



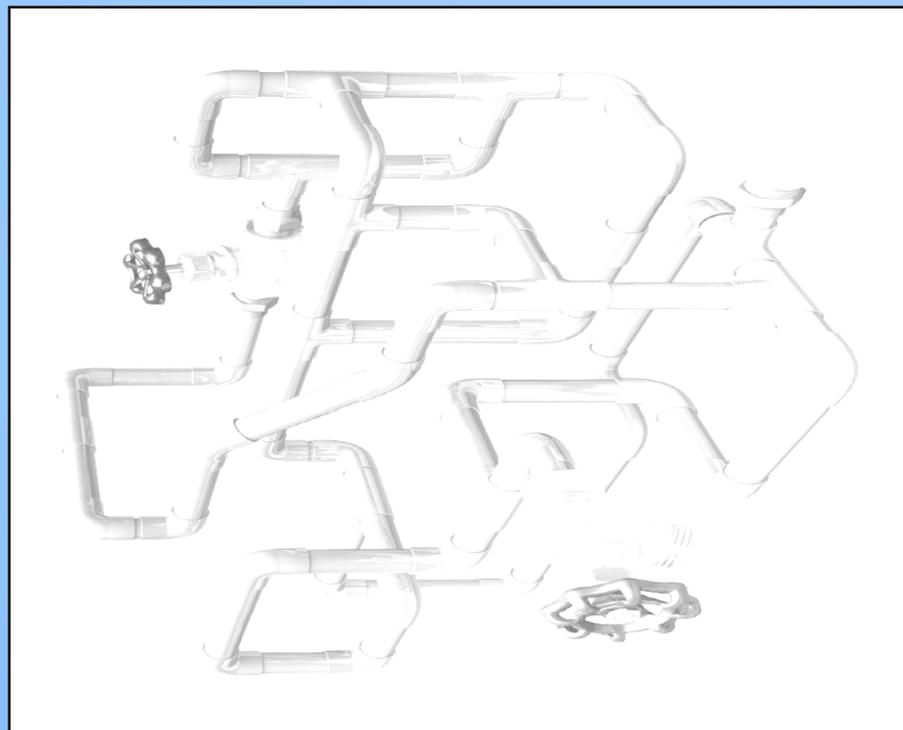
Security Content Automation Protocol

Presented by: Peter Mell, NIST
National Vulnerability Database Program Manager
SCAP Validation Program Manager



A Definition of SCAP

SCAP is a suite of vulnerability management standards that together enable standardization and automation of vulnerability management, measurement, and technical policy compliance checking (soon remediation) along with enhanced product and database integration capabilities with machine readable reporting.



SCAP is about Communication and Measurement

Languages

Standardizing the format by which we communicate

- Community developed and agreed upon
- Machine readable XML
 - Reporting
 - Representing security checklists
 - Detecting machine state

Enumerations

Standardizing the information we communicate

- Simple Identifiers
 - Standard based, community agreed upon
 - Product Names
 - Vulnerabilities
 - Configuration Issues

SCAP is about Communication and Measurement

Measurement Systems

Standardizing how we measure security characteristics using repeatable quantitative systems

- Community developed and agreed upon
- Repeatable
- Quantitative
- Translucent (you can see the individual metrics and input values)



Security Content Automation Protocol (SCAP)

Standardizing How We Communicate

MITRE



CVE

Common Vulnerability Enumeration

Standard nomenclature and dictionary of security related software flaws

MITRE



CCE

Common Configuration Enumeration

Standard nomenclature and dictionary of software misconfigurations

MITRE



CPE

Common Platform Enumeration

Standard nomenclature and dictionary for product naming



XCCDF

eXtensible Checklist Configuration Description Format

Standard XML for specifying checklists and for reporting results of checklist evaluation

MITRE



OVAL

Open Vulnerability and Assessment Language

Standard XML for test procedures



CVSS

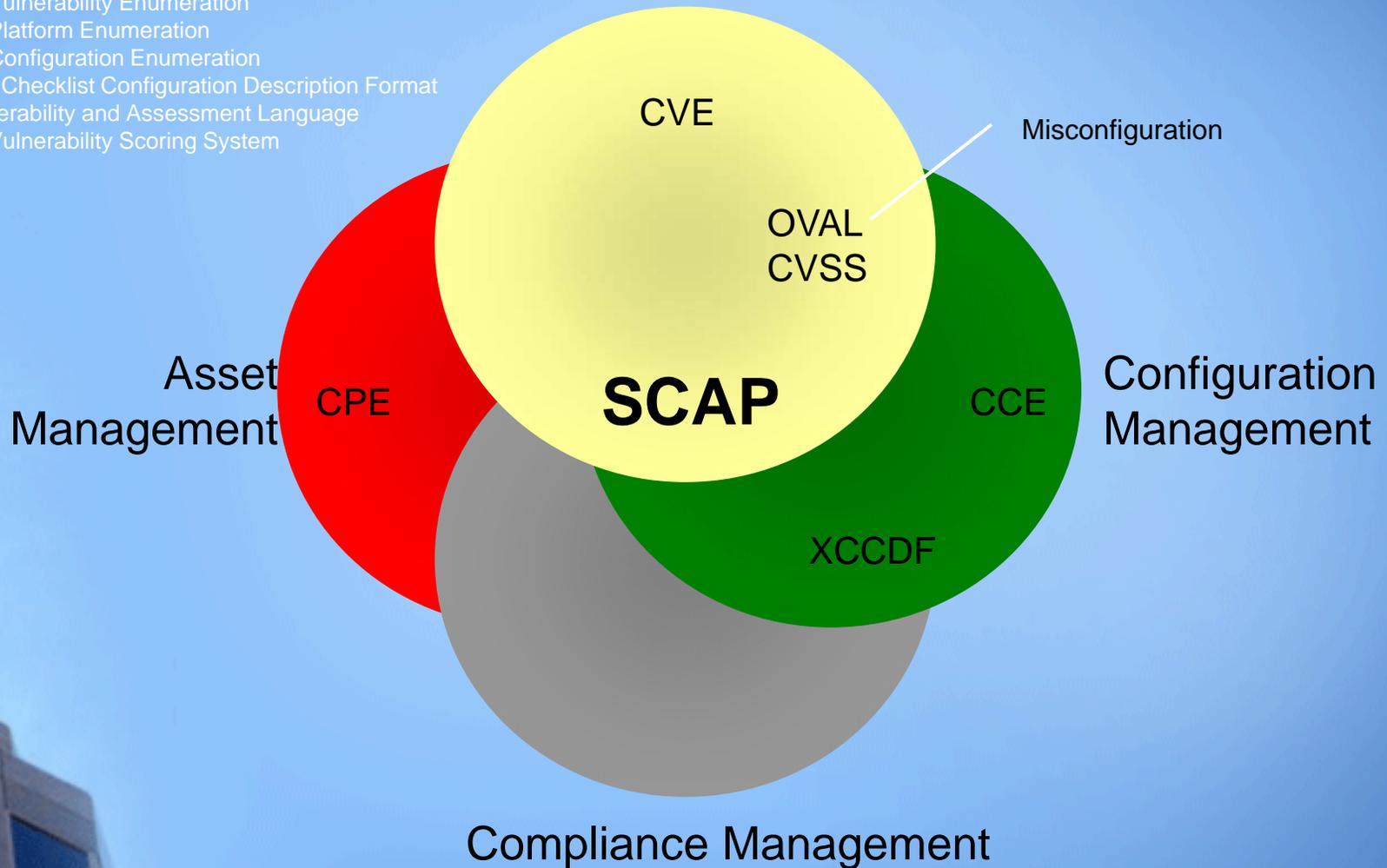
Common Vulnerability Scoring System

Standard for measuring the impact of vulnerabilities

Integrating IT and IT Security Through SCAP

Vulnerability Management

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System



eXtensible Checklist Configuration Description 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.
- **Specification:** <http://nvd.nist.gov/xccdf.cfm>
- **Schema Location:** <http://nvd.nist.gov/xccdf.cfm>

Common Vulnerability Scoring System (CVSS)

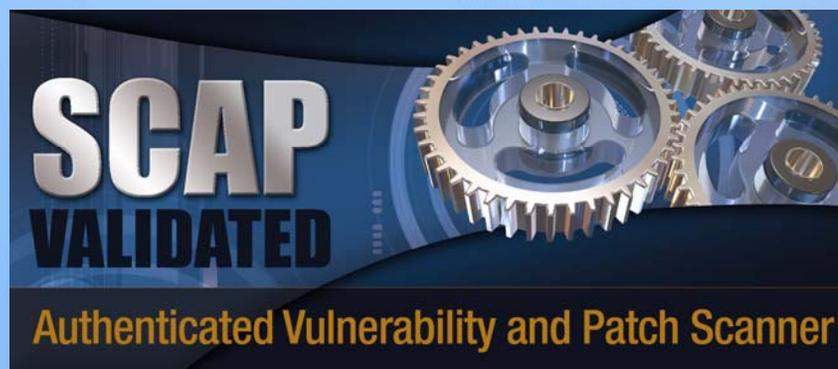


- **Definition:** CVSS is a scoring system that provides an open framework for determining the impact of information technology vulnerabilities and a format for communicating vulnerability characteristics.
- **Specification:**
<http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf>
- **SCAP CVSS Base Scores:** <http://nvd.nist.gov>

SCAP Validation Program



- Provides product conformance testing for Security Content Automation Protocol (SCAP) and the SCAP component standards
- National Voluntary Laboratory Accreditation Program
 - Independent testing laboratories
 - Reports validated by NIST
- <http://nvd.nist.gov/validation.cfm> (Validation Program)
- <http://nvd.nist.gov/scapproducts.cfm> (Validated Products)



SCAP Validation Capabilities

Currently being validated	Currently on list, not yet being validated
FDCC Scanner	Intrusion Detection and Prevention Systems (IDPS)*
Authenticated Vulnerability and Patch Scanner	Patch Remediation*
Authenticated Configuration Scanner	Malware Tool*
Unauthenticated Vulnerability Scanner	Asset Scanner*
Mis-configuration Remediation	
Vulnerability Database	
Mis-configuration Database	

SCAP Component Standards

Common Vulnerabilities and Exposures (CVE)	http://cve.mitre.org
Common Configuration Enumeration (CCE)	http://cce.mitre.org
Common Platform Enumeration (CPE)*	http://cpe.mitre.org
Common Vulnerability Scoring System (CVSS)	http://www.first.org/cvss/index.html
eXtensible Configuration Checklist Document Format (XCCDF)	http://nvd.nist.gov/xccdf.cfm
Open Vulnerability Assessment Language (OVAL)	http://oval.mitre.org

* Not currently available for validation

19 SCAP Validated Products from 13 Vendors



SCAP Validation Program was started February 2008



Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

National Vulnerability Database

- NVD is the U.S. government repository of public computer vulnerability information.
- It is designed to be based on and support vulnerability management standards (especially SCAP)
- It receives 69 million hits per year
- Used by Payment Card Industry, Federal Desktop Core Configuration, DHS, GSA Smartbuy, and security products

NIST

National Checklist Program Hosted at National Vulnerability Database Website

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities **Checklists** Product Dictionary Impact Metrics Data Feeds Statistics

Home ISAP/SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
 28360 CVE Vulnerabilities
 118 Checklists
 91 US-CERT Alerts
 2016 US-CERT Vuln Notes
 2966 OVAL Queries
 12969 Vulnerable Products
Last updated: 12/07/07
CVE Publication rate: 12 vulnerabilities / day

Email List

National Checklist Program Repository

Details on the National Checklist Program (NCP) are available [here](#).

NCP contains 118 checklists covering 150 products

Keyword Search: Search
 (try a checklist or product name)

View all by category:

Product Category	The checklists are listed by the main product category of the IT product, e.g. firewall, IDS, operating system, web server, etc.
Vendor	The checklists are listed by the manufacturer of the IT product.
Submitting Organization	The name of the organization and authors that produce the checklist.

Recent Updates (includes updates from the last 6 months)

The symbol denotes newly added checklists
 The symbol denotes updated checklists.

12/03/2007	Desktop Application Security Checklist
	Gold Standard Benchmark for Cisco IOS, Level 1 and 2 Benchmarks

National Checklist Program	
Checklist Summary #10: Desktop Application Security Checklist	
Checklist Item Name	Desktop Application Security Checklist
Checklist Item Version Number	Version 2, Release 1.8
Status	Final
Creation Date	10/25/2007
Original Publication Date	2003-02-28
Revision Date	12/03/2007
Product Category	Web Browser
Vendor (s)	Microsoft Netscape
Product (s)	Microsoft ie Microsoft ie Netscape Communicator Netscape Communicator Netscape Communicator Netscape Netscape Netscape Communicator Netscape Communicator
Product Version (s)	Microsoft ie 5.5 Microsoft ie 6.0 Netscape Communicator 4.76 Netscape Communicator 4.77 Netscape Communicator 4.78 Netscape Netscape 6.2.3 Netscape Communicator 4.79 Netscape Communicator 4.8
CPE Name (s)	cpe:/a:Microsoft:ie:5.5 cpe:/a:Microsoft:ie:6.0



Questions?

Peter Mell

NVD Program Manager

SCAP Validation Program Manager

301-975-5572

mell@nist.gov



SCAP Validation Tools: <http://nvd.nist.gov/scaproducts.cfm>

SCAP Validation Homepage: <http://nvd.nist.gov/validation.cfm>