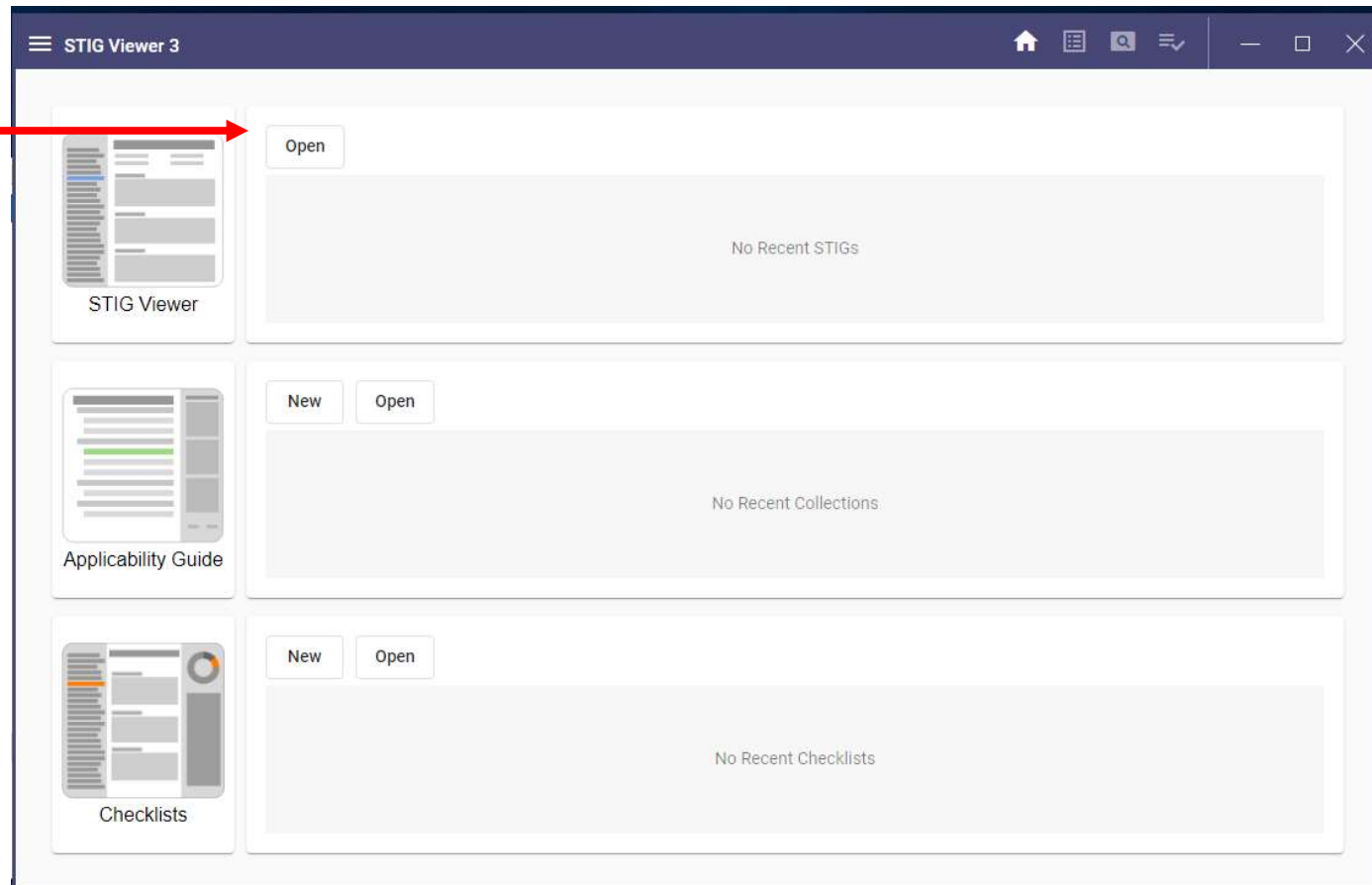


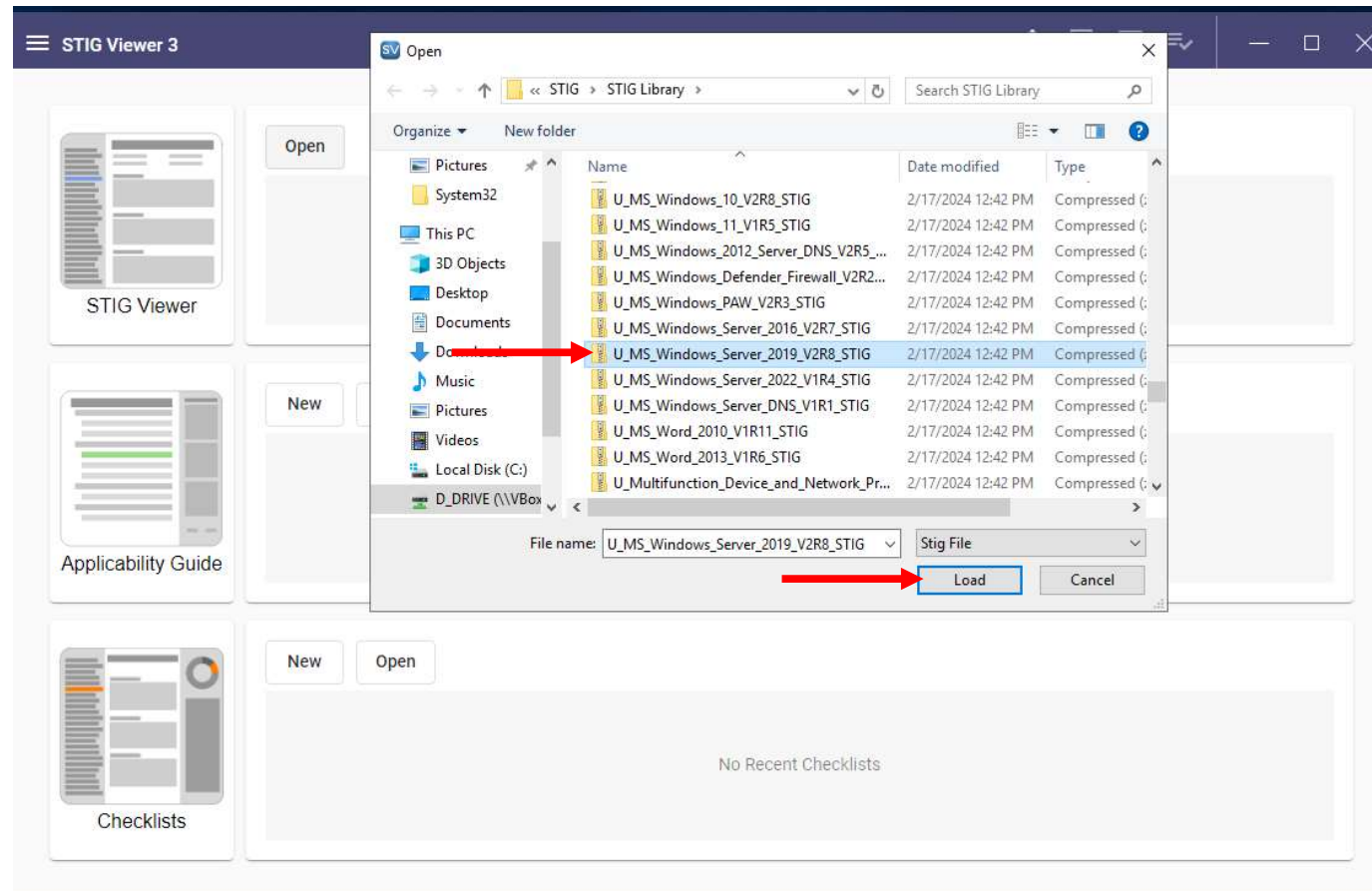
Basic Intro to STIG Viewer and SCAP

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.

The screenshot displays the STIG Viewer 3 application interface. The left sidebar, titled "STIG Rules", contains a tree view for "MICROSOFT WINDOWS SERVER 2019". Under this category, there are links for "Overview", "Revision History", and "Read Me". Below these, a list of rules is shown, including "V-205624" through "V-205633". The main pane on the right, titled "Microsoft Windows Server 2019", displays the "Microsoft Windows Server 2019 Security Technical Implementation Guide" with a release date of 8 and a benchmark date of 09 Nov 2023. It lists several security rules, each with a unique identifier (e.g., SRG-OS-000002-GPOS-00002 V-205624) and a description of the required configuration for Windows Server 2019.

STIG Rules

Overview

MICROSOFT WINDOWS SERVER 2019

- Overview**
U_MS_Windows_Server_2019_V2R8_Overv...
- Revision History**
U_MS_Windows_Server_2019_V2R8_Revisi...
- Read Me**
U_Readme_SRG_and_STIG.pdf

Group ID

- V-205624**
Windows Server 2019 must automatically remove o...
- V-205625**
Windows Server 2019 must be configured to audit ...
- V-205626**
Windows Server 2019 must be configured to audit ...
- V-205627**
Windows Server 2019 must be configured to audit ...
- V-205628**
Windows Server 2019 must be configured to audit ...
- V-205629**
Windows Server 2019 must have the number of allo...
- V-205630**
Windows Server 2019 must have the period of time ...
- V-205631**
Windows Server 2019 required legal notice must be ...
- V-205632**
Windows Server 2019 title for legal banner dialog b...
- V-205633**

274 Rules

Microsoft Windows Server 2019

Microsoft Windows Server 2019 Security Technical Implementation Guide
Release: 8 Benchmark Date: 09 Nov 2023

- SRG-OS-000002-GPOS-00002 V-205624
Windows Server 2019 must automatically remove or disable temporary user accounts after 72 hours.
- SRG-OS-000004-GPOS-00004 V-205625
Windows Server 2019 must be configured to audit Account Management - Security Group Management successes.
- SRG-OS-000004-GPOS-00004 V-205626
Windows Server 2019 must be configured to audit Account Management - User Account Management successes.
- SRG-OS-000004-GPOS-00004 V-205627
Windows Server 2019 must be configured to audit Account Management - User Account Management failures.
- SRG-OS-000004-GPOS-00004 V-205628
Windows Server 2019 must be configured to audit Account Management - Computer Account Management successes.
- SRG-OS-000021-GPOS-00005 V-205629
Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less.
- SRG-OS-000021-GPOS-00005 V-205630
Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.
- SRG-OS-000023-GPOS-00006 V-205631
Windows Server 2019 required legal notice must be configured to display before console logon.

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

STIG Viewer 3

Microsoft Windows Server 2019

STIG Rules

Overview

MICROSOFT WINDOWS SERVER 2019

Overview
U_MS_Windows_Server_2019_V2R8

Revision History
U_MS_Windows_Server_2019_V2R8

Read Me
U_Readme_SRG_and_STIG.pdf

Group ID

V-205624
Windows Server 2019 must automatically remove or disable temporary user accounts after 72 hours.

V-205625
Windows Server 2019 must be configured to audit Account Management - Security Group Management successes.

V-205626
Windows Server 2019 must be configured to audit Account Management - User Account Management successes.

V-205627
Windows Server 2019 must be configured to audit Account Management - User Account Management failures.

V-205628
Windows Server 2019 must be configured to audit Account Management - Computer Account Management successes.

V-205629
Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less.

V-205630
Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.

V-205631
Windows Server 2019 required legal notice must be configured to display before console logon.

V-205632
Windows Server 2019 required legal notice must be configured to display before console logon.

V-205633
Windows Server 2019 required legal notice must be configured to display before console logon.

274 Rules

Actions:

- ☒ Create checklist from STIG
- ☐ Export STIG

Rule List Display:

Rule ID Group ID STIG ID

☒ Show Rule Title

☒ Show Documents List

Group By:

None Origin STIG

Server 2019 Security Technical Implementation Guide

Version: 09 Nov 2023

SRG-OS-000004-GPOS-00004 V-205624

SRG-OS-000021-GPOS-00005 V-205625

SRG-OS-000021-GPOS-00005 V-205626

SRG-OS-000021-GPOS-00005 V-205627

SRG-OS-000004-GPOS-00004 V-205628

SRG-OS-000021-GPOS-00005 V-205629

SRG-OS-000021-GPOS-00005 V-205630

SRG-OS-000023-GPOS-00006 V-205631

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

The screenshot displays the 'STIG Checklists' application interface. On the left, a sidebar titled 'Checklist Rules' shows a list of rules under the 'All' category. The rules are grouped by ID, with the first group being 'V-257503' for 'Microsoft Windows Server 2019'. The total count of rules is 274. On the right, the detailed view for the selected rule 'V-257503' is shown. It includes the rule title, discussion, and a summary of findings. A red arrow points to the '274 Rules' count in the top right corner of the interface.

STIG Checklists

★ New Checklist X +

Checklist Rules [Filter] [Settings] [Save] [Import] [Export] [Edit Checklist]

All Cat I Cat II Cat III

Group ID

- V-257503 Windows Server 2019 must have PowerSh...
- V-236001 The Windows Explorer Preview pane must ...
- V-214936 Windows Server 2019 must have a host-ba...
- V-205925 Windows Server 2019 must disable autom...
- V-205924 Windows Server 2019 must preserve zone ...
- V-205923 Windows Server 2019 default permissions ...
- V-205922 Windows Server 2019 session security for ...
- V-205921 Windows Server 2019 session security for ...
- V-205920 Windows Server 2019 must be configured t...
- V-205919 Windows Server 2019 LAN Manager authe...
- V-205918 Windows Server 2019 must prevent PKU2...
- V-205917 Windows Server 2019 must prevent NTLM ...
- V-205916 Windows Server 2019 services using Local...
- V-205915 Windows Server 2019 must be configured t...
- V-205914 Windows Server 2019 must not allow anon...

274 Rules

Microsoft Windows Server 2019
Release: 8 Benchmark Date: 09 Nov 2023

GROUP ID: V-257503 RULE ID: SV-257503r921895 STIG ID: WN19-CC-000530

SEVERITY: CAT II CLASSIFICATION: Unclassified

Rule Title:
Windows Server 2019 must have PowerShell Transcription enabled.

Discussion:
Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Enabling PowerShell Transcription will record detailed information from the processing of PowerShell commands and scripts. This can provide additional

Comments Finding Details

Not Reviewed 274 Not A Finding 0

Open 0 Not Applicable 0

Checklist Type: Computing

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Target Comments

Role: None

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

The screenshot displays the 'STIG Checklists' application interface. The top navigation bar includes a 'New Checklist' button and a 'Checklist Rules' dropdown menu. The main content area is divided into three sections: a list of rules on the left, a detailed view of a selected rule in the center, and a summary panel on the right.

Checklist Rules: The 'Checklist Rules' dropdown menu is open, showing a filter for 'Cat I'. The list of rules is filtered to show 33 CAT I Rules. The rules are listed with their Group ID and a brief description.

Microsoft Windows Server 2019: The detailed view shows the following information:

- Release: 8 Benchmark Date: 09 Nov 2023
- GROUP ID: V-205919
- RULE ID: SV-205919r857347
- STIG ID: WN19-SO-000310
- SEVERITY: CAT I
- LEGACY IDS: SV-103389, V-93301
- CLASSIFICATION: Unclassified

Rule Title: Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM.

Discussion: The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone or nondomain-joined computers that are running later versions.

Check Text: If the following registry value does not exist or is not

Summary Panel: The summary panel shows a circular progress indicator with '33 Rules'. It also includes a legend for 'Not Reviewed' (33), 'Open' (0), 'Not A Finding' (0), and 'Not Applicable' (0). The 'Checklist Type' is set to 'Computing'. Other fields include 'Host Name', 'IP Address', 'MAC Address', 'Fully Qualified Domain Name', 'Target Comments', 'Role', 'Workstation', and 'Technology Area'.

Another option
you can do is
select Edit
Checklist

The screenshot displays the 'STIG Checklists' application interface. The top navigation bar includes a menu icon, the title 'STIG Checklists', and standard window controls. Below the navigation bar, there's a tab for '*New Checklist' and a '+ New Checklist' button. The main area is divided into three sections:

- Checklist Rules:** A sidebar on the left with filters for 'All', 'Cat I', 'Cat II' (selected), and 'Cat III'. It lists 227 rules, with the top one being 'V-257503: Windows Server 2019 must have PowerShell Transcription enabled'. A summary at the bottom indicates '227 CAT II Rules'.
- Rule Details:** The central pane shows details for the selected rule 'V-257503'. It includes the title 'Microsoft Windows Server 2019', release information, and a table with the following data:

GROUP ID:	RULE ID:	STIG ID:
V-257503	SV-257503r921895	WN19-CC-000530

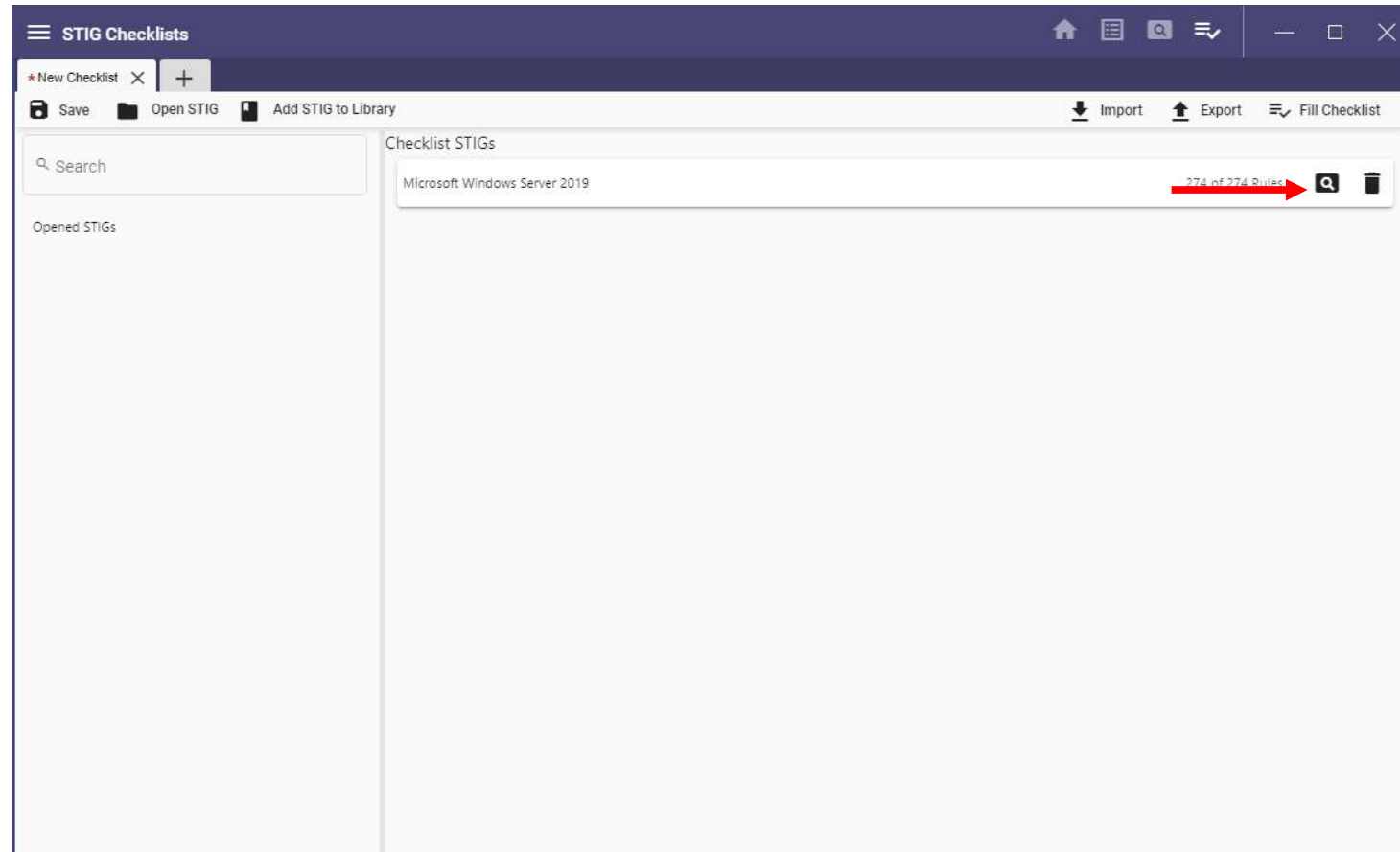
SEVERITY:	CLASSIFICATION
CAT II	Unclassified

Rule Title: Windows Server 2019 must have PowerShell Transcription enabled.

Discussion: Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Enabling PowerShell Transcription will record detailed information from the processing of PowerShell commands and scripts. This can provide additional
- Form Fields:** The rightmost pane contains a form for editing the checklist. It includes a circular progress indicator showing '227 Rules' (227 Not Reviewed, 0 Not A Finding, 0 Open, 0 Not Applicable). Below this are dropdown menus for 'Checklist Type' (set to 'Computing') and 'Role' (set to 'Workstation'). There are also input fields for 'Host Name', 'IP Address', 'MAC Address', 'Fully Qualified Domain Name', and 'Target Comments'. At the bottom, there are two text areas labeled 'Comments' and 'Finding Details'.

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

STIG Checklists

New Checklist X +

Filter

FILTERS

Content

Title

Severity

STIG ID

Group ID

Rule ID

CAT III (Low)

+ Add Filter

✓ Apply

RULE ID: SV-205624r857301

LEGACY IDS: SV-103063, V-92975

STIG ID: WN19-00-000300

CLASSIFICATION: Unclassified

Rule Title:

Windows Server 2019 must automatically remove or disable temporary user accounts after 72 hours.

Discussion:

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Check Text:

Review temporary user accounts for expiration dates.

Determine if temporary user accounts are used and identify any that exist. If none exist, this is NA.

Domain Controllers:

Open "PowerShell".

Enter "Search-ADAccount -AccountExpiring | FT Name, AccountExpirationDate".

INCLUDED RULES

- V-205632
- V-205664
- V-205691
- V-205726
- V-205800
- V-205819
- V-205856
- V-205857
- V-205858
- V-205859
- V-205860
- V-205870
- V-205871
- V-205923

FILTERED RULES

- V-205624
- V-205625

Back to Checklist Builder

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

The screenshot displays the 'STIG Checklists' application interface. On the left, a sidebar lists 274 rules under the 'All' category. The main panel shows the details for rule V-257503, titled 'Microsoft Windows Server 2019'. The rule is categorized as 'CAT II' and 'Unclassified'. The 'Rule Title' is 'Windows Server 2019 must have PowerShell Transcription enabled.' The 'Discussion' section explains that maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises. It also mentions that enabling PowerShell Transcription will record detailed information from the processing of PowerShell commands and scripts. On the right, a summary panel shows a donut chart indicating 274 rules, with a legend for 'Not Reviewed' (274), 'Not A Finding' (0), 'Open' (0), and 'Not Applicable' (0). Below the chart, there are input fields for 'Host Name', 'IP Address', 'MAC Address', 'Fully Qualified Domain Name', 'Target Comments', and 'Role' (set to 'None').

STIG Checklists

* New Checklist X +

Checklist Rules [Filter] [Settings] [Save] [Import] [Export] [Edit Checklist]

All Cat I Cat II Cat III

Group ID

- V-257503 Windows Server 2019 must have PowerSh...
- V-236001 The Windows Explorer Preview pane must ...
- V-214936 Windows Server 2019 must have a host-ba...
- V-205925 Windows Server 2019 must disable autom...
- V-205924 Windows Server 2019 must preserve zone ...
- V-205923 Windows Server 2019 default permissions ...
- V-205922 Windows Server 2019 session security for ...
- V-205921 Windows Server 2019 session security for ...
- V-205920 Windows Server 2019 must be configured t...
- V-205919 Windows Server 2019 LAN Manager authe...
- V-205918 Windows Server 2019 must prevent PKU2...
- V-205917 Windows Server 2019 must prevent NTLM ...
- V-205916 Windows Server 2019 services using Local...
- V-205915 Windows Server 2019 must be configured t...
- V-205914 Windows Server 2019 must not allow anon...

274 Rules

Microsoft Windows Server 2019
Release: 8 Benchmark Date: 09 Nov 2023

GROUP ID: V-257503 RULE ID: SV-257503r921895 STIG ID: WN19-CC-000530

SEVERITY: CAT II CLASSIFICATION: Unclassified

Rule Title:
Windows Server 2019 must have PowerShell Transcription enabled.

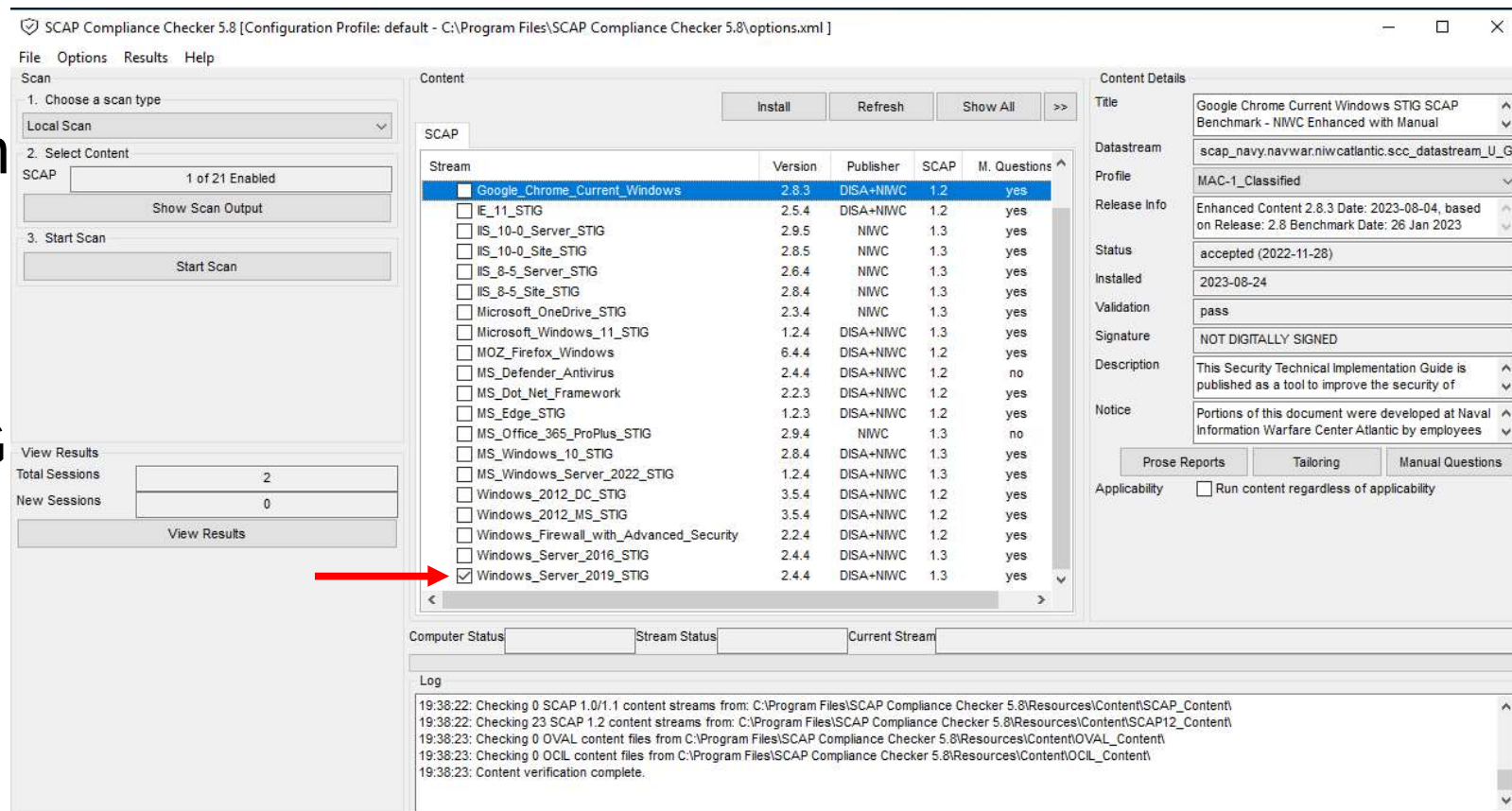
Discussion:
Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Enabling PowerShell Transcription will record detailed information from the processing of PowerShell commands and scripts. This can provide additional

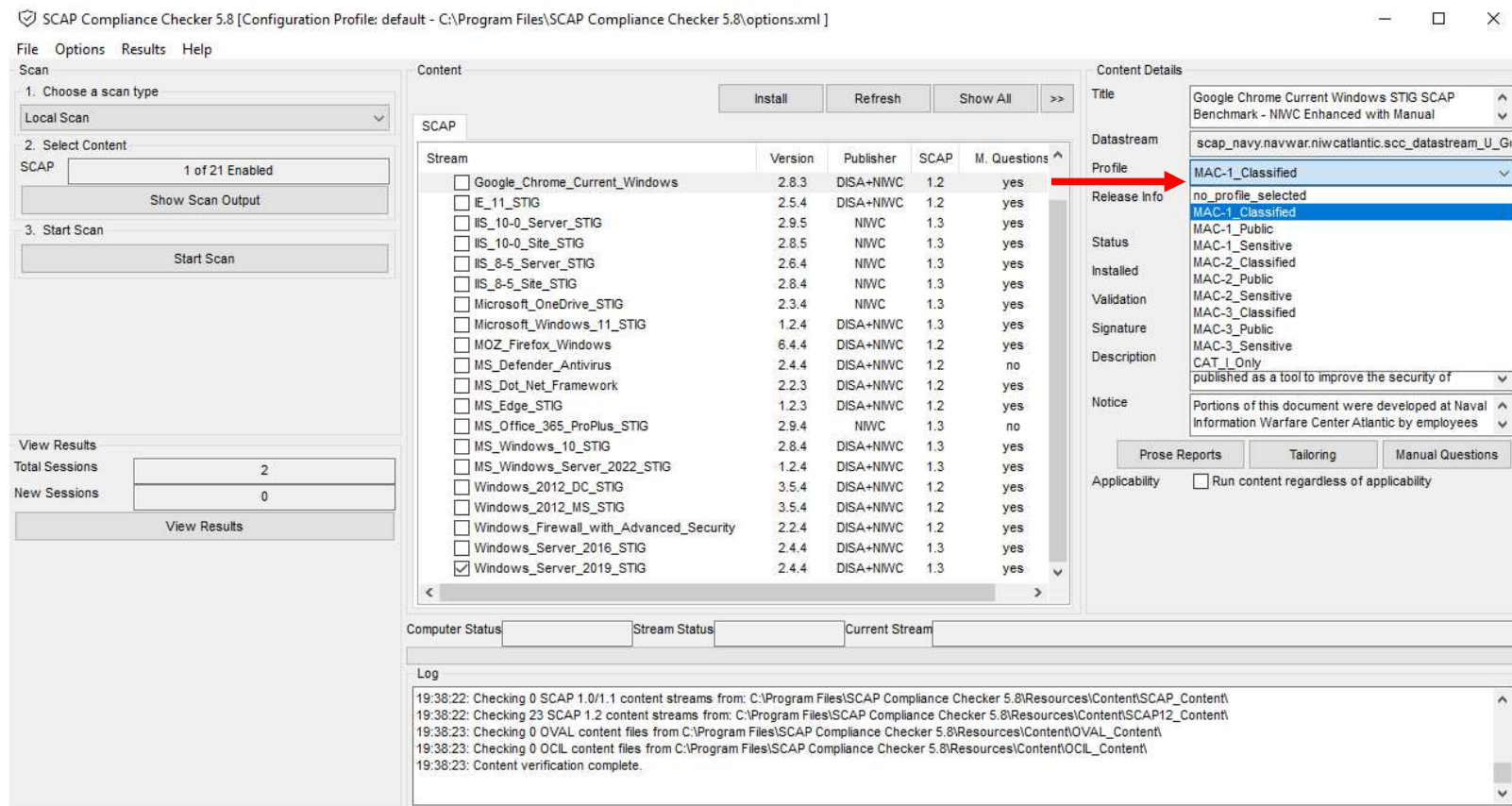
Comments Finding Details

Host Name IP Address MAC Address Fully Qualified Domain Name Target Comments Role: None

