



# Security Compliance with OpenSCAP

Automatically find vulnerabilities and configuration issues of your infrastructure

Martin Preisler  
Software Engineer, Red Hat, Inc.

# AGENDA

- **software flaws - vulnerabilities**
  - checking machines for vulnerabilities
  - checking containers for vulnerabilities
- **configuration flaws - weaknesses**
  - what is a security policy
  - SCAP introduction
  - security compliance for a single machine
  - security policy customization
  - remediation
  - using SCAP with Red Hat Satellite 6
- **future plans**

There will be demos!

# AGENDA

Security is a very broad topic. In this session we will be discussing:

- **software flaws - vulnerabilities**
- configuration flaws - weaknesses

# 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

# VULNERABILITIES

**Known** vulnerabilities are *much* worse.

- CVE-2016-1283
- Details are 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:

- 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

# 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:

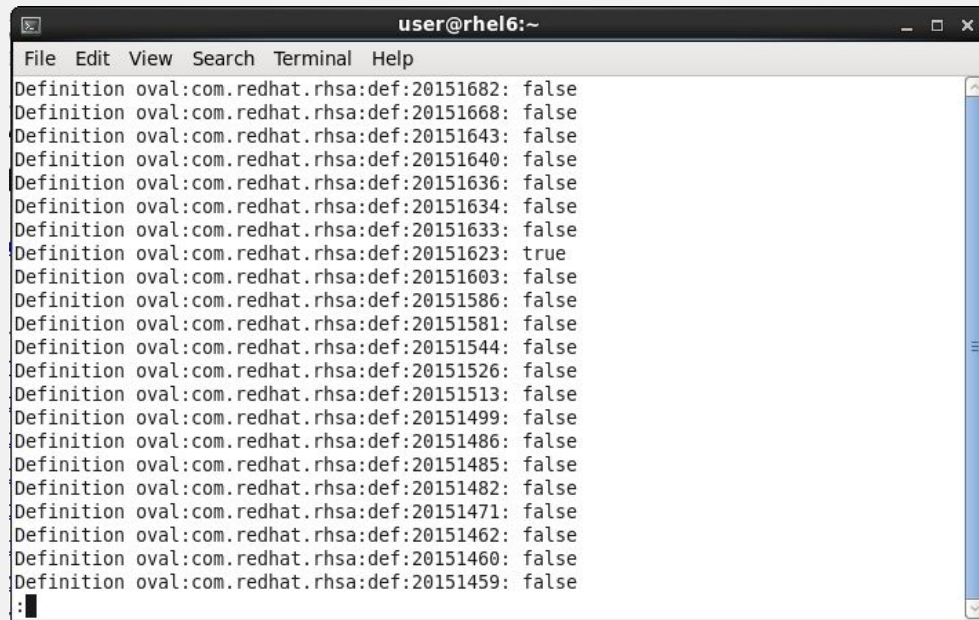
1. Download the CVE data
2. Execute the oscap tool
3. Review the results

# 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, each with a unique ID and a boolean result. The results are as follows:

Definition ID	Result
oval:com.redhat.rhsa:def:20151682	false
oval:com.redhat.rhsa:def:20151668	false
oval:com.redhat.rhsa:def:20151643	false
oval:com.redhat.rhsa:def:20151640	false
oval:com.redhat.rhsa:def:20151636	false
oval:com.redhat.rhsa:def:20151634	false
oval:com.redhat.rhsa:def:20151633	false
oval:com.redhat.rhsa:def:20151623	true
oval:com.redhat.rhsa:def:20151603	false
oval:com.redhat.rhsa:def:20151586	false
oval:com.redhat.rhsa:def:20151581	false
oval:com.redhat.rhsa:def:20151544	false
oval:com.redhat.rhsa:def:20151526	false
oval:com.redhat.rhsa:def:20151513	false
oval:com.redhat.rhsa:def:20151499	false
oval:com.redhat.rhsa:def:20151486	false
oval:com.redhat.rhsa:def:20151485	false
oval:com.redhat.rhsa:def:20151482	false
oval:com.redhat.rhsa:def:20151471	false
oval:com.redhat.rhsa:def:20151462	false
oval:com.redhat.rhsa:def:20151460	false
oval:com.redhat.rhsa:def:20151459	false

The terminal ends with a prompt character ': '.

# VULNERABILITY SCAN RESULTS

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

A terminal window titled 'user@rhel6:~' displays the output of a vulnerability scan. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The output consists of a list of definitions, each with a unique identifier and a boolean value. Most values are 'false', but one is 'true'. An arrow points to the line where the value is 'true'.

```
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>Error</div> <div>Unknown</div> <div>Other</div> </div>				
ID	Result	Class	Reference ID	Title
oval:com.redhat.rhsa:def:20151623	true	patch	[ <a href="#">RHSA-2015:1623-01</a> ], [ <a href="#">CVE-2015-5364</a> ], [ <a href="#">CVE-2015-5366</a> ]	RHSA-2015:1623: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151834	false	patch	[ <a href="#">RHSA-2015:1834-02</a> ], [ <a href="#">CVE-2015-4500</a> ], [ <a href="#">CVE-2015-4506</a> ], [ <a href="#">CVE-2015-4509</a> ], [ <a href="#">CVE-2015-4511</a> ], [ <a href="#">CVE-2015-4517</a> ], [ <a href="#">CVE-2015-4519</a> ], [ <a href="#">CVE-2015-4520</a> ], [ <a href="#">CVE-2015-4521</a> ], [ <a href="#">CVE-2015-4522</a> ], [ <a href="#">CVE-2015-7174</a> ], [ <a href="#">CVE-2015-7175</a> ], [ <a href="#">CVE-2015-7176</a> ], [ <a href="#">CVE-2015-7177</a> ], [ <a href="#">CVE-2015-7180</a> ]	RHSA-2015:1834: firefox security update (Critical)
oval:com.redhat.rhsa:def:20151833	false	patch	[ <a href="#">RHSA-2015:1833-00</a> ], [ <a href="#">CVE-2015-5165</a> ]	RHSA-2015:1833: qemu-kvm security update (Moderate)
oval:com.redhat.rhsa:def:20151814	false	patch	[ <a href="#">RHSA-2015:1814-00</a> ], [ <a href="#">CVE-2015-5567</a> ], [ <a href="#">CVE-2015-5568</a> ], [ <a href="#">CVE-2015-5570</a> ], [ <a href="#">CVE-2015-5571</a> ], [ <a href="#">CVE-2015-5572</a> ], [ <a href="#">CVE-2015-5573</a> ], [ <a href="#">CVE-2015-5574</a> ], [ <a href="#">CVE-2015-5575</a> ], [ <a href="#">CVE-2015-5576</a> ], [ <a href="#">CVE-2015-5577</a> ], [ <a href="#">CVE-2015-5578</a> ], [ <a href="#">CVE-2015-5579</a> ], [ <a href="#">CVE-2015-5580</a> ], [ <a href="#">CVE-2015-5581</a> ], [ <a href="#">CVE-2015-5582</a> ], [ <a href="#">CVE-2015-5584</a> ], [ <a href="#">CVE-2015-5587</a> ], [ <a href="#">CVE-2015-5588</a> ], [ <a href="#">CVE-2015-6676</a> ], [ <a href="#">CVE-2015-6677</a> ], [ <a href="#">CVE-2015-6678</a> ], [ <a href="#">CVE-2015-6679</a> ], [ <a href="#">CVE-2015-6682</a> ]	RHSA-2015:1814: flash-plugin security update (Critical)
oval:com.redhat.rhsa:def:20151741	false	patch	[ <a href="#">RHSA-2015:1741-00</a> ], [ <a href="#">CVE-2015-3281</a> ]	RHSA-2015:1741: haproxy security update (Important)
oval:com.redhat.rhsa:def:20151715	false	patch	[ <a href="#">RHSA-2015:1715-00</a> ], [ <a href="#">CVE-2015-3247</a> ]	RHSA-2015:1715: spice-server security update (Important)
oval:com.redhat.rhsa:def:20151712	false	patch	[ <a href="#">RHSA-2015:1712-00</a> ], [ <a href="#">CVE-2015-1291</a> ], [ <a href="#">CVE-2015-1292</a> ], [ <a href="#">CVE-2015-1293</a> ], [ <a href="#">CVE-2015-1294</a> ], [ <a href="#">CVE-2015-1295</a> ], [ <a href="#">CVE-2015-1296</a> ], [ <a href="#">CVE-2015-1297</a> ], [ <a href="#">CVE-2015-1298</a> ], [ <a href="#">CVE-2015-1299</a> ], [ <a href="#">CVE-2015-1300</a> ], [ <a href="#">CVE-2015-1301</a> ]	RHSA-2015:1712: chromium-browser security update (Important)
oval:com.redhat.rhsa:def:20151708	false	patch	[ <a href="#">RHSA-2015:1708-00</a> ], [ <a href="#">CVE-2015-1802</a> ], [ <a href="#">CVE-2015-1803</a> ], [ <a href="#">CVE-2015-1804</a> ]	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	[ <a href="#">RHSA-2015:1643-00</a> ], [ <a href="#">CVE-2015-3636</a> ]	kernel security and bug fix update (Moderate)
oval:com.redhat.rhsa:def:20151640	false	patch	[ <a href="#">RHSA-2015:1640-00</a> ], [ <a href="#">CVE-2015-3238</a> ]	RHSA-2015:1640: pam security update (Moderate)
oval:com.redhat.rhsa:def:20151636	false	patch	[ <a href="#">RHSA-2015:1636-00</a> ], [ <a href="#">CVE-2015-5621</a> ]	RHSA-2015:1636: net-snmp security update (Moderate)
oval:com.redhat.rhsa:def:20151634	false	patch	[ <a href="#">RHSA-2015:1634-00</a> ], [ <a href="#">CVE-2015-3416</a> ]	RHSA-2015:1634: sqlite security update (Moderate)
oval:com.redhat.rhsa:def:20151633	false	patch	[ <a href="#">RHSA-2015:1633-00</a> ], [ <a href="#">CVE-2015-0248</a> ], [ <a href="#">CVE-2015-0251</a> ], [ <a href="#">CVE-2015-3187</a> ]	RHSA-2015:1633: subversion security update (Moderate)
oval:com.redhat.rhsa:def:20151623	false	patch	[ <a href="#">RHSA-2015:1623-01</a> ], [ <a href="#">CVE-2015-5364</a> ], [ <a href="#">CVE-2015-5366</a> ]	<a href="#">RHSA-2015:1623</a> : kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151603	false	patch	[ <a href="#">RHSA-2015:1603-01</a> ], [ <a href="#">CVE-2015-5127</a> ], [ <a href="#">CVE-2015-5128</a> ], [ <a href="#">CVE-2015-5129</a> ], [ <a href="#">CVE-2015-5130</a> ], [ <a href="#">CVE-2015-5131</a> ], [ <a href="#">CVE-2015-5132</a> ], [ <a href="#">CVE-2015-5133</a> ], [ <a href="#">CVE-2015-5134</a> ], [ <a href="#">CVE-2015-5539</a> ], [ <a href="#">CVE-2015-5540</a> ], [ <a href="#">CVE-2015-5541</a> ], [ <a href="#">CVE-2015-5544</a> ], [ <a href="#">CVE-2015-5545</a> ], [ <a href="#">CVE-2015-5546</a> ], [ <a href="#">CVE-2015-5547</a> ], [ <a href="#">CVE-2015-5548</a> ], [ <a href="#">CVE-2015-5549</a> ], [ <a href="#">CVE-2015-5550</a> ],	RHSA-2015:1603: flash-plugin security



# DEMO: FIND VULNERABILITIES ON RED HAT ENTERPRISE LINUX 7

# 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

# ATOMIC SCAN

New feature in Atomic 1.4

Scan containers and container images for CVEs.

```
root@t440s ~ # atomic scan 6c3a84d798dc
```

Container/Image	Cri	Imp	Med	Low
-----	---	---	---	---
6c3a84d798dc	0	0	4	0

# ATOMIC SCAN detailed

--detail prints out the errata and CVE details and references

```
root@t440s ~ # atomic scan --detail 6c3a84d798dc
6c3a84d798dc
OS      : Red Hat Enterprise Linux Server release 7.2 (Maipo)
Moderate : 4
  CVE    : RHSA-2016:0008: openssl security update (Moderate)
  CVE URL : https://access.redhat.com/security/cve/CVE-2015-7575
  RHSA ID  : RHSA-2016:0008-00
  RHSA URL : https://rhn.redhat.com/errata/RHSA-2016-0008.html

  CVE    : RHSA-2016:0007: nss security update (Moderate)
  CVE URL : https://access.redhat.com/security/cve/CVE-2015-7575
  RHSA ID  : RHSA-2016:0007-00
  RHSA URL : https://rhn.redhat.com/errata/RHSA-2016-0007.html

  CVE    : RHSA-2015:2617: openssl security update (Moderate)
  CVE URL : https://access.redhat.com/security/cve/CVE-2015-3194
  RHSA ID  : RHSA-2015:2617-00
  RHSA URL : https://rhn.redhat.com/errata/RHSA-2015-2617.html

  CVE    : RHSA-2015:2550: libxml2 security update (Moderate)
  CVE URL : https://access.redhat.com/security/cve/CVE-2015-1819
  RHSA ID  : RHSA-2015:2550-01
  RHSA URL : https://rhn.redhat.com/errata/RHSA-2015-2550.html
```

# 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`

# DEMO: ATOMIC SCAN ON RED HAT ENTERPRISE LINUX 7

# 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.

## **RUN OSCP TOOL**

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

# FOCUS OF THIS SESSION

Security is a very broad topic. In this session we will be discussing:

- software flaws - vulnerabilities
- **configuration flaws - weaknesses**



# SECURITY POLICY

what it means to secure a system

Usually in text form or a PDF. Security policy contains a set of rules, each rule has:

- description
- rationale
- how to check
- how to fix

# SECURITY POLICY EXAMPLE

excerpt from PCI-DSS

PCI DSS Requirements	Testing Procedures	Guidance
<b>1.1.5</b> Description of groups, roles, and responsibilities for management of network components	<b>1.1.5.a</b> Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.	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.
	<b>1.1.5.b</b> Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	
<b>1.1.6</b> 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.  Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	<b>1.1.6.a</b> 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.	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.  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.
	<b>1.1.6.b</b> Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.	
	<b>1.1.6.c</b> Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	

# AUTOMATING A SECURITY POLICY

for non-interactive machine processing

- very long bash script
- set of scripts with some harness running them
- proprietary solution
- SCAP

# WHAT IS SCAP?

a way to express security policies in machine readable form.

SCAP is a NIST standard. It contains a set of data formats for security policies.

- rule metadata - description, rationale, identifiers
- automatic compliance checking
- automatic fixing

SCAP uses other technologies such as XCCDF, OVAL, CPE, CVE and OCIL.

# ADVANTAGES OF SCAP

standards help avoid lock-in

- royalty free
- multiple implementations
- can mix and match scanner tools and security policies
- deploy a heterogenous mix of tools from different vendors

# SCAP SECURITY POLICY EXAMPLE

HTML guide generated from SCAP security policy

## 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
```

# 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?

...?

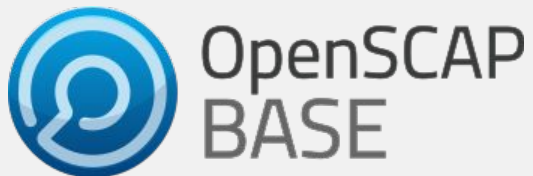


# USE-CASE 2: SECURITY COMPLIANCE FOR A SINGLE MACHINE

# OPENSCAP

open-source SCAP 1.2 implementation

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



# SCAP SECURITY GUIDE

open-source SCAP security policy project

- community project
- content for multiple products - Red Hat Enterprise Linux, 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:

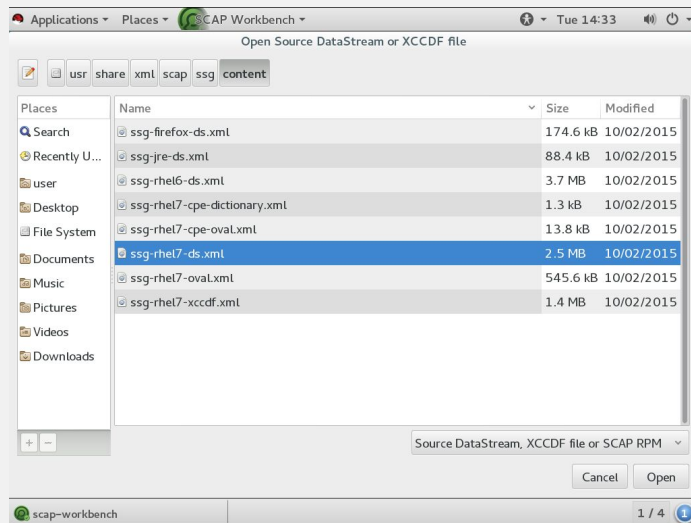
- Red Hat Enterprise Linux 7.2
- OpenSCAP and SCAP Workbench
- PCI-DSS from SCAP Security Guide

# INSTALL THE NECESSARY TOOLS

(assuming Red Hat Enterprise Linux 7.2)

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

# START SCAP-WORKBENCH



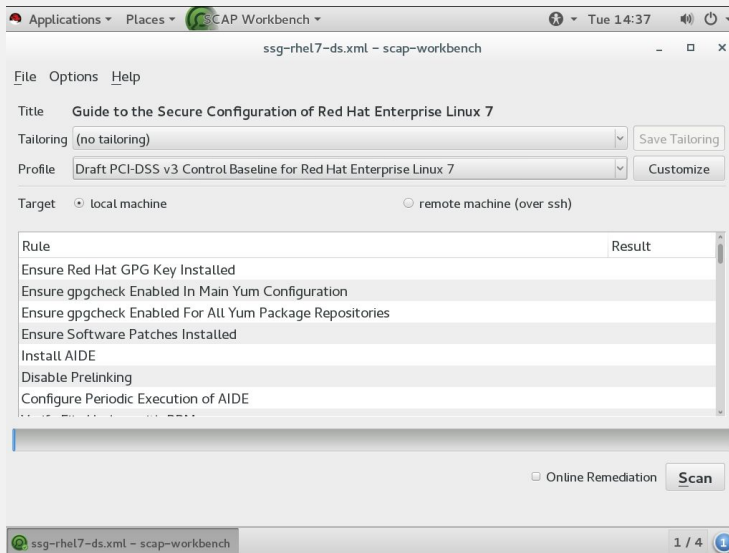
After starting *SCAP Workbench* we will be asked to select the security policy we want to load.

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

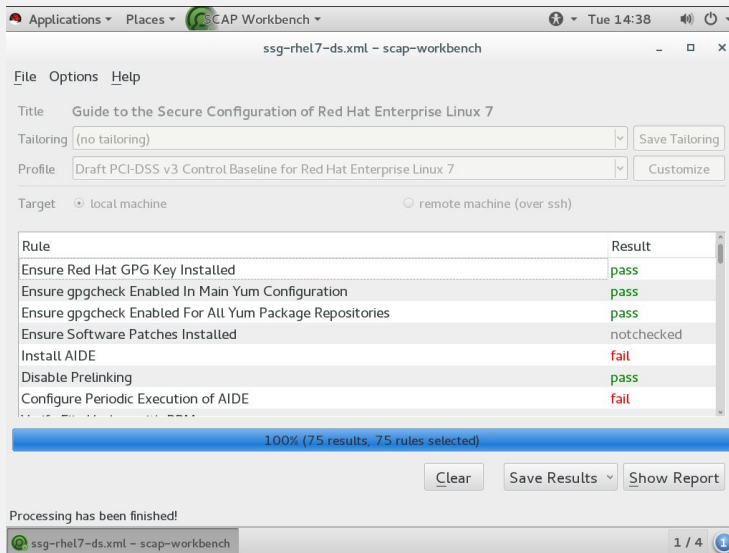
1. select the *PCI-DSS* profile
2. keep *local machine* selected
3. click *Scan*



# 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	<div><div>65.17%</div></div>

# 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

The screenshot shows a window titled "Customizing 'Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7 [CUSTOMIZED]'" with a toolbar containing "Undo History", "Deselect All", and a "Search" button. The main area is a tree view of controls. Under "Verify Proper Storage and Existence of PasswordHashes", "Set Password Expiration Parameters" is expanded, and "Set Password Minimum Length in login.defs" is selected. The right pane, "Selected Item Properties", shows the following details for the selected item:

- Title:** Set Password Minimum Length in login.defs
- ID:** nt\_rule\_accounts\_password\_minlen\_login\_defs
- Type:** xccdf:Rule
- Description:** To specify password length requirements for new accounts, edit the file /etc/login.defs and add or correct the following lines: PASS\_MIN\_LEN 14 The DoD requirement is 14. The FISMA requirement is 12. If a program consults /etc/login.defs and also another PAM module (such as pam\_pwquality) during a password change operation, then the most restrictive must be satisfied. See PAM section for more information about enforcing password quality requirements.
- Security Identifiers:** [http://cve.mitre.org] - CCE-27123-9
- Depends on Values:**
  - [minimum password length = 12](#)
  - [A conditional clause for check statements. = This is a placeholder.](#)

At the bottom of the window are buttons for "Confirm changes", "Discard changes", and "Delete profile".

# 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.

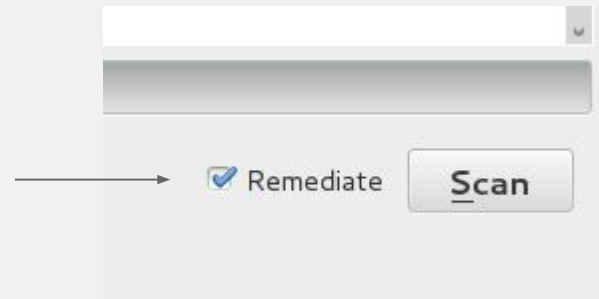
# DEMO: CONTENT CUSTOMIZATION

# 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:

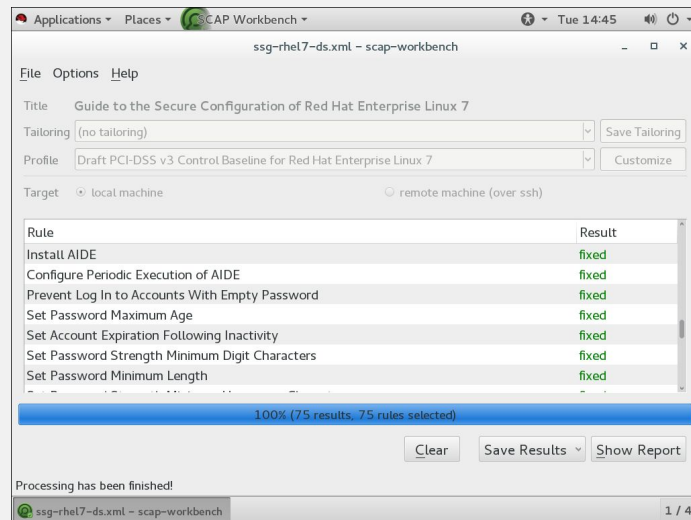
- remediation is potentially dangerous
- remediation **cannot be undone!**





# 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

74 passed

### Severity of failed rules

### Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	65.168396	100.000000	65.17%

# DEMO: COMMAND-LINE SCANNING OF RED HAT ENTERPRISE LINUX 7

# 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 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
```

Read more: <https://martin.preisler.me/2015/10/evaluate-virtual-machines-for-scap-compliance/>

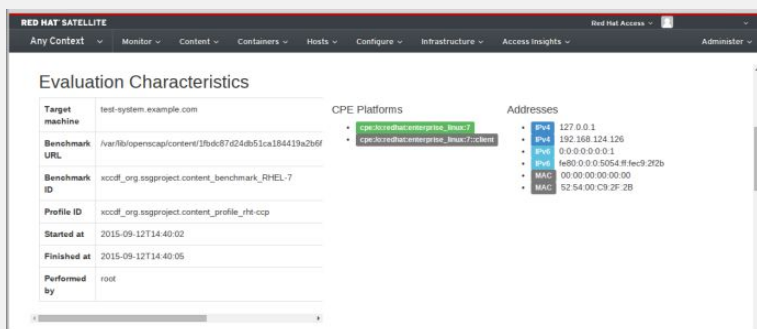
# USE-CASE 3: SECURITY COMPLIANCE FOR AN INFRASTRUCTURE

# 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 to create new SCAP policies

The screenshot shows the Red Hat Satellite 6 web interface. The top navigation bar includes 'RED HAT SATELLITE' and various menu items like 'Default Organization', 'Monitor', 'Content', 'Containers', 'Hosts', 'Configure', 'Infrastructure', and 'Access Insights'. The 'Hosts' menu is currently selected. The main content area is titled 'SCAP Contents' and features a search bar. A modal dialog is open, titled 'File Upload', with tabs for 'Locations' and 'Organizations'. The 'File Upload' tab is active, showing a 'Title \*' field, a 'Scap file \*' field with a 'Choose File' button, and a notice: 'Notice: You need to [install](#) OpenSCAP on your hosts, and upload this content to the hosts as well.' The dialog has 'Cancel' and 'Submit' buttons at the bottom.



# SCAP IN RED HAT SATELLITE 6

see past results

RED HAT SATELLITE

Default Organization Monitor Content Containers Hosts Configure Infrastructure Access Insights

Red Hat Access Admin User

Administer

### Compliance Reports

Filter ... Search

Host	Date	Passed	Failed	Other	
node10.local.lan	4 days ago	✓	✗	■	View Report
node10.local.lan	8 days ago	✓	✗	■	View Report

Displaying all 2 entries

# 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. The top navigation bar includes the 'RED HAT SATELLITE' logo, a 'Default Organization' dropdown, and several menu items: Monitor, Content, Containers, Hosts, Configure, Infrastructure, and Access Insights. On the right side of the navigation bar, there is a 'Red Hat Access' dropdown and a user profile for 'Admin User' with an 'Administer' link.

The main content area shows a compliance report for a host. The report is organized into sections, each with a summary of results:

- 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**: 6x fail

At the bottom of the page, the URL [https://sat61.local.lan/compliance/arf\\_reports/1#](https://sat61.local.lan/compliance/arf_reports/1#) is visible.

# SCAP IN RED HAT SATELLITE 6

Further references...

Red Hat Satellite 6.1 Feature Overview: OpenSCAP

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

# FUTURE PLANS

# REWORKED ATOMIC SCAN

Faster and more robust execution, less privileges required

- Atomic does the mounting
- The OpenSCAP-daemon container does the scanning

# STANDARD COMPLIANCE

Automated standard compliance checking

- Automated SCAP policy management - no need to specify content
- Not specific to the workload
- Planned for future versions of Atomic

# SPECIALIZED PCI-DSS REPORT

HTML report customized for PCI-DSS compliance

- Maps PCI-DSS IDs to policy rules instead of the other way around

# REMEDIATIONS FOR CONTAINERS AND VMs

Put containers and virtual machines into compliance without installing SCAP tools on them

- Change configuration of a container or container image
- Planned for future versions of Atomic



# MORE SCAP POLICY OPTIONS

Continuously extend and improve the provided SCAP policies

- HIPPA
- SOX

# FURTHER READING

- [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7/html/Security\\_Guide/chap-Compliance\\_and\\_Vulnerability\\_Scanning.html](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Compliance_and_Vulnerability_Scanning.html)
- <https://www.open-scap.org/>
- <https://github.com/OpenSCAP/scap-security-guide/wiki/Collateral-and-References>



# THANK YOU!

## Questions?



[plus.google.com/+RedHat](https://plus.google.com/+RedHat)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[twitter.com/RedHatNews](https://twitter.com/RedHatNews)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)