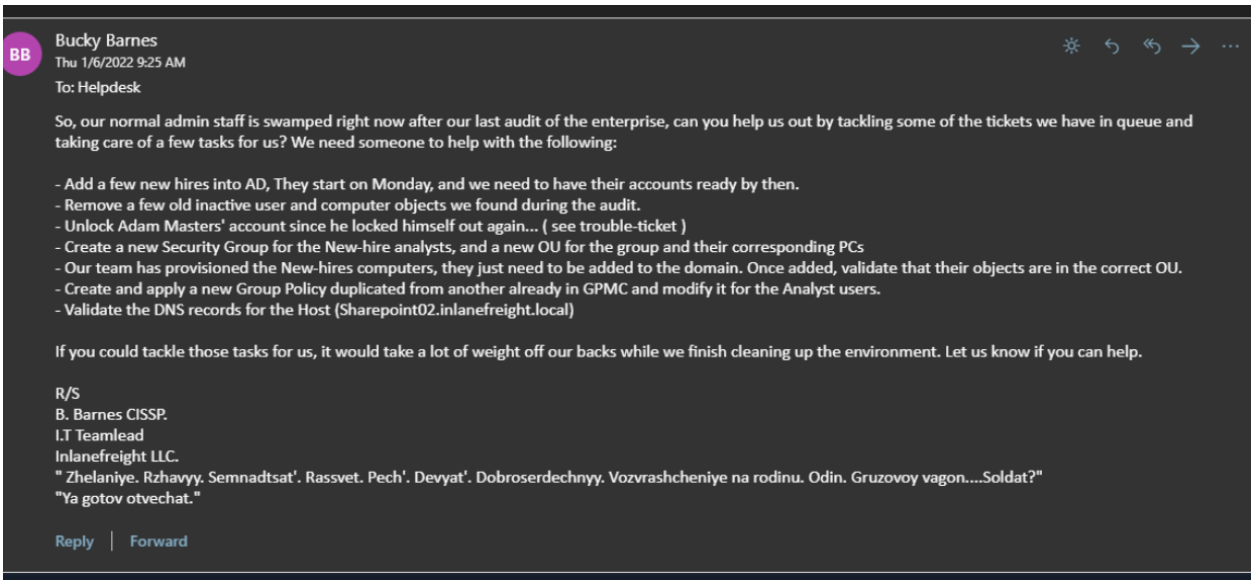
AD Administration:



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

Task 1: Manage Users

Our first task of the day includes adding a few new-hire users into AD. We are just going to create them under the "inlanefreight.local" scope, drilling down into the "Corp > Employees > HQ-NYC > IT " folder structure for now. Once we create our other groups, we will move them into the new folders. You can utilize the Active Directory PowerShell module (New-ADUser), the Active Directory Users and Computers snap-in, or MMC to perform these actions.

Users to Add:

User

Andromeda Cepheus

Orion Starchaser

Artemis Callisto

Each user should have the following attributes set, along with their name:

Attribute

full name

email (first-initial.lastname@inlanefreight.local) ( ex. j.smith@inlanefreight.local )

display name

User must change password at next logon

Users to Remove

User

Mike O'Hare

Paul Valencia

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 you unlock his user account and force him to change his password at the next login.

Solution:

Via Powershell:

Open Powershell as an Administrator:

Import-Module -Name ActiveDirectory

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"}

Add A User(Via GUI)

We will add the new user Andromeda Cepheus to our domain. We can do so by:

Right-click on "IT" > Select "New" > "User". A popup window will appear with a field for you to fill in.

Add the user's First and Last name Andromeda Cepheus, set the "User Logon Name:" as acepheus, and then hit Next.

Now supply the new user with a password of NewP@ssw0rd123!, confirm the password again, and check the box for " User must change password at next login", then hit next. Select "Finish" in the last window if all attributes look correct.

Right-click on "IT" > Select "New" > "User". A popup window will appear with a field for you to fill in.

Add the user's First and Last name Artemis Callisto, set the "User Logon Name:" as ACallisto, and then hit Next.

Now supply the new user with a password of NewP@ssw0rd123!, confirm the password again, and check the box for " User must change password at next login", then hit next. Select "Finish" in the last window if all attributes look correct.

Users to Remove

PowerShell to Remove a User

Remove-ADUser -Identity pvalencia

Remove via ADUC MMC

The most straightforward method from the ADUC snap-in will be to use the find functionality. Inlanefreight has many users across several OU's. To use find:

Right-click on Employees and select "find".

Type in the username you wish to search for, in this case, "Mike O'Hare" and hit "Find Now." If a user has that name, the search results will appear lower in the find window.

Now, right-click on the user and select delete. A popup window will appear to confirm the deletion of the user. Hit yes.

To validate the user is deleted, you can use the Find feature again to search for the user

Now we need to help Adam Masters out and unlock his account again.

To UNLOCK a user account we can:

PowerShell To Unlock a User

```
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.

Reset User Password (Set-ADAccountPassword)

```
PS C:\htb> Set-ADAccountPassword -Identity 'amasters' -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "NewP@ssw0rdReset!" -Force)
```

Force Password Change (Set-ADUser)

```
PS C:\htb> Set-ADUser -Identity amasters -ChangePasswordAtLogon $true
```

Unlock from Snap-in

Unlocking this user account will take several steps. The first is to unlock the account, then we set it so that the user must change his password at the next login, and then we reset his password to a temporary one so that he can log in and reset it himself. We can do so by:

right-click on the user and select Reset Password.

In the next window, type in the temporary password, confirm it, and check the boxes for "User must change password at next logon" and "Unlock the user's account."

Once done, hit OK to apply changes. If no error occurs, you will get a prompt informing you that the user's password was changed.

TASK 2: Task 2: Manage Groups and Other Organizational Units

Next up for us 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 OU named the same under the IT hive. The New-ADOrganizationalUnit PowerShell command should enable you to quickly add a new security group. We can also utilize the AD Users and Computers snap-in like in Task-1 to complete this task.

Next up for us 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 OU named the same under the IT hive. The New-ADOrganizationalUnit PowerShell command should enable you to quickly add a new security group. We can also utilize the AD Users and Computers snap-in like in Task-1 to complete this task.

Create a New AD OU and Security Group from PowerShell

To create a new OU and Group, we can perform the following actions:

```
PS C:\htb> New-ADOrganizationalUnit -Name "Security Analysts" -Path "OU=IT,OU=HQ-NYC,OU=Employees,OU=CORP,DC=INLANEFREIGHT,DC=LOCAL"
```

First, we created the new OU to hold our Analysts and their resources. Next, we need to create a security group for these users.

PS C:\htb> New-ADGroup -Name "Security Analysts" -SamAccountName analysts -GroupCategory Security -GroupScope Global -DisplayName "Security Analysts" -Path "OU=Security Analysts,OU=IT,OU=HQ-NYC,OU=Employees,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL" -Description "Members of this group are Security Analysts under the IT OU"

From MMC Snap-in

This will be a quick two-step process for us. We first need to create a new OU to host our Security Analysts. To do so, we will :

navigate to the "Corp > Employees > HQ-NYC > IT "OU. We are going to build out a new container within IT.

Right-click on IT and select "New > Organizational Unit". A new window should appear.

input the name Security Analysts into the Name field and leave the default option set for the Protect checkbox. Hit OK, and the OU should be created.

Now that we have our OU, let's create the Security Group for our Analysts.

Right-click on our new OU Security Analysts and select "New > Group" and a popup window should appear.

Input the name of the group Security Analysts

Select the Group scope Domain local

ensure group type says Security not "Distribution".

Once you check the options, hit OK.

Add User to Group via PowerShell

PS C:\htb> Add-ADGroupMember -Identity analysts -Members ACepheus,OStarchaser,ACallisto

From MMC Snap-in

To add the users to the security group, we can:

Find the user you wish to add

Right-click on the user and select "Add to a group". A new window will appear for you to specify the group name.

type in part or all of the group you wish to add the user to. In this case, we are adding Andromeda to the Security Analysts group. If our query matches one or more groups, another dialog box will appear, providing us with a list of groups to choose from. Pick the group you need and hit "OK".

The choice you selected will now be highlighted in the previous window. More than one group can be selected at a time if necessary. Once done, hit "OK."

If no issues arise, you will get a new popup informing you that the operation is completed. To validate, we can view the group or user properties.

TASK 3

Next, we 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. We will need to make the following changes to the Policy Object:

we 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, make sure the Group Policy is applied to the Security Analysts OU. This will require the use of the Group Policy Management snap-in found under Tools in the Server Manager window. For more of a challenge, the Copy-GPO cmdlet in PowerShell can also be utilized.

To Duplicate a Group Policy Object we can use the `Copy-GPO` cmdlet or do it from the Group Policy Management Console.

Duplicate the Object via PowerShell

```
PS C:\htb> Copy-GPO -SourceName "Logon Banner" -TargetName "Security Analysts Control"
```

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.

Link the New GPO to an OU

```
PS C:\htb> New-GPLink -Name "Security Analysts Control" -Target "ou=Security Analysts,ou=IT,OU=HQ-NYC,OU=Employees,OU=Corp,dc=INLANEFREIGHT,dc=LOCAL" -LinkEnabled Yes
```

The command above will take the new GPO we created, link it to the OU Security Analysts, and enable it. For now, that's all we are going to do from PowerShell. We still need to make a few modifications to the policy, but we will perform these actions from Group Policy Management Console. Editing GPO preferences from PowerShell can be a bit daunting and way beyond the scope of this module.

Modify a GPO via GPMC

To modify our new policy object:

We need to open GPMC and expand the Group Policy Objects hive so we can see what GPOs exist.

Right-click on the policy object we wish to modify and select "Edit. The Group Policy Management Editor should pop up in a new window.

From here, we have several options to enable or disable.

We need to modify the removable media settings and ensure they are set to block any removable media from access. We will expressly allow security analysts to access PowerShell and CMD since their daily duties require it.

location of removable media policy settings = User Configuration > Policies > Administrative Templates > System > Removable Storage Access.

Location of Command Prompt settings = User Configuration > Policies > Administrative Templates > System.

For Computer settings, we need to ensure the Logon Banner is applied and that the password policy settings for this group are strengthened.

Location of Logon Banner settings = Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.

For reference, this setting should already be enabled since the GPO we copied was for a Logon Banner. We are validating the settings and ensuring it is enabled and applied.

Location of Password Policy settings = Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.

TASK 4:

Task 4 Add and Remove Computers To The Domain

Our new users will need computers to perform their daily duties. The helpdesk has just finished provisioning them and requires us to add them to the INLANEFREIGHT domain. Since these analyst positions are new, we will need to ensure that the hosts end up in the correct OU once they join the domain so that group policy can take effect properly.

The host we need to join to the INLANEFREIGHT domain is named: ACADEMY-IAD-W10 and has the following credentials for use to login and finish the provisioning process:

User == image

Password == Academy_student_AD!

Once you have access to the host, utilize your htb-student_adm: Academy_student_DA! account to join the host to the domain.

Solution: Task 4

To add the localhost to a domain via PowerShell, Open a PowerShell session as administrator, and then we can use the following command:

PowerShell Join a Domain

```
PS C:\htb> Add-Computer -DomainName INLANEFREIGHT.LOCAL -Credential INLANEFREIGHT\HTB-student_adm -Restart
```

This string utilizes the domain (INLANEFREIGHT.LOCAL) we wish to join the host to, and we must specify the user whose credentials we will use to authorize the join. (HTB-student_ADM). Specifying the restart at the string is necessary because the join will not occur until the host restarts again, allowing it to acquire settings and policies from the domain.

Add via the GUI

To add the computer to the domain from the localhost GUI is a bit different. Follow these steps to join it to the domain:

From the computer you wish to join the domain, open the Control Panel and navigate to "System and Security > System."

Now select the "Change Settings" icon in the Computer name section. Another dialog box will pop up asking you for administrator credentials. In the next window, we need to select the change icon next to the portion that says, "To rename this computer or change its domain or workgroup, click change" This will open yet another window for you to modify the computer's name, domain, and workgroup. Check that the computer's name matches the naming standard you wish to use for the domain before joining. Doing so will ease the administrative burden of renaming a domain-joined host later.

next, we need to enter the name of the domain we wish to join the computer to (INLANEFREIGHT.LOCAL) and click OK. You may receive a warning about NetBIOS name resolution. That is an issue outside the scope of this lab. For now, move forward.

You will be prompted for domain credentials to complete this action. Utilize the domain administrator account you have been given at the beginning of this lab. (htb-student_adm).

If all goes well, you will be presented with a prompt welcoming you to the domain. The computer needs to restart to apply changes and new group policy settings it will receive from the domain.

Add to a New OU

Move A Computer Object To A New OU

1. Looking in the Computers OU, select our newly joined host and right click it. Select the option to "Move"

2.In the popup, drill down to the Security Analysts OU.

3.Select the Security Analysts OU and hit OK.

4.If we look in that OU we will now see a new Computer object within.