Security compliance automation with Red Hat Satellite

Matt Micene
Solution Architect, DLT Solutions

@cleverbeard

@nzwulf
Compliance is a major problem

- About half of the CVEs exploited in 2014 went from publish to pwn in less than a month." - Verizon Breach Investigations Report, 2015

- "We found that 99.9% of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published." - Verizon Breach Investigations Report, 2015

“YourApp™ from MyCO poised to revolutionize the industry”
– MyCo CEO
Meet Simon, MyCo Lead System Engineer
Regulations, Catalogs, Guidelines
ZDNET TOLD ME OUR SERVERS HAVE POODLES

I'LL NEED YOU TO PATCH ALL THE BASHES
Advanced Persistent Marketing

Poster created by Ken Westin, 2015, used with permission of author. Hi Ken!
Meet Sarah, MyCo CISO
Sarah's initial SWAG

- Need local values for 50 controls (password lengths, login timeouts, etc)
- Only YourApp new systems in scope
- Project team bringing Security in late

C2S Profile = 250 controls
YourApp Env = 35 systems
HAPPY FRIDAY SIMON, IF YOU COULD JUST AUDIT ALL THE SYSTEMS

BY MONDAY, THAT'D BE GREAT
Simon's back of the napkin

Number of Controls * Time per Control * Number of Hosts
Minutes per Hour

\[
\frac{250 \times 1 \text{ min} \times 35}{60 \text{ min}}
\]

145 hours or ~18 Days
# 'dev' option (not prefixed with 'no') present in the list?
if [ $? -eq 0 ]
then
    # 'dev' option found, replace with 'nodev'
    DEV_ShM_OPTS="${DEV_ShM_OPTS//dev/nodev}"
fi

# at least one 'nodev' present in the options list?
if [ $? -eq 0 ]
then
    # 'nodev' not found yet, append it
    DEV_ShM_OPTS="${DEV_ShM_OPTS#*\}$DEV_ShM_OPTS,noderv"
fi

# DEV_ShM_OPTS now contains final list of mount options. Replace original form of /dev/shm row
# in /etc/fstab with the corrected version
sed -i 's/#\$\{DEV_ShM_HEAD\}\(.*\)\$\{DEV_ShM_TAIL\}\$\{DEV_ShM_OPTS\}\$\{DEV_ShM_TAIL\}#' /etc/fstab

# Load /etc/fstab's /dev/shm row into DEV_ShM_FSTAB variable separating start &
# end of the filesystem mount options (4-th field) with the '#' character
DEV_ShM_FSTAB=$(sed -n "s/\$\{[[:space:]]\}\+$\{/\$\{DEV_ShM_TAIL\}\$\{DEV_ShM_OPTS\}\$\{DEV_ShM_TAIL\}\$\{[[:space:]]\}\+$\{/\$\{DEV_ShM.Head\}\+
s/\$\{[[:space:]]\}\+$\{/\$\{DEV_ShM.Tail\}\$\{DEV_ShM_OPTS\}\$\{DEV_ShM.Tail\}\$\{[[:space:]]\}\+$\{/\$\{DEV_ShM.Fstab\}\n"

# Save the:
# * 1-th, 2-nd, 3-rd fields into DEV_ShM_HEAD variable
# * 4-th field into DEV_ShM_OPTS variable, and
# * 5-th, and 6-th fields into DEV_ShM_TAIL variable
# splitting DEV_ShM_FSTAB variable value based on the '#' separator
IFS='\#' read DEV_ShM_HEAD DEV_ShM_OPTS DEV_ShM_TAIL <<< "DEV_ShM_FSTAB"
SCAP

Brought to you by the letters NVD and CVE!

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

#redhat #rhsummit
What does Simon need?

- SCAP Content
- SCAP Scanner
- Centralization
The final controls!
Final policy

• **Annual** audits
  - Requires **2 additional** regular reviews

• Need local values for **100 controls** (password lengths, login timeouts, etc)

• **15 current production systems** added to scope

• **DR site** also required

C2S Profile = **400 controls**
YourApp Env = **100 systems**
### Simon's new napkin

<table>
<thead>
<tr>
<th>Number of Controls</th>
<th>Time per Control</th>
<th>Number of Hosts</th>
<th>Minutes per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>1 min</td>
<td>100</td>
<td>60 min</td>
</tr>
</tbody>
</table>

\[
\frac{400 \times 1 \text{ min} \times 100}{60 \text{ min}} \approx 666 \text{ hours} \quad \text{or} \quad \approx 83 \text{ Days}
\]
SPOILER ALERT!
What Simon's compliance system can do

C2S Run time = \( 73 \) seconds

\[
\frac{400 \times 5.5 \text{ s} \times 100}{60 \text{ min}}
\]

\(~61 \text{ hours or } ~8 \text{ Days}\)
~8 Days *

• Mostly **computer** time, highly parallel
• **Little** administrator interaction required
• Still ...
• Oh, and **150** more checks (**62.5%** more work)

~75 Days saved
Or **90.36 %**
The Tool Chain that Simon Built
What does Simon need?

- SCAP Content
- SCAP Scanner
- Centralization
The Content

SCAP Scanner

Centralization
SCAP (Security Content Automation Protocol) 1.2

NIST SP 800-126 Rev. 2

- **CCE™**: Common Configuration Enumeration
- **CPE™**: Common Platform Enumeration
- **CVE®**: Common Vulnerabilities and Exposures
- **CVSS**: Common Vulnerability Scoring System
- **CCSS**: Common Configuration Scoring System
- **XCCDF**: The Extensible Configuration Checklist Description Format
- **OVAL®**: Open Vulnerability and Assessment Language
- **OCIL**: Open Checklist Interactive Language
- **AI**: Asset Identification
- **ARF**: Asset Reporting Format
SCAP (Security Content Automation Protocol) 1.2

NIST SP 800-126 Rev. 2

- CCE™: Common Configuration Enumeration
- CPE™: Common Platform Enumeration
- CVE®: Common Vulnerabilities and Exposures
- CVSS: Common Vulnerability Scoring System
- CCSS: Common Configuration Scoring System
- XCCDF: The Extensible Configuration Checklist Description Format
- OVAL®: Open Vulnerability and Assessment Language
- OCIL: Open Checklist Interactive Language
- AI: Asset Identification
- ARF: Asset Reporting Format
Great who makes it?
Red Hat provided feeds

Red Hat Product Security are committed to providing tools and security data to help security measurement. Part of this commitment is our participation at board level in various projects such as MITRE CVE and OVAL. We also provide reports and metrics, but more importantly, we also provide the raw data below so customers and researchers can produce their own metrics, for their own unique situations, and hold us accountable.

CVRF Documents

The Common Vulnerability Reporting Framework (CVRF) standard enables organisations to share information about security issues with a consistent and common format. We provide Red Hat security advisories in CVRF format.

- CVRF compatibility FAQ
- Link to CVRF documents
- CVRF 11 samples (zip) (updated 2015-05-15)

OVAL Definitions

OVAL definitions are available for all vulnerabilities that affect Red Hat Enterprise Linux 3, 4, 5, 6, 7:

- OVAL compatibility FAQ
- OVAL definitions (consolidated XML file, .bz2) (constantly updated)
- OVAL repository (separate files)

Vulnerability Statements and Acknowledgements

We publish acknowledgements and official statements for vulnerabilities currently under investigation and for vulnerabilities that do not affect our products and services. These statements appear on our in CVE pages

- cve-metadata-from-bugzilla.xml (XML feed, updated twice a day)
<Profile id="common">
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">This profile contains items common to general-purpose Fedora installations.</description>
  <select idref="disable_prelink" selected="true"/>
  <select idref="ensure_gpgcheck_globally_activated" selected="true"/>
  <select idref="ensure_gpgcheck_never_disabled" selected="true"/>
  <select idref="file_permissions_library_dirs" selected="true"/>
  <select idref="file_ownership_library_dirs" selected="true"/>
  <select idref="file_permissions_binary_dirs" selected="true"/>
  <select idref="file_ownership_binary_dirs" selected="true"/>
  <select idref="no_direct_root_logins" selected="true"/>
  <select idref="restrict_serial_port_logins" selected="true"/>
  <select idref="no_uidzero_except_root" selected="true"/>
  <select idref="no_empty_passwords" selected="true"/>
  <select idref="no_hashes_outside_shadow" selected="true"/>
  <select idref="no_netrc_files" selected="true"/>
  <select idref="accounts_password_minlen_login_defs" selected="true"/>
  <select idref="accounts_minimum_age_login_defs" selected="true"/>
  <select idref="accounts_maximum_age_login_defs" selected="true"/>
  <select idref="accounts_password_warn_age_login_defs" selected="true"/>
  <select idref="root_path_no_groupother_writable" selected="true"/>
  <select idref="service_ntpd_enabled" selected="true"/>
  <select idref="ntpd_specify_remote_server" selected="true"/>
  <select idref="sshd_disable_root_login" selected="true"/>
  <select idref="sshd_disable_empty_passwords" selected="true"/>
  <select idref="sshd_set_idle_timeout" selected="true"/>
  <select idref="sshd_set_keepalive" selected="true"/>
  <refine-value idref="var_accounts_password_minlen_login_defs" selector="12"/>
  <refine-value idref="var_accounts_minimum_age_login_defs" selector="7"/>
  <refine-value idref="var_accounts_maximum_age_login_defs" selector="30"/>
  <refine-value idref="var_accounts_password_warn_age_login_defs" selector="7"/>
  <refine-value idref="sshd_idle_timeout_value" selector="5_minutes"/>
</Profile>
XCCDF Profile
<Profile id="common">
  <title xml:lang="en-US">Common Profile for General-Purpose Fedora Systems</title>
  <description xml:lang="en-US">This profile contains items common to general-purpose Fedora installations.</description>
  <select idref="disable_prelink" selected="true"/>
  <select idref="ensure_gpgcheck_globally_activated" selected="true"/>
  <select idref="ensure_gpgcheck_never_disabled" selected="true"/>
  <select idref="file_permissions_library_dirs" selected="true"/>
  <select idref="file_permissions_binary_dirs" selected="true"/>
  <select idref="file_ownership_library_dirs" selected="true"/>
  <select idref="file_ownership_binary_dirs" selected="true"/>
  <select idref="no_direct_root_logins" selected="true"/>
  <select idref="securetty_root_login_console_only" selected="true"/>
  <select idref="restrict_serial_port_logins" selected="true"/>
  <select idref="no_uidzero_except_root" selected="true"/>
  <select idref="no_empty_passwords" selected="true"/>
  <select idref="no hashes outside shadow" selected="true"/>
  <select idref="no_netrc_files" selected="true"/>
  <select idref="accounts_password_mintlen_login_defs" selected="true"/>
  <select idref="accounts_minimum_age_login_defs" selected="true"/>
  <select idref="accounts_maximum_age_login_defs" selected="true"/>
  <select idref="accounts_password_warn_age_login_defs" selected="true"/>
  <select idref="root_path_no_groupother writable" selected="true"/>
  <select idref="service_ntpd_enabled" selected="true"/>
  <select idref="ntpd_spectry_remote_server" selected="true"/>
  <select idref="sshd_disable_root_login" selected="true"/>
  <select idref="sshd_disable_empty_passwords" selected="true"/>
  <select idref="sshdacct_idle_timeout" selected="true"/>
  <select idref="sshdacct_keepalive" selected="true"/>
  <refine-value idref="var_accounts_password_mintlen_login_defs" selector="12"/>
  <refine-value idref="var_accounts_minimum_age_login_defs" selector="7"/>
  <refine-value idref="var_accounts_maximum_age_login_defs" selector="30"/>
  <refine-value idref="var_accounts_password_warn_age_login_defs" selector="7"/>
  <refine-value idref="sshd_idle_timeout_value" selector="5 minutes"/>
</Profile>
XCCDF Rule

Set Password Hashing Algorithm in /etc/login.defs:

In <xhtml:code>/etc/login.defs</xhtml:code>, add or correct the following line to ensure the system will use SHA-512 as the hashing algorithm:

```xml
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRIPT_METHOD SHA512</pre>
```

Using a stronger hashing algorithm makes password cracking attacks more difficult.

Reference:
- [IA-7](http://iase.disa.mil/stigs/cci/Pages/index.aspx)
- [AES](http://www.w3.org/1999/xhtml) (en-US)

Rationale:
XCCDF Rule

<Rule id="set_password_hashing_algorithm_logindefs" selected="false" severity="medium"/>
<title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Set Password Hashing Algorithm in /etc/login.defs</title>
<description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
In <xhtml:code>/etc/login.defs</xhtml:code>, add or correct the following line to ensure the system will use SHA-512 as the hashing algorithm:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD_SHA512</pre>
</description>


Using a stronger hashing algorithm makes password cracking attacks more difficult.
</rationale>

<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref name="oval:sgs:der:208" href="ssg-fedora-oval.xml"/>
</check>
<check system="ocil-transitional">
  <check-export export-name="it does not" value-id="conditional_clause"/>
</check>
<check-content xmlns="http://www.w3.org/1999/xhtml"/>
</check>
<check system="http://www.w3.org/1999/xhtml">
Inspect <xhtml:code>/etc/login.defs</xhtml:code> and ensure the following line appears:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD_SHA512</pre>
</check-content>
</check>
</Rule>
XCCDF Rule

<Rule id="set_password_hashing_algorithm_logindefs" selected="false" severity="medium"/>
<title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Set Password Hashing Algorithm in /etc/login.defs</title>
<description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">In /etc/login.defs, add or correct the following line to ensure the system will use SHA-512 as the hashing algorithm:
<pref xmlns="http://www.w3.org/1999/xhtml">ENCRIPT_METHOD SHA512</pref>
</description>

<rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Using a stronger hashing algorithm makes password cracking attacks more difficult. </rationale>

<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref name="oval:ssg:der:208" href="ssg-redora-oval.xml"/>
</check>
<check system="ocil-transitional">
  <check-export export-name="it does not" value-id="conditional_clause"/>
  <check-content xmlns:xhtml="http://www.w3.org/1999/xhtml">
  Inspect /etc/login.defs and ensure the following line appears:
  <pref xmlns="http://www.w3.org/1999/xhtml">ENCRIPT_METHOD SHA512</pref>
  </check-content>
</check>
</Rule>
OVAL Entities

DEFINITION

TEST

OBJECT

STATE

TEST

OBJECT

STATE
OVAL Definition

<definition class="compliance" id="oval:ssg:def:208" version="2">
  <metadata>
    <title>Set SHA51Z Password Hashing Algorithm in /etc/login.defs</title>
    <affected family="unix">
      <platform>Red Hat Enterprise Linux 6</platform>
      <platform>Red Hat Enterprise Linux 7</platform>
    </affected>
    <description>The password hashing algorithm should be set correctly in /etc/login.defs.</description>
  </metadata>
  <reference source="JL" ref_id="RHEL6_20150201" ref_url="test_attestation"/>
  <reference source="JL" ref_id="RHEL7_20150201" ref_url="test_attestation"/>
  <reference source="JL" ref_id="FEDORA20_20150201" ref_url="test_attestation"/>
  <reference ref_id="set_password_hashing_algorithm_logindefs" source="ssg"/>
  <criterion operator="AND">
    <criterion test_ref="oval:ssg:tst:209"/>
  </criterion>
</definition>
OVAL Walking back the cat

<ind:variable_test id="oval:ssg:tst:209" check="all" comment="The value of ENCRYPT_METHOD should be set appropriately in /etc/login.defs" version="1">
  <ind:object object_ref="oval:ssg:obj:367"/>
  <ind:state state_ref="oval:ssg:ste:368"/>
</ind:variable_test>

<ind:variable_object id="oval:ssg:obj:367" version="1">
  <ind:var_ref>oval:ssg:var:451</ind:var_ref>
</ind:variable_object>

<local_variable id="oval:ssg:var:451" datatype="string" comment="The value of last ENCRYPT_METHOD directive in /etc/login.defs" version="1">
  <regex_capture pattern="ENCRIPT_METHOD\s+\((\w+)\)">
    <object_component item_field="subexpression" object_ref="oval:ssg:obj:450"/>
  </regex_capture>
</local_variable>

<ind:filecontent54_object id="oval:ssg:obj:450" version="1">
  <!-- Read whole /etc/login.defs as single line so we can retrieve last ENCRYPT_METHOD directive occurrence -->
  <ind:behavior singleline="true"/>
  <ind:filepath>/etc/login.defs</ind:filepath>
  <!-- Retrieve last (uncommented) occurrence of ENCRYPT_METHOD directive -->
  <ind:pattern operation="pattern match">.*\n[^*]\*(ENCRIPT_METHOD\s+\w+).*\n</ind:pattern>
  <ind:instance datatype="int" operation="greater than or equal">1</ind:instance>
</ind:filecontent54_object>

<ind:variable_state id="oval:ssg:ste:368" version="1">
  <ind:value operation="equals" datatype="string">SHA512</ind:value>
</ind:variable_state>
A plug for upstream

- Sane separation of files with XSLT to create valid content
- OVAL in single check file with human readable IDs
- XCCDF in descriptive structure
- Modify make file to include and build content or RPM

```xml
<definition class="compliance" id="set_password_hashing_algorithm_logindefs" version="2">
  <meta>
    <title>Set SHA512 Password Hashing Algorithm in /etc/login.defs</title>
    <effect domain="null"/>
    <platform multi="all"/>
  </meta>
  <description>The password hashing algorithm should be set correctly in /etc/login.defs.</description>
  <reference source="31" ref="BHEL6_20150201" ref_url="test_attestation"/>
  <reference source="31" ref="BHEL7_20150201" ref_url="test_attestation"/>
  <reference source="31" ref="TEHRA00_20150201" ref_url="test_attestation"/>
</meta>

<decision test_ref="test_etc_login_defs_encrypt_method"/>
</definition>
```
What about the analyst?
Guide to the Secure Configuration of Red Hat Enterprise Linux 6

Customization (no customization)

Profile: C2S for Red Hat Enterprise Linux 6

Target: Local Machine

Audit logs are stored in the /var/log/audit directory. Ensure that it has its own partition or logical volume at installation time, or migrate it later using LVM. Make absolutely certain that it is large enough to store all audit logs that will be created by the auditing daemon.

Ensure /var/log/audit Located On Separate Partition

Ensure /home Located On Separate Partition

Ensure Red Hat GPG Key Installed

To ensure the system can cryptographically verify base software packages come from Red Hat (and to connect to the Red Hat Network to receive them), the Red Hat GPG key must properly be installed. To install the Red Hat GPG key, run:

```
$ sudo zha_register
```

If the system is not connected to the Internet or an RHN Satellite, then install the Red Hat GPG key from trusted media such as the Red Hat installation CD-ROM or DVD. Assuming the disc is mounted in /media/drom, use the following command as the root user to import it into the keysring:

```
$ sudo rpm --import /media/cdrom/RPM-GPG-KEY
```
<scapTailoring xmlns:scap="http://checklists.nist.gov/scap/1.2" id="scap_tailoring_default">
  <benchmark href="/usr/share/xml/scap/sgg/content/sgg-rhel6-ds.xml"/>
  <version time="2015-04-20T09:51:07">1</benchmark>
  <profile id="xccdf_com.dlt.content_profile_C25_baseline" extends="xccdf_org.ssgproject.content_profile_C25">
    <select idref="xccdf_org.ssgproject.content_rule_set_password_hashing_algorithm_libuserconf" selected="true"/>
    <select idref="xccdf_org.ssgproject.content_rule_root_path_no_groupother_writable" selected="true"/>
    <select idref="xccdf_org.ssgproject.content_rule_root_path_no_dot" selected="true"/>
    <select idref="xccdf_org.ssgproject.content_rule_network_disable_zeroconf" selected="true"/>
    <set-value idref="xccdf_org.ssgproject.content_value_var_umask_for_daemons" value="022"/>
    <set-value idref="xccdf_org.ssgproject.content_value_var_accounts_password_minlen_login_defs" value="8"/>
    <set-value idref="xccdf_org.ssgproject.content_value_var_accounts_password_minimum_age_login_defs" value="0"/>
    <set-value idref="xccdf_org.ssgproject.content_value_var_accounts_password_warn_age_login_defs" value="14"/>
    <set-value idref="xccdf_org.ssgproject.content_value_var_accounts_passwords_pam_falillock_unlock_time" value="900"/>
  </profile>
</scapTailoring>
The Scanner

Centralization
OpenSCAP

NIST validated SCAP scanner by Red Hat

https://nvd.nist.gov/scappproducts.cfm
The Centralization
Workflow

- Red Hat RPMs
- Upstream Content
- Custom Created
- Red Hat Satellite
- OSCAP
- Tailoring
- Reporting
SATELLITE 5
WORK FLOW
Use RPMs

```
[root@ep-mgmt01 ~]# gpg --list-keys
/root/.gnupg/pubring.gpg

pub  2048R/96D46A3F 2015-04-09
uid           Package Builder (This is for signing local RPMs) <pkgs@dlt.com>
sub  2048R/4558B67D 2015-04-09

[root@ep-mgmt01 noarch]# rpm --resign rhssa-scap-1.0-2.el6.noarch.rpm
Enter pass phrase:
Pass phrase is good.
rhssa-scap-1.0-2.el6.noarch.rpm:

[root@ep-sat01 pub]# rhnpush -c rhssa-scap-el6 /tmp/rhssa-scap-1.0-2.el6.noarch.rpm
```

```
[root@localhost ~]# ls -l /usr/share/xml/scap/ssg/content
1780 total
-rw-r--r--. 1 root root  600 Aug  8 2014 ssg-rhel6-cpe-dictionary.xml
-rw-r--r--. 1 root root 3712 Aug  8 2014 ssg-rhel6-cpe-oval.xml
-rw-r--r--. 1 root root 2875837 Aug  8 2014 ssg-rhel6-ds.xml
-rw-r--r--. 1 root root 768150 Aug  8 2014 ssg-rhel6-oval.xml
-rw-r--r--. 1 root root 1242376 Aug  8 2014 ssg-rhel6-xccdf.xml

[root@localhost ~]# ls -l /usr/share/xml/scap/ssg/rhss/
27976 total
-rw-r--r--. 1 root root 1776419 Apr  9 12:41 com.redhat.rhssa-all.xccdf.xml
-rw-r--r--. 1 root root 26869032 Apr  9 12:46 com.redhat.rhssa-all.xml
```
Scanning hosts

```
Command: /usr/bin/oscap xccdf eval
Command-line Arguments: --profile xccdf_com.dlt.content_profile_C2S_baseline --tailoring-file /
Path to XCCDF document*: /usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
Schedule no sooner than: April 29, 2015 1:43 PM EDT
```

Tip: Certain versions of OpenSCAP may require the --profile command-line argument. --profile specifies a particular profile from the XCCDF document.
### Scan list

#### OpenSCAP Scans

<table>
<thead>
<tr>
<th>Test Result</th>
<th>Completed</th>
<th>Compliance</th>
<th>P</th>
<th>F</th>
<th>E</th>
<th>U</th>
<th>N</th>
<th>K</th>
<th>S</th>
<th>I</th>
<th>X</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>xccdf_org.open-scap_testresult_default-profile</code></td>
<td>Thu Apr 23 13:31:51 EDT 2015</td>
<td>99 %</td>
<td>2544</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2565</td>
<td></td>
</tr>
<tr>
<td><code>xccdf_org.open-scap_testresult_default-profile</code></td>
<td>Mon Apr 20 13:41:09 EDT 2015</td>
<td>99 %</td>
<td>2544</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2565</td>
<td></td>
</tr>
<tr>
<td><code>xccdf_org.open-scap_testresult_xccdf_com.dlt.content_profile_C25_baseline</code></td>
<td>Mon Apr 20 13:38:37 EDT 2015</td>
<td>46 %</td>
<td>88</td>
<td>91</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>210</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><code>xccdf_org.open-scap_testresult_xccdf_com.dlt.content_profile_C25_baseline</code></td>
<td>Mon Apr 20 13:34:46 EDT 2015</td>
<td>46 %</td>
<td>88</td>
<td>91</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>210</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Tip: Compliance column represents unweighted pass/fail ration. Compliance = P / (Total - S - I).
<table>
<thead>
<tr>
<th>XCCDF Rule Identifier</th>
<th>XCCDF Ident Tags</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>xccdf_org.ssgproject.content_rule.ensure_gpgcheck_never_disabled</td>
<td>CCE-26647-8</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule.aide_periodic_cron_checking</td>
<td>CCE-27222-9</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule.rpm_verify_hashes</td>
<td>CCE-27223-7</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule.mount_option_nodev_removable_partitions</td>
<td>CCE-26860-7</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule.mount_option_noexec_removable_partitions</td>
<td>CCE-27169-5</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule.mount_option_nosuid_removable_partitions</td>
<td>CCE-27056-1</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_userowner_shadow_file</td>
<td>CCE-26947-2</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_groupowner_shadow_file</td>
<td>CCE-26967-0</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions_etc_shadow</td>
<td>CCE-26992-8</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_owner_etc_group</td>
<td>CCE-26822-7</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_groupowner_etc_group</td>
<td>CCE-26930-8</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions_etc_group</td>
<td>CCE-26954-8</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_owner_etc_gshadow</td>
<td>CCE-27026-4</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_groupowner_etc_gshadow</td>
<td>CCE-26975-3</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions_etc_gshadow</td>
<td>CCE-26951-4</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_owner_etc_passwd</td>
<td>CCE-26953-0</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_groupowner_etc_passwd</td>
<td>CCE-26856-5</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions_etc_passwd</td>
<td>CCE-26868-0</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions_binary_dirs</td>
<td>CCE-27289-8</td>
<td>pass</td>
</tr>
<tr>
<td>XCCDF Rule Identifier</td>
<td>First Scan</td>
<td>Second Scan</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_rpm_verify_hashes</td>
<td>pass</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions/etc_group</td>
<td>pass</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_service_cgen_red_disabled</td>
<td>pass</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_set_password_hashing_algorithm_systemauth</td>
<td>fail</td>
<td>fail</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_dns_server_authorize_zone_transfers</td>
<td>notselected</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_permissions/etc_shadow</td>
<td>pass</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_kernel_module_ipv6_option_disabled</td>
<td>fail</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_chmod</td>
<td>fail</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_default_secure_redirects</td>
<td>fail</td>
<td>fail</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_default_rp_filter</td>
<td>pass</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_network_ipv6_disable_rpc</td>
<td>pass</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_ftp_present_banner</td>
<td>pass</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_ftp_log_transactions</td>
<td>pass</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_package_openswan_installed</td>
<td>fail</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_ownership_binary_dirs</td>
<td>pass</td>
<td>notselected</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_sysctl_kernel_randomize_va_space</td>
<td>fail</td>
<td>fail</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_sshd_limit_user_access</td>
<td>notchecked</td>
<td>notchecked</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_file_groupowner/etc_shadow</td>
<td>pass</td>
<td>pass</td>
</tr>
<tr>
<td>xccdf_org.ssgproject.content_rule_service_audited_enabled</td>
<td>notselected</td>
<td>pass</td>
</tr>
</tbody>
</table>
Diff to any!
Change some defaults

Enable Staging Contents
Enable Software Crash Reporting
Enable Upload Of Crash Files
Crash File Upload Size Limit
Enable Upload Of Detailed SCAP Files
SCAP File Upload Size Limit
Allow Deletion of SCAP Results
Allow Deletion After (period in days)
# Detailed Report

## Score

<table>
<thead>
<tr>
<th>system</th>
<th>score</th>
<th>max</th>
<th>%</th>
<th>bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>um:xccdf:scoring:default</td>
<td>67.51</td>
<td>100.00</td>
<td>67.51%</td>
<td></td>
</tr>
</tbody>
</table>

## Results overview

### Rule Results Summary

<table>
<thead>
<tr>
<th>pass</th>
<th>fixed</th>
<th>fail</th>
<th>error</th>
<th>not selected</th>
<th>not checked</th>
<th>not applicable</th>
<th>informational</th>
<th>unknown</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>0</td>
<td>91</td>
<td>0</td>
<td>210</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>400</td>
</tr>
</tbody>
</table>

### Title

<table>
<thead>
<tr>
<th>Title</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure /tmp Located On Separate Partition</td>
<td>fail</td>
</tr>
<tr>
<td>Ensure /home Located On Separate Partition</td>
<td>fail</td>
</tr>
<tr>
<td>Ensure Red Hat GPG Key Installed</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure gpgcheck Enabled In Main Yum Configuration</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure gpgcheck Enabled For All Yum Package Repositories</td>
<td>pass</td>
</tr>
<tr>
<td>install AIDE</td>
<td>fail</td>
</tr>
<tr>
<td>Disable Prelinking</td>
<td>fail</td>
</tr>
<tr>
<td>Build and Test AIDE Database</td>
<td>notchecked</td>
</tr>
<tr>
<td>Configure Periodic Execution of AIDE</td>
<td>pass</td>
</tr>
<tr>
<td>Verify and Correct File Permissions with RPM</td>
<td>fail</td>
</tr>
<tr>
<td>Verify File Hashes with RPM</td>
<td>pass</td>
</tr>
<tr>
<td>Add nodev Option to Non-Root Local Partitions</td>
<td>fail</td>
</tr>
</tbody>
</table>
Scanning groups with SSM
Scanning groups with SSM

Targeted Systems

<table>
<thead>
<tr>
<th>System</th>
<th>OpenSCAP Scan Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>ep-builder02.lab.dlt.com</td>
<td>No</td>
</tr>
<tr>
<td>ep-srvr160.lab.dlt.com</td>
<td>Yes</td>
</tr>
<tr>
<td>ep-srvr161.lab.dlt.com</td>
<td>Yes</td>
</tr>
<tr>
<td>ep-web01.lab.dlt.com</td>
<td>No</td>
</tr>
<tr>
<td>scap-target</td>
<td>Yes</td>
</tr>
<tr>
<td>scap-target02</td>
<td>Yes</td>
</tr>
</tbody>
</table>

OpenSCAP xccdf scanning

In Progress Systems

<table>
<thead>
<tr>
<th>System</th>
<th>Earliest execution</th>
<th>Base Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>ep-srvr160.lab.dlt.com</td>
<td>5/1/15 9:23:00 AM EDT</td>
<td>Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)</td>
</tr>
<tr>
<td>ep-srvr161.lab.dlt.com</td>
<td>5/1/15 9:23:00 AM EDT</td>
<td>Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)</td>
</tr>
<tr>
<td>scap-target</td>
<td>5/1/15 9:23:00 AM EDT</td>
<td>Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)</td>
</tr>
<tr>
<td>scap-target02</td>
<td>5/1/15 9:23:00 AM EDT</td>
<td>Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)</td>
</tr>
</tbody>
</table>
Advanced searches

CVE-2014-6271
System built after scans

- System Events:
  - Checked In: 4/29/15 3:11:01 PM EDT
  - Registered: 4/27/15 4:37:58 PM EDT
  - Last Booted: 4/27/15 4:40:10 PM EDT (Schedule System Reboot)
  - OSA Status: offline as of 4/29/15 1:40:47 PM EDT

#redhat #rhsummit
Automation

• Cron + Satellite API
• Use with a different change manager
• http://github.com/nzwulfin/rhsummit15
SATELLITE 6
WORK FLOW
From Tailoring to Profile

```
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2" id="xccdf_scap-workbench_tailoring_default">
  <xccdf:benchmark href="/usr/share/xml/scap/sgg/content/sgg-rhel6-ds.xml"/>
  <xccdf:version time="2015-05-12T09:41:39">1</xccdf:version>
  <xccdf:Profile id="C2S_customized" extends="xccdf_org.ssgproject.content_profile_C2S">
    <refine-value idref="xccdf_org.ssgproject.content_value_var_umask_for_daemons" selector="027"/>
    <refine-value idref="xccdf_org.ssgproject.content_value_var_accounts_user_umask" selector="027"/>
    <refine-value idref="xccdf_org.ssgproject.content_value_var_accounts_maximum_age_login_defs" selector="90"/>
  </Profile>
</xccdf:Tailoring>
```

C2S for Red Hat Enterprise Linux 6 [CUSTOMIZED]

This profile demonstrates compliance against the U.S. Government Commercial Cloud Services (C2S) baseline with modifications made for OurCo.
Upload Datastream

SCAP Contents

Filter ...

<table>
<thead>
<tr>
<th>Title</th>
<th>Locations</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSG_RHEL_7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**File Upload**

- **Title**: New_SG_Content
- **Scap file**: No file selected.

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

Cancel  Submit
Create scan profile

New Compliance Policy

Name *
SSG_For_RHEL_7_with_RHCCP_Profile

Description
SCAP Security Guide for RHEL 7 with the Red Hat Certified Cloud Provider Policy
Create scan profile

New Compliance Policy

1. Create policy
2. SCAP Content
3. Schedule
4. Locations
5. Organizations
6. Hostgroups

Scap content: SSG_RHEL_7

XCCDF Profile: Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

Notice: Ensure the selected SCAP content exists on your hosts.
New Compliance Policy

- Period: Weekly
- Weekday: Tuesday
Create scan profile

New Compliance Policy

Locations

Selected items

Default Location
Create scan profile

New Compliance Policy

1. Create policy
2. SCAP Content
3. Schedule
4. Locations
5. Organizations
6. Hostgroups

Organizations

Selected items
Default Organization
Create scan profile

New Compliance Policy

Hostgroups

All Items

Filter

RHEL6_Dev_Servers
RHEL6_Prod_Servers
RHEL7_Dev_Servers

Selected items

RHEL7_Prod_Servers
Reporting
Reporting

Compliance policy: SCAP_Security_Guide_for_RHEL_7

Hosts Breakdown
- Compliant with the policy: 0
- Not compliant with the policy: 2
- Inconclusive results: 0
- Never audited: 0

Total hosts: 2

Latest reports for policy: SCAP_Security_Guide_for_RHEL_7

<table>
<thead>
<tr>
<th>Host</th>
<th>Date</th>
<th>Passed</th>
<th>Failed</th>
<th>Other</th>
<th>View Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-0001.example.com</td>
<td>8 days ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node-0004.example.com</td>
<td>8 days ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node-0003.example.com</td>
<td>8 days ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node-0002.example.com</td>
<td>8 days ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

100% Incompliant hosts
Reporting

OpenSCAP Evaluation Report

Evaluation Characteristics

<table>
<thead>
<tr>
<th>Target machine</th>
<th>CPE Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>devnode-0003.example.com</td>
<td>cpe:/o:rhel:enterprise:7.4:en:64bit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Benchmark ID</th>
<th>Benchmark URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>test123</td>
<td>/data/open/scap/content/RHEL-7.cpe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile ID</th>
<th>Start at</th>
<th>Finished at</th>
<th>Performed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>scodf-rhel7-0-0.cpe</td>
<td>2015-04-22T01:00:02</td>
<td>2015-04-22T01:00:05</td>
<td>root</td>
</tr>
</tbody>
</table>

Addresses

- IP: 192.168.124.111
- MAC: 00:00:00:00:00:00
- MAC: 02:54:00:DF:D6:69

Compliance and Scoring

The target system did not satisfy the conditions of 33 rules! Please review rule results and consider applying remediation.

Rule results

<table>
<thead>
<tr>
<th>Passed</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>55</td>
</tr>
</tbody>
</table>

Severity of failed rules

<table>
<thead>
<tr>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>17</td>
<td>4</td>
</tr>
</tbody>
</table>
Reporting

Rule results
- 24 passed
- 0 failed

Severity of failed rules
- 12 low
- 17 medium
- 4 high

Score
<table>
<thead>
<tr>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>xcloud scoring:default</td>
<td>66.064819</td>
<td>100.000000</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

Rule Overview
- pass
- fail
- fixed
- error
- informational
- unknown
- notapplicable
- notchecked

Title
- Guide to the Secure Configuration of Red Hat Enterprise Linux 7
  - Introduction
  - System Settings
    - Environments
    - Environments
  - Installing and Maintaining Software
  - Disk Partitioning

Result
- low
- not checked
- not applicable
- pass
- fail

Tags:
#redhat #rhsummit
Install tools on client

Edit RHEL7_Dev_Servers

Included Classes
- mod
- foreman_scap_client

Available Classes
- access_insights_client
- foreman_scap_client
- mod
- stdlib
Matt Micene
Solution Architect, DLT Solutions

@cleverbeard
@nzwulfin
Resources

- John Boyd and the OODA Loop
- Satellite API scripts and RPM spec file
- OpenSCAP Github Organization
- Red Hat Security Data site
- Red Hat Security RHSA Checklist
- Anton Chuvakin: Highlights from '14 Verizon PCI Report
- NIST Validated SCAP tools