**PRAKTIKUM KERENTANAN VDI**



Nama : Choirun Annas

NRP : 3122640032

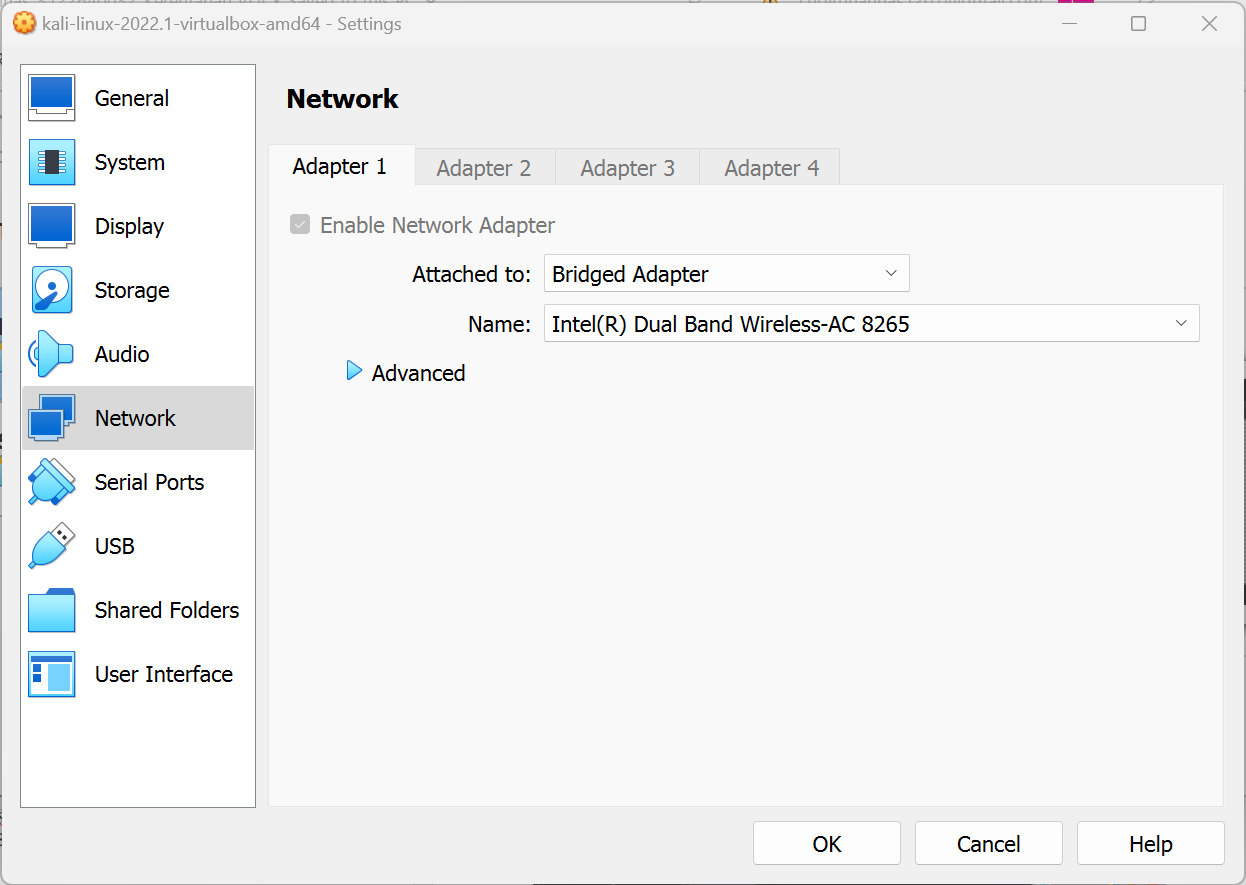
Mata Kuliah : Keamanan Jaringan

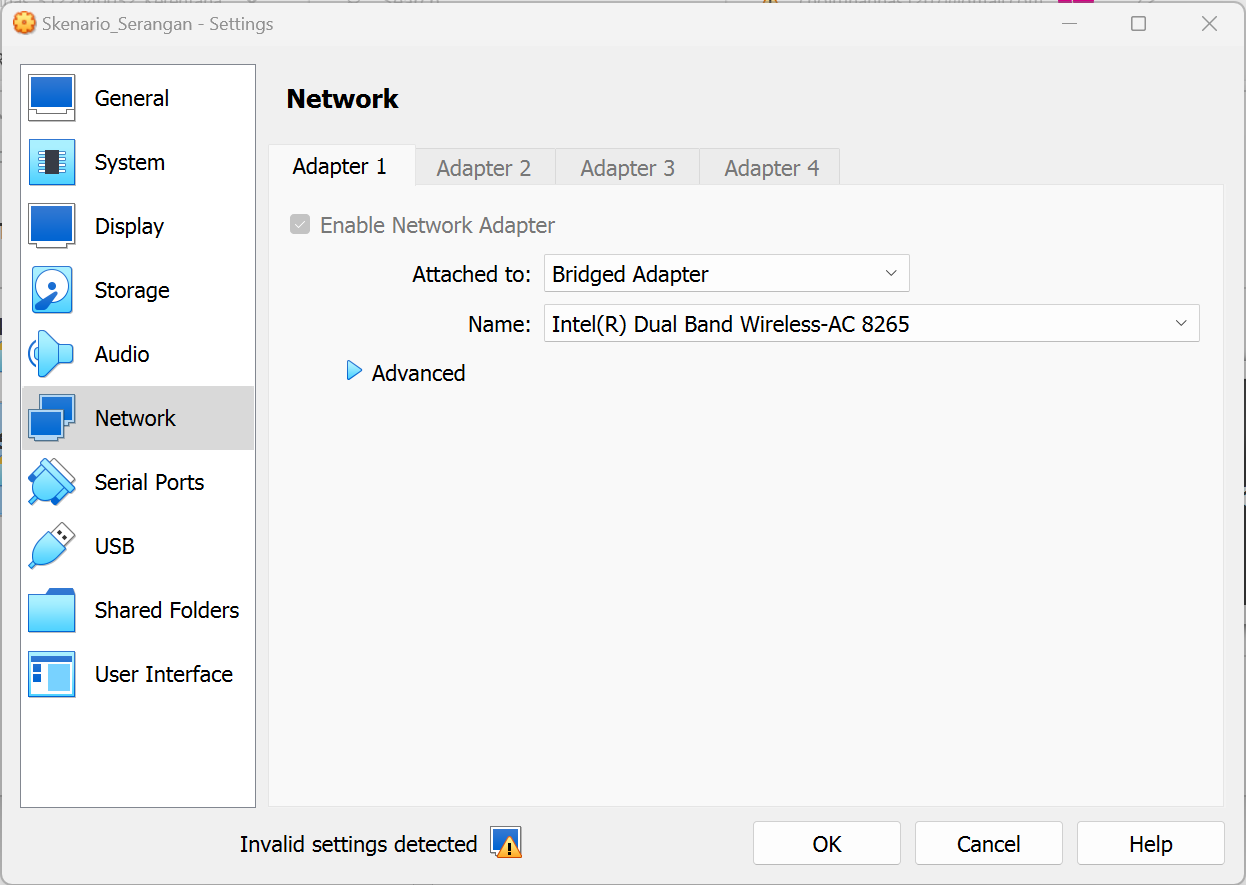
Dosen : Bapak Dr. Ferry Astika Saputra ST, M.Sc

Laporan Praktikum

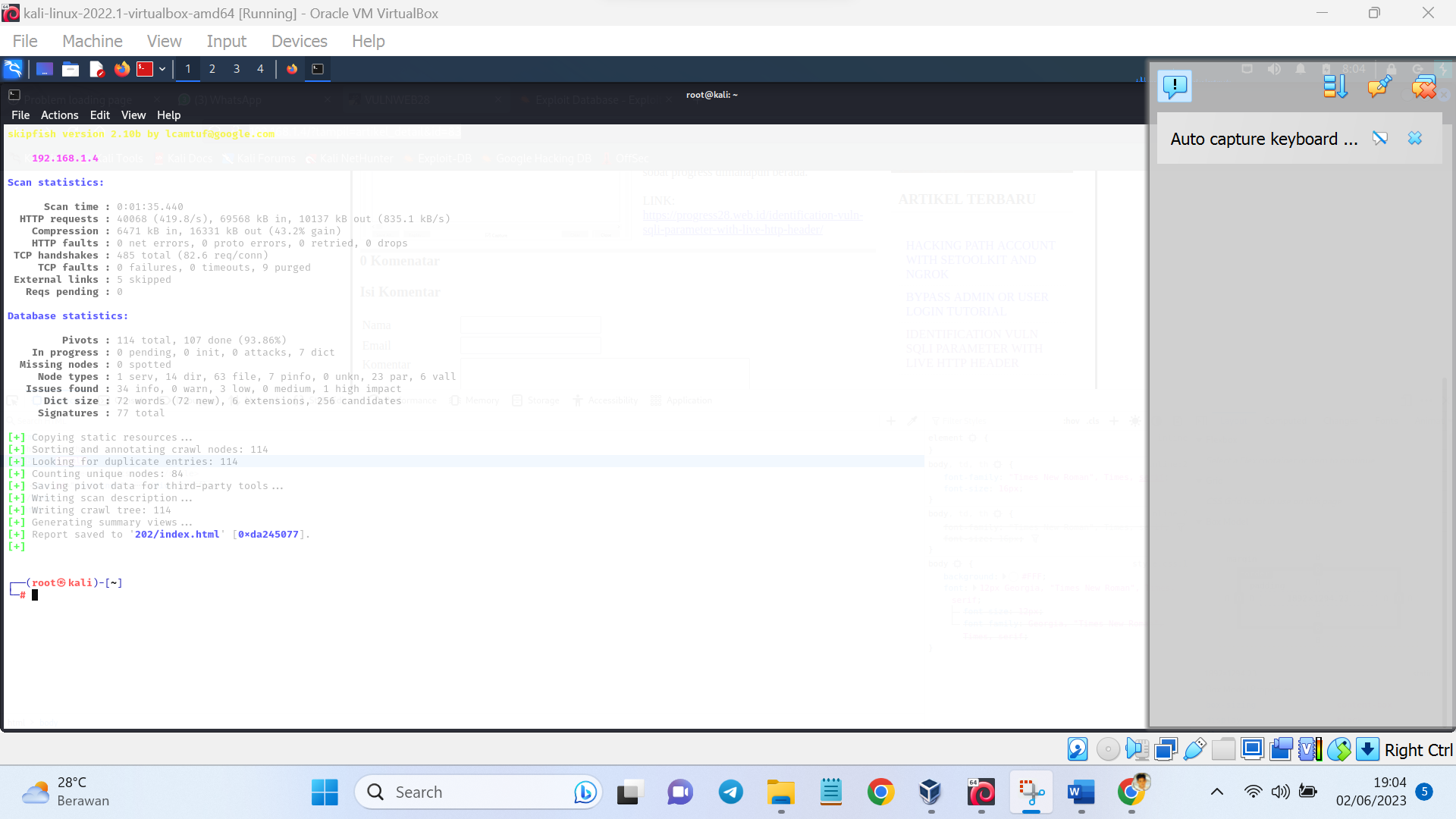
Mengambil data database Menggunakan (sqlmap)

1. Atur network VDI menjadi bridge adapter

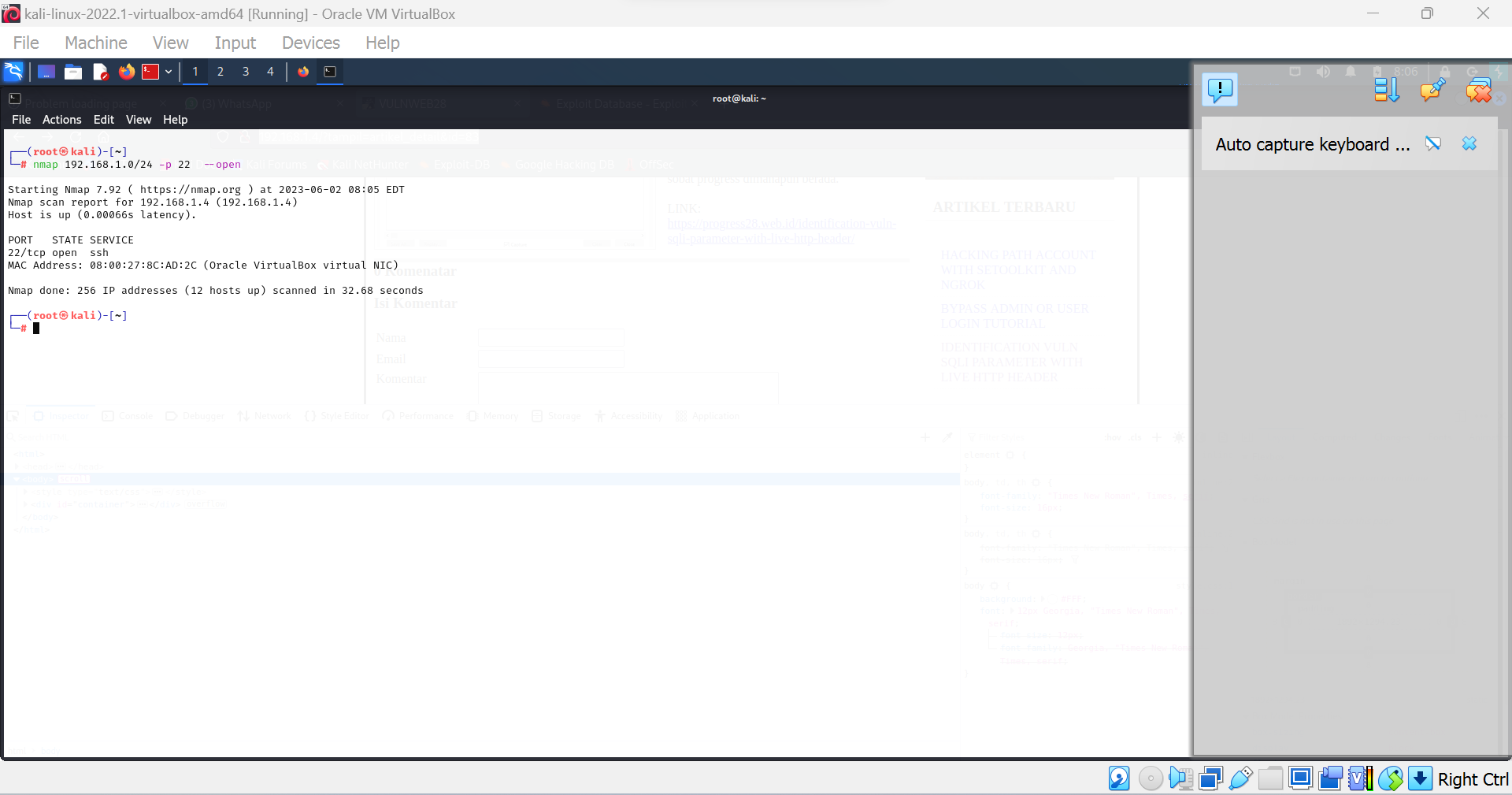




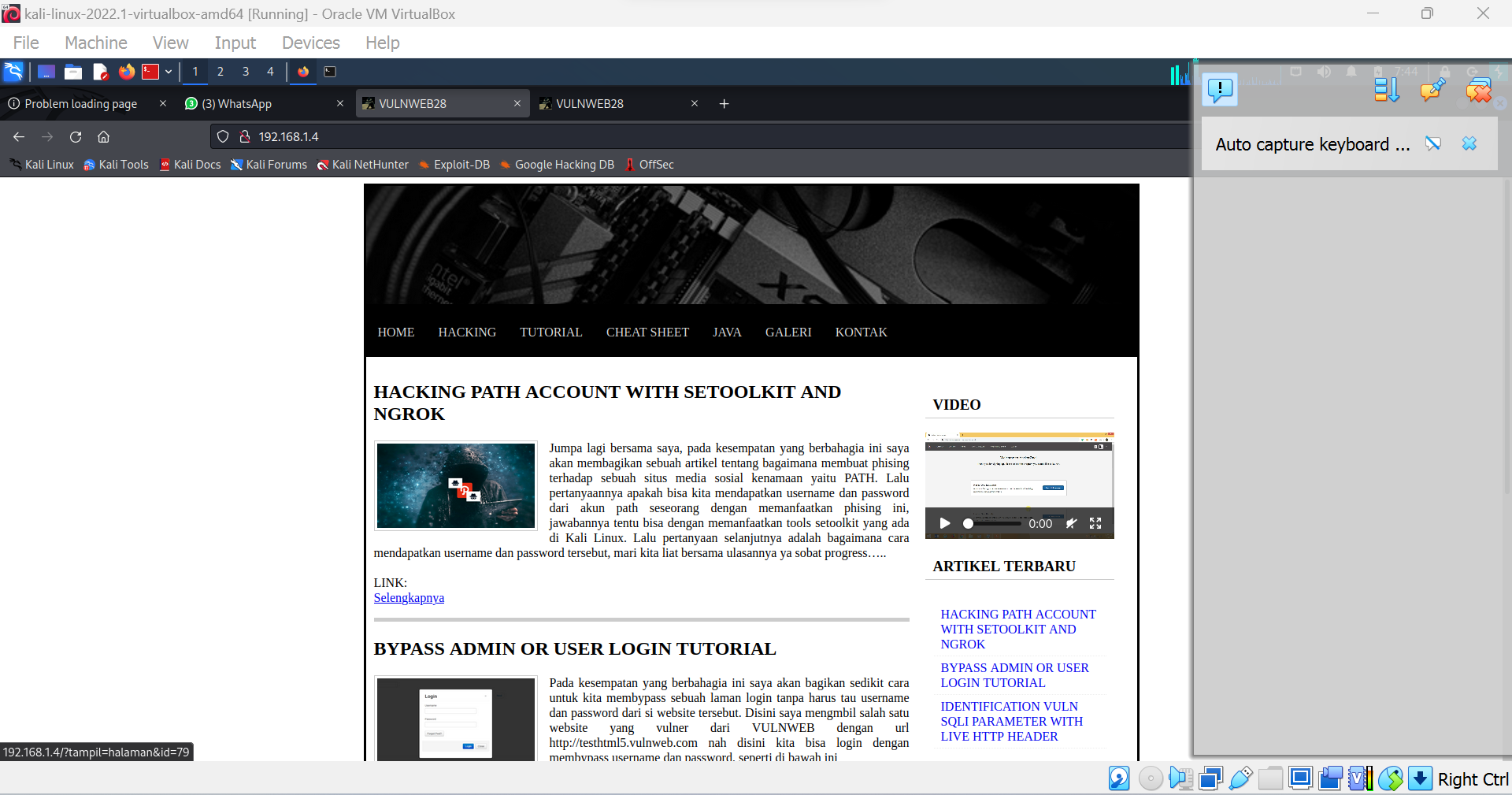
skipfish -o 202 (ip ssh VDI)



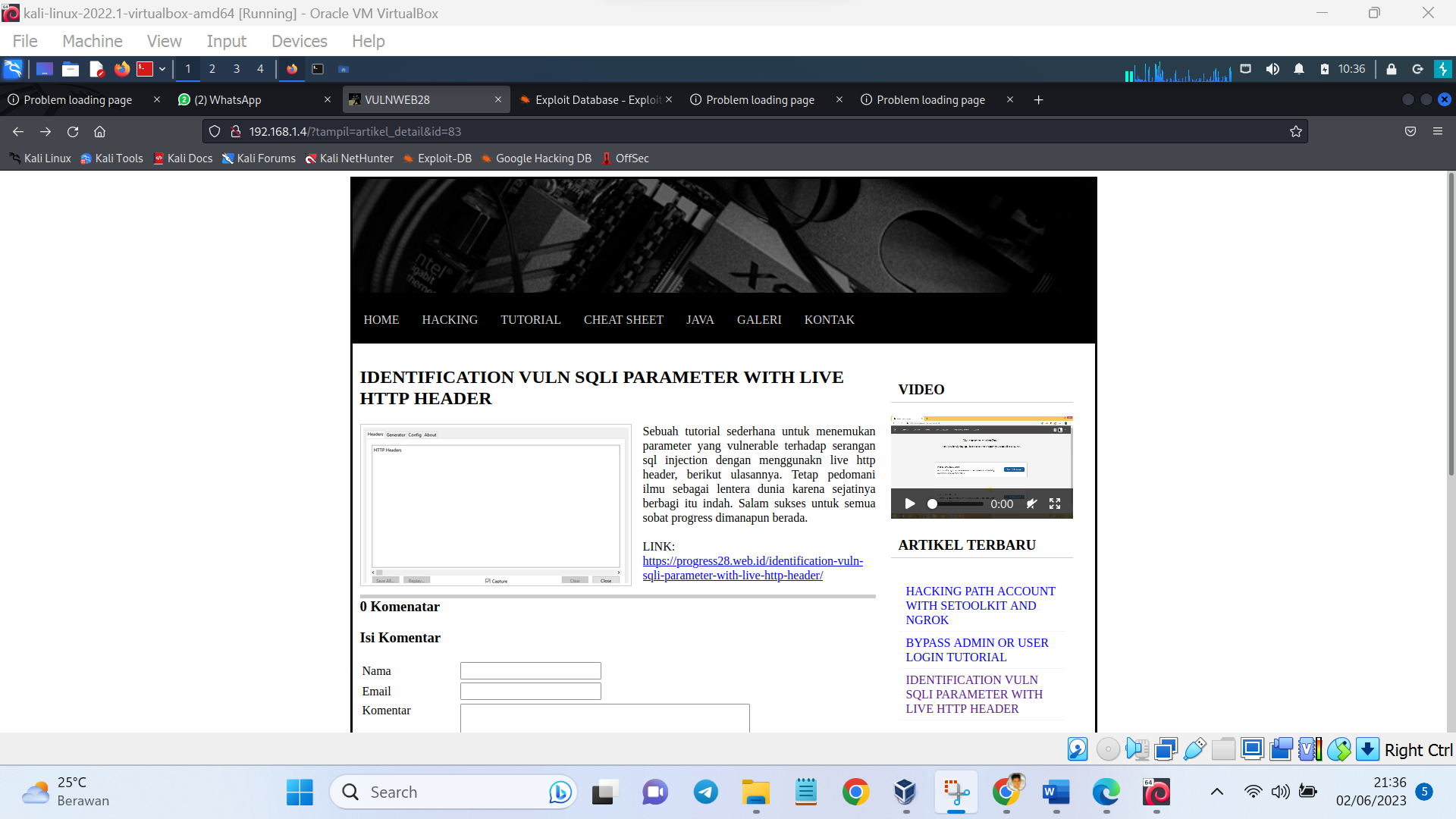
2. Panggil ip VDI serangan menggunakan nmap lewat ip di kali linux



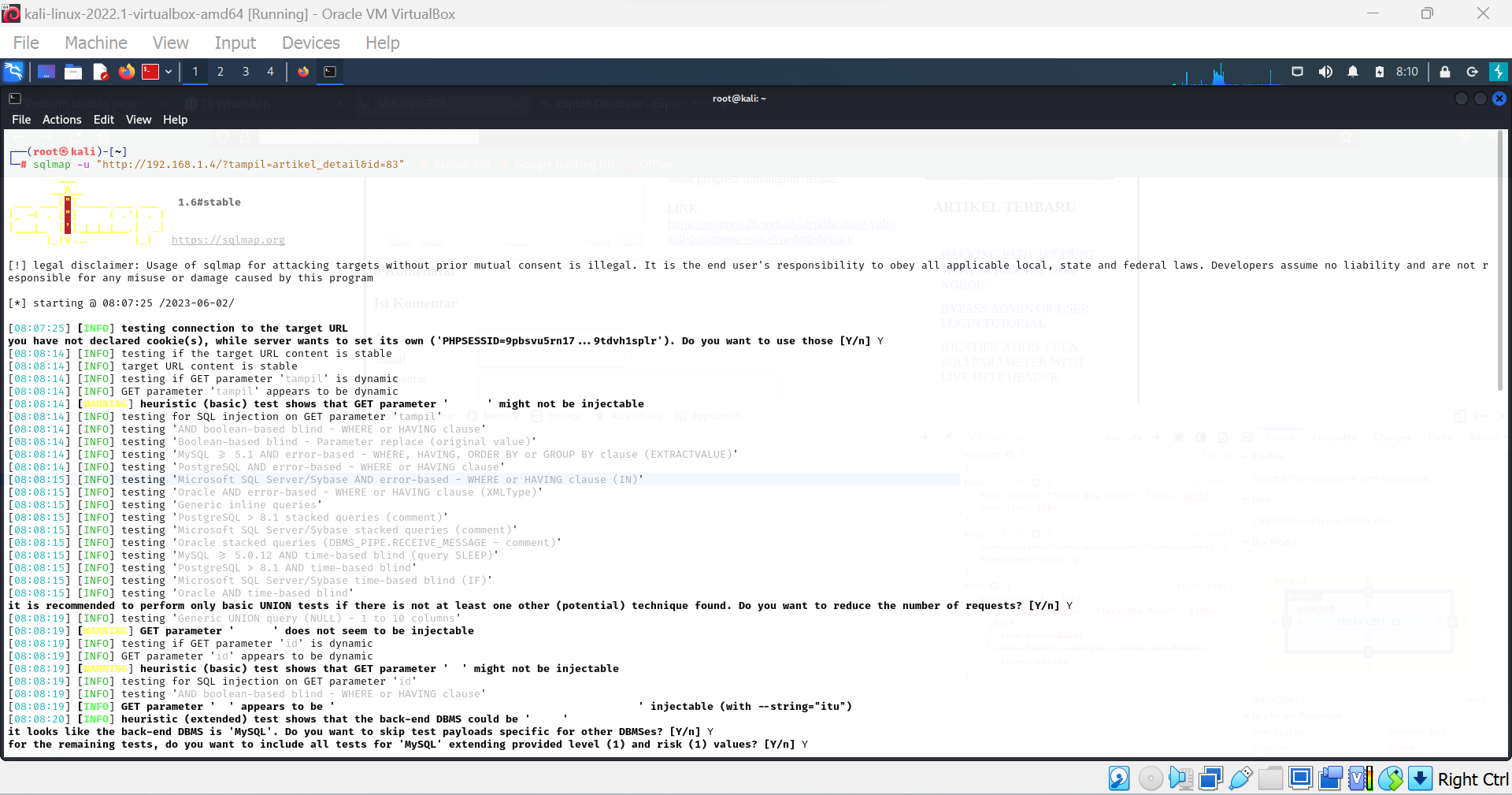
3. Taruh link ip ke web browser maka muncul website VULNWEB28



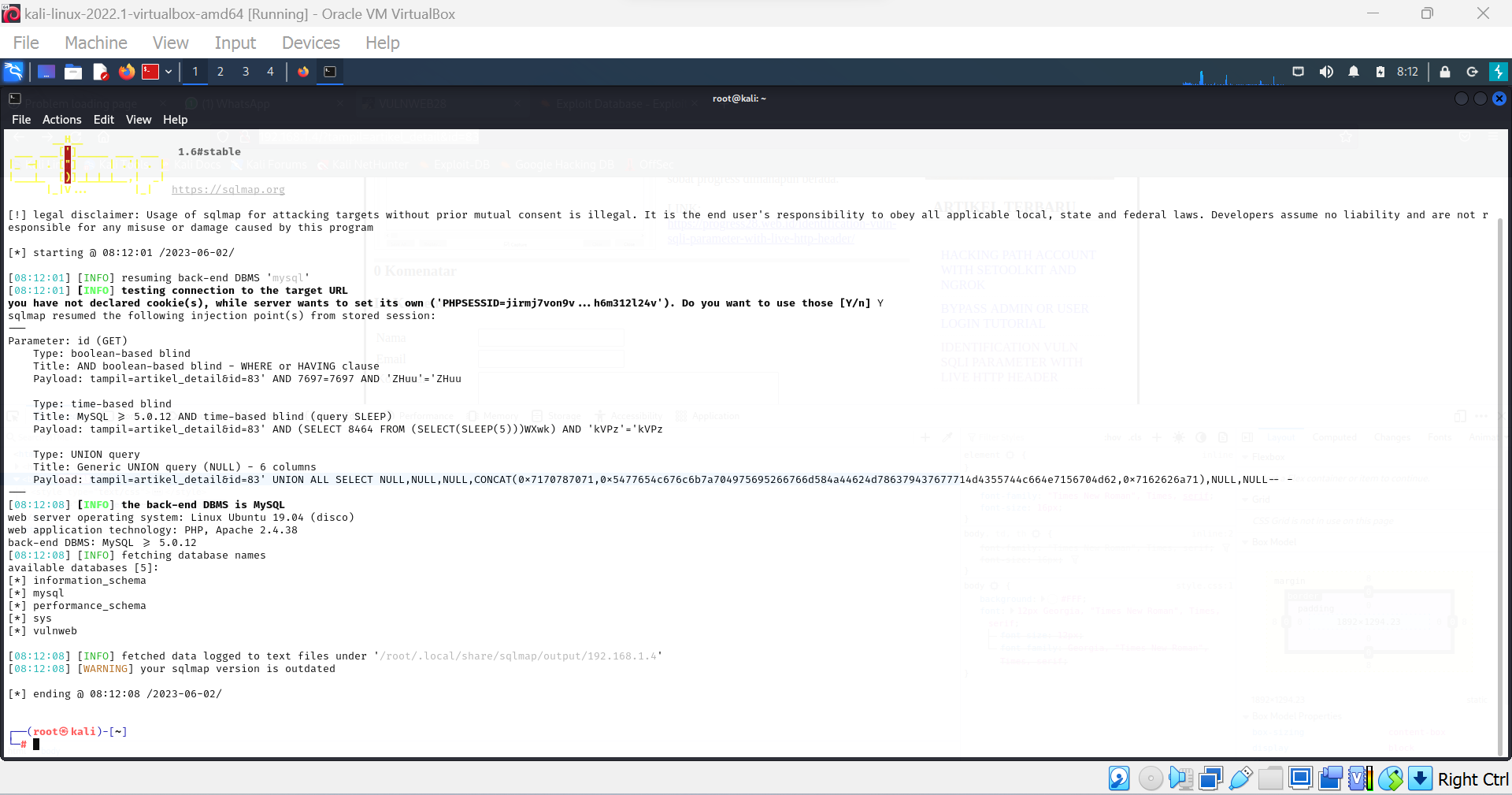
Cari link yg menggunakan id pada website di sini saya memakai id 85



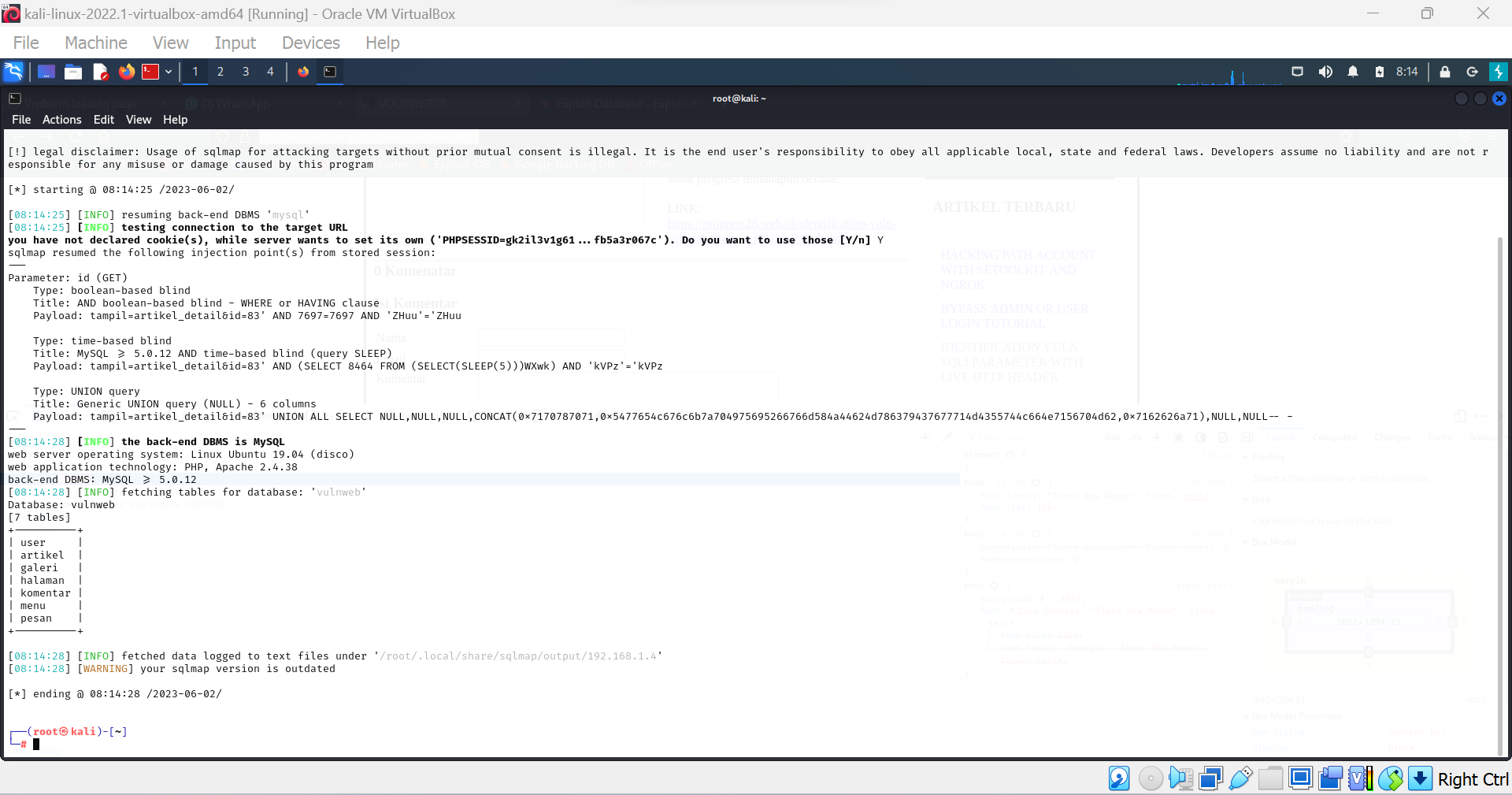
4. Melakukan sqlmap pada link website sqlmap -u <http://192.168.1.4/?tampil=artikel_detail&id=83> --dbs



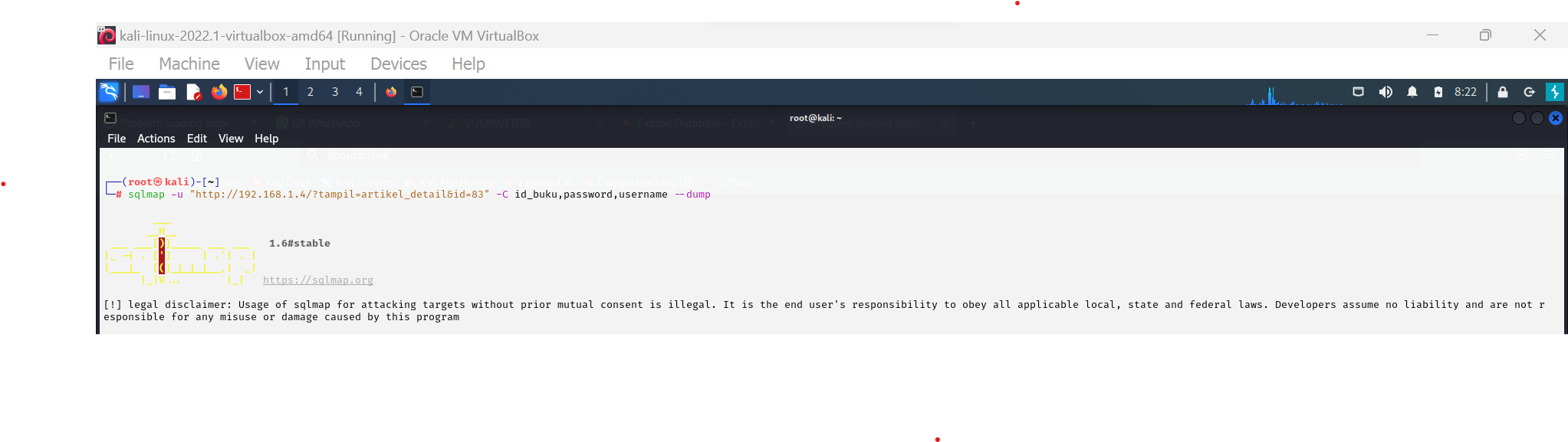
5. Setelah muncul daftar database pilih vulnweb

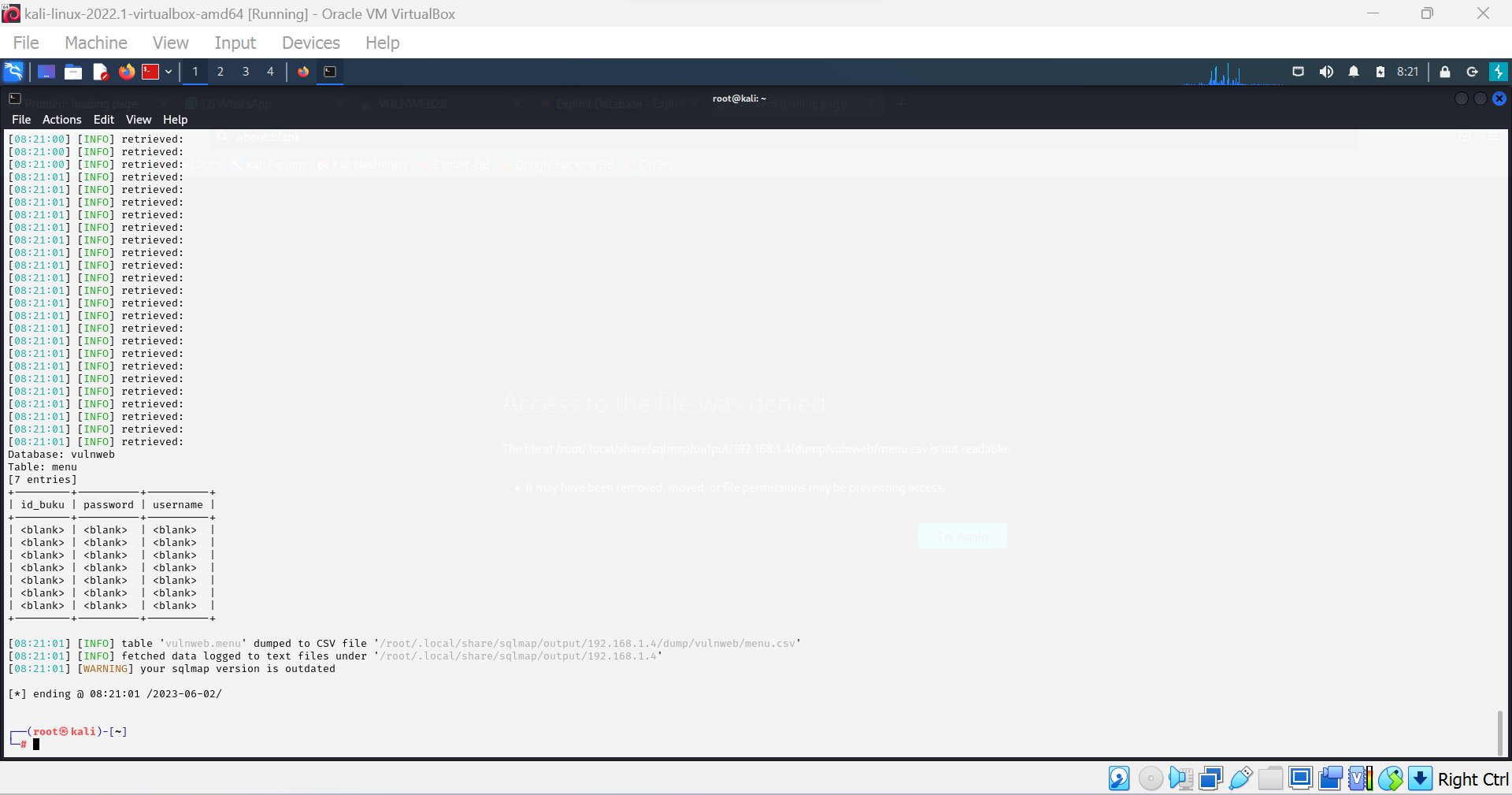


6. Lakukan pemanggilan database sqlmap -u "http://192.168.1.4/?tampil=artikel\_detail&id=83" -D idvulnewb --tables



7. sqlmap -u "http://192.168.1.4/?tampil=artikel\_detail&id=83" -C id\_buku,password,username –dump untuk memanggil data dari kolom yang dimasukkan

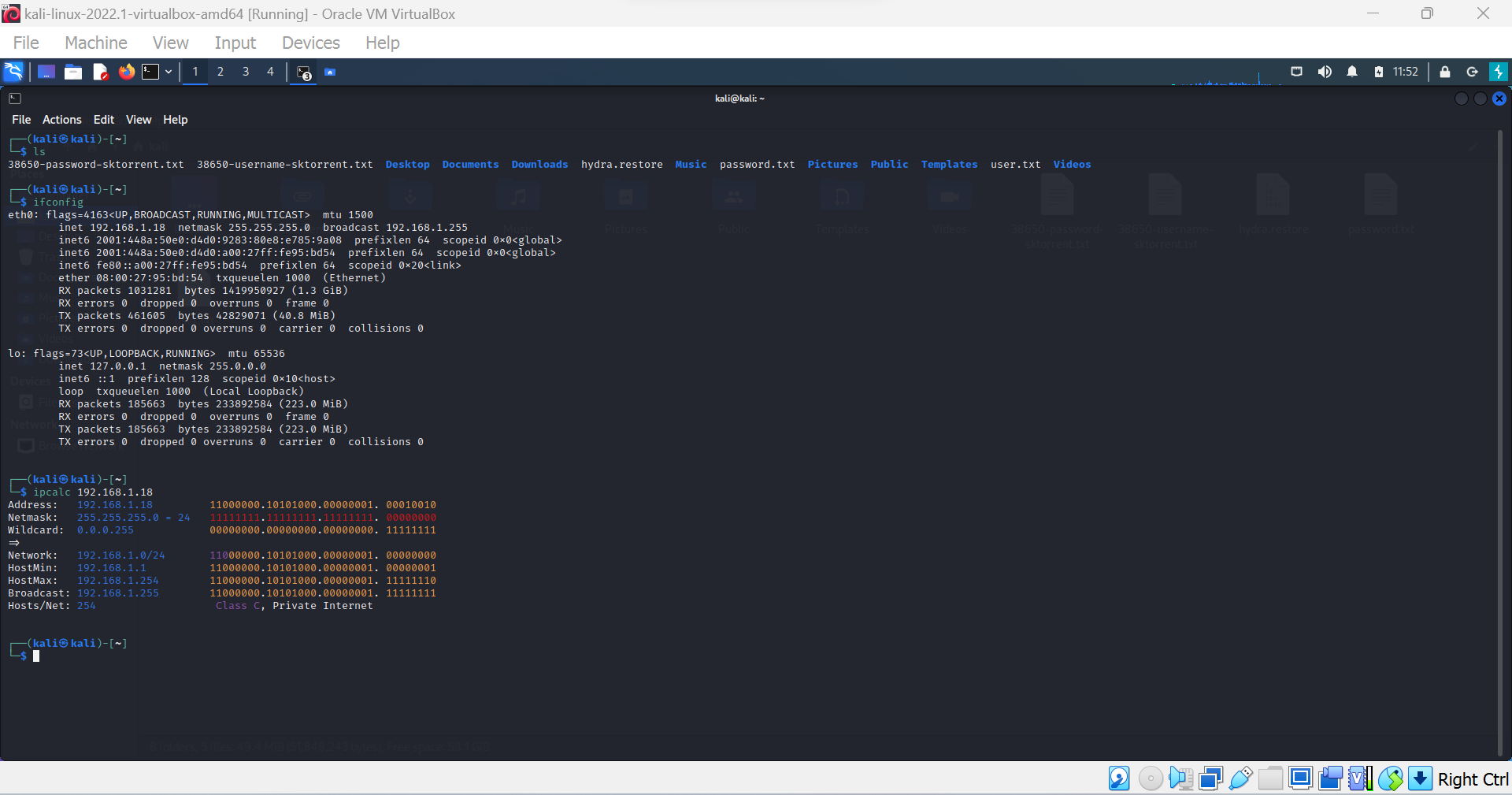




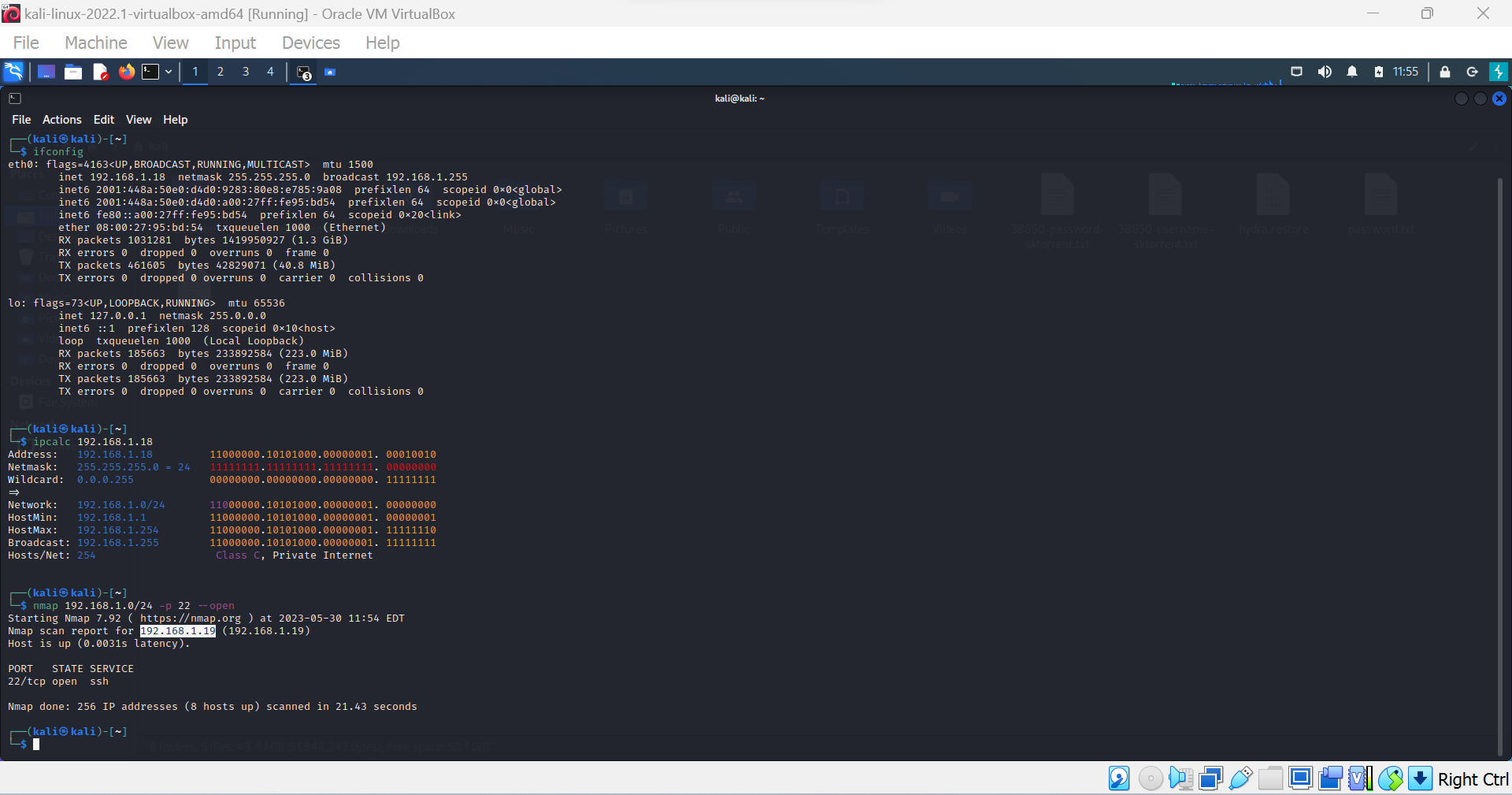
Hasilnya akan muncul file csv dari website vulnewb pada percobaan diatas saya mencoba mengambil data user dari database vulnweb.

Mencari tahu password root Menggunakan (hydra - untuk bruteforce attack)

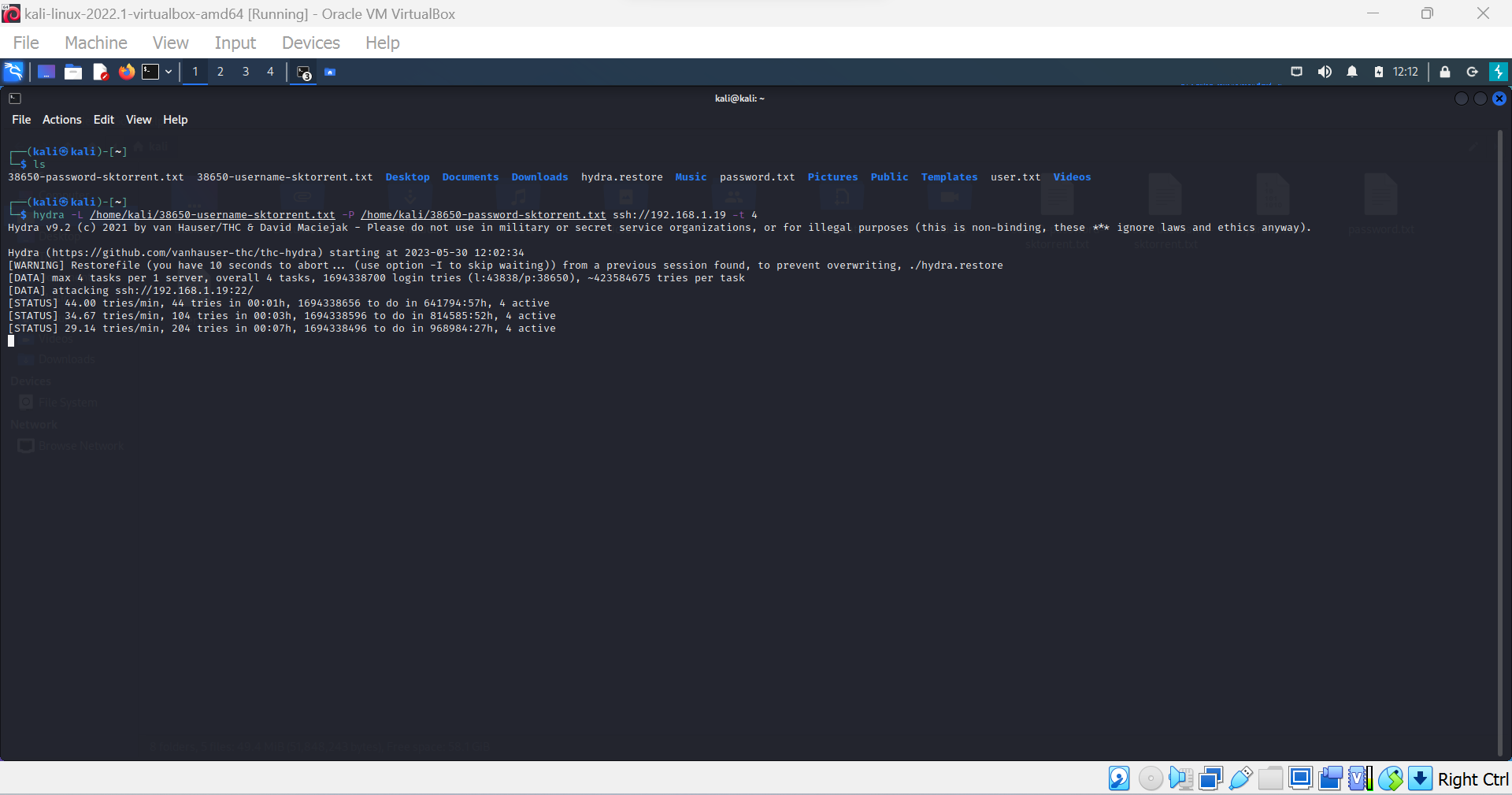
1. Siapkan file txt username dan password



2. Mengecek port terbuka dan lakukan nmap untuk menemukan ssh VDI



3. Lakukan hydra untuk melakukan attack untuk menemukan username dan password yang cocok



Hasil : Dalam proses tersebut saya menghabiskan waktu sekitar 20 jam lebih untuk melakukan attack ke VDI dengan proses percobaan kemungkinan sebesar 100 ribu data dan kurang 4 miliar data kemungkinan data yang belum di cek. Saya menggunakan data dari <https://github.com/duyet/bruteforce-database> untuk melakukan brute force attack