



Compliance for Containers using SCAP Content

Watson Sato
Software Engineer

Gabriel Alford
Technical Account Manager

2018.01.26

SCAP

Security Content Automation Protocol

NIST Certified SCAP scanners

- IBM Big Fix Compliance
- Nexpose
- OpenSCAP
- Qualys
- SCAP Compliance Checker (SCC)
- Security Center (Nessus)
- Secutor Compliance Automation Toolkit



nexpose



OpenSCAP



Nessus
vulnerability scanner

Source: <https://nvd.nist.gov/scap/validated-tools>

AGENDA

- Scope
- Scanning containers
- Remediating containers
- Challenges
- Future Plans
- Q&A

Scope

- OpenSCAP tools to scan and remediate containers
- Use existing SCAP content
- Differences between scan/remediate machine and container
- Not in Scope
 - SCAP standard
 - Write SCAP content

Scanning Containers

Workflow

- SCAP Scanner - OpenSCAP
- SCAP Content
 - CVE Feed - Linux distribution
 - Policy or Standard - SCAP Security Guide (SSG)
- Containers

Scanning Containers

Tools

- `oscap-docker`
 - Wrapper on openscap scanner
- `atomic scan`
 - openscap scanner container
 - Based on openscap-daemon

Types of scan

- Known vulnerabilities
- Configuration compliance

Scanning Containers

oscap-docker

- Mounts and scan the container image filesystem
- Offline scan
- Where to get it?
 - openscap-containers package
- Usage examples
 - Scan for known vulnerabilities in RHEL7 image
 - Scan for compliance of Fedora against Common Baseline

oscap-docker - known vulnerabilities

```
oscap-docker image-cve <image>
```

```
$ sudo oscap-docker image-cve  
registry.access.redhat.com/rhel7
```

```
Definition oval:com.redhat.rhsa:def:20180061: false  
Definition oval:com.redhat.rhsa:def:20180029: false  
Definition oval:com.redhat.rhsa:def:20180023: false  
...  
Definition oval:com.redhat.rhsa:def:20173263: true
```

oscap-docker - known vulnerabilities

```
oscap-docker image <image> oval eval <cve_feed>
```

```
$ wget  
https://www.redhat.com/security/data/oval/Red_Hat_Enterprise_Linux_7.xml
```

```
$ sudo oscap-docker image  
registry.access.redhat.com/rhel7 oval eval  
./Red_Hat_Enterprise_Linux_7.xml
```

```
Definition oval:com.redhat.rhsa:def:20180061: false  
Definition oval:com.redhat.rhsa:def:20180029: false  
Definition oval:com.redhat.rhsa:def:20180023: false  
...  
Definition oval:com.redhat.rhsa:def:20173263: true
```

oscap-docker - configuration compliance

```
oscap-docker image <image> --profile <profile> <policy>
```

```
$sudo oscap-docker image docker.io/library/fedora \  
xccdf eval --profile common \  
/usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
```

```
Title    Verify and Correct File Permissions with RPM  
Rule  
xccdf_org.ssgproject.content_rule_rpm_verify_permissions  
Result   fail  
...
```

Scanning Containers

atomic scan

- Mounts and scans the container image filesystem
- Offline scan
- SCAP content already bundled within
- Where to get it?
 - `$ docker pull openscap/openscap`
 - `$ sudo atomic install openscap/openscap`
- Usage examples
 - Scan for known vulnerabilities in RHEL7 image
 - Scan for compliance of Fedora against Common Baseline

atomic scan - known vulnerabilities

atomic scan <image>

```
$sudo atomic scan registry.access.redhat.com/rhel7
```

```
...
```

```
registry.access.redhat.com/rhel7 (cf55adcfe21a6f2)
```

The following issues were found:

```
RHSA-2017:3263: curl security update (Moderate)
```

```
Severity: Moderate
```

```
RHSA ID: RHSA-2017:3263-01
```

```
RHSA URL: https://access.redhat.com/errata/RHSA-2017:3263
```

```
Associated CVEs:
```

```
    CVE ID: CVE-2017-1000257
```

```
    CVE URL:
```

```
https://access.redhat.com/security/cve/CVE-2017-1000257
```

Files associated with this scan are in
/var/lib/atomic/openscap/2018-01-16-15-41-51-995565.

atomic scan - configuration compliance

```
atomic scan --scan_type configuration_compliance  
--scanner_args profile=<profile> <image>
```

```
$sudo atomic scan --scan_type configuration_compliance  
--scanner_args profile=common docker.io/fedora
```

...

```
docker.io/fedora (422dc563ca3260a)
```

The following issues were found:

...

```
Verify and Correct File Permissions with RPM  
Severity: Low  
XCCDF result: fail
```

...

```
Files associated with this scan are in  
/var/lib/atomic/openscap/2018-01-16-15-38-59-952202.
```

Remediating Containers

Remediating Containers

Tools

- `atomic scan`
 - `--remediate` option

Types of scan

- Configuration compliance

Remediating Containers

`atomic scan --remediate`

- Performs scan of the image
- Uses SCAP Content bundled in image
- Builds fix script for failed Rules
- Generates a new image
- Original image remains the same
- Usage example:
 - Bring Fedora container into compliance with Common Baseline

atomic scan - remediate

```
atomic scan --scan_type configuration_compliance  
--scanner_args --remediate <image>
```

```
$ sudo atomic scan --scan_type configuration_compliance  
--scanner_args profile=common --remediate docker.io/fedora  
...
```

```
docker.io/fedora (422dc563ca3260a)
```

```
The following issues were found:
```

```
...  
    Verify and Correct File Permissions with RPM  
    Severity: Low  
    XCCDF result: fail  
...
```

```
Files associated with this scan are in  
/var/lib/atomic/openscap/2018-01-16-15-43-53-985028.
```

atomic scan - remediate

```
atomic scan --scan_type configuration_compliance  
--scanner_args --remediate <image>
```

...

Remediating target

422dc563ca3260ad9ef5c47a1c246f5065d7f177ce51f4dd208efd82967ff1
82.

...

Remediating rule 2/39:

'xccdf_org.ssgproject.content_rule_rpm_verify_permissions'

...

Successfully built 30429bccee47

Successfully built remediated image **30429bccee47** from
422dc563ca3260ad9ef5c47a1c246f5065d7f177ce51f4dd208efd82967ff1
82.

Challenges

Challenges

- Containers are an image and not a full instance operating system
- Writing SCAP content for containers
 - Physical vs Virtual vs Container

Rule	Physical	Virtual	Container
Service auditd Enabled	Applicable	Applicable	Not Applicable?
Set Minimum Password Length	Applicable	Applicable	Applicable?
Separate Partition for /tmp	Applicable	Applicable	Not Applicable?

Challenges

- Scanning of images is done in chrooted environment
 - Cannot check session environment variables
 - `$ env | grep $JBOSS_HOME`
 - Services may not exist
- Fixes to runtime environment do not make sense
 - Missing services
 - Missing commands

Future Plans

Future Plans

- Writing content for container infrastructure

Q&A



THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos