SELinux

Rejy M Cyriac (rmc)
RHC{SA,E,SS,DS,VA,A,I}

- Program Manager - Technical
- Red Hat, Inc.
Contact Info

- email:
  - rejy@redhat.com
  - rejymc@fedoraproject.org

- IRC:
  - rejy @
    #fedora, #fedora-selinux, #fedora-india
  on FreeNode
Agenda

- Quick Refresh
  - What is SELinux?
  - How does SELinux work?
- Access Denied !!!
- Trouble-shoot
- Making sense of the error logs
- SELinux Utilities
- Building Custom Policy Modules
What is SELinux?

- Security Principles
What is SELinux?

- Security Principles
  - Least Privilege
What is SELinux?

- Security Principles
  - Least Privilege
  - Closed First
What is SELinux?

- Security Principles
  - Least Privilege
  - Closed First
  - Mandatory Access Control (MAC)
What is SELinux?

- Security Principles
  - Least Privilege
  - Closed First
  - Mandatory Access Control (MAC)
  - Very Fine Grained Access Control
    - Users
    - Files
    - Directories
    - Sockets
    - Ports
    - etc...
What SELinux Can Do...

- Confine programs to minimum privilege required
What SELinux Can Do...

- Confine programs to minimum privilege required
- Prevent system access to private data
What SELinux Can Do...

- Confine programs to minimum privilege required
- Prevent system access to private data
- Protect against process exploits by various mechanisms
What SELinux Can Do...

- Control privilege escalation
- Prevent unauthorized reading and/or modification of data and programs
- Logging of security breaches
- Fine granulated access control implementation
- Role Based Access Control (RBAC)
- MLS/MCS – Multi-Level Security/Multi-Category Security
What SELinux Cannot Do...

- Not a complete Security Solution, but only an element in the Security Infrastructure Stack
What SELinux Cannot Do...

- Not a complete Security Solution, but only an element in the Security Infrastructure Stack
- Cannot substitute for DAC, but adds another layer of security
What SELinux Cannot Do...

- Not a complete Security Solution, but only an element in the Security Infrastructure Stack
- Cannot substitute for DAC, but adds another layer of security
- Cannot audit software code
What SELinux Cannot Do...

- Not a complete Security Solution, but only an element in the Security Infrastructure Stack
- Cannot substitute for DAC, but adds another layer of security
- Cannot audit software code
- Cannot substitute for data encryption
What SELinux Cannot Do...

- Not a complete Security Solution, but only an element in the Security Infrastructure Stack
- Cannot substitute for DAC, but adds another layer of security
- Cannot audit software code
- Cannot substitute for data encryption
- Cannot pull-in bug-fixes for applications
What SELinux Cannot Do...

- Not a complete Security Solution, but only an element in the Security Infrastructure Stack
- Cannot substitute for DAC, but adds another layer of security
- Cannot audit software code
- Cannot substitute for data encryption
- Cannot pull-in bug-fixes for applications
- Not a Centralized Access Control system for networks
How Does SELinux Work?

- SELinux – Basic Concepts
  - Subjects vs. Objects
  - Labeling
  - Type Enforcement
  - SELinux Booleans
How Does SELinux Work?

- Subjects vs. Objects
  - Processes vs. Resources (Files, Directories, Ports, Sockets...etc.)
How Does SELinux Work?

- Labeling
  - Security Context Label for **ALL** subjects and objects on system
How Does SELinux Work?

- Labeling
  - Security Context Label for **ALL** subjects and objects on system
  - Files and Directories: labels stored as extended attributes on the filesystem
How Does SELinux Work?

- Labeling
  - Security Context Label for **ALL** subjects and objects on system
  - Files and Directories: labels stored as extended attributes on the filesystem
  - Processes, Ports, etc.: the kernel manages labels
How Does SELinux Work?

- Labeling
  - The Security Context format:
    user_identity:role:type:sensitivity:category_level
How Does SELinux Work?

- Labeling
  - The Security Context format:
    user_identity:role:type:sensitivity:category_level

    system_u:object_r:httpd_config_t:s0
How Does SELinux Work?

- Labeling
  - Setting/Modifying/Restoring the Security Context label
- chcon
  - to change file security context
  - -t option for specifying context type
  - --reference to use a reference file's security context rather than directly specifying context value
How Does SELinux Work?

- **Labeling**
  - Setting/Modifying/Restoring the Security Context label
- **restorecon**
  - to restore file(s) default security context(s)
  - uses information from
    /etc/selinux/targeted/contexts/files/file_contexts
    (and other files in that directory) to determine what a file or directory's context should be
How Does SELinux Work?

- Type Enforcement
  - Enforcing Access Control using Security Context type
How Does SELinux Work?

- Type Enforcement
  - Enforcing Access Control using Security Context type
  - Deny *ALL* access from *ALL* subjects on *ALL* objects unless explicitly allowed in policy
How Does SELinux Work?

- Type Enforcement
  - Enforcing Access Control using Security Context type
  - Deny ALL access from ALL subjects on ALL objects unless explicitly allowed in policy
  - 'allow' rules form majority of the Policy
How Does SELinux Work?

- Type Enforcement
  - allow subject with specific type...specific access to...specific object classes...with specific type
How Does SELinux Work?

- Type Enforcement
  - allow subject with specific type...specific access to...specific object classes...with specific type

- allow httpd_t httpd_config_t : file { ioctl read getattr lock open } ;
How Does SELinux Work?

- SELinux Booleans
  - An SELinux policy 'allow' rule, subject to a condition being true
How Does SELinux Work?

- SELinux Booleans
  - An SELinux policy 'allow' rule, subject to a condition being true
  - Will have an initial state of either 'OFF' or 'ON'
How Does SELinux Work ?

- SELinux Booleans
  - An SELinux policy 'allow' rule, subject to a condition being true
  - Will have an initial state of either 'OFF' or 'ON'
  - State can be switched temporarily or permanently
How Does SELinux Work?

- SELinux Booleans
  - Relevant Commands
    - `getsebool <boolean>|-a`
    - `setsebool [-P] <boolean> 0|1`
    - `semanage boolean -l`
Access Denied !!!

- Isolate Source of Denial
Trouble-shoot Cause

- SELinux Errors
  - If you see an SELinux error, it means that something is wrong!
Trouble-shoot Cause

- SELinux Errors
  - If you see an SELinux error, it means that something is wrong!
  - Turning off SELinux is like putting a sticker on top of the check-engine warning light in your car !!!
Trouble-shoot Cause

- SELinux Errors
  - It may mean that labeling is wrong
Trouble-shoot Cause

- SELinux Errors
  - It may mean that labeling is wrong
    - Use the tools to examine and fix the labels.
Trouble-shoot Cause

- SELinux Errors
  - It may mean that the policy needs to be tweaked.
Trouble-shoot Cause

- SELinux Errors
  - It may mean that the policy needs to be tweaked.
  - Booleans
    - `getsebool -a | grep <service name>`
    - `setsebool [-P] <boolean> 0|1`
Trouble-shoot Cause

- SELinux Errors
  - It may mean that the policy needs to be tweaked.
    - Booleans
      - `getsebool -a | grep <service name>`
      - `setsebool [-P] <boolean> 0|1`
    - Policy Module
      - `audit2allow`
      - `semodule`
Trouble-shoot Cause

- SELinux Errors
  - There could be a bug in the policy
Trouble-shoot Cause

- SELinux Errors
  - There could be a bug in the policy
    - Report it
      - Bugzilla
      - Support
Trouble-shoot Cause

- SELinux Errors
  - You have been, or are being, broken into
Trouble-shoot Cause

- SELinux Errors
  - You have been, or are being, broken into
    - Roll out the army!
• Making sense of the error logs
  
  - SELinux Errors
    - Audit (log) messages captured in raw format at
      - /var/log/audit/audit.log
Making sense of the error logs

- SELinux Errors
  - Audit (log) messages captured in raw format at
    - /var/log/audit/audit.log
  - Install setroubleshoot and setroubleshoot-server for translated messages to be made available at
    - /var/log/messages
Making sense of the error logs

- SELinux Errors

- type=AVC msg=audit(1399611459.052:546): avc: denied { read } for pid=4102 comm="/usr/sbin/httpd" name="index.html" dev="dm-2" ino=4589125 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:user_home_t:s0 tclass=file

- type=SYSCALL msg=audit(1399611459.052:546): arch=c000003e syscall=2 success=no exit=-13 a0=7f1be878f8f8 a1=80000 a2=0 a3=7f1be878c320 items=0 ppid=4098 pid=4102 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="/usr/sbin/httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
Making sense of the error logs

- SELinux Errors

May 9 10:27:53 localhost setroubleshoot: SELinux is preventing /usr/sbin/httpd from read access on the file. For complete SELinux messages, run sealert -l c68b231e-73d4-4a68-bc88-19bcd8a77478
May 9 10:27:53 localhost python: SELinux is preventing /usr/sbin/httpd from read access on the file.

***** Plugin catchall_boolean (89.3 confidence) suggests ***************

If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content' boolean.
You can read 'user_selinux' man page for more details.
Do
setsebool -P httpd_read_user_content 1

***** Plugin catchall (11.6 confidence) suggests ***************

If you believe that httpd should be allowed read access on the file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep /usr/sbin/httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp
### Making sense of the error logs

#### SELinux Errors

<table>
<thead>
<tr>
<th>Additional Information:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Context</td>
<td><code>system_u:system_r:httpd_t:s0</code></td>
</tr>
<tr>
<td>Target Context</td>
<td><code>unconfined_u:object_r:user_home_t:s0</code></td>
</tr>
<tr>
<td>Target Objects</td>
<td><code>[ file ]</code></td>
</tr>
<tr>
<td>Source</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>Source Path</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>Host</td>
<td><code>localhost.localdomain</code></td>
</tr>
<tr>
<td>Source RPM Packages</td>
<td><code>httpd-2.4.9-2.fc20.x86_64</code></td>
</tr>
<tr>
<td>Target RPM Packages</td>
<td></td>
</tr>
<tr>
<td>Policy RPM</td>
<td><code>selinux-policy-3.12.1-158.fc20.noarch</code></td>
</tr>
<tr>
<td>Selinux Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Policy Type</td>
<td><code>targeted</code></td>
</tr>
<tr>
<td>Enforcing Mode</td>
<td>Enforcing</td>
</tr>
<tr>
<td>Host Name</td>
<td><code>localhost.localdomain</code></td>
</tr>
<tr>
<td>Platform</td>
<td><code>Linux localhost.localdomain 3.14.2-200.fc20.x86_64</code></td>
</tr>
<tr>
<td>Alert Count</td>
<td>1</td>
</tr>
<tr>
<td>First Seen</td>
<td><code>2014-05-09 10:27:39 IST</code></td>
</tr>
<tr>
<td>Last Seen</td>
<td><code>2014-05-09 10:27:39 IST</code></td>
</tr>
<tr>
<td>Local ID</td>
<td><code>c68b231e-73d4-4a68-bc88-19bcd8a77478</code></td>
</tr>
</tbody>
</table>
• SELinux Utilities

• sesearch
• semanage
• audit2why
• sealert
• seaudit
• apol
Building Custom Policy Modules

- Useful Tools
  - selinux-policy-devel
  - audit2allow
  - semodule
Building Custom Policy Modules

- Policy Language
  - Policy Module Name and Version
  - Requires
  - New Types
  - Rules
  - Booleans
Building Custom Policy Modules

- Macros
  - For access vectors
  - For rules
Useful Links

- SELinux Project wiki - http://selinuxproject.org
- SELinux NSA Home - http://www.nsa.gov/research/selinux
- Dan Wlash's Blog - http://danwalsh.livejournal.com/
Questions?

- Ask them now!
- Contact me at:
  - rejy@redhat.com
  - rejymc@fedoraproject.org
  - rejy @ #fedora, #fedora-selinux, #fedora-india on FreeNode

fedora

fedoraproject.org