**VULNERABILITY ASSESSMENT AND PENETRATION**

**TESTING REPORT**

revuripenchalasujith.cse2021@citchennai.net

**210421104127**

**OUTLINE**

1.Vulnerability Assessment and Penetration Testing

1.1 Introduction

1.2 Objectives

1.3 Requirements

2.Methodologies

3.Methodologies

4.Setting up academy virtual machine

4.1Download the academy file in the system

4.2Splunk Installation

5.Setting up the kali machine

**1.VULNERABILITY ASSESSMENT AND PENETRATION TESTING**

**1.1 INTRODUCTION:**

VAPT, short for Vulnerability Assessment and Penetration Testing, is a thorough process for finding and fixing security weaknesses in computer systems, networks, and applications. Vulnerability Assessment (VA) detects potential flaws using tools and manual checks, while Penetration Testing (PT) simulates attacks to evaluate system defenses. Overall, VAPT helps assess and enhance system security against real-world threats.

**1.2 OBJECTIVE:**

1. Download the Academy VM from [here](https://drive.google.com/file/d/1hXEWVXfVYMUaJeo8uu5vz9kt8RwTwcsg/view?usp=sharing)

2. Unzip the 7z file using winrar/winzip/7z to get the VMDisk files

3. Open the VMware Player, select Open VM, and then select the extracted VM

4. Edit the VM and change the network settings to Bridged before switching on the VM

5. Use the username and password in the root password.txt file to log in

**Note:** By default, this VM's network settings will be disabled. So, there won't be any IP Address

6. Search the web, and find the solution to turn on the network device ens33 (Hint: unix.stackexchange.com)

7. Once you get connected to the internet, configure your own SIEM Cloud instance in this machine so that any malicious activity can be monitored and tracked

8. Once the SIEM instance is configured, make sure you enable the log files and add the respective directory to the monitor list.

9. Make a note of the IP Address of the VM, exit to the root login page by simply typing 'exit' on a terminal

10. Now, Go to your Attacker machine, use all the skills that you have learned till now, break into the system, and find the root flag

**3.METHODOLOGIES:**

Vulnerability Assessment and Penetration Testing (VAPT) includes several key methodologies:

* Enumeration: Identifying active hosts, ports, and services on a network.
* Scanning: Using tools to search for vulnerabilities and weaknesses in systems and networks.
* Exploitation: Attempting to exploit identified vulnerabilities to gain unauthorized access or perform malicious actions.
* Post-Exploitation: Assessing the extent of access gained and potential damage that could be inflicted.
* Reporting: Documenting findings, recommendations, and remediation steps

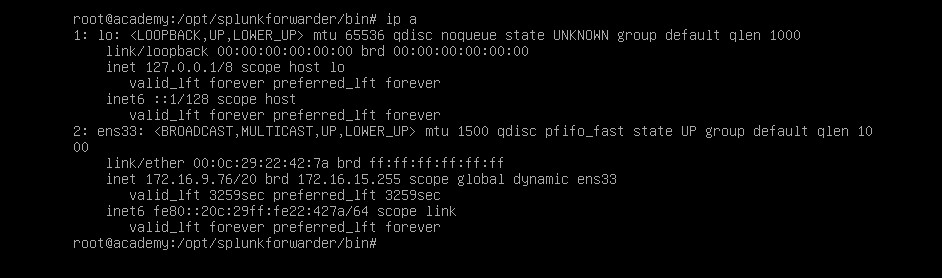
for stakeholders

**4.** **Configuring the Academy Virtual Machine within VMware:**

* Upon launching the Academy Virtual Machine within VMware, proceed by entering your login credentials.



* To locate the IP address of the Academy Virtual Machine, execute the following commands:
* **ip link set dev ens33 up**: This command activates the network interface named "ens33". It's like switching on the network connection.
* **dhclient -v ens33**: This command requests an IP address for the "ens33" interface from a DHCP server. It's like asking for a unique address on the network so your virtual machine can communicate with other devices.
* **ens33:** This is the name of the network interface on your virtual machine. It's like the label for your network connection.
* Get the ip address of academy machine by using the command.
* **ip a**: This command quickly shows the IP address and other network details of the machine

