Introduction to

Security Enhanced Linux

Clint Savage
For
Backcountry.com

What is SELinux?

- Developed by the NSA to prevent world access to file system, process, ports and more
- Mach - first implementation of SELinux as a distro
  - Made a kernel implementation instead
- Available in Linux since ~RHEL4 (2005)

SELinux – Core Concepts

- Mandatory Access Control (MAC) vs Discretionary Access Control (DAC)
- Policy determines access restrictions
- If not defined, denied by default

SELinux – Security Contexts

- All files, process, ports, etc. have a security context
  - Because everything is a file, this makes security easy.
- There are 5 parts to a context
  - user:role:type:sensitivity:category
  - eg. user_u:object_r:httpd_t:s0:c0
  - RHEL doesn’t use sensitivity or category (yet)

SELinux – Displaying Context

Displaying contexts is simple

- Files

  $ ls -ldZ /var/www/httpd

  drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/

- Processes

  ps -efZ | grep httpd

  unconfined_u:system_r:httpd_t:s0 root 10613 1 6 09:49 ? 00:00:00 /usr/sbin/httpd

  unconfined_u:system_r:httpd_t:s0 apache 10615 10613 0 09:49 ? 00:00:00 /usr/sbin/httpd

SELinux – Targeted Policy

- Default Policy on CentOS / RHEL / Fedora
  - Ubuntu supports SELinux but doesn't enable by default
- Local processes are most *unconfined*
  - SELinux doesn't enforce upon ls, mv, cp, etc.
- Uses type enforcement
  - Type in the context is used to enforce most rules

SELinux – Changing Contexts

- Userland tools to change SELinux Contexts
  - chcon
    - Can change user, role, type, etc.
    - chcon -t tmp_t /etc/hosts
  - restorecon
    - Uses the policy to apply the rule
    - Generally recommended over chcon
    - restorecon /etc/hosts

SELinux – Management

- Three basic modes
  - Enforcing
    - Policy is in force, access is limited, errors logged
  - Permissive
    - Policy is not in force, access is not limited, errors logged
  - Disabled
    - NEVER USE THIS
    - SELinux is not running at all
    - Policy isn’t used, errors not are logged

SELinux – Turning it on/off

- Changing modes
  - Changing enforcement allowed in targeted policy
  - getenforce
    - Reports permissive or enforcing modes
  - setenforce 0 | 1
    - 0 = Permissive, 1 = Enforcing
  - Edit /etc/sysconfig/selinux
    - Can set policy and mode

SELinux – Example

- Let’s show a semi practical example
  - httpd process has access to files with httpd_syscontent_t type in the selinux context
  - Putting a file in /var/www/html without that context will fail when selinux is enforcing

SELinux -- Troubleshooting

- setroubleshoot (daemon is setroubleshootd)
  - Provides human readable information about selinux messages
  - Explains how to deal with the errors and such

SELinux – Other Tools

- Semanage
  - Get a list of contexts and what they apply
  - Permanent modifications of policy
    - Add a new policy rule
    - Modify a policy rule to be more strict / lenient
- Audit2allow
  - Provides a way to create selinux modules when the current policy doesn't have anything (remember, default is deny)

SELinux – Conclusion

- Use SELinux in permissive mode to help configure your box with better security
- NEVER EVER disable SELinux – there is no reason to do this!!
- Use chcon and restorecon to test policy changes
- Use setroubleshoot to solve problems
- Use semanage to permanently modify the SELinux policy