**NAMA SEKOLAH : SMK NEGERI 2 BANDUNG**

Selasa 14 Mei 2024

**Ketua Tim :**

Muhammad Akhtar Khawarizmi

**Anggota Tim :**

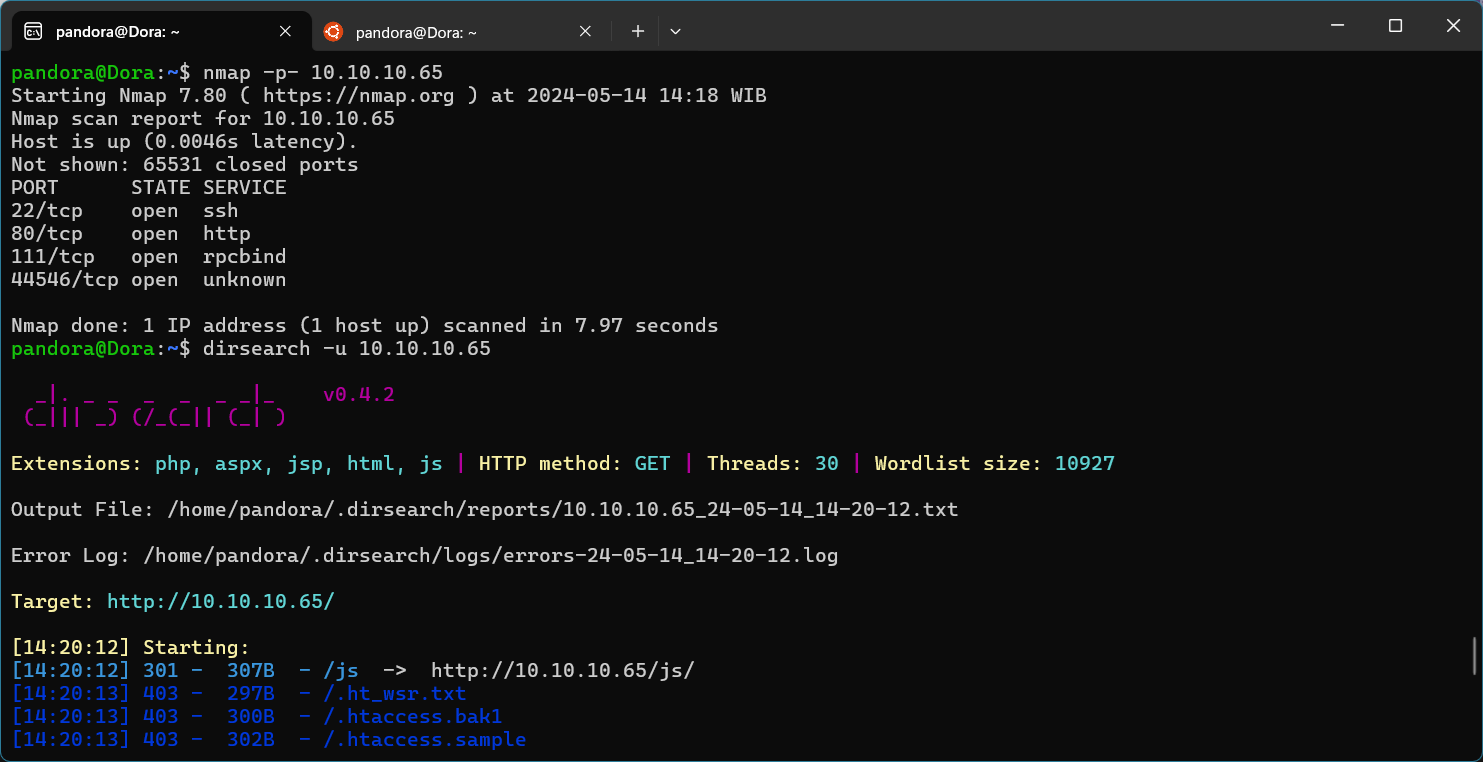
Harvi Muhammad Zakhir

SOAL NO 2

CTF kali ini ada di ip 10.10.10.65

**Recon**

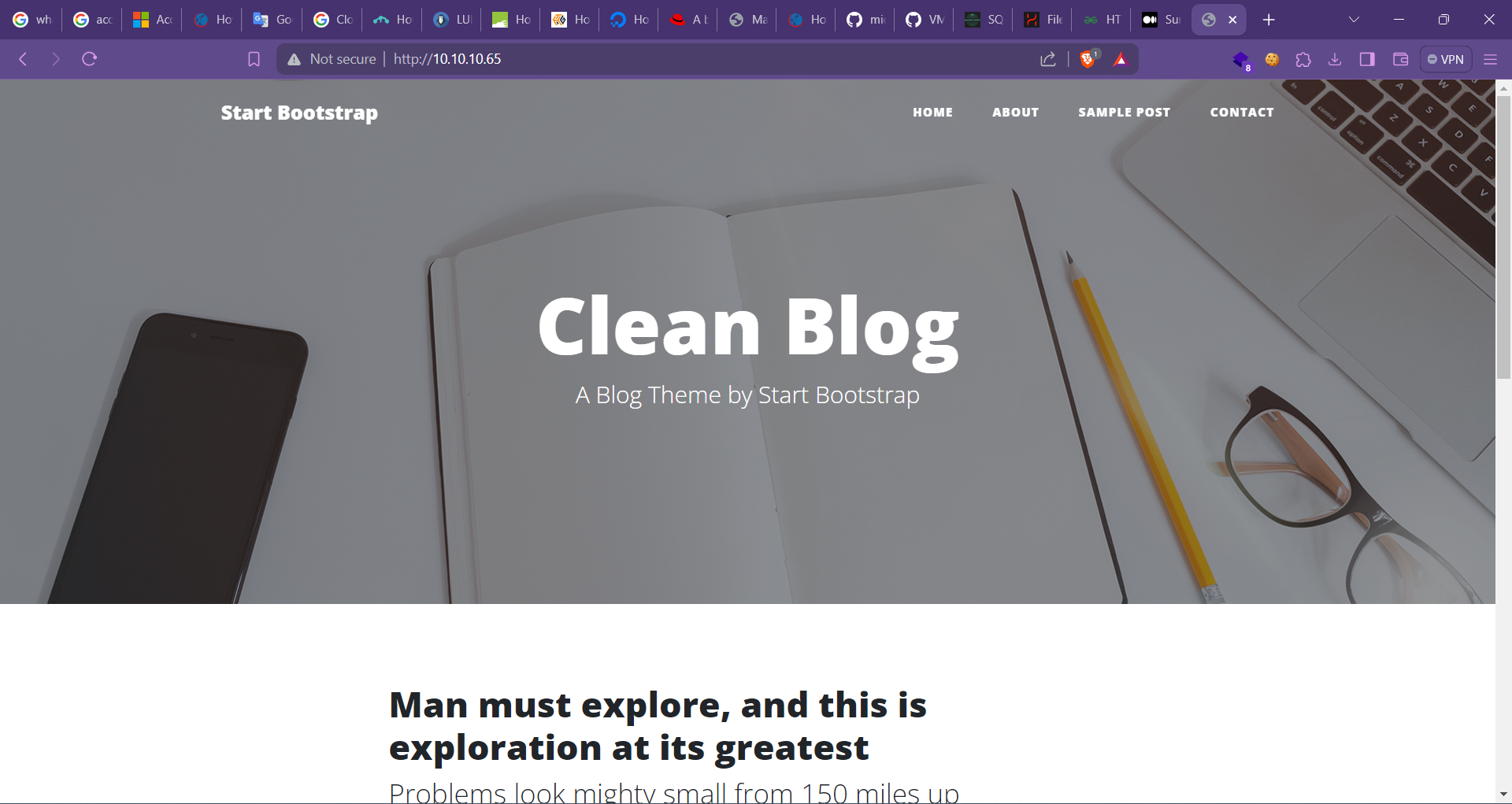
Untuk recon saya akan menggunakan nmap terlebih dahulu pada wsl ubuntu



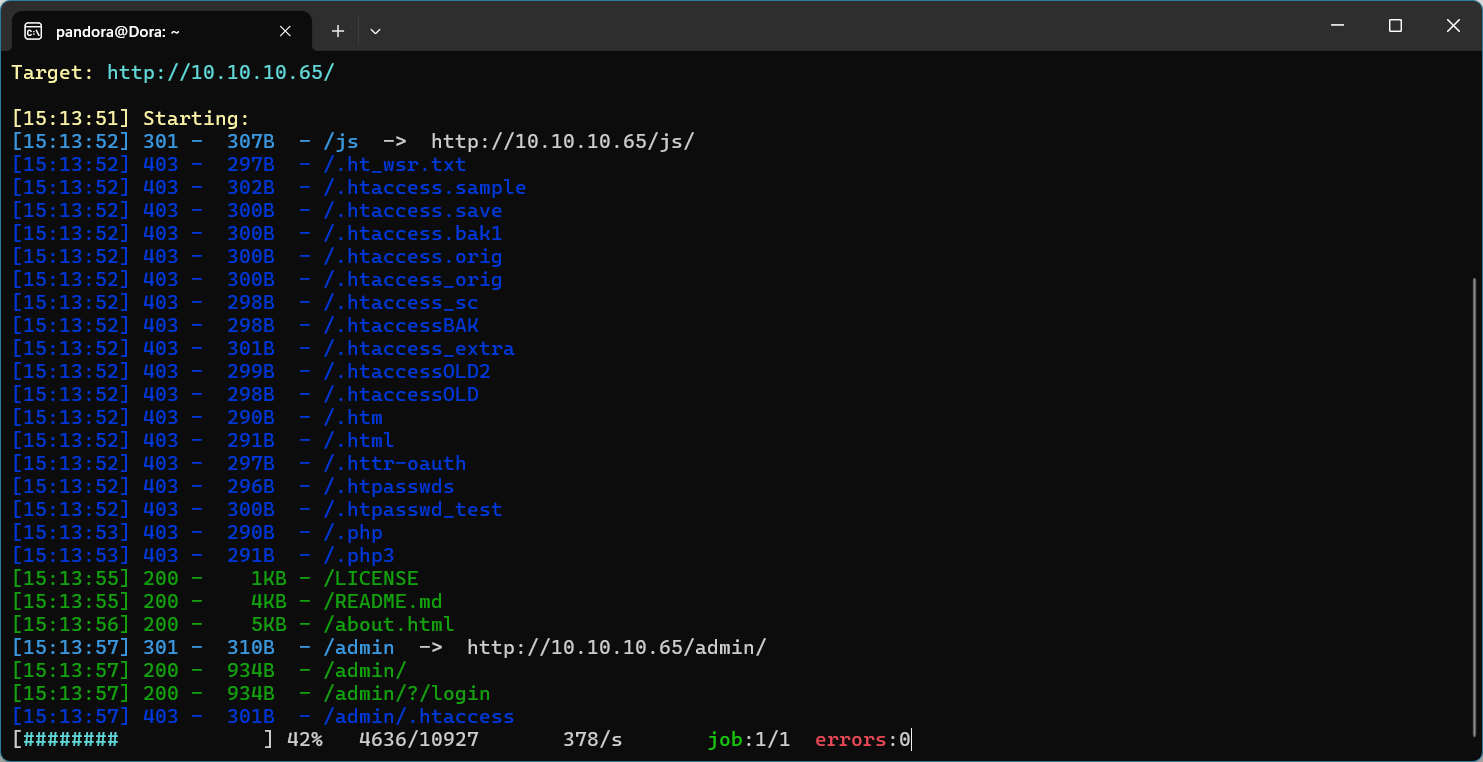
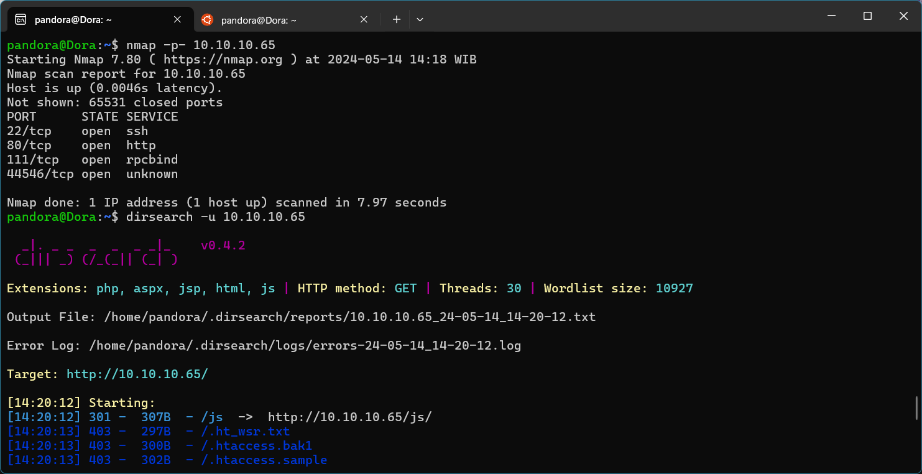
Dapat dilihat beberapa port terbuka, yang menarik adalah port 22 dan 80

Port 22 biasanya digunakan untuk mengakses SSH atau SecureShell yang dapat mengendalikan server sedangkan port 80 mengidentifikasikan service http atau HyperTextTransferProtocol yang dimana menyediakan tampilan website.

Setelah ditelusuri website merupakan website blog.



Tidak banyak yang bisa ditelusuri. Website biasanya terdiri dari berbagai macam direktori, maka dari itu saya akan mencoba menelusuri direktorinya dengan menggunakan tool dirsearch.



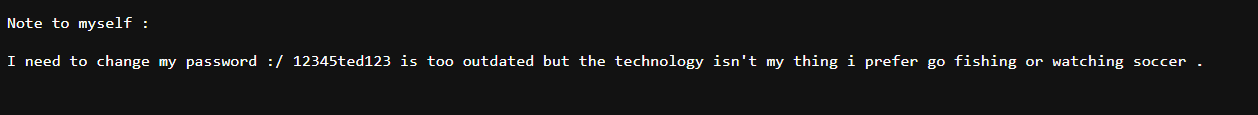
**Exploit**

Setelah mengetahui beberapa kelemahan target kita mulai membobol kelemahan tersebut.

Ada path yang menarik, /admin maka saya akan mencoba menelusuri path tersebut.

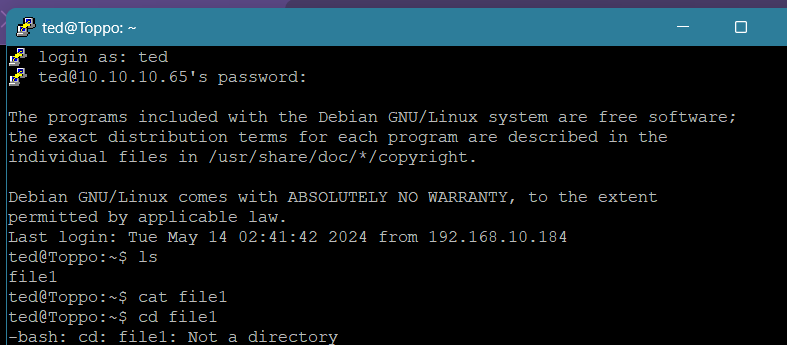


Kita mendapat sebuah file “notes.txt” mari kita coba akses file tersebut.



Berikut isinya. Kita mengetahui ada password.

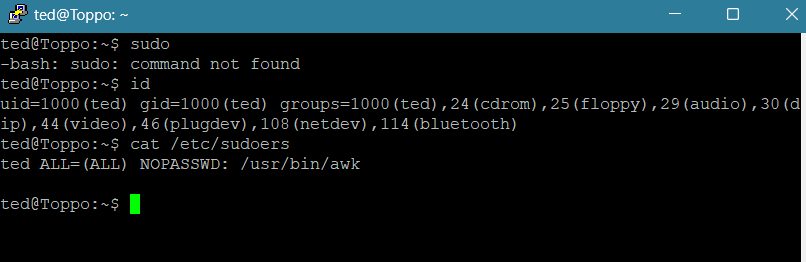
Kita bisa coba untuk login ssh menggunakan putty. Pertama saya menggunakan username user, admin, dan root tapi gagal. Di password terdapat kata ted, mungkin pemiliknya bernama ted. Mari kita coba ted, akhirnya bisa deh



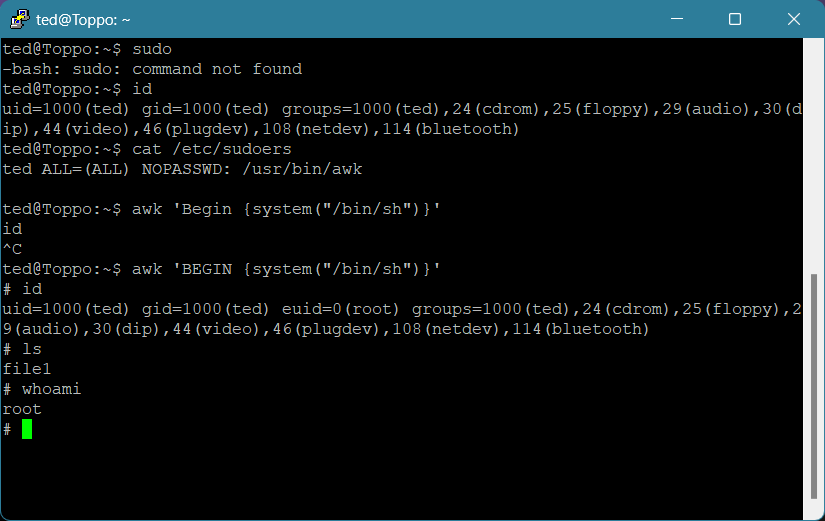
**Post Exploit**

Di langkah terakhir biasanya langkah ini dipakai untuk mencari data atau upload backdoor. Karena disini konteksnya ctf maka kita akan cari flagnya di dalam ssh ini.

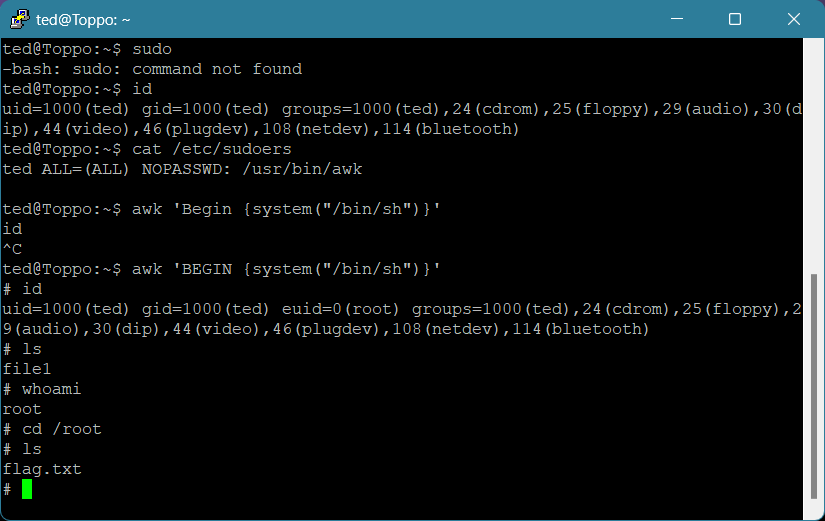
Saya mencoba untuk ls dan ada file1, ternyata setelah saya membuka menggunakan cat file1, isinya kosong wkwkwkkw.

Setelah sejenak berfikir saya ingin mencoba masuk shell root tapi ketika sudo, Anehnya tidak ada sudo? Saya pun mencoba untuk mencari sudoers dengan membaca /etc/sudoers

Ternyata sudoersnya bernama awk dan tidak ada password. Baiklah mari kita aktifkan shell untuk root dengan command berikut



Akhirnya kita bisa masuk kedalam shell dari root. Lanjut lagi cari flag deh



Ketemu flag nya tinggal di cat