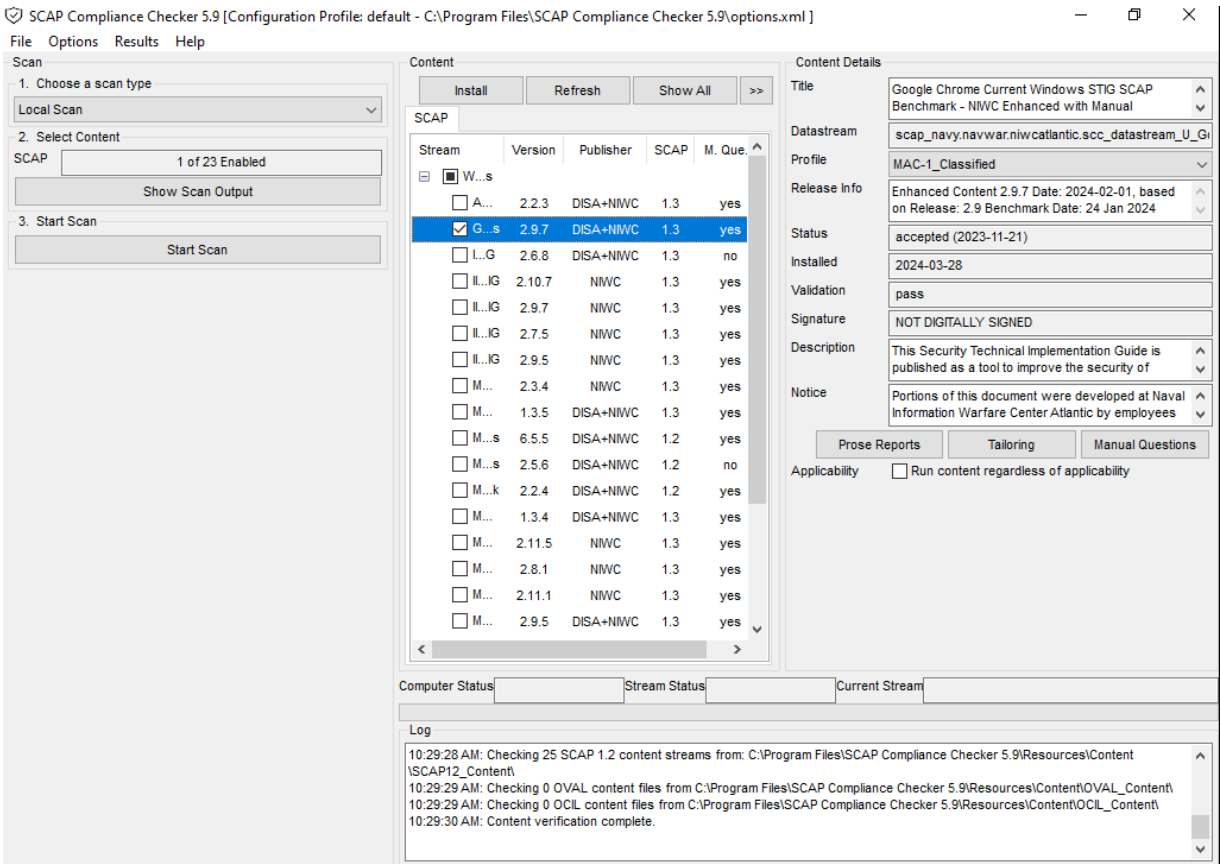


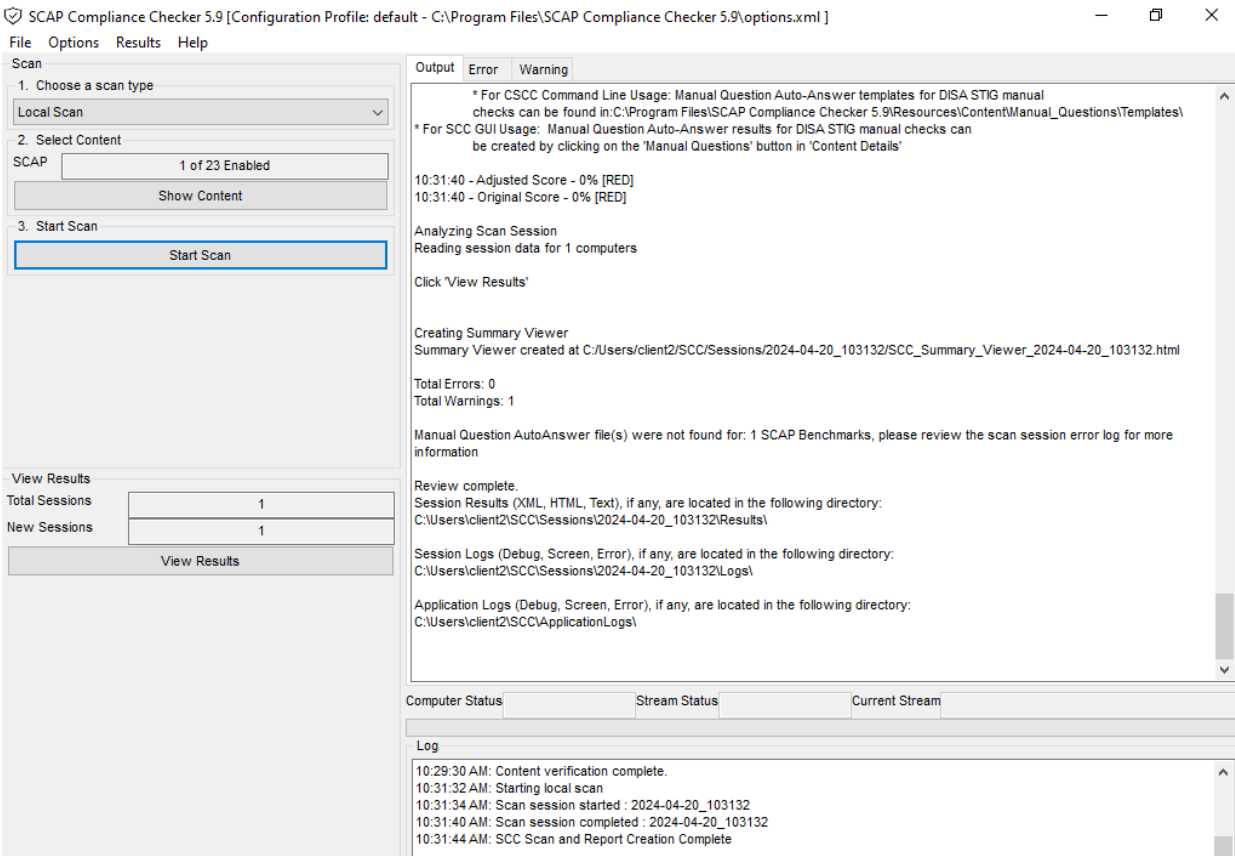
# **Security Compliance OpenScap**

**Student: Yagub Hajiyev**

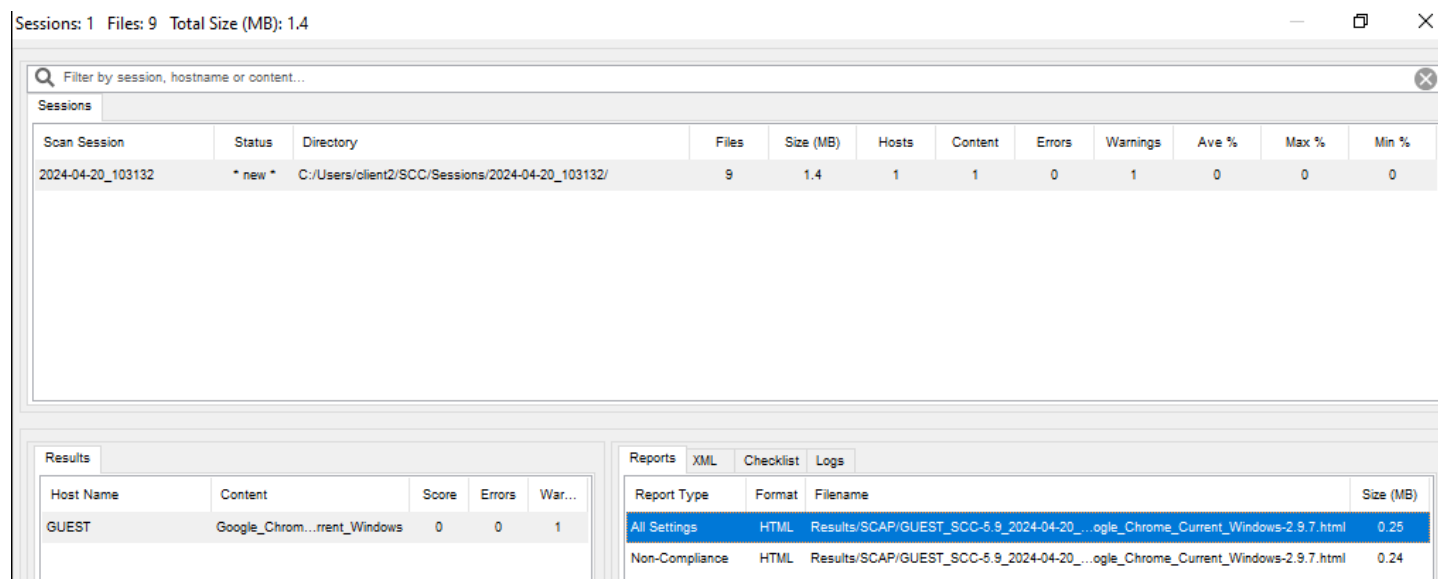
Once we open the tool, we choose **Google\_Chrome\_Content\_Windows** option and **Start Scan**.



After finishing scan, press **“View Results”** button.



In the opened window, we can find the reports in **HTML** format, just double click on the report.



The screenshot shows the SCC Report Viewer interface. The top bar indicates 'Sessions: 1 Files: 9 Total Size (MB): 1.4'. Below is a search bar and a 'Sessions' tab. The 'Sessions' table lists a single session for '2024-04-20\_103132'. Below this is a 'Results' tab with a table showing results for 'GUEST' on 'Google\_Chrom...rrent\_Windows' with a score of 0 and 1 error. To the right, there are tabs for 'Reports', 'XML', 'Checklist', and 'Logs'. The 'Reports' table lists two reports: 'All Settings' and 'Non-Compliance', both in HTML format, with their respective filenames and sizes.

Session	Status	Directory	Files	Size (MB)	Hosts	Content	Errors	Warnings	Ave %	Max %	Min %
2024-04-20_103132	* new *	C:/Users/client2/SCC/Sessions/2024-04-20_103132/	9	1.4	1	1	0	1	0	0	0

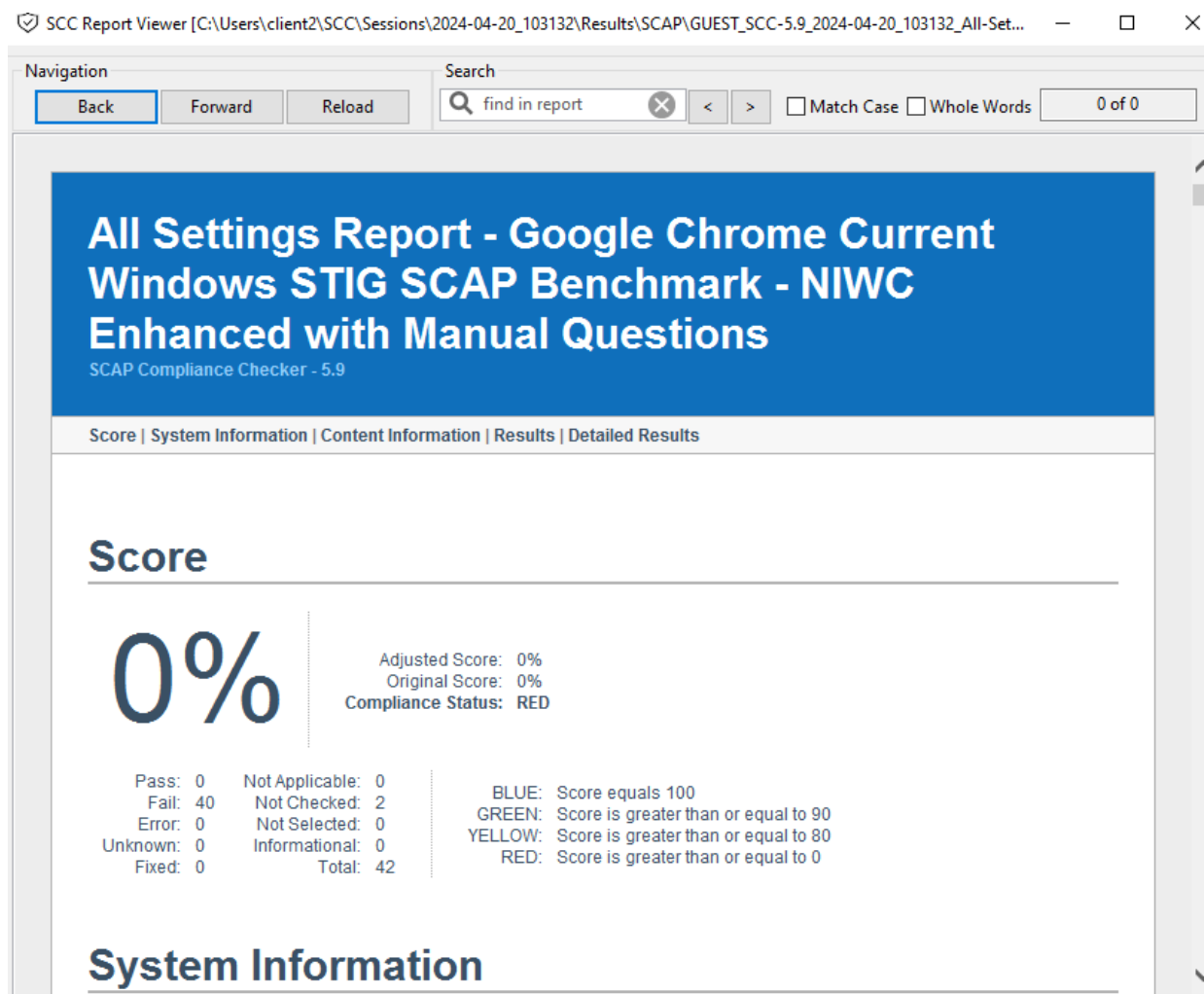
  

Host Name	Content	Score	Errors	War...
GUEST	Google_Chrom...rrent_Windows	0	0	1

Report Type	Format	Filename	Size (MB)
All Settings	HTML	Results/SCAP/GUEST_SCC-5.9_2024-04-20_103132_Google_Chrome_Current_Windows-2.9.7.html	0.25
Non-Compliance	HTML	Results/SCAP/GUEST_SCC-5.9_2024-04-20_103132_Google_Chrome_Current_Windows-2.9.7.html	0.24

This report give all essential information about our scanning process. Below, the figure displays the some of the fails which each of them refers to a unique misconfiguration. For better security, we need to get rid of these misconfiguration one by one. As you see, the initial score is 0%, because none of misconfiguration is solved yet. In this lab I solved first three of them.



The screenshot shows the 'All Settings Report - Google Chrome Current Windows STIG SCAP Benchmark - NIWC Enhanced with Manual Questions'. The report is generated by 'SCAP Compliance Checker - 5.9'. The navigation bar includes 'Back', 'Forward', and 'Reload' buttons, along with a search bar and checkboxes for 'Match Case' and 'Whole Words'. The main content area displays the 'Score' section, which shows a large '0%' score. Below the score, there is a table with the following data:

Score	Adjusted Score: 0%	Original Score: 0%	Compliance Status: RED
Pass: 0	Not Applicable: 0	BLUE: Score equals 100	
Fail: 40	Not Checked: 2	GREEN: Score is greater than or equal to 90	
Error: 0	Not Selected: 0	YELLOW: Score is greater than or equal to 80	
Unknown: 0	Informational: 0	RED: Score is greater than or equal to 0	
Fixed: 0	Total: 42		

The 'System Information' section is also visible at the bottom of the report.

