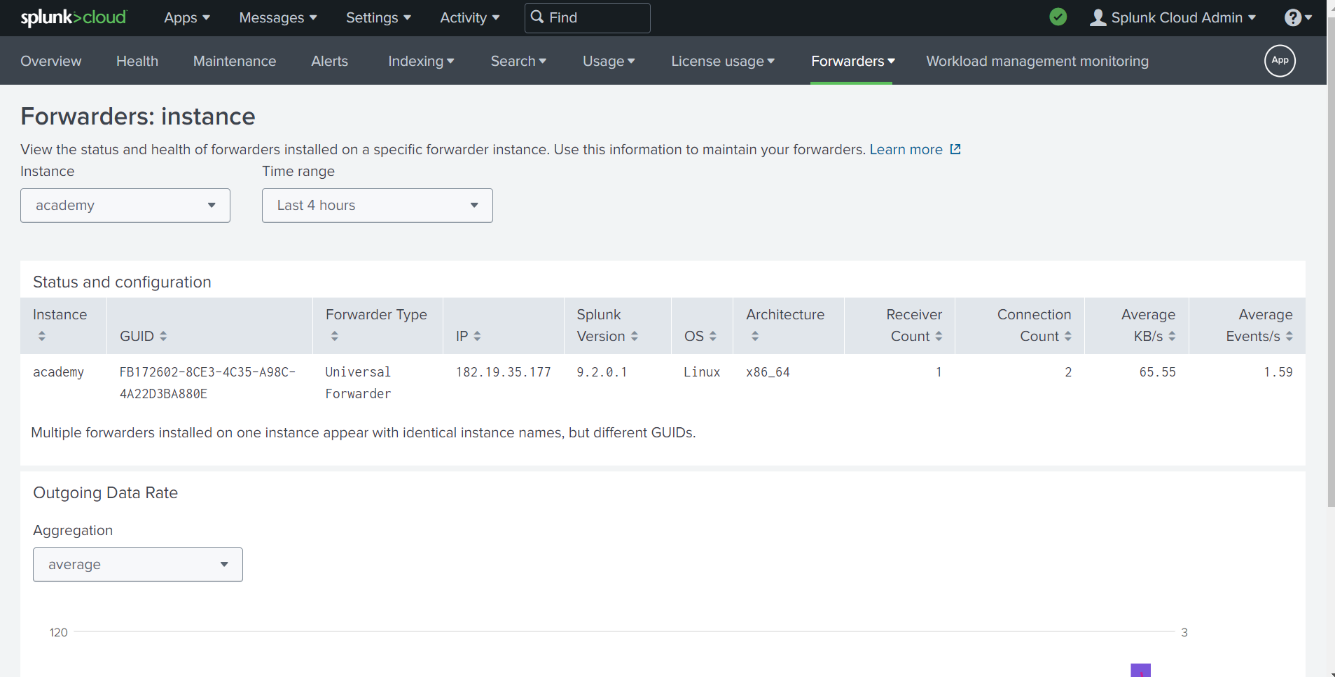


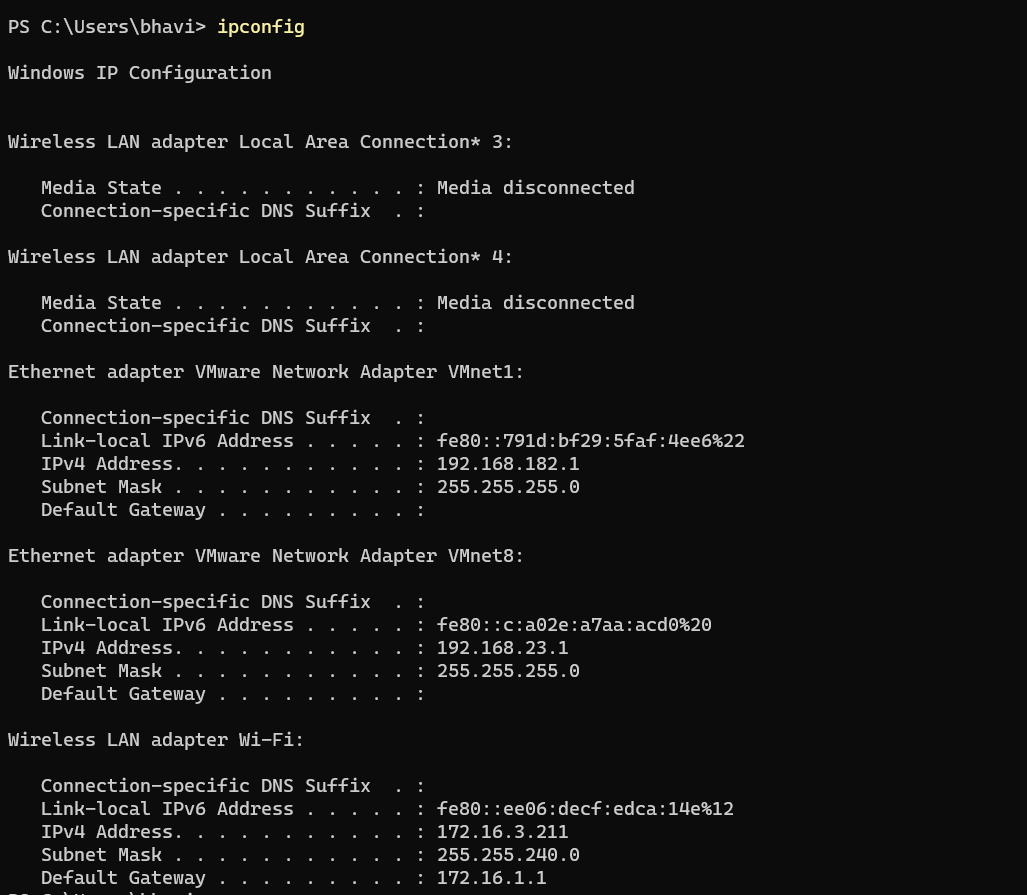
4.4 Download Splunk forwarder:

We can download the splunk forwarder by using the commands:

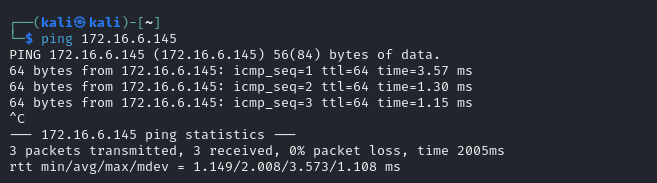
* + Wget -O splunkforwarder-9.22.0.1-d8ae995bf219-linux-2.6-amd64.deb “https://download.splunk.com/products/universalfrowarder/releases/9.2.0.1/linux/splunkforwarder-9.22.0.1-d8ae995bf219-linux-2.6-amd64.deb
  + Useradd -m splunkfwd
  + Export SPLUNK\_HOME=”/opt/splunkforwarder”
  + Now create a directory – mkdir $SPLUNK\_HOME
  + dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb
  + chown -R splunkfwd:splunkfwd $SPLUNK\_HOME
  + $SPLUNK\_HOME /bin/splunk start –accept-license
  + Cd/opt/splunkforwarder/bin
  + ./splunk
  + ./splunk add forward-server 172.16.13.255.
  + ./splunk install app splunkclouduf.spl ,
  + ./splunk list forward-server
  + ./splunk add monitor /var/log
  + ./splunk restart

Configure the universal forwarder to forward the logs to the remote cloud server.



4.5 Ip address of windows:

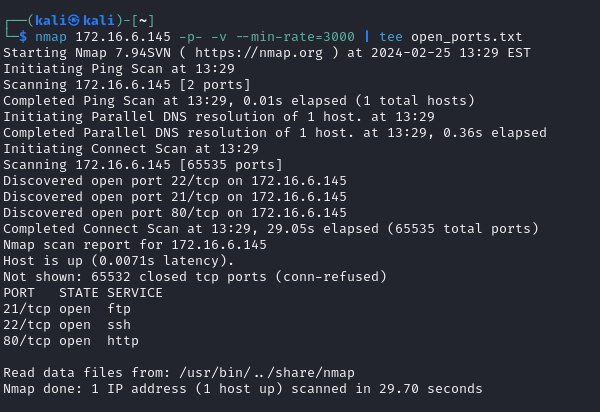
We need to ping Academy IP address in kali. This will transfer the packets .



* 5 SERVICE ENUMERATION:

Service enumeration is a method used to find out the service version that is available on a particular port on the target system. This version information is important, because with this information the penetration tester can search for security vulnerabilities that exist for that software version.

Here we will use nmap command to provide services.



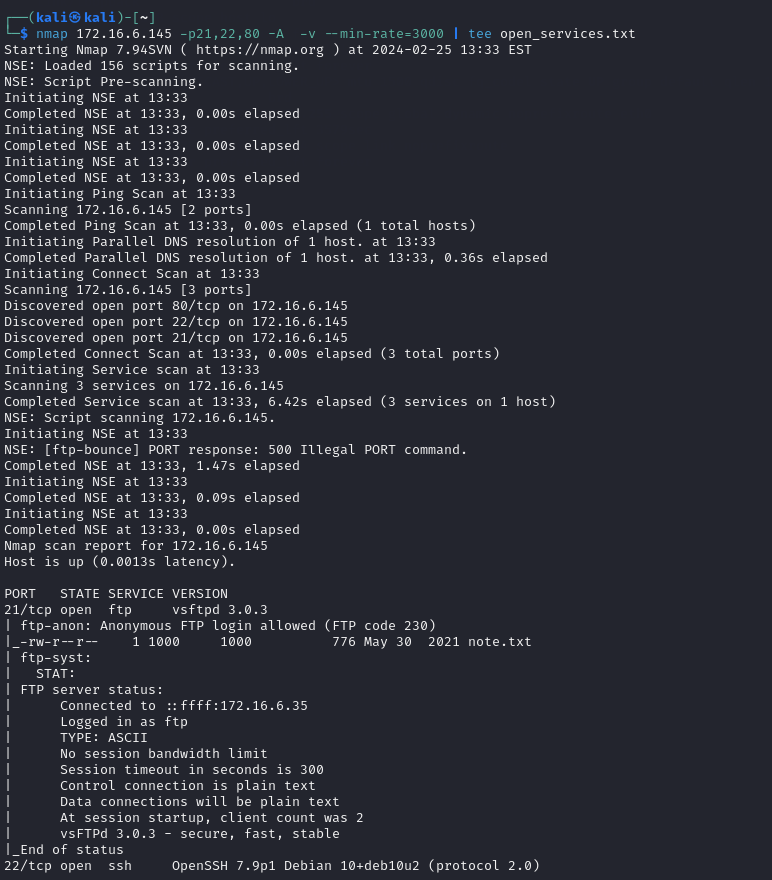
In the above command, open\_ports is used to facilitate various network services, such as web browsing, email, file transfers, and remote access.

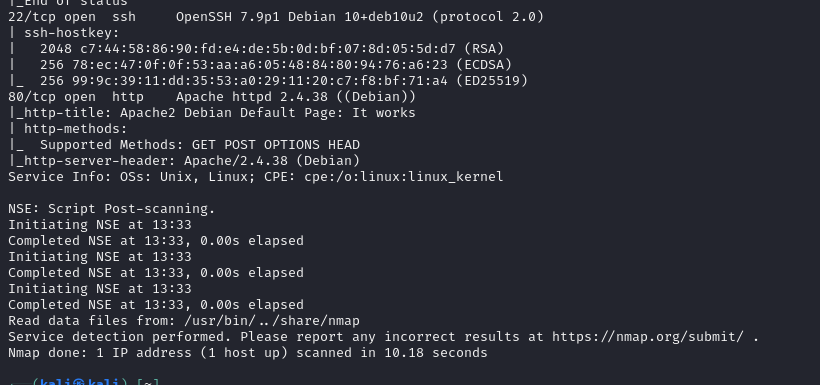
* Nmap = It is a tool to scan the ports
* -v = It represents verbos
* --min-rate = 3000 = giving the faster speed access
* tee = write the output in the file and display in the terminal

we got three services along with the ports:

* ftp – port no 21
* ssh – port no 22
* http – port no 80

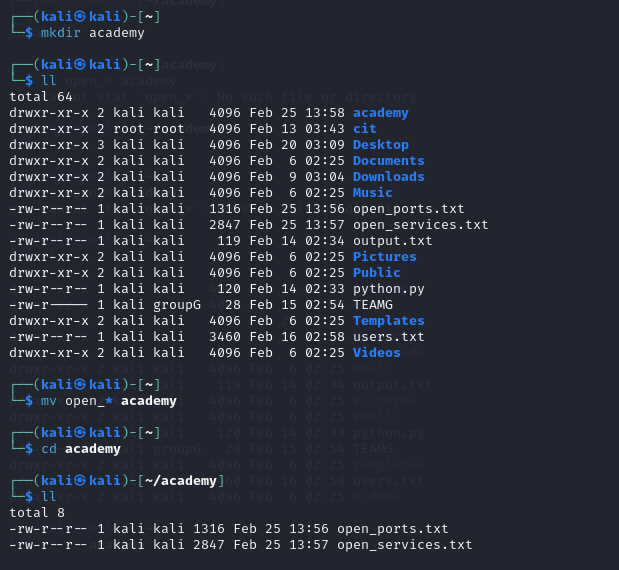
Here is the another command to brief about the services .



