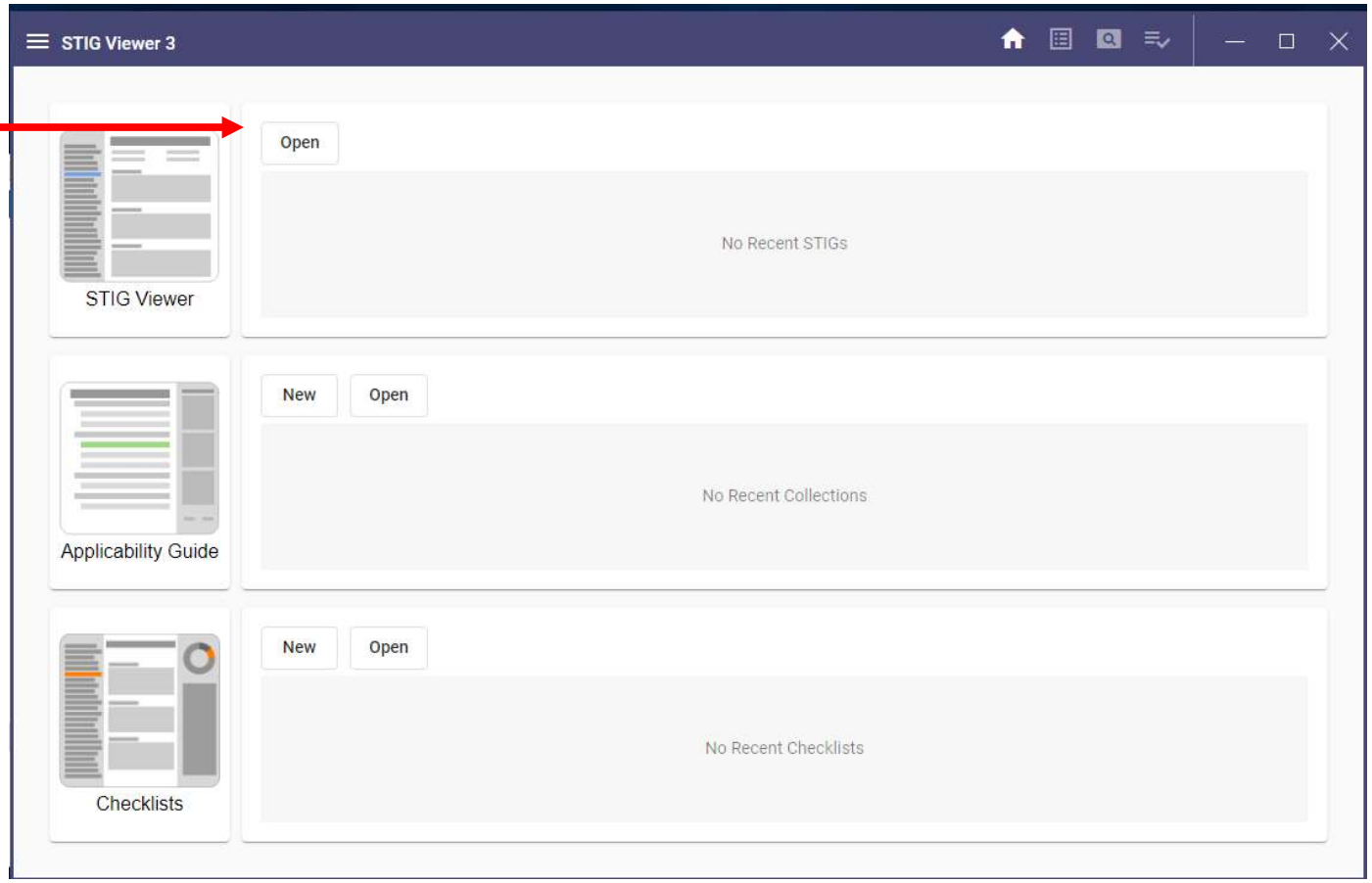
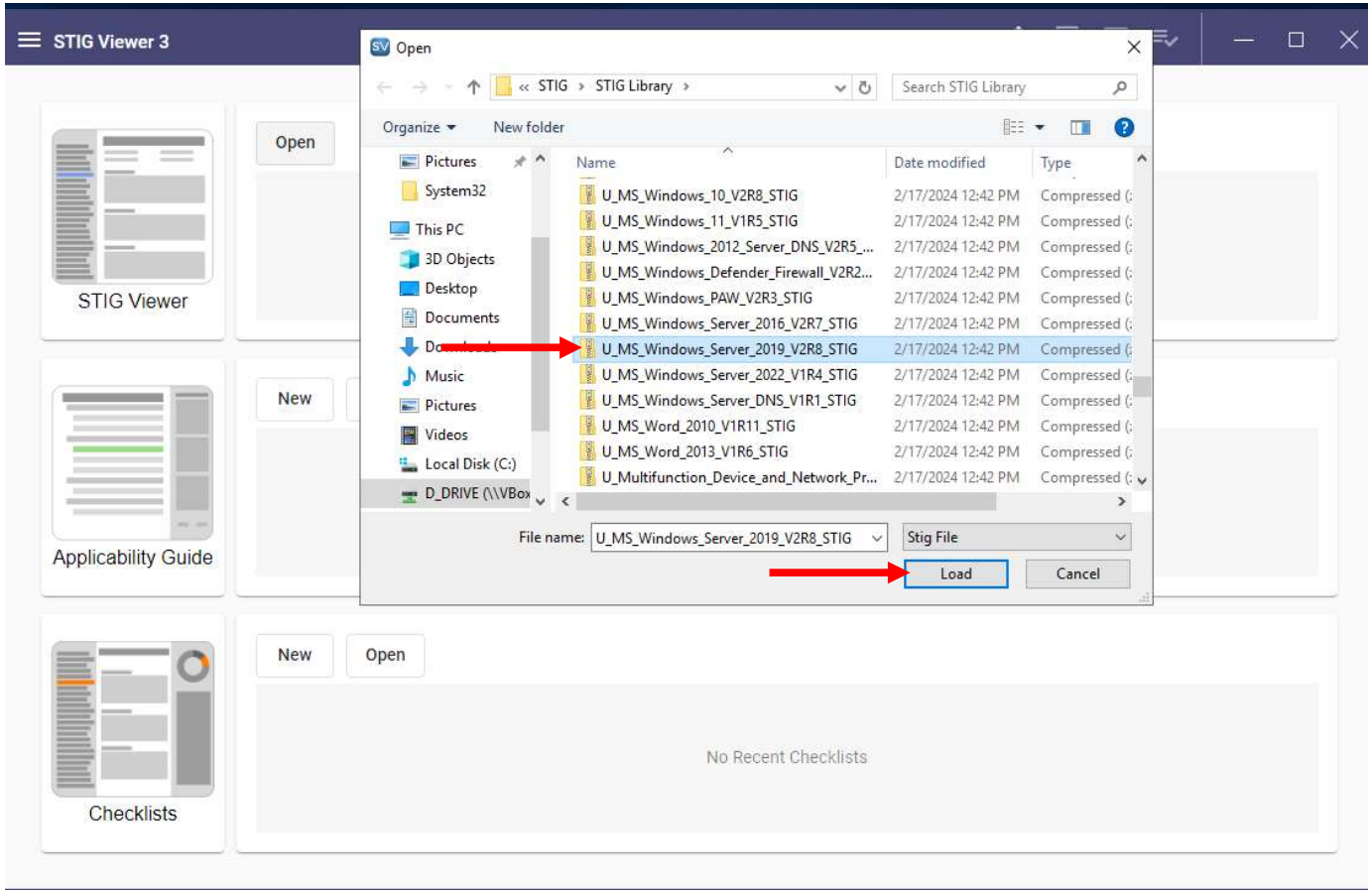
Basic Intro to STIG Viewer and SCAP

By: Chris Gaynor

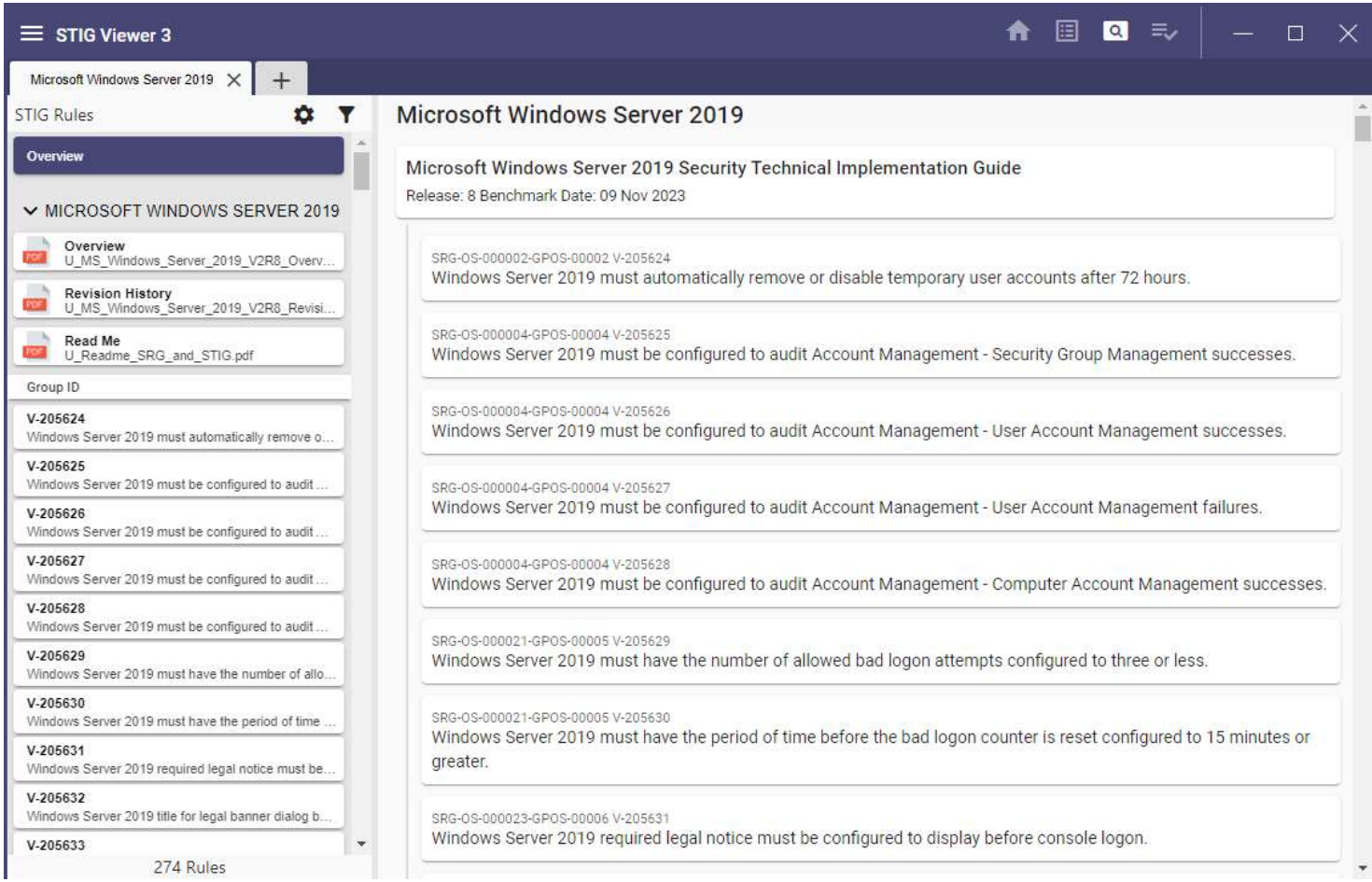
First we want to open STIG Viewer and from here we will select Open



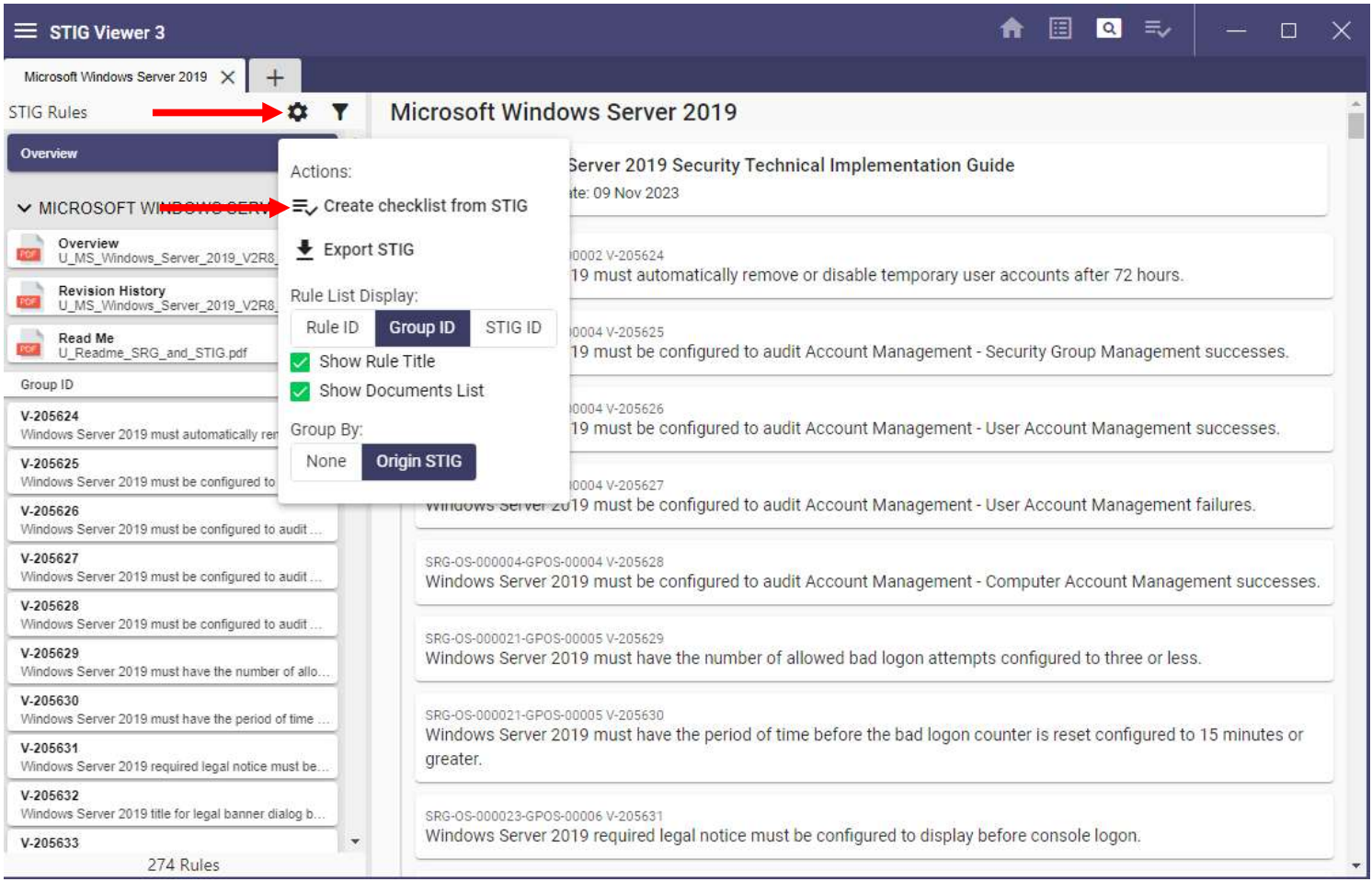
Load the proper STIG from the library. I'm using this on a Win Server 2019 so that is what I will select.



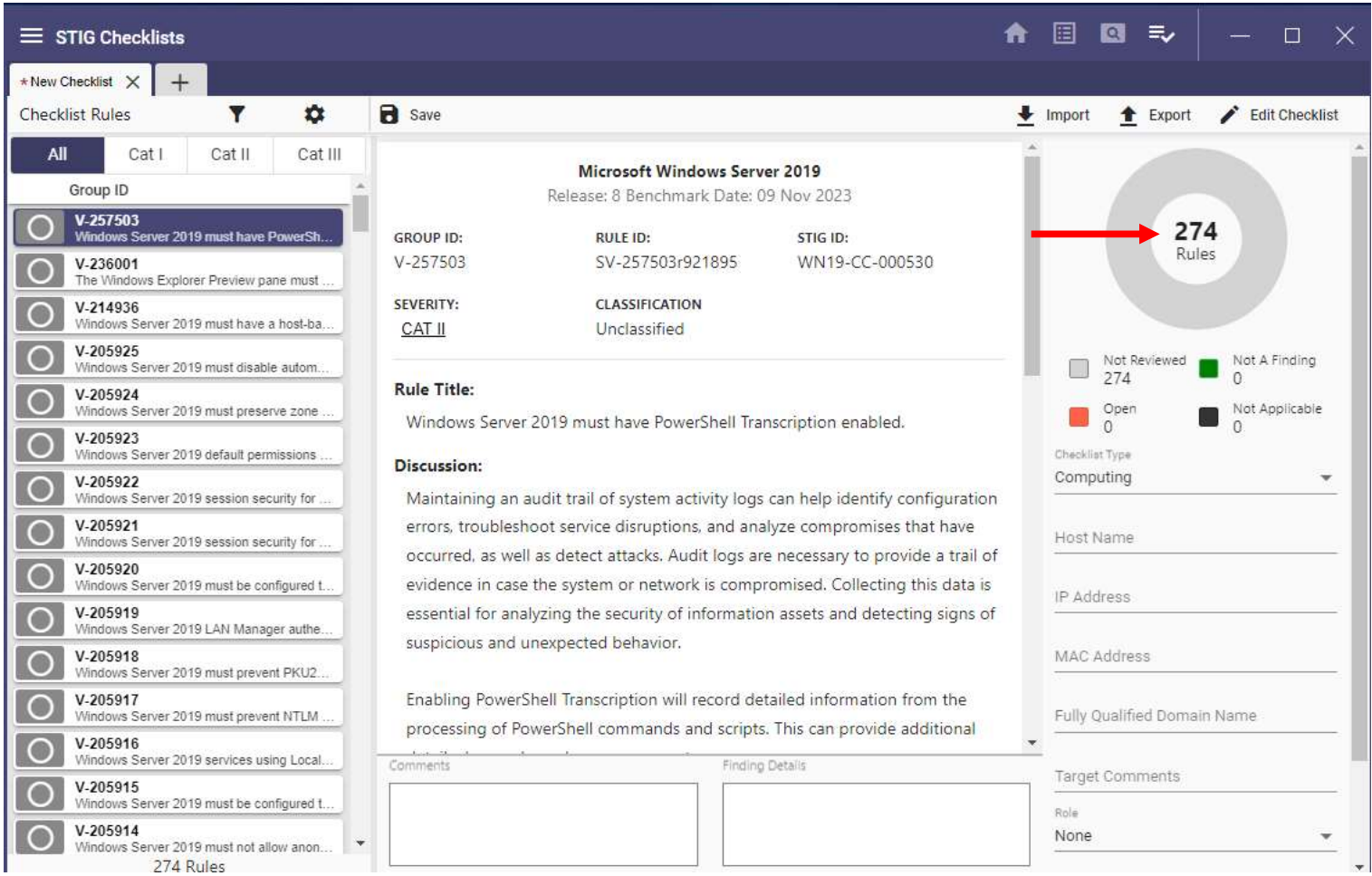
The STIG rules associated with your library selected should now be loaded.



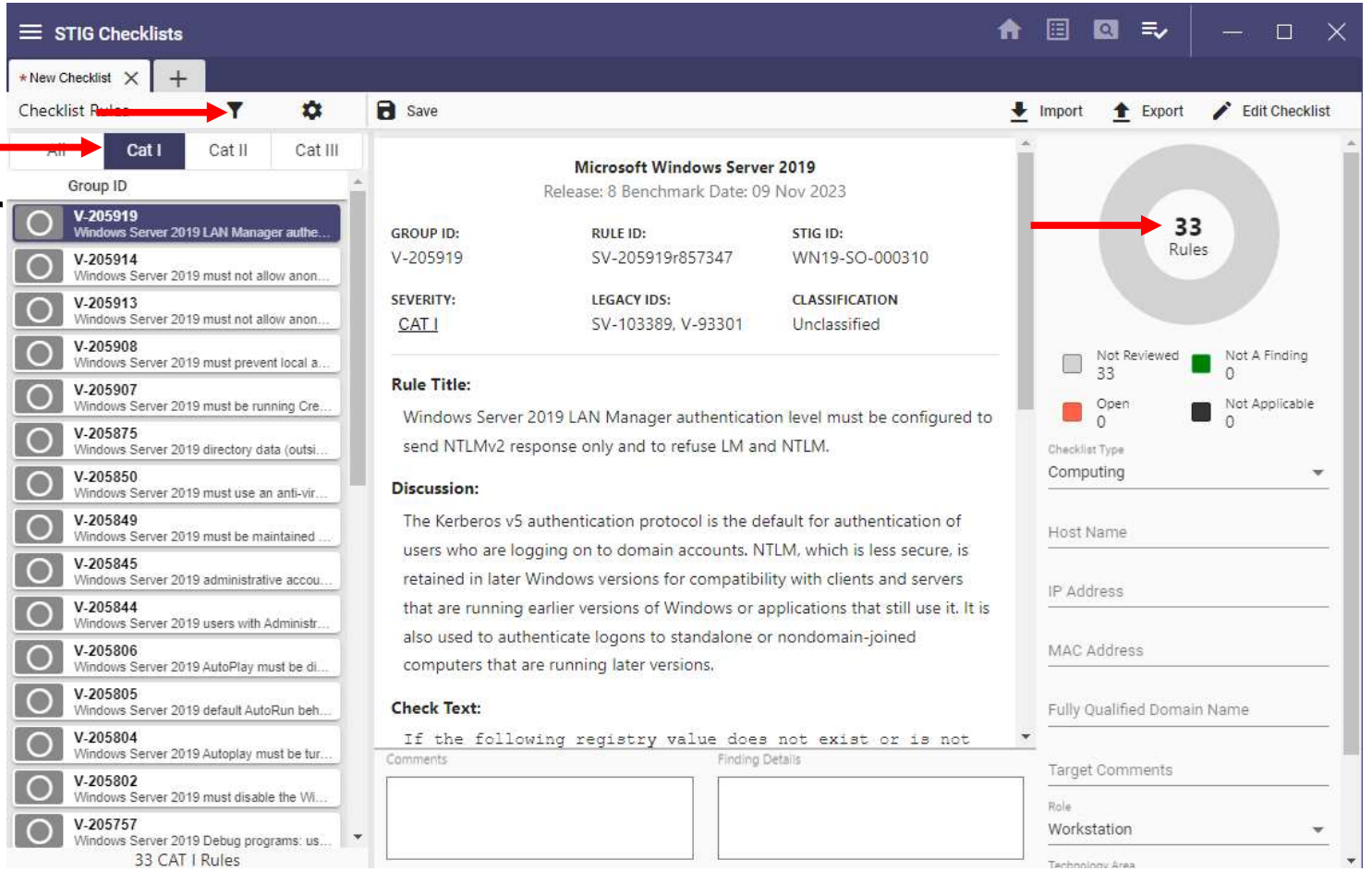
Next select the rule list settings (gear icon) and then Create checklist from STIG



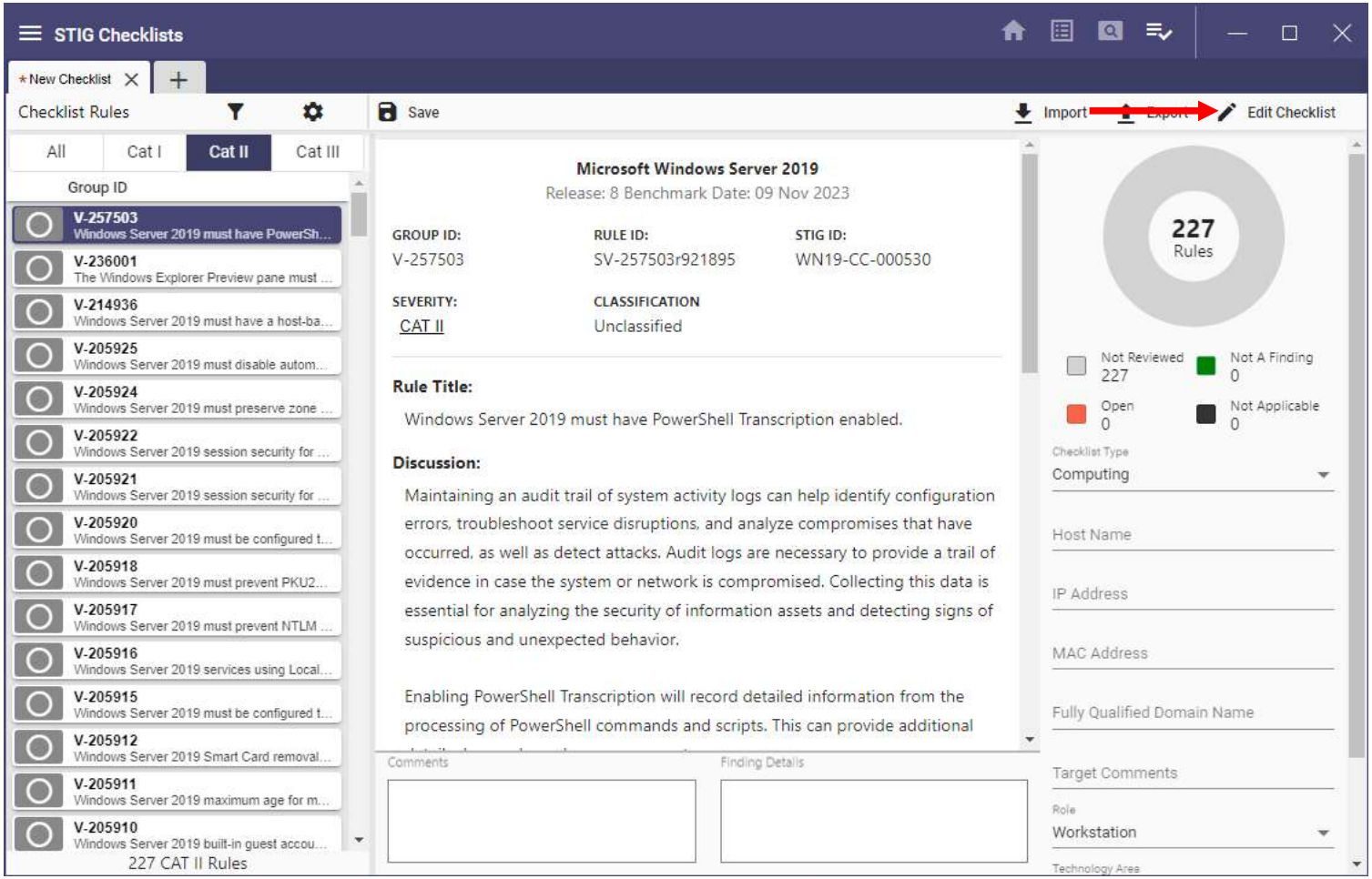
You will now see a checklist for all rules that were populated. You will note there are 274 rules for this particular checklist.



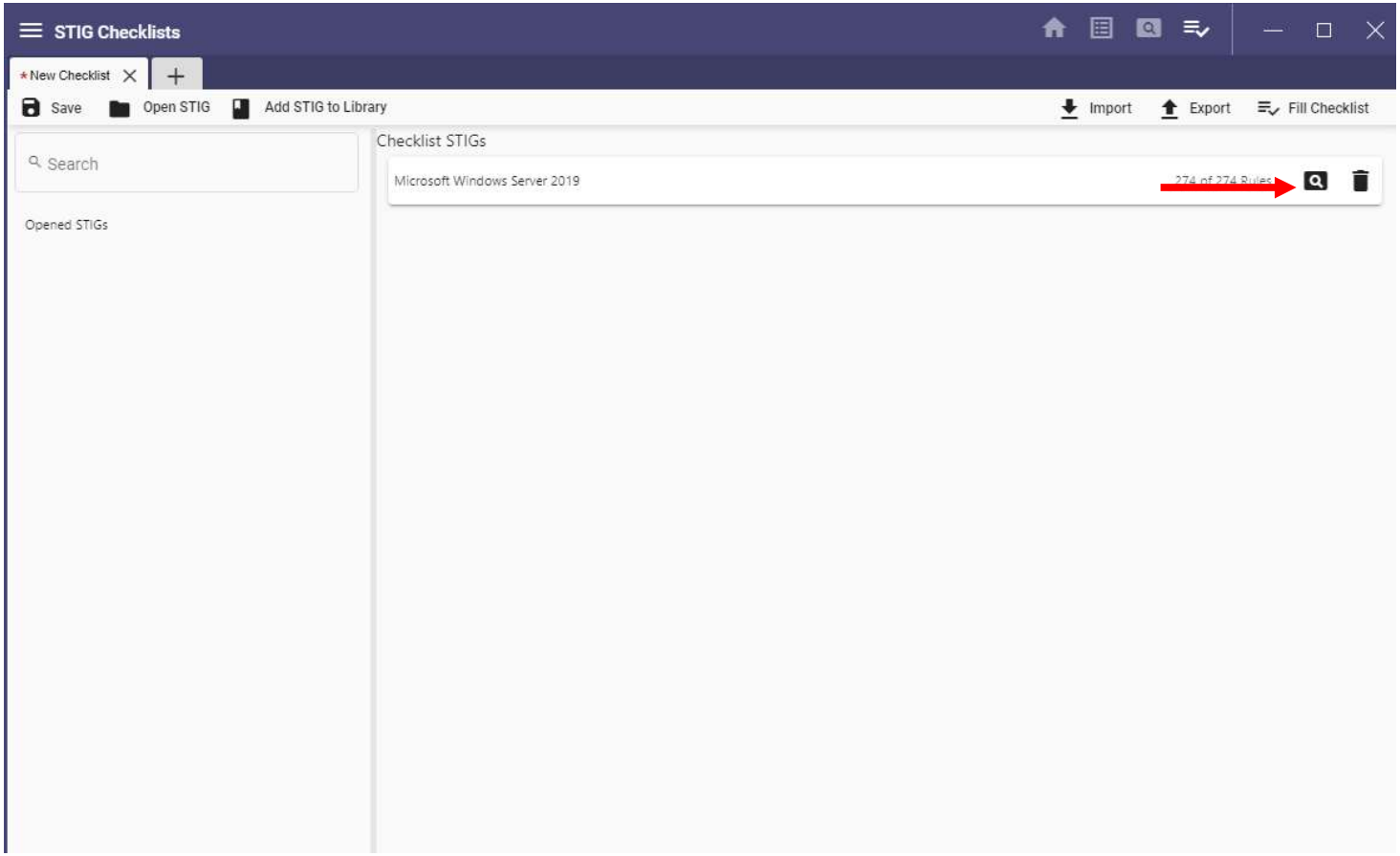
You can also filter by a variety of options or select severity category. Notice we only have 33/274 CAT I STIGS



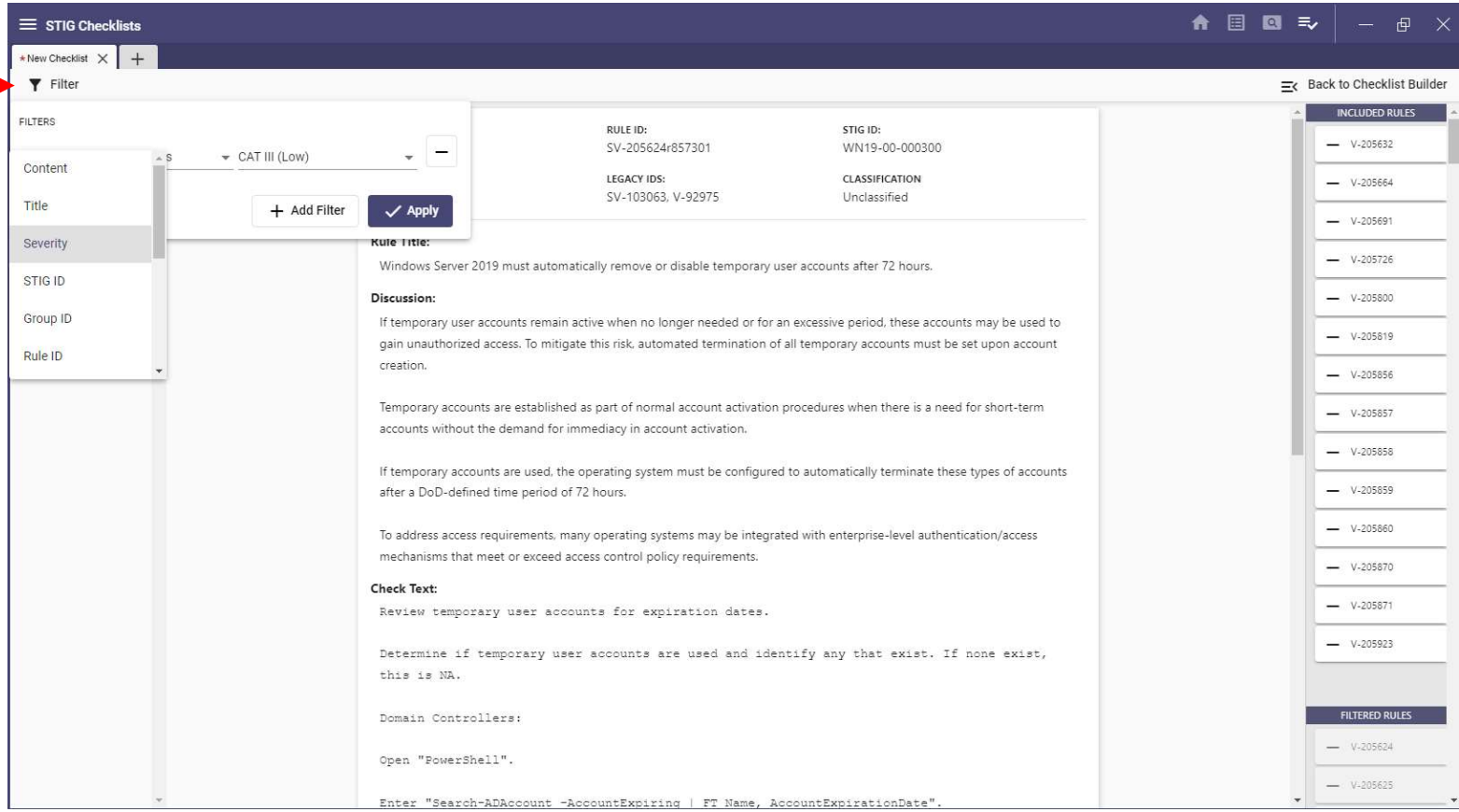
Another option you can do is select Edit Checklist



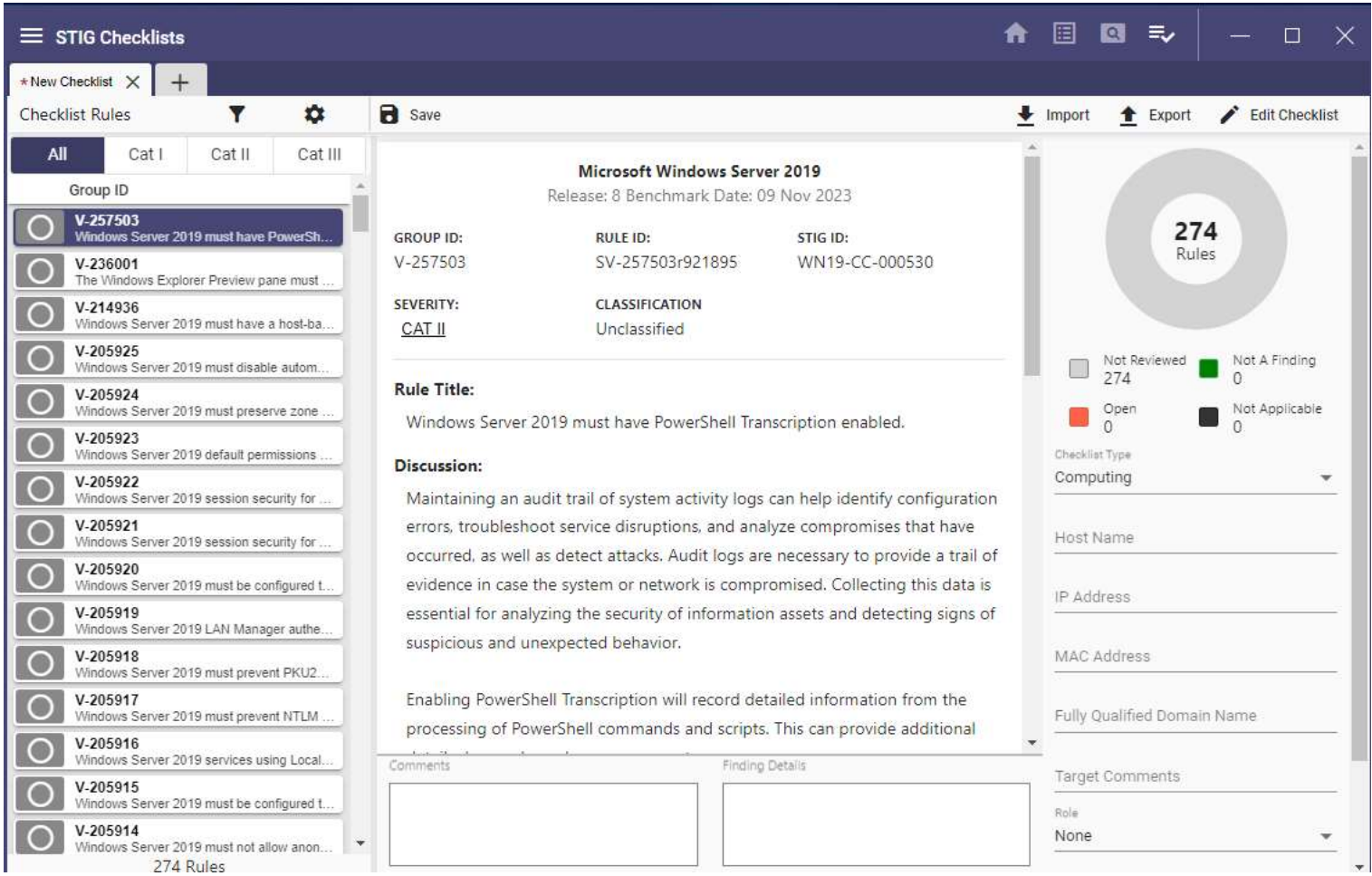
This will then enable you to select the STIG checklist and select magnifying glass to add/remove individual rules



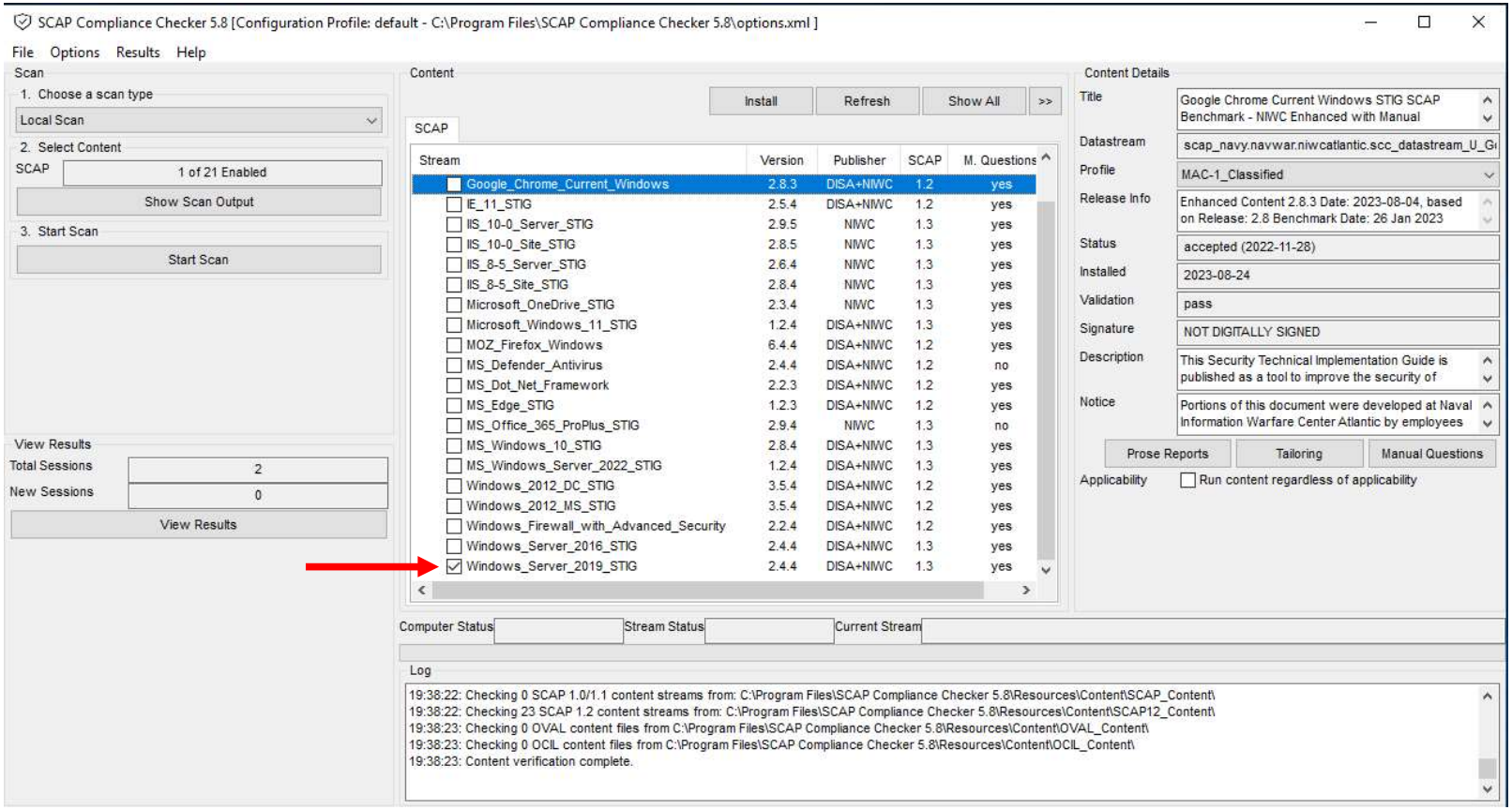
Here I opted to filter by severity but there are many more options



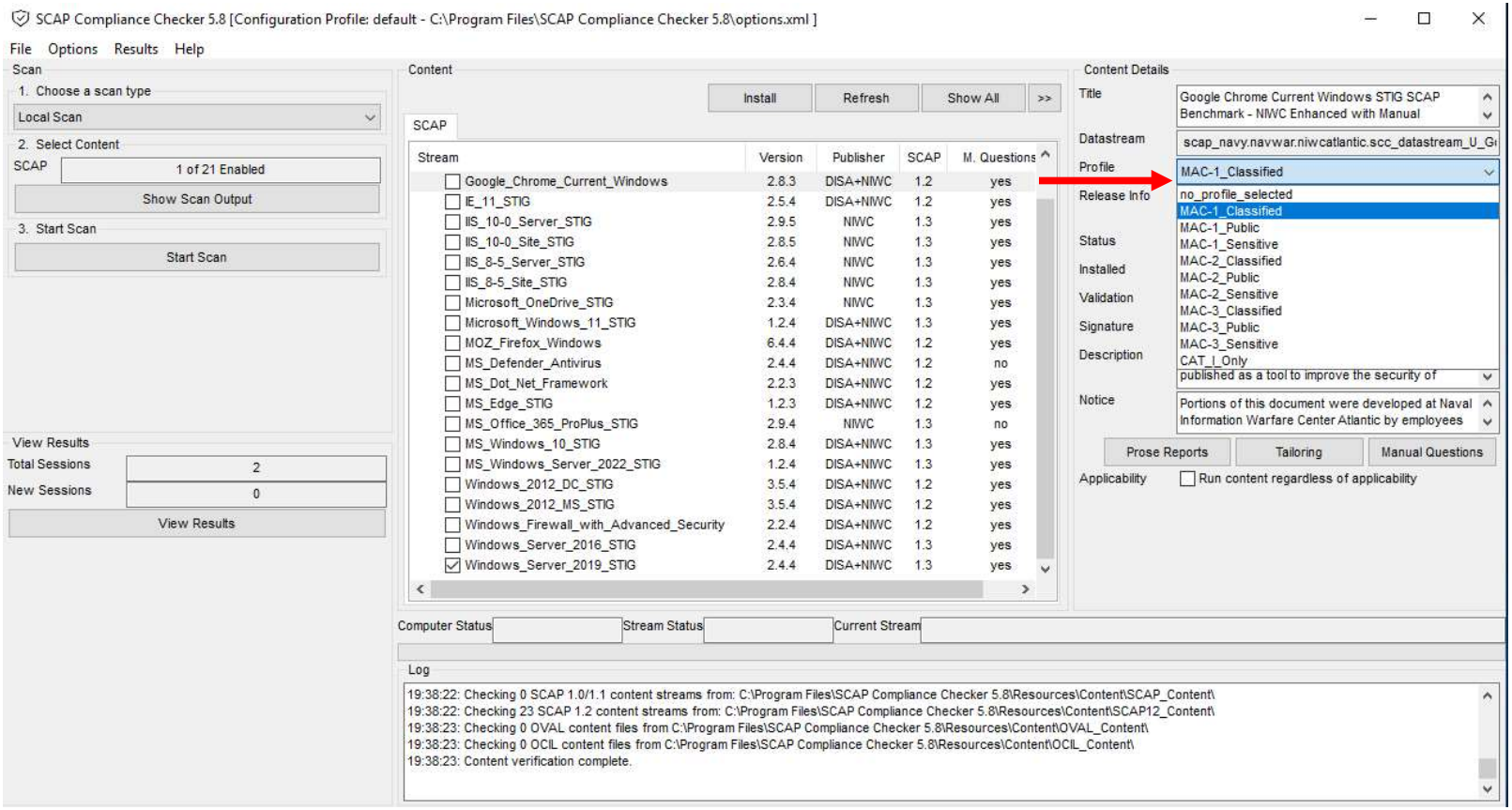
For the purpose of this we are going to use the initial checklist for all 274 rules



Next Lets open SCAP and once loaded select the matching STIG that you pulled up in STIG Viewer.

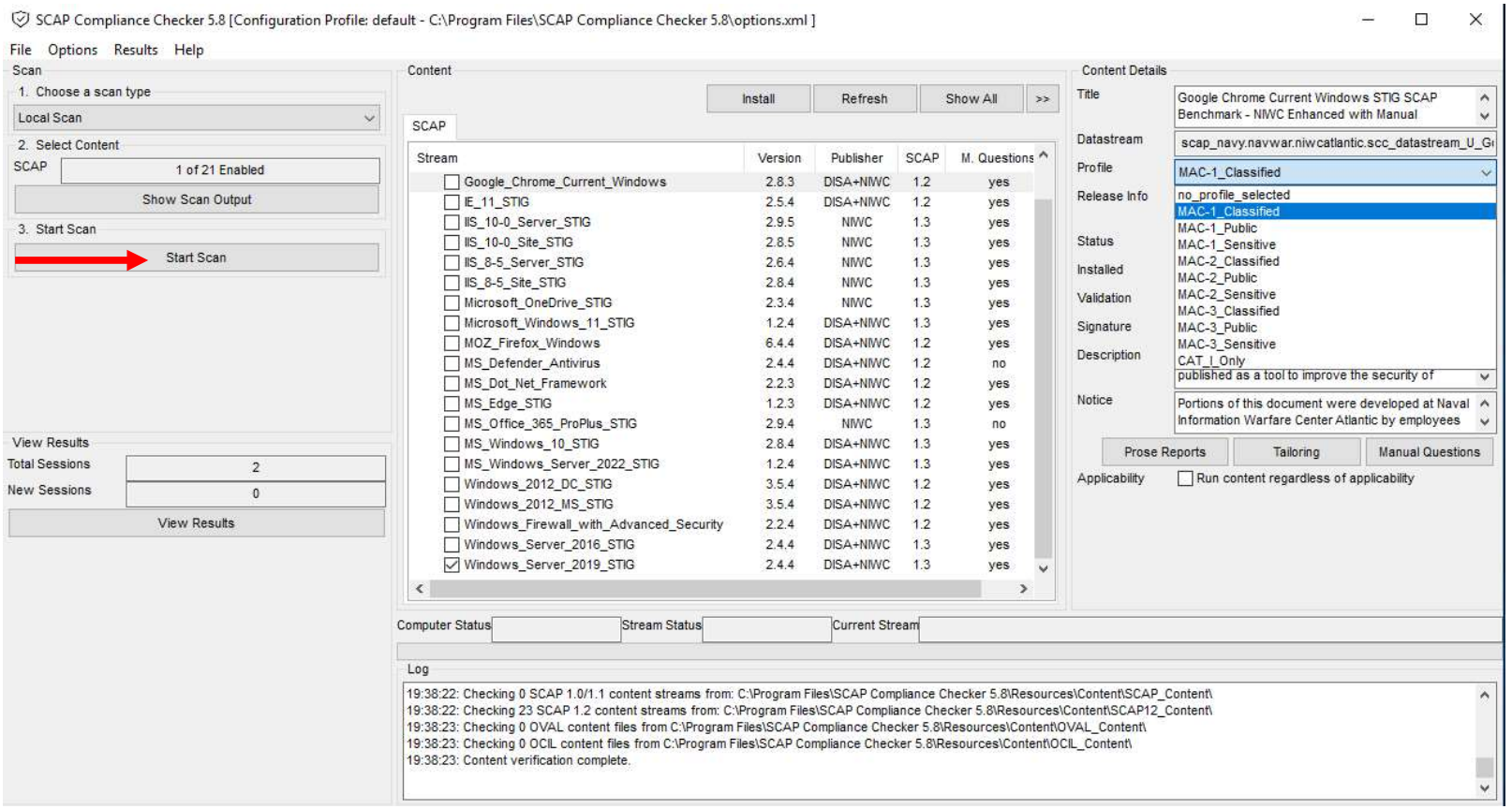


Notice on the right hand side we have MAC-1 but there are numerous options.

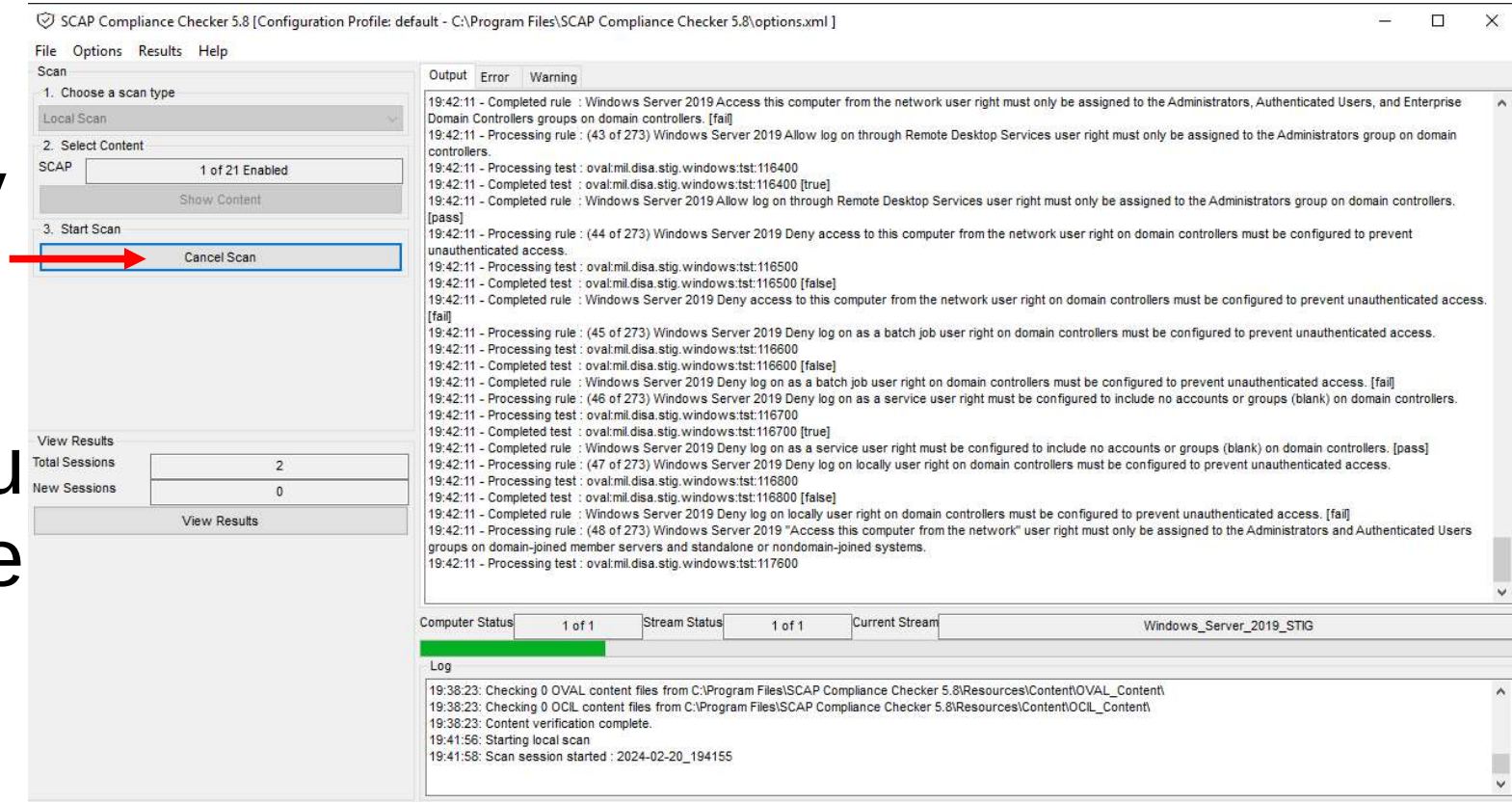


Learn more about Mission Assurance Category (MAC) in the United States Department of Defense 8500-series of policies

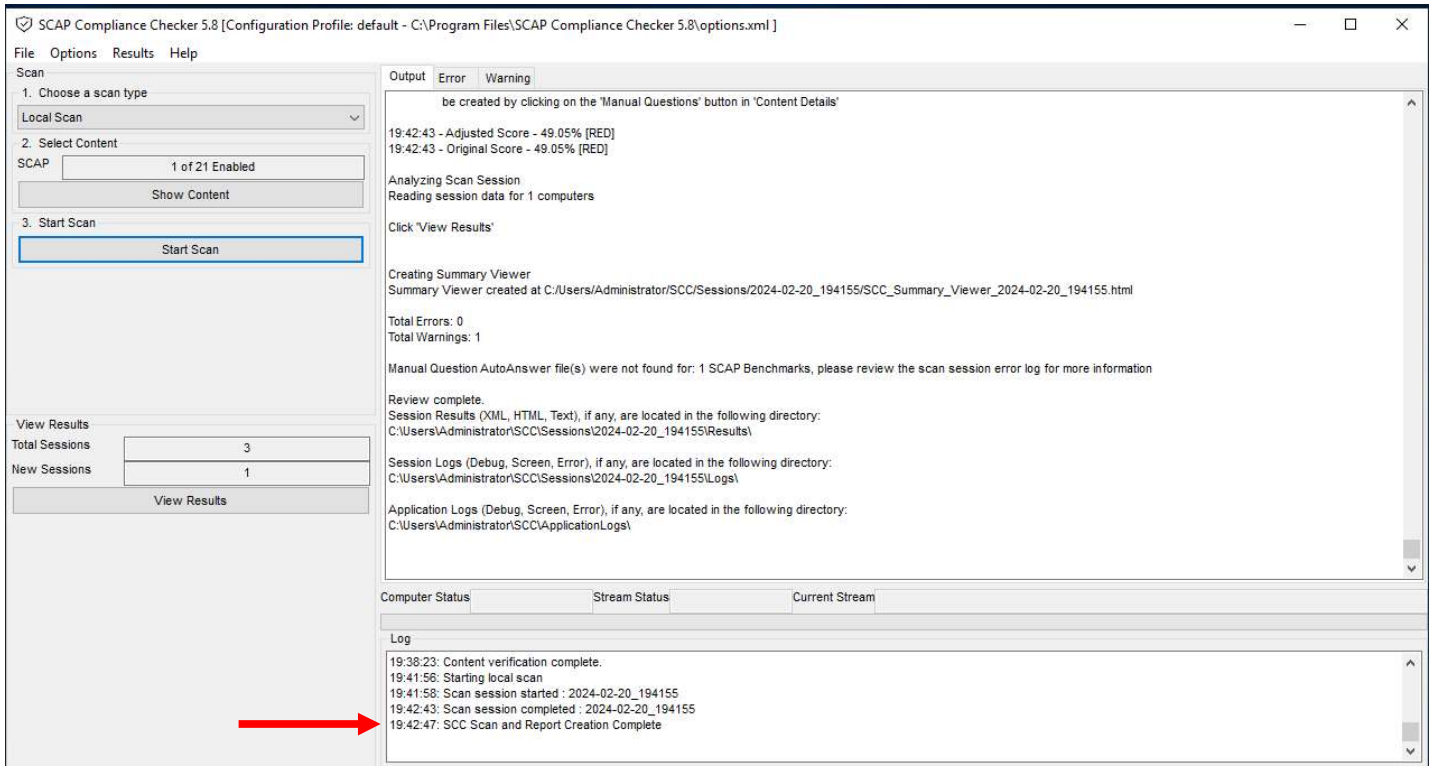
Once everything is set we then start scan



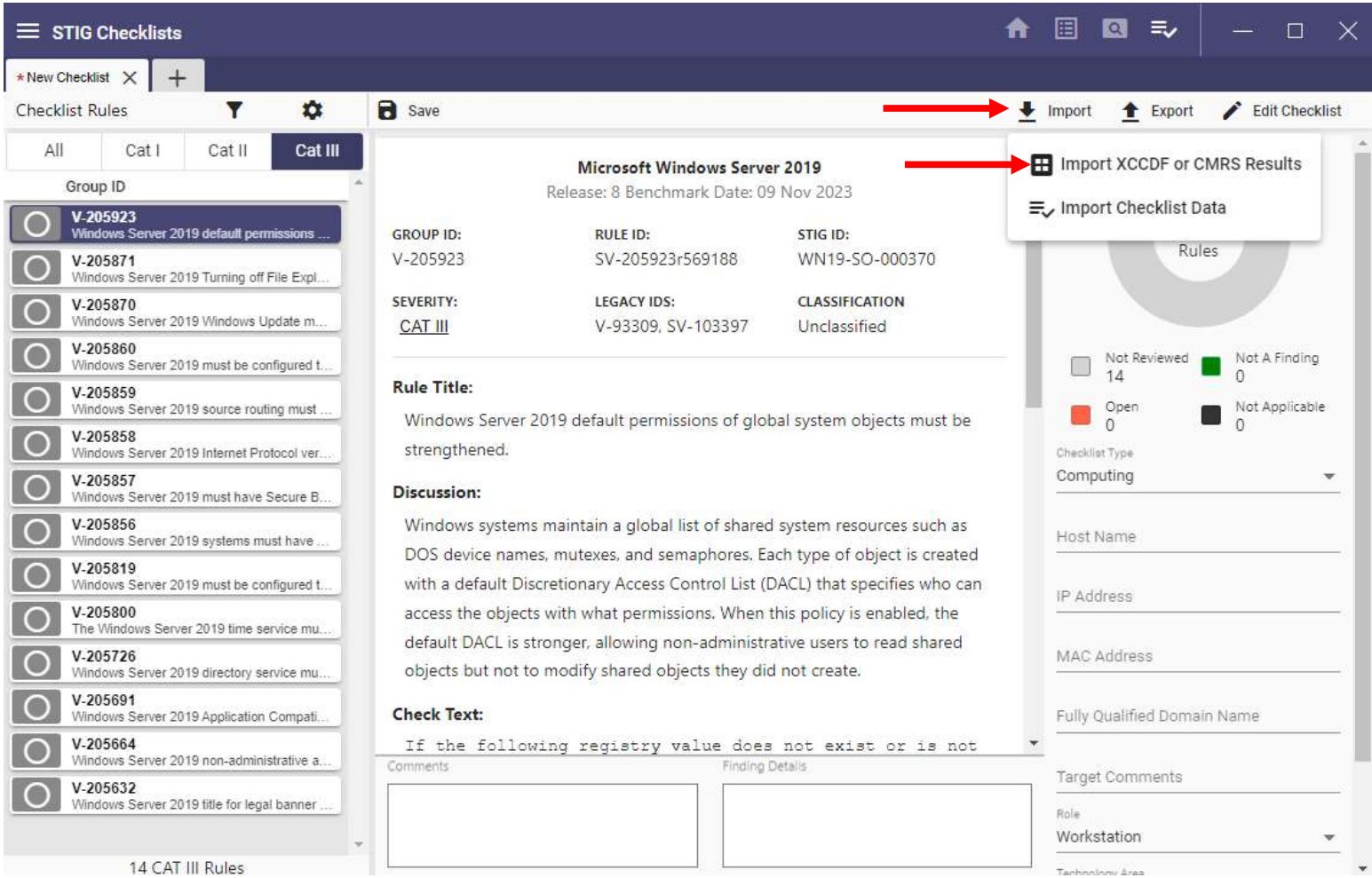
Time will vary here and depending if necessary you can cancel the



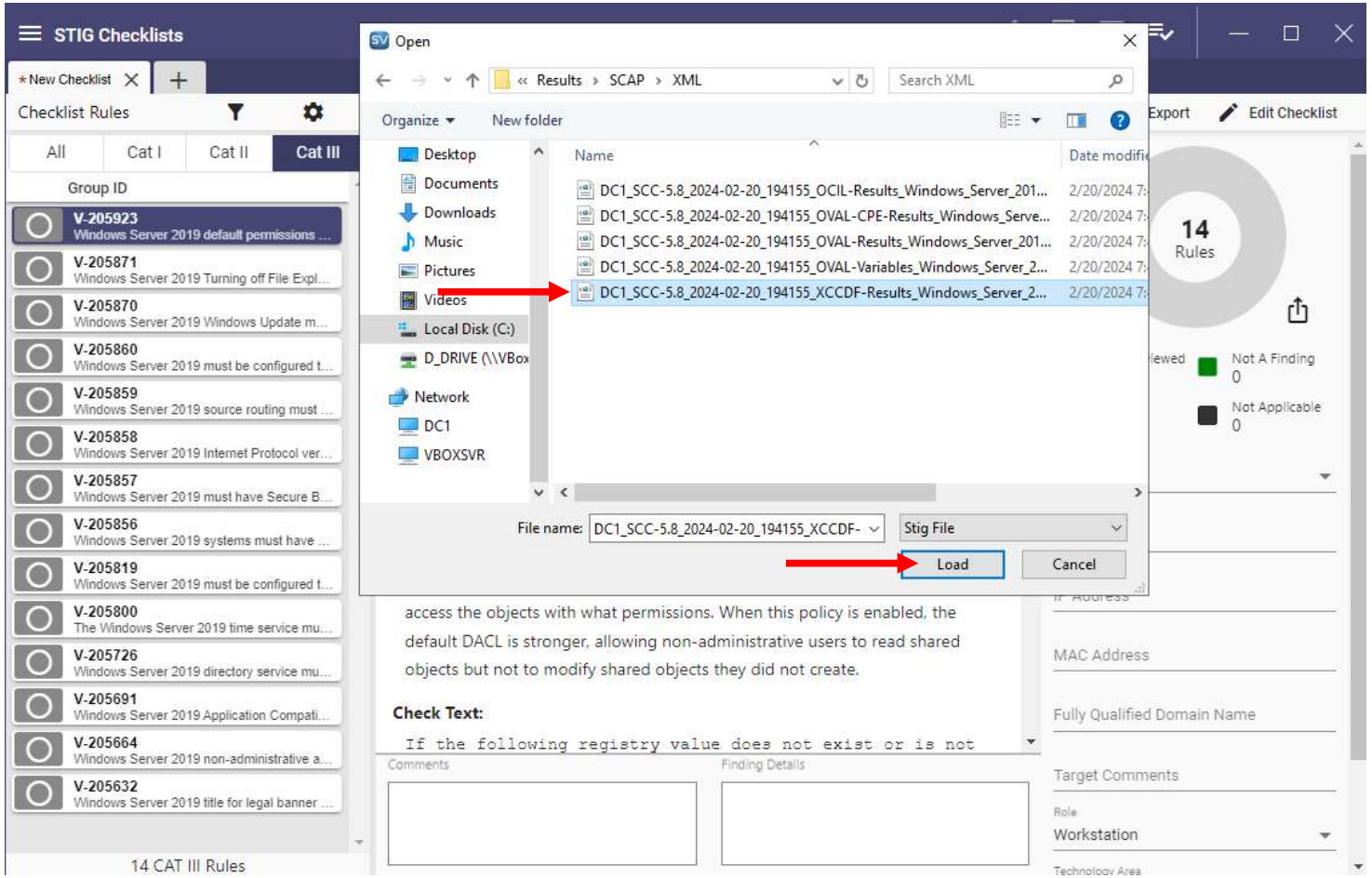
Once complete it will create multiple log files but for this we want the XCCDF.



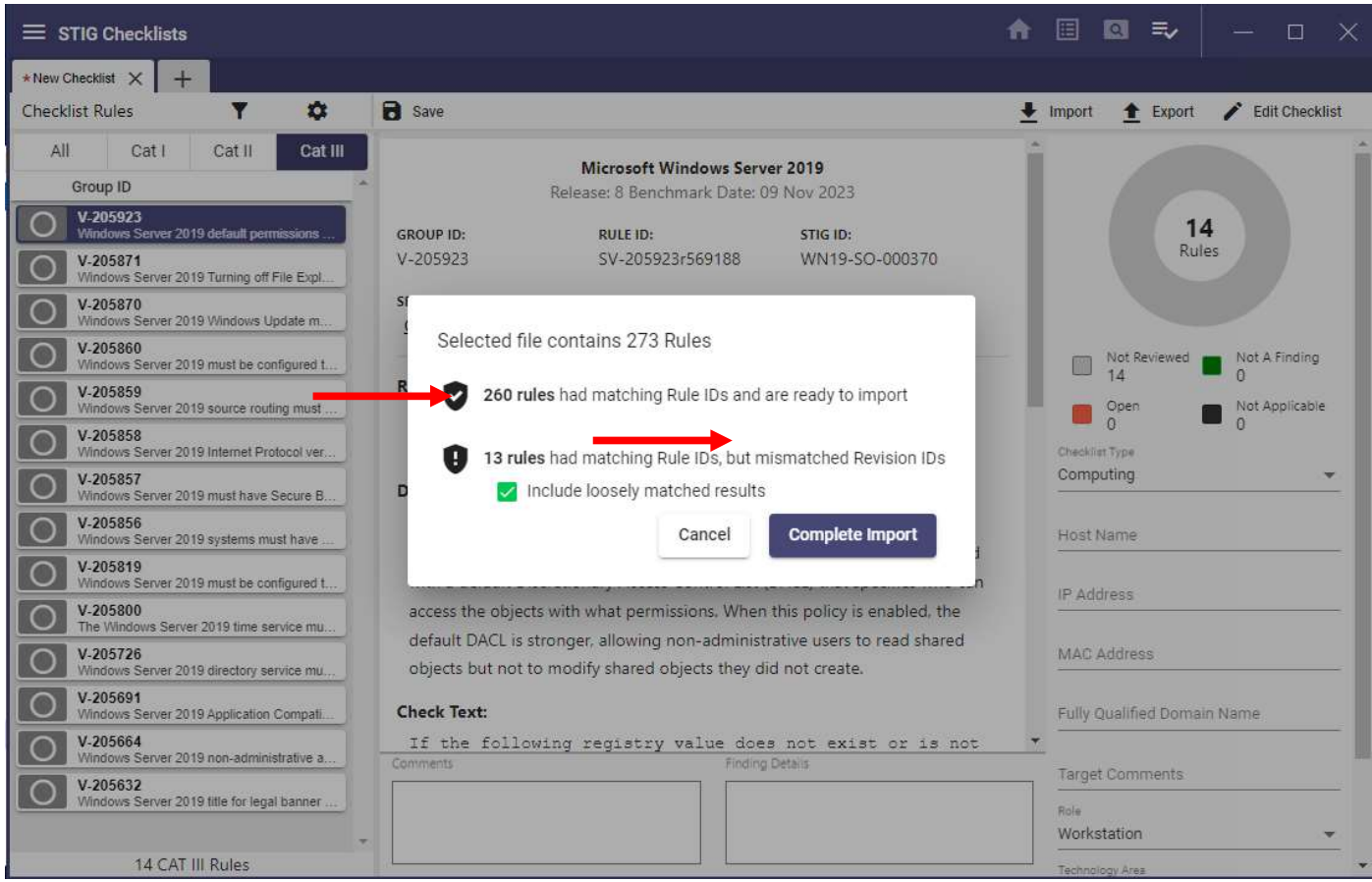
We will now go back into STIG Viewer and select Import and we want the XCCDF



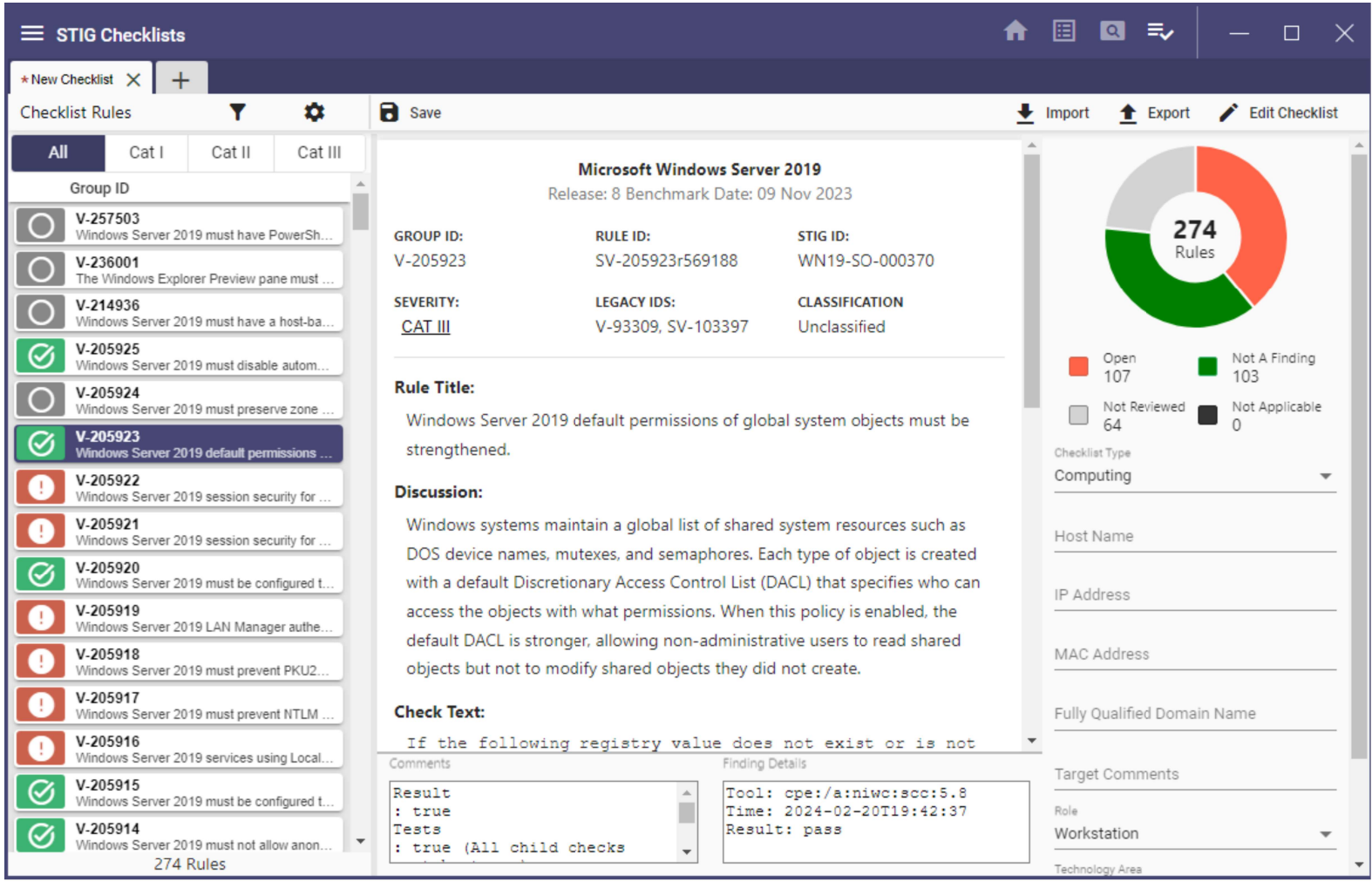
Navigate to the XCCDF log, select, and load



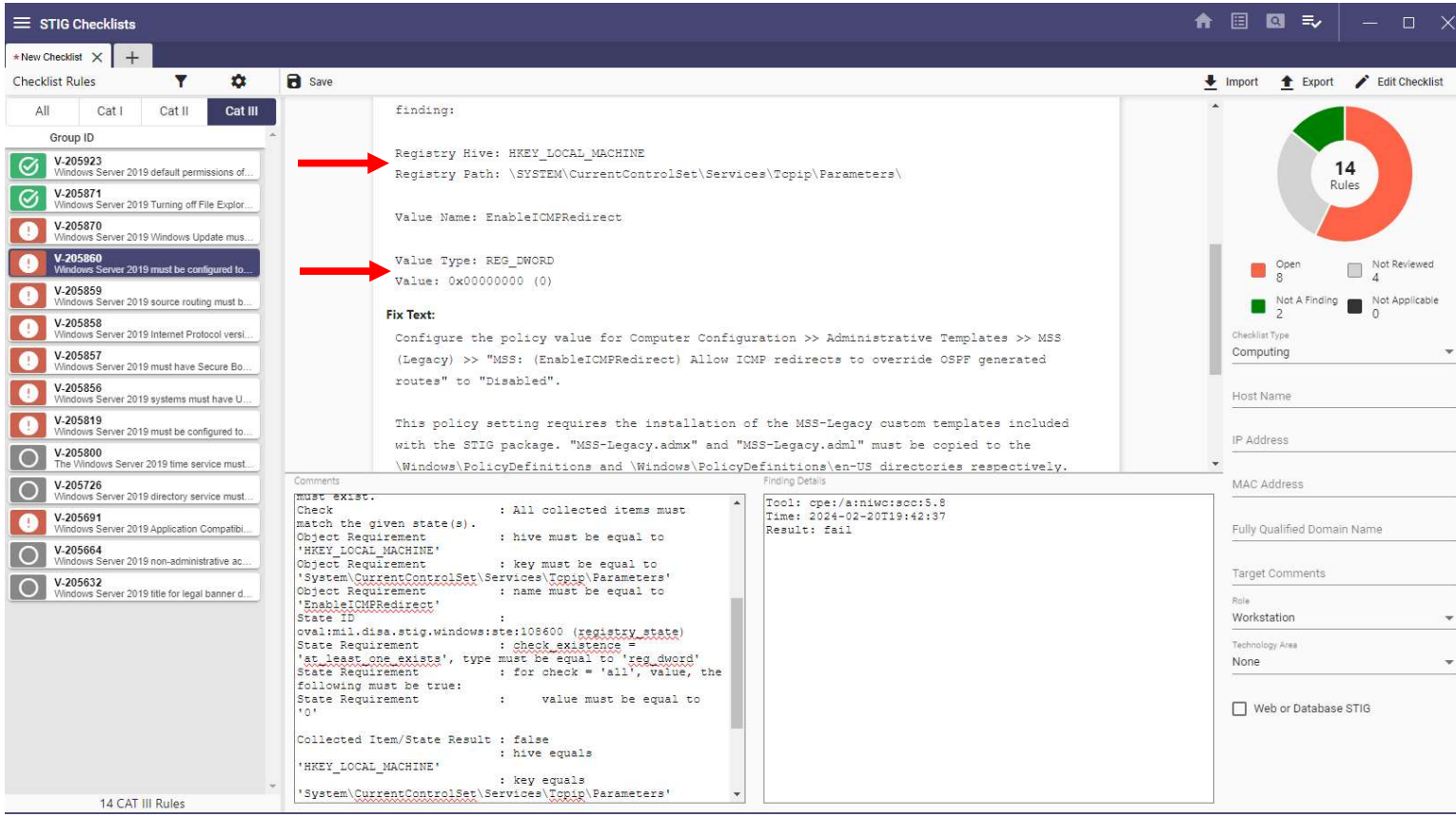
Notice it didn't match every rule exactly. Earlier I did go through and notice a few that had Revision ID discrepencies. I am going to include those and then Complete Import



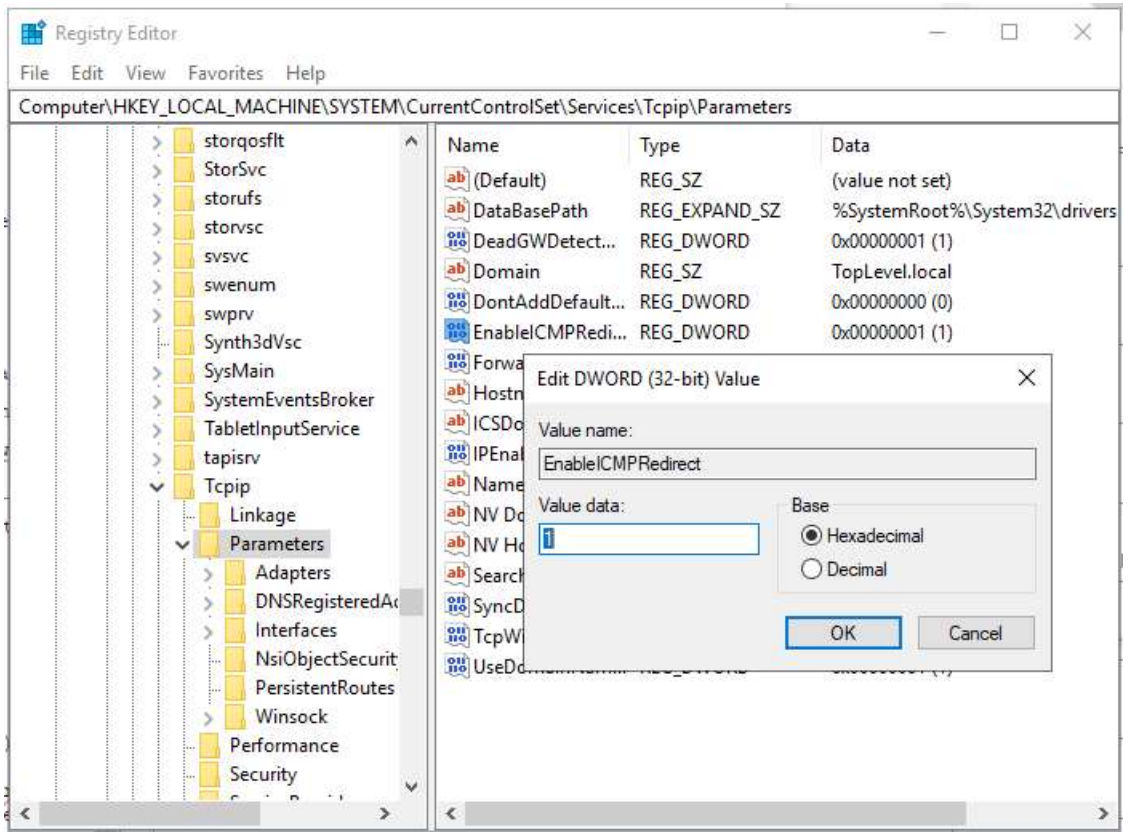
You will now see in a short time SCAP has provided you a solid head start on your way to hardening the system.



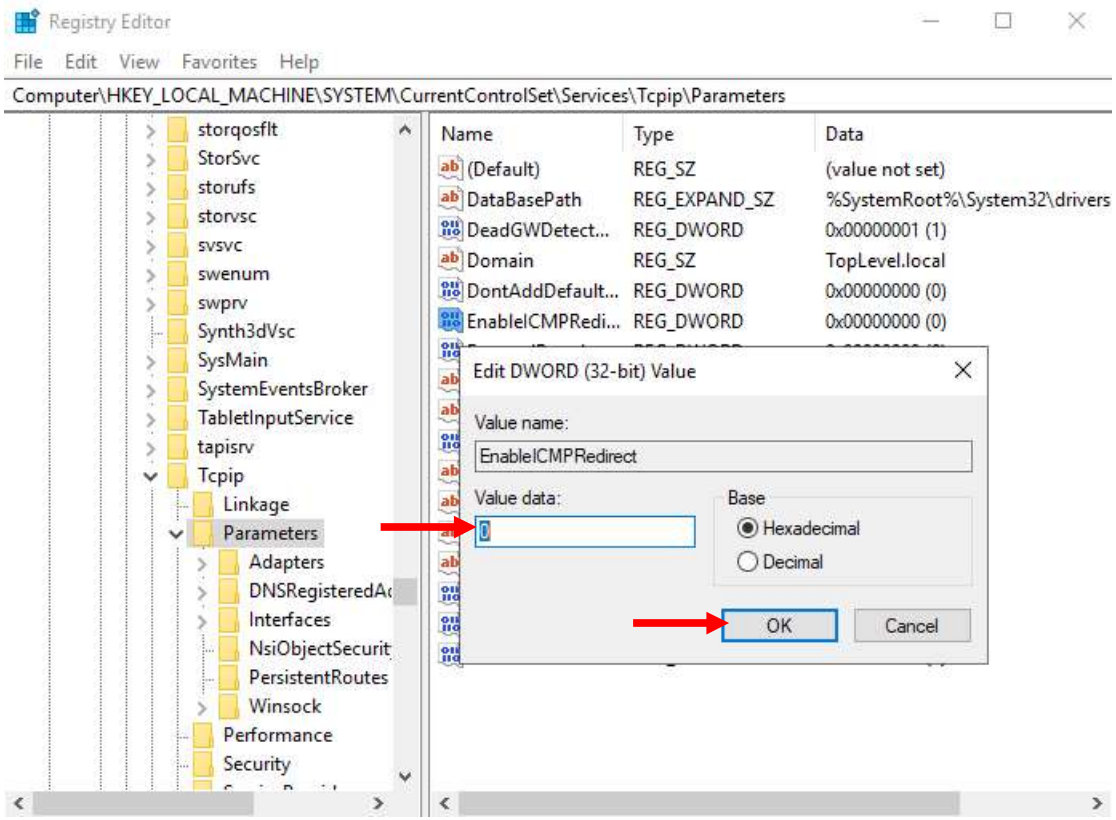
We now need to start resolving what was not reviewed or left open. Lets resolve the one selected. It tells us the registry path and setting



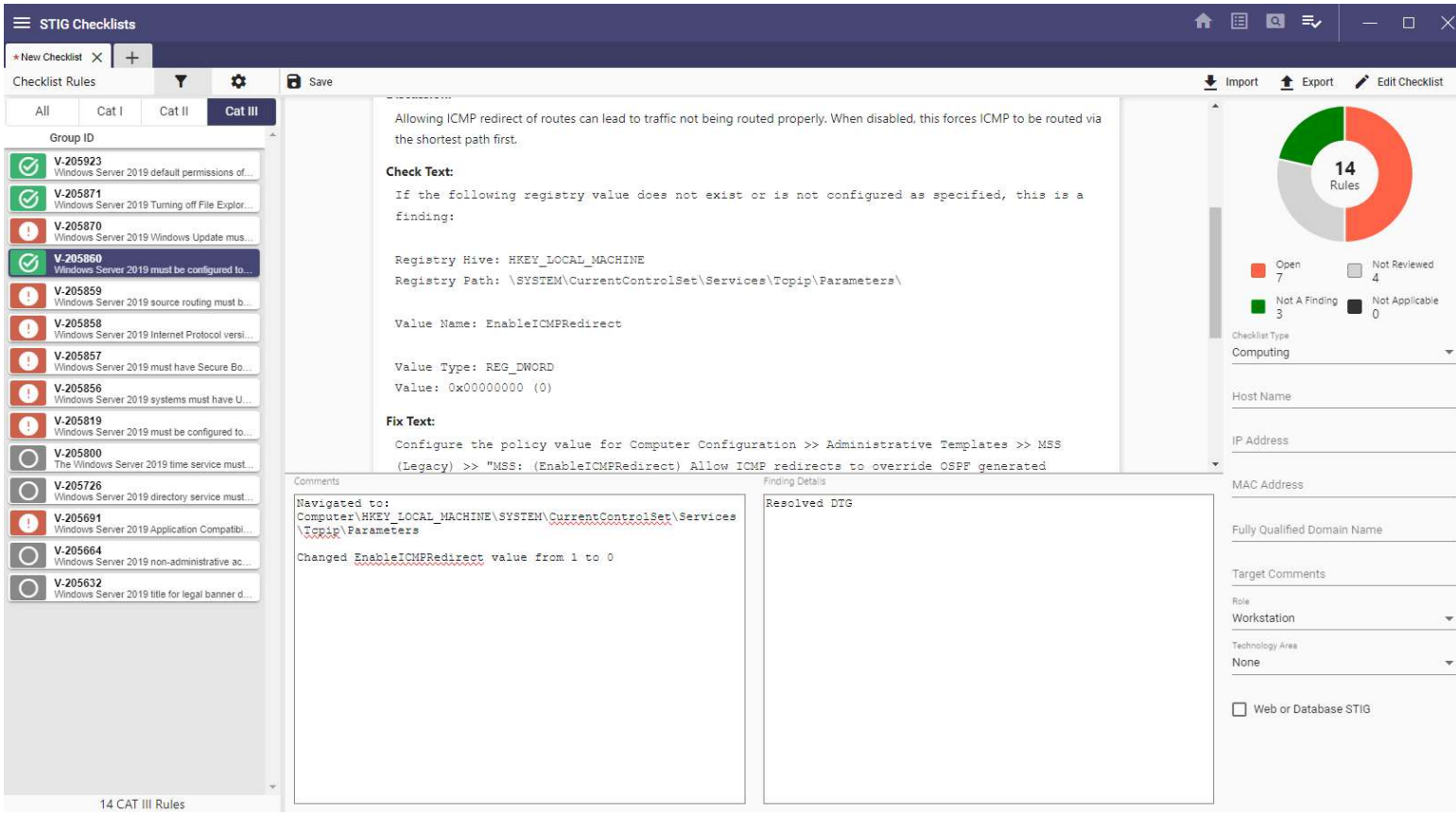
Next navigate to the path it told us and you will notice the value should be 0 but is a 1.



Simply change the value to “0” as directed and select OK



Lets input a comment and Finding Details along noting the resolution and DTG and finally change the rule to green as it is now not a finding.



This was done on an unregistered version of 2019 server on a personal VM. Due to this there is going to be a portion of STIG's missed or not applicable.

Also, SCAP is helpful but not a one stop shop. You will still need to go through and manually review, resolve, comment, etc.

Once done you will want to leverage ACAS and do an IA scan checking for any additional findings that need resolution.