SCC Report Viewer [C:\Users\client2\SCC\Sessions\2024-04-20\_103132\Results\SCAP\GUEST\_SCC-5.9\_2024-04-20\_103132\_All-Set...

Navigation: Back Forward Reload

Search: find in report ☐ Match Case ☐ Whole Words 0 of 0

## Manual Checks

# Results: Medium Severity (CAT II)

### Automated Checks

- o V-221558 - Firewall traversal from remote host must be disabled. - Fail
- o V-221559 - Site tracking users location must be disabled. - Fail
- o V-221561 - Sites ability to show pop-ups must be disabled. - Fail
- o V-221562 - Extensions installation must be blocklisted by default. - Fail
- o V-221563 - Extensions that are approved for use must be allowlisted. - Fail
- o V-221564 - The default search providers name must be set. - Fail
- o V-221565 - The default search provider URL must be set to perform encrypted searches. - Fail
- o V-221566 - Default search provider must be enabled. - Fail
- o V-221567 - The Password Manager must be disabled. - Fail
- o V-221570 - Background processing must be disabled. - Fail
- o V-221571 - Google Data Synchronization must be disabled. - Fail
- o V-221572 - The URL protocol schema javascript must be disabled. - Fail
- o V-221573 - Cloud print sharing must be disabled. - Fail
- o V-221574 - Network prediction must be disabled. - Fail
- o V-221575 - Metrics reporting to Google must be disabled. - Fail
- o V-221576 - Search suggestions must be disabled. - Fail
- o V-221577 - Importing of saved passwords must be disabled. - Fail
- o V-221578 - Incognito mode must be disabled. - Fail
- o V-221579 - Online revocation checks must be performed. - Fail
- o V-221580 - Safe Browsing must be enabled. - Fail
- o V-221581 - Browser history must be saved. - Fail
- o V-221586 - Deletion of browser history must be disabled. - Fail
- o V-221587 - Prompt for download location must be enabled. - Fail
- o V-221588 - Download restrictions must be configured. - Fail
- o V-221590 - Safe Browsing Extended Reporting must be disabled. - Fail
- o V-221591 - WebUSB must be disabled. - Fail
- o V-221592 - Chrome Cleanup must be disabled. - Fail

1) **V-221558 - Firewall traversal from remote host must be disabled - Fail** : Click on the failed scan to see detailed information about it. It will carry you to the other part of report, here find the “**Fix Text**” option and read it.

SCC Report Viewer [C:\Users\client2\SCC\Sessions\2024-04-20\_103132\Results\SCAP\GUEST\_SCC-5.9\_2024-04-20\_103132\_All-Set...

Navigation: Back Forward Reload

Search: find in report ☐ Match Case ☐ Whole Words 0 of 0

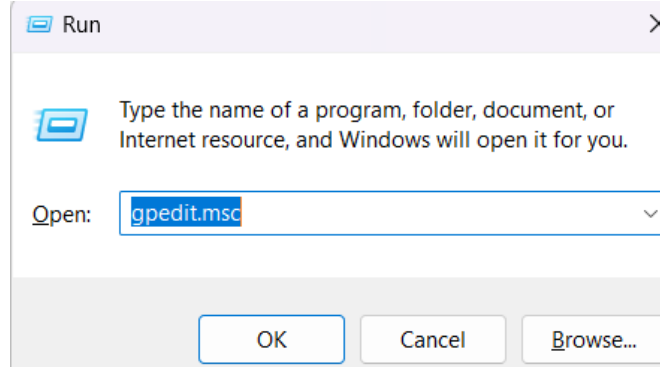
### V-221558 - Firewall traversal from remote host must be disabled.

Rule ID:	xccdf_mil.disa.stig_rule_SV-221558r879534_rule
Test Type:	Automated
Result:	Fail
Version:	DTBC-0001
Identities:	<a href="#">SV-57545</a> <a href="#">V-44711</a> <a href="#">CCI-001414 (NIST SP 800-53: AC-4; NIST SP 800-53A: AC-4.1 (iii); NIST SP 800-53 Rev 4: AC-4; NIST SP 800-53 Rev 5: AC-4)</a>
Description:	Remote connections should never be allowed that bypass the firewall, as there is no way to verify if they can be trusted. Enables usage of STUN and relay servers when remote clients are trying to establish a connection to this machine. If this setting is enabled, then remote clients can discover and connect to this machine even if they are separated by a firewall. If this setting is disabled and outgoing UDP connections are filtered by the firewall, then this machine will only allow connections from client machines within the local network. If this policy is left not set the setting will be enabled.
Fix Text:	Windows group policy: 1. Open the group policy editor tool with gpedit.msc 2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Remote Access Policy Name: Enable firewall traversal from remote access host Policy State: Disabled Policy Value: N/A
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Google Chrome Current Windows Publisher: DISA Type: DPMS Target Subject: Google Chrome Current Windows Identifier: 4081

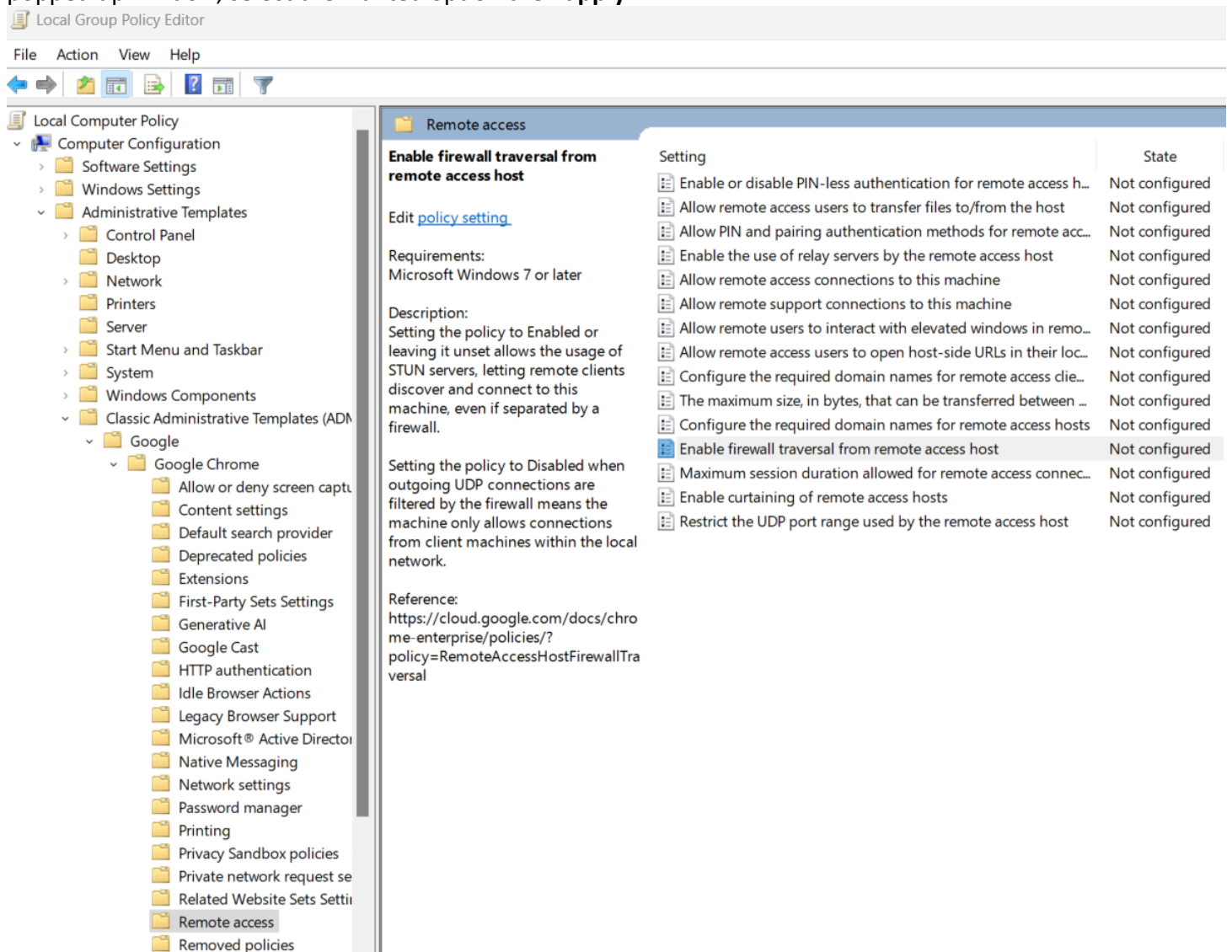
Fortunately this tool provide us with remediation steps to solve the misconfiguration problem. In the **“Fix Text”** section follow the given steps.

Fix Text:	Windows group policy: 1. Open the group policy editor tool with gpedit.msc 2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Remote Access Policy Name: Enable firewall traversal from remote access host Policy State: Disabled
-----------	---

Press **Windows+R** keys and type **gpedit.msc** to open the “**Local Group Policy Editor**” window.



In the opening window find the policy given in the second step of “**Fix Text**” and double click on it and in the popped up window, select the wanted option then **apply**.



Enable firewall traversal from remote access host

Previous Setting Next Setting

☐ Not Configured Comment:

☐ Enabled

☒ Disabled Supported on: Microsoft Windows 7 or later

Options:

Help:

Setting the policy to Enabled or leaving it unset allows the usage of STUN servers, letting remote clients discover and connect to this machine, even if separated by a firewall.

Setting the policy to Disabled when outgoing UDP connections are filtered by the firewall means the machine only allows connections from client machines within the local network.

Reference: <https://cloud.google.com/docs/chrome-enterprise/policies/?policy=RemoteAccessHostFirewallTraversal>

OK Cancel Apply

## 2) V-221559 - Site tracking users location must be disabled:

SCC Report Viewer [C:\Users\client2\SCC\Sessions\2024-04-20\_103132\Results\SCAP\GUEST\_SCC-5.9\_2024-04-20\_103132\_All-Set...

Navigation Back Forward Reload Search find in report Match Case Whole Words 0 of 0

### V-221559 - Site tracking users location must be disabled.

Rule ID:	xccdf_mil.disa.stig_rule_SV-221559r879627_rule
Test Type:	Automated
Result:	Fail
Version:	DTBC-0002
Identities:	<a href="#">SV-57557</a> <a href="#">V-44723</a> <a href="#">CCI-001166 (NIST SP 800-53: SC-18 (1); NIST SP 800-53A: SC-18 (1) 1 (i); NIST SP 800-53 Rev 4: SC-18 (1); NIST SP 800-53 Rev 5: SC-18 (1))</a>
Description:	<p>Website tracking is the practice of gathering information as to which websites were accessed by a browser. The common method of doing this is to have a website create a tracking cookie on the browser. If the information of what sites are being accessed is made available to unauthorized persons, this violates confidentiality requirements, and over time poses a significant OPSEC issue. This policy setting allows you to set whether websites are allowed to track the user's physical location. Tracking the user's physical location can be allowed by default, denied by default or the user can be asked every time a website requests the physical location.</p> <p>1 = Allow sites to track the user's physical location 2 = Do not allow any site to track the user's physical location 3 = Ask whenever a site wants to track the user's physical location</p>
Fix Text:	<p>Windows group policy:</p> <ol style="list-style-type: none"><li>1. Open the group policy editor tool with gpedit.msc</li><li>2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\</li></ol> <p>Policy Name: Default geolocation setting Policy State: Enabled Policy Value: Do not allow any site to track the users' physical location</p>
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Google Chrome Current Windows

Local Group Policy Editor

File Action View Help

Local Computer Policy

- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
    - Desktop
    - Network
    - Printers
    - Server
    - Start Menu and Taskbar
    - System
    - Windows Components
    - Classic Administrative Templates (AD)
      - Google
        - Google Chrome
          - Allow or deny screen capt
          - Content settings

Content settings

**Default geolocation setting**

Edit [policy setting](#).

Requirements:  
Microsoft Windows 7 or later

Description:  
Setting the policy to 1 lets sites track the users' physical location as the default state. Setting the policy to 2 denies this tracking by default. You can set the policy to ask whenever a site wants to track the users' physical location.

Leaving the policy unset means the AskGeolocation policy applies, but users can change this setting.

Setting	State
Automatically select client certificates for these sites	Not configured
Allow automatic fullscreen on these sites	Not configured
Block automatic fullscreen on these sites	Not configured
Allow clipboard on these sites	Not configured
Block clipboard on these sites	Not configured
Allow cookies on these sites	Not configured
Block cookies on these sites	Not configured
Limit cookies from matching URLs to the current session	Not configured
Data URL support for SVGUseElement.	Not configured
Default clipboard setting	Not configured
Default cookies setting	Not configured
Control use of the File System API for reading	Not configured
Control use of the File System API for writing	Not configured
<b>Default geolocation setting</b>	<b>Not configured</b>
Default images setting	Not configured

Default geolocation setting

Default geolocation setting

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on: Microsoft Windows 7 or later

Options:

Default geolocation setting

Do not allow any site to track the users' physical location

Help:

Setting the policy to 1 lets sites track the users' physical location as the default state. Setting the policy to 2 denies this tracking by default. You can set the policy to ask whenever a site wants to track the users' physical location.

Leaving the policy unset means the AskGeolocation policy applies, but users can change this setting.

Reference: <https://cloud.google.com/docs/chrome-enterprise/policies/?policy=DefaultGeolocationSetting>

OK Cancel Apply



3) V-221561 - Sites ability to show pop-ups must be disabled:

SCC Report Viewer [C:\Users\client2\SCC\Sessions\2024-04-20\_103132\Results\SCAP\GUEST\_SCC-5.9\_2024-04-20\_103132\_All-Set...

Navigation: Back Forward Reload Search: find in report Match Case Whole Words 0 of 0

### V-221561 - Sites ability to show pop-ups must be disabled.

Rule ID:	xccdf_mil.disa.stig_rule_SV-221561r879587_rule
Test Type:	Automated
Result:	Fail
Version:	DTBC-0004
Identities:	<a href="#">SV-57553</a> <a href="#">V-44719</a> <a href="#">CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a)</a>
Description:	<p>Chrome allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. If you enable this policy setting, most unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you disable this policy setting, scripts can continue to create pop-up windows, and pop-ups that hide other windows. Recommend configuring this setting to '2' to help prevent malicious websites from controlling the pop-up windows or fooling users into clicking on the wrong window. If you do not configure this policy setting, most unwanted pop-up windows are prevented from appearing. If this policy is left not set, 'BlockPopups' will be used and the user will be able to change it.</p> <p>1 = Allow all sites to show pop-ups 2 = Do not allow any site to show pop-ups</p>
Fix Text:	<p>Windows group policy: 1. Open the group policy editor tool with gpedit.msc 2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\ Policy Name: Default popups setting Policy State: Enabled Policy Value: Do not allow any site to show popups</p>
Severity:	medium
Weight:	10.0

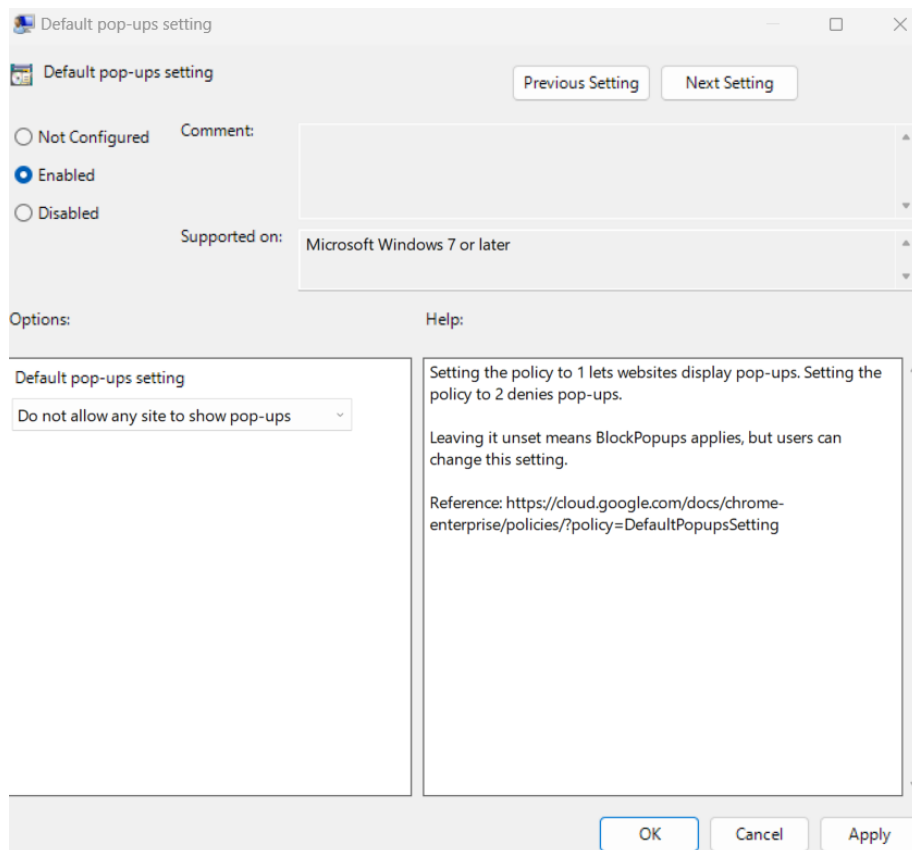
Local Group Policy Editor

File Action View Help

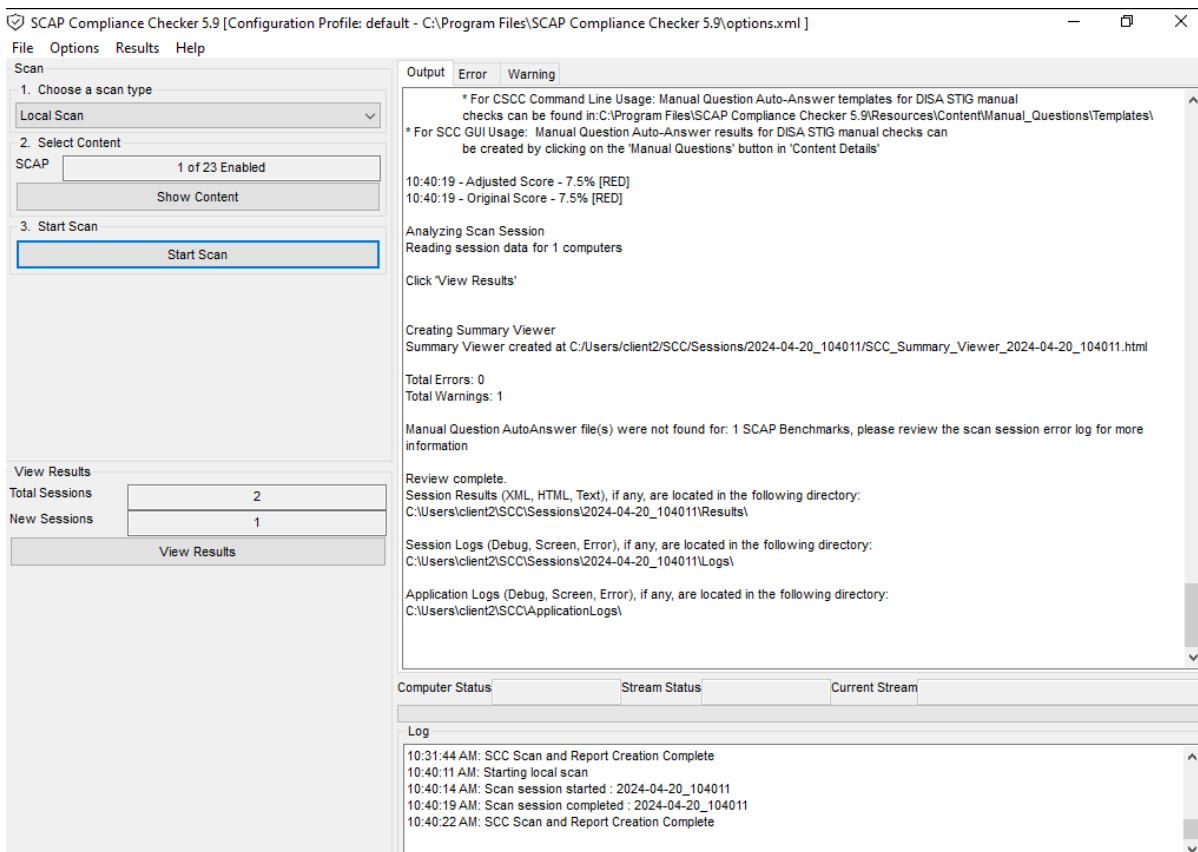
Content settings

Setting	State
Block cookies on these sites	Not configured
Limit cookies from matching URLs to the current session	Not configured
Data URL support for SVGUseElement.	Not configured
Default clipboard setting	Not configured
Default cookies setting	Not configured
Control use of the File System API for reading	Not configured
Control use of the File System API for writing	Not configured
Default geolocation setting	Enabled
Default images setting	Not configured
Control use of insecure content exceptions	Not configured
Control use of JavaScript JIT	Not configured
Default JavaScript setting	Not configured
Default Local Fonts permission setting	Not configured
Default notification setting	Not configured
Default pop-ups setting	Not configured





After changing policy configurations, we should scan it again in order to check if our mitigation steps were successful or not. You can see that the **“Total Sessions”** number is 2, which means we scanned twice. Press the **“View Results”** button to see the new report.



Filter by session, hostname or content...											
Sessions											
Scan Session	Status	Directory	Files	Size (MB)	Hosts	Content	Errors	Warnings	Ave %	Max %	Min %
2024-04-20_104011	* new *	C:/Users/client2/SCC/Sessions/2024-04-20_104011/	9	1.39	1	1	0	1	7.5	7.5	7.5
2024-04-20_103132		C:/Users/client2/SCC/Sessions/2024-04-20_103132/	9	1.4	1	1	0	1	0	0	0

Results					Reports XML Checklist Logs			
Host Name	Content	Score	Errors	War...	Report Type	Format	Filename	Size (MB)
GUEST	Google_Chrom...rrent_Windows	7.5	0	1	All Settings	HTML	Results/SCAP/GUEST_SCC-5.9_2024-04-20_...ogle_Chrome_Current_Windows-2.9.7.html	0.25
					Non-Compliance	HTML	Results/SCAP/GUEST_SCC-5.9_2024-04-20_...ogle_Chrome_Current_Windows-2.9.7.html	0.22

When you open the new report, you will see that the **Score** had been changed after mitigation steps. In this example my score rose up to 7.5%, which means my system is more secure than the former one.

SCC Report Viewer [C:\Users\client2\SCC\Sessions\2024-04-20\_104011\Results\SCAP\GUEST\_SCC-5.9\_2024-04-20\_104011\_All-Set...

Navigation: Back Forward Reload Search: find in report 0 of 0

## All Settings Report - Google Chrome Current Windows STIG SCAP Benchmark - NIWC Enhanced with Manual Questions

SCAP Compliance Checker - 5.9

Score | System Information | Content Information | Results | Detailed Results

### Score

**7.5%**

Adjusted Score: 7.5%  
Original Score: 7.5%  
Compliance Status: RED

Pass: 3	Not Applicable: 0	BLUE: Score equals 100
Fail: 37	Not Checked: 2	GREEN: Score is greater than or equal to 90
Error: 0	Not Selected: 0	YELLOW: Score is greater than or equal to 80
Unknown: 0	Informational: 0	RED: Score is greater than or equal to 0
Fixed: 0	Total: 42	

Below we can see that the first three misconfigurations are solved properly.

SCC Report Viewer [C:\Users\client2\SCC\Sessions\2024-04-20\_104011\Results\SCAP\GUEST\_SCC-5.9\_2024-04-20\_104011\_All-Set...

Navigation: Back Forward Reload

Search: find in report ☐ Match Case ☐ Whole Words 0 of 0

## Results: Medium Severity (CAT II)

### Automated Checks

- o V-221558 - Firewall traversal from remote host must be disabled. - Pass
- o V-221559 - Site tracking users location must be disabled. - Pass
- o V-221561 - Sites ability to show pop-ups must be disabled. - Pass
- o V-221562 - Extensions installation must be blocklisted by default. - Fail
- o V-221563 - Extensions that are approved for use must be allowlisted. - Fail
- o V-221564 - The default search providers name must be set. - Fail
- o V-221565 - The default search provider URL must be set to perform encrypted searches. - Fail
- o V-221566 - Default search provider must be enabled. - Fail
- o V-221567 - The Password Manager must be disabled. - Fail
- o V-221570 - Background processing must be disabled. - Fail
- o V-221571 - Google Data Synchronization must be disabled. - Fail
- o V-221572 - The URL protocol schema javascript must be disabled. - Fail
- o V-221573 - Cloud print sharing must be disabled. - Fail
- o V-221574 - Network prediction must be disabled. - Fail
- o V-221575 - Metrics reporting to Google must be disabled. - Fail
- o V-221576 - Search suggestions must be disabled. - Fail
- o V-221577 - Importing of saved passwords must be disabled. - Fail
- o V-221578 - Incognito mode must be disabled. - Fail
- o V-221579 - Online revocation checks must be performed. - Fail
- o V-221580 - Safe Browsing must be enabled. - Fail
- o V-221581 - Browser history must be saved. - Fail
- o V-221586 - Deletion of browser history must be disabled. - Fail
- o V-221587 - Prompt for download location must be enabled. - Fail
- o V-221588 - Download restrictions must be configured. - Fail
- o V-221590 - Safe Browsing Extended Reporting must be disabled. - Fail
- o V-221591 - WebUSB must be disabled. - Fail
- o V-221592 - Chrome Cleanup must be disabled. - Fail
- o V-221593 - Chrome Cleanup reporting must be disabled. - Fail
- o V-221594 - Google Cast must be disabled. - Fail
- o V-221595 - Autoplay must be disabled. - Fail
- o V-221597 - Anonymized data collection must be disabled. - Fail