Overview

The purpose of this Power Shell script is not to replace the Windows 10 Benchmark, but to enhance its capabilities by significantly reducing the number of "Not Reviewed" vulnerabilities.

Usage

1. Run the SCAP Tool using the latest Windows 10 Benchmark on the host under review. Note the location of where the SCAP Tool placed the resulting XCCDF file. **Ensure the latest Windows 10 Benchmark was used to scan the host under review.** If the latest Windows 10 Benchmark is not used, additional "Not Reviewed" vulnerabilities may be present in the final Windows 10 checklist.
2. Unzip the contents of the script zip file named "U_Windows_10_V1R17_STIG_PS" onto the host under review. This action will place the script file folder named "U_Windows_10_V1R17_STIG_PS" onto the host under review. Open the unzipped folder named "U_Windows_10_V1R17_STIG_PS" and place the XCCDF file created in step one into the folder named "Seed_XCCDF" of the unzipped script file structure (See Figure 1). **Please note that only one XCCDF file can be present in the "Seed_XCCDF" folder.**

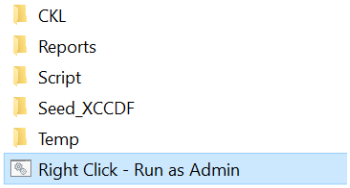

Figure 1

3. Right click the .bat file named "Right Click – Run as Admin" and run the file as the Administrator. This will start execution of the Power Shell Script and open a command window that displays the progress of the script. Please note, you will be prompted to answer questions before the script begins checking the "Not Reviewed" vulnerabilities left behind by the SCAP Tool.
4. Once the script has completed checking the "Not Reviewed vulnerabilities, it will automatically import the XCCDF results from the Seed_XCCDF folder and create a final checklist (ckl) that contains both the SCAP scan results and the Power Shell script results. The final checklist will automatically be placed into the folder named **"Reports"** of the script file structure (See Figure 1). This final checklist can now be opened in STIG viewer as normal. You will not have to import any XCCDF results into STIG viewer. Just open the final report in STIG viewer by selecting "Checklist" and then by selecting "Open Checklist from File". Please note, the script will not alter any checks that were completed by the SCAP scanner. It only attempts to address the "Not Reviewed" vulnerabilities left behind by the SCAP scanner. **Do not remove or alter the checklist located in the CKL folder. This checklist is a template that is used by the Power Shell script.**
5. For those checks that are site information dependent, the script will gather information from the host and place this information into the "Finding Details" section for that particular vulnerability check (See Figure 2). This information is meant to help you make a decision as to whether the host is compliant or non-compliant.

Figure 2