***Milestone 2 Start***

Use this template file to organize screenshots demonstrating completion of each rubric item. Your screenshots do not need to match the example ones. You will also need to meet with your instructor during class time to demonstrate your working Virtual Machines and answer any questions they may have to receive your mark.

* View the FSMO in your domain and save a screenshot of the output in the same folder as you save the output from the system information Powershell script you wrote in Milestone 1

|  |  |
| --- | --- |
| * Screenshot of FSMO roles saved | 2 |

Include screenshot(s) of the FSMO roles

A screenshot of a computer

Description automatically generated

* Create the following OU’s off the root of your domain:
  + Marketing
  + Sales
  + IS
  + Accounting
* Under the Accounting OU, create an Accounts Receivable (AR) and an Accounts Payable (AP) OU
* Create appropriate groups for each department in the department OU
* Create appropriate user templates for each department in the department OU

|  |  |
| --- | --- |
| * OU's Properly Created | 6 |
| * Departmental Local and Global Groups Created | 6 |
| * Departmental Templates Created | 3 |

Include 6 screenshot(s) of the above OUs (and sub-OUs) with groups and templates

A screenshot of a computer

Description automatically generated

* Usernames should be *FirstInitialLastName. Eg. ASmith*
* Create the following users and add them to the appropriate groups:

|  |  |
| --- | --- |
| Marketing | Addie Smith |
|  | Martha Jones |
| Sales | James Jury |
|  | Adam First |
| IS | Amanda Love |
|  | Semore Class |
| Accounting | Ida Boss |
|  | Susan Black |
| AR | Ivonna Cash |
|  | Eddie Money |
| AP | Jason Poor |
|  | Francais Broke |

* Make sure all user password are set not to expire including the Administrator password (This is not best practice in the workplace!)
* Make sure all passwords are set to Password01

|  |  |
| --- | --- |
| * Users Created and Placed in Proper OU's | 6 |
| * User Naming Convention is Correct | 2 |

Include 6 screenshot(s) of the Users in their OusA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

## Powershell Script

* Create a PowerShell that accepts 0-3 OU-name command-line arguments.
* There should not be any error if there are less than three.
* Create OU's based on the arguments and then create 25 users within the correct OU ([param1] user 1, [param1] user 2, etc).
* Users should be given a password of “Password 01” and should be enabled.
* Groups should be created (using command-line arguments) within the OUs. The users should be added to the correct group.
* Use your script to create audit users, training users and branch users, using “audit”, “training” and “branch” as command line arguments, these should NOT be coded in.

|  |  |
| --- | --- |
| * Powershell script accepts up to three command line arguments. No error thrown if less than three | 2 |
| * Groups created within the correct OU in Script | 3 |
| * 25 users created (through the script) in each OU with the correct naming convention, password set and user enabled | 3 |
| * Users added to correct groups through the script | 3 |
| * Best coding practices are followed | 2 |

Include screenshot(s) of the script (you will also submit the file)

A screenshot of a computer program

Description automatically generated

Include screenshot(s) showing the new OUs, Groups and new Members created by the Script

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## RODC

* Pre-stage a RODC.
* Save a screenshot of the pre-stage setup in your system information folder.
* The passwords of the branch users (created with the Powershell script) will be the only passwords saved on the RODC.
  + This is found in the Password Replication Policy of the RODC
  + <https://www.rebeladmin.com/2014/10/password-replication-in-rodc/>
* Install the RODC using the pre-stage that you have set up.

|  |  |
| --- | --- |
| * Screenshot of pre-stage RODC is present | 2 |
| * DNS Name Resolution Works | 2 |

Include screenshot(s) of the pre-stage RODC

A screenshot of a computer

Description automatically generated

Include a screenshot showing the Server Manager page of the RODC VM, the IP address and Windows Update status should be visible

A screenshot of a computer

Description automatically generated

Include a screenshot of a external DNS lookup on the RODC

A screenshot of a computer

Description automatically generated

Include a screenshot of the Password Replication Policy showing the Branch users on the RODC

A screenshot of a computer

Description automatically generated

* Run your system information Powershell Script that you set up in Milestone 1 and save the RODC relevant output.
* After running that script delete the RODC & save the affected users information to a file to confirm the password resets
  + You can delete the RODC's computer account using the Active Directory Users and Computers MMC snap-in.
  + The RODC account is in the Domain Controllers container.
  + When you delete the computer object, you'll be prompted for confirmation, and once you confirm you'll be given the option to reset all passwords that were stored on the RODC, as shown here.
  + Resetting the passwords effectively renders the stolen RODC useless from a malicious hacker's perspective.
  + Note you can also reset the computer account passwords, but this generally isn't required.
  + You can also export a list of all the accounts whose passwords are reset.
  + Users whose passwords have been reset will have to contact support to get a new password.
  + You can use the exported list of accounts from the delete phase to notify users in advance and proactively arrange new passwords.

|  |  |
| --- | --- |
| * System information was run and shows the RODC setup | 3 |
| * Branch Users affected by a password reset are saved in a file | 3 |

Include screenshot(s) of the RODC system information.

A picture containing screenshot, text

Description automatically generated

Also include the text file containing all the system information and the file containing the accounts whose passwords were reset, if the file is empty then a step was likely missed.