

**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

The screenshot shows the DISA STIG Viewer application interface. The main window displays a list of STIGs (Security Technical Implementation Guides) with columns for Vul ID and Rule Name. The list includes various rules such as V-63319, V-63321, V-63323, etc. On the right side, there is a panel for 'General Information' and 'Check Content'. The 'General Information' panel shows details for the selected rule, including the Rule Title, Rule ID, Severity, and Class. The 'Check Content' panel provides a detailed description of the rule and its requirements.

Vul ID	Rule Name
V-63319	WN10-00-000005
V-63321	WN10-CC-000310
V-63323	WN10-00-000010
V-63325	WN10-CC-000315
V-63327	WN10-00-000015
V-63329	WN10-CC-000320
V-63331	WN10-00-000020
V-63333	WN10-CC-000325
V-63335	WN10-CC-000330
V-63337	WN10-00-000030
V-63339	WN10-CC-000335
V-63341	WN10-CC-000340
V-63343	WN10-00-000025
V-63345	WN10-00-000035
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63355	WN10-00-000055
V-63357	WN10-00-000060
V-63359	WN10-00-000065
V-63361	WN10-00-000070
V-63363	WN10-00-000075
V-63365	WN10-00-000080
V-63367	WN10-00-000085
V-63369	WN10-CC-000350
V-63371	WN10-00-000090
V-63373	WN10-00-000095
V-63375	WN10-CC-000355
V-63377	WN10-00-000100
V-63379	WN10-EM-000005
V-63381	WN10-00-000105
V-63383	WN10-00-000110
V-63385	WN10-00-000115
V-63387	WN10-EM-000010
V-63389	WN10-00-000120

Now we have the overall non remediated vulnerabilities

DISA STIG Viewer: 2.3

File Import Export

STIG Explorer Checklist X

Overall Totals CAT I CAT II CAT III

Open: 0 Not Reviewed: 278  
Not a Finding: 0 Not Applicable: 0

Not Reviewed Not Applicable

Target Data

Computing

Host Name  
IP Address  
MAC Address  
Fully Qualified Domain Name

Get Host Data

Role

☒ None  
☐ Workstation  
☐ Member Server  
☐ Domain Controller  
☐ Web or Database STIG

STIG

Status	Vul ID	Rule Name
NR	V-63319	WN10-00-000005
NR	V-63321	WN10-CC-000310
NR	V-63323	WN10-00-000010
NR	V-63325	WN10-CC-000315
NR	V-63327	WN10-00-000015
NR	V-63329	WN10-CC-000320
NR	V-63331	WN10-00-000020
NR	V-63333	WN10-CC-000325
NR	V-63335	WN10-CC-000330
NR	V-63337	WN10-00-000030
NR	V-63339	WN10-CC-000335
NR	V-63341	WN10-CC-000340
NR	V-63343	WN10-00-000025
NR	V-63345	WN10-00-000035
NR	V-63347	WN10-CC-000345
NR	V-63349	WN10-00-000040
NR	V-63351	WN10-00-000045
NR	V-63353	WN10-00-000050
NR	V-63355	WN10-00-000055
NR	V-63357	WN10-00-000060
NR	V-63359	WN10-00-000065
NR	V-63361	WN10-00-000070
NR	V-63363	WN10-00-000075
NR	V-63365	WN10-00-000080
NR	V-63367	WN10-00-000085
NR	V-63369	WN10-CC-000350
NR	V-63371	WN10-00-000090
NR	V-63373	WN10-00-000095
NR	V-63375	WN10-CC-000355
NR	V-63377	WN10-00-000100
NR	V-63379	WN10-EM-000005
NR	V-63381	WN10-00-000105
NR	V-63383	WN10-00-000110
NR	V-63385	WN10-00-000115
NR	V-63387	WN10-EM-000010

General Information

**Windows 10 Security Technical Implementation Guide :: Release: 5 Benchmark Date: 22 Jul 2016**

**Rule Title:** Domain-joined systems must use Windows 10 Enterprise Edition.

**STIG ID:** WN10-00-000005 **Severity:** CAT II

**Rule ID:** SV-77809r1\_rule **Class:** Unclass

**Vuln ID:** V-63319

Status: ☒ Not Reviewed ☐ Open ☐ Not a Finding ☐ Not Applicable Severity Override

Vuln Information

Discussion Check Content Fix Text CCI

Features such as Credential Guard uses virtualization based security to protect secrets that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise.

Finding Details

Comments

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

Vuln Information

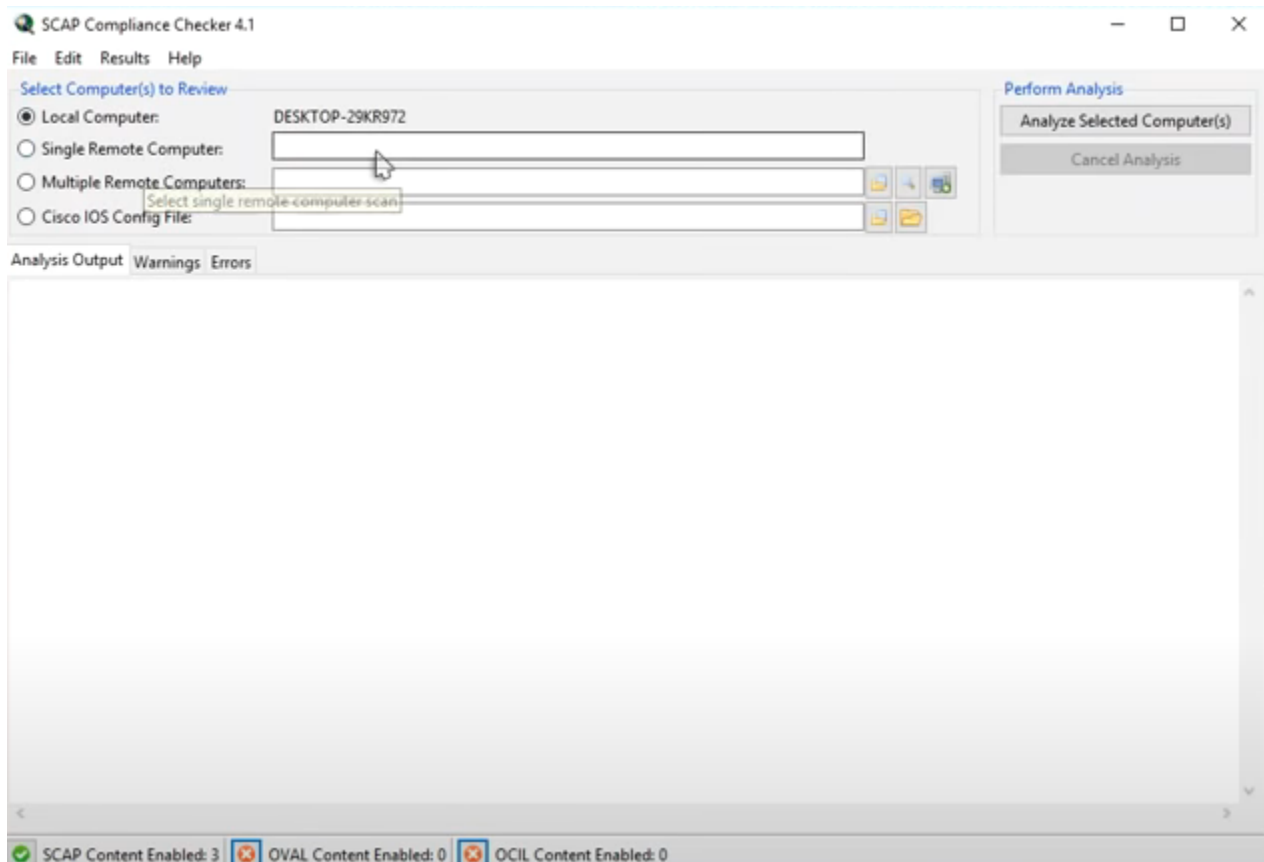
Discussion Check Content Fix Text CCI

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Always install with elevated privileges" to "Disabled".

Finding Details

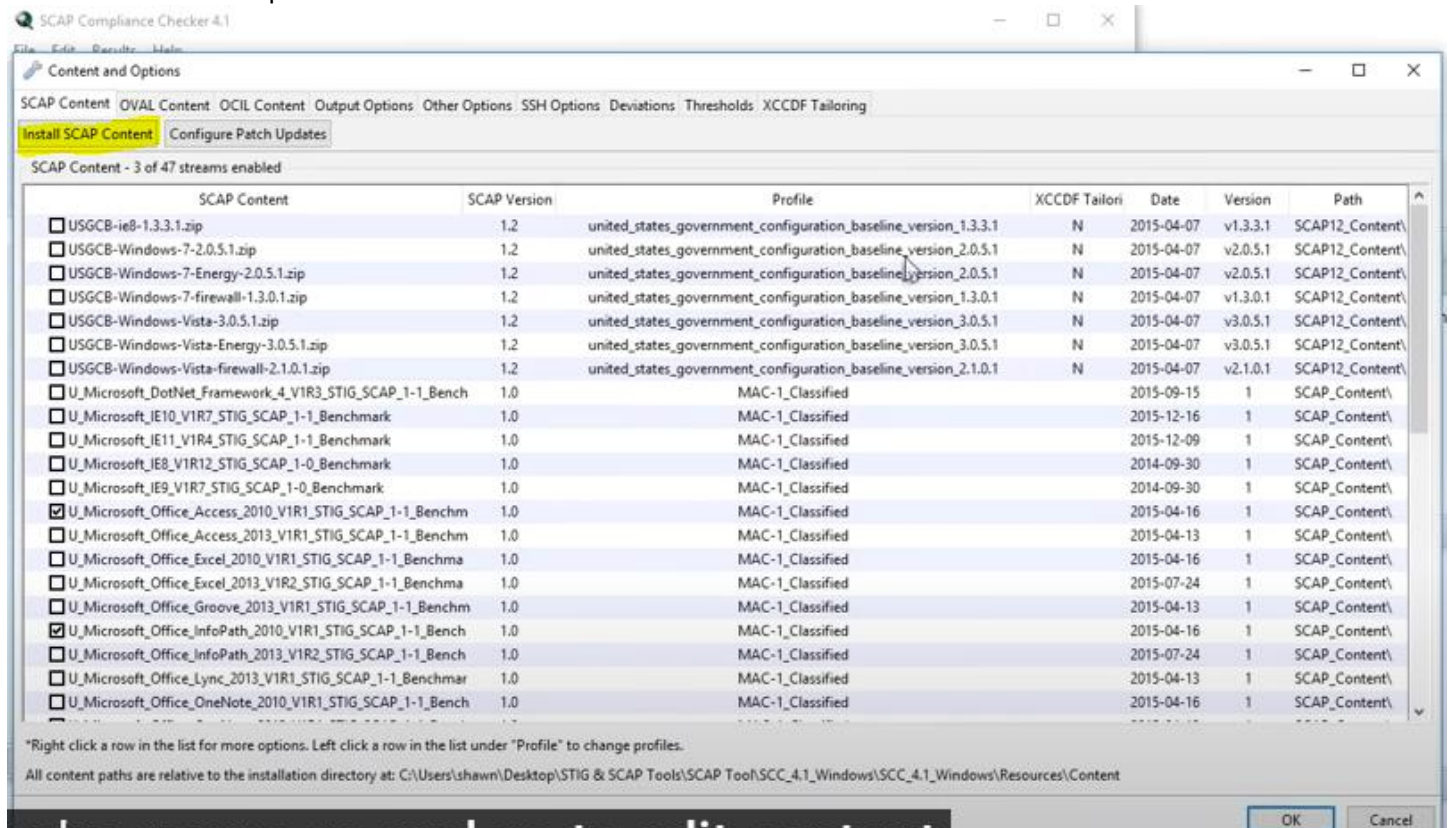
Comments

## SCAP TOOL



Hit the Analyze Selected Computer

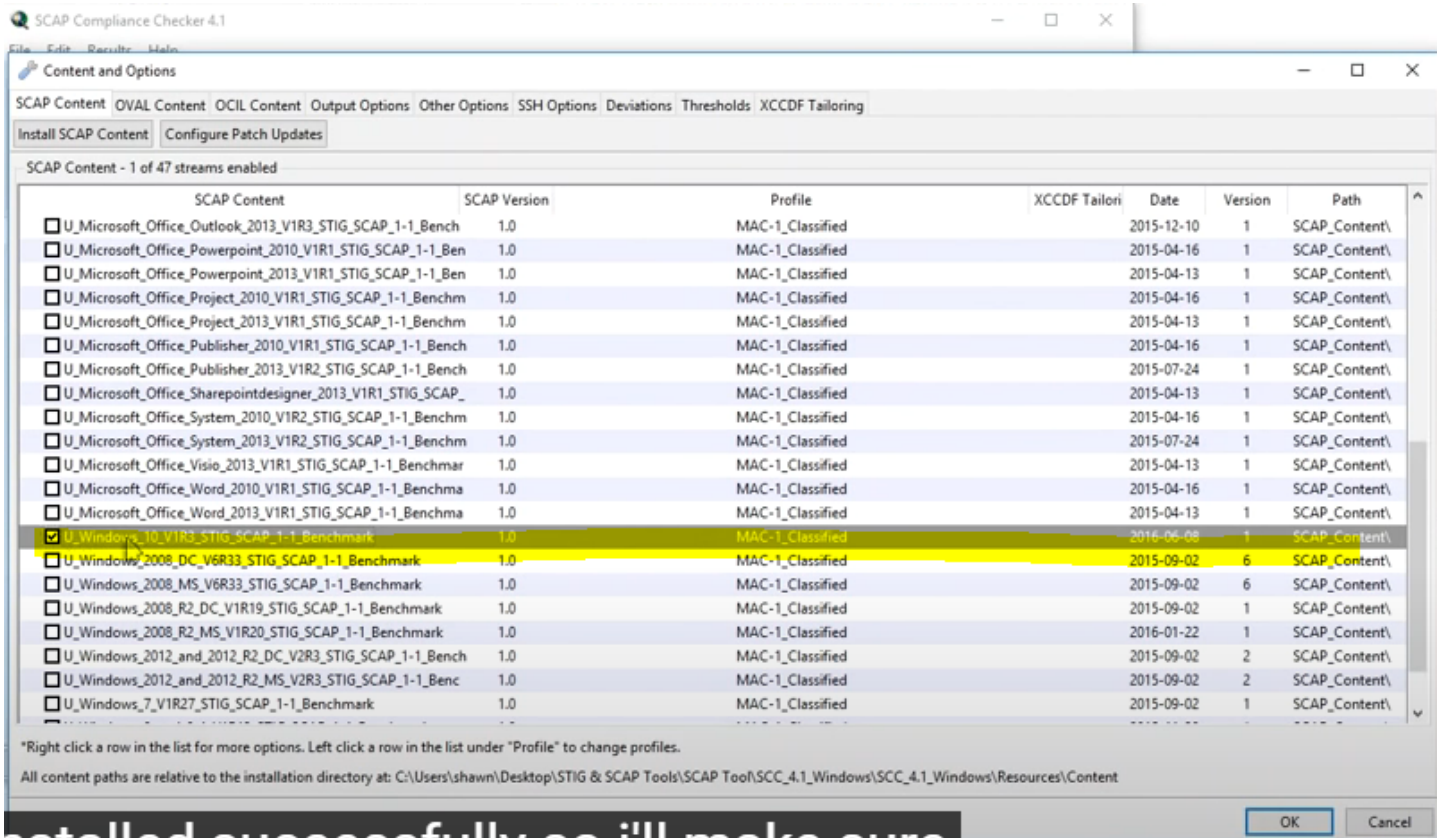
Edit >> Content and Options



Click Install SCAP Content >> Go to Benchmark folder and get the windows\_10\_SCAP... >> Open

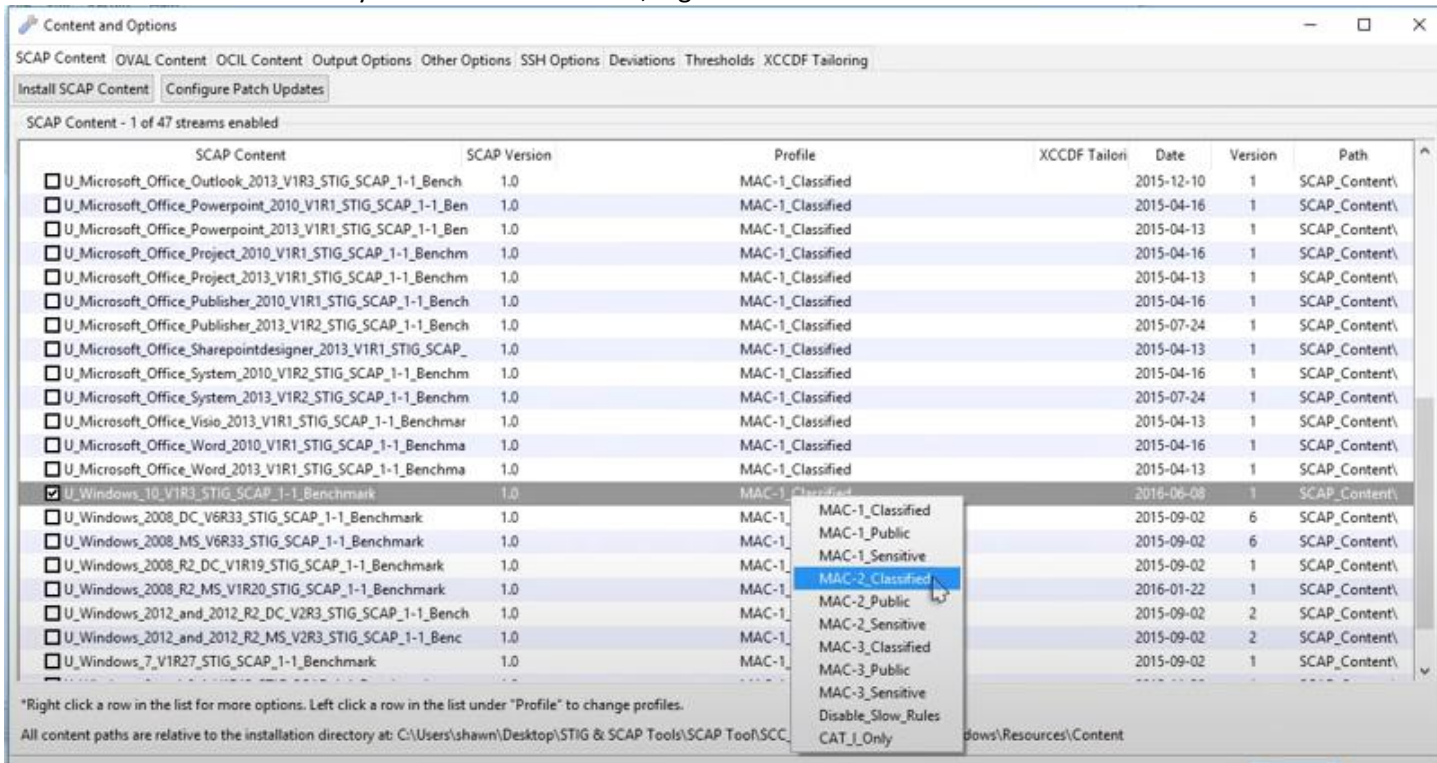
Once installed you selected



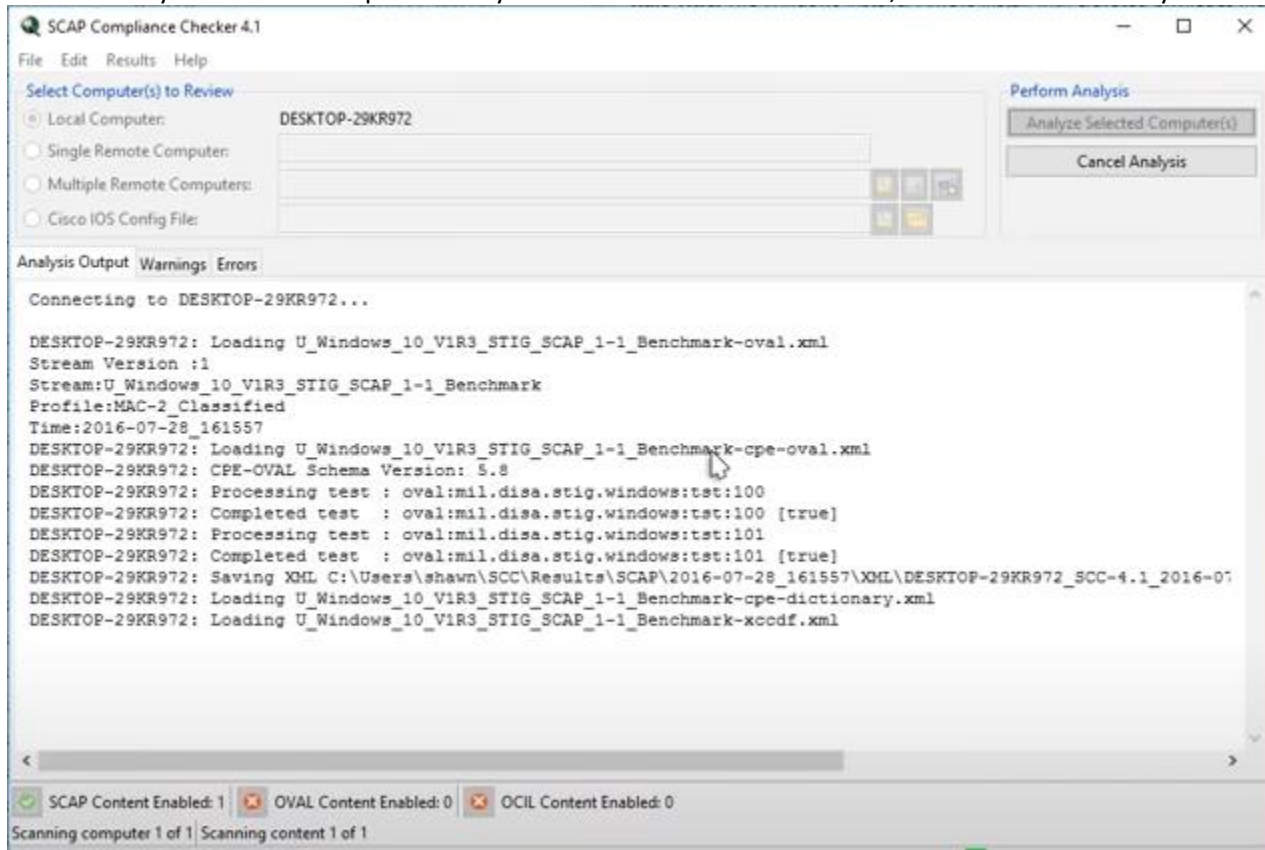


installed successfully so i'll make sure

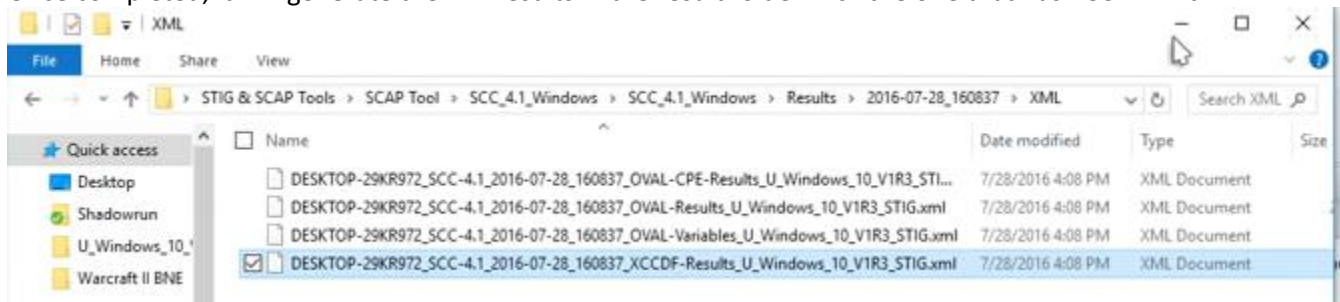
You can select to automatically fix which classification, Right Click on Profile area



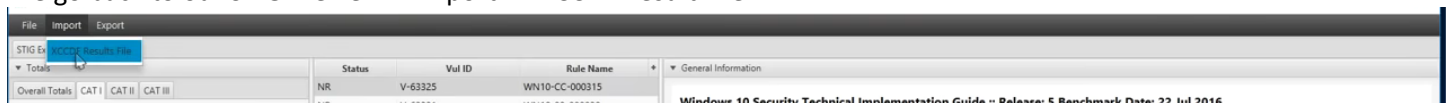
Hit the “Analyze Selected Computer” # if you have the McAfee or Antivirus, disable it. It will slow your scan down.



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. They are color coded based on the profiles.

The screenshot shows the DISA STIG Viewer 2.3 interface. On the left, a pie chart displays the status of checks: Open (red), Not a Finding (green), Not Reviewed (grey), and Not Applicable (white). The table lists various rules with their status, vulnerability IDs, and names. The right pane provides detailed information for the selected rule, including its title, ID, severity, and class.

**Windows 10 Security Technical Implementation Guide :: Release: 5 Benchmark Date: 22 Jul 2016**  
**Rule Title:** Domain-joined systems must use Windows 10 Enterprise Edition.  
**STIG ID:** WN10-00-000005  
**Rule ID:** SV-77809r1\_rule  
**Severity:** CAT II  
**Vuln ID:** V-63319  
**Class:** Unclass

**Status:** ☐ Not Reviewed ☐ Open ☒ Not a Finding ☐ Not Applicable **Severity Override**

**Vuln Information**  
 Discussion | Check Content | Fix Text | CCI  
 Features such as Credential Guard uses virtualization based security to protect secrets that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise.

**Finding Details**

**Comments**

you they're all color-coded again red being the

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

The screenshot shows the 'Save As' dialog box in DISA STIG Viewer 2.3. The file is being saved to 'This PC > Desktop > STIG & SCAP Tools > Checklists'. The file name is 'windows10stigcheck' and the save type is 'Checklist files (\*.ckl)'.

**Save As**

← → ↑ ↓ This PC > Desktop > STIG & SCAP Tools > Checklists Search Checklists

Organize New folder

Documents  
 Email attachmer  
 Fixes  
 Harley  
 Malwarebytes  
 N64 Roms  
 Pictures  
 Public  
 Resume  
 Shadowrun  
 Work

This PC

Network

File name: windows10stigcheck

Save as type: Checklist files (\*.ckl)



You then go and start adding the finding details and comments

STIG Explorer Checklist X

Overall Totals: CAT I, CAT II, CAT III

Open: 13, Not Reviewed: 5, Not a Finding: 10, Not Applicable: 0, Total: 28

Target Data: Computing, DESKTOP-29KR972, 192.168.192.1, 00:50:56:C0:00:01, DESKTOP-29KR972, Get Host Data

Role: None, Workstation, Member Server, Domain Controller, Web or Database STIG

Status	Vul ID	Rule Name
O	V-63325	WN10-CC-000315
NR	V-63331	WN10-00-000020
O	V-63335	WN10-CC-000330
NR	V-63337	WN10-00-000030
O	V-63347	WN10-CC-000345
NF	V-63349	WN10-00-000040
NR	V-63351	WN10-00-000045
NF	V-63353	WN10-00-000050
NR	V-63361	WN10-00-000070
NF	V-63377	WN10-00-000100
O	V-63379	WN10-EM-000005
NF	V-63429	WN10-AC-000045
O	V-63651	WN10-CC-000155
O	V-63667	WN10-CC-000180
O	V-63671	WN10-CC-000185
O	V-63673	WN10-CC-000190
NR	V-63739	WN10-SO-000140
NF	V-63745	WN10-SO-000145
O	V-63749	WN10-SO-000150
NF	V-63759	WN10-SO-000165
NF	V-63797	WN10-SO-000195
O	V-63801	WN10-SO-000205
O	V-63809	WN10-SO-000225
NF	V-63847	WN10-UR-000015
NF	V-63859	WN10-UR-000045
NF	V-63869	WN10-UR-000065
O	V-68845	WN10-00-000145
O	V-68849	WN10-00-000150

General Information: Windows 10 Security Technical Implementation Guide :: Release: 5 Benchmark Date: 22 Jul 2016  
Rule Title: The Windows Installer Always install with elevated privileges must be disabled.  
STIG ID: WN10-CC-000315  
Rule ID: SV-77815r1\_rule  
Vuln ID: V-63325  
Severity: CAT I  
Class: Unclass

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable

Vuln Information: Discussion, Check Content, Fix Text, CCI

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Always install with elevated privileges" to "Disabled"

Finding Details: Modified the Windows 10 Workstation GPO setting "Always install with elevated privileges" and set to "Disabled"

Comments: This setting is in the "Windows 10 Workstation" GPO.

Not Finding is Green

STIG Explorer Checklist X

Overall Totals: CAT I, CAT II, CAT III

Open: 12, Not Reviewed: 5, Not a Finding: 11, Not Applicable: 0, Total: 28

Target Data: Computing, DESKTOP-29KR972, 192.168.192.1, 00:50:56:C0:00:01, DESKTOP-29KR972, Get Host Data

Role: None, Workstation, Member Server, Domain Controller, Web or Database STIG

Status	Vul ID	Rule Name
NF	V-63325	WN10-CC-000315
NR	V-63331	WN10-00-000020
O	V-63335	WN10-CC-000330
NR	V-63337	WN10-00-000030
O	V-63347	WN10-CC-000345
NF	V-63349	WN10-00-000040
NR	V-63351	WN10-00-000045
NF	V-63353	WN10-00-000050
NR	V-63361	WN10-00-000070
NF	V-63377	WN10-00-000100
O	V-63379	WN10-EM-000005
NF	V-63429	WN10-AC-000045
O	V-63651	WN10-CC-000155
O	V-63667	WN10-CC-000180
O	V-63671	WN10-CC-000185
O	V-63673	WN10-CC-000190
NR	V-63739	WN10-SO-000140
NF	V-63745	WN10-SO-000145
O	V-63749	WN10-SO-000150
NF	V-63759	WN10-SO-000165
NF	V-63797	WN10-SO-000195
O	V-63801	WN10-SO-000205
O	V-63809	WN10-SO-000225
NF	V-63847	WN10-UR-000015
NF	V-63859	WN10-UR-000045
NF	V-63869	WN10-UR-000065
O	V-68845	WN10-00-000145
O	V-68849	WN10-00-000150

General Information: Windows 10 Security Technical Implementation Guide :: Release: 5 Benchmark Date: 22 Jul 2016  
Rule Title: The Windows Installer Always install with elevated privileges must be disabled.  
STIG ID: WN10-CC-000315  
Rule ID: SV-77815r1\_rule  
Vuln ID: V-63325  
Severity: CAT I  
Class: Unclass

Status: ☐ Not Reviewed ☐ Open ☒ Not a Finding ☐ Not Applicable

Vuln Information: Discussion, Check Content, Fix Text, CCI

Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

Finding Details: Modified the Windows 10 Workstation GPO setting "Always install with elevated privileges" and set to "Disabled".

NR is Not Reviewed