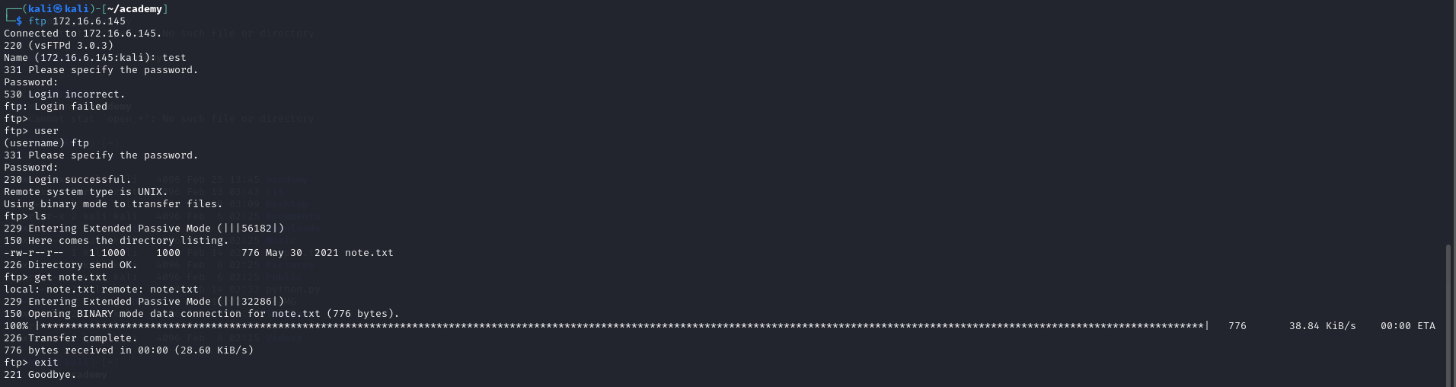


5.1 Creating the Directory:

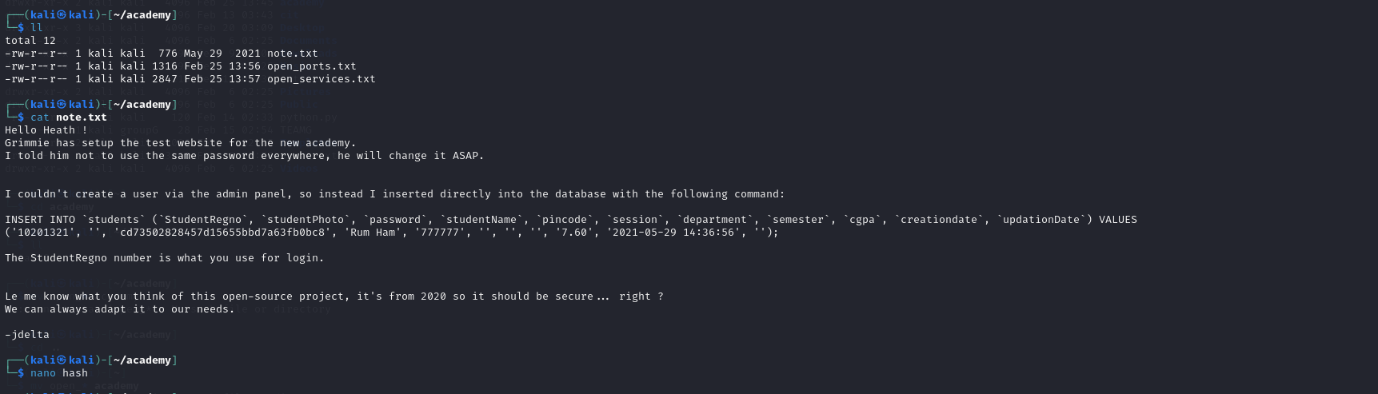
We created a directory called academy and moving services to academy . Now go inside the academy directory and check the files present in it.



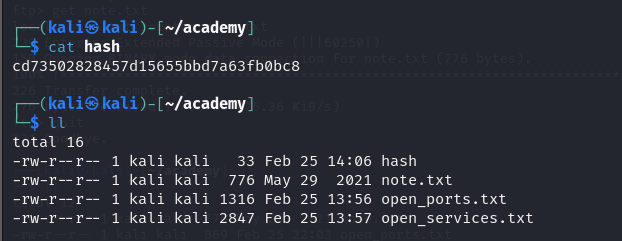
* 1. Ftp Server :
* FTP is actually used to transfer the data, including login credentials.
* FTP servers are often targeted by attackers seeking to exploit vulnerabilities and gain unauthorized access to internal networks.
* FTP servers typically require users to authenticate themselves with a username and password.
* For securing FTP servers, we need Proper access control.
* Here we get note.txt in ftp and transfer the bytes which are needed further .



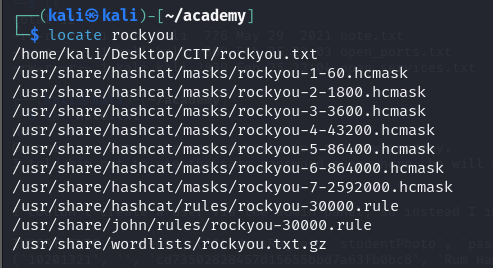
* To read the file, we use cat command, so cat note.txt.
* In cat note.txt, we need to copy the studentPhoto and paste it in the nano command and store it using hash.
* The command which is present in the note file is DBMS command which is used to store the database.



In academy directory, we need to see the hash and list all the files present.



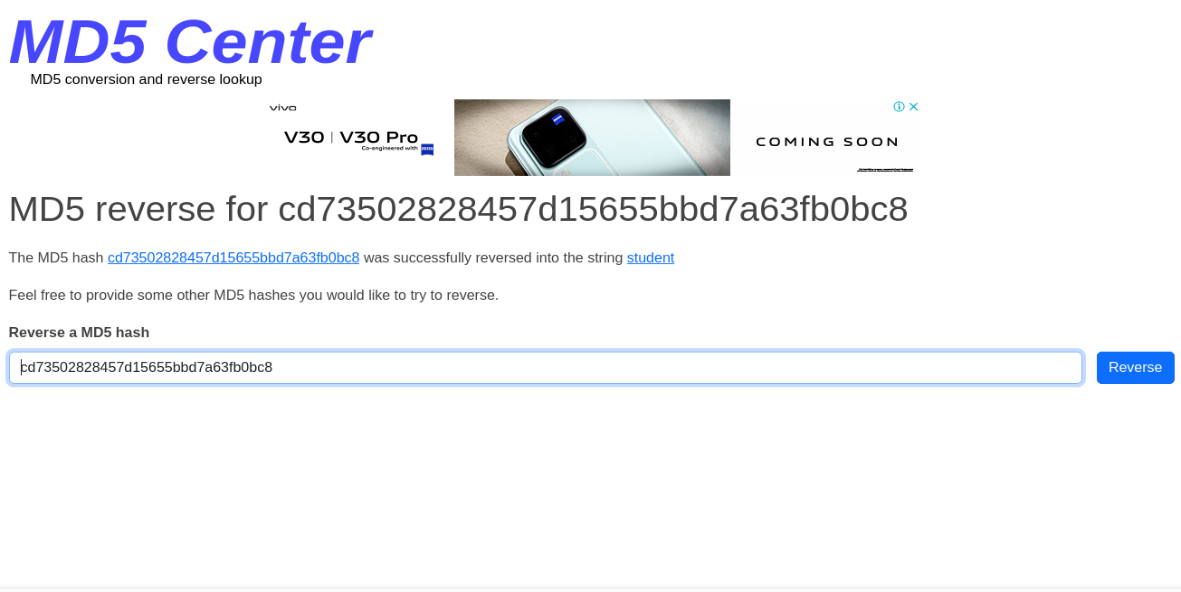
We need to locate the rockyou text. Rockyou is a file which contains large number of passwords. We can get Rockyou from the github platform .



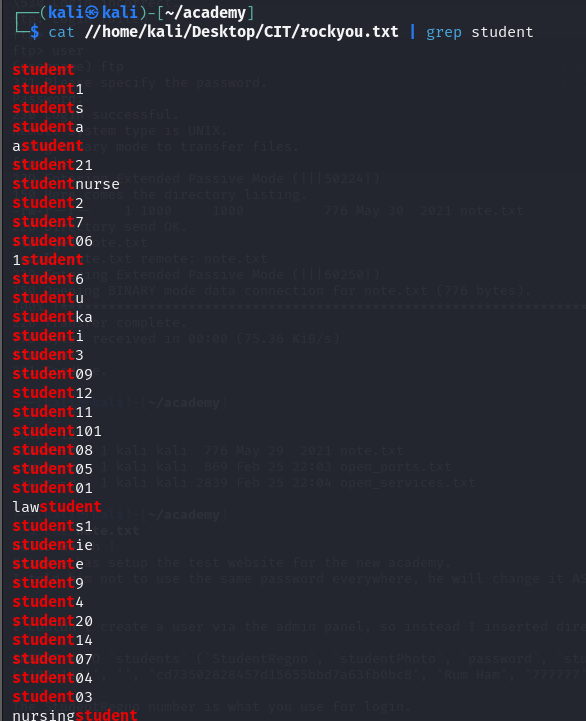
Now, we need to convert the hash into a string, this is done using MD5 conversion.

5.2.1 MD5 –

* Message Digest Method 5
* It is used for the conversion of hash into string
* It is a cryptographic hash algorithm



Through MD5, we got to know that, we contained a hash which stands as Student .So we must see student in the rockyou list.



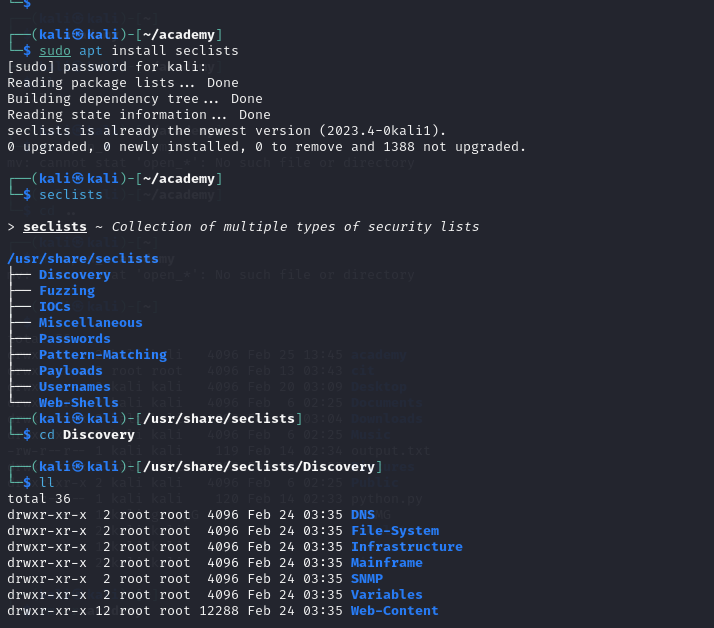
* 1. INSTALLATION OF SECLISTS :

SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more.

There are three methods to install secLists . They are:

* apt
* apt-get
* aptitude

After installing, you can access the seclists under the path: /usr/share/seclists. There are different types of lists that are included in this folder. Then we should go inside the Discovery and see all the files present .

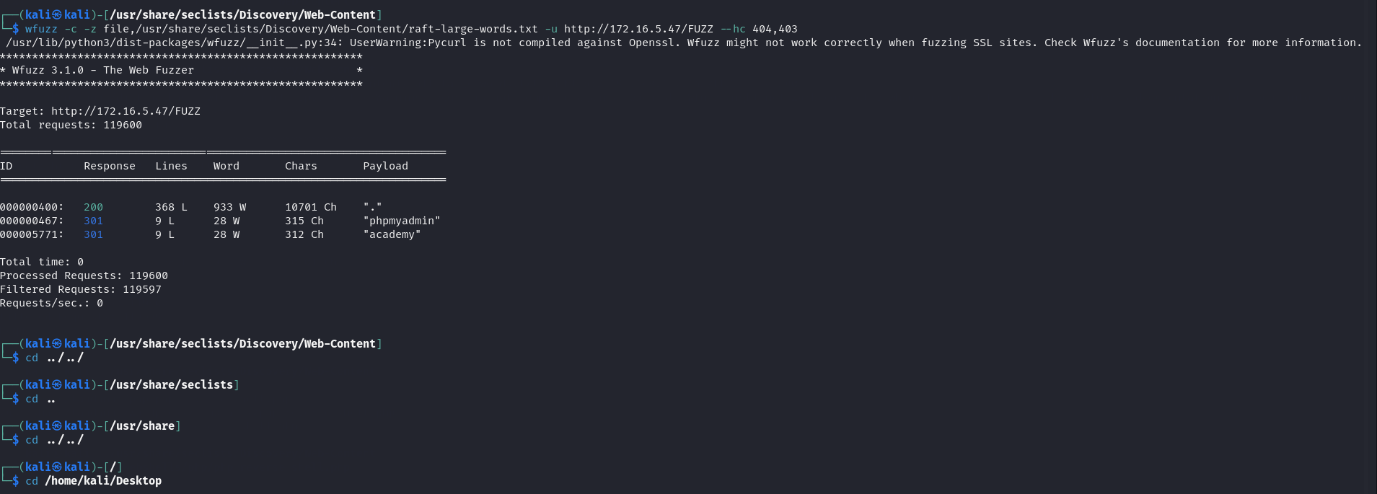


5.3.1 Now we should use WFUZZ Command:

Wfuzz is a command line tool written in python. It is used to discover common vulnerabilities in web applications through the method of fuzzing. Fuzzing is a quality assurance technique used to detect vulnerabilities.

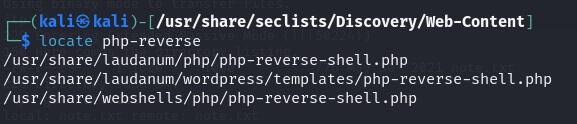
In wfuzz command,

* -c = output with colours
* --hc = hide code

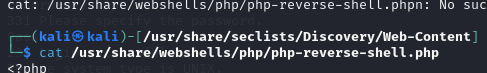


5.3.2 Locate php-reverse:

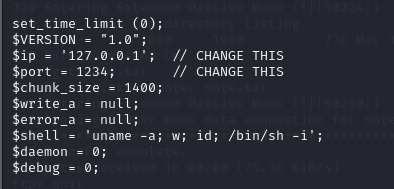
* Php is called as Hyper Text Pre Processor.
* It is used to break the security system.
* It is used to show where php reverse file is present.



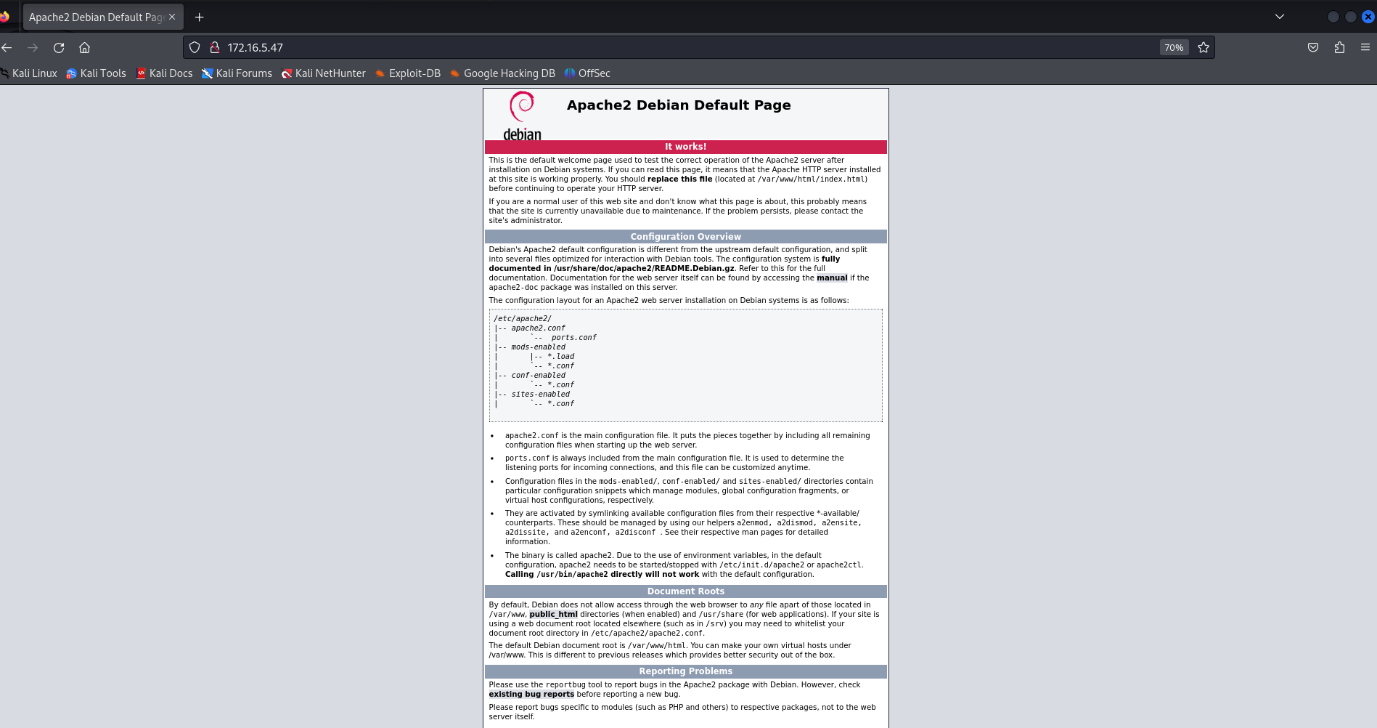
File present in php reverse:



Through this command, we will get the file and and we have to change the ip address to academy and also we need to change the port number which is present in the file.



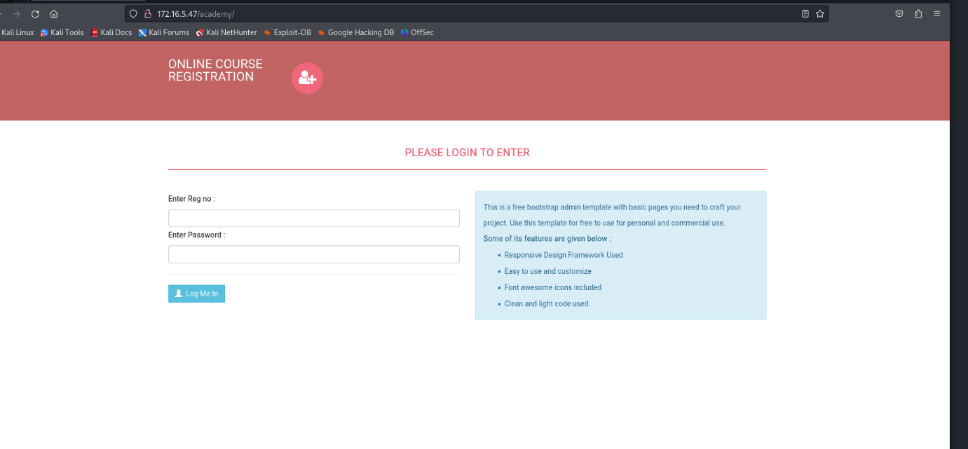
Now, we should open firefox in kali which is a VM Ware WorkStation and type the ip address of target machine i.e, Academy, Then we will get one default page called Apache Debian Default Page.



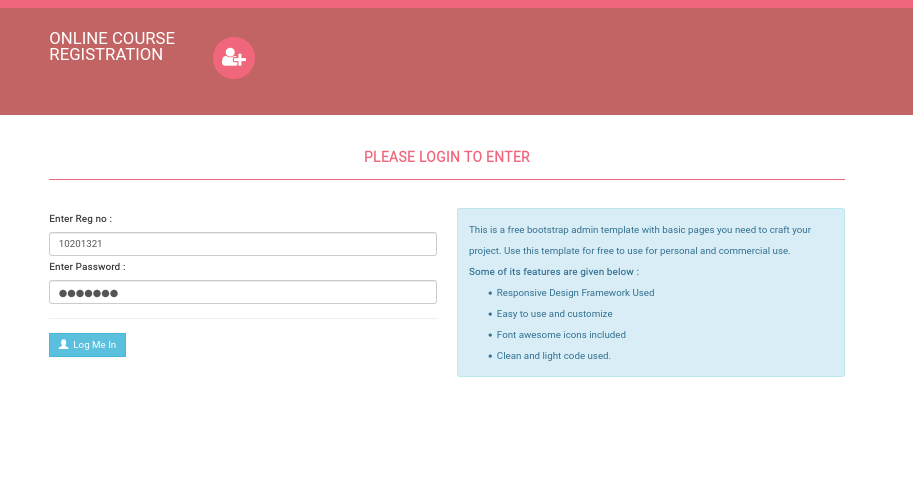
* 1. LOGIN PAGE:

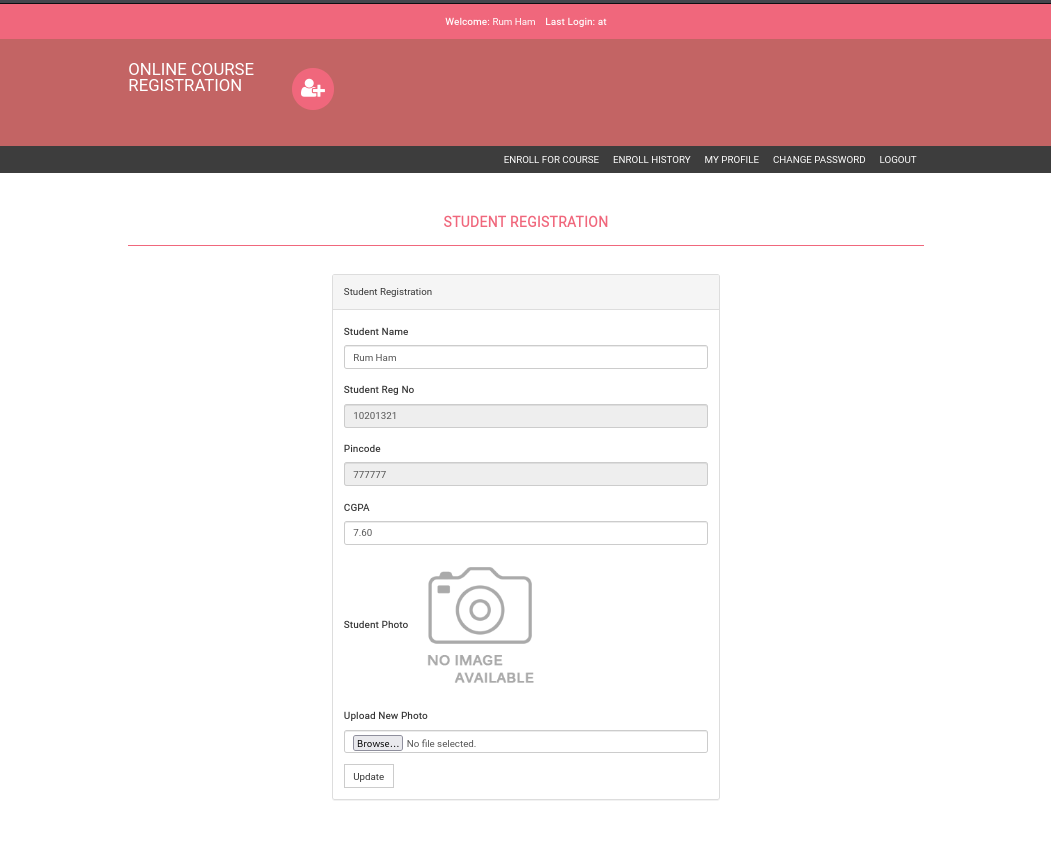
Atlast, we will get the login page of Academy if we type the ip address of target along with target machine name i.e, /academy in the Firefox.