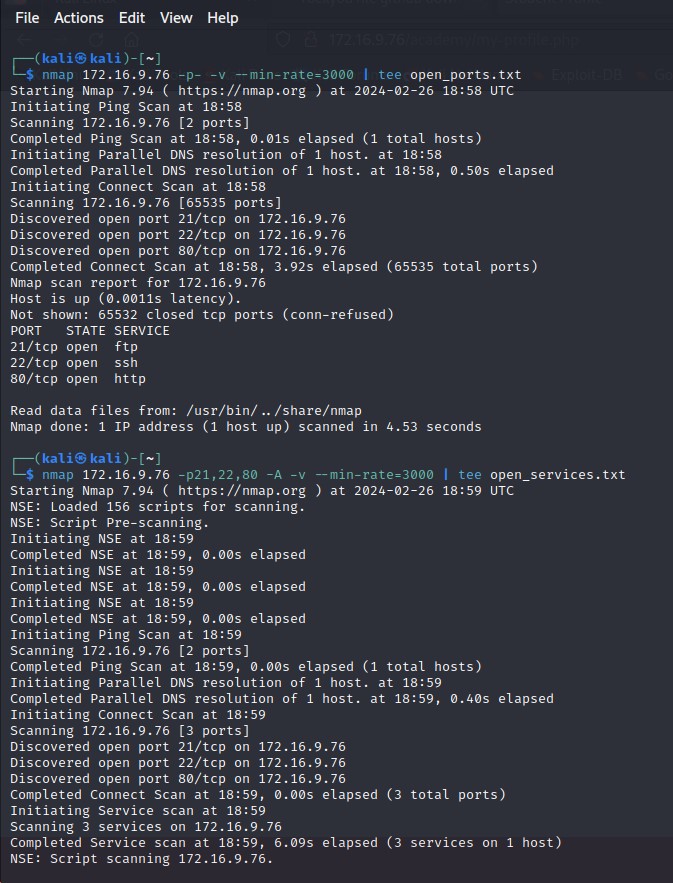


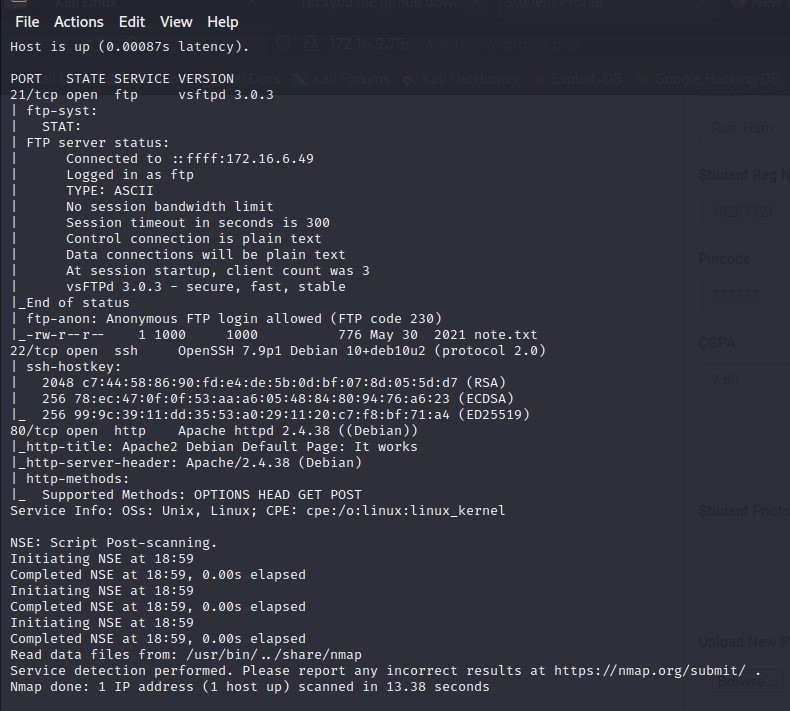
**4.2 Splunk Installation:**

* Download the Splunk Forwarder onto the Academy Machine using the following commands:
* 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>
* useradd -m splunkfwd
* export SPLUNK\_HOME="/opt/splunkforwarder"
* 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
* After commands are given the splunk is downloaded successfully in the academy virtual machine
* Note the ip address of the 3 machines in the system i.e. for windows machine, kali and academy virtual machines.
* Windows ip address: 172.16.6.42
* Kalu ip address: 172.16.6.49
* Academy ip address : 172.16.9.76

**5.Configuring the Kali Virtual Machine:**

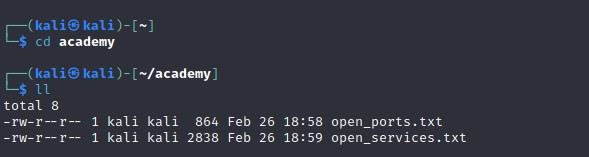
**5.1 NMAP :** Nmap, short for "Network Mapper," is a powerful open-source tool used for network exploration and security auditing. It finds out who's there, what they're doing, and what kind of computers they're using.

