NIST Interagency Report 7511
Revision 1 (Draft)

National Institute of
Standards and Technology
U.S. Department of Commerce

Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements (DRAFT)

Peter Mell
Stephen Quinn
John Banghart
David Waltermire

NIST Interagency Report 7511
Revision 1 (Draft)

Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements (DRAFT)

Peter Mell
Stephen Quinn
John Banghart
David Waltermire

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2009

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7511 Revision 1 (Draft)
41 pages (Apr. 2009)

Acknowledgements

The authors, Peter Mell and Stephen Quinn of the National Institute of Standards and Technology (NIST) and John Banghart and David Waltermire of Booz Allen Hamilton, would like to thank the many people that reviewed and contributed to this document. In particular, the following individuals provided invaluable feedback: Dawn Adams (EWA-Canada), Stephen Allison (Booz Allen Hamilton), Scott Armstrong (Secure Elements), Matt Barrett (NIST), Andrew Bove (Secure Elements), Scott Carpenter (Secure Elements), Mark Cox (Red Hat), Jonathan Frazier (Gideon Technologies), Tim Grance (NIST), Robert Hollis (Threatguard), Kent Landfield (McAfee), Ken Lassesen (Lumension), Karen Scarfone (NIST), and Joseph Wolfkiel (Department of Defense).

Abstract

This report defines the requirements and associated test procedures necessary for products to achieve one or more Security Content Automation Protocol (SCAP) validations. Validation is awarded based on a defined set of SCAP capabilities and/or individual SCAP components by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program.

Audience

The audiences for the SCAP Validation Program test requirements include laboratories that are accredited to do SCAP product testing for the program, vendors that are interested in receiving SCAP validation for their products, and government agencies and integrators seeking to deploy SCAP tools in their environments. The laboratories use the information in this report to guide their testing and to ensure that all necessary requirements are met by a product before recommending to NIST that the product be awarded the requested validation. Vendors may use the information in this report to understand what features their products must have to be eligible to receive any of the SCAP validations. Government agencies and integrators use the information to gain insight into the criteria that products being considered for procurement must meet to be validated. The secondary audience for this publication is end users, which can review the test requirements to determine what a validated product had to do to be awarded a validation, as well as to better understand what SCAP validation means.

Comments

Comments on this report are welcome. Please direct them to John Banghart (john.banghart@nist.gov).

Table of Contents

List of Tables

1. Introduction to SCAP and the SCAP Validation Program

The Security Content Automation Protocol (SCAP) is a specification established by NIST for expressing and manipulating security data in standardized ways. Currently, SCAP can enumerate product names and vulnerabilities (both software flaws and configuration issues); identify the presence of vulnerabilities; and assign severity scores to software flaw vulnerabilities. Adoption of SCAP makes it easier for organizations to automate ongoing security monitoring, vulnerability management, and security policy compliance evaluation reporting. An example of how SCAP can be used is to quickly find known vulnerabilities so that they can be remediated to prevent attackers from exploiting them.

The specifications that comprise SCAP are as follows:

- Extensible Configuration Checklist Description Format (XCCDF), an Extensible Markup Language (XML) specification for structured collections of security configuration rules used by operating system (OS) and application platforms
- Open Vulnerability and Assessment Language (OVAL), an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches
- Common Configuration Enumeration (CCE), a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings)
- Common Platform Enumeration (CPE), a naming convention for hardware, OS, and application products
- Common Vulnerabilities and Exposures (CVE), a dictionary of names for publicly known security-related software flaws
- Common Vulnerability Scoring System (CVSS), a method for classifying characteristics of software flaws and assigning severity scores based on these characteristics.

The SCAP specification defines what SCAP's components are and how they relate to each other within the context of SCAP. However, the SCAP specification does not define the SCAP components themselves; each component has its own standalone specification. The SCAP components were created and are maintained by several entities, including the MITRE Corporation, the National Security Agency (NSA), and the Forum of Incident Response and Security Teams (FIRST).

NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD). All of the content in NVD, as well as the high-level SCAP specification, is freely available from NIST. SCAP content is also created and made available by non-U.S. government organizations. SCAP can be used for automating activities such as ongoing security monitoring, vulnerability management, and security policy compliance evaluation reporting.

1.1 Purpose and Scope of the Program

The NIST SCAP Validation Program is designed to test the ability of products to use the features and functionality available through SCAP and its components. An information technology (IT) product vendor can obtain one or more validations for a product. These validations are based on the test requirements defined in this document. Products can be validated for SCAP itself in the context of a

particular product capability[1]. Note that SCAP validation for a particular capability may not require all the tests that are applicable to each of the six SCAP components. This document defines current capability validations, which include capabilities such as Federal Desktop Core Configuration (FDCC) Scanner, Authenticated Vulnerability and Patch Scanner, Misconfiguration Remediation, and Vulnerability Database. At this time, validations are not being awarded based on the individual component specifications (XCCDF, OVAL, CCE, CVE, CPE, and CVSS.)

Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) (http://ts.nist.gov/standards/accreditation/index.cfm). Accreditation requirements are defined in NIST Handbook 150 and NIST Handbook 150-17. Independent laboratories conduct the tests contained in this document on IT security products and deliver the results to NIST. Based on the independent laboratory test report, the SCAP Validation Program then validates the product under test. The validation certificates awarded to vendor products are publicly posted on the NIST SCAP Validated Products web page (http://nvd.nist.gov/scapproducts.cfm).[2]

SCAP validation will focus on evaluating specific versions of vendor products based on the platforms they support. Validation certificates will be awarded on a platform-by-platform basis for the version of the product that was validated. Currently, official SCAP content is primarily focused on Microsoft Windows operating systems. Thus, vendors seeking validation will be evaluated based on the ability of the product to operate on the Windows target platform. SCAP validation will expand to include other operating systems in 2009.

1.2 Superseded Compatibility Programs

This publication supersedes the draft Security Content Automation Protocol (SCAP) Validation Program Test Requirements Version 1.0 that was released in August 2008 and the Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements that was released in April 2009. This publication will be used for SCAP validation effective January 31, 2009.

[1] The SCAP Validation Program defines capability as “a specific function or functions of a product”. Further information can be found in Section 2.3.

[2] The SCAP Validation Program does not provide physical certificates to the participating vendors.

2. Versions and Definitions

2.1 Versions

For all test requirements that reference particular specifications, the versions indicated in the following section should be used.

2.1.1 Federal Desktop Core Configuration (FDCC)

Definition: The FDCC is a security configuration and policy developed for use on U.S. Federal government Windows XP and Windows Vista systems.

Versions: Versions 1.2.0.0 and 1.2.1.0. FDCC versioning is constructed using the following scheme:

> FDCC SCAP version w.x.y.z where:
>
> w = Configuration settings major number. If there are changes to the configuration settings, the major number will be revised upward.
>
> x = Indicates correction in either XCCDF or OVAL, but does not indicate configuration setting changes, nor does it communicate versions of XCCDF or OVAL. Corrections can also include the addition of previously manual checks that are now automated.
>
> y = OVAL version, where 0=5.4, 1=5.3, 2=5.5, 3=5.6, and so on.
>
> z = XCCDF version, where 0=1.1.4, 1=1.1.5, 2=1.1.6, 3=1.2, and so on.

Specification: http://fdcc.nist.gov/

For the purposes of testing, vendors may choose either version 1.2.0.0 or version 1.2.1.0 for validation.

2.1.2 Security Content Automation Protocol (SCAP)

Definition: SCAP is a specification for expressing and manipulating security data in standardized ways. SCAP uses several individual specifications in concert to automate ongoing security monitoring, vulnerability management, and security policy compliance evaluation reporting. The SCAP version allows the versions of the SCAP components to be referred to collectively.

Version: 1.0

Specification: http://scap.nist.gov/

SCAP 1.0 includes:

- XCCDF 1.1.4
- OVAL 5.3
- CCE 5.0
- CPE 2.2

- CVE
- CVSS 2.0

2.1.3 eXtensible Configuration Checklist Document Format (XCCDF)

Definition: XCCDF is an XML-based language for representing security checklists, benchmarks, and related documents in a machine-readable form. An XCCDF document represents a structured collection of security configuration rules for one or more applications and/or systems. The XCCDF specification also defines a data model and format for storing the results of benchmark compliance testing.

Version: 1.1.4

Specification: http://nvd.nist.gov/xccdf.cfm

Schema Location: http://nvd.nist.gov/xccdf.cfm

2.1.4 Open Vulnerability and Assessment Language (OVAL)

Definition: OVAL is an XML-based language used for communicating the details of vulnerabilities, patches, security configuration settings, and other machine states in a machine-readable form.

Version: 5.3[3]

Specification: http://oval.mitre.org/

Schema Location: http://oval.mitre.org/language/download/schema/version5.4/index.html

2.1.5 Common Configuration Enumeration (CCE)

Definition: CCE is a format to describe system configuration issues to facilitate correlation of configuration data across multiple information sources and tools.

Version: 5.0

Specification: http://cce.mitre.org/

Schema Location: http://cce.mitre.org/

2.1.6 Common Platform Enumeration (CPE)

Definition: CPE is a structured naming scheme for IT platforms (hardware, operating systems, and applications) for the purpose of identifying specific platform types.

Version: 2.2

Specification: http://cpe.mitre.org/

Schema Location: http://cpe.mitre.org/specification/index.html

Dictionary: http://nvd.nist.gov/cpe.cfm

[3] OVAL 5.4 is used in FDCC version 1.2.0.0 and is acceptable for validation ONLY for FDCC Scanners.

2.1.7 Common Vulnerabilities and Exposures (CVE)

Definition: CVE is a format to describe publicly known information security vulnerabilities and exposures. Using this format, new CVE IDs will be created, assigned, and referenced in content on an as-needed basis without a version change.

Version: N/A

Specification: http://cve.mitre.org/

Dictionary: http://nvd.nist.gov/

2.1.8 Common Vulnerability Scoring System (CVSS)

Definition: CVSS is a scoring system that provides an open framework for determining the relative severity of software flaw vulnerabilities and a standardized format for communicating vulnerability characteristics.

Version: 2.0

Specification: http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf

SCAP CVSS Base Scores: http://nvd.nist.gov/

2.2 Document Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in Request for Comment (RFC) 2119[4].

The availability of an Internet connection, wireless or wired, during the evaluation of each test requirement will be indicated by the statements “permitted” or “not permitted”. When “permitted” is indicated, a product may make full use of any available network connection to access Internet-based resources. If “not permitted” is indicated, then no Internet network connectivity shall be provided during evaluation of the test procedure. Every effort has been made in the test requirements to avoid mandating that the capability to run in the presence or absence of Internet connectivity be supported by a product. Use of an Internet connection in some test procedures is disallowed to ensure that the functionality being evaluated in the tool exists directly within the tool and not as the result of utilizing an Internet-based capability. Access to a local area network (LAN) shall be allowed in all tests to support client-server based implementations.

2.3 Common Definitions

The following definitions represent key terms used in this document.

Authenticated Scanner: A product that runs with privileges on a target system to conduct its assessment.

[4] For more information, please refer to Internet Engineering Task Force (IETF) RFC 2119, Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997, http://www.ietf.org/rfc/rfc2119.txt?number=2119.

CCE ID: An identifier for a specific configuration defined within the official CCE Dictionary and that conforms to the CCE specification. For more information please see the CCE specification reference in Section 2.1.

Comparison Utility: A utility provided to the accredited laboratory testers by NIST for use in the validation of product data sets as defined by certain testing requirements.

CPE Name: An identifier for a unique uniform resource identifier (URI) given to a specific platform type that conforms to the CPE specification. For more information please see the CPE specification reference in Section 2.1.

CVE ID: An identifier for a specific software flaw defined within the official CVE Dictionary and that conforms to the CVE specification. For more information please see the CVE specification reference in Section 2.1.

Derived Test Requirement/Test Requirement: A statement of requirement, needed information, and associated test procedures necessary to test a specific SCAP feature.

Interrelation: The aggregation of two or more SCAP components resulting in testing requirements that extend or replace the testing requirements for each individual SCAP component that forms the combination.

Import: A process available to end-users by which an SCAP data file can be loaded manually into the vendor product. During this process, the vendor process may optionally translate this file into a proprietary format.

Machine-Readable: Tool output that is in a structured format, typically XML, that can be consumed by another program using consistent processing logic.

Major Revision: Any increase in the version of an SCAP component's specification or SCAP related data set that involves substantive changes that will break backwards compatibility with previous releases. See also SCAP revision.

Minor Revision: Any increase in version of an SCAP component's specification or SCAP related data set that may involve adding additional functionality, but that preserves backwards compatibility with previous releases. See also SCAP revision.

Misconfiguration: A setting within a computer program that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system. CCE can be used for enumerating misconfigurations. (Note: NIST generally defines a vulnerability as including both software flaws and configuration issues [misconfigurations]. For the purposes of the validation program and dependent procurement language, the SCAP Validation program is defining vulnerability and misconfiguration as two separate entities, with "vulnerability" referring strictly to software flaws.)

OVAL ID: An identifier for a specific OVAL definition that conforms to the format for OVAL IDs. For more information please see the OVAL specification reference in Section 2.1.

Product: A security software application, appliance, or security database that has one or more capabilities.

Product Output: Information produced by a product. This includes the product user interface, human-readable reports, and machine-readable reports. There are no constraints on the format. When this output is evaluated in a test procedure, either all or specific forms of output will be sampled as indicated by the test procedure.

Reference Product: A product provided to accredited laboratory testers by NIST for use as a baseline for testing requirements. The product exhibits the behavior that is deemed to be correct.

SCAP Capability: A specific function or functions of a product as defined below:

- FDCC Scanner: the capability to audit and assess a target system to determine its compliance with the FDCC requirements.
- Authenticated Configuration Scanner: the capability to audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges.
- Authenticated Vulnerability and Patch Scanner: the capability to scan a target system to locate and identify the presence of known vulnerabilities and evaluate the software patch status to determine compliance with a defined patch policy using target system logon privileges
- Unauthenticated Vulnerability Scanner: the capability of determining the presence of known vulnerabilities by evaluating the target system over the network
- Intrusion Detection and Prevention System (IDPS): the capability to monitor a system or network for unauthorized or malicious activities. An intrusion prevention system actively protects the target system or network against these activities.
- Vulnerability Remediation: the capability to install patches on a target system in compliance with a defined patching policy.
- Misconfiguration Remediation: the capability to alter the configuration of a target system to bring it into compliance with a defined set of configuration recommendations.
- Asset Scanner: the capability to actively discover, audit, and assess asset characteristics including: installed and licensed products; location within the world, a network or enterprise; ownership; and other related information on IT assets such as workstations, servers, and routers.
- Asset Database: the capability to store and report on asset characteristics including: installed and licensed products; location within the world, a network or enterprise; ownership; and other related information on IT assets such as workstations, servers, and routers.
- Vulnerability Database: a catalog of security-related software flaws labeled with CVEs where applicable. This data is made accessible to users through a search capability or data feed and contains descriptions of software flaws, references to additional information (e.g., links to patches or vulnerability advisories), and impact scores. The user-to-database interaction is provided independent of any scans, intrusion detection, or reporting activities. Thus, a product that only scans to find vulnerabilities and then stores the results in a database does not meet the requirements for an SCAP vulnerability database (such a product would map to a different SCAP capability). A product that presents the user general knowledge about vulnerabilities, independent of a particular environment, would meet the definition of an SCAP vulnerability database.
- Misconfiguration Database: a catalog of security-related configuration issues labeled with CCEs where applicable. This data is made accessible to users through a search capability or data feed and contains descriptions of configuration issues and references to additional information (e.g.,

configuration guidance, mandates, or other advisories). The user-to-database interaction is provided independent of any configuration scans or intrusion detection activities. Thus, a product that only scans to find misconfigurations and then stores the results in a database does not meet the requirements for an SCAP misconfiguration database (such a product would map to a different SCAP capability). A product that presents the user general knowledge about security-related configuration issues, independent of a particular environment, would meet the definition of an SCAP vulnerability database.

- Malware Tool: the capability to identify and report on the presence of viruses, worms, Trojan horses, spyware, or other malware on a target system.

SCAP Component: One of the six specifications that comprise SCAP: CCE, CPE, CVE, CVSS, OVAL, and XCCDF.

SCAP-Expressed Data Stream: A collection of four or more related XML files containing SCAP data using the SCAP components that provide the data necessary to evaluate systems for compliance with a configuration-based security policy. Patch checking content may also be included in this bundle. Files included for SCAP 1.0 are listed below, with the "XXXX" in each name representing a unique prefix for the bundle (e.g., fdcc-xp, fdcc-vista):

- XXXX-xccdf.xml - XCCDF 1.1.4 content
- XXXX-cpe-oval.xml - CPE OVAL 5.3 definitions
- XXXX-cpe-dictionary.xml - Minimal CPE 2.2 dictionary
- XXXX-oval.xml - OVAL 5.3 compliance definitions

SCAP Revision: A version of the SCAP specification, designated by a revision number in the format nn.nn.nn, where the first nn is the major revision number, the second nn number is the minor revision number, and the final nn number is the refinement number. A specific SCAP revision will populate all three fields, even if that means using zeros to show no minor revision or refinement number has been used to date. A leading zero will be used to pad single-digit revision or refinement numbers.

Software Flaw: See Vulnerability.

Target Platform: The target operating system or application on which a vendor product will be evaluated using a platform-specific validation lab test suite. These platform-specific test suites consist of specialized SCAP content used to perform the test procedures defined in this document.

Unauthenticated Scanner: A scanning product that runs without privileges against a target system to conduct its assessment which could include network data and port scans.

Vulnerability: An error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur. CVE is a common means of enumerating vulnerabilities.

XCCDF Content: A file conforming to the XCCDF schema.

3. Vendor Product Validation Testing Requirements

The following guidelines must be followed by all vendors seeking validation of a product:

1. Vendors must provide the required vendor information detailed within the applicable derived test requirements.

2. For tests that require testers to import a NIST-provided XCCDF or OVAL test file(s), vendors may indicate whether or not this import should be a standalone file or part of an SCAP-expressed data stream.

3. All SCAP tests require an SCAP-expressed data stream as input. Therefore, vendor products must be able to import valid SCAP-expressed data streams.

Vendors may update validated products, but the new version is **not** automatically validated. To validate an updated product, the vendor must send documentation to the laboratory that performed the existing validation explaining the validation-related changes to the product. This statement will be posted publicly by NIST with the product's validation and thus must not contain proprietary information. The vendor may provide the laboratory additional proprietary details that will not be sent to NIST and will not be publicly posted.

The laboratory will review the changes, list the impacted testing requirements, and retest those requirements. The laboratory will then provide NIST a test report that summarizes how the product was changed and provides relevant test results. NIST will review the report and make a decision regarding whether to validate the updated product. If validation is granted, the newly validated product will have the same expiration date as the originally validated product since full testing of all requirements was not performed. Because of this, vendors may wish to fully retest an updated product if the expiration date is near and if a significant amount of retesting is required for the update.

4. Derived Test Requirements for Specific SCAP Components

This section contains the Derived Test Requirements (DTR) for each of the six SCAP components for the purpose of allowing individual validation of each SCAP component within a product. Version information and download location, listed in Section 2.1, should be referenced to ensure that the correct version is being used prior to testing. SCAP-specific requirements are found in Section 5.

Each DTR includes the following information:

- The DTR name. This is comprised of the acronym followed by ".R" to denote it is a requirement, and then the requirement number within the component section (CVE, CCE, etc.)
- Required vendor information. This states what information vendors are required to provide to the testing lab for the test to be conducted.
- Required test procedure(s). This defines one or more tests that the testing laboratory will conduct to determine the product's ability to meet the stated requirement.

4.1 XCCDF

The following XCCDF requirements are used to achieve XCCDF validation or in conjunction with other non-XCCDF test requirements for SCAP validation. Thus, all of the tests are focused exclusively on XCCDF and do not cover how XCCDF interrelates with other SCAP components. Section 6 includes a capability matrix that indicates which of the XCCDF test requirements are used in SCAP validation.

Because of the versatility of the XCCDF language, it can be used in a variety of roles. Some of the test requirements have been classified based on their specific role and these are in turn applied to the relevant SCAP capability.

XCCDF.R.1: The product's documentation (printed or electronic) must state that it uses XCCDF and explain the relevant details to the users of the product.

Required Vendor Information

XCCDF.V.1: The vendor shall indicate where in the product documentation information regarding the use of XCCDF can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

XCCDF.T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of XCCDF is present and verify that the XCCDF documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

XCCDF.R.2: The vendor must assert that the product implements the XCCDF specification and provide a high-level summary of the implementation approach.

Required Vendor Information

XCCDF.V.2: The vendor shall provide a 150 to 500 word English language document to the lab that asserts that the product implements the XCCDF specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses CPE versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

XCCDF.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the XCCDF specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements XCCDF.

XCCDF.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

XCCDF.R.3: The product shall report XCCDF content that is invalid according to the XCCDF schema.

Required Vendor Information

XCCDF.V.3: The vendor shall provide instructions on how and where XCCDF schema errors will be displayed within the product output.

Required Test Procedure

Internet Connectivity: Not permitted

XCCDF.T.3: The tester shall attempt to import known invalid XCCDF content into the vendor product and examine the product output to validate that the tool reports the content as invalid according to the XCCDF schema.

XCCDF.R.4: The product shall be able to process XCCDF files and generate XCCDF Results in accordance with the XCCDF specification for the target platform.

Required Vendor Information

XCCDF.V.4: The vendor shall provide instructions on how to import XCCDF files for execution and provide instructions on where the XCCDF Results can be located for visual inspection. Use of any XCCDF-capable check system(s) is permitted. The purpose of this requirement is to ensure that the product produces valid XCCDF Results and a matching pass/fail result for a given Rule.

Required Test Procedure

Internet Connectivity: Not permitted

XCCDF.T.4.1: The tester shall import a known valid XCCDF file for the target platform into the vendor tool and execute it according to the tool operation instructions provided by the vendor.

The tester will inspect the output to validate that it includes the same checks and uses the same check parameters as that produced by the NIST XCCDF reference implementation.

XCCDF.T.4.2: The tester shall validate the resulting XCCDF result output using the XCCDF schema. This validation must not produce any validation errors.

XCCDF.T.4.3: The tester shall compare the product results to those produced by the XCCDF reference implementation to ensure that the pass/fail results match for each Rule.

NOTE: If the product is not seeking OVAL validation, results will indicate that the Rules were not executed. This is acceptable.

XCCDF.R.5: The user shall be able to select a specific XCCDF Profile when executing an XCCDF file on the target platform. The product will execute the XCCDF content using the chosen profile.

Required Vendor Information

XCCDF.V.5: The vendor shall provide instructions on how the user can select an XCCDF Profile when executing a valid XCCDF content file.

Required Test Procedures

Internet Connectivity: Not permitted

XCCDF.T.5: The tester shall validate that the product produces results applicable to the chosen XCCDF profile on the target platform.

XCCDF.R.6: The product shall be able to import an XCCDF file and generate human-readable prose (close correspondence to the patterns of everyday speech) from valid XCCDF documents. This requirement includes both XCCDF checklists and output result files.

Required Vendor Information

XCCDF.V.6: The vendor shall provide instructions on how the product generates human-readable prose from valid XCCDF documents.

Required Test Procedures

Internet Connectivity: Permitted

XCCDF.T.6: The tester shall use the vendor product to generate human-readable prose from a valid XCCDF document.

4.2 OVAL

The following OVAL requirements are used in conjunction with other non-OVAL test requirements for SCAP validation. Thus, all of the tests are focused exclusively on OVAL and do not cover how OVAL interrelates with other SCAP components. Section 6 includes a capability matrix that indicates which of the OVAL test requirements are used in SCAP validation.

OVAL.R.1: The product's documentation (printed or electronic) must state that it uses OVAL and explain relevant details to the users of the product.

Required Vendor Information

OVAL.V.1: The vendor shall indicate where in the product documentation information regarding the use of OVAL can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

OVAL.T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of OVAL is present and to verify that the OVAL documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

OVAL.R.2: The vendor must assert that the product implements the OVAL specification and provide a high-level summary of the implementation approach.

Required Vendor Information

OVAL.V.2: The vendor shall provide a 150 to 500 word English language document to the accredited validation lab that asserts that the product implements the OVAL specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses OVAL versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

OVAL.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the OVAL specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements OVAL.

OVAL.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

OVAL.R.3: The product shall report and optionally reject OVAL content that is invalid according to the OVAL XML schemas and schematron stylesheets.

Required Vendor Information

OVAL.V.3: The vendor shall provide instructions on how validation of OVAL content is performed and where errors from validation will be displayed within the product output.

Required Test Procedure

Internet Connectivity: Not permitted

OVAL.T.3.1: The tester shall attempt to import known invalid OVAL Definition content into the vendor product and examine the product output to validate that the product reports and optionally rejects the content as invalid according to the OVAL Definition schema and schematron stylesheets.

OVAL.R.4: The product output shall enable users to view the XML OVAL Definitions being consumed by the tool (e.g., within the product user interface or through an XML dump of the OVAL definitions to a file).

Required Vendor Information

OVAL.V.4: The vendor shall provide instructions on how the user can view the XML OVAL Definitions being consumed by the product.

Required Test Procedure

Internet Connectivity: Not permitted

OVAL.T.4: The tester shall follow the provided vendor instructions to view the XML OVAL Definitions being consumed by the product and verify that access is provided as stated.

OVAL.R.5: The product shall be able to correctly evaluate a valid OVAL Definition file against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results format.

NOTE: This requirement is deferred until January 2010 for all SCAP Capabilities.

Required Vendor Information

OVAL.V.5: The vendor shall provide instructions on how a valid OVAL Definitions file can be imported into the product for interpretation. The vendor shall also provide instructions on where the resultant OVAL XML Full Results output can be viewed by the tester.

For OVAL.T.5.5, the vendor shall indicate how two or more values can be specified for a variable used by one OVAL Definition.

Required Test Procedure

Internet Connectivity: Not permitted

OVAL.T.5.1: The tester shall run the tool using valid OVAL Definitions files against the target systems of the target platform type. The results shall be compared against results from the OVAL reference implementation and they must produce the same pass/fail result for each OVAL definition and criteria contained within the definition.

OVAL.T.5.2: The tester shall validate the resulting OVAL XML Full Results output using the OVAL schema and schematron style sheets. Both of these validations must not produce any validation errors.

OVAL.T.5.3: The tester shall validate that the resulting OVAL XML Full Results are available for viewing by the user.

OVAL.T.5.4: The tester shall inspect the product output and compare it against the reference results to ensure the proper use of result types ("not evaluated", "error", etc.)

OVAL.T.5.5: When an OVAL Definition has been evaluated more than once on a single target system, each time with different values for the variables, the tester shall validate that the OVAL XML Full Results file includes unique variable instance values for each individual case.

4.3 CCE

The following CCE requirements are used to achieve CCE validation or in conjunction with other non-CCE test requirements for SCAP validation. Thus, all of the tests in this sub-section are focused exclusively on CCE and do not cover how CCE interrelates with other SCAP components. Section 6 includes a capability matrix that indicates which of the CCE test requirements are used in SCAP validation.

CCE.R.1: The product's documentation (printed or electronic) must state that it uses CCE and explain relevant details to the users of the product.

Required Vendor Information

CCE.V.1: The vendor shall indicate where in the product documentation information regarding the use of CCE can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

CCE.T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of CCE is present and to verify that the CCE documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

CCE.R.2: The vendor must assert that the product implements the CCE specification and provide a high-level summary of the implementation approach.

Required Vendor Information

CCE.V.2: The vendor shall provide a 150 to 500 word English language document to the lab that asserts that the product implements the CCE specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses CCE versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

CCE.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the CCE specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements CCE.

CCE.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

CCE.R.3: The product shall display the associated CCE ID for each configuration issue definition in the product output (i.e., the product displays CCE IDs).

Required Vendor Information

CCE.V.3: The vendor shall provide instructions on how product output can be generated that contains a listing of all security configuration issue items both with and without CCE IDs. Instructions shall include where the CCE IDs and the associated vendor supplied and/or official CCE descriptions can be located within the product output.

Required Test Procedure

Internet Connectivity: Permitted

CCE.T.3: The tester shall visually inspect, within the product output, a random set of 30 security configuration issue items, to ensure that the CCE IDs are displayed. This test is not intended to determine whether the product correctly maps to CCE or whether it provides a complete mapping.

CCE.R.4: The product shall provide a means to view the CCE Description for each displayed CCE ID within the product output.

NOTE: This requirement is deferred until January 2010 for all SCAP Capabilities.

Required Vendor Information

CCE.V.4: The vendor shall provide instructions noting where the CCE ID can be located within the product output. The vendor shall provide procedures and a test environment (if necessary) so that the product will output configuration issues with associated CCE IDs.

Required Test Procedures

Internet Connectivity: Permitted

CCE.T.4: The tester shall inspect the CCE IDs from the product output and verify that the official CCE Description[5] is available. The vendor may provide additional CCE descriptions and information and should not be penalized for doing so. The tester shall perform this using a randomly selected set of 10% of the total CCE IDs available in the product output, up to a maximum of 30.

[5] The official CCE descriptions are found at http://cce.mitre.org/lists/cce_list.html.

CCE.R.5: The product shall indicate the correct CCE ID for each configuration issue referenced within the product that has an associated CCE ID (i.e., the product's CCE mapping must be correct).

Required Vendor Information

CCE.V.5: None.

Required Test Procedures

Internet Connectivity: Permitted

CCE.T.5: Using the product output from CCE.R.3 the tester shall compare the vendor data against the official CCE description. The tester shall perform the comparison using a randomly selected set comprised of 10% of the total configuration issue items with CCE IDs, up to a maximum of 30. The tester does not need to rigorously prove that the vendor's configuration issue description matches the official CCE description, but merely needs to identify that the two appear to be same. This test ensures that the product correctly maps to CCE, but does not test for completeness of the mapping.

CCE.R.6: The product shall associate an existing CCE ID to each configuration issue referenced within the product for which a CCE ID exists (i.e., the product's CCE mapping must be complete).

Required Vendor Information

CCE.V.6: None.

Required Test Procedures

Internet Connectivity: Permitted

CCE.T.6: Using the list of configuration issue items produced in CCE.R.3, the tester shall examine the descriptions and search the CCE dictionary for all corresponding CCE IDs. The tester shall perform this using a randomly selected set comprised of 10% of the total configuration issue items with no CCE IDs, up to a maximum of 30. The tester does not need to rigorously prove that no CCE ID exists, only that there does not appear to be a match. This test ensures that the product has a complete mapping to CCE, but does not test the correctness of the mapped data.

CCE.R.7: The product shall allow users to locate configuration issue items using CCE names.

Required Vendor Information

CCE.V.7: The vendor shall provide documentation (printed or electronic) indicating how security configuration issue items can be located using CCE names.

Required Test Procedures

Internet Connectivity: Permitted

CCE.T.7: The tester shall verify that security configuration issue items can be located using CCE names. The tester shall perform this using a randomly selected set comprised of 10% of the total configuration issue items, up to a maximum of 30.

CCE.R.8: For all static or product bundled CCE data, the product shall indicate the date the data was last generated and updated. The generated date is when the data was originally created/officially published. The updated date is the date the product obtained its copy of the data.

Required Vendor Information

CCE.V.8: The vendor shall provide instructions on where the dates for all offline CCE data can be inspected in the product output.

Required Test Procedure

Internet Connectivity: Not permitted

CCE.T.8: The tester shall visually inspect the product output for the dates of all static or bundled CCE data included with the vendor product.

4.4 CPE

The following CPE requirements are used to achieve CPE validation or in conjunction with other non-CPE test requirements for SCAP validation. Thus, all of the tests are focused exclusively on CPE and do not cover how CPE interrelates with other SCAP components. Section 6 includes a capability matrix that indicates which of the CPE test requirements are used in SCAP validation.

CPE.R.1: The product's documentation (printed or electronic) must state that it uses CPE and explain relevant details to the users of the product.

Required Vendor Information

CPE.V.1: The vendor shall indicate where in the product documentation information regarding the use of CPE can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

CPE.T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of CPE is present and to verify that the CPE documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

CPE.R.2: The vendor must assert that the product implements the CPE specification and provide a high-level summary of the implementation approach.

Required Vendor Information

CPE.V.2: The vendor shall provide a 150 to 500 word English language document to the lab that asserts that the product implements the CPE specification and provides a high-level summary of

the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses CPE versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

CPE.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the CPE specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements CPE.

CPE.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

CPE.R.3: If the product natively contains a product dictionary (as opposed to dynamically importing content containing CPE names), the product must contain CPE naming data from the current official CPE Dictionary.

NOTE: This requirement does not apply if the product is using the official dynamic CPE Dictionary as provided on the NVD web site or as part of an SCAP-expressed data stream.

Required Vendor Information

CPE.V.3.1: The vendor shall provide a list of all CPE names included in the product using the standard CPE Dictionary XML schema as provided in the CPE Specification version cited in Section 2.1.

CPE.V.3.2: If the vendor product includes CPE names that are not in the official CPE Dictionary, a listing of exceptions must be provided.

Required Test Procedure

Internet Connectivity: Permitted

CPE.T.3: Using the NIST-provided CPE Validation Utility, the tester shall import the vendor-provided list of CPE Names for comparison against the official CPE Dictionary. Before each tool is tested, the latest CPE Dictionary must be loaded into the utility. The tester shall verify that all exceptions found by the CPE Validation Utility match the list of exceptions provided by the vendor.

CPE.R.4: A product's machine-readable output must provide the CPE naming data using CPE names.

NOTE: This requirement does not apply if the product does not produce machine-readable output.

Required Vendor Information

CPE.V.4: The vendor shall provide procedures and/or a test environment where machine-readable output containing the CPE naming data can be produced and inspected. The vendor shall provide

a translation tool to create human-readable data for inspection if the provided output is not in a human-readable format (e.g., binary data, encrypted text).

Required Test Procedure

Internet Connectivity: Permitted

CPE.T.4: The tester shall manually inspect the vendor-identified machine-readable output and ensure that CPE naming data is correct according to the CPE specification. The tester will do this by randomly choosing up to 30 vendor and product names in the product output that are also included in the official CPE Dictionary.

4.5 CVE

The following CVE requirements are used in conjunction with other non-CVE test requirements for SCAP validation. Thus, all of the tests in this sub-section are focused exclusively on CVE and do not cover how CVE interrelates with other SCAP components. Section 6 includes a capability matrix that indicates which of the CVE test requirements are used in SCAP validation.

CVE.R.1: The product's documentation (printed or electronic) must state that it uses CVE and explain relevant details to the users of the product.

Required Vendor Information

CVE.V.1: The vendor shall indicate where in the product documentation information regarding the use of CVE can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file). This must be separate from any results reporting.

Required Test Procedures

Internet Connectivity: Permitted

CVE.T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of CVE is present and to verify that the CVE documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

CVE.R.2: The vendor must assert that the product implements the CVE specification and provide a high-level summary of the implementation approach.

Required Vendor Information

CVE.V.2: The vendor shall provide a 150 to 500 word English language document to the lab that asserts that the product implements the CVE specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses CVE versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

CVE.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the CVE specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements CVE.

CVE.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

CVE.R.3: The product shall include the CVE ID(s) associated with each software flaw and/or patch definition in the product output (i.e., the product displays CVE IDs).

Required Vendor Information

CVE.V.3: The vendor shall provide instructions, and a test environment (if necessary), indicating how product output can be generated that contains a listing of all software flaws and patches both with and without CVE IDs. CVE IDs should be used wherever possible. Instructions shall include where the CVE IDs and the associated vendor-supplied and/or official CVE descriptions can be located within the product output.

Required Test Procedures

Internet Connectivity: Permitted

CVE.T.3: The tester shall visually inspect, within the product output, a randomly selected set comprised of 10% of the total CVE IDs available in the product output, up to a maximum of 30 to ensure that the CVE IDs are displayed. This test is not intended to determine whether the product correctly maps to CVE or whether it provides a complete mapping.

CVE.R.4: The product shall provide a means to view the CVE Description and CVE references for each displayed CVE ID[6] within the product output.

Required Vendor Information

CVE.V.4: The vendor shall provide instructions on the where the CVE IDs can be located within the product output. The vendor shall provide procedures and a test environment (if necessary) so that the product will output vulnerabilities with associated CVE IDs. Instructions shall include where the CVE IDs and the associated vendor-supplied and official CVE descriptions can be located within the product output.

Required Test Procedures

Internet Connectivity: Permitted

CVE.T.4: The tester shall select a random sampling of CVE IDs from within the available forms of the product output. The tester shall determine that the product output enables the user to view, at minimum, the official CVE description and references.[7] The vendor may provide additional CVE descriptions and information and should not be penalized for doing so. The tester shall

[6] This requirement can be met be providing a URL to the NVD CVE or MITRE CVE vulnerability summaries for the CVE IDs in question.

[7] The official CVE description and references are found at http://nvd.nist.gov/.

perform this using a randomly selected set comprised of 10% of the total CVE IDs available in the product output, up to a maximum of 30.

CVE.R.5: The product shall indicate the correct CVE ID for each software flaw and/or patch definition referenced within the product that has an associated CVE ID (i.e., the product's CVE mapping must be correct).

Required Vendor Information

CVE.V.5: None

Required Test Procedures

Internet Connectivity: Permitted

CVE.T.5: Using the product output from CVE.R.3 the tester shall compare the vendor data against the official NVD CVE ID description and references. The tester shall perform this test using a randomly selected set comprised of 10% of the total software flaws and/or patches with CVE IDs, up to a maximum of 30. The tester does not need to rigorously prove that the vendor's software flaw and/or patch description matches the NVD CVE description, but merely needs to identify that the two descriptions appear to pertain to the same vulnerability. This test ensures that the product correctly maps to CVE, but does not test for completeness of the mapping.

CVE.R.6: The product shall associate an existing CVE ID to each software flaw and/or patch referenced within the product for which a CVE ID exists (i.e., the product's CVE mapping must be complete).

Required Vendor Information

CVE.V.6: None.

Required Test Procedures

Internet Connectivity: Permitted

CVE.T.6: Using the list of software flaws and/or patch definitions produced in CVE.R.3, the tester shall examine the descriptions and search the NVD for any corresponding CVE IDs. The tester shall perform this using a randomly selected set comprised of 10% of the total software flaws and/or patches with no CVE IDs, up to a maximum of 30. The tester does not need to rigorously prove that no CVE ID exists, only that there does not appear to be a match. This test ensures that the product has a complete mapping to CVE, but does not test the correctness of the mapped data.

4.6 CVSS

The following CVSS requirements are used to achieve CVSS validation or in conjunction with other non-CVSS test requirements for SCAP validation. Thus, all of the tests are focused exclusively on CVSS and do not cover how CVSS interrelates with other SCAP components. Section 6 includes a capability matrix that indicates which of the CVSS test requirements are used in SCAP validation.

CVSS.R.1: The product's documentation (printed or electronic) must state that it uses CVSS and explain relevant details to the users of the product. If external CVSS data is imported into the product, the documentation must state the source.

Required Vendor Information

CVSS.V.1: The vendor shall indicate where in the product documentation information regarding the use of CVSS can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

CVSS.T.1: The tester shall visually inspect the provided product documentation to verify that information regarding the product's use of CVSS is documented, verify that the source of the CVSS data is specified, and verify that the CVSS documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

CVSS.R.2: The vendor must assert that the product implements the CVSS specification and provide a high-level summary of the implementation approach.

Required Vendor Information

CVSS.V.2: The vendor shall provide a 150 to 500 word English language document to the accredited validation lab that asserts that the product implements the CVSS specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses CVSS versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

CVSS.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the CVSS specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements CVSS.

CVSS.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

CVSS.R.3: The product provides CVSS base scores for each security-related software flaw referenced in the product.

Required Vendor Information

CVSS.V.3.1: The vendor shall provide documentation and/or procedures that explain how to view software flaws and associated CVSS base scores within the product output.

CVSS.V.3.2: The vendor shall provide documentation and/or procedures that explain how to produce a report of all software flaws supported by the tool along with their associated CVSS base scores.

Required Test Procedure

Internet Connectivity: Permitted

CVSS.T.3.1: The tester shall validate that the product output provides severity scores labeled as CVSS scores for a random sample of 30 security-related software flaws referenced in the product output. The tester does not need to validate the correctness of the scores within this test.

CVSS.T.3.2: The tester shall validate that the product provides severity scores labeled as CVSS scores for 30 randomly chosen security-related software flaws referenced by the tool. The tester does not need to validate the correctness of the scores within this test.

CVSS.R.4: The product provides a CVSS vector string along with each CVSS base score[8].

Required Vendor Information

CVSS.V.4: The vendor shall provide documentation and/or procedures that explain how to view the CVSS vector string for all software flaws in the product that have CVSS base scores.

Required Test Procedure

Internet Connectivity: Permitted

CVSS.T.4.1: The tester shall randomly choose 10 CVSS vector strings provided by the product and validate that they conform to the CVSS version vector specification as described in Section 2. The vectors chosen should all be unique vectors (each one is different from the others).

CVSS.T.4.2: For each of the 10 CVSS vectors used in CVSS.T.4.1, the tester shall validate that the associated CVSS vector calculates to the same CVSS base score as provided by the product. The tester shall use the NVD CVSS calculator reference implementation to perform the calculations.

CVSS.R.5: The product enables users to refine[9] CVSS base scores to produce CVSS temporal scores for each CVSS base score provided by the product. Alternately, the product may directly provide temporal scores[10].

NOTE: The required elements for temporal scoring are available from NIST Interagency Report (IR) 7435, Section 2.2.

Required Vendor Information

[8] The requirements for CVSS vectors are available from NIST IR 7435, Section 2.4.

[9] This could be achieved through a wide variety of mechanisms including user importation of temporal data, access to subscription services, and/or linkage to a CVSS calculator.

[10] This can be achieved by a product hyperlinking from the product's CVSS score to the NVD CVSS calculator reference implementation. Instructions for how vendors can do this are available at http://nvd.nist.gov/cvss.cfm.

CVSS.V.5: The vendor will provide documentation explaining how users can refine CVSS base scores to produce CVSS temporal scores for each CVSS base score provided by the product. Alternately, the vendor will provide documentation stating that they directly provide temporal scores for the user. It is possible that a product will provide a combination of both approaches.

Required Test Procedure

Internet Connectivity: Permitted

CVSS.T.5.1: The tester shall validate that the product either enables users to refine CVSS base scores to produce CVSS temporal scores or directly provides temporal scores for a set of chosen software flaws referenced in the product.

CVSS.T.5.2: For the set of chosen software flaws in CVSS.T.3.1 (reuse of previous sample), the tester shall perform the same CVSS base score refinement using the NVD CVSS calculator reference implementation and validate that the resultant NVD CVSS calculator and product temporal scores are equal.

CVSS.R.6: The product enables users to customize[11] CVSS base scores to produce CVSS environmental scores for each software flaw referenced in the product[12].

Required Vendor Information

CVSS.T.6: The vendor will provide documentation explaining how users can customize CVSS base scores to produce CVSS environmental scores for each CVSS base score provided by the product.

Required Test Procedure

Internet Connectivity: Not permitted

CVSS.T.6.1: The tester shall validate that the product enables users to customize CVSS base scores to produce CVSS environmental scores for 10 randomly chosen software flaws referenced in the product.

---

[11] This could be achieved through a wide variety of mechanisms including user importation of temporal data, access to subscription services, and linkage to a CVSS calculator, such as hyperlinking from the product's CVSS base score to the NVD CVSS calculator reference implementation. Instructions for how vendors can do this are available at http://nvd.nist.gov/cvss.cfm.

[12] The required elements for environmental scoring are available from NIST IR 7435, Section 2.3. It is possible for a vendor to automatically collect the environmental metrics from the network, configuration database, system inventory, or some other source such that the user does not have to manually customize the scores. This is actually the preferred implementation approach.

CVSS.T.6.2: For the 10 randomly chosen software flaws in CVSS.T.6.1, the tester shall perform the same CVSS base score customization using the NVD CVSS calculator reference implementation and validate that the NVD CVSS calculator and product environmental scores are equal.

5. SCAP Derived Test Requirements

This section builds on the SCAP component-specific requirements from Section 4. This section defines the requirements for validation of SCAP-specific behaviors for the SCAP components when they are used in conjunction with one another.

5.1 Federal Desktop Core Configuration (FDCC)

FDCC.R.1: The product shall be able to correctly assess a target system using the FDCC SCAP-expressed data streams as input.

Required Vendor Information

FDCC.V.1: The vendor shall provide instructions on how to execute a previously imported valid FDCC SCAP-expressed data stream.

Required Test Procedures

Internet Connectivity: Not permitted

Per vendor instruction in FDCC.V.1, the lab will make the necessary configuration changes to the target platform and document what has been changed. The pass/fail comparison of these changes shall not impact the Pass or Fail result of the test.

The FDCC data streams to be used for each of the following tests are:

- Windows Vista
- Windows XP
- Windows XP Firewall
- Windows Vista Firewall
- Internet Explorer 7

All these data streams are found in the official FDCC bundles available from http://fdcc.nist.gov/download.cfm.

FDCC.T.1.1: The tester shall evaluate an FDCC compliant target platform, both domain connected and standalone, and compare the pass/fail results from the product to the results produced by the NIST reference implementation to ensure that they match.

FDCC.T.1.2: The tester shall evaluate an FDCC partial-compliant target platform, both domain connected and standalone, and compare the pass/fail results from the product to the results produced by the NIST reference implementation to ensure that they match.

FDCC.T.1.3: The tester shall evaluate an FDCC more secure target platform, both domain connected and standalone, and compare the pass/fail results from the product to the results produced by the NIST reference implementation to ensure that they match.

FDCC.R.2: The product shall be able to produce specified FDCC results (both the human and machine-readable versions).

Required Vendor Information

FDCC.V.2: None

Required Test Procedure

Internet Connectivity: Permitted

FDCC.T.2.1: The tester shall validate the XCCDF results produced, on the target platform by the product, against the FDCC reporting Schematron stylesheet[13] and must verify that no validation errors are produced.

FDCC.T.2.2: The product documentation shall indicate to the user how they can access the product output as defined in FDCC.T.2.1. The product interface shall make this output available through the product GUI or other user interface.

NOTE: FDCC.T.2.3 is deferred until January 2010.

FDCC.T.2.3: The tester shall validate that the human-readable FDCC assessment results provide the CCE ID and the associated pass/fail status corresponding to the XCCDF results required in FDCC.T.2.1. The required result format is the CCE ID, followed by a comma, followed by the words "pass" or "fail" followed by a new line. Example:

CCE-1222-1,pass
CCE-3233-7,fail

FDCC.R.3: If the vendor product requires a specific configuration of the target platform that is not in compliance with the FDCC, the vendor shall provide documentation indicating which settings must be changed and a rationale for each changed setting. Products should only require changes to the target platform so that it can function correctly.

NOTE: Pursuant to OMB Memorandum 07-18:[14] "The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC)." Products undergoing SCAP validation are also required by OMB to make this self-assertion and that listing their non-complaint settings for FDCC.R.3 in no way negates the OMB M-07-18 requirement.

Required Vendor Information

FDCC.V.3: The vendor shall provide an English language document to the lab that indicates which settings must be changed and a rationale for each changed setting. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released.

Required Test Procedure

[13] http://nvd.nist.gov/fdcc/fdcc_reporting.cfm
[14] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf

Internet Connectivity: Permitted

FDCC.T.3: The tester shall review the provided documentation to ensure that each indicated setting includes an associated rationale.

5.2 General SCAP Requirements

SCAP.R.1: The product's documentation (printed or electronic) must state that it uses SCAP and explain relevant details to the users of the product.

Required Vendor Information

SCAP.V.1: The vendor shall indicate where in the product documentation information regarding the use of SCAP can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

SCAP.T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of SCAP is present and verify that the SCAP documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

SCAP.R.2: The vendor must assert that the product implements the SCAP specification and provide a high-level summary of the implementation approach.

Required Vendor Information

SCAP.V.2: The vendor shall provide a 150 to 500 word English language document to the lab that asserts that the product implements the SCAP specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released.

Required Test Procedures

Internet Connectivity: Permitted

SCAP.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the SCAP specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements SCAP.

SCAP.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

SCAP.R.3: The SCAP capabilities claimed by the vendor for the product under test must match the scope of the product's asserted capabilities for the target platform.

Required Vendor Information

SCAP.V.3.1: The vendor shall indicate which one or more of the defined SCAP capabilities their product is being tested for.

SCAP.V.3.2: The vendor shall provide product documentation that enumerates the general product capabilities for the target platform (e.g., antivirus, intrusion detection, firewall) that relate to the asserted SCAP capabilities.

Required Test Procedure

Internet Connectivity: Permitted

SCAP.T.3.1: The tester shall ensure that all tests associated with the asserted SCAP capabilities of the product are conducted.

SCAP.T.3.2: The tester shall review product documentation to ensure that the product has implemented the SCAP capabilities for which it is being tested (e.g., Authenticated Configuration Scanner, Asset Database).

SCAP.R.4: For all static or product bundled SCAP data (i.e., CCE, CPE, CVE and data streams), the product shall indicate the date the data was last generated and updated. The generated date is when the data was originally created/officially published. The updated date is the date the product obtained its copy of the data.

Required Vendor Information

SCAP.V.4: The vendor shall provide instructions on where the dates for all offline SCAP data can be inspected in the product output.

Required Test Procedure

Internet Connectivity: Not permitted

SCAP.T.4: The tester shall visually inspect the product output for the dates of all static or bundled SCAP data included with the vendor product.

5.3 XCCDF + OVAL (Input)

SCAP.R.5: The product shall be able to import an XCCDF data file for the target platform and correctly load the included Rules and their associated OVAL Definitions on a target system.

Required Vendor Information

SCAP.V.5: The vendor shall provide documentation and instruction on how to import an SCAP-expressed data stream for the target platform, including XCCDF and OVAL content, into the product.

Required Test Procedures

Internet Connectivity: Not permitted

SCAP.T.5: The tester shall import valid SCAP-expressed data streams for the target platform into the vendor product and execute them on a target system. Results of the scan shall be visually

compared to the results from the NIST reference implementation to validate that the results match. This test is to ensure that the product's XCCDF and OVAL integration is working correctly.

5.4 XCCDF + OVAL (Output)

SCAP.R.6: XCCDF Results files and OVAL Results files shall be produced by the product in compliance with the XCCDF and OVAL Results schemas.

NOTE: This requirement is being deferred until January 1st, 2010 for the FDCC Scanner capability. All products seeking validation or re-validation subsequent to this date will be required to meet this requirement as part of the validation testing of their product for those capabilities that require it.

Required Vendor Information

SCAP.V.6: The vendor shall provide instruction on where the corresponding XCCDF and OVAL results files can be located for inspection.

Required Test Procedures

Internet Connectivity: Not permitted

SCAP.T.6: The tester shall visually inspect XCCDF and OVAL results to verify that they are valid according to the associated specification for each. The output is also compared to the results from the NIST reference implementation to verify completeness and accuracy of the XCCDF and OVAL results.

5.5 XCCDF + CCE

SCAP.R.7: For all CCE IDs in the XCCDF input document, the product shall correctly display the CCE ID with its associated XCCDF Rule in the product output.

Required Vendor Information

SCAP.V.7: The vendor shall provide instructions on where the XCCDF Rules and their associated CCE IDs can be visually inspected within the product output.

Required Test Procedures

Internet Connectivity: Permitted

SCAP.T.7: The tester shall visually inspect a random sample of 10% of the XCCDF Rules, up to a total of 30, within the product output and reports to validate that the CCE IDs for each inspected XCCDF Rule match those found in the XCCDF source file.

5.6 XCCDF + OVAL + CPE

SCAP.R.8: The product shall be able to determine the validity of imported SCAP XCCDF/OVAL files by evaluating the associated OVAL definition for the CPE Name on an XCCDF <Benchmark>, <Group>, or <Rule> and verifying that the associated XCCDF content applies to the target system.

Required Vendor Information

SCAP.V.8: The vendor shall provide instructions on how the product indicates the validity of the imported SCAP-expressed data stream to a target platform. Instructions should also describe how the imported data stream is indicated to not be valid for a target platform. This requirement is testing the use of the OVAL check associated with a CPE name via the CPE dictionary to determine applicability of the data stream.

Required Test Procedures

Internet Connectivity: Permitted

SCAP.T.8: The tester shall import an SCAP-expressed data stream into the tool that contains a CPE Name and related OVAL definition not applicable for the target system. The tester shall verify that the product declines to execute the non-applicable tests.

5.7 CVSS + CVE

SCAP.R.9: If the product uses CVE, it shall include NVD CVSS base scores and vector strings for each CVE ID referenced in the product.

Required Vendor Information

SCAP.V.9: The vendor shall provide documentation explaining where the NVD CVSS base scores and vector strings can be located with the corresponding CVE ID.[15] The vendor may optionally provide the tester information on how the product can be updated with new NVD CVSS base scores and vector strings prior to testing.

Required Test Procedure

Internet Connectivity: Permitted

SCAP.T.9: The tester shall update the product's NVD base scores and vectors (using the vendor-provided update capability if it exists) and validate that the product displays the NVD CVSS base scores and vectors for 15 randomly chosen CVE IDs referenced in the product. The CVEs chosen must have an NVD vulnerability summary "last revision" date that is at least 30 days old. A link to the information on the NVD web site is sufficient for this test.

5.8 SCAP-Expressed Data Stream Import

SCAP.R.10: The product shall enable the user to import an SCAP-expressed data stream.

Required Vendor Information

SCAP.V.10: The vendor shall provide documentation explaining how an SCAP-expressed data stream can be imported into the product and subsequently executed.

Required Test Procedure

Internet Connectivity: Not Permitted

[15] A link to the information on the NVD web site is sufficient for this test.

SCAP.T.10.1: The tester shall verify that the product documentation includes instructions on how the end user can import an SCAP-expressed data stream.

SCAP.T.10.2: The tester shall import a valid SCAP-expressed data stream into the vendor product and ensure that the imported content is available for execution. NOTE: Test FDCC.T.1 can substitute for this test.

5.9 Compliance Mapping Output

SCAP.R.11: When processing SCAP-expressed data streams that contain compliance mappings to included CCEs, the product shall output the compliance mappings.

NOTE: This requirement is being deferred until January 1st, 2010. All products seeking validation or re-validation subsequent to this date will be required to meet this requirement as part of the validation testing of their product for those capabilities that require it.

Required Vendor Information

SCAP.V.11: The vendor shall provide documentation explaining where CCE compliance mappings can be viewed within the product output.

Required Test Procedure

Internet Connectivity: Not Permitted

SCAP.T.11: Using the vendor product, the tester shall execute a valid SCAP-expressed data stream with CCE compliance mapping information and view the resultant output to ensure that the CCE compliance mappings are correct.

5.10 Misconfiguration Remediation

SCAP.R.12: The product shall be able to input a valid SCAP-expressed data stream and remediate non-compliant settings on the target system according to the Rules included in that stream.

Required Vendor Information

SCAP.V.12: The vendor shall provide instructions on how an SCAP-expressed data stream can be imported and executed on the target system to remediate non-compliant settings. The vendor shall also provide instructions on where the results of the remediation action can be viewed within the product output.

Required Test Procedure

Internet Connectivity: Not Permitted

SCAP.T.12: Using the vendor product, the tester shall execute the test suite data stream on the target platform's (based on what the vendor is applying for) partial-compliant virtual hard drive (VHD). Once the vendor product has completed execution, the tester shall manually inspect each of the known non-compliant settings to ensure that the vendor product has correctly set them to the expected values.

6. Derived Test Requirements for Specific Capabilities

This section contains Derived Test Requirements for each of the defined SCAP capabilities. When a tool is submitted for validation, the submitting organization will provide a list of capabilities the tool possesses, as defined in this document. The information regarding capabilities will be provided by the vendor as part of their submission package. To determine the correct test requirements for that tool, the tester creates the union of all these capabilities, using the provided chart.

The matrix currently contains a total of 12 SCAP capabilities. However, only the following SCAP capabilities are available for validation at this time: FDCC Scanner, Authenticated Configuration Scanner, Authenticated Vulnerability and Patch Scanner, Unauthenticated Vulnerability Scanner, and Misconfiguration Remediation. As additional capabilities are available for validation, this list will be updated. Vendors who wish to seek validation for an SCAP capability not listed above should contact NIST at scap-validation@nist.gov.

The following chart summarizes the required *SCAP components* for each *SCAP capability* together with the specific requirements necessary to achieve SCAP validation. Columns that are shaded in light gray are not currently available for validation. A red D in front of the requirement ID or in a box indicates that the requirement has been deferred until January 31st, 2010 for all capabilities or specific ones, respectively.

Table 6-1. Required SCAP Components for Each SCAP Capability

Require-ment ID	FDCC Scanner	Authenticated Configuration Scanner	Authenticated Vulnera-bility and Patch Scanner	Unauthenticated Vulnerability Scanner	IDPS	Vulnerability Remediation	Misconfiguration Remediation	Asset Scanner	Asset Database	Vulnerability Database	Misconfiguration Database	Malware Tool
FDCC.R.1	X											
FDCC.R.2	X											
FDCC.R.3	X											
XCCDF.R.1	X	X										
XCCDF.R.2	X	X										
XCCDF.R.3	X	X										
XCCDF.R.4	X	X					X					
XCCDF.R.5	X	X										
XCCDF.R.6												
OVAL.R.1	X	X	X									
OVAL.R.2	X	X	X									
OVAL.R.3	X	X	X									
OVAL.R.4	X	X	X									
D OVAL.R.5	X	X	X									
CCE.R.1	X	X					X				X	

Require-ment ID	FDCC Scanner	Authenticated Configuration Scanner	Authenticated Vulnera-bility and Patch Scanner	Unauthenticated Vulnerability Scanner	IDPS	Vulnerability Remediation	Misconfiguration Remediation	Asset Scanner	Asset Database	Vulnerability Database	Misconfiguration Database	Malware Tool
CCE.R.2	X	X					X				X	
CCE.R.3	X	X					X				X	
D CCE.R.4	X	X					X				X	
CCE.R.5	X	X					X				X	
CCE.R.6	X	X					X				X	
CCE.R.7	X	X					X				X	
CCE.R.8	X	X					X				X	
CPE.R.1	X	X	X	X	X	X	X	X	X	X	X	X
CPE.R.2	X	X	X	X	X	X	X	X	X	X	X	X
CPE.R.3	X	X	X	X	X	X	X	X	X	X	X	X
CPE.R.4	X	X	X	X	X	X	X	X	X	X	X	X
CVE.R.1	X		X	X	X	X				X		X
CVE.R.2	X		X	X	X	X				X		X
CVE.R.3	X		X	X	X	X				X		X
CVE.R.4	D		X	X	X	X				X		X
CVE.R.5	X		X	X	X	X				X		X
CVE.R.6	X		X	X	X	X				X		X
CVSS.R.1	X		X	X	X	X				X		X
CVSS.R.2	X		X	X	X	X				X		X
CVSS.R.3										X		
CVSS.R.4										X		
CVSS.R.5										X		
CVSS.R.6										X		
SCAP.R.1	X	X	X	X	X	X	X	X	X	X	X	X
SCAP.R.2	X	X	X	X	X	X	X	X	X	X	X	X
SCAP.R.3	X	X	X	X	X	X	X	X	X	X	X	X
SCAP.R.4	X	X	X	X	X	X	X	X	X	X	X	X
SCAP.R.5	X	X				X						
SCAP.R.6	D	X				X						
SCAP.R.7	X	X					X					
SCAP.R.8	X	X				X						
SCAP.R.9	X		X	X	X	X				X		X
SCAP.R.10	X	X	X			X						
D SCAP.R.11												
SCAP.R.12							X					

7. Appendix A—Acronyms and Abbreviations

This appendix contains selected acronyms and abbreviations used in the publication.

CCE Common Configuration Enumeration
CCSS Common Configuration Scoring System
CPE Common Platform Enumeration
CVE Common Vulnerabilities and Exposures
CVSS Common Vulnerability Scoring System

DTR Derived Test Requirements

FDCC Federal Desktop Core Configuration
FIRST Forum of Incident Response and Security Teams

ID Identifier
IDPS Intrusion Detection and Prevention System
IETF Internet Engineering Task Force
IR Interagency Report
IT Information Technology
ITL Information Technology Laboratory

LAN Local Area Network

NIST National Institute of Standards and Technology
NSA National Security Agency
NVD National Vulnerability Database
NVLAP National Voluntary Laboratory Accreditation Program

OS Operating System
OVAL Open Vulnerability and Assessment Language

PDF Portable Document Format

RFC Request for Comment

SCAP Security Content Automation Protocol

URI Uniform Resource Identifier
U.S. United States

VHD Virtual Hard Drive

XCCDF Extensible Configuration Checklist Document Format
XML Extensible Markup Language