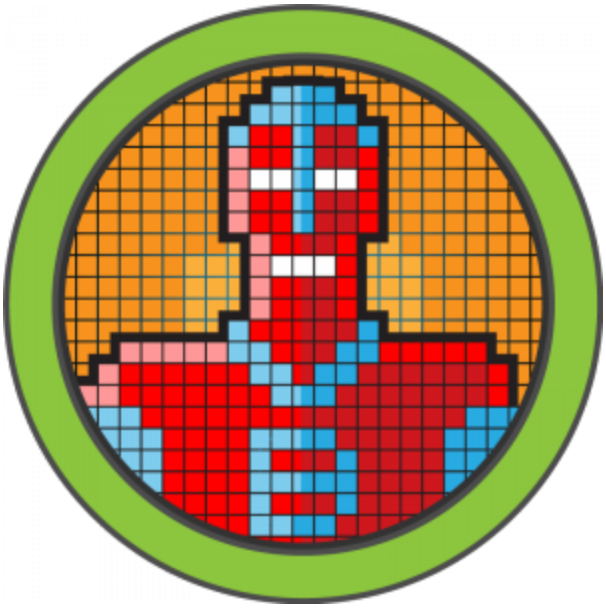


Descripción

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

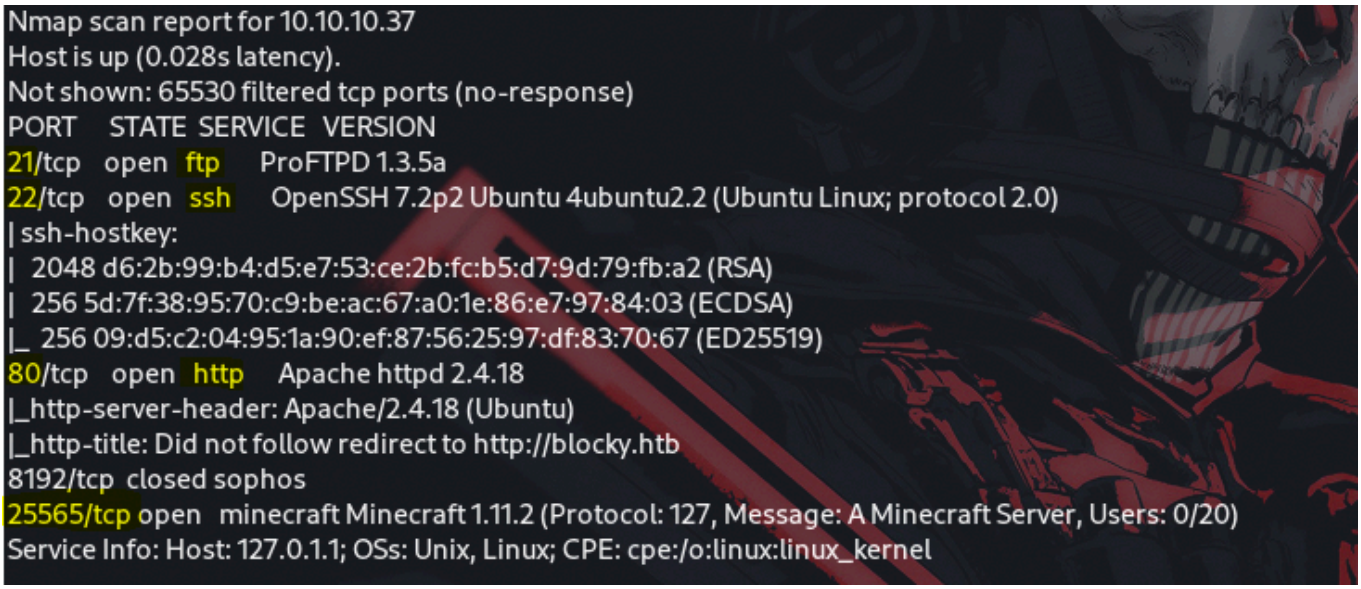
Herramientas empleadas en esta máquina

- NMAP
- GOBUSTER

Enumeración

Hacemos un escaneo para ver servicios activos

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

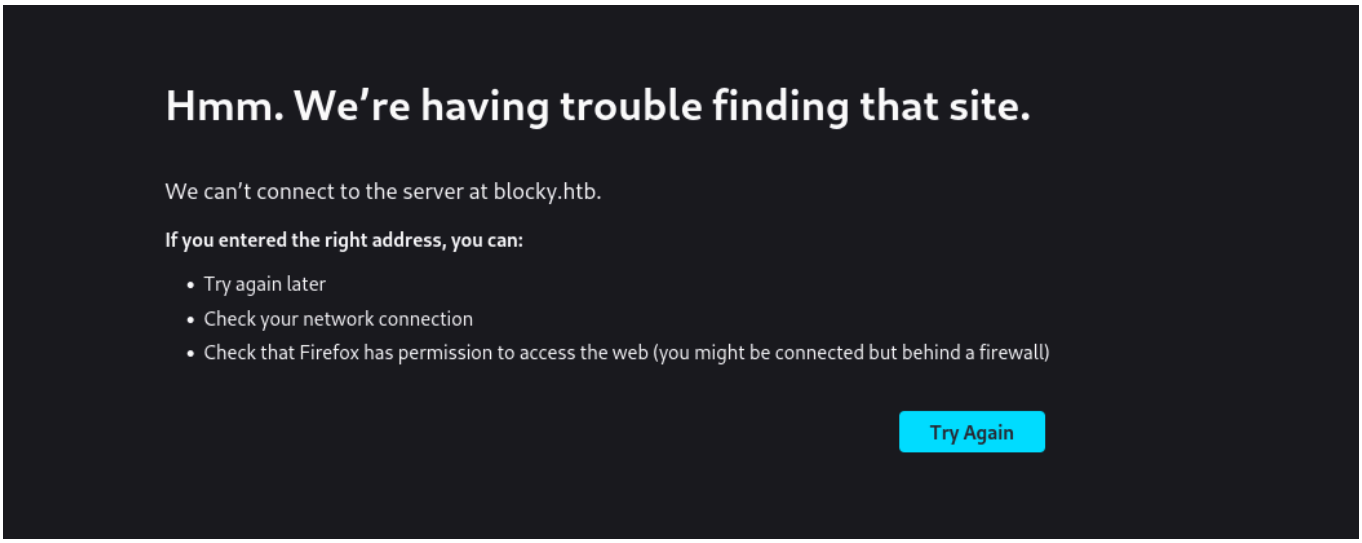


En el resultado del nmap podemos encontrar varios servicios activos interesantes como **FTP** y **SSH**, también tenemos el puerto **80** con una web

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

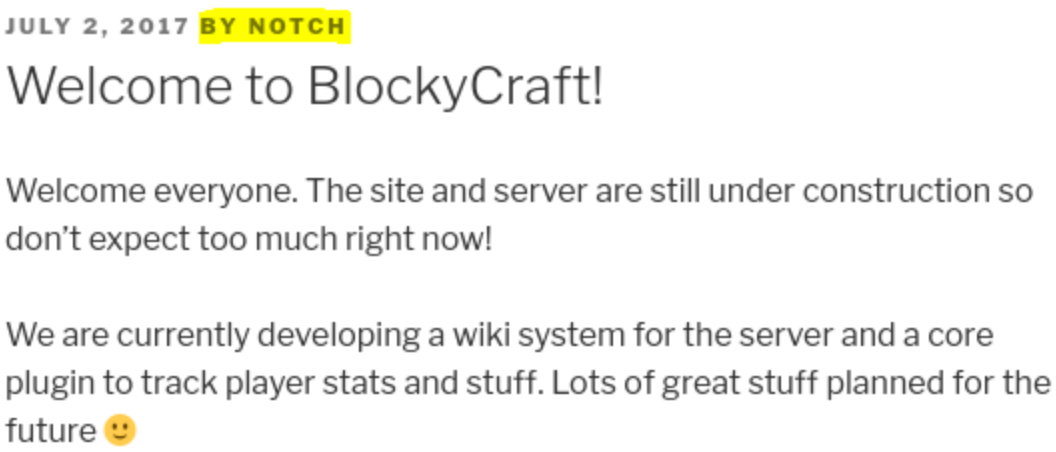
Vamos a asignar la IP al dominio **blocky.htb**

```
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



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
```

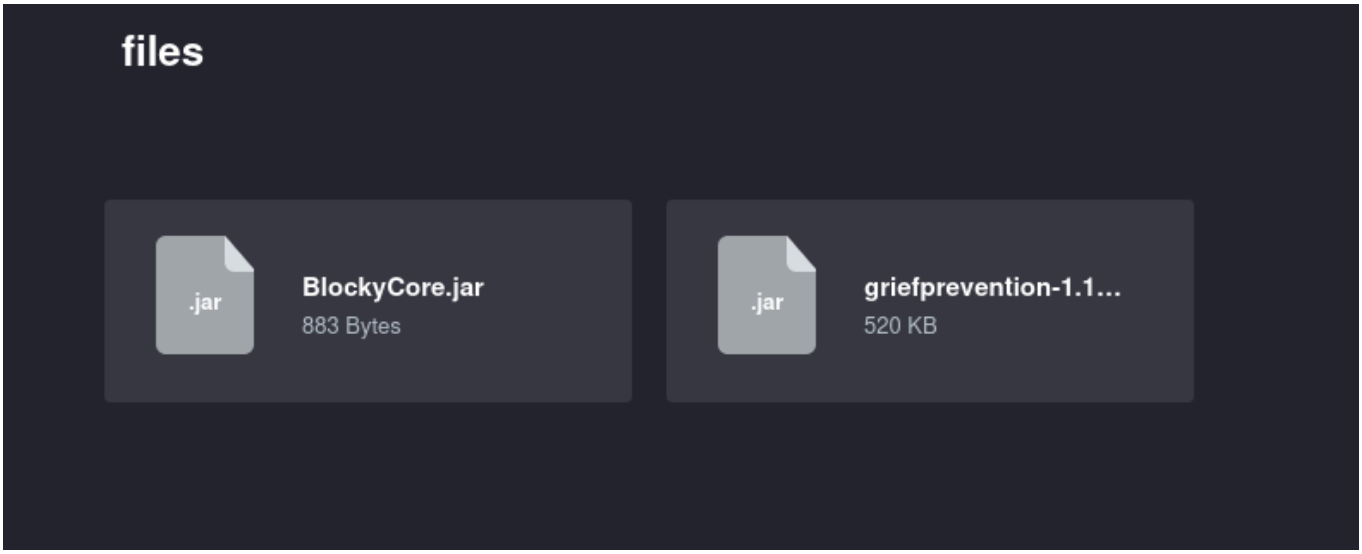
```
/.htpasswd        (Status: 403) [Size: 294]
/.hta             (Status: 403) [Size: 289]
/.htaccess        (Status: 403) [Size: 294]
/index.php        (Status: 301) [Size: 0] [--> http://blocky.htb/]
/javascript       (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/phpmyadmin       (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



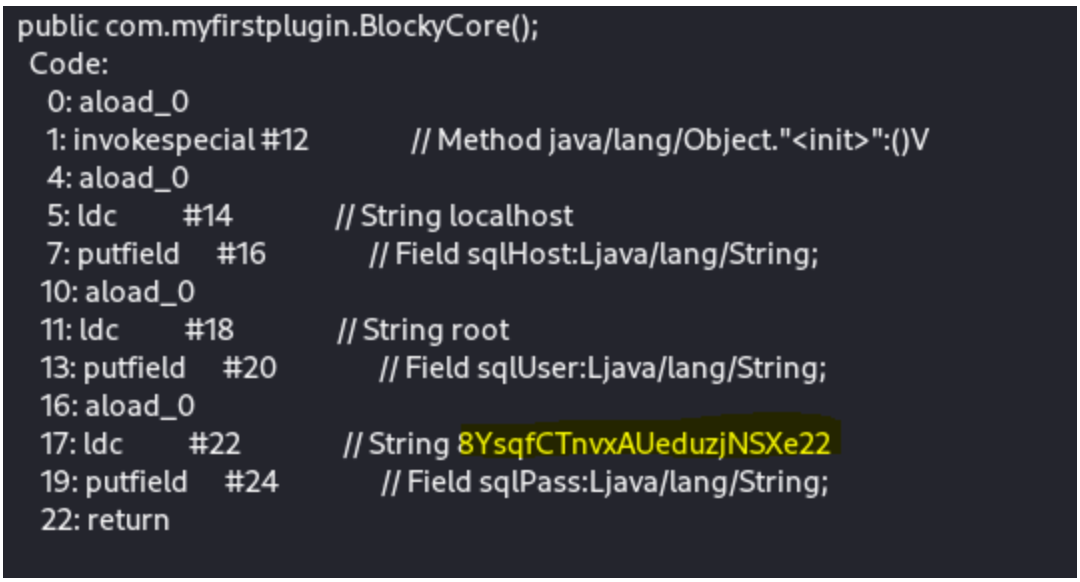
Vamos a descargar el archivo **BlockyCore.jar** , clicamos en el archivito y lo tendremos en la carpeta **Downloads**

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
```

