MLS Ecosystem Implementation

Josh Koontz

November 15, 2015

System Implementation Overview

- RHEL Installation
- Base System Configuration
- Network Configuration
- Security Testing
- Additional Software
- Trusted Networking
- Additional Services

RHEL Installation

- Install with CSCF kickstart file to automate
  - Manually partition disk drives
  - Manually set the root password
  - Consistent software packages

- Install on existing RHEL Installation
  - Partitioning changes
  - RPM dependencies built-in

Base System Configuration

Series of RPMs

- Provide consistent system configuration
- Modification to RPMs is version controlled

- Legal Banner + Hardening
  - Sets a banner at login
  - Hardens the system to meet or exceed security controls
  - Applys some custom system configurations
    - Audit Configurations
    - Pam modules

Base System Configuration

- SELinux Configs
  - Polyinstantiated tmp directories
    - Creates base directories
    - Sets configuration to polyinstantiate /tmp and /var/tmp
  - Custom SELinux polices
    - Modifications to make system more usable
    - Added Operations Admin, opsadm_u
  - Custom SELinux config files
    - Allow logins for custom SELinux users
    - Set bash/tcsh prompt to include SELinux context of user
  - Custom SELinux users
    - sysadm_u Allowed access to sysadm_r role
    - secure_u Allowed access to secadm_r and auditadm_r
    - opsadm_u Allowed access to opsadm_r role

Base System Configuration

- Software Docs
  Collection of documents and scripts to install software
  - IPtables
  - Netlabels
  - Apache
  - MySQL
  - OpenMPI

Base System Configuration

- User Mods
  - Provides standard method to build users consistently
  - Creates user file structure layout
  - Maps Linux users to SELinux user
  - Separates user creation into 2 scripts
    - Provides role based access controls
- Initial install creates sample users
  - sysadm
  - secadm
  - user41a
  - user41b
  - user51a
  - user51b

Base System Configuration

- System Administrator script
  - Creates user and group
    - Unique uid and gid
  - Creates user file structure
    - Home directories in /export/home
    - Long term storage in /sci_dat_stor
    - Fast workspace storage in /wrk
    - /$DIR/$LEVEL/$GROUP/$USER
      /export/home/unclass/group1/user1
  - Places privileged user's home directories in /home

Base System Configuration

- Security Administrator script
  - Creates SELinux file context rules for user directories
    - Maps existing /home rules to /export/home
    - Includes MLS level for each user directory
  - Creates user mapping to SELinux users
    - Standard users are mapped to user_u
    - Privileged users are mapped to sysadm_u or secure_u
  - Verifies SELinux context on user's home directories

Network Configuration

- Assign Networks to interfaces
- Apply IPtables rules
- Apply netlabel rules

Network Configuration

Assign Networks to interfaces

- Admin network – eth0
  - Configured for privileged user access only
  - Ex: 192.168.99.2/24

- User networks – eth1, eth2, etc.
  - Separate network for each security level
  - Ex: 192.168.100.2/24, 192.168.101.2/24

Network Configuration

Apply IPtables rules

- Admin network – eth0 – 192.168.99.2/24
  - Allow ssh access only from 192.168.99.0/24
- User networks – eth1 – 192.168.100.2/24
  - Allow ssh access only from 192.168.100.0/24
  - Allow http access from everywhere
- User networks – eth2 – 192.168.101.2/24
  - Allow ssh access from everywhere
  - Allow tomcat access only from 192.168.101.0/24

Network Configuration

Apply netlabel rules (based on incoming IP)

- Overall

  map delete default
  map add default address:0.0.0.0/0 protocol:unlbl
  cipsov4 add pass doi:32 tags:2,1
  map add default addresss:127.0.0.0/8 protocol:cipsov4,32

- Admin network – eth0 – 192.168.99.2/24

  Local & Trusted:
  map add default address:192.168.99.2 protocol:cipsov4,32

  Remote & Untrusted:
  unlbl add interface:eth0 address:192.168.99.0/24
  label:system_u:object_r:netlabel_peer_t:s0-s15:c0.c1023

Network Configuration

Apply netlabel rules (based on incoming IP)

- User networks – eth1 – 192.168.100.2/24

  Local and Trusted:
  map add default address:192.168.100.2 protocol:cipsov4,32

  Remote and Untrusted:
  unlbl add interface:eth1 address:192.168.100.0/24
  label:system_u:object_r:netlabel_peer_t:s5:c1

- User networks – eth2 – 192.168.101.2/24

  Local and Trusted:
  map add default address:192.168.101.2 protocol:cipsov4,32

  Remote and Untrusted:
  unlbl add interface:eth2 address:0.0.0.0/0
  label:system_u:object_r:netlabel_peer_t:s4:c1


Security Testing

- Security Control Verifications
- Audit Configuration Verification
- Role Based Access Controls Implemented
- SELinux User Login Mappings
- MLS File System Checks
- MLS Network Checks

Security Testing

Security Control Verifications

- SCAP – Security Content Automation Protocol
- OpenSCAP
  - Application to verify and remediate system configuration against a standard SCAP security guide or SSG
- OpenSCAP Output checked against MLS profile
  - # yum install openscap openscap-utils scap-security-guide
  - Scan with CSCF profile
    # oscap xccdf eval --profile CSCF-MLS-RHEL6 --results results.xml --report report-mls.html --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictonary.xml /usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml

Security Testing

Audit Configuration Verification

- Audit daemon provides ability to track security-relevant information on your system
  - System Changes
  - File accesses
  - Binary Executions
  - System Calls
  - Modification to audit configuration
  - Authentication to the system

Security Testing

Audit Configuration Verification

- OpenSCAP Output
  - Verifies auditd configuration is in place

- Spot check with ausearch to verify
  - Who: Userid along with SELinux label of subject and object
  - What: Action that was attempted to be performed and result
  - When: Date and time, type, and outcome of an event
  - Where: File system location, file and inode

Security Testing

Role Based Access Control (RBAC)

- user_r
  - General least privileged user role. No access to su or sudo
- staff_r
  - General role. Often used to transition to a higher privileged role.
- sysadm_r
  - Privileged role with access to all system administration functions except security and audit functions
- secadm_r
  - Privileged role that can only modify SELinux policies and labels
- auditadm_r
  - Privileged role that can only modify the audit subsystem

Security Testing

Role Based Access Controls Implemented

- user_r
  - Can general user issue su command?
- Is SELinux policy in place to disable sysadm_r from performing tasks reserved for secadm_r?
  - semodule –l sysadm_secadm
    sysadm_secadm 1.0.0 Disabled
- sysadm_r
  - Can user in the sysadm_r role modify audit log? no
  - Can user in the sysadm_r role modify SELinux policy? no
- secadm_r
  - Can user in the secadm_r role modify SELinux policy? yes

Security Testing

SELinux User Login Mappings

- SELinux users have access to appropriate roles
  - # semanage user –l
- Linux users are mapped to proper SELinux Users with an appropriate MLS Range
  - # semanage login -l

Security Testing

MLS File System Checks

- List security levels of user directories
  - # ls –Z /export/home /sci_dat_stor /wrk
- Show polyinstantiated /tmp and /var/tmp
  - # ls –al /tmp /var/tmp
  - $ ls –al /tmp /var/tmp
- Tests to verify SELinux MLS is working
    - As a user51a user create a file in /export/home/s51/share
      - Open up group permissions with chmod g+rw filename
    - As a user41a user create a file in /export/home/s41/share
      - Open up group permissions with chmod g+rw filename
    - Verify user51a can r/w file in s51/share
    - Verify user51a can only read file in s41/share
    - Verify user41a can r/w file in s41/share
    - Verify user41a can not read file in s51/share

Security Testing

MLS Network Checks

- Networks – show netlabel mappings
  - # netlabelctl unlbl list -p

- Try to login as user to higher level
  - $ ssh user51a@hostname_51
  - $ ssh user41a@hostname_51


Security Testing

Demo:

MLS Filesystem and Checks


Additional Software

- xinetd -> sshd
- httpd
- OpenMPI

Additional Software

xinetd -> sshd

- Labeled Flag to Xinetd
  - Launches sshd at same level as incoming network
- SSHD pam module
  - session required pam_selinux.so open use_current_range
  - Allows a user to login if the user's login is mapped to an MLS Range that includes the level on the incoming network

Additional Software

Httpd

- Run at user level instead of default system level
- Setup all configuration files and directories like installing multiple instances on same server
  - /etc/httpd_new
  - /var/www_new
  - /var/log/httpd_new
  - /var/run/httpd_new
  - /etc/init.d/httpd_new
- Launch process at user level
  - SELinux policy need to allow transition into a level
  - Runcon command added to startup script to transition

Additional Software

OpenMPI

- Install from source or rpm
- User launched software generally just works
  - Processes run in user_t:$LEVEL context

Trusted Networking

- # cat /etc/netlabel.rules

```
map delete default
map add default address:0.0.0.0/0 protocol:unlbl
cipsov4 add pass doi:32 tags:2,1
map add default addresss:127.0.0.0/8 protocol:cipsov4,32

# eth0
map add default address:192.168.99.2 protocol:cipsov4,32
unlbl add interface:eth0 address:192.168.99.0/24 label:system_u:object_r:netlabel_peer_t:s0-s15:c0.c1023

#eth1
map add default address:192.168.100.2 protocol:cipsov4,32
unlbl add interface:eth1 address:192.168.100.0/24 label:system_u:object_r:netlabel_peer_t:s5:c1

#eth2
map add default address:192.168.101.2 protocol:cipsov4,32
unlbl add interface:eth2 address:0.0.0.0/0 label:system_u:object_r:netlabel_peer_t:s4:c1
```

Trusted Networking

- New interconnect ib0
  - ib0 = 192.168.200.2/24
- Add this line to /etc/netlabel.rules to passthrough/trust the incoming label on the entire subnet
  map add default address:192.168.200.0/24 protocol:cipsov4,32
- Verify security level on the network connections:
  - # netstat –atnZ
  - # ps –efZ | grep user

Additional Services

- Resource Manager
- Network File System
- Native InfiniBand
- MLS Database
- System Monitoring / Log Aggregation