Time to harden up

SELinux is no longer an option
SELinux

• Overview
• How to use it
• Retrofit
/* selinuxfs pseudo filesystem for exporting the security policy API.
Based on the proc code and the fs/nfsd/nfsctl.c code. */

#include "flask.h"
#include "avc.h"
#include "avc_ss.h"
#include "security.h"
#include "objsec.h"
#include "conditional.h"

/* Policy capability filenames */
static char *policycap_names[] = {
"network_peer_controls",
"open_perms"
};
NOT
Real
First ?
Install Notes
Setting SELinux to permissive mode when installing the content management server on Red Hat Enterprise Linux 5

Red Hat Enterprise Linux® 5 enables SELinux by default which interferes with the installation process of Software Knowledge Base Toolkit. To ensure the proper installation and usage of the toolkit, the SELinux setting must be changed from the enforcing mode to either permissive or disabled mode.

Procedure

- If you want to disable SELinux only for the installation process, use the setenforce 0 command to set the SELinux to permissive mode.

  **Note:** SELinux will be fully enabled again the next time the system is restarted or if when the setenforce 1 command is entered on the command line.

- If you want to permanently disable SELinux, go to the SELinux configuration file that is located in the /etc/selinux/ directory and set the value of the SELINUX attribute to permissive or disabled.

  **Note:** Note that in the case of server installation, the SELinux enforcing mode cannot be set back to its default value on Red Hat Enterprise Linux 5 because then the server will stop working correctly.
Permissive
!=
ON
Permissive = Testing
Enabled
Enabled & Enforcing
I ALWAYS TURN SELINUX ON.

DOESN’T EVERYONE?
Policy
What
A brief history

- Created by the United States National Security Agency (NSA) as set of patches to the Linux kernel using Linux Security Modules (LSM)
- Released by the NSA under the GNU General Public License (GPL) in 2000
- Adopted by the upstream Linux kernel in 2003
  - Red Hat Enterprise Linux since RHEL 4
  - Debian from etch
  - Ubuntu from 8.04
What is SELinux?

• MAC vs. DAC
• Labeling
• Type Enforcement
• Policy
MAC vs. DAC

- Typical Unix/Linux: Discretionary Access Control (DAC)
  - User ownership
  - Group ownership
  - Permissions

- If I want, I have the ability (discretion) to `chmod +rwx` my home directory. Nothing will stop me, and in a DAC system, nothing will stop others from getting in.
MAC vs. DAC

- In DAC systems, `root` is omnipotent.

Bow before me, for I am root.
MAC vs. DAC

- SELinux system: Mandatory Access Control (MAC)
- On MAC systems, policy is set centrally and fixed
- Even if you change the DAC settings on your home directory, if a mandatory system policy is in place which prevents another user or process from accessing it, you're generally safe.
MAC vs. DAC

- MAC can be incredibly fine grained. Policies can be set to determine access between:
  - Users
  - Files
  - Directories
  - Memory
  - Sockets
  - tcp/udp ports
  - etc...
Labeling

- Different components of the system - files, directories, running processes, sockets, ports, users and so on – are assigned different labels for their security context.
Labeling

• For example, in the Apache web server, you'll see the following labels:
  • /usr/sbin/httpd has the context 
    system_u:object_r:httpd_exec_t:s0
  • /etc/httpd/ has the context 
    system_u:object_r:httpd_config_t:s0
  • /var/www/html/ has the context 
    system_u:object_r:httpd_sys_content_t:s0
  • /var/log/httpd/ has the context 
    system_u:object_r:httpd_log_t:s0
Labeling

For example, in the Apache web server, you'll see the following labels:

- /usr/lib64/httpd/modules/ has the context system_u:object_r:httpd_modules_t:s0
- /etc/rc.d/init.d/httpd has the context system_u:object_r:httpd_initrc_exec_t:s0
- ...etc
Labeling

- When httpd is run, it has the label `unconfined_u:system_r:httpd_t:s0`
- The http ports (80, 443, 488, 8008, 8009, 8443) are labeled `http_port_t`
Labeling

• These labels are used to enforce policies.
Labeling

• There are other fields in the SELinux context
  • `system_u:object_r:httpd_exec_t:s0`
  • User (root, unconfined_u, user_u, system_u)
    - Not the same as Linux user! There are usually a very limited number of SELinux users, and typically all regular Linux users will run as the same SELinux user
    - User files and processes will typically be labeled unconfined_u
    - System files and processes will often be labeled system_u
  • SELinux User is not used in targeted policy
Type Enforcement

• Type enforcement is just a definition of how types interact.
• Processes running with httpd_t context should probably be able to access the configuration files labeled with httpd_config_t
• Processes running with httpd_t context should probably not be able to access files with type shadow_t!
Policy

- Policy is just the rule set that defines how these labeled objects interact.
- The default policy in RHEL 6 is the targeted policy.
  - Unless covered by a targeted policy, processes run unconfined.
  - Hundreds of apps covered by policy.
- The MLS/MCS policies are far more fine grained.
  - If not explicitly allowed, everything is denied.
Why
Where
SELINIX IS SO EASY BECAUSE IT JUST WORKS
Why Not?
How
Turn it on

```bash
# setenforce -help
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
# setenforce 1
```
Check it is on

# getenforce
Enforcing
# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
Relabel your filesystem

# fixfiles onboot
System will relabel on next boot

# ls -l /.autorelabel
-rw-r--r--. 1 root root 0 Jan 12 18:18 /.autorelabel

# reboot
Viewing labels

• Many utilities support the -Z argument
• For example
  • ls -Z
  • cp -Z
  • ps -Z
  • id -Z
Creating labels

- SELinux aware apps
  - chcon
  - restorecon
  - semanage fcontext
    - See /etc/selinux/targeted/contexts/files/file_contexts
  - RPMs

- Users creating files
  - New files inherit context
  - Moved files maintain context
What does it mean if I get an SELinux error?

- When you see an SELinux denial, it means that something is wrong.
- It can mean that the labeling is wrong
- The policy needs to be tweaked
- There's a bug in the app or the policy
- You've been or are being broken into!
Permissive = Testing
Apache vs. SELinux

• Create content and move it

```bash
[root@host15 ~]# echo "This is my foo" > foo.html
[root@host15 ~]# mv foo.html /var/www/html/
[root@host15 ~]# 
```
Forbidden

You don't have permission to access /foo.html on this server.

Apache/2.2.15 (Red Hat) Server at host15.tc.redhat.com Port 80
Move vs copy

```
[root@host15 ~]# ls -Z /var/www/html/ 
-rw-r--r-- root root unconfined_u:object_r:admin_home_t:s0 foo.html 
[root@host15 ~]#  
```
Apache vs. SELinux

• We need to change the context
Apache vs. SELinux

- Hardest way - figure out the context and use chcon

```bash
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# chcon -u unconfined_u -r object_r -t httpd_sys_content_t /var/www/html/foo.html
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 foo.html
[root@host15 ~]#
```
This is my foo
Apache vs. SELinux

• Easier way - use chcon --reference
Apache vs. SELinux

• Easiest way - restorecon

```
[root@host15 ~]# mv foo.html /var/www/html/
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# restorecon -vR /var/www/html/
restorecon reset /var/www/html/foo.html context unconfined_u:object_r:admin_home_t:s0->system_u:object_r:httpd_sys_content_t:s0
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 foo.html
[root@host15 ~]#]
```
Apache and public_html

• Allowing Apache to access Paul's home directory so we can access http://host15.tc.redhat.com/~paul
  • Fix httpd.conf
  • Set permissions to allow httpd to access /home/paul
  • Reload Apache
  • As Paul, create index.html
  • Fire up the browser
Forbidden

You don't have permission to access /~paul/ on this server.

Apache/2.2.15 (Red Hat) Server at host14.tc.redhat.com Port 80
Things to check

- /var/log/httpd/access.log
- /var/log/httpd/error.log
```
[root@host15 ~]# cat /var/log/httpd/error_log
[Wed May 04 02:23:21 2011] [notice] SELinux policy enabled; httpd running as context unconfined_u:system_r:httpd_t:s0
[Wed May 04 02:23:21 2011] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed May 04 02:23:21 2011] [notice] Digest: generating secret for digest authentication ...
[Wed May 04 02:23:21 2011] [notice] Digest: done
[Wed May 04 02:23:21 2011] [warn] ./mod_dnssd.c: No services found to register
[Wed May 04 02:23:21 2011] [notice] Apache/2.2.15 (Unix) DAV/2 configured -- resuming normal operations
[Wed May 04 02:23:32 2011] [error] [client 10.10.10.3] (13)Permission denied: access to /~paul denied
[Wed May 04 02:23:33 2011] [error] [client 10.10.10.3] (13)Permission denied: access to /~paul denied
[Wed May 04 02:23:33 2011] [error] [client 10.10.10.3] (13)Permission denied: access to /~paul denied
[root@host15 ~]#
```
Things to check

- /var/log/messages
May 4 00:06:03 host14 setroubleshoot: SELinux is preventing the http daemon from reading users' home directories. For complete SELinux messages, run sealert -l 3c93734c-4444-4df9-b29a-6ece47b0b2cc
May 4 00:06:03 host14 setroubleshoot: SELinux is preventing the http daemon from reading users' home directories. For complete SELinux messages, run sealert -l 3c93734c-4444-4df9-b29a-6ece47b0b2cc
SELinux has denied the http daemon access to users' home directories. Someone is attempting to access your home directories via your http daemon. If you have not setup httpd to share home directories, this probably signals an intrusion attempt.

Allowing Access:

If you want the http daemon to share home directories you need to turn on the httpd_enable_homedirs boolean: "setsebool -P httpd_enable_homedirs=1" You may need to also label the content that you wish to share. The man page httpd_selinux will have further information. 'man httpd_selinux'.

Fix Command:

setsebool -P httpd_enable_homedirs=1
setsebool -P httpd_enable_homedirs=1

<table>
<thead>
<tr>
<th>Source Context</th>
<th>system_u:system_r:httpd_t:s0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Context</td>
<td>unconfinned_u:object_r:home_root_t:s0</td>
</tr>
<tr>
<td>Target Objects</td>
<td>/home/paul/public_html/index.html [ file ]</td>
</tr>
<tr>
<td>Source</td>
<td>httpd</td>
</tr>
<tr>
<td>Source Path</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>Port</td>
<td>&lt;Unknown&gt;</td>
</tr>
<tr>
<td>Host</td>
<td>host14.tc.redhat.com</td>
</tr>
<tr>
<td>Source RPM Packages</td>
<td>httpd-2.2.15-5.el6</td>
</tr>
<tr>
<td>Target RPM Packages</td>
<td>selinux-policy-3.7.19-54.el6_0.5</td>
</tr>
<tr>
<td>Policy RPM</td>
<td>targeted</td>
</tr>
<tr>
<td>Selinux Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Enforcing</td>
</tr>
<tr>
<td>Enforcing Mode</td>
<td>httpd_enable_homedirs</td>
</tr>
<tr>
<td>Host Name</td>
<td>host14.tc.redhat.com</td>
</tr>
<tr>
<td>Platform</td>
<td>Linux host14.tc.redhat.com 2.6.32-71.24.1.el6.x86_64 #1 SMP Sat Mar 26 16:05:19 EDT 2011 x86_64 x86_64</td>
</tr>
<tr>
<td>Alert Count</td>
<td>2</td>
</tr>
<tr>
<td>First Seen</td>
<td>Wed May 4 00:06:01 2011</td>
</tr>
</tbody>
</table>
SELinux – LCA Sys Admin 2012

root@host14:~

2.6.32-71.24.1.el6.x86_64 #1 SMP Sat Mar 26
16:05:19 EDT 2011 x86_64 x86_64

Alert Count
First Seen Wed May 4 00:06:01 2011
Last Seen Wed May 4 00:06:01 2011
Local ID 3c93734c-4444-4df9-b29a-6ece47b0b2cc
Line Numbers

Raw Audit Messages

node=host14.tc.redhat.com type=AVC msg=audit(1304485561.334:21462): avc: denied
  { getattr } for pid=1586 comm="httpd" path="/home/paul/public_html/index.html"
  dev=vda3 ino=285113 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined
  u:object_r:home_root_t:s0 tclass=file

node=host14.tc.redhat.com type=SYSCALL msg=audit(1304485561.334:21462): arch=c0000003e
syscall=6 success=no exit=-13 a0=7f0e9a1afee0 a1=7ffffc84b500 a2=7ffffc84b500
a3=1 items=0 ppid=1575 pid=1586 auid=4294967295 uid=48 gid=48 euid=48 suid=48
fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd"
subj=system_u:system_r:httpd_t:s0 key=(null)

[root@host14 ~]#
### SELinux – LCA Sys Admin 2012

<table>
<thead>
<tr>
<th>Alert Count</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Seen</td>
<td>Wed May 4 00:06:01 2011</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Wed May 4 00:06:01 2011</td>
</tr>
<tr>
<td>Local ID</td>
<td>3c93734c-4444-4df9-b29a-6ece47b0b2cc</td>
</tr>
</tbody>
</table>

**Raw Audit Messages**

```
	node=host14.tc.redhat.com type=SYSCALL msg=audit(1304485561.334:21462): arch=x86_64 syscall=6 success=no exit=-13 a0=7f0e9a1afee0 a1=7ffffff8b500 a2=7ffffff8b500 a3=1 items=0 ppid=1575 pid=1586 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
```

```bash
[root@host14 ~]# setsebool -P httpd_enable_homedirs=1
[root@host14 ~]#  
```
This is my page
Booleans

- Booleans just turn something on or off
  - getsebool
  - setsebool
[root@host15 ~]# getsebool -a
abrt_anon_write --> off
allow_console_login --> on
allow_corosync_rw_tmpfs --> off
allow_cvs_read_shadow --> off
allow_daemons_dump_core --> on
allow_daemons_use_tty --> on
allow_domain_fd_use --> on
allow_execcheap --> off
allow_execmem --> on
allow_execmod --> on
allow_execstack --> on
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
allow_ftpd_use_cifs --> off
allow_ftpd_use_nfs --> off
allow_gssd_read_tmp --> on
allow_guest_exec_content --> off
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
allow_java_execstack --> off
allow_kerberos --> on
[root@host15 ~]# getsebool -a | grep http
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> on
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> on
httpd_execmem --> off
httpd_read_user_content --> off
httpd_setrlimit --> off
httpd_ssi_exec --> off
httpd_tmp_exec --> off
httpd_tty_comm --> on
httpd_unified --> on
httpd_use_cifs --> off
httpd_use_gpg --> off
httpd_use_nfs --> off
[root@host15 ~]#
[root@host15 ~]# getsebool -a | grep nfs
allow_ftpd_use_nfs --> off
allow_nfsd_anon_write --> off
git_system_use_nfs --> off
httpd_use_nfs --> off
nfs_export_all_ro --> on
nfs_export_all_rw --> on
qemu_use_nfs --> on
samba_share_nfs --> off
use_nfs_home_dirs --> on
virt_use_nfs --> off
xen_use_nfs --> off
[root@host15 ~]#
How can I see what booleans have been set?

• /etc/selinux/targeted/modules/active/booleans.local

```bash
# cat /etc/selinux/targeted/modules/active/booleans.local
httpd_enable_homodirs=1
```

When in doubt...

- Restore labels
mkdir public_html

```
[paul@host15 ~]$ echo "This is my page" > public_html/index.html
[paul@host15 ~]$ ls -Z
drwxrwxr-x. paul paul unconfined_u:object_r:user_home_t:s0 public_html
[paul@host15 ~]$ 
[paul@host15 ~]$ 
[paul@host15 ~]$ 
[paul@host15 ~]$ restorecon -vR /home/paul/
restorecon reset /home/paul/public_html context unconfined_u:object_r:user_home_t:s0->unconfined_u:object_r:httpd_user_content_t:s0
restorecon reset /home/paul/public_html/index.html context unconfined_u:object_r:user_home_t:s0->unconfined_u:object_r:httpd_user_content_t:s0
[paul@host15 ~]$ 
```
Install Audit

- `/var/log/audit/audit.log`
setroubleshoot

• Provides tools to help diagnose SELinux problems
  • `yum install setroubleshoot-server`

• Analyse your audit.log
  • `sealert -a`
Retrofit

• Apply SELinux to an existing webserver
  • Debain Lenny
  • 1.5 GB Xen Virtual Image
  • 96 MB Ram
  • Small Image designed for fast recover
  • Close to stateless
Retrofit

- Initial preparation
  - Backup VM
  - Increase VM Size
  - Upgrade to Debian Squeeze
    - Post upgrade cleanups
    - Confirm websites still work as expected
  - Post upgrade backup
  - Install SELinux support plus auditd
Install & Enable SELinux

# This pulls in a lot of additional packages
apt-get install selinux-basics selinux-policy-default auditd

# configure GRUB and PAM and to create /.autorelabel
selinux-activate

reboot

# check that everything has been setup correctly and to catch common SELinux problems
check-selinux-installation
debian:/var/log/audit# sestatus

SELinux status: enabled
SELinuxfs mount: /selinux
Current mode: permissive
Mode from config file: permissive
Policy version: 24
Policy from config file: default
Deal with `/var/log/audit/audit.log`

Jan 6 12:23:43 debian kernel: [ 74.427105] type=1400 audit(1325805811.932:7): avc: denied { getattr } for pid=841 comm="apache2" path="/home/www/photos" dev=xvda2 ino=73097 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:user_home_t:s0 tclass=dir

```
ls -lZ /var/www /home/www -d
  drwxr-sr-x  28 steve users unconfined_u:object_r:user_home_dir_t:s0 4096 Jun 6 2009 /home/www
  drwxr-xr-x  3 root root system_u:object_r:httpd_sys_content_t:s0 4096 May 13 2010 /var/www

chcon -R --reference /var/www /home/www
```
Update the policy

```
semanage fcontext -a -t httpd_sys_content_t "/home/www(/.*)?"
semanage fcontext -a -t httpd_sys_script_exec_t "/home/www/cgi-bin(/.*)?"

restorecon -R /home/www

# Allow cgi-bin support
semanage boolean -m --on httpd_enable_cgi

# Allow access to our NFS mounted images
semanage boolean -m --on httpd_use_nfs
```
The hardest part

Everything other than debugging SELinux
Questions
References

• SELinux Project Page
  http://selinuxproject.org/

• Red Hat Security-Enhanced Linux Docs

• Running key services under SELinux

• Tips on Apache and SELinux
  http://selinuxproject.org/page/ApacheRecipes

• SELinux and Debian
  http://wiki.debian.org/SELinux/Setup
Images

- **Real World Logo**

- **MTV Logo**

- **Tivoli Installer**

- **Ass**
  - http://www.theanimalangel.org/whiteboys.jpg

- **Tux**
  - http://upload.wikimedia.org/wikipedia/commons/a/af/Tux.png

- **Flames**
  - http://www.flickr.com/photos/wwarby/5109439137/