SELinux in 20 Minutes

LCA Miniconf
Jan. 28th, Canberra AU

Who's talking?

- Sander van Vugt
- Author, technical trainer and consultant
  - High Availability, Performance and trying to understand SELinux
- mail@sandervanvugt.com
- Www.sandervanvugt.com
  - Check my SELinux article on http://www.sandervanvugt.com/index.php?site=view&topic=88

Who's listening?

This talk is for sysadmins that normally would just switch off SELinux because they don't know how to handle it

Without SELinux

- How are you going to ensure that a web server that's running hundreds of scripts is secure?
- Intruders just could break in through a script, get shell access and do nasty things from there

The purpose of SELinux

- Block all syscalls
- Allow only those syscalls that have been specifically allowed
- Which probably blocks many services that you actually need

The core element: the Policy

- Used to define which object gets access to which other object
- Implemented by working with contexts
  - User
  - Role
  - Type
- Rules define which source objects get access to which target objects
- Different policies for different environments
-

The modular policy

- Input files are in /etc/selinux/refpolicy/policy
  - .te files contain everything a module should have
  - .if files define how other modules get access to this module
  - .fc files contain labeling instructions
- Compiled policy files have the .pp extension and can be managed with semodule

Managing SELinux

- Use sestatus [-v] to see if it's alive
- Set permissive mode to start from scratch
- Use semanage to set context
- Use setsebool to switch on/off specific rules
- Use semodule to work with modules
- Switch on auditing and check the /var/log/audit/audit.log
- Use audit2allow to convert denials into something that works

And do not use setenforce to turn it off!

Just use audit2allow instead

- audit2allow -w -a presents the audit information in a more readable way
- audit2allow -a shows the type enforcement rule that allows the denied access
- audit2allow -a -M blah creates a .te file and a compiled .pp file that will allow the denied access
- Use semodule -i to enable this module

Common admin commands

- semanage -a -t httpd_sys_content_t “/web/(.*)?”
- restorecon -Rv /web
- getsebool -a | grep something
- setsebool -P something_setting = on

Installing SELinux

- Easy on distributions that have it by default
- A bit complicated on distributions that don't do SELinux by default
  - A generic policy cannot set context for all objects on an unknown distribution

Enabling SELinux on OpenSUSE 12.2

- Switch on kernel options: security=selinux selinux=1 enforcing=0
- Download and install the source policy
- Compile the source policy
  - Modify /etc/selinux/refpolicy/build.conf
  - Don't forget /etc/selinux/config

Continuing the configuration

- Use the selinux-ready command
- Relabel the file system
- Start analyzing and modifying to make it match (audit2why is useful!)
- Once it all works, use setenforce 1 to enable SELinux protection
- Tip: use unconfined_t on services that you want to run without selinux protection

Additional questions?

Mail me at mail@sander.fr