AD Audit

Purpose: Run an initial audit on an Active Directory site

This script is intended for information gathering purposes. It does NOT make any changes to the active directory site you run it against.

This script will gather the following information, and export the information into a CSV file:

* All groups in the AD structure
* All members of groups in the AD structure
* All enabled/disabled user accounts in the AD structure
* All enabled/disabled computers in the AD structure
* All “inactive” users and computers in the AD structure
  + “Inactive” is determined based on last logon time for users, using the time frame provided in the daysInactive parameter. I.E. 30/60/90/120 days
* All GPOs in AD structure
* Generates reports on every GPO in AD structure
* Information about all Domain Controllers in the AD structure
  + Gathers list of DCs
  + Gathers information about each DC
    - IP address
    - Enabled/disabled
    - Location
    - ReadOnly status
    - Operating system
  + Runs dcdiag on each DC
* Replication status for the domain
* FSMO role holders for the domain

All information gathered is exported to the location of your choosing. The script will create, as needed, the folder structures in the location you chose to save. I’ve tried to make the folder structure as logical as possible.

Parameters for the script are below:

* exportPath – Path to the location you wish to save the information gathered
* daysInactive – How many days should an account be inactive for. Must be a number of days

To run the script, you will need to launch PowerShell in an elevated session. I would recommend using a Domain Admin or higher credentials. Once in the elevated PowerShell session, you will have to launch the command like the screen shot below.

