

Automated Security Compliance Evaluation of Your Infrastructure with SCAP

Martin Preisler
Red Hat, Inc.

What is our high-level goal?

- set-up our infrastructure with security in mind
- and keep it that way!
- keep costs of the above low
 - full automation!

Prerequisites

- RHEL 7 or CentOS 7
 - preferred
- RHEL 6 or CentOS 6
 - can follow most examples
- Fedora 22
- Windows or MacOS X
 - can follow some examples

Additional repositories

- Base repositories may have old versions
- For latest versions of tools and content, enable these:
 - <https://copr.fedoraproject.org/coprs/isimluk/OpenSCAP/>
 - <https://copr.fedoraproject.org/coprs/mpreisle/SSG/>
- The links have instructions

SCAP Introduction

What is a security policy?

- What it means to secure a system
- Set of rules to follow
 - description
 - rationale
 - how to check
 - how to fix
- Text - PDF, spreadsheet, ...

PCI DSS Requirements	Testing Procedures	Guidance
<p>1.1.5 Description of groups, roles, and responsibilities for management of network components</p>	<p>1.1.5.a Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.</p>	<p>This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.</p>
	<p>1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.</p>	
<p>1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.</p> <p>Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.</p>	<p>1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.</p>	<p>Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed.</p> <p>If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed.</p>
	<p>1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.</p>	
	<p>1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.</p>	

What is SCAP?

- **S**ecurity **C**ontent **A**utomation **P**rotocol
- NIST standard
- express security policies with machine readable code
- several data-formats specified
- XCCDF and OVAL are the main components

Network Configuration and Firewalls

group

Most machines must be connected to a network of some sort, and this brings with it the substantial risk of network attack. This section discusses the security impact of decisions about networking which must be made when configuring a system.

This section also discusses firewalls, network access controls, and other network security frameworks, which allow system-level rules to be written that can limit an attackers' ability to connect to your system. These rules can specify that network traffic should be allowed or denied from certain IP addresses, hosts, and networks. The rules can also specify which of the system's network services are available to particular hosts or networks.

▼ contains 1 rule

IPSec Support

group

Support for Internet Protocol Security (IPsec) is provided in Red Hat Enterprise Linux 7 with Libreswan.

▼ contains 1 rule

Install libreswan Package

rule

The Libreswan package provides an implementation of IPsec and IKE, which permits the creation of secure tunnels over untrusted networks. The `libreswan` package can be installed with the following command:

```
$ sudo yum install libreswan
```

Rationale:

Providing the ability for remote users or systems to initiate a secure VPN connection protects information when it is transmitted over a wide area network.

identifiers: CCE-RHEL7-CCE-TBD

references: [AC-17](#), [MA-4](#), [SC-9](#), [1130](#), [1131](#), [Req-4](#)

Remediation script:

```
yum -y install libreswan
```

Lot of vendors who support SCAP

- 11 certified vendors as of September 2015
- IBM, Microsoft, Red Hat, Tripwire, Saint, Qualys, Intel Security, ...
- <https://nvd.nist.gov/scapproducts.cfm>
- several more vendors implement SCAP but aren't certified
- heterogenous deployments are possible, vendor lock-in is unlikely

Two types of SCAP security policies

- **Vulnerability Assessment**

- detect CVEs
- Heartbleed
- Shellshock
- Ghost
- VENOM

- **Security Compliance**

- proper configuration
- USGCB
- DISA STIG
- PCI-DSS

Two main use-cases

- **Vulnerability Assessment**

- are my machines vulnerable?
 - to Heartbleed?
 - to Shellshock?
 - to Ghost?
 - to VENOM?

- **Security Compliance**

- is root login over ssh forbidden?
- is /tmp on a separate partition?
- are we using strict password policy?
- are obsolete/insecure services removed?
 - telnet, rsh

The world without SCAP

The world without SCAP



Maybe not this bad, but...

- manual compliance
 - error prone
 - doesn't scale
- endless bash scripts
 - dangerous, prone to bugs
 - customization
- proprietary tools
 - vendor lock-in

OpenSCAP

- implementation of SCAP 1.2
- and several standards outside SCAP 1.2
- NIST-certified
- free software - LGPL2+

Goal 1: Vulnerability Assessment

Practical vulnerability assessment

- let us check CVEs on RHEL 7
- workflow:
 - a. download the vulnerability database
 - b. evaluate local machine against the data

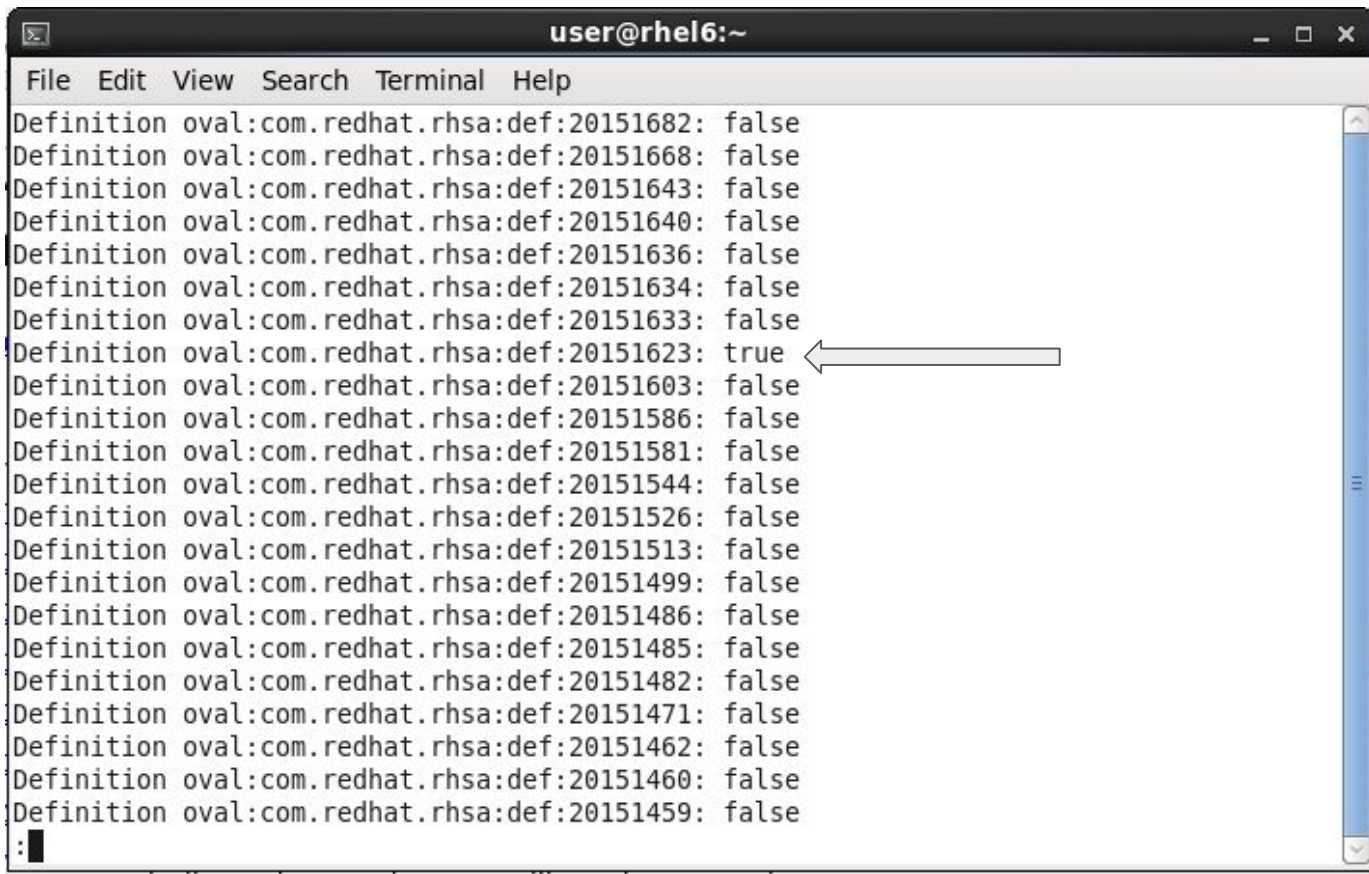
```
# wget http://www.redhat.com/security/data/oval/Red\_Hat\_Enterprise\_Linux\_7.xml
```

```
# oscap oval eval --results /tmp/results.xml --report /tmp/report.html
```

```
Red_Hat_Enterprise_Linux_7.xml
```

```
$ firefox /tmp/report.html
```

Vulnerability assessment results



```
user@rhel6:~  
File Edit View Search Terminal Help  
Definition oval:com.redhat.rhsa:def:20151682: false  
Definition oval:com.redhat.rhsa:def:20151668: false  
Definition oval:com.redhat.rhsa:def:20151643: false  
Definition oval:com.redhat.rhsa:def:20151640: false  
Definition oval:com.redhat.rhsa:def:20151636: false  
Definition oval:com.redhat.rhsa:def:20151634: false  
Definition oval:com.redhat.rhsa:def:20151633: false  
Definition oval:com.redhat.rhsa:def:20151623: true  
Definition oval:com.redhat.rhsa:def:20151603: false  
Definition oval:com.redhat.rhsa:def:20151586: false  
Definition oval:com.redhat.rhsa:def:20151581: false  
Definition oval:com.redhat.rhsa:def:20151544: false  
Definition oval:com.redhat.rhsa:def:20151526: false  
Definition oval:com.redhat.rhsa:def:20151513: false  
Definition oval:com.redhat.rhsa:def:20151499: false  
Definition oval:com.redhat.rhsa:def:20151486: false  
Definition oval:com.redhat.rhsa:def:20151485: false  
Definition oval:com.redhat.rhsa:def:20151482: false  
Definition oval:com.redhat.rhsa:def:20151471: false  
Definition oval:com.redhat.rhsa:def:20151462: false  
Definition oval:com.redhat.rhsa:def:20151460: false  
Definition oval:com.redhat.rhsa:def:20151459: false  
:
```

We are vulnerable!

<div><div><div></div><div>×</div></div><div><div></div><div>✓</div></div><div><div></div><div>Error</div></div><div><div></div><div>Unknown</div></div><div><div></div><div>Other</div></div></div>				
ID	Result	Class	Reference ID	Title
oval:com.redhat.rhsa:def:20151623	true	patch	[RHSA-2015:1623-01], [CVE-2015-5364], [CVE-2015-5366]	RHSA-2015:1623: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151834	false	patch	[RHSA-2015:1834-02], [CVE-2015-4500], [CVE-2015-4506], [CVE-2015-4509], [CVE-2015-4511], [CVE-2015-4517], [CVE-2015-4519], [CVE-2015-4520], [CVE-2015-4521], [CVE-2015-4522], [CVE-2015-7174], [CVE-2015-7175], [CVE-2015-7176], [CVE-2015-7177], [CVE-2015-7180]	RHSA-2015:1834: firefox security update (Critical)
oval:com.redhat.rhsa:def:20151833	false	patch	[RHSA-2015:1833-00], [CVE-2015-5165]	RHSA-2015:1833: qemu-kvm security update (Moderate)
oval:com.redhat.rhsa:def:20151814	false	patch	[RHSA-2015:1814-00], [CVE-2015-5567], [CVE-2015-5568], [CVE-2015-5570], [CVE-2015-5571], [CVE-2015-5572], [CVE-2015-5573], [CVE-2015-5574], [CVE-2015-5575], [CVE-2015-5576], [CVE-2015-5577], [CVE-2015-5578], [CVE-2015-5579], [CVE-2015-5580], [CVE-2015-5581], [CVE-2015-5582], [CVE-2015-5584], [CVE-2015-5587], [CVE-2015-5588], [CVE-2015-6676], [CVE-2015-6677], [CVE-2015-6678], [CVE-2015-6679], [CVE-2015-6682]	RHSA-2015:1814: flash-plugin security update (Critical)
oval:com.redhat.rhsa:def:20151741	false	patch	[RHSA-2015:1741-00], [CVE-2015-3281]	RHSA-2015:1741: haproxy security update (Important)
oval:com.redhat.rhsa:def:20151715	false	patch	[RHSA-2015:1715-00], [CVE-2015-3247]	RHSA-2015:1715: spice-server security update (Important)
oval:com.redhat.rhsa:def:20151712	false	patch	[RHSA-2015:1712-00], [CVE-2015-1291], [CVE-2015-1292], [CVE-2015-1293], [CVE-2015-1294], [CVE-2015-1295], [CVE-2015-1296], [CVE-2015-1297], [CVE-2015-1298], [CVE-2015-1299], [CVE-2015-1300], [CVE-2015-1301]	RHSA-2015:1712: chromium-browser security update (Important)
oval:com.redhat.rhsa:def:20151708	false	patch	[RHSA-2015:1708-00], [CVE-2015-1802], [CVE-2015-1803], [CVE-2015-1804]	RHSA-2015:1708: libXfont security update (Important)

Fix: Install updates and reboot

- `# yum update`
- remove the old vulnerable kernel
- `# reboot`

oval:com.redhat.rhsa:def:20151643	false	patch	[RHSA-2015:1643-00], [CVE-2015-3636]	kernel security and bug fix update (Moderate)
oval:com.redhat.rhsa:def:20151640	false	patch	[RHSA-2015:1640-00], [CVE-2015-3238]	RHSA-2015:1640: pam security update (Moderate)
oval:com.redhat.rhsa:def:20151636	false	patch	[RHSA-2015:1636-00], [CVE-2015-5621]	RHSA-2015:1636: net-snmp security update (Moderate)
oval:com.redhat.rhsa:def:20151634	false	patch	[RHSA-2015:1634-00], [CVE-2015-3416]	RHSA-2015:1634: sqlite security update (Moderate)
oval:com.redhat.rhsa:def:20151633	false	patch	[RHSA-2015:1633-00], [CVE-2015-0248], [CVE-2015-0251], [CVE-2015-3187]	RHSA-2015:1633: subversion security update (Moderate)
oval:com.redhat.rhsa:def:20151623	false	patch	[RHSA-2015:1623-01], [CVE-2015-5364], [CVE-2015-5366]	RHSA-2015:1623 : kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151603	false	patch	[RHSA-2015:1603-01], [CVE-2015-5127], [CVE-2015-5128], [CVE-2015-5129], [CVE-2015-5130], [CVE-2015-5131], [CVE-2015-5132], [CVE-2015-5133], [CVE-2015-5134], [CVE-2015-5539], [CVE-2015-5540], [CVE-2015-5541], [CVE-2015-5544], [CVE-2015-5545], [CVE-2015-5546], [CVE-2015-5547], [CVE-2015-5548], [CVE-2015-5549], [CVE-2015-5550],	RHSA-2015:1603: flash-plugin security

How does CVE scanning work?

- RHSA OVAL feed is a list of RHSAs
- Each item contains associated CVE IDs
- Each item contains a list of affected packages and versions
- OpenSCAP goes over all CVE items and evaluates whether your system has any affected package
- If so, OpenSCAP reports that the system is vulnerable

Implications:

- We only detect known vulnerabilities
- We only detect what Red Hat has fixed

What about other OSes?

- CVE scanning requires OS vendor support
- CVE database files are required
- currently supported by Red Hat, SUSE, Oracle and Canonical

Goal 2: Security Compliance

Security Compliance

- pro-active security
- machines configured according to rules
- most commonly the rules try to:
 - reduce attack surface
 - enforce auditing
 - harden the system
- often a requirement for government contractors
- often a requirement for businesses

Goals

- a security policy that doesn't break functionality
- based on the PCI-DSS draft profile
- add rules specific to our use-case
- remove some of the rules that threaten existing functionality

RHEL 7 PCI-DSS compliance

Compliance and Scoring

The target system did not satisfy the conditions of 44 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules

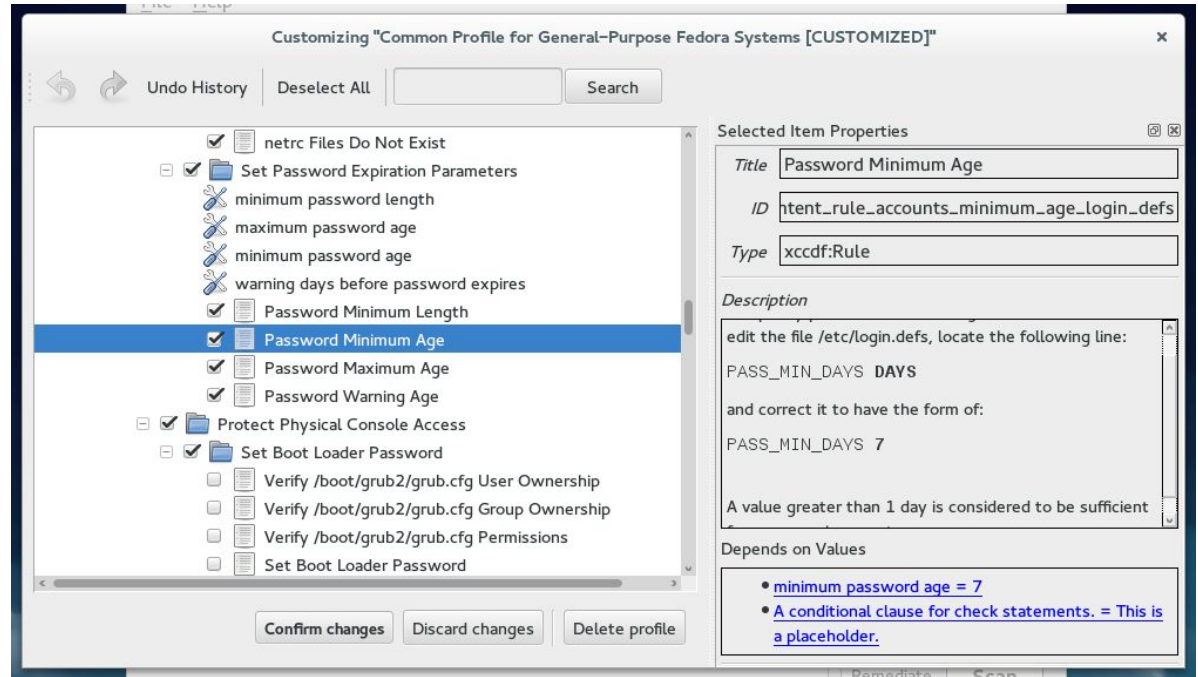


Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	64.126724	100.000000	<div><div>64.13%</div></div>

XCCDF profile

- benchmark vs. profile
- which rules are selected
- what values are used
 - password length



SCAP Security Guide

- community driven, very active, contributors welcome!
- open source - public domain
- many products:
 - RHEL 5, 6, 7
 - Firefox
 - JRE
- many profiles:
 - USGCB
 - PCI-DSS
 - STIG
- <http://static.open-scap.org/ssg-guides/ssg-rhel7-guide-index.html>

SCAP Workbench

- GPLv3+, free software
- graphical user interface for OpenSCAP
- scan local machines
- scan remote machines
- **customize security policies**

Shopping list

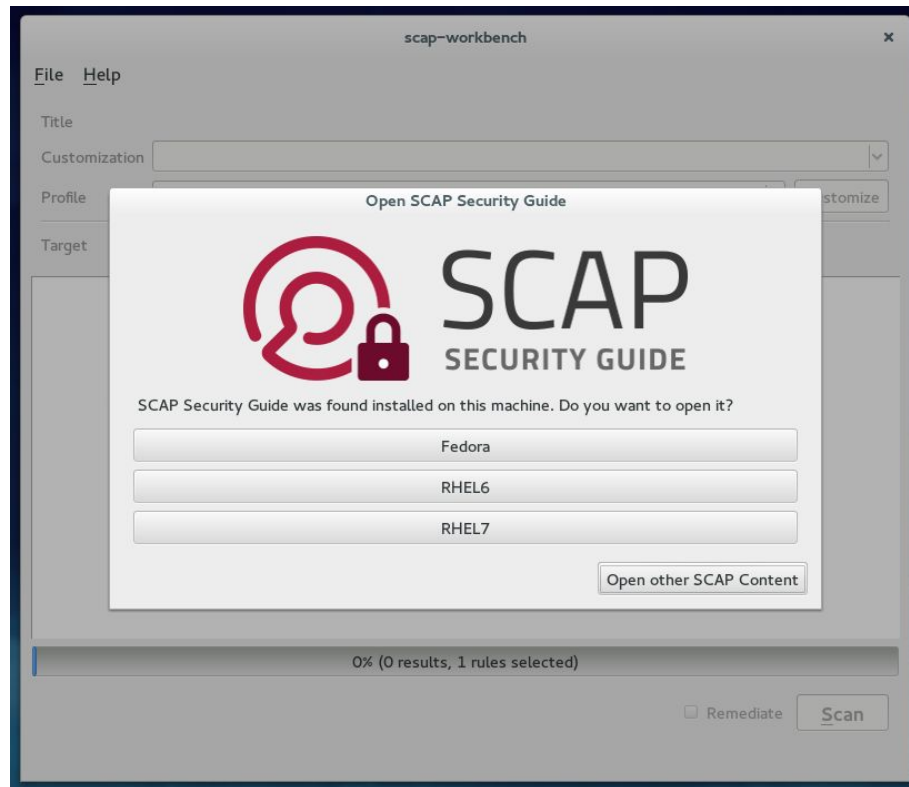
- Linux desktop or Windows or MacOS X
 - you already have it
 - **RHEL 7** or **CentOS 7** recommended
- SCAP Security Guide
 - public domain, free!
- SCAP Workbench
 - GPLv3+, free!

#yum install scap-workbench

<https://github.com/OpenSCAP/scap-workbench/releases>

Start SCAP Workbench, select content

- `$ scap-workbench`
- Select the content based on the machine you want to scan



Initial scan

- select the “PCI-DSS v3” profile
- scan without any customization to establish baseline
- get a list of failing rules to handle
- for simplicity we will scan local machine
- in practice you would most likely scan a remote server



home



Trash

File Help

Title Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Customization (no customization)

Profile Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

Customize

Target ☒ Local Machine

☐ Remote Machine (over SSH)

- ▶ Install AIDE
- ▶ Disable Prelinking
- ▶ Configure Periodic Execution of AIDE
- ▶ Verify and Correct File Permissions with RPM
- ▶ Verify File Hashes with RPM
- ▶ Verify User Who Owns shadow File
- ▶ Verify Group Who Owns shadow File
- ▶ Verify Permissions on shadow File
- ▶ Verify User Who Owns group File
- ▶ Verify Group Who Owns group File
- ▶ Verify Permissions on group File

fail

fail

fail

fail

pass

pass

pass

pass

pass

pass

pass

100% (82 results, 82 rules selected)

Clear

Save Results

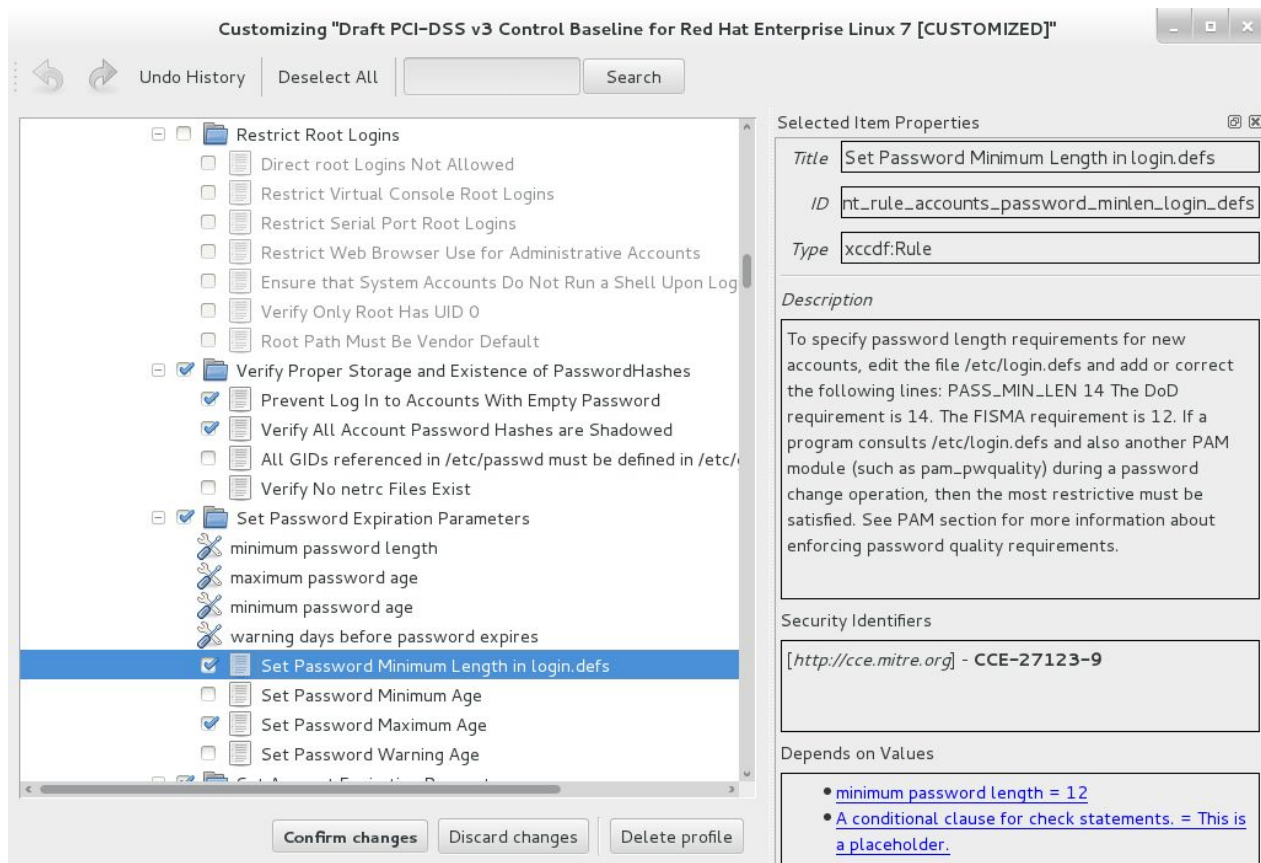
Show Report

Browsing the results

- ARF vs. XCCDF result
- HTML report
- OVAL details

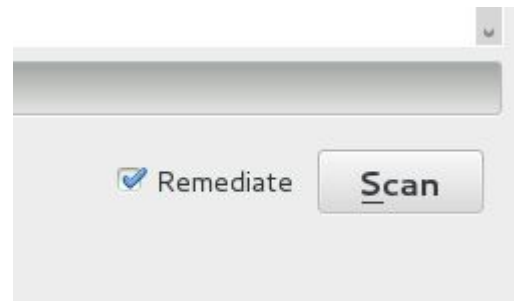
Enable GNOME3 Screensaver Lock After Idle Period	medium	fail
▶ Configure Console Screen Locking		
▶ Hardware Tokens for Authentication		
▶ Warning Banners for System Accesses		
▶ Network Configuration and Firewalls		
▶ Configure Syslog		
▼ System Accounting with auditd 34x fail 1x notchecked		
▼ Configure auditd Data Retention 3x fail		
Configure auditd Number of Logs Retained	medium	pass
Configure auditd Max Log File Size	medium	pass
Configure auditd max_log_file_action Upon Reaching Maximum Log Size	medium	pass
Configure auditd space_left Action on Low Disk Space	medium	fail
Configure auditd admin_space_left Action on Low Disk Space	medium	fail
Configure auditd mail_acct Action on Low Disk Space	medium	pass
Configure auditd to use audispd's syslog plugin	medium	fail
▼ Configure auditd Rules for Comprehensive Auditing 20x fail		

Making adjustments



Remediation

- We now have a profile defined
- We still need to change configuration of the machine
- Remediation **cannot be undone!**
 - consider saving a snapshot of the VM
 - this is potentially dangerous!



Remediation

ssg-centos7-ds.xml - SCAP Workbench

File Help

Title Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Customization (unsaved changes)

Profile Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 [CUSTOMIZED] Customize

Target ☒ Local Machine ☐ Remote Machine (over SSH)

▶ Record Events that Modify the System's Discretionary Access Controls - removexattr	fixed
▶ Record Events that Modify the System's Discretionary Access Controls - setxattr	fixed
▶ Record Attempts to Alter Logon and Logout Events	fail
▶ Record Attempts to Alter Process and Session Initiation Information	fixed
▶ Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)	fixed
▶ Ensure auditd Collects Information on the Use of Privileged Commands	fail
▶ Ensure auditd Collects Information on Exporting to Media (successful)	fixed
▶ Ensure auditd Collects File Deletion Events by User	fixed
▶ Ensure auditd Collects System Administrator Actions	fixed
▶ Ensure auditd Collects Information on Kernel Module Loading and Unloading	fixed
▶ Make the auditd Configuration Immutable	fail

100% (82 results, 82 rules selected)

Processing has been finished!

Clear Save Results Show Report

Save the final policy

- View the report to verify
- Click File -> Save Customization Only

RHEL 7 PCI-DSS compliance: Final result

Compliance and Scoring

The target system did not satisfy the conditions of 1 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	98.958328	100.000000	98.96%

What about other profiles?

- the same can be done with other SSG profiles
- USGCB
- DISA STIG
- CCP = Certified Cloud Provider
- ...

What if we need new rules?

- writing SCAP content from scratch is hard
- very very hard, steep learning curve, very few skills transfer
- collaborate with other projects, use their infrastructure
- SCAP Security Guide is a very good SCAP content upstream
 - check out <https://github.com/OpenSCAP/scap-security-guide>

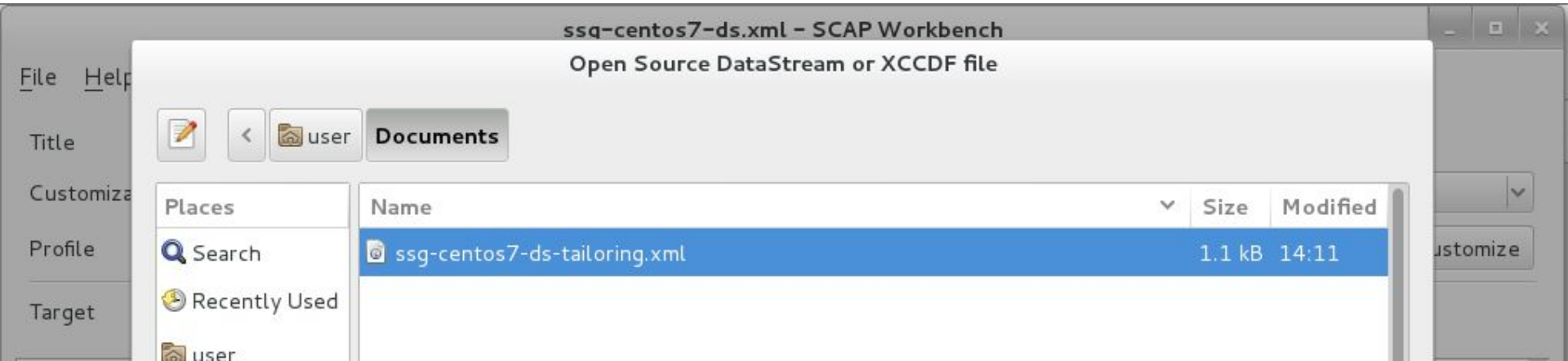
Goal 3: Deploying Compliance Policy

Our Compliance Policy

- original content comes from SCAP Security Guide
- customization file is separate
- customization file is all we take from previous demonstration
- SSG can be updated while we keep using the same customization file

SCAP Workbench

- already discussed



`oscap`

- NIST-certified!
- command line
- `# yum install openscap-scanner scap-security-guide`
- `# oscap xccdf eval --tailoring-file ssg-rhel7-ds-tailoring.xml --profile xccdf_org.ssgproject.content_profile_pci-dss_customized /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml`
- replace *rhel7* with *centos7* if necessary
- `--report report.html` to get the HTML report

`oscap` scanning

Ident CCE-RHEL7-CCE-TBD

Result **pass**

Title **Ensure Logrotate Runs Periodically**

Rule xccdf_org.ssgproject.content_rule_ensure_logrotate_activated

Ident CCE-RHEL7-CCE-TBD

Result **pass**

Title **Enable auditd Service**

Rule xccdf_org.ssgproject.content_rule_service_auditd_enabled

Ident CCE-RHEL7-CCE-TBD

Result **notchecked**

Title **Enable Auditing for Processes Which Start Prior to the Audit Daemon**

Rule xccdf_org.ssgproject.content_rule_bootloader_audit_argument

Ident CCE-RHEL7-CCE-TBD

Result **pass**

Title **Configure auditd Number of Logs Retained**

Rule xccdf_org.ssgproject.content_rule_auditd_data_retention_num_logs

Ident CCE-RHEL7-CCE-TBD

Result **pass**

Title **Configure auditd Max Log File Size**

Rule xccdf_org.ssgproject.content_rule_auditd_data_retention_max_log_file

Ident CCE-RHEL7-CCE-TBD

Result **pass**

Title **Configure auditd max_log_file_action Upon Reaching Maximum Log Size**

Rule xccdf_org.ssgproject.content_rule_auditd_data_retention_max_log_file_act
ion

Ident CCE-RHEL7-CCE-TBD

Result **pass**

`oscap` optional arguments

- --remediate
- --results
- --results-arf
- --report

`oscap info`

- Show info about given SCAP file
- List profiles for XCCDFs or DataStreams

`oscap` is powerful but also complex

- we provide wrapper scripts for common use-cases
- remote machine scanning
- container scanning
- virtual machine scanning

`oscap-ssh`

- scan remote machines using ssh
- wrapper around oscap
- command line
- similar arguments as `oscap`
- `$ oscap-ssh root@192.168.1.2 22 xccdf eval --tailoring-file ssg-rhel7-ds-tailoring.xml --profile xccdf_org.ssgproject.content_profile_pci-dss_customized /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml`
- replace *rhel7* with *centos7* if necessary
- Online scan

`oscap-vm`

- scan local virtual machines or their storage images
- wrapper around oscap
- command line
- similar arguments as `oscap`
- convenient CVE scanning
- ```
$ oscap-vm domain $ID xccdf eval --tailoring-file ssg-rhel7-ds-tailoring.xml --
profile xccdf_org.ssgproject.content_profile_pci-dss_customized
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```
- Offline scan

# `oscap-docker`

- scan local containers or container images
- wrapper around oscap
- command line
- similar arguments as `oscap`
- convenient CVE scanning
- ```
$ oscap-docker container $ID xccdf eval --tailoring-file ssg-rhel7-ds-tailoring.xml --profile xccdf_org.ssgproject.content_profile_pci-dss_customized /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```
- Offline scan

OSCAP Anaconda Addon

- GUI support
- kickstart support
- Compliance at first boot



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

PRE-RELEASE / TESTING

us

Help!

LOCALIZATION



DATE & TIME

Americas/New York timezone



KEYBOARD

English (US)



LANGUAGE SUPPORT

English (United States)

SECURITY



SECURITY POLICY

No profile selected



SOFTWARE



INSTALLATION SOURCE

http://192.168.122.1/virtuals/rhel7_repo/



SOFTWARE SELECTION

Minimal Install

SYSTEM



INSTALLATION DESTINATION

Automatic partitioning selected



KDUMP

Kdump is enabled



NETWORK & HOST NAME

Quit

Begin Installation

We won't touch your disks until you click 'Begin Installation'.

Done

 us

Help!

Change content

Apply security policy:

ON

Choose profile below:

Default

The implicit XCCDF profile. Usually, the default contains no rules.

Standard System Security Profile

This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.

Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

This is a *draft* profile for PCI-DSS v3

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

This is a *draft* SCAP profile for Red Hat Certified Cloud Providers

Common Profile for General-Purpose Systems

This profile contains items common to general-purpose desktop and server installations.

Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server

This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

Select profile

Changes that were done or need to be done:



No profile selected

Goal 4: Deploying Compliance Policy for multiple machines

Satellite 6

- Red Hat product
- Systems Management
- SCAP integration
 - compliance of many machines
- Foreman, SCAPTimony and OpenSCAP

Satellite 6

SCAP Contents

Filter ... ▾

Title
Red Hat rhel6 default content
Red Hat rhel7 default content

File Upload

Locations

Organizations

Title *

Scap file * No file chosen

Upload SCAP DataStream file


Notice: You need to [install](#) OpenSCAP on your hosts, and upload this content to the hosts as well.

Satellite 6

▼ System Settings 25x fail 1x notchecked		
▼ Installing and Maintaining Software 6x fail 1x notchecked		
▼ Disk Partitioning 4x fail		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
▼ Updating Software 1x fail 1x notchecked		
Ensure Red Hat GPG Key Installed	high	pass
Ensure gpgcheck Enabled In Main Yum Configuration	high	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	high	fail
Ensure Software Patches Installed	high	notchecked
▼ Software Integrity Checking 1x fail		
▼ Verify Integrity with AIDE 1x fail		
Install AIDE	medium	fail
▶ Verify Integrity with RPM		
▶ Additional Security Software		
▶ File Permissions and Masks		
▶ SELinux		
▼ Account and Access Control 16x fail		
▼ Protect Accounts by Restricting Password-Based Login 3x fail		
▶ Protect Passwords		

Satellite 5 / Spacewalk

[English \(change\)](#) | [Knowledgebase](#) | [Documentation](#) | USER: [mlessard](#) | ORGANIZATION: [Red Hat](#) | [Preferences](#) | [Sign Out](#)

 RED HAT NETWORK SATELLITE

Systems

[Overview](#) | **[Systems](#)** | [Errata](#) | [Channels](#) | [Audit](#) | [Configuration](#) | [Schedule](#) | [Users](#) | [Admin](#) | [Help](#)

NO SYSTEMS SELECTED

Overview

Systems

All

Virtual Systems

Out of Date

Untitled

Ungrouped

Inactive

Recently Registered

Proxy

Duplicate Systems

System Currency

System Groups

System Set Manager



Advanced Search

Activation Keys

Stored Profiles

Custom System Info

Kickstart










 **vm1.mlc.dom** 

[Details](#) | [Software](#) | [Configuration](#) | [Provisioning](#) | [Groups](#) | **[Audit](#)** | [Events](#)


[List Scans](#) | [Schedule](#)

OpenSCAP Scans

1 - 9 of 9

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
 xccdf_org.open-scap_testresult_stig-rhel6-server	Thu Jun 27 12:58:22 EDT 2013	40 %	90	97	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 15:52:26 EDT 2013	40 %	90	97	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 09:11:43 EDT 2013	39 %	88	99	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 09:05:11 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Wed Jun 19 08:45:35 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Fri Jun 14 10:02:35 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Tue Jun 11 10:43:36 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_stig-rhel6-server	Tue Jun 11 10:40:14 EDT 2013	39 %	87	100	1	3	0	32	184	0	0	407
 xccdf_org.open-scap_testresult_default-profile	Tue Jun 11 10:38:07 EDT 2013	N/A	0	0	0	0	0	0	407	0	0	407

1 - 9 of 9

 [Download CSV](#)

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

Future: OpenSCAP-daemon

- early stages
- a service providing a dbus API
- unified scanning interface
 - local, remote machines
 - containers
 - virtual machines
- Atomic integration
- Plan: Cockpit integration
- interactive command line interface
- CVE scanning

Where to go from here?

- <http://www.open-scap.org>
 - home page
- <http://static.open-scap.org>
 - documentation, user manuals, HTML guides for SSG
- <https://github.com/OpenSCAP>
 - we appreciate feedback
 - we appreciate pull requests even more!

Questions?

- @MartinPreisler
- mpreise@redhat.com
- @OpenSCAP
- <https://www.redhat.com/mailman/listinfo/open-scap-list>

Slides and other materials will be available at <http://martin.preisler.me/slides/>

Thanks for your attention!

SCE

- Alternative to OVAL
- Any executable as a check
 - bash
 - python
 - ...
- A way to gradually move to SCAP