

# What is SELinux trying to tell me?

The 4 key causes of SELinux errors.

# SELinux Problem Solutions

1. SELinux == Labeling
2. SELinux Needs to Know
3. SELinux Policy/Apps can have bugs.
4. You could be **COMPROMISED!!!!**

# SELinux == Labeling

- Every process and object on the machine has a label associated with it
- If your files are not labeled correctly access might be denied.
  - If you use alternative paths for confined domains SELinux needs to KNOW.
  - http files in /srv/myweb instead of /var/www/html? Tell SELinux.
    - # semanage fcontext -a -t httpd\_sys\_content\_t '/srv/myweb(/.\*)?'
    - # restorecon -R /srv/myweb

# SELinux == Labeling

The screenshot shows the SELinux Administration tool interface. On the left, a 'Select:' menu is open, highlighting 'File Labeling'. The main window displays a table of SELinux file specifications. A dialog box titled 'Add File Labeling' is overlaid on the table, showing the following fields:

- File Specification: `/srv/myweb(/.*)?`
- File Type: `all files`
- SELinux Type: `httpd_sys_content_t`
- MLS: `s0`

The dialog box has 'Cancel' and 'OK' buttons. The background table shows various file specifications and their corresponding SELinux types and file types.

File Specification	SELinux Type	File Type
/		directory
/*		all files
/[^/]+		regular file
/afs		directory
/a?quota\(user group\)		regular file
Λ.autofsck		regular file
Λ.autorelabel		regular file
/bin	bin_t:s0	directory
/bin/*	bin_t:s0	all files
/bin/alsaunmute	alsa_exec_t:s0	regular file
/bin/bash	shell_exec_t:s0	regular file
/bin/bash2	shell_exec_t:s0	regular file
/bin/d?ash	shell_exec_t:s0	regular file

# SELinux == Labeling

- Fedora 11 introduces equivalency labeling
  - `semanage fcontext -a -e /srv/myweb /var/www`
    - Tells SELinux to label all files directories under `/srv/myweb` the same as `/var/www`
    - `/srv/myweb/cgi-bin/mycgi.cgi` will get labeled `httpd_sys_script_t`
  - `semanage fcontext -a -e /export/home /home`
    - Label all files under `/export/home` as if they were under `/home`
    - `/export/home/dwalsh/.ssh` will get labeled `ssh_home_t`

# SELinux needs to KNOW

→ How did you configure your apache server?

Tell SELinux!!

→ If you want httpd to send email

→ # setsebool -P httpd\_can\_sendmail 1

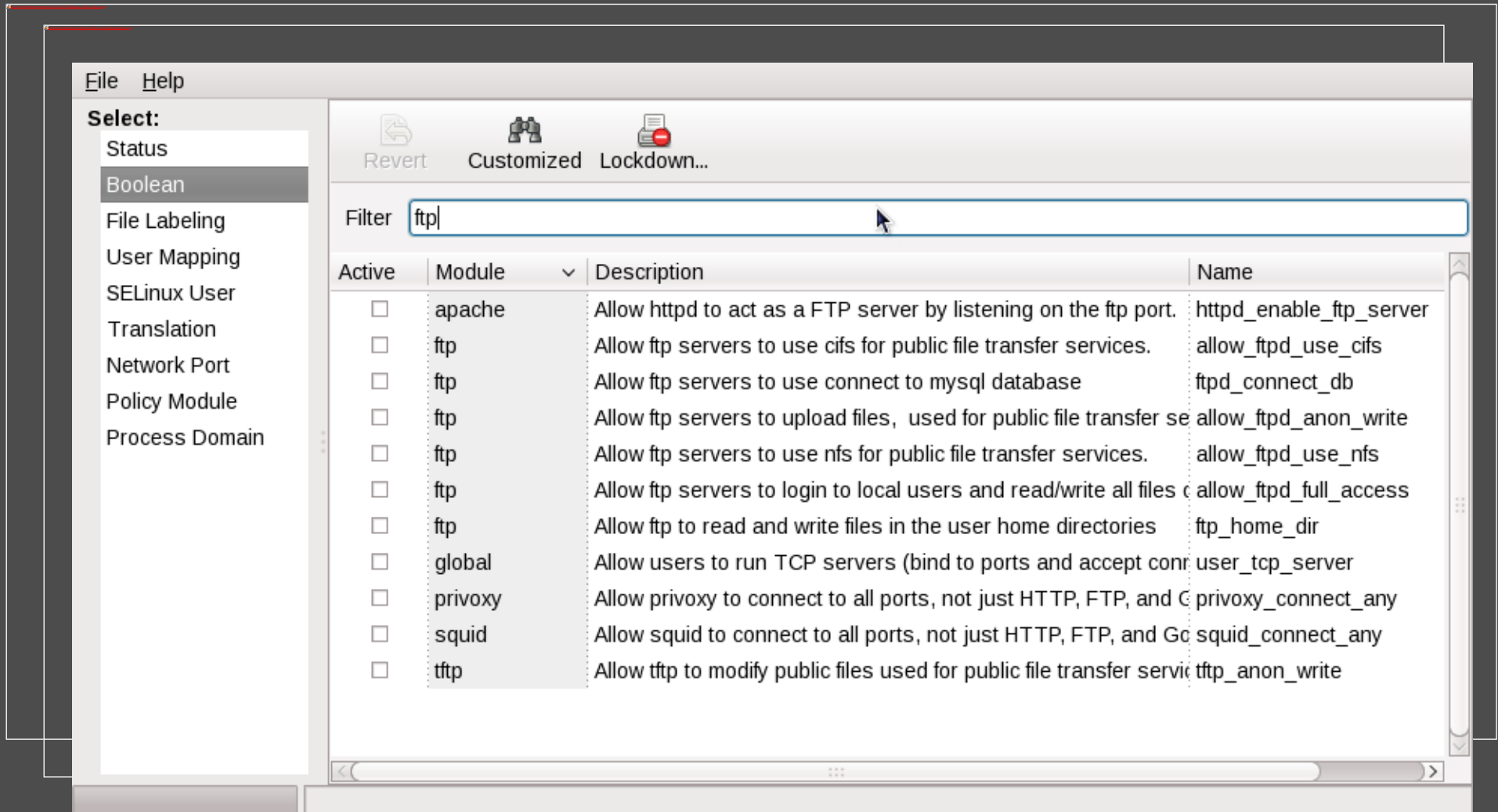
→ Vsftp setup for users to login

→ # setsebool -P ftp\_home\_dir 1

→ Http is setup to listen on port 8585

→ # semanage port -a -t http\_port\_t -p tcp 8585

# SELinux needs to KNOW



The screenshot shows the SELinux Manager application window. The left sidebar has a 'Select:' menu with options: Status, Boolean (selected), File Labeling, User Mapping, SELinux User, Translation, Network Port, Policy Module, and Process Domain. The main area has a toolbar with 'Revert', 'Customized', and 'Lockdown...' buttons. A search filter 'ftp' is entered in the top text box. Below is a table of SELinux modules.

Active	Module	Description	Name
<input type="checkbox"/>	apache	Allow httpd to act as a FTP server by listening on the ftp port.	httpd_enable_ftp_server
<input type="checkbox"/>	ftp	Allow ftp servers to use cifs for public file transfer services.	allow_ftpd_use_cifs
<input type="checkbox"/>	ftp	Allow ftp servers to use connect to mysql database	ftpd_connect_db
<input type="checkbox"/>	ftp	Allow ftp servers to upload files, used for public file transfer se	allow_ftpd_anon_write
<input type="checkbox"/>	ftp	Allow ftp servers to use nfs for public file transfer services.	allow_ftpd_use_nfs
<input type="checkbox"/>	ftp	Allow ftp servers to login to local users and read/write all files c	allow_ftpd_full_access
<input type="checkbox"/>	ftp	Allow ftp to read and write files in the user home directories	ftp_home_dir
<input type="checkbox"/>	global	Allow users to run TCP servers (bind to ports and accept conn	user_tcp_server
<input type="checkbox"/>	privoxy	Allow privoxy to connect to all ports, not just HTTP, FTP, and G	privoxy_connect_any
<input type="checkbox"/>	squid	Allow squid to connect to all ports, not just HTTP, FTP, and Gc	squid_connect_any
<input type="checkbox"/>	tftp	Allow tftp to modify public files used for public file transfer servi	tftp_anon_write

# SELinux needs to KNOW





# SELinux Policy/Apps Can Have bugs

- SELinux Policy might have a bug
  - Unusual Code Paths
  - Configurations
  - Redirection of stdout
- Apps have bugs
  - Leaked File Descriptors
  - Executable Memory
  - Badly built libraries
- Report the bugs in Bugzilla so we can fix them

# SELinux Policy/Apps Can Have bugs!!!

- You can tell SELinux to just allow
  - Selinux is blocking postgresql
    - Labeling is correct? No appropriate boolean?
    - Use audit2allow to build a policy module
      - `#grep postgresql /var/log/audit/audit.log | audit2allow -M mypostgresql`
      - `# semodule -i mypostsq1.pp`
  - Examine mypostgresql.te
    - Make sure you are not allowing too much?
    - Ask for help?
      - #fedora
      - Fedora-selinux mail list
      - [dwalsh@redhat.com](mailto:dwalsh@redhat.com)

# You could be COMPROMISED!!!

- Current tools do not do a good job of differentiating
  - If you have a confined domain that tries to:
    - Load a kernel module
    - Turn off SELinux enforcing mode
    - Write to etc\_t? shadow\_t
    - Modify iptables rules
    - Sendmail????
    - others
  - You might be compromised