JBoss SCAP based STIG

Security Content Automation Protocol based Security Technical Information Guide for JBoss Enterprise Application Platform (and SOA-P)

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant
Presentation v1.2 May 1, 2012

What is SCAP?

The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality.

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

What is supported?

Languages:

- Extensible Configuration Checklist Description Format (XCCDF) - Version: 1.1.4
- Open Vulnerability and Assessment Language (OVAL) - Version: 5.10
- Open Checklist Interactive Language (OCIL) - Version: 2.0

Enumerations:

- Common Configuration Enumeration (CCE) - Version: 5.0
- Common Platform Enumeration (CPE) - Version: 2.3
- Common Vulnerabilities and Exposures (CVE) - Version: None

Metrics:

- Common Vulnerability Scoring System (CVSS) - Version: 2.0
- Common Configuration Scoring System (CCSS) - Version: 1.0

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

What is XCCDF?

The Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems.

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

RED HAT CONSULTING

What is OVAL?

Open Vulnerability and Assessment Language (OVAL) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

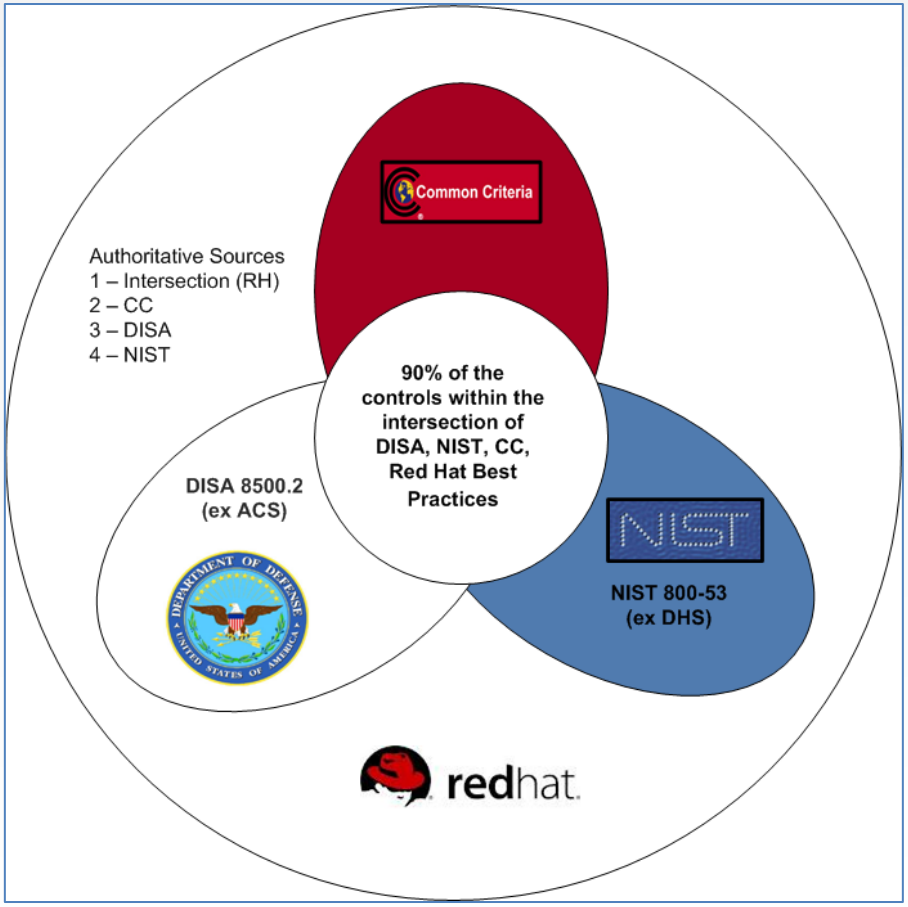
What is OCIL?

Open Checklist Interactive Language (OCIL) provides the conceptual framework for representing non-automatable questions.

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

RED HAT CONSULTING

Security Controls



Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

RED HAT CONSULTING

Security Controls

DoD (Department of Defense) 8500.2 (IA control assigned per CIA Triad leg)

1. DC - Security Design & Configuration
2. IA- Identification and Authentication
3. EC - Enclave and Computing Environment
4. EB - Enclave Boundary Defense
5. PE - Physical and Environmental
6. PR - Personnel
7. CO - Continuity
8. VI - Vulnerability and Incident Management

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

RED HAT CONSULTING

Security Controls

NIST (National Institute of Standards and Technology) 800.53

1. AC - Access Control
2. AT - Awareness and Training
3. AU - Audit and Accountability
4. CA - Certification, Accreditation, and Security Assessments
5. CM - Configuration Management
6. CP - Contingency Planning
7. IA - Identification and Authentication
8. IR - Incident Response
9. MA - Maintenance
10. MP - Media Protection
11. PE- Physical and Environmental Protection
12. PL - Planning
13. PS - Personnel Security
14. RA - Risk Assessment
15. SA - System and Services Acquisition
16. SC - System and Communications Protection
17. SI - System and Information Integrity
18. PM - Program Management

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

Tools in use

Editors
Eclipse with XML Plugin

Validators/Interpreters
SPAWAR SCC (SCAP Compliance Checker)
- Performs compliance scanning using SCAP content
- Performs vulnerability scanning using OVAL content
- Performs manual interview checks using OCIL content
- Creates XCCDF XML results
- Creates OVAL XML results
- Creates ARF XML results
- Creates Cyberscope Autofeed

XCCDF Interpreter (XCCDFEXEC)
- An open-source Java-based XCCDF reference implementation

OVAL Interpreter (OVALDI)
- Based on a set of OVAL Definitions the interpreter collects system information, evaluates it, and generates a detailed OVAL Results file.

Related
- Aqueduct
- OpenSCAP
- SCAP Workbench (Evaluated)
- eSCAP Editor (Evaluated)
- Recommendation tracker (Evaluated)

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

Content Sources

- DISA Controls – 8500.2 Information Assurance Implementation
- DISA Application Services v1:r1
- DISA Web Server v7:r1
- NIST Controls – 800.53 Recommended Security Controls for Federal Information Systems and Organizations
- SOA Best Practices Mapping with DISA/NIST Controls
- JBoss EAP 5 Common Criteria Certification Guide
- JBoss EAP 5 Security Guide
- JBoss EAP 5 Slimming Guide

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

Milestones

Week 1 – May 24 to May 1
- CCC/Best Practices complete in authoritative source list

Week 2 – May 2 to May 8
- Review CCC/Best Practices items
- Work Questionnaires (OCIL) from authoritative source list
- Work Automations (OVAL) from authoritative source list
- DISA/NIST controls Complete in authoritative source list

Week 3 – May 9 to May 15
- Review DISA/NIST control items
- Testing of content through xccdfexec
- Work Questionnaires (OCIL) from authoritative source list
- Work Automations (OVAL) from authoritative source list

Week 4 – May 16 to May 22
- Work Automations (OVAL) from authoritative source list

Week 5 – May 23 to May 29
- Work Automations (OVAL) from authoritative source list

Week 6 – May 30 to June 5
- Final Review of content
- Test content through xccdfexec and scc

Week 7 – June 6 to June 12
- Submit content to SPAWAR Cybersecurity and Red Hat
- Post message to gov-sec and middleware-consulting

Week 8 – June 13 to June 19
- SCAP Content and authoritative source list for evaluation by NIST/DISA

Week 9 – June 19
- Validate through Customers

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

Deliverables

The STIG will be packaged in a zip file that contains numerous files. <product-version> can be jboss-eap-5 and jboss-soa-p-5. There will be a readme file included in the zip file which is unique to that particular STIG. The readme.txt file will document the specific files for that technology.

Generally the following files will be included in the zip file:

- <product-version>-readme.txt – Important info about the files for the particular technology.
- <product-version>-ocil.xml – This is the STIG XML file that contains the manual check procedures.
- <product-version>-xccdf.xml - This is the STIG XML file that contains the automated check procedures.
- <product-version>.xsl – This is the transformation file that will allow the XML to be presented in a “human friendly” format.
- <product-version>-TechnologyOverview.pdf – This file will contain the introductory and background information, as well as screen captures, network diagrams, and other important information that could not be stored in the XML file.
- <product-version>-oval.xml – This file contains the detailed OVAL check code. This will only be provided if OVAL exists for the technology.
- <product-version>-cpe-oval.xml - This is OVAL code that will provide information to the tool on how to check to see if the product being evaluated exists on the system.
- <product-version>-cpe-dictionary.xml – This is the file that contains the CPE information about the product.

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

Acronyms

- CCE - Common Configuration Enumeration
- CPE - Common Platform Enumeration
- CVE - Common Vulnerabilities and Exposures
- CVSS - Common Vulnerability Scoring System
- HBSS - Host Based Security System
- OCIL – Open Checklist Interactive Language
- OVAL - Open Vulnerability Assessment Language
- SCAP - Security Content Automation Protocol
- STIG - Security Technical Implementation Guide
- XCCDF - eXtensible Configuration Checklist Description Format
- XML - eXtensible markup language
- XSLT - XSL Transformations

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

References

- NIST Special Publication (SP) 800-126 rev 2
- http://scap.nist.gov/
- http://scap.nist.gov/specifications/xccdf/
- http://oval.mitre.org/
- http://scap.nist.gov/specifications/ocil/
- http://scap.nist.gov/specifications/ai/
- http://scap.nist.gov/specifications/arf/
- http://cce.mitre.org/
- http://scap.nist.gov/specifications/cpe
- http://cve.mitre.org/
- http://www.first.org/cvss/
- http://www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

RED HAT CONSULTING

References

- http://sourceforge.net/projects/xccdfexec/
- http://sourceforge.net/projects/ovaldi/
- http://www.open-scap.org/page/Main_Page
- https://fedorahosted.org/scap-workbench/
- http://www.g2-inc.com/escape
- http://www.redhat.com/solutions/industry/government/certifications.html
- http://docs.redhat.com/docs/en-US/JBoss_Enterprise_Application_Platform/5/pdf/Security_Guide/JBoss_Enterprise_Application_Platform-5-Security_Guide-en-US.pdf
- http://docs.redhat.com/docs/en-US/JBoss_Enterprise_Application_Platform_Common_Criteria_Certification/5/html/Common_Criteria_Configuration_Guide/index.html
- http://iase.disa.mil/stigs/app_security/app_sec/app_sec.html
- http://iase.disa.mil/stigs/app_security/web_server/general.html
- http://csrc.nist.gov/groups/SMA/fisma/assessment.html

Kenneth Peeples, Architect
James Lopez, Consultant
Tim Falls, Consultant
Bryan Saunders, Consultant

RED HAT CONSULTING