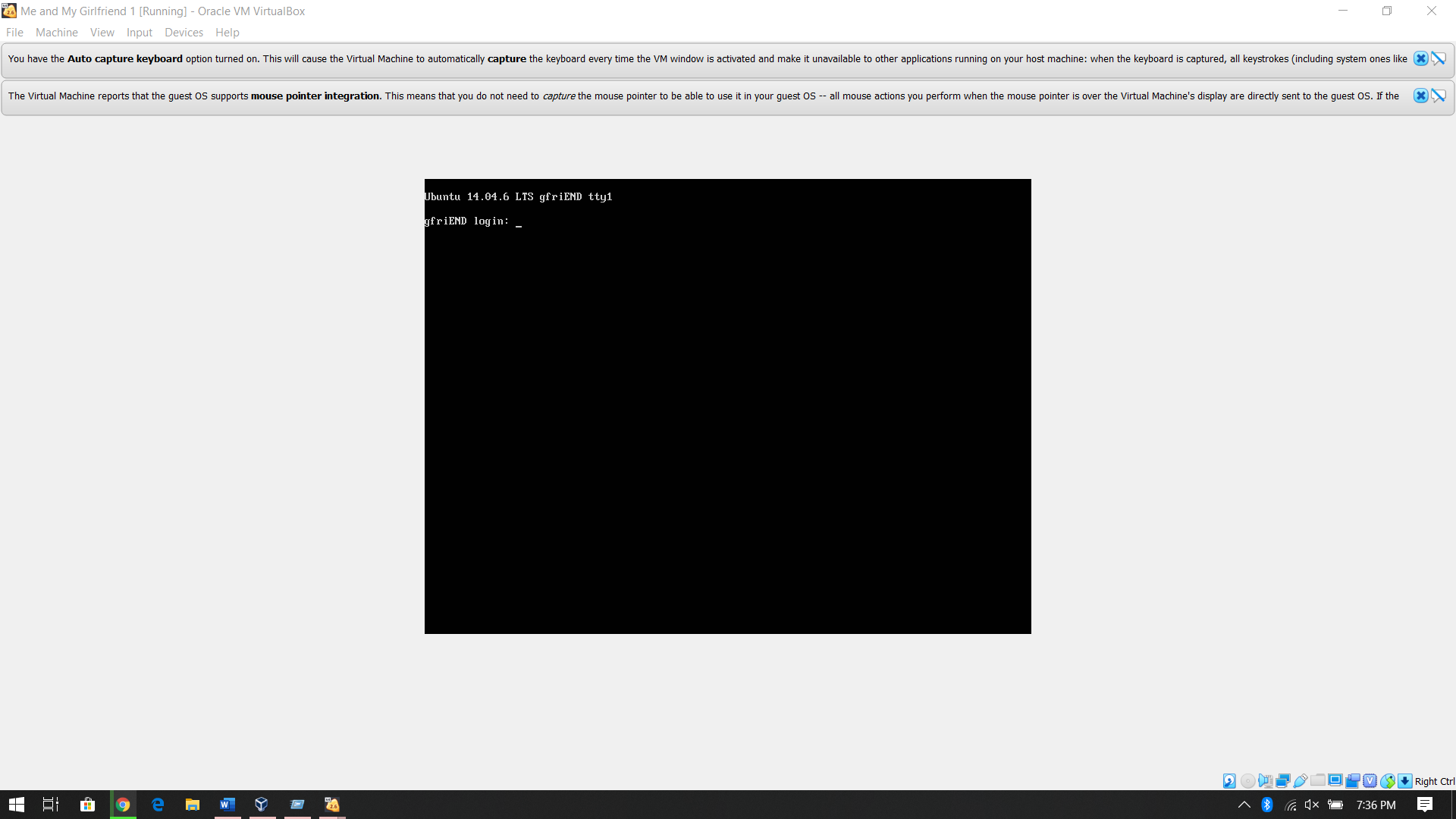
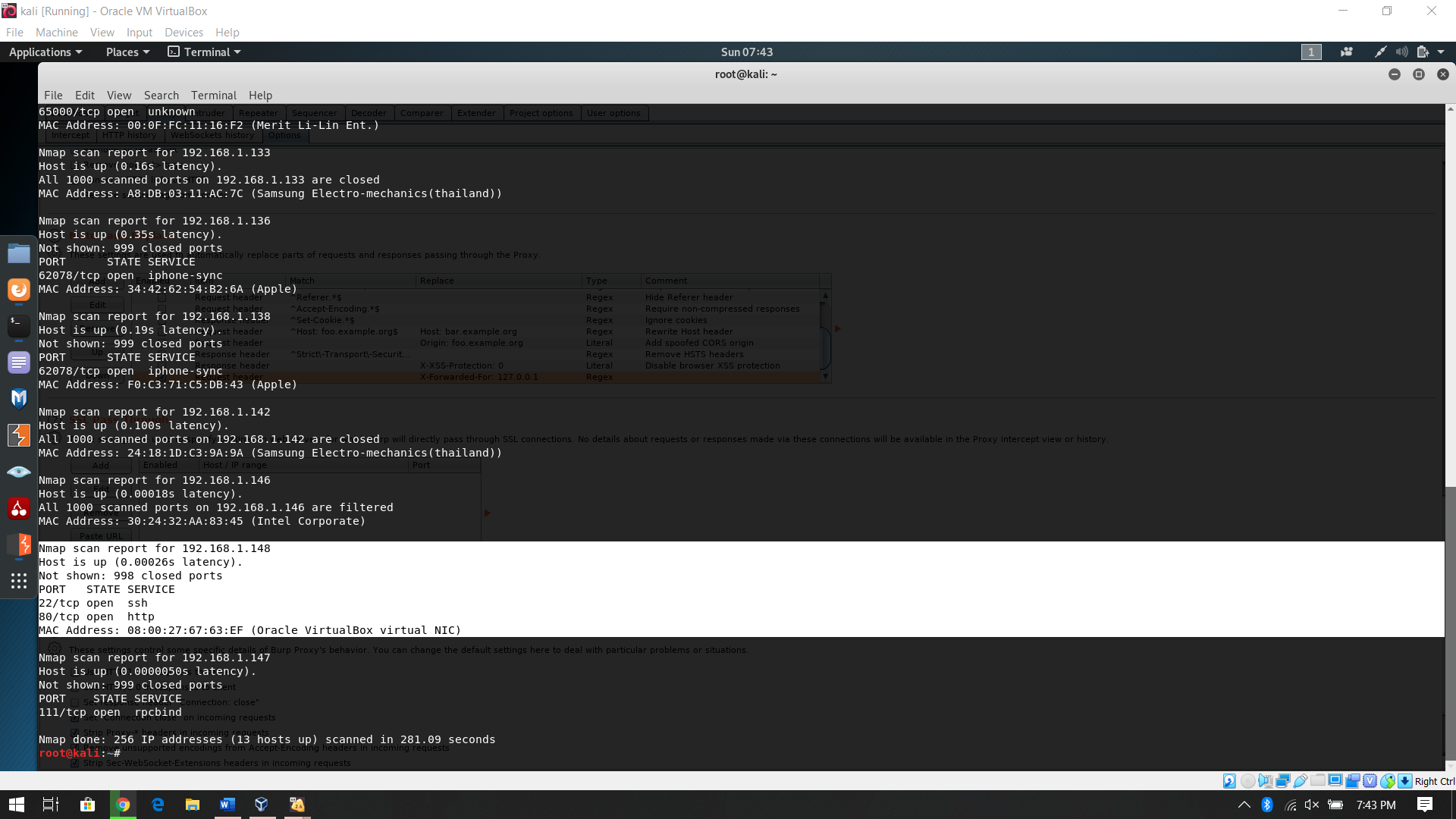
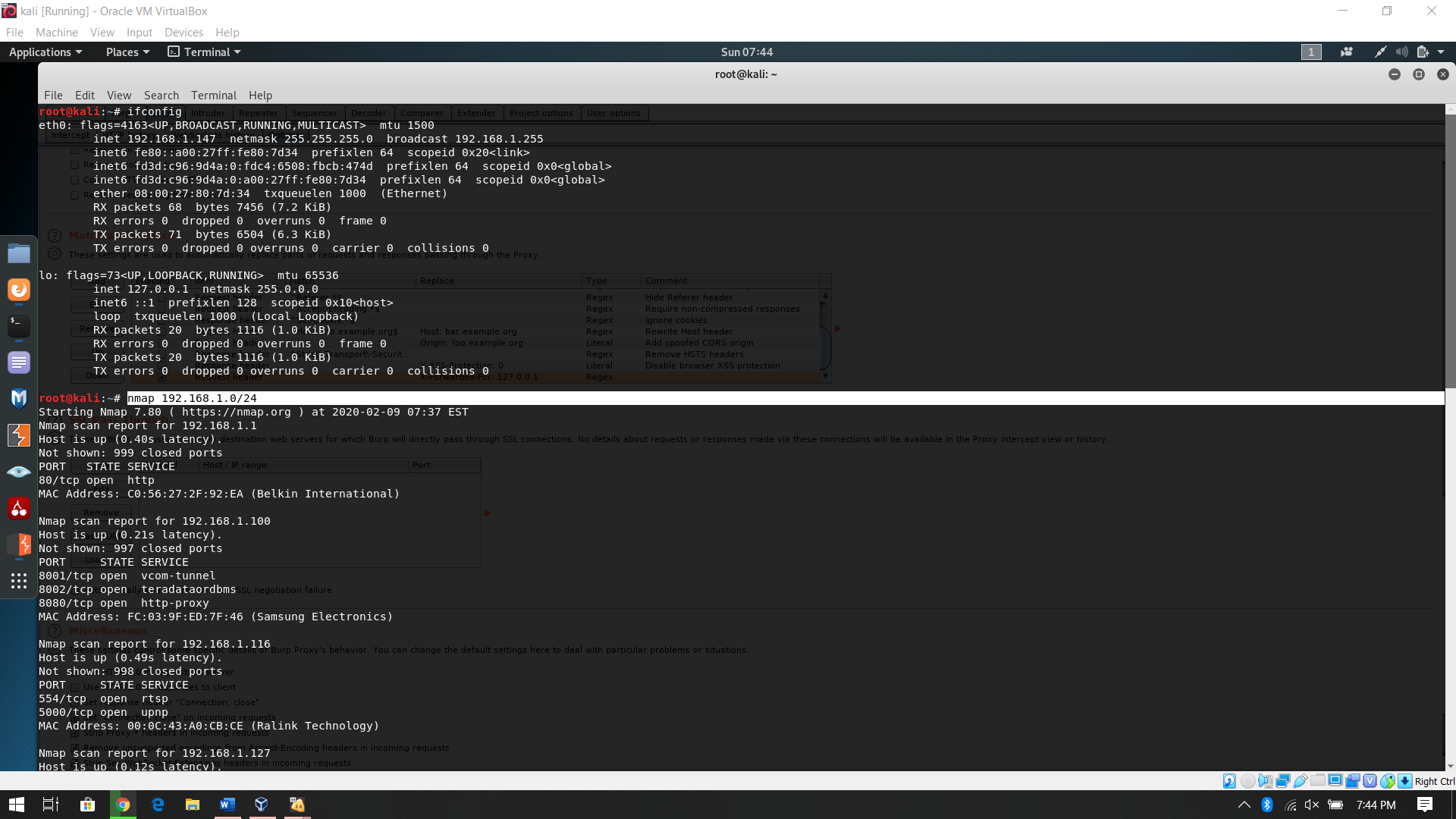
Me and my girlfriend

Link: <https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/>

Diberikan sebuah ova berisikan server yang dipassword



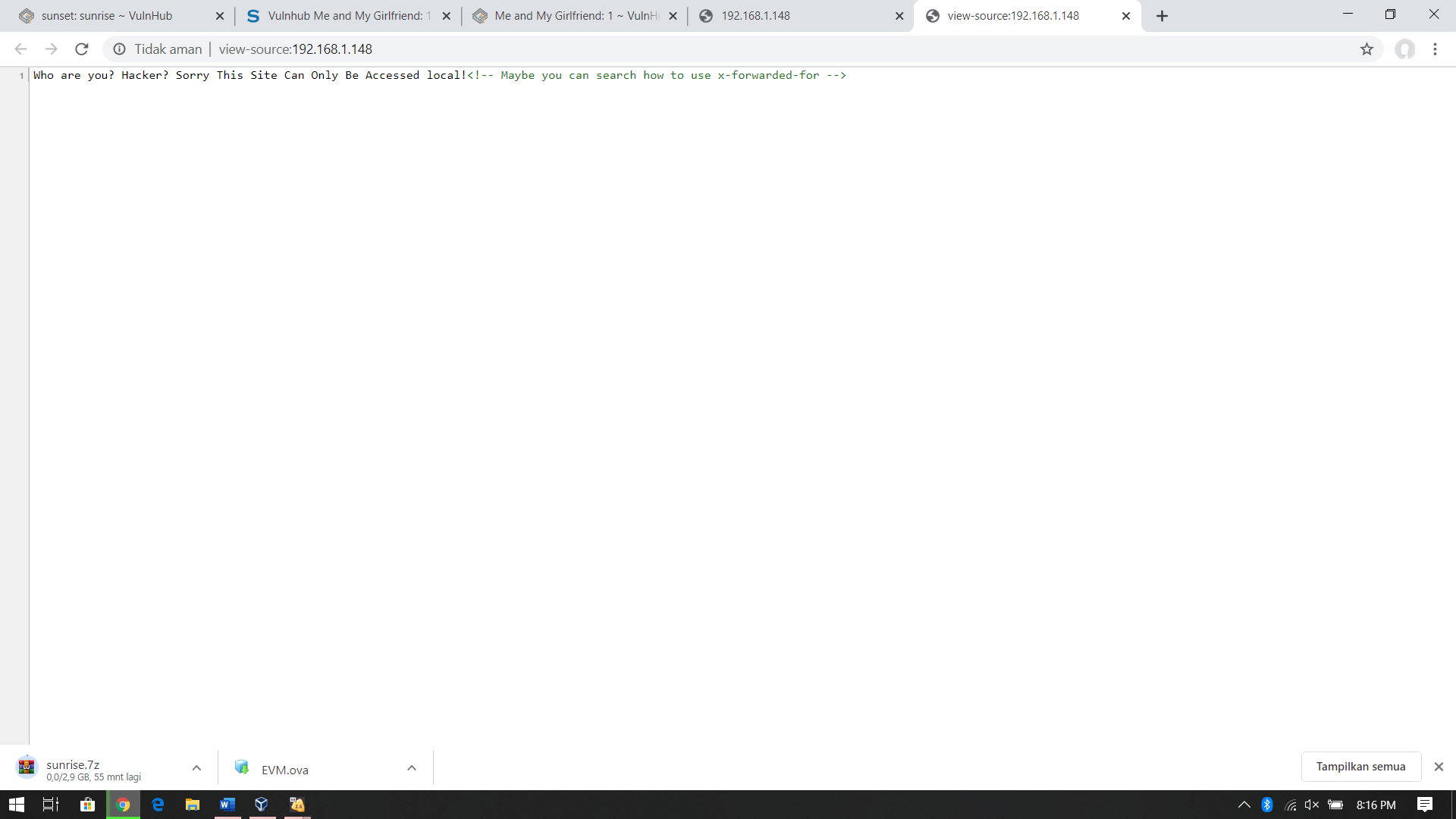
Kemudian lakukan nmap untuk mengetahui ip server



Ip 192.168.1.148 terdapat open port ssh dan http dan saat dibuka menmpilkan seperti iniA screenshot of a computer

Description automatically generated

Saat mencoba inspect element ternyata terdapat hint



X-Forwarded-For merupakan request header yang hanya ditemukan ketika mengakses sebuah server menggunakan proxy HTTP.

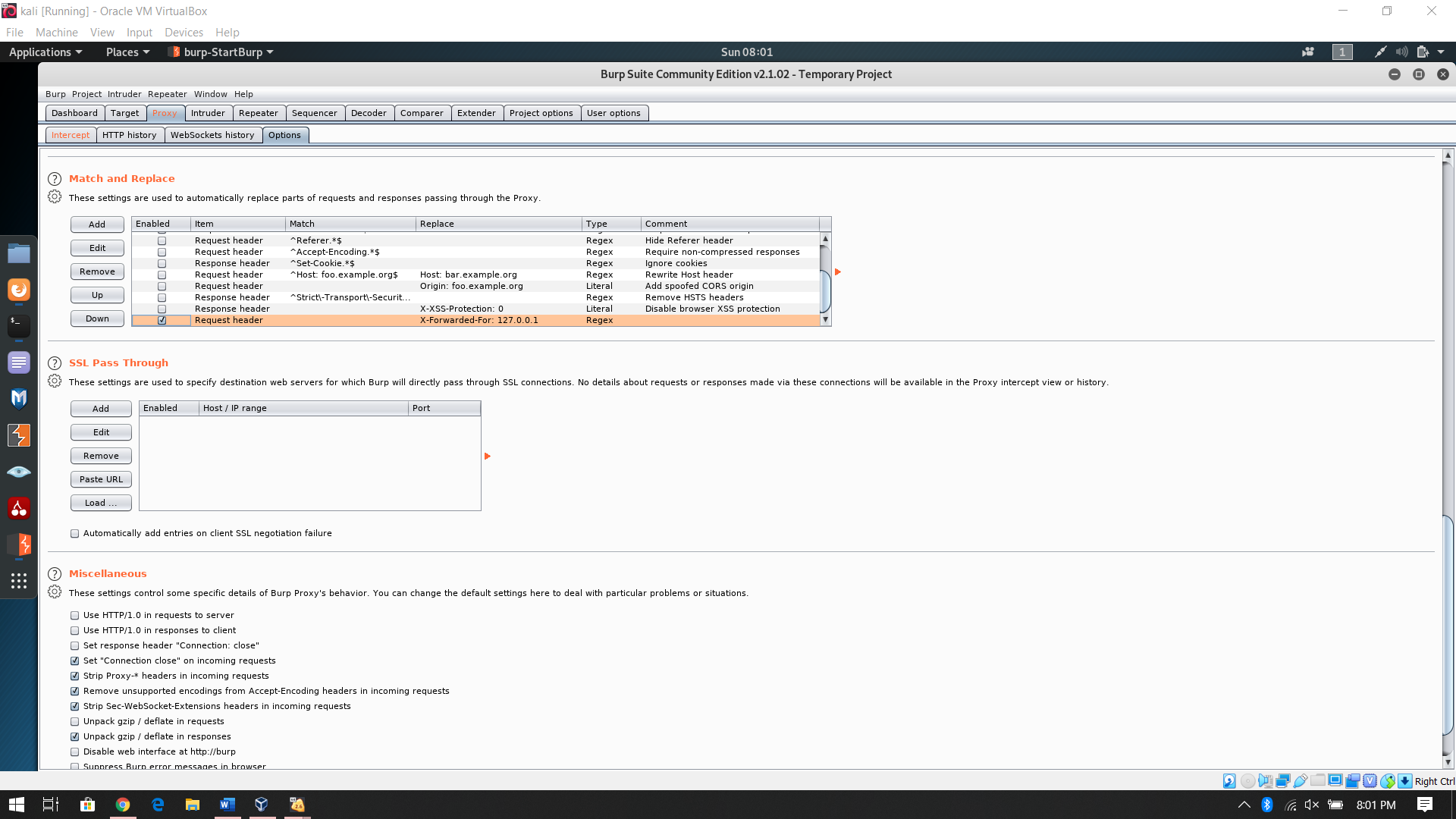
Karena hanya bisa di akses oleh local maka saya mengirimkan request dengan default ip localhost 127.0.0.1 sehingga dikenali sebagai local.

Hal yang saya lakukan adalah menambah request header manual menggunakan burp suite

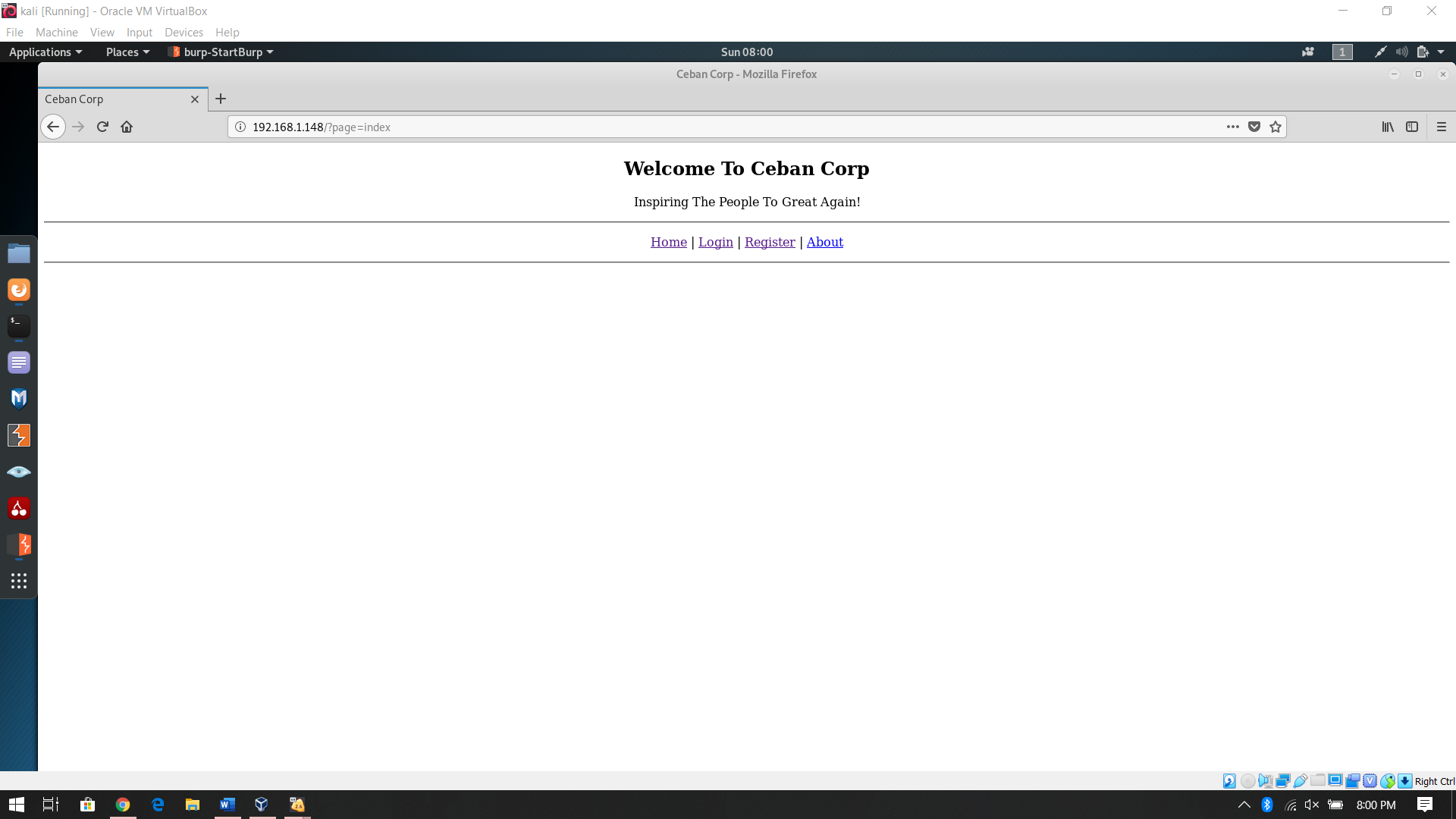
A screenshot of a computer

Description automatically generated

Atau jika tidak ingin menulis ulang maka bisa dilakukan seperti ini

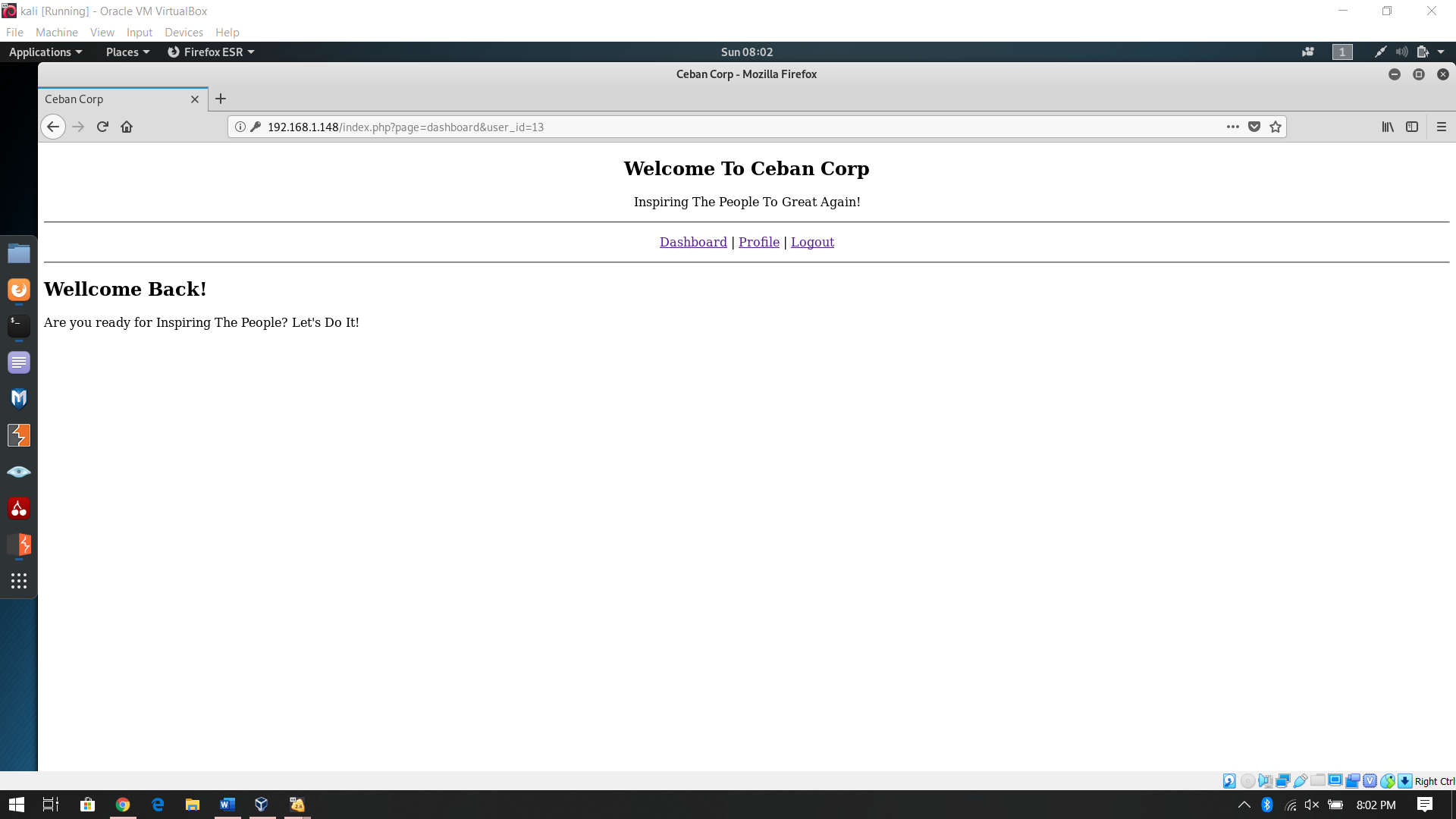


Kemudian barulah web dapat diakses

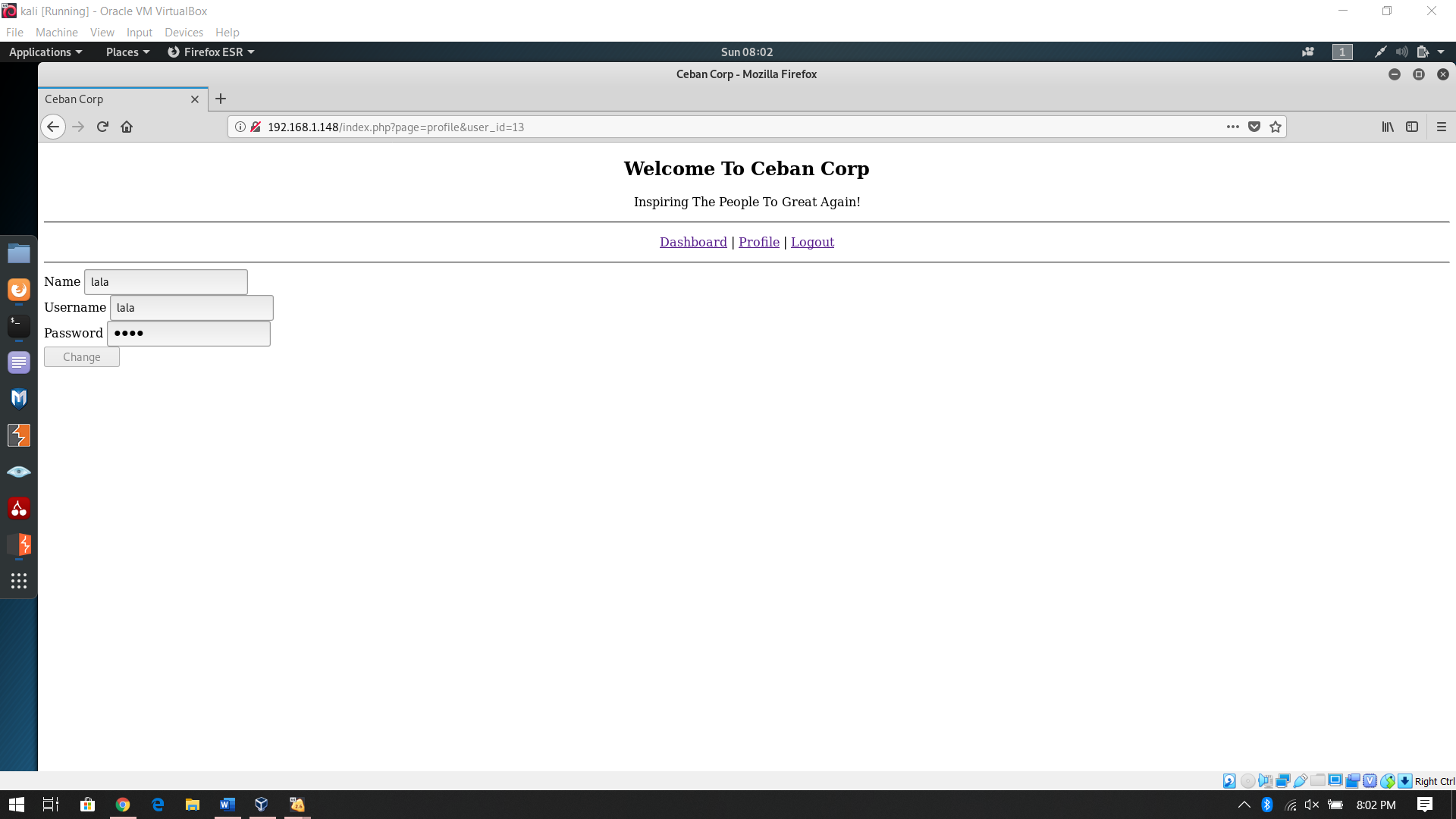


Kemudian lakukan register dan login seperti user biasa

Tampilan web setelah login akan menjadi seperti ini

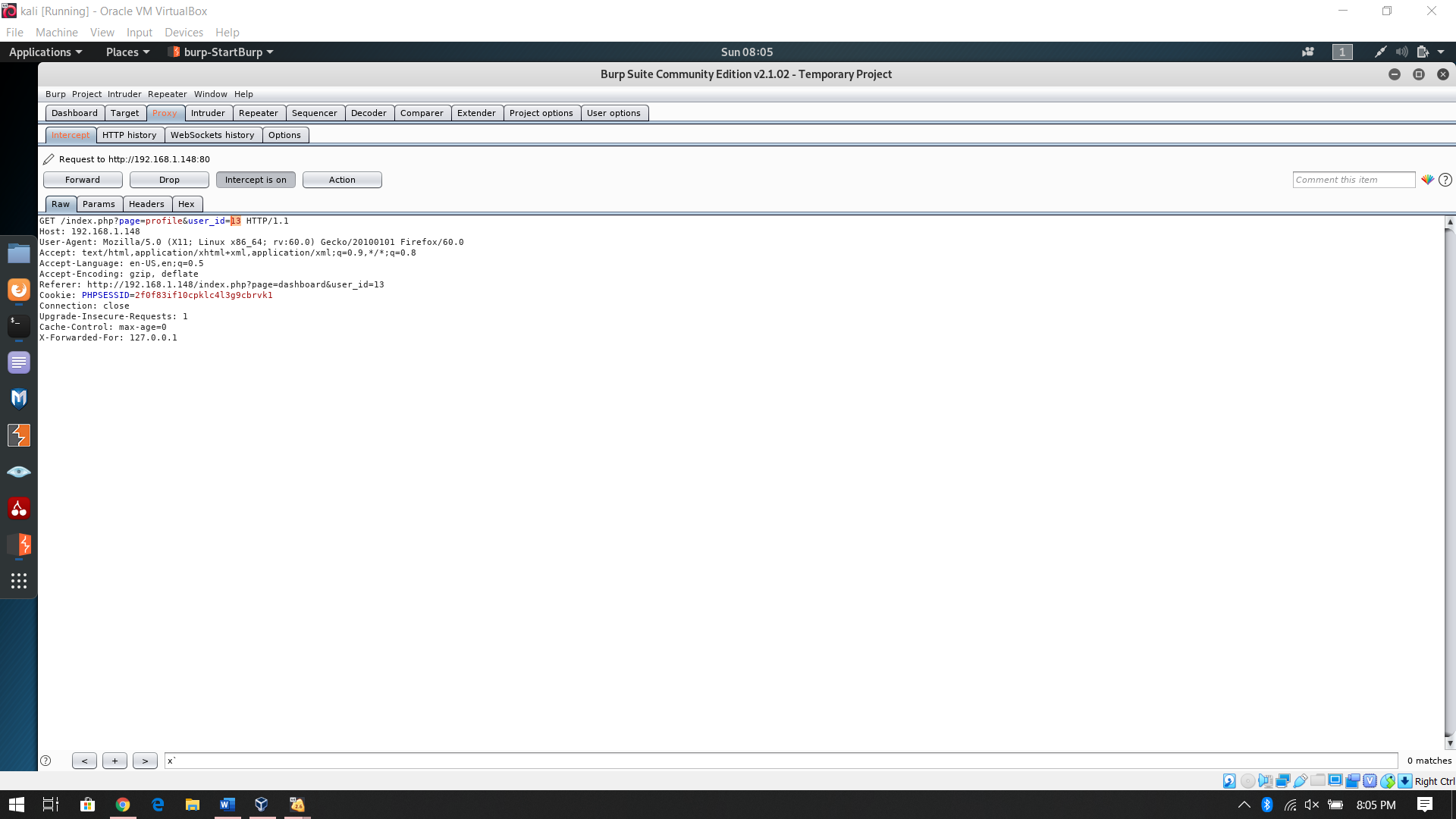


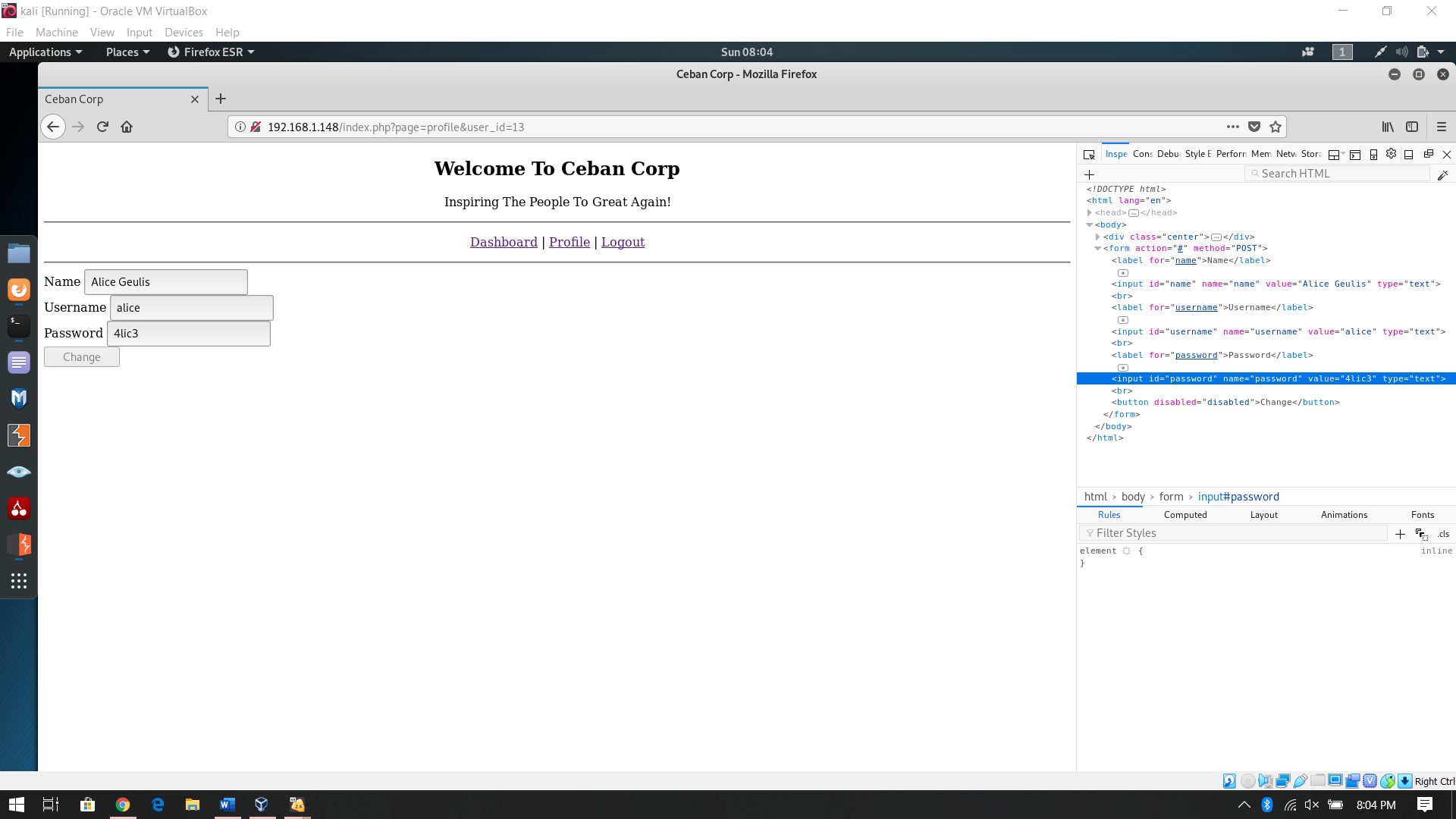
Lalu saya mencoba melihat page profile yang ternyata memunculkan username dan password dari user sesuai dengan user id yang terdapat di url



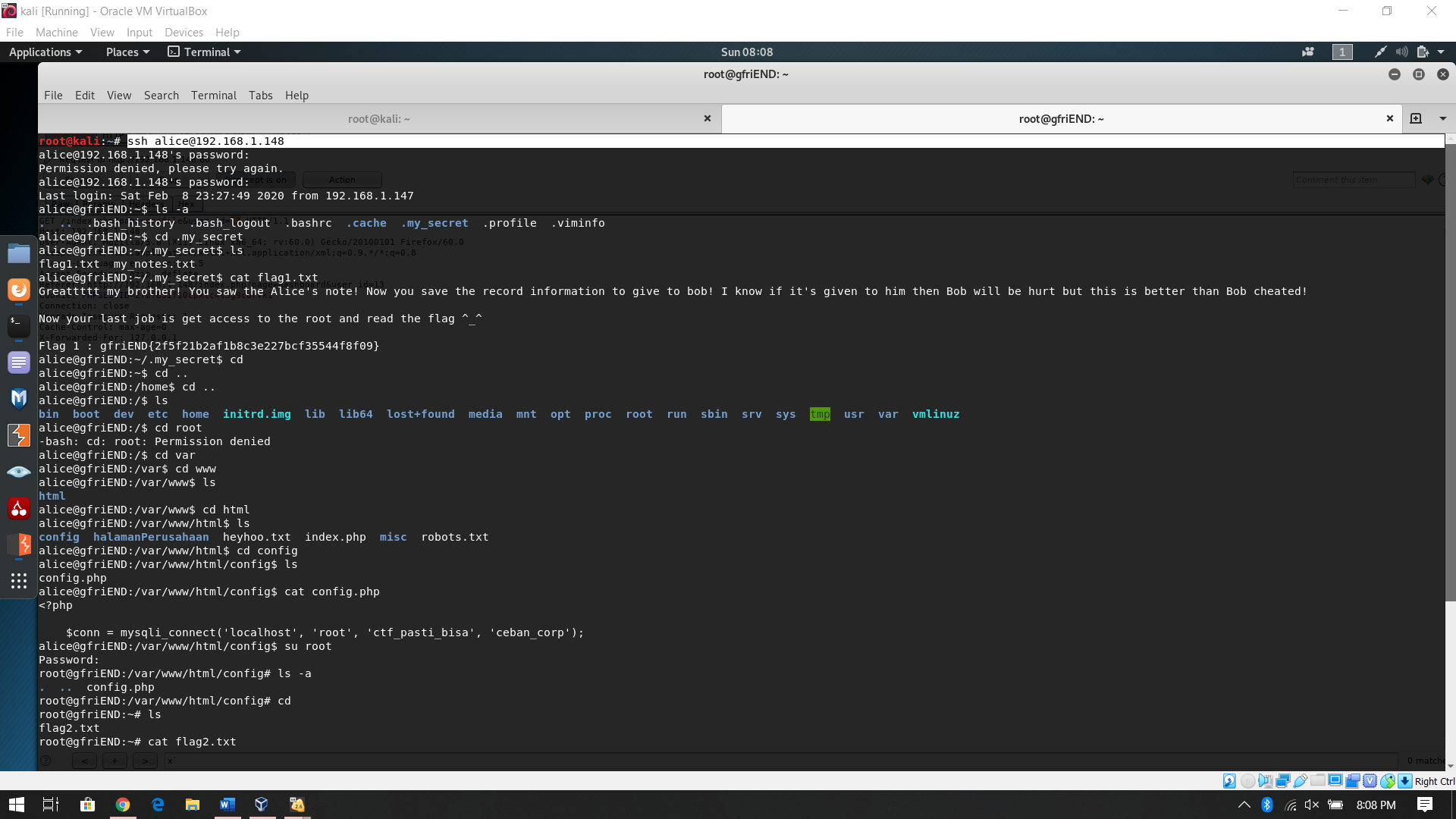
saya merubah user id untuk mencari tahu user lain yang ada

Kemudian pada user id 5 terdapat user yang bernama alice sesuai dengan soal



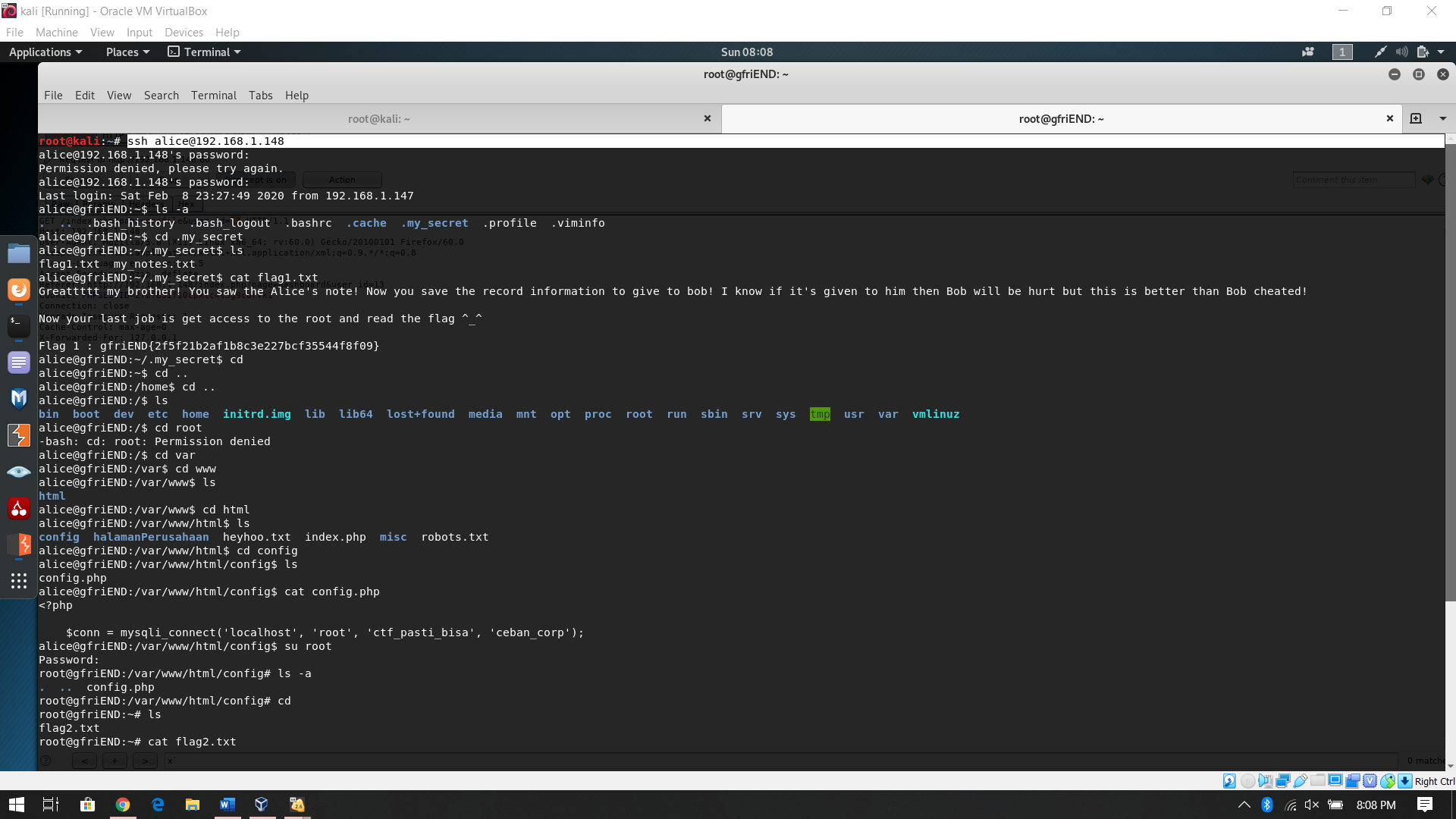


Setelah mendapatkan username dan password, karena port ssh terbuka maka saya mencoba connect melalui ssh dan berhasil mendapatkan flag1.

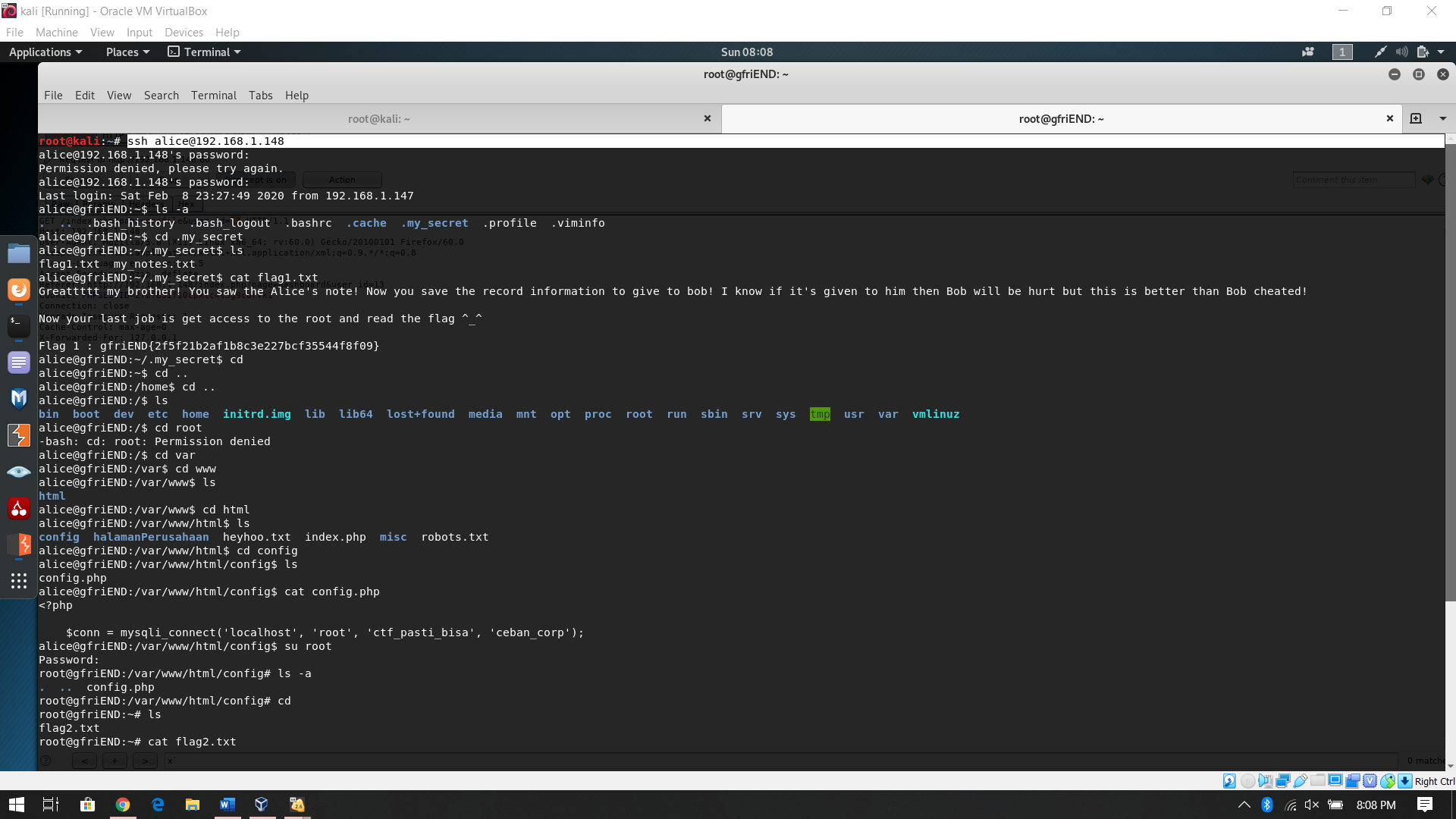


Namun untuk mendapatkan flag2, kita harus menjadi root

Lalu saya melihat lihat file config dan kemudian terdapat username dan password root



Saya menggunakan command ‘su root’ untuk menjadi root. ‘su’ merupakan singkatan dari substitute user atau switch user yang memungkinkan kita mengganti akun di current login session.



Terdapat flag2.txt di root

