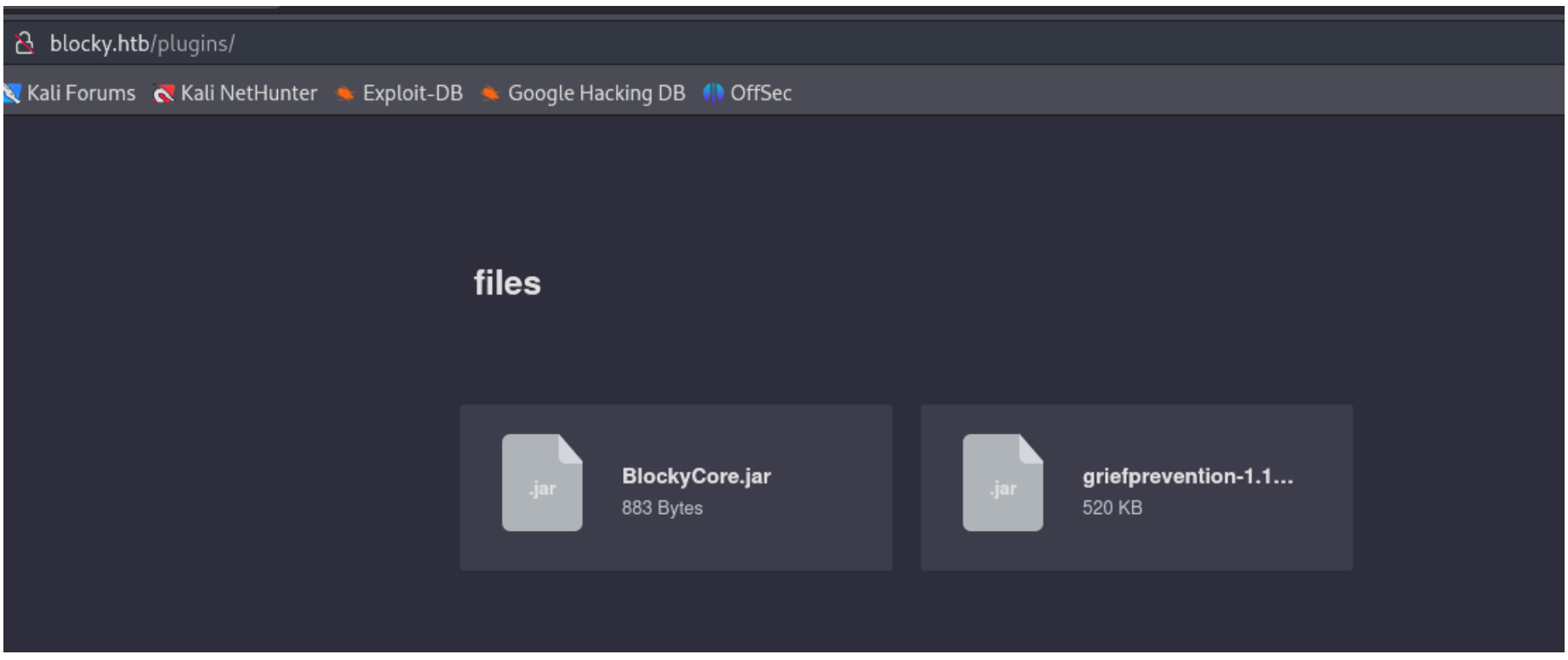
Blocky - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

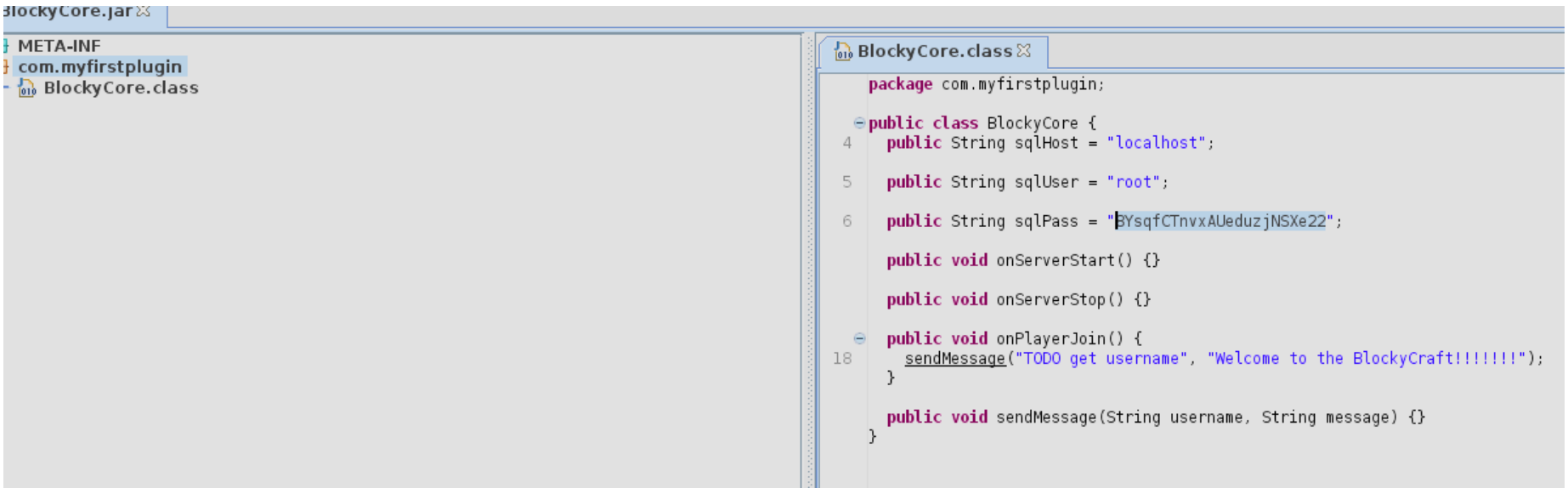
```
PORT      STATE SERVICE   REASON         VERSION
21/tcp    open  ftp       syn-ack ttl 63 ProFTPD 1.3.5a
22/tcp    open  ssh       syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDXqVh031OUgTdcXsDwffHKL6T9f1GfJ1/x/b/dywX42sDZ5m1Hz46bKmbnWa0YD3LSRkStJDtyNX
Wp9ZDBzlW3aY8qa+y339OS3gp3aq277zYDnnA62U7rIltYp91u5VPBKi3DITVaSgzA8mcpHRr30e3cEGaLCxty58U2/lyCnx3I0Lh5rEbipQ1G7Cr6NM
82pjI/0T2gpA/vlZJH0elbMXW40Et6bOs2oK/V2bVozpoRyoQuts8zcRmCViVs8B3p7T1Qh/Z+7Ki91vgicfy4fl
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5suOAio9ut2hOQYLN39Uhni8i4E/W
MgFRAXYLhilNF8=
|   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-title: Did not follow redirect to http://blocky.htb
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
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
```

Encontramos 2 archivos ".jar" en la siguiente ruta:

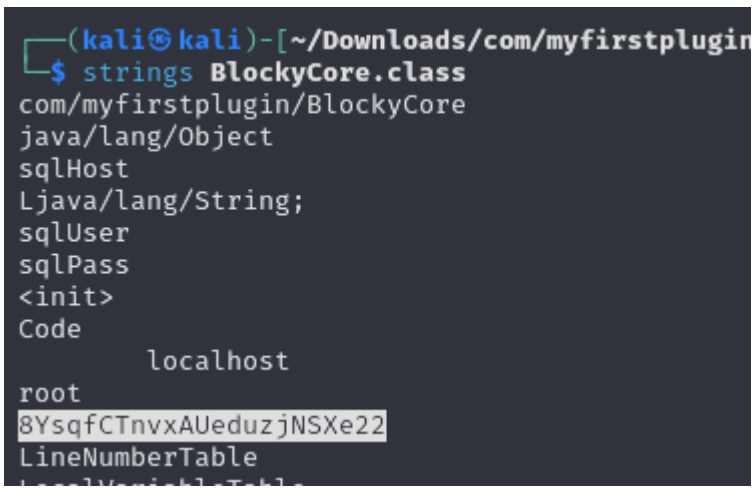


Nos los descargamos. Hay una herramienta que sirve para ver el contenido de los archivos "java". Se llama jd-gui. Lo instalamos y lo hiciamos escribiendo el nombre:

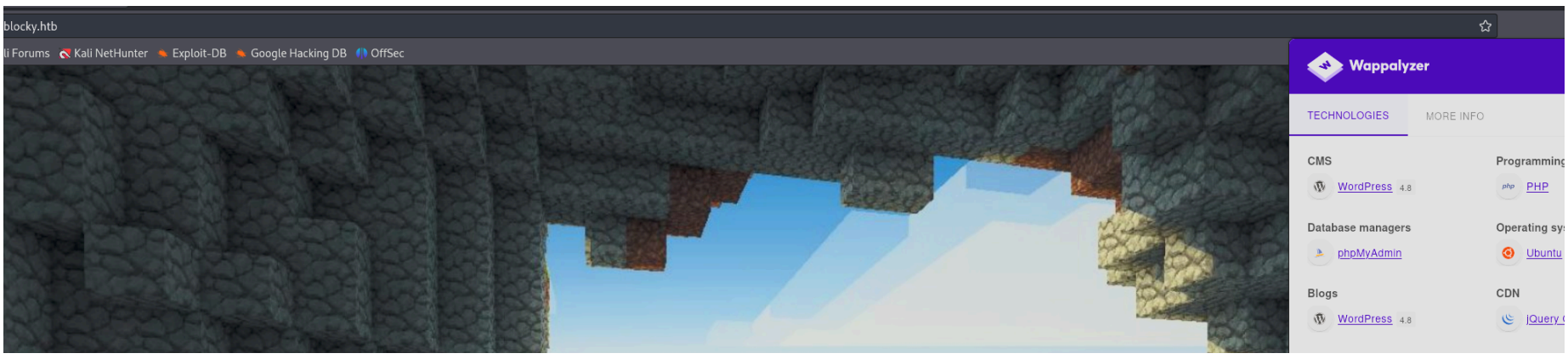
Podemos ver una contraseña:

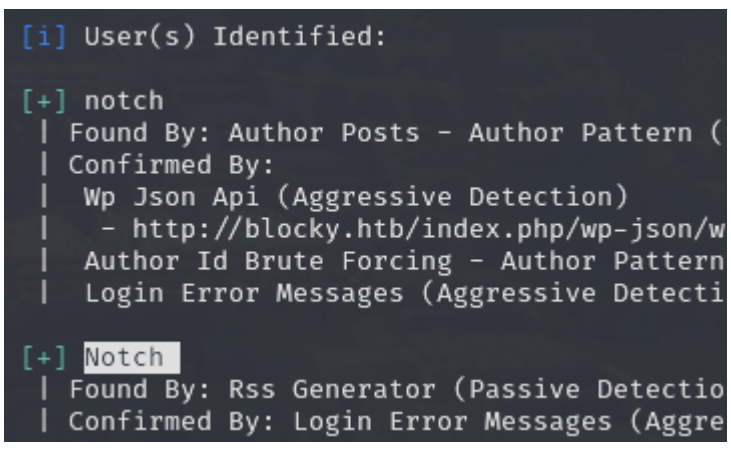


Esto se podia ver tambien con strings:

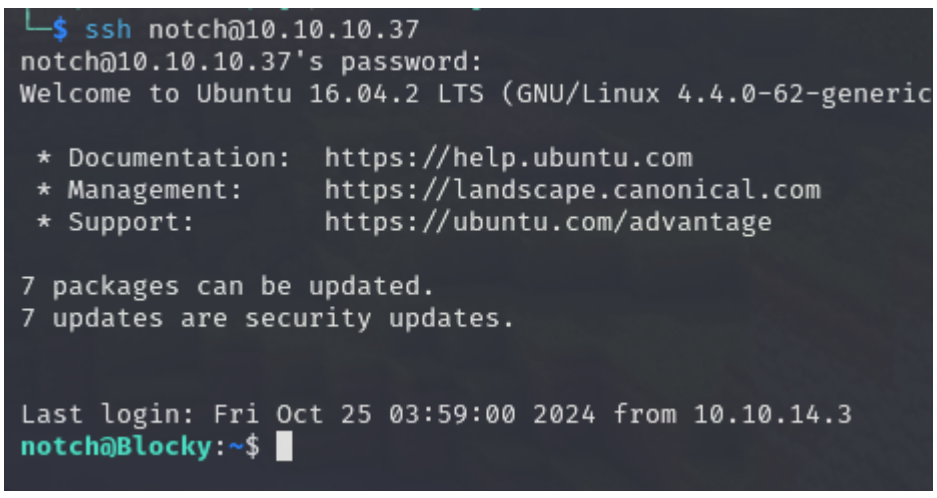


Como vemos que la pagina principal es un wordpress podemos enumerar usuarios con wpscan





Como sabemos un usuario y una contraseña vamos a intentar conectarnos por SSH:



ESCALADA DE PRIVILEGIOS

Vamos a ver los permisos que podemos ejecutar como sudo:

```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Sorry, try again.
[sudo] password for notch:
Matching Defaults entries for notch on Blo
    env_reset, mail_badpass, secure_path=/

User notch may run the following commands
    (ALL : ALL) ALL
notch@Blocky:~$
```

Como podemos ejecutar todos comandos como sudo hacemos sudo su para pasar a root:

```
notch@Blocky:~$ sudo su
root@Blocky:/home/notch# whoami
root
```