RecipeSELinux

This page documents how to get tiki working on Fedora Core 3 with SELinux enabled.

Background and Introduction

SELinux (Security-Enhanced Linux) is a set of modifications to the Linux kernel and several additional packages that provide extra security to a Linux system beyond the normal protections built into Linux/Unix.

SELinux is installed by default with Fedora Core 3. The default mode, or Policy Type, for SELinux is "Targeted". Targeted operation allows most activities to proceed normally, but can audit the operation of specific servers, including apache httpd, for the purposes of detecting and preventing possible security breaches.

Fedora Core 3 SELinux FAQ is a FAQ dealing with SELinux under Fedora Core 3. It contains links to the primary information sources regarding SELinux. Fedora Core 3 Apache HTTP SELinux Policy details understanding and customizing the SELinux policy for Apache httpd.

The gui for controlling SELinux is available from the Applications->System Settings->Security Level menu selection. Or by the command line: [root ~]# system-config-securitylevel

Under the default installation for Fedora Core 3, SELinux prevents Apache httpd from running Tiki. To allow tiki to run you must edit the SELinux policy file, contained in /etc for Apache httpd. The files are:
/etc/selinux/targeted/src/policy/types/apache.te
/etc/selinux/targeted/src/policy/macros/program/apache_macros.te
/etc/selinux/targeted/src/policy/file_contexts/program/apache.fc
/etc/selinux/targeted/src/policy/domains/program/apache.te

This document details one strategy for modifing the SELinux policy to allow apache to run tikiwiki.

Requsites

This document assumes you are running Fedora Core 3 and have root access.

You must have the following rpm's installed:
httpd
system-config-httpd
httpd-suexec
httpd-manual
selinux-policy-targeted
libselinux
libselinux-devel
selinux-policy-strict
selinux-policy-targeted-sources

Check for rpmnew config files that may have been left by yum update:
cd etc/
find . -name "*.rpmnew" -print
You have to merge them into you changed config files or replace the outdated config files, e.g.:

root@grant targeted# cd /etc/selinux/targeted/policy/
root@grant policy# mv policy.18.rpmnew policy.18
root@grant policy# cd /etc/selinux/targeted/contexts/files/
root@grant files# mv file_contexts.rpmnew file_contexts

Check for the latest versions of the packages we'll be using, e.g.:
yum -y update

Add new Policies

To update the policies, you need to become root on the machine.

Add the following file as /etc/selinux/targeted/src/policy/domains/misc/local.te

```
allow httpd_sys_script_t self:capability { chown dac_override fowner fsetid };
allow httpd_sys_script_t devpts_t:chr_file { read write };
allow httpd_sys_script_t devpts_t:chr_file { getattr ioctl };

allow httpd_sys_script_t devpts_t:dir search;
```

To compile the new rules, enter the following commands:

```
cd /etc/selinux/targeted/src/policy make reload
```