

Lab Assignment



Cybersecurity Professional Program

Microsoft Security

PowerShell

MS-07-L2

**PowerShell for
Active Directory**

Lab Objective

Learn how to use PowerShell to manage an Active Directory domain.

Lab Mission

Practice PowerShell Active Directory commands and manage objects using the bulk action method.

Lab Duration

40–50 minutes

Requirements

- Familiarity with Active Directory
- Knowledge of Windows Server 2016 GUI

Resources

Environment and tools:

- VirtualBox:
 - Windows Server 2016 (Server1)
 - Windows 10 Client
- Extra files:
 - ***Create-Users.ps1***
 - ***Userlist.csv***

Lab Task 1: Manage Active Directory by Using PowerShell

On Server1, use PowerShell commands to create and manage users for the domain.

- 1 Create an organizational unit (OU) named *IT* using the ***New-ADOrganizationalUnit IT*** command.

```
PS C:\Users\Administrator> New-ADOrganizationalUnit IT
```

- 2 Create a user account named *Josep* in the IT OU by using the ***New-ADUser -Name "Josep" -SamAccountName "Josep" -path "OU=IT, DC=Cyber, DC=local"*** command.

```
PS C:\Users\Administrator> New-ADUser -Name "Josep" -SamAccountName "Josep" -path "OU=IT, DC=Cyber, DC=local"
```

- 3 Use ***Set-ADAccountPassword Josep*** to set a password for the new user. (Hint: when asked for the current password, leave it empty and press ***Enter***).

```
PS C:\Users\Administrator> SET-ADAccountPassword Josep
Please enter the current password for 'CN=Josep,OU=IT,DC=cyber,DC=local'
Password:
Please enter the desired password for 'CN=Josep,OU=IT,DC=cyber,DC=local'
Password: *****
```

- 4 Enable the Josep account by using ***Enable-ADAccount Josep***

```
PS C:\Users\Administrator> Enable-ADAccount Josep
```

- 5 Create a global security group for users in the IT department. Name it ***IT-GRP***, and make sure you create it in the IT OU. To do so, use the ***New-ADGroup "IT-GRP" -path "ou=IT, dc=Cyber, dc=local" -GroupScope Global -GroupCategory Security*** command.

```
PS C:\Users\Administrator> New-ADGroup "IT-GRP" -path "OU=IT, DC=Cyber, DC=Local" -GroupScope Global -GroupCategory Security
PS C:\Users\Administrator>
```

- 6 Add Josep to the IT group by using ***Add-ADGroupMember "IT-GRP" -Members Josep***

```
PS C:\Users\Administrator> Add-ADGroupMember "IT-GRP" -Members Josep
PS C:\Users\Administrator>
```

- 7 Add a Department IT parameter to the user by running ***Set-ADUser Josep -Department "IT"***

```
PS C:\Users\Administrator> Set-ADUser Josep -Department "IT"
PS C:\Users\Administrator>
```

- 8 Use the following command to see the user properties and verify that all the changes were made: ***Get-ADUser Josep -Properties department***

Note: You can use the ***-Properties*** flag with an asterisk to see all user properties: ***Get-ADUser Josep -Properties ****

```
PS C:\Users\Administrator> Get-ADUser Josep -Properties department

Department           : IT
DistinguishedName     : CN=Josep,OU=IT,DC=cyber,DC=local
Enabled               : True
GivenName             :
Name                  : Josep
ObjectClass            : user
ObjectGUID            : 3d3c485e-d489-4ab4-a3be-2f0092b47368
SamAccountName         : Josep
SID                   : S-1-5-21-3539338704-3261642708-3860110303-1105
Surname               :
UserPrincipalName      :

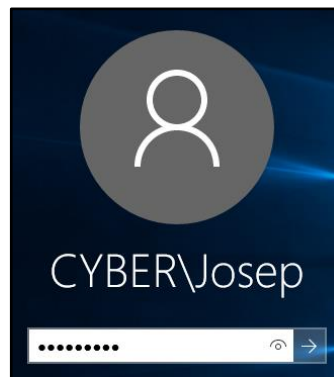
PS C:\Users\Administrator> Get-ADUser Josep -Properties *

AccountExpirationDate : 
accountExpires        : 9223372036854775807
AccountLockoutTime    : 
AccountNotDelegated   : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy  : {}
AuthenticationPolicySilo : {}
BadLogonCount         : 0
badPasswordTime       : 0
badPwdCount            : 0
CannotChangePassword  : False
CanonicalName         : cyber.local/IT/Josep
Certificates          : {}
City                  : 
CN                    : Josep
codePage               : 0
Company               : 
CompoundIdentitySupported : {}
Country               : 
countryCode           : 0
Created               : 1/12/2022 1:58:48 PM
createTimeStamp       : 1/12/2022 1:58:48 PM
Deleted               : 
Department            : IT
Description           : 
DisplayName           : 
DistinguishedName     : CN=Josep,OU=IT,DC=cyber,DC=local
```

- 9** Use the following command to verify group members:
Get-ADGroupMember IT-GRP

```
PS C:\Users\Administrator> Get-ADGroupMember IT-GRP
distinguishedName : CN=Josep,OU=IT,DC=cyber,DC=local
name              : Josep
objectClass       : user
objectGUID        : 3d3c485e-d489-4ab4-a3be-2f0092b47368
SamAccountName    : Josep
SID               : S-1-5-21-3539338704-3261642708-3860110303-1105
```

- 10** Log in to the Josep user account via the Windows 10 client machine.

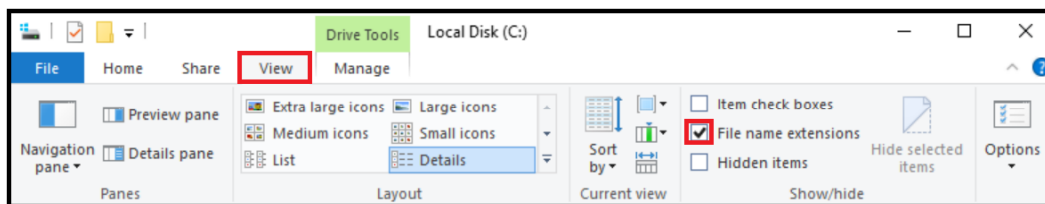


Lab Task 2: Work with PowerShell Scripts

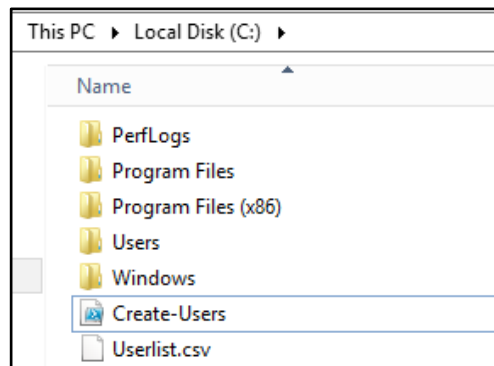
Use a PowerShell script to add domain users via a .csv file:

- **Create-Users.ps1**—a PowerShell script that creates users automatically from a list
- **Userlist.csv**—a list of users and additional information

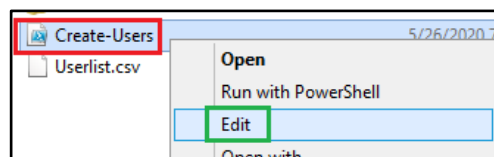
Note: If the file extensions do not appear, select the following option on the **View** tab:



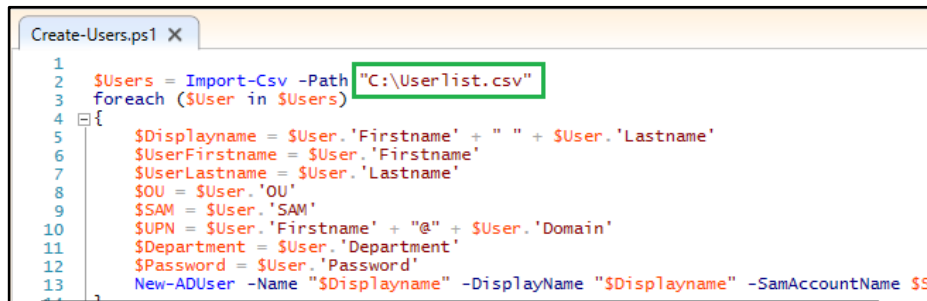
- 1 On Server1, use the **SIP** to install **Guest Additions** to drag and drop the extra files into Server1.
- 2 Move the files to the **C:** drive.



- 3 Edit **Create-Users.ps1** with PowerShell ISE by right-clicking it and choosing **Edit**.



- 4 Make sure the path of **Userlist.csv** is correct (leave it open).

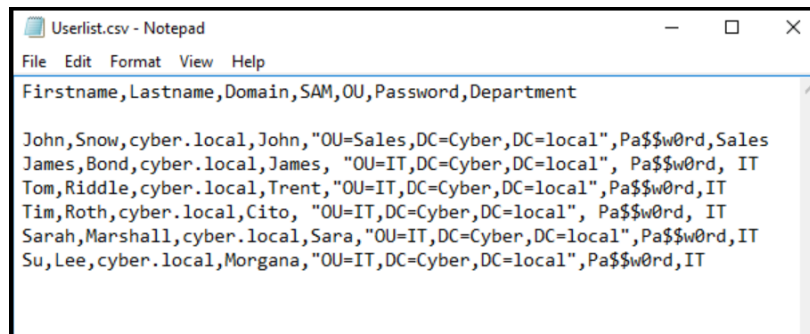


```
1 $Users = Import-Csv -Path "C:\Userlist.csv"
2 foreach ($User in $Users)
3 {
4     $Displayname = $User.'Firstname' + " " + $User.'Lastname'
5     $UserFirstname = $User.'Firstname'
6     $UserLastname = $User.'Lastname'
7     $OU = $User.'OU'
8     $SAM = $User.'SAM'
9     $UPN = $User.'Firstname' + "@" + $User.'Domain'
10    $Department = $User.'Department'
11    $Password = $User.'Password'
12    New-ADUser -Name "$Displayname" -DisplayName "$Displayname" -SamAccountName $S
```

- 5 Edit the CSV file with Excel or Notepad and add five users of your choice to the IT department. Then save the changes.

Note: Avoid creating users with the same first names or SamAccountName, as it may cause errors. You can use, for example:

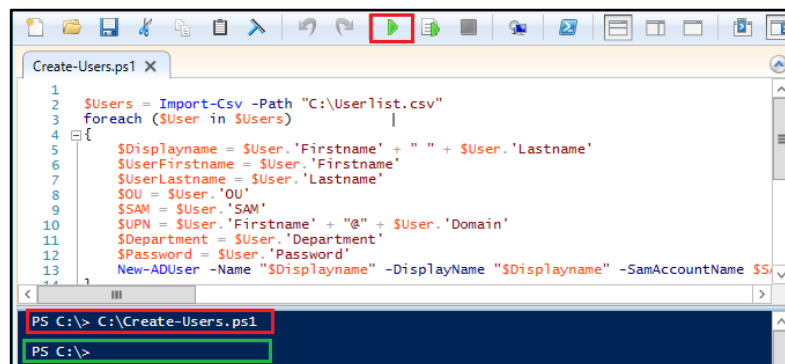
John,Snow,cyber.local,John,"OU=Sales,DC=Cyber,DC=local",Pa\$\$w0rd,Sales



```
File Edit Format View Help
Firstname,Lastname,Domain,SAM,OU>Password,Department
John,Snow,cyber.local,John,"OU=Sales,DC=Cyber,DC=local",Pa$$w0rd,Sales
James,Bond,cyber.local,James, "OU=IT,DC=Cyber,DC=local", Pa$$w0rd, IT
Tom,Riddle,cyber.local,Trent,"OU=IT,DC=Cyber,DC=local",Pa$$w0rd,IT
Tim,Roth,cyber.local,Cito, "OU=IT,DC=Cyber,DC=local", Pa$$w0rd, IT
Sarah,Marshall,cyber.local,Sara,"OU=IT,DC=Cyber,DC=local",Pa$$w0rd,IT
Su, Lee, cyber.local,Morgana,"OU=IT,DC=Cyber,DC=local",Pa$$w0rd,IT
```

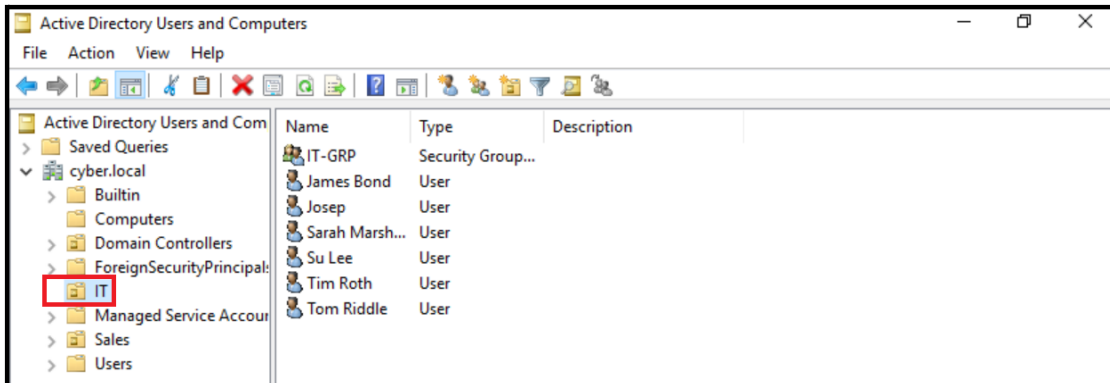
- 6 Run the script by clicking the green play icon or pressing **F5** on your keyboard.

Note: Make sure the PowerShell is in the proper path of the file for the program to execute.



```
PS C:\> C:\Create-Users.ps1
PS C:\>
```

7 Verify the users were created by opening Active Directory Users and Computers.



Lab Task 3: Manage a User Account by Using the Bulk Action Method

Practice using commands that will allow you to manage multiple users collectively.

- 1 Create two new users, **Test1** and **Test2**, in the IT OU via PowerShell with no additional parameters by using the following commands:

New-ADUser -Name Test1 -SamAccountName Test1 -path "OU=IT, DC=Cyber, DC=local"

New-ADUser -Name Test2 -SamAccountName Test2 -path "OU=IT, DC=Cyber, DC=local"

```
PS C:\Users\Administrator> New-ADUser -Name Test1 -SamAccountName Test1 -path "OU=IT, DC=Cyber, DC=local"
```

```
PS C:\Users\Administrator> New-ADUser -Name Test2 -SamAccountName Test2 -path "OU=IT, DC=Cyber, DC=local"
```

- 2 Show all users of the IT OU by using
Get-ADUser -Filter * -SearchBase "OU=IT, DC=Cyber, DC=local" -SearchScope subtree

```
PS C:\Users\Administrator> Get-ADUser -filter * -SearchBase "OU=IT, DC=Cyber, DC=local" -SearchScope subtree

DistinguishedName : CN=Josep,OU=IT,DC=cyber,DC=local
Enabled           : True
GivenName        :
Name             : Josep
ObjectClass       : user
ObjectGUID        : 01e070ae-7ef8-4500-906d-69d96a14d894
SamAccountName    : Josep
SID              : S-1-5-21-1869861495-3084386665-490034514-1110
Surname          :
UserPrincipalName :

DistinguishedName : CN=Sam Even,OU=IT,DC=cyber,DC=local
Enabled           : True
GivenName         : Sam
Name              : Sam Even
ObjectClass        : user
ObjectGUID         : 6b32b62f-f046-4272-9da2-c79152f409ca
SamAccountName     : Sam
SID               : S-1-5-21-1869861495-3084386665-490034514-1113
Surname           : Even
UserPrincipalName  : Sam@Cyber.com
```

- 3 Show all users from the domain for which the Department parameter equals IT. You will not see the two new users. Do you know why?

Get-ADUser -Filter "department -eq 'IT'"

```
PS C:\Users\Administrator> GET-ADUser -Filter "department -eq 'IT'"
DistinguishedName : CN=Josep,OU=IT,DC=cyber,DC=local
Enabled           : True
GivenName         :
Name              : Josep
ObjectClass       : user
ObjectGUID        : 3d3c485e-d489-4ab4-a3be-2f0092b47368
SamAccountName    : Josep
SID               : S-1-5-21-3539338704-3261642708-3860110303-1105
Surname           :
UserPrincipalName :
```

Or ***Get-ADUser -Filter {department -like "IT"}***

```
PS C:\Users\Administrator> GET-ADUser -Filter {department -like "IT"}
DistinguishedName : CN=Josep,OU=IT,DC=cyber,DC=local
Enabled           : True
GivenName         :
Name              : Josep
ObjectClass       : user
ObjectGUID        : 3d3c485e-d489-4ab4-a3be-2f0092b47368
SamAccountName    : Josep
SID               : S-1-5-21-3539338704-3261642708-3860110303-1105
Surname           :
UserPrincipalName :
```

- 4 To get all users from the IT OU for which the Department parameter is empty and set it to *IT* via a single command, run ***Get-ADUser -Filter {department -notlike "*"} -SearchBase "ou=IT, dc=Cyber, dc=local" | Set-ADUser -Department "IT"***

```
PS C:\Users\Administrator> Get-ADUser -Filter {department -notlike "*"} -SearchBase "ou=IT, dc=Cyber, dc=local" | Set-AD
User -Department "IT"
PS C:\Users\Administrator>
```

- 5 Repeat Step 3. You should now see the new users.