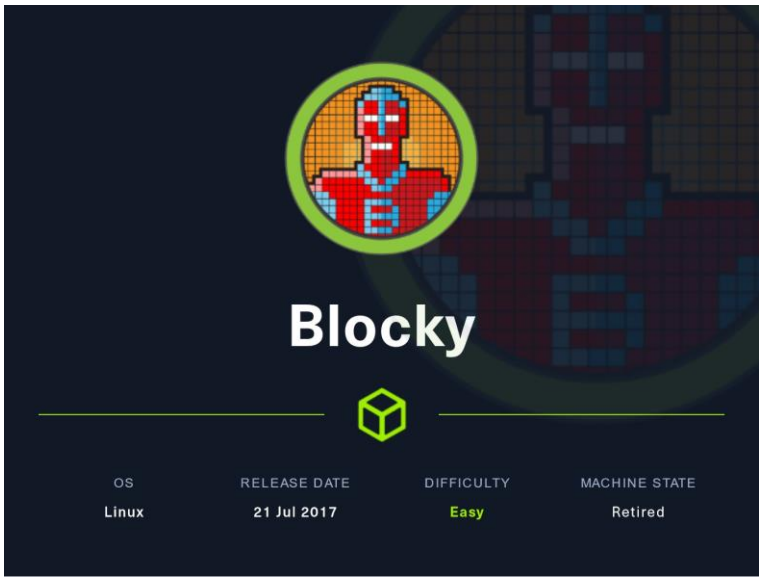
# Máquina Blocky




19 Noviembre 2023

**Hack The Box**
**Creado por: dandy_loco**

HACKTHEBOX

# 1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

```
┌──(root㉿kali)-[/home/kali/HTB/Blocky]
└─# ping -c 1 10.10.10.37
PING 10.10.10.37 (10.10.10.37) 56(84) bytes of data.
64 bytes from 10.10.10.37: icmp_seq=1 ttl=63 time=32.5 ms

── 10.10.10.37 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 32.476/32.476/32.476/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
File: targeted

# Nmap 7.94 scan initiated Sat Nov 18 07:58:47 2023 as: nmap -sCV -p 21,22,80,25565 -n -Pn -vvv -oN targeted 10.10.10.37
Nmap scan report for 10.10.10.37
Host is up, received user-set (0.032s latency).
Scanned at 2023-11-18 07:58:48 CET for 12s

PORT      STATE SERVICE   REASON         VERSION
21/tcp    open  ftp       syn-ack ttl 63 ProFTPD 1.3.5a
22/tcp    open  ssh       syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDXqVh031OUgTdcXsDwffHKL6T9f1GfJ1/x/b/dywX42sDZ5m1Hz46bKmbnWa0YD3LSRkStJDtyNXptzmEp31Fs2DUndVKui3LCcyKXY6FSVWp9ZDBzlW3aY8qa+y339OS3gp3aq277zYDnnA62U7rIltYp91u5VPBKi3DITVaSgzA8mcpHRr30e3cEGaLCxty58U2/lyCnx3I0Lh5rEbipQlG7Cr6NMgmGtW6LrlJRQiWA1OK2/tbZbLhwtkjB82pJI/0T2gpA/vlZJH0elbMXW40Et6bOs2oK/V2bVozpoKyoQuts8zcRmCViVs8B3p7T1Qh/Z+7Ki91vgicfy4fl
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5suOAio9ut2hOQYLN39Uhni8l4E/Wdir1gHxDCLMoNPQXDOnEUO1QQVbioUUMgFRAXYLhilNF8=
|   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILqVrP5vDD4MdQ2v3ozqDPxG1XXZOp5VPpVsFUROL6Vj
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://blocky.htb
25565/tcp open  minecraft syn-ack ttl 63 Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Nov 18 07:59:00 2023 -- 1 IP address (1 host up) scanned in 13.00 seconds
```

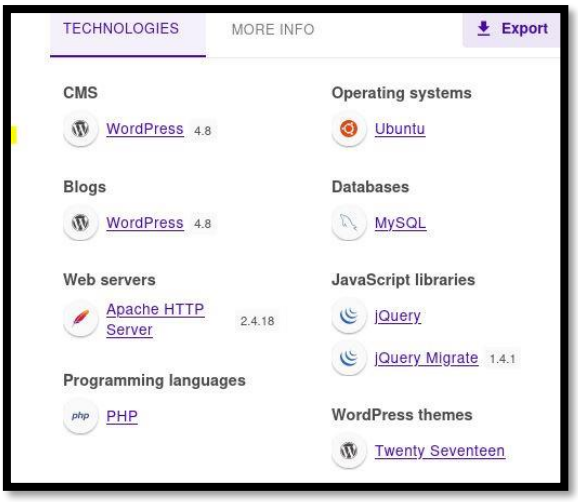
El resultado de Nmap vemos que se intenta redirigir a http://blocky.htb. Creamos la entrada en nuestro fichero hosts.

```
┌──(root㉿kali)-[/home/kali/HTB/Blocky]
└─# cat /etc/hosts
File: /etc/hosts
1   127.0.0.1   localhost
2   127.0.1.1   kali
3
4
5   10.10.10.37 blocky.htb
6
7   # The following lines are desirable for IPv6 capable hosts
8   ::1     localhost ip6-localhost ip6-loopback
9   ff02::1 ip6-allnodes
10  ff02::2 ip6-allrouters
```

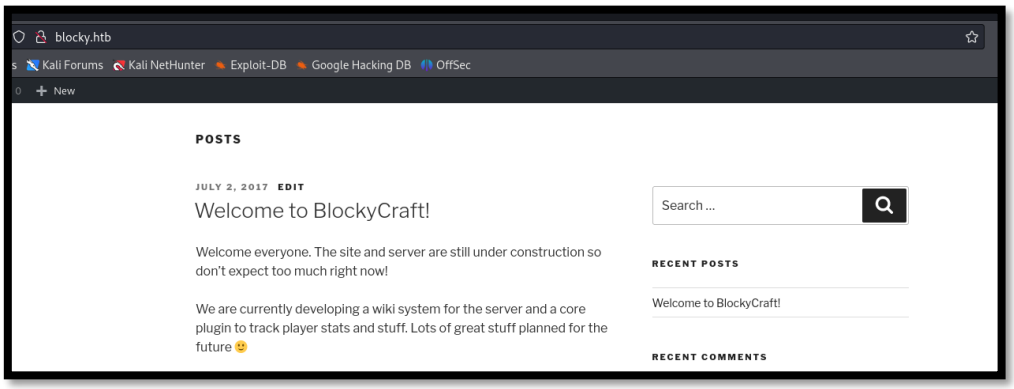
Mediante el uso de whatweb, intentamos averiguar las tecnologías del servicio web que está disponible en el puerto TCP/80.

```
┌──(root㉿kali)-[/home/kali/HTB/Blocky]
└─# whatweb http://10.10.10.37
http://10.10.10.37 [302 Found] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.37], RedirectLocation[http://blocky.htb], Title[302 Found]
http://blocky.htb [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.37], JQuery[1.12.4], MetaGenerator[WordPress 4.8], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[BlockyCraft &#8211; Under Construction!], UncommonHeaders[link], WordPress[4.8]
```

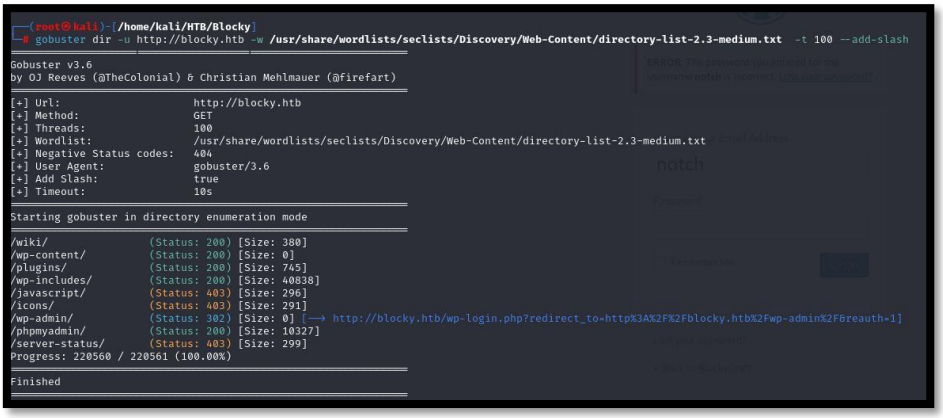
Abrimos la web en nuestro navegador y confirmamos las tecnologías con el plugin wappalyzer.




Según la información de la propia web, parece que se encuentra aun en desarrollo. El comentario, no realiza un usuario “notch”. Realizamos un descubrimiento de directorios por fuerza bruta.

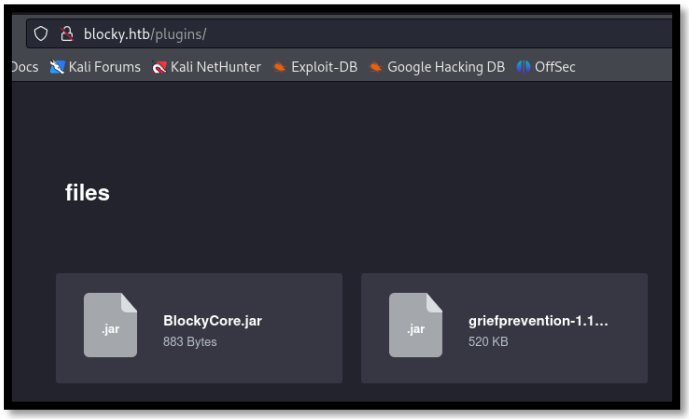



```
1. gobuster dir -u http://blocky.htb/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -t 100
```

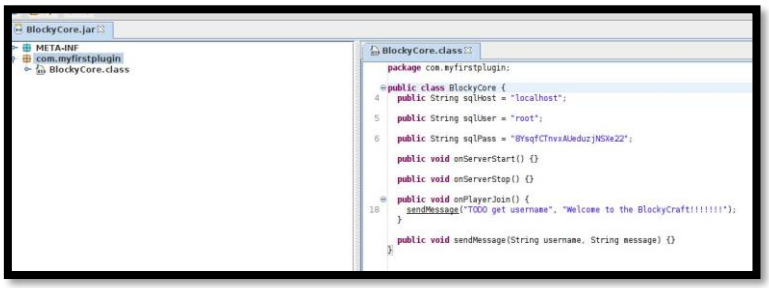


Revisamos el directorio “wiki”, pero no encontramos nada interesante.


Revisamos el contenido del directorio plugins y descubrimos dos ficheros jar.




Con jd-gui, revisamos el contenido del fichero BlockyCore.jar. Conseguimos lo que parece el usuario de bbdd.




```
1. root: 8YsqfCTnvxAUeduzjNSXe22
```

Podemos usar dicha credencial con el usuario “notch” para acceder por ssh a la máquina víctima, simplificando la intrusión. No obstante, entendemos que la vía intencionada para acceder a la misma es otra.

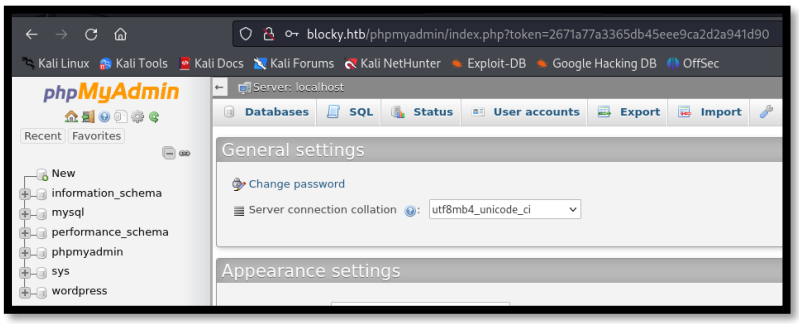
# 2. Análisis de vulnerabilidades

En la enumeración de directorios de la web, vimos que había un directorio denominado Phpmyadmin.

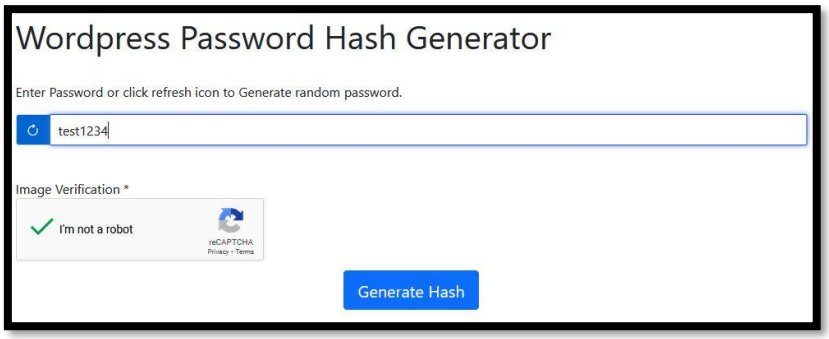
**¿Qué es Phpmyadmin?**

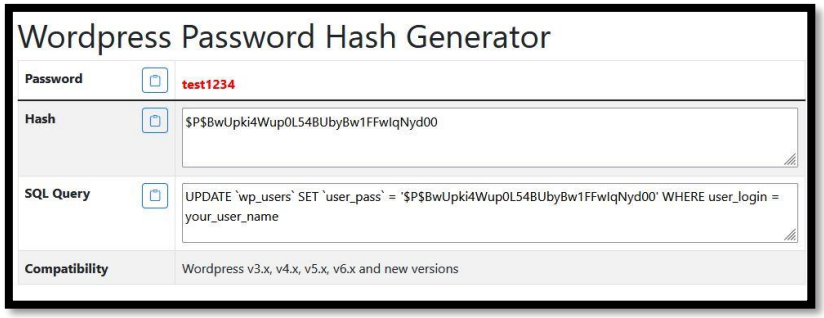
Es una herramienta escrita en PHP con la intención de manejar la administración de MySQL a través de páginas web, utilizando un navegador web.

Usamos la credencial anteriormente obtenida y conseguimos acceso a la aplicación Phpmyadmin.

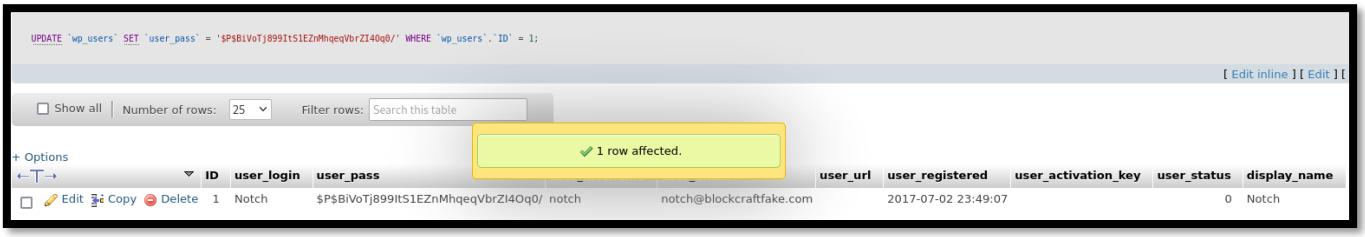



Tenemos acceso a modificar la clave del usuario de “notch”, para la web de WordPress, desde Phpmyadmin. Primero debemos codificar la clave que queramos poner. Podemos usar para ello esta web.



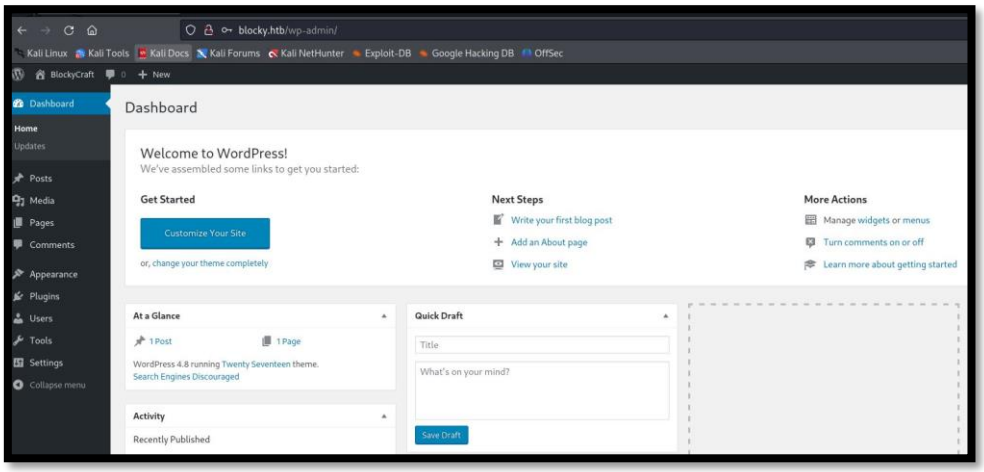



Actualizamos la clave que acabamos de generar.



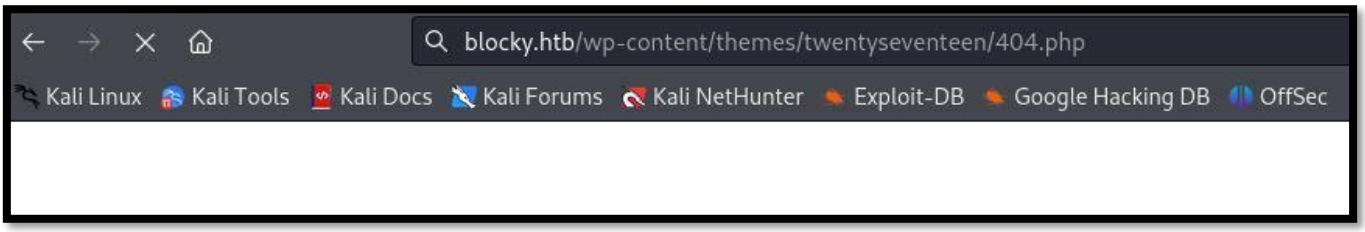

# 3. Explotación y acceso

Accedemos a la administración del Wordpress con el usuario “notch” y clave “test1234”.




Tenemos una vía potencial de ganar acceso a la máquina víctima siguiente este enlace.
Por tanto, modificamos la plantilla de error 404.php.


Nos ponemos en escucha por el puerto 443 con netcat y realizamos la petición a la web.

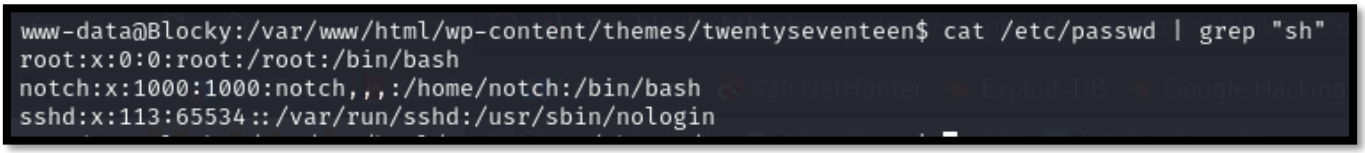




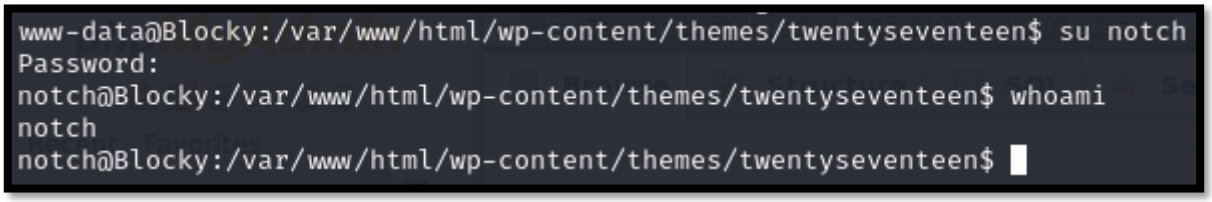
# 4. Movimiento lateral

Tras realizar el tratamiento de la TTY habitual, comprobamos que estamos en la máquina víctima, y no en un contenedor o similar.


Tras comprobar los usuarios del sistema, entendemos que nos tenemos que convertir en "notch".



Comprobamos si se está realizando una reutilización de contraseñas.




# 5. Escalada de privilegios

Comprobamos los permisos de sudoers que tenemos, y vemos que tenemos una via directa de convertirnos en root.


Ejecutamos “sudo su” y conseguimos resolver la máquina.

Sin embargo, nos devuelve un error de “ACCESS_DENIED”.


Revisamos la documentación y parece que puede que nos falte el parámetro ConfigurationName. Probamos de nuevo.

```
1. Enter-PSSession -Computer 10.10.10.210 -credential $cred -Authentication Negotiate -ConfigurationName
jea_test_account
```

Logramos acceder al sistema. Ya solo nos queda leer la flag de root. Para ello, usamos la función definida “Check-file”, que vimos anteriormente. En esta máquina, no está pensada para que puedas convertirte en administrador, de una forma interactiva.

```
1. Check-File C:\ProgramData\..\Users\Administrator\Desktop\root.txt
```