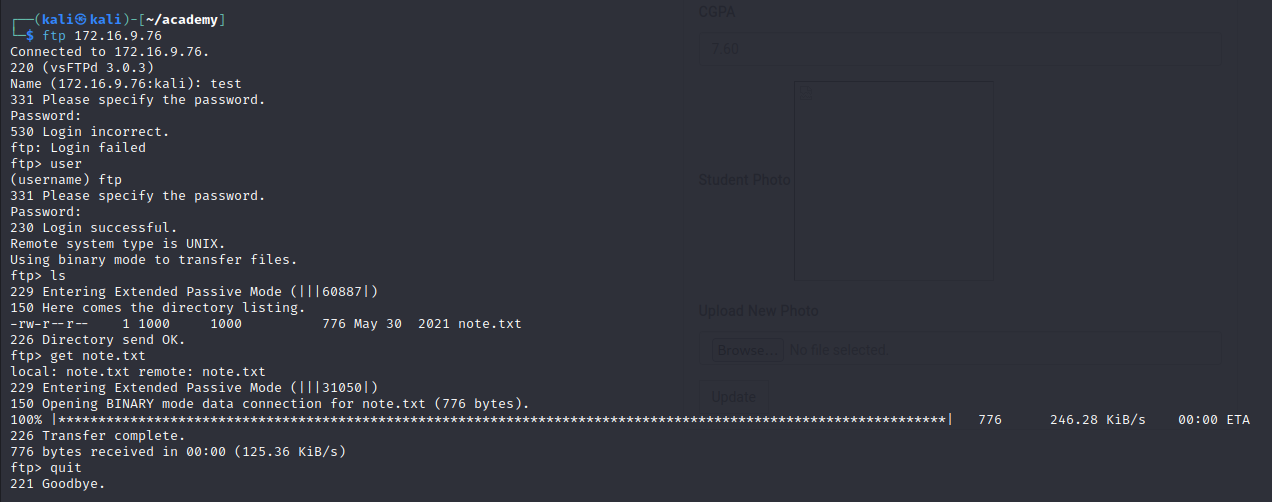




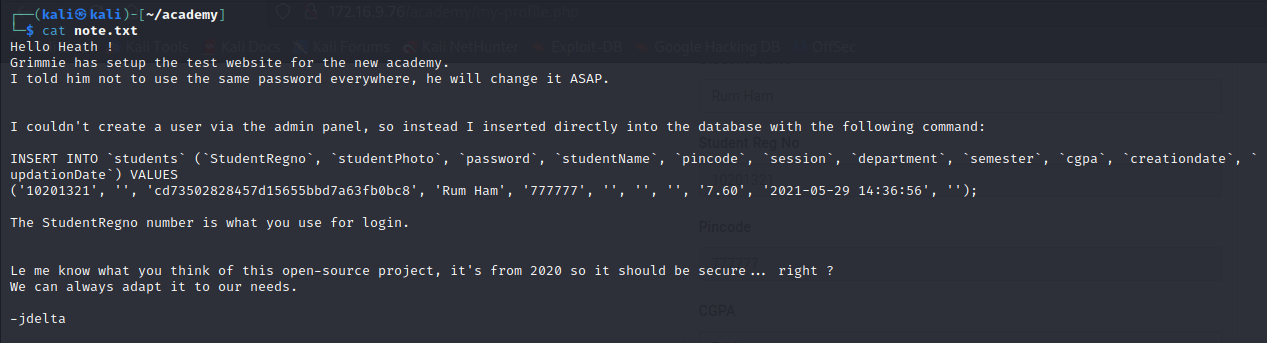
**5.2 Create Academy Directory**

* Next , create a academy directory by using the following command**:**
* **mkdir academy**: This command creates a new directory named "academy".
* **cd academy**: This command changes your current directory to the "academy" directory.
* **ll**: This command lists the files and directories in the current directory**.**

