SELinux (англ. *Security-Enhanced Linux — Linux* с улучшенной безопасностью) — реализация системы принудительного расширенного контроля доступа. При этом *SELinux* действует поверх встроенной безопасности *Linux,* поэтому через *SELinux* нельзя разрешить то, что запрещено через права доступа пользователей или групп. Система *SELinux* (*SELinux*) реализованная на уровне ядра ОС.

По существу, SELinux реализует принудительную (или мандатную) модель управления доступом (англ. Mandatory Access Control, MAC) поверх существующей дискреционной (или избирательной) модели (англ. Discretionary Access Control, DAC), то есть разрешений на чтение, запись, выполнение.

При использовании избирательной политики контроля доступа операционная система дает доступ к ресурсам основывается на правах доступа пользователя трех уровней - *rwx* для типов пользователей владелец, группа-владелец и остальные.

В *SELinux* права доступа задаются помощи специально определенных политик. Политики работают на уровне системных вызовов и применяются ядром ОС или на уровне приложения. Политики *SELinux* описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила *SELinux* «прозрачны» для приложений, и не требуется никакой их модификации. В состав некоторых дистрибутивов входят готовые политики, в которых права могут определяться на основе совпадения типов процесса (субъекта) и файла (объекта) — это основной механизм SELinux.

В Security Enhanced Linux механизм мандатного управления доступом реализован в виде двух форм:

MLS (Multi-Level Security, многоуровневая система безопасности) / MCS (Multi Categories Security, мультикатегорийная безопасность) - нет записи вниз, нет чтения вверх, то есть субъект с уровнем допуска «секретно» может получить доступ к объекту с таким же уровнем секретности или ниже.

TE (Type Enforcement, принудительная типизация доступа) - каждый субъект и объект системы, ассоциируется с меткой, определяющей особенности его доступа.

Для проверки статуса *SELinux* можно воспользоваться командой

sestatus.

По умолчанию *SELinux* поддерживается многими дистрибутивами *Linux*. В дополнение к *SELinux* рекомендуется установить следующие утилиты:

- *policycoreutils-python* – базовый набор утилит для работы с *SELinux*
- *setroubleshoot* — инструмент, который анализирует сообщения об отказах *AVC*, сравнивает их со значениями в своей базе данных, а затем в

удобочитаемом виде выводит сообщения об отказе с пояснениями и предлагает возможные варианты решения проблемы.

Результат команды показывает статус: включение-выключение *SELinux,* Текущий режим (*Current mode*,) например - *enforcing*. Используемая сейчас политика *SELinux*, например *targeted*.

В *SELinux* возможны следующие режимы работы.

- *Enforcing*. Выбор этого значения приводит к применению текущей политики *SELinux*, при этом будут блокироваться все действия, нарушающие политику. Информация о заблокированных действиях заносится в журнальный файл. Режим *Enforcing* можно изменить без перезагрузки системы.
- *Permissive*. При указании этого параметра модулем *syslog* фиксируются попытки выполнения действий, противоречащих текущей политике безопасности, однако фактического блокирования действий не происходит. Режим *Permissive*, как правило, используется для отладки правил доступа. Смена этого режима на любой другой также не требует перезагрузки.
- *Disabled*. Данное значение в параметре *SELINUX* файла настроек полностью отключает подсистему обеспечения мандатного контроля доступа. При включении *SELinux* в любом режиме необходимо заново установить метки безопасности в файловой системе (обычно это делается в процессе перезагрузки системы и может потребовать несколько минут).

В режимах *Enforcing* и *Permissive SELinux* сохраняет сообщения в журнальный файл о заблокированных действиях от имени *AVC (Access Vector Cache)*. Однако разница между этими режимами, помимо блокирования и разрешения действий, противоречащих политике безопасности, заключается еще и в том, что в режиме *Enforcing*, чтобы не перегружать систему избыточными сообщениями, в файл записывается информация только о первом нарушении объектом области разрешений. В режиме *Permissive* сохраняется запись о каждом из таких нарушений, поэтому в данном режиме удобно проводить отладку политики безопасности.

В *SELinux* возможны следующие типы политики:

- *targeted* - защищает основные системные сервисы, например, веб-сервер, *DHCP, DNS*, но не трогает все остальные программы.
- *strict* - самая строгая политика, управляет не только сетевыми службами, но и программами пользователя.
- *minimum – модифицированная политика targeted*, распространяющаяся только на отдельные файлы.

- *mls* - содержит не только правила, но и различные уровни безопасности. Она позволяет реализовать многоуровневую систему безопасности на основе *SELinux*.

Также можно добавить свои политики. Для применения политики необходимо перезагрузить компьютер, и желательно чтобы *SELinux* во время этой перезагрузки был в режиме аудита (*permissive*). Также, чтобы система обновила все метки в файловой системе, возможно, придется создать пустой файл в корне: *sudo vi /.autolabel.*

Политика SELinux — это набор правил, которыми руководствуется механизм безопасности SELinux. Политика определяет набор правил для конкретного окружения. Политикой *SELinux* можно управлять через настройки конфигурационного файла, который находится по адресу /etc/selinux/config. В данном файле можно выполнять менять настройки в режиме суперпользователя.

Задание 1.

1. Определите, используется ли SELinux, при помощи запроса

   $ ldd /bin/ls | grep selinux
2. Переведите SELinux в режим аудита.
3. Поменяйте политику SELinux.
4. Перезагрузите ПК.
5. Проверьте результат при помощи проверки статуса SELinux.

Примечание. Режим *SELinux* можно также поменять при помощи команды

sudo setenforce (setenforce 0 = permissive)

Посмотреть используемый режим *SELinux* можно командой:

getenforce

Каждый файл и каждый процесс имеет свою *SELinux* метку, которую принято называть контекстом. Каждая метка содержит такую информацию, как как пользователь, роль, тип и т.д. Мы будем оперировать типом, являющимся атрибутом *Type Enforcement.* Он определяется доменом для процессов и типом для файлов. В правилах *SELinux* описаны разрешенные типы взаимодействия. Доступ разрешается только в случае наличия соответствующего правила.

Какая метка будет присвоена тому или иному файлу или процессу определяется политикой, например *targeted*. Посмотреть контекст *SELinux* можно с помощью команды:

ls -Z для файлов и папок (также *semanage fcontext -l и ls --context)*;

ps Z для процессов;

id -Z для пользователей;

netstat -Z для портов.

Контекст предоставляет нам информацию о пользователе (например, *system_u*), его роли (например, *object_r*), о типе или домене (например, *admin_home_t*) и уровне (*s0*). Домен – это перечень того, что процессы могут делать или какие действия процесс может выполнять над различными объектами. Тип – атрибут объекта, он определяет, кто может получить к нему доступ. Роль – это атрибут RBAC (Role-based access control, Управление доступом на основе ролей), «промежуточное звено» между пользователем *SELinux* и доменами. Он определяет, в какие домены может входить пользователь. Иными словами: роль – это список доменов, которые пользователь имеет право запускать. Уровень – этот атрибут используется в политиках *MLS/MCS*.

Если вы впервые включаете *SELinux*, то сначала нужно настроить контекст и метки. Процесс назначения меток и контекста известен как маркировка. Чтобы начать маркировку, в файле конфигурации изменим режим на permissive. После этого лучше создать в корне файл *autorelabel* (*touch /.autorelabel*) и перезагрузить систему. После того, как маркировки будут установлены, можно вернуть режим *enforce*.

Задание 2.

1. Посмотрите на особенности контекстов безопасности корневого каталога *Linux*.

При этом стоит обращать внимание на третье с конца поле. Для файлов или папок оно называется типом, а для процессов доменом. Например, у папки */bin* тип *bin_t*. Это значит, что в отношении папки имеется специальные указания.

2. Изучите особенности контекста таких файлов, как */etc/passwd /etc/group, /etc/shadow, /etc/login.defs /etc/sudoers /etc/shadow $ ls -Z /etc/passwd /usr/bin/passwd, /usr/sbin/useradd*.
3. Изучите особенности контекста таких папок, как *root/ и home/*.
4. Изучите особенности контекста суперпользователя и вашего пользователя.
5. Изучите особенности контекста таких процессов, как *httpd* и *bash*. При этом обращать внимание на третье с начала поле. Например, политика unconfined_t, это означает, что им будут доступны все без исключения ресурсы в системе.
6. Изучите особенности контекста таких процессов, как смена пароля пользователя ($(*pgrep passwd*)).
7. Изучите особенности контекста таких портов, как *auditd*.

Вы можете добавить дополнительные правила присвоения меток файлам в политику с помощью утилиты *semanage* или использовав специальную команду *chcon*. Например, если вы хотели бы чтобы у вас был веб-сервер, который вместо каталога */var/www/html/* использовал */home/{usr_name}/html/*. Простые попытки доступа к такому серверу *SELinux* сочтет это нарушением политики, и вы не сможете просматривать ваши веб-страницы. Это

потому, что вы не установили контекст безопасности, связанный с *HTML*-файлами. Для разрешения этой проблемы необходимо установить тип *httpd_sys_content_t* для нужной директории и всех файлов в ней. Для этого надо выполнить команды:

sudo semanage fcontext -a -t httpd_sys_content_t "/home/{usr_name}/html(/.)?"*

После этого необходимо перезагрузить контекст для папки или создать /.autolabel и перезагрузить ПК. Перезагрузка контекста может быть сделана как

restorecon -R -v /home/{usr_name}/html.

также можно задать временный контекст при помощи команды

sudo chcon -Rv --type=httpd_sys_content_t /home/{usr_name}/html;

также можно прописать полный контекст

sudo chcon -Rv system_u:object_r:httpd_sys_content_t:s0 /home/{usr_name}/html.

Возможно, в ходе маркировки могут возникнуть какие-то ошибки. Чтобы проверить, работает ли *SELinux* правильно и не блокирует ли он доступ к какому-либо порту, приложению и т. д. нужно посмотреть логи. Лог *SELinux* находится в */var/log/audit/audit.log*, но вам не нужно читать его целиком, чтобы найти ошибки. Можно использовать утилиту *audit2why* для поиска ошибок. Запустите следующую команду:

audit2why < /var/log/audit/audit.log.

Также можно проверить информацию об ошибках при помощи утилит *sealert* и непосредственно проверки *avc,* например при помощи запроса

ausearch -m avc -ts recent.

Задание 3.

1. Создайте в базовой директории папку mail и проверьте ее контекст.
2. Поверьте контекст папки mail в директории var.
3. Задайте папке mail в вашей директории такой же контекст при помощи команды *chcon*.
4. проверьте контекст.
5. перезагрузите папку, для которой вы изменили контекст и снова проверьте контекст.
6. Задайте контекст при помощи *semanage.*
7. проверьте контекст.
8. перезагрузите папку, для которой вы изменили контекст и снова проверьте контекст.
9. Проверьте, что переключение не дало ошибок – проверив логи.
10. Сделайте вывод о различии этих вариантов.

Переключатели (*booleans*) позволяют изменять части политики во время работы, без необходимости создания новых политик. Они позволяют вносить изменения без перезагрузки или перекомпиляции политик *SELinux*. Посмотреть на то, какие есть переключатели можно при помощи команды

semanage boolean -l .

Переключить один из переключателей, без перезагрузки ПК можно при помощи команды

setsebool {name} on .

Задание 4.

1. Проверьте состояние переключателей политики для *ftp* протокола.
2. переключите *ftp* для *home dir*.
3. Проверьте результат.
4. Проверьте, что переключение не дало ошибок – проверив логи.

Задание 5.

1. Установите *httpd elinks.*

2. Создайте новое хранилище для файлов *web*-сервера: web.

3. Создайте файл *index.html* в каталоге и поместите в файл текст, например: *Welcome to web-server*.

4. В файле */etc/httpd/conf/httpd.conf* измените параметр

DocumentRoot: DocumentRoot "/web"

и добавьте следующий раздел, определяющий правила доступа:

<Directory "/web">

AllowOverride None

Require all granted

</Directory>

5. Запустите веб-сервер и службу *httpd*

(*systemctl start httpd; systemctl enable httpd*)

7. При обращении к веб-серверу в текстовом браузере *elinks: elinks http://localhost* Вы увидите веб-страницу *Red Hat* по умолчанию, а не содержимое только что созданного файла index.html.

8. Переключите SELinux в разрешающий режим: setenforce 0

9. Снова обратитесь к веб-серверу: elinks http://localhost Теперь вы получите доступ к своей пользовательской веб-странице. Это показывает, что SELinux делает что-то для блокировки доступа.

10. Примените метку httpd_sys_content_t к /web.

11. Восстановите контекст безопасности: restorecon -R -v /web