Tenable SCAP Standards Declarations

May 29, 2015

(Revision 11)

Table of Contents

[Center for Internet Security (CIS) 3](#_Toc420673284)

[Common Criteria (NIAP) 3](#_Toc420673285)

[Common Vulnerability Enumeration (CVE) 3](#_Toc420673286)

[Common Configuration Enumeration (CCE) 4](#_Toc420673287)

[Common Platform Enumeration (CPE) 4](#_Toc420673288)

[Common Vulnerability Scoring System (CVSS) 4](#_Toc420673289)

[Extensible Configuration Checklist Document Format (XCCDF) 4](#_Toc420673290)

[Open Vulnerability Assessment Language (OVAL) 5](#_Toc420673291)

[Asset Identification 5](#_Toc420673292)

[Asset Reporting Format (ARF) 5](#_Toc420673293)

[SCAP Implementation 5](#_Toc420673294)

[About Tenable Network Security 6](#_Toc420673295)

# Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a non-profit organization that provides consensus best practice standards for security configuration for a variety of platforms and applications. The CIS benchmarks are defined through a consensus of user organizations, security professionals, auditors and software vendors.

Tenable Network Security is a member of the Center for Internet Security (CIS) and develops configuration assessment technologies for Nessus and SecurityCenter to implement audits that test for best practice settings based on the CIS benchmarks. These technologies are submitted to CIS for certification and CIS then validates Tenable’s ability to test for correct and incorrect settings across a wide variety of applications and operating systems.

# Common Criteria (NIAP)

The National Information Assurance Project (NIAP) is a U.S. Government initiative between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIAP sponsors a variety of projects and activities, including the Common Criteria Evaluation and Validation Scheme (CCEVS). The Common Criteria is a standard for evaluation of security measures in a given product. Many government agencies require that products deployed into their environments be evaluated under the Common Criteria process.

Tenable is Common Criteria (CC) certified at Evaluation Assurance Level Two (EAL2) Augmented with ALC\_FLR.2 for the SecurityCenter 4.4, Nessus 5.0.1, Passive Vulnerability Scanner (PVS) 3.6, Log Correlation Engine (LCE) 3.6, 3D Tool 2.0.1, and xTool 2.1 products. The Target Of Evaluation (TOE) includes all the components that comprise a full deployment of the SecurityCenter suite.

# Common Vulnerability Enumeration (CVE)

Tenable Network Security uses Common Vulnerability Enumeration (CVE) nomenclature for many different processes accomplished by the SecurityCenter, including the following:

* All vulnerabilities identified by Tenable’s research group for the Nessus vulnerability scanner or the Passive Vulnerability Scanner have relevant CVE entries, if available.
* Tenable has a public web interface that can be used to search plugins by associated CVE entries. Newly released CVE entries are added several times a week and updates to older CVE entries are frequently made.
* Any vulnerability displayed in the “Detailed Vulnerability List” mode in SecurityCenter lists all relevant CVE references, if available. This data is also displayed through reporting and exporting via CSV content.
* The text of any CVE value can be used as a search parameter within the SecurityCenter filters. For example, if the text “CVE-2014” is entered in the vulnerability text filter field, SecurityCenter will display all matching vulnerabilities that had a CVE entry from the year 2014. Specific CVE entries can be used in a search for more detailed results.
* CVE entries are also displayed when vulnerability descriptions are browsed within SecurityCenter.
* Through the Log Correlation Engine, SecurityCenter employs CVE for vulnerability to IDS event correlation so that an IDS event from a third party product can be correlated with all discovered vulnerabilities that have the same CVE entry.

# Common Configuration Enumeration (CCE)

Tenable’s support for CCE data starts directly with Extensible Configuration Checklist Document Format (XCCDF) content. To parse XCCDF content directly, Tenable employs SecurityCenter to read XML content and generate a Nessus audit policy based on XML content.

As an XCCDF library is parsed within SecurityCenter, CCE IDs, their descriptions, and their associated reference material can be displayed. This information can be included in the actual audit policies generated for Nessus.

Within SecurityCenter, CCE IDs can be viewed in “Scan Results” and then selecting “CCE-ID” scan filter. after an audit has been completed. CCE ID descriptions, the policy value from the audit file, and the remote value from a scanned host are also included under “Scan Results”.

As Nessus completes its configuration audit, the text files produced are gathered by SecurityCenter. Once in SecurityCenter, users can search the obtained data by CCE through the “Vulnerability Text” field.

# Common Platform Enumeration (CPE)

Tenable Network Security uses Common Platform Enumeration (CPE) to ensure that configuration audits are performed on the correct operating systems. While processing XCCDF content, relevant CPE checks for the audit policy are built into the resulting Nessus audit policy. This ensures that if the wrong policy is used on an operating system not intended by the audit, a detailed error report will be produced.

Within SecurityCenter, an inadvertent scan of a system with the wrong policy can also be recognized and prevented. Although SecurityCenter has “asset logic” that can be used to ensure that Windows 7 audits are run on Windows 7 computers, it is very plausible to envision a customer simply auditing a network range that contains Windows 7, Windows 2008, and Windows Vista systems. In this case, for the incorrect CPE platforms, the audit will not be performed but the correct audits will still be automatically enabled.

# Common Vulnerability Scoring System (CVSS)

Tenable’s research group uses CVSS version 2 scores available from the National Vulnerability Database (NVD). The actual CVSS scoring strings and scores are used to map severity ratings of vulnerabilities audited by Nessus and the Passive Vulnerability Scanner.

When a test for a new vulnerability is produced by Tenable, there will sometimes not be a corresponding NVD entry for it at the time of the original test. In those cases, Tenable performs its own scoring according to NIST guidelines. When NVD entries or CVSS scores are available, Tenable synchronizes with NVD. If there is a discrepancy between what Tenable has scored and what NVD has scored, Tenable provides feedback to NIST.

Tenable Network Security uses the CVSS base score to select Nessus and PVS severity ratings for vulnerability plugins. Values from 1 through 3 receive a “Low/Informational” rating, 4 through 6 receive a “Medium/Warning” rating and 7 through 9 receive a “High/Hole” severity level. CVSS scores of 10 have a severity level of “Critical” and also have their risk factor marked as “Critical”.

In some cases, Tenable is unable to synchronize scores with NVD. This may happen because a Nessus or PVS plugin checks for a vulnerability for which there is no CVE/NVD entry or because NIST has not scored the entry manually (NIST labels these as “approximated” scores). In these cases, Tenable will re-score the plugins using the CVSSv2 standard when resources are available to do so.

# Extensible Configuration Checklist Document Format (XCCDF)

SecurityCenter directly imports XCCDF content into the product.

A SecurityCenter administrator can download the XCCDF content from a given source (such as NIST NVD <http://web.nvd.nist.gov/view/ncp/repository>, a third party product, or a Tenable product) and then upload the policy into SecurityCenter. Within SecurityCenter, a user can select a XCCDF Benchmark and Profile with which to run a compliance scan.

# Open Vulnerability Assessment Language (OVAL)

While processing XCCDF content, the entire body of OVAL checks is analyzed to produce a corresponding Nessus/SecurityCenter audit policy file. Nessus and SecurityCenter support all of the various OVAL check types from simple registry checks to the more complex logic checks that require multiple if/then decision trees.

If the tests described in the OVAL content change, the corresponding audit content will change as well. If the OVAL content contains an error, the corresponding audit policies will contain the same error. In each of these cases, SecurityCenter uses the OVAL definitions to produce the specific Nessus audit content.

As NIST updates the OVAL content for various tests, SecurityCenter does not need to be updated as it natively interprets OVAL.

Nessus performs the checks described by OVAL through several proprietary methods that leverage remote credentials of target Windows and Linux systems.

No agents are required on the target platform to perform any of the required audits described by OVAL. However, SecurityCenter does install a dissolvable agent that runs the compliance scan on the target.

# Asset Identification

Asset Identification is used to differentiate sets of information about assets. The Asset Identification portion of a SecurityCenter report is generated based on values retrieved from the system during a scan, and supports version 1.1.

# Asset Reporting Format (ARF)

Tenable Network Security makes use of ARF (Asset Reporting Format), which is a format for expressing the transport format of information about assets and the relationships between assets and reports, within SecurityCenter. ARF 1.1 reports are generated by using the provided SCAP content and the XCCDF/OVAL results from the execution of the SCAP content. The OVAL results included match the OVAL result type selected for the scan. The OVAL results included in the ARF report can be one of the following types: full results with system characteristics, full results without system characteristics, or thin results.

# SCAP Implementation

SecurityCenter and Nessus have the ability to import SCAP content. SCAP comprises multiple standards including OVAL, CVE, CVSS, XCCDF, CPE, OCIL, CCSS, Asset Identification, ARF, and CCE, as previously described in this document.

SecurityCenter and Nessus support SCAP by integrating each aspect of OVAL, CVE, CVSS, XCCDF, CPE, Asset Identification, ARF, and CCE to help organizations accurately test their infrastructure and ensure that it is configured with the correct settings.

OVAL, CCE, CPE and XCCDF define policies, configuration settings and testing methodology for these configuration settings.

Tenable customers use SecurityCenter, which is compatible with these standards, to run SCAP compliance scans against targets through the Nessus vulnerability scanner. SCAP content is uploaded to SecurityCenter via the UI. SecurityCenter then runs the scan based on the profile/benchmark selected to perform a configuration audit of target systems. Once the scan is finished, SecurityCenter generates reports in four formats (ARF, XCCDF, OVAL, and Nessus).

SecurityCenter can be used to report and analyze many different types of configuration and vulnerability data for large and small enterprises. SecurityCenter also manages re-scanning of systems (also known as remediation scanning) to verify compliance.

In addition, SecurityCenter can also manage the Passive Vulnerability Scanner and multiple Log Correlation Engine instances. Each of these products can be used to monitor network traffic and logs for evidence that an asset has undergone a change that may indicate a non-compliant state. These checks may also indicate that new hosts have been connected to the network and may require auditing.

# 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 many of the world’s largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit [tenable.com](http://www.tenable.com/).