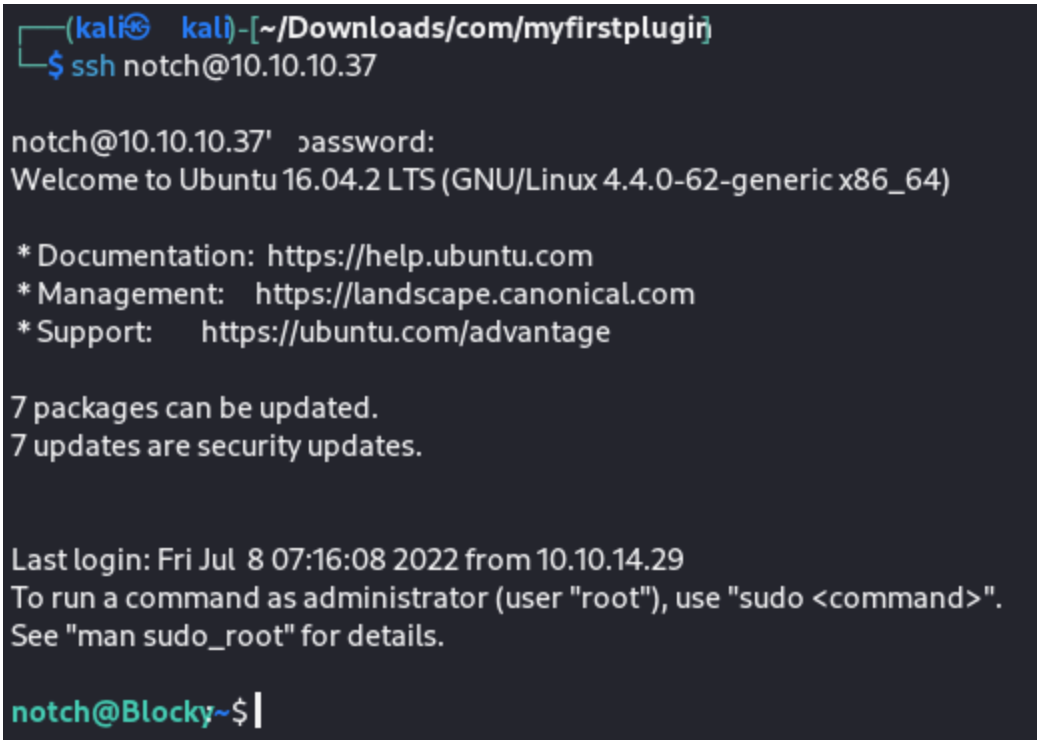


Una vez abierto podremos ver una **string** con números y letras, esa es la contraseña del usuario, abajo nos pone **Field sqlPass** por lo que podemos deducir que se trata de unas credenciales

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

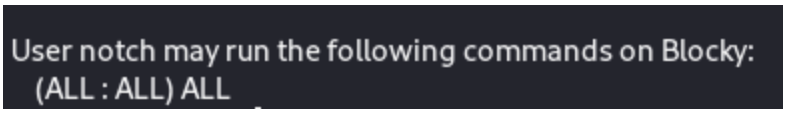


Comprobamos los usuarios y podemos ver que no tenemos privilegios, no somos root

Escalada de Privilegios

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

```
sudo -l
```



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**

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