A Security State of Mind: Container Security

Chris Van Tuin
Chief Technologist, West
cvantuin@redhat.com
AGENDA

Why Linux Containers?
What are Linux Containers?
Container Security
OpenSCAP
THE NEED FOR SPEED
THE ACCELERATION OF APPLICATION DELIVERY FOR THE BUSINESS

HOW
- Waterfall
- Agile
- DevOps

WHAT
- Monolithic Apps
- N-tier Apps w/ Appservers
- Microservices w/ APIs

WHERE
- Physical Server
- VMs
- Containers

FASTER AND HIGHER QUALITY
THE PROBLEM: FRICTION

Need more apps and services faster to be ahead of competitors

Regulatory compliance and keeping infrastructure secure
APPLICATION DELIVERY VIA CONTAINERS

LINE OF BUSINESS

DEVELOPMENT

Increases business agility
Accelerates developer productivity
Scales to public cloud faster

OPERATIONS

SECURITY / COMPLIANCE
WHAT ARE LINUX CONTAINERS?

• Package Once Deploy Anywhere

• Containers provide lightweight isolation of process, network, filesystem spaces

• Docker builds on Linux containers, adds an API, image format, runtime, and a delivery and sharing model
BUILD, SHIP, RUN

Dockerfile
FROM fedora:latest
CMD echo "Hello"

Build
“docker build or commit”

Image
docker.io
Private Registry
Red Hat Certified

Ship
“docker push or pull <IMAGE_ID>”

Container
Physical, Virtual, Cloud

Run
“docker run <IMAGE_ID>”
TRADITIONAL OS VS CONTAINERS

Traditional OS

Containers

HARDWARE

HOST OS

LIBS

APP A

APP B

LIBS B

LIBS A

LIBS

CONTAINER

APP A

LIBS

CONTAINER

APP B

LIBS
UNDERLYING TECHNOLOGY

- Containers
- DOCKER CLI
- SYSTEMD
- Cgroups
- Namespaces
- SELinux
- RHEL Kernel
- Drivers
- Hardware (Intel, AMD) or Virtual Machine
IMAGE-BASED CONTAINERS WITH DOCKER TECHNOLOGY

- Docker container images have layers
- All image layers are read only
- When a container is run the topmost layer is read-write
CONTAINER SECURITY
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
TOP CURRENT CONTAINER CHALLENGES

What are the top three challenges your organization has experienced so far in its use of containers?

- Security: 53%
- Variable performance: 44%
- Integration with existing development tools and processes: 41%
- Management: 35%
- Lack of certification or digital structure: 35%
- Scalability: 32%
- Consistency (lack of standards): 31%
- Training and Education (lack of skills): 29%

*Based on 271 IT and Development respondents in an online survey among senior IT leaders in B2C, B2B, and NO*.

Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January 2015.
“Patch?
The servers are behind the firewall.”

- Anonymous (far too many to name), 2005 - …
“CONTAINERS DO NOT CONTAIN”

- Dan Walsh, Red Hat
RESOURCES NOT NAMESPACED

- Kernel keyring
- Kernel itself and modules
- Devices
- System time
- UIDs*
  - *RHEL 7.2 Tech Preview
  - *Kernel boot option, user_namespace.enable=1
CONTAINER SECURITY RISKS

- Kernel exploits
- Denial of Service attacks
- Container breakouts
- Poisoned images
- Compromised secrets
CONTAINER IMAGES
64% of official images in Docker Hub contain high priority security vulnerabilities

examples:
- ShellShock (bash)
- Heartbleed (OpenSSL)
- Poodle (OpenSSL)

SECURITY IMPLICATIONS

What's inside the container and where it comes from matters.
Compliance and Vulnerability Audits with OpenSCAP
National Institute of Standards and Technology

automating vulnerability management, security management, and compliance checking
# Common Vulnerability and Exposures (CVE)

## CVE-2015-5477

**Impact:** Important  
**Public:** 2015-07-28  
**CWE:** CWE-456 -> CWE-617  
**Bugzilla:** 1247361: CVE-2015-5477 bind: TKEY query handling flaw leading to denial of service  

### Details

A flaw was found in the way BIND handled requests for TKEY DNS resource records. A remote attacker could use this flaw to make named (functioning as an authoritative DNS server or a DNS resolver) exit unexpectedly with an assertion failure via a specially crafted DNS request packet.

Find out more about CVE-2015-5477 from the [MITRE CVE dictionary](https://cve.mitre.org) and [NIST NVD](https://nvd.nist.gov).
Set Password Minimum Length in login.defs
To specify password length requirements for new accounts, edit the file /etc/login.defs and add or correct the following lines:
PASS_MIN_LEN

The DoD requirement is 14. The FISMA requirement is 12. If a program consults /etc/login.defs and also another PAM module (such as pam_cracklib) during a password change operation, then the most restrictive must be satisfied. See PAM section for more information about enforcing password quality requirements.
OpenSCAP
Scan physical servers, virtual machines, docker images and containers for Compliance (CCEs) and known Vulnerabilities (CVEs)

Content
SCAP Security Guide for RHEL
CCE-27002-5
Set Password Minimum Length
CVE-2015-5477

Scan
OpenSCAP
FOREMAN

Reports
Compliance and Scoring
Rule result breakdown
Failed rules by severity breakdown
Score

CVE DATABASE
CVE-2015-5477
Impact: severe
Priority: 7.2
OpenSCAP Tools
USE CASE #1: Scan for Compliance

- Are password quality requirements set?
- Are obsolete services enabled, e.g. telnet?
- Is openssh properly configured?
- Is /tmp on a separate partition?
oscap xccdf eval --profile rht-ccp \\  
--report /var/www/html/report.html \\  
--results /var/www/html/results.html \\  
--cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml \ 
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
**OpenSCAP Evaluation Report**

**Evaluation Characteristics**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target machine</td>
<td>ose-master1.chrisvantuin.com</td>
</tr>
<tr>
<td>Benchmark URL</td>
<td>/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml</td>
</tr>
<tr>
<td>Profile ID</td>
<td>rhc-ccp</td>
</tr>
<tr>
<td>Started at</td>
<td>2015-07-31T14:56:59</td>
</tr>
<tr>
<td>Finished at</td>
<td>2015-07-31T14:57:17</td>
</tr>
<tr>
<td>Performed by</td>
<td>root</td>
</tr>
</tbody>
</table>

**CPE Platforms**

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

**Addresses**

- IPv4: 127.0.0.1, 172.16.205.216, 172.16.42.1, 172.16.43.1, 10.1.2.1
- IPv6: fe80::0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0, fe80::fe75c:0:29ff:fe75c:0:297
- MAC addresses: 6E-8E-C0:68:F2, 26:A6:54:0F:83:72
Compliance and Scoring

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

Rule result breakdown

- 34 passed
- 33 failed

Failed rules by severity breakdown

- 3 high
- 16 medium
- 14 low

Score

<table>
<thead>
<tr>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>48.935184</td>
<td>100.000000</td>
<td>48.94%</td>
</tr>
</tbody>
</table>
## REPORT

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Failure Count</th>
<th>Score</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verify Proper Storage and Existence of Password Hashes</strong></td>
<td>Prevent Log In to Accounts With Empty Password</td>
<td>1</td>
<td>high</td>
<td>fail</td>
</tr>
<tr>
<td></td>
<td>Verify All Account Password Hashes are Shadowed</td>
<td></td>
<td>medium</td>
<td>pass</td>
</tr>
<tr>
<td><strong>Set Password Expiration Parameters</strong></td>
<td>Set Password Minimum Length in login.defs</td>
<td>2</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td></td>
<td>Set Password Minimum Age</td>
<td></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td></td>
<td>Set Password Warning Age</td>
<td></td>
<td>low</td>
<td>pass</td>
</tr>
<tr>
<td><strong>Protect Accounts by Configuring PAM</strong></td>
<td></td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Set Password Quality Requirements</strong></td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Set Password Quality Requirements, if using pam_pwquality</strong></td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set Password Retry Prompts Permitted Per-Session</td>
<td></td>
<td></td>
<td>low</td>
<td>pass</td>
</tr>
<tr>
<td>Set Password Strength Minimum Digit Characters</td>
<td></td>
<td></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Strength Minimum Uppercase Characters</td>
<td></td>
<td></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Strength Minimum Special Characters</td>
<td></td>
<td></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Strength Minimum Lowercase Characters</td>
<td></td>
<td></td>
<td>low</td>
<td>fail</td>
</tr>
</tbody>
</table>
REMEDIATION

Set Password Strength Minimum Digit Characters

<table>
<thead>
<tr>
<th>Rule ID</th>
<th>accounts_password_pam_dcredit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>fail</td>
</tr>
<tr>
<td>Time</td>
<td>2015-07-31T14:57:17</td>
</tr>
<tr>
<td>Severity</td>
<td>low</td>
</tr>
<tr>
<td>Identifiers and References</td>
<td>CCE-27183-5</td>
</tr>
<tr>
<td></td>
<td>IA-5(b), IA-5(c), 194, 194, 71,</td>
</tr>
</tbody>
</table>

The `pam_pwquality` module’s `dcredit` parameter controls requirements for usage of digits in a password. When set to a negative number, any password will be required to contain that many digits. When set to a positive number, `pam_pwquality` will grant +1 additional length credit for each digit. Add `dcredit=-1` after `pam_pwquality.so` to require use of a digit in passwords.

**Remediation script:**

```
var_password_pam_dcredit="-1"
if grep -q "dcredit" /etc/pam.d/system-auth; then
    sed -i --follow-symlink "s/\(dcredit *= \*\)/\1$var_password_pam_dcredit/" /etc/pam.d/system-auth
else
    sed -i --follow-symlink "/pam_pwquality.so/ s/\(dcredit=.*/$var_password_pam_dcredit/" /etc/pam.d/system-auth
fi
```
USE CASE #2: Scan for Known Vulnerabilities

What RPMs need updating?

What is the criticality of the vulnerability?

What is the vulnerability?

What CVEs have and have not been addressed?
# obtain RHSA file from Red Hat for RHEL
wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml

# run Vulnerability scan

# view the Report
firefox /var/www/html/oval-report.html
# REPORT

## OVAL Results Generator Information

<table>
<thead>
<tr>
<th>Schema Version</th>
<th>Product Name</th>
<th>Product Version</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.10.1</td>
<td>cpe:/a:open-scap:oscap</td>
<td>2015-07-31</td>
<td>15:03:03</td>
<td></td>
</tr>
</tbody>
</table>

- #x: 6
- #✓: 2665
- #Error: 0
- #Unknown: 0
- #Other: 0

## OVAL Definition Generator Information

<table>
<thead>
<tr>
<th>Schema Version</th>
<th>Product Name</th>
<th>Product Version</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.10.1</td>
<td>Red Hat OVAL Patch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Definition Merger</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- #Definitions: 2671 Total
- #Tests: 23552
- #Objects: 2353
- #States: 4093
- #Variables: 0

## System Information

- **Host Name**: ose-master1.chrisvantuin.com
- **Operating System**: Linux
- **Operating System Version**: #1 SMP Fri May 15 21:38:46 EDT 2015
- **Architecture**: x86_64

**Interface Information**

- **Interface Name**: lo
- **IP Address**: 127.0.0.1
- **MAC Address**: 00:00:00:00:00:00
<table>
<thead>
<tr>
<th>ID</th>
<th>Result</th>
<th>Class</th>
<th>Reference ID</th>
<th>Title</th>
</tr>
</thead>
</table>
USE CASE #3: Containers

- Is the docker image compliant?
- Is the docker image patched?
- Is the docker container compliant?
- Is the docker container patched?
# install oscap-docker
yum install openscap-utils

# install docker
subscription-manager repos --enable=rhel-7-server-extras-rpms
subscription-manager repos --enable=rhel-7-server-optional-rpms
yum install openscap-scanner docker
systemctl stop firewalld.service
systemctl disable firewalld.service
systemctl start docker.service
systemctl enable docker.service

# get RHEL6.2 docker image
docker pull docker.io/richxsl/rhel6.2
# Compliance Scan
oscap-docker image docker.io/richxsl/rhel6.2 xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp \
    /usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml

# Vulnerability Scan on RHEL 6.2 image

# start a container named myrhel62
docker run --name myrhel62 -it docker.io/richxsl/rhel6.2 /bin/bash

# Compliance Scan
oscap-docker container myrhel62 xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp \
    /usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml

# Vulnerability Scan
Guide to the Secure Configuration of Fedora

Customization: (no customization)
Profile: Common Profile for General-Purpose Fedora Systems

Target: Local Machine

- Password Minimum Length: fail
- Password Minimum Age: fail
- Password Maximum Age: fail
- Password Warning Age: pass
OSCAP ANACONDA ADDON

LOCALIZATION

DATE & TIME
Europe/Prague timezone

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY PROFILE
Misconfiguration detected

SOFTWARE

INSTALLATION SOURCE
Closest mirror

SOFTWARE SELECTION
Custom software selected

Data stream: scap.org.open-scap_datastream_tst

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

https://fedorahosted.org/oscap-anaconda-addon
Without

**Compliance and Scoring**

The target system did not satisfy the conditions of 44 rules! Please review rule results and consider applying remediation.

<table>
<thead>
<tr>
<th>Rule results</th>
<th>37 passed</th>
<th>44 failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity of failed rules</td>
<td>1 low</td>
<td>0 medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score</th>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>urn.xwlfs/scoring.default</td>
<td>64.12/724</td>
<td>100.00/0000</td>
<td>84.12%</td>
</tr>
</tbody>
</table>

64%

With

**Compliance and Scoring**

The target system did not satisfy the conditions of 1 rules! Please review rule results and consider applying remediation.

<table>
<thead>
<tr>
<th>Rule results</th>
<th>72 passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity of failed rules</td>
<td>1 low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score</th>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>urn.xwlfs/scoring.default</td>
<td>98.95/00326</td>
<td>100.00/0000</td>
<td>98.95%</td>
</tr>
</tbody>
</table>

99%
## Compliance Reports

<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>scap1.local lan</td>
<td>5 days ago</td>
<td>13</td>
<td>11</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>scap2.local lan</td>
<td>5 days ago</td>
<td>13</td>
<td>11</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>scap2.local lan</td>
<td>5 days ago</td>
<td>13</td>
<td>11</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Displaying all 3 entries
CONTAINER BEST PRACTICES

- Only run container images from trusted parties
- Container apps should drop privileges
- Host operating system matters
- Apply kernel security fixes
- Do not disable selinux
- Examine container images for security flaws
<table>
<thead>
<tr>
<th>Best Practices</th>
<th>RHEL Security Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardening</td>
<td>SELinux</td>
</tr>
<tr>
<td>Audit Log</td>
<td>syslog / systemd-journald</td>
</tr>
<tr>
<td>Identity Management</td>
<td>RHEL IdM</td>
</tr>
<tr>
<td>Security Blog</td>
<td>securityblog.redhat.com</td>
</tr>
<tr>
<td>Three Pigs Coloring Book</td>
<td><a href="https://t.co/4KH6iSZZ2H">https://t.co/4KH6iSZZ2H</a></td>
</tr>
</tbody>
</table>
THANK YOU!

Chris Van Tuin
cvantuin@redhat.com