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

SCAP Compliance Checker 5.8 [Configuration Profile: default - C:\Program Files\SCAP Compliance Checker 5.8\options.xml]

File Options Results Help

Scan

1. Choose a scan type

Local Scan

2. Select Content

SCAP 1 of 21 Enabled

Show Scan Output

3. Start Scan

Start Scan

View Results

Total Sessions 2

New Sessions 0

View Results

Content

Install Refresh Show All >>

SCAP

Stream	Version	Publisher	SCAP	M. Questions
<input type="checkbox"/> Google_Chrome_Current_Windows	2.8.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> IE_11_STIG	2.5.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> IIS_10-0_Server_STIG	2.9.5	NIWC	1.3	yes
<input type="checkbox"/> IIS_10-0_Site_STIG	2.8.5	NIWC	1.3	yes
<input type="checkbox"/> IIS_8-5_Server_STIG	2.6.4	NIWC	1.3	yes
<input type="checkbox"/> IIS_8-5_Site_STIG	2.8.4	NIWC	1.3	yes
<input type="checkbox"/> Microsoft_OneDrive_STIG	2.3.4	NIWC	1.3	yes
<input type="checkbox"/> Microsoft_Windows_11_STIG	1.2.4	DISA+NIWC	1.3	yes
<input type="checkbox"/> MOZ_Firefox_Windows	6.4.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> MS_Defender_Antivirus	2.4.4	DISA+NIWC	1.2	no
<input type="checkbox"/> MS_Dot_Net_Framework	2.2.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> MS_Edge_STIG	1.2.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> MS_Office_365_ProPlus_STIG	2.9.4	NIWC	1.3	no
<input type="checkbox"/> MS_Windows_10_STIG	2.8.4	DISA+NIWC	1.3	yes
<input type="checkbox"/> MS_Windows_Server_2022_STIG	1.2.4	DISA+NIWC	1.3	yes
<input type="checkbox"/> Windows_2012_DC_STIG	3.5.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Windows_2012_MS_STIG	3.5.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Windows_Firewall_with_Advanced_Security	2.2.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Windows_Server_2016_STIG	2.4.4	DISA+NIWC	1.3	yes
<input checked="" type="checkbox"/> Windows_Server_2019_STIG	2.4.4	DISA+NIWC	1.3	yes

Content Details

Title Google Chrome Current Windows STIG SCAP Benchmark - NIWC Enhanced with Manual

Datastream scap_navy.navwar.niwcatlantic.scc_datastream_U_Gi

Profile MAC-1_Classified

Release Info no_profile_selected

Status MAC-1_Public

Installed MAC-1_Sensitive

Validation MAC-2_Classified

Signature MAC-2_Public

Description MAC-2_Sensitive

Notice CAT_I_Only

Prose Reports Tailoring Manual Questions

Applicability ☐ Run content regardless of applicability

Computer Status Stream Status Current Stream

Log

19:38:22: Checking 0 SCAP 1.0/1.1 content streams from: C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\SCAP_Content\

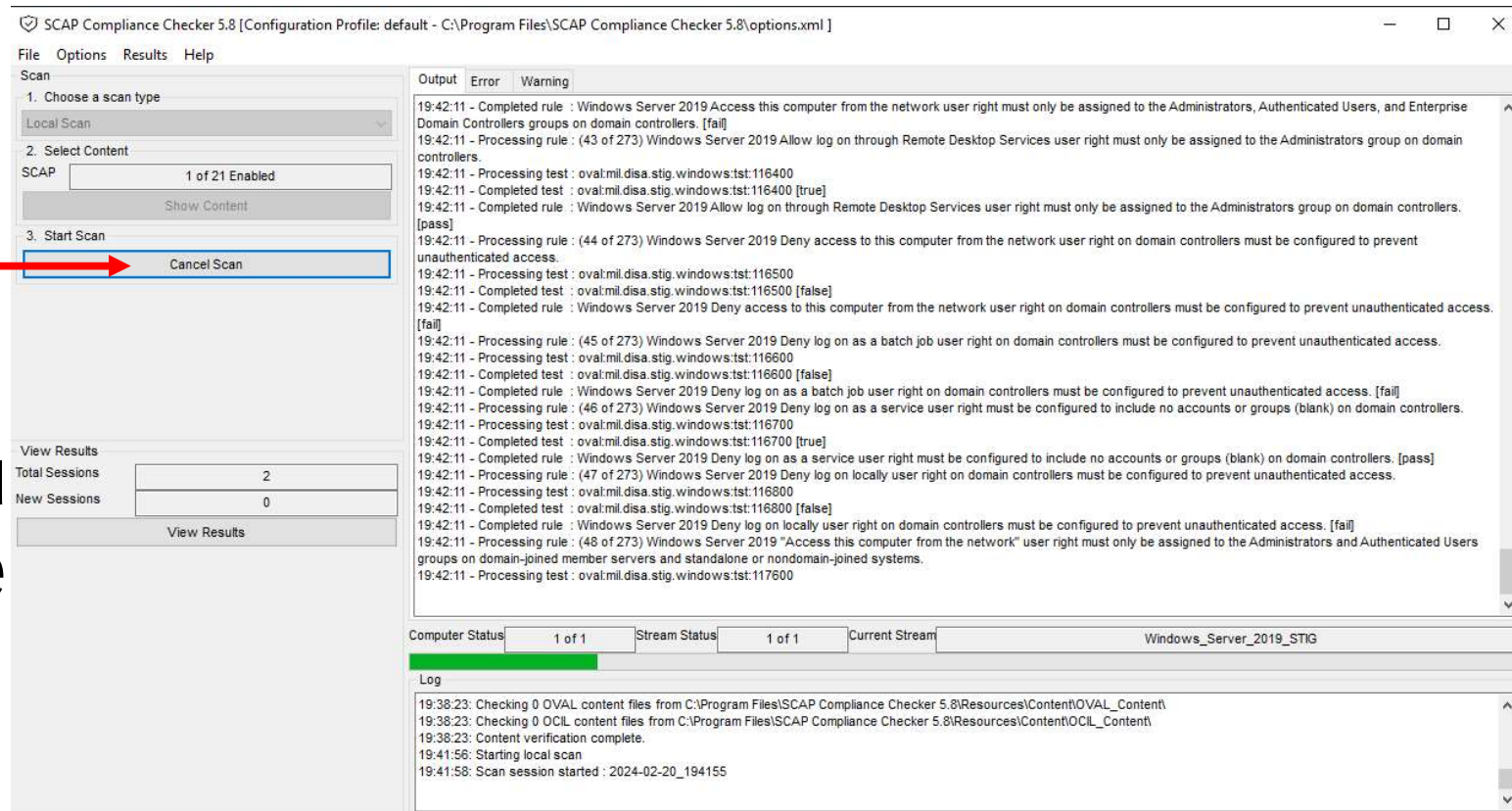
19:38:22: Checking 23 SCAP 1.2 content streams from: C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\SCAP12_Content\

19:38:23: Checking 0 OVAL content files from C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\OVAL_Content\

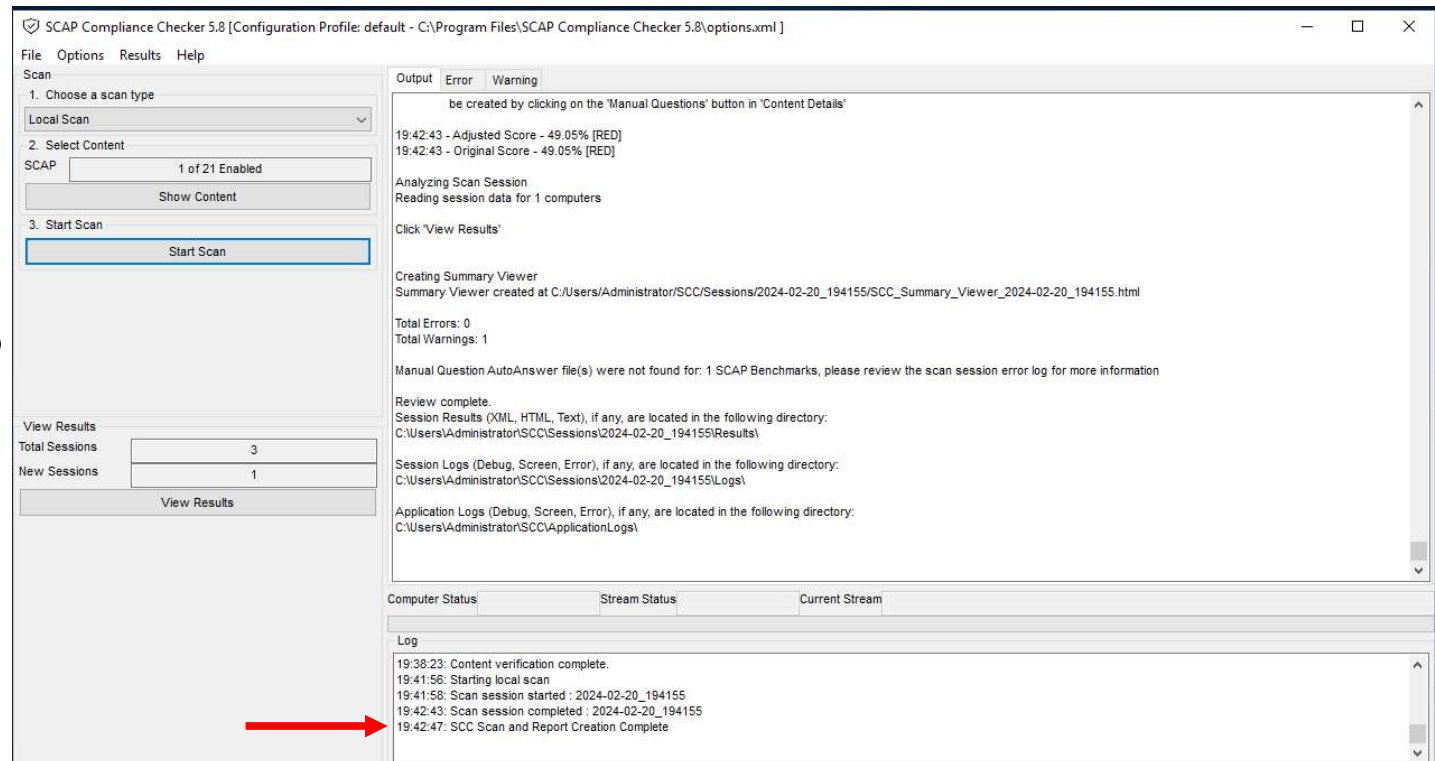
19:38:23: Checking 0 OCIL content files from C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\OCIL_Content\

19:38:23: Content verification complete.

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

The screenshot displays the 'STIG Checklists' application interface. On the left, a list of rules is shown under the 'Cat III' tab, including 'V-205923 Windows Server 2019 default permissions ...' and others. The main panel shows details for 'Microsoft Windows Server 2019', including its release and benchmark date, and a table of attributes like GROUP ID, RULE ID, STIG ID, SEVERITY, LEGACY IDS, and CLASSIFICATION. The 'Check Text' field contains the text: 'If the following registry value does not exist or is not'. On the right, a sidebar shows a progress chart and a list of fields to be populated, such as Host Name, IP Address, and MAC Address. A red arrow points to the 'Import' button in the top right corner, and another red arrow points to the 'Import XCCDF or CMRS Results' option in the dropdown menu.

STIG Checklists

* New Checklist X +

Checklist Rules [Filter] [Settings] [Save] [Import] [Export] [Edit Checklist]

All Cat I Cat II **Cat III**

Group ID

- V-205923 Windows Server 2019 default permissions ...
- V-205871 Windows Server 2019 Turning off File Expl...
- V-205870 Windows Server 2019 Windows Update m...
- V-205860 Windows Server 2019 must be configured t...
- V-205859 Windows Server 2019 source routing must ...
- V-205858 Windows Server 2019 Internet Protocol ver...
- V-205857 Windows Server 2019 must have Secure B...
- V-205856 Windows Server 2019 systems must have ...
- V-205819 Windows Server 2019 must be configured t...
- V-205800 The Windows Server 2019 time service mu...
- V-205726 Windows Server 2019 directory service mu...
- V-205691 Windows Server 2019 Application Compati...
- V-205664 Windows Server 2019 non-administrative a...
- V-205632 Windows Server 2019 title for legal banner ...

14 CAT III Rules

Microsoft Windows Server 2019
Release: 8 Benchmark Date: 09 Nov 2023

GROUP ID:	RULE ID:	STIG ID:
V-205923	SV-205923r569188	WN19-SO-000370

SEVERITY:	LEGACY IDS:	CLASSIFICATION
CAT III	V-93309, SV-103397	Unclassified

Rule Title:
Windows Server 2019 default permissions of global system objects must be strengthened.

Discussion:
Windows systems maintain a global list of shared system resources such as DOS device names, mutexes, and semaphores. Each type of object is created with a default Discretionary Access Control List (DACL) that specifies who can access the objects with what permissions. When this policy is enabled, the default DACL is stronger, allowing non-administrative users to read shared objects but not to modify shared objects they did not create.

Check Text:
If the following registry value does not exist or is not

Comments Finding Details

Target Comments

Role Workstation

Technician/Analyst

Navigate to
the XCCDF
log, select,
and load

The screenshot displays the STIG Checklists application interface. On the left, a list of 14 CAT III Rules is shown, including V-205923 through V-205632. A red arrow points from the 'Videos' folder in the file explorer to the file 'DC1_SCC-5.8_2024-02-20_194155_XCCDF-Results_Windows_Server_2...'. Below the file explorer, the 'File name' field is set to 'DC1_SCC-5.8_2024-02-20_194155_XCCDF-' and the 'Load' button is highlighted with a red arrow. The right side of the application shows a summary of 14 Rules, with a status bar indicating 'Not A Finding' and 'Not Applicable' counts.

STIG Checklists

New Checklist X +

Checklist Rules

All Cat I Cat II Cat III

Group ID

- V-205923 Windows Server 2019 default permissions ...
- V-205871 Windows Server 2019 Turning off File Expl...
- V-205870 Windows Server 2019 Windows Update m...
- V-205860 Windows Server 2019 must be configured t...
- V-205859 Windows Server 2019 source routing must ...
- V-205858 Windows Server 2019 Internet Protocol ver...
- V-205857 Windows Server 2019 must have Secure B...
- V-205856 Windows Server 2019 systems must have ...
- V-205819 Windows Server 2019 must be configured t...
- V-205800 The Windows Server 2019 time service mu...
- V-205726 Windows Server 2019 directory service mu...
- V-205691 Windows Server 2019 Application Compati...
- V-205664 Windows Server 2019 non-administrative a...
- V-205632 Windows Server 2019 title for legal banner ...

14 CAT III Rules

Open

Results > SCAP > XML

Search XML

Organize New folder

Desktop Documents Downloads Music Pictures Videos Local Disk (C:) D_DRIVE (\\VBox Network DC1 VBOXSVR

File name: DC1_SCC-5.8_2024-02-20_194155_XCCDF- Stig File

Load Cancel

access the objects with what permissions. When this policy is enabled, the default DACL is stronger, allowing non-administrative users to read shared objects but not to modify shared objects they did not create.

Check Text:

If the following registry value does not exist or is not

Comments Finding Details

14 Rules

Not A Finding 0

Not Applicable 0

MAC Address

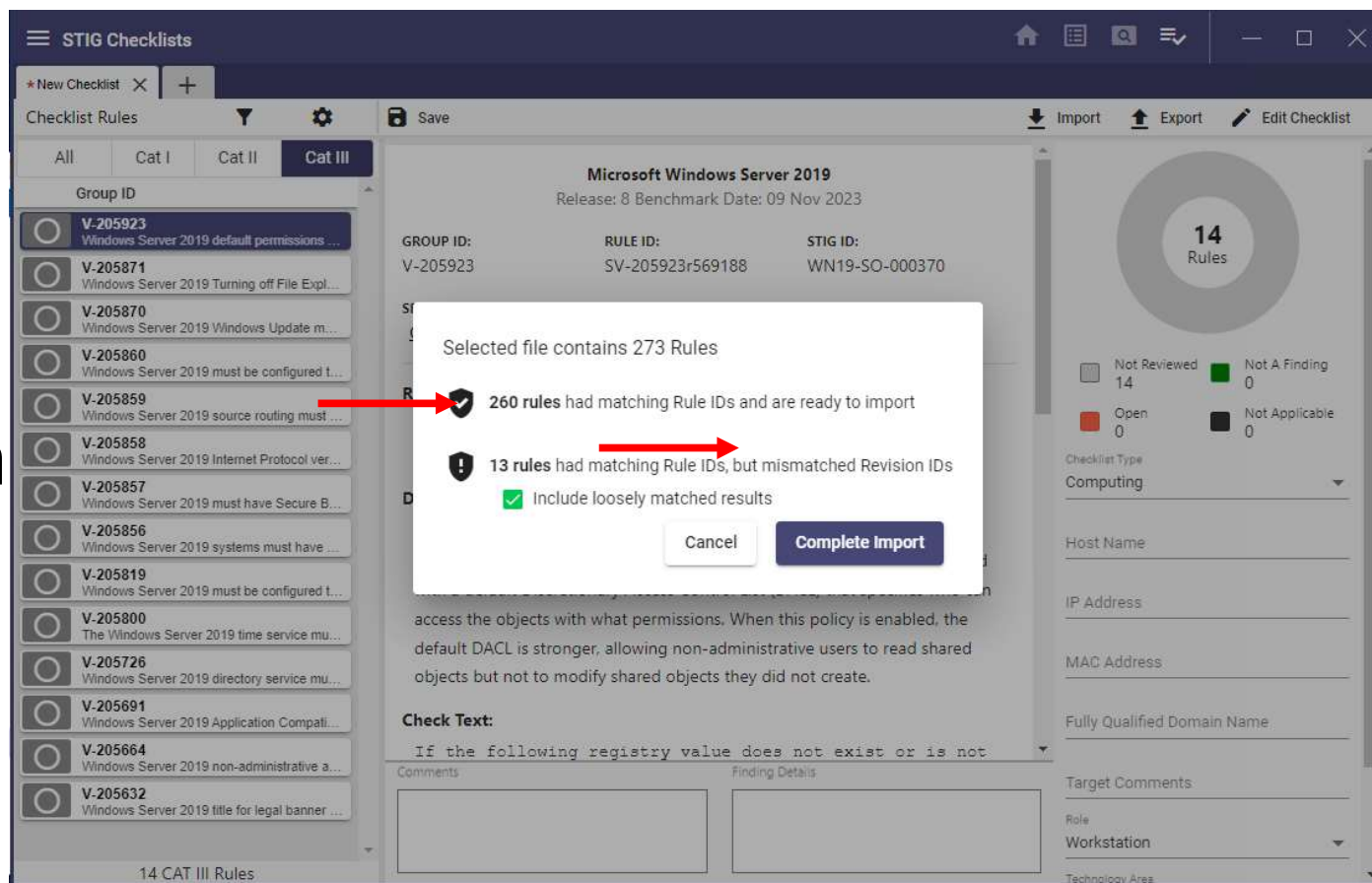
Fully Qualified Domain Name

Target Comments

Role Workstation

Technology Area

Notice it didn't match every rule exactly. Earlier I did go through and notice a few that had Revision ID discrepancies. 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.

STIG Checklists

New Checklist

+

Checklist Rules

All

Cat I

Cat II

Cat III

Group ID

V-257503

Windows Server 2019 must have PowerSh...

V-236001

The Windows Explorer Preview pane must ...

V-214936

Windows Server 2019 must have a host-ba...

V-205925

Windows Server 2019 must disable autom...

V-205924

Windows Server 2019 must preserve zone ...

V-205923

Windows Server 2019 default permissions ...

V-205922

Windows Server 2019 session security for ...

V-205921

Windows Server 2019 session security for ...

V-205920

Windows Server 2019 must be configured t...

V-205919

Windows Server 2019 LAN Manager authen...

V-205918

Windows Server 2019 must prevent PKU2...

V-205917

Windows Server 2019 must prevent NTLM ...

V-205916

Windows Server 2019 services using Local...

V-205915

Windows Server 2019 must be configured t...

V-205914

Windows Server 2019 must not allow anon...

274 Rules

Save

Import

Export

Edit Checklist

Microsoft Windows Server 2019

Release: 8 Benchmark Date: 09 Nov 2023

GROUP ID:

V-205923

RULE ID:

SV-205923r569188

STIG ID:

WN19-SO-000370

SEVERITY:

CAT III

LEGACY IDS:

V-93309, SV-103397

CLASSIFICATION

Unclassified

Rule Title:

Windows Server 2019 default permissions of global system objects must be strengthened.

Discussion:

Windows systems maintain a global list of shared system resources such as DOS device names, mutexes, and semaphores. Each type of object is created with a default Discretionary Access Control List (DACL) that specifies who can access the objects with what permissions. When this policy is enabled, the default DACL is stronger, allowing non-administrative users to read shared objects but not to modify shared objects they did not create.

Check Text:

If the following registry value does not exist or is not

Comments

Result: true

Tests: true (All child checks

Finding Details

Tool: cpe:/a:niwc:scd:5.8

Time: 2024-02-20T19:42:37

Result: pass

274 Rules

Open: 107, Not A Finding: 103, Not Reviewed: 64, Not Applicable: 0

Checklist Type: Computing

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Target Comments

Role: Workstation

Technology Area

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

STIG Checklists

New Checklist

+

Checklist Rules

All

Cat I

Cat II

Cat III

Group ID

V-205923

Windows Server 2019 default permissions of...

V-205871

Windows Server 2019 Turning off File Explor...

V-205870

Windows Server 2019 Windows Update mus...

V-205860

Windows Server 2019 must be configured to...

V-205859

Windows Server 2019 source routing must b...

V-205858

Windows Server 2019 Internet Protocol versi...

V-205857

Windows Server 2019 must have Secure Bo...

V-205856

Windows Server 2019 systems must have U...

V-205819

Windows Server 2019 must be configured to...

V-205800

The Windows Server 2019 time service must...

V-205726

Windows Server 2019 directory service must...

V-205691

Windows Server 2019 Application Compatibi...

V-205664

Windows Server 2019 non-administrative ac...

V-205632

Windows Server 2019 title for legal banner d...

14 CAT III Rules

finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

Value Name: EnableICMPRedirect

Value Type: REG_DWORD
Value: 0x00000000 (0)

Fix Text:
Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" to "Disabled".

This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. "MSS-Legacy.admx" and "MSS-Legacy.adml" must be copied to the \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively.

Comments
must exist.
Check : All collected items must match the given state(s).
Object Requirement : hive must be equal to 'HKEY_LOCAL_MACHINE'
Object Requirement : key must be equal to 'System\CurrentControlSet\Services\Tcpip\Parameters'
Object Requirement : name must be equal to 'EnableICMPRedirect'
State ID :
oval:mil.dise.stig.windows:ste:108600 (registry_state)
State Requirement : check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'
State Requirement : for check = 'all', value, the following must be true:
State Requirement : value must be equal to '0'

Collected Item/State Result : false
'HKEY_LOCAL_MACHINE' : hive equals
'System\CurrentControlSet\Services\Tcpip\Parameters' : key equals

Finding Details
Tool: cpe:/a:niwoc:scv:5.8
Time: 2024-02-20T19:42:37
Result: fail

14 Rules

Open 8

Not Reviewed 4

Not A Finding 2

Not Applicable 0

Checklist Type
Computing

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

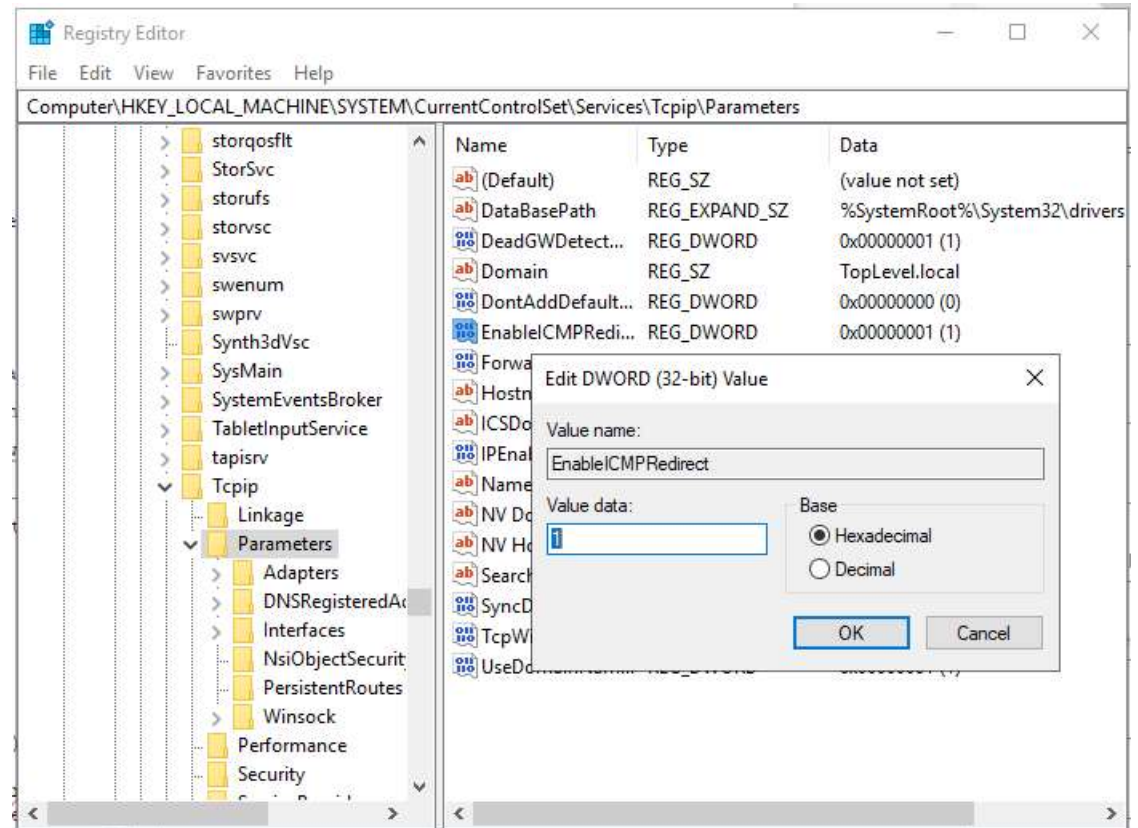
Target Comments

Role
Workstation

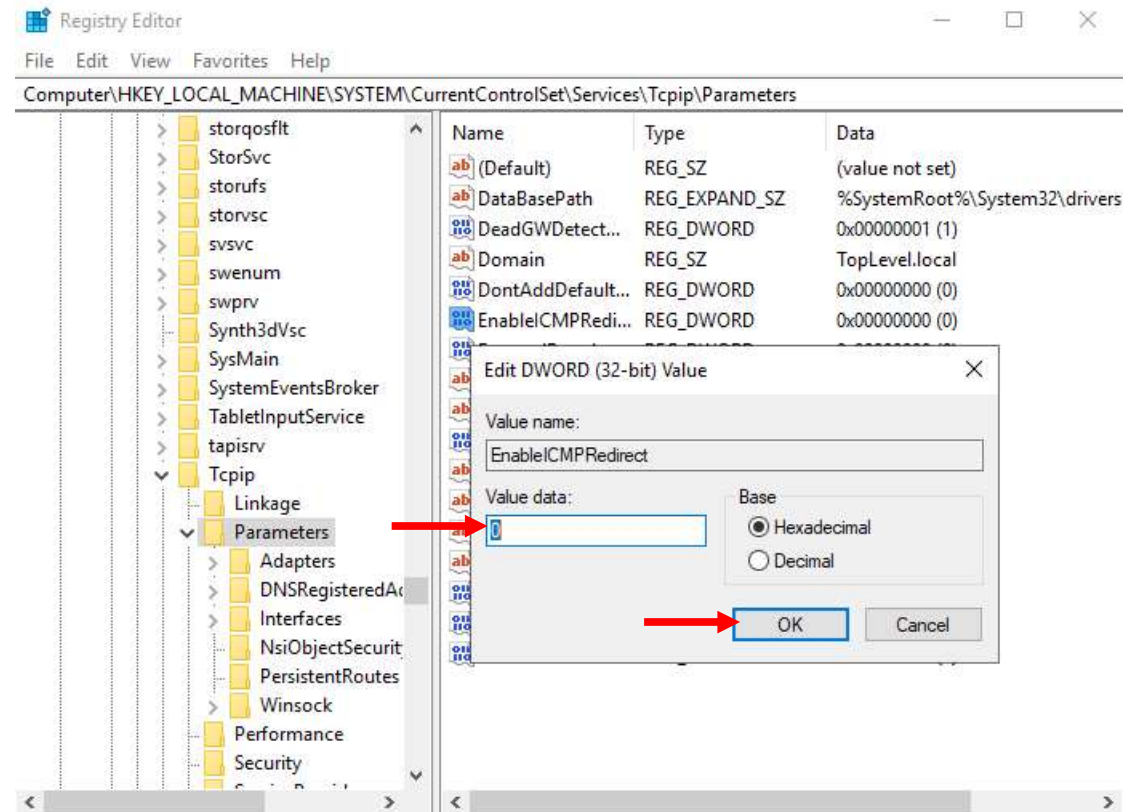
Technology Area
None

☐ Web or Database STIG

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.

STIG Checklists

New Checklist X +

Checklist Rules

All Cat I Cat II Cat III

Group ID

- V-205923 Windows Server 2019 default permissions of...
- V-205871 Windows Server 2019 Turning off File Explor...
- V-205870 Windows Server 2019 Windows Update mus...
- V-205860 Windows Server 2019 must be configured to...
- V-205859 Windows Server 2019 source routing must b...
- V-205858 Windows Server 2019 Internet Protocol versi...
- V-205857 Windows Server 2019 must have Secure Bo...
- V-205856 Windows Server 2019 systems must have U...
- V-205819 Windows Server 2019 must be configured to...
- V-205800 The Windows Server 2019 time service must...
- V-205726 Windows Server 2019 directory service must...
- V-205691 Windows Server 2019 Application Compatibi...
- V-205664 Windows Server 2019 non-administrative ac...
- V-205632 Windows Server 2019 title for legal banner d...

14 CAT III Rules

Save

Allowing ICMP redirect of routes can lead to traffic not being routed properly. When disabled, this forces ICMP to be routed via the shortest path first.

Check Text:

If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

Value Name: EnableICMPRedirect

Value Type: REG_DWORD
Value: 0x00000000 (0)

Fix Text:

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated

Comments

Navigated to: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Changed EnableICMPRedirect value from 1 to 0

Finding Details

Resolved DTG

14 Rules

Open 7 Not Reviewed 4 Not A Finding 3 Not Applicable 0

Checklist Type
Computing

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Target Comments

Role
Workstation

Technology Area
None

☐ Web or Database STIG

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.