A Security State of Mind: Container Security

Chris Van Tuin
Chief Technologist, West
cvantuin@redhat.com
“Patch?
The servers are behind the firewall.”

- Anonymous (far too many to name), 2005 - …
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
“Only the Paranoid Survive”

- Andy Grove, 1998
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

LINE OF BUSINESS
- Need more apps and services faster to be ahead of competitors

SECURITY / COMPLIANCE
- Regulatory compliance and keeping infrastructure secure

DEVELOPMENT

OPERATIONS
APPLICATION DELIVERY VIA CONTAINERS

LINE OF BUSINESS

DEVELOPMENT

Increases business agility
Accelerates developer productivity
Scales to public cloud faster

OPERATIONS

SECURITY / COMPLIANCE
LINUX CONTAINERS
WHAT ARE LINUX CONTAINERS?

• Used to create containers for software applications / microservices

• 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
TRADITIONAL OS VS CONTAINERS

Traditional OS

Containers
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
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%

Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January 2015
THREE LITTLE PIGS
CONTAINER SECURITY

As explained by The Three Little Pigs (Credit: Dan Walsh & Máirín Duffy)

Once upon a time there were Three Little Pigs, who had different types of homes to choose from...
House = Physical Hosts
Duplex = Virtualization
Apartment = Containers with separation
Hostel = Services on same host
Park = SELinux Disabled
CONTAINER SECURITY
CONTAINERS DO NOT CONTAIN

Not All Resources Are Namespaced
RESOURCES NOT NAMESPACED

- UIDs
- Kernel keyring
- Kernel itself and modules
- Devices
- System time
CONTAINER SECURITY RISKS

- Kernel exploits
- Denial of Service attacks
- Container breakouts
- Poisoned images
- Compromised secrets
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
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

#include<stdio.h>
main()
{
    printf("Hello World");
}

public class HelloWorld {
    public static void main(String[] args) {
        System.out.println("Hello, World");
    }
}

var http = require('http');
var server = http.createServer(
    function (request, response) {
        response.writeHead(200, {
            "Content-Type": "text/plain"
        });
        response.end("Hello World\n");
    });
server.listen(8000);

$s = "hello world";
$s = $s/(\d{1,2})\(\d{1,2}\)$\(\d{4}\)$\(\d{2}\)$\(\d{2}\)$\(\d{2}\)
print $s.

<?php Print "Hello, World!"; ?>

# of critical, important and moderate vulnerabilities identified and fixed by Red Hat in RHEL 7 since GA

physical
virtual
private cloud
public cloud
VULNERABILITIES PER PACKAGE TOP 20 (2014)
Compliance and Vulnerability Audits with OpenSCAP
National Institute of Standards and Technology

automating vulnerability management, security management, and compliance checking
CVE-2015-5477

Impact: Important
Public: 2015-07-26
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

Reports
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-ccep \
--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

<table>
<thead>
<tr>
<th>Title</th>
<th>Rule</th>
<th>Ident</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Host-Based Authentication</td>
<td>disable_host_auth</td>
<td>CCE-26870-6</td>
<td>pass</td>
</tr>
<tr>
<td>Disable SSH Root Login</td>
<td>sshd_disable_root_login</td>
<td>CCE-26946-4</td>
<td>fail</td>
</tr>
<tr>
<td>Disable SSH Access via Empty Passwords</td>
<td>sshd_disable_empty_passwords</td>
<td>CCE-26864-9</td>
<td>fail</td>
</tr>
</tbody>
</table>
**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
- 1 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>Task</th>
<th>Severity</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Proper Storage and Existence of Password Hashes</td>
<td>1x fail</td>
<td>fail</td>
</tr>
<tr>
<td>Prevent Log In to Accounts With Empty Password</td>
<td>high</td>
<td>fail</td>
</tr>
<tr>
<td>Verify All Account Password Hashes are Shadowed</td>
<td>medium</td>
<td>pass</td>
</tr>
<tr>
<td>Set Password Expiration Parameters</td>
<td>2x fail</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Minimum Length in login.defs</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Minimum Age</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Warning Age</td>
<td>low</td>
<td>pass</td>
</tr>
<tr>
<td>Protect Accounts by Configuring PAM</td>
<td>10x fail</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Quality Requirements</td>
<td>5x fail</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Quality Requirements, if using pam_pwquality</td>
<td>6x fail</td>
<td>pass</td>
</tr>
<tr>
<td>Set Password Retry Prompts Permitted Per-Session</td>
<td>low</td>
<td>pass</td>
</tr>
<tr>
<td>Set Password Strength Minimum Digit Characters</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Strength Minimum Uppercase Characters</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Strength Minimum Special Characters</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Set Password Strength Minimum Lowercase Characters</td>
<td>low</td>
<td>fail</td>
</tr>
</tbody>
</table>
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>
</tbody>
</table>

Identifiers and References
- **Identifiers**: CCE-27163-5
- **References**: IA-5(b), IA-5(c), 194, 194, 71

The pam_pwhash 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_pwhash will grant +1 additional length credit for each digit. Add dcredit=-1 after pam_pwhash.so so that 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_pwhash.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?
## Important: bind security update

**Advisory:** RHSA-2015:1443-1  
**Type:** Security Advisory  
**Severity:** Important  
**Issued on:** 2015-07-20  
**Last updated on:** 2015-07-20  
**Affected Products:** Red Hat Enterprise Linux Desktop (v. 7)  
**CVEs:** [cve.mitre.org](http://cve.mitre.org)  

### Updated packages

**Red Hat Enterprise Linux Desktop (v. 7)**

- SRPMS:  
  - bind-9.9.4-18.el7 12.src.rpm  
  - MD5: 59b447db796

### Details

Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having Important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.
# BACKPORTING and FALSE POSITIVES

“Heartbleed” - openssl vulnerability

<table>
<thead>
<tr>
<th>Community “Upstream”</th>
<th>NOTIFICATION</th>
<th>IMPACT</th>
<th>REMEDIATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2014-0160</td>
<td>openssl-1.0.1 before 1.0.1g</td>
<td>openssl-1.0.1g</td>
<td></td>
</tr>
</tbody>
</table>

| Red Hat “Downstream” | RHSA-2014:0376-1 | RHEL 6 openssl-1.0.1e-15 through openssl-1.0.1e-16.el6_5.4 | openssl-1.0.1e-16.el6_5.7 with backport from openssl-1.0.1g |
# obtain RHSA file from Red Hat for RHEL
wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml

# run Vulnerability scan
oscap oval eval --results /var/www/html/rhsa-results-oval.xml
--report /var/www/html/oval-report.html com.redhat.rhsa-all.xml

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

Evaluation done.
**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></td>
<td>2015-07-31</td>
<td>15:03:03</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#x</th>
<th>#✓</th>
<th>#Error</th>
<th>#Unknown</th>
<th>#Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>2665</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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>3</td>
<td>2015-07-30</td>
<td>13:16:01</td>
</tr>
<tr>
<td></td>
<td>Definition Merger</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#Definitions</th>
<th>#Tests</th>
<th>#Objects</th>
<th>#States</th>
<th>#Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>2671 Total</td>
<td>23552</td>
<td>2353</td>
<td>4093</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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 container compliant?
- Is the docker image patched?
- Is the docker container patched?
# install oscap-docker
wget https://raw.githubusercontent.com/OpenSCAP/container-compliance/master/oscap-docker
chmod 755 oscap-docker

# 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
```
```

---

DOCKER IMAGES ("offline")

---

DOCKER CONTAINERS ("online")
# Customize Profiles

**scap-workbench**

<table>
<thead>
<tr>
<th>Title</th>
<th>Guide to the Secure Configuration of Fedora</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customization</td>
<td>(no customization)</td>
</tr>
<tr>
<td>Profile</td>
<td>Common Profile for General-Purpose Fedora Systems</td>
</tr>
<tr>
<td>Target</td>
<td>Local Machine</td>
</tr>
</tbody>
</table>

- **Password Minimum Length**: fail
- **Password Minimum Age**: fail
- **Password Maximum Age**: fail
- **Password Warning Age**: pass
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
| RESOURCES |  |
|-----------|  |
| **Best Practices** | **RHEL Security Guide** |
| **Hardening** | **SELinux** |
| **Audit Log** | **syslog / systemd-journald** |
| **Identity Management** | **RHEL IdM** |
| **Security Blog** | **securityblog.redhat.com** |
| **Three Pigs Coloring Book** | **https://t.co/4KH6iSZZ2H** |
THANK YOU!

Chris Van Tuin
cvantuin@redhat.com