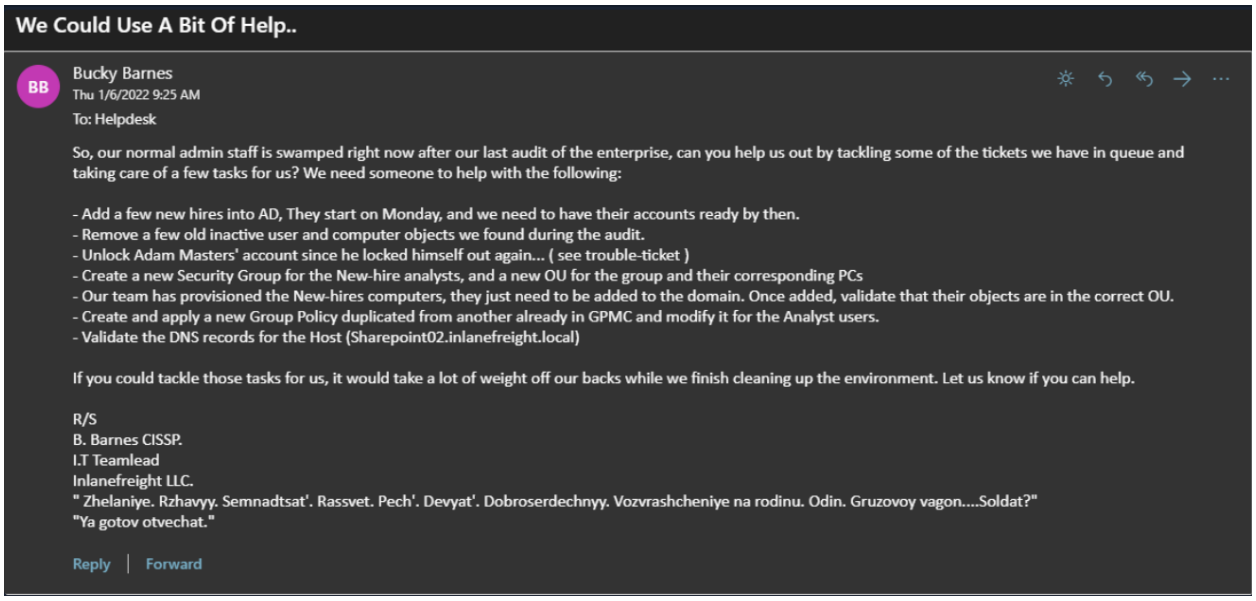
Active Directory Administration

Project Description

Let's consider the following case:



We Could Use A Bit Of Help..

BB

Bucky Barnes
Thu 1/6/2022 9:25 AM
To: Helpdesk

So, our normal admin staff is swamped right now after our last audit of the enterprise, can you help us out by tackling some of the tickets we have in queue and taking care of a few tasks for us? We need someone to help with the following:

- Add a few new hires into AD, They start on Monday, and we need to have their accounts ready by then.
- Remove a few old inactive user and computer objects we found during the audit.
- Unlock Adam Masters' account since he locked himself out again... (see trouble-ticket)
- Create a new Security Group for the New-hire analysts, and a new OU for the group and their corresponding PCs
- Our team has provisioned the New-hires computers, they just need to be added to the domain. Once added, validate that their objects are in the correct OU.
- Create and apply a new Group Policy duplicated from another already in GPMC and modify it for the Analyst users.
- Validate the DNS records for the Host (Sharepoint02.inlanefreight.local)

If you could tackle those tasks for us, it would take a lot of weight off our backs while we finish cleaning up the environment. Let us know if you can help.

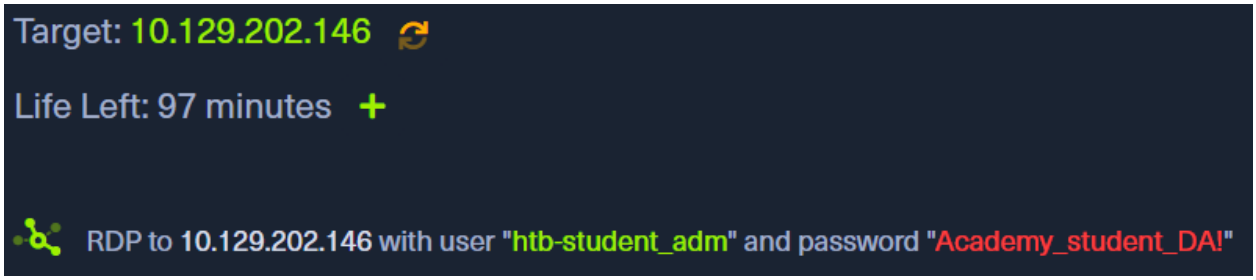
R/S
B. Barnes CISSP.
I.T Teamlead
Inlanefreight LLC.
" Zhelaniye. Rzhavyy. Semnadtsat'. Rassvet. Pech'. Devyat'. Dobroserdechnyy. Vozvrashcheniye na rodinu. Odin. Gruzovoy vagon....Soldat?"
"Ya gotov otvechat."

Reply | Forward

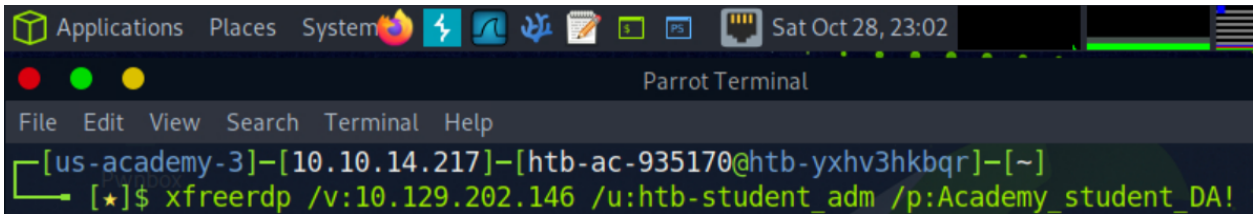
In this section, I will serve as a domain administrator to Inlanefreight for a day. I have been tasked to help the IT department close some work orders, so I will be performing actions such as adding and removing users and groups, managing group policy, and more.

Walkthrough

For this project, I will have access to a domain-joined Windows server from which I can perform any actions needed to complete this project. I will utilize Remote Desktop Protocol (RDP) from Pwnbox to the Windows Server.



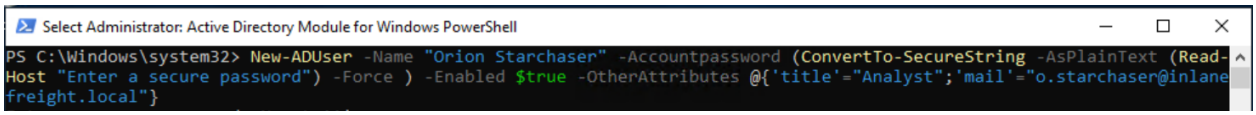
In the image above, I spawned the target host and obtained an IP address, username, and a password.



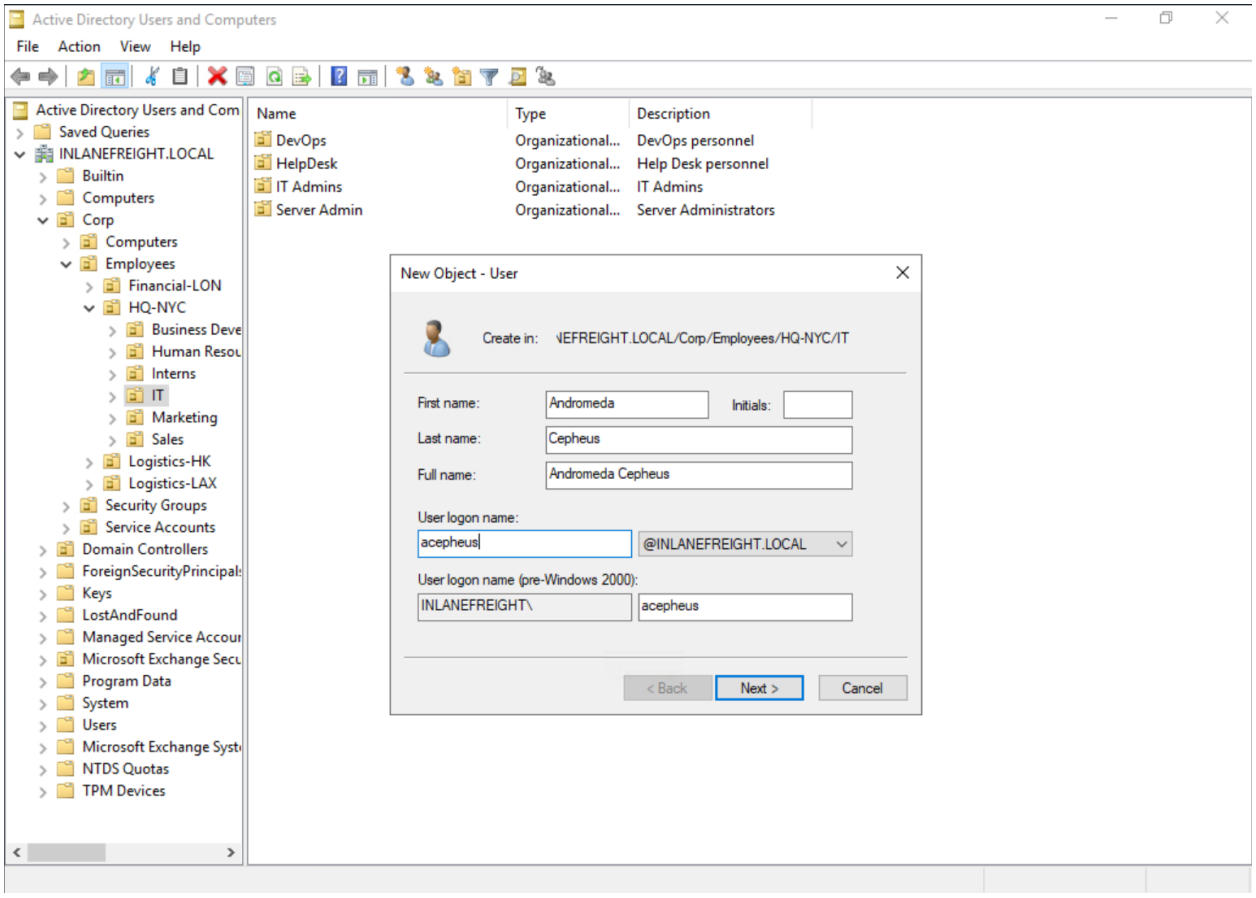
Then, I opened a terminal in pwnbox, used xfreerdp to connect with the target and entered the command xfreerdp /v:10.129.202.146 /u:htb-student_adm /p:Academy_student_DA! as displayed above. Once connected, I will open PowerShell to begin the tasks.

Task 1: Manage Users

The first task includes adding a few new-hire users into AD. I will create them under the “inlanefreight.local” scope, drilling down into the "Corp > Employees > HQ-NYC > IT" folder structure for now. Users to add are: Orion Starchaser, Andromeda Cepheus, and Artemis Callisto. Each user should have the following attributes: full name, email, display name, and User must change password at next logon. For the first user, I ran PowerShell as an administrator and entered the following command to add the user along with their attributes: PS C:\htb> New-ADUser -Name "Orion Starchaser" -Accountpassword (ConvertTo-SecureString -AsPlainText (Read-Host "Enter a secure password") -Force) -Enabled $true-OtherAttributes@{‘title’=”Analyst”;’mail’=o.starchaser@inlanefreight.local"}. After I hit enter, a prompt appeared, then entered a secure password for the user.



For the other two users, I will use the Active Directory Users and Computers (ADUC). As demonstrated in the picture below, I began adding a new user under the IT folder.



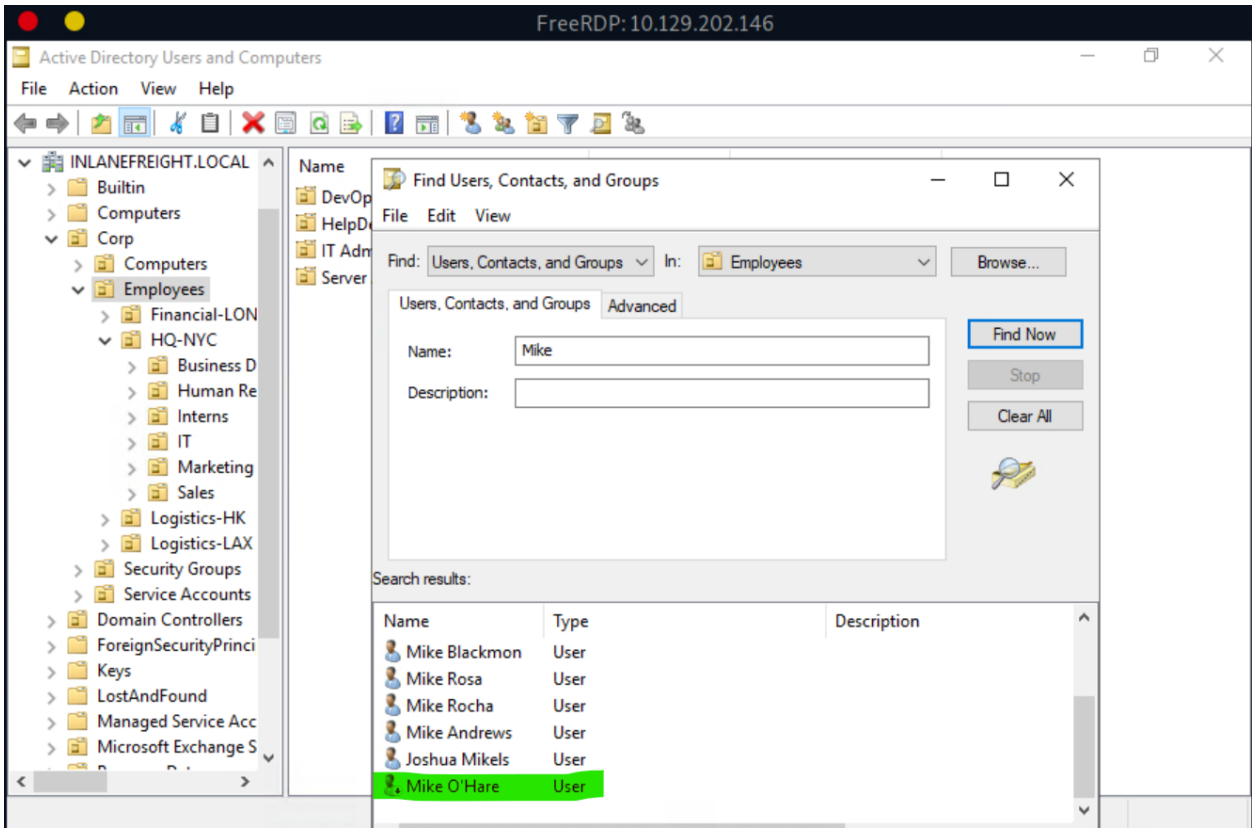
After I hit next, I assigned the password NewP@ssw0rd123! and checked the box for “User must change password at next logon”. Then, I hit Next, and finally Finish. These same steps were repeated to add the user Artemis Callisto.

Next, I’ll proceed to remove users. Users to remove are Paul Valencia and Mike 0’Hare. The first one will be removed through Powershell. As demonstrated in the picture below, The Remove-ADUser cmdlet targets the user by its user logon name.

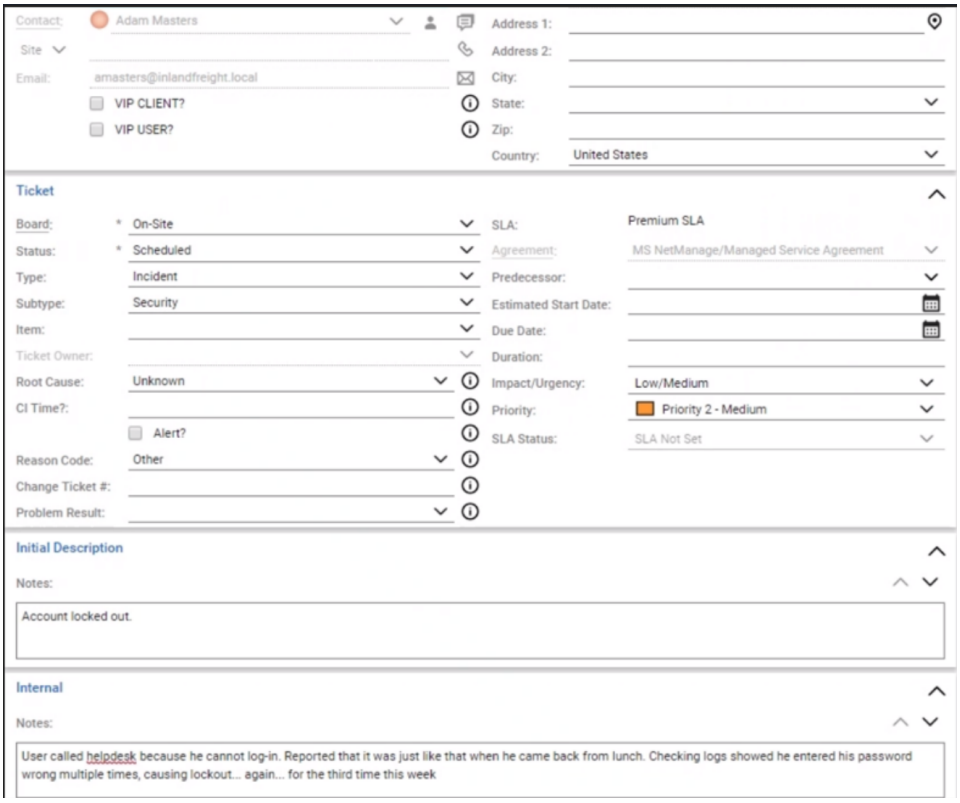
```
Active Directory Module for Windows PowerShell
PS C:\Users\htb-student_adm> Remove-ADUser -Identity pvalencia

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove" on target "CN=Paul
Valencia,OU=Sales,OU=HQ-NYC,OU=Employees,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
```

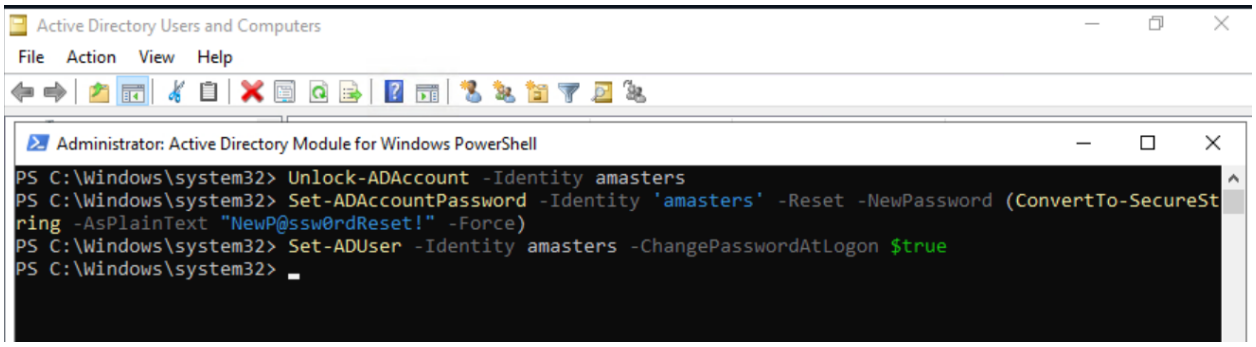
For the second user, I will remove them through ADUC. From the Employees folder, I right-clicked it, hit the Find option, and typed the user's name. As seen in the image below, the user was found at the bottom of the list. To remove the user, I right-clicked their name, and hit Delete.



Lastly, Adam Masters has submitted a trouble ticket over the phone saying his account is locked because he typed his password wrong too many times. The helpdesk has verified his identity and that his Cyber awareness training is up to date. The ticket requests that I unlock his user account and force him to change his password at the next login.

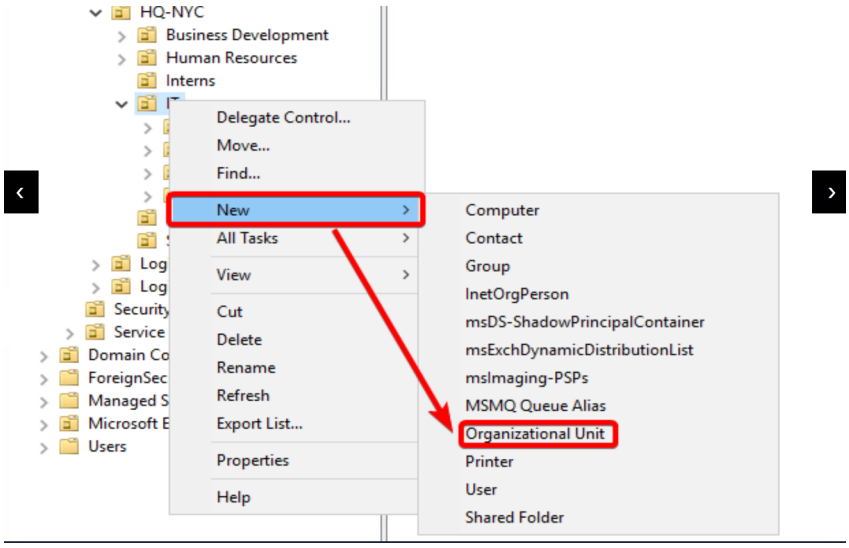


I used PowerShell to unlock the user by using the following command: PS C:\htb> Unlock-ADAccount -Identity amasters. We also need to set a new password for the user and force them to change the password at the next logon. We will do this with the SetADAccountPassword and Set-ADUser cmdlets.

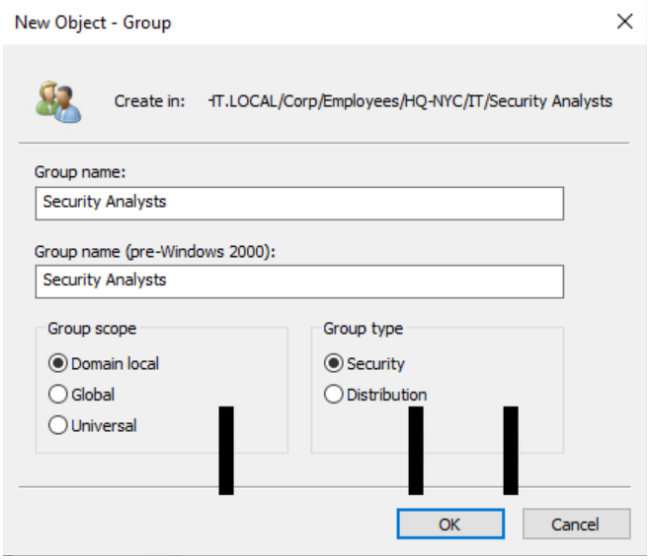


Task 2: Manage Groups and Other Organizational Units

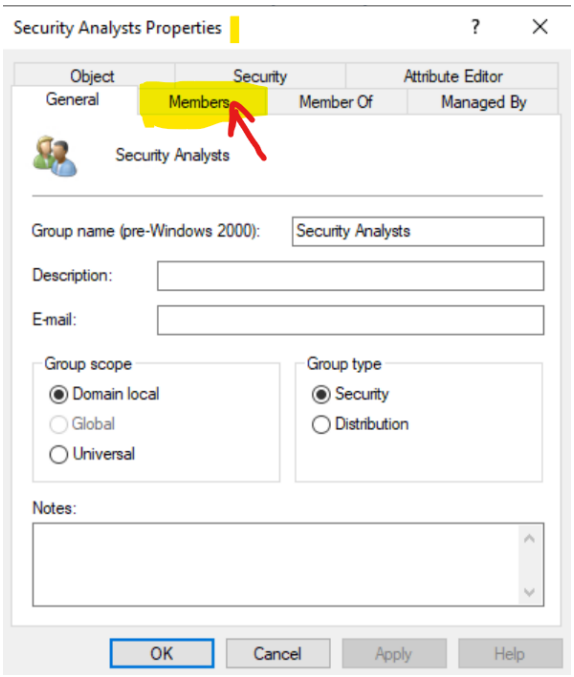
Next up is to create a new Security Group called Analysts and then add our new hires into the group. This group should also be nested in an Organizational Unit (OU) named the same under the IT hive. From the IT hive, I right-clicked on it, selected New, then Organizational Unit.



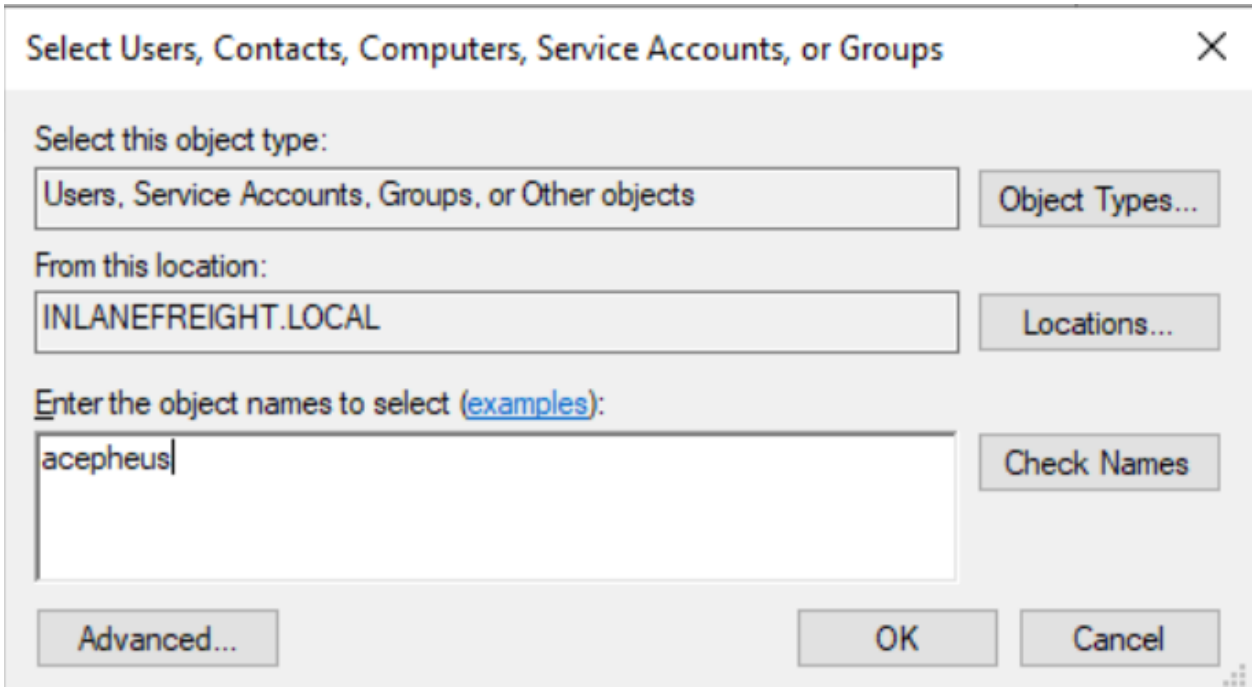
Then, I proceeded to create a group by right-clicking the Security Analysts OU, hit New, and then Group. From there, I named the group Security Analysts, set the group scope to Domain local and the group type to Security, as seen below.



Now I need to add users to this new group. From the Security Analyst group, I right-clicked on it, hit Properties, then went to the Members tab.



From the Members tab, I clicked the Add button, then typed the user's logon name and hit OK. These steps are repeated for the rest of the other users.



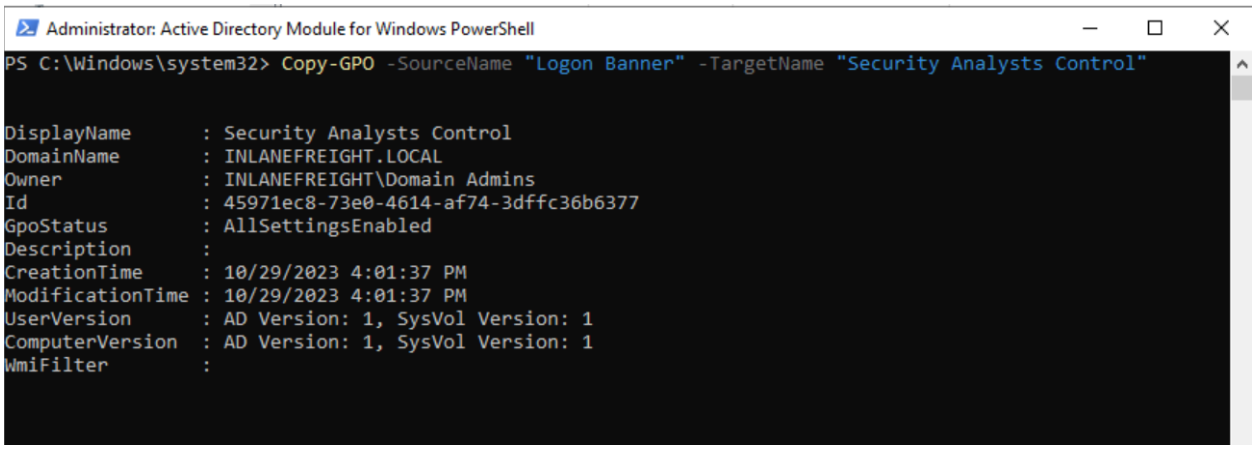
Task 3: Manage Group Policy Objects (GPO)

Next, I have been asked to duplicate the group policy *Logon Banner*, rename it *Security Analysts Control*, and modify it to work for the new Analysts OU. I will need to make the following changes to the Policy Object:

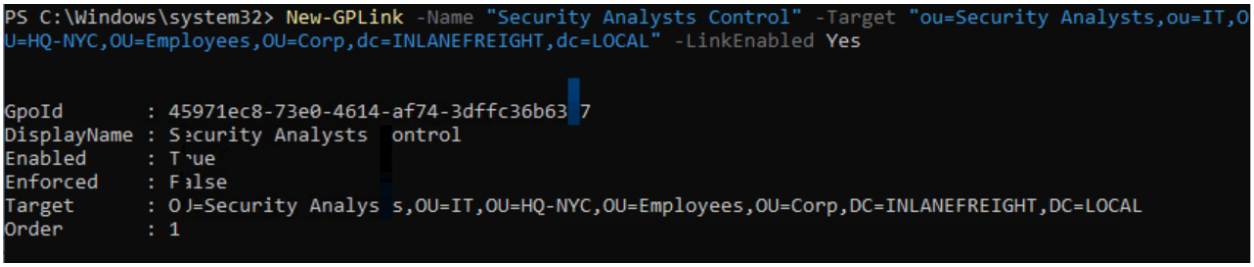
- I will be modifying the Password policy settings for users in this group and expressly allowing users to access PowerShell and CMD since their daily duties require it.
- For computer settings, we need to ensure the Logon Banner is applied and that removable media is blocked from access.

Once done, I'll make sure the Group Policy is applied to the Security Analysts OU.

To duplicate a Group Policy Object I can use the 'Copy-GPO' cmdlet:



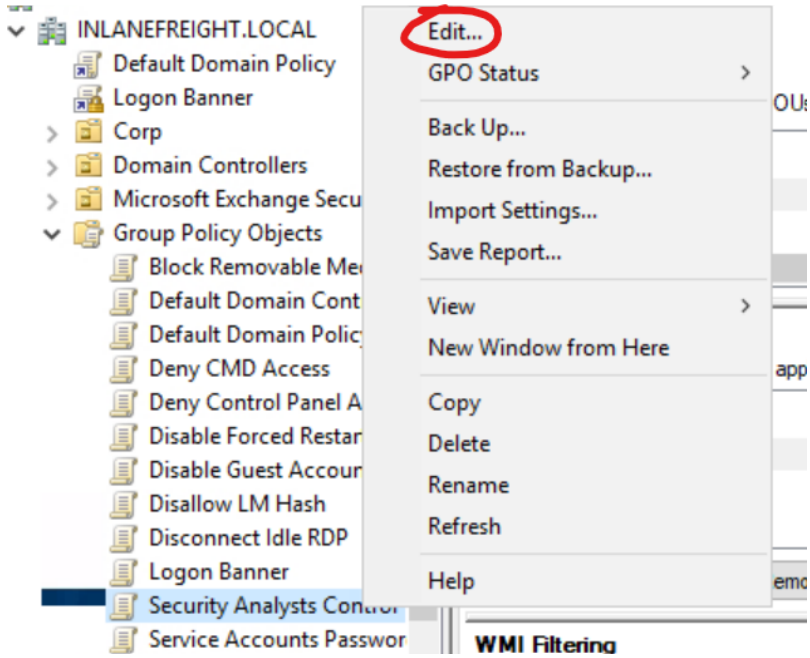
The command above will take Logon Banner GPO and copy it to a new object named Security Analyst Control. This object will have all the old attributes of the Logon Banner GPO, but it will not be applied to anything until we link it. The command below will take the new GPO we created, link it to the OU Security Analysts, and enable it.



Modify a GPO via Group Policy Management Console

User Configuration Group Policies

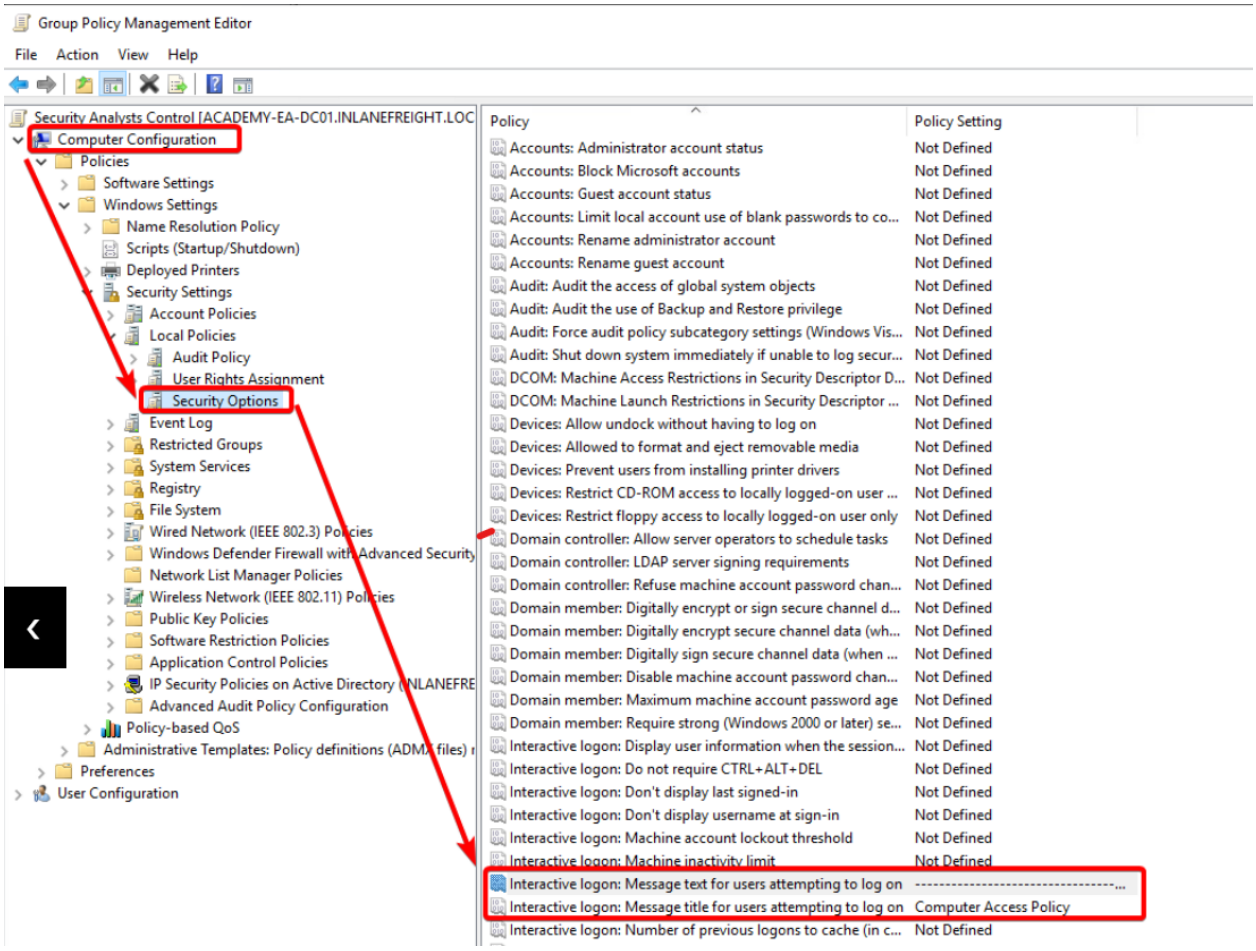
The following image will guide us through modifying group policies that affect Users directly. I will be modifying the policies affecting users' access to the command prompt as well as their ability to use removable media.



As seen above, I right-clicked the Security Analyst Control GPO and selected Edit. This will bring up the Group Policy Configuration Editor Window.

User Configuration Group Policies

The following image will walk us through modifying group policies that affect computers in the group. I will be modifying the policies affecting the Logon Banner for the host, and setting a more restrictive password policy.



Summary

In this project, I covered how to manage users by adding/removing them. I managed to unlock a user's account that has been locked. I also covered how to create a group and how to add members to that group. Lastly, I covered how to manage group policies.