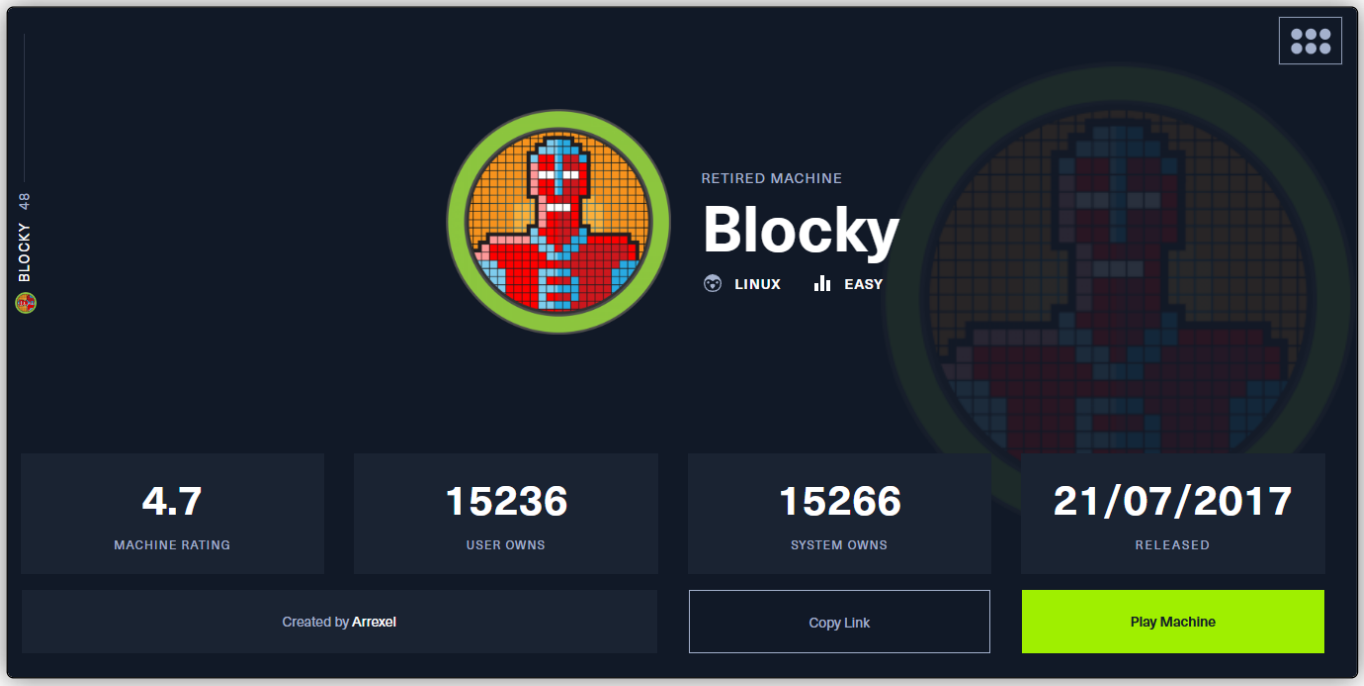
262- BLOCKY

1. BLOCKY

https://app.hackthebox.com/machines/Blocky

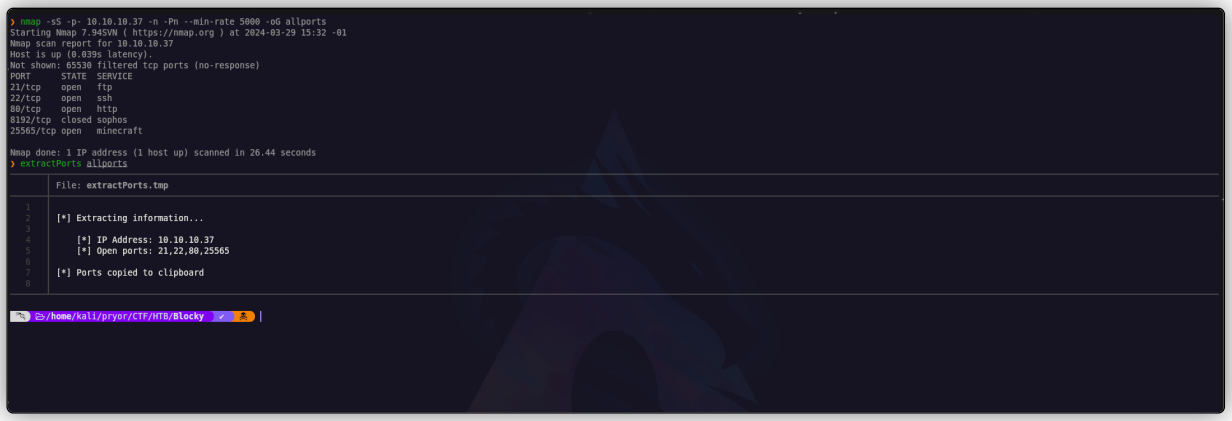


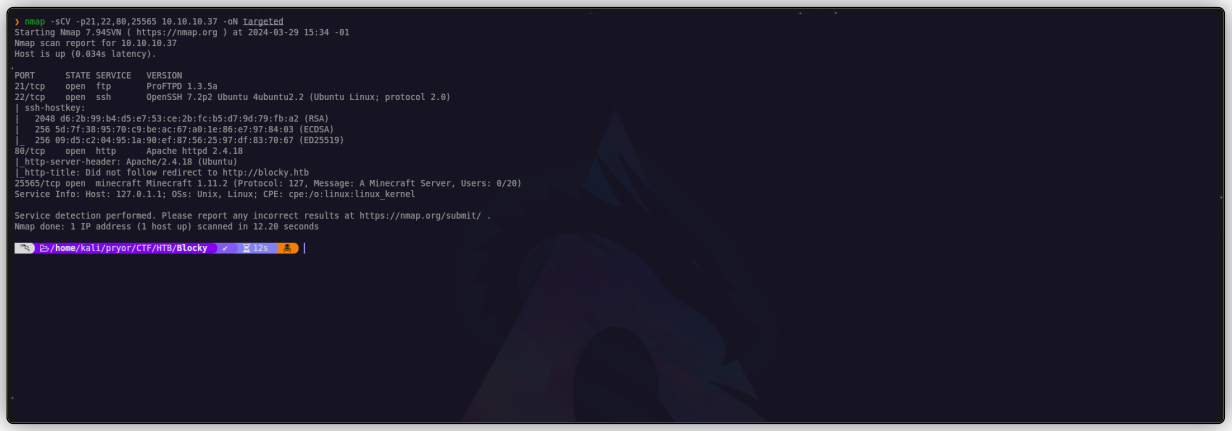
1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

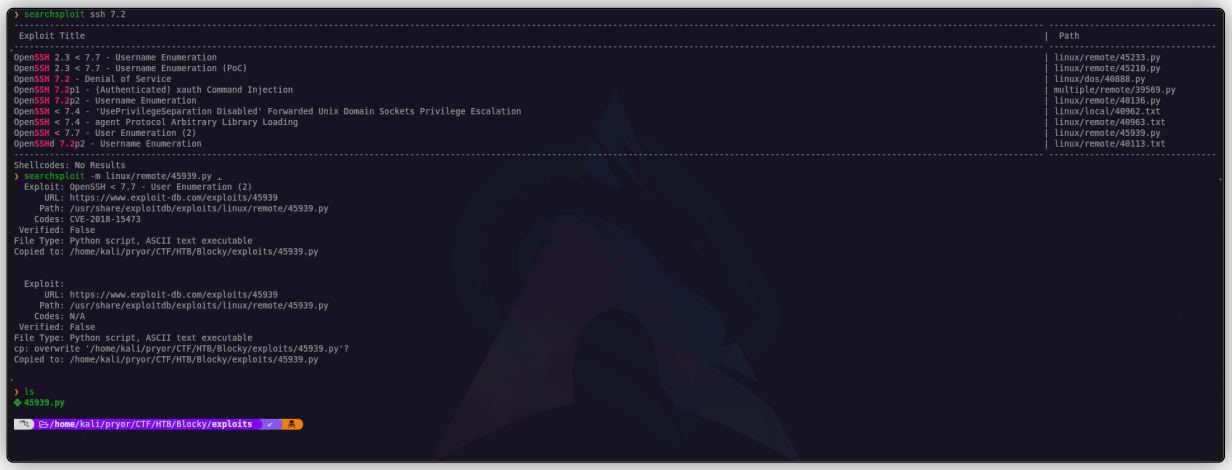
- 

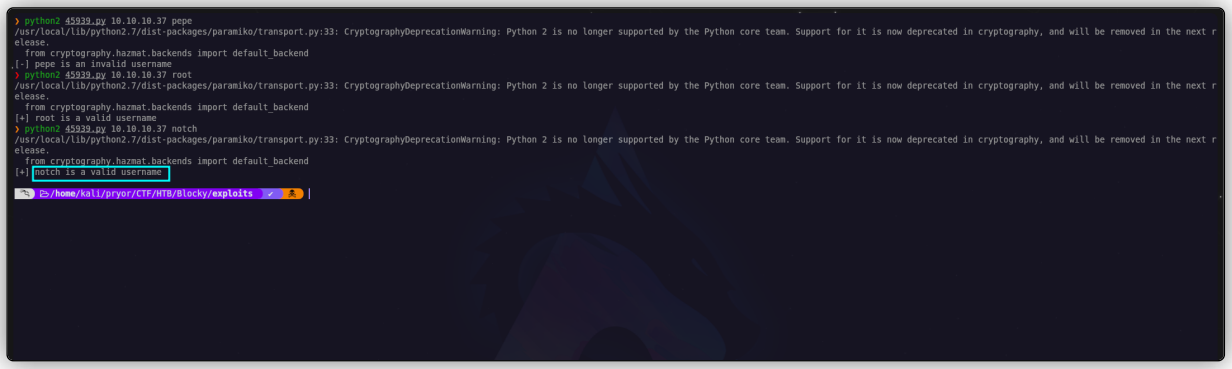
1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos, entre otros puertos: *21, 22 y 80* abiertos.
  - 

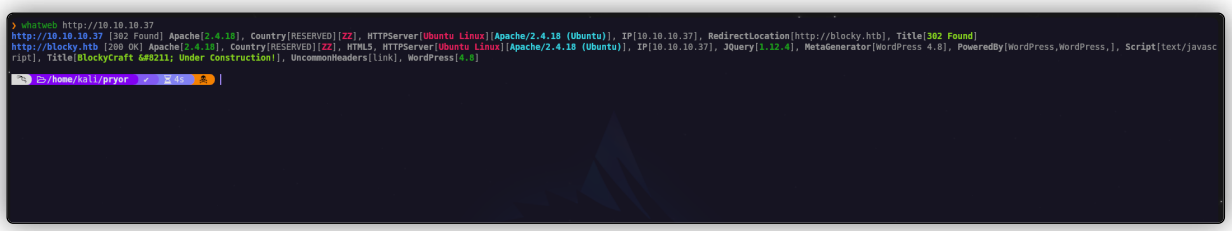
- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. Curiosamente, tenemos *Minecraft 1.11.2* corriendo en un puerto. Añadimos el dominio *blocky.htb* a nuestro /etc/hosts para poder acceder desde el navegador.
  - 

1.3. SSH user enumeration

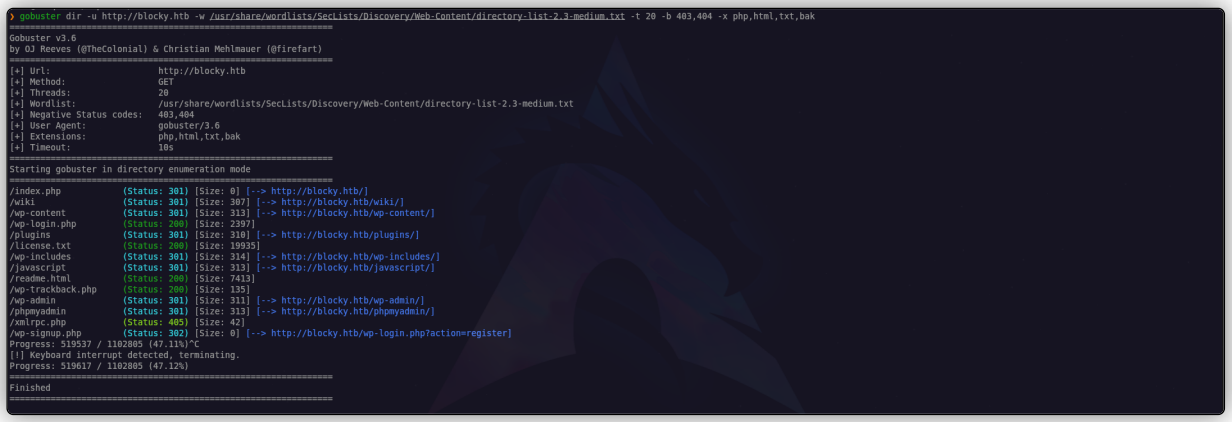
- CVE-2018-15473:
- Ya que tenemos *OpenSSH 7.2.p2*, que es una versión bastante obsoleta, podemos usar el siguiente exploit para enumerar usuarios válidos a nivel de sistema. Recordemos que las versiones vulnerables son inferiores a la *7.7*. Usamos este comando para traernos el exploit a nuestro directorio actual: `searchsploit -m linux/remote/45939.py .`.
  - 

- Podemos ejecutar el script, proporcionando la IP del objetivo y un usuario para comprobar si este es válido a nivel de sistema. Vemos que *root* y *notch* (creador de Minecraft) son usuarios válidos a nivel de sistema.
  - 

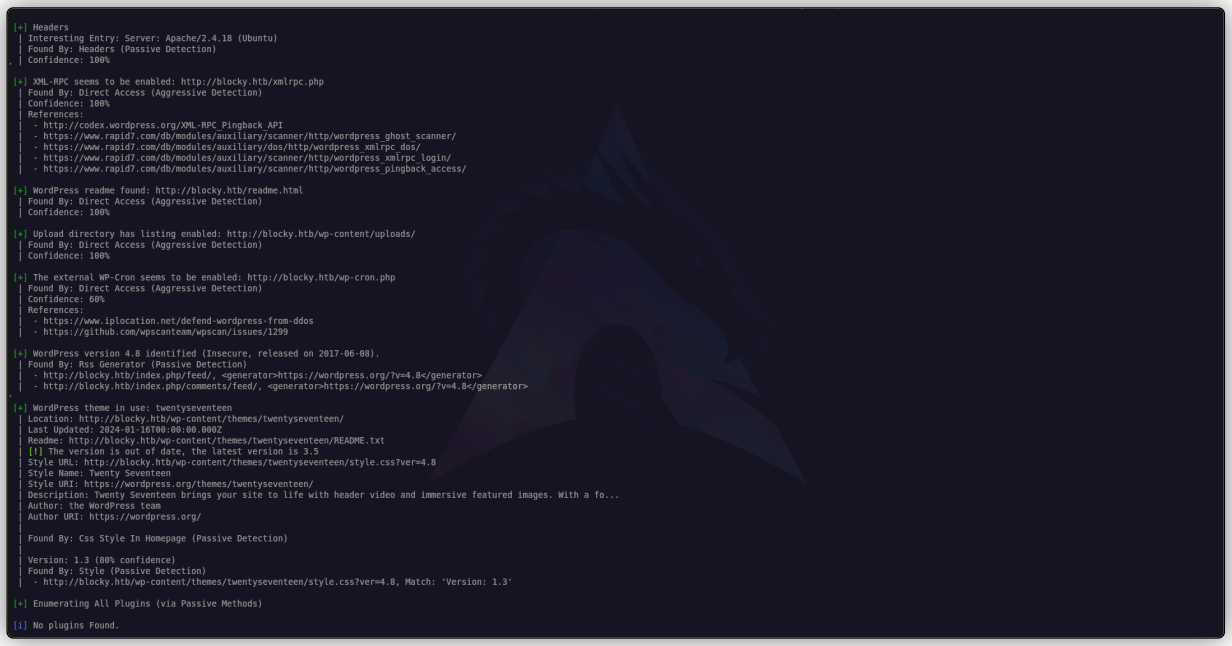
1.4. Tecnologías web

- Whatweb: nos reporta lo siguiente. Entre otras cosas, vemos que nos enfrentamos a un *Wordpress 4.8*.
  - 

1.5. Fuzzing web

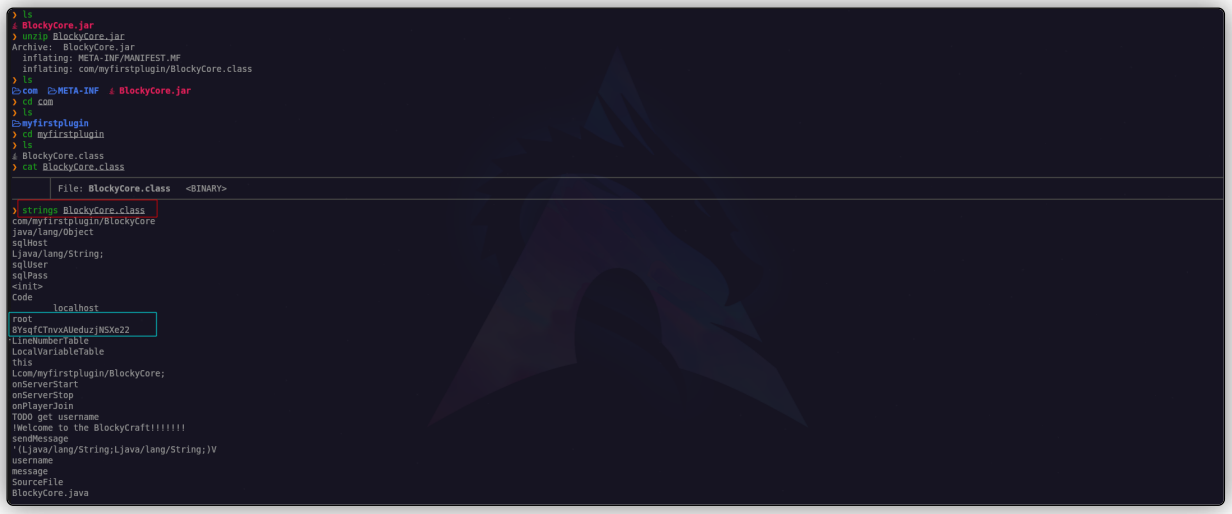
- **Gobuster**: usamos esta herramienta para descubrir directorios. Encontramos varios directorios típicos de *Wordpress* que pueden resultar interesantes.
  - 
```
❯ gobuster dir -u http://blocky.htb -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -b 403,404 -x php,html,txt,bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blocky.htb
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 301) [Size: 0] [--> http://blocky.htb/]
/wiki                 (Status: 301) [Size: 307] [--> http://blocky.htb/wiki/]
/wp-content           (Status: 301) [Size: 313] [--> http://blocky.htb/wp-content/]
/wp-login.php         (Status: 200) [Size: 2397]
/plugins              (Status: 301) [Size: 310] [--> http://blocky.htb/plugins/]
/license.txt          (Status: 200) [Size: 19935]
/wp-includes          (Status: 301) [Size: 314] [--> http://blocky.htb/wp-includes/]
/javascript           (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/readme.html          (Status: 200) [Size: 7413]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 311] [--> http://blocky.htb/wp-admin/]
/phpmyadmin           (Status: 301) [Size: 313] [--> http://blocky.htb/phpmyadmin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://blocky.htb/wp-login.php?action=register]
Progress: 519537 / 1102805 (47.11%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 519617 / 1102805 (47.12%)
===============================================================
Finished
===============================================================
```

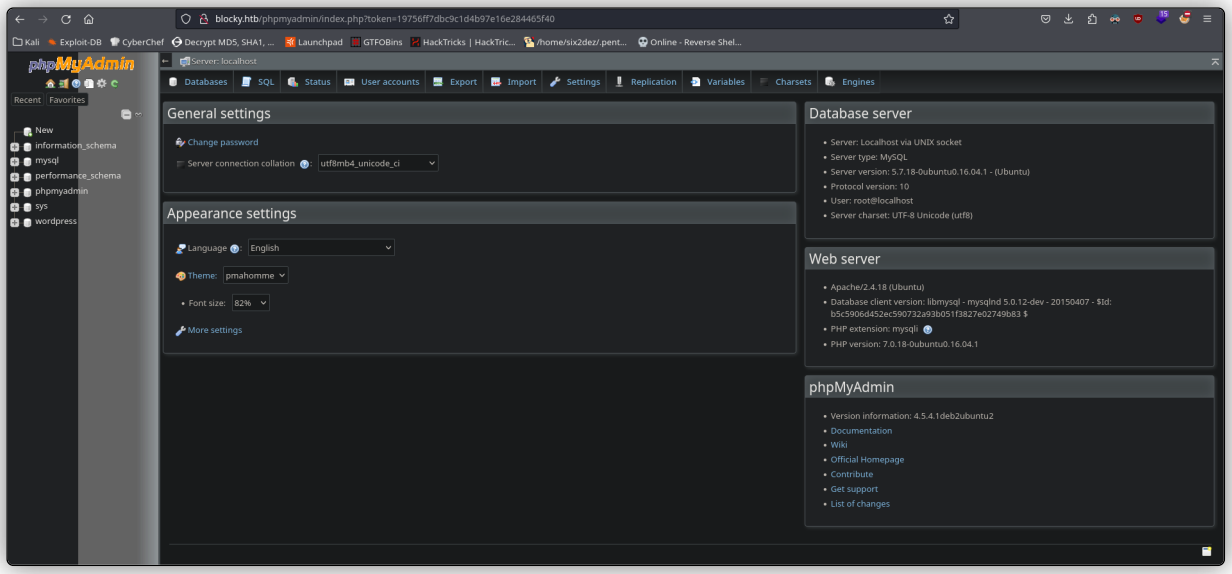
1.6. Wordpress enumeration

- **Wpscan**: usamos esta herramienta para obtener más información sobre el CMS de Wordpress que está corriendo en el servidor. Buscamos exploits para las versiones y plugins encontrados, pero en principio, no encontramos nada relevante.
  - 
```
[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blocky.htb/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://blocky.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blocky.htb/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blocky.htb/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 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blocky.htb/index.php/feed/, <generator>https://wordpress.org/?v=4.8</generator>
 |  - http://blocky.htb/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.8</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://blocky.htb/wp-content/themes/twentyseventeen/
 | Last Updated: 2024-01-16T00:00:00.000Z
 | Readme: http://blocky.htb/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 3.5
 | Style URL: http://blocky.htb/wp-content/themes/twentyseventeen/style.css?ver=4.8
 | 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/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blocky.htb/wp-content/themes/twentyseventeen/style.css?ver=4.8, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.
```

1.7. Information leakage

- Tras explorar diferentes directorios, encontramos unas credenciales en un archivo llamado *BlockyCore.class*, el cual se encontraba en el directorio /plugin. Este es un archivo *.jar*, pero pudimos descomprimirlo igualmente con: `unzip BlockyCore.jar`.

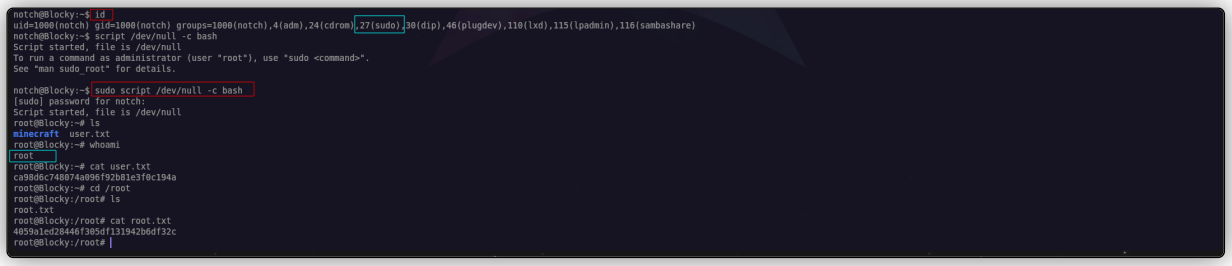
- 

- Tratamos de conectarnos por SSH y FTP, pero estas credenciales resultaron ser de la base de datos MySQL, a la cual accedemos via web por /phpmyadmin. No obstante, no encontramos nada relevante en la base de datos.
- 

1.8. Privesc via sudo group

- Buscamos otra alternativa para ganar acceso al sistema. Conseguimos acceso por SSH con el usuario *notch* y la contraseña que descubrimos previamente. Realizamos el *tratamiento de la TTY*.
- 

- Descubrimos que estamos en el *grupo sudo*, por tanto, tan solo ejecutamos un comando y proporcionamos nuevamente la contraseña. Obtenemos acceso como root.

- 

> - También podríamos haber intentado escalar nuestros privilegios a través del *grupo lxd*.