
RED HAT
SUMMIT
LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.
June 11-14, 2013
Boston, MA
redhat.

Tackling Compliance with Red Hat

Jack Rieden – Sr. Manager, Software Engineering
Steve Grubb – Sr. Principal Engineer
Red Hat
June 12, 2013

Overview

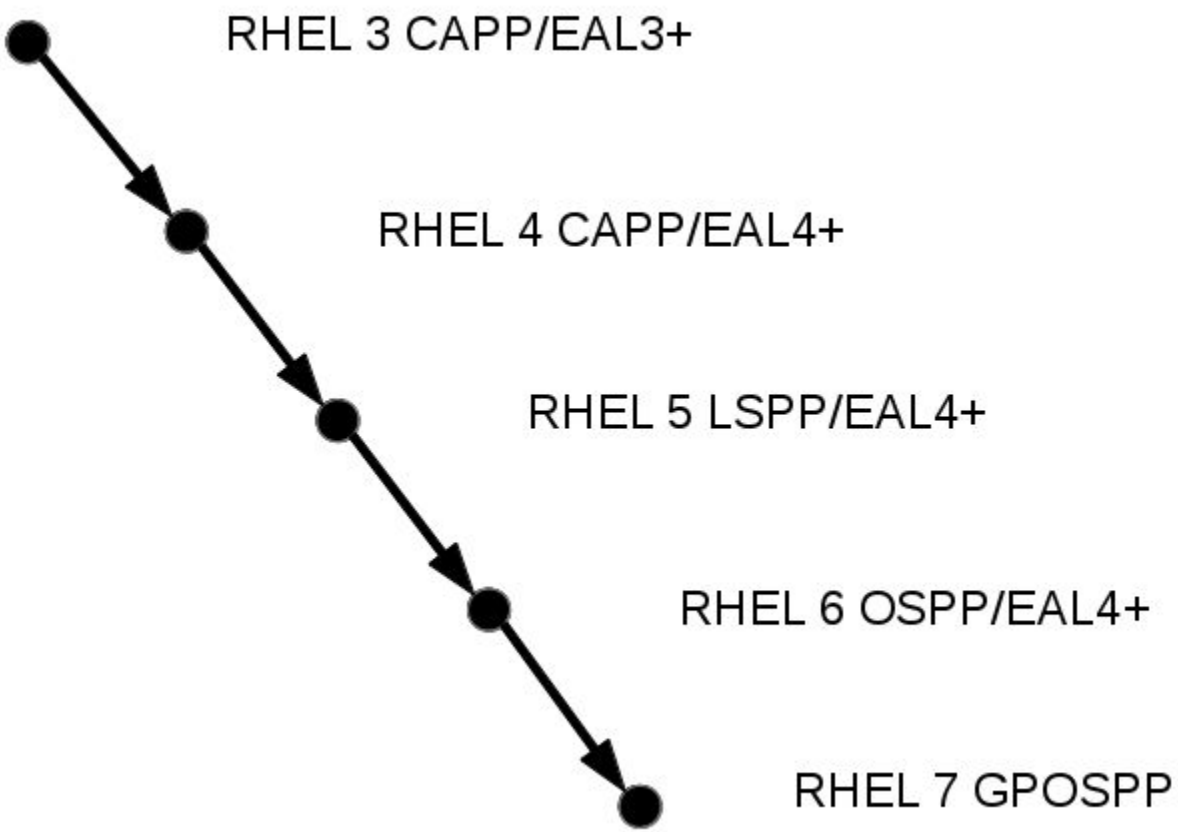
- Common Criteria
- FIPS 140
- Other Standards
- Participating in Standards
- Guidance
- Auditing of System Configuration


I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO I DO IT IN PRODUCTION
memegenerator.net

Common Criteria

- Choose Protection Profile
- Choose packages that form evaluated configuration
- Gap Analysis
- Open Bugzillas

Where we've been...and next stop



Select Packages for Evaluated Configuration

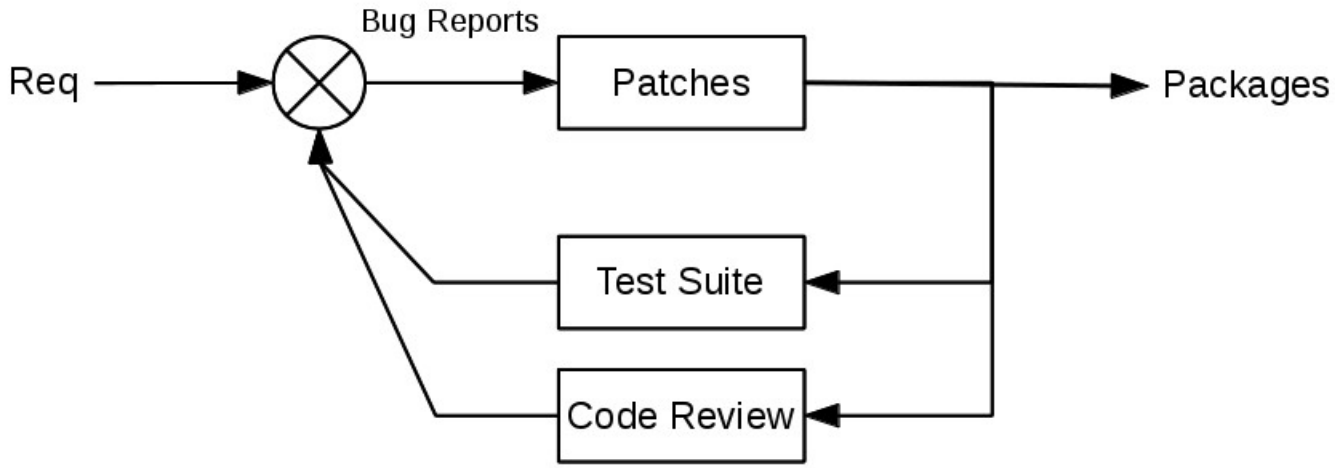
- Basic Rules
  - Minimal install
  - Add packages needed for test suite
  - Add common admin packages

- RHEL 7
  - Adding sssd
  - Openswan added to base PP

Gap Analysis (from around F18 beta)

