Отчёт по лабораторной работе №9

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Задание

1. Продемонстрировать навыки по управлению режимами SELinux.
2. Продемонстрировать навыки по восстановлению контекста безопасности SELinux.
3. Настроить контекст безопасности для нестандартного расположения файлов вебслужбы.
4. Продемонстрировать навыки работы с переключателями SELinux.

# 3 Выполнение лабораторной работы

## 3.1 Управление режимами SELinux

Запускаем терминала и получаем полномочия суперпользователя, используя *su -* (рис. 1)

Режим суперпользователя

Рис. 1: Режим суперпользователя

Посмотрим текущую информацию о состоянии SELinux, используя *sestatus -v* (рис. 2)

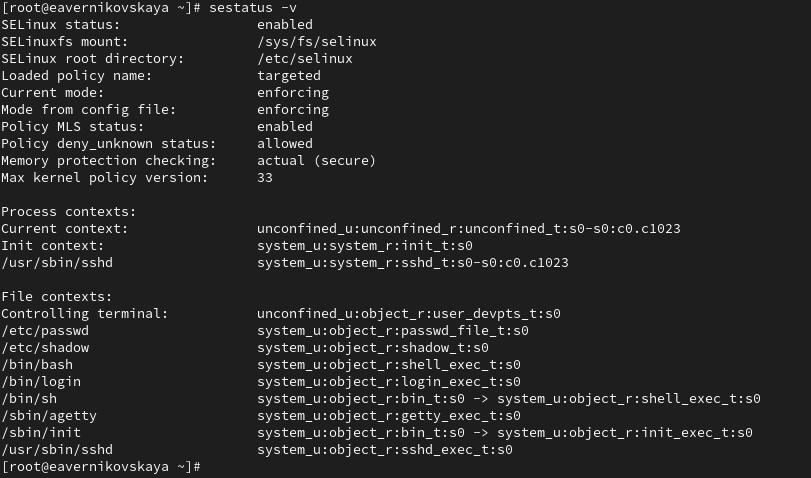


Рис. 2: Состояние SELinux (1)

**Основная информация о статусе SELinux:**

* **SELinux status:** enabled — SELinux включен в системе
* **SELinuxfs mount:** /sys/fs/selinux — путь, где монтируется файловая система SELinux
* **SELinux root directory:** /etc/selinux — корневой каталог, в котором хранятся конфигурационные файлы SELinux
* **Loaded policy name:** targeted — в системе загружена политика targeted, которая защищает определенные сервисы
* **Current mode:** enforcing — SELinux работает в режиме enforcing, то есть все запрещенные действия блокируются
* **Mode from config file:** enforcing — конфигурационный файл настроен на режим enforcing
* **Policy MLS status:** enabled — включена поддержка многоуровневой безопасности (MLS)
* **Policy deny\_unknown status:** allowed — неизвестные действия разрешены, но это обычно не рекомендуется
* **Memory protection checking:** actual (secure) — используется актуальная защита памяти
* **Max kernel policy version:** 33 — максимальная версия политики, поддерживаемая ядром

**Контексты процессов:**

* **Current context:** unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023 — текущий контекст пользователя, использующего терминал, показывает, что пользователь не ограничен политиками SELinux
* **Init context:** system\_u:system\_r:init\_t:s0 — контекст процесса инициализации (init), который запускается от имени system\_u
* **/usr/sbin/sshd:** system\_u:system\_r:sshd\_t:s0-s0:c0.c1023 — контекст для демона sshd (Secure Shell Daemon), запущенного от имени system\_u, чтобы ограничить его права в системе

**Контексты файлов:**

Каждая строка в этом разделе показывает файлы и процессы с их соответствующими SELinux-контекстами

* **Controlling terminal:** unconfined\_u:object\_r:user\_devpts\_t:s0 — терминал, к которому подключен пользователь, в контексте user\_devpts\_t
* **/etc/passwd и /etc/shadow:** находятся в контексте passwd\_file\_t и shadow\_t, что ограничивает доступ к этим файлам для повышения безопасности
* **/bin/bash:** контекст shell\_exec\_t, указывающий, что это исполняемый файл командной оболочки
* **/usr/sbin/sshd:** контекст sshd\_exec\_t, что позволяет SELinux определять, что этот файл — исполняемый файл SSH

Посмотрим, в каком режиме работает SELinux: *getenforce*. По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing) (рис. 3)

Режим работы SELinux (1)

Рис. 3: Режим работы SELinux (1)

Изменим режим работы SELinux на разрешающий (Permissive): *setenforce 0* (рис. 4)

Изменение режима работы SELinux на Permissive

Рис. 4: Изменение режима работы SELinux на Permissive

После, снова вводим *getenforce* (рис. 5)

Режим работы SELinux (2)

Рис. 5: Режим работы SELinux (2)

В файле /etc/sysconfig/selinux с помощью редактора устанавливаем параметр disabled: *SELINUX=disabled* (рис. 6), (рис. 7), (рис. 8)

Окрытие файла /etc/sysconfig/selinux (1)

Рис. 6: Окрытие файла /etc/sysconfig/selinux (1)

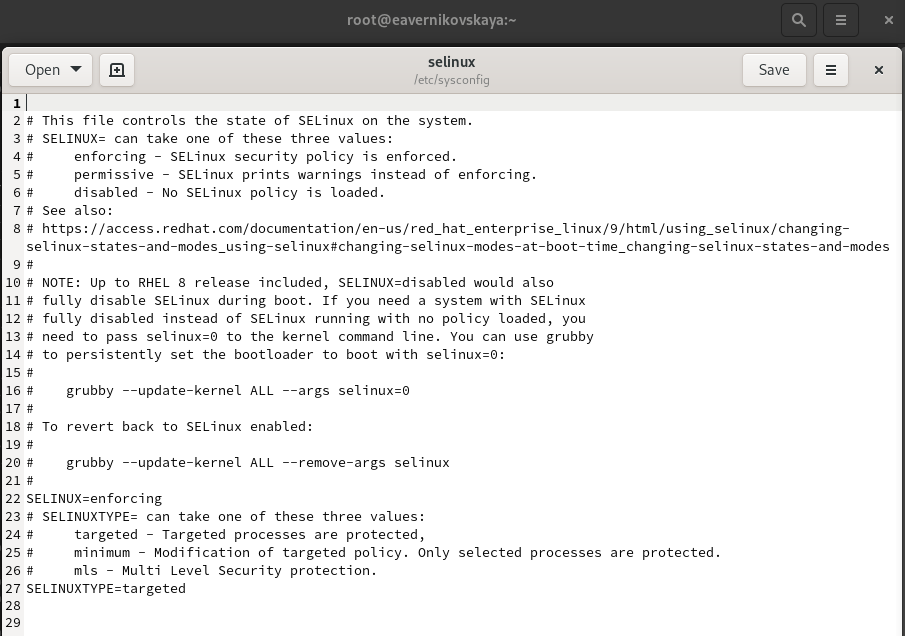


Рис. 7: Файл /etc/sysconfig/selinux (1)

SELINUX=disabled

Рис. 8: SELINUX=disabled

Далее перезапускаем систему (рис. 9)

Перезапуск системы

Рис. 9: Перезапуск системы

После перезагрузки запускаем терминал и получаем полномочия администратора. Далее смотрим статус SELinux. Мы увидем, что SELinux теперь отключён (рис. 10)

Режим работы SELinux (3)

Рис. 10: Режим работы SELinux (3)

Попробуем переключить режим работы SELinux: *setenforce 1*. Мы не сможем этого сделать, так как SELinux отключён (рис. 11)

Попытка изменения режима работы SELinux

Рис. 11: Попытка изменения режима работы SELinux

В файле /etc/sysconfig/selinux с помощью редактора устанавливаем параметр enforcing: *SELINUX=enforcing* (рис. 12), (рис. 13), (рис. 14)

Окрытие файла /etc/sysconfig/selinux (2)

Рис. 12: Окрытие файла /etc/sysconfig/selinux (2)

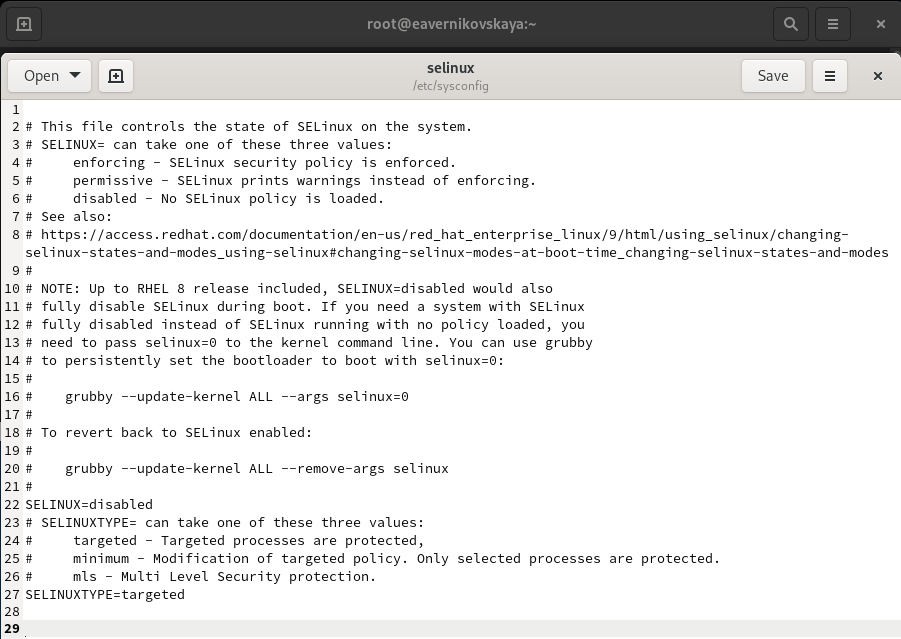


Рис. 13: Файл /etc/sysconfig/selinux (2)

SELINUX=enforcing

Рис. 14: SELINUX=enforcing

Снова перезагружаем систему. Во время загрузки системы мы, получили предупреждающее сообщение о необходимости восстановления меток SELinux (рис. 15)

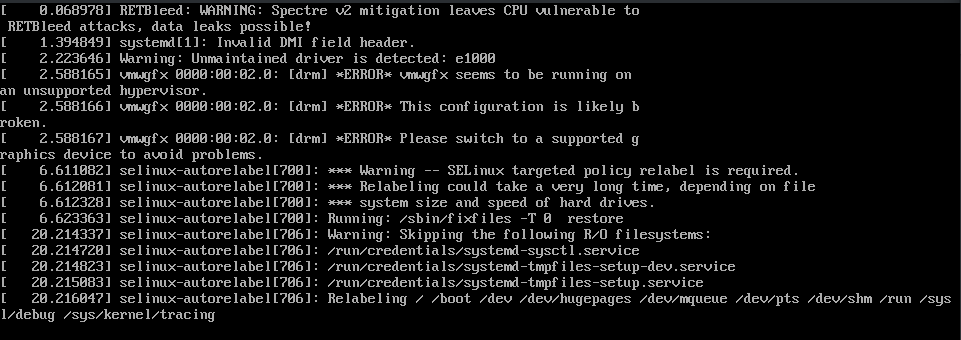


Рис. 15: Перезагрузка системы + предупреждающее сообщение

После перезагрузки в терминале с полномочиями администратора посмотрим текущую информацию о состоянии SELinux. Система работает в принудительном режиме (enforcing) использования SELinux (рис. 16)

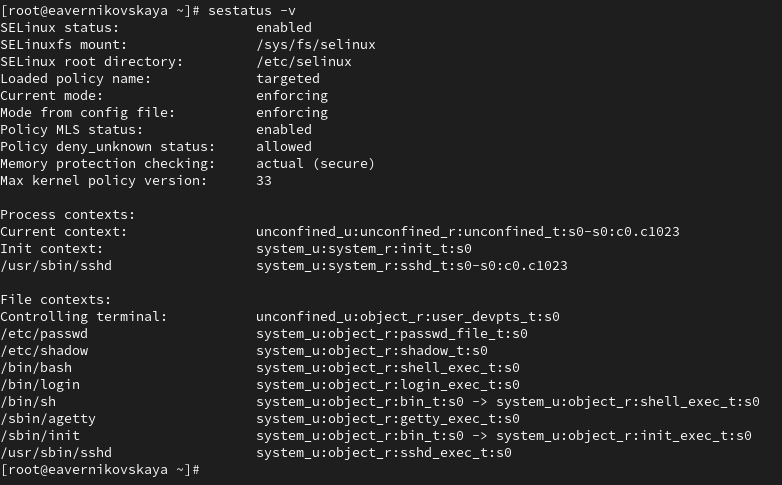


Рис. 16: Состояние SELinux (2)

## 3.2 Использование restorecon для восстановления контекста безопасности

Посмотрим контекст безопасности файла /etc/hosts: *ls -Z /etc/hosts*. Мы увидем, что у файла есть метка контекста net\_conf\_t (рис. 17)

Контекст безопасности файла /etc/hosts (1)

Рис. 17: Контекст безопасности файла /etc/hosts (1)

Скопируем файл /etc/hosts в домашний каталог, с помощью *cp /etc/hosts ~/* (рис. 18)

Копирование файла /etc/hosts в домашний каталог

Рис. 18: Копирование файла /etc/hosts в домашний каталог

Проверяем контекст файла ~/hosts: *ls -Z ~/hosts*. Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin\_home\_t (рис. 19)

Контекст безопасности файла ~/hosts

Рис. 19: Контекст безопасности файла ~/hosts

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: *mv ~/hosts /etc* (рис. 20)

Перезапись существующего файла hosts из домашнего каталога в каталог /etc

Рис. 20: Перезапись существующего файла hosts из домашнего каталога в каталог /etc

Далее проверим, что тип контекста по-прежнему установлен на admin\_home\_t: *ls -Z /etc/hosts* (рис. 21)

Контекст безопасности файла /etc/hosts (2)

Рис. 21: Контекст безопасности файла /etc/hosts (2)

Далее исправим контекст безопасности: *restorecon -v /etc/hosts* Опция -v покажет процесс изменения (рис. 22)

Исправление контекста безопасности

Рис. 22: Исправление контекста безопасности

Прверим, что тип контекста изменился (рис. 23)

Контекст безопасности файла /etc/hosts (3)

Рис. 23: Контекст безопасности файла /etc/hosts (3)

Для массового исправления контекста безопасности на файловой системе вводим *touch /.autorelabel* (рис. 24)

Массовое исправление контекста безопасности

Рис. 24: Массовое исправление контекста безопасности

После перезапускаем систему. Во время перезапуска нажимаем клавишу Esc, чтобы мы видели загрузочные сообщения. Мы увидим, что файловая система автоматически перемаркирована (рис. 25)



Рис. 25: Перезагрузка системы + загрузочные сообщения

## 3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Устанавливаем необходимое программное обеспечение (рис. 26), (рис. 27)

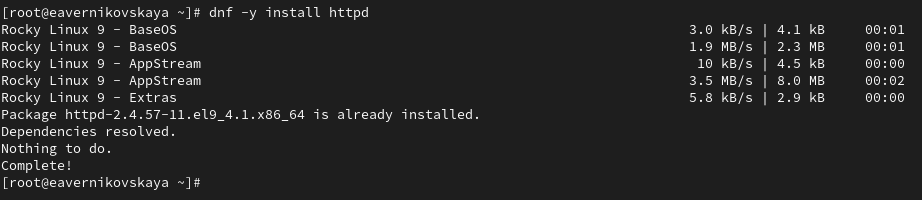


Рис. 