# Overview

In this guided practice you will create some common objects in Active Directory from the GUI and the command line.

# Objectives

Be able to create the common Active Directory objects from the GUI and command line including user accounts, computer accounts, security groups, distribution groups, and contact objects.

# Prerequisites

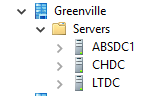
Guided practice – Configuring AD Replication is complete.

# Scenario

The ABS Corporation is still in the process of restructuring its logical and physical structure. The logical structure will involve creating additional OU and moving existing Active Directory objects into the OUs into a single domain. The physical structure change will involve moving from a 3-site setup to a single Active Directory site. In addition, the ABS Corporation has group policy resource access requirements that require additional Active Directory objects to implement. You will create the required objects in this guided practice.

# Tasks

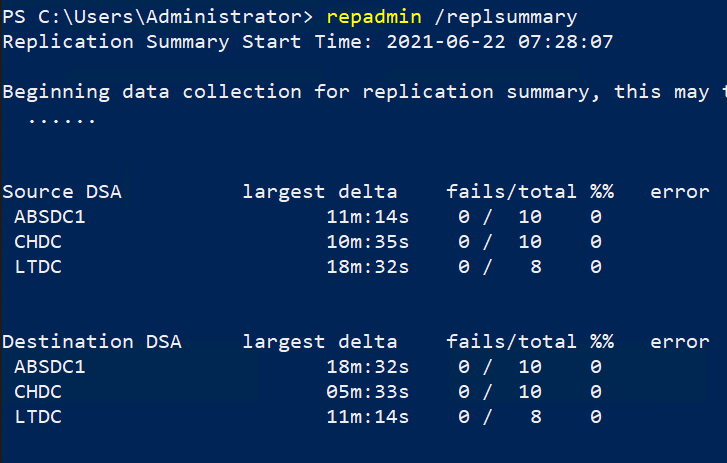
## Verify Active Replication

1. Log onto **CIS256-DC1** as **Administrator**.
2. Configure a single Active Directory site as follows:
   1. Move the **10.1.2.0/24** subnet to the **Greenville** site.
      1. Right click the **10.1.2.0/24** subnet and select **Properties**.
      2. In the **Site:** dropdown box, select **Greenville** and then click OK.
   2. Move the **10.1.3.0/24** subnet to the **Greenville** site.
   3. Verify that the **10.1.1.0/24** subnet is in the **Greenville** site.
   4. Move the **LTDC** domain controller to the **Greenville** site.
      1. Right click **LTDC** server, select **Move…**
      2. Select **Greenville** and then click OK.
   5. Move the **CHDC** domain controller to the **Greenville** site.
3. All servers should be in the Greenville site.  
   
4. Verify that Active Directory replication is up to date and has no errors.

repadmin /syncall /AedP

repadmin /replsummary

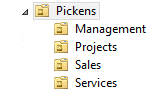
There should be no errors. If there are errors, troubleshoot the error using the tools you learned in the previous exercise.



1. **Warning**: Do not proceed until Active Directory Replication is up to date.

## Create OUs to support Domain Consolidation

Organizational units are required to support moving the users from the **Lametech** domain to the **Absorp** domain. The new OU structure requires a **Pickens** OU that contains an OU for the **Services**, **Sales**, **Projects**, and **Management** departments.

To create the required OUs, perform the following:

1. Logon to the **CIS256-DC1** as the **Absadmin**
2. Open **Active Directory Users and Computers** and create an **OU** for **Pickens.**
3. Create an **OU** for **Services**, **Sales**, **Projects**, and **Management** in the **Pickens** OU
4. The OU structure should look like the figure.

## Move Lametech users to the Abscorp domain

Before demoting the Pickens domain controller, we will need to move the users to the **Abscorp** domain. The users should be placed in their respective OUs.

To move the users in the Management OU of the **Lametech** domain to the **Abscorp** domain, perform the following:

1. **Login** to the **CIS256**-**DC1** virtual machine as the **Absadmin**
2. Open a **PowerShell** session with **administrative** rights and type the following command:

Get-ADUser -Filter \* -SearchBase "OU=Management,DC=lametech,DC=com" -Server ltdc.lametech.com | Move-ADObject -TargetPath "OU=Management,OU=Pickens,DC=ABSCorp,DC=com" -TargetServer absdc1.abscorp.com

1. **Note**: you will have some errors due to name conflicts as you did in a previous guided practice. In real life we would resolve these user naming conflicts, but for the purpose of this guided practice we will just ignore them.
2. Modify the command above to **move** the **users** **from** the **Sales**, **Projects**, and **Services** OUs in the **Lametech** domain to the OUs created above in the **Abscorp** domain.
3. Verify that the users have been moved to the **ABScorp** domain before proceeding.

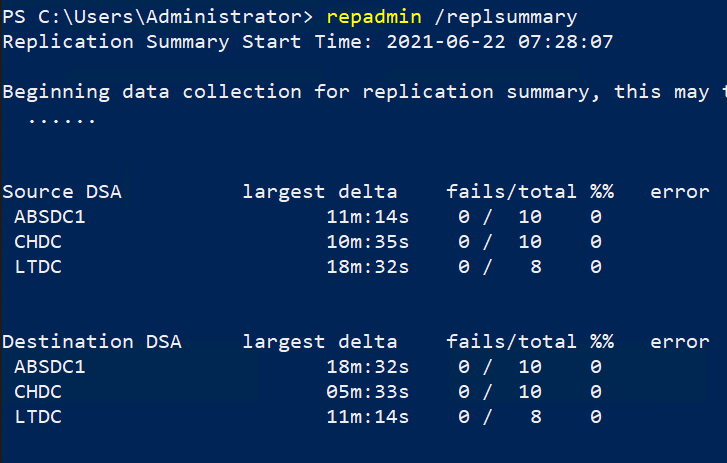
## Remove the Lametech domain

Now that the users have been moved to the new domain, the **Lametech.com** domain is no longer needed and will be removed. When the domain is removed you will add it as an additional domain controller in the **ABSCorp** domain.

1. Logon to the **CIS256-DC1** virtual machine as the **ABSAdmin.**
2. Transferthe **Domain Naming Master** to **ABSDC1**.
3. Force replication updates on **LTDC** and **ABSDC1** to ensure all DCs know the current **Domain Naming Master**. To do this, open an elevated PowerShell session and type the following commands. There should be no errors. You must correct replication errors prior to proceeding.

repadmin /syncall /AdeP

repadmin /replsummary



1. Logon to the **CIS256-DC3** virtual machine as the **ABSCorp Administrator** and **demote** the domaincontroller using the procedure you learned previously. You can continue creating OUs in the next step while the domain controller is being demoted. This is the last Domain Controller in the domain.
2. Once the domain is removed, you can turn off the virtual machine and delete it. **CIS256-DC3** will not be used for the remainder of the course.

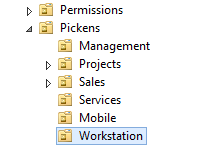
## Creating OUs to support Group POlicy

ABS Corporation wishes to have different group policy settings that apply to workstations and mobile devices. To support this the company needs to create two OUs at each location. These OUs will be named Workstations and Mobile.

To create the OU named **Workstation**, perform the following:

1. Logon to the **CIS256-DC1** virtual machine as the **absadmin**.
2. Open **PowerShell** with **Administrative** rights.
3. Type the following command to create the OU:

New-ADOrganizationalUnit -Name Workstation -path “OU=Greenville,DC=abscorp,DC=com”

1. Modify the command above to create the OU **Mobile** in the **Greenville** OU
2. Use the steps above to createsimilarOUs in the **Pickens** and **Charlotte** OUs.
3. Use the steps above to create an OU named **Permissions** in the root of the **ABSCorp** domain.
4. The **Permissions** OU and the OU structure for the **Pickens** location is shown in the figure on the right. The **Greenville** and **Charlotte** locations should be similar depending on the departments at each location.

## Creating Groups to Support Assigning Access To Resources

ABS Corporation will be configuring shared folders and printers for use by the employees within the departments and their organization. They will be using the AGGUDLP grouping strategy to implement security on these shared resources. In this step you will create the groups necessary to implement the grouping strategy and secure these resources.

### Creating Global Groups for the Departments and Locations

To create a global group for the IT department at ABS Corporation in Greenville.

1. Logon to the **CIS256-DC1** virtual machine using the **administrator** account.
2. Open a **PowerShell** prompt with **administrative** privileges.
3. Type the following command:

New-ADGroup -name GV-IT -GroupScope Global -GroupCategory Security -path “OU=Greenville,DC=abscorp,DC=com”

### Adding Users to Groups

1. To add users to the group you previously created type the following in a **PowerShell** Administrative shell:

Add-ADGroupMember -Identity GV-IT -Members (Get-ADUser -filter \* -SearchBase “OU=IT,OU=Greenville,DC=abscorp,DC=com”)

* 1. This command uses the **Get-ADUser** command to find all the users in the **IT** OU inside of **Greenville** and add them to the **GV-IT** group. The same can be done by browsing to the Greenville **IT** OU in **Active Directory Users and Computers** and selecting all the users and **choosing Add to group** from the context menu.

1. Create the following groups and add the respective users to the group using the steps above or the GUI.

| Group Name | Group Scope | Group Category (Type) | Location | Members |
| --- | --- | --- | --- | --- |
| GV-Management | Global | Security | Greenville OU | Personnel in the Management Department at Greenville |
| GV-Projects | Global | Security | Greenville OU | Personnel in the Projects Department at Greenville |
| GV-Sales | Global | Security | Greenville OU | Personnel in the Sales Department at Greenville |
| Greenville | Global | Security | Greenville OU | Personnel at the Greenville Location |
| CH-Management | Global | Security | Charlotte OU | Personnel in the Management Department at Charlotte |
| CH-IT | Global | Security | Charlotte OU | Personnel in the IT Department at Charlotte |
| CH-Engineering | Global | Security | Charlotte OU | Personnel in the Engineering Department at Charlotte |
| Charlotte | Global | Security | Charlotte OU | Personnel at the Charlotte Location |
| ABS-Employees | Global | Security | Users folder | All ABS employees |
| ABS-Management | Global | Security | Users folder | Management Employees from all locations |

1. Normally, you would create groups that represented the departments and employees in Pickens, but we have omitted these to save time.

## Create the Folder structure For ABS Corporation

1. Logon to the **CIS256-DC1** virtual machine using the **ABSAdmin** account.
2. Open **PowerShell** without Administrative rights.

ABS Corporation requires shared folders to implement group policy, user configuration and storage, and collaboration.

To create a folder in PowerShell, type the following:

New-Item -Path C:\Shares\Redirect -ItemType Directory

The example above creates the folder **Redirect** and the folder **Shares.**

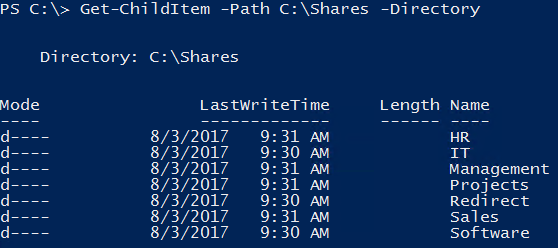
**CIS256-DC1 (ABSDC1) virtual machine:**

1. Create the additional folders below.

* C:\Shares\Software
* C:\Shares\IT
* C:\Shares\Projects
* C:\Shares\Sales
* C:\Shares\Management
* C:\Shares\HR

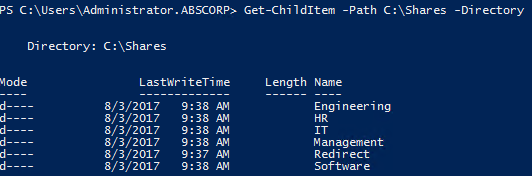
1. Type the following command to verify that all of the folders were created:

Get-ChildItem -Path C:\Shares –Directory

1. Your output should look like the screenshot below.
2. Create the folder structure below on the Charlotte domain controller to support this.
   1. Log on as **ABSAdmin** and open **PowerShell** without Administrative rights.

**CIS256-DC2 (CHDC) virtual machine:**

* 1. C:\Shares\Redirect
  2. C:\Shares\Software
  3. C:\Shares\IT
  4. C:\Shares\Engineering
  5. C:\Shares\Management
  6. C:\Shares\HR

1. Use the previous command to verify the folders were created. You should see the output below.

## Creating Shared Folders

1. Open **PowerShell** with **Administrative** rights.
2. The following command will share the **C:\Shares\Redirect** folder with the name **Redirect** and the **Full Control** permissions granted to the **Everyone** group.

