Selinux

Иртегов Д.В.

Новосибирский гос. Университет

2022

Что такое selinux

- Mandatory access control – принудительные права доступа
- Вводит дополнительную систему прав на файлы
  - Типы (обычно атрибут файла, например etc_t или httpd_sys_content_t)
  - Домены (обычно атрибут процесса, например httpd_t)
  - Роли и правила (rules), которые определяют, какие домены имеют доступ к каким типам, например, httpd_t может читать httpd_sys_content_t
- Как правило, типы файлов определяются политикой
- Произвольно менять типы файлов и процессов могут только процессы домена unconfined_t, напр. интерактивный шелл root

Как это работает

$ ls -Z /var/www/html/file1
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file1

- Политика говорит, что файлы в /var/www/html имеют тип httpd_sys_content_t
- Файлы в других местах такого типа не имеют
- Если httpd поломают или админ ошибется в его настройке, он не получит доступа за пределы /var/www/html
- Упрощает жизнь аудиторам систем безопасности

Что делать если правила selinux слишком ограничивают?

- Подумать еще раз
  - Большинство приложений имеет готовые политики, которые рассчитаны на разумные умолчания и seboolean для разумных вариантов использования
- Поставить тип файлам руками
  - хрупко, новые файлы могут не получить новых типов
- Создать свою политику или изменить существующую
  - много писанины, но рекомендованный способ
- Отключить selinux
  - Плохая идея

Утилиты

- ls -lZ – посмотреть selinux атрибуты файла
- ps -Z – посмотреть selinux атрибуты процессов
- chcon – произвольно установить атрибуты файлов (в т.ч. рекурсивно)
- restorecon – установить атрибуты файлов в соответствии с действующими политиками
- semanage fcontext – установить правило, как если бы оно было частью политики
  - semanage fcontext -a -t httpd_sys_content_t "/my(/.*)?"

Seboolean

- Флаги, позволяющие кастомизировать политику
- Например, httpd_enable_homedirs разрешает httpd доступ к файлам /home/*/public_html
- Список флагов можно получить командой semanage boolean –l
  - Он длинный и не все внятно документированы
  - Флаги – часть политик, новые политики могут добавлять новые флаги

Что-то идет не так?

- Включить и выключить selinux
  - Setenforce (permissive/enforcing)
  - Совсем выключить: в /etc/selinux/config написать SELINUX=disabled и перезагрузиться
- В permissive Selinux ругается на все операции, которые в enforcing он бы запретил
- **ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts recent**
- **dmesg | grep -i -e type=1300 -e type=1400**

Как получить человеко-читаемое сообщение?

- Sealert (пакет policycoreutils-python-utils)

```
$ sealert -l "*"
SELinux is preventing /usr/bin/passwd from write access on the file
/root/test.

*****  Plugin leaks (86.2 confidence) suggests ****************************

If you want to ignore passwd trying to write access the test file,
because you believe it should not need this access.
Then you should report this as a bug.
You can generate a local policy module to dontaudit this access.
Do
# ausearch -x /usr/bin/passwd --raw | audit2allow -D -M my-passwd
# semodule -X 300 -i my-passwd.pp

*****  Plugin catchall (14.7 confidence) suggests **************************

...

Raw Audit Messages
type=AVC msg=audit(1553609555.619:127): avc:  denied  { write } for
pid=4097 comm="passwd" path="/root/test" dev="dm-0" ino=17142697
scontext=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
```