Applied SCAP:
Automating Security Compliance and Remediation

Shawn Wells

Maintainer, SCAP Security Guide

31-JULY-2014

45 MINUTES, 3 GOALS (+15 MIN Q&A)

1. Detail Security Automation Technology + Initiatives
    - Native Tooling [OpenSCAP]
    - Configuration Compliance [SCAP Security Guide]
    - Evolving Remediation Capabilities [currently, bash + puppet]

45 MINUTES, 3 GOALS (+15 MIN Q&A)

1. Detail Security Automation Technology + Initiatives
   - Native Tooling [OpenSCAP]
   - Configuration Compliance [SCAP Security Guide]
   - Evolving Remediation Capabilities [currently, bash + puppet]

2. Live Demo
   - Configuration Compliance Scanning
   - Patch & Vulnerability Scanning
   - Certification/Accreditation Paperwork Generation

45 MINUTES, 3 GOALS (+15 MIN Q&A)

1. Detail Security Automation Technology + Initiatives
   - Native Tooling [OpenSCAP]
   - Configuration Compliance [SCAP Security Guide]
   - Evolving Remediation Capabilities [currently, bash + puppet]

2. Live Demo
   - Configuration Compliance Scanning
   - Patch & Vulnerability Scanning
   - Certification/Accreditation Paperwork Generation

3. Discuss Roadmap (Gov't Plans, Packaging, Future Profiles)

FIRST, AN SCAP PRIMER

- A family of specifications managed by NIST

- Really a bunch of XML schema
  - which are data formats
  - so not a protocol at all, it turns out
  - openly defined, community developed, and *evolving*

... So, what kind of data do these formats organize?

FIRST, AN SCAP PRIMER

- Defines standardized formats … *okay, but why bother?*

- Because you’ll get:
  - Standardized inputs (e.g. a compliance baseline, status query)
  - Standardized outputs (results)

- Provides the enterprise ***liberty*** with regard to product choices
  - Avoids vendor lock-in, enables interoperability
  - Provides common technical position to vendors
  - Federal procurement language *requires* SCAP support in some cases

SCAP Security Guide

https://fedorahosted.org/scap-security-guide/

Contributors Include...

NATIONAL RECONNAISSANCE OFFICE
UNITED STATES OF AMERICA

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

OAK RIDGE
National Laboratory

ARL
U.S. Army Research Laboratory

TRESYS
TECHNOLOGY

LOCKHEED MARTIN

DEFENSE INFORMATION SYSTEMS AGENCY

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

redhat

In A Nutshell, SCAP Security Guide…

… has had 2,408 commits from 36 contributors, representing 224,872 lines of code

… took an estimated 43 years of effort (COCOMO model)

… has become upstream for all Red Hat STIGs, NIST NVD for JBoss, NSA's RHEL SNAC Guides

DISA STIG, Version 1, Release 2, Section 1.1:

“The consensus content was developed using an open source project called SCAP Security Guide. The project’s website is https://fedorahosted.org/scap-security-guide/.

Except for differences in formatting to accommodate the DISA STIG publishing process, the content of the RHEL6 STIG should mirror the SCAP Security Guide content with only minor divergences as updates from multiple sources work through the consensus process”

RHEL 5 STIG:

RHEL 6 STIG:

RHEL 7 STIG:

RHEL 5 STIG:	1,988 DAYS
RHEL 6 STIG:	
RHEL 7 STIG:	

RHEL 5 STIG:	1,988 DAYS
RHEL 6 STIG:	932 DAYS
RHEL 7 STIG:	

RHEL 5 STIG:	1,988 DAYS
RHEL 6 STIG:	932 DAYS
RHEL 7 STIG:	+/- 90 DAYS

TECH + INITIATIVES

Native Tooling, Configuration Compliance, Evolving Remediation Capabilities

TOOLS

vs

CONTENT

OpenSCAP

SCAP ACRONYM: XCCDF

- eXtensible Configuration Checklist Description Format
  - Human(ish) readable, format for configuration <Rule>s
  - <Rule>s selected to form <Profile>s
    - <refine-value>s

SCAP ACRONYM: OVAL

- Open Vulnerability and Assessment Language
  - Specifies how to get information about system configuration
  - Stores it in a structured, well defined format

XCCDF PROFILES

- Shipping as of 16-APR-2014:
  - C2S: Commercial baseline derived from CIS v1.2.0 [1] (go google “Amazon C2S”…)
  - CS2: RHEL6 baseline example for Intelligence Community
  - CSCF: NRO’s Centralized Super Computer Facility (CSCF) Baseline (cross domain controls from CNSSI 1253)
  - STIG: U.S. DoD RHEL6 baseline, produced by DISA FSO

[1] https://benchmarks.cisecurity.org/tools2/linux/CIS_Red_Hat_Enterprise_Linux_6_Benchmark_v1.2.0.pdf

REMEDIATION CAPABILITIES

- Bash first

```
<fix system="urn:xccdf:fix:script:sh">
  yum -y install screen
</fix>
```

REMEDIATION CAPABILITIES

- Bash first

- Soon(ish), puppet

```
<fix-group id="puppet-clip”
  system="urn:xccdf:fix:script:puppet xmlns="http://checklists.nist.gov/xccdf/1.1">

    <fix rule="disable_vsftp">class vsftp</fix>
    <fix rule="package_aide_installed">class aide</fix>

</fix-group>
```

<result>Error</result>

```
<rule-result idref="xccdf_moc.elpmaxe.www_rule_1”
 time="2013-03-22T19:15:11" weight="1.000000">

   <result>error</result>

   <message severity="info">
     Fix execution comleted and returned: 1
   </message>

   <message severity="info">
     Loaded plugins: auto-update-debuginfo, langpacks, presto,
     refresh-packagekit

     You need to be root to perform this command.
   </message>
 </rule-result>
```

<result>Fixed</result>

```
<rule-result idref="xccdf_moc.elpmaxe.www_rule_1” time="2014-03-22T19:16:03" weight="1.000000">
  <result>fixed</result>
  <message severity="info">Fix execution completed and returned: 0</message>
  <message severity="info">
    ….
    Remove 1 Package
    Installed size: 53 k
    Downloading Packages:
    Running Transaction Check
    Running Transaction Test
    Transaction Test Succeeded
    Running Transaction
      Erasing     :  1:telnet-server-0.17-51.fc16.x86_64   1/1
      Verifying   :  1:telnet-server-0.17-51.fc16.x86_64   1/1

    Removed:
      telnet-server.x86_64 1:0.17-51.fc16
  </message>
```

REMEDIATION REVIEW

- Bash first
- Soon(ish), puppet
- Reference Šimon Lukašík's blog for a great write-up: http://isimluk.livejournal.com/3573.html
- Thank you Peter Vrabec & Martin Preisler for the work on OpenSCAP!

LIVE DEMO

Patch & vuln. Scanning, configuration baseline scanning, Certification & Accreditation Paperwork Generation

ROADMAP

Gov't Initiatives, SSG Packaging, Future Profiles

Government Initiatives

- Continuous Diagnostics and Mitigations (CDM) http://www.dhs.gov/cdm
- SCAP path forward
- Evaluation + Configuration activities for Certification and Accreditation

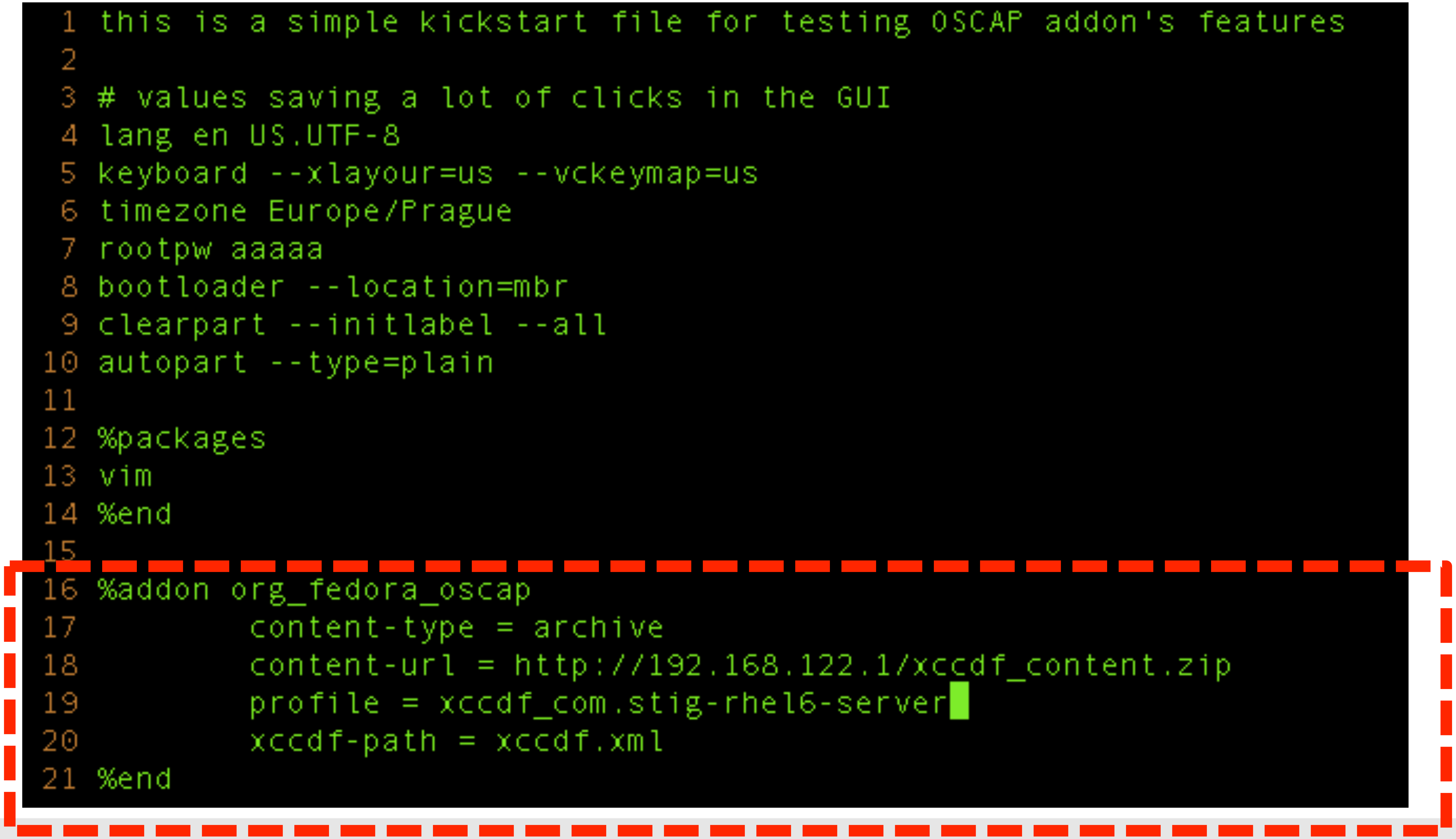
RPM Packaging

- Currently in EPEL, both Fedora and RHEL *(thank you, Jan Lieskovsky!)*
- SSG scheduled to ship in RHEL 6.6
  - https://bugzilla.redhat.com/show_bug.cgi?id=1038655
- RHEL 7 GA

SCAP + Anaconda Integration

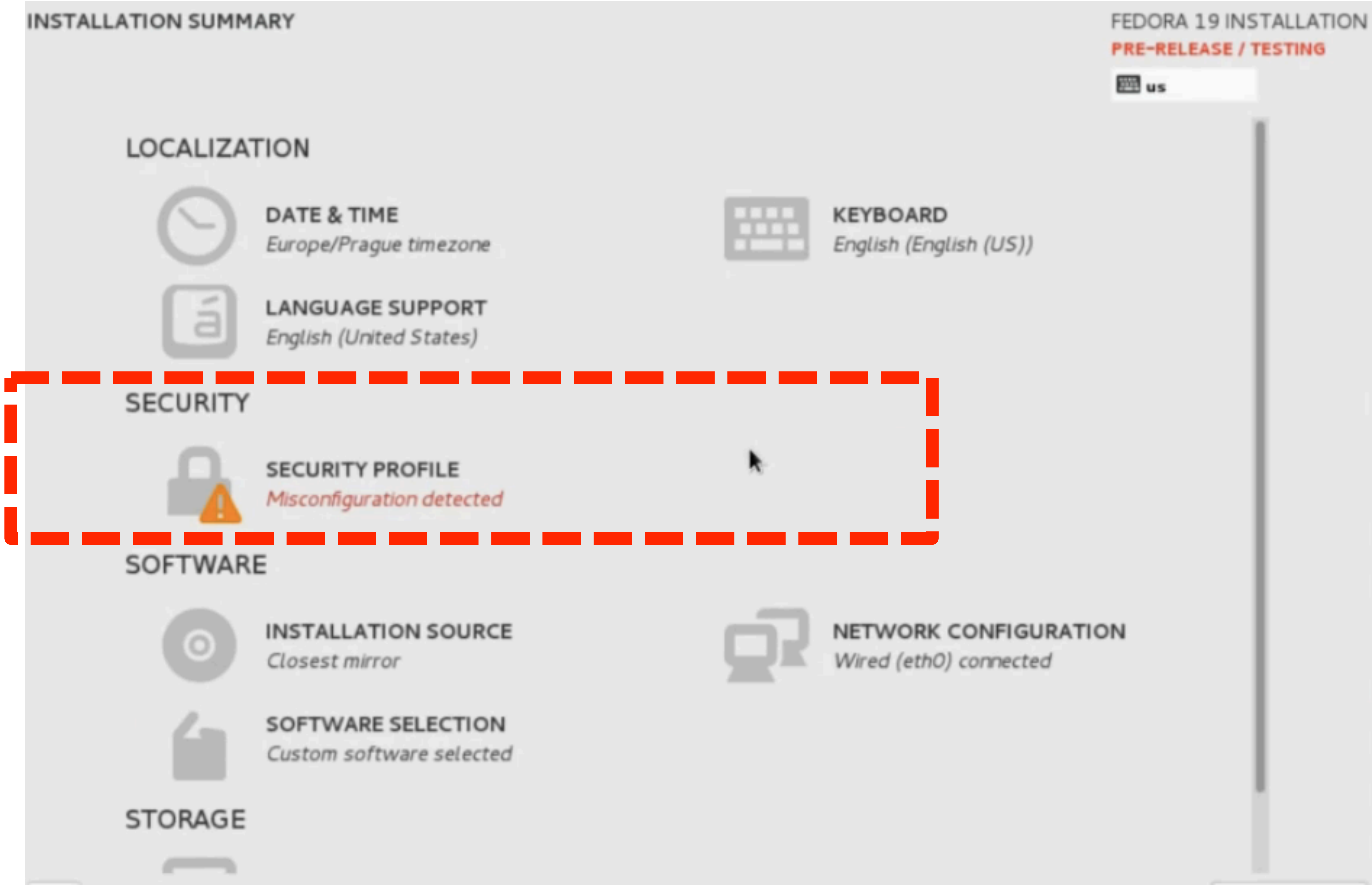
- <fix> elements targeting installation process
- Kickstart support allowing specification of SCAP content
- UI screen(s) that provide ways to set values
- Project started as Vratislav Podzimek's masters thesis
  http://is.muni.cz/th/324874/fi_m/?lang=en (thanks, Vratislav!)
- https://fedorahosted.org/oscap-anaconda-addon/

SCAP + Anaconda Integration (1 / 3)



```
this is a simple kickstart file for testing OSCAP addon's features

# values saving a lot of clicks in the GUI
lang en US.UTF-8
keyboard --xlayour=us --vckeymap=us
timezone Europe/Prague
rootpw aaaaa
bootloader --location=mbr
clearpart --initlabel --all
autopart --type=plain

%packages
vim
%end

%addon org_fedora_oscap
        content-type = archive
        content-url = http://192.168.122.1/xccdf_content.zip
        profile = xccdf_com.stig-rhel6-server
        xccdf-path = xccdf.xml
%end
```

SCAP + Anaconda Integration (2 / 3)



INSTALLATION SUMMARY

FEDORA 19 INSTALLATION

PRE-RELEASE / TESTING

us

LOCALIZATION

DATE & TIME
Europe/Prague timezone

KEYBOARD
English (English (US))

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY PROFILE
Misconfiguration detected

SOFTWARE

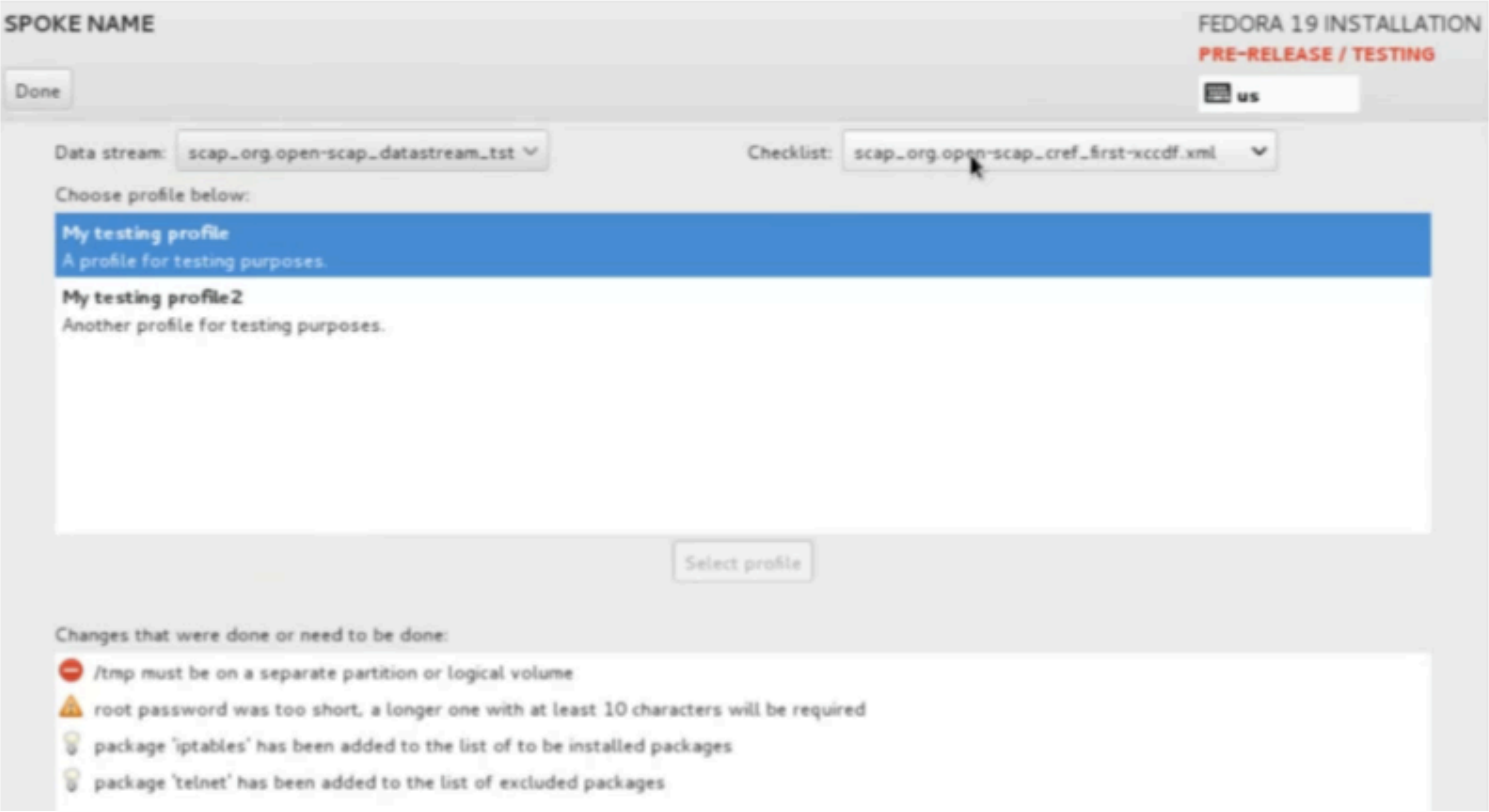
INSTALLATION SOURCE
Closest mirror

NETWORK CONFIGURATION
Wired (eth0) connected

SOFTWARE SELECTION
Custom software selected

STORAGE

SCAP + Anaconda Integration (3 / 3)



Data stream: scap_org.open-scap_datastream_tst

Checklist: scap_org.open-scap_cref_first-xccdf.xml

Choose profile below:

My testing profile
A profile for testing purposes.

My testing profile2
Another profile for testing purposes.

Changes that were done or need to be done:

- /tmp must be on a separate partition or logical volume
- root password was too short, a longer one with at least 10 characters will be required
- package 'iptables' has been added to the list of to be installed packages
- package 'telnet' has been added to the list of excluded packages

SCAP Workbench

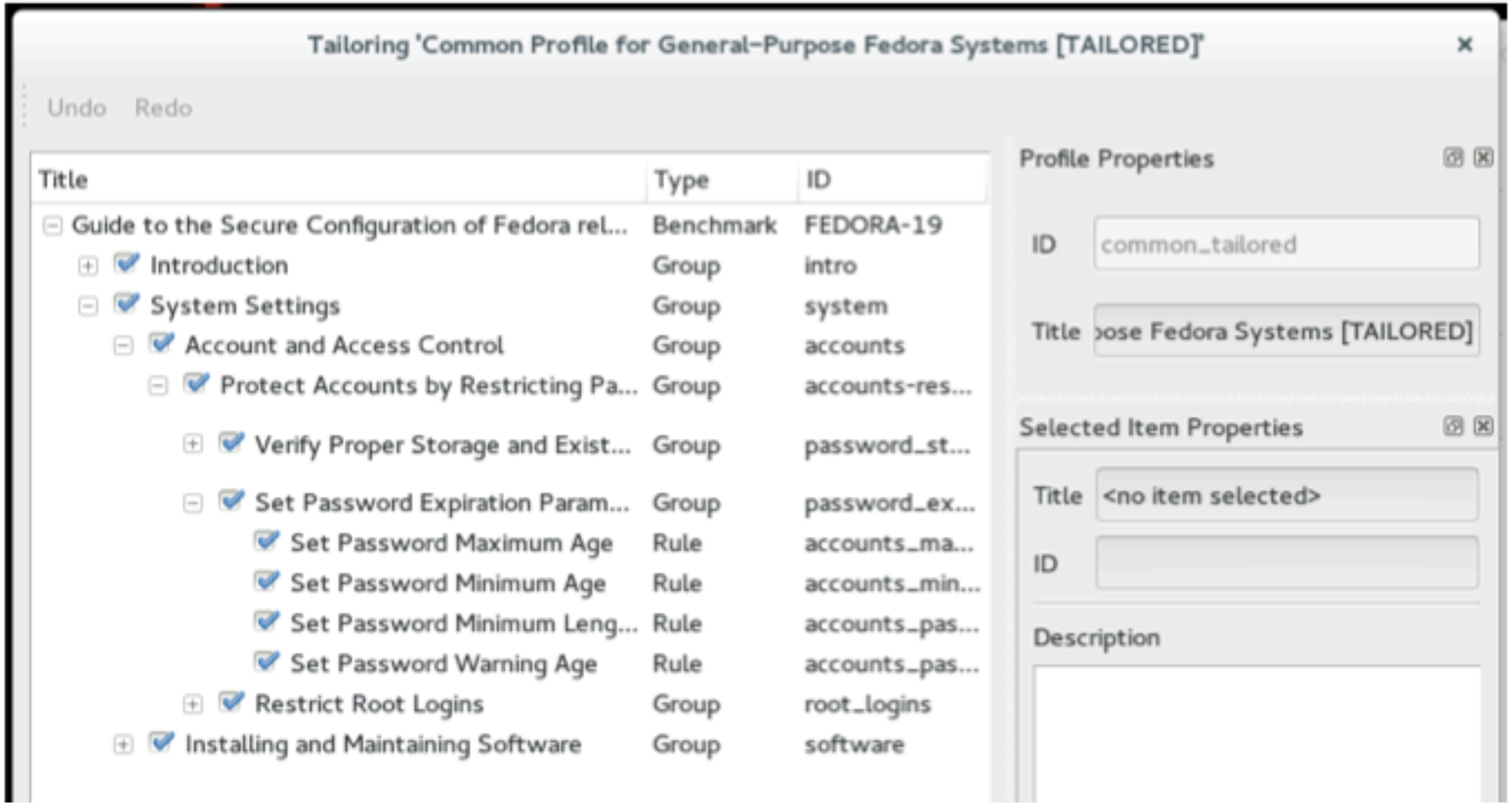
GUI tool that serves as an SCAP scanner and provides tailoring functionality.

Primary Goals:

- Lower the initial barrier of using SCAP.
- Great for hand-tuning content before enterprise deployment (e.g. via spacewalk/RHN Satellite)

https://fedorahosted.org/scap-workbench/

SCAP Workbench (1/2)



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

Undo Redo

Title	Type	ID
⊟ Guide to the Secure Configuration of Fedora rel...	Benchmark	FEDORA-19
⊞ ☑ Introduction	Group	intro
⊟ ☑ System Settings	Group	system
⊟ ☑ Account and Access Control	Group	accounts
⊟ ☑ Protect Accounts by Restricting Pa...	Group	accounts-res...
⊞ ☑ Verify Proper Storage and Exist...	Group	password_st...
⊟ ☑ Set Password Expiration Param...	Group	password_ex...
☑ Set Password Maximum Age	Rule	accounts_ma...
☑ Set Password Minimum Age	Rule	accounts_min...
☑ Set Password Minimum Leng...	Rule	accounts_pas...
☑ Set Password Warning Age	Rule	accounts_pas...
⊞ ☑ Restrict Root Logins	Group	root_logins
⊞ ☑ Installing and Maintaining Software	Group	software

Profile Properties

ID: common_tailored

Title: ose Fedora Systems [TAILORED]

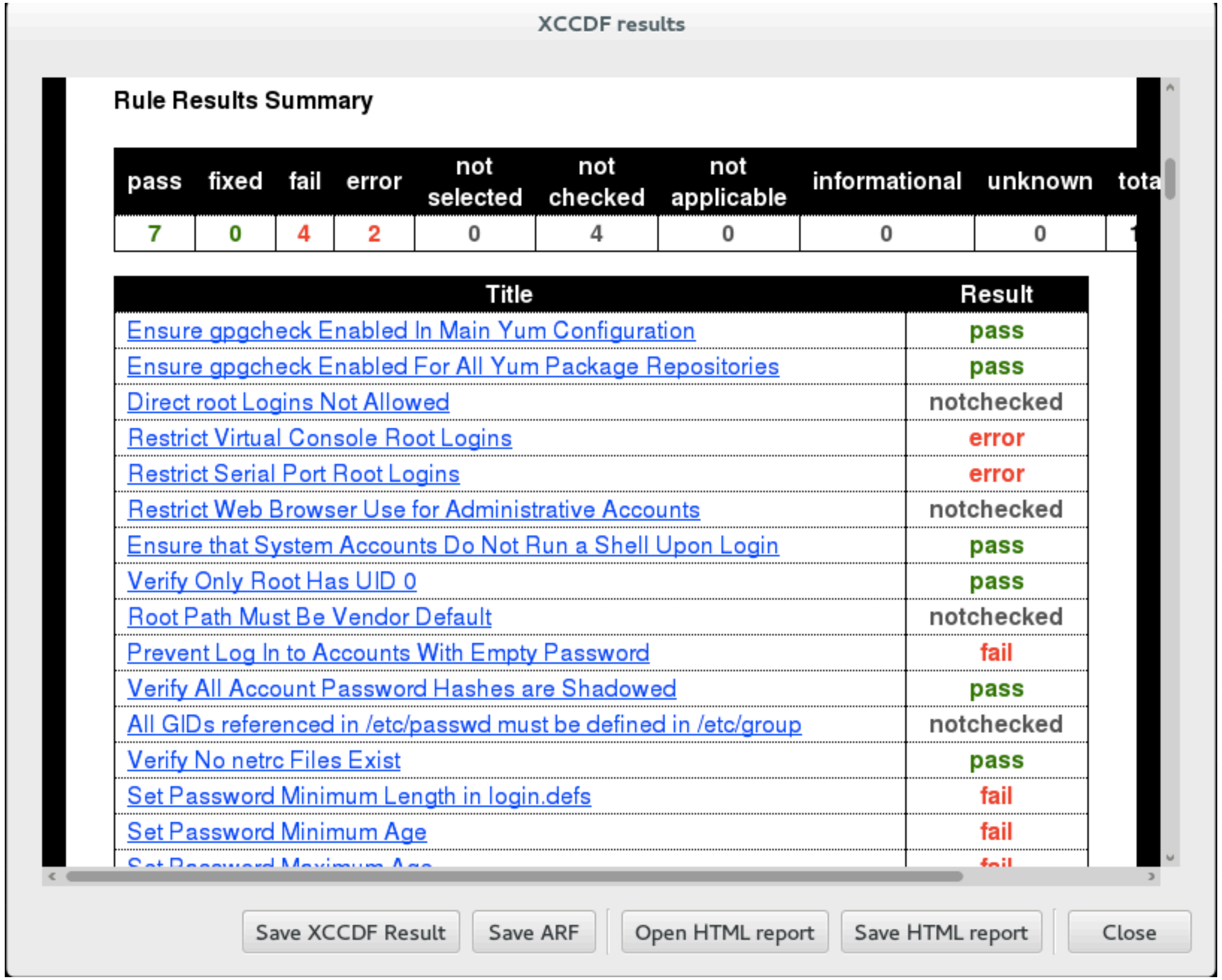
Selected Item Properties

Title: <no item selected>

ID:

Description

SCAP Workbench (2 / 2)



Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	tota
7	0	4	2	0	4	0	0	0	1

Title	Result
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	pass
Direct root Logins Not Allowed	notchecked
Restrict Virtual Console Root Logins	error
Restrict Serial Port Root Logins	error
Restrict Web Browser Use for Administrative Accounts	notchecked
Ensure that System Accounts Do Not Run a Shell Upon Login	pass
Verify Only Root Has UID 0	pass
Root Path Must Be Vendor Default	notchecked
Prevent Log In to Accounts With Empty Password	fail
Verify All Account Password Hashes are Shadowed	pass
All GIDs referenced in /etc/passwd must be defined in /etc/group	notchecked
Verify No netrc Files Exist	pass
Set Password Minimum Length in login.defs	fail
Set Password Minimum Age	fail
Set Password Maximum Age	fail

WE CAN DO MORE WHEN WE WORK TOGETHER

SUPPLEMENTAL

Helpful Links

Helpful Links (to community projects)

SCAP Security Guide:	https://fedorahosted.org/scap-security-guide/
OpenSCAP:	http://open-scap.org/
OSCAP Anaconda:	https://fedorahosted.org/oscap-anaconda-addon/
SCAP Workbench:	https://fedorahosted.org/scap-workbench/

Helpful Links (to government baselines)

- DISA’s Security Technical Implementation Guides (STIGs)
  http://iase.disa.mil/stigs/

- NIST National Checklist Program Repository
  http://web.nvd.nist.gov/view/ncp/repository

- NSA Security Configuration Guides
  http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/

Helpful Links (to communities of interest)

- Red Hat’s Government Security User Group (gov-sec)
  http://www.redhat.com/mailman/listinfo/gov-sec

- Military Open Source Software (Mil-OSS)
  http://mil-oss.org/

Replicating the Demo

- *Assumes RHEL 6 and EPEL already enabled!*
- *Assumes httpd installed, DocumentRoot /var/www/html/*
- *My IP was 10.211.55.3. Change as appropriate.*
- *This is meant to replicate the demo, not fully explain it.*
  Come to Summit next year!

Step 1: Install

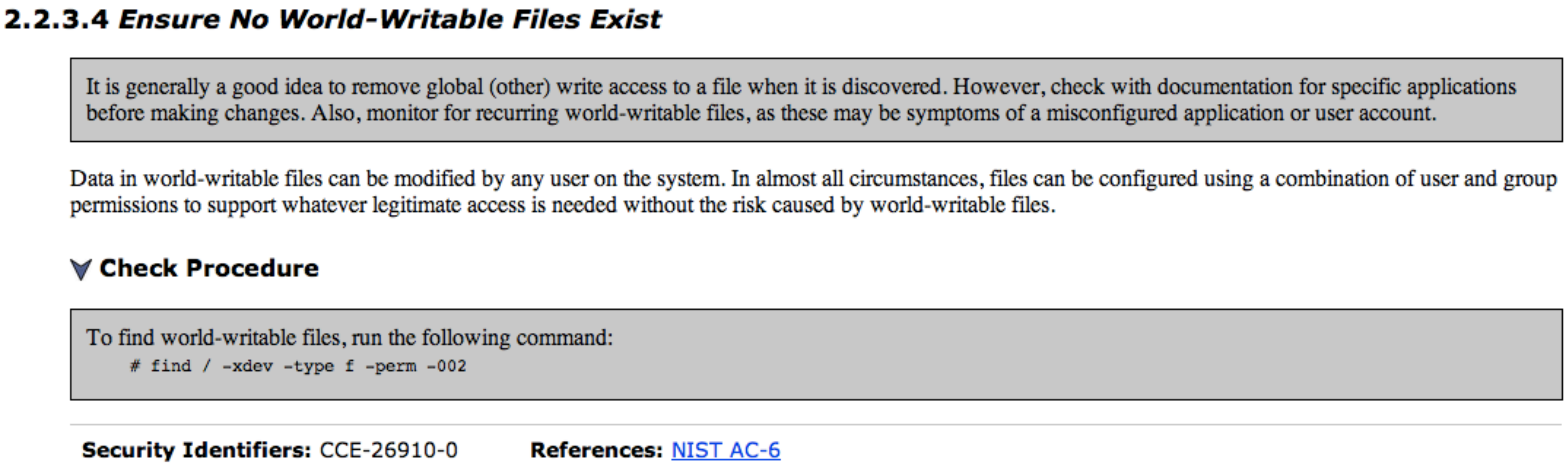
```
$ yum install scap-security-guide

$ rpm –ql scap-security-guide
. . .
/usr/share/doc/scap-security-guide-0.1/rhel6-guide.html
...
/usr/share/man/en/man8/scap-security-guide.8.gz
...
/usr/share/xml/scap/ssg/content
...
/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
```

Step 2: Review Prose Guide

```
$ cp /usr/share/doc/scap-security-guide-0.1/*.html /var/www/html
```

```
$ firefox http://10.211.55.3/rhel6-guide.html
```

- Review “Check Procedure,” “Security Identifiers,” “References”



2.2.3.4 *Ensure No World-Writable Files Exist*

It is generally a good idea to remove global (other) write access to a file when it is discovered. However, check with documentation for specific applications before making changes. Also, monitor for recurring world-writable files, as these may be symptoms of a misconfigured application or user account.

Data in world-writable files can be modified by any user on the system. In almost all circumstances, files can be configured using a combination of user and group permissions to support whatever legitimate access is needed without the risk caused by world-writable files.

Check Procedure

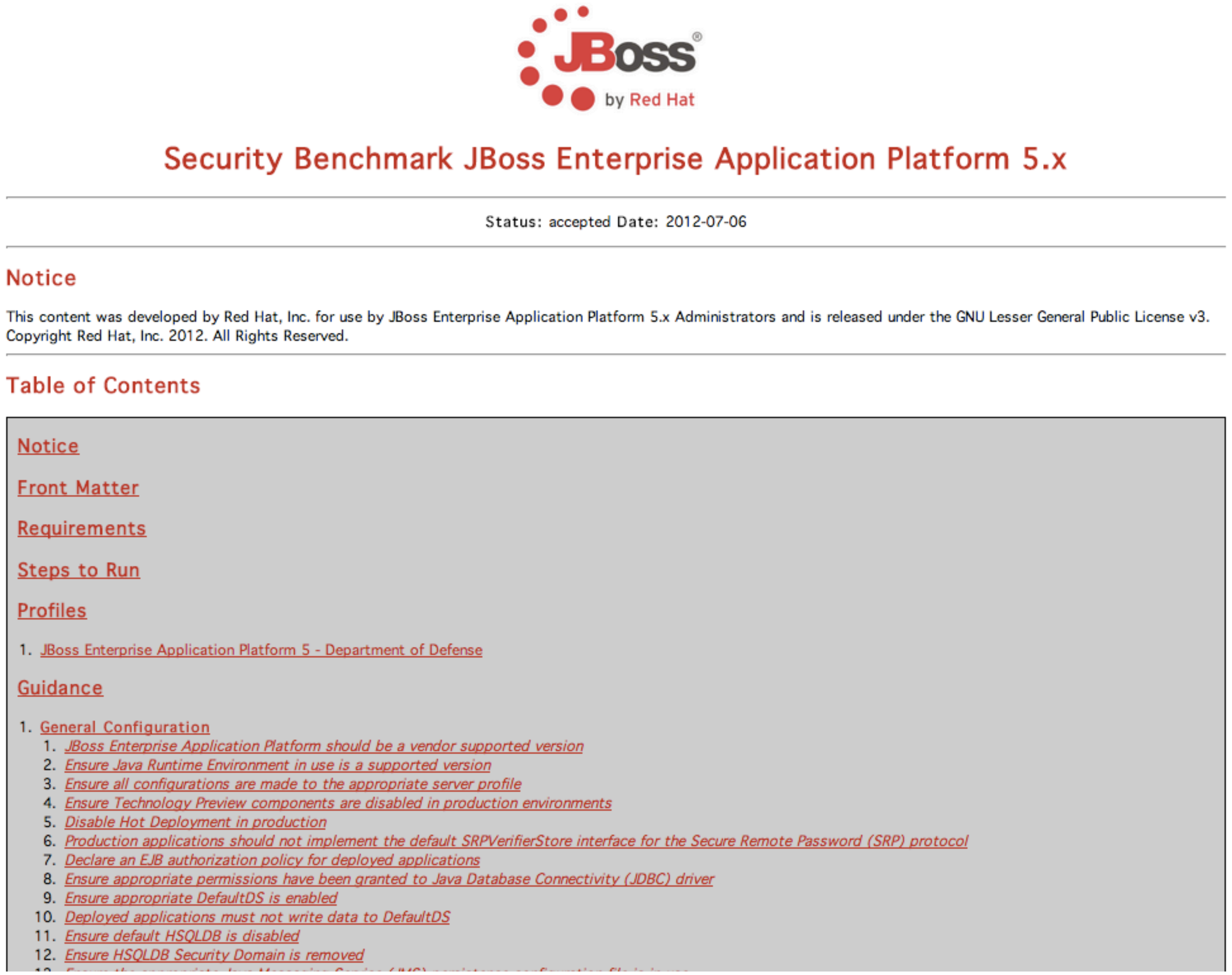
To find world-writable files, run the following command:

```
    # find / -xdev -type f -perm -002
```

Security Identifiers: CCE-26910-0 **References:** NIST AC-6

Step 3: JBoss, too!

```
$ firefox http://10.211.55.3/JBossEAP5_Guide.html
```



Security Benchmark JBoss Enterprise Application Platform 5.x

Status: accepted **Date:** 2012-07-06

Notice

Table of Contents

Step 4: XCCDF vs DATASTREAMS

```
$ grep "<Profile" /usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
  <Profile id="xccdf_org.ssgproject.content_profile_CS2”>
  <Profile id="xccdf_org.ssgproject.content_profile_stig-rhel6-server-upstream">
```

```
$ grep "<Profile" /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
  <Profile id="CS2”>
  <Profile id="stig-rhel6-server-upstream”>
```

Step 5: Run a scan!

```
$ sudo oscap xccdf eval --profile C2S \
  --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml \
  --report /var/www/html/summit-report.html \
  --results /var/www/html/summit-results.xml \
  /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

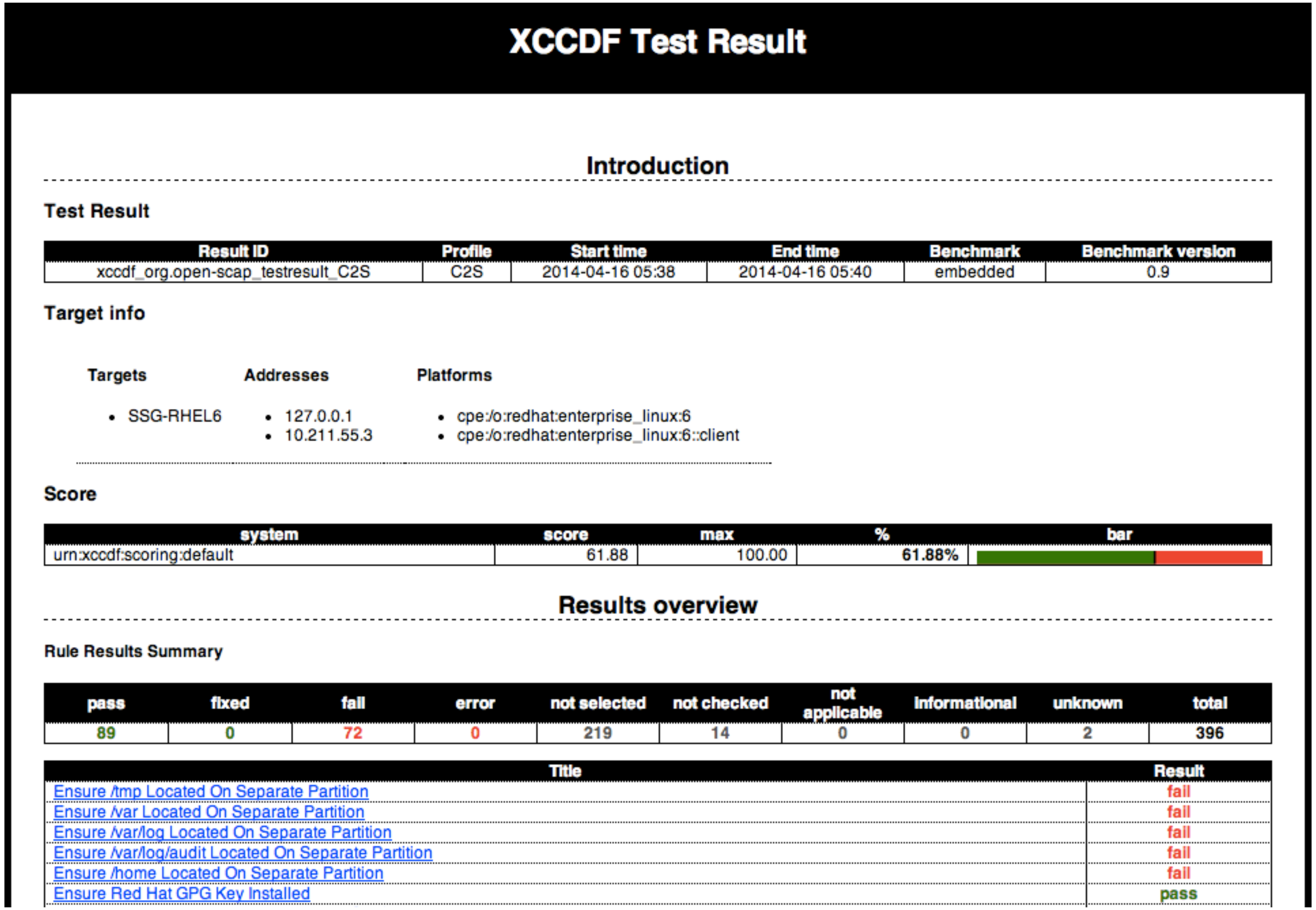
Console Output:

- Pass
- Fail
- “notchecked”: (a) not applicable; (b) no OVAL associated
  … and unclear which reason!

Step 6: HTML Results

```
$ firefox /var/www/html/summit-report.html
```

Step 6: HTML Results



XCCDF Test Result

Introduction

Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_C2S	C2S	2014-04-16 05:38	2014-04-16 05:40	embedded	0.9

Target info

Targets	Addresses	Platforms
SSG-RHEL6	127.0.0.1 10.211.55.3	cpe:/o:redhat:enterprise_linux:6 cpe:/o:redhat:enterprise_linux:6::client

Score

system	score	max	%	bar
urn:xccdf:scoring:default	61.88	100.00	61.88%	🟩🟥

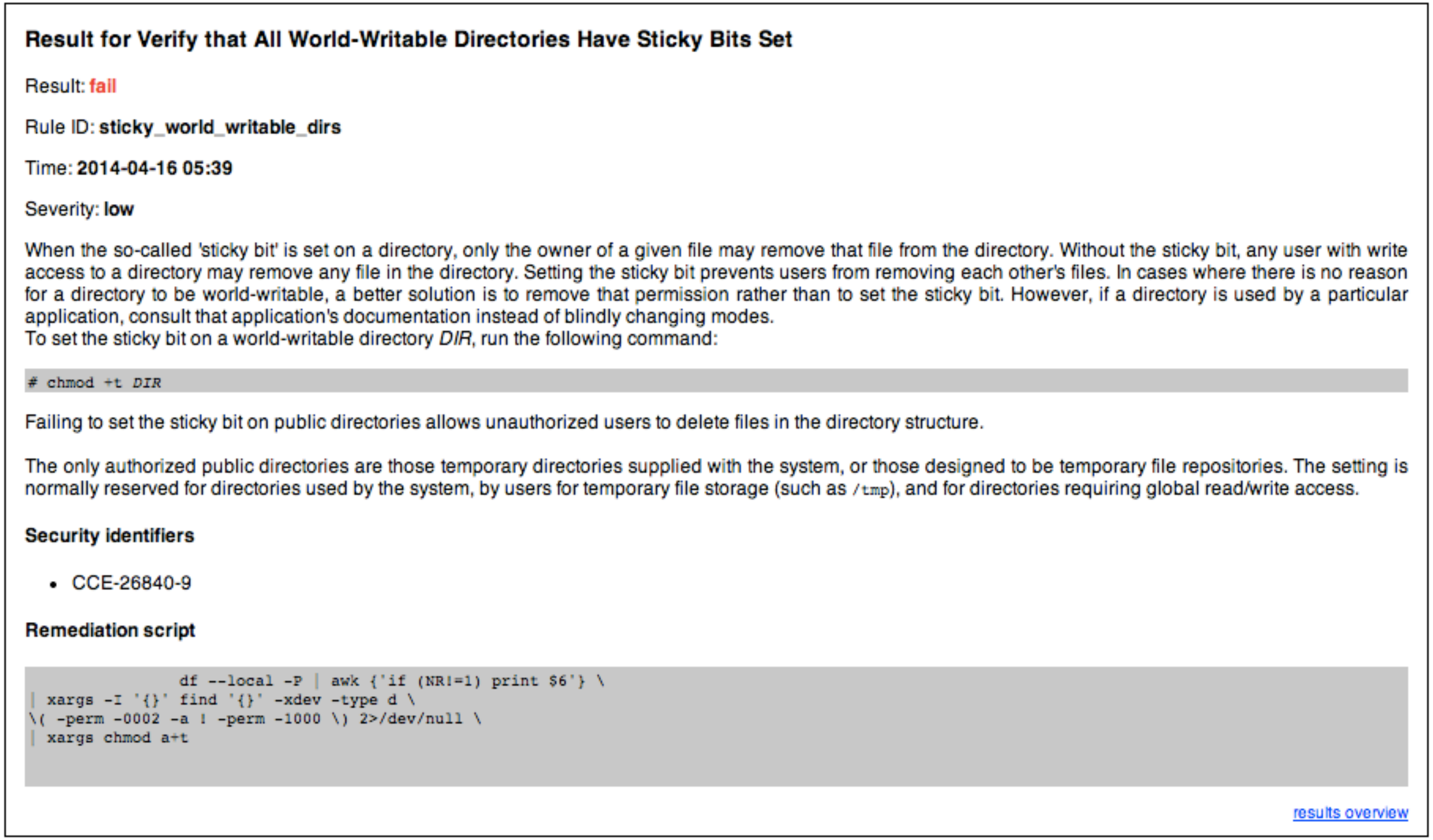
Results overview

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
89	0	72	0	219	14	0	0	2	396

Title	Result
Ensure /tmp Located On Separate Partition	fail
Ensure /var Located On Separate Partition	fail
Ensure /var/log Located On Separate Partition	fail
Ensure /var/log/audit Located On Separate Partition	fail
Ensure /home Located On Separate Partition	fail
Ensure Red Hat GPG Key Installed	pass

Step 6: HTML Results



Result for Verify that All World-Writable Directories Have Sticky Bits Set

Result: **fail**

Rule ID: **sticky_world_writable_dirs**

Time: **2014-04-16 05:39**

Severity: **low**

When the so-called 'sticky bit' is set on a directory, only the owner of a given file may remove that file from the directory. Without the sticky bit, any user with write access to a directory may remove any file in the directory. Setting the sticky bit prevents users from removing each other's files. In cases where there is no reason for a directory to be world-writable, a better solution is to remove that permission rather than to set the sticky bit. However, if a directory is used by a particular application, consult that application's documentation instead of blindly changing modes.
To set the sticky bit on a world-writable directory *DIR*, run the following command:

```
# chmod +t DIR
```

Failing to set the sticky bit on public directories allows unauthorized users to delete files in the directory structure.

The only authorized public directories are those temporary directories supplied with the system, or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system, by users for temporary file storage (such as `/tmp`), and for directories requiring global read/write access.

Security identifiers

- CCE-26840-9

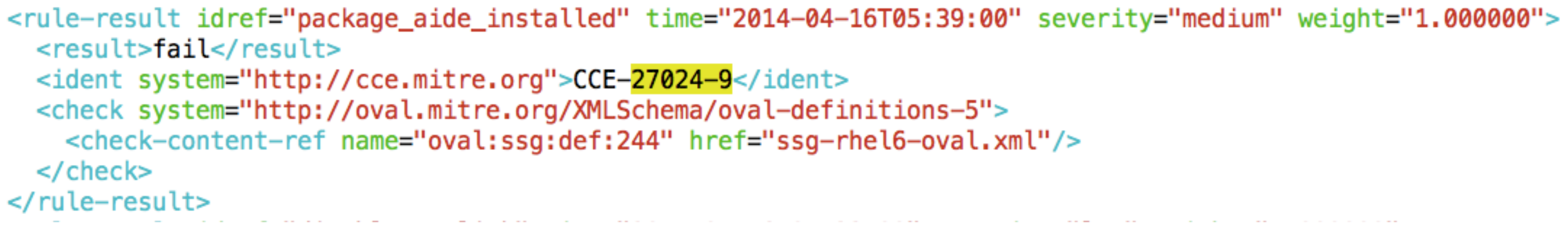
Remediation script

```
                df --local -P | awk {'if (NR!=1) print $6'} \
| xargs -I '{}' find '{}' -xdev -type d \
\( -perm -0002 -a ! -perm -1000 \) 2>/dev/null \
| xargs chmod a+t
```

Step 7: XML Results

```
$ firefox /var/www/html/summit-results.xml
```

```
/CCE-27024-9
```

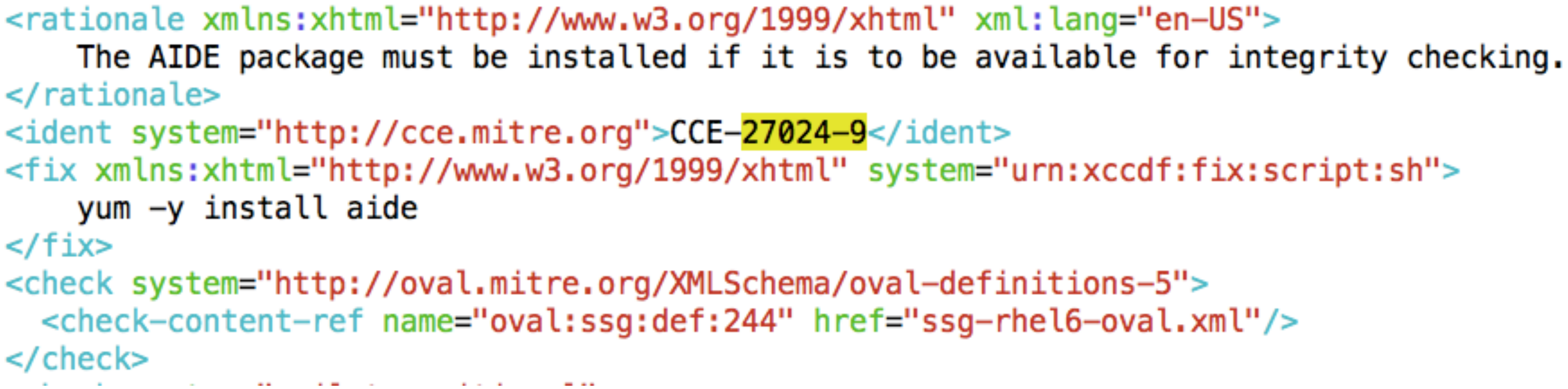


```
<rule-result idref="package_aide_installed" time="2014-04-16T05:39:00" severity="medium" weight="1.000000">
  <result>fail</result>
  <ident system="http://cce.mitre.org">CCE-27024-9</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
  </check>
</rule-result>
```

Step 8: Remediation

/CCE-27024-9 (← type that again)

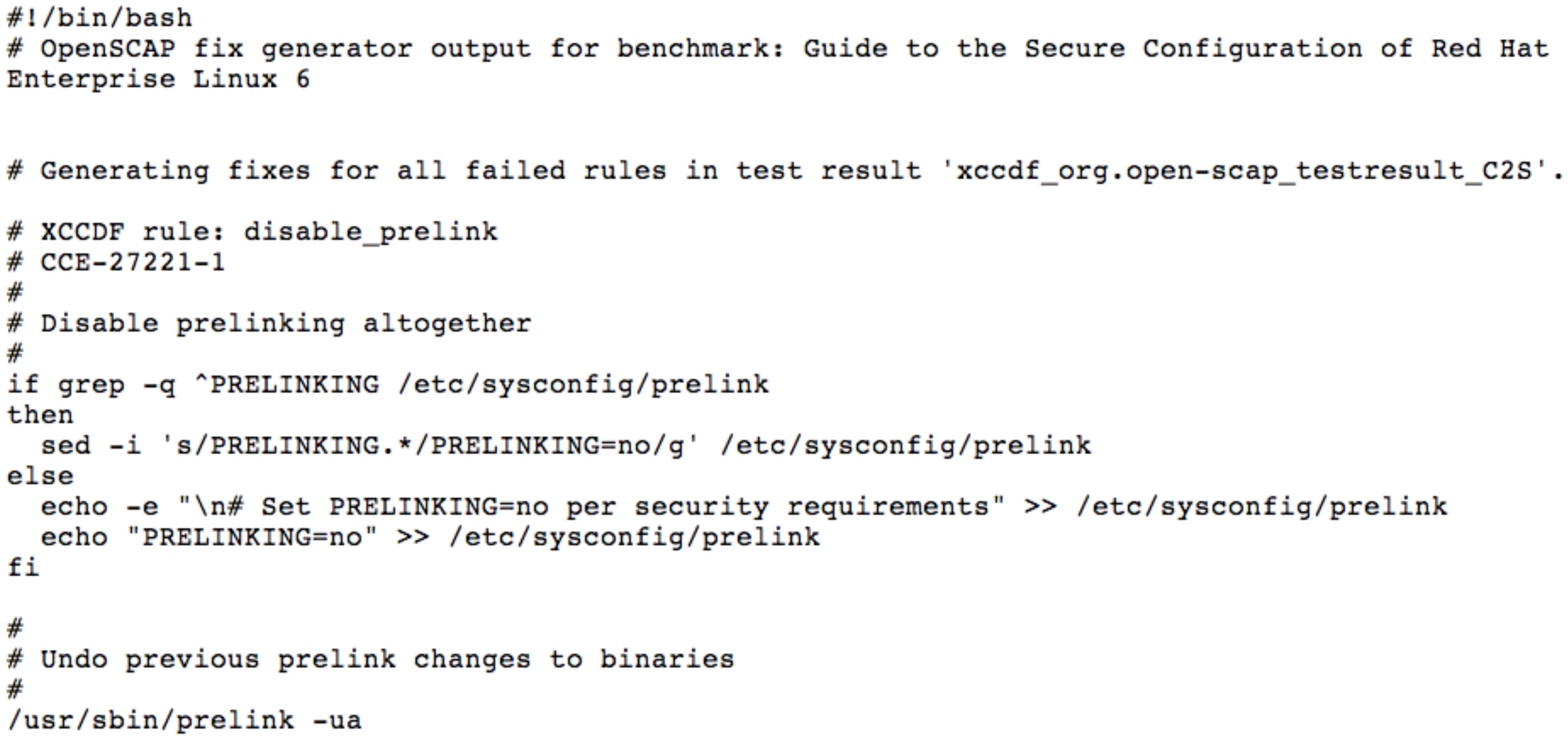
note the <fix> tag!



```
<rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
    The AIDE package must be installed if it is to be available for integrity checking.
</rationale>
<ident system="http://cce.mitre.org">CCE-27024-9</ident>
<fix xmlns:xhtml="http://www.w3.org/1999/xhtml" system="urn:xccdf:fix:script:sh">
    yum -y install aide
</fix>
<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
</check>
```

Step 8: Remediation

```
$ oscap xccdf generate fix --result-id xccdf_org.open-scap_testresult_C2S \
  /var/www/html/summit-results.xml \
  > /var/www/html/summit-script.sh.txt
```



```
#!/bin/bash
# OpenSCAP fix generator output for benchmark: Guide to the Secure Configuration of Red Hat
Enterprise Linux 6


# Generating fixes for all failed rules in test result 'xccdf_org.open-scap_testresult_C2S'.

# XCCDF rule: disable_prelink
# CCE-27221-1
#
# Disable prelinking altogether
#
if grep -q ^PRELINKING /etc/sysconfig/prelink
then
  sed -i 's/PRELINKING.*/PRELINKING=no/g' /etc/sysconfig/prelink
else
  echo -e "\n# Set PRELINKING=no per security requirements" >> /etc/sysconfig/prelink
  echo "PRELINKING=no" >> /etc/sysconfig/prelink
fi

#
# Undo previous prelink changes to binaries
#
/usr/sbin/prelink -ua
```