New-SmbShare -Name Redirect -Path C:\Shares\Redirect -FullAccess Everyone

1. Share each of the folders above with the same settings on the **Greenville** and **Charlotte** servers
   1. **Note**: The shared folders can also be created with the following PowerShell command. This will work on both servers.

Get-ChildItem -Path C:\Shares -Directory | % { New-SmbShare -Name $\_.Name -Path $\_.FullName -FullAccess Everyone }

* 1. The above command lists the directories in the **C:\Shares** folder and sends the directory objects through the pipeline. The object is represented by the **$\_** variable the **Name** property and **FullName** properties are used to provide values for the **Name** and **Path** parameters. The **%** symbol is an alias for the **ForEach-Object** cmdlet which is used to run commands on an object passing through a pipeline.

1. Verify the folders were shared with the following cmdlet: ***Get-SmbShare.***

## Securing the ABS Corporation Folder structure

In the previous sections you have created global groups and added accounts to those groups (AG). You have also nested some global groups within other groups (GU). You will now create domain local groups and place the global or universal groups within these and assign these groups permissions (DLP) to resources (folders) to implement your grouping strategy and secure the folder structure.

ABS Corporation uses the following naming standard for domain local groups used for assigning permissions:

* Groups will be in the **Permissions** OU.
* Groups will be named as follows:
  + Server Name - **ABSDC1** or **CHDC**
  + A “-“dash character
  + The name of the shared folder
  + A “-“dash character
  + The type of access the group has **-R** for **Read and Execute**, **-M** for **Modify**, **-F** for **Full Control**
  + **Example**: **ABSDC1-Redirect-F** would be the name of the group that has full control of the shared folder named **Redirect** on **ABSDC1.**

The **IT** group in **Greenville** needs **full control** of the shares folder on **ABSDC1**.

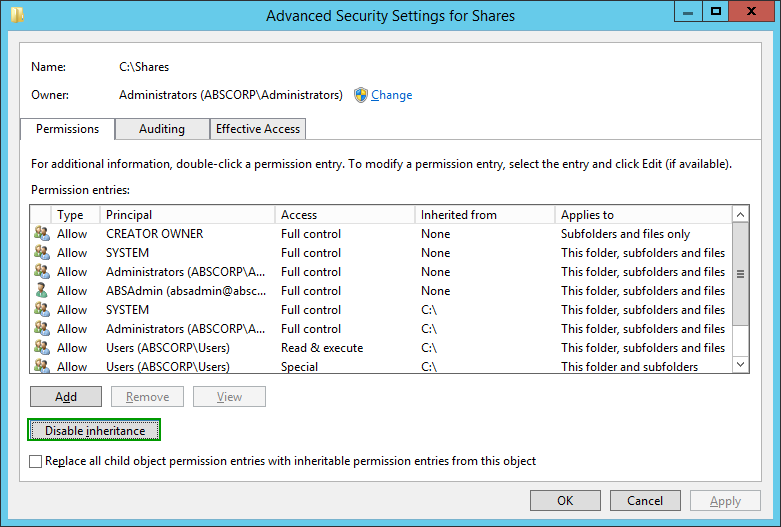
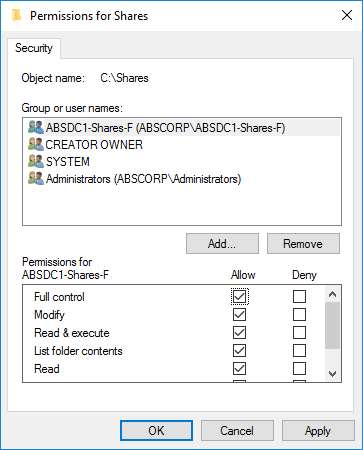
Use the following procedure to implement security on the IT share in Greenville:

1. Login to the **CIS256-DC1** virtual machine as the **ABSCorp** **Administrator**.
2. Create the domain local group using the following command:

New-ADGroup -Name ABSDC1-Shares-F -GroupScope DomainLocal -GroupCategory Security -Path “OU=Permissions,DC=abscorp,DC=com”

1. Add the IT global group to the group using the following command:

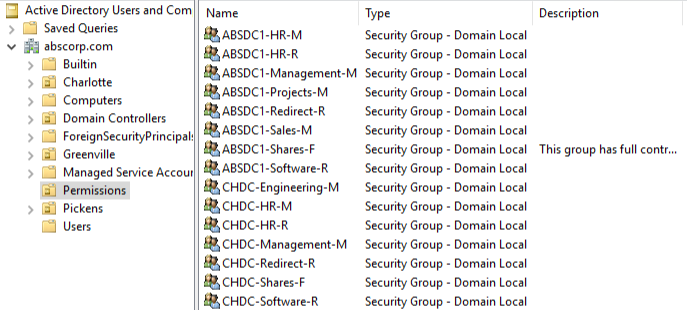
Add-ADGroupMember -Identity ABSDC1-Shares-F -Members GV-IT

1. Disable inherited permissions on the **C:\Shares** folder as follows:
   1. Open the **properties C:\Shares** folder.
   2. On the **Security** **tab**, **click** the **Advanced** button.
   3. In the **Advanced Security for Shares** dialog box, click the **Disable inheritance** button as shown in the figure to the right.
   4. The **Block Inheritance** dialog box will open, **select** the **Convert inherited permissions to explicit permission on this object** option.
   5. In the **Advanced Security for Shares** dialog box, click the **OK** button.
   6. On the **Security** page of the **Shares** **properties** dialog box, click the **Edit** button and remove the users (**ABSCorp\Users**) entry.
   7. Click **OK** to close.
2. Open the **properties** of the **C:\Shares** folder. **Configure** **security** so that the **ABSDC1-Shares-F** group has **full** control. Make sure the **Creator Owner**, **System**, and **Administrators** group permissions are not changed.
3. **Optional** - Configure the description for the group above. This could have also been done when you created the group. Use the following command to set the description for the group above:

Set-AdGroup -Identity ABSDC1-Shares-F -Description “This group has full control permissions for the C:\Shares folder located on ABSDC1”

Configure the following security settings on the remaining folders using the **AGDLP** strategy shown above: (**Note**: you will have to create Domain local groups for each of the permissions assigned, for example: a Domain local group named **ABSDC1-Software-R** should be made for giving read access to the **Software** share on **ABSDC1**)

| Folder | Permissions |
| --- | --- |
| CIS256-DC1 (ABSDC1) | |
| C:\Shares\Redirect | GV-IT has full control, Greenville has read access |
| C:\Shares\Software | GV-IT has full control, Greenville has read access |
| C:\Shares\IT | GV-IT has full control |
| C:\Shares\Sales | GV-IT has full control, GV-Sales has Modify |
| C:\Shares\Management | GV-IT has full control, GV-Management has Modify |
| C:\Shares\Projects | GV-IT has full control, GV-Projects has Modify |
| C:\Shares\HR | GV-IT has full control, ABS-Management has Modify, ABS-Employees have read |
|  | |
| CIS256-DC2 (CHDC) | |
| C:\Shares\Redirect | CH-IT has full control, Charlotte has read access |
| C:\Shares\Software | CH-IT has full control, Charlotte has read access |
| C:\Shares\IT | CH-IT has full control |
| C:\Shares\Engineering | CH-IT has full control, CH-Engineering has Modify |
| C:\Shares\Management | CH-IT has full control, CH-Management has Modify |
| C:\Shares\HR | CH-IT has full control, ABS-Management has Modify, ABS-Employees have read |

When you are done creating the groups your Permissions OU should contain the groups shown in the figure below: (**Note**: groups were not created for **ABSDC1-IT-F**, **CHDC-Redirect-F** because **GV-IT** and **CH-IT** respectively already have full control permissions through inheritance from **ABSDC1-Shares-F** and **CHDC-Shares-F**)

## Submission Requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

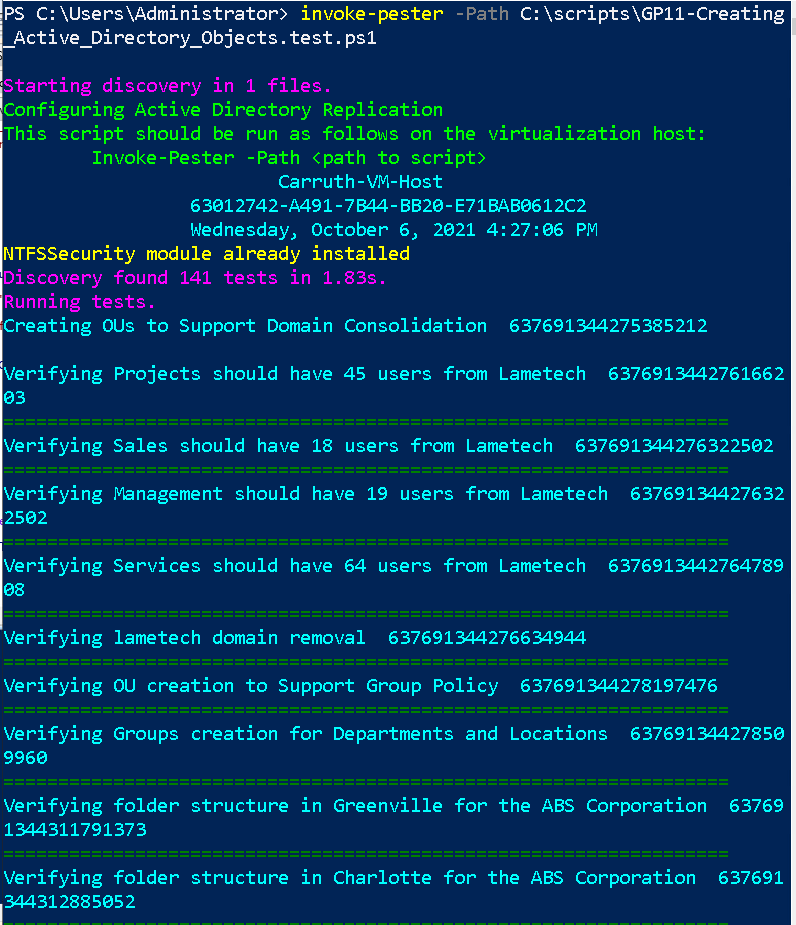
Invoke-Pester -Path C:\Scripts\GP011-Creating\_Active\_Directory\_ Objects.test.ps1

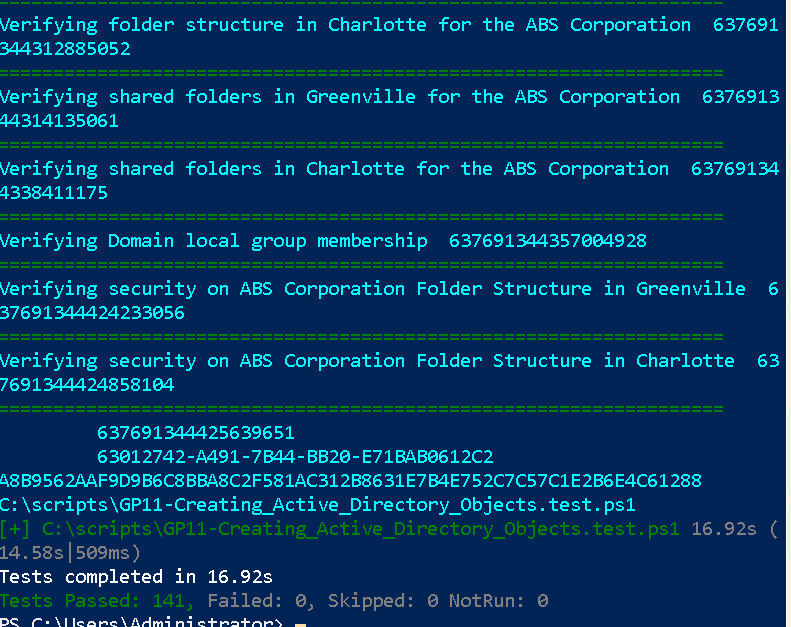
**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP011-Creating\_Active\_Directory\_ Objects.test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below.





1. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document.**
2. **Upload** the **document** in the submission area for the assignment.