DEVNATION FEDERAL

June 8th, 2017 | Washington D.C.

Security Compliance for modern infrastructures with OpenSCAP

Martin Preisler

Software Engineer at Red Hat, Inc.

mpreisle@redhat.com

SECURITY COMPLIANCE

- configuration
- hardening

- is root login over ssh forbidden?
- is SELinux enabled and enforcing?
- are we using strict password policy?
- are obsolete / insecure services disabled?
- ...?

SCAP

- Security Content Automation Protocol
- NIST standard
- a set of data formats
  - XCCDF
  - OVAL
  - CPE
  - CVE
  - CCE

OpenSCAP

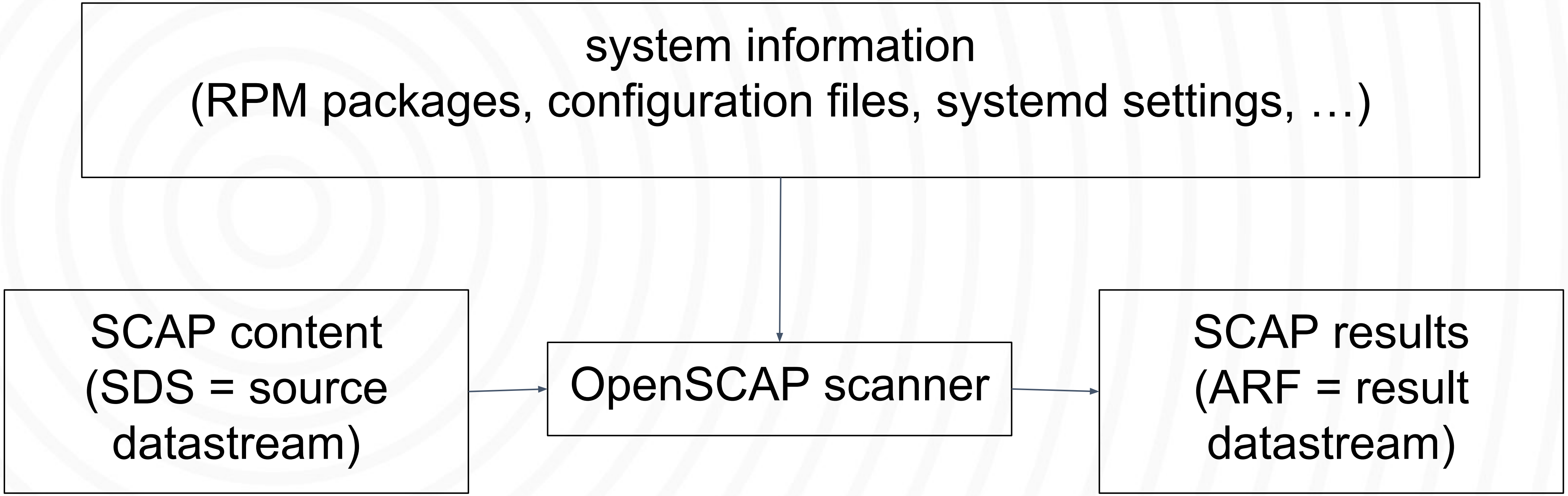
- SCAP 1.2 implementation
- certified by NIST since 2014
- library and a command-line interface
- included in Red Hat Enterprise Linux base channel

OpenSCAP
BASE

SCAP Workbench

- GUI frontend for OpenSCAP
- scan local machines
- scan remove machines
- included in Red Hat Enterprise Linux base channel
- also available for Windows and MacOS X

SCANNING A SINGLE MACHINE



system information
(RPM packages, configuration files, systemd settings, …)

SCAP content
(SDS = source datastream)

OpenSCAP scanner

SCAP results
(ARF = result datastream)

SCAP SECURITY GUIDE

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

SCAP
SECURITY GUIDE

SCANNING A SINGLE MACHINE

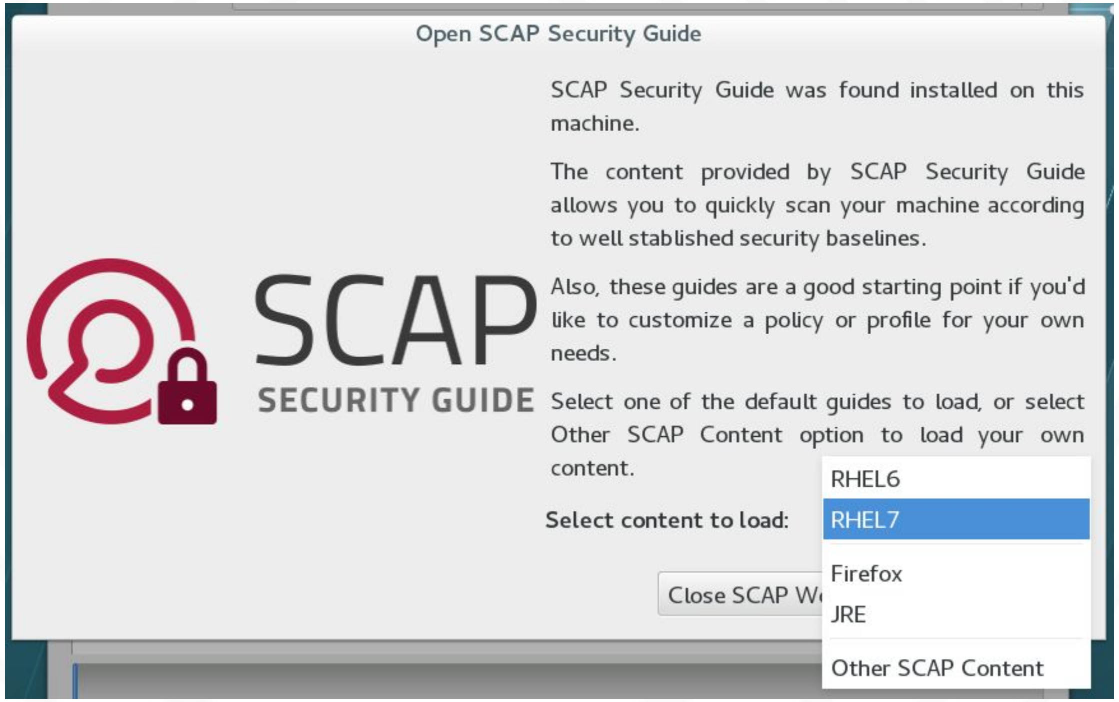
- We will need the following to perform a USGCB scan:
  - Red Hat Enterprise Linux 7.3
  - OpenSCAP and SCAP Workbench
  - USGCB profile from SCAP Security Guide

INSTALL THE NECESSARY TOOLS

(assuming Red Hat Enterprise Linux 7.3)

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

SCAP WORKBENCH 1/3



Open SCAP Security Guide

SCAP Security Guide was found installed on this machine.

The content provided by SCAP Security Guide allows you to quickly scan your machine according to well stablished security baselines.

Also, these guides are a good starting point if you'd like to customize a policy or profile for your own needs.

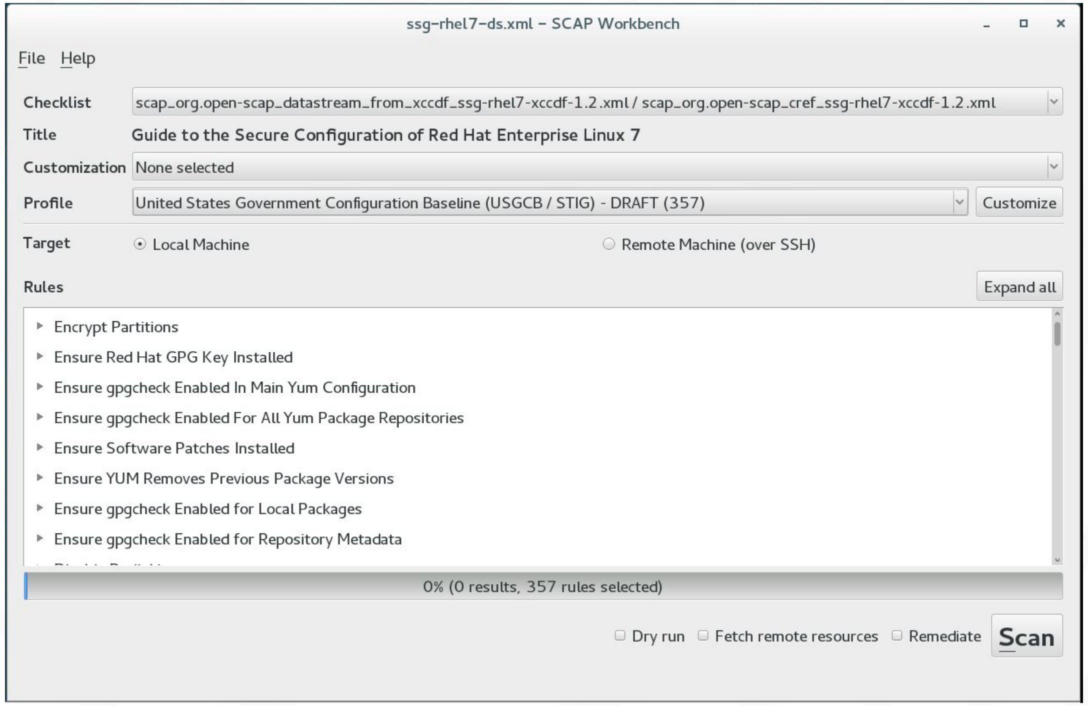
Select one of the default guides to load, or select Other SCAP Content option to load your own content.

Select content to load: RHEL7

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

Let’s select RHEL7.

SCAP WORKBENCH 2/3



Checklist: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml / scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml

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

Customization: None selected

Profile: United States Government Configuration Baseline (USGCB / STIG) - DRAFT (357)

Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

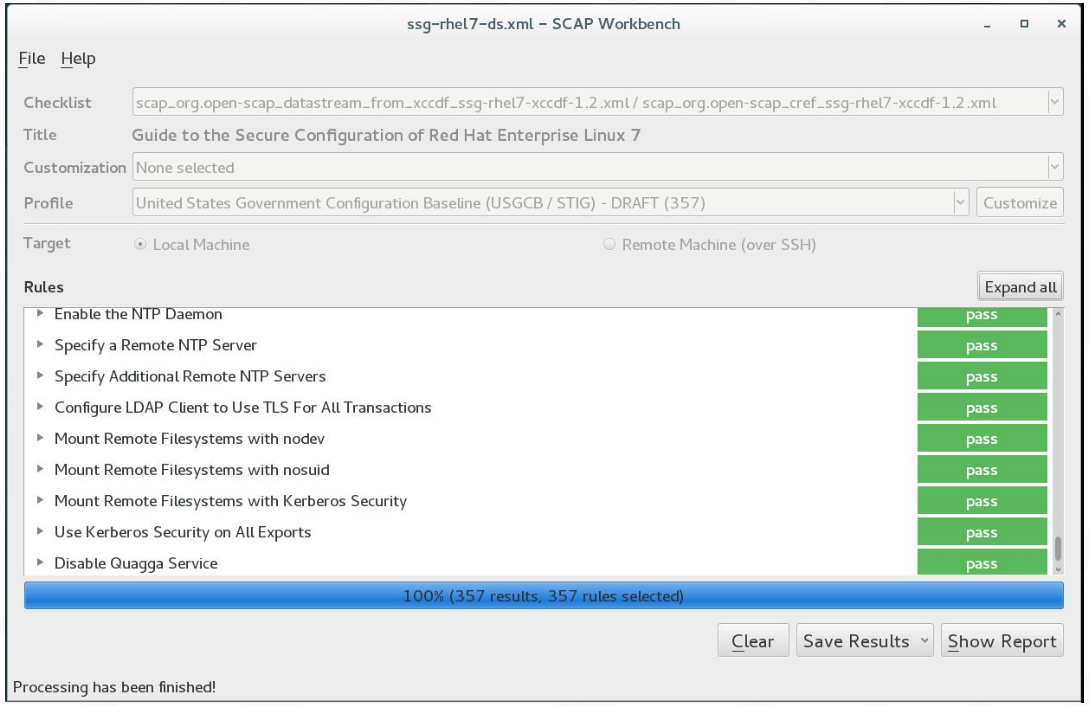
- Encrypt Partitions
- Ensure Red Hat GPG Key Installed
- Ensure gpgcheck Enabled In Main Yum Configuration
- Ensure gpgcheck Enabled For All Yum Package Repositories
- Ensure Software Patches Installed
- Ensure YUM Removes Previous Package Versions
- Ensure gpgcheck Enabled for Local Packages
- Ensure gpgcheck Enabled for Repository Metadata

0% (0 results, 357 rules selected)

□ Dry run □ Fetch remote resources □ Remediate **Scan**

1. select the USGCB profile
2. keep local machine selected
3. click Scan

SCAP WORKBENCH 3/3



Checklist: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml / scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml

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

Customization: None selected

Profile: United States Government Configuration Baseline (USGCB / STIG) - DRAFT (357)

Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

Enable the NTP Daemon	pass
Specify a Remote NTP Server	pass
Specify Additional Remote NTP Servers	pass
Configure LDAP Client to Use TLS For All Transactions	pass
Mount Remote Filesystems with nodev	pass
Mount Remote Filesystems with nosuid	pass
Mount Remote Filesystems with Kerberos Security	pass
Use Kerberos Security on All Exports	pass
Disable Quagga Service	pass

100% (357 results, 357 rules selected)

Processing has been finished!

1. select the USGCB profile
2. keep local machine selected
3. click Scan

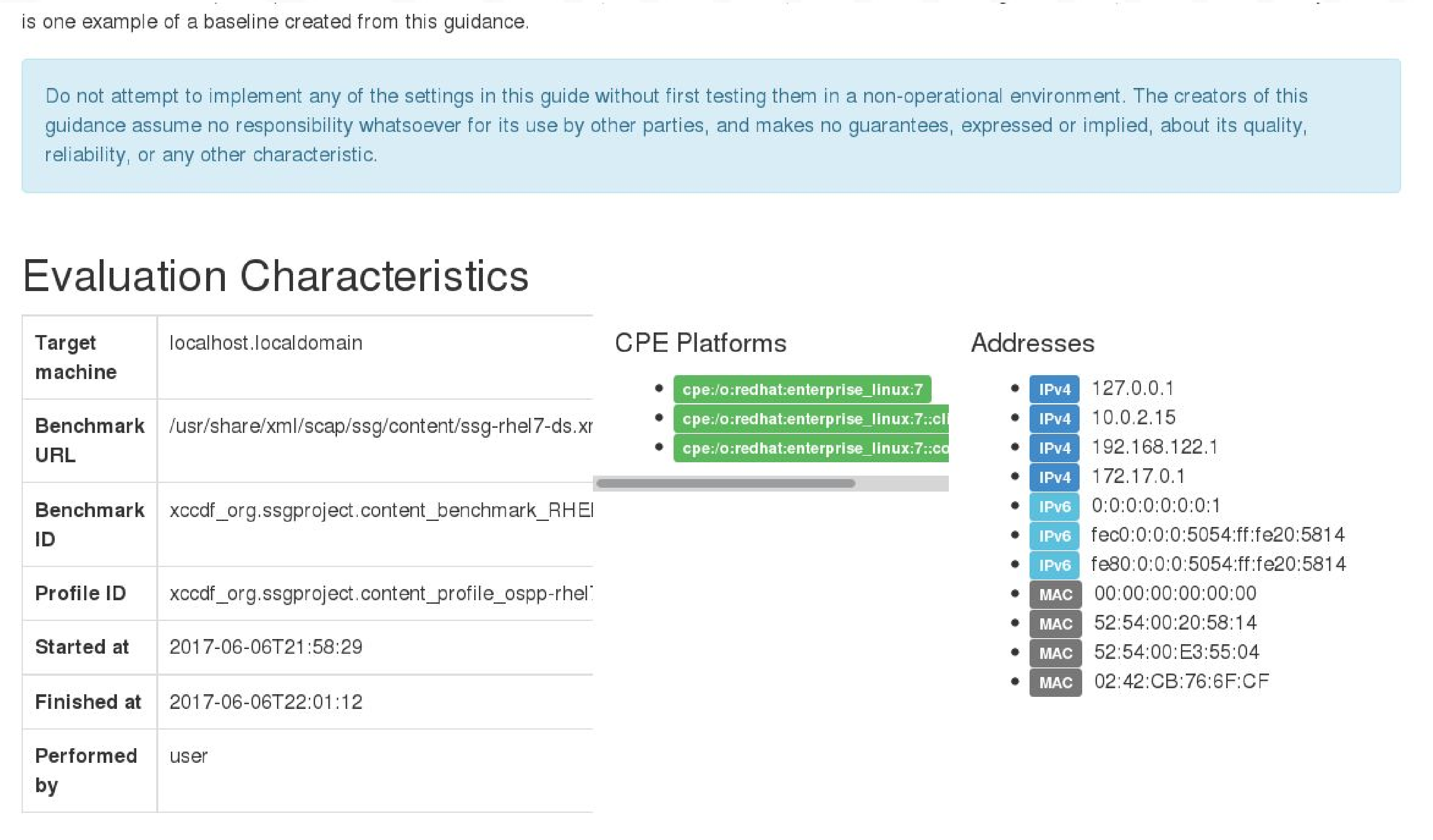
RESULTS AND REPORT

- Result formats
  - XCCDF results, OVAL results
  - ARF results (recommended!)
- HTML report
  - generated from results
  - human readable and interactive
  - allows filtering, sorting, grouping

COMMAND-LINE

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

HTML REPORT 1/5



is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Target machine	localhost.localdomain
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xr
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEl
Profile ID	xccdf_org.ssgproject.content_profile_ospp-rhel
Started at	2017-06-06T21:58:29
Finished at	2017-06-06T22:01:12
Performed by	user

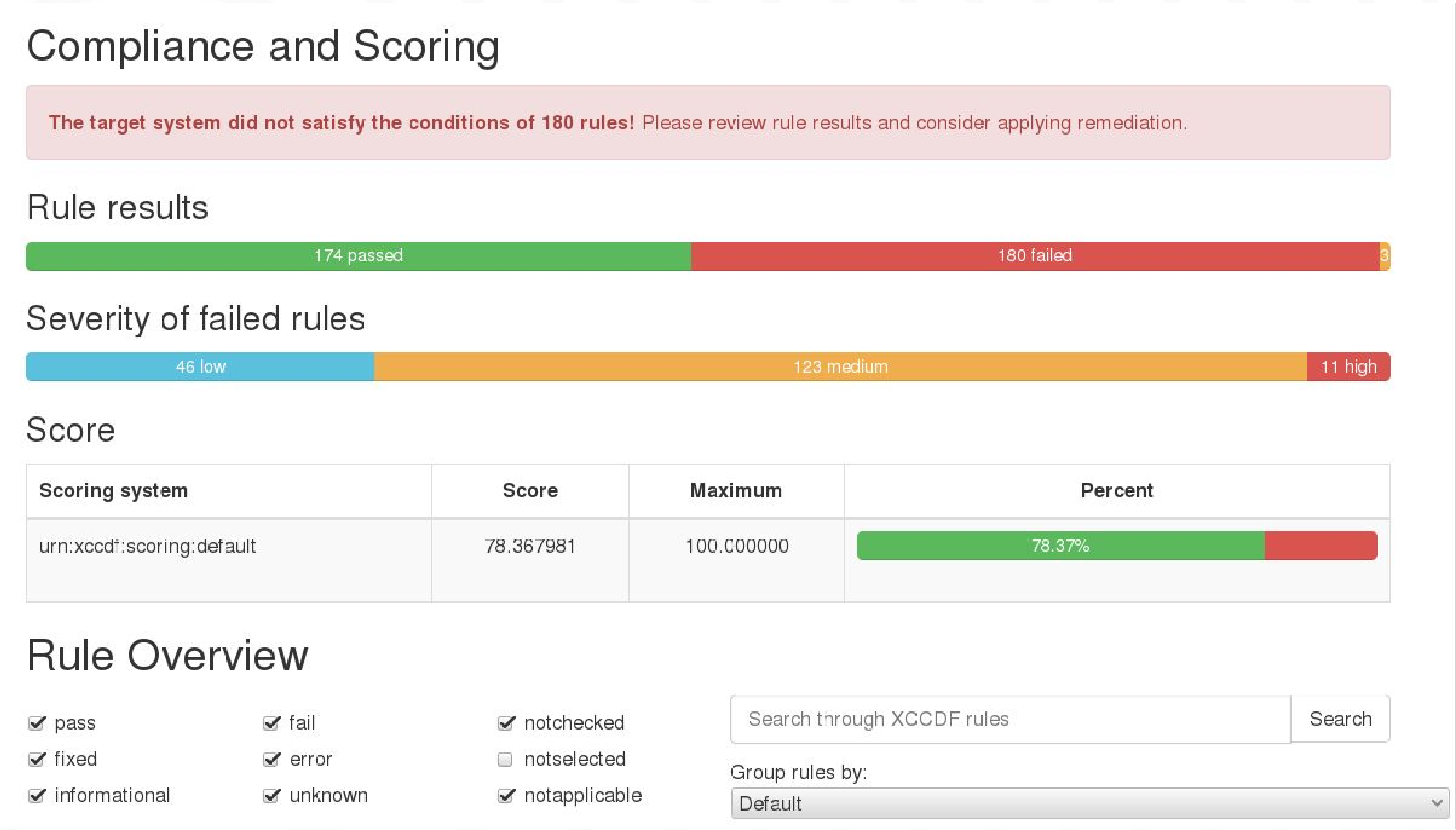
CPE Platforms

- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::cl
- cpe:/o:redhat:enterprise_linux:7::co

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv4 192.168.122.1
- IPv4 172.17.0.1
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fec0:0:0:0:5054:ff:fe20:5814
- IPv6 fe80:0:0:0:5054:ff:fe20:5814
- MAC 00:00:00:00:00:00
- MAC 52:54:00:20:58:14
- MAC 52:54:00:E3:55:04
- MAC 02:42:CB:76:6F:CF

HTML REPORT 2/5



Compliance and Scoring

The target system did not satisfy the conditions of 180 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	78.367981	100.000000	78.37%

Rule Overview

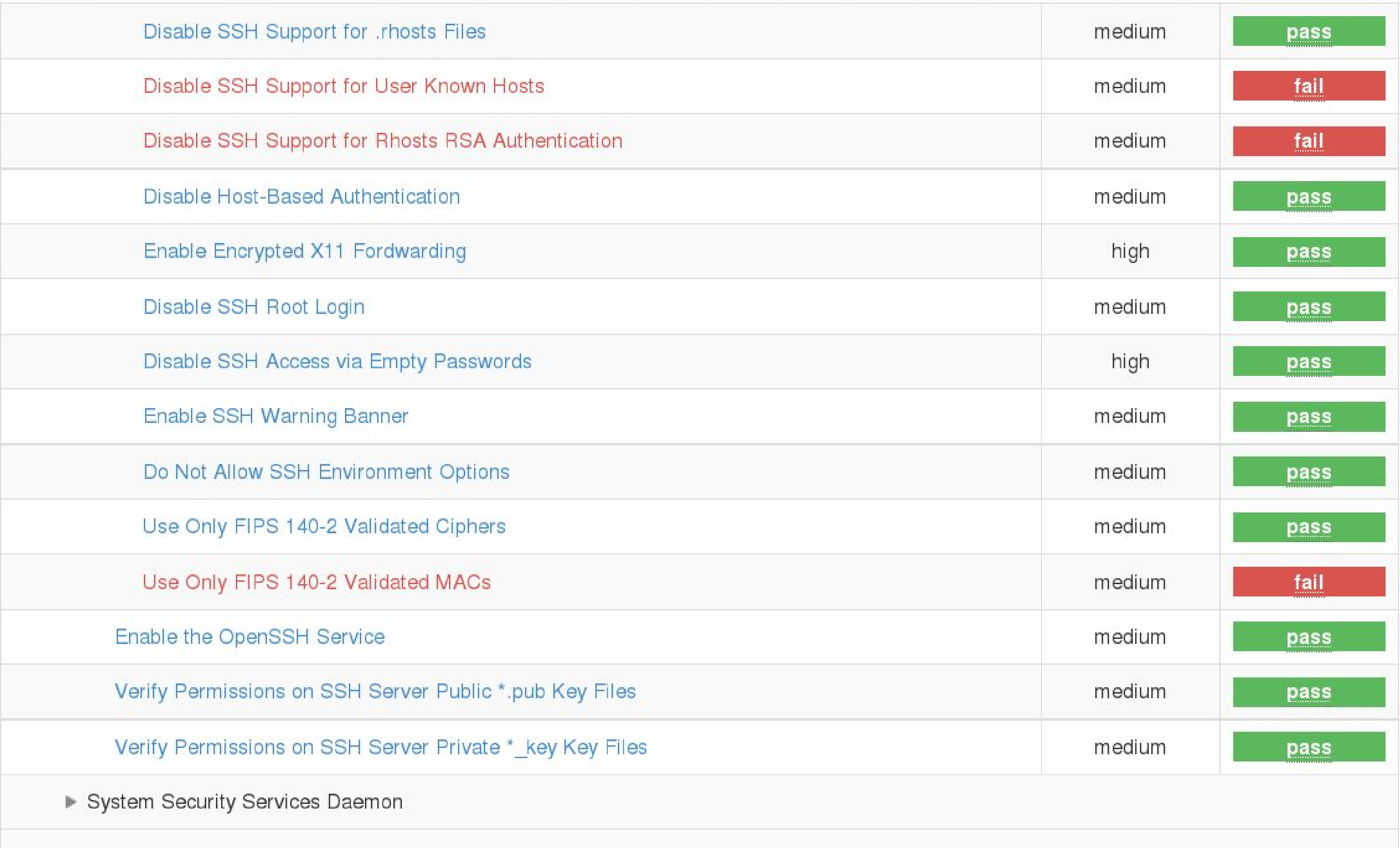
☑ pass
☑ fixed
☑ informational

☑ fail
☑ error
☑ unknown

☑ notchecked
☐ notselected
☑ notapplicable

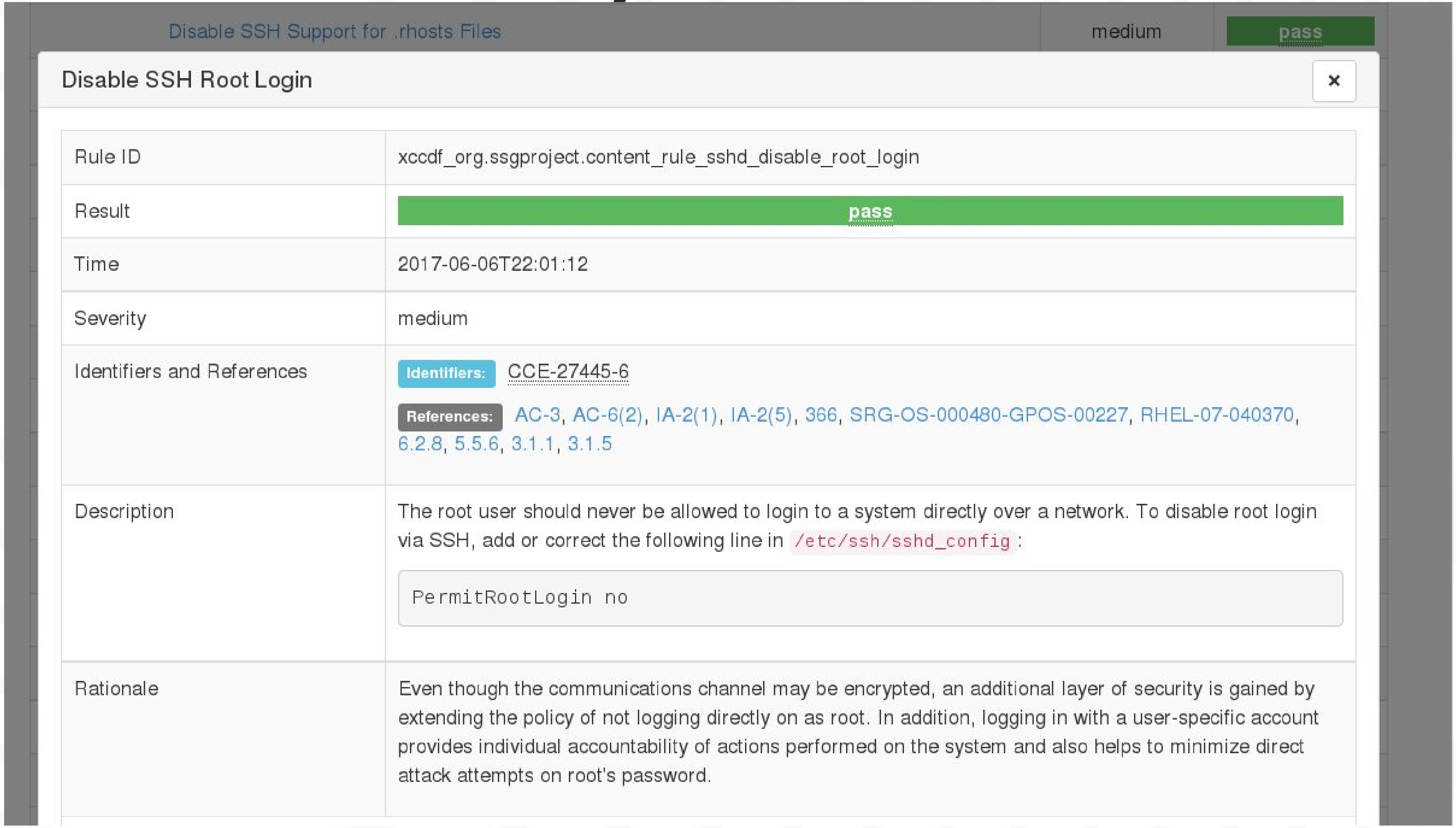
Group rules by: Default

HTML REPORT 3/5



Disable SSH Support for .rhosts Files	medium	pass
Disable SSH Support for User Known Hosts	medium	fail
Disable SSH Support for Rhosts RSA Authentication	medium	fail
Disable Host-Based Authentication	medium	pass
Enable Encrypted X11 Fordwarding	high	pass
Disable SSH Root Login	medium	pass
Disable SSH Access via Empty Passwords	high	pass
Enable SSH Warning Banner	medium	pass
Do Not Allow SSH Environment Options	medium	pass
Use Only FIPS 140-2 Validated Ciphers	medium	pass
Use Only FIPS 140-2 Validated MACs	medium	fail
Enable the OpenSSH Service	medium	pass
Verify Permissions on SSH Server Public *.pub Key Files	medium	pass
Verify Permissions on SSH Server Private *_key Key Files	medium	pass
▶ System Security Services Daemon		

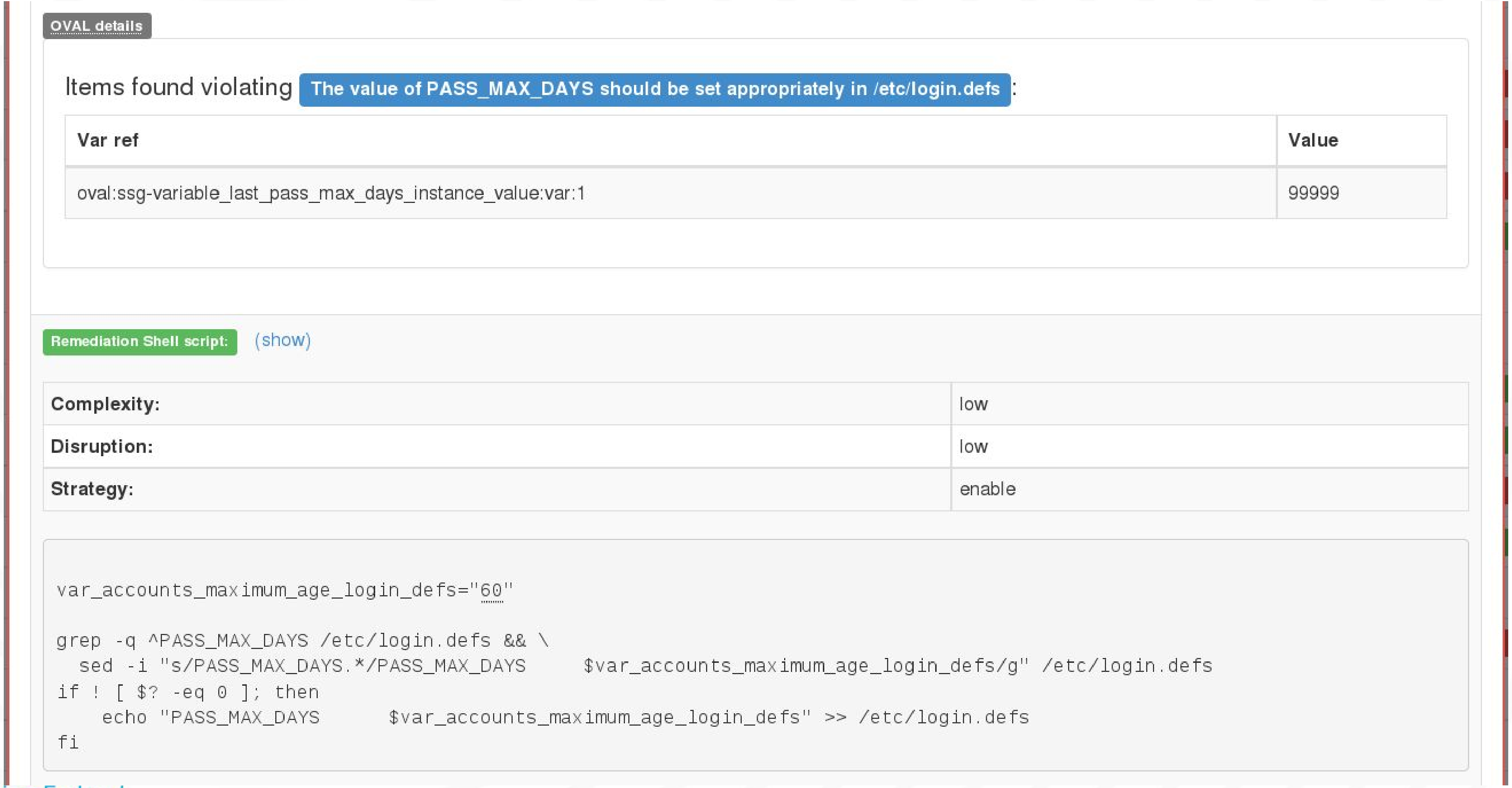
HTML REPORT 4/5



Disable SSH Root Login

Rule ID	xccdf_org.ssgproject.content_rule_sshd_disable_root_login
Result	pass
Time	2017-06-06T22:01:12
Severity	medium
Identifiers and References	Identifiers: CCE-27445-6 References: AC-3, AC-6(2), IA-2(1), IA-2(5), 366, SRG-OS-000480-GPOS-00227, RHEL-07-040370, 6.2.8, 5.5.6, 3.1.1, 3.1.5
Description	The root user should never be allowed to login to a system directly over a network. To disable root login via SSH, add or correct the following line in `/etc/ssh/sshd_config`: `PermitRootLogin no`
Rationale	Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging directly on as root. In addition, logging in with a user-specific account provides individual accountability of actions performed on the system and also helps to minimize direct attack attempts on root's password.

HTML REPORT 5/5



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

Var ref	Value
oval:ssg-variable_last_pass_max_days_instance_value:var:1	99999

Complexity:	low
Disruption:	low
Strategy:	enable

```
var_accounts_maximum_age_login_defs="60"

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
```

COMMAND-LINE FOR VM

```
# oscap-vm domain rhel7.3 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/rhel7.3.qcow2 xccdf
eval --profile
xccdf_org.ssgproject.content_profile_stig-rhel7-server-upstream
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

COMMAND-LINE FOR CONTAINERS

```
# 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
```

Putting machines into compliance

- “remediation”
- online remediation with --remediate
  - happens right after evaluation
- offline remediation
  - get results
  - generate remediations from results
  - OR generate remediations from a profile

Putting machines into compliance

- bash remediations
  - available everywhere
  - idempotent

```
sysctl_net_ipv4_conf_all_secure_redirects_value="0"

# Set runtime for net.ipv4.conf.all.secure_redirects
#
/sbin/sysctl -q -n -w
net.ipv4.conf.all.secure_redirects=$sysctl_net_ipv4_conf_all_secure_redirects_value

# If net.ipv4.conf.all.secure_redirects present in /etc/sysctl.conf, change value to
appropriate value
#   else, add "net.ipv4.conf.all.secure_redirects = value" to /etc/sysctl.conf

replace_or_append '/etc/sysctl.conf' '^net.ipv4.conf.all.secure_redirects'
"$sysctl_net_ipv4_conf_all_secure_redirects_value" 'CCE-80159-7'
```

Putting machines into compliance

- ansible remediations
  - new feature in SSG 0.1.33
  - not full coverage yet

```
- name: Ensure sysctl net.ipv4.conf.all.secure_redirects is set
   sysctl:
     name: net.ipv4.conf.all.secure_redirects
     value: 0
     state: present
     reload: yes
   tags:
     - sysctl_net_ipv4_conf_all_secure_redirects
     - medium
     - CCE-80159-7
```

Writing custom content

- git clone https://github.com/OpenSCAP/scap-security-guide.git

```
cd scap-security-guide
cd build
cmake ../
make -j 4
```

Writing custom content

- SCAP Security Guide is split into products
- Each product:
  - is a library of rules, checks and remediations
  - has one or more profiles
- Find the product you want to change
- Or create a new product in the repository

Writing custom content

- simple / derivative rules
  - use templates
  - add the package or service name to a CSV and rebuild
- complex / from scratch rules
  - have to use OVAL

Questions?

Also check out:

- https://www.open-scap.org/
- #openscap IRC channel on freenode