Introduction to Active Directory:

Link to challenge:

https://academy.hackthebox.com/module/74

(log in required)

Class: Tier 0 | Fundamental | General

Active Directory Fundamentals:

Active Directory Structure:

Question: What Active Directory structure can contain one or more domains?

Answer: forest

Method: "Active Directory is arranged in a hierarchical tree structure, with a forest at the top containing one or more domains, which can themselves have nested subdomains."

Question: True or False; It can be common to see multiple domains linked together by trust relationships?

Answer: True

Method: "It is common to see multiple domains (or forests) linked together via trust relationships in organizations that perform a lot of acquisitions."

Question: Active Directory provides authentication and <____> within a Windows domain environment.

Answer: authorization

Method: "AD provides authentication and authorization functions within a Windows domain environment."

Active Directory Terminology:

Question: What is known as the "Blueprint" of an Active Directory environment?

Answer: Schema

Method: "The Active Directory schema is essentially the blueprint of any enterprise environment."

Question: What uniquely identifies a Service instance? (full name, space-separated, not abbreviated)

Answer: Service Principal Name

Method: "A Service Principal Name (SPN) uniquely identifies a service instance."

Question: True or False; Group Policy objects can be applied to user and computer objects.

Answer: True

Method: "GPO settings can be applied to both user and computer objects."

Question: What container in AD holds deleted objects?

Answer: Tombstone

Method: "A tombstone is a container object in AD that holds deleted AD objects."

Question: What file contains the hashes of passwords for all users in a domain?

Answer: NTDS.DIT

Method: "The NTDS.DIT file can be considered the heart of Active Directory. It is stored on a Domain Controller at C:\Windows\NTDS\ and is a database that stores AD data such as information about user and group objects, group membership, and, most important to attackers and penetration testers, the password hashes for all users in the domain."

Active Directory Objects:

Question: True or False; Computers are considered leaf objects.

Answer: True

Method: "Computers are leaf objects because they do not contain other objects."

* Leaf object – an object that does not contains another object in it.

Question: <___> are objects that are used to store similar objects for ease of administration. (Fill in the blank)

Answer: Organizational Units

Method: "An organizational unit, or OU from here on out, is a container that systems administrators can use to store similar objects for ease of administration."

Question: What AD object handles all authentication requests for a domain?

Answer: Domain Controller

Method: "Domain Controllers are essentially the brains of an AD network. They handle authentication requests, verify users on the network, and control who can access the various resources in the domain"

Active Directory Functionality:

Question: What role maintains time for a domain?

Answer: PDC Emulator

Method: "The PDC Emulator also maintains time within the domain."

Question: What domain functional level introduced Managed Service Accounts?

Answer: Windows Server 2008 R2

Method: "Authentication mechanism assurance, Managed Service Accounts"

Question: What type of trust is a link between two child domains in a forest?

Answer: Cross-link

Method: Cross link: "a trust between child domains to speed up authentication."

Question: What role ensures that objects in a domain are not assigned the same SID? (full name)

Answer: Relative ID Master

Method: "The RID Master assigns blocks of RIDs to other DCs within the domain that can be used for new objects. The RID Master helps ensure that multiple objects are not assigned the same SID. Domain object SIDs are the domain SID combined with the RID number assigned to the object to make the unique SID."

Active Directory Protocols:

Kerberos, DNS, LDAP, MSRPC:

Question: What networking port does Kerberos use?

Answer: 88

Method: "we can often locate Domain Controllers by performing port scans looking for open port 88 using a tool such as Nmap."

Question: What protocol is utilized to translate names into IP addresses? (acronym)

Answer: DNS

Method: "DNS is used to resolve hostnames to IP addresses and is broadly used across internal networks and the internet."

Question: What protocol does RFC 4511 specify? (acronym)

Answer: LDAP

Method: "The latest LDAP specification is Version 3, published as RFC 4511."

NTLM Authentication:

Question: What Hashing protocol is capable of symmetric and asymmetric cryptography?

Answer: Kerberos

Method: Kerberos cryptographic technique: "Symmetric key cryptography & asymmetric cryptography"

Question: NTLM uses three messages to authenticate; Negotiate, Challenge, and <__>. What is the missing message? (fill in the blank)

Answer: AUTHENTICATE

Method: "NT LAN Manager (NTLM) hashes are used on modern Windows systems. It is a challenge-response authentication protocol and uses three messages to authenticate: a client first sends a NEGOTIATE_MESSAGE to the server, whose response is a CHALLENGE_MESSAGE to verify the client's identity. Lastly, the client responds with an AUTHENTICATE_MESSAGE."

Question: How many hashes does the Domain Cached Credentials mechanism save to a host by default?

Answer: 10

Method: "Hosts save the last ten hashes for any domain users that successfully log into the machine in the HKEY_LOCAL_MACHINE\SECURITY\Cache registry key."

All About Users:

User and Machine Accounts:

Question: True or False; A local user account can be used to login to any domain connected host.

Answer: False

Method: "Local accounts are stored locally on a particular server or workstation. These accounts can be assigned rights on that host either individually or via group membership. Any rights assigned can only be granted to that specific host and will **not** work across the domain."

Question: What default user account has the SID "S-1-5-domain-500" ?

Answer: Administrator

Method: "Administrator: this account has the SID S-1-5-domain-500 and is the first account created with a new Windows installation."

Question: What account has the highest permission level possible on a Windows host

Answer: SYSTEM

Method: " A SYSTEM account is the highest permission level one can achieve on a Windows host and, by default, is granted Full Control permissions to all files on a Windows system."

Question: What user naming attribute is unique to the user and will remain so even if the account is deleted?

Answer: ObjectGUID

Method: ObjectGUID: "This is a unique identifier of the user. In AD, the ObjectGUID attribute name never changes and remains unique even if the user is removed."

Active Directory Groups:

Question: What group type is best utilized for assigning permissions and right to users?

Answer: Security

Method: "The Security groups type is primarily for ease of assigning permissions and rights to a collection of users instead of one at a time."

Question: True or False; A "Global Group" can only contain accounts from the domain where it was created.

Answer: True

Method: "A global group can only contain accounts from the domain where it was created."

Question: Can a Universal group be converted to a Domain Local group? (yes or no)

Answer: yes

Method: "A Universal Group can be converted to a Domain Local Group without any restrictions."

Active Directory Rights and Privileges:

Question: What built-in group will grant a user full and unrestricted access to a computer?

Answer: Administrators

Method: Administrators: "Members have full and unrestricted access to a computer or an entire domain if they are in this group on a Domain Controller."

Question: What user right grants a user the ability to make backups of a system?

Answer: SeBackupPrivilege

Method: SeBackupPrivilege: "This grants a user the ability to create system backups and could be used to obtain copies of sensitive system files that can be used to retrieve passwords such as the SAM and SYSTEM Registry hives and the NTDS.dit Active Directory database file."

Question: What Windows command can show us all user rights assigned to the current user?

Answer: whoami /priv

Method: "After logging into a host, typing the command whoami /priv will give us a listing of all user rights assigned to the current user."

Digging in Deeper:

Security in Active Directory:

Question: Confidentiality, <___>, and Availability are the pillars of the CIA Triad. What term is missing? (fill in the blank)

Answer: Integrity

Method: "When we think about cybersecurity, one of the first things that come up is the balance between Confidentiality, Integrity, and Availability, also known as the CIA Triad."

Question: What security policies can block certain users from running all executables?

Answer: Application Control Policies

Method: Application Control Policies : "This may include blocking certain users from running all executables, Windows Installer files, scripts, etc."

Examining Group Policy:

Question: Computer settings for Group Policies are gathered and applied at a <___> minute interval? (answer is a number, fill in the blank)

Answer: 90

Method: "Windows performs periodic Group Policy updates, which by default is done every 90 minutes with a randomized offset of +/- 30 minutes for users and computers."

Question: True or False: A policy applied to a user at the domain level would be overwritten by a policy at the site level.

Answer: False

Method: Site Policy: " You could specify those settings at the site level and ensure they are linked so as not to be overwritten by domain policy." – the default overwriting is in the opposite direction (site level policy is overwritten by domain level policy)

Question: What Group Policy Object is created when the domain is created?

Answer: Default Domain Policy

Method: "The Default Domain Policy is the default GPO that is automatically created and linked to the domain."

Getting Our Hands Dirty:

AD Administration: Guided Lab Part I:

Question: Once you have finished the tasks, type "COMPLETE" to move on.

Answer: COMPLETE

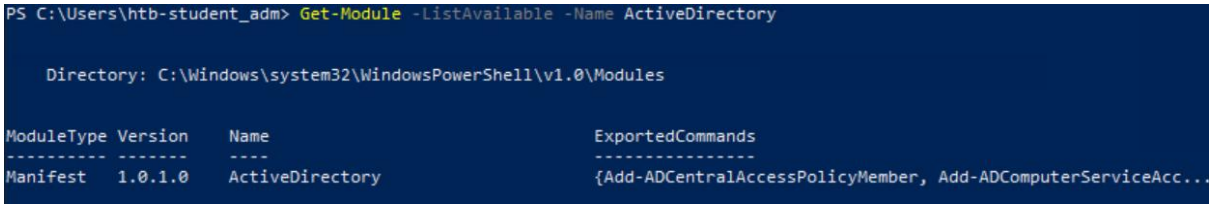
Method: first, we connect to the windows machine with the command:

```
xfreerdp /v:<Target IP> /u:htb-student_adm
/p:Academy_student_DA! /dynamic-resolution
```

when logged in, before we even start with executing the tasks required – lets confirm active directory is installed on the machine.

We will use the PowerShell command:

```
Get-Module -ListAvailable -Name ActiveDirectory
```

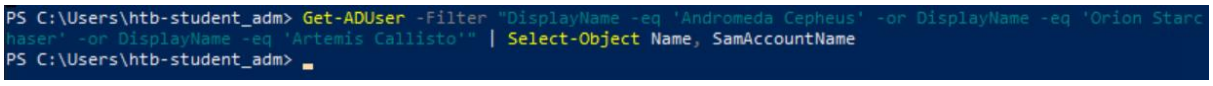


The instance above confirms active directory existence on target's machine.

Task 1:

Now lets add new users, before we do that, lets confirm they are not already exist using the command:

```
Get-ADUser -Filter "DisplayName -eq 'Andromeda Cepheus' -or
DisplayName -eq 'Orion Starchaser' -or DisplayName -eq
'Artemis Callisto'" | Select-Object Name, SamAccountName
```



No results.

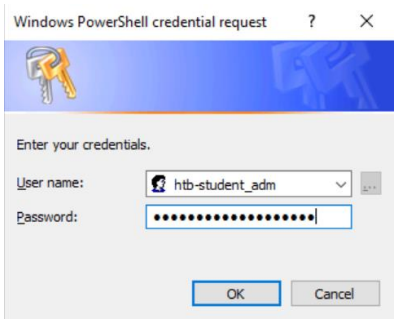
Now we are free to add them, open PowerShell on ADMINISTRATOR privileges.

Then, we will use the command:

```
$credential = Get-Credential
$users = @(
    @{
        Name="Andromeda Cepheus"
        GivenName="Andromeda"
        Surname="Cepheus"
        SamAccountName="acepheus"
        UserPrincipalName="a-cepheus@inlanefreight.local"
        EmailAddress="a-cepheus@inlanefreight.local"
        DisplayName="Andromeda Cepheus"
    },
    @{
        Name="Orion Starchaser"
        GivenName="Orion"
        Surname="Starchaser"
        SamAccountName="ostarchaser"
        UserPrincipalName="o-starchaser@inlanefreight.local"
        EmailAddress="o-starchaser@inlanefreight.local"
        DisplayName="Orion Starchaser"
    },
    @{
        Name="Artemis Callisto"
        GivenName="Artemis"
        Surname="Callisto"
        SamAccountName="acallisto"
        UserPrincipalName="a-callisto@inlanefreight.local"
        EmailAddress="a-callisto@inlanefreight.local"
        DisplayName="Artemis Callisto"
    }
)
$users | ForEach-Object {
    New-ADUser -Name $_.Name `
               -GivenName $_.GivenName `
               -Surname $_.Surname `
               -SamAccountName $_.SamAccountName `
               -UserPrincipalName $_.UserPrincipalName `
               -EmailAddress $_.EmailAddress `
               -DisplayName $_.DisplayName `
               -AccountPassword (ConvertTo-SecureString
"P@ssw0rd" -AsPlainText -Force) `
               -PasswordNeverExpires $false `
               -ChangePasswordAtLogon $true `
               -Enabled $true
}
```

The ‘$credential = Get-Credential’ line will request credentials from us

We will enter the same credentials we used to login to the windows machine, provided for us by the module: ‘htb-student_adm:Academy_student_DA!’



When done, we need to verify users addition. We will use the same command from before:

```
Get-ADUser -Filter "DisplayName -eq 'Andromeda Cepheus' -or
DisplayName -eq 'Orion Starchaser' -or DisplayName -eq
'Artemis Callisto'" | Select-Object Name, SamAccountName
```

```
PS C:\Windows\system32> Get-ADUser -Filter "DisplayName -eq 'Andromeda Cepheus' -or DisplayName -eq 'Orion Starchaser' -
or DisplayName -eq 'Artemis Callisto'" | Select-Object Name, SamAccountName

Name              SamAccountName
----              --------------
Artemis Callisto  acallisto
Orion Starchaser  ostarchaser
Andromeda Cepheus acepheus
```

Users added!

Now, Before we remove Mike O'Hare and Paul Valencia, lets first confirm their existence – we will use the command:

```
Get-ADUser -Filter "DisplayName -eq 'Paul Valencia' -or
DisplayName -eq 'Mike O''Hare'" | Select-Object Name,
SamAccountName
```

To get them both by the property ‘DisplayName’:

```
PS C:\Users\htb-student_adm> Get-ADUser -Filter "DisplayName -eq 'Paul Valencia' -or DisplayName -eq 'Mike O''Hare'"
| Select-Object Name, SamAccountName

Name          SamAccountName
----          --------------
Mike O'Hare   mohare
Paul Valencia pvalencia
```

the command will use filter based on 'DisplayName' to get them both and filter out everyone else.

In addition, and command will display their 'SamAccountName' – their logon name which can be used for

```
Get-ADUser -Identity <SamAccountName>
```

Here is an example on 'mohare' – Mike Ohare's SamAccountName:

```
PS C:\Users\htb-student_adm> Get-ADUser -Identity mohare


DistinguishedName : CN=Mike O'Hare,OU=Audit,OU=Financial-LON,OU=Employees,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL
GivenName         : Mike
Name              : Mike O'Hare
ObjectClass       : user
ObjectGUID        : ee09d68e-2058-4438-ba9a-07227cd770c1
SamAccountName    : mohare
SID               : S-1-5-21-3842939050-3880317879-2865463114-6103
Surname           : O'Hare
UserPrincipalName : mohare@INLANEFREIGHT.LOCAL
```

Now that their existence is confirm, time to remove them, we will use the command:

```
Get-ADUser -Filter {SamAccountName -eq "mohare"} | Remove-
ADUser

Get-ADUser -Filter {SamAccountName -eq "pvalencia"} |
Remove-ADUser
```

Where their SamAccountName is obtained via the filter command:

```
PS C:\Windows\system32> Get-ADUser -Filter {SamAccountName -eq "mohare"} | Remove-ADUser

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove" on target "CN=Mike
O'Hare,OU=Audit,OU=Financial-LON,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"): A
PS C:\Windows\system32>
PS C:\Windows\system32> Get-ADUser -Filter {SamAccountName -eq "pvalencia"} | Remove-ADUser

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"): A
PS C:\Windows\system32>
```

We are first asked to confirm deletion.

When done, we confirm deletion by searching their names again:

```
PS C:\Windows\system32> Get-ADUser -Filter "DisplayName -eq 'Paul Valencia' -or DisplayName -eq 'Mike O''Hare'" | Select
-Object Name, SamAccountName
PS C:\Windows\system32>
```

No results were found, deletion confirmed.

Now, for helping Adam, first lets discover his SamAccountName:

```
Get-ADUser -Filter "DisplayName -eq 'Adam Masters'" |
Select-Object Name, SamAccountName
```

```
PS C:\Windows\system32> Get-ADUser -Filter "DisplayName -eq 'Adam Masters'"| Select-Object Name, SamAccountName

Name         SamAccountName
----         --------------
Adam Masters amasters
```

His SamAccountName is ‘amasters’.

One that we have that we can reset his password with the following command:

```
Unlock-ADAccount -Identity "amasters"

Set-ADUser -Identity "amasters" -ChangePasswordAtLogon:$true
```

Task 2: we will use the following commands with ADMINISTRATOR PowerShell:

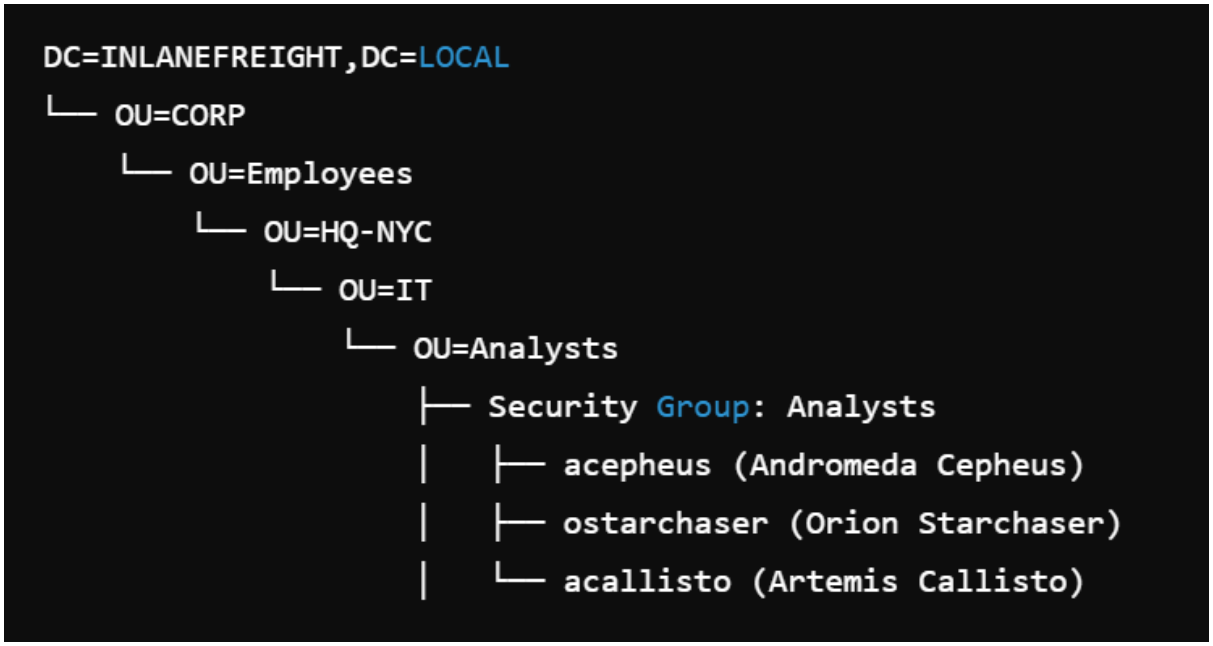
```
New-ADOrganizationalUnit -Name "Analysts" -Path
"OU=IT,OU=HQ-
NYC,OU=Employees,OU=CORP,DC=INLANEFREIGHT,DC=LOCAL"

New-ADGroup -Name "Analysts" -GroupScope Global -GroupCategory Security
-Path "OU=Analysts,OU=IT,OU=HQ-
NYC,OU=Employees,OU=CORP,DC=INLANEFREIGHT,DC=LOCAL"

Add-ADGroupMember -Identity "Analysts" -Members "acepheus",
"ostarchaser", "acallisto"
```

The first command creates the Active directory's OU (organizational Unit) called 'Analysts', and it will be nested under OU 'IT', 'HQ-NYC', ;Employees' and DC (Domain Component) 'INLANEFREIGHT', 'LOCAL;

The second command creates new group called 'Analysts', placed under the OU called 'Analysts' and the other OU and DC.

The third command adds the created users from Task 1 to the new 'Analysts' group.

Here is an hierarchy chart of the active directory after our new addition:



Task 3: we will run the commands:

```
# Define variables
$sourceGpoName = "Logon Banner"
$newGpoName = "Security Analysts Control"
$gpoName = "Security Analysts Control"

# Step 1: Copy the GPO
Copy-GPO -SourceName $sourceGpoName -TargetName $newGpoName

# Step 2: Set password policy settings
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System"
-ValueName "MaximumPasswordAge" -Type DWord -Value 30
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System"
-ValueName "MinimumPasswordLength" -Type DWord -Value 8
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System"
-ValueName "PasswordComplexity" -Type DWord -Value 1

# Step 3: Allow PowerShell and CMD access
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Policies\Microsoft\Windows\System" -ValueName
"EnableLUA" -Type DWord -Value 0
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell" -ValueName
"ExecutionPolicy" -Type String -Value "RemoteSigned"

# Step 4: Set logon banner text
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System"
-ValueName "LegalNoticeText" -Type String -Value "welcome"

Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System"
-ValueName "LegalNoticeCaption" -Type String -Value "Security
Notice"

# Step 5: Block removable media access
Set-GPRegistryValue -Name $gpoName -Key
"HKLM\Software\Policies\Microsoft\Windows\RemovableStorageDevices
" -ValueName "Deny_All" -Type DWord -Value 1

# Step 6: Link GPO to the Analysts OU
New-GPLink -Name $gpoName -Target "OU=Analysts,OU=IT,OU=HQ-
NYC,OU=Employees,OU=CORP,DC=INLANEFREIGHT,DC=LOCAL"
```

Lets analyze:

Step 1: we copy the ‘Logon Banner’ policy to ‘Security Analysts Control’ policy:

```
PS C:\Windows\system32> $sourceGpoName = "Logon Banner"
PS C:\Windows\system32> $newGpoName = "Security Analysts Control"
PS C:\Windows\system32> $gpoName = "Security Analysts Control"
PS C:\Windows\system32> Copy-GPO -SourceName $sourceGpoName -TargetName $newGpoName


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 12:57:54 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

Step 2: we commit the password policy modifications:

```
PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "MaximumPasswordAge" -Type DWord -Value
30


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 12:58:06 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :


PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "MinimumPasswordLength" -Type DWord -Val
ue 8


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 12:58:06 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 3, SysVol Version: 3
WmiFilter        :


PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "PasswordComplexity" -Type DWord -Value
1


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 12:58:08 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 4, SysVol Version: 4
WmiFilter        :
```

Their force the group users to select password at least complexity 1, at least 8 characters long, and to be used for a t least 30 days.

Step 3: enable cmd and powershell:

```
PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Policies\Microsoft\Windows\System" -ValueName "DisableCMD" -Type DWord -Value 0


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 1:00:30 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 6, SysVol Version: 6
WmiFilter        :
```

```
PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell" -ValueName "ExecutionPolicy" -Type String -Value "RemoteSigned
"


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 1:14:56 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 10, SysVol Version: 10
WmiFilter        :
```

Now the group users have cmd and powershell enabled.

Step 4: set logon banner text – what message will be displayed for the group's user in certain situations?

```
PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "LegalNoticeText" -Type String -Value "Y
our Logon Banner Text Here"


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 1:01:06 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 7, SysVol Version: 7
WmiFilter        :


PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "LegalNoticeCaption" -Type String -Value
 "Security Notice"


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 1:01:08 AM
UserVersion      : AD Version: 1, SysVol Version: 1
```

Step 5: block removeable media – block access for removable media storage (like USB and hard-drive):

```
PS C:\Windows\system32> Set-GPRegistryValue -Name $gpoName -Key "HKLM\Software\Policies\Microsoft\Windows\RemovableStorageDevices" -ValueName "Deny_All" -Type DWord -Value 1


DisplayName      : Security Analysts Control
DomainName       : INLANEFREIGHT.LOCAL
Owner            : INLANEFREIGHT\Domain Admins
Id               : 87358140-88c8-4bfd-9395-19a154560121
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/26/2024 12:57:54 AM
ModificationTime : 6/26/2024 1:01:28 AM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 9, SysVol Version: 9
WmiFilter        :
```

Step 6: link and enable the group policy media to the OU, and activate it:

```
PS C:\Windows\system32> New-GPLink -Name $gpoName -Target "OU=Analysts,OU=IT,OU=HQ-NYC,OU=Employees,OU=CORP,DC=INLANEFREIGHT,DC=LOCAL"


GpoId       : 87358140-88c8-4bfd-9395-19a154560121
DisplayName : Security Analysts Control
Enabled     : True
Enforced    : False
Target      : OU=Analysts,OU=IT,OU=HQ-NYC,OU=Employees,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL
Order       : 1
```

AD Administration: Guided Lab Part II:

Question: Once you have finished the tasks, type "COMPLETE" to move on.

Answer: COMPLETE

Method: Task 4:

First, we will connect to the windows machine with the command:

```
xfreerdp /v:<Target IP> /u:image /p:Academy_student_AD! /dynamic-resolution
```

then, on powershell – ADMINISTRATOR

we will run the command:

```
Add-Computer -ComputerName ACADEMY-IAD-W10 -LocalCredential ACADEMY-IAD-W10\image -DomainName INLANEFREIGHT.LOCAL -Credential INLANEFREIGHT\htb-student_adm -Restart
```

we are requested to confirm credentials (that is because the DC – domain controller who does adding the computers to the AC domain:

ACADEMY-IAD-W10\Image:Academy_student_DA!

When the credentials are confirm, the computer will restart.

When the computer is restarted and back online the computer should be registered to the domain, we can confirm it with this command:

```
Get-ADComputer -Identity "ACADEMY-IAD-W10" -Properties * | select CN,CanonicalName,IPv4Address
```

```
PS C:\Users\image> Get-ADComputer -Identity "ACADEMY-IAD-W10" -Properties * -Credential $credential | Select-Object CN,
CanonicalName, IPv4Address

CN             CanonicalName                                 IPv4Address
--             -------------                                 -----------
ACADEMY-IAD-W10 INLANEFREIGHT.LOCAL/Computers/ACADEMY-IAD-W10 172.16.6.135
```

Computer registration confirmed!