VAPT REPORT

[lankipallijahanavi.cse2021@citchennai.net](mailto:lankipallijahanavi.cse2021@citchennai.net)

210421104086

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.

Table of Contents

1. **Vulnerability Assessment and Penetration Testing** 
   1. Introduction
   2. Objective
   3. Requirements
2. **High-Level Summary**
3. **Methodologies**
4. **Independent tasks**
   1. Download the Academy VM
   2. Unzip the file
   3. Install the Academy VM
   4. Accessing the Academy virtual machine
   5. Enabling network in the academy
   6. Finding kali's IP address
   7. Finding Windows IP address
   8. Starting ssh in PowerShell
   9. Implementing Splunk Cloud
5. **Vulnerability analysis**
6. **Vulnerability exploitation**
7. **Reverse shell**
8. **Gaining the user access**
9. **LinPEAS**
10. **Gaining the root access**

PROJECT REPORT

1. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

1.1 Introduction:

A vulnerability assessment is an information security process used to identify weaknesses or vulnerabilities in a computer system or network. The purpose of vulnerability assessment is to determine the system’s vulnerabilities. The assessment can be performed manually or automatically. If performed manually, the tester will follow an assessment procedure to identify the vulnerabilities. If the manual assessment is not sufficient or time-consuming, then an automated vulnerability assessment can be used.

1.2 Objective:

This project report helps you understand all the steps to identify, analyze, and prioritize vulnerabilities within a network or system. The main objective of this assessment is to perform vulnerability analysis and monitor logs by using a Splunk cloud remote server.

1.3 Requirements:

The main requirements to complete this assessment are:

* Academy Virtual Machine Workstation.
* Kali Virtual Machine Workstation.
* Splunk and Splunk cloud Remote server.

2. High-level Summary:

While performing the attacks, we can gain access to multiple machines. During the testing, we had administrative-level access to multiple systems. The systems were successfully exploited and access granted. We use Cloud instances for configuring logs and security

3. Methodologies:

We adopted a comprehensive approach for penetration testing to ensure the security of the academy login page. The following breakdown illustrates how we identified and exploited various systems, encompassing all individual vulnerabilities discovered.

The five steps used in this task are:

* Information gathering
* Service Enumeration.
* Gaining Access.
* Maintaining Access.
* Clear the footprints

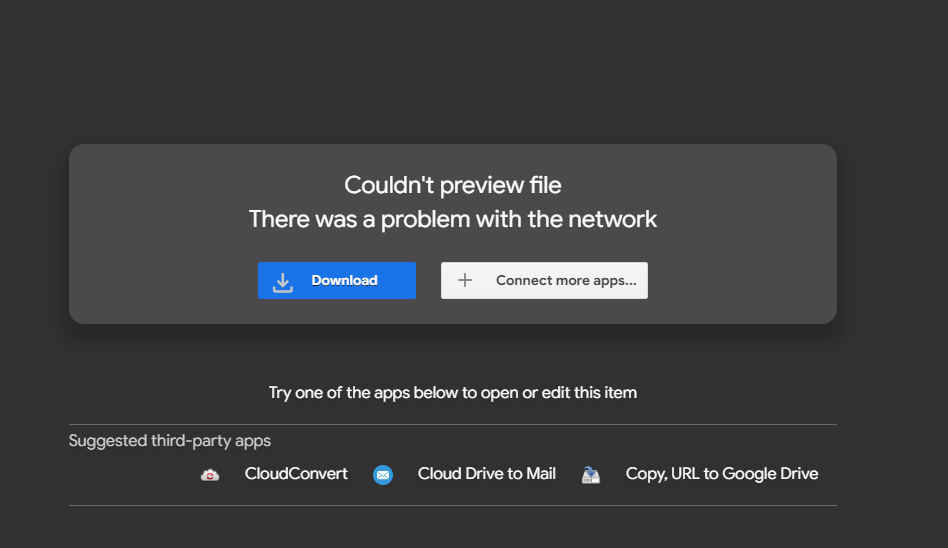
4. Independent tasks:

4.1. Download the Academy VM:

Click the "Download Now" button next to the chosen installer file.

Review the End User License Agreement (EULA) and accept it if you agree to the terms.

The download will begin.

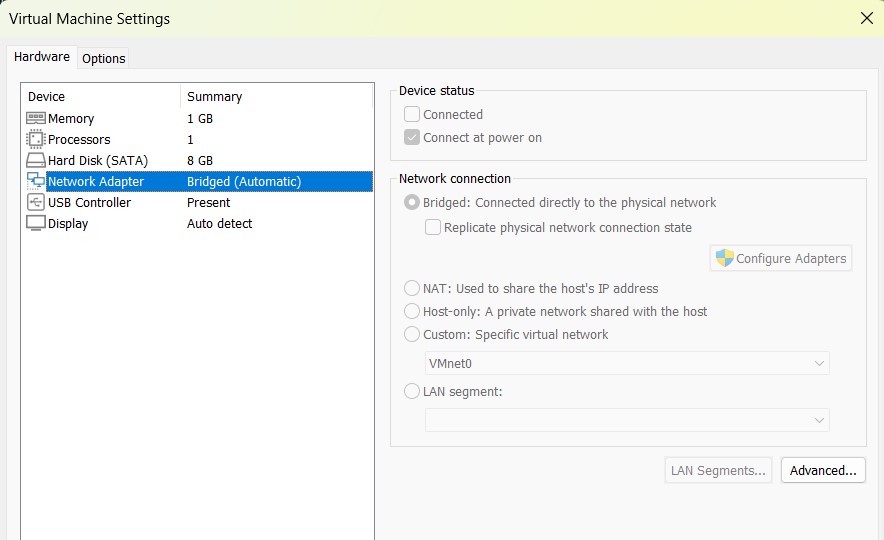


4.2. Unzip the 7z file:

Unzip the zip file Extract the files and copy them to the directory.

4.3. Install the Academy VM:

Open the VMware Player, select Open VM, and then select the extracted VM and import the Academy VM in the VM Ware workstation.  Edit the Virtual machine and change the network settings to Bridge before switching on the Virtual machine.



4.4. Accessing the Academy Virtual Machine:

By using the root password.txt file get the username and password and login to the Academy Machine.

Username: root Password: tcm

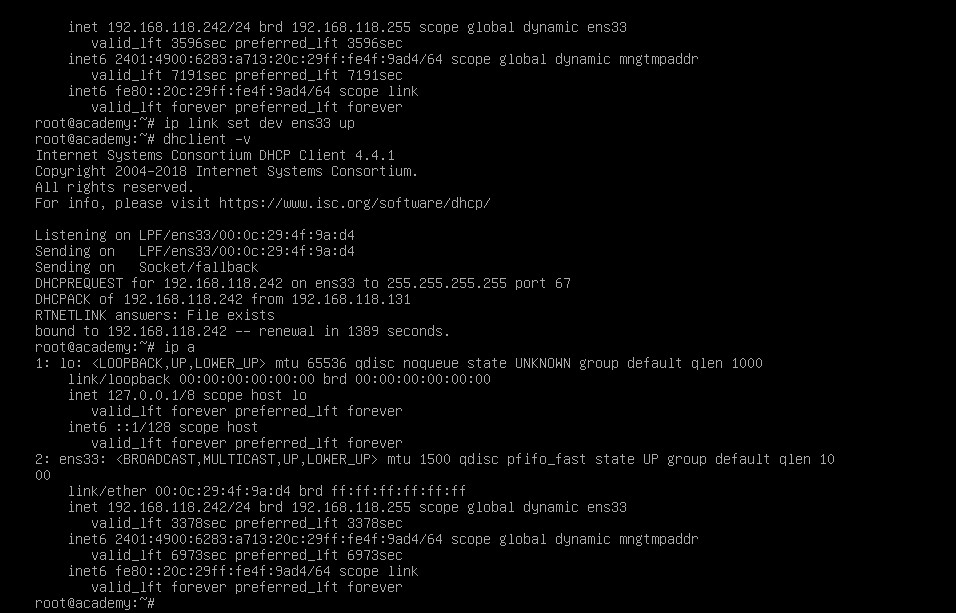
4.5. Enabling network in Academy Machine:

The network settings are disabled by default on a virtual machine (VM), which means that the VM won't have network connectivity, and it won't be assigned an IP address automatically. To enable network settings and assign an IP address to the VM, follow these specific commands

ip link set dev ens33 up

dhclient -v

ip a



After using those commands network is enabled in our academy machine and we get our Target IP address: 192.168.118.242

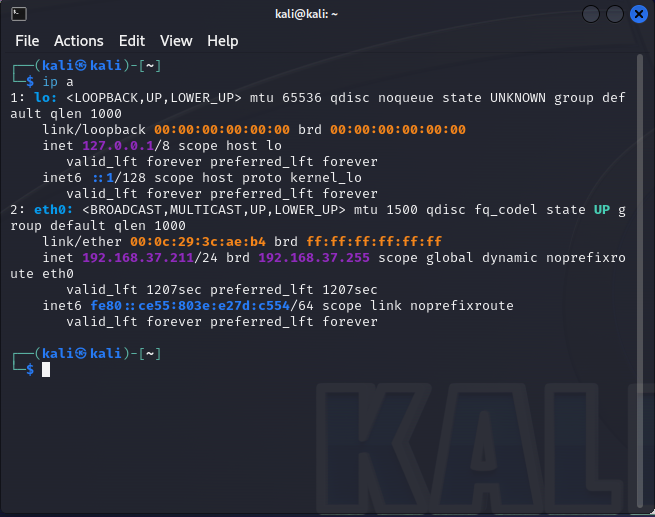
Now we need to find the ip addresses of both the Kali machine and Windows. and we need to check the same subnet of Ip address.

Target IP address (Academy): 192.168.118.242

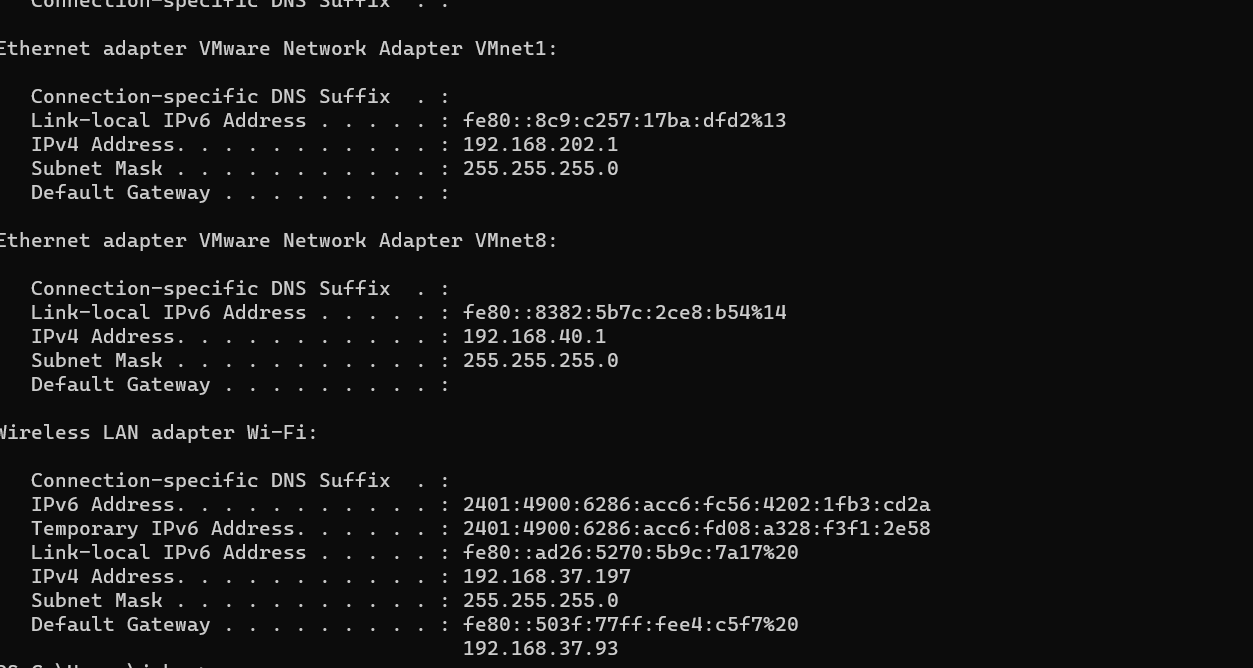
Attacker IP address (Kali): 192.168.118.211

Windows IP address: 192.168.37.197

4.6.Finding Kali IP address:

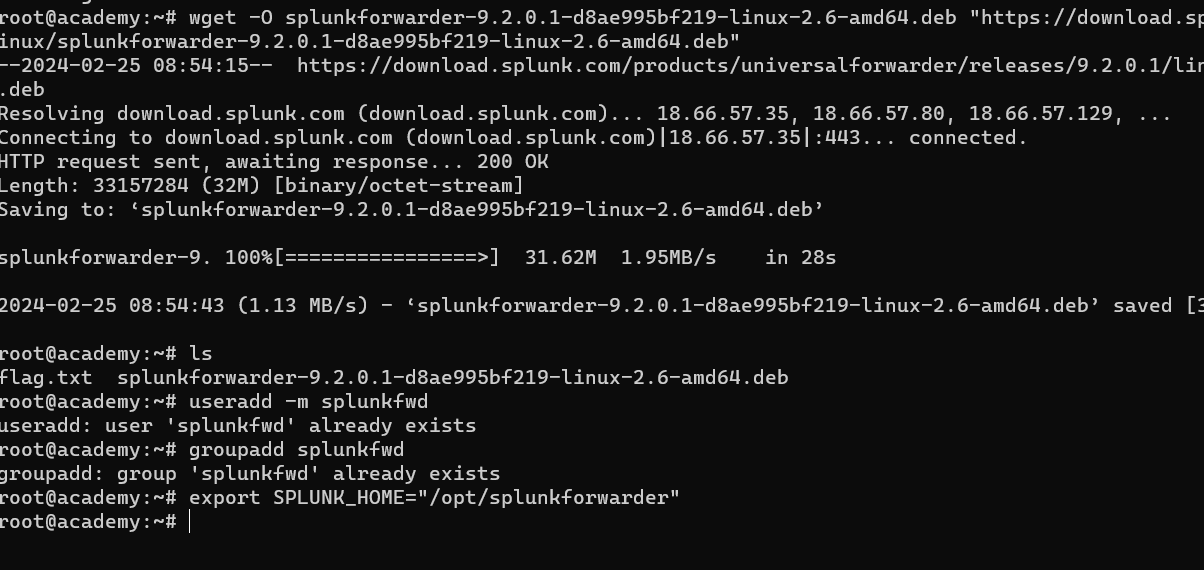


4.7.Finding Windows IP address:



4.8. Starting ssh in PowerShell:

Open Windows Powershell start the SSH server using the target machine's IP address and get the root access over there. Next, we need to install the ‘ Slunk Universal Forwarder’ in our machine by using the ‘wget’ tool.



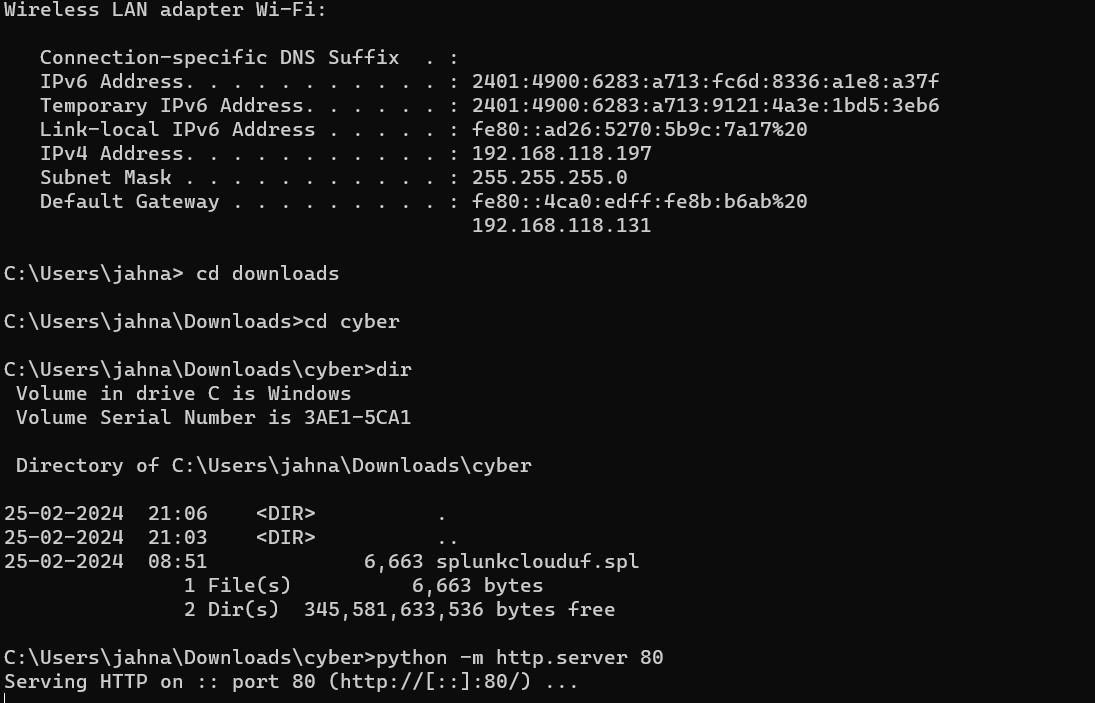
After it is downloaded and saved, we must install it and run it. Here by using ‘DPKG’ install the Splunk universal forwarder. The below image shows how it is done. After installing Splunk forwarder set a username and password.



Create a directory named cyber in your Windows machine and transfer the Splunkclouduf.spl to the directory.

After this, we will start a Python server. so for that first open your command prompt (Windows) and enter the command to start up the server in that directory. By default, this will run the contents of the directory on a local web server.

Python -m http server 80



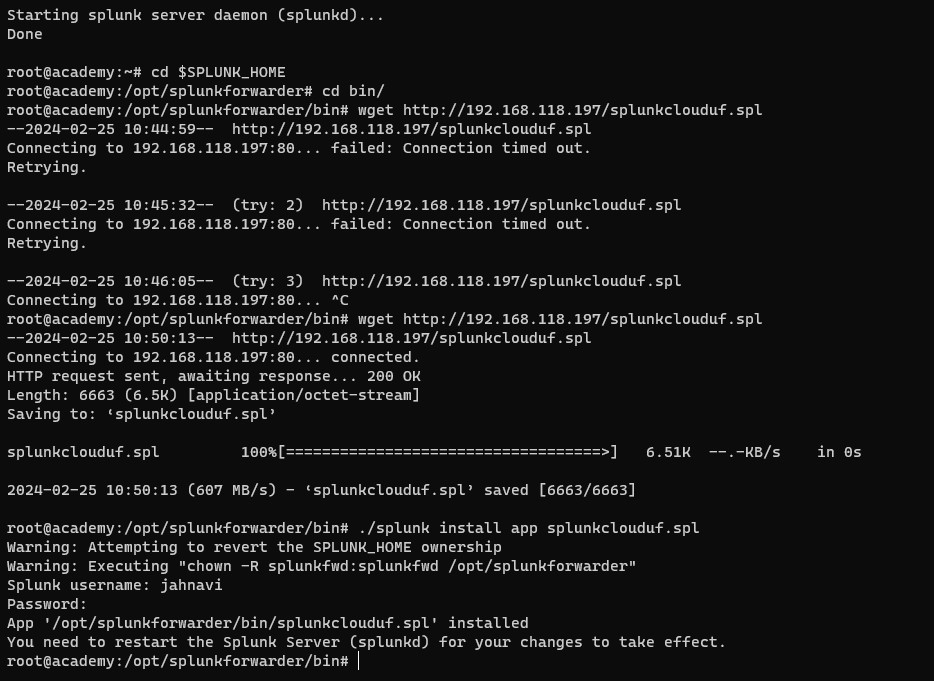
4.9. Implementing Splunk-Cloud

To monitor the forwarder logs, Splunk Cloud is accessed from a remote server.

After installing ‘splunkclouduf.spl’ , start the Splunk service by using ‘./splunk’.

Add the remote cloud servers' IP addresses to make it forward logs.

Till here the academy machine part ends and we can start using Kali Linux our attacker machine.



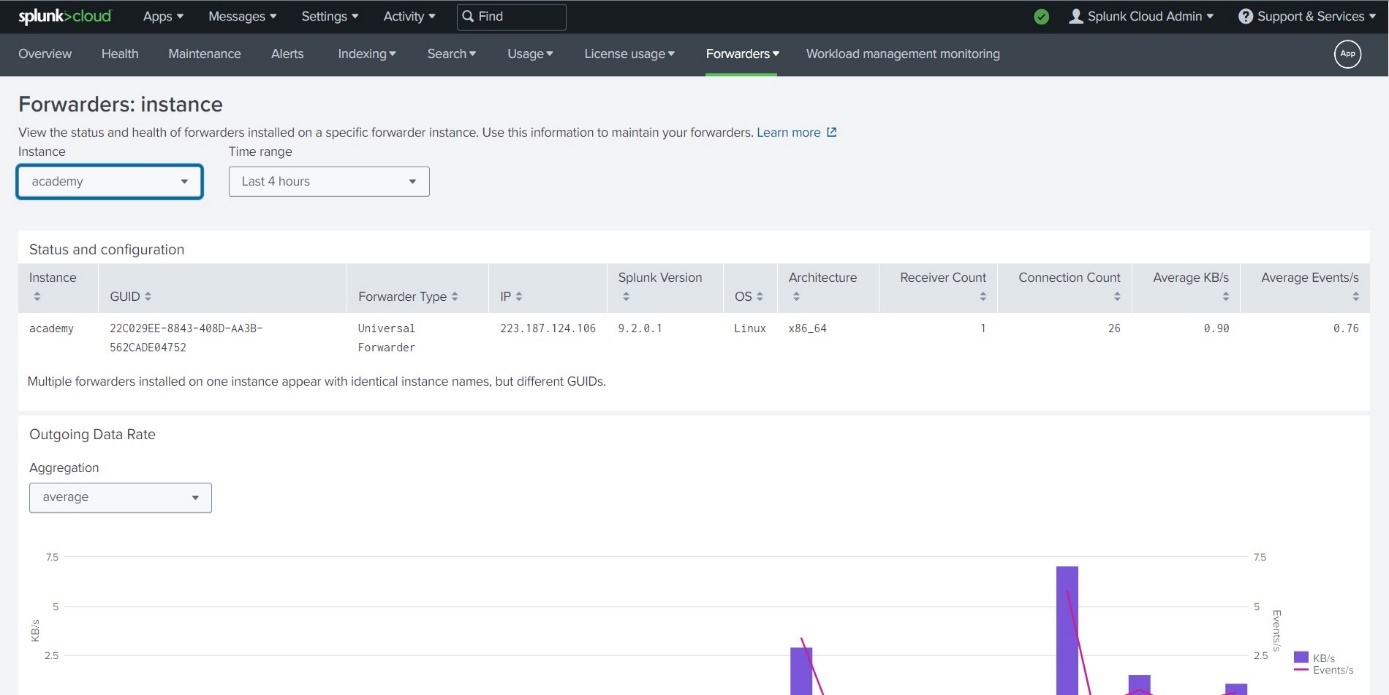
./splunk install app splunkclouduf.spl ,

./splunk list forward-server

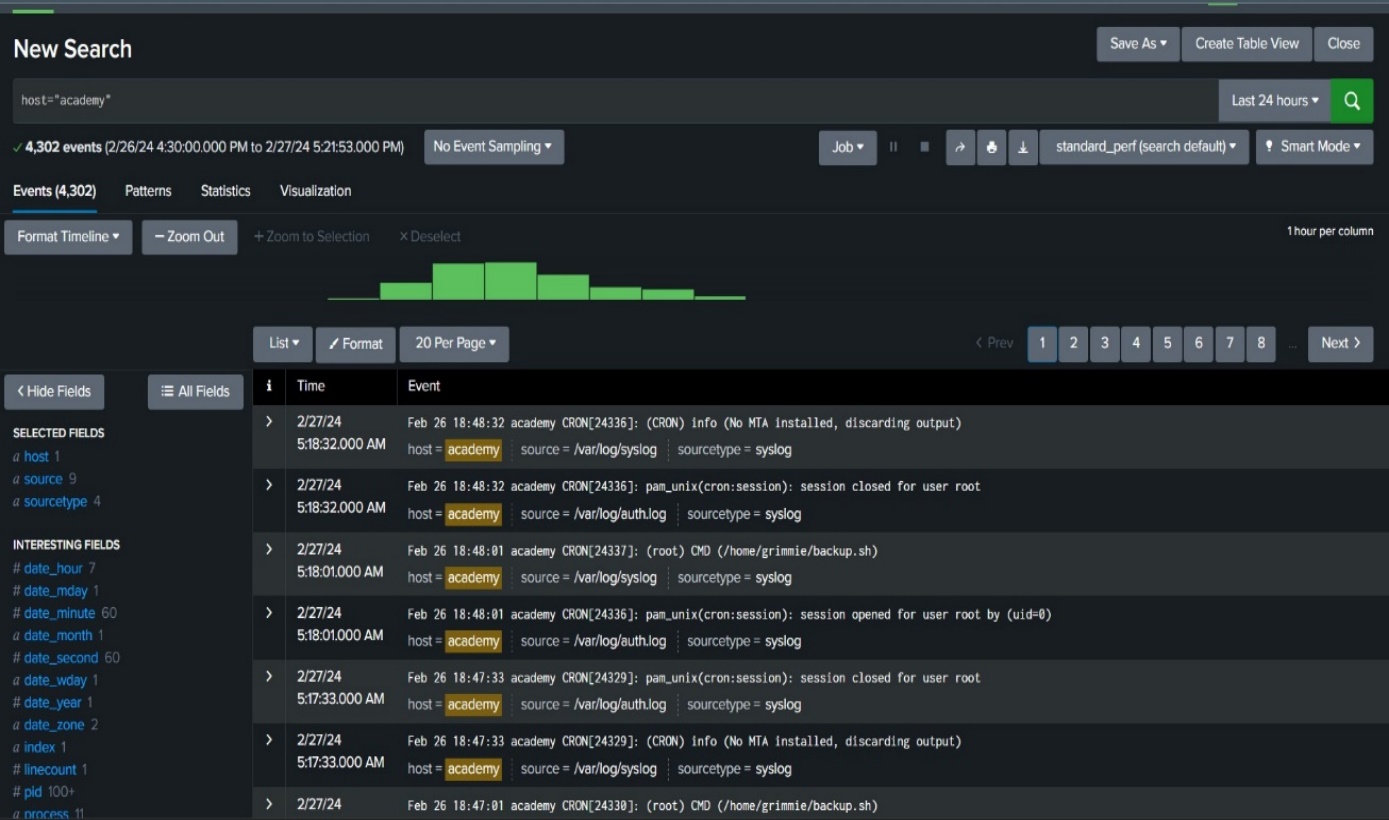
./splunk add monitor /var/log

./splunk restart

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



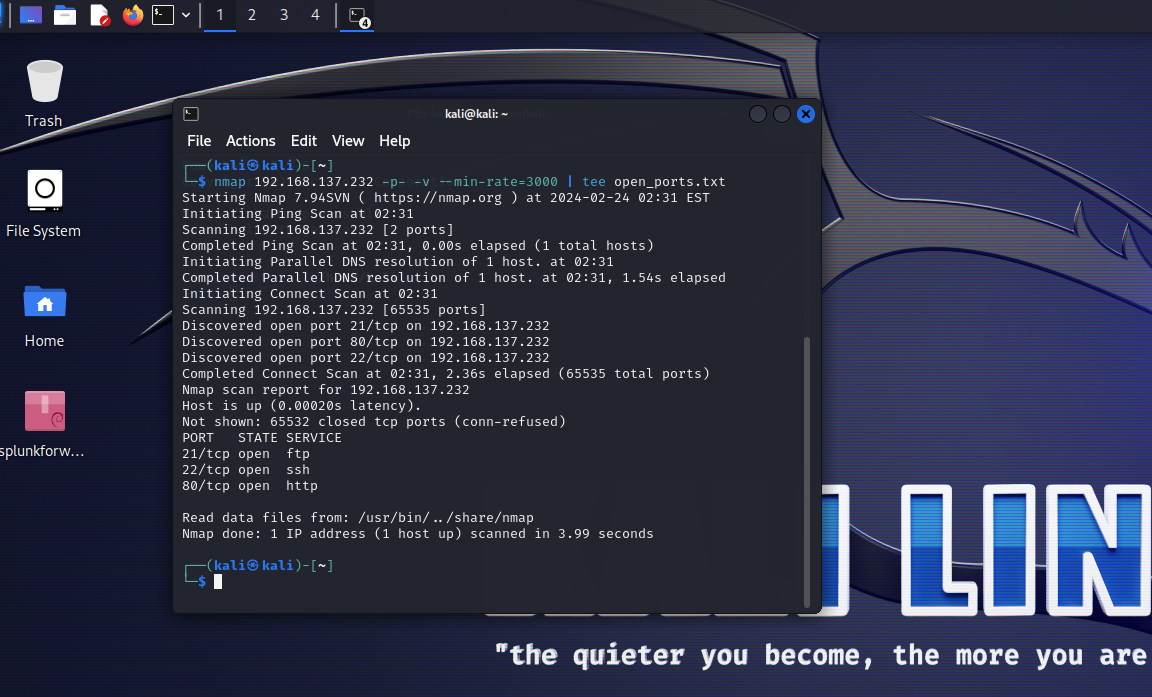
The Splunk cloud server contains the forwarder of the academy machine and we can find all the log information in the Splunk Cloud server. Through this we can detect the security threats in the academy virtual machine.



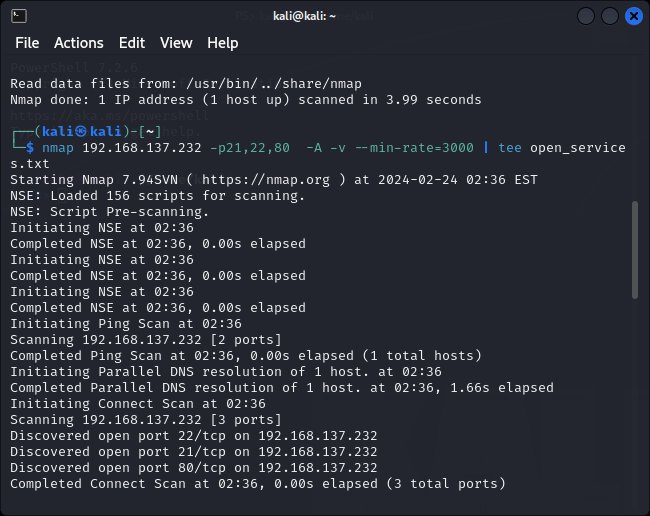
5. Vulnerability analysis:

Here we are going to use Nmap to find open ports and services and more details about the machine.

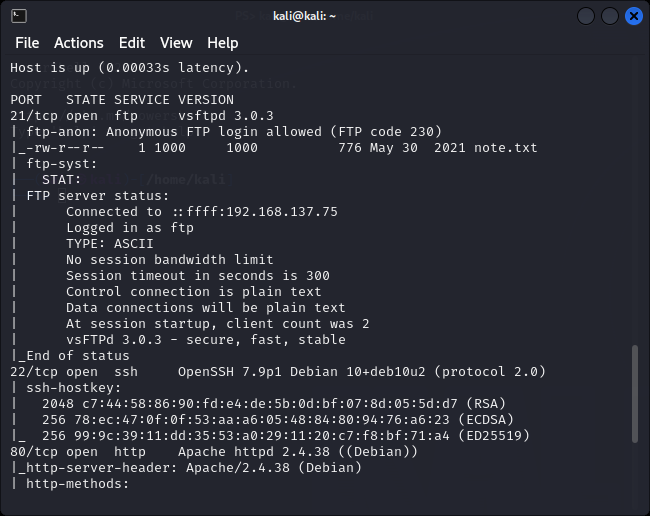
Nmap finds the available open ports and services in the target machine using the IP address.



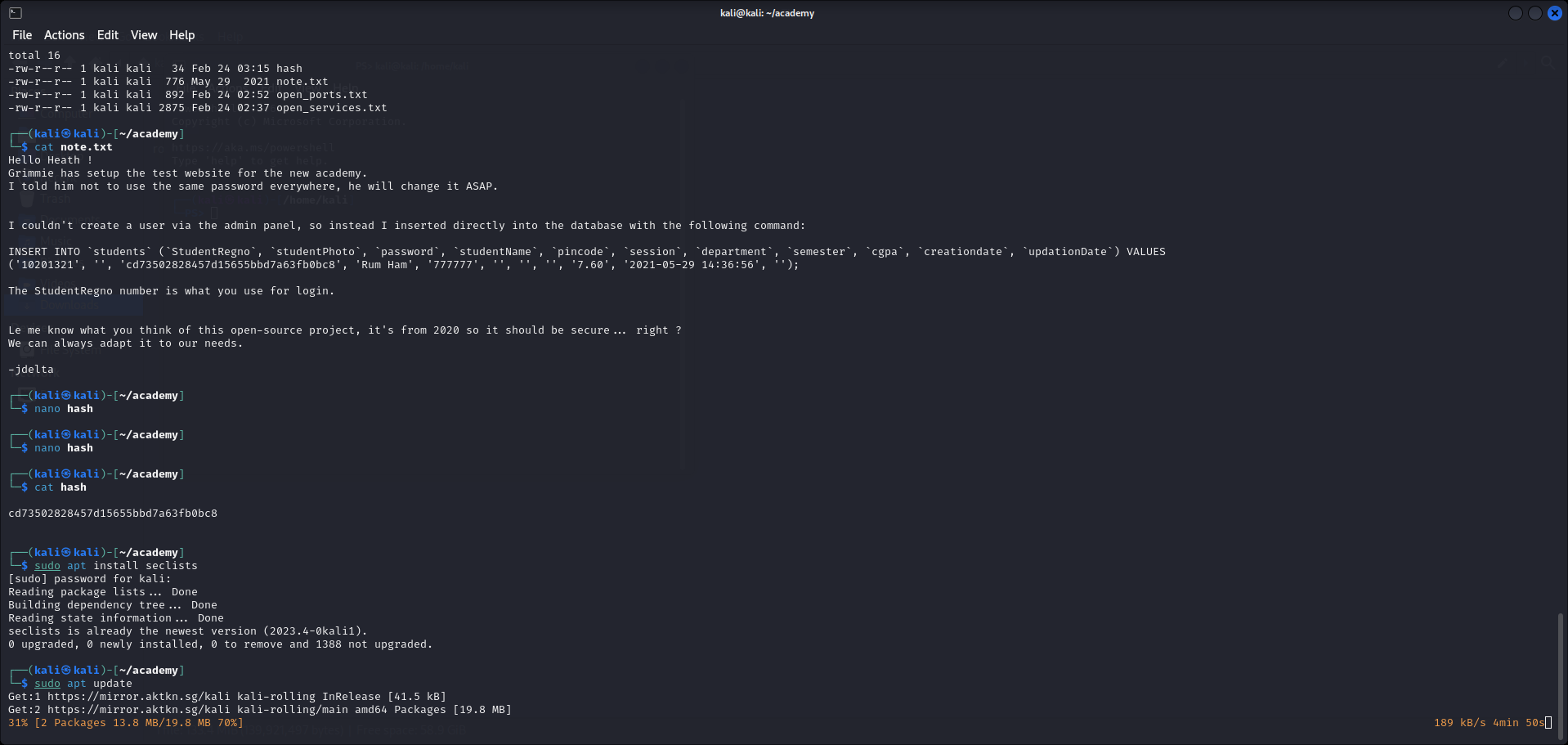
Here we can see that ports 21,22,80 are open and available to access.



Now to find out the username and password we will go with the FTP port. we find the login credentials for accessing the FTP service from the target machine.



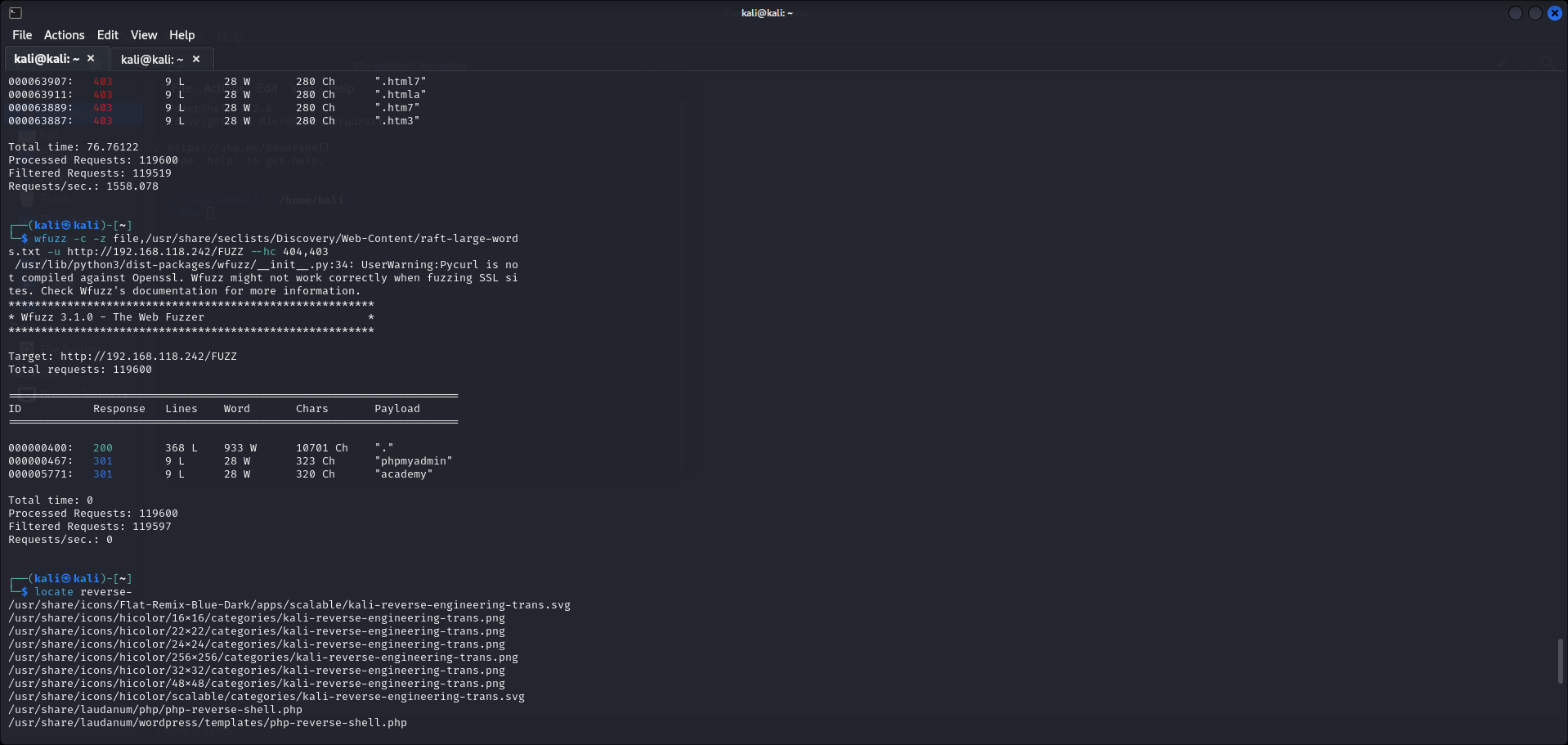
After login to FTP, Use the ‘get’ command to get the note.txt from the Academy machine. We will get a hash code in the note.txt file which will be used for login into the website which runs on the target machine IP address.



Save the hash code in the hash file. After this, we need to convert this hash code into a string using md5 decrypt.

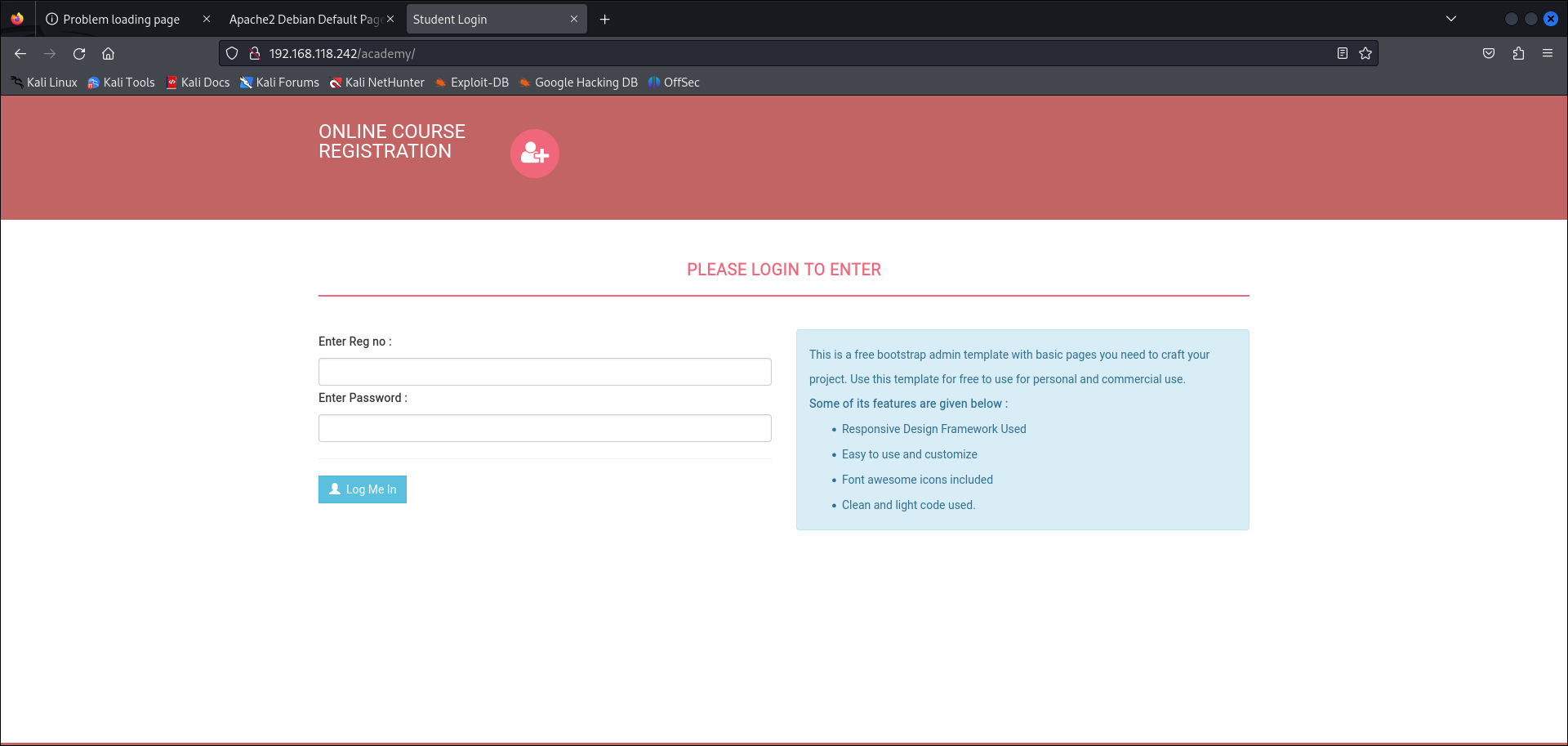
6. Vulnerability exploitation:

Here we will use WFUZZ which is used to discover common vulnerabilities in web applications through the method of fuzzing. Fuzzing is the concept of trying many known vulnerable inputs with a web application determine if any of the inputs compromise the web application.



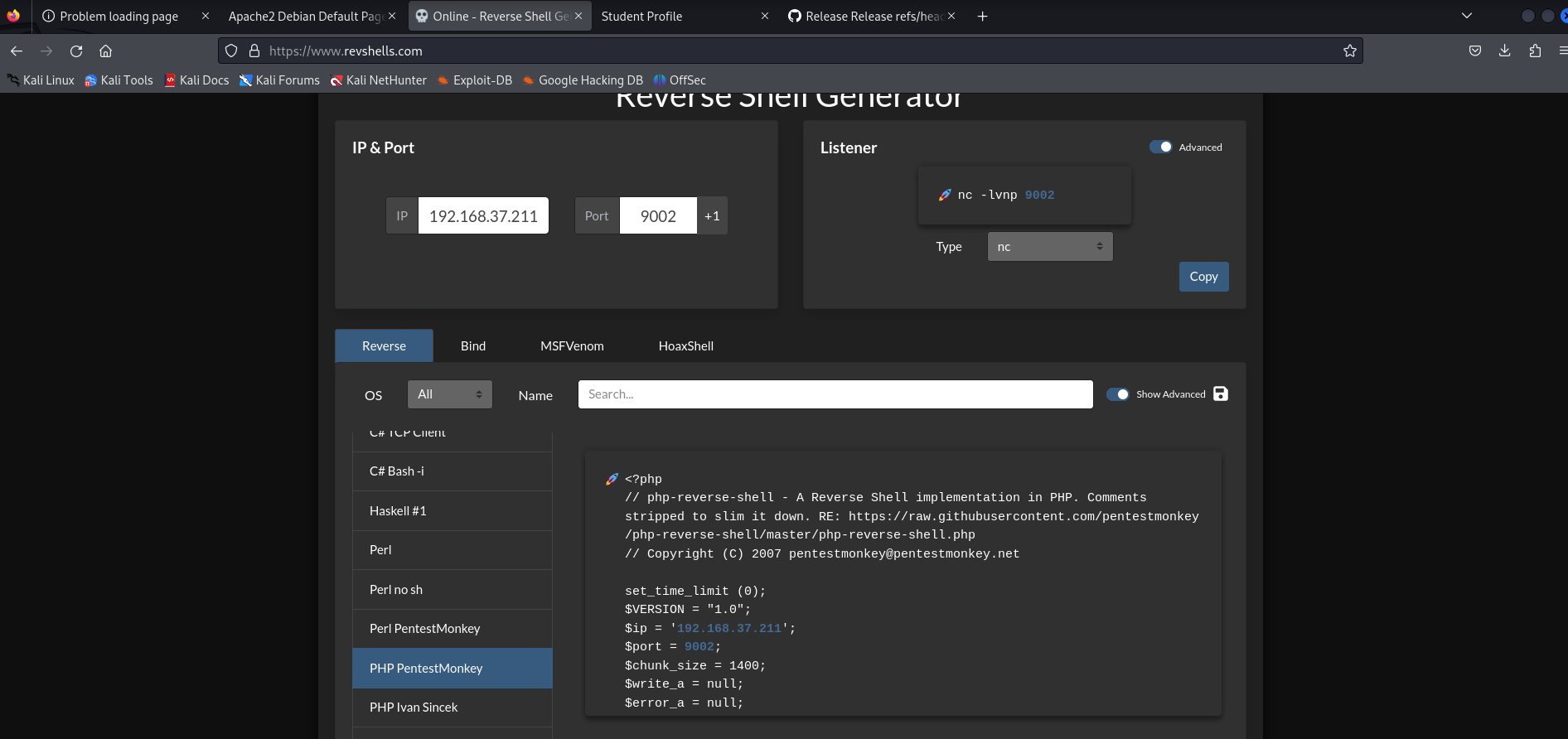
After executing the WFUZZ we will get the web page which can be used to get access to the site.

Use the student register number provided in the note.txt and the password ‘student’ which we got after cracking the hash value using md5 sum to log into the website.

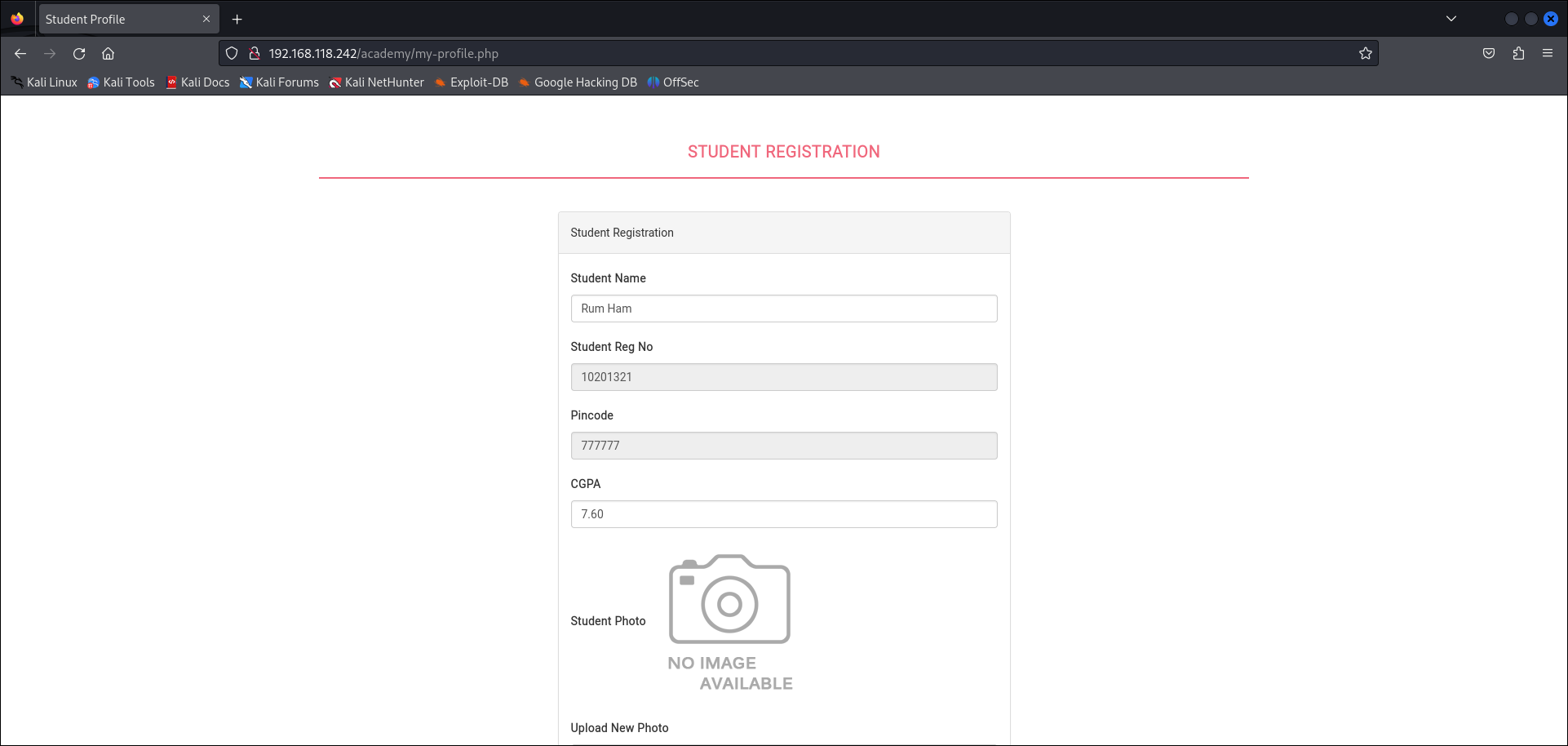


7. Reverse shell:

We use reverseshells.com to get the php file. Here we will use the attacker machine IP address and port to generate the php file.



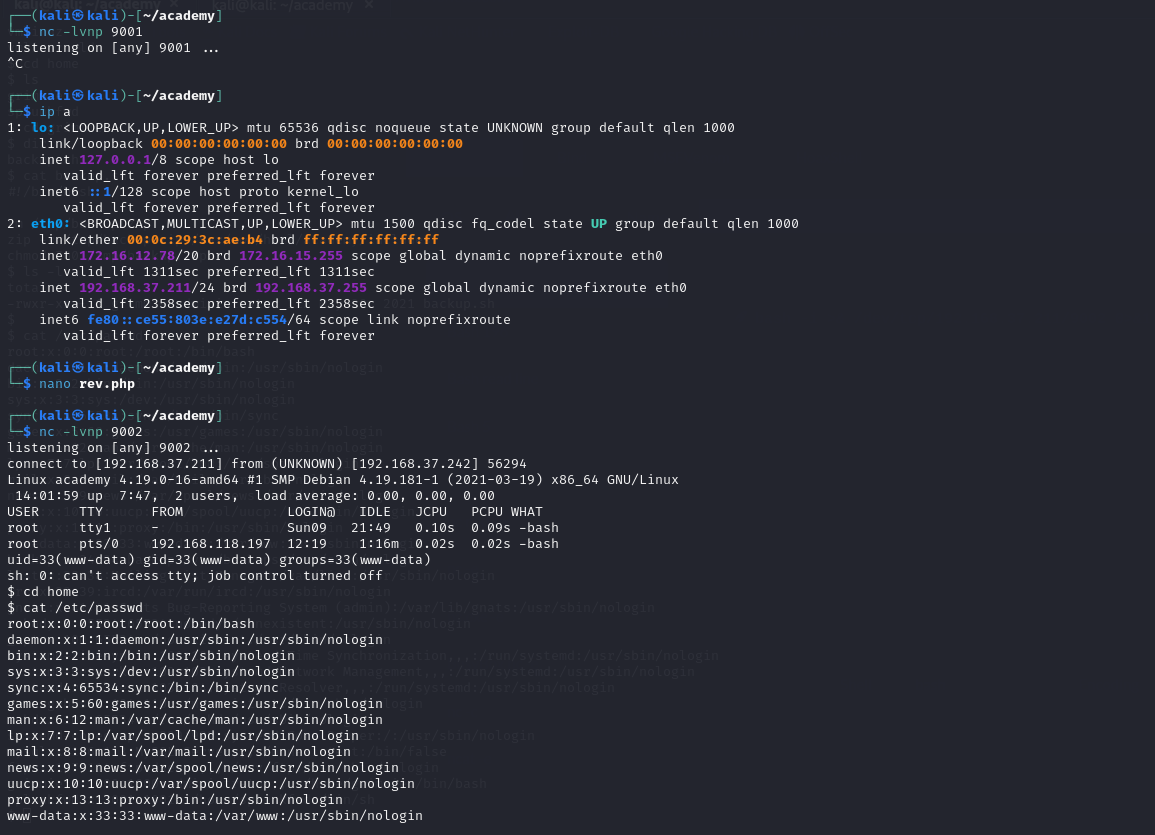
Upload the file in the upload photo field, we must submit the PHP file to the website that will be stored on the web server. Then we will gain remote access to the academy virtual machine.



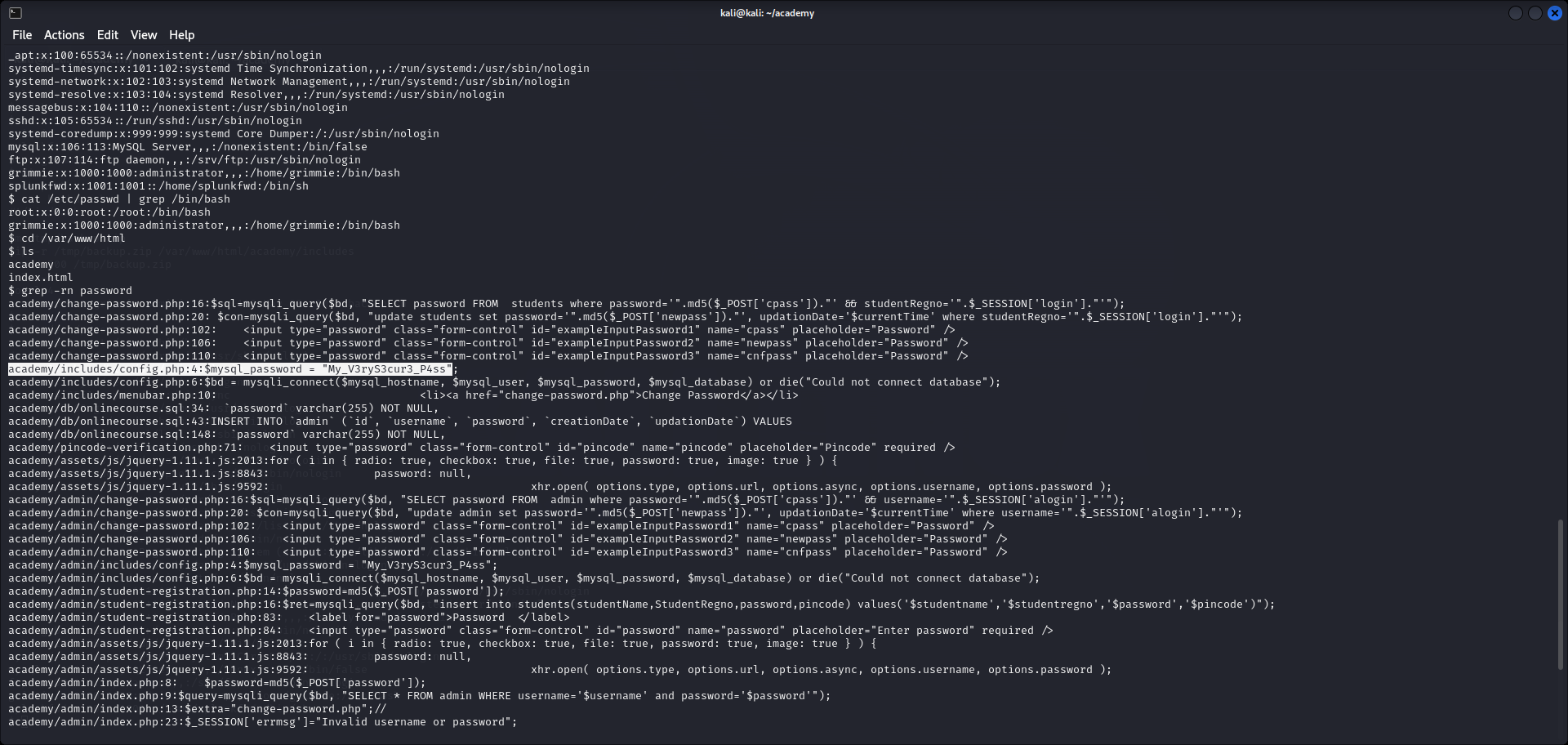
After updating the student profile we will get remote access to our academy machine

8. Gaining user access:

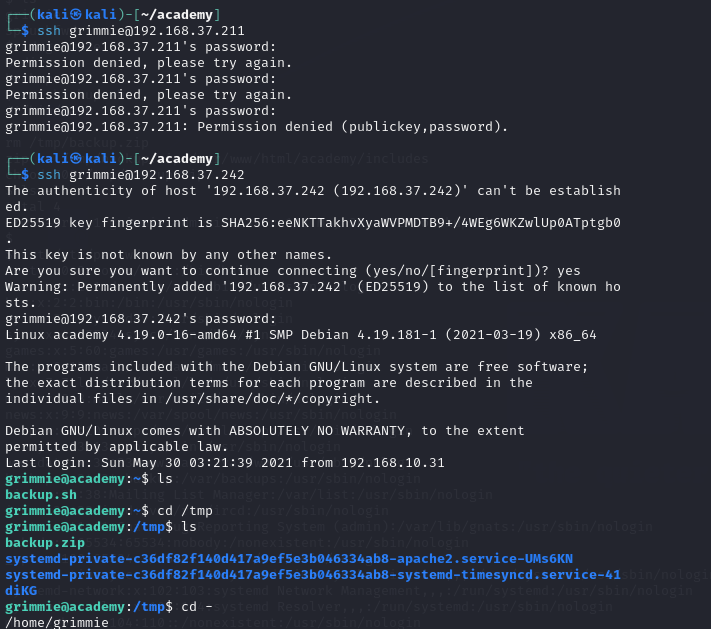
Here we will check the list of files and directories and also check for the users in the academy machine. We found two users root and grimmie .



Enter into the academy directory and search for the password using the grep command ‘grep -rn password’ and we got a password and now we are going to save all these findings in a text file named ‘findings.txt’.

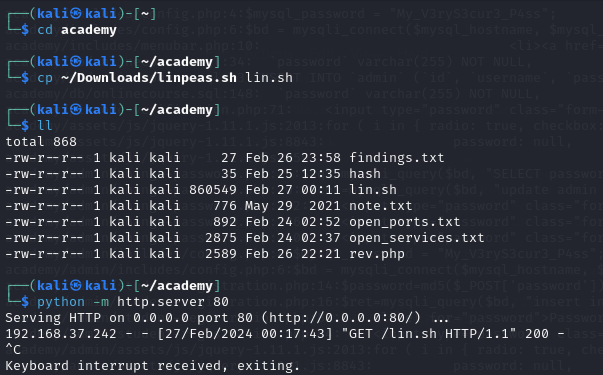


Start the SSH using the academy IP address for running user grimmie, ssh ‘[grimmie@192.168.37.211](mailto:grimmie@192.168.37.211)’, after entering the password we can successfully login as grimmie.



Now we are going to download the linpeas file from the GitHub repository. Linpeas file will be downloaded in the Kali machine so, we using a Python server to transfer this file to the academy machine.

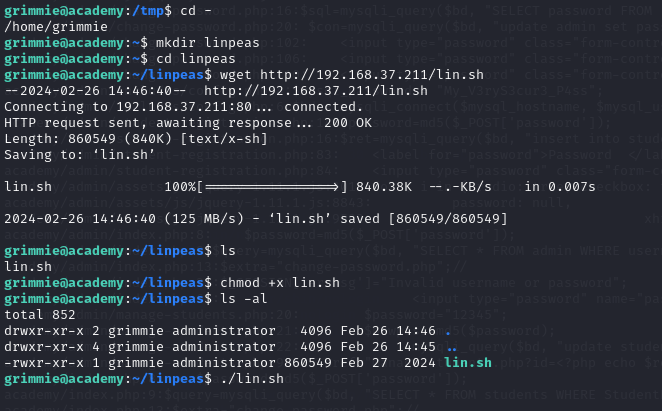




9. LinPEAS:

LinPEAS - Linux Privilege Escalation Awesome Script

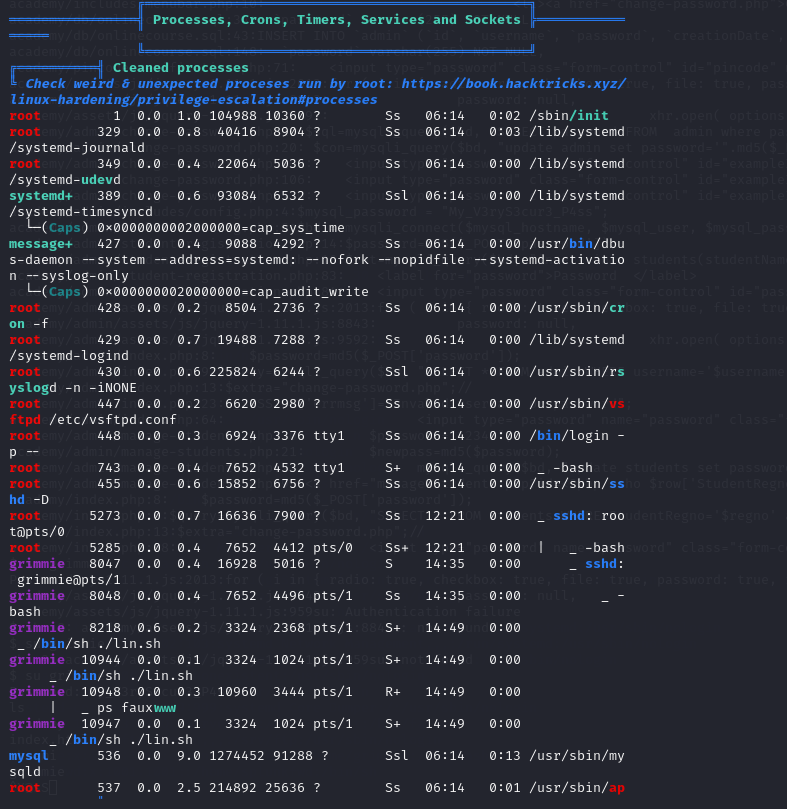
LinPEAS is a script that searches for possible paths to escalate privileges on Linux. Privilege escalation is the act of exploiting a bug, design flow, or configuration in an application to gain elevated access to resource.

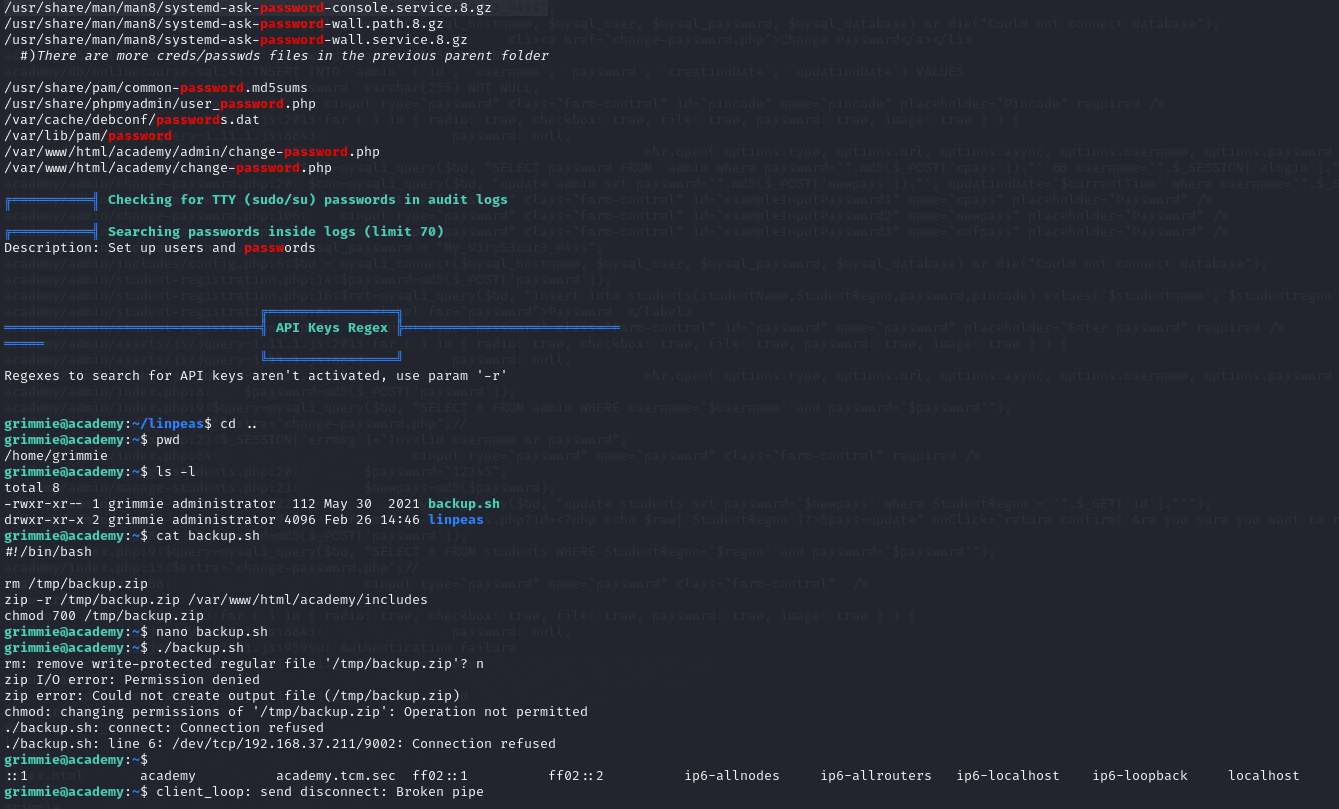


We change the file permissions of the LinPEAS file to the executable file and execute lin.sh in the academy machine.

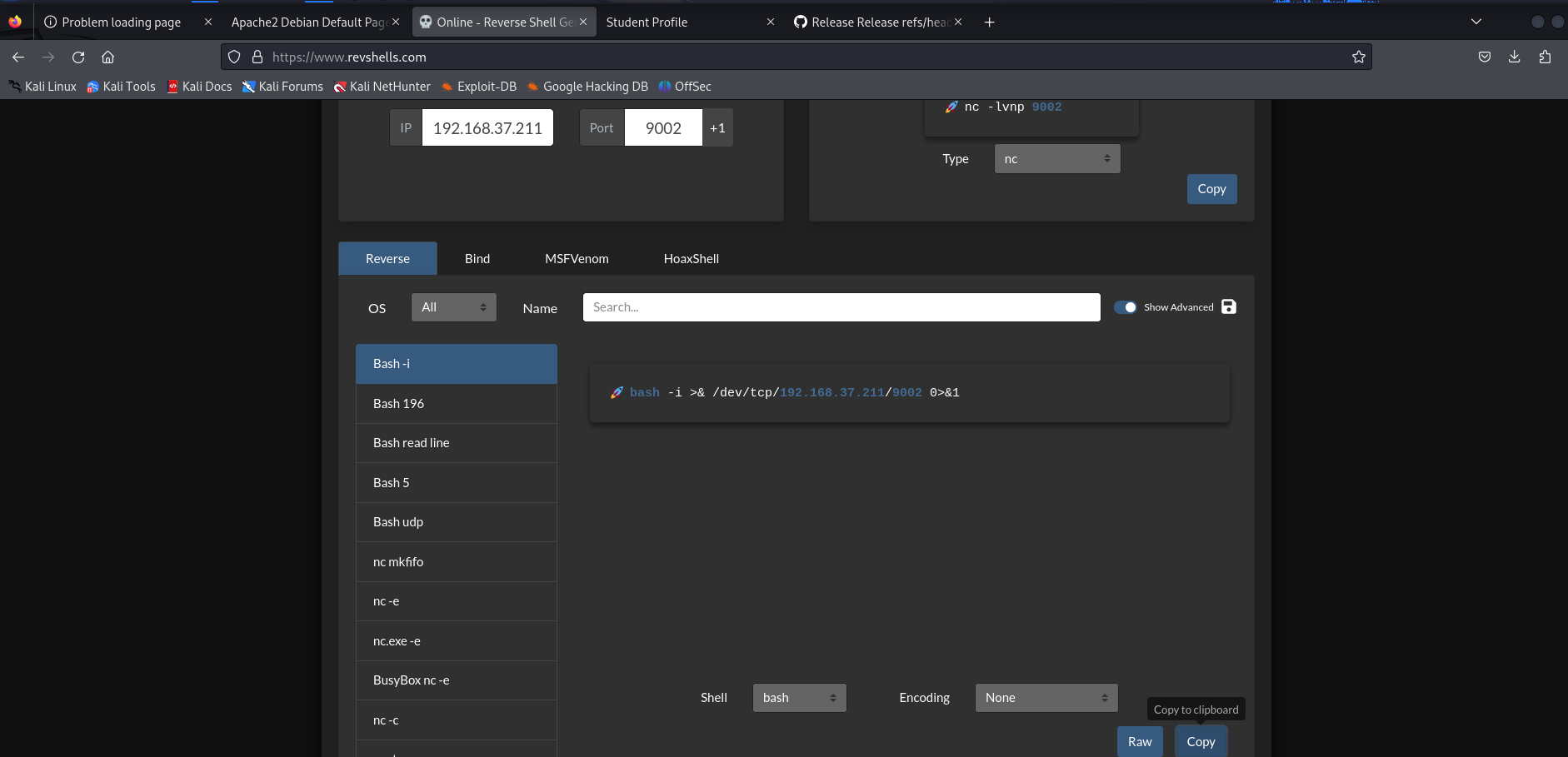








By using reverseshell.com , we got a bash command which is added to the backup.sh file that we have found in the home directory and we are going to add and execute the ‘nc -lvnp 9002’ command after that we execute the file.



One of the administrators started so, we automatically got the root access to the academy machine.

10. Gaining the root access:

Finally, the academy virtual machine is exploited and gained the root access. Now we can access all files available in academy virtual machine.

