

Nessus 6.1 SCAP Assessments

November 18, 2014

(Revision 1)

Table of Contents

- Overview.....3**
 - Standards and Conventions.....3
 - Abbreviations.....3
 - Simple Assessment Procedure.....3
 - XCCDF Certified vs. Lower-Tier Content.....4
- Operation.....4**
 - Downloading SCAP XCCDF Content.....4
- Working with Nessus.....5**
 - Loading SCAP Content into Nessus.....5
 - Analyzing Scan Results.....9
 - Technical Issues.....12
 - Exporting Scan Results.....12
 - Troubleshooting.....14
- About Tenable Network Security.....15**

Overview

This document describes how to use Tenable's Nessus to generate SCAP content audits as well as view and export the scan results.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in **courier** (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd  
/opt/sc4/daemons  
#
```



Important notes and considerations are highlighted with this symbol and grey text boxes.



Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Abbreviations

The following abbreviations are used throughout this documentation:

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerability Enumeration
NIST	National Institute of Standards and Technology
OVAL	Open Vulnerability and Assessment Language
SCAP	Security Content Automation Protocol
USGCB	United States Government Configuration Baseline
XCCDF	Extensible Configuration Checklist Description Format

Simple Assessment Procedure

To perform a certified SCAP assessment, follow these high-level steps:

1. Download certified [NIST SCAP content](#) in its zip file format. Note that the entire zip file must be obtained for use with Nessus.
2. Create a scan or policy using Nessus' SCAP Compliance Audit library template. Add a scan name, target(s), and credentials for the target system(s).

3. Upload the SCAP content zip file to the Nessus scan or policy in the appropriate Active SCAP Components section under “SCAP File (zip)”. From the SCAP XML file, select the appropriate data stream, benchmark, and profile to be used in the desired audit.
4. Perform a vulnerability scan based on the selected scan or policy.
5. When the scan is completed, view the results within Nessus’ “Scans” section.

Each of these steps is documented in detail later in this document.

XCCDF Certified vs. Lower-Tier Content

Tenable designed Nessus 5.2 and higher to work with the official [XCCDF Tier IV content](#) used in the SCAP program. Beta quality XCCDF-compliant content (Tier 3 and below) is also available from NIST. Tier definitions are listed below:

- IV – Will work in any SCAP validated tool
- III – May work in any SCAP validated tool
- II – Non-SCAP automation content
- I – Non-automated prose content

Operation



Performing SCAP assessments as described in this document requires Nessus 5.2 or higher utilizing the HTML5 web interface. For information about performing SCAP assessments using Tenable’s SecurityCenter, refer to the “[SecurityCenter 4.7 SCAP Assessments and CyberScope Reporting](#)” document.

Downloading SCAP XCCDF Content

Nessus users can obtain the various SCAP bundles at <http://web.nvd.nist.gov/view/ncp/repository>. Bundles can be downloaded collectively as a single .zip archive depending on the platform to be assessed and the version of SCAP and OVAL desired to be used in an assessment. SCAP content uses the following archive file naming convention:

`<platform>-<OVAL version number>-<SCAP content version number>.zip`

For example, if the file name is WinXP-53-2.0.1.0.zip, the “53” in the file name indicates OVAL version 5.3.

Download the file for OVAL version 5.3. When this file is unzipped, multiple files relating to the specific platform are extracted:

Name	Type	Compressed size	Password p...
USGCB-Windows-XP-cpe-dictionary	XML Document	1 KB	No
USGCB-Windows-XP-cpe-oval	XML Document	2 KB	No
USGCB-Windows-XP-oval	XML Document	47 KB	No
USGCB-Windows-XP-patches	XML Document	150 KB	No
USGCB-Windows-XP-xccdf	XML Document	79 KB	No

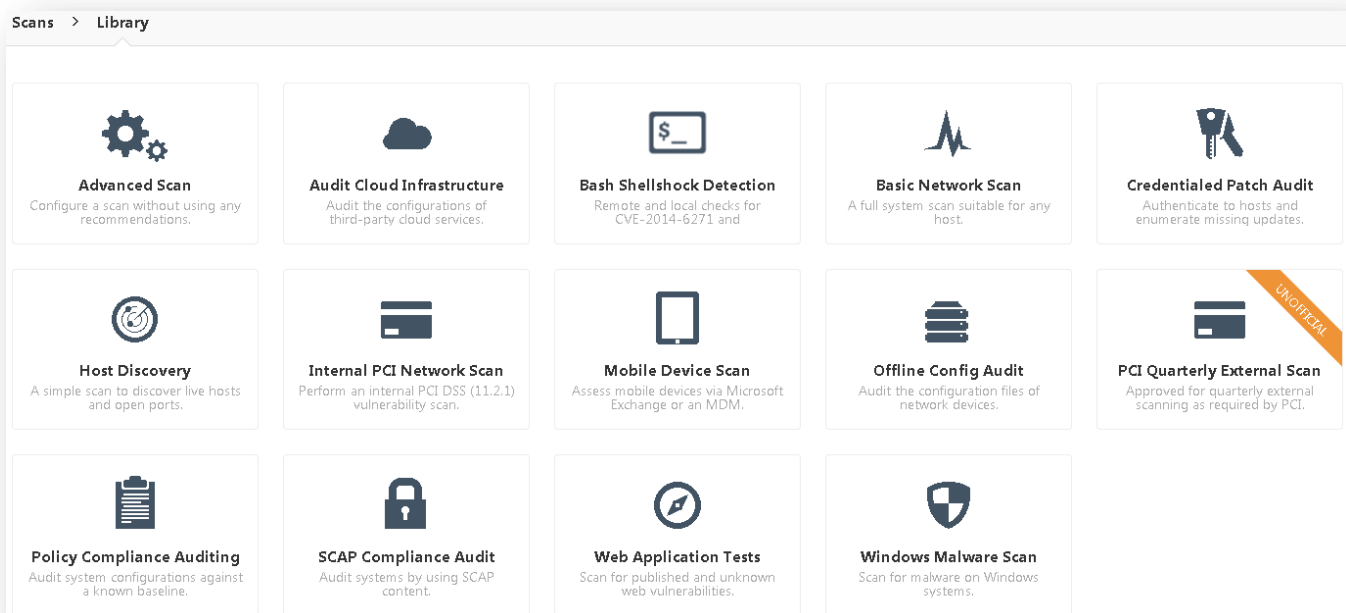
SCAP Content Supporting Files

The following sections describe how to load these files into Nessus and generate audit policies that can be used for SCAP assessments.

Working with Nessus

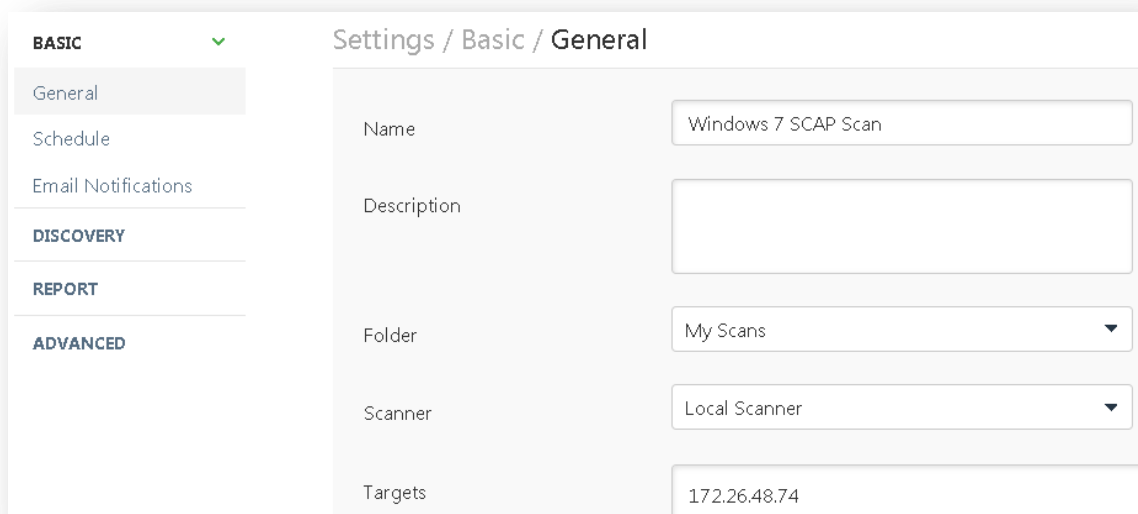
Loading SCAP Content into Nessus

To load XCCDF content into Nessus, navigate to “**Scans**” and select “**New Scan**” in Nessus. Next, select “**SCAP Compliance Audit**”:



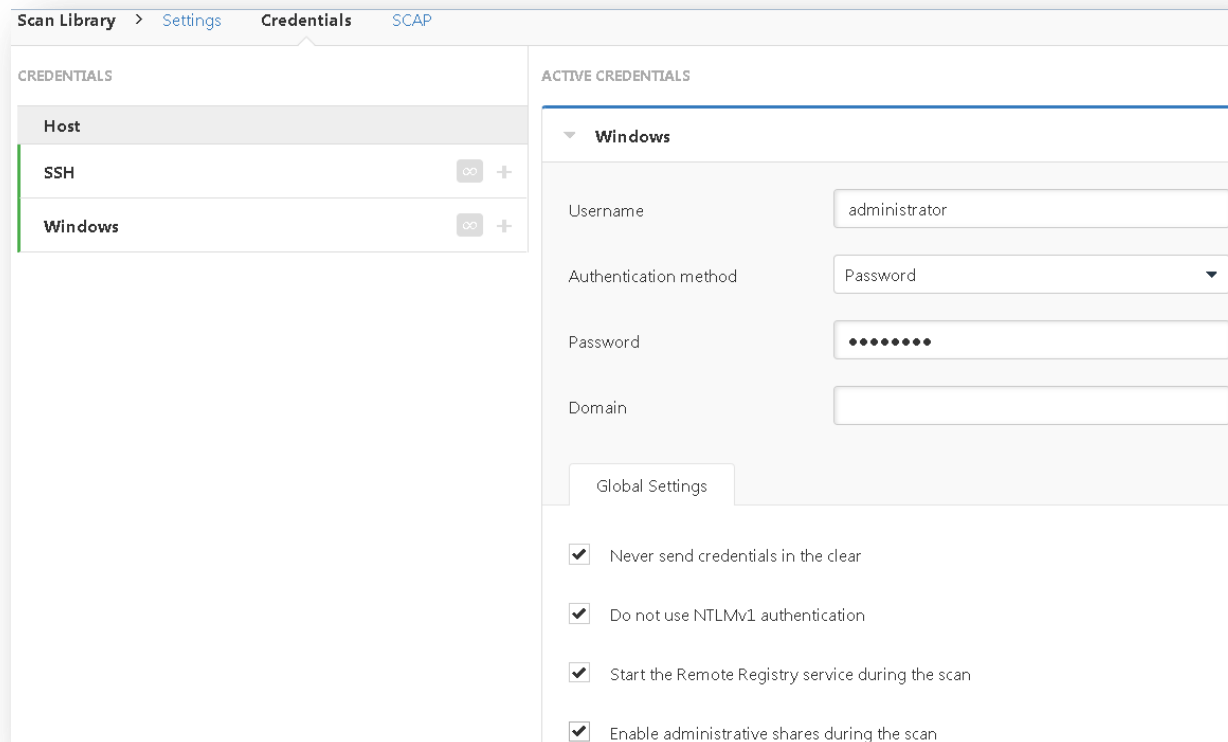
“New Scan” Screen Selection

Under “Settings”, select “Basic” and “General”. Name the scan and provide a description for the scan, if desired. Enter the target IP address or range in the box next to “Targets”:



Settings / Basic / General	
Name	Windows 7 SCAP Scan
Description	
Folder	My Scans
Scanner	Local Scanner
Targets	172.26.48.74

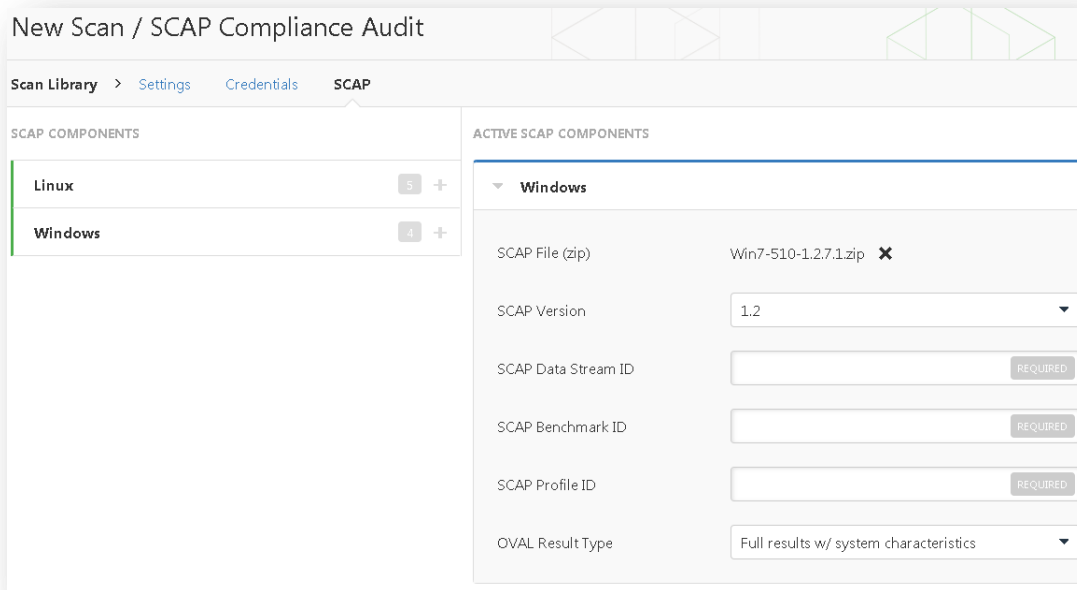
Next, under “Credentials”, enter an account/username and password for the target system to be scanned. Note that the credentials used must have administrator/root level access to the target system:



ACTIVE CREDENTIALS	
Windows	
Username	administrator
Authentication method	Password
Password	••••••••
Domain	
Global Settings	
<input checked="" type="checkbox"/>	Never send credentials in the clear
<input checked="" type="checkbox"/>	Do not use NTLMv1 authentication
<input checked="" type="checkbox"/>	Start the Remote Registry service during the scan
<input checked="" type="checkbox"/>	Enable administrative shares during the scan

For scanning Windows systems, select “**Start the Remote Registry service during the scan**” to ensure that the scan target’s registry can be accessed during a SCAP compliance scan. In addition, “**Enable administrative shares during the scan**” must be enabled to allow Nessus to access Windows’ administrative shares during a SCAP compliance scan.

Under “**SCAP**”, select the “+” next to the scan target’s operating system type to add a SCAP component. Next, click “**Add File**” to upload a valid SCAP content file from the local system:



When processing SCAP 1.2 content, there cannot be more than one XML file in the SCAP content zip file. If more than one XML file exists in a zip file, extract the specific XML file to be used for the SCAP compliance scan, create a zip file from the single XML file, and upload the new zip file to Nessus.

Select the SCAP Version that is appropriate for the SCAP file (1.0, 1.1, or 1.2). The Data Stream ID (SCAP 1.2 only), Benchmark ID and Profile ID need to be extracted by opening the SCAP XML files in a text editor and copying them into the above preferences. Note that for SCAP 1.0/1.1 the Data Stream ID is blank (since it is not required and is not available in the XML files):

```
<?xml version="1.0" encoding="UTF-8"><data-stream-collection xmlns="http://scap.nist.gov/schema/scap/source/1.2" xmlns:cat="urn:oasis:names:tc:entity:xmlns:xml:catalog" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="scap.gov.nist.collection_USGCB-Windows-7-1.2.3.1.zip" schematron-version="1.0" xsi:schemaLocation="http://scap.nist.gov/schema/scap/source/1.2 http://scap.nist.gov/schema/scap/1.2/scap-source-data-stream_1.2.xsd">
  <data-stream id="scap.gov.nist.datastream_USGCB-Windows-7-1.2.3.1.zip" scap-version="1.2" timestamp="2012-02-24T10:00:00" use-case="CONFIGURATION">
```

“Data Stream” Selection

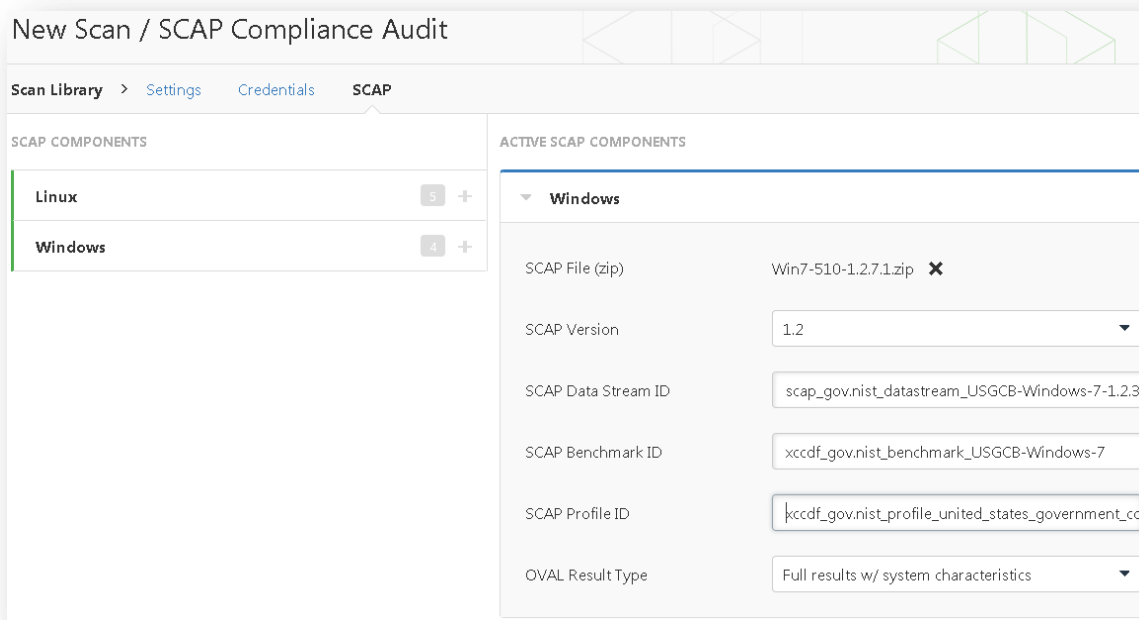
```
<xccdf:Benchmark xmlns:cdf="http://checklists.nist.gov/xccdf/1.1" xmlns:cpe2="http://cpe.mitre.org/language/2.0" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2" xmlns:xhtml="http://www.w3.org/1999/xhtml" id="xccdf.gov.nist.benchmark_USGCB-Windows-7" resolved="0" style="SCAP_1.2" xml:lang="en-US" xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.2 http://scap.nist.gov/schema/xccdf/1.2/xccdf_1.2.xsd http://cpe.mitre.org/dictionary/2.0 http://scap.nist.gov/schema/cpe/2.3/cpe-dictionary_2.3.xsd">
```

“Benchmark” Selection

```
<xccdf:Profile id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1">  
<xccdf:title>United States Government Configuration Baseline 1.2.3.1</xccdf:title>  
<xccdf:description>This profile represents guidance outlined in United States Government Configuration Baseline for desktop systems with  
Microsoft Windows 7 installed.</xccdf:description>
```

“Profile” Selection

After loading the SCAP content and specifying the version, Data Stream, Benchmark ID, and Profile ID, the SCAP Compliance Checks option should appear similar to the screenshot below:

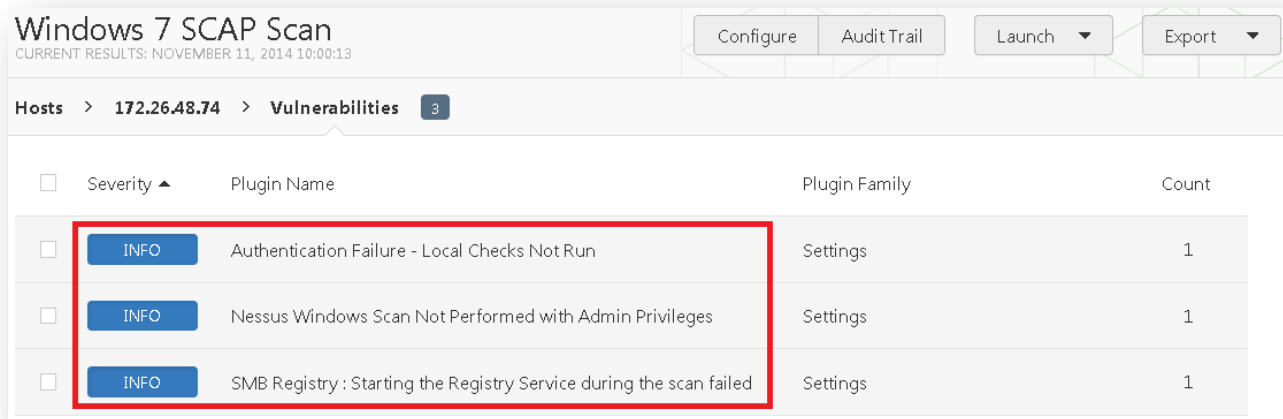


When finished, click “**Save**” to save the scan.

At a minimum, SCAP scans and policies must include the following:

- The specific SCAP content file(s) to be used, as well as the applicable data stream ID (only required for SCAP 1.2), benchmark ID, and profile ID.
- Valid credentials for the target system(s) to be scanned.

The Windows Remote Registry service is crucial to read Windows registry settings specified by XCCDF policies and content. Nessus has the ability to start this service and then turn it off when the audit is done. If there are issues with starting the service during a scan, the scan results will show these findings (highlighted below):



Windows 7 SCAP Scan
CURRENT RESULTS: NOVEMBER 11, 2014 10:00:13

Configure Audit Trail Launch Export

Hosts > 172.26.48.74 > Vulnerabilities 3

<input type="checkbox"/>	Severity ▲	Plugin Name	Plugin Family	Count
<input type="checkbox"/>	INFO	Authentication Failure - Local Checks Not Run	Settings	1
<input type="checkbox"/>	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
<input type="checkbox"/>	INFO	SMB Registry : Starting the Registry Service during the scan failed	Settings	1

In addition to enabling the Windows Remote Registry service, the Windows Management Instrumentation (WMI) service must also be started to enable the scanner to run a successful compliance check against the remote host(s). Please refer to Microsoft’s documentation on starting the WMI service on the Windows host(s) to be scanned.



SCAP compliance audits require sending an executable named “tenable_ovaldi_3ef350e0435440418f7d33232f74f260.exe” to the remote host. For systems that run security software (e.g., McAfee Host Intrusion Prevention), they may block or quarantine the executable required for auditing. For those systems, an exception must be made for either the host or the executable sent.

Analyzing Scan Results

When scans complete, the results will be available in the “Scans” interface.

When selecting a scan result from the “Scans / My Scans” section, four menu items are shown on the left: Hosts, Vulnerabilities, Compliance, and Notes. For the purposes of a SCAP compliance scan, the Compliance section will be the primary focus:

Status	Plugin Name	Plugin Family	Count
FAILED	CCE-10021-4: Audit Policy Change	SCAP Windows Compliance Checks	1
FAILED	CCE-10059-4: Turn on Responder (RSPNDR) driver	SCAP Windows Compliance Checks	1
FAILED	CCE-10061-0: Turn off printing over HTTP	SCAP Windows Compliance Checks	1
FAILED	CCE-10090-9: Do not allow passwords to be saved	SCAP Windows Compliance Checks	1
FAILED	CCE-10103-0: Always prompt client for password upon connection	SCAP Windows Compliance Checks	1
FAILED	CCE-10137-8: Prevent Windows anytime upgrade from running	SCAP Windows Compliance Checks	1
FAILED	CCE-10140-2: Turn off Search Companion content file updates	SCAP Windows Compliance Checks	1
FAILED	CCE-10150-1: Fax Service	SCAP Windows Compliance Checks	1

Scan Details

- Name: Windows 7 SCAP Scan
- Folder: My Scans
- Status: Completed
- Policy: SCAP Compliance Audit
- Scanner: Local Scanner
- Targets: 172.26.48.75
- Start time: November 11, 2014 10:53:16
- End time: November 11, 2014 10:56:03
- Elapsed: 3 minutes

Compliance

- Passed (Green)
- Warning (Yellow)
- Failed (Red)

Nessus Scan Results (Compliance)

Scan results will show “Passed” or “Failed” values for each individual compliance check. Clicking on an individual check displays additional information, including reference information for the plugin used for the check:

FAILED CCE-10103-0: Always prompt client for password upon connection

Description
Always prompt client for password upon connection
The “Always Prompt Client for Password upon Connection” policy should be set correctly for Terminal Services.

Audit File
Win7-510-1.2.7.1.zip

Policy Value
xccdf_gov.nist_rule_always_prompt_for_password_upon_connection: PASSED

Output
xccdf gov.nist rule always prompt for password upon connection: FAILED

Reference Information

- UPDATED-DATE: 2012-02-24T10:00:00
- RULE-ID: xccdf_gov.nist_benchmark_USGCB-Windows-7xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1:xccdf_gov.nist_rule_always_prompt_for_password_upon_connection
- GENERATED-DATE: 2012-02-24T10:00:00
- SCAN-DATE: 2014-11-11T16:53:40
- OVAL-DEF: oval:gov.nist.usgcb.windowsseven:def275
- CCE: CCE-10103-0
- SEVERITY: unknown

Individual Compliance Check Result for a Scanned Host



If a specific check is “notselected”, “notapplicable”, or “notchecked” in the SCAP content used for a scan, those checks are reported as “SKIPPED”.

SCAP XML Results can be viewed under the Vulnerabilities tab:

The screenshot shows the Nessus interface for a "Windows 7 SCAP Scan". The top navigation bar includes "Scans" and "Policies". The main header shows the scan name and current results: "CURRENT RESULTS: NOVEMBER 11, 2014 10:53:16". Below the header, there are buttons for "Configure", "Audit Trail", "Launch", and "Export", along with a search box for "Filter Vulnerabilities". The main content area shows a list of vulnerabilities under the "Vulnerabilities" tab. The table has columns for "Severity", "Plugin Name", "Plugin Family", and "Count". Two entries are visible:

Severity	Plugin Name	Plugin Family	Count
INFO	SCAP Information	Policy Compliance	1
INFO	SCAP XML Results	Policy Compliance	1

On the right side, "Scan Details" are displayed:

- Name: Windows 7 SCAP Scan
- Folder: My Scans
- Status: Completed
- Policy: SCAP Compliance Audit
- Scanner: Local Scanner

Raw XML results are provided in SCAP, XCCDF, and OVAL formats, and are included as attachments within the SCAP XML Results finding:

The screenshot shows the details of the "SCAP XML Results" finding. The "Description" section states: "This script reports SCAP content results including attached ARF, OVAL, and XCCDF results." The "Output" section shows a message: "The SCAP results are attached". Below this, there is a table with columns for "Port" and "Host". The "Host" column shows "xccdf_results_windows_0.xml". To the right, "Plugin Details" are displayed:

- Severity: Info
- ID: 66758
- Version: \$Revision\$
- Type: local
- Family: Policy Compliance
- Published: 2012/07/11

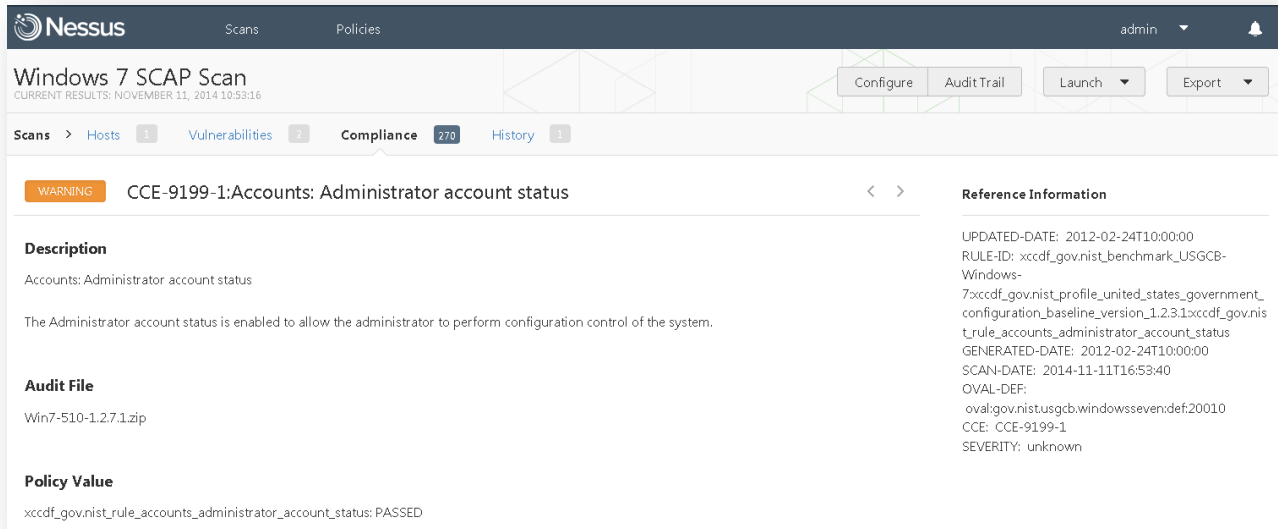
Below the plugin details, "Risk Information" is shown: "Risk Factor: None".

Note that PowerShell checks will not run on the target unless Microsoft .NET Framework 2.0 and Microsoft Visual C++ 2008 redistributable package or Microsoft .NET Framework 4.0 and Microsoft Visual C++ 2010 redistributable package runtime are installed on the target. Additionally, OCIL checks are not supported in Nessus SCAP compliance scans.

Technical Issues

There are several technical issues to be aware of when analyzing the test results:

- The Compliance Check Test Error will show as “ERROR” (and as a “Warning”) if an audit cannot be performed. It will report as “PASSED” if there was an error at one point, but scans have later proceeded without issue.



- Tenable engineered the logic generated by Nessus to perform a “CPE Platform Check”. This check ensures that the host you are scanning for is the correct OS. For example, if you scanned a Windows 2008 platform with a Windows 7 scan or policy, you would get a single result indicating a failure of this check. If this error is reported on a system that has the correct CPE, make sure the remote registry service is running before re-running the scan or use the option “**SMB Registry : Start the Registry Service during the scan**”.
- Xccdf_Scan_Check is a check derived from the XCCDF content that identifies a variety of the parameters used.

Exporting Scan Results

To export your scan results for importing into SecurityCenter or another Nessus instance, choose the “**Nessus**” export format. This provides a `.nessus` file of the report results. The name of the file will be in the format of `<scan_name>_<scan_id>.nessus` where the scan name is the actual scan name used in Nessus. Screen captures of the export process are shown below:

Windows 7 SCAP Scan
CURRENT RESULTS: NOVEMBER 11, 2014 10:53:16

Configure Audit Trail Launch Export Filter Compliance

Scans > Hosts 1 Vulnerabilities 2 Compliance 270 History 1

Status	Plugin Name	Plugin Family	Count
FAILED	CCE-10021-4: Audit Policy Change	SCAP Windows Compliance Checks	1
FAILED	CCE-10059-4: Turn on Responder (RSPNDR) driver	SCAP Windows Compliance Checks	1
FAILED	CCE-10061-0: Turn off printing over HTTP	SCAP Windows Compliance Checks	1

Scan Details

- Name: Windows 7 SCAP Scan
- Folder: My Scans
- Status: Completed
- Policy: SCAP Compliance Audit
- Scanner: Local Scanner

Opening Windows_7_SCAP_Scan_1mq6x.nessus

You have chosen to open:

- Windows_7_SCAP_Scan_1mq6x.nessus**
which is: nessus File (61.4 KB)
from: https://172.26.34.49:8834

What should Firefox do with this file?

Open with

Save File

Do this automatically for files like this from now on.

OK Cancel

Exporting Nessus Scan Results

This data can be used by many of the dashboards and reports that are available in Tenable's SecurityCenter, such as the one below that maps NIST SP 800-53 values to actual CCE settings. Below is a screenshot of the corresponding dashboard based on USGCB XCCDF content after scanning a single Windows 7 host:

SCAP Audit Summary - Top 25 Linux Compliance Failed Checks

Plugin ID	Name	Severity	Total
1003887	CCE-18031-5:ipsec_tools_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configurati...	High	1
10038...	CCE-17504-2:irda_tools_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configurati...	High	1
10038...	CCE-18200-6:talk_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configurati...	High	1
10038...	CCE-17250-2:pam_ccreds_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configurati...	High	1
10038...	CCE-17742-8:usgcb-rhel5desktop-rule-2.6.1.0:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government...	High	1
1003881	CCE-15018-5:postfix_network_listening:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_config...	High	1
10038...	CCE-14068-1:postfix_package_installation:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_co...	High	1
10038...	CCE-14495-6:sendmail_package_installation:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government...	High	1
1003878	CCE-14825-4:isdn4k_utils_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configura...	High	1
10038...	CCE-14412-1:noddev_option_on_tmp:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configura...	High	1

SCAP Audit Summary - Compliance Summary

	Systems	Passed	Manual Check	Failed
Windows	1	30%	3%	67%
Linux	1	39%	13%	48%

SCAP Audit Summary - Network Summary

IP Address	Score	Info	Medium	High	Total
10.31.104.0/24	1811	80	7	179	266
172.26.48.0/24	1322	101	34	122	257

SCAP Audit Summary - Top 25 Windows Compliance Failed Checks

Plugin ID	Name	Severity	T...
10046...	CCE-14830-4:SV-25139r1_rule:Windows_7_STIG_1MAC-1_Public	High	1
10046...	CCE-14109-3:SV-25138r1_rule:Windows_7_STIG_1MAC-1_Public	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) must be installed on the system.VMS Target WL...	High	1
10046...	CCE-15041-7:SV-25143r1_rule:Windows_7_STIG_1MAC-1_Public	High	1
10046...	CCE-10777-1:SV-25107r1_rule:Windows_7_STIG_1MAC-1_Public	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomizat...	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) ...	High	1
1004641	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software is not e...	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer must b...	High	1
10046...	noCCE:Local administrator accounts must have their privileged token filtered to prevent elevated privileg...	High	1

SCAP Audit Summary - Top 10 CCE's

CCE ID	Info	Medium	High	Host Total
CCE-10783-1	0	0	1	1
CCE-10865-3	0	0	1	1
CCE-10015-5	0	0	1	1
CCE-10019-4	0	0	1	1
CCE-10061-0	0	0	1	1
CCE-10078-4	0	0	1	1
CCE-10090-8	0	0	1	1
CCE-10083-3	0	0	1	1
CCE-10093-0	0	0	1	1
CCE-10093-1	0	0	1	1

Troubleshooting

If a scan fails to launch correctly, or if a scan does not display results as expected, the scan's audit trail will show what errors were logged during the scan's execution. Click the **"Audit Trail"** button (highlighted below) to display the audit trail:

Windows 7 SCAP Scan
CURRENT RESULTS: NOVEMBER 11, 2014 19:53:16

Buttons: Configure, **Audit Trail**, Launch, Export, Filter Compliance

Scans > Hosts 1 | Vulnerabilities 2 | **Compliance 270** | History 1

Status	Plugin Name	Plugin Family	Count	Scan Details
FAILED	CCE-10021-4:Audit Policy Change	SCAP Windows Compliance Checks	1	Name: Windows 7 SCAP Scan Folder: My Scans Status: Completed Policy: SCAP Compliance Audit Scanner: Local Scanner
FAILED	CCE-10059-4:Turn on Responder (RSPNDR) driver	SCAP Windows Compliance Checks	1	
FAILED	CCE-10061-0:Turn off printing over HTTP	SCAP Windows Compliance Checks	1	

"Audit Trail" Button

Windows 7 SCAP Scan
CURRENT RESULTS: NOVEMBER 11, 2014 11:25:27

Scans > Hosts 1 Vulnerabilities 3 History ?

Authentication Failure - Local Checks Not Run

Description
Local security checks have been disabled for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution
Address the problem(s) so that local security checks are enabled.

Output
- It was not possible to log into the remote host via smb (invalid credentials).

Audit Trail

Plugin ID: 24269
Host: Host (Example: localhost)
Search

Can't connect to the 'root\CIMV2' WMI namespace.

Exit	Hosts
24269/0	172.26.48.75

Audit Trail Results

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data.

Tenable is relied upon by more than 24,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments. We offer customers peace of mind thanks to the largest install base, the best expertise, and the ability to identify their biggest threats and enable them to respond quickly.

For more information, please visit tenable.com.