Defense Security Service
Industrial Security Field Operations
National Industrial Security Program
(NISP) Authorization Office (NAO)

Getting Started with the SCAP Compliance Checker and STIG Viewer Job Aid

February 2017

Revision Log

Date	Revision	Description of Change
2017FEB06	1.2	Updated to reflect OBMS Tool Availability

SCAP Compliance Checker

The SCAP Compliance Checker is an automated compliance scanning tool that leverages the DISA Security Technical Implementation Guidelines (STIGs) and operating system (OS) specific baselines to analyze and report on the security configuration of an information system. The tool can be run locally on the host system to be scanned, or scans can be conducted across a network from any machine on the domain. In either scanning environment, the following requirement applies: The user conducting the scan must have administrative privileges on the machine to be scanned. If the machine to be scanned is not hosting the tool, domain-level administrative privileges (or individual local administrator accounts) are required to remotely scan other systems on the network.

Obtaining the SCAP Tool

The SCAP Compliance Checker can be obtained in two ways, depending upon the possession of a DoD PKI token:

PKI enabled:

- Navigate to DISA's Information Assurance Support Environment (IASE) webpage at the following URL: http://iase.disa.mil/stigs/scap/Pages/index.aspx , and scroll to the bottom section titled "SCAP Tools".
- Identify the appropriate version of the tool that corresponds to the Operating System that will host the application, and provide your PKI credentials when prompted to start the download of the ZIP file.

Non-PKI Enabled:

- Navigate to the DSS ODAA Business Management System via NCAISS at the following URL: https://ncaiss.dss.mil
- Log into OBMS using your appropriate credentials
- Once logged into OBMS, navigate to the top of the home page and click on "ODAA Bulletin Board".
- Click on "Headquarters Bulletin Board" under the Headquarters section.

- In the Headquarters bulletin board, click on the forum post with the title corresponding to the SCAP Compliance Checker installer you require (e.g. "SCAP Compliance Checker Applications – Windows").
- Download the ZIP file, unarchive, and install the application.

Installing the SCAP Compliance Checker:

Within the ZIP file for each Operating System version of the SCAP Compliance Checker is an included PDF, instructing the user on the appropriate way to install and configure the software executable on the host system. The user will need to be logged onto the system as an Administrator in order for the package to install correctly.

STIG Viewer

The STIG Viewer is a Java-based application that will be used in conjunction with the SCAP Compliance Checker scan results in order to view the compliance status of the system's security settings. The STIG Viewer can also be used in a manual fashion (e.g. without SCAP tool results) to conduct a manual audit of information system security controls. Use of the viewer does not require administrator privileges, provided that the required software packages to support Java applications have been installed on the system.

Obtaining the DISA STIG Viewer (Version 2.4.1)

The DISA STIG Viewer is an unclassified, non-PKI controlled tool that can be accessed and downloaded on DISA's IASE website at the following URL: http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

The tool requires no installation, and runs as a Java application from any directory on the host machine.

Operating System Baselines

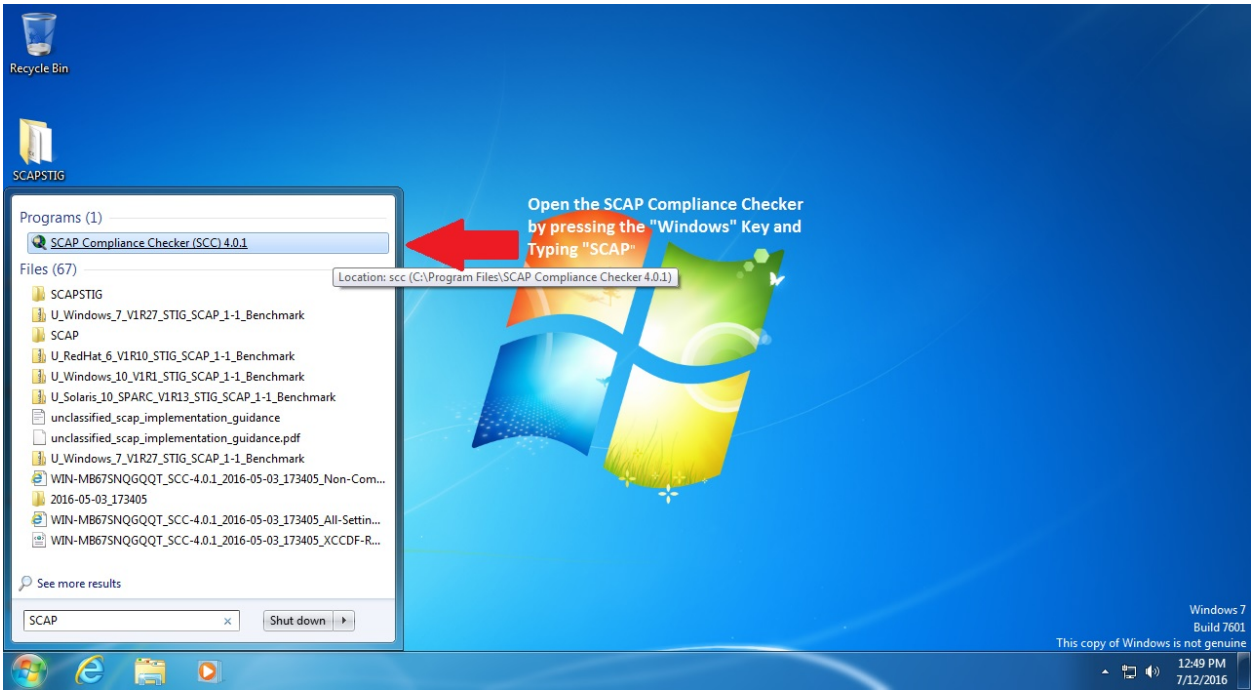
The STIG Viewer leverages operating System baselines to generate checklists used for vulnerability assessments. These baselines are version- specific, so ensure that you download the appropriate baseline for the operating system you wish to assess. For purposes of viewing scan results of machines other than the host machine, download the baseline representing the scanned

system's architecture. The baselines are unclassified; non-PKI controlled, and can be downloaded by navigating to DISA's IASE website at the following URL:

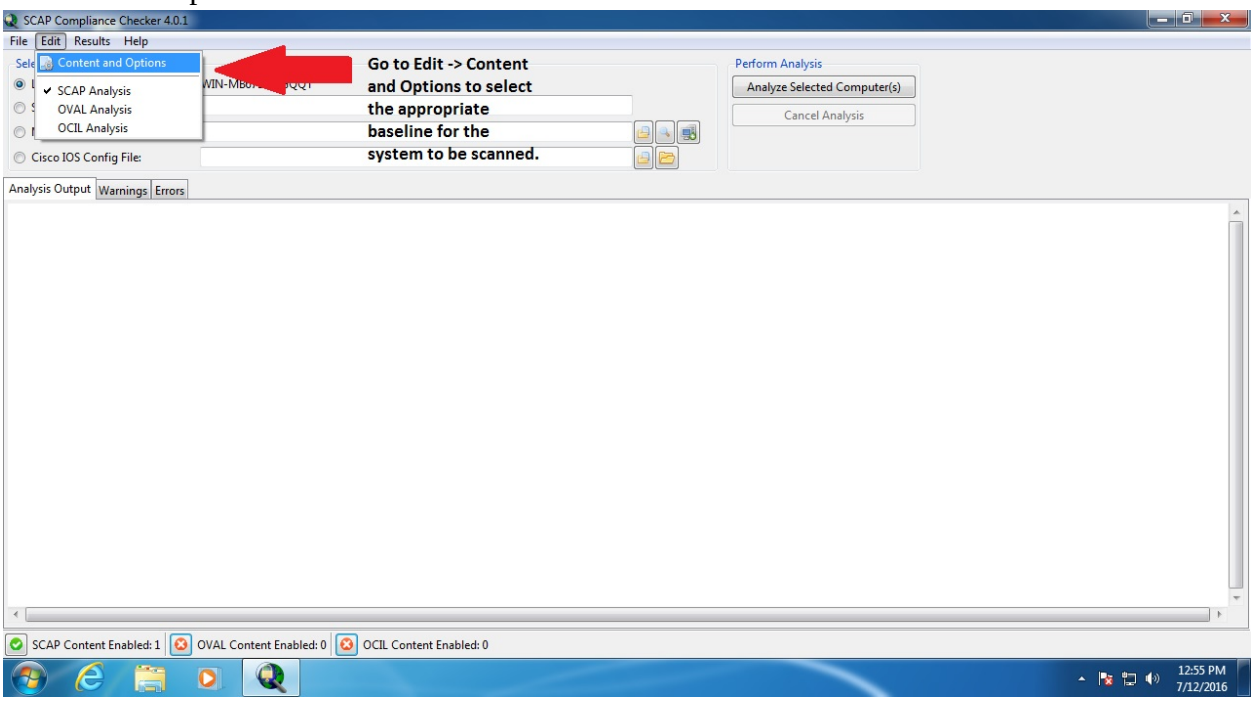
http://iase.disa.mil/stigs/os/Pages/index.aspx

Scanning with SCAP CC and STIG Viewer

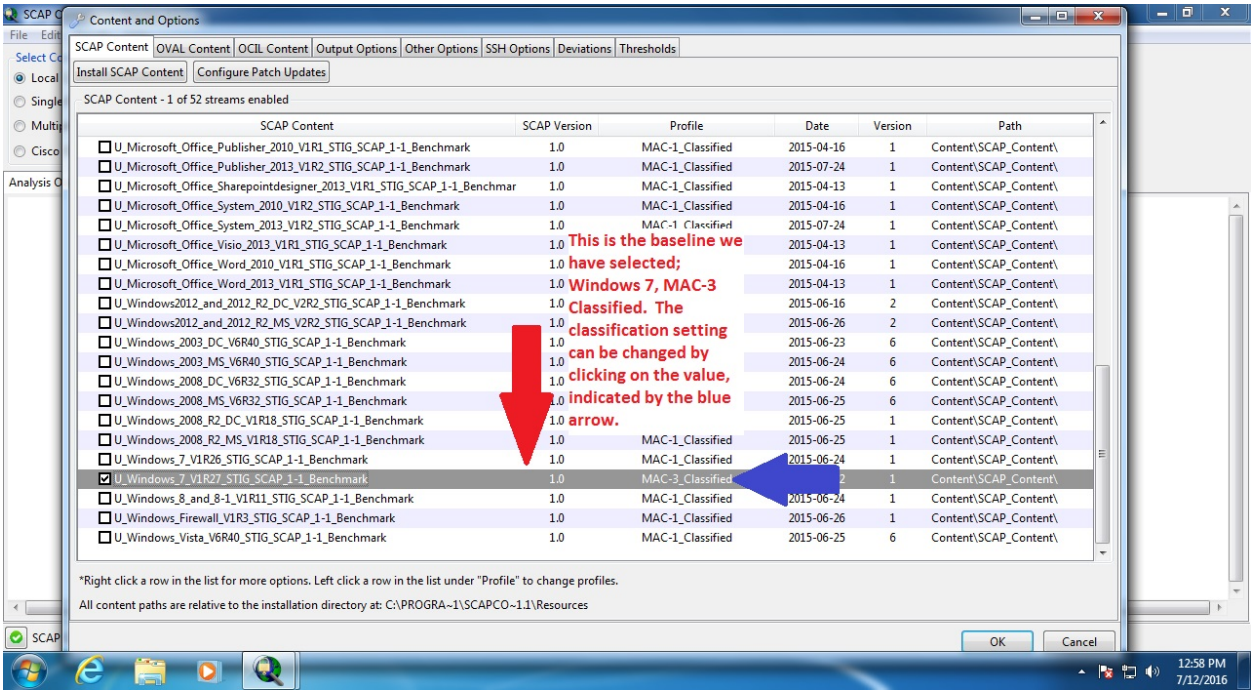
1. Open the SCAP Compliance Checker Application.



2. Select the appropriate baseline for the system that is to be scanned. First, click Edit -> Content and Options:

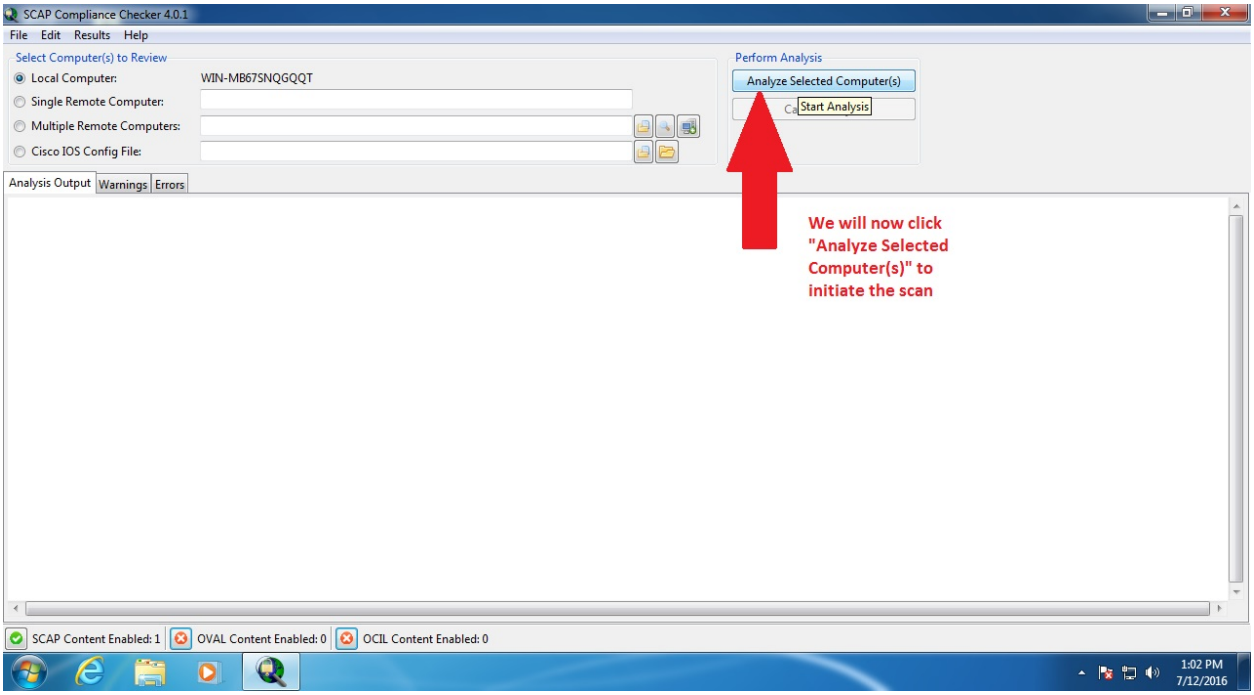


3. Next check the box for the appropriate baseline that corresponds to the system being scanned. Also, be sure to designate the scan profile as "MAC-3 Classified":

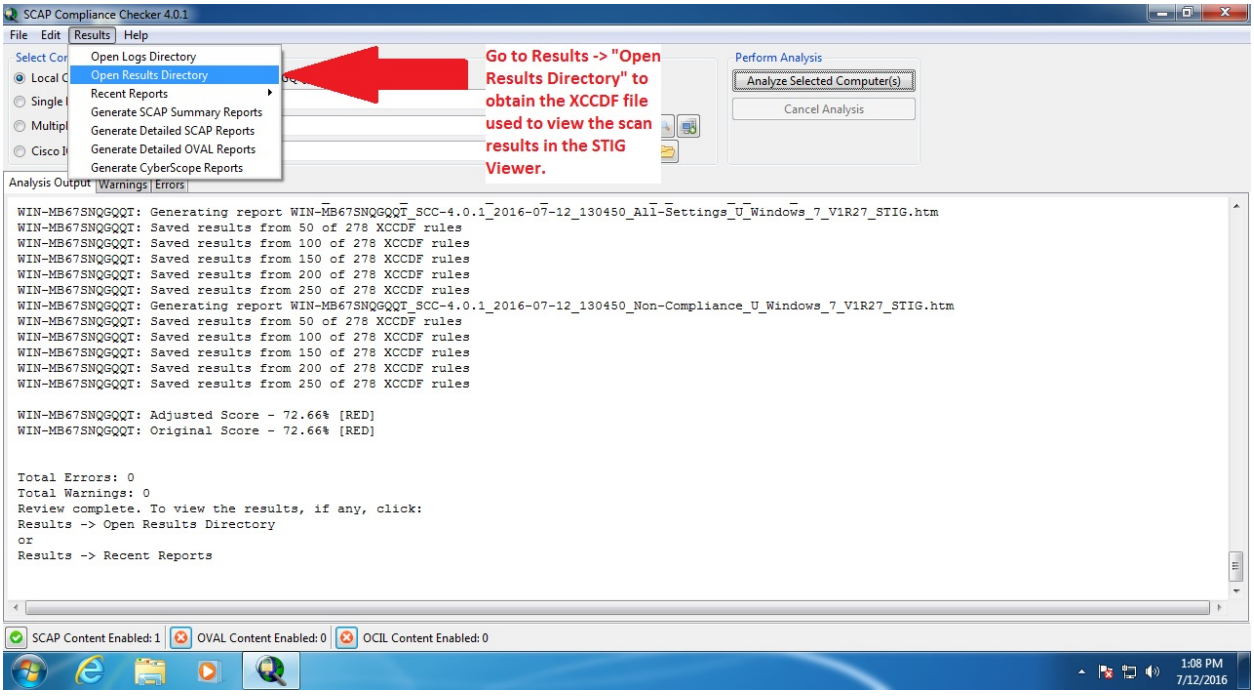


4. Click OK to save the configuration settings.

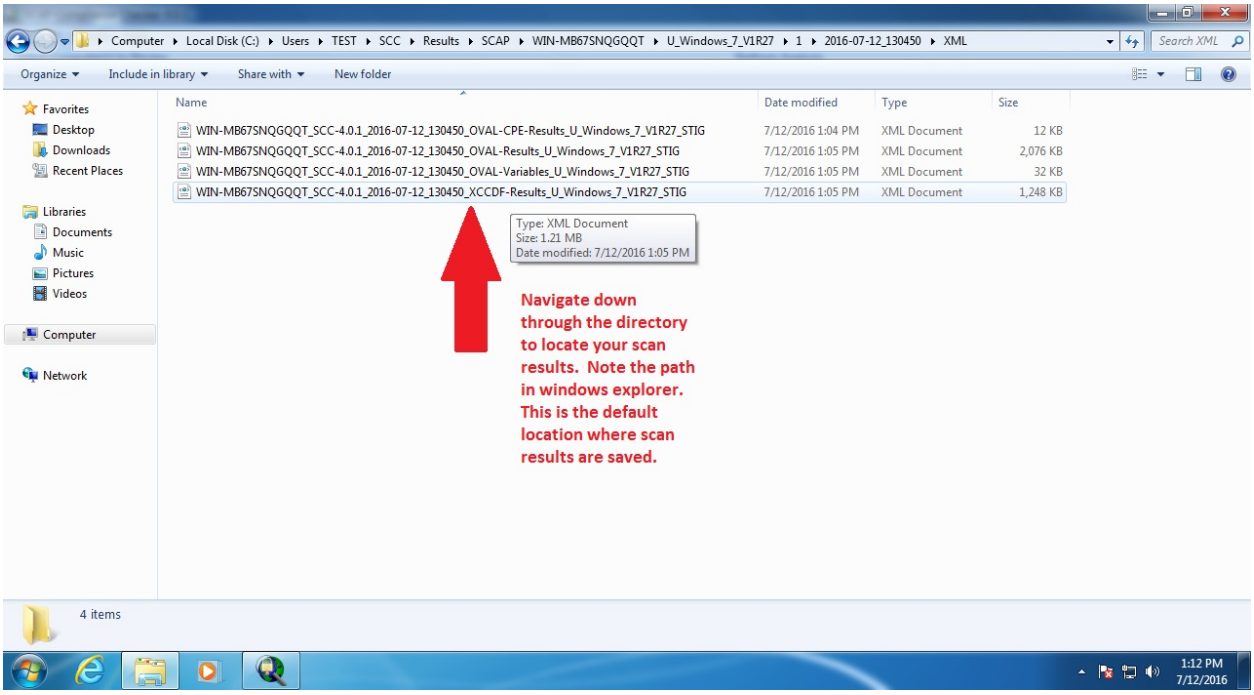
5. Initiate the scan of the system as shown below:



6. Once the scan has completed, view the directory containing the results of the scan by clicking "Results -> Open Results Directory" as shown below:

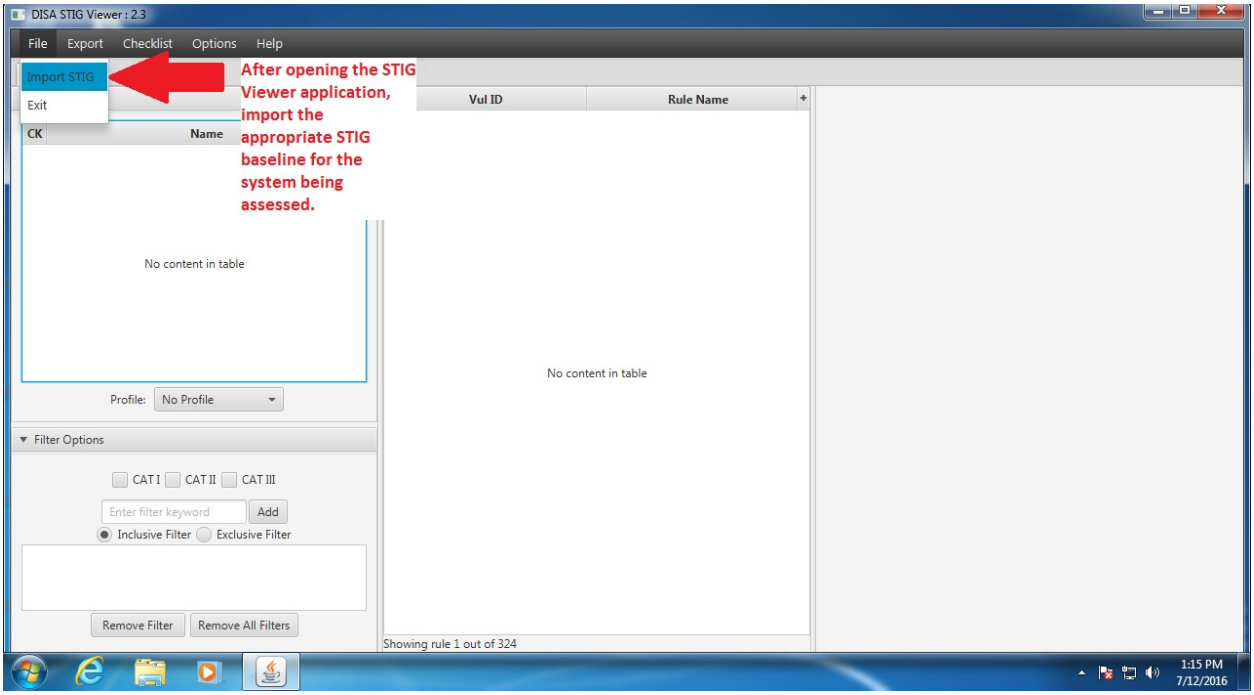


7. This will open the scan results directory. Take note of the XML file containing “XCCDF”. This is the scan results file that you will import into the STIG Viewer to analyze the compliance state of the machine:

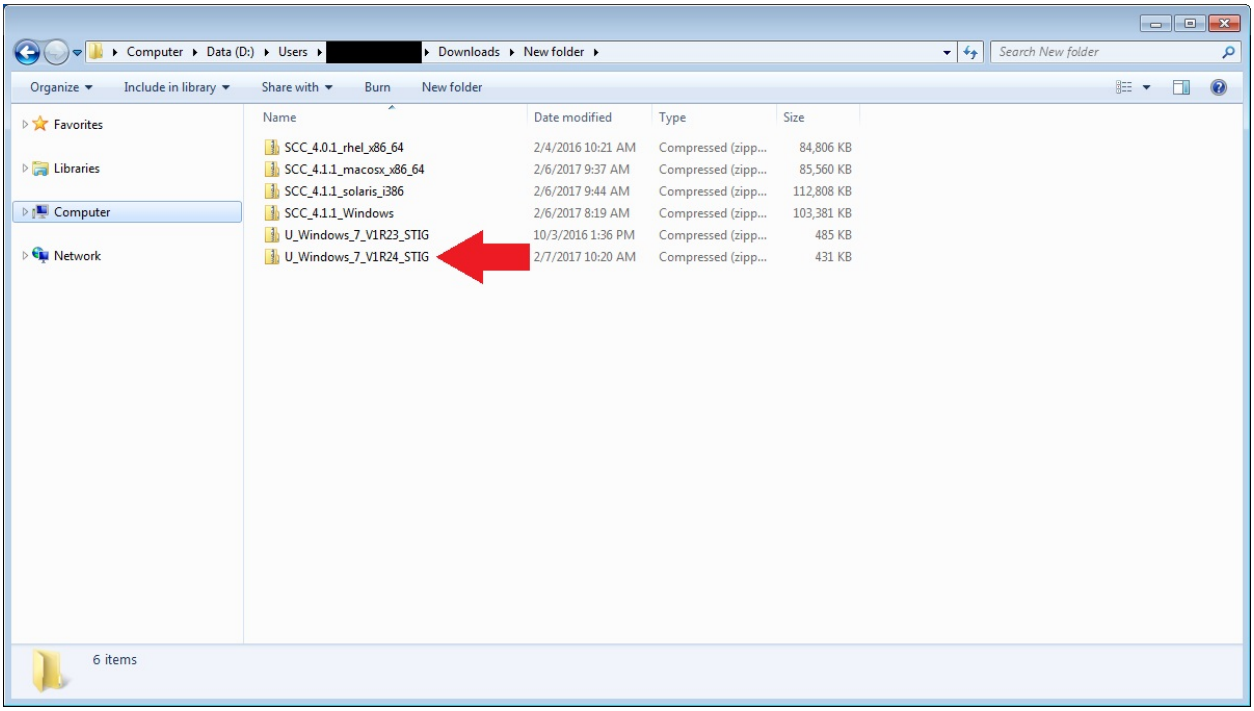


8. Open the STIG Viewer application.

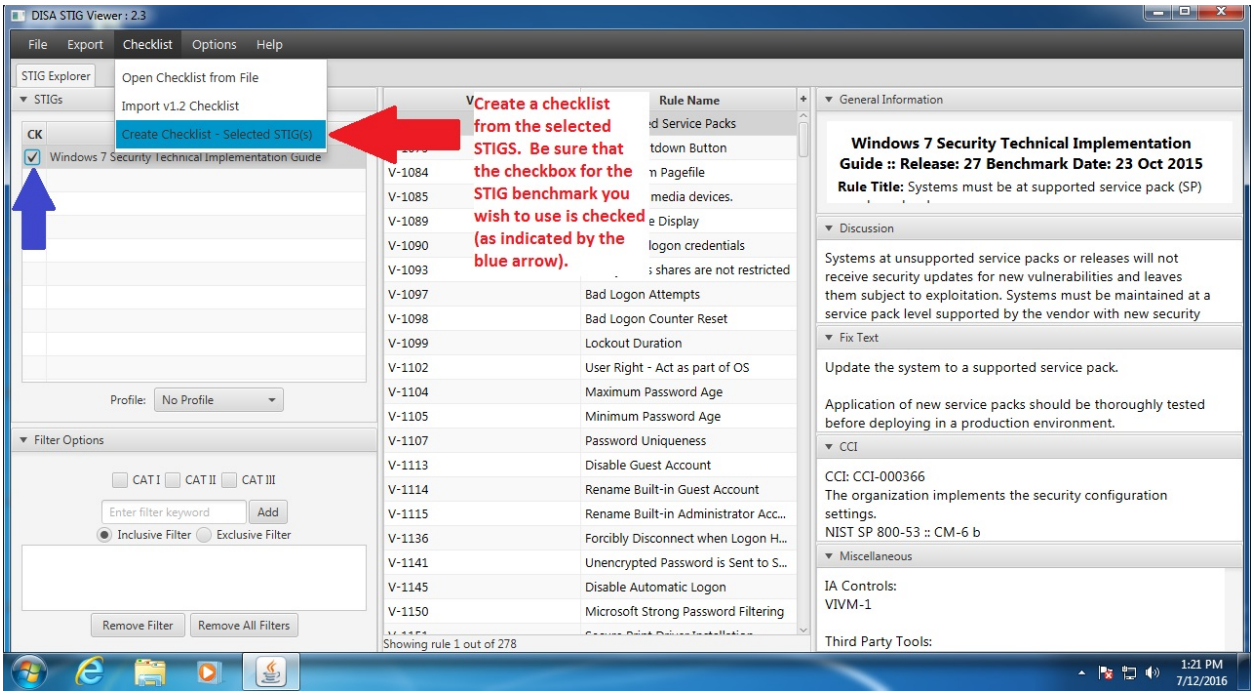
9. Once the STIG Viewer application is running, import the appropriate STIG baseline previously downloaded in Section 3. First, click “File -> Import STIG”:



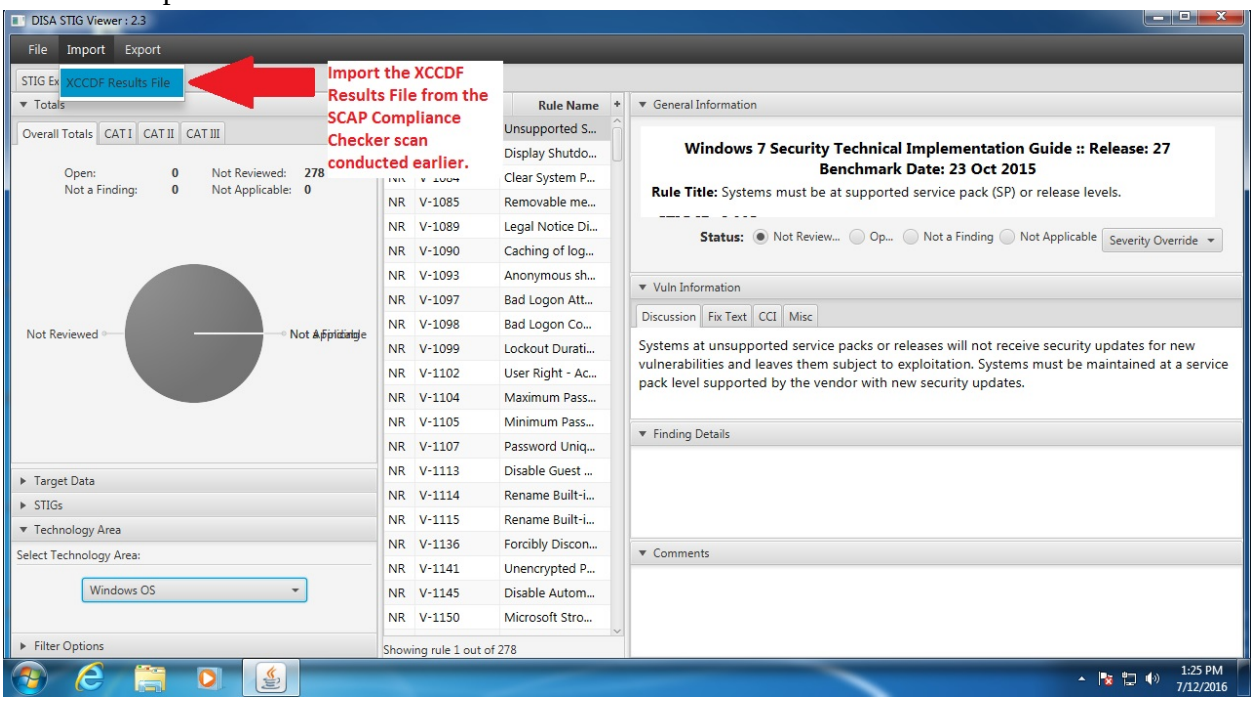
10. Next, navigate to the directory where you have stored the downloaded baseline. Select the ZIP file containing the desired baseline and select “Open”:



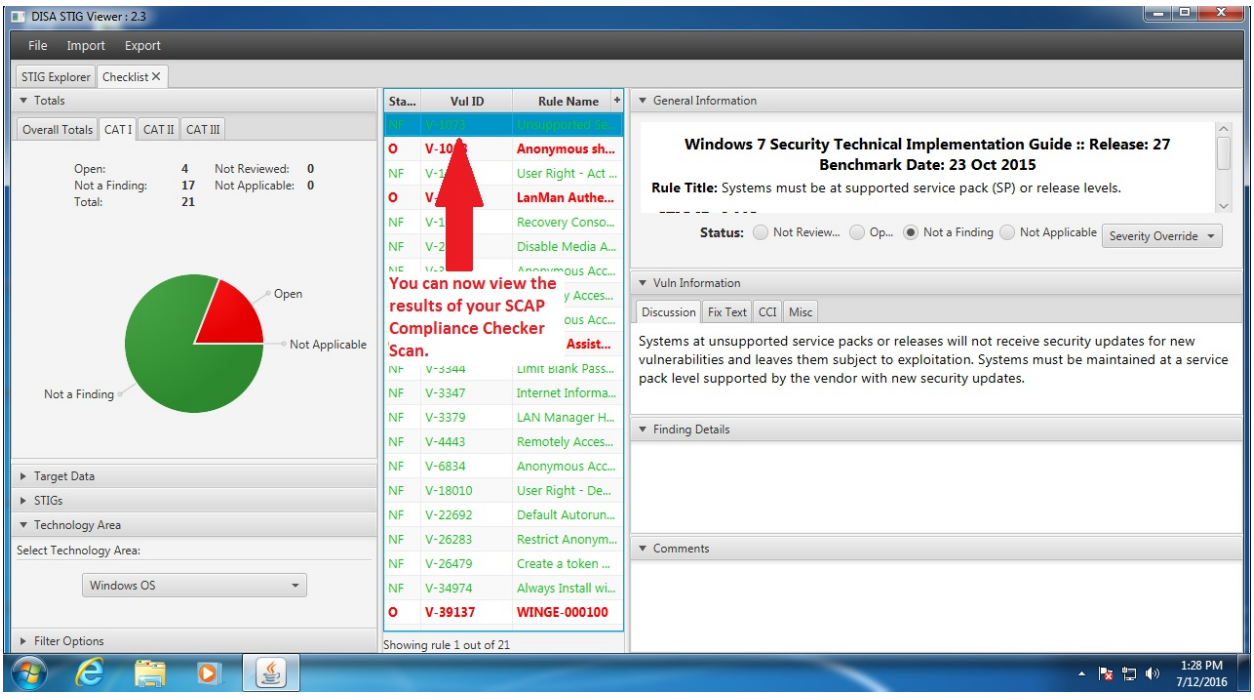
11. Create a checklist from the STIG baseline you just selected by navigating to the top bar and clicking “Checklist -> Create Checklist – Selected STIG(s)”:



12. Import the SCAP Compliance Checker XCCDF scan results file from Step 7. To do this, click on “Import -> XCCDF Results File”:



13. You can now view the results of the SCAP Compliance Checker scan against the STIG baseline for your operating system:



If you have any questions or concerns, please contact your assigned ISSP, or visit the DSS NAO RMF website located at the following address: www.dss.mil/rmf