Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

Presenters:

Robin Price II and **Martin Preisler**

Abstract:

OpenSCAP is a family of open source SCAP tools and content that help users create standard security checklists for enterprise systems. Natively shipping in Red Hat Enterprise Linux, OpenSCAP provides practical security hardening advice for Red Hat technologies and links to compliance requirements, making deployment activities like certification and accreditation easier.

Audience/Intro/Prerequisites:

This lab is geared towards linux system administrators that have completed the Red Hat Certified System Admistration (RHCSA), the Red Hat Certified Engineer (RHCE) certification or have similar skillsets.

Attendees, during this session, will...

- Develop a foundational knowledge around the **S**ecurity **C**ontent **A**utomation **P**rotocol
- Go hands-on with OpenSCAP from the command-line.
- Understand the OpenSCAP tool and security standards used to generate reports and remediation.

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

BEFORE YOU BEGIN...

You should have a standard base installation of Red Hat Enterprise Linux 7.3

OPENSCAP CLI LAB: INSTALLATION

- Install **OpenSCAP** and the **SCAP Security Guide** packages.

```
[root@serverX ~]# yum install openscap-scanner scap-security-guide
...
Dependencies Resolved
================================================================================
Package                    Arch       Version         Repository      Size
================================================================================
Installing:
 openscap-scanner          x86_64     1.2.10-3.el7_3  rhel-dvd         48 k
 scap-security-guide       noarch     0.1.30-5.el7_3  rhel-dvd        767 k
...
```

The `oscap` tool does not provide any security policies on its own — you have to obtain the rule sets from a separate package. On **Red Hat Enterprise Linux**, default policies are provided by **SCAP Security Guide (SSG)**.

OPENSCAP CLI LAB: EVALUATION

- Run the **OpenSCAP** command while using the `-V --version` option.

```
[root@serverX ~]# oscap -V
...
==== Supported specifications ====
XCCDF Version: 1.2
OVAL Version: 5.11.1
CPE Version: 2.3
CVSS Version: 2.0
CVE Version: 2.0
Asset Identification Version: 1.1
Asset Reporting Format Version: 1.1
==== Capabilities added by auto-loaded plugins ====
No plugins have been auto-loaded...

==== Paths ====
```

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

```
Schema files: /usr/share/openscap/schemas
Default CPE files: /usr/share/openscap/cpe
Probes: /usr/libexec/openscap

==== Inbuilt CPE names ====
Red Hat Enterprise Linux - cpe:/o:redhat:enterprise_linux
Red Hat Enterprise Linux 5 - cpe:/o:redhat:enterprise_linux:5
Red Hat Enterprise Linux 6 - cpe:/o:redhat:enterprise_linux:6
...
==== Supported OVAL objects and associated OpenSCAP probes ====
system_info                  probe_system_info
family                       probe_family
filehash                     probe_filehash
...
```

The **`oscap -V`** command is great for reviewing what specifications versions, builtin **CPE** names, supported **OVAL** objects and associated **OpenSCAP** probes are installed.

- Locate the **SCAP** content installed on the system from the **SCAP Security Guide** package.

```
[root@serverX ~]# rpm -ql scap-security-guide | grep content
/usr/share/xml/scap/ssg/content
/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-oval.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-oval.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

- Select a security profile by examining the **Source Data Stream** `(-ds.xml)` file with the **`oscap info`** module.

```
[root@serverX ~]# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Document type: Source Data Stream
Imported: 2017-02-14T13:33:08

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Generated: (null)
Version: 1.2
```

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

```
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml
                Status: draft
                Generated: 2017-02-14
                Resolved: true
                Profiles:
                        xccdf_org.ssgproject.content_profile_standard
                        xccdf_org.ssgproject.content_profile_pci-dss
                        xccdf_org.ssgproject.content_profile_rht-ccp
                        xccdf_org.ssgproject.content_profile_common
...
                Referenced check files:
                        ssg-rhel7-oval.xml
                        system: http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-oval.xml
        Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-cpe-oval.xml
        Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-oval.xml
Dictionaries:
        Ref-Id: scap_org.open-scap_cref_output--ssg-rhel7-cpe-dictionary.xml
```

Each security policy can have multiple profiles which provide policies implemented according to specific security baselines. Every profile can select different rules and use different values. One of the capabilities of **`oscap`** is to display information about the SCAP contents within a file. When examining an XCCDF document or a SCAP data stream, generally, the most useful information is about profiles, checklists, and streams.

- Example of a profile is the **Certified Cloud Providers (CCP).** We will use this profile going forward.

```
Profiles:
                ...
                xccdf_org.ssgproject.content_profile_rht-ccp
                ...
```

OPENSCAP CLI LAB: SCANNING AND REPORTING

- From the information provided, perform an acutal scan from the terminal now that we have determined which security policy and profile we want to use.

```
[root@serverX ~]# oscap xccdf eval --profile
xccdf_org.ssgproject.content_profile_rht-ccp --results-arf arf.xml --report
report.html /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

- The options can be broken down as follows:

```
# oscap xccdf eval \
 --profile xccdf_org.ssgproject.content_profile_rht-ccp \
 --results-arf arf.xml \
 --report report.html \
 /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

  - **`xccdf eval`**
    - The **`oscap`** tool calls on the **`xccdf`** module.
    - The **`xccdf`** module is used with the eval operation which then allows us to perform the evaluation.
    - The XCCDF module will try to load all OVAL Definition files referenced from XCCDF automatically.
  - **`--profile`** `PROFILE`
    - Select a particular profile from the data stream file (INPUT file) at the end of the command.
  - **`--results-arf`** `FILE`
    - This option tells oscap that we want the results stored as an Assest Reporting Format (ARF) in a file called **`arf.xml`**.
    - It is recommended to use this option instead of **`--results`** when dealing with datastreams. This is because **`--results`** will write XCCDF results into the FILE.
  - **`--report`** `FILE`
    - Write HTML report into FILE. You also have to specify a **`--results/--results-arf`** for this feature to work.

    `/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml`
    - This is the `INPUT_FILE` needed to perform the evaluation.
    - Print result of each rule to standard output, including rule title, rule id and security identifier(CVE, CCE).

IMPORTANT NOTE:

The **ssg-rhel7-ds.xml** file which is **Source DataStream** with **XCCDF 1.2** built inside. The advantage of **Source DataStream** is that you have everything you need bundled in one file - **XCCDF**, **OVAL**(s), **CPE**(s), and it supports digital signatures.

The evaluation process usually takes a few minutes, depending on the number of selected rules. Similarly to **SCAP Workbench**, **`oscap`** will also provide you an overview of results after it's finished, and you will find reports saved and available for review in your current working directory.

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

```
[root@serverX ~]# oscap xccdf eval --profile
xccdf_org.ssgproject.content_profile_rht-ccp --results-arf arf.xml --report
report.html /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Title   Ensure /tmp Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_tmp
Ident   CCE-27173-4
Result  fail

Title   Ensure /var Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_var
Ident   CCE-26404-4
Result  fail

Title   Ensure /var/log Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_var_log
Ident   CCE-26967-0
Result  fail

Title   Ensure /var/log/audit Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_var_log_audit
Ident   CCE-26971-2
Result  fail

Title   Ensure Red Hat GPG Key Installed
Rule    xccdf_org.ssgproject.content_rule_ensure_redhat_gpgkey_installed
Ident   CCE-26957-1
Result  pass
Title   Ensure gpgcheck Enabled In Main Yum Configuration
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Ident   CCE-26989-4
Result  pass
```

You can now perform a local SCAP compliance scan and generate reports using the command line.

- You can now review the report by opening the file with `firefox`

```
[root@serverX ~]# firefox report.html
```

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Red Hat Enterprise Linux 7

with profile Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7 formatted in the eXtensible Configuration Checklist Description Format (XCCDF).

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG for Red Hat Enterprise Linux 7 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	1up.rdu.redhat.com
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_org.ssgproject.content_profile_rht-ccp
Started at	2016-06-12T12:41:09
Finished at	2016-06-12T12:41:16
Performed by	rprice

CPE Platforms

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

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.1.58
- IPv4 172.17.42.1
- IPv4 10.10.10.1
- IPv4 192.168.100.1
- IPv4 10.3.225.21
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:124a:7dff:fea1:24df
- MAC 00:00:00:00:00:00
- MAC 10:4A:7D:A1:24:DF
- MAC 56:84:7A:FE:97:99
- MAC 52:54:00:90:6D:7C
- MAC 52:54:00:EA:30:83

Compliance and Scoring

The target system did not satisfy the conditions of 26 rules! Furthermore, the results of 10 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

32 passed | 26 failed | 11 other

Severity of failed rules

12 low | 12 medium | 2 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	37.615738	100.000000	37.62%

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

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

OPENSCAP CLI LAB: ONLINE REMEDIATION

- Online remediation executes fix elements at the time of scanning. Evaluation and remediation are performed as a part of a single command.
- To enable online remediation, use the `--remediate` command-line option

```
[root@serverX ~]# oscap xccdf eval --remediate --profile
xccdf_org.ssgproject.content_profile_rht-ccp --results scan-xccdf-results.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

The output of this command consists of two sections. The first section shows the result of the scan prior to the remediation, and the second section shows the result of the scan after applying the remediation. The second part can contain only fixed and error results. The fixed result indicates that the scan performed after the remediation passed. The error result indicates that even after applying the remediation, the evaluation still does not pass.

OPENSCAP CLI LAB: OFFLINE REMEDIATION (OPTIONAL)

- Offline remediation allows you to postpone fix execution. In next step, the system is only evaluated, and the results are stored in a **TestResult** element in an **XCCDF** file.

```
[root@serverX ~]# oscap xccdf eval --profile
xccdf_org.ssgproject.content_profile_rht-ccp --results scan-xccdf-results.xml
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

- In this next step, `oscap` executes the fix scripts and verifies the result. It is safe to store the results into the **INPUT FILE**, no data will be lost.

```
[root@serverX ~]# oscap xccdf remediate --results remediation-results.xml scan-
xccdf-results.xml
```

During offline remediation, a new **TestResult** element is created that is based on the input one and inherits all the data. The newly created **TestResult** differs only in the rule-result elements that have failed. For those, remediation is executed.

OPENSCAP CLI LAB: REMEDIATION REVIEW (OPTIONAL)

- The review mode allows users to store remediation instructions to a file for further review. The remediation content is not executed during this operation.
- To generate remediation instructions in the form of a shell script, run:

```
[root@serverX ~]# oscap xccdf generate fix --template urn:xccdf:fix:script:sh
--profile xccdf_org.ssgproject.content_profile_rht-ccp --output my-remediation-
script.sh /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

- Review the remediation script with your editor of choice. You can take the shell script and use with your configuration manager of choice.

```
[root@serverX ~]# gedit my-remediation-script.sh
```

Practical OpenSCAP, Security Standard Compliance and Reporting

Part 1: CLI (command-line)

OPENSCAP CLI LAB: VULNERABILITY SCANNING (HOMEWORK)

The **Red Hat Security Response Team** provides **OVAL** definitions for all vulnerabilities(identified by **CVE** name) that affect **Red Hat Enterprise Linux 3, 4, 5, 6, and 7**. This enable users to perform a vulnerability scan and diagnose whether a system is vulnerable or not.

- Download the content from Red Hat.

```
[root@serverX ~]# wget
http://www.redhat.com/security/data/metrics/com.redhat.rhsa-all.xccdf.xml
[root@serverX ~]# wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-
all.xml
```

- Run the scan

```
[root@serverX ~]# oscap xccdf eval --results results.xml --report report.html
com.redhat.rhsa-all.xccdf.xml
```

This will take several minutes to complete.

- This is sample output. It reports that **`Red Hat Security Advisor (RHS-2015:1090)`** was issued but the update has not been applied – this means the system is affected by multiple **`CVE's (CVE-2015-1863, CVE-2015-4142)`**. Your output may be similar - but not exactly the same.

```
...
Title   RHSA-2015:1090: wpa_supplicant security and enhancement update (Important)
Rule    oval-com.redhat.rhsa-def-20151090
Ident   CVE-2015-1863
Ident   CVE-2015-4142
Result  pass
...
```

- You can now review the report by opening the file with `firefox`.

```
[root@serverX ~]# firefox report.html
```