Test Plan for RedHat Enterprise Linux version 6.2 Common Criteria Certification

Owner: Debora Velarde Babb (dvelarde@us.ibm.com)

IBM Linux Technology Center – Security
15400 SW Koll Pkwy
Beaverton, OR 97006

Table of Contents

Chapter 1 Document control information

1.1 Change History

Revision	Date	Author	Changes
0.1	12/02/10	Debora Babb	First draft based on Test Plan for RHEL version 5 CAPP EAL4, RBAC, and LSPP evaluation
0.2	02/22/11	Debora Babb	Addition of Chapter 12 Test environment setup. Updates to most sections.
0.3	05/02/11	Debora Babb	Modified reviewers. Removed references to RHEV-H. Modified chapters 6 and 7.
0.4	05/05/11	Debora Babb	Updates to test case descriptions. Added section 12.6. Changes to Chapter 13. Added Chapter 14 Known Errors place holder.
0.5	05/09/11	Debora Babb	Added chapter on Test Execution Modes. Removed chapter about additional packages needed for test. Added mention of OSPP and MLS to overview. Minor corrections.
0.6	09/22/11	Debora Babb	Changed from RHEL 6.1 to RHEL 6.2. Updated Reviewers. Removed references to 3rd 'catcher' system.
0.7	11/21/11	Debora Babb	Updates/additions to Chapter 9 test descriptions and Chapter 12 Test Execution.
0.8	11/29/11	Debora Babb	Added test matrix
0.9	12/14/11	Debora Babb	Updated test matrix. Added audit-remote to tests descriptions. Moved SGI to list of platforms claiming the virtualization extension.
0.1	12/21/11	Debora Babb	Removed detailed instructions; now point reader to README files included in audit-test suite.
1.0	2012-01-25	Stephan Müller	Fixing remaining issues

1.2 Reviewers

Name	Company
James Czyzak	IBM
Tony Ernst	SGI
Linda Knippers	HP

Eduard Benes	Red Hat

Chapter 2 Availability

2.1 Availability

This document is distributed as part of the Red Hat Enterprise Linux V 6.2 Common Criteria Evaluation test cases.

2.2 Completeness

Completeness of this document can be verified by checking the “Last Page” is marked.

2.3 Obsolete copies, retention, and disposition

It is your responsibility to ensure you have the most recent version of this document and to properly dispose of all obsolete copies.

2.4 Alternation and duplication

You may make copies of this document. You must contact the author to make changes to the document.

Chapter 3 Overview

3.1 Purpose

The purpose of the testing for this evaluation is to demonstrate the correct operation of security functions identified in the *Red Hat Enterprise Linux 6.2, Red Hat Enterprise Virtualization Hypervisor 6.2 Security Target* which includes compliance with the Operating System Protection Profile. The phrase "correct operation" is defined to include appropriate failures for unauthorized or invalid access to security functions.

3.2 Scope

The test cases identified in this test plan are limited to those areas that enforce the secure operation of Red Hat Enterprise Linux 6.2. Only features and functions contained in the *Security Target* are addressed. Test cases are designed to verify the correct operation of security related user programs,

databases, files, and system calls. Testing for system availability in a stress environment is beyond the scope of this plan.

Testing of alternate installation methods shall be covered by atsec.

Chapter 4 Environment

4.1 Software and hardware

Red Hat Enterprise Linux 6.2 Server will be tested. Additional software is listed in the "Installation of test environment" section of this document.

The configuration details will be provided by the *Evaluated Configuration Guide for Red Hat Enterprise Linux 6.2* in its current version. The machines must be installed according to the instructions in the *Evaluated Configuration Guide*, including required package updates. The setup of the test machines must conform strictly to the instructions and configuration details described in the *Evaluated Configuration Guide*.

4.1.1 Platforms

Final executions will be conducted on the following platforms:

- RHEL6.2 Server, 64 bit, IBM System p Power 750
- RHEL6.2 Server, 64 bit, IBM System x x3850X5 E7520
- RHEL6.2 Server, 64 bit, IBM System x x3620M3 E5620
- RHEL6.2 Server, 64 bit, IBM System z z10
- RHEL6.2 Server, 64 bit, SGI UV 1000
- RHEL6.2 Server, 64 bit, HP ProLiant DL360 G6 (Intel Xeon – base/capp testing), ProLiant DL360 G7 (Intel Xeon – mls/lspp testing), ProLiant DL385 G7 (AMD Opteron)
- RHEL6.2 Server, 64 bit, Dell PowerEdge R720

Although tests will not be run on a client configuration, since client packages are a subset of the server packages the client code can be considered tested.

Both 32-bit and 64-bit compilation and execution will be supported and tested on all platforms using the 64-bit kernel as listed above.

Testing will be done using the Symmetrical Multiprocessing (SMP) kernel on all platforms.

Virtualization testing will be conducted on the platforms that are listed as support virtualization in the ST (namely the Intel/AMD processor hardware).

4.1.2 Installation Mode

Each platform will be installed and tested in two modes:

- Base/CAPP mode

- MLS mode

4.1.3 Test Matrix

A summary of which test cases need to be run on the different platforms is provided in the following table. All tests must be executed in 64-bit mode. Tests which must also be run in 32-bit mode are indicated below. A description of the test cases is provided in Chapter 9.

Test Bucket	**All Platforms** **Base/CAPP mode**	**All Platforms** **MLS mode**	**Platforms claiming Virtualization extension must also run** **Base/CAPP mode**	**Platforms claiming Virtualization extension must also run** **MLS mode**
audit-remote	X	X		
audit-tools	X	X		
audit-trail-protection	X	X		
crypto	X	X		
fail-safe	X	X		
filter (64-bit)	X	X		
libpam	X	X		
kvm			X	X
kvm-cgroups			X	X
kvm-iommu			X	X
miscellaneous	X	X		
network	X	X		
netfilter-iptables	X	X		
netfilter-ebtables			X	X
syscalls (64-bit)	X	X		
syscalls (32-bit)	X	X		
trustedprograms	X	X		
LTP (64 bit)	X	X		
LTP (32 bit)	X	X		

4.1.4 Additional hardware

Additional hardware may include:

- a serial terminal or a PC with terminal emulation for some manual tests
- a chassis
- ethernet switches
- power modules

Chapter 5 Assumptions and dependencies

5.1 Assumptions

- The majority of the test cases will execute locally to the test target machine (for example, not as a remote client). Network testing will include executions utilizing a sending system and a receiving system, and also will include executions to localhost. SSL testing will also involve connections to a second system.
- Multiple test suites are not running concurrently on the same machine.
- The test cases have control of the execution environment. No other activity that changes system configuration can be performed simultaneously with the test cases.

5.2 Dependencies

- Completion and availability of the kickstart script and installation of the system according to the ECG.
- Availability of suitable hardware.
- Availability of all software described in the Target of Evaluation (TOE), including the audit subsystem and network packages.
- Availability of sufficient test personnel.
- Dependencies for tests are documented in README.run, README.netfilter

Chapter 6 Test approach and methodology

The purpose of the test effort is to verify RHEL6.2 Security Target compliance of RHEL6.2 and to perform some amount of Functional Verification Testing of the audit component.

The audit-test test suite (http://sourceforge.net/projects/audit-test/) was used and adapted as needed for execution on RHEL6.2. The test case developers will submit patches for any changes needed to the audit-test developer mailing list. A snapshot of audit-test will be created and used for final testing.

New tests will be written for areas not tested in previous evaluations. Those tests will be added to the audit-test suite whenever possible.

A subset of the ltp test suite will also be run.

Bug reports will be written where appropriate.

To count as an official run, all tests must be executed on the RHEL6.2 GA code plus any additional required packages with the proper configuration. Configuration details are provided by the *Evaluated Configuration Guide* included in the Evaluated Configuration rpm package.

The setup of the test machines must conform strictly to the instructions and configuration details described in the *Evaluated Configuration Guide*.

Manual testing is performed only when automated options are not available.

Chapter 7 Target of Evaluation Compliance

The additional packages required for the test environment are all permitted according to the *Evaluated Configuration Guide (ECG).* There are no configuration violations such as setuid and setgid binaries, daemons, startup scripts, or other prohibited changes. After installation of the test environment, the system remains compliant with the Target of Evaluation (TOE).

Chapter 8 Test execution modes

Testing will be run in two different modes: base and mls. Base mode uses the default SELinux policy in enforcing mode. MLS mode uses the MLS policy in enforcing mode.

During the postinstall phase the kickstart configuration script will prompt you to choose base or mls.

Changing from one mode to the other requires re-running the kickstart script to re-install and re-configure the system.

8.1 LTP tests

A subset of the Linux Test Project test cases will also be run. The Linux Test Project test suite is available from http://ltp.sourceforge.net. The following tests will be run:

- syscalls test cases (executed in both 64 bit and 32 bit)
- network/tcp_cmds/ping
- network/tcp_cmds/ssh
- network/tcp_cmds/host
- commands/su

Chapter 9 Installation of test environment

9.1 RedHat installation

The system must be installed with Red Hat Enterprise Linux 6.2 per the Evaluated Configuration Guide. A kickstart script is included in the Evaluated Configuration rpm file which can be used to

automate much of the installation process described in the Evaluated Configuration Guide. For instructions on how to install the operating system, refer to the *Evaluated Configuration Guide for Red Hat Enterprise Linux 6.2*.

9.2 Add a test user

An administrative user must be created. You will be prompted by the kickstart configuration script to create an administrative user (example: ealuser). In case ealuser is inadvertently deleted, below are instructions for its creation.

- On the console login as root.
- Create an administrator user:

```
useradd -m -c "ealuser" -G wheel ealuser
```

- Create a password for the user according to the password policy:

```
passwd ealuser
```

- Change the user password expiration information:

```
chage -m 1 -M 60 -W 7 ealuser
```

Chapter 10 Installation of testcases

10.1 Download test cases

Download the final audit-test suite with the following command:

git clone git://audit-test.git.sourceforge.net/gitroot/audit-test/audit-test

Download the LTP tarball from the following URL:

http://sourceforge.net/projects/ltp/files/LTP%20Source/ltp-20110915/ltp-full-20110915.bz2/download

10.2 Installation of test cases

The test cases need to be installed on both the TOE server and the Network Server.

For instructions on how to install the test cases, refer to the **audit-test/audit/README.run** file contained within the audit-test tarball.

Chapter 11 Test environment setup

The configuration for the networking, net filtering (iptables, ip6tables, and ebtables), audit-remote, and trustedprograms tests requires setting up IP addressing for two systems:

1. TOE
2. network server

The test cases should be installed on both the TOE and the network server. Instructions on how to install the TOE system are included in the **audit-test/audit/README.run** file. Instructions on how to install the network server are included in the **audit-test/audit/README.netwk_svr**.

11.1 Setup for netfilter test cases

Additional setup steps are needed in order to run the netfiltering iptables and ebtables test cases. For information on how to perform the required setup, refer to the audit-test/audit/README.netfilter.

11.2 Setup needed for KVM tests

The KVM tests will attempt to install guest virtual machine images. Therefore, an ISO image of an installation media that should be used to install the virtual machine environments is needed. Edit the **audit-test/kvm/config.bash** file and set the "install_media" configuration parameter to the path and file name of the ISO image to be used as the install media for the virtual machine environments.

Some test cases may fail if not executed with the "SystemLow-SystemHigh" SELinux level (e.g. Logging in as a normal user and executing **su** or **sudo**). The default SELinux level for normal users is "s0". To change the default SELinux level for normal users to "SystemLow-SystemHigh", use the following command:

semanage login -m -r SystemLow-SystemHigh __default__

11.2.1 Remounts needed for KVM tests

If your system is installed with a separate /tmp partition, run the following remount commands:

mount -o remount,exec /dev/mapper/VolGroup01-temp
mount -o remount,suid /dev/mapper/VolGroup01-temp

Chapter 12 Test execution

12.1 audit-test

In the top level directory of the audit-test test suite, there are a number of README files which contain information about running the tests, packages required for the tests to run and developing new tests. The tests can be run in both capp and lspp mode. The mode is set vi an environment variable PPROFILE.

12.1.1 Complete setup steps

Before successfully running the audit-test suite, you must have completed the setup steps described in Section 12.

12.1.2 Building audit-test

To build the audit-test suite in either 32-bit or 64-bit mode, refer to the section “Build the audit-test suite” of the **audit-test/audit/README.run** file.

Note: When switching between 32-bit and 64-bit modes, **make clean** should be run from the **/usr/local/eal4_testing/audit-test/** directory.

12.1.3 Running audit-test

After all setup steps are completed and the test suite is built, refer to a**udit-test/audit/README.run** for instructions on how to run the test cases.

12.2 LTP tests

A subset of the LTP test cases are now run automatically when a 'make run' is executed from the top audit-test directory. For information on how to build and run the LTP tests, refer to **audit-test/ltp/README.ltp**.

Chapter 13 Known errors

Chapter 14 Legal notices

This work represents the view of the author and does not necessarily represent the view of IBM.

The following are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries: IBM®, eServer(TM), BladeCenter®, System x(TM), System p(TM), System i(TM), System z(TM), and z/VM®. A full list of U.S. trademarks owned by IBM may be found at this location:

```
http://www.ibm.com/legal/copytrade.shtml
```

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat and its logo are registered trademarks of Red Hat, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. Support regarding capabilities of non-IBM products should be addressed to the suppliers of those products.

Any statements about support or other commitments may be changed or cancelled at any time without

notice. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. This Information is provided "AS IS" without warranty of any kind.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice. This docuoment is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk

Last Page