Format:- **172.16.5.47/academy**

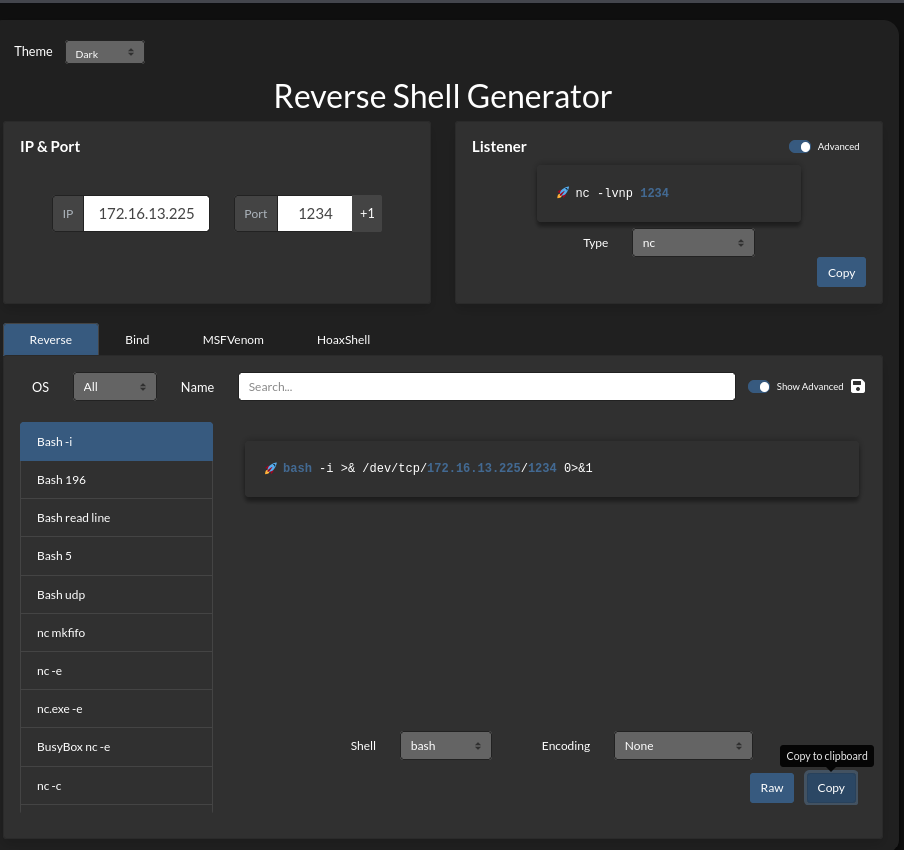
****

* Now we need to enter the Registration Number and Password to run the application.
* This Registration Number and password is present in the database which has been created before .

 Then we will get a Student Registration page:

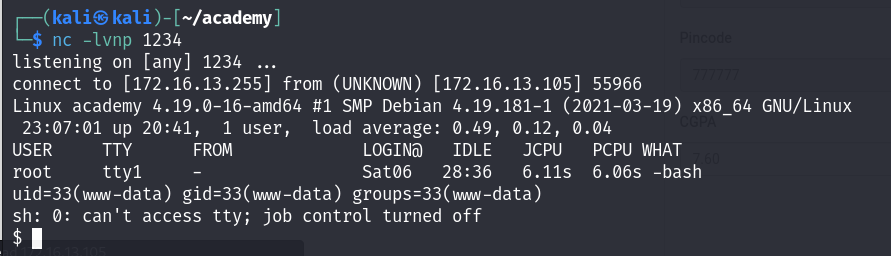


6. Reverse Shell Generator:

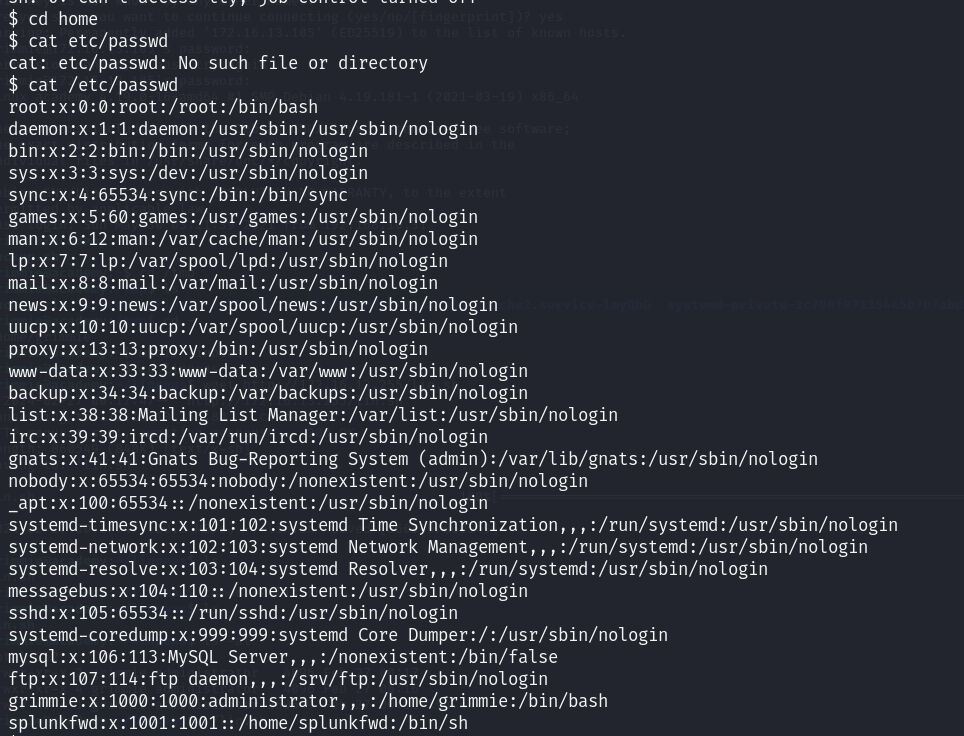


In reverse shell generator ,

* We must use kali ip address and any default port number .
* We have to select and copy the listener and paste it in the kali.



Then we must see the files present in the home directory.



7. Privilege Escalation:

There are two types of Escalations:

* Horizontal Escalation
* Vertical Escalation

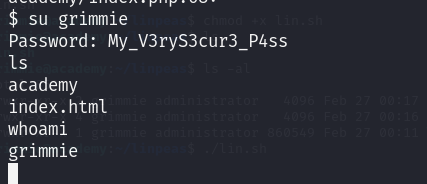
7.1 Horizontal Escalation –

* + Attackers gain the access with limited permissions.
  + Here, Horizontal Escalation is done while changing from www data to grimmie.



Here we can see all the passwords present in the listener and select the mysql password from it .

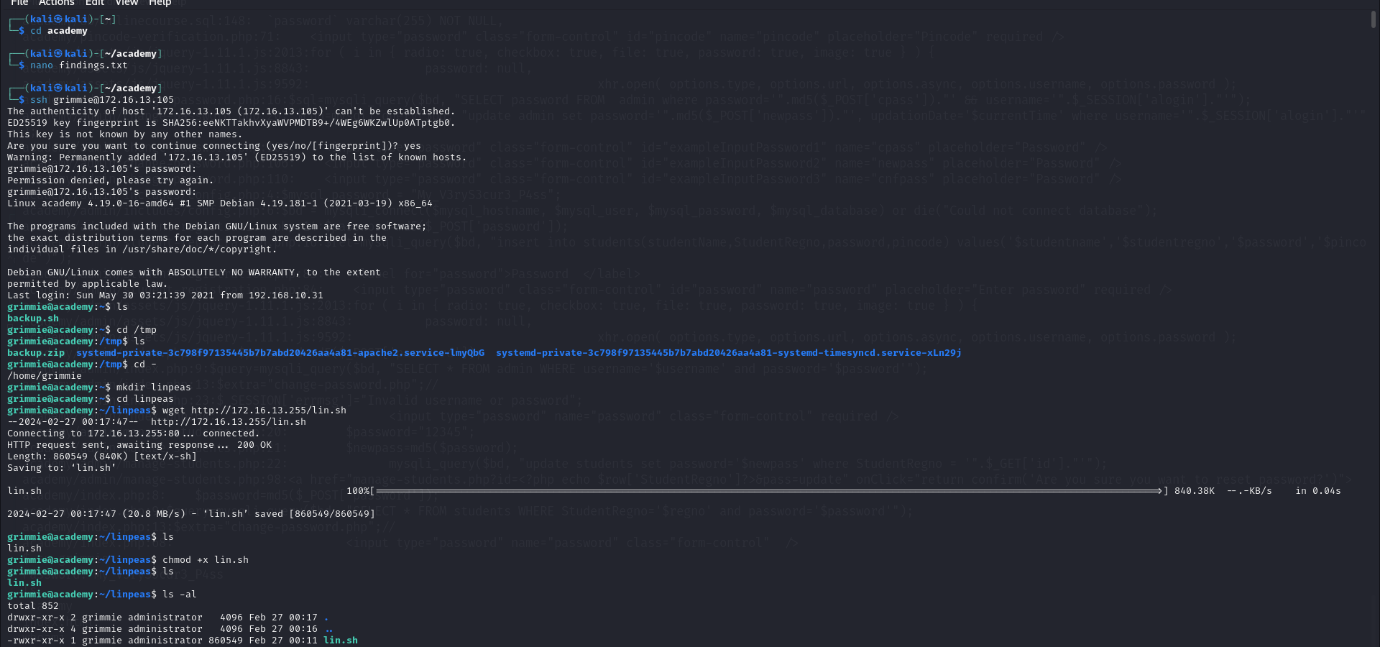
7.1.1 Access the Grimmie:



* Now we must use Grimmie as a user access.
* We must download linpeas in the Github platform from the Firefox.
* And create a directory called linpeas in the Grimmie.
* And go inside the Directory.

7.2 Vertical Escalation –

* + Attackers gain access without any permissions.
  + It is done while changing Grimmie to root .



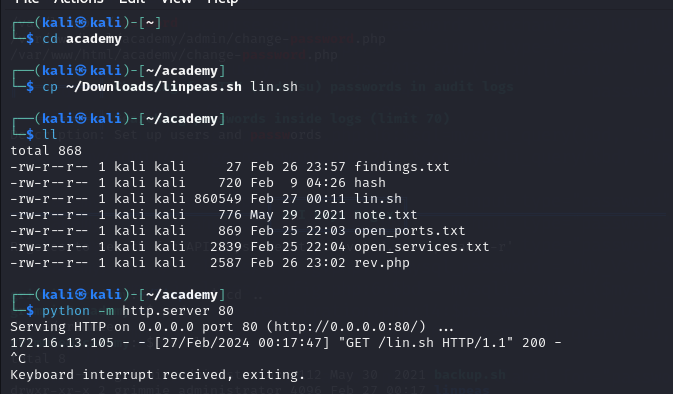
* + We must change linpeas as lin.sh.
  + The permissions which is given has to be executed.

LINPEAS:

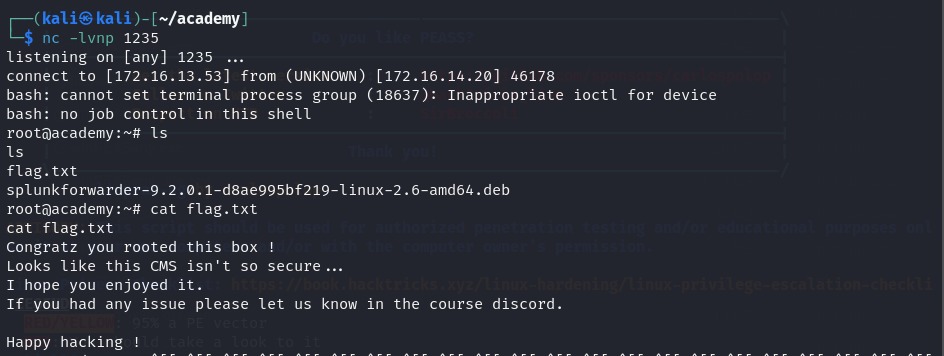
* Linux Privilege Escalation Awesome Script
* It searches for possible paths to escalate privileges on linux.



* Now, In another terminal, we must go inside the academy directory and run the python server.



* Now, we must check the present working directory.
* And check the files present in the directory.
* In backup.sh file, we must do changes such as copying the password which has been taken from the Grimmie.
* We should come back to Academy directory and run the nc -lvnp 1235 command.
* nv –lvnp is used to receive the reverse shells and get the root access.
* Now we list through ls command, we will get the flag.txt.
* Finally, we have exploited academy machine.
* Successfully we have rooted the box .



**\*\* HAPPY HACKING\*\***