



OpenSCAP

Šimon Lukašík

Agenda

- Compliance Audit
- Why we are doing it
- What is SCAP
- OpenSCAP ecosystem
- Future challenges

appetizer

Compliance Audit

- Proactive security
- Security Policy
- Why?
 - Military (stig)
 - Government regulations (cc, usgcb)
 - FISMA Act.
 - ISO/EIC 27000 standard series
 - Card industry (pci dss)

demo

What is SCAP

- Group of many standards
- Automated compliance checking
- Governed by NIST
 - <http://scap.nist.gov/>
 - Industry standard
- Current version: 1.2

SCAP Components



SCAP Component Standards

Enumeration

CCE

CVE

CPE

Assessment Language

OVAL

OCIL

SCE

use

use

use

Checklist

XCCDF

instantiate

CVE
Feed

CCE
List

CPE
Dictionary

XCCDF
Benchmark

OVAL
Results

OVAL
Definitions

OCIL
Questionnaire

Shell
Scripts

SCAP 1.1 Document Formats

SCAP 1.2 Document Formats

Asset Report
Format

include

MEETING IN PROGRESS

WTF?!



DON'T WORRY.

SECURITY

No acronyms. No security. No problem.



SCAP
SECURITY GUIDE



SCAP
WORKBENCH



Foreman
OpenSCAP



Ruby Gem
OpenSCAP



Puppet
OpenSCAP



SCAPtimony



open-scap.org

Title Verify permissions on 'shadow' file
Rule rule-2.2.3.1.i
Ident CCE-4130-1
Result pass

Title Verify permissions on 'group' file
Rule rule-2.2.3.1.j
Ident CCE-3967-7
Result pass

Title Verify permissions on 'gshadow' file
Rule rule-2.2.3.1.k
Ident CCE-3932-1
Result pass

Title Verify permissions on 'passwd' file
Rule rule-2.2.3.1.l
Ident CCE-3566-7
Result pass

Title Verify that All World-Writable Directories Have Sticky B
Rule rule-2.2.3.2.a
Ident CCE-3399-3
Result



github.com/OpenSCAP/scap-security-guide

demo



github.com/OpenSCAP/scap-workbench

File Help

Title Guide to the Secure Configuration of Fedora

Tailoring (no tailoring)



Save Tailoring

Profile Common Profile for General-Purpose Fedora Systems



Customize

Target ☒ local machine☐ remote machine (over ssh)

Rule	Result
netrc Files Do Not Exist	pass
Password Minimum Length	fail
Password Minimum Age	fail
Password Maximum Age	fail
Password Warning Age	pass
NTP Daemon Enabled	fail
Remote NTP Server Specified	fail
SSH Root Login Disabled	pass
SSH Access via Empty Passwords Disabled	pass
SSH Idle Timeout Interval Used	pass
SSH Client Alive Count Used	pass

100% (24 results, 24 rules selected)

Clear

Save Results ▾

Show Report

Processing has been finished!

Tailoring "Common Profile for General-Purpose Fedora Systems [TAILORED]"



Undo History

Deselect All

Search

- ☒ Log In to Accounts With Empty Password Imposed
- ☒ Password Hashes For Each Account Shadowed
- ☐ All GIDs referenced in /etc/passwd Defined in /etc/passwd
- ☒ netrc Files Do Not Exist
- ☐ ☒ Set Password Expiration Parameters
 - minimum password length
 - maximum password age
 - minimum password age
 - warning days before password expires
 - ☒ Password Minimum Length
 - ☐ Password Minimum Age
 - ☐ Password Maximum Age
 - ☒ Password Warning Age
- ☐ ☒ Services
 - ☐ ☒ Network Time Protocol
 - ☒ NTP Daemon Enabled
 - ☒ Remote NTP Server Specified
 - ☐ ☒ SSH Server
 - SSH session Idle time
 - ☐ ☒ Configure OpenSSH Server if Necessary
 - ☒ SSH Root Login Disabled
 - ☒ SSH Access via Empty Passwords Disabled

Selected Item Properties



Title Password Maximum Age

ID content_rule_accounts_maximum_age_login_defs

Type xccdf:Rule

Description

To specify password maximum age for new accounts, edit the file /etc/login.defs and add or correct the following line, replacing the DAYS item appropriately:
PASS_MAX_DAYS DAYS A value of 180 days is sufficient for many environments.

Profile Properties



Title General-Purpose Fedora Systems [TAILORED]

ID ssgproject.content_profile_common_tailored2

Description

This profile contains items common to general-purpose Fedora installations.

Confirm tailoring

Discard changes

Delete profile

File HelpTitle **Guide to the Secure Configuration of Fedora**

Tailoring (unsaved changes)



Save Tailoring

Profile Common Profile for General-Purpose Fedora Systems



Customize

Target

Rule

Prelinkin

gpgched

gpgched

Shared L

Shared L

System I

System I

Direct r

Virtual C

Serial Port Root Logins Restricted

Only Root Has UID 0

Save as RPM

Package Name ssg-fedora-ds

Version

1

Release

1



Summary

License

Unspecified



Cancel

OK

☐ Online Remediation

Scan



SPACEWALK

spacewalk.redhat.com



Overview

Systems

All

Virtual Systems

Out of Date

Requiring Reboot

Untitled

Ungrouped

Inactive

Recently Registered

Proxy

Duplicate Systems

System Currency

System Groups

System Set Manager

Advanced Search

Activation Keys

Stored Profiles

Custom System Info

Kickstart

Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed

bob.example.com

remove from ssm | delete system

Details

Software

Groups

Virtualization

Audit

Events

List Scans

Schedule

OpenSCAP Scans

														1 - 10 of 10	
Xccdf Test Result			Completed	Compliance	P	F	E	U	N	K	S	I	X	Total	
	OSCAP-Test-united_states_government_configuration_baseline		Thu Jul 12 09:31:52 EDT 2012	46 %	116	105	3	25	0	1	8	0	0	258	
	OSCAP-Test-united_states_government_configuration_baseline		Thu Jul 12 08:22:15 EDT 2012	46 %	115	106	3	25	0	1	8	0	0	258	
	OSCAP-Test-united_states_government_configuration_baseline		Thu Jul 12 07:37:45 EDT 2012	46 %	115	106	3	25	0	1	8	0	0	258	
	OSCAP-Test-united_states_government_configuration_baseline		Thu Jul 12 07:27:50 EDT 2012	46 %	116	105	3	25	0	1	8	0	0	258	
	OSCAP-Test-desktop		Thu Jul 12 07:14:04 EDT 2012	48 %	74	75	0	4	0	2	251	0	0	406	
	OSCAP-Test-ftp		Thu Jul 12 07:12:48 EDT 2012	48 %	76	72	0	11	0	1	246	0	0	406	
	OSCAP-Test-united_states_government_configuration_baseline		Wed Jul 11 09:33:03 EDT 2012	46 %	116	105	3	25	0	1	8	0	0	258	
	OSCAP-Test-united_states_government_configuration_baseline		Wed Jul 11 09:30:16 EDT 2012	46 %	116	105	3	26	0	1	7	0	0	258	
	OSCAP-Test-united_states_government_configuration_baseline		Wed Jul 11 09:27:35 EDT 2012	46 %	116	105	3	26	0	1	7	0	0	258	
	OSCAP-Test-default-profile		Wed Jul 11 09:23:15 EDT 2012	N/A	0	0	0	0	0	0	258	0	0	258	

Download CSV

1 - 10 of 10

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



- OpenSCAP
- All Scans
- XCCDF Diff
- Advanced Search
- Log Review

OpenSCAP Diff

Details of XCCDF Scan

Full Comparison

Only Changed Items

Only Invariant Items

1 - 3 of 3

Field Names	First Scan	Second Scan
Id:	862	875
Started:	2012-07-12 07:35:10.0	2012-07-12 08:19:23.0
Completed:	2012-07-12 07:37:44.0	2012-07-12 08:22:14.0

1 - 3 of 3

XCCDF Rule Results

Display

25

▼

items per page

1 - 2 of 2

XCCDF Rule Identifier	First Scan	Second Scan
talk_server_package	fail	pass
usgcb-rhel5desktop-rule-2.4.2.c	pass	fail

1 - 2 of 2

OpenSCAP

All Scans

Advanced Search

Log Review



OpenSCAP Search

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

Specify your search criteria below.

Xccdf Legend

P - Pass

F - Fail

E - Error

U - Unknown

N - Not applicable

K - Not checked

S - Not selected

I - Informational

X - Fixed

Search XCCDF Rules For:

CCE-3818-2

Search

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

With Result:

fail

Where to Search:

- ☐ Search all systems
- ☒ Search system set manager

Scan Dates to Search:

☒ Search Scans Performed Between Dates

Start Date: June 1 2012 12:00 AM EDT

End Date: June 17 2012 6:51 AM EDT

Show Search Result As:

- ☒ List of XCCDF Rule Results
- ☐ List of XCCDF Scans

Filter by Result:

Go

Display 25 items per page

1 - 2 of 2

XCCDF Rule Identifier	XCCDF Ident Tags	Result
bootloader_password	CCE-3818-2	fail
usgcb-rhel5desktop-rule-2.3.5.2.d	CCE-3818-2	fail

1 - 2 of 2



OSCAP Anaconda Addon

fedorahosted.org/oscap-anaconda-addon

Choose profile below:

Common Profile for General-Purpose Systems

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

Desktop Baseline

This profile is for a desktop installation of RHEL 6.

Server Baseline

This profile is for RHEL 6 acting as a server.




Pre-release Draft STIG for RHEL 6 Server

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

Default

The default profile.

Changes needed to be done:

-  /tmp is not on a separate partition
-  /var/log is not on a separate partition
-  root password may be not strong enough

LOCALIZATION



DATE & TIME

America/New_York timezone



KEYBOARD

English (English (US))

SECURITY



SECURITY PROFILE

Misconfiguration detected

SOFTWARE



INSTALLATION SOURCE

Not ready



SOFTWARE SELECTION

Installation source not set up



NETWORK CONFIGURATION

Wired (eth0) connected

Quit

Begin Installation

We won't touch your disks until you hit this button.



Please complete items marked with this icon before continuing to the next step.







github.com/OpenSCAP/foreman_openscap



Compliance policy: fedora20-common-profile

Hosts Breakdown





















 Compliant with the policy	2
 Not compliant with the policy	0
 Inconclusive results	0
 Never audited	0

Total hosts: 2

Host Breakdown Chart

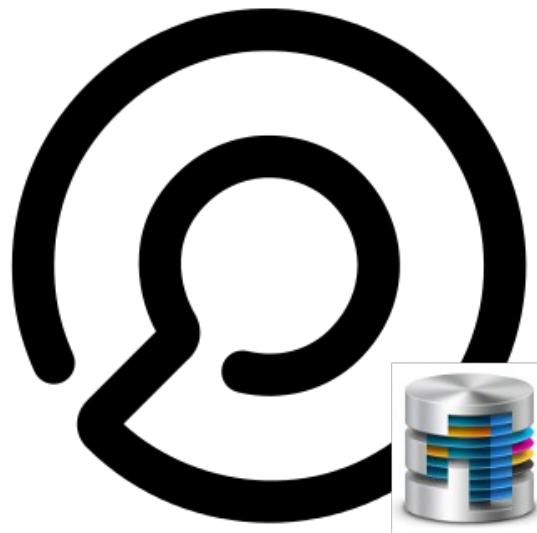


Latest reports for policy: fedora20-common-profile

Host	Date	Passed	Failed	Other	
 fedora20.mydomain	1 day ago	 0	 0	 0	View Report
 fedora20.mydomain	3 months ago	 0	 0	 0	View Report
 fedora20.mydomain	3 months ago	 0	 0	 0	View Report
 fedora20.mydomain	3 months ago	 0	 0	 0	View Report
 fedora20.mydomain	3 months ago	 0	 0	 0	View Report

Scale SCAP

- vendor neutral and centralized SW inventory
- vendor neutral CI compliance monitoring
- vendor neutral threat life-cycle management
- organization defined targeting
- better understanding of given system's purpose by auditing infrastructure



github.com/OpenSCAP/scapimoney

Thanks!

isimluk.livejournal.com
twitter.com/openscap