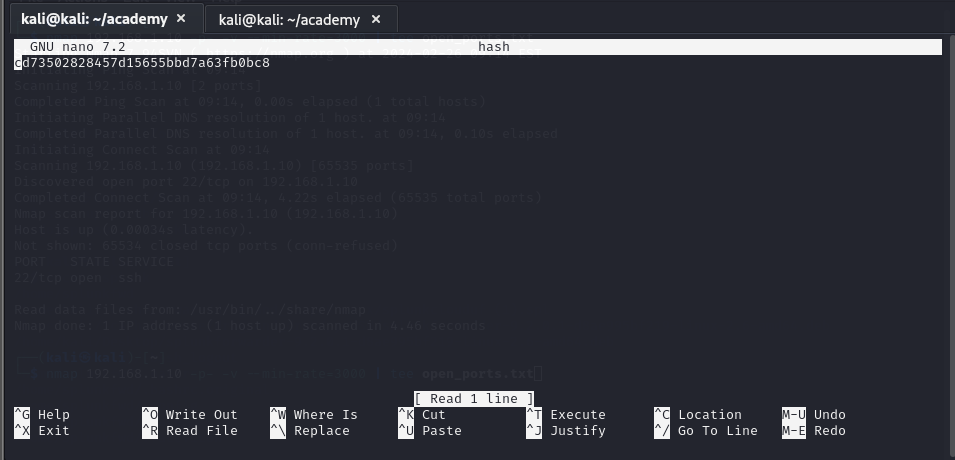




We have to check the content in the note.txt.file



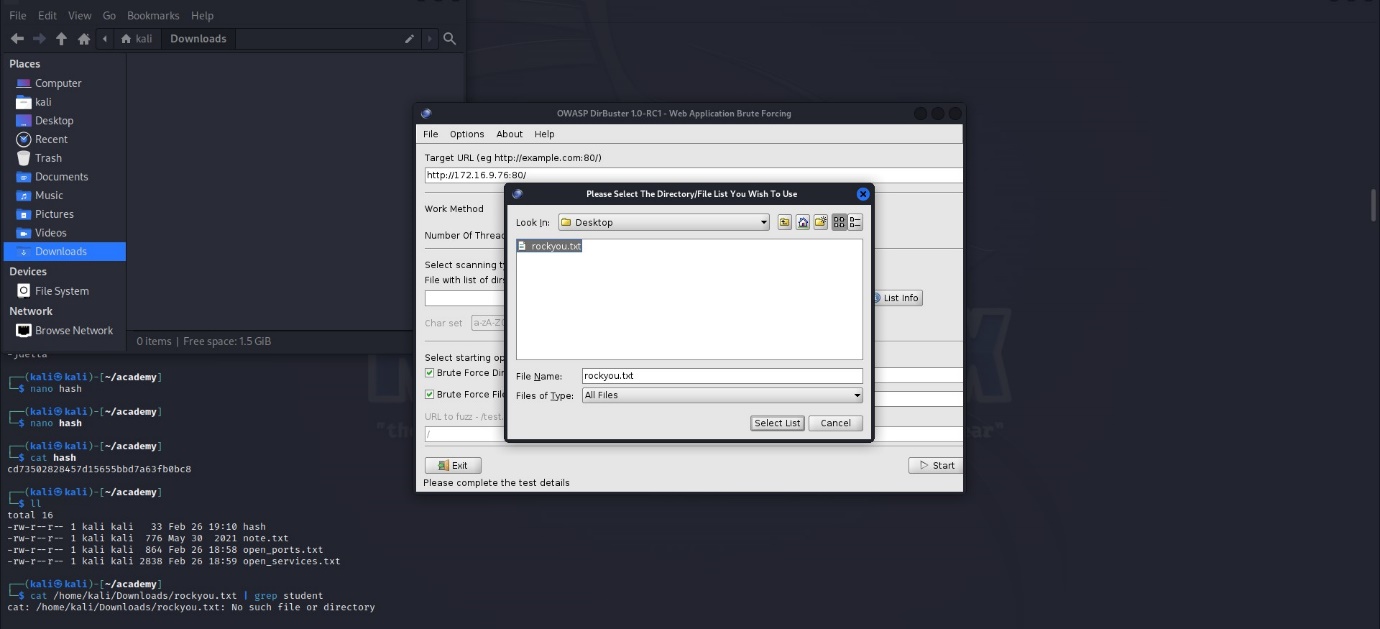
Copy the hash then create the new file “ hash” then now paste by using the “ nano command”



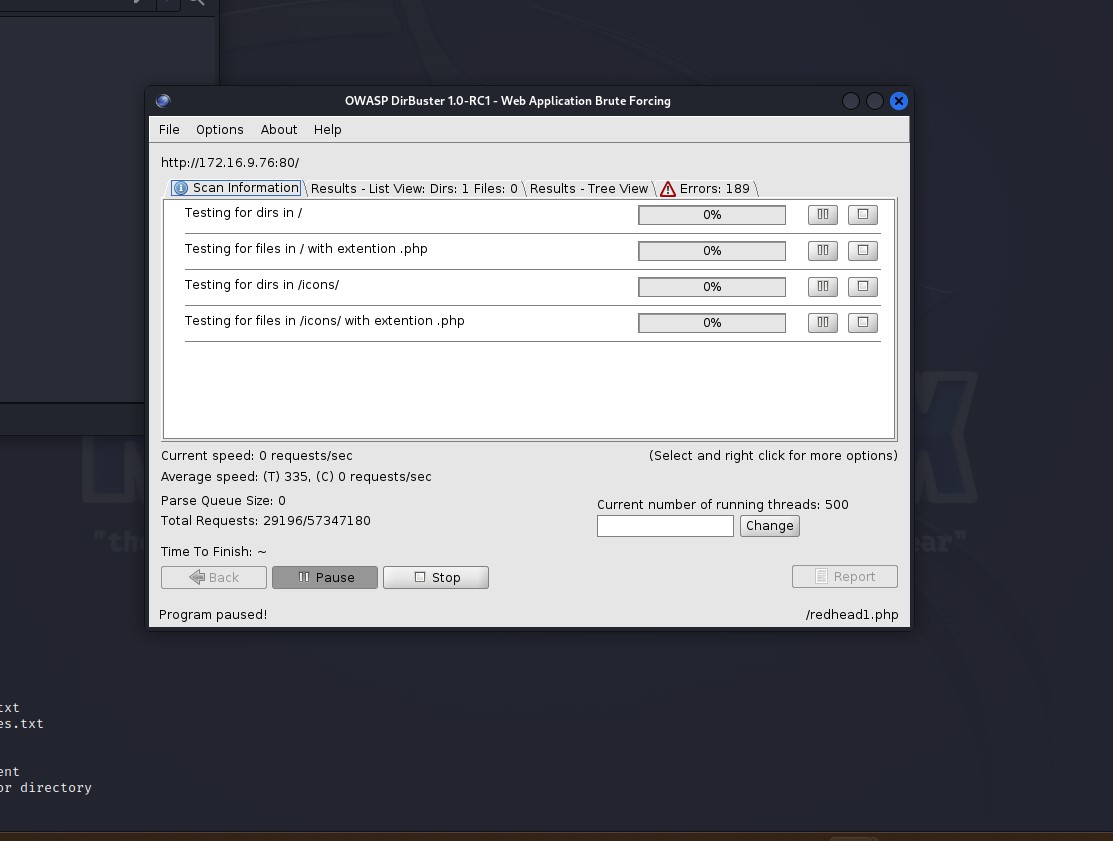
**5.3 DirBuster:**

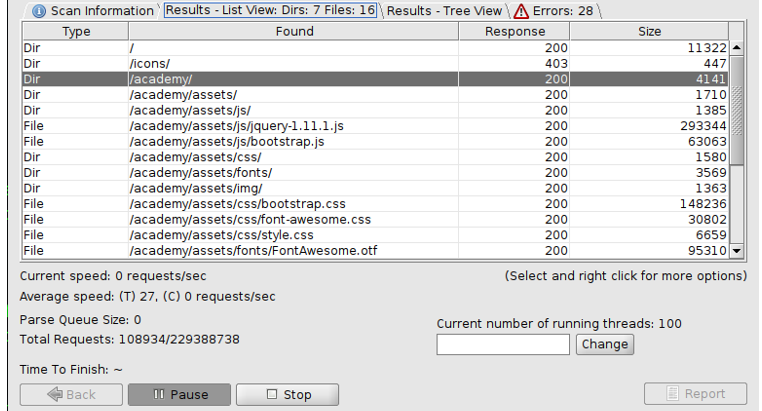
Use Dirbuster tool. Provide the target ip-address in the required box in the format = <http://172.16.9.76:80/> and use the wordlist “rockyou.txt” as the dictionary attack file or the list based brute force attack method with it’s directory inorder to decode the password.

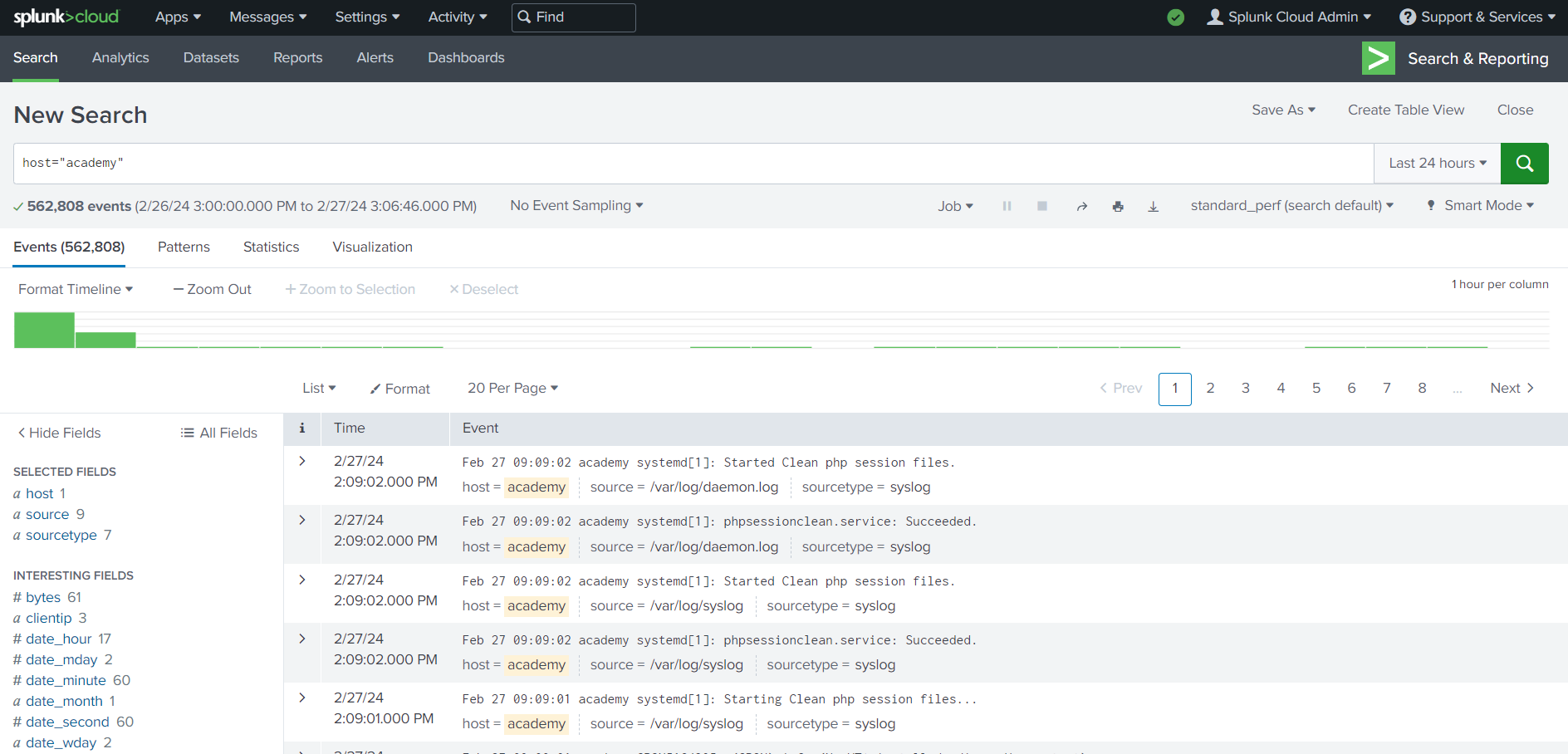
And click start.

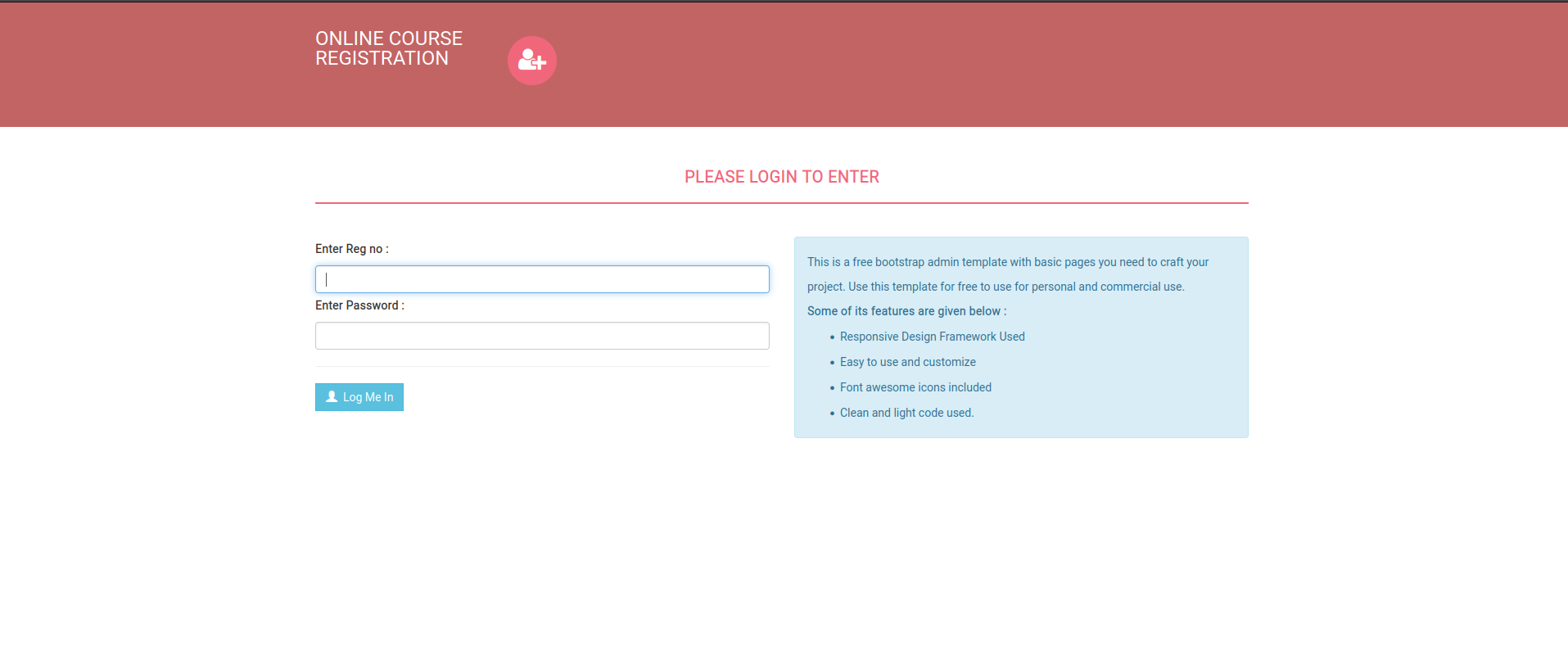


After it runs for a period of time. Navigate to the Result menu bar in the top right and search for /academy with 200 response code. Right click on it and open in browser.



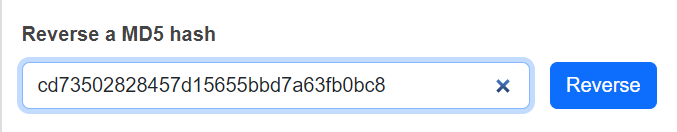


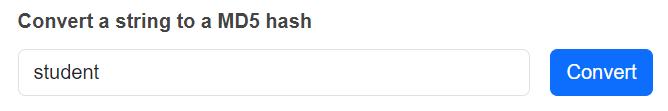




**Login to the website:**

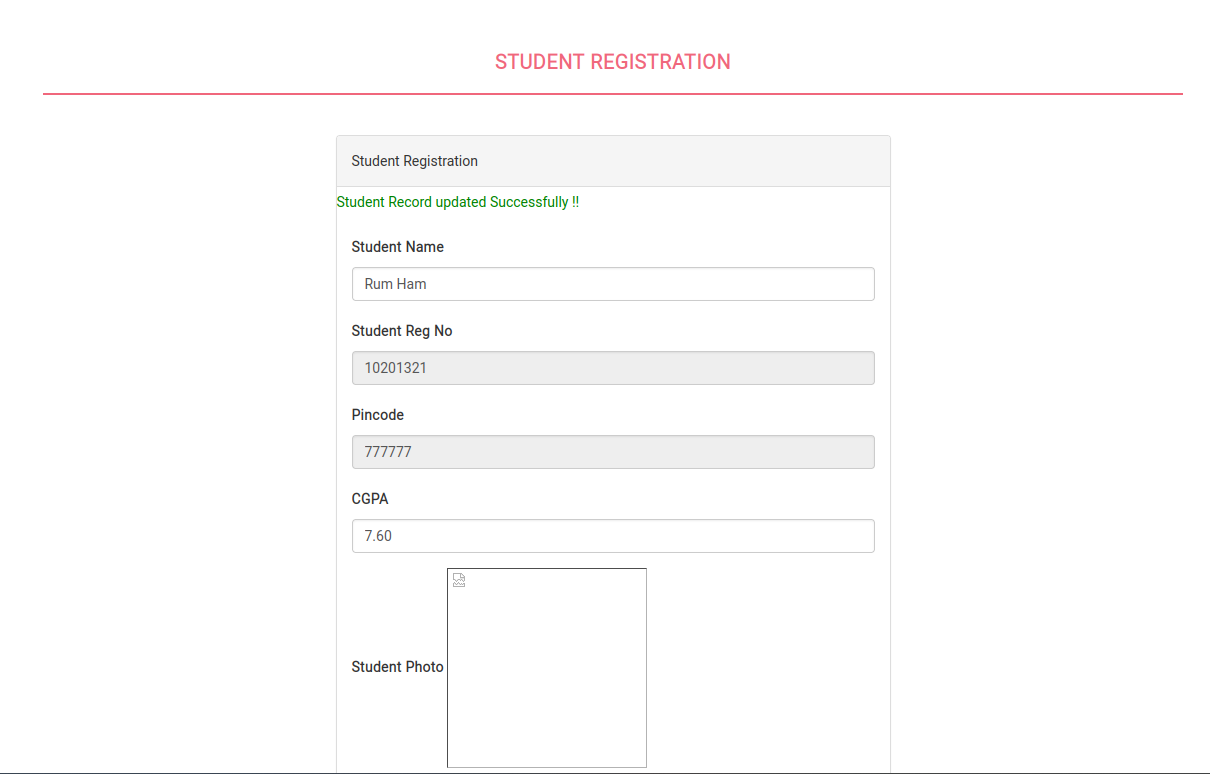
Find Login DetailsTo find the login details and password, open note.txt and copy the user name .The password is in the hash format so convert to using md5 gromweb website



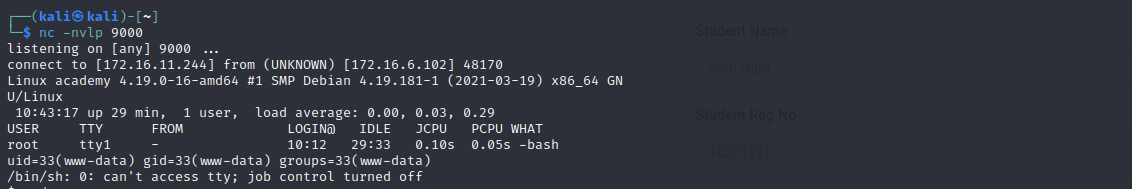


**REVERSE SHELL**

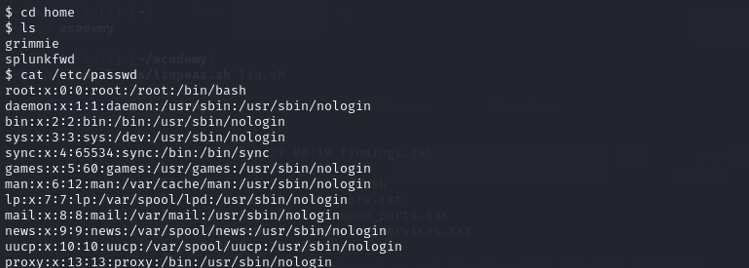
* Open reverse shell in firefox and give the IP address of academy
* Now open the PHP system and copy the command and paste in the new file in the academy directory which is rev\_1.php
* Now upload the rev.php in the myprofile page and there will be success message



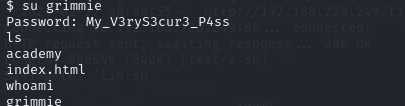
* Now the access came for the website



* Now open home directory and check the context in /etc/passwd
* cd home
* cat /etc/passwd



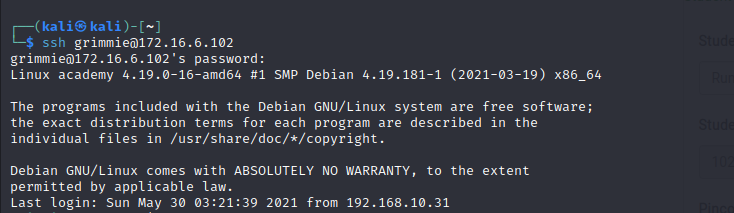
* Then, Open /var/www/html list the files
* Find the password using the grep -rn password commad
* Copy the password. Convert the user into grimmie

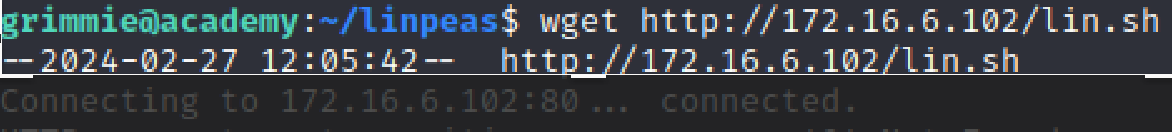


* Open new Terminal and go to academy and create and new file called findings.txt and paste the password in the file like
* nano findings
* Paste- grimmie: My\_V3ryS3cur3\_P4ss

**GRIMMIE AS ROOT:**

* To make grimmie as root use ssh command with academy IP address





* List the files present in the linpeas and give the execute access to lin.sh
* Now open lin.sh file

**PYTHON SERVER:**

* Open new terminal and get to academy directory
* Copy the lin.sh in the downloads linpeas directory
* cp ~/Downloads/linpeas.sh lin.sh
* Starts Python's built-in HTTP server on port 80 to serve files and directories locally.
* python -m http.server 80.Now we can get access to academy file using the command: nc -lvnp 9000