tenable
network security®

Nessus v6 SCAP Assessments

November 18, 2014

(Revision 1)

Table of Contents

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.
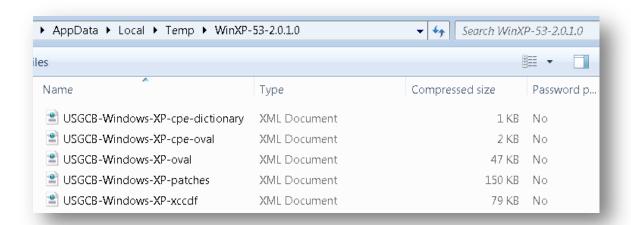
Downloading SCAP XCCDF Content

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:
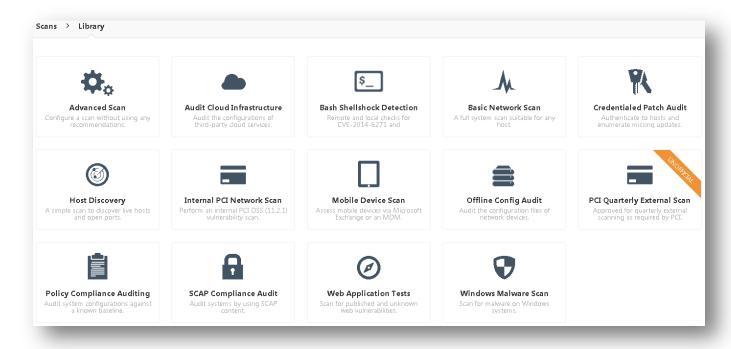
SCAP Content Supporting Files

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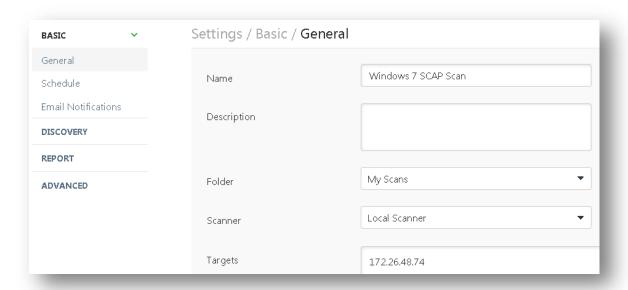
Working with Nessus

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**":
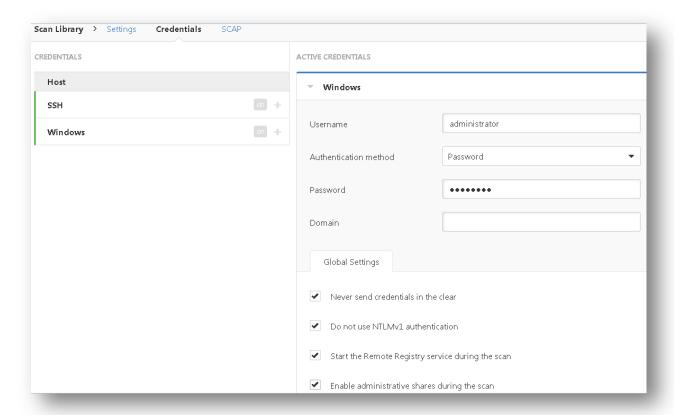

"New Scan" Screen Selection

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**":
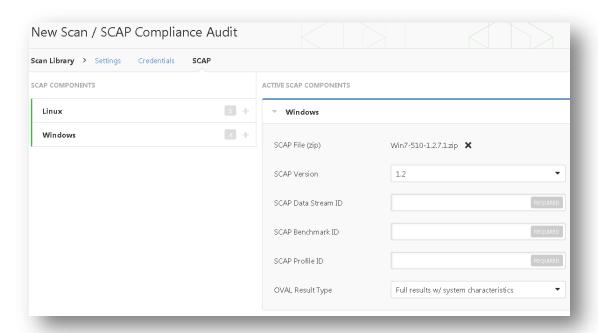

Next, under "**Credentials**", enter an account/username and password for the target system to be scanned. Note that the credentials used must have administrator/root level access to the target system:

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):

"Data Stream" Selection

"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:
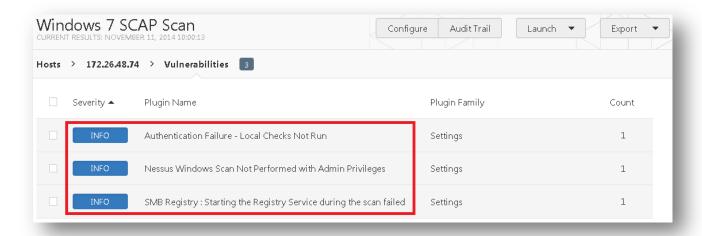

When finished, click "**Save**" to save the scan.

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):

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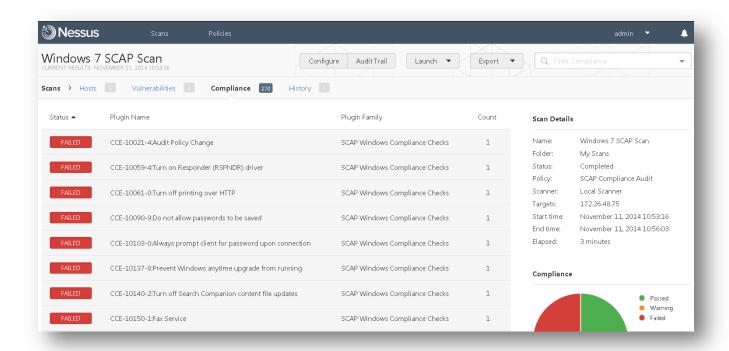
> SCAP compliance audits require sending an executable named "tenable_ovaldi_3ef350e0435440418f7d33232f74f260.exe" to the remote host. For systems that run security software (e.g., McAfee Host Intrusion Prevention), they may block or quarantine the executable required for auditing. For those systems,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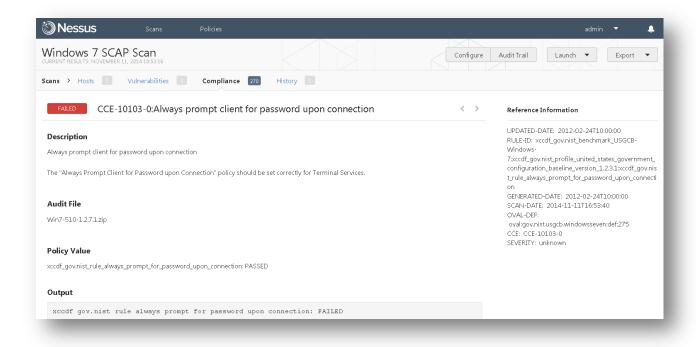
Analyzing Scan Results

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:

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:
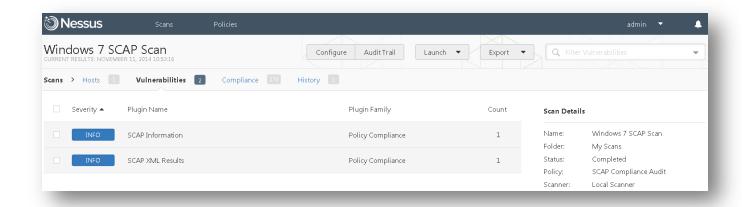

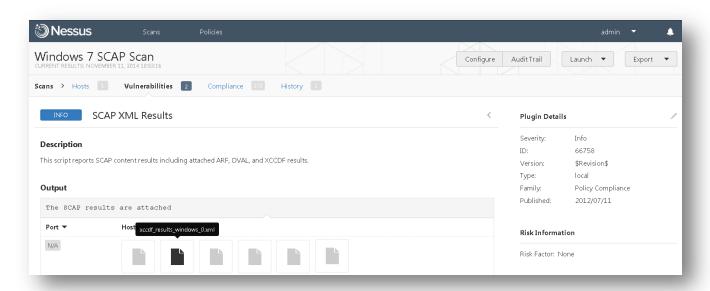
Individual Compliance Check Result for a Scanned Host

> ⚠ 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:

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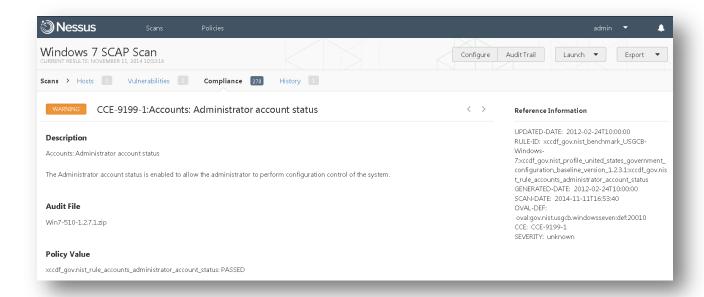

Note that PowerShell checks will not run on the target unless Microsoft .NET Framework 2.0 and Microsoft Visual C++ 2008 redistributable package or Microsoft .NET Framework 4.0 and Microsoft Visual C++ 2010 redistributable package runtime are installed on the target. Additionally, OCIL checks are not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

Technical Issues

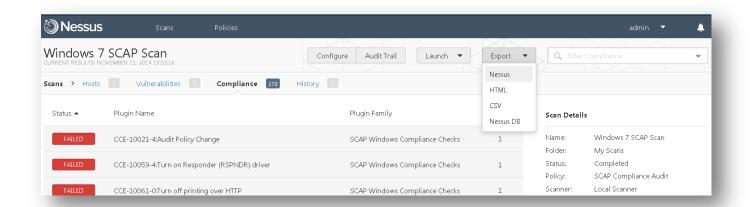There are several technical issues to be aware of when analyzing the test results:

- 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.
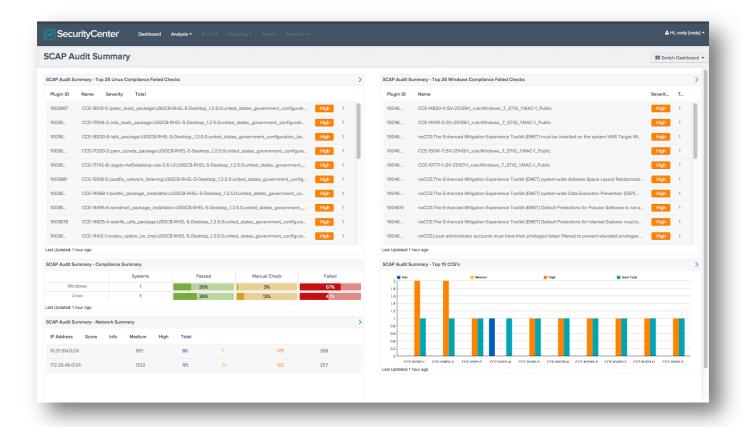
Exporting Scan Results

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:
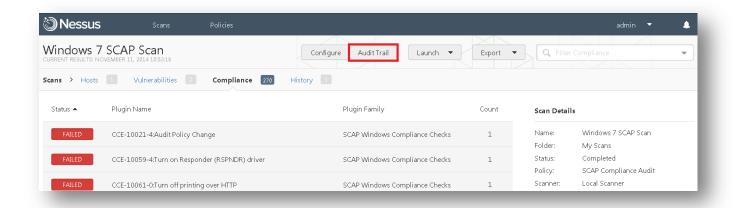
Exporting Nessus Scan Results

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:
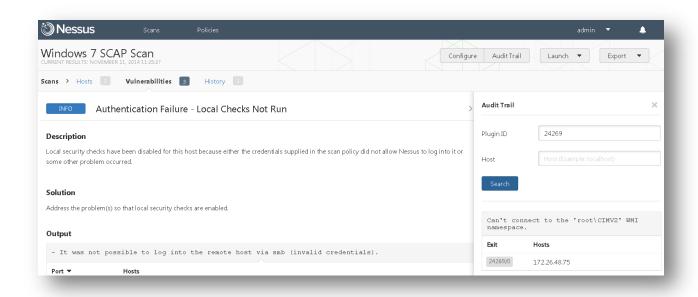

Troubleshooting

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:

"Audit Trail" Button

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.