Introduction to OpenSCAP

Tim Speetjens

Solution Architect, Red Hat Belux

April 2013

Agenda

- Introduction
- What’s SCAP
- Running checks
- Tools integration
- Content authoring
- Demo
- Summary

Security Practices Overview

- Secure configuration auditing
  - Are appropriate permissions set on /tmp?
- Patch level auditing
  - Does my system contain vulnarable packages?
- Active vulnerability scanning
  - Try to break things
- Network intrusion detection
  - Sniff the network

Compliance Checks

- Define security requirements
  - Which checks do I want to run?
- Check your system settings
  - Check each requirement on each system
- Define a measurement
  - How compliant are my systems?

Make security measurable!

Historic approach

- Define a checklist
- Connect to each system
- Check requirement manually, and flag as Pass or Fail
- Compile report

Does not scale, prone to errors, no reuse

Scripted approach

- Define a checklist
- Connect to each system
- Check requirement with custom script
- Compile report out of script results

Does not scale, prone to errors, little reuse, difficult to maintain

Standards based automation

- Reusable tests, even on multiple platforms
- Modular and configurable
- Layered approach – abstracted checks
- Content, auditing and authoring tools separated
- Integration with system management tools

SCAP

The Security Content Automation Protocol

CPE:	Common Platform Enumeration
CCE:	Common Configuration Enumeration
CVE:	Common Vulnerabilities and Exposures
CVSS:	Common Vulnarability Scoring System
OVAL:	Open Vulnarability and Assessment Language
XCCDF:	Extensible Configuration Checklist Description Format

OpenSCAP

- Open Source implementation
- SCAP 1.2 compliant
- Library
- Scanners
- XSLT transformations
- Content

