



redhat.

Security Compliance for Containers and VMs with OpenSCAP

Automatically find vulnerabilities and configuration issues of your infrastructure

Martin Preisler
@MartinPreisler
mpreisle@redhat.com
Senior Software Engineer, Red Hat, Inc.

GOALS

- Hands on demos of real world use-cases
- Check software flaws - vulnerabilities
- Check configuration flaws - weaknesses
- Customizing existing security policies
- Automate everything
- Scale it to an infrastructure level

NON-GOALS

- We have very limited time
- Won't cover extensive theory
- Won't cover writing SCAP policies - out of scope

Feel free to catch me after the talk to discuss these!

FOLLOW ALONG!

- You can follow along the demos
- Red Hat Enterprise Linux 7 or CentOS 7 preferred
- Fedora, OpenSuse, Debian or Ubuntu work in some cases
- I will use various distributions for demos

CHECKING FOR VULNERABILITIES

VULNERABILITY

what is a software vulnerability...

- A weakness that can be exploited by a threat
- A weakness in the software that allows attacker to reduce information assurance
- Can lead to compromise of security

VULNERABILITIES

Undiscovered vulnerabilities are bad.

- But not all that bad, everybody has them
- It's a lot of effort to use those for exploits
- Mitigate with SELinux or AppArmor

VULNERABILITIES

Known vulnerabilities are *much worse*.

- CVE-2016-1283
- Details are publicly available
- Ready-made exploits often publicly available

VULNERABILITIES

Known vulnerabilities are sometimes so bad that they have *fancy names*!

- Shellshock, POODLE, VENOM, ...

VULNERABILITIES

... and sometimes even logos!

Known vulnerabilities:

- assigned CVEs - CVE-2014-0160
- details are public for everyone
- ready-made exploits may be available



VULNERABILITIES

Not all vulnerabilities are equal.

Let's prioritize:

- all vulnerabilities are dangerous
- there is not much we can do about the undiscovered ones
- let's **never** have any **known** ones in our infrastructure!

USE-CASE 1: AUTOMATICALLY CHECK VULNERABILITIES

SCAP VULNERABILITY SCANNING

A standardized way to scan for vulnerabilities.

- Prerequisites: CVE feed, SCAP scanner
- CVE feed contains a database of CVEs
 - With version ranges of affected software
 - Supplied by software vendor

OPENS CAP

open-source SCAP 1.2 implementation

- [certified by NIST since 2014](#)
- library and a command-line interface
- GUI frontend is available - *SCAP Workbench*



VULNERABILITY ASSESSMENT ON RHEL 6

Let's discuss how to scan a single Red Hat Enterprise Linux 6 machine.

There are three steps to perform:

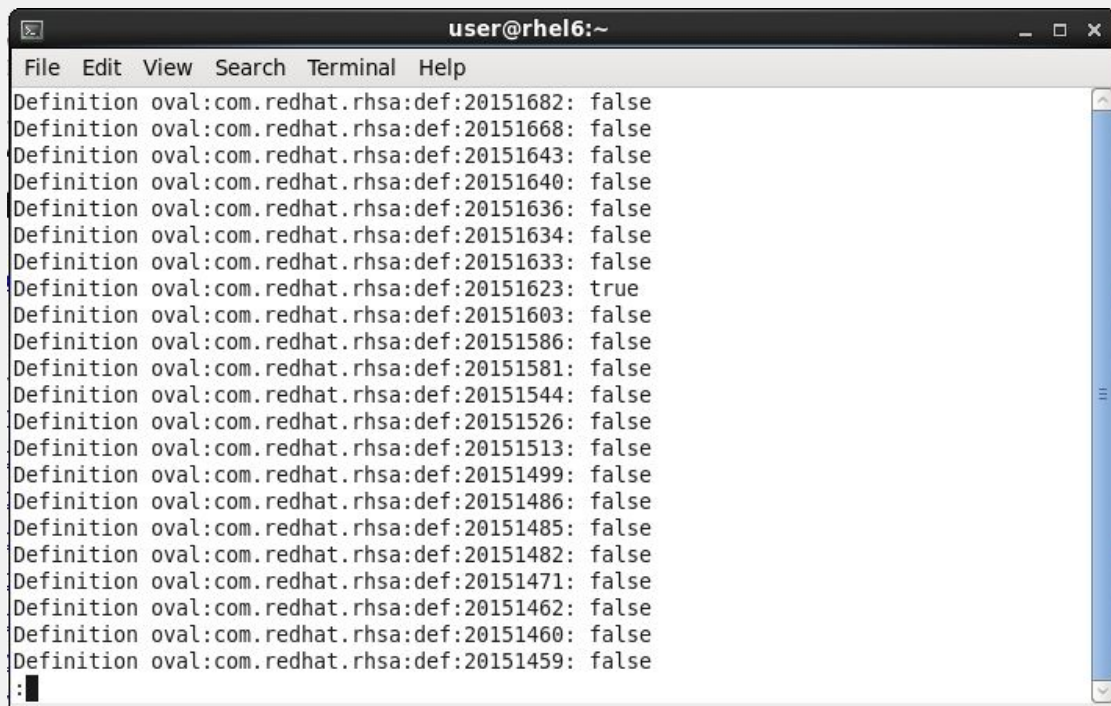
1. Download the CVE data
2. Execute the oscap tool
3. Review the results

COMMANDS TO SCAN RHEL 6 FOR CVEs

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
# oscap oval eval --results /tmp/results.xml --report /tmp/report.html
Red_Hat_Enterprise_Linux_6.xml
# firefox /tmp/report.html
```


VULNERABILITY SCAN RESULTS

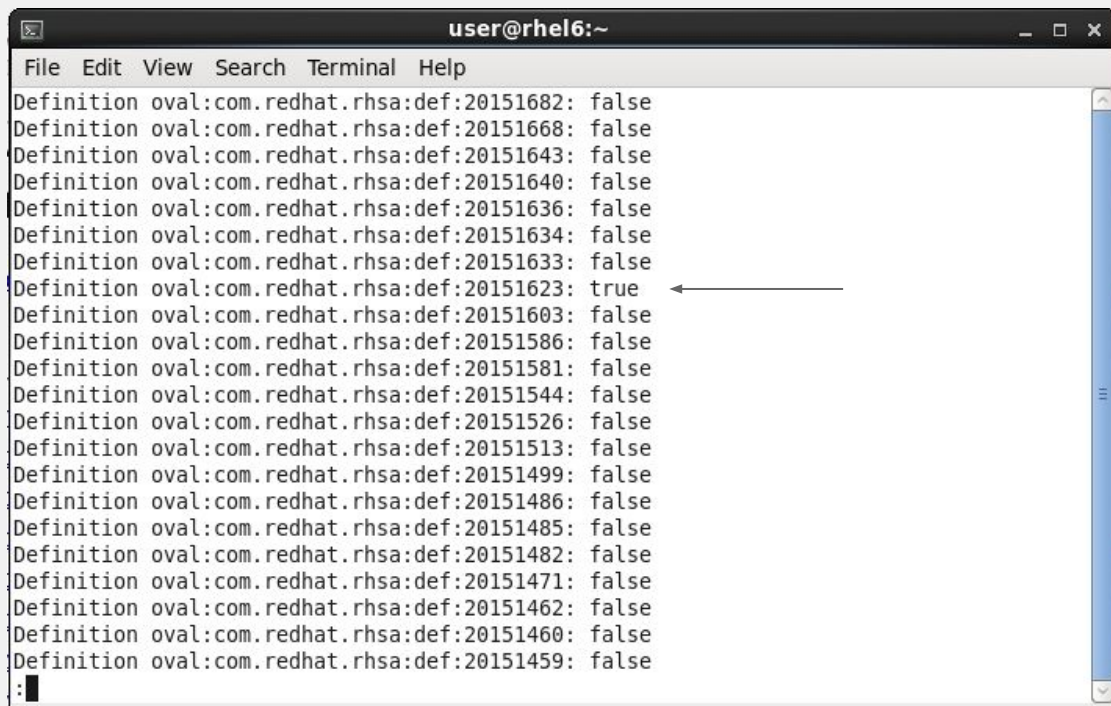
After the command is invoked this is what we can see in stdout.

A terminal window titled 'user@rhel6:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The window displays a list of 20 vulnerability definitions from Red Hat Security Advisories (RHSA). Each line follows the format 'Definition oval:com.redhat.rhsa:def:20151682: false'. The 8th entry, 'Definition oval:com.redhat.rhsa:def:20151623: true', is highlighted with a blue background. The terminal ends with a prompt character ':'.

```
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  
:  
:
```

VULNERABILITY SCAN RESULTS

After the command is invoked this is what we can see in stdout.

A terminal window titled 'user@rhel6:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The window displays a list of 20 vulnerability definitions. Each line follows the format 'Definition oval:com.redhat.rhsa:def:20151682: false'. The 9th line, 'Definition oval:com.redhat.rhsa:def:20151623: true', is highlighted with a blue background and has a white arrow pointing to it from the right. The terminal ends with a prompt character ':|'.

```
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  
:|
```

VULNERABILITY SCAN RESULTS

Let's see more details by opening the HTML report.

<div><div><div>×</div><div>✓</div><div>Error</div><div>Unknown</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)

VULNERABILITY SCAN RESULTS

After installing system updates and rebooting the vulnerability is gone.

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

DEMO on Red Hat Enterprise Linux 7.3

ADVANTAGES

A.k.a. “Why don’t you just run ``yum check-update``?”

- Works offline
- Works if a repository is completely missing
- ... or outdated
- Even if yum is not available

IMPORTANT CAVEATS

Limitations of OpenSCAP vulnerability scanning.

- Only detects vulnerabilities in Red Hat packages
 - Not in EPEL
 - Not in 3rd party vendor repos
 - Not in software that doesn't come from RPMs
- Only detects vulnerabilities important enough to be fixed in RHSAs

CVE FEEDS FOR OTHER OSeS

- Canonical provides CVE feeds for Ubuntu
 - Use <https://people.canonical.com/~ubuntu-security/oval/>
- SUSE provides CVE feeds for SLES and others
 - Use <https://support.novell.com/security/oval/>

DEMO on openSUSE 13.2

(--skip-valid to save time, validating openSUSE OVAL takes ~4 minutes in the VM)

WHAT ABOUT CONTAINERS?

Scanning containers one by one like this is impractical...

Production deployments are increasingly using containers. This brings new challenges.

- installing the oscap tool in every container is impractical
- single-purpose containers → many different containers and images

ONLINE vs. OFFLINE SCANNING

- Running oscap on scanned machine is **online scanning**
- Offline scanning works without installing OpenSCAP on the target
 - Scan a VFS root
 - Scan VM storage image
 - Scan a container
- Offline scanning is limited
 - Cannot query processes, DBus, etc...

OSCAP-DOCKER

Wrapper around oscap, uses offline scanning

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
# oscap-docker container $ID oval eval --results /tmp/results.xml
--report /tmp/report.html Red_Hat_Enterprise_Linux_6.xml
# firefox /tmp/report.html
```

OSCAP-CHROOT

A more generic wrapper around oscap, uses offline scanning

```
# cd /tmp
# wget https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_6.xml
mount any VFS to /mnt/scan-target - container, VM storage, etc...
# oscap-chroot /mnt/scan-target oval eval --results /tmp/results.xml
--report /tmp/report.html Red_Hat_Enterprise_Linux_6.xml
# firefox /tmp/report.html
```

ATOMIC SCAN

New feature in Atomic 1.4, functionality reworked in 1.10

Scan containers and container images for CVEs.

```
# atomic scan 59d5a49b0f75
```

```
59d5a49b0f75 (registry.access.redhat.com/rhel6:latest)
```

```
59d5a49b0f75 passed the scan
```

ATOMIC SCAN

New feature in Atomic 1.4, functionality reworked in 1.10

```
# atomic scan rhel7.2
```

```
rhel7.2 (c453594215e4370)
```

The following issues were found:

```
RHSA-2016:1025: pcre security update (Important)
```

```
Severity: Important
```

```
RHSA URL: https://rhn.redhat.com/errata/RHSA-2016-1025.html
```

```
RHSA ID: RHSA-2016:1025-00
```

```
Associated CVEs:
```

```
    CVE ID: CVE-2015-2328
```

```
    CVE URL: https://access.redhat.com/security/cve/CVE-2015-2328
```

```
    CVE ID: CVE-2016-3191
```

```
    CVE URL: https://access.redhat.com/security/cve/CVE-2016-3191
```

Files associated with this scan are in
/var/lib/atomic/openscap/2016-06-07-10-27-59-394638.

DEMO on Red Hat Enterprise Linux 7.3

(atomic is in extras)

ATOMIC SCAN WITH MULTIPLE TARGETS

Scan all your containers and container images with a single command.

Three options are available, scan all containers, scan all images and scan both.

- `atomic scan --containers`
- `atomic scan --images`
- `atomic scan --all`

HOW DOES ATOMIC SCAN WORK?

we can't trust what we don't understand...

DETECT OS VERSION

Different operating systems have different CVEs.

DOWNLOAD CVE FEED

Based on the OS version we download CVE feed from the vendor.

MOUNT CONTAINER, RUN OSCAP-CHROOT

Atomic does all the mounting.

OpenSCAP compares installed versions with version ranges in the CVE feed.

CHECKING FOR SECURITY COMPLIANCE

TWO TYPES OF SCAP SECURITY POLICIES

VULNERABILITY ASSESSMENT

detect CVEs

Heartbleed

Shellshock

Ghost

VENOM

...

SECURITY COMPLIANCE

proper configuration

hardening

USGCB

PCI-DSS

DISA STIG

...

TWO SCAP USE-CASES

VULNERABILITY ASSESSMENT

are my machines vulnerable to:

Heartbleed?

Shellshock?

Ghost?

VENOM?

...?

SECURITY COMPLIANCE

is root login over ssh forbidden?

is SELinux enabled and enforcing?

are we using strict password policy?

are obsolete / insecure services
disabled?

...?

SCAP CONSUMERS

VULNERABILITY ASSESSMENT

Everybody who has an attack surface

SECURITY COMPLIANCE

Regulatory:

- Government agencies, contractors
- Financial companies
- Health care, Energy
- ...

Pro-active security

USE-CASE 2: SECURITY COMPLIANCE FOR A SINGLE MACHINE

SCAP SECURITY GUIDE

open-source SCAP security policy project

- community project
- content for multiple products - RHEL, Fedora, CentOS, Firefox, ...
- multiple policies for each product - USGCB, PCI-DSS, DISA STIG, ...



SCANNING A SINGLE MACHINE

let's set-up a Red Hat Enterprise Linux 7.2 machine as close to PCI-DSS as possible

We will need the following to perform a PCI-DSS scan:

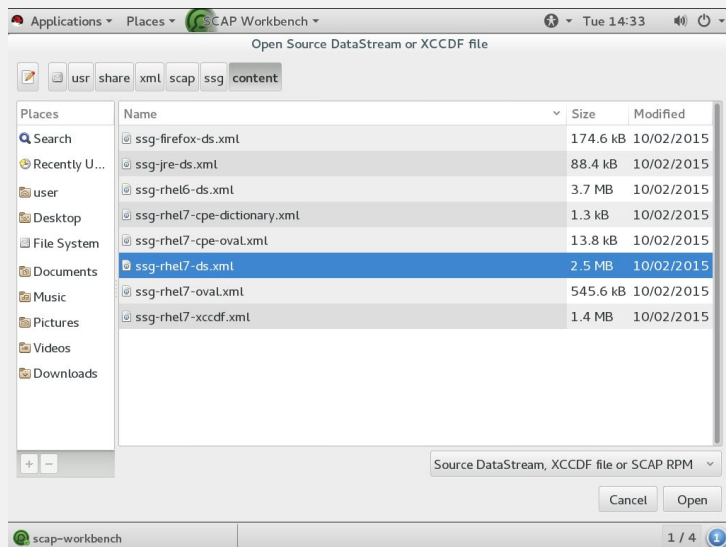
- Red Hat Enterprise Linux 7.2
- OpenSCAP and SCAP Workbench
- PCI-DSS from SCAP Security Guide

INSTALL THE NECESSARY TOOLS

(assuming Red Hat Enterprise Linux 7.2)

```
# yum install scap-security-guide  
# yum install scap-workbench
```

START SCAP-WORKBENCH

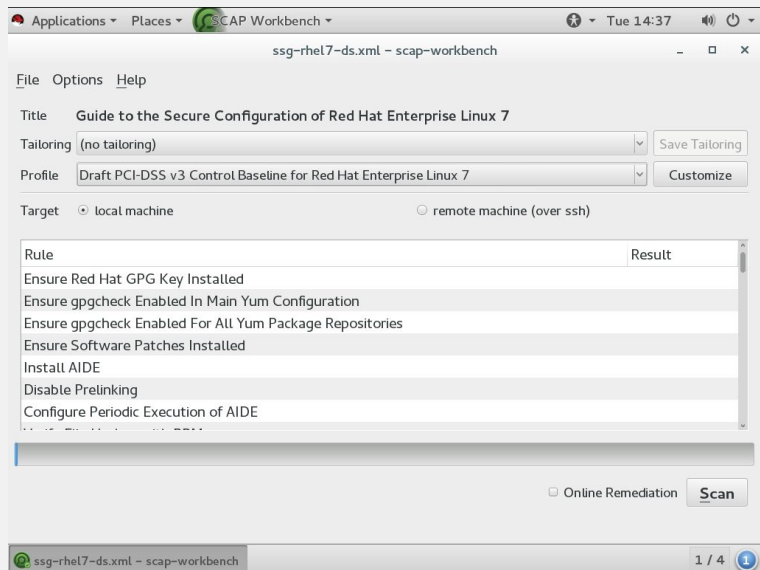


After starting *SCAP Workbench* we will be asked to select the security policy we want to load.

Let's select *ssg-rhel7-ds.xml*, which is a security policy for Red Hat Enterprise Linux 7 in the datastream SCAP format.

INITIAL SCAN

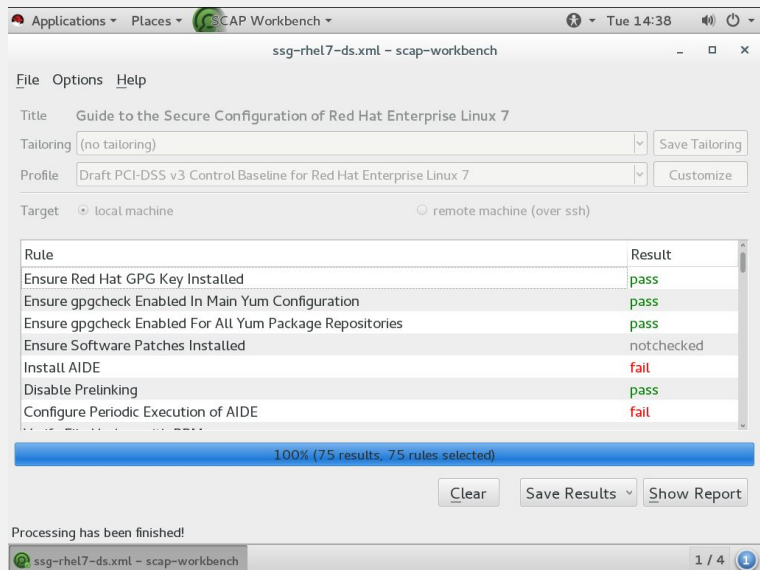
let's do a quick scan to establish a baseline



1. select the *PCI-DSS* profile
2. keep *local machine* selected
3. click *Scan*

INITIAL SCAN

let's do a quick scan to establish a baseline



1. select the *PCI-DSS* profile
2. keep *local machine* selected
3. click *Scan*

INITIAL RESULTS

Compliance and Scoring

The target system did not satisfy the conditions of 43 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	65.168396	100.000000	 65.17%

INITIAL RESULTS

► Configure Syslog		
▼ System Accounting with auditd 31x fail		
▼ 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 27x fail		
▼ Records Events that Modify Date and Time Information 5x fail		
Record attempts to alter time through adjtimex	low	fail
Record attempts to alter time through settimeofday	low	fail
Record Attempts to Alter Time Through stime	low	fail

INITIAL RESULTS

Set Password Maximum Age	
Rule ID	xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
Result	fail
Time	2016-02-16T15:06:16
Severity	medium
Identifiers and References	<div>identifiers: CCE-27051-2</div> <div>references: IA-5(f), IA-5(g), IA-5(1)(d), 180, 199, 76, Test attestation on 20121026 by DS</div>
Description	<p>To specify password maximum age for new accounts, edit the file <code>/etc/login.defs</code> and add or correct the following line, replacing <code>DAYS</code> appropriately:</p> <pre>PASS_MAX_DAYS DAYS</pre> <p>A value of 180 days is sufficient for many environments. The DoD requirement is 60.</p>
Rationale	<p>Setting the password maximum age ensures users are required to periodically change their passwords. This could possibly decrease the utility of a stolen password. Requiring shorter password lifetimes increases the risk of users writing down the password in a convenient location subject to physical compromise.</p>

INITIAL RESULTS

OVAL details

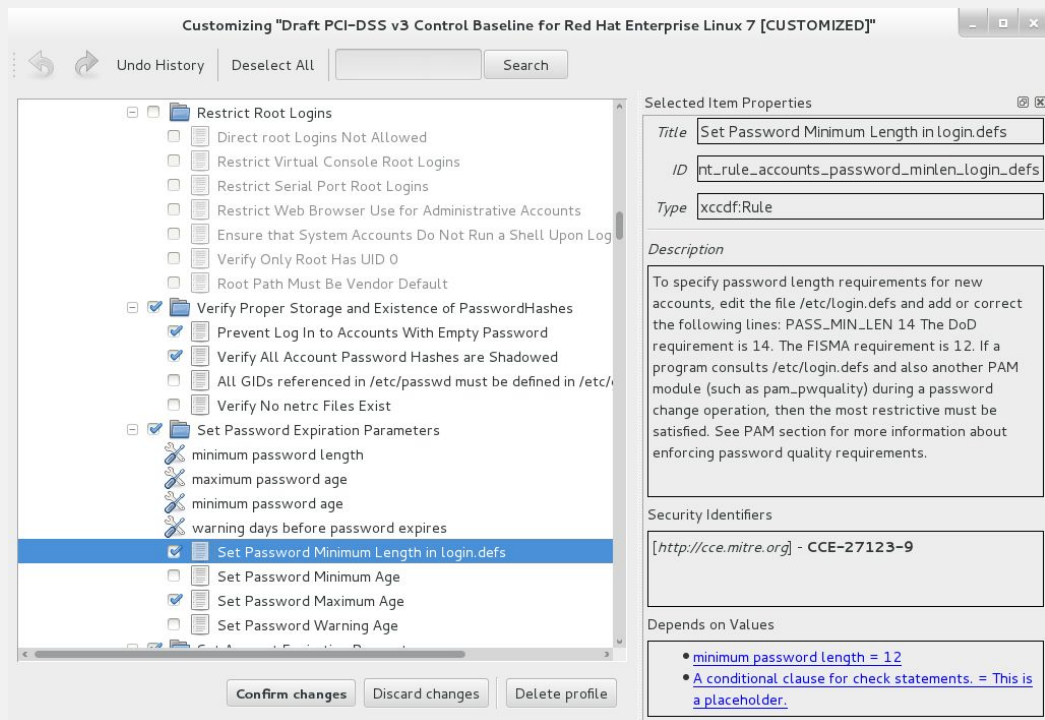
Items found violating **The value of PASS_MAX_DAYS should be set appropriately in /etc/login.defs :**

Var ref	Value
oval:ssg:var:1310	99999

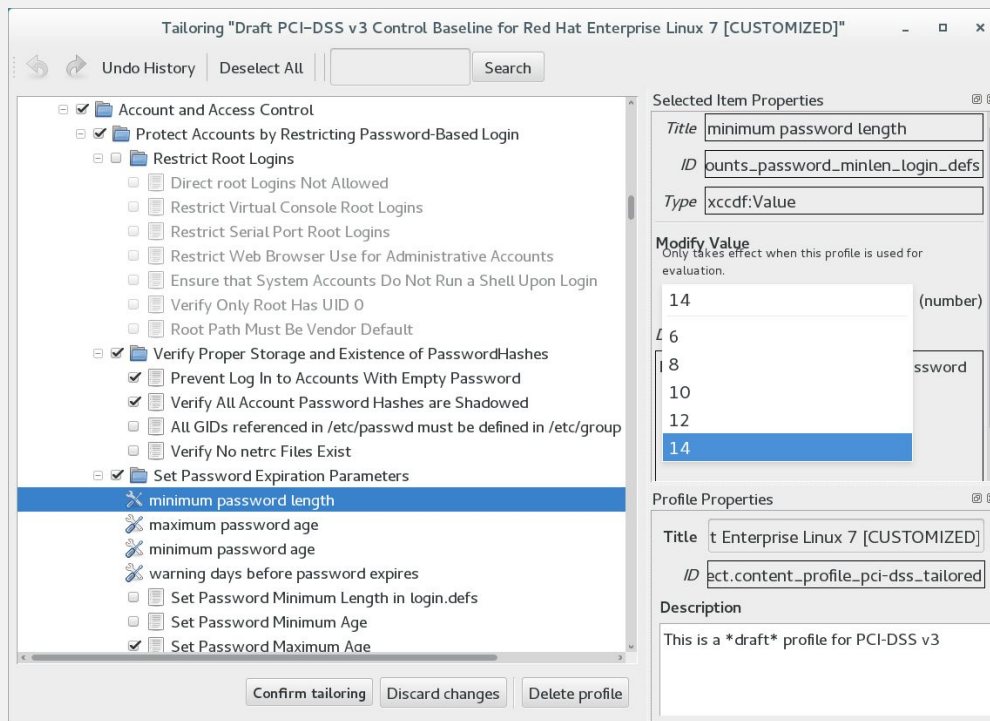
Remediation script:

```
var_accounts_maximum_age_login_defs="90"
grep -q ^PASS_MAX_DAYS /etc/login.defs && \
sed -i "s/PASS_MAX_DAYS.*/PASS_MAX_DAYS    $var_accounts_maximum_age_login_defs/g" /etc/login.defs
if ! [ $? -eq 0 ]; then
    echo "PASS_MAX_DAYS    $var_accounts_maximum_age_login_defs" >> /etc/login.defs
fi
```

MAKING ADJUSTMENTS



MAKING ADJUSTMENTS



SAVING THE FINAL POLICY

we now have the final security policy, let's save it for later deployment

Click File → *Save Customization Policy*

Instead of saving the entire policy we will save the difference between stock policy and our final policy. This enables us to get improvements and bug fixes.

TAILORING FILE

The result of Tailoring

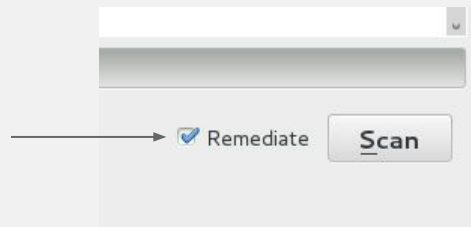
```
<?xml version="1.0" encoding="UTF-8"?>
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2"
id="xccdf_scap-workbench_tailoring_default">
  <xccdf:benchmark href="/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml"/>
  <xccdf:version time="2016-06-02T11:04:09">1</xccdf:version>
  <xccdf:Profile id="xccdf_org.ssgproject.content_profile_pci-dss_customized"
extends="xccdf_org.ssgproject.content_profile_pci-dss">
    <xccdf:title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">PCI-DSS
v3 Control Baseline for Red Hat Enterprise Linux 7 [CUSTOMIZED]</xccdf:title>
    <xccdf:description>...</xccdf:description>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_interval"
selected="true"/>
  </xccdf:Profile>
</xccdf:Tailoring>
```

AUTOMATICALLY FIXING THE ISSUES

Check *Remediate* to automatically fix issues after scanning

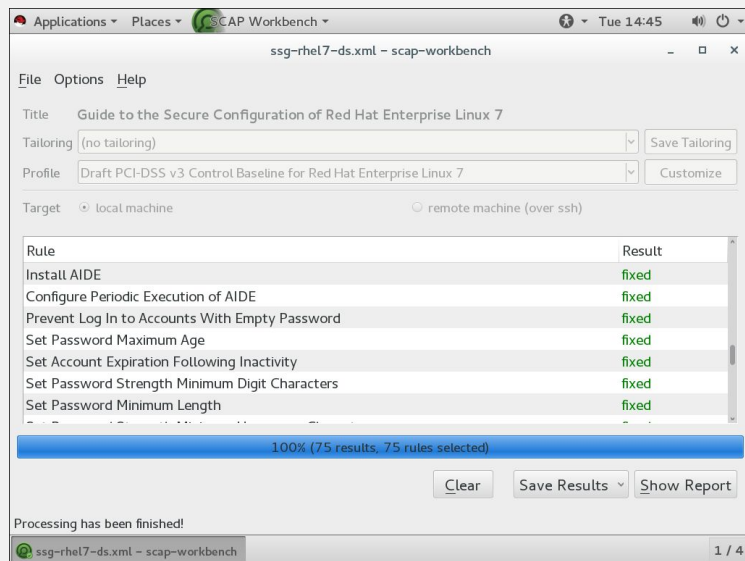
We now have a profile defined, let's put the machine closer to compliance. Keep this in mind when doing automatic remediation:

- remediation is potentially dangerous
- remediation **cannot be undone!**



REMEDIATION WITH SCAP-WORKBENCH

let's do a quick scan to establish a baseline



- *fixed* means the remediation was successful
- some fixes require reboot
- some rules cannot be automatically fixed - these still show as *failed*

FINAL RESULTS

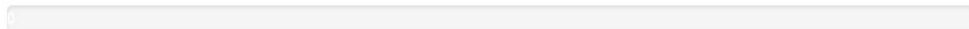
Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	65.168396	100.000000	<div><div>65.17%</div></div>

DEMO on Fedora 25

COMMAND-LINE SCANNING OF RED HAT ENTERPRISE LINUX 7

SCANNING A PHYSICAL MACHINE

Use `oscap`, the OpenSCAP command line interface

```
oscap xccdf eval --profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
--results results.xml --results-arf arf.xml --report report.html  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

results.xml, arf.xml and report.html are the same files we get from SCAP Workbench

SCANNING A CONTAINER

a command-line interface similar to oscap, scans a container “from the outside”

```
oscap-docker container $ID xccdf eval --profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

```
oscap-docker image $ID xccdf eval --profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

SCANNING ANY VFS

a command-line interface similar to oscap, scans a VFS “from the outside”

```
oscap-chroot /mnt/scan-target xccdf eval --profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

```
oscap-chroot /mnt/scan-target xccdf eval --profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

SCANNING A VIRTUAL MACHINE

a command-line interface similar to oscap, scans a VM “from the outside”

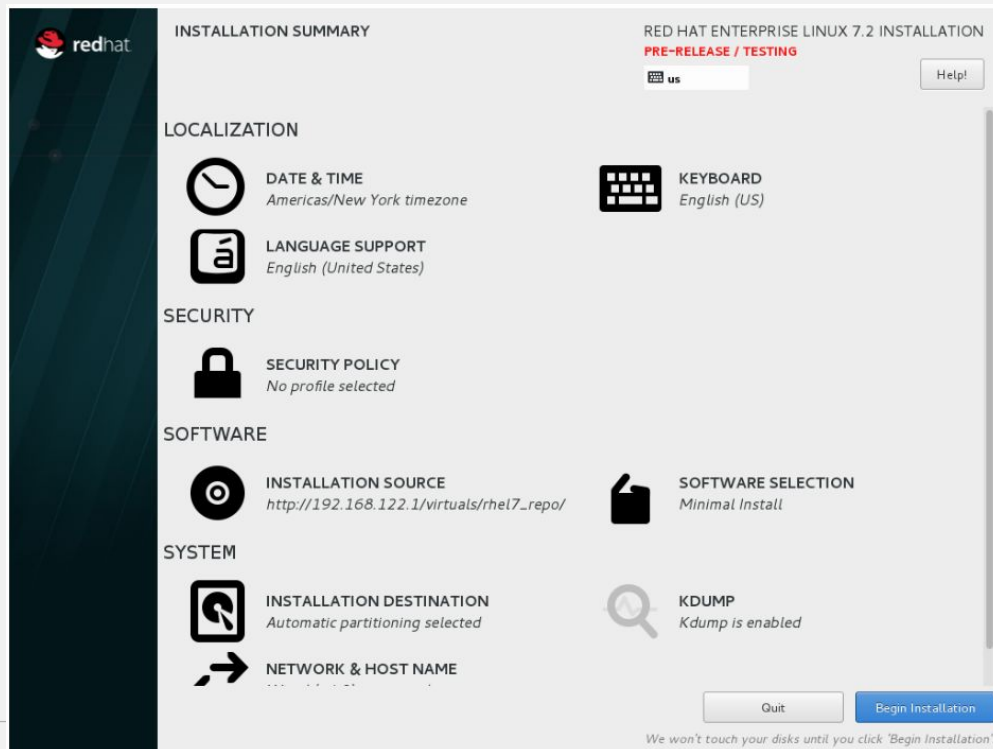
```
oscap-vm domain rhel7.2 xccdf eval --profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

```
oscap-vm image /var/lib/libvirt/images/rhel7.2.qcow2 xccdf eval  
--profile  
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

ANACONDA INSTALLER INTEGRATION

OSCAP ANACONDA ADDON

SCAP integration in the installer GUI



OSCAP ANACONDA ADDON

SCAP integration in the installer GUI

SECURITY POLICY

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION
PRE-RELEASE / TESTING

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

KICKSTART INTEGRATION

The same functionality is available in kickstart `oscap_anaconda_addon` block

```
%addon org_fedora_oscap
    content-type = datastream
    content-url = https://www.example.com/scap/testing_ds.xml
    datastream-id = scap_example.com_datastream_testing
    xccdf-id = scap_example.com_cref_xccdf.xml
    profile = xccdf_example.com_profile_my_profile
    fingerprint = 240f2f18222faa98856c3b4fc50c4195
%end
```

WHY OSCAP ANACONDA ADDON

- Install machines in a compliant state
- Provision VMs with compliance in mind

SCANNING AN INFRASTRUCTURE

MANY OPTIONS

Every infrastructure is different...

- For small infrastructures:
 - OpenSCAP-daemon
- For large(r) infrastructures:
 - Red Hat Satellite 6 (Foreman)
 - SUSE Manager
 - Red Hat CloudForms (ManageIQ)
 - Red Hat Satellite 5 (Spacewalk)

OPENSAP-DAEMON

- Continuous scanning, result storage
- Interactive, useful defaults
- Unified task interface, can scan:
 - Local machine
 - Remote machine over SSH
 - Container, container image
 - VMs, VM storage images
 - VFS

OPENSAP-DAEMON SCAN TARGET

- Unified task interface, can scan:
 - localhost
 - ssh://user@machine:port
 - ssh+sudo://user@machine:port
 - docker-image://rhel7
 - docker-container://furious_einstein
 - vm-domain://my_vm
 - vm-image:///var/lib/libvirt/images/my_vm.qcow2
 - chroot:///mnt/some_vfs

OPENSAP-DAEMON

- Enable the following COPR repo:

<https://copr.fedorainfracloud.org/coprs/openscapmaint/openscap-latest/>

```
# yum install openscap-daemon
```

```
# systemctl enable oscapd
```

```
# systemctl start oscapd
```


OPENSAP-DAEMON

```
# oscapd-cli task
```

```
# oscapd-cli task-create -i
```

```
# oscapd-cli result
```

```
# oscapd-cli result 1 1
```

```
# oscapd-cli result 1 1 report
```

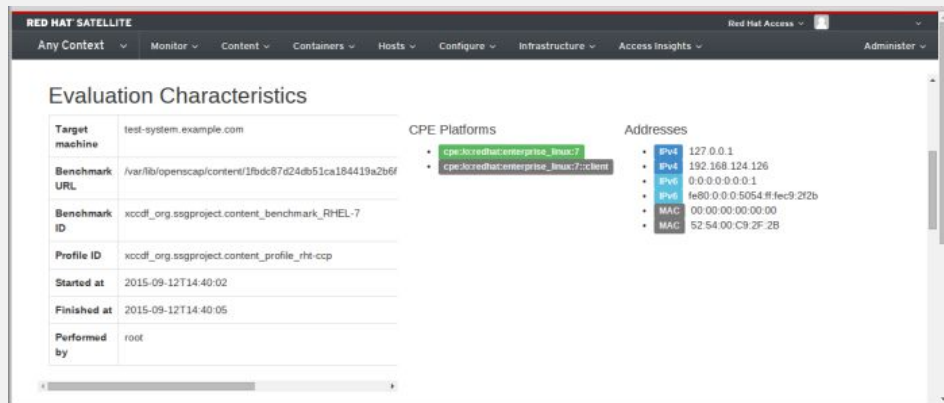
DEMO on Fedora 25

SCAP IN RED HAT SATELLITE 6

Red Hat Satellite 6 can be used to scan your infrastructure.

Feature highlights:

- upload SCAP content
- assign policies to hosts and hostgroups
- schedule continuous checks
- view HTML reports



SCAP IN RED HAT SATELLITE 6

upload SCAP content

File Upload

Locations

Organizations

Title *

SCAP Security Guide for RHEL7

Scap file *

Choose File

ssg-rhel7-ds.xml

Upload SCAP DataStream file

Cancel

Submit

SCAP IN RED HAT SATELLITE 6

use the uploaded SCAP content to create policies

New Compliance Policy



Name *

Description

Cancel

Next

SCAP IN RED HAT SATELLITE 6

use the uploaded SCAP content to create policies

New Compliance Policy

1 Create policy

2 SCAP Content

3 Schedule

4 Locations

5 Organizations

6 Hostgroups

SCAP Content

rhel7_ssg

XCCDF Profile

Default XCCDF profile

Default XCCDF profile

Common Profile for General-Purpose Systems

United States Government Configuration Baseline (USGCB / STIG)

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

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

<

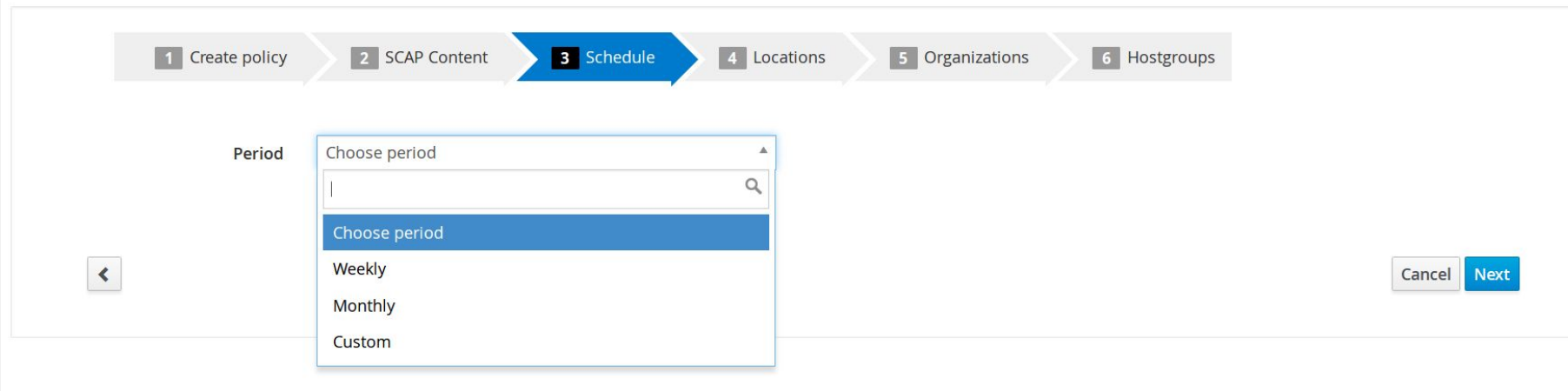
Cancel

Next

SCAP IN RED HAT SATELLITE 6

use the uploaded SCAP content to create policies

New Compliance Policy



The image shows the 'New Compliance Policy' wizard in Red Hat Satellite 6. At the top, a progress bar indicates six steps: 1. Create policy, 2. SCAP Content, 3. Schedule (highlighted in blue), 4. Locations, 5. Organizations, and 6. Hostgroups. Below the progress bar, the 'Period' section is active. It features a dropdown menu with the text 'Choose period' and a search icon. The dropdown is open, showing a list of options: 'Choose period' (highlighted in blue), 'Weekly', 'Monthly', and 'Custom'. To the left of the dropdown is a back arrow button, and to the right are 'Cancel' and 'Next' buttons.

1 Create policy 2 SCAP Content 3 Schedule 4 Locations 5 Organizations 6 Hostgroups

Period

Choose period

Choose period

Weekly

Monthly

Custom

< Cancel Next

SCAP IN RED HAT SATELLITE 6

see past results








Compliance Reports

Filter ...

×

Q Search

▼

<input type="checkbox"/>	Host	Reported At	Passed	Failed	Other	
<input type="checkbox"/>	 [blurred host name]	about 7 hours ago	108	113	3	Delete
<input type="checkbox"/>	 [blurred host name]	4 days ago	108	113	3	Delete
<input type="checkbox"/>	 [blurred host name]	4 days ago	14	44	3	Delete
<input type="checkbox"/>	 [blurred host name]	4 days ago	14	44	3	Delete
<input type="checkbox"/>	 [blurred host name]	4 days ago	14	44	3	Delete
<input type="checkbox"/>	 [blurred host name]	4 days ago	108	113	3	Delete
<input type="checkbox"/>	 [blurred host name]	4 days ago	14	44	3	Delete

SCAP IN RED HAT SATELLITE 6

browse and filter in the rule result overview

Show log messages:

All messages

[Back](#)






[Delete](#)

[Host details](#)

[View full report](#)

[Download XML in bzip](#)

Reported at 2016-06-09 21:00:39 -0400

Severity	Message	Resource	Result
High	Ensure Red Hat GPG Key Installed 	xccdf_org.ssgproject.content_...	pass
Low	Record Events that Modify the System's Discretionary Access Controls - setxattr 	xccdf_org.ssgproject.content_...	fail
Low	Ensure auditd Collects System Administrator Actions 	xccdf_org.ssgproject.content_...	fail
Low	Ensure auditd Collects Information on the Use of Privileged Commands 	xccdf_org.ssgproject.content_...	fail
Low	Record Events that Modify the System's Discretionary Access Controls - chown 	xccdf_org.ssgproject.content_...	fail

SCAP IN RED HAT SATELLITE 6

browse HTML report for details of a past result

The screenshot displays the Red Hat Satellite 6 web interface for viewing a compliance report. The top navigation bar includes the 'RED HAT SATELLITE' logo, a menu with 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', 'Configure', 'Infrastructure', and 'Access Insights', and user information for 'Red Hat Access' and 'Admin User'.

The main content area shows a hierarchical list of compliance checks. The 'System Settings' section is expanded, showing a summary of '25% fail' and '1x notchecked'. Below this, the 'Installing and Maintaining Software' section is also expanded, showing '6x fail' and '1x notchecked'. The 'Disk Partitioning' section is further expanded, showing a table of checks:

Check Name	Severity	Result
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

Below the 'Disk Partitioning' section, the 'Updating Software' section is expanded, showing '1x fail' and '1x notchecked'. It contains a table of checks:

Check Name	Severity	Result
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

The 'Software Integrity Checking' section is also expanded, showing '1x fail'. It contains a table of checks:

Check Name	Severity	Result
Install AIDE	medium	fail

Below the 'Software Integrity Checking' section, the 'Verify Integrity with RPM' section is expanded, showing '1x fail'. It contains a table of checks:

Check Name	Severity	Result
Verify Integrity with RPM	medium	fail

The 'Account and Access Control' section is expanded, showing '10x fail'. It contains a table of checks:

Check Name	Severity	Result
Protect Accounts by Restricting Password-Based Login	high	fail

The URL at the bottom of the page is https://sat61.local.lan/compliance/arf_reports/1#.

SCAP IN RED HAT SATELLITE 6

further references...

Red Hat Satellite 6.1 Feature Overview: OpenSCAP

<https://www.youtube.com/watch?v=p4uNlzYld-Y>

SUSE MANAGER

- Continuous scans
- Result storage
- Low-level compared to Satellite 6

The screenshot displays the SUSE Manager web interface. The top navigation bar includes links for Knowledgebase, Documentation, and a user profile (admin). A search bar is present with a dropdown menu set to 'Systems'. Below the navigation bar, a secondary bar shows '0 systems selected' and buttons for 'Manage' and 'Clear'. The main interface has a sidebar on the left with a dark theme, containing links for Overview, Salt Master, Systems (highlighted), All, Physical Systems, Virtual Systems, Bare Metal Systems, Out of Date, Requiring Reboot, Non Compliant, Without System Type, Ungrouped, Inactive, Recently Registered, and Proxy. The main content area shows the system 'sumac.suse.de' with a question mark icon and buttons for 'Delete System' and 'Add to SSM'. Below this, there are tabs for Details, Software, Configuration, Provisioning, Groups, Audit (selected), and Events. Under the Audit tab, there are sub-tabs for 'List Scans' and 'Schedule'. The 'Schedule' sub-tab is active, showing the 'Schedule New XCCDF Scan' form. The form includes fields for 'Command:' (containing '/usr/bin/oscapp xccdf eval'), 'Command-line Arguments:', 'Path to XCCDF document *:', and 'Schedule no sooner than:' (with a date picker set to 2/23/16 and a time picker set to 4:41 pm CET). A green 'Schedule' button is at the bottom. A tip at the bottom of the form states: 'Tip: Certain versions of OpenSCAP may require the --profile command-line argument. --profile specifies a particular profile from the XCCDF document.'

SUSE MANAGER

- Continuous scans
- Result storage
- Low-level compared to Satellite 6

The screenshot displays the SUSE Manager web interface. The top navigation bar is teal and includes links for Knowledgebase, Documentation, a user profile (admin), and system settings. A search bar is present with a dropdown menu set to 'Systems'. Below the navigation bar, a secondary teal bar contains tabs for Overview, Systems, Patches, Channels, Audit, Configuration, Schedule, Users, Admin, and Help. On the left side, a dark sidebar lists navigation options: CVE Audit, Subscription Matching, OpenSCAP (highlighted in blue), All Scans, XCCDF Diff, and Advanced Search. The main content area is titled 'OpenSCAP Search' and contains a search form. The form includes a text input for 'Search XCCDF Rules For:' with a search button, a dropdown for 'With Result:' set to 'any', and radio buttons for 'Where to Search:' (selected: Search all systems, unselected: Search system set manager). There is also a checkbox for 'Scan Dates to Search:' (unselected: Search Scans Performed Between Dates) and radio buttons for 'Show Search Result As:' (selected: List of XCCDF Rule Results, unselected: List of XCCDF Scans). Examples of search criteria are provided: 'no_hashes_outside_shadow', 'CCE-14300-8'.

SUSE Manager

Knowledgebase Documentation admin

Systems Search

0 systems selected Manage Clear

Overview Systems Patches Channels Audit Configuration Schedule Users Admin Help

CVE Audit

Subscription Matching

OpenSCAP

All Scans

XCCDF Diff

Advanced Search

OpenSCAP Search

OpenSCAP Search will return finished OpenSCAP scans from all scans you have access.

Specify your search criteria below.

Search XCCDF Rules For: Search

Examples: 'no_hashes_outside_shadow', 'CCE-14300-8'

With Result: any

Where to Search: ☒ Search all systems ☐ Search system set manager

Scan Dates to Search: ☐ Search Scans Performed Between Dates

Show Search Result As: ☒ List of XCCDF Rule Results ☐ List of XCCDF Scans

SCAP IN RED HAT SATELLITE 5

Red Hat Satellite 5 can be used to scan your infrastructure.

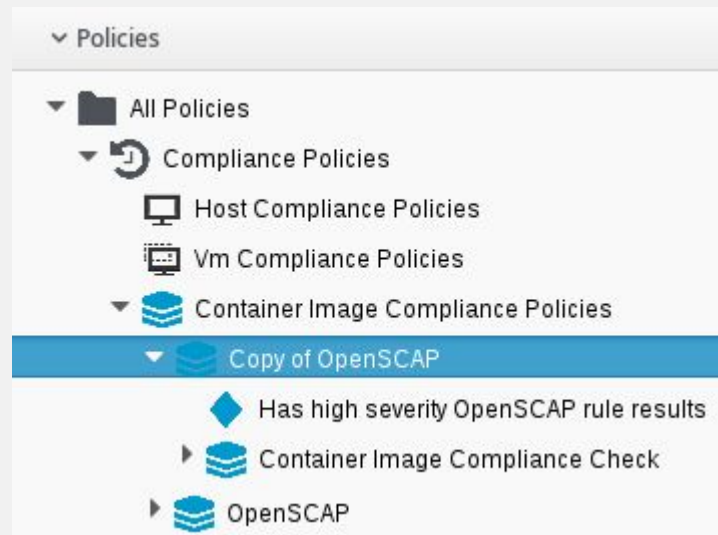
- Obsolete!
- Continuous scans
- Result storage
- Low-level compared to Satellite 6

The screenshot displays the Red Hat Network Satellite 5 web interface. At the top, there's a navigation bar with links for 'English (change)', 'Knowledgebase', 'Documentation', 'USER: admin', 'ORGANIZATION: RHN Satellite team', 'Preferences', and 'Sign Out'. Below this is a header with the 'RED HAT NETWORK SATELLITE' logo and a search bar. A secondary navigation bar includes 'Overview', 'Systems', 'Errata', 'Channels', 'Audit', 'Configuration', 'Schedule', 'Users', 'Admin', and 'Help'. A status bar indicates '1 SYSTEM SELECTED' with 'MANAGE' and 'CLEAR' buttons. On the left, a sidebar menu lists various system management options. The main content area is titled 'Satellite Test Client' and features tabs for 'Details', 'Software', 'Configuration', 'Provisioning', 'Groups', 'Audit', and 'Events'. The 'Schedule' tab is active, showing a 'Schedule New XCCDF Scan' form. This form includes fields for 'Command' (set to '/usr/bin/oscsp xccdf eval'), 'Command-line Arguments', 'Path to XCCDF document*', and a 'Schedule no sooner than' date/time picker (set to July 23, 2012, 8:38 PM EDT). A 'Schedule' button is at the bottom right. A tip at the bottom states: 'Tip: The --profile command-line argument might be required by certain versions of OpenSCAP. It determines a particular profile from XCCDF document.'

CLOUDFORMS

Red Hat CloudForms contains SCAP integration for container scanning

- Can auto-disable containers if they have high severity compliance failures
- Can auto-disable containers if they have CVEs



CLOUDFORMS

Red Hat CloudForms can provision machines compliant to SCAP profiles

- Uses the SCAP integration in Kickstart and Anaconda

```
%addon org_fedora_oscap
  content-type = datastream
  content-url = https://<%= @host.puppetmaster %><%=
@host.params['scap_download_path'] %>
  profile = <%= pol_hash['profile_id'] %>
%end
```


COMMUNITY

where to get more answers

- IRC: #openscap on irc.freenode.net
- Mailing lists
- <https://www.open-scap.org/>
- Twitter! @OpenSCAP



redhat.

THANK YOU! Questions?

Martin Preisler
mpreisle@redhat.com
Senior Software Engineer, Red Hat, Inc.



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos