Лабораторная работа №9

Отчет

Устинова Виктория Вадимовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов веб- службы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

3 Выполнение лабораторной работы

Просмотрите текущую информацию о состоянии SELinux(рис. 3.1).

Рис. 3.1: переходим в андмин. и смотрим информацию, селинукс активен и работает нормально

Посмотрите, в каком режиме работает SELinux, измените режим работы SELinux на разрешающий (Permissive)(рис. 3.2).

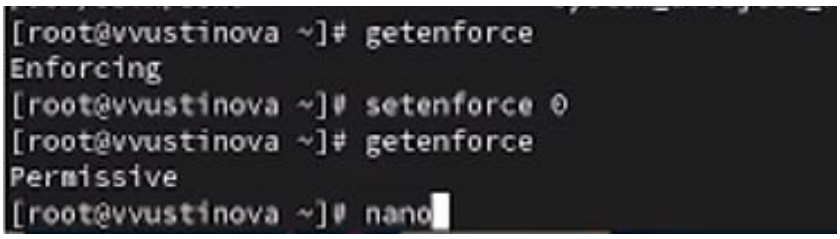

Рис. 3.2: SELinux работает в режиме enforcing, мы переключили его на Permissive

В файле /etc/sysconfig/selinux с помощью редактора установите disabled(рис. 3.3).

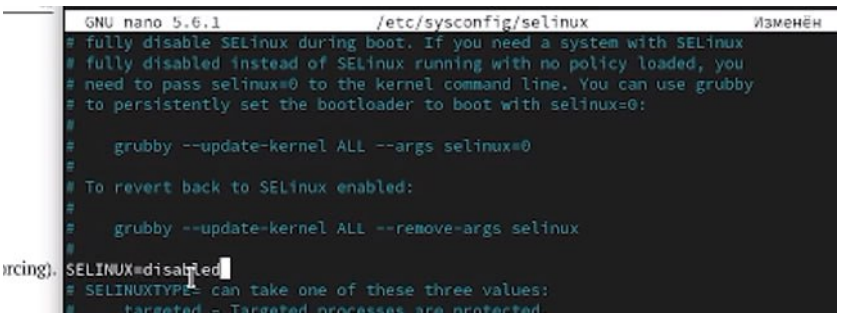

Рис. 3.3: заменяем enforcing на disabled и перезапускаем систему

После перезагрузки, посмотрите статус SELinux, попробуйте переключить режим работы SELinux(рис. 3.4).

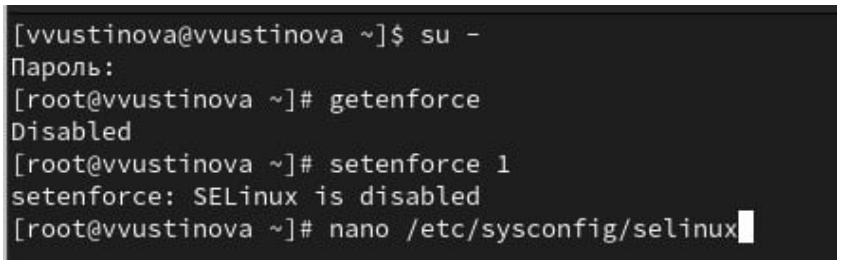

Рис. 3.4: Статус стал: disabled, не удается перкключить на режим работы потому что она отключена

Откройте файл /etc/sysconfig/selinux с помощью редактора и установите enforcing(рис. 3.5).

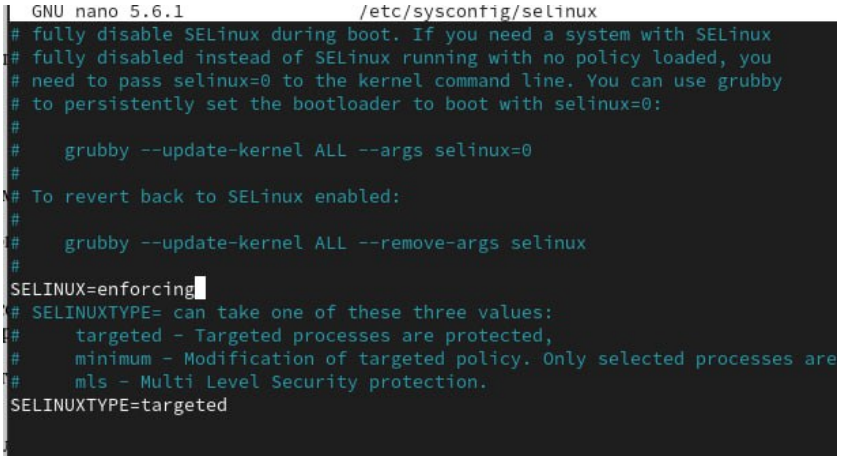

Рис. 3.5: Снова меняем, только теперь на enforcing

После перезагрузки, убедитесь, что система работает в принудительном режиме (enforcing) использования SELinux.(рис. 3.6).

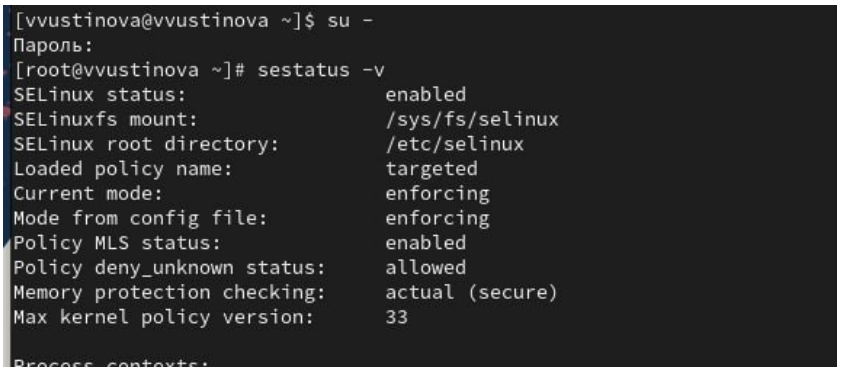

Рис. 3.6: Она активна и работает в принудительном режиме все верно

Посмотрите контекст безопасности файла /etc/hosts, Скопируйте файл /etc/hosts в домашний каталог, Проверьте контекст файла ~/hosts(рис. 3.7).

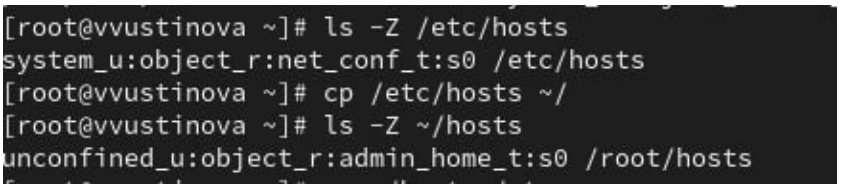

Рис. 3.7: у файла есть метка контекста net_conf_t., после копирования(что считается созданием нового файла) контекст стал admin_home_t.

Попытайтесь перезаписать существующий файл hosts из домашнего каталога в каталог /etc, убедитесь, что тип контекста по-прежнему установлен на admin_home_t(рис. 3.8).

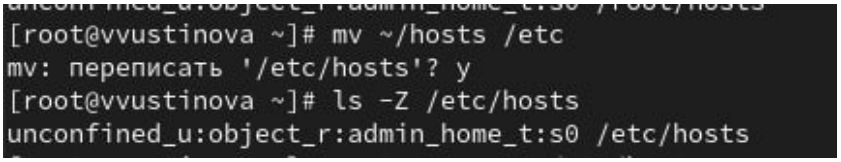

Рис. 3.8: Поддтвержаем перезаписывание файла и тип контекста все еще admin_home_t

Исправьте контекст безопасности, убедитесь, что тип контекста изменился,

для массового исправления контекста безопасности на файловой системе введите(рис. 3.9).

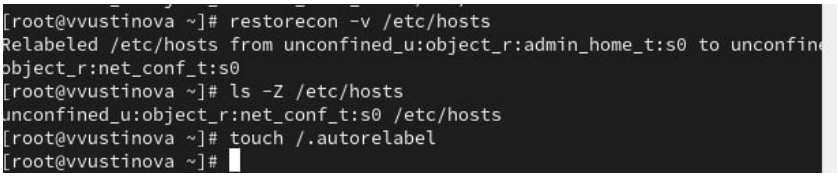

Рис. 3.9: Опция -v показывает процесс изменения, тип контекста изменился на net_conf_t, вводим команду и перезапускаем машину

Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения(рис. 3.10).

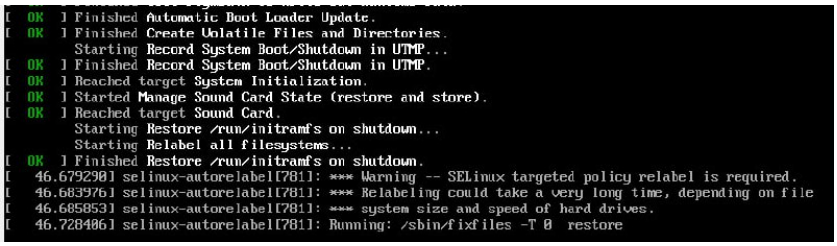

Рис. 3.10: нажимаем esc во время перезапуска и видим, что система перемаркированна автоматически

Создайте новое хранилище для файлов web-сервера, создайте файл index.html в каталоге с контентом веб-сервера, и поместите туда: Welcome to my web-server(рис. 3.11).

Рис. 3.11: создаем новое хранилище, переходим туда и создаем файл, через редактор nano добавляем туда строчку

В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot “/var/www/html” и ниже добавьте строку(рис. 3.12).

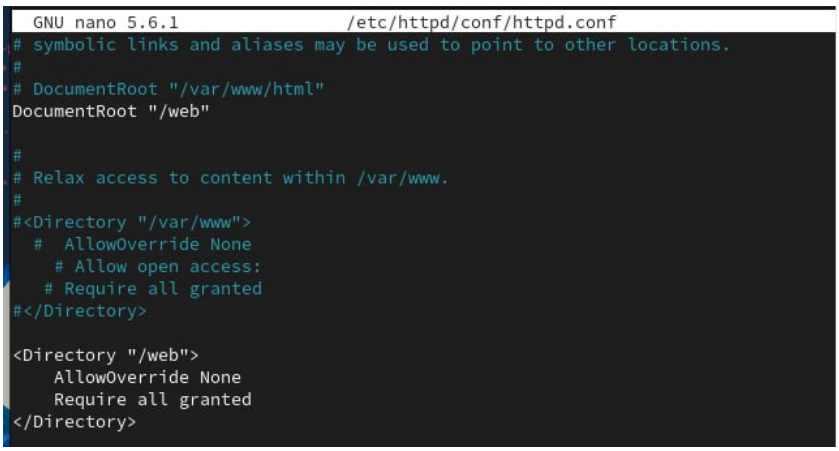

Рис. 3.12: Комментируем строчку и добавляем ниже:DocumentRoot “/web”, также ниже комментируем целый раздел и вместо него пишем другое

Запустите веб-сервер и службу httpd, в терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx, вы увидите веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.(рис. 3.13).

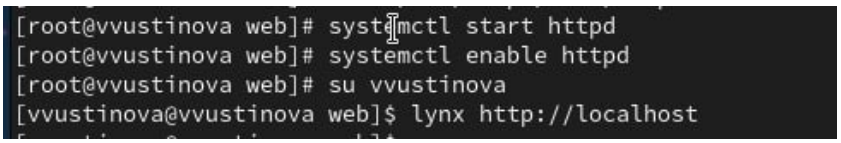

Рис. 3.13: Мы открыли файл и вышли из него

В терминале с полномочиями администратора примените новую метку контекста к /web, восстановите контекст безопасности(рис. 3.14).

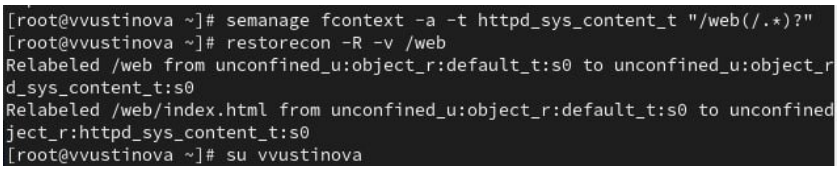

Рис. 3.14: Проделали все действия, и презагружаем машину

Теперь вы получите доступ к своей пользовательской веб-странице.В случае успеха на экране должна быть отображена запись «Welcome to my web-server».(рис. 3.15).

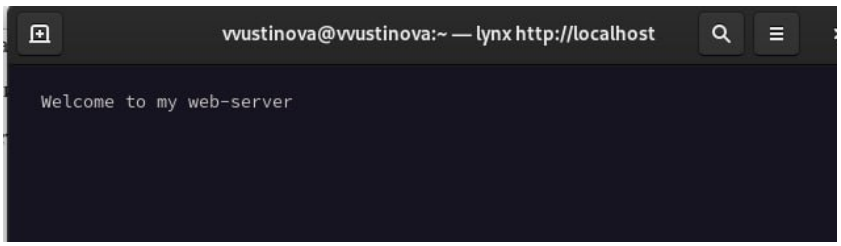

Рис. 3.15: Открываем и смотрим, у нас все получилось!

Посмотрите список переключателей SELinux для службы ftp, Вы увидите переключатель ftpd_anon_write с текущим значением off, для службы ftpd_anon посмотрите список переключателей (рис. 3.16).

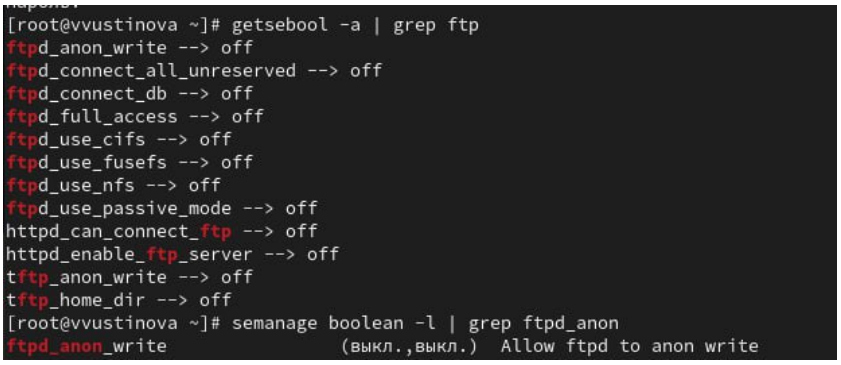

Рис. 3.16: Видим что все переключатели выключены

Измените текущее значение переключателя для службы ftpd_anon_write с off на on, овторно посмотрите список переключателей SELinux для службы ftpd_anon_write, посмотрите список переключателей с пояснением(рис. 3.17).

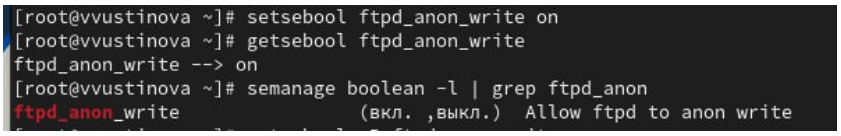

Рис. 3.17: Настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Измените постоянное значение переключателя для службы ftpd_anon_write с off на on, посмотрите список переключателей:(рис. 3.18).

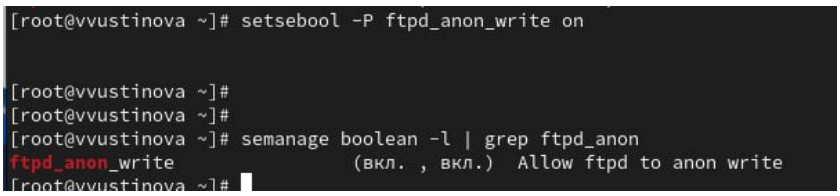

Рис. 3.18: Теперь все включено, переключатели разрешают анонимную запись на FTP сервер через селинукс

4 Выводы

Мы успешно получили навыки работы с контекстом безопасности и политиками SELinux.

5 Ответы на контрольные вопросы

1. Временно поставить SELinux в разрешающем режиме. Для этого используется команда setenforce 0. Это переводит SELinux из режима принудительного выполнения (enforcing), где он блокирует неразрешенные действия, в режим разрешения (permissive), где он лишь регистрирует нарушения, но не блокирует их. Это полезно для диагностики.

2. Список всех доступных переключателей SELinux. Чтобы получить полный список всех булевых переключателей SELinux и их текущее состояние, используйте команду semanage boolean -l. Эта команда также покажет краткое описание каждого переключателя.

3. Имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? Для автоматического анализа логов SELinux и получения легко читаемых, интерпретированных сообщений об отказах (denials), а также предложений по их устранению, необходимо установить пакет setroubleshoot-server. Он предоставляет утилиту sealert.

4. Команды, чтобы применить тип контекста httpd_sys_content_t к каталогу /web. Для применения файлового контекста httpd_sys_content_t к каталогу /web (и всем его подкаталогам), вам потребуется выполнить две команды: • Сначала добавьте правило для контекста файла: semanage fcontext -a -t httpd_sys_content_t “/web(/.*)?“. Эта команда говорит SELinux, что данный тип контекста должен применяться к указанному пути. • Затем примените

это правило к файловой системе: restorecon -Rv /web. Эта команда изменит контексты файлов на диске в соответствии с правилами fcontext.

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? Чтобы полностью отключить SELinux, необходимо отредактировать конфигурационный файл /etc/selinux/config. В этом файле нужно найти строку SELINUX=enforcing (или SELINUX=permissive) и изменить ее на SELINUX=disabled. После сохранения файла потребуется перезагрузить систему, чтобы изменения вступили в силу.

6. Где SELinux регистрирует все свои сообщения? SELinux регистрирует все свои сообщения, включая отказы доступа (AVC denials) и другие события, в системном журнале аудита. Этот журнал обычно находится по адресу /var/log/audit/audit.log. Просматривать его можно также с помощью утилиты journalctl.

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? Для получения более конкретной информации о контекстах, связанных с FTP, можно использовать следующие команды: • Для просмотра существующих правил файловых контекстов: semanage fcontext -l | grep ftp. • Для просмотра булевых переключателей, влияющих на FTP: semanage boolean -l | grep ftp. • Чтобы узнать, какие типы (types) в политике SELinux существуют для FTP, можно использовать seinfo -t | grep ftp.

8. Сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать? Самый быстрый способ определить, является ли SELinux причиной проблемы, это временно перевести его в разрешающий режим (permissive) с помощью команды setenforce 0. После этого попробуйте снова запустить проблемный сервис. Если сервис начинает работать нормально, то проблема связана с

политикой SELinux. Не забудьте вернуть SELinux в принудительный режим (setenforce 1) после завершения диагностики.