Packages: openscap, openscap-utils, openscap-content

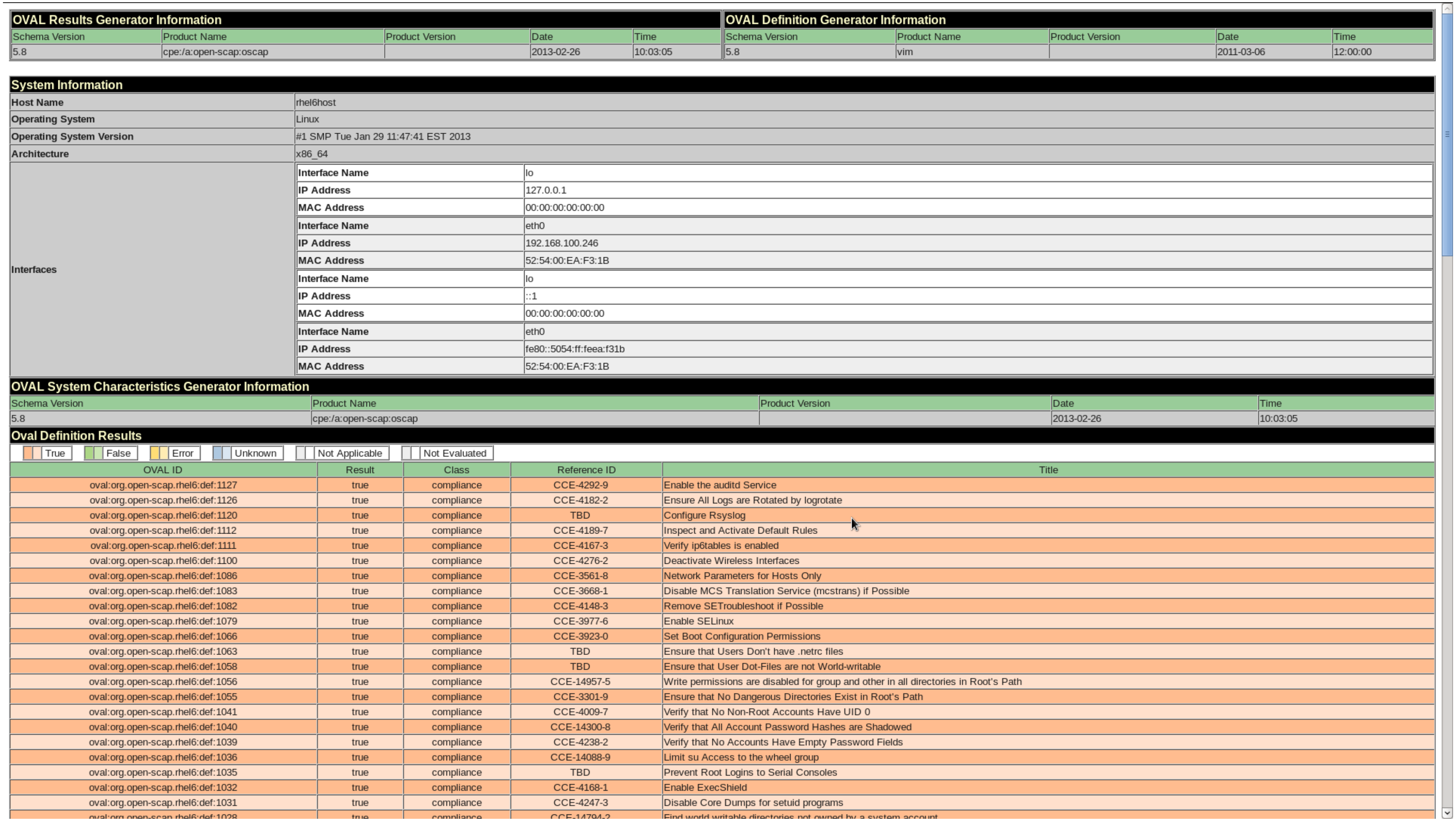
CLI – oscap oval

```
[root@rhel6host ~]# oscap oval -h
oscap -> oval

Open Vulnerability and Assessment Language

Usage: oscap [options] oval command

Commands:
 collect - Probe the system and create system  characteristics
    eval        - Probe the system and evaluate definitions
                  from OVAL Definition file
    analyse     - Evaluate provided system characteristics file
    validate    - Validate OVAL XML content
    generate    - Convert an OVAL file to other formats
    List-probes - List supported object types (i.e. probes)
```

CLI - OVAL evaluation

```
[root@rhel6host ~]# oscap oval eval \
> --results oval-results.xml \
> --report oval-report.html \
> /usr/share/openscap/scap-rhel6-oval.xml

Definition oval:org.open-scap.rhel6:def:1142: false
Definition oval:org.open-scap.rhel6:def:1141: false
Definition oval:org.open-scap.rhel6:def:1140: false
Definition oval:org.open-scap.rhel6:def:1139: false
...
Evaluation done.
```

OVAL report



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.8	cpe:/a:open-scap:oscap		2013-02-26	10:03:05

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.8	vim		2011-03-06	12:00:00

System Information

Host Name	rhel6host	
Operating System	Linux	
Operating System Version	#1 SMP Tue Jan 29 11:47:41 EST 2013	
Architecture	x86_64	
Interfaces	**Interface Name**	lo
	IP Address	127.0.0.1
	MAC Address	00:00:00:00:00:00
	Interface Name	eth0
	IP Address	192.168.100.246
	MAC Address	52:54:00:EA:F3:1B
	Interface Name	lo
	IP Address	::1
	MAC Address	00:00:00:00:00:00
	Interface Name	eth0
	IP Address	fe80::5054:ff:feea:f31b
	MAC Address	52:54:00:EA:F3:1B

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.8	cpe:/a:open-scap:oscap		2013-02-26	10:03:05

Oval Definition Results

🟧 True 🟩 False 🟨 Error 🟦 Unknown □ Not Applicable □ Not Evaluated

OVAL ID	Result	Class	Reference ID	Title
oval:org.open-scap.rhel6:def:1127	true	compliance	CCE-4292-9	Enable the auditd Service
oval:org.open-scap.rhel6:def:1126	true	compliance	CCE-4182-2	Ensure All Logs are Rotated by logrotate
oval:org.open-scap.rhel6:def:1120	true	compliance	TBD	Configure Rsyslog
oval:org.open-scap.rhel6:def:1112	true	compliance	CCE-4189-7	Inspect and Activate Default Rules
oval:org.open-scap.rhel6:def:1111	true	compliance	CCE-4167-3	Verify ip6tables is enabled
oval:org.open-scap.rhel6:def:1100	true	compliance	CCE-4276-2	Deactivate Wireless Interfaces
oval:org.open-scap.rhel6:def:1086	true	compliance	CCE-3561-8	Network Parameters for Hosts Only
oval:org.open-scap.rhel6:def:1083	true	compliance	CCE-3668-1	Disable MCS Translation Service (mcstrans) if Possible
oval:org.open-scap.rhel6:def:1082	true	compliance	CCE-4148-3	Remove SETroubleshoot if Possible
oval:org.open-scap.rhel6:def:1079	true	compliance	CCE-3977-6	Enable SELinux
oval:org.open-scap.rhel6:def:1066	true	compliance	CCE-3923-0	Set Boot Configuration Permissions
oval:org.open-scap.rhel6:def:1063	true	compliance	TBD	Ensure that Users Don't have .netrc files
oval:org.open-scap.rhel6:def:1058	true	compliance	TBD	Ensure that User Dot-Files are not World-writable
oval:org.open-scap.rhel6:def:1056	true	compliance	CCE-14957-5	Write permissions are disabled for group and other in all directories in Root's Path
oval:org.open-scap.rhel6:def:1055	true	compliance	CCE-3301-9	Ensure that No Dangerous Directories Exist in Root's Path
oval:org.open-scap.rhel6:def:1041	true	compliance	CCE-4009-7	Verify that No Non-Root Accounts Have UID 0
oval:org.open-scap.rhel6:def:1040	true	compliance	CCE-14300-8	Verify that All Account Password Hashes are Shadowed
oval:org.open-scap.rhel6:def:1039	true	compliance	CCE-4238-2	Verify that No Accounts Have Empty Password Fields
oval:org.open-scap.rhel6:def:1036	true	compliance	CCE-14088-9	Limit su Access to the wheel group
oval:org.open-scap.rhel6:def:1035	true	compliance	TBD	Prevent Root Logins to Serial Consoles
oval:org.open-scap.rhel6:def:1032	true	compliance	CCE-4168-1	Enable ExecShield
oval:org.open-scap.rhel6:def:1031	true	compliance	CCE-4247-3	Disable Core Dumps for setuid programs
oval:org.open-scap.rhel6:def:1028	true	compliance	CCE-14794-2	Find world writable directories not owned by a system account

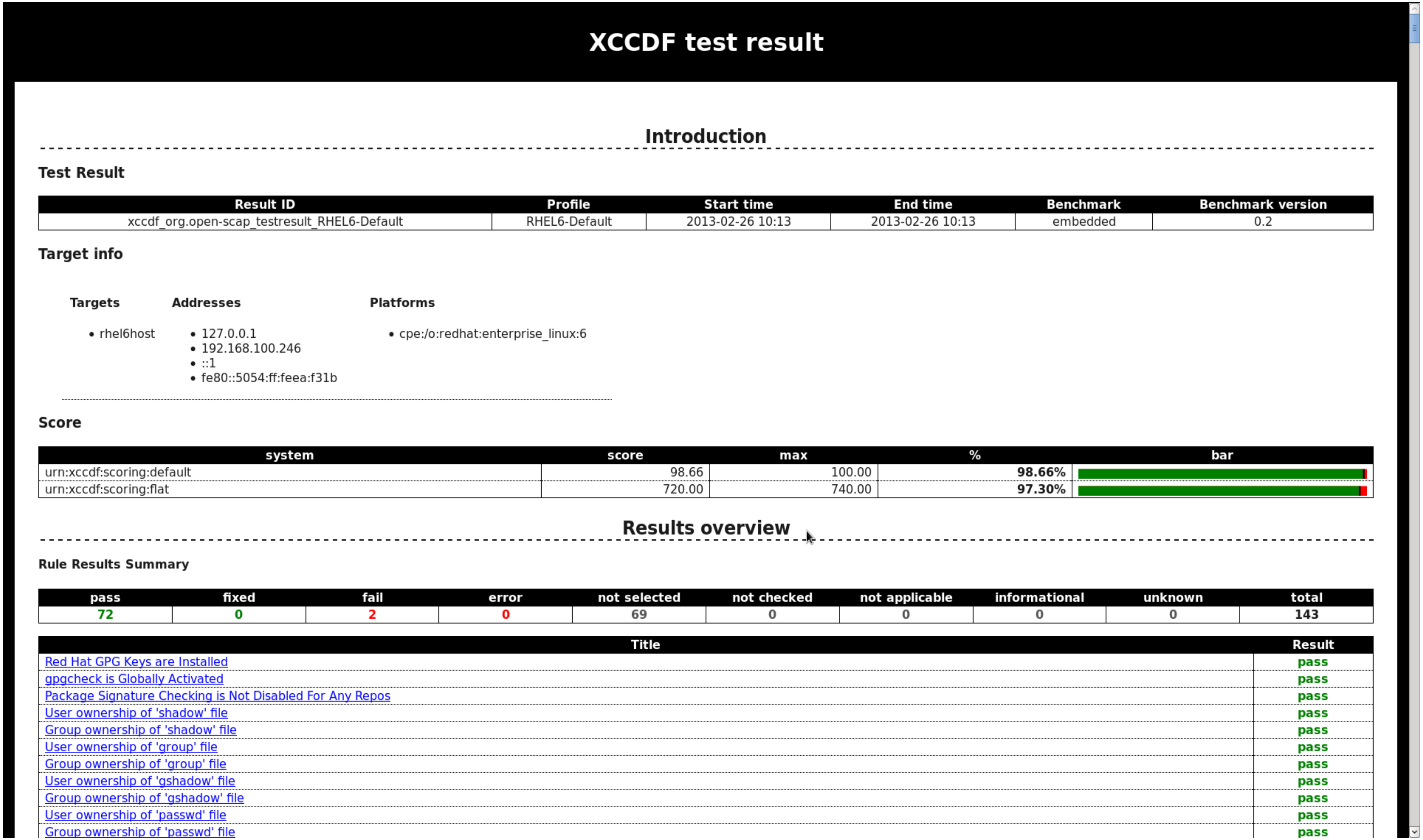
CLI – oscap xccdf

```
[root@rhel6host ~]# oscap xccdf -h
oscap -> xccdf

eXtensible Configuration Checklist Description Format

Usage: oscap [options] xccdf command [command-specific-options]

Commands:
 eval     - Perform evaluation driven by XCCDF file and use OVAL as
            checking engine
 resolve  - Resolve an XCCDF document
 validate - Validate XCCDF XML content
 export-oval-variables - Export XCCDF values as OVAL
                         external-variables document(s)
 generate - Convert XCCDF Benchmark to other formats
```

CLI – XCCDF evaluation

```
[root@rhel6host ~]# oscap xccdf eval \
> --profile RHEL6-default \
> --results xccdf-results.xml \
> --report xccdf-report.html \
> /usr/share/openscap/scap-rhel6-xccdf.xml

Title   Red Hat GPG Keys are Installed
Rule    rule-1005
Ident   CCE-14440-2
Result  pass


Title   gpgcheck is Globally Activated
Rule    rule-1007
Ident   CCE-14914-6
Result  pass
...
```

XCCDF report



XCCDF test result

Introduction

Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_RHEL6-Default	RHEL6-Default	2013-02-26 10:13	2013-02-26 10:13	embedded	0.2

Target info

Targets	Addresses	Platforms
• rhel6host	• 127.0.0.1 • 192.168.100.246 • ::1 • fe80::5054:ff:feea:f31b	• cpe:/o:redhat:enterprise_linux:6

Score

system	score	max	%	bar
urn:xccdf:scoring:default	98.66	100.00	**98.66%**	🟩🟥
urn:xccdf:scoring:flat	720.00	740.00	**97.30%**	🟩🟥

Results overview

Rule Results Summary

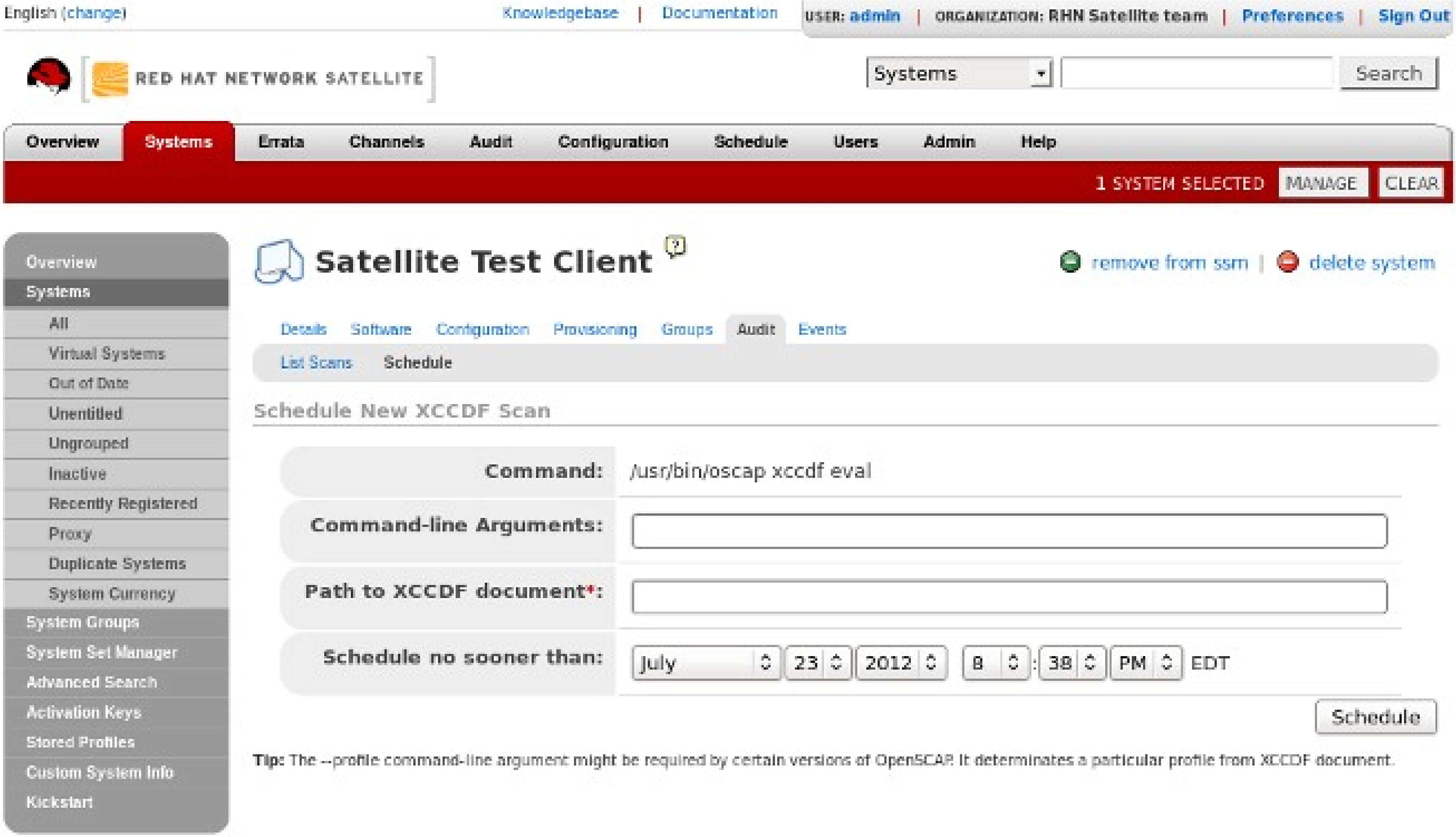
pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
72	0	2	0	69	0	0	0	0	143

Title	Result
Red Hat GPG Keys are Installed	pass
gpgcheck is Globally Activated	pass
Package Signature Checking is Not Disabled For Any Repos	pass
User ownership of 'shadow' file	pass
Group ownership of 'shadow' file	pass
User ownership of 'group' file	pass
Group ownership of 'group' file	pass
User ownership of 'gshadow' file	pass
Group ownership of 'gshadow' file	pass
User ownership of 'passwd' file	pass
Group ownership of 'passwd' file	pass

Spacewalk/Satellite Integration

- Since Spacewalk 1.7, Satellite 5.5
- Scheduling of audit scans (WebUI and via API)
- Client package: spacewalk-openscap (available in rhn-tools channel)
- Additional reports in spacewalk-reports (system-history-scap, scap-scan, scap-scan-results)
- Scan differences in time

RHN Satellite: Schedule Scan



Schedule New XCCDF Scan

Command: /usr/bin/oscap xccdf eval

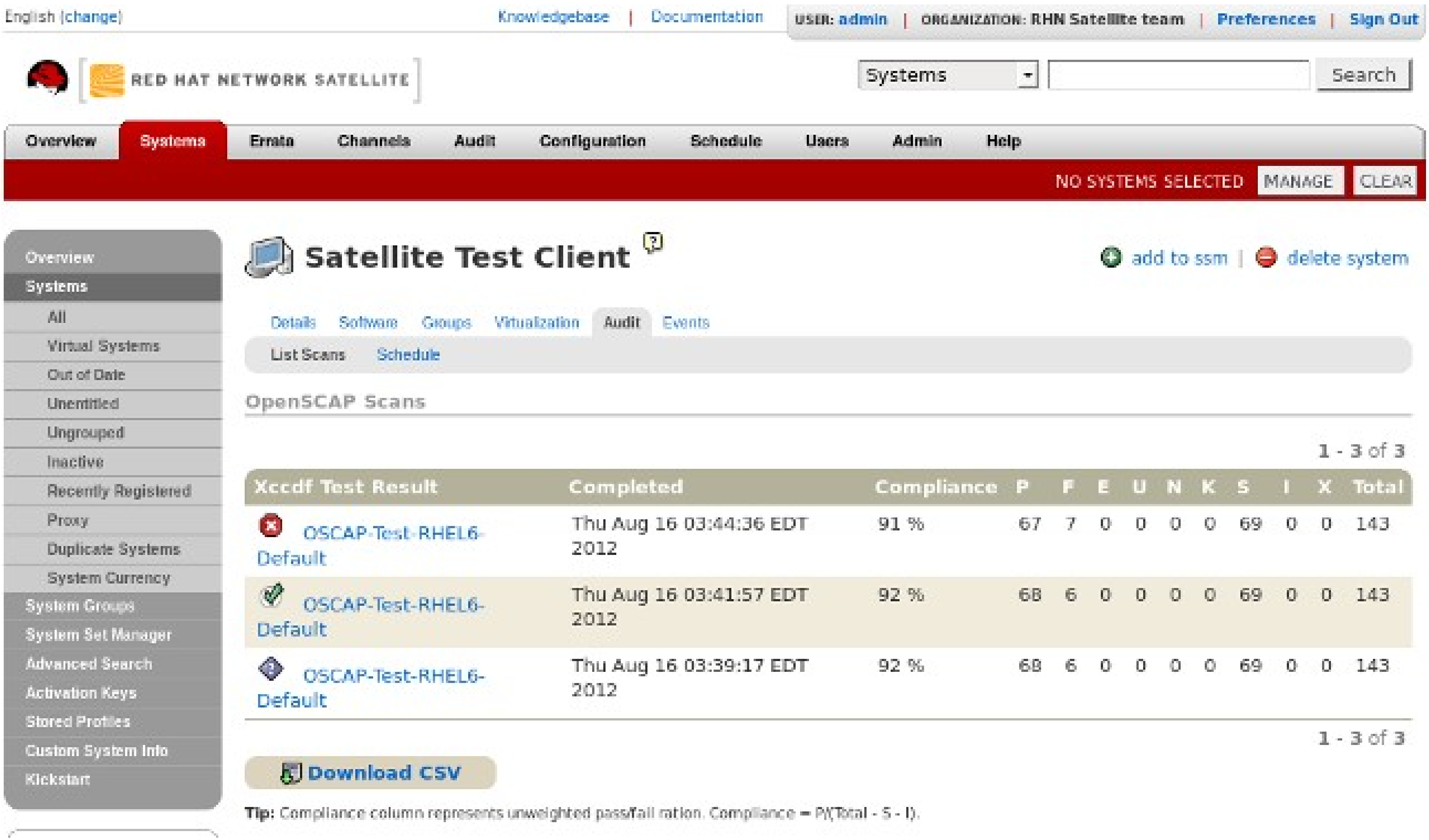
Command-line Arguments:

Path to XCCDF document*:

Schedule no sooner than: July 23 2012 8 : 38 PM EDT

Tip: The --profile command-line argument might be required by certain versions of OpenSCAP. It determinates a particular profile from XCCDF document.

RHN Satellite: List Scans



Satellite Test Client

OpenSCAP Scans

1 - 3 of 3

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
OSCAP-Test-RHEL6-Default	Thu Aug 16 03:44:36 EDT 2012	91 %	67	7	0	0	0	0	69	0	0	143
OSCAP-Test-RHEL6-Default	Thu Aug 16 03:41:57 EDT 2012	92 %	68	6	0	0	0	0	69	0	0	143
OSCAP-Test-RHEL6-Default	Thu Aug 16 03:39:17 EDT 2012	92 %	68	6	0	0	0	0	69	0	0	143

1 - 3 of 3

Tip: Compliance column represents unweighted pass/fail ration. Compliance = P/(Total - S - I).

Content Authoring: OVAL

Contains checks that are used in xccdf

- Low level
- Combination of
  - Definitions
  - Tests
  - Objects
  - States
  - Variables

Validate with: `oscap oval validate <file>`

OVAL tests

- Unix schema
  - dnscache
  - file
  - fileextendedattribute
  - gconf
  - interface
  - password
  - process
  - process58
  - routingtable
  - runlevel
  - shadow
  - sysctl
  - uname
  - xinetd
- Linux schema
  - dpkginfo
  - iflisteners
  - inetlisteningservers
  - partition
  - rpminfo
  - rpmverify
  - selinuxboolean
  - selinuxsecuritycontext
- Independent schema
  - family
  - filehash
  - filehash58
  - environmentvariable
  - environmentvariable58
  - ldap57
  - textfilecontent
  - textfilecontent54
  - xmlfilecontent

OVAL excerpt

```
...
  <definitions>
    <definition class="compliance" id="oval:ssg:def:298" version="1">
      <metadata>
        <title>Verify /etc/shadow Permissions</title>
        <affected family="unix">
          <platform>Red Hat Enterprise Linux 6</platform>
        </affected>
        <description>/etc/shadow must be owned by 0, group owned by 0, and has mode 0000. </description>
      <reference source="ssg" ref_id="file_permissions_etc_shadow"/></metadata>
      <criteria>
        <criterion test_ref="oval:ssg:tst:299"/>
      </criteria>
    </definition>
  </definitions>
  <tests>
    <unix:file_test check="all" check_existence="all_exist"
        comment="/etc/shadow mode and ownership" id="oval:ssg:tst:299" version="1">
      <unix:object object_ref="oval:ssg:obj:1639"/>
      <unix:state state_ref="oval:ssg:ste:1640"/>
      <unix:state state_ref="oval:ssg:ste:1641"/>
      <unix:state state_ref="oval:ssg:ste:1642"/>
    </unix:file_test>
</tests>
...
```

OVAL excerpt

```
...
 <objects>
  <unix:file_object comment="/etc/shadow" id="oval:ssg:obj:1639" version="1">
   <unix:path>/etc</unix:path>
   <unix:filename>shadow</unix:filename>
  </unix:file_object>
 </objects>
 <states>
<unix:file_state id="oval:ssg:ste:1640" version="1">
   <unix:user_id datatype="int" operation="equals">0</unix:user_id>
  </unix:file_state>
  <unix:file_state id="oval:ssg:ste:1641" version="1">
   <unix:group_id datatype="int" operation="equals">0</unix:group_id>
  </unix:file_state>
  <unix:file_state id="oval:ssg:ste:1642" version="1">
   <unix:suid datatype="boolean">false</unix:suid>
   <unix:sgid datatype="boolean">false</unix:sgid>
   <unix:sticky datatype="boolean">false</unix:sticky>
   ...
   <unix:oread datatype="boolean">false</unix:oread>
   <unix:owrite datatype="boolean">false</unix:owrite>
   <unix:oexec datatype="boolean">false</unix:oexec>
  </unix:file_state>
 </states>
...
```

Content Authoring: XCCDF

Reference checks that are defined in oval

- Higher level
- Organized in profiles
- Checks are selected (or not)
- May include report content
- Optional remediation

Validate with:

```
oscap xccdf validate <file>
```

XCCDF excerpt

```
…
<Benchmark>
  <status date="2013-04-04+02:00">draft</status>
  <title>Test XCCDF check for Red Hat Enterprise Linux 6</title>
  <description>This is test content for LOADays</description>
  <reference href="TODO::INSERT"/>
  <platform idref="cpe:/o:redhat:enterprise_linux:6"/>
  <platform idref="cpe:/o:redhat:enterprise_linux:6::client"/>
  <version>0.0.1</version>

  <Rule id="ensure_shadow_permissions" severity="high" selected="true">
        <title>Verify /etc/shadow Permissions</title>
        <description>Ensure /etc/shadow permissions </description>
        <reference/>
        <rationale>It's essential that /etc/shadow has the right permissions</rationale>
        <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
          <check-content-ref href="sample-oval.xml" name="oval:ssg:def:298"/>
        </check>
  </Rule>
</Benchmark>
…
```

Demo

Red Hat provided content

- Openscap-content package

  Oval and xccdf example files

- OVAL definitions for all errata

  http://www.redhat.com/security/data/oval/

- Openscap security guide
  - Open source content

Related projects and resources

- OpenSCAP

    open-scap.org

- Scap Security Guide

    fedorahosted.org/scap-security-guide/

- Simon Lukasik blog

    isimluk.livejournal.com

- NIST and others

    nist.gov

- Red Hat knowledge base and articles

    ex: www.redhat.com/about/news/archive/2013/3/red-hat-openscap-under-evaluation-to-meet-scap-1-2-nist-standard

Summary

- OpenSCAP provides automated, repeatable and interoperable security scanning tools
- SCAP addresses both configuration practices and software vulnarabilities
- Usable STIG and supplier content exist
- Tools and profiles make security auditing manageble

Thank you