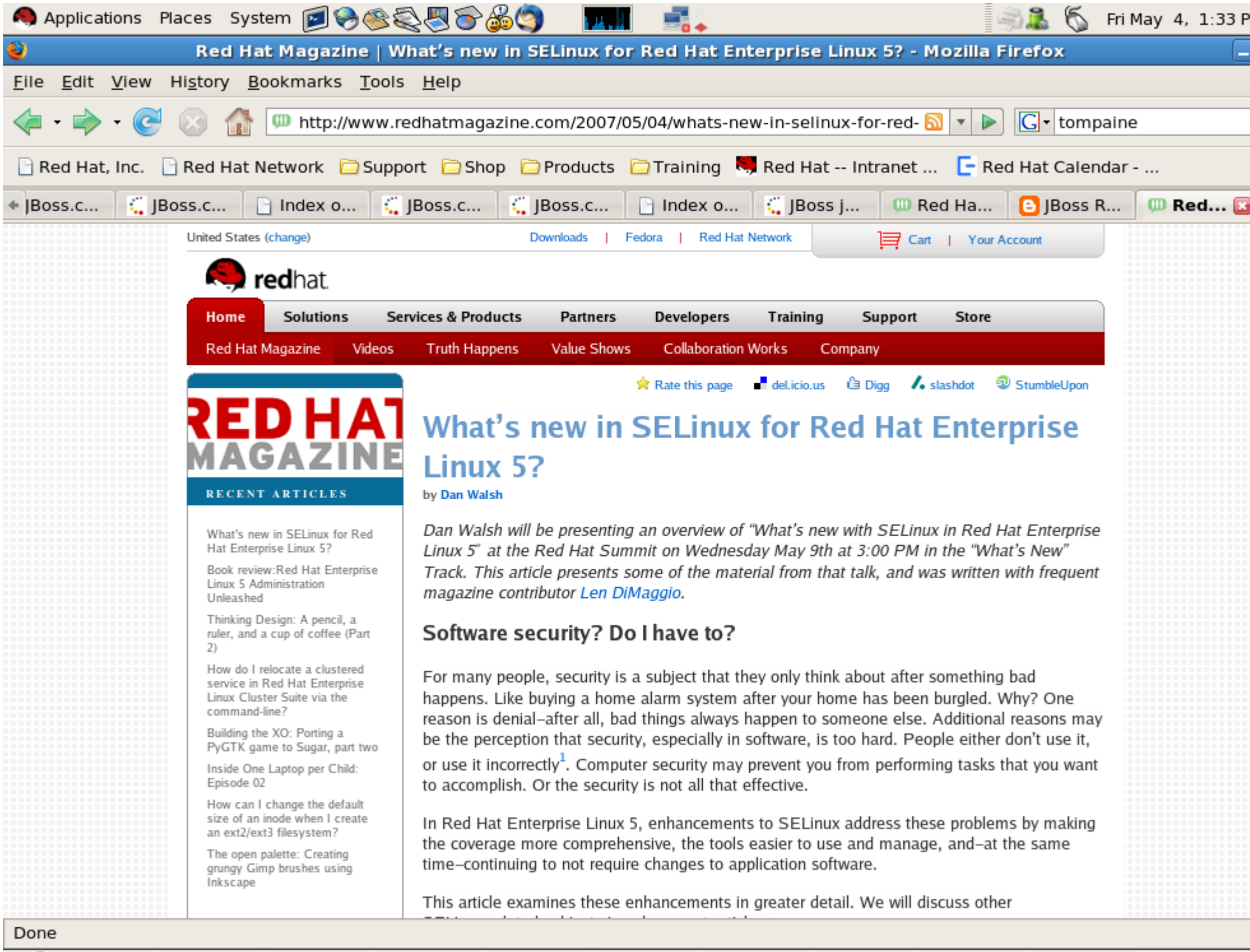
SELinux: Best Practices and What's New in Red Hat Enterprise Linux 5

Name Dan Walsh

Date Wednesday May 9th 2007


Applications Places System
Fri May 4, 1:33 PM
Red Hat Magazine | What's new in SELinux for Red Hat Enterprise Linux 5? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.redhatmagazine.com/2007/05/04/whats-new-in-selinux-for-red-
tompaine
Red Hat, Inc. Red Hat Network Support Shop Products Training Red Hat -- Intranet ... Red Hat Calendar - ...
United States (change) Downloads | Fedora | Red Hat Network Cart | Your Account
redhat
Home Solutions Services & Products Partners Developers Training Support Store
Red Hat Magazine Videos Truth Happens Value Shows Collaboration Works Company
RED HAT MAGAZINE
RECENT ARTICLES
What's new in SELinux for Red Hat Enterprise Linux 5?
Book review:Red Hat Enterprise Linux 5 Administration Unleashed
Thinking Design: A pencil, a ruler, and a cup of coffee (Part 2)
How do I relocate a clustered service in Red Hat Enterprise Linux Cluster Suite via the command-line?
Building the XO: Porting a PyGTK game to Sugar, part two
Inside One Laptop per Child: Episode 02
How can I change the default size of an inode when I create an ext2/ext3 filesystem?
The open palette: Creating grungy Gimp brushes using Inkscape
Rate this page del.icio.us Digg slashdot StumbleUpon
What's new in SELinux for Red Hat Enterprise Linux 5?
by Dan Walsh
Dan Walsh will be presenting an overview of "What's new with SELinux in Red Hat Enterprise Linux 5" at the Red Hat Summit on Wednesday May 9th at 3:00 PM in the "What's New" Track. This article presents some of the material from that talk, and was written with frequent magazine contributor Len DiMaggio.
Software security? Do I have to?
For many people, security is a subject that they only think about after something bad happens. Like buying a home alarm system after your home has been burgled. Why? One reason is denial–after all, bad things always happen to someone else. Additional reasons may be the perception that security, especially in software, is too hard. People either don't use it, or use it incorrectly[1]. Computer security may prevent you from performing tasks that you want to accomplish. Or the security is not all that effective.
In Red Hat Enterprise Linux 5, enhancements to SELinux address these problems by making the coverage more comprehensive, the tools easier to use and manage, and–at the same time–continuing to not require changes to application software.
This article examines these enhancements in greater detail. We will discuss other
Done

All Software SUCKS!

- MALWARE
- SPYWARE
- VIRUS
- WORMS
- Stolen Personal Data
  - Marshalls
  - Fidelity
  - US Government
- Microsoft Windows

RED HAT :: SAN DIEGO :: 2007

SUMMIT

LEAVE SELinux On EVERYWHERE!

- STOP credit card data from being stolen
- STOP SPAM mail attacks from your compromised servers.
- STOP worms from attaching your web sites
- STOP trusting your Applications to do the **Right** thing.
- SELinux is your last line of DEFENSE.

S.M.U.T

- **S**ecure
- **M**anageable
- **U**ltra **T**rusted

Secure

- Red Hat Enterprise Linux 4
  - 15 Targets
  - Built on Fedora Core 2/3 Experience
- Red Hat Enterprise Linux 5
  - 200 Targets
  - Built on Fedora Core 2/3/4/5/6 RHEL4 Experience

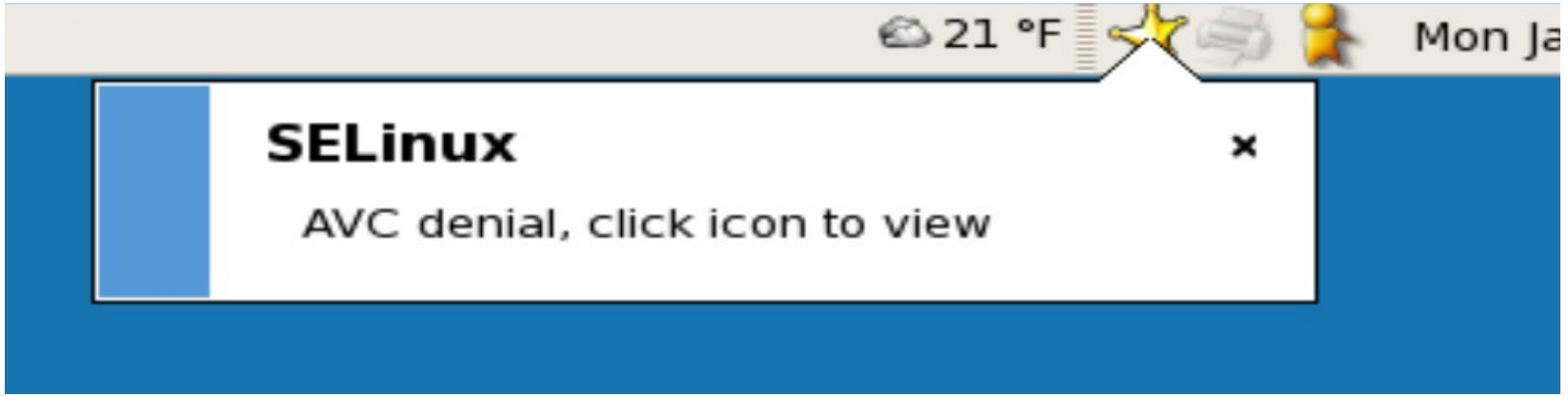
- All system applications minimal privilege
- Entire System Space is covered by SELinux policy
- All processes started during boot up have defined SELinux domains
- User space logins are still allowed to run execute Unconfined.
  - Executable Memory checks confine user space to help prevent Buffer Overflow attacks.

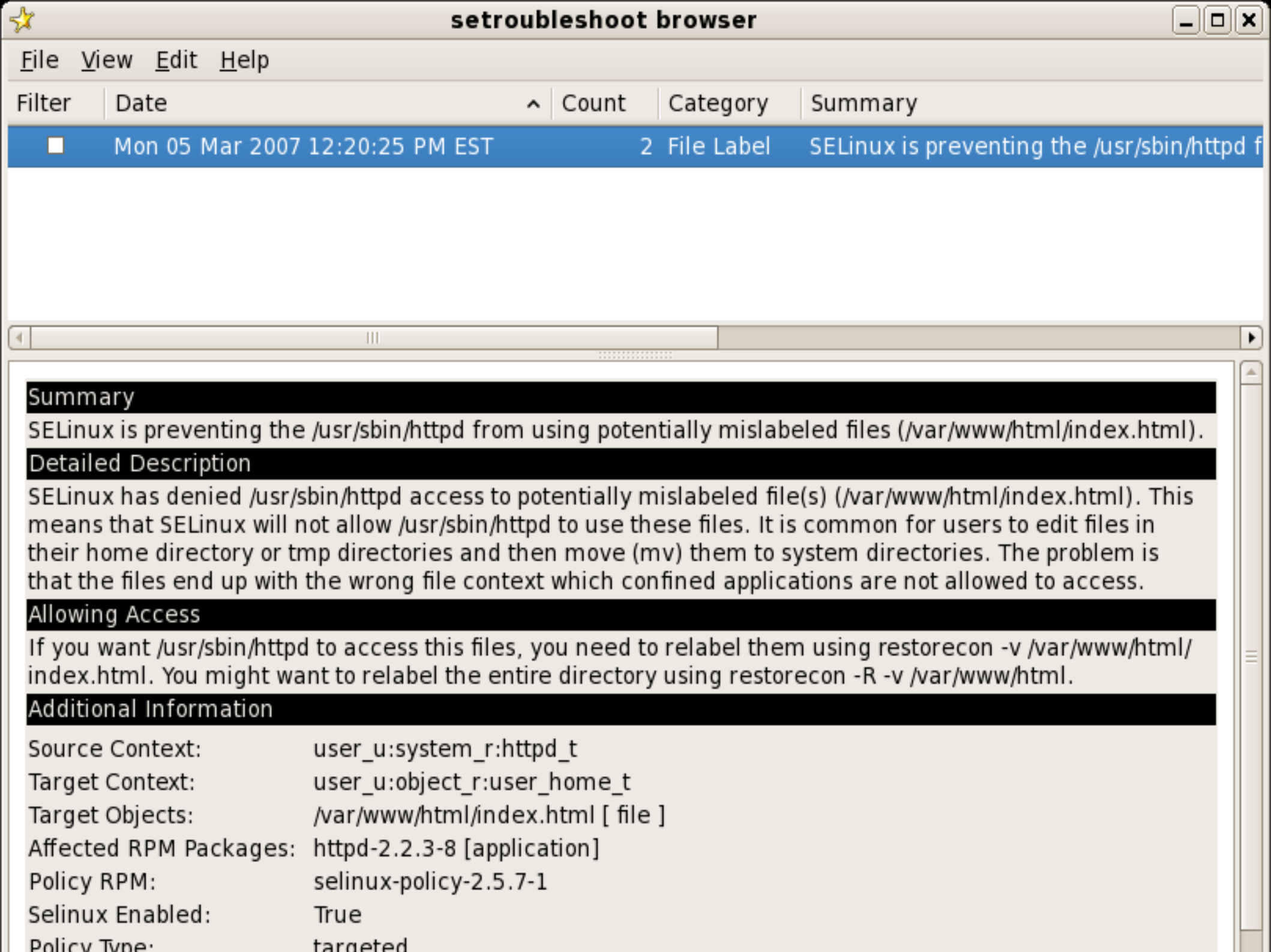
Manageable - Troubleshooting

What the H**L is going on????

- tail /var/log/audit/audit.log

  type=AVC msg=audit(1176392795.244:2036): avc: denied { getattr } for pid=6705 comm="httpd" name="index.html" dev=dm-0 ino=3180003 scontext=user_u:system_r:httpd_t:s0 tcontext=system_u:object_r:user_home_t:s0 tclass=file



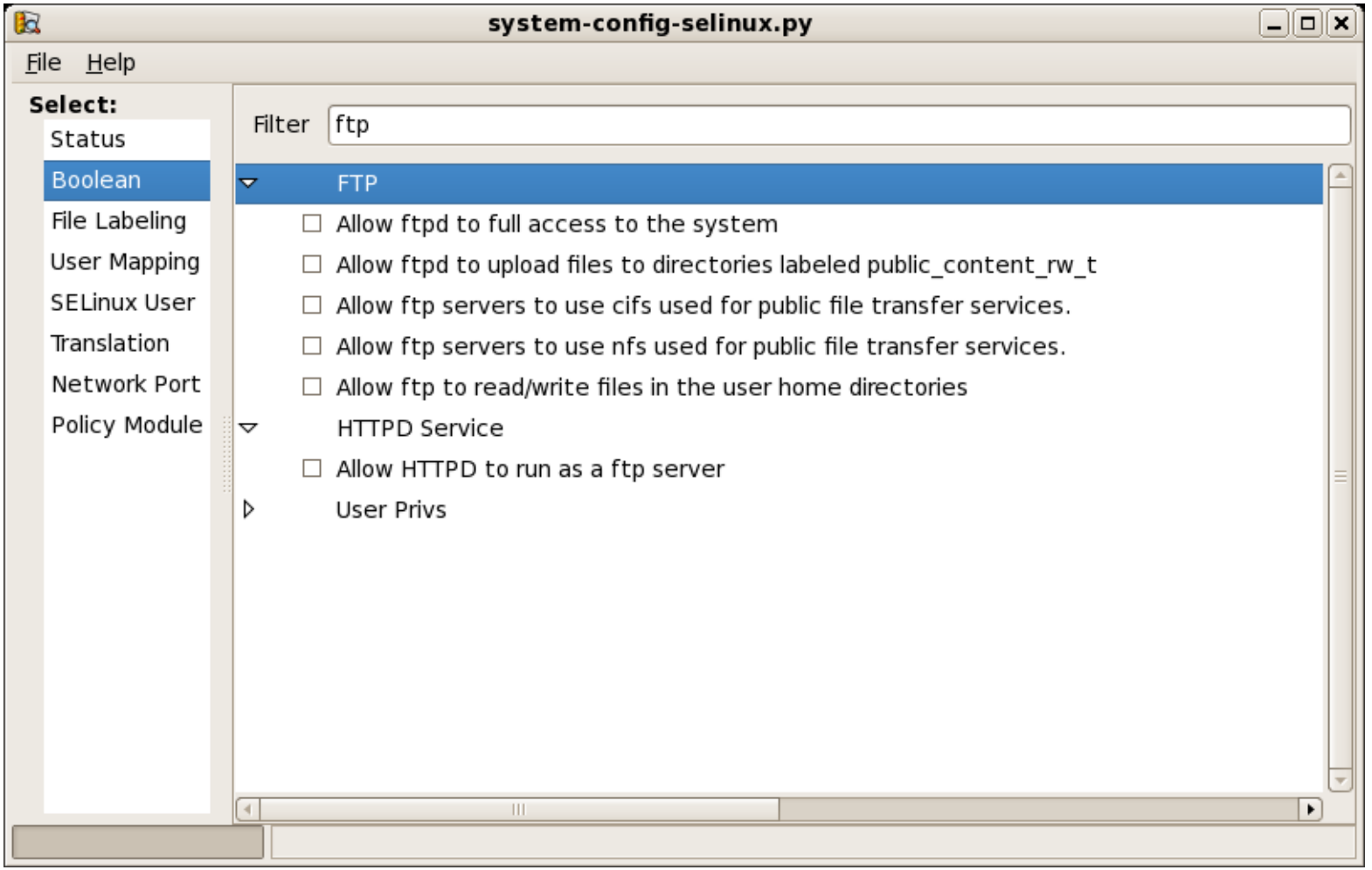

setroubleshoot browser
File View Edit Help
Filter Date Count Category Summary
Mon 05 Mar 2007 12:20:25 PM EST 2 File Label SELinux is preventing the /usr/sbin/httpd f
Summary
SELinux is preventing the /usr/sbin/httpd from using potentially mislabeled files (/var/www/html/index.html).
Detailed Description
SELinux has denied /usr/sbin/httpd access to potentially mislabeled file(s) (/var/www/html/index.html). This means that SELinux will not allow /usr/sbin/httpd to use these files. It is common for users to edit files in their home directory or tmp directories and then move (mv) them to system directories. The problem is that the files end up with the wrong file context which confined applications are not allowed to access.
Allowing Access
If you want /usr/sbin/httpd to access this files, you need to relabel them using restorecon -v /var/www/html/index.html. You might want to relabel the entire directory using restorecon -R -v /var/www/html.
Additional Information
Source Context: user_u:system_r:httpd_t
Target Context: user_u:object_r:user_home_t
Target Objects: /var/www/html/index.html [file]
Affected RPM Packages: httpd-2.2.3-8 [application]
Policy RPM: selinux-policy-2.5.7-1
Selinux Enabled: True
Policy Type: targeted

Manageable - Troubleshooting

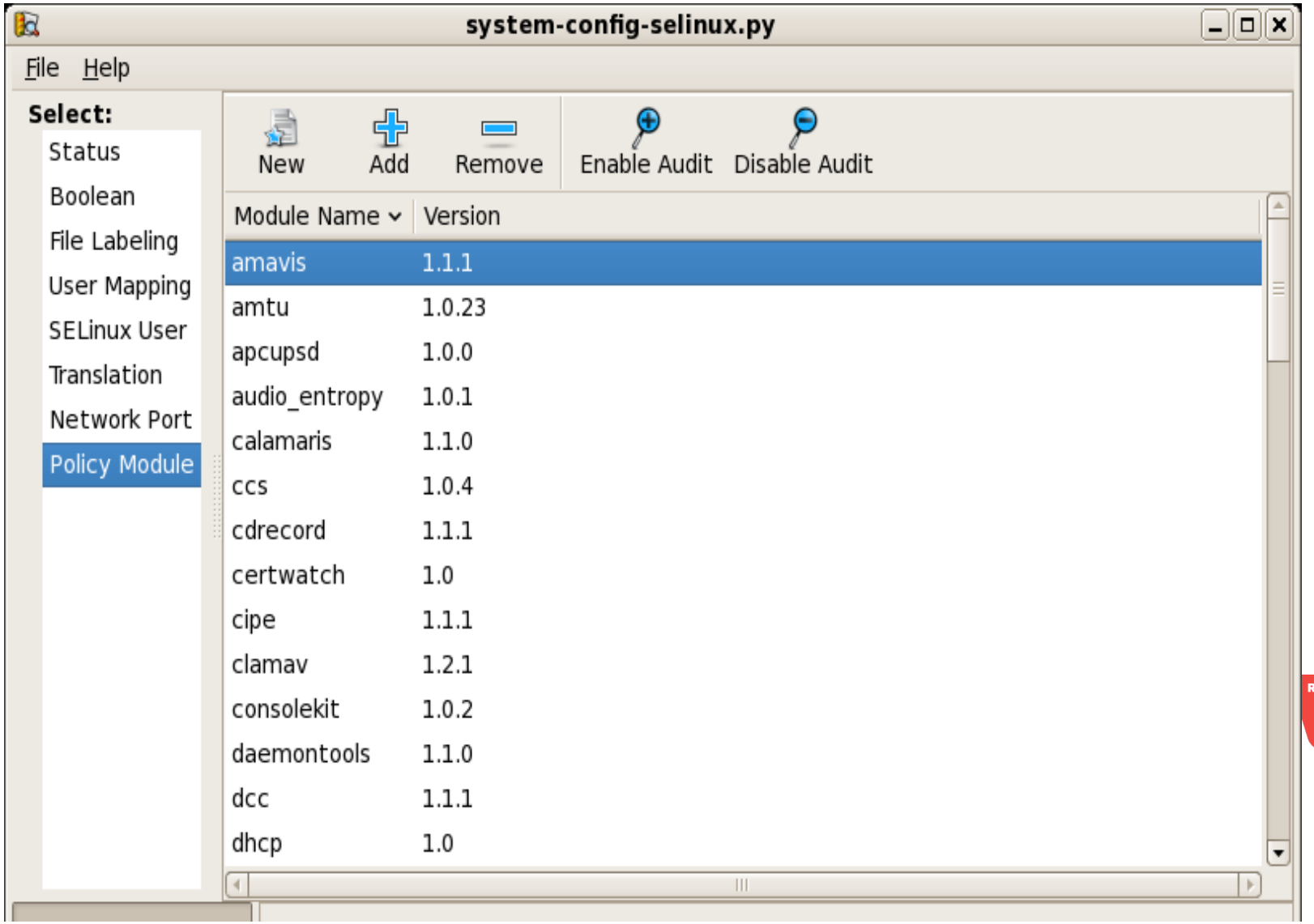
Just make it work????

```
# grep httpd /var/log/audit/audit.log | audit2allow -M myhttp
# semodule -i myhttpd.pp
```

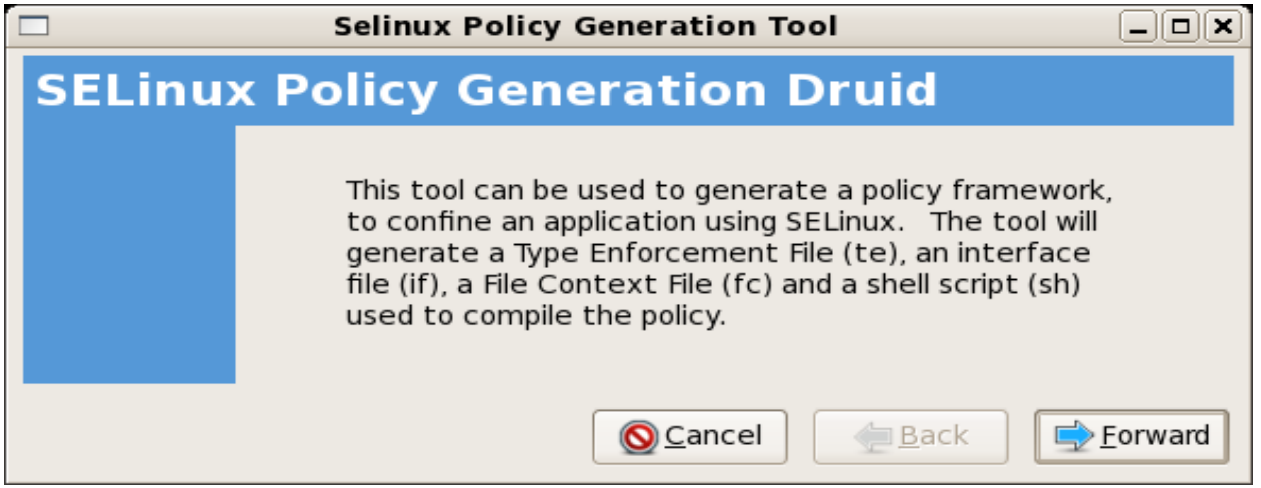
Manageable - Configurable

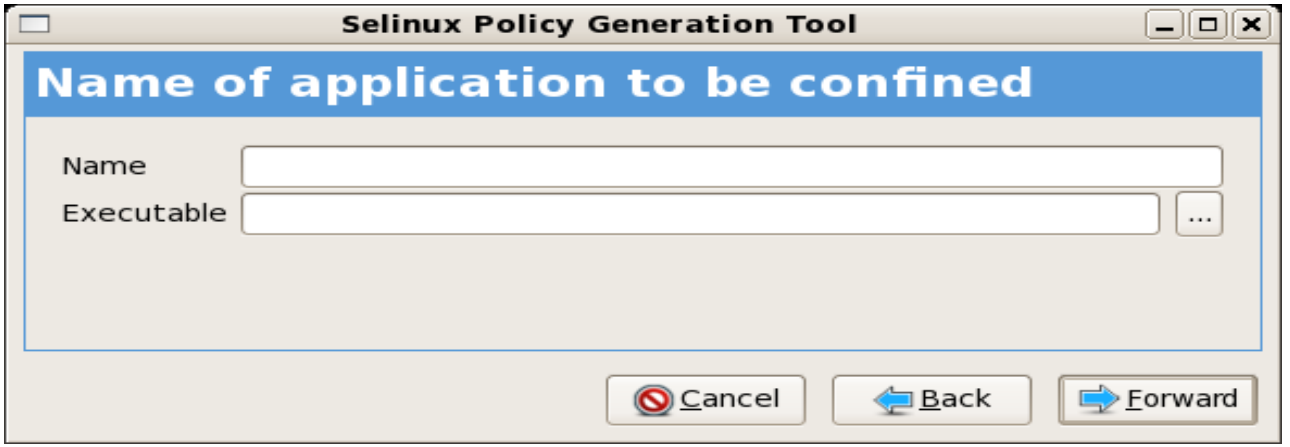


Manageable - Customizable



Manageable - Customizable





Manageable - Bugzilla Module

```
========================= Policy ========================================
policy_module(bugzilla, 1.0)
apache_content_template(bugzilla)
allow httpd_bugzilla_script_t self:netlink_route_socket r_netlink_socket_perms;
files_search_var_lib(httpd_bugzilla_script_t)
optional_policy(`
        mysql_search_db(httpd_bugzilla_script_t)
        mysql_stream_connect(httpd_bugzilla_script_t)
')
optional_policy(`
        postgresql_stream_connect(httpd_bugzilla_script_t)
')
============================== File context ============================
/usr/share/bugzilla(/.*)? -d gen_context(system_u:object_r:httpd_bugzilla_content_t,s0)
/usr/share/bugzilla(/.*)? -- gen_context(system_u:object_r:httpd_bugzilla_script_exec_t,s0)
/var/lib/bugzilla(/.*)?         gen_context(system_u:object_r:httpd_bugzilla_script_rw_t,s0)
```

Ultra Secure

Ultra Secure

- Collaborative Effort

Ultra Secure

- Standards
  - Controlled Access Protection Profile - EAL4/CAPP
  - Labeled Security Protection Profile - EAL4+/LSPP
  - Multi Level Security (MLS)
  - SELinux is the only mainstream OS in the world with MLS AND Type Enforcement.
  - SELinux is being used all over Department of Defense including War Zones.
  - Unlike Trusted OS's
    - SELinux == Red Hat Enterprise Linux

S.M.U.T

- **S**ecure
- **M**anageable
- **U**ltra **T**rusted

If you want to protect your data.

Run it on

Red Hat Enterprise Linux 5

with SELinux

Leave
SELinux
running Everywhere

BONUS – Who wants to write Policy???

Today – Here 5:15

Harbor Island 2

Conference Room

Writing SELinux Policy B.O.F.