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 from 70 down to 3.

Usage

1. Run the SCAP Tool using the latest Windows 10 Benchmark on the host under review. Create a checklist in STIG Viewer using STIG U_Windows_10_V1R14_STIG and import the XCCDF results into the STIG checklist and then save the checklist containing the SCAP results onto the host under review. Please note, you must use STIG checklist U_Windows_10_V1R14_STIG in STIG viewer.

2. Unzip the contents of the script zip file named "U_Windows_10_V1R14_STIG_PS" onto the host under review. This action will place the script file folder named "U_Windows_10_V1R14_STIG_PS" onto the host under review. Open the unzipped folder named "U_Windows_10_V1R14_STIG_PS "and place the checklist created in step one into the folder named "Seed_ckl" of the unzipped script file structure (See Figure 1). Please note that only one checklist (.ckl) file can be present in the "Seed_ckl" folder. If you rerun the SCAP tool and create a new seed checklist, you must delete the old checklist out of the "Seed_ckl" folder before running the script.

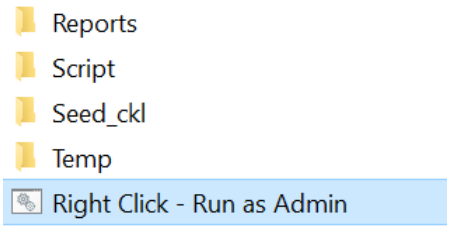

Figure 1

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 3 questions before the script begins checking the "Not Reviewed" vulnerabilities in the checklist created in step 1.
4. Once the script has completed, it will place a final checklist 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. 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.
5. For those checks that are site information dependent, the script will gather information from the host and place this information into the "Comments" 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