redhat.

Security Compliance with OpenSCAP

Automatically find vulnerabilities and configuration issues of your infrastructure

Martin Preisler
Software Engineer, Red Hat, Inc.

FOCUS OF THIS SESSION

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

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

VULNERABILITIES

Undiscovered vulnerabilities are bad.

- But not all that bad, everybody has them
- It’s a lot of effort to use those for exploits

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:

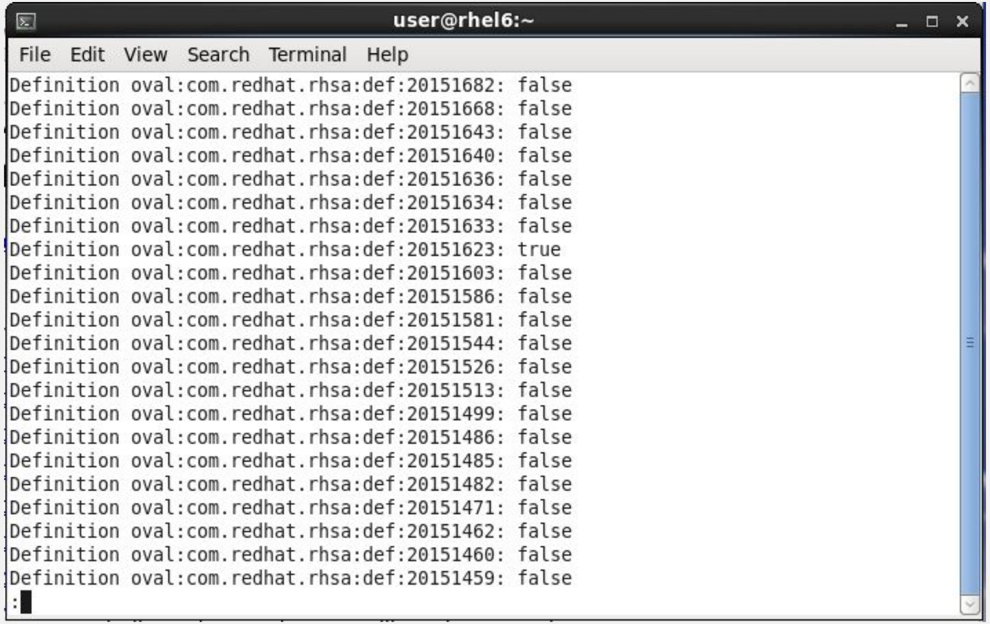
1. Download the CVE data
2. Execute the oscap tool
3. Review the results

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

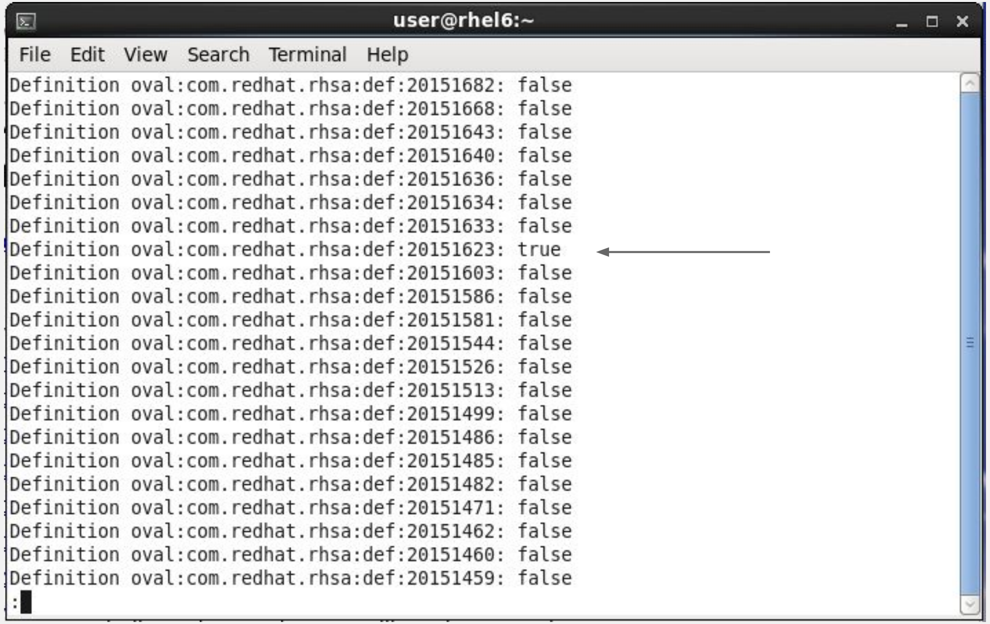
After the command is invoked this is what we can see in stdout.



```
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

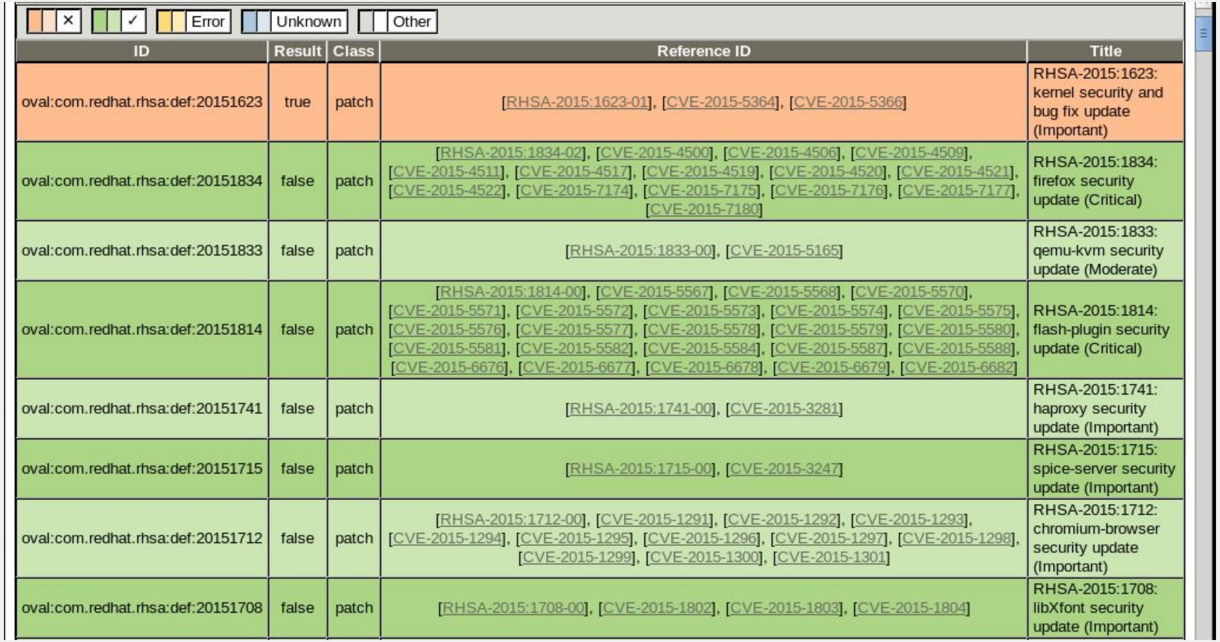
After the command is invoked this is what we can see in stdout.



```
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

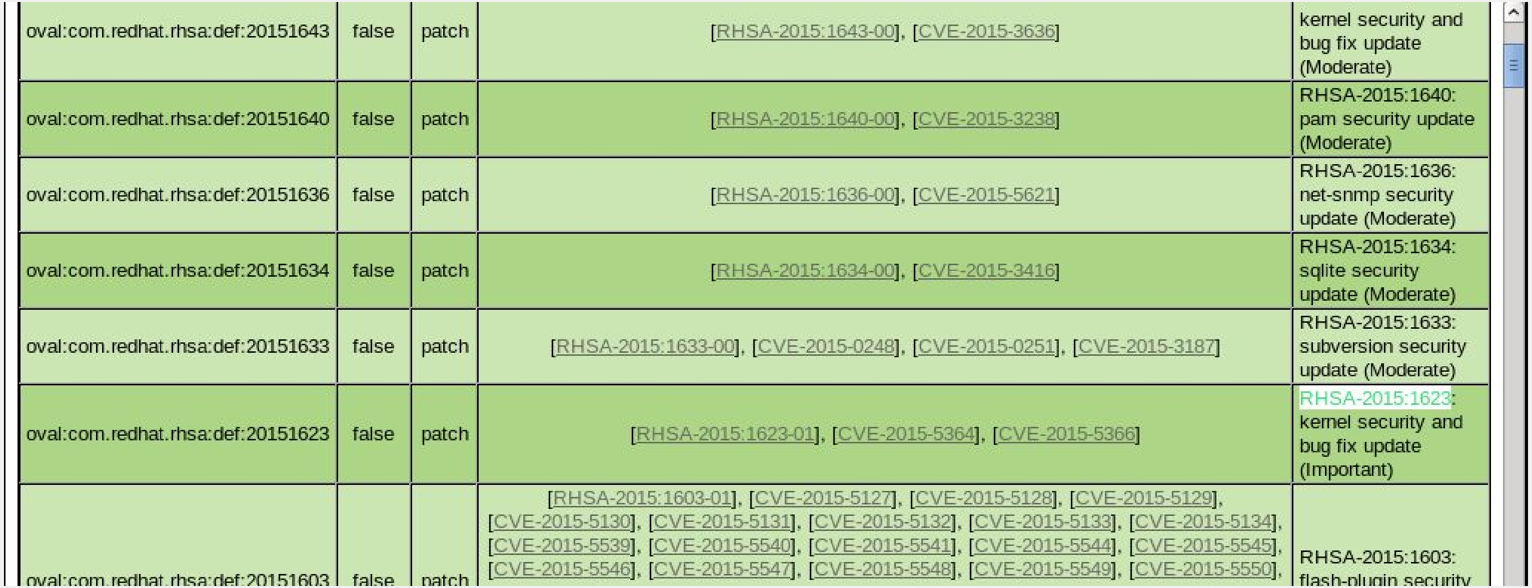
Let’s see more details by opening the HTML report.



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

WHAT ABOUT CONTAINERS?

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

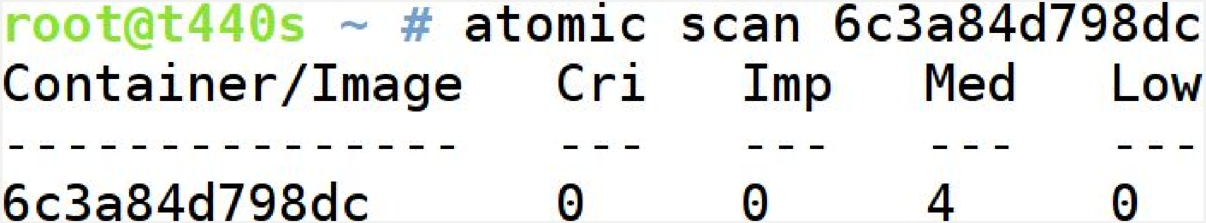
Production deployments are increasingly using containers. This brings new challenges.

- 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

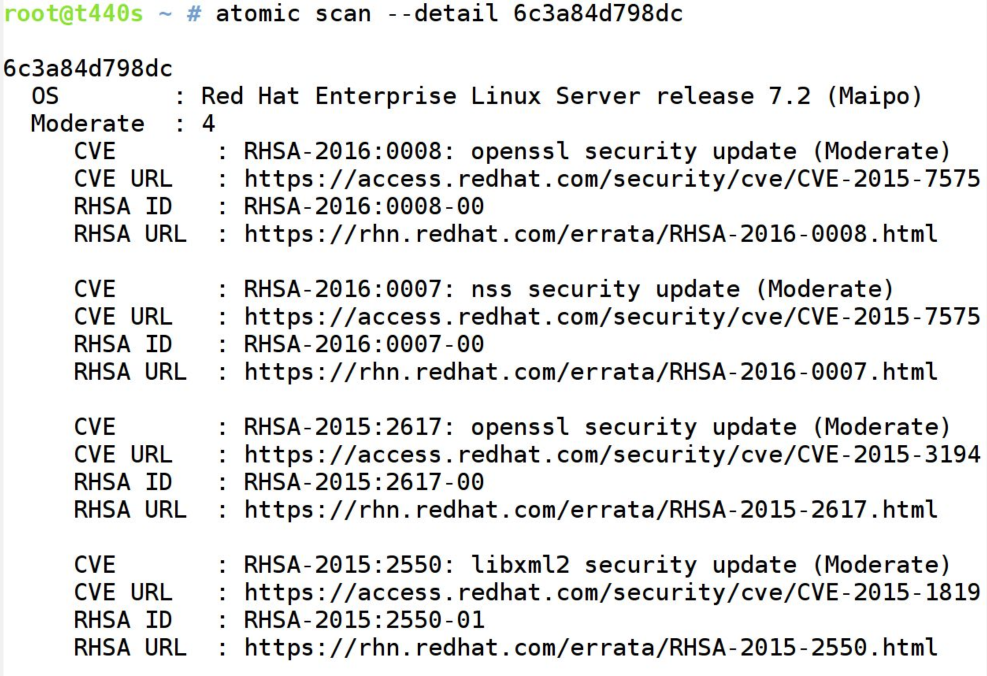
Scan containers and container images for CVEs.



```
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

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 OSCAP 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

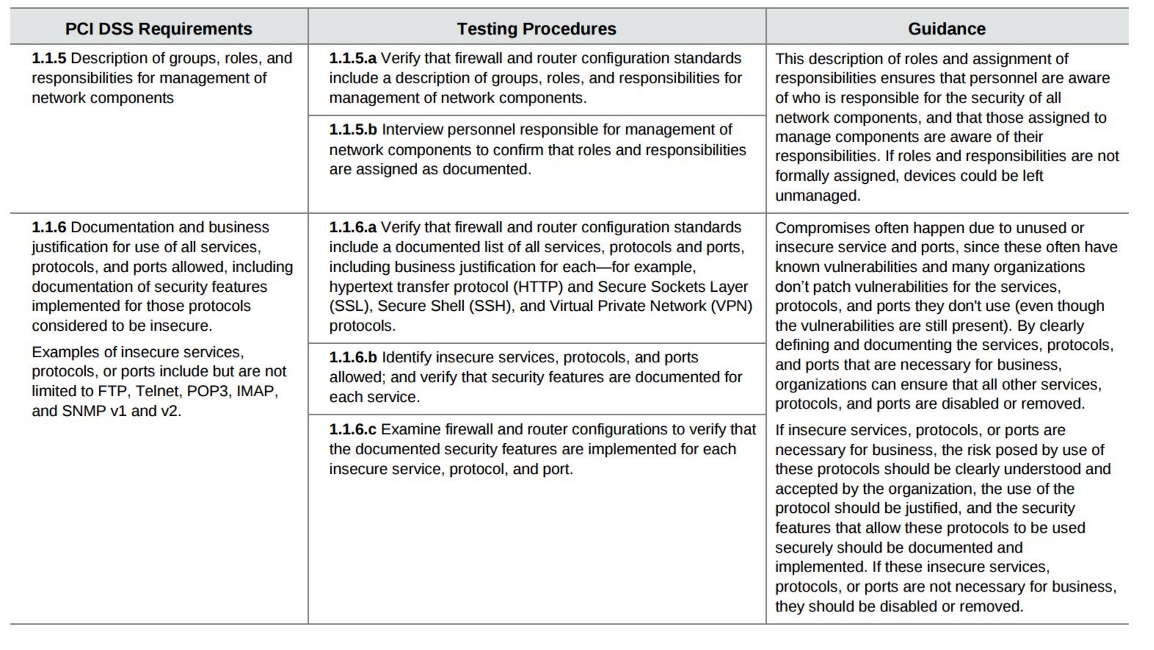
what it means to secure a system

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
1.1.5 Description of groups, roles, and responsibilities for management of network components	**1.1.5.a** 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.
	1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	
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. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	**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.	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.
	1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.	
	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.	

WHAT IS SCAP?

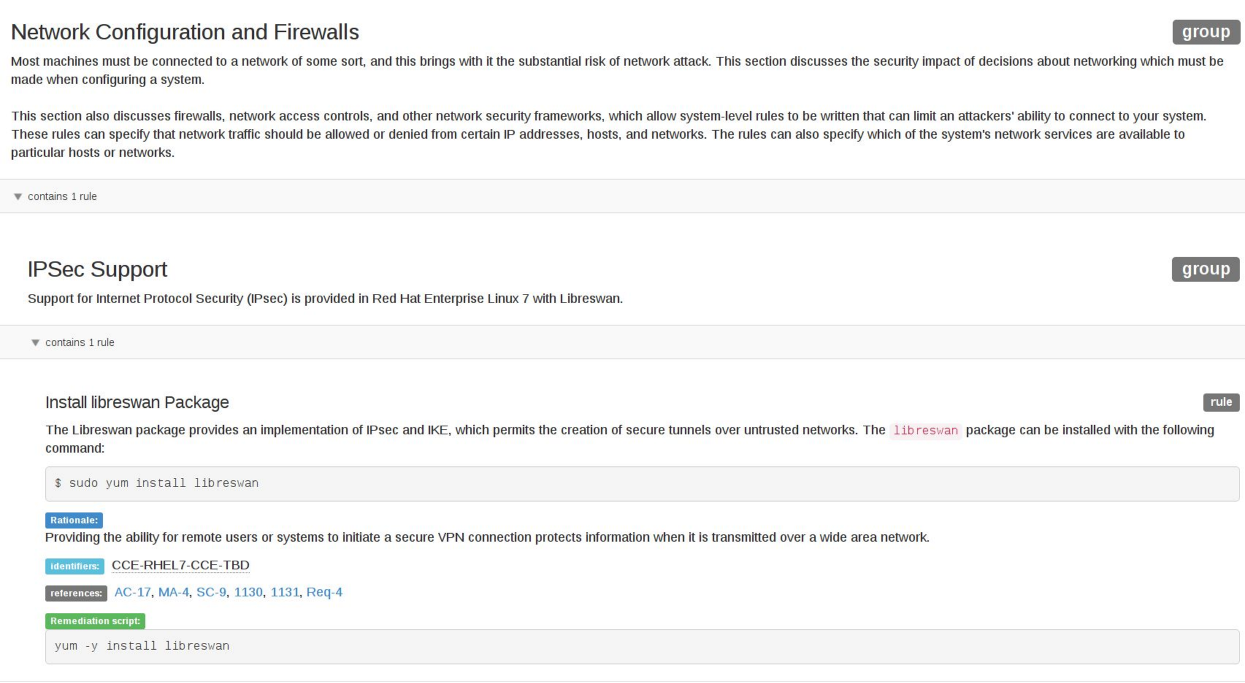
a way to express security policies in machine readable form.

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 SECURITY POLICY EXAMPLE

HTML guide generated from SCAP security policy



Network Configuration and Firewalls

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.

IPSec Support

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

Install libreswan Package

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*

OpenSCAP BASE

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:

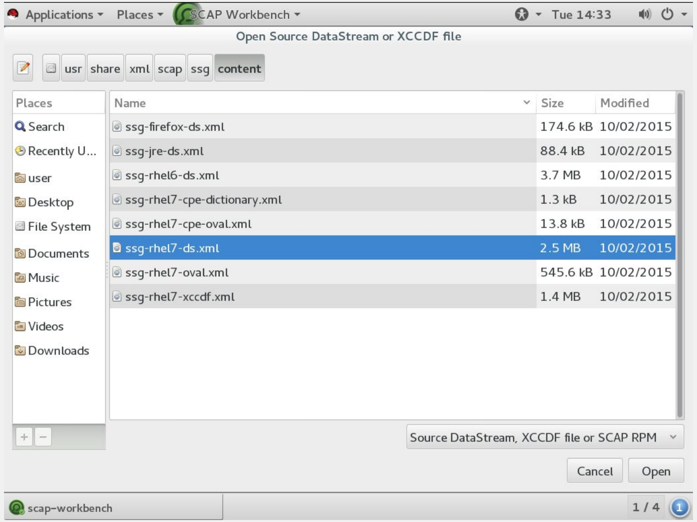
- Red Hat Enterprise Linux 7.2
- OpenSCAP and SCAP Workbench
- PCI-DSS from SCAP Security Guide

INSTALL THE NECESSARY TOOLS

(assuming Red Hat Enterprise Linux 7.2)

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

START SCAP-WORKBENCH



Open Source DataStream or XCCDF file

usr share xml scap ssg content

Name	Size	Modified
ssg-firefox-ds.xml	174.6 kB	10/02/2015
ssg-jre-ds.xml	88.4 kB	10/02/2015
ssg-rhel6-ds.xml	3.7 MB	10/02/2015
ssg-rhel7-cpe-dictionary.xml	1.3 kB	10/02/2015
ssg-rhel7-cpe-oval.xml	13.8 kB	10/02/2015
ssg-rhel7-ds.xml	2.5 MB	10/02/2015
ssg-rhel7-oval.xml	545.6 kB	10/02/2015
ssg-rhel7-xccdf.xml	1.4 MB	10/02/2015

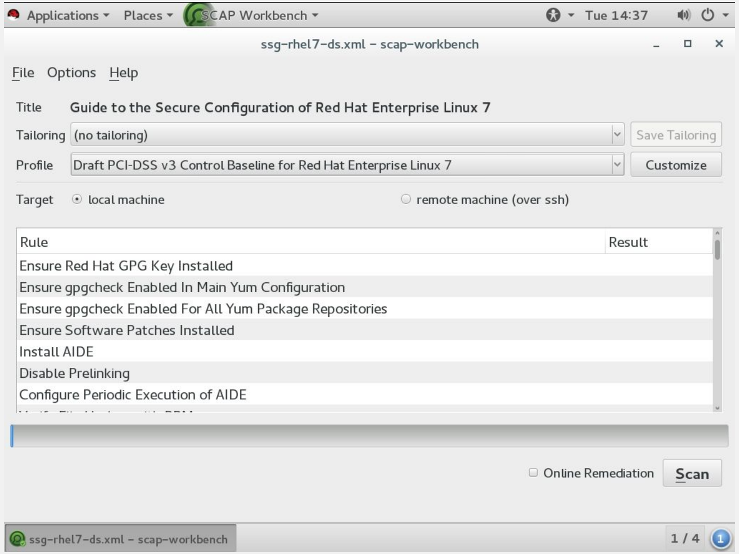
Source DataStream, XCCDF file or SCAP RPM

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



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

Tailoring (no tailoring)

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

Target ● local machine ○ remote machine (over ssh)

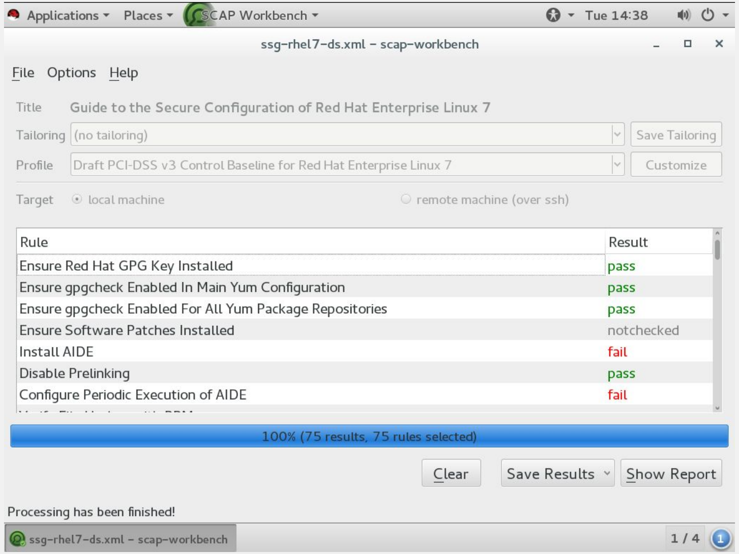
Rule	Result
Ensure Red Hat GPG Key Installed	
Ensure gpgcheck Enabled In Main Yum Configuration	
Ensure gpgcheck Enabled For All Yum Package Repositories	
Ensure Software Patches Installed	
Install AIDE	
Disable Prelinking	
Configure Periodic Execution of AIDE	

□ Online Remediation

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



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

Tailoring (no tailoring)

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

Target ● local machine ○ remote machine (over ssh)

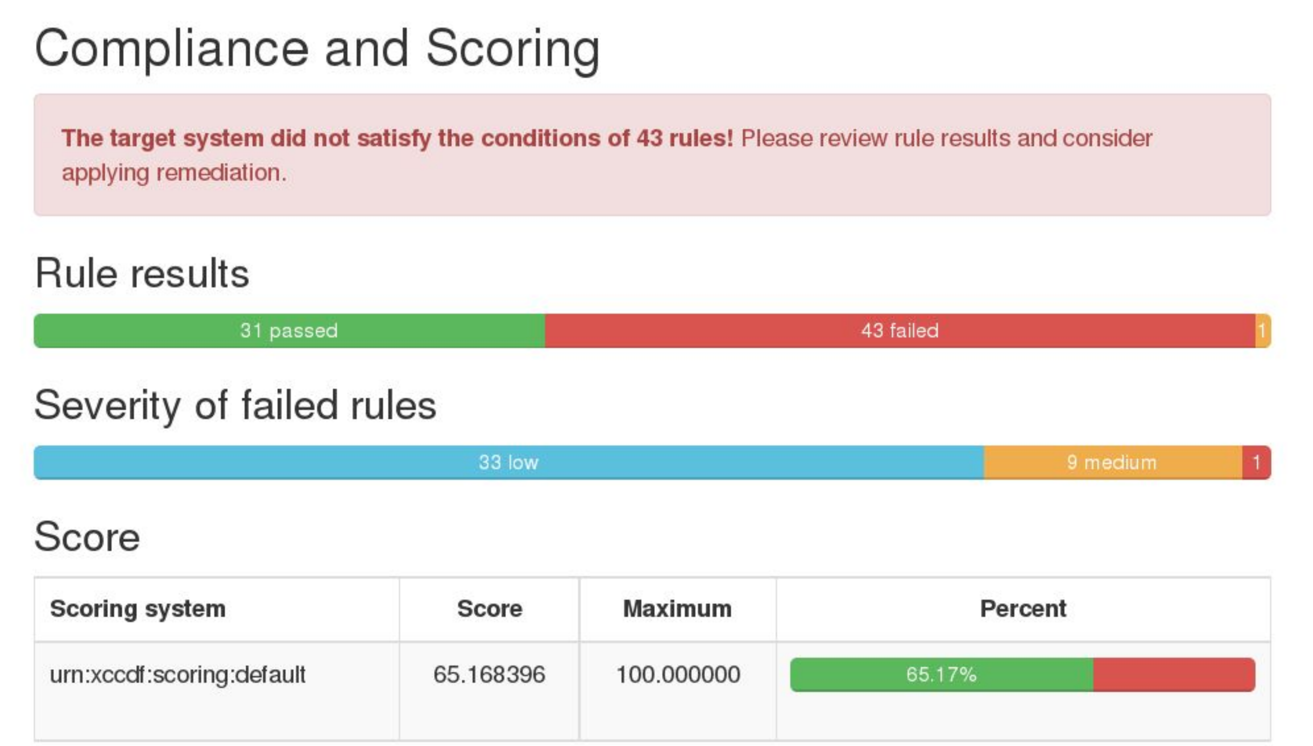
Rule	Result
Ensure Red Hat GPG Key Installed	pass
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	pass
Ensure Software Patches Installed	notchecked
Install AIDE	fail
Disable Prelinking	pass
Configure Periodic Execution of AIDE	fail

100% (75 results, 75 rules selected)

Processing has been finished!

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

31 passed | 43 failed | 1

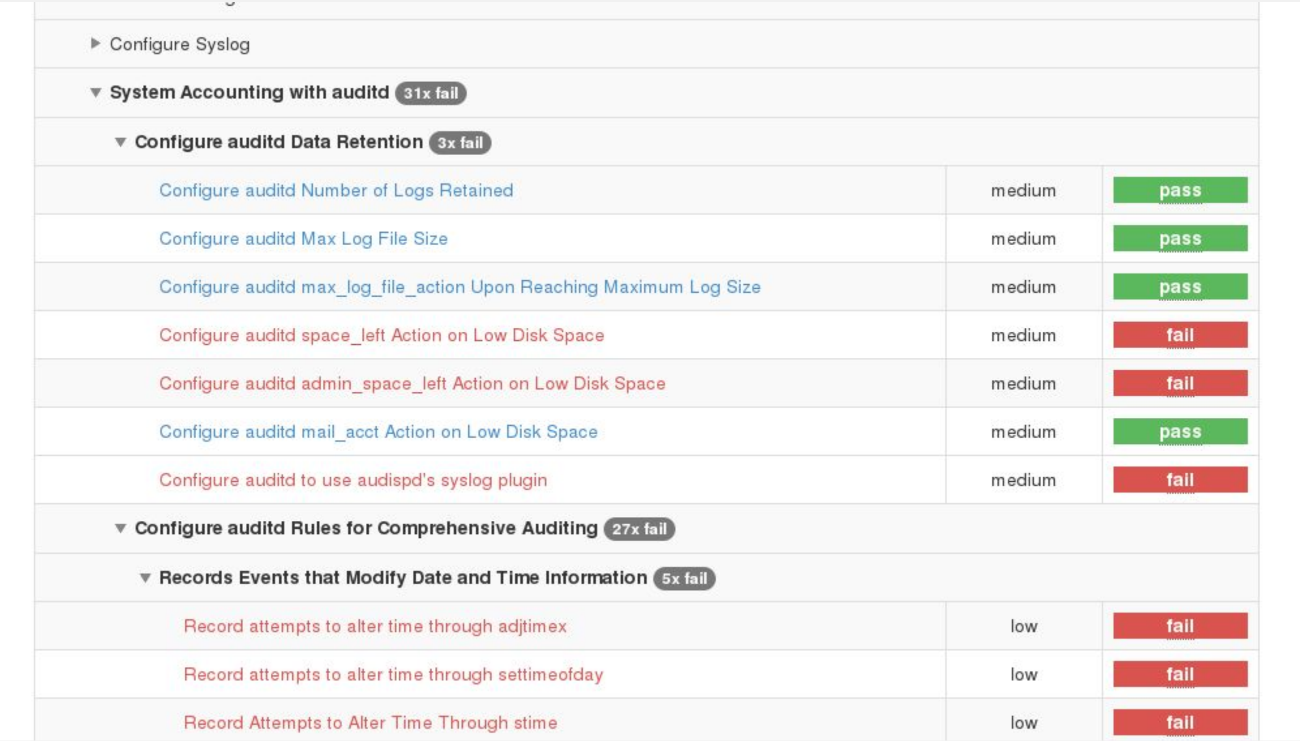
Severity of failed rules

33 low | 9 medium | 1

Score

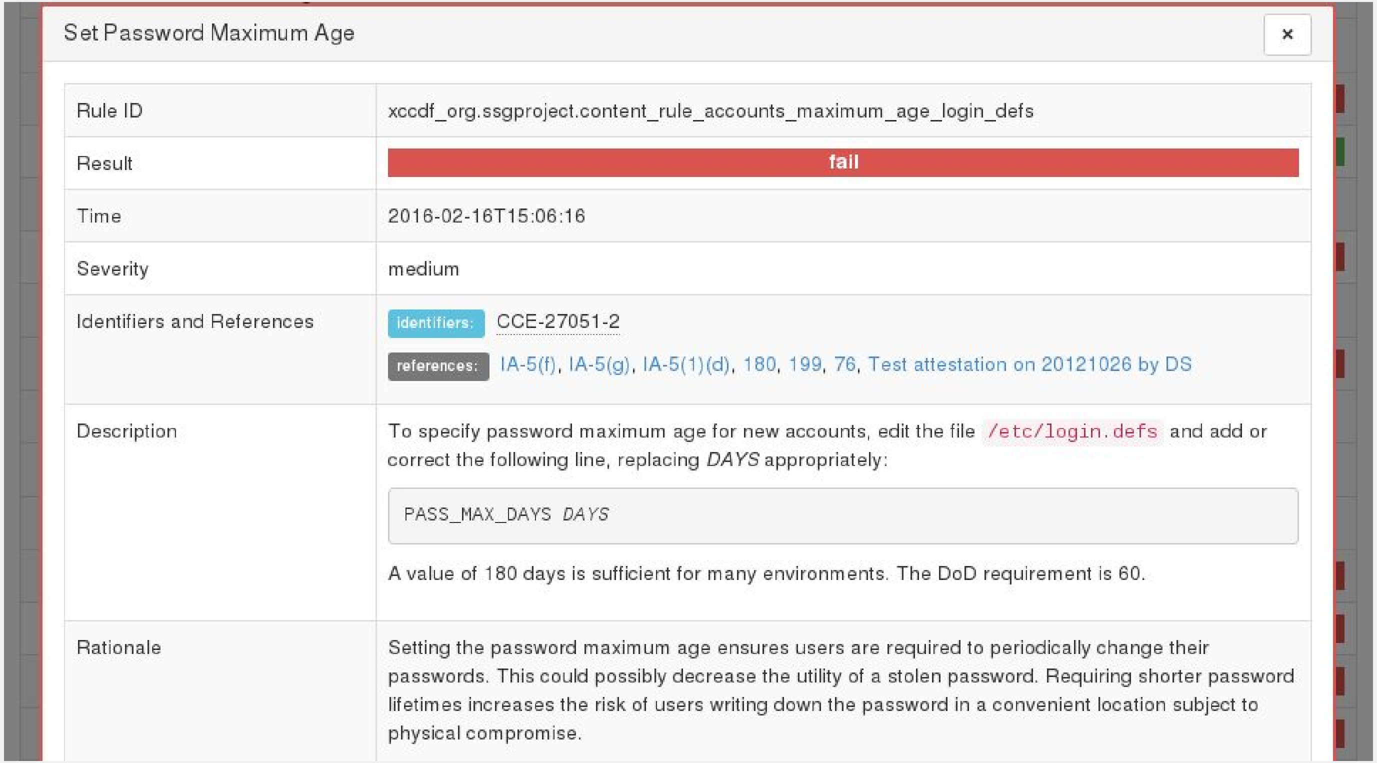
Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	65.168396	100.000000	65.17%

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

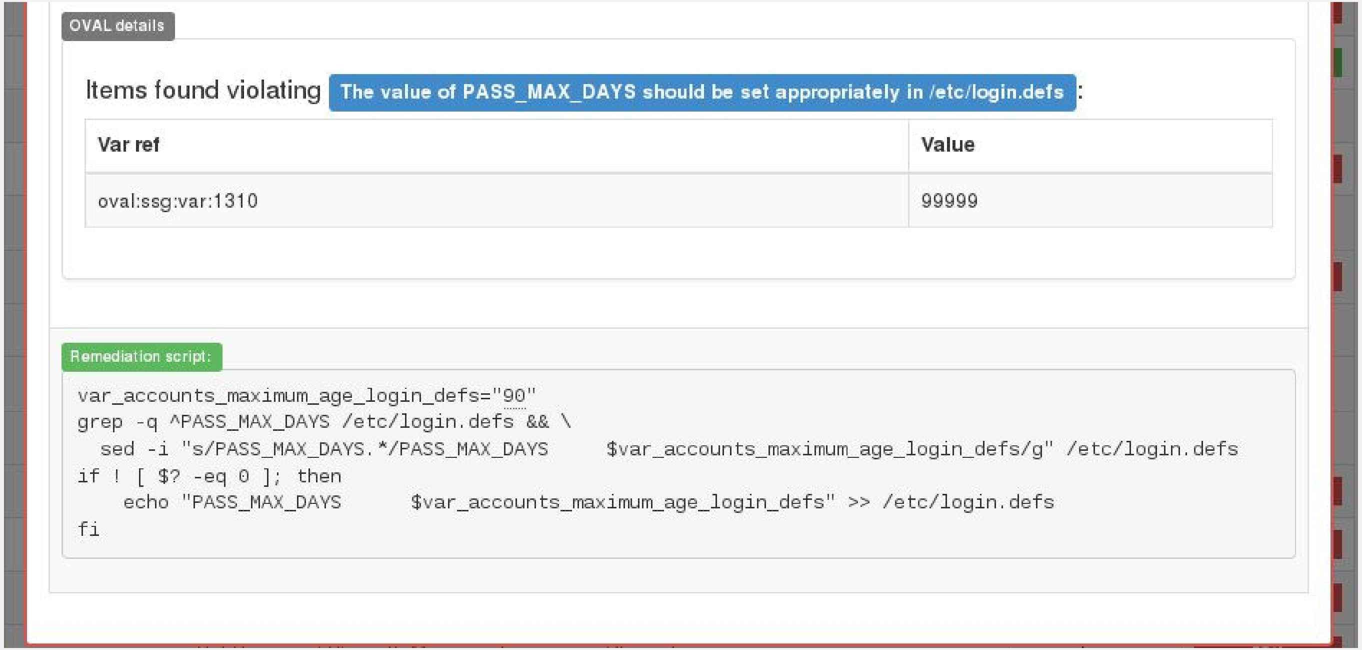
INITIAL RESULTS



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	identifiers: CCE-27051-2 references: IA-5(f), IA-5(g), IA-5(1)(d), 180, 199, 76, Test attestation on 20121026 by DS
Description	To specify password maximum age for new accounts, edit the file `/etc/login.defs` and add or correct the following line, replacing *DAYS* appropriately: `PASS_MAX_DAYS DAYS` A value of 180 days is sufficient for many environments. The DoD requirement is 60.
Rationale	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.

INITIAL RESULTS



OVAL details

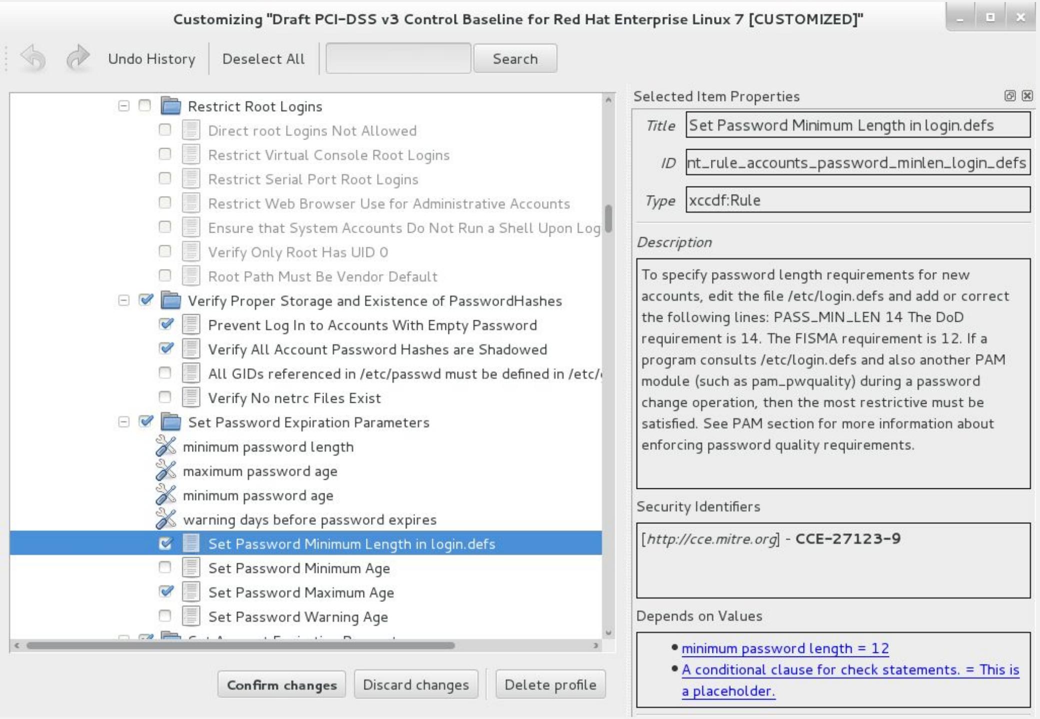
Items found violating The value of PASS_MAX_DAYS should be set appropriately in /etc/login.defs :

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



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

- ☐ Restrict Root Logins
  - ☐ Direct root Logins Not Allowed
  - ☐ Restrict Virtual Console Root Logins
  - ☐ Restrict Serial Port Root Logins
  - ☐ Restrict Web Browser Use for Administrative Accounts
  - ☐ Ensure that System Accounts Do Not Run a Shell Upon Log
  - ☐ Verify Only Root Has UID 0
  - ☐ Root Path Must Be Vendor Default
- ☑ Verify Proper Storage and Existence of PasswordHashes
  - ☑ Prevent Log In to Accounts With Empty Password
  - ☑ Verify All Account Password Hashes are Shadowed
  - ☐ All GIDs referenced in /etc/passwd must be defined in /etc/
  - ☐ Verify No netrc Files Exist
- ☑ Set Password Expiration Parameters
  - minimum password length
  - maximum password age
  - minimum password age
  - warning days before password expires
  - ☑ Set Password Minimum Length in login.defs
  - ☐ Set Password Minimum Age
  - ☑ Set Password Maximum Age
  - ☐ Set Password Warning Age

Selected Item Properties

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://cce.mitre.org*] - **CCE-27123-9**

Depends on Values

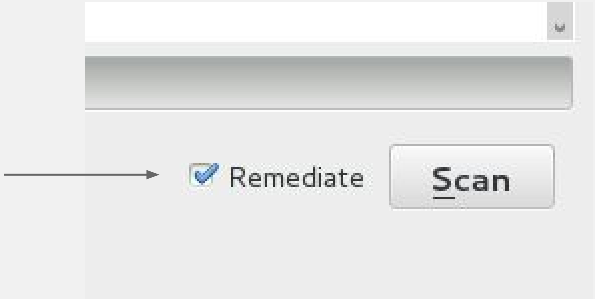
- minimum password length = 12
- A conditional clause for check statements. = This is a placeholder.

AUTOMATICALLY FIXING THE ISSUES

Check *Remediate* to automatically fix issues after scanning

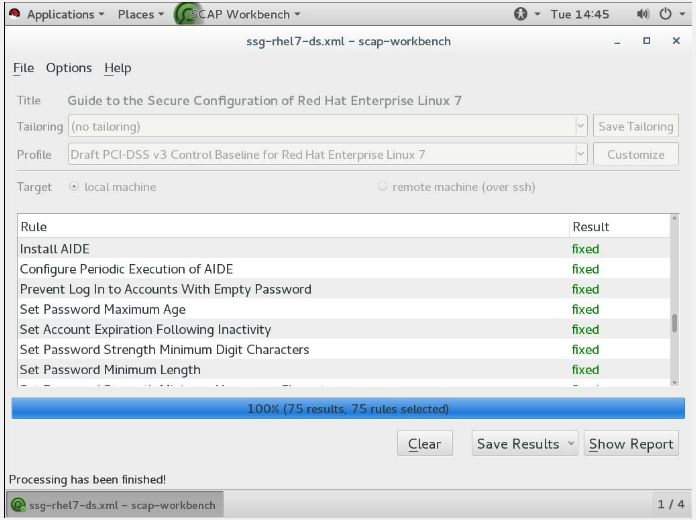
We now have a profile defined, let's put the machine closer to compliance. Keep this in mind when doing automatic remediation:

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



REMEDIATION WITH SCAP-WORKBENCH

let’s do a quick scan to establish a baseline



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

Tailoring: (no tailoring)

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

Target: ● local machine ○ remote machine (over ssh)

Rule	Result
Install AIDE	fixed
Configure Periodic Execution of AIDE	fixed
Prevent Log In to Accounts With Empty Password	fixed
Set Password Maximum Age	fixed
Set Account Expiration Following Inactivity	fixed
Set Password Strength Minimum Digit Characters	fixed
Set Password Minimum Length	fixed

100% (75 results, 75 rules selected)

Processing has been finished!

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

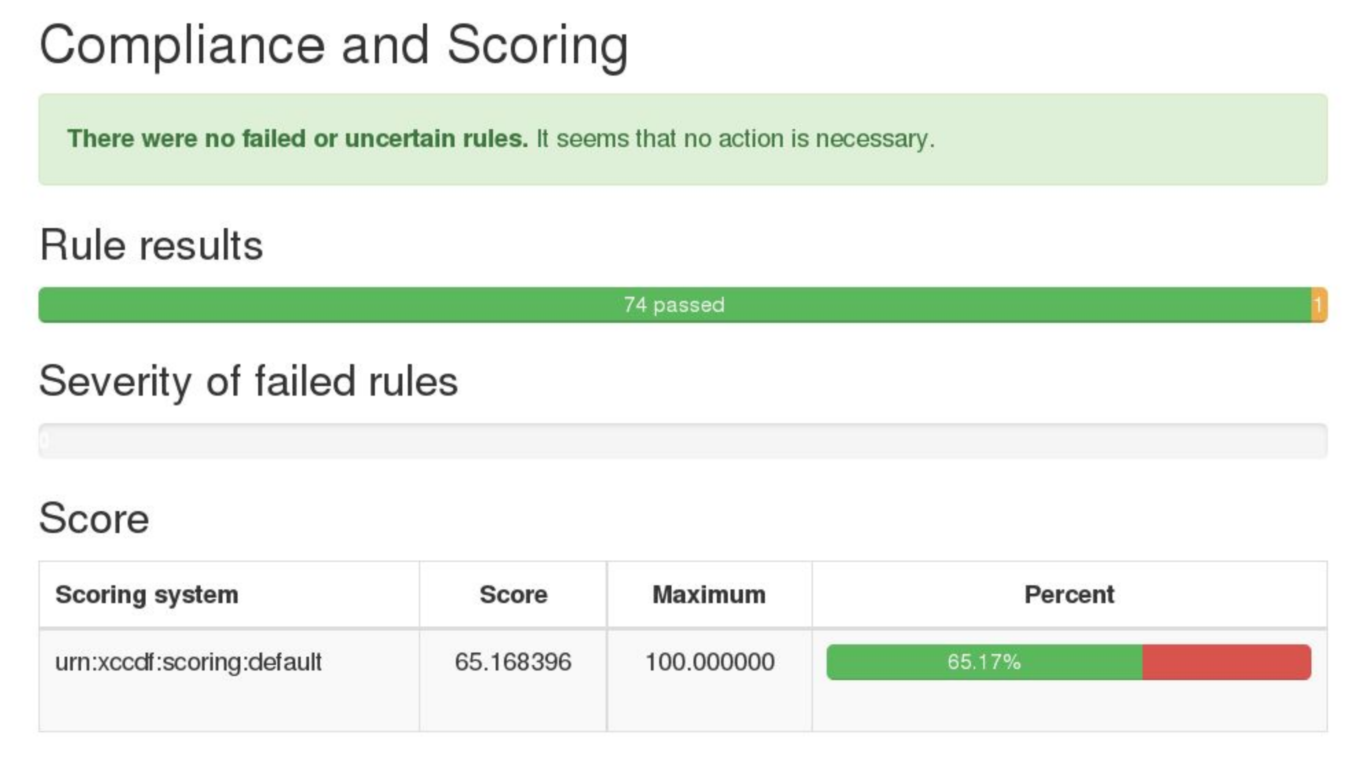
SAVING THE FINAL POLICY

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.

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	65.17%

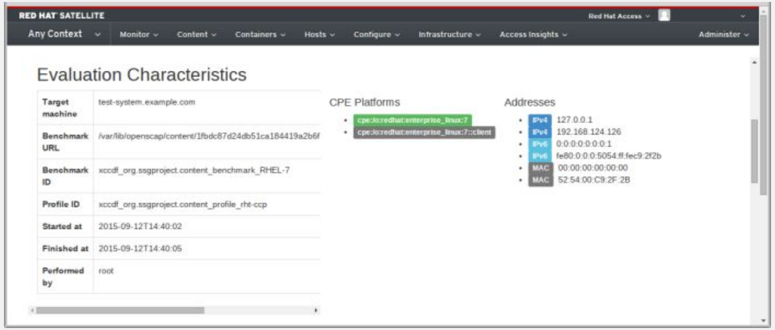
USE-CASE 3:
SECURITY COMPLIANCE FOR AN INFRASTRUCTURE

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



Evaluation Characteristics

Target machine	test-system.example.com
Benchmark URL	/var/lib/openscap/content/1fbdc87d24db51ca184419a2b6f
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_org.ssgproject.content_profile_rht-ccp
Started at	2015-09-12T14:40:02
Finished at	2015-09-12T14:40:05
Performed by	root

CPE Platforms

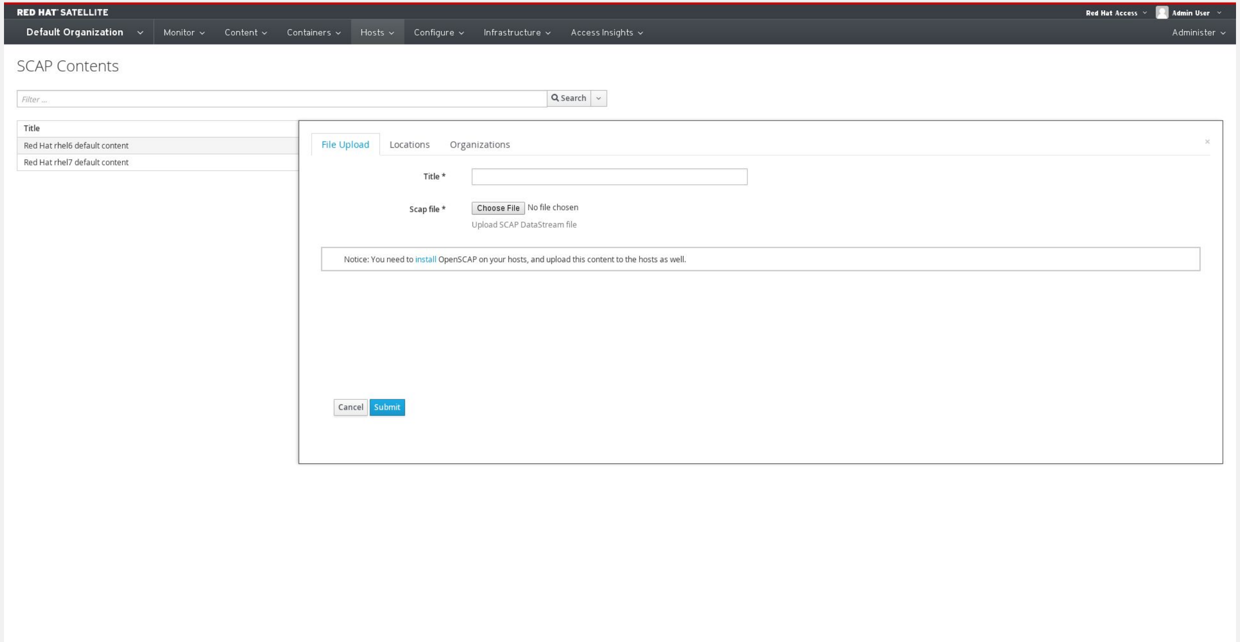
- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.124.126
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:5054:ff:fec9:2f2b
- MAC 00:00:00:00:00:00
- MAC 52:54:00:C9:2F:2B

SCAP IN RED HAT SATELLITE 6

upload SCAP content to create new SCAP policies



Title
Red Hat rhel6 default content
Red Hat rhel7 default content

Title *

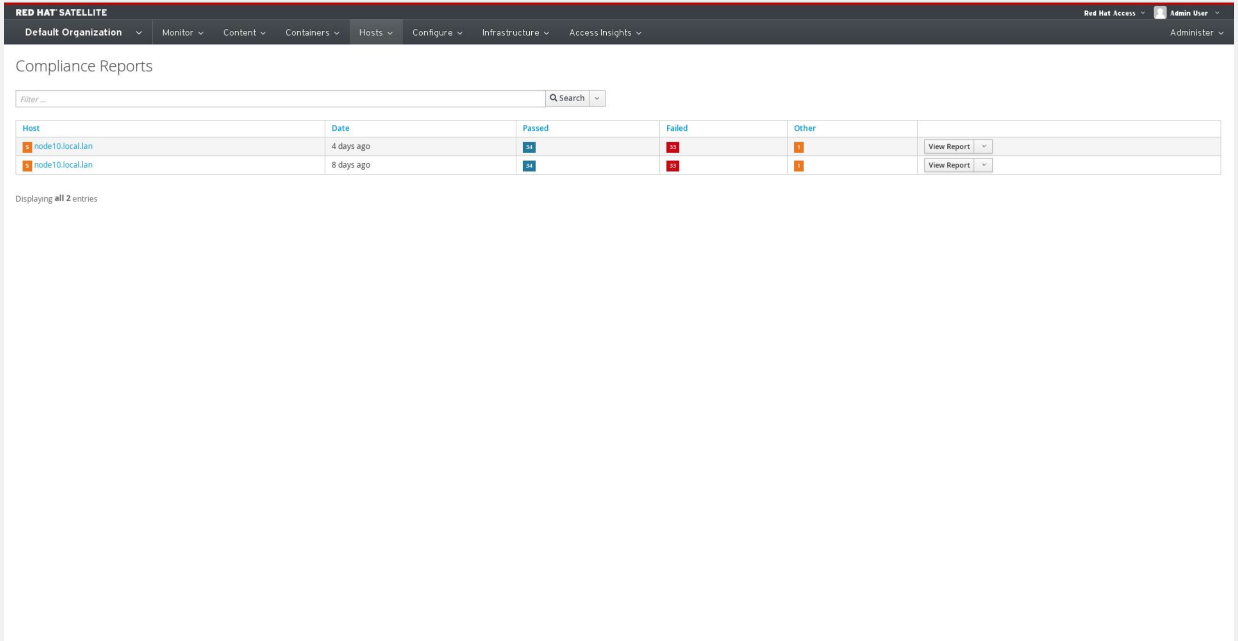
Scap file * No file chosen

Upload SCAP DataStream file

Notice: You need to install OpenSCAP on your hosts, and upload this content to the hosts as well.

SCAP IN RED HAT SATELLITE 6

see past results



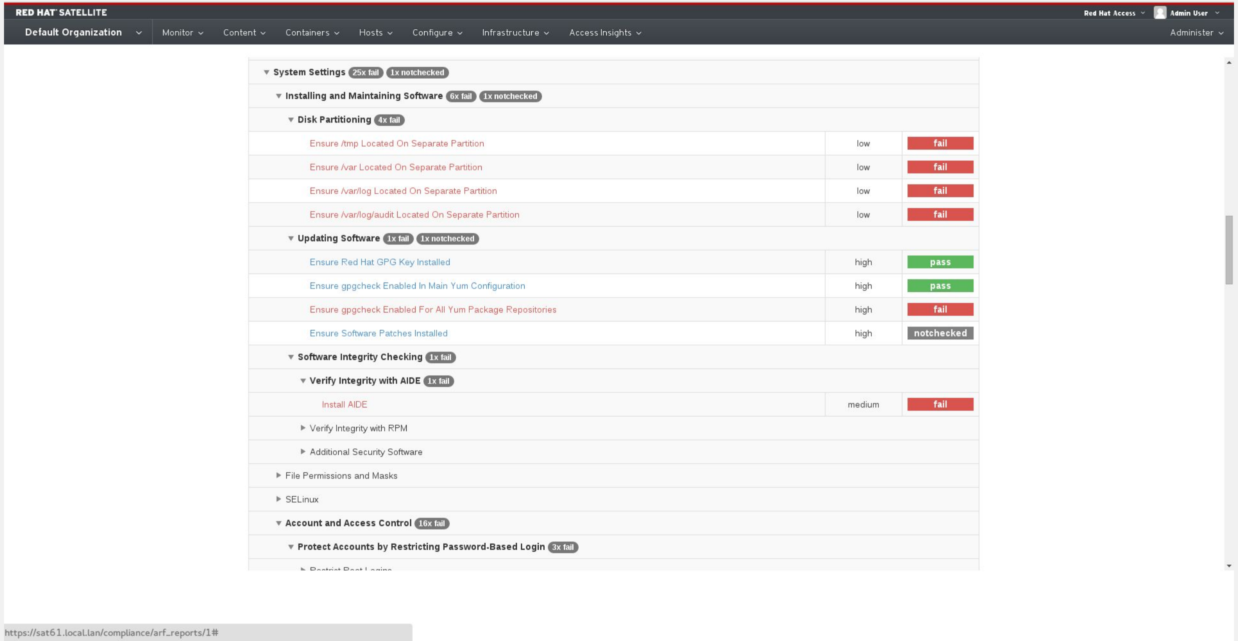
Compliance Reports

Host	Date	Passed	Failed	Other	
S node10.local.lan	4 days ago	34	33	1	View Report
S node10.local.lan	8 days ago	34	33	1	View Report

Displaying **all 2** entries

SCAP IN RED HAT SATELLITE 6

browse HTML report for details of a past result



▼ **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		
▶ Restrict Root Logins		

https://sat61.local.lan/compliance/arf_reports/1#

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos