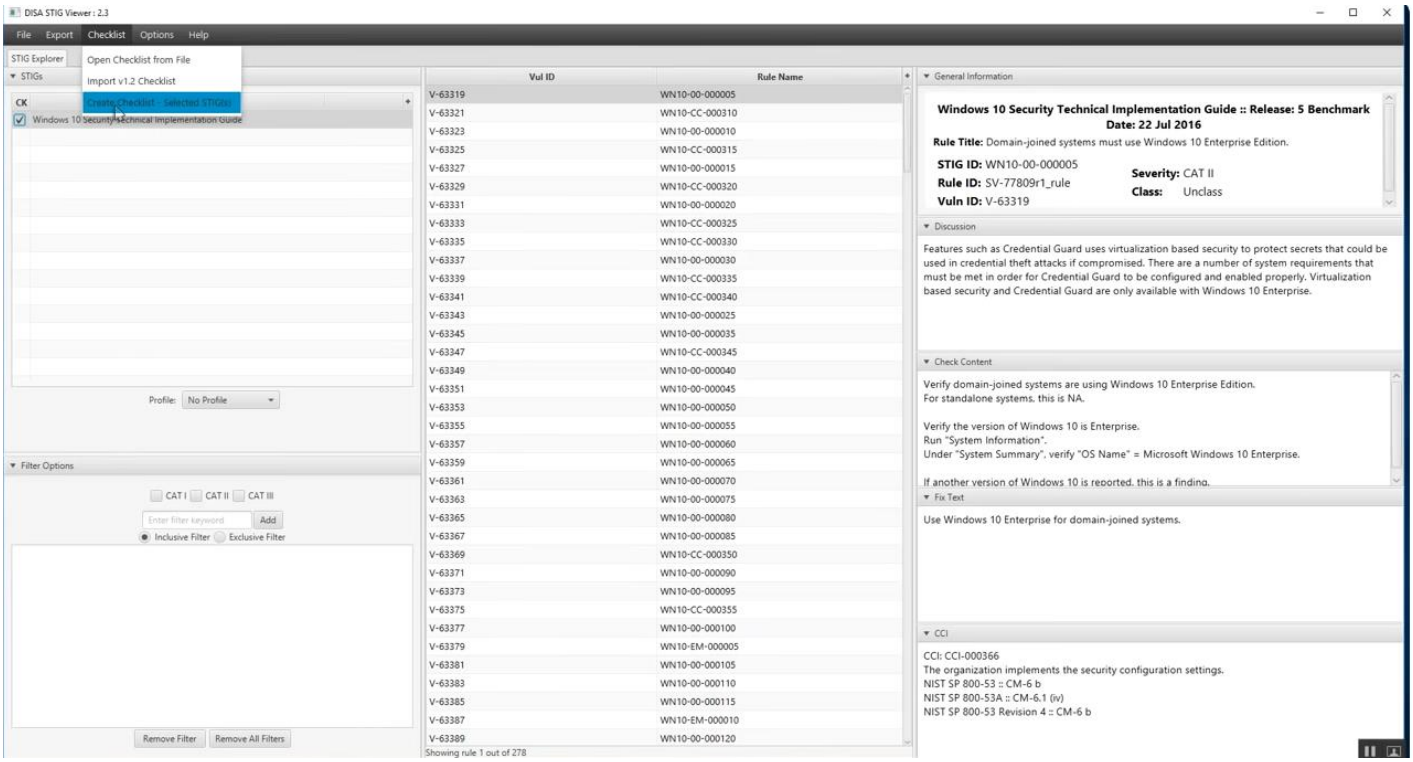
SCAP **stands for Security Content Automation Protocol.** SCAP scans compare the system you are scanning to a baseline (benchmark) which are open security standards of security to find compliance or non-compliance of system.

1. **National Institute for Standards and Technology (NIST)** provides reference guidance across the federal government
2. **Federal Information Security Management Act (FISMA)** provides guidance for civilian agencies
3. **Defense Information Systems Agency (DISA)** provides another layer of requirements for (DoD) systems.

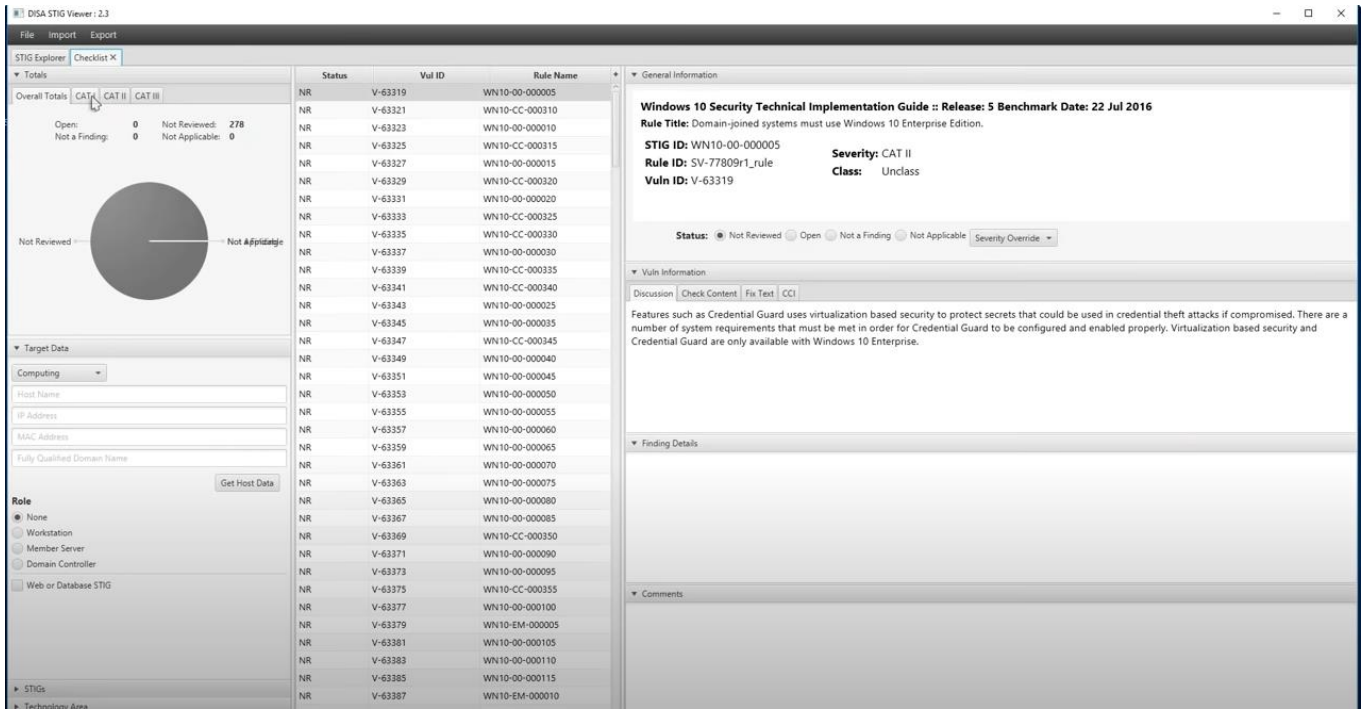
DoD must comply with the technical testing and hardening frameworks known by Security Technical Implementation Guide (**STIG**). According to DISA, STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack.

There are several common testing tools that implement STIGs. Some, like **Assured Compliance Assessment Solution** (**ACAS**), were developed by industry specifically for DISA

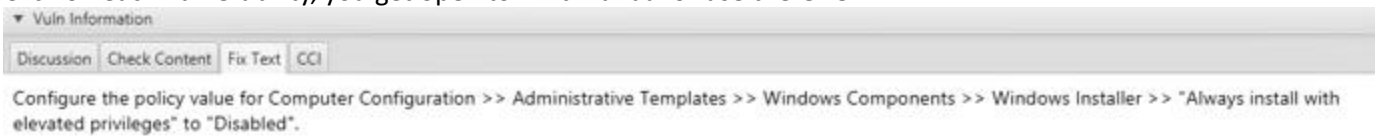
Load STIGViewer.jar >> File >> Import >> STIGS >> "e.g.Windows_10_STIGS" >> …manual_STIGS" >> Open
Check Mark the STIGS on the right Window Under STIGS window
Click on Checklist Tab, choose Create Checklist – Selected STIGs

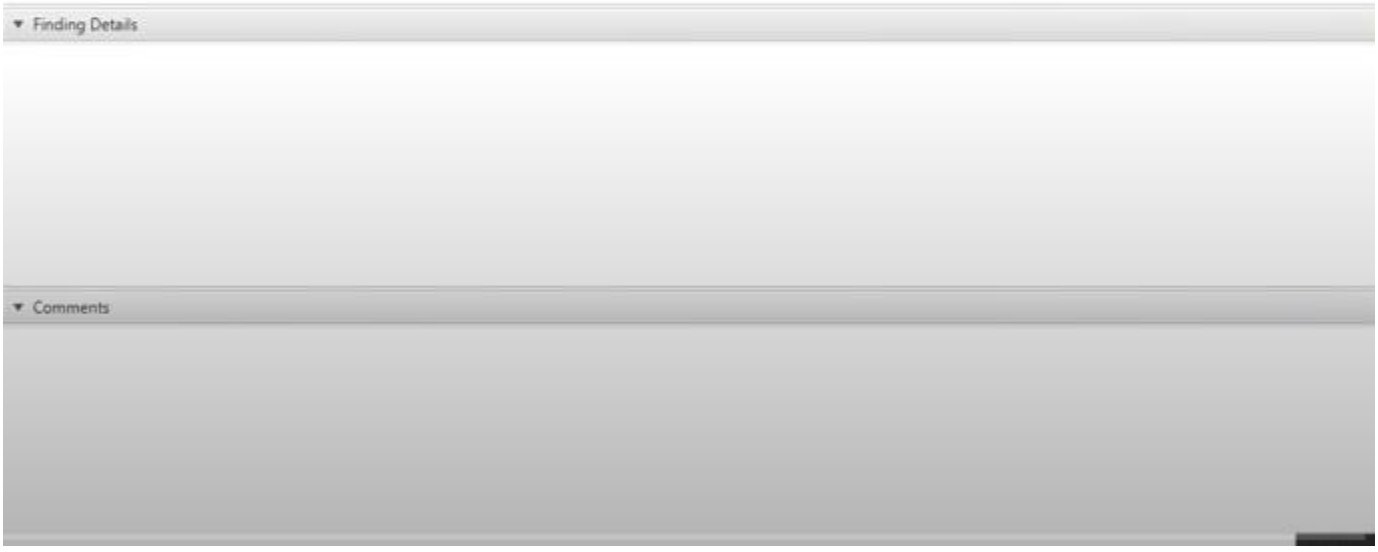


Now we have the overall non remediated vulnerabilities

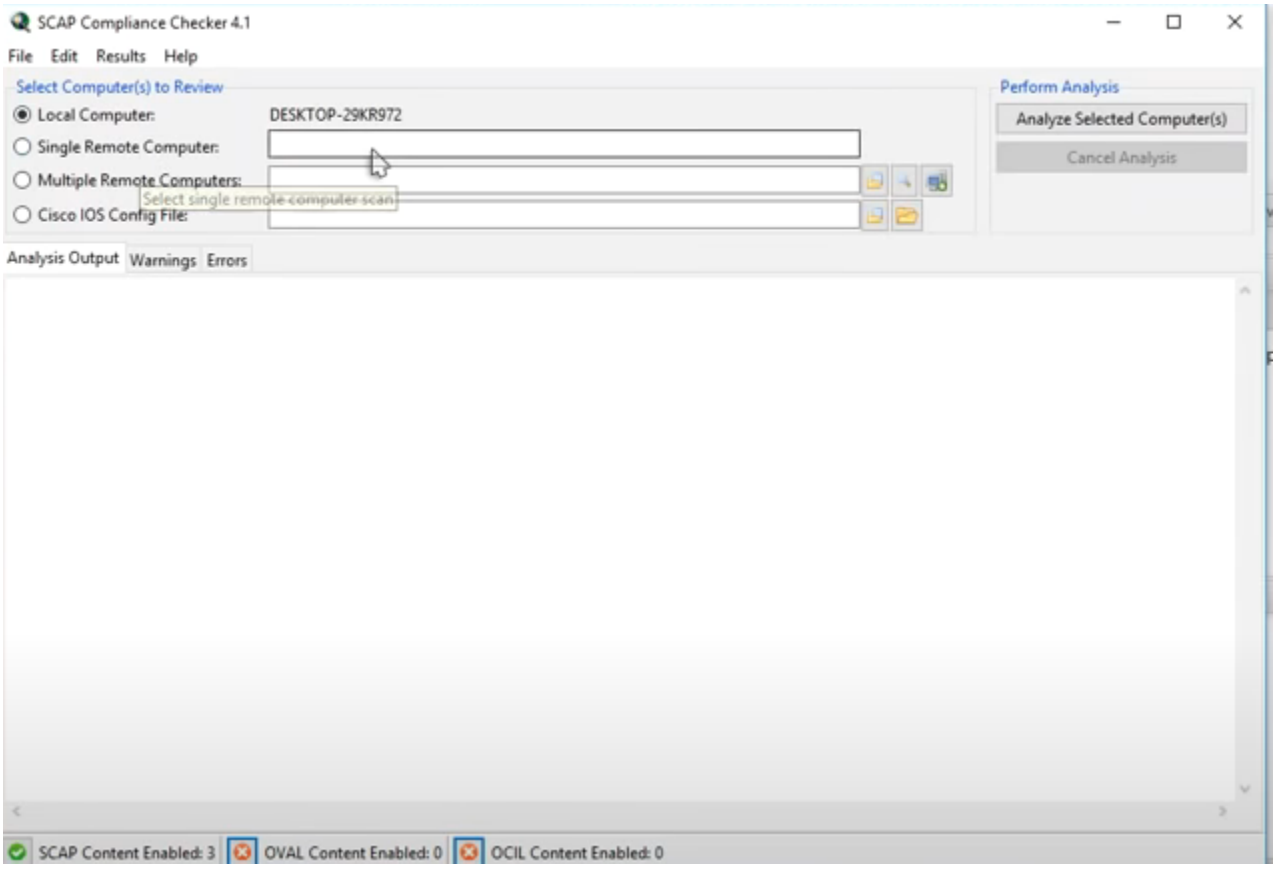


Click on each vulnerability, you get open to fix it manual or use the GPO



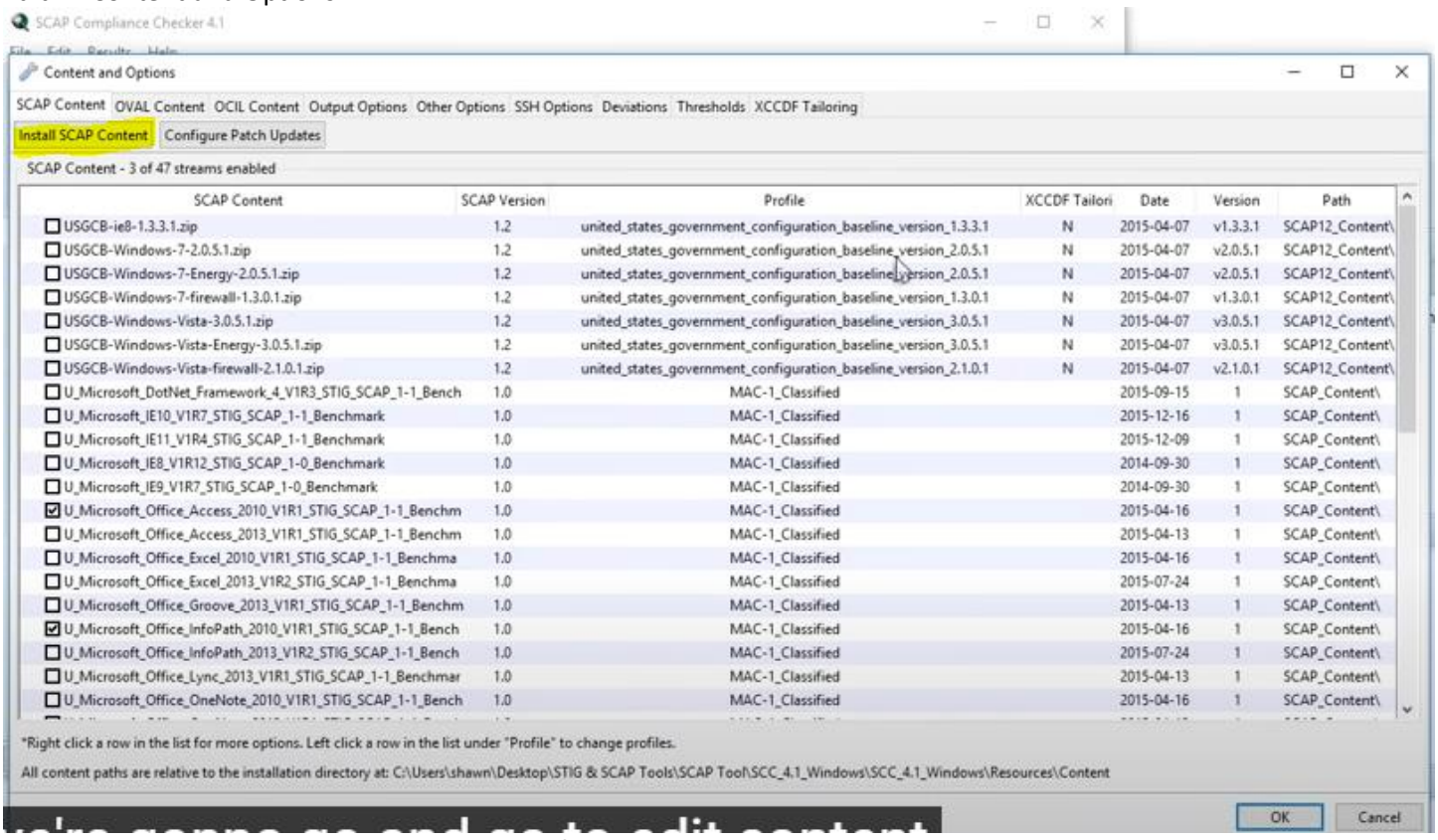


SCAP TOOL



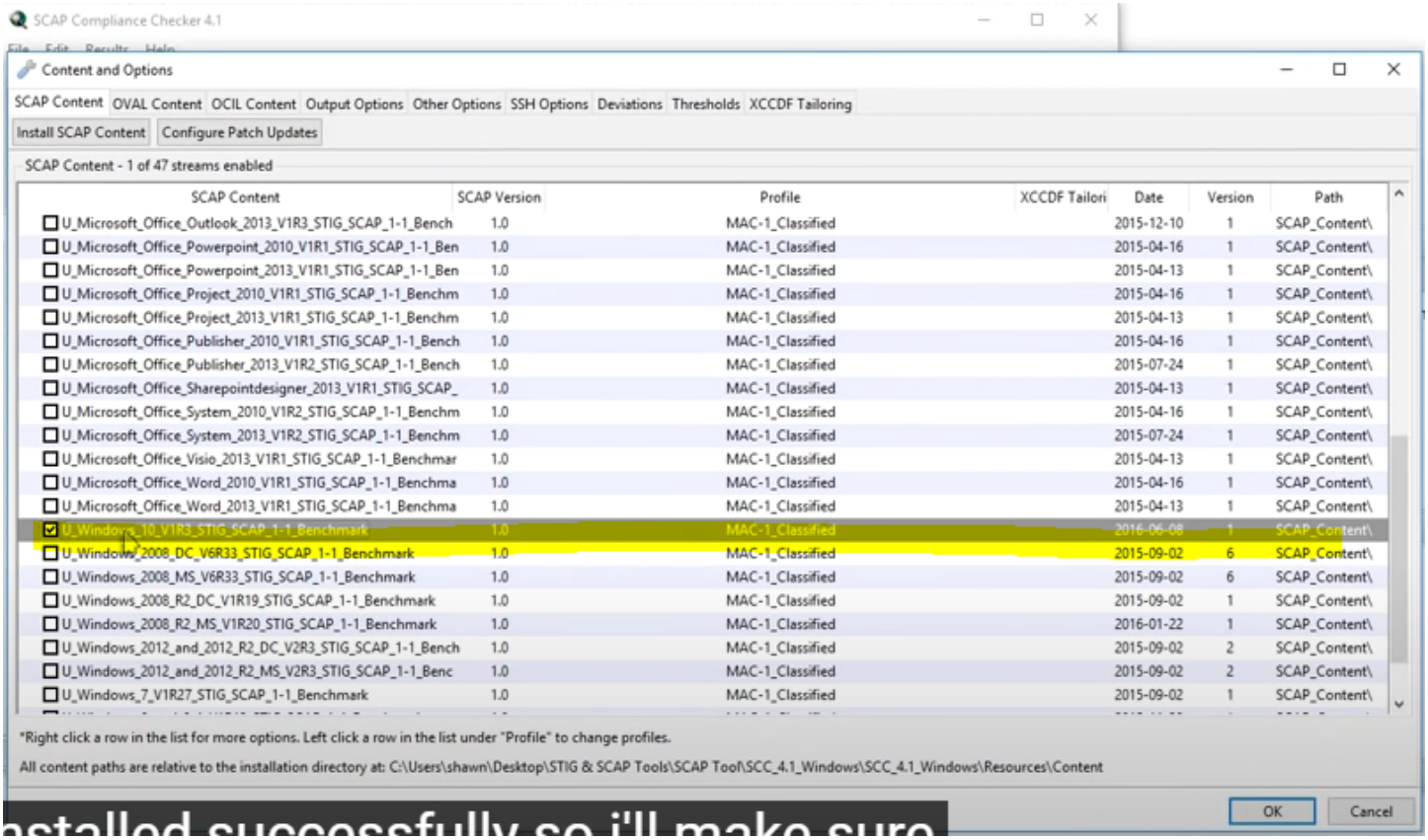
Hit the Analyze Selected Computer

Edit >> Content and Options



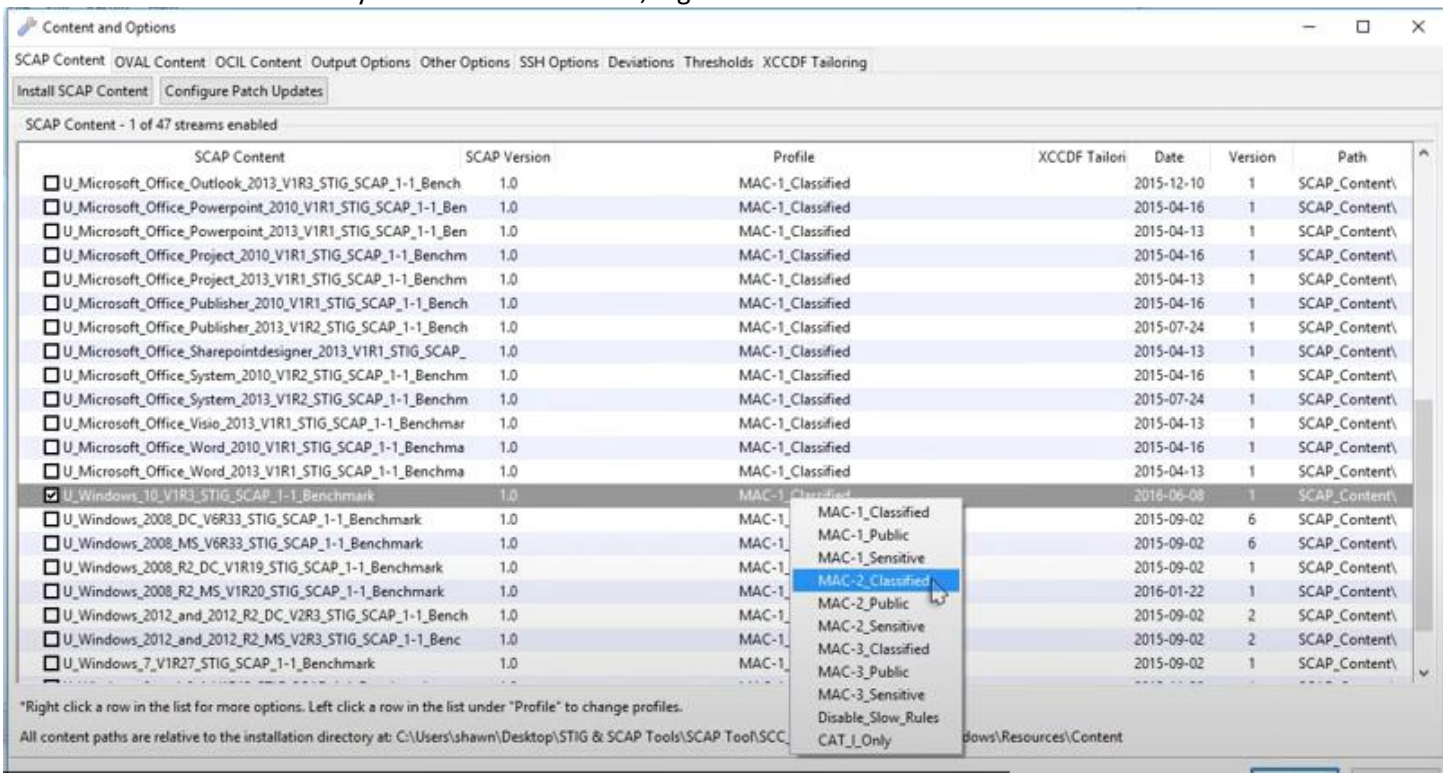
Click Install SCAP Content >> Go to Benchmark folder and get the windows_10_SCAP… >> Open

Once installed you selected

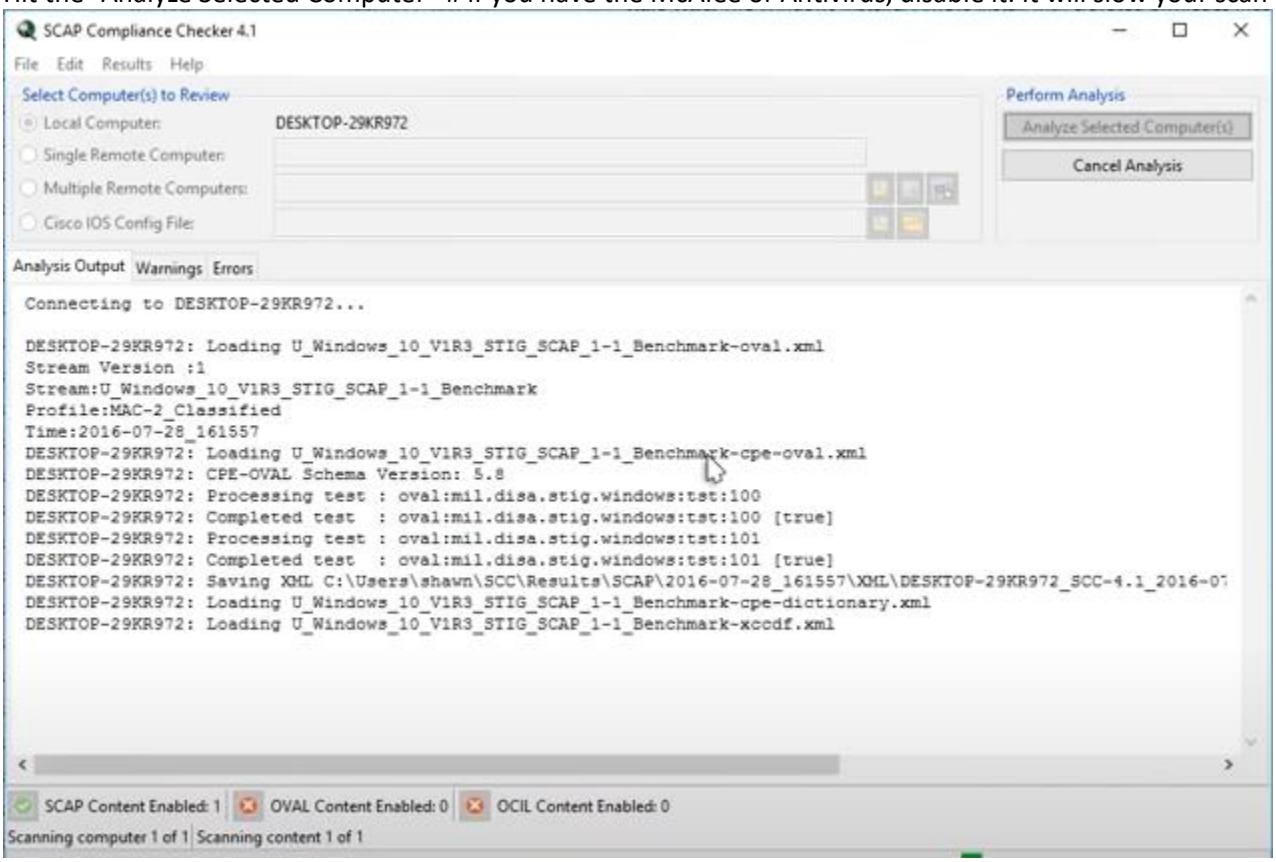


nstalled successfully so i'll make sure

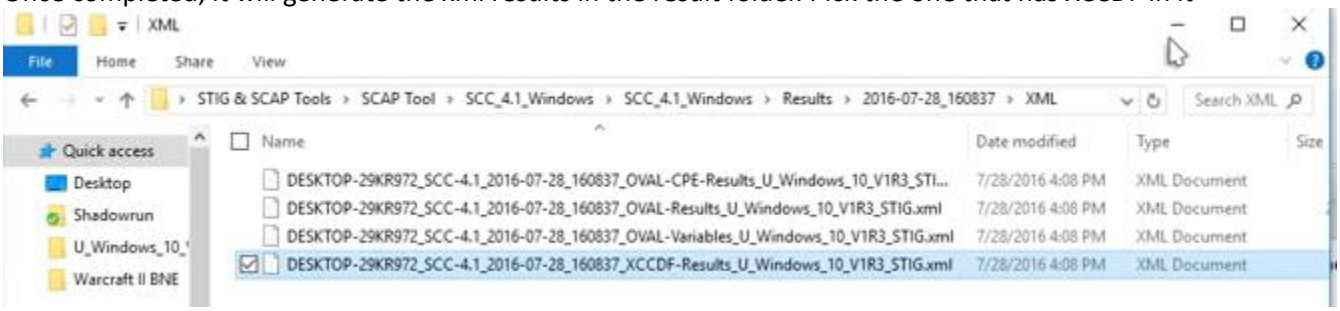
You can select to automatically fix which classification, Right Click on Profile area



Hit the “Analyze Selected Computer” # if you have the McAfee or Antivirus, disable it. It will slow your scan down.

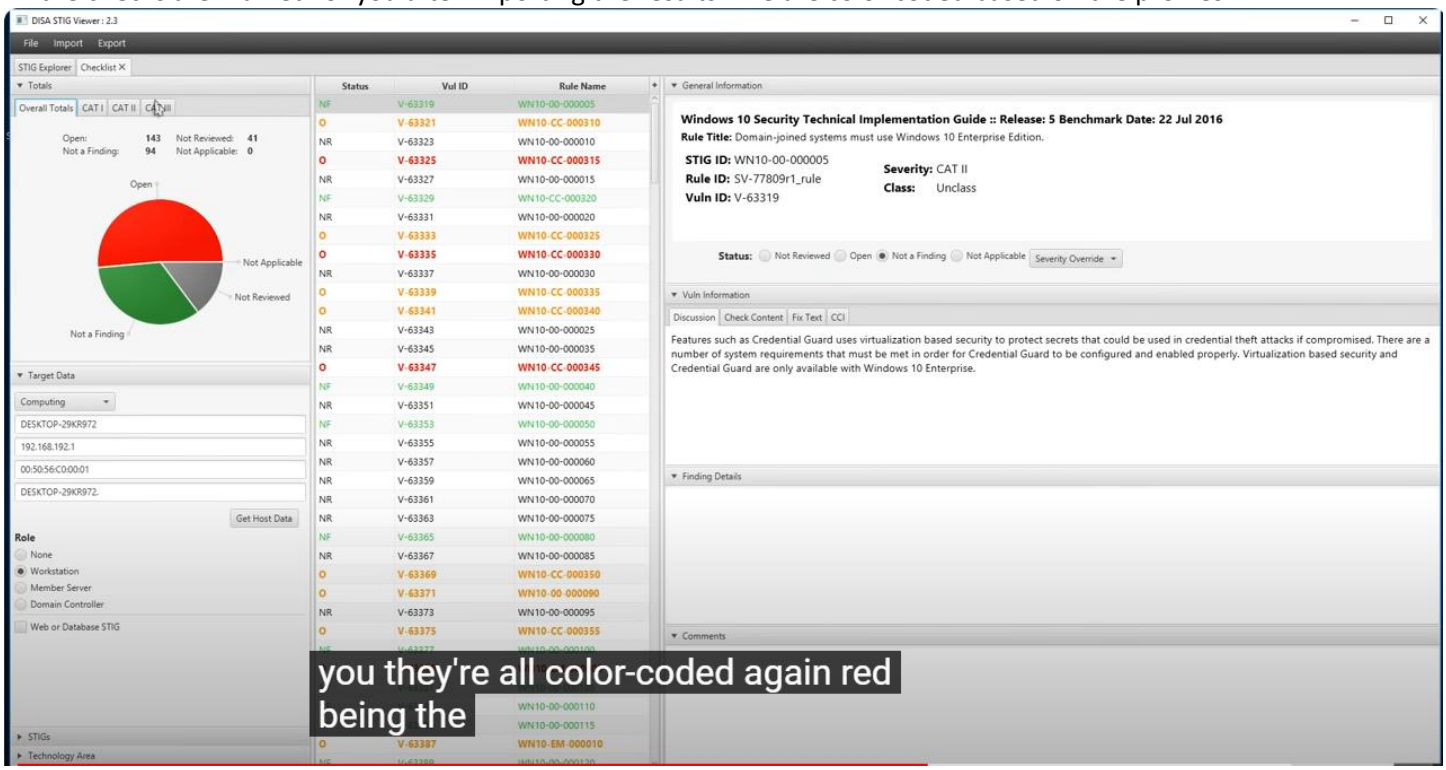


Once completed, it will generate the xml results in the result folder. Pick the one that has XCCDF in it

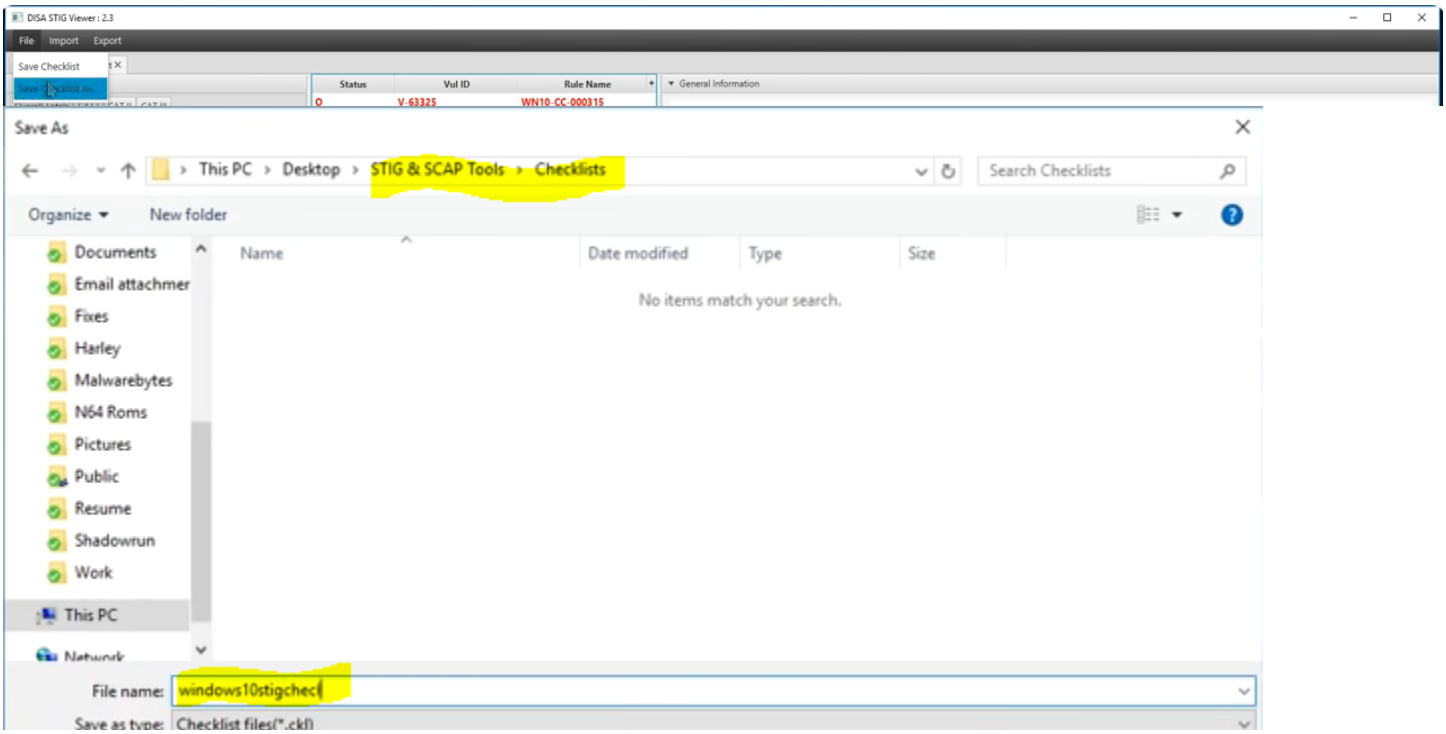


We go back to our STIG Viewer >> Import >> XCCDF Result File >

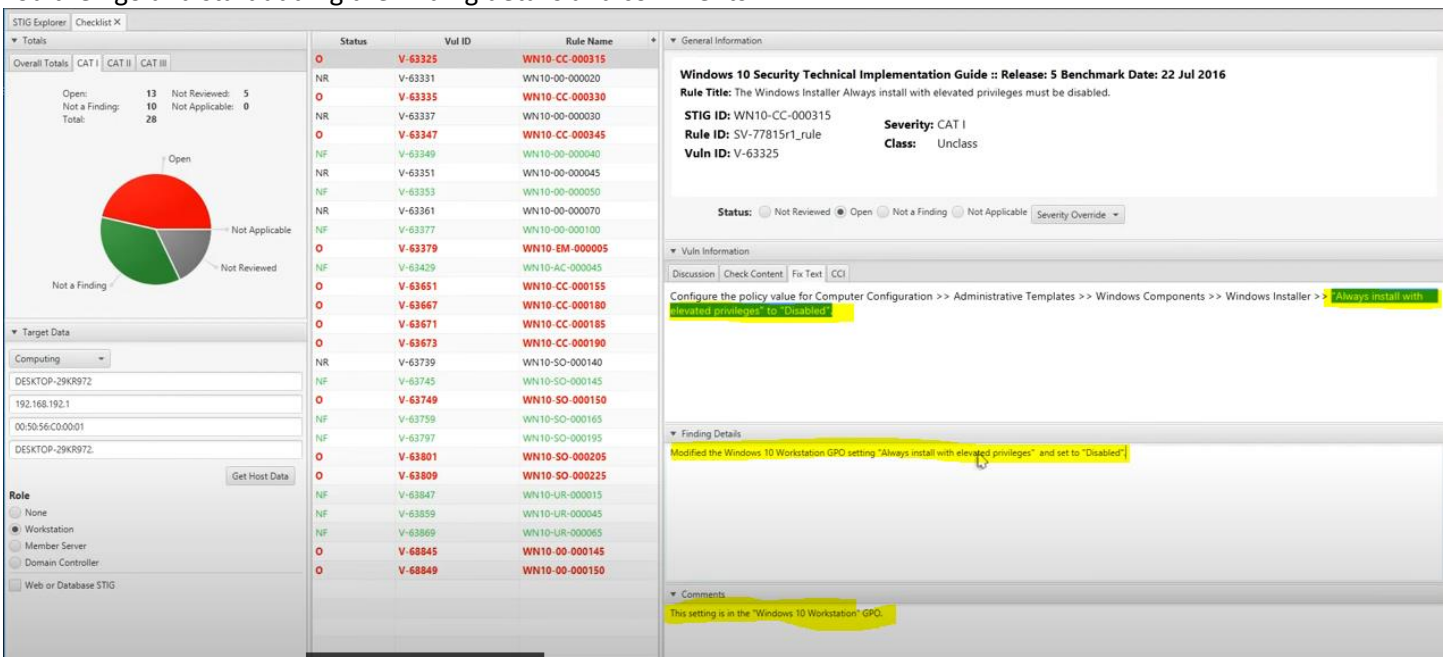
All the checks are marked for you after importing the results. The are color coded based on the profiles.



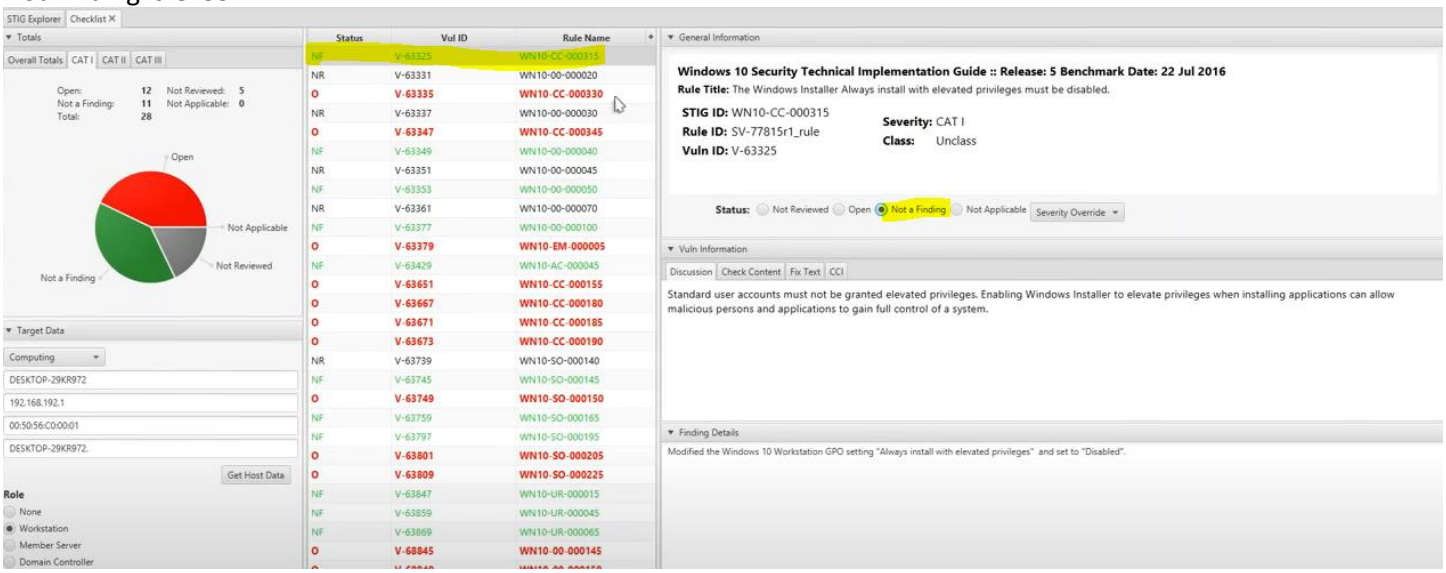
Once you review everything you can save this checklist, create a new folder checklist>> file name



You then go and start adding the finding details and comments



Not Finding is Green



NR is Not Reviewed