- /sys/kernel/debug was world readable
- System won't boot in MLS mode
- Systemd networking support not MLS capable
- Polyinstantiated directories not working
- /dev/shm needs to be polyinstantiated
- In openswan, audit initialization of trusted channel
- Need typical sssd configuration
- Is sssd MLS capable?
- Tracker bz is 853068

The project

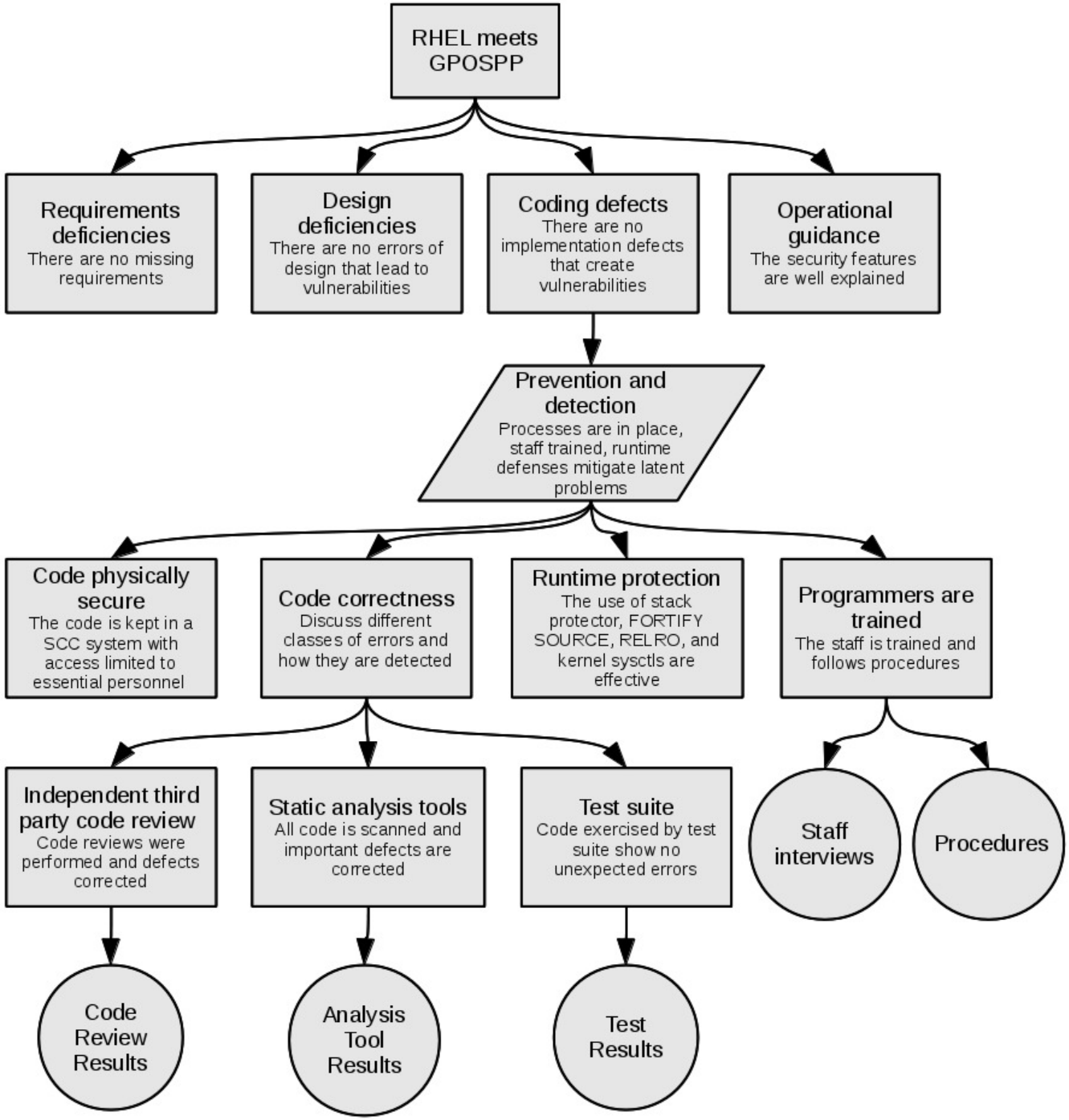


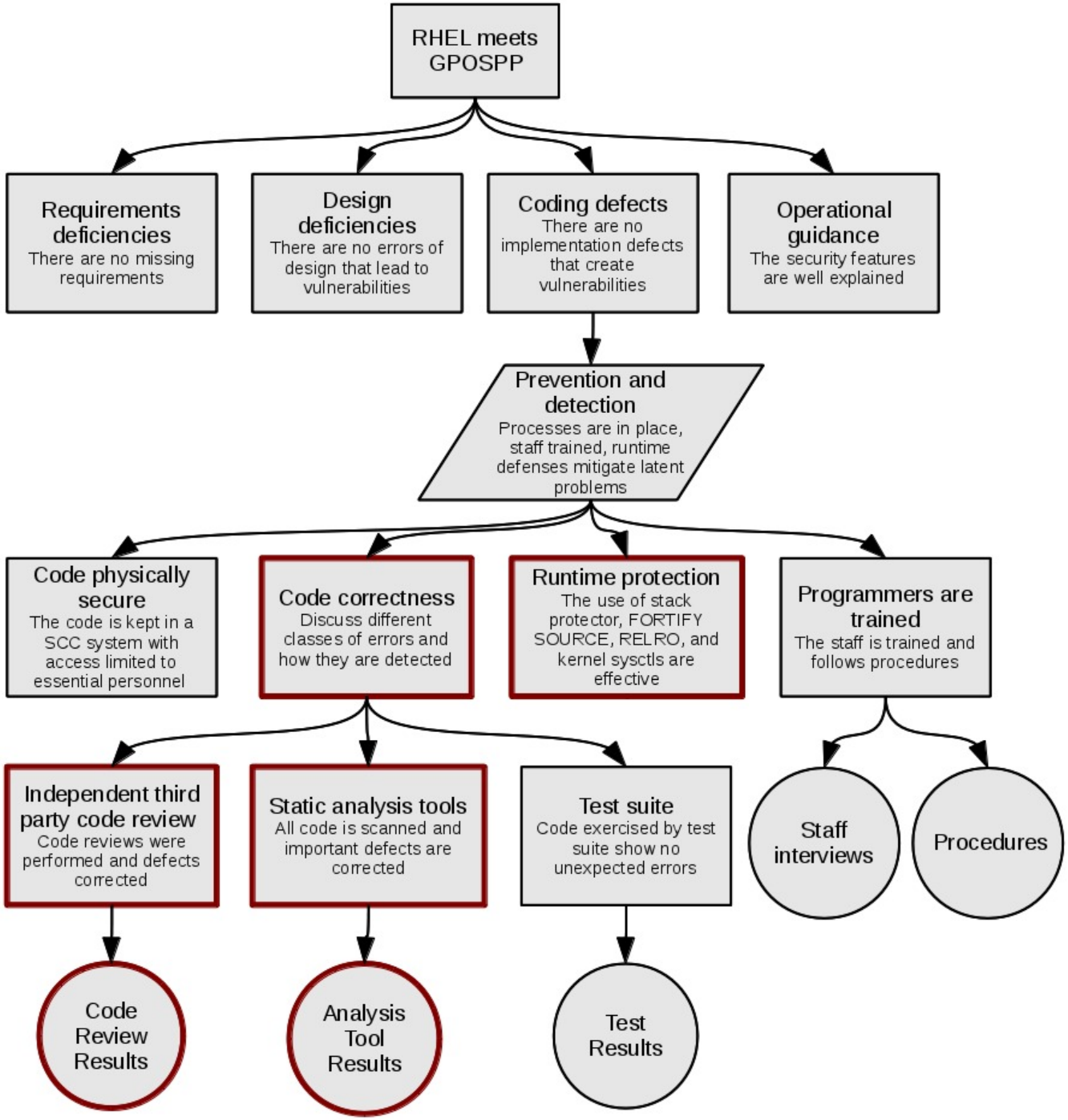
Common Criteria Objectives

- Assurance Argument
- Reduce Code Footprint
- Reduce Number of apps with privileges
- Code Review
- Protection Mechanisms
- Test Suite

Assurance Argument

- Goal of a Common Criteria Evaluation is to pass cert
- An argument must be put together to prove it
  - Top level claim supported by evidence
    - Should be true or false
  - Supported by argument
    - Broken up into subclaims
  - Subclaims have either more subclaims, arguments, or evidence
- The rigor of this argument is the Assurance Level (EAL)


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
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


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
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

Code reviews

```
/* Setup the master secret */
if ((ret = _gnutls_generate_master (session, 0), 0) < 0) {
      gnutls_assert ();
      return ret;
}
```

Static Analysis – early F19, absolute most

Package	total number reported
sblim-cmpi-samba-1.0-6.fc19	8252
kernel-3.7.0-0.rc6.git0.1.fc19	5400
gcc-4.7.2-8.fc19	5187
qt-4.8.3-8.fc19	4735
llvm-3.1-12.fc19	2870
webkitgtk3-1.10.1-1.fc18	2638
virtuoso-opensource-6.1.6-2.fc19	1920
kdelibs-4.9.3-2.fc19	1716
samba-4.0.0-168.fc19.rc5	1404
sane-backends-1.0.23-4.fc19	1206
mysql-5.5.28-1.fc18	1146
xulrunner-17.0-0.2.b6.fc19	1079
qemu-1.2.0-25.fc19	1037
thunderbird-16.0.1-2.fc19	997
kdepim-4.9.3-2.fc19	917

Static Analysis – early F19, most reported warnings

Warning	total number reported
RESOURCE_LEAK (CWE-404):	12374
UNINIT_CTOR (CWE-457):	10051
DELETE_ARRAY (CWE-459):	6910
FORWARD_NULL (CWE-476):	6830
CHECKED_RETURN (CWE-252):	4854
DEADCODE (CWE-561):	4475
UNINIT (CWE-457):	3350
SIZEOF_MISMATCH (CWE-569):	2998
UNUSED_VALUE (CWE-563):	2414
TAINTED_SCALAR (CWE-20):	2264
UNREACHABLE (CWE-561):	2001
ARRAY_VS_SINGLETON (CWE-119):	1974
CONSTANT_EXPRESSION_RESULT (CWE-569):	1862
STRING_OVERFLOW (CWE-120):	1773
NO_EFFECT (CWE-398):	1764

Static Analysis – early F19, most common warnings

Warning	Number of packages with one of these
FORWARD_NULL	351
CHECKED_RETURN	351
DEADCODE	331
RESOURCE_LEAK	330
UNINIT	306
CONSTANT_EXPRESSION_RESULT	280
REVERSE_INULL	224
UNUSED_VALUE	221
NEGATIVE_RETURNS	212
MISSING_BREAK	190
TOCTOU	184
NO_EFFECT	177
TAINTED_SCALAR	173
NULL_RETURNS	168
STRING_OVERFLOW	155

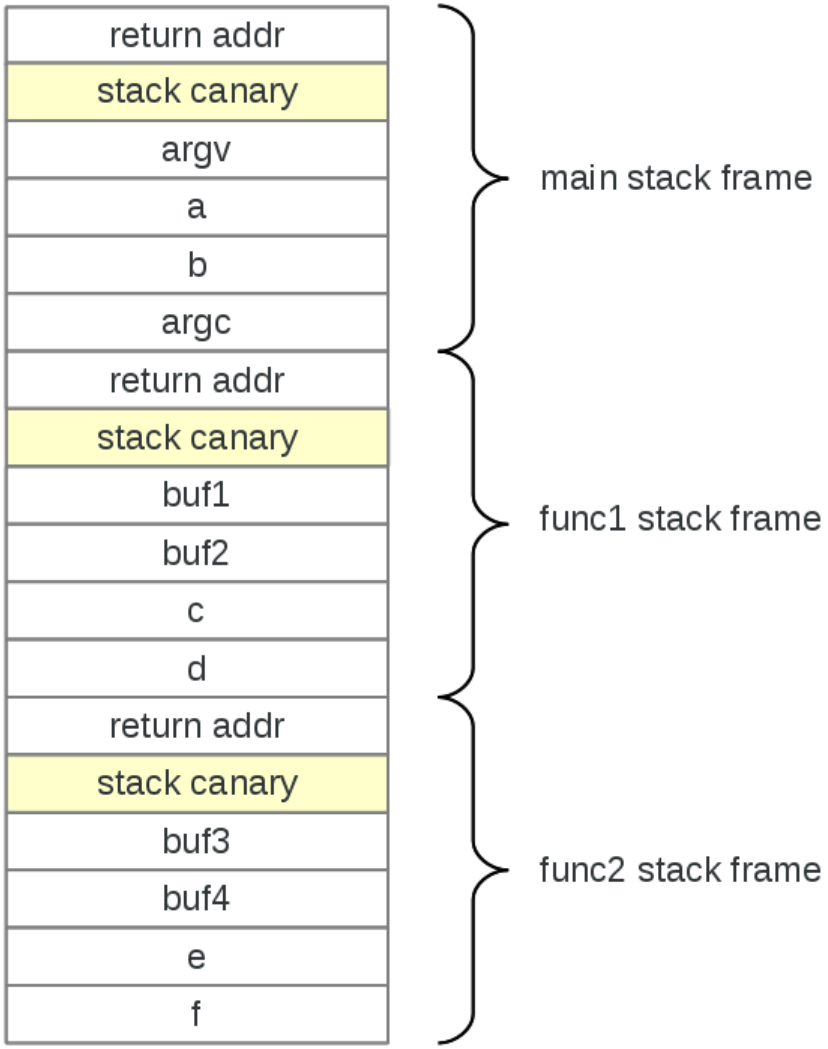
Static Analysis – early F19, rpm w/most of a specific warning

Warning	Number reported	Package
BAD_ALLOC_ARITHMETIC (CWE-119):	4	findutils-4.5.10-7.fc19
BAD_ALLOC_STRLEN (CWE-131):	2	openldap-2.4.33-3.fc19
BAD_FREE (CWE-590):	48	kernel-3.7.0-0.rc6.git0.1.fc19
CHROOT (CWE-243):	2	libarchive-3.0.4-3.fc19
CTOR_DTOR_LEAK (CWE-401):	31	clucene-2.3.3.4-7.fc18
DEADCODE (CWE-561):	486	kernel-3.7.0-0.rc6.git0.1.fc19
DELETE_ARRAY (CWE-459):	6896	sblim-cmpi-samba-1.0-6.fc19
FORWARD_NULL (CWE-476):	519	libguestfs-1.19.66-1.fc19
MISSING_BREAK (CWE-484):	368	kernel-3.7.0-0.rc6.git0.1.fc19
MISSING_LOCK (CWE-366):	59	openldap-2.4.33-3.fc19
NULL_RETURNS (CWE-476):	104	kernel-3.7.0-0.rc6.git0.1.fc19
ORDER_REVERSAL (CWE-557):	11	openldap-2.4.33-3.fc19
READLINK (CWE-170):	4	iscsi-initiator-utils-6.2.0.872-19.fc18
RESOURCE_LEAK (CWE-404):	3132	gcc-4.7.2-8.fc19
REVERSE_INULL (CWE-476):	107	kernel-3.7.0-0.rc6.git0.1.fc19
REVERSE_NEGATIVE (CWE-394):	15	sane-backends-1.0.23-4.fc19
STRAY_SEMICOLON (CWE-398):	20	libvpx-1.1.0-2.fc18
STRING_NULL (CWE-170):	110	mysql-5.5.28-1.fc18
STRING_SIZE (CWE-170):	84	fakechroot-2.9-27.fc18
TOCTOU (CWE-367):	28	evolution-data-server-3.7.1-1.fc19
UNCAUGHT_EXCEPT (CWE-248):	39	libconfig-1.4.9-1.fc19
UNINIT_CTOR (CWE-457):	2135	qt-4.8.3-8.fc19
UNREACHABLE (CWE-561):	829	gcc-4.7.2-8.fc19
USE_AFTER_FREE (CWE-416):	50	dbus-1.6.8-2.fc18
VARARGS (CWE-234):	58	virtuoso-opensource-6.1.6-2.fc19
WRAPPER_ESCAPE (CWE-416):	4	llvm-3.1-12.fc19

Stack Protector

- ASLR (PIE) alone is not enough – exec & DSO
- Gcc has built in stack protector
  - Add random number into call frame
  - Check on return
  - Abort program if its altered
  - Re-arrange the layout so less things get damaged on overflow
- Using it
- -fstack-protector or -fstack-protector-all
- --param=ssp-buffer-size=4

Stack Protector



Stack protector gotcha's

- alloca(3) not covered unless optimizations are used
- Many cases are NOT covered
  - Wide characters
  - Char arrays in structures / unions
  - Integer arrays
  - Access via pointer arithmetic

-fstack-protector-strong

- Similar to -stack-protector but includes:
  - Local array definitions
  - Passing references of local frame add
- In F19 gcc 4.8-6 and higher

  Comparison of function coverage:

	plain	strong	all
openssh	15%	34%	100%
openssl	4%	14%	100%
gnutls	11%	36%	100%
bind	14%	41%	100%
qemu	5%	19%	100%

Recommendations

- Daemon, setuid, network facing, parser of untrusted data
  - PIE, FULL RELRO, FORTIFY_SOURCE, -fstack-protector-strong, no executable stack, no executable memory
- Other apps
  - Partial RELRO, FORTIFY_SOURCE, -fstack-protector, no executable stacks, no executable memory

More info:

http ://people.redhat.com/sgrubb/swa

https ://www.youtube.com/watch?v=T4NadnbfYjY

FIPS-140

- For each RHEL major release
  - Look at SP 800-131 for changes
  - Enable as many algorithms as acceptable
  - Review key handling
  - Add/update self tests
  - New Security Policy

FIPS-140 Review key handling

- Keys are protected from disclosure
- Keys are derived by approved RNG
- Key generation method must take as many or more operations than determining the value of the key
- Keys are zeroized as soon as their use is no longer required

FIPS-140 Self Tests

- Failure of test causes module to enter error state
  - In error state, no crypto operations are permitted
  - No data output may occur in error state
- Power-up self tests must run when module instantianted
  - Automatic, no user intervention
  - Known answer test for all algorithms encrypt, decrypt,RNG
  - Software integrity test

FIPS-140 Self Tests

- Continuous tests
  - On power-up, a block of random numbers are read for later comparison
  - Each read will compare against last read to check for stuck answers. (Throwback to HW based crypto stuck latch.)

FIPS-140 Admin Advice

- Install dracut-fips and possibly dracut-fips-aesni
- Disable prelink - /etc/sysconfig/prelink
- Unprelink all files – prelink -u -a
- Add fips=1 to boot prompt
- Add boot=<device> if separate partition

Should just work

FIPS-140 Developer Advice

- Find the Security Policy (SP) for intended crypto module
- Initialize the library in accordance with SP
  - Do not start threads until library is initialized
- Follow all recommendations in the SP
- Follow key size recommendations in NIST SP 800-131
- RNG shall not be seeded with process ID or time
- Allow for cipher/hash/key size in configuration file

Other Standards

- SP 800-131 Transition Recommendations
- SP 800-53 Security Controls
- SP 800-90b RBG
- NISPOM
- PCI DSS
- Government Standards (Australia, Canada, Germany, UK)

Participating in Standards

- Protection Profiles
  - OSPP
  - GPOSPP
  - VPP
- DISA STIG
- SCAP
  - OVAL
  - CCE
  - CEE
- TCG
  - D-RTM
  - VTP
  - TNC
- USGCB
- CIS

Guidance

- CIS
- USGCB
- DISA STIG

Auditing of System Configuration

- data correlation is:
  - Mostly manual
  - Key word driven
  - Costly
  - Error prone
  - Pair-wise between data sets
  - Not scalable

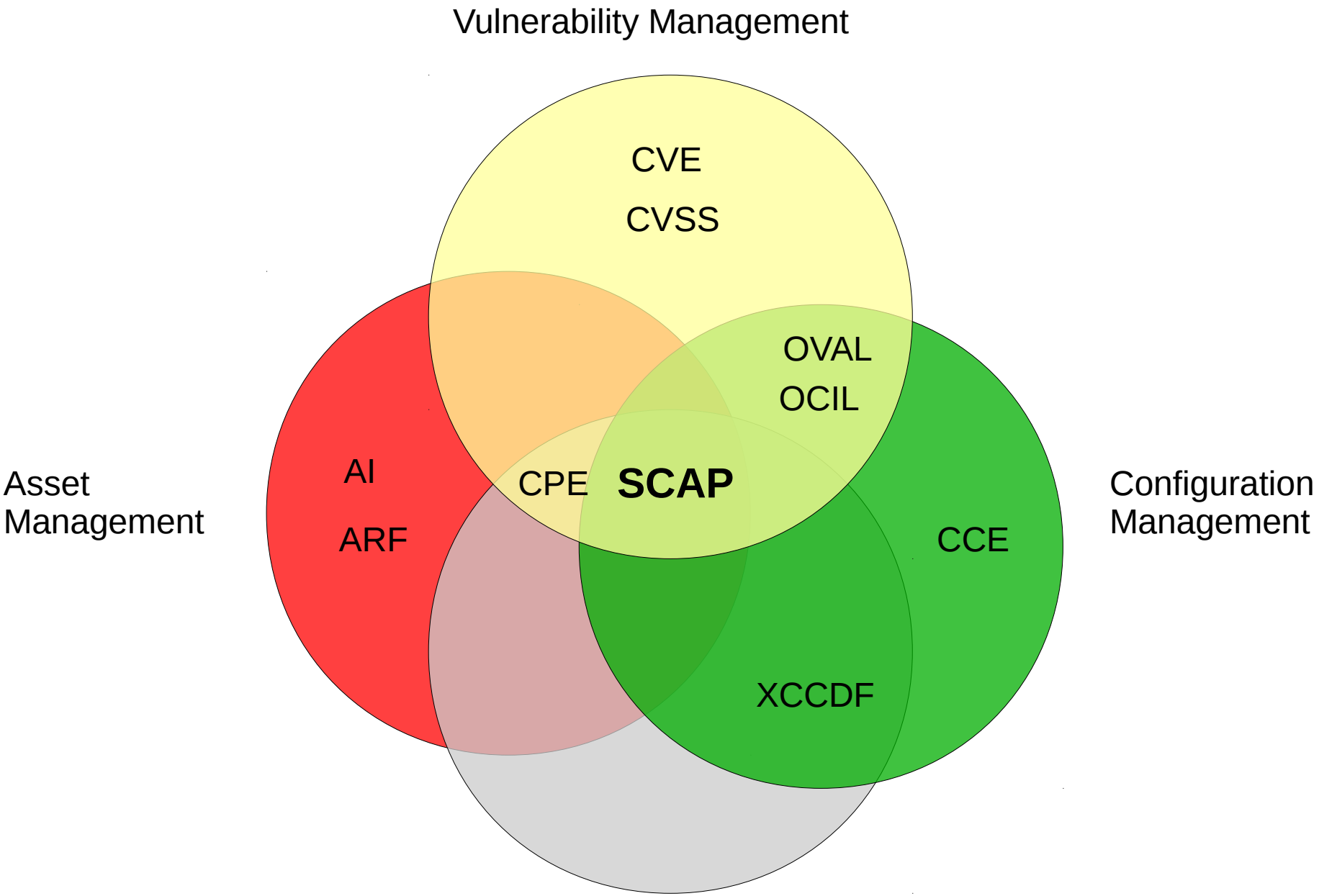
- result:
  - Data is locked in proprietary repositories

Auditing of System Configuration

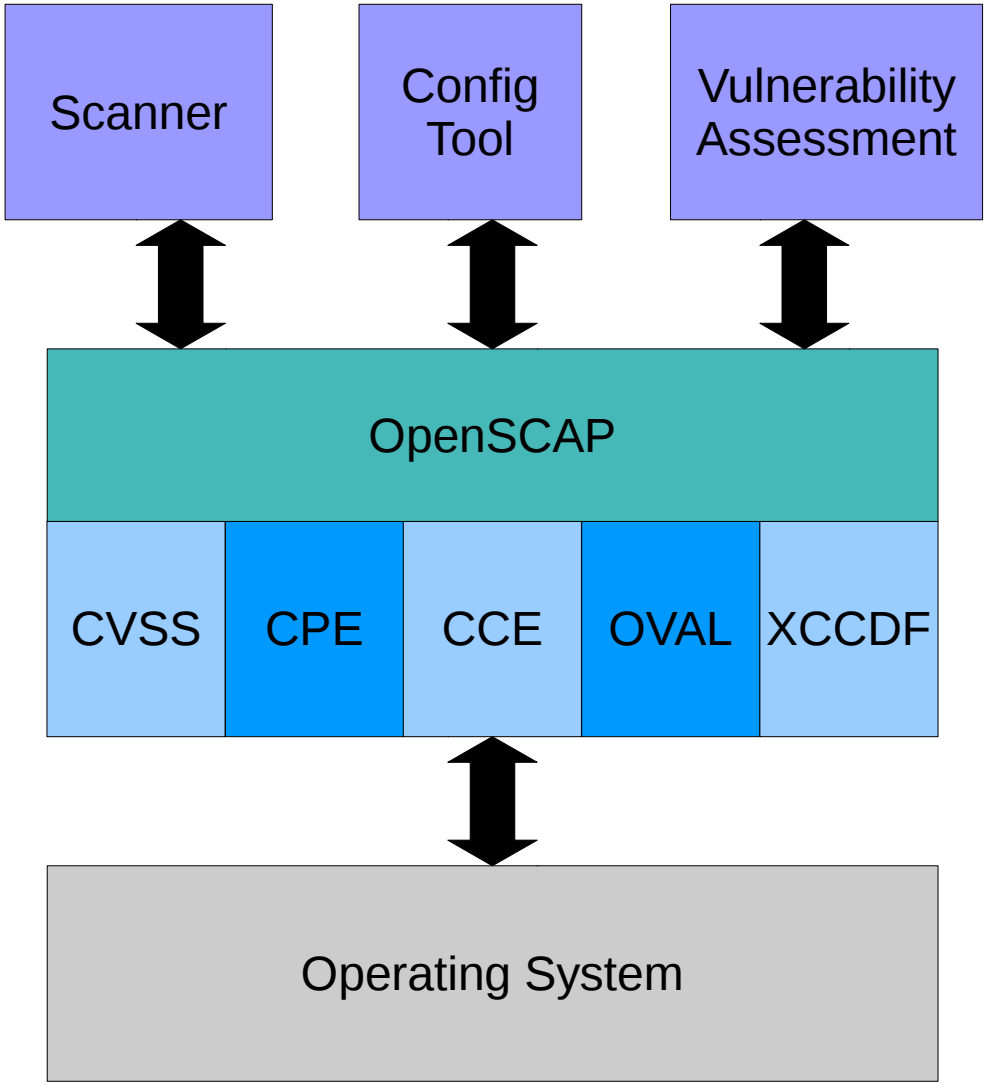
- common identifiers:
  - Community agree upon “tags”
  - Easily added to legacy repositories & tools

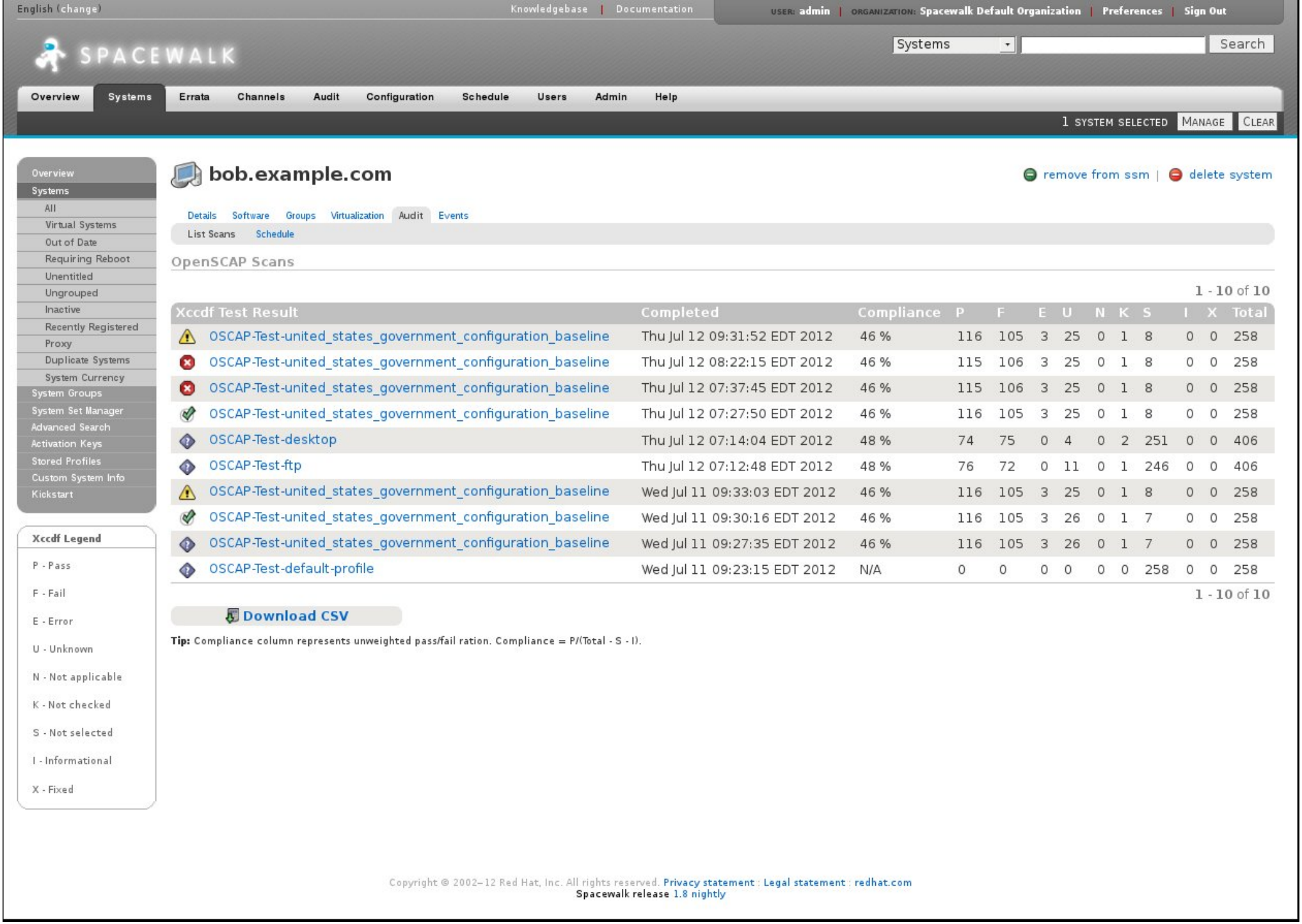
- KEY: common identification enables correlation!
  - Faster
  - More accurate
  - Less expensive

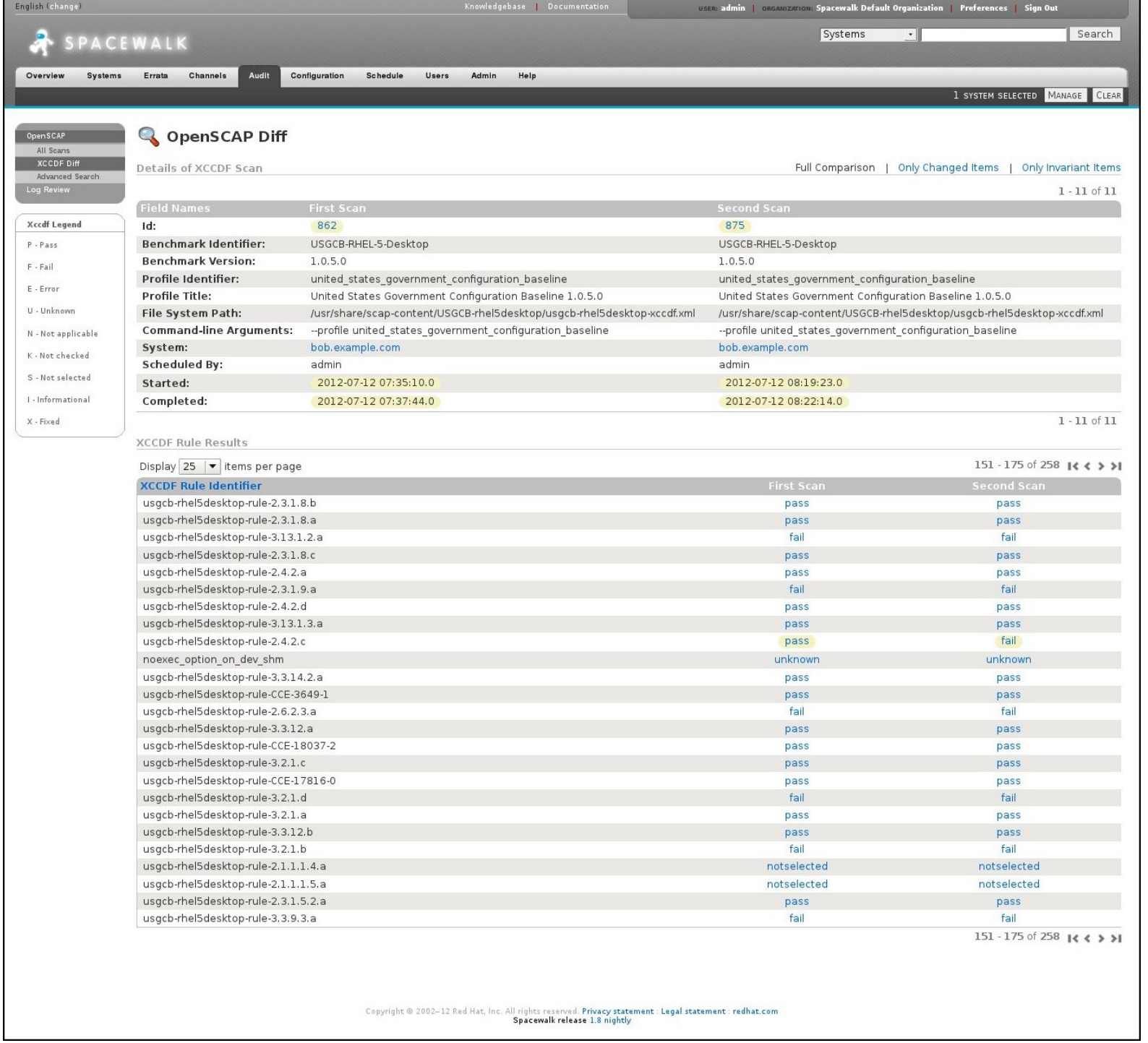
SCAP


Vulnerability Management
CVE
CVSS
OVAL
OCIL
AI
ARF
CPE
SCAP
CCE
XCCDF
Asset Management
Configuration Management
Compliance Management

OpenSCAP




English (change)
Knowledgebase | Documentation
USER: admin | ORGANIZATION: Spacewalk Default Organization | Preferences | Sign Out
SPACEWALK
Systems
Search
Overview
Systems
Errata
Channels
Audit
Configuration
Schedule
Users
Admin
Help
1 SYSTEM SELECTED
MANAGE
CLEAR
Overview
Systems
All
Virtual Systems
Out of Date
Requiring Reboot
Unentitled
Ungrouped
Inactive
Recently Registered
Proxy
Duplicate Systems
System Currency
System Groups
System Set Manager
Advanced Search
Activation Keys
Stored Profiles
Custom System Info
Kickstart
bob.example.com
remove from ssm | delete system
Details
Software
Groups
Virtualization
Audit
Events
List Scans
Schedule
OpenSCAP Scans
1 - 10 of 10
Xccdf Test Result
Completed
Compliance
P
F
E
U
N
K
S
I
X
Total
OSCAP-Test-united_states_government_configuration_baseline
Thu Jul 12 09:31:52 EDT 2012
46 %
116
105
3
25
0
1
8
0
0
258
OSCAP-Test-united_states_government_configuration_baseline
Thu Jul 12 08:22:15 EDT 2012
46 %
115
106
3
25
0
1
8
0
0
258
OSCAP-Test-united_states_government_configuration_baseline
Thu Jul 12 07:37:45 EDT 2012
46 %
115
106
3
25
0
1
8
0
0
258
OSCAP-Test-united_states_government_configuration_baseline
Thu Jul 12 07:27:50 EDT 2012
46 %
116
105
3
25
0
1
8
0
0
258
OSCAP-Test-desktop
Thu Jul 12 07:14:04 EDT 2012
48 %
74
75
0
4
0
2
251
0
0
406
OSCAP-Test-ftp
Thu Jul 12 07:12:48 EDT 2012
48 %
76
72
0
11
0
1
246
0
0
406
OSCAP-Test-united_states_government_configuration_baseline
Wed Jul 11 09:33:03 EDT 2012
46 %
116
105
3
25
0
1
8
0
0
258
OSCAP-Test-united_states_government_configuration_baseline
Wed Jul 11 09:30:16 EDT 2012
46 %
116
105
3
26
0
1
7
0
0
258
OSCAP-Test-united_states_government_configuration_baseline
Wed Jul 11 09:27:35 EDT 2012
46 %
116
105
3
26
0
1
7
0
0
258
OSCAP-Test-default-profile
Wed Jul 11 09:23:15 EDT 2012
N/A
0
0
0
0
0
0
258
0
0
258
1 - 10 of 10
Download CSV
Tip: Compliance column represents unweighted pass/fail ration. Compliance = P/(Total - S - I).
Xccdf Legend
P - Pass
F - Fail
E - Error
U - Unknown
N - Not applicable
K - Not checked
S - Not selected
I - Informational
X - Fixed
Copyright © 2002–12 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
Spacewalk release 1.8 nightly


English (change)
Knowledgebase | Documentation
USER: admin | ORGANIZATION: Spacewalk Default Organization | Preferences | Sign Out
SPACEWALK
Systems
Search
Overview Systems Errata Channels Audit Configuration Schedule Users Admin Help
1 SYSTEM SELECTED MANAGE CLEAR
OpenSCAP
All Scans
XCCDF Diff
Advanced Search
Log Review
Xccdf Legend
P - Pass
F - Fail
E - Error
U - Unknown
N - Not applicable
K - Not checked
S - Not selected
I - Informational
X - Fixed
OpenSCAP Diff
Details of XCCDF Scan
Full Comparison | Only Changed Items | Only Invariant Items
1 - 11 of 11
Field Names | First Scan | Second Scan
Id: | 862 | 875
Benchmark Identifier: | USGCB-RHEL-5-Desktop | USGCB-RHEL-5-Desktop
Benchmark Version: | 1.0.5.0 | 1.0.5.0
Profile Identifier: | united_states_government_configuration_baseline | united_states_government_configuration_baseline
Profile Title: | United States Government Configuration Baseline 1.0.5.0 | United States Government Configuration Baseline 1.0.5.0
File System Path: | /usr/share/scap-content/USGCB-rhel5desktop/usgcb-rhel5desktop-xccdf.xml | /usr/share/scap-content/USGCB-rhel5desktop/usgcb-rhel5desktop-xccdf.xml
Command-line Arguments: | --profile united_states_government_configuration_baseline | --profile united_states_government_configuration_baseline
System: | bob.example.com | bob.example.com
Scheduled By: | admin | admin
Started: | 2012-07-12 07:35:10.0 | 2012-07-12 08:19:23.0
Completed: | 2012-07-12 07:37:44.0 | 2012-07-12 08:22:14.0
1 - 11 of 11
XCCDF Rule Results
Display 25 items per page
151 - 175 of 258
XCCDF Rule Identifier | First Scan | Second Scan
usgcb-rhel5desktop-rule-2.3.1.8.b | pass | pass
usgcb-rhel5desktop-rule-2.3.1.8.a | pass | pass
usgcb-rhel5desktop-rule-3.13.1.2.a | fail | fail
usgcb-rhel5desktop-rule-2.3.1.8.c | pass | pass
usgcb-rhel5desktop-rule-2.4.2.a | pass | pass
usgcb-rhel5desktop-rule-2.3.1.9.a | fail | fail
usgcb-rhel5desktop-rule-2.4.2.d | pass | pass
usgcb-rhel5desktop-rule-3.13.1.3.a | pass | pass
usgcb-rhel5desktop-rule-2.4.2.c | pass | fail
noexec_option_on_dev_shm | unknown | unknown
usgcb-rhel5desktop-rule-3.3.14.2.a | pass | pass
usgcb-rhel5desktop-rule-CCE-3649-1 | pass | pass
usgcb-rhel5desktop-rule-2.6.2.3.a | fail | fail
usgcb-rhel5desktop-rule-3.3.12.a | pass | pass
usgcb-rhel5desktop-rule-CCE-18037-2 | pass | pass
usgcb-rhel5desktop-rule-3.2.1.c | pass | pass
usgcb-rhel5desktop-rule-CCE-17816-0 | pass | pass
usgcb-rhel5desktop-rule-3.2.1.d | fail | fail
usgcb-rhel5desktop-rule-3.2.1.a | pass | pass
usgcb-rhel5desktop-rule-3.3.12.b | pass | pass
usgcb-rhel5desktop-rule-3.2.1.b | fail | fail
usgcb-rhel5desktop-rule-2.1.1.1.4.a | notselected | notselected
usgcb-rhel5desktop-rule-2.1.1.1.5.a | notselected | notselected
usgcb-rhel5desktop-rule-2.3.1.5.2.a | pass | pass
usgcb-rhel5desktop-rule-3.3.9.3.a | fail | fail
151 - 175 of 258
Copyright © 2002–12 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
Spacewalk release 1.8 nightly

Questions?

sgrubb@redhat.com