OpenShift Security

SHAWN WELLS
Chief Information Security Officer
U.S. Public Sector

unclass: shawn@redhat.com
JWICS: sdwell2@nsa.ic.gov
(+1) 443-534-0130

45 MINUTES, 3 GOALS

1. Review OpenShift Security Framework

    - sVirt

    - MCS & Type Enforcement

2.

3.

45 MINUTES, 3 GOALS

1.   Review OpenShift Security Framework

   • sVirt

   • MCS & Type Enforcement

2. Review compliance tech + initiatives

   • Upstream: SCAP Security Guide (SSG)

   • Downstream: NSA SNAC Guides & STIGs

3.

45 MINUTES, 3 GOALS

1. Review OpenShift Security Framework

   - sVirt

   - MCS & Type Enforcement

2. Review compliance tech + initiatives

   - Upstream: SCAP Security Guide (SSG)

   - Downstream: NSA SNAC Guides & STIGs

3. SCAP Demo

   - OpenSCAP + SSG

   - C&A Document Generation

OpenShift Multi-tenancy

- Think of the gears as boxes, nodes as the truck

- We don't care what's inside the box, it's just cargo

OpenShift Multi-tenancy

OpenShift Multi-tenancy

system_u:system_r:svirt_t:s0:c379,c680   system_u:system_r:svirt_t:s0:c41,c368

RHEL

HYPERVISOR (RHEV, OpenStack, KVM...)

OpenShift Multi-tenancy

NSA C63 (aka NIAP) & Red Hat:
where we've been… and next stop

RHEL 3 CAPP/EAL3+

RHEL 4 CAPP/EAL4+

RHEL 5 LSPP/EAL4+

RHEL 6 OSPP/EAL4+

RHEL 7 GPOSPP
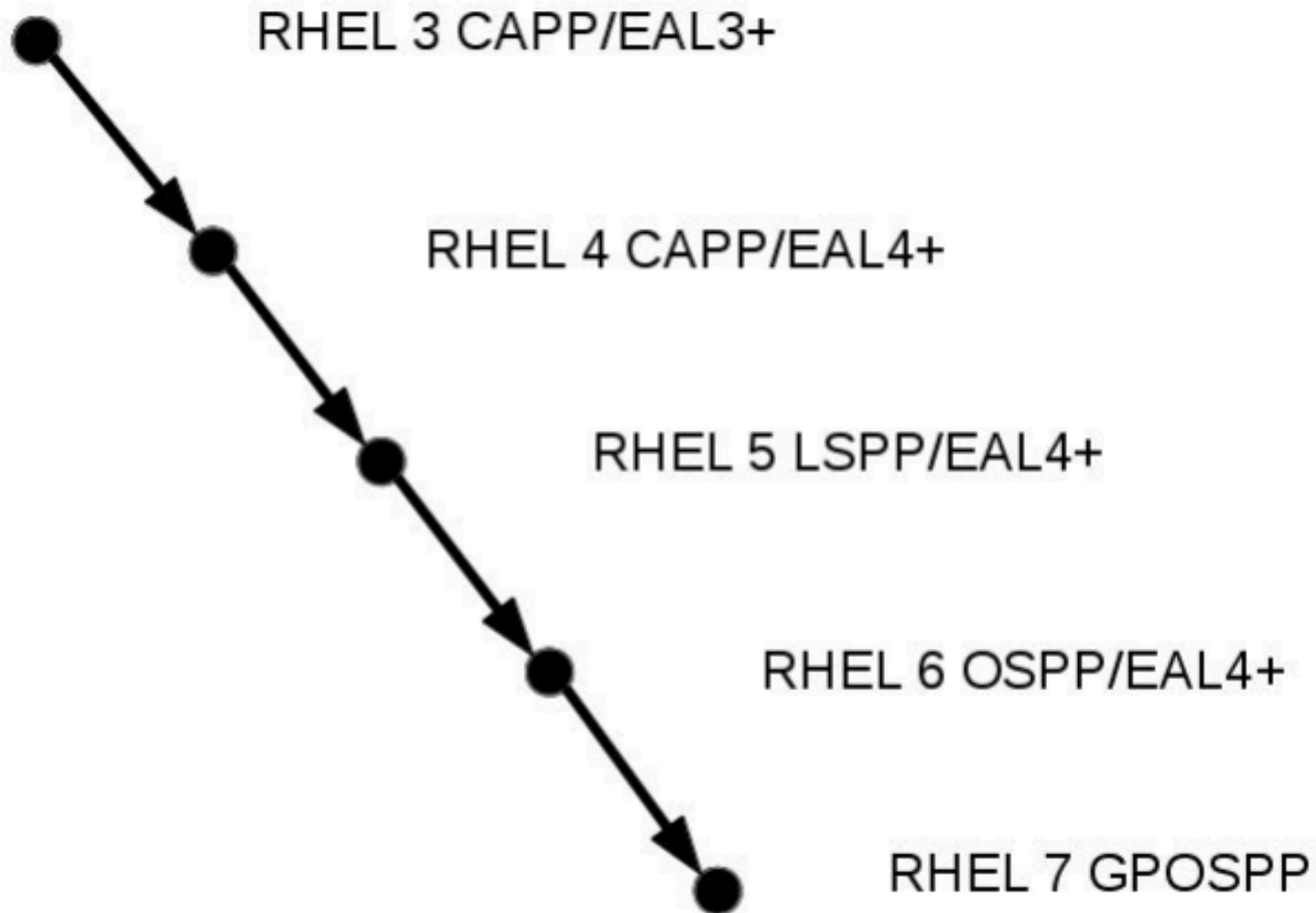
	Red Hat Enterprise Linux 6 with KVM	Red Hat Enterprise Linux 5.6 with KVM	IBM z/VM Version 5 Release 3 (for IBM System z Mainframes)	VMWare vSphere 5.0	VMWare ESXi 4.1	Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050
Certification Date	2012-10-08	2012-04-20	2008-08-06	2012-05-18	2010-12-15	2009-07-24
EAL Level	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+
CAPP	YES	YES	YES	NO	NO	NO
RBAC	YES	YES	NO	NO	NO	NO
LSPP	YES	YES	YES	NO	NO	NO

CAPP: Users control data access'
RBAC: Users classified into roles ("BackupAdm," "AuditAdm"…)
LSPP: Compartmentalizes users and applications from each other. Enables MLS.

RHEL meets GPOSPP

Requirements deficiencies
There are no missing requirements

Beta Programs + Customer Advisory Panels

Design deficiencies
There are no errors of design that lead to vulnerabilities

Coding defects
There are no implementation defects that create vulnerabilities

Operational guidance
The security features are well explained

Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems

Code physically secure
The code is kept in a SCC system with access limited to essential personnel

Code correctness
Discuss different classes of errors and how they are detected

Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective

Programmers are trained
The staff is trained and follows procedures

Independent third party code review
Code reviews were performed and defects corrected

Static analysis tools
All code is scanned and important defects are corrected

Test suite
Code exercised by test suite show no unexpected errors

Staff interviews

Procedures

Code Review Results

Analysis Tool Results

Test Results

12

RHEL meets GPOSPP

Requirements deficiencies
There are no missing requirements

Design deficiencies
There are no errors of design that lead to vulnerabilities

Coding defects
There are no implementation defects that create vulnerabilities

Operational guidance
The security features are well explained

FIPS Certs

Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems

Code physically secure
The code is kept in a SCC system with access limited to essential personnel

Code correctness
Discuss different classes of errors and how they are detected

Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective

Programmers are trained
The staff is trained and follows procedures

Independent third party code review
Code reviews were performed and defects corrected

Static analysis tools
All code is scanned and important defects are corrected

Test suite
Code exercised by test suite show no unexpected errors

Staff interviews

Procedures

Code Review Results

Analysis Tool Results

Test Results

13

```
RHEL meets GPOSPP
 ├── Requirements deficiencies
 │     There are no missing requirements
 ├── Design deficiencies
 │     There are no errors of design that lead to vulnerabilities
 ├── Coding defects
 │     There are no implementation defects that create vulnerabilities
 │        └── Prevention and detection
 │              Processes are in place, staff trained, runtime defenses mitigate latent problems
 │                ├── Code physically secure
 │                │     The code is kept in a SCC system with access limited to essential personnel
 │                │        └── Independent third party code review
 │                │              Code reviews were performed and defects corrected
 │                │                 └── Code Review Results
 │                ├── Code correctness
 │                │     Discuss different classes of errors and how they are detected
 │                │        ├── Static analysis tools
 │                │        │     All code is scanned and important defects are corrected
 │                │        │        └── Analysis Tool Results
 │                │        └── Test suite
 │                │              Code exercised by test suite show no unexpected errors
 │                │                 └── Test Results
 │                ├── Runtime protection
 │                │     The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
 │                └── Programmers are trained
 │                      The staff is trained and follows procedures
 │                        ├── Staff interviews
 │                        └── Procedures
 └── Operational guidance
       The security features are well explained
```

docs.redhat.com

14

15

Atsec

Common Criteria

!=

Compliance Policy

STIG

==

Compliance Policy

```
                    RHEL meets
                     GPOSPP

   Requirements      Design         Coding defects    Operational
   deficiencies      deficiencies   There are no      guidance
   There are no      There are no   implementation    The security features
   missing           errors of      defects that      are well explained
   requirements      design that    create
                     lead to        vulnerabilities
                     vulnerabilities

                    Prevention and
                     detection
                    Processes are in place,
                    staff trained, runtime
                    defenses mitigate latent
                    problems

   Code physically   Code correctness   Runtime protection   Programmers are
   secure            Discuss different  The use of stack     trained
   The code is kept  classes of errors  protector, FORTIFY   The staff is trained and
   in a SCC system   and how they are   SOURCE, RELRO, and   follows procedures
   with access       detected           kernel sysctls are
   limited to                           effective
   essential personnel

   Independent third  Static analysis tools  Test suite          Staff        Procedures
   party code review  All code is scanned    Code exercised by   interviews
   Code reviews were  and important defects  test suite show no
   performed and      are corrected          unexpected errors
   defects corrected

   Code              Analysis           Test
   Review            Tool               Results
   Results           Results
```

SCAP Security Guide Project (SSG)

19

SCAP Security Guide

In a Nutshell, SCAP Security Guide:

… has had 1,943 commits from 24 contributors, representing 164,355 lines of source

… took an estimated 43 years of effort (COCOMO model)

… has become upstream for DISA RHEL6 STIG, NIST NVD for JBoss EAP, NSA SNAC guide in progress

RHEL5 STIG Delay: 1,988 days

RHEL5 STIG Delay: 1,988 days

RHEL6 STIG Delay: 932 days

STIG Version 1, Release 2, Section 1.1:

"The consensus content was developed using an open source project called SCAP Security Guide. The project's website is https://fedorahosted.org/scap-security-guide/. Except for differences in formatting to accommodate the DISA STIG publising process, the content of the RHEL6 STIG should mirror the SCAP Security Guide content with only minor divergences as updates from multiple sources work through the consensus process"

AC-19(e)	Disable GNOME Automounting	The system's default desktop environment, GNOME, will mount devices and rem inserted into the system. Disable automount and autorun within GNOME by run

```
# gconftool-2 --direct \
        --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory
        --type bool \
        --set /apps/nautilus/preferences/media_automount false
# gconftool-2 --direct \
        --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory
        --type bool \
        --set /apps/nautilus/preferences/media_autorun_never true
```

These settings can be verified by running the following:

```
$ gconftool-2 --direct \
        --config-source xml:read:/etc/gconf/gconf.xml.mandatory \
        --get /apps/nautilus/preferences/media_automount
$ gconftool-2 --direct \
        --config-source xml:read:/etc/gconf/gconf.xml.mandatory \
        --get /apps/nautilus/preferences/media_autorun_never
```

CM-7	Disable Mounting of cramfs	To configure the system to prevent the `cramfs` kernel module from being loaded

```
install cramfs /bin/false
```

This effectively prevents usage of this uncommon filesystem.

CM-7	Disable Mounting of freevxfs	To configure the system to prevent the `freevxfs` kernel module from being load

```
install freevxfs /bin/false
```

This effectively prevents usage of this uncommon filesystem.

CM-7	Disable Mounting of jffs2	To configure the system to prevent the `jffs2` kernel module from being loaded,

```
install jffs2 /bin/false
```

This effectively prevents usage of this uncommon filesystem. **25**

SCAP Security Guide

- Guidance broken into profiles:

  - RHEL6 STIG

  - CS2 ⭐

  - NIST NVD (JBoss only)

oval:com.redhat.rhsa:def:20130744	true	patch	RHSA-2013:0744-01 CVE-2012-6537 CVE-2012-6538 CVE-2012-6546 CVE-2012-6547 CVE-2013-0349 CVE-2013-0913 CVE-2013-1767 CVE-2013-1773 CVE-2013-1774 CVE-2013-1792 CVE-2013-1796 CVE-2013-1797 CVE-2013-1798 CVE-2013-1826 CVE-2013-1827	RHSA-2013:0744: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20130898	false	patch	RHSA-2013:0898-00 CVE-2013-1993	RHSA-2013:0898: mesa security update (Moderate)
oval:com.redhat.rhsa:def:20130896	false	patch	RHSA-2013:0896-00 CVE-2013-2007	RHSA-2013:0896: qemu-kvm security and bug fix update (Moderate)

us

LOCALIZATION

DATE & TIME
Europe/Prague timezone

KEYBOARD
English (English (US))

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY PROFILE
Misconfiguration detected

SOFTWARE

INSTALLATION SOURCE
Closest mirror

NETWORK CONFIGURATION
Wired (eth0) connected

SOFTWARE SELECTION
Custom software selected

STORAGE

Done

⌨ us

Data stream: scap_org.open-scap_datastream_tst ⌄   Checklist: scap_org.open-scap_cref_first-xccdf.xml ⌄

Choose profile below:

My testing profile
A profile for testing purposes.

My testing profile2
Another profile for testing purposes.

Select profile

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

```
 1 this is a simple kickstart file for testing OSCAP addon's features
 2
 3 # values saving a lot of clicks in the GUI
 4 lang en US.UTF-8
 5 keyboard --xlayour=us --vckeymap=us
 6 timezone Europe/Prague
 7 rootpw aaaaa
 8 bootloader --location=mbr
 9 clearpart --initlabel --all
10 autopart --type=plain
11
12 %packages
13 vim
14 %end
15
16 %addon org_fedora_oscap
17         content-type = archive
18         content-url = http://192.168.122.1/xccdf_content.zip
19         profile = xccdf_com.stig-rhel6-server
20         xccdf-path = xccdf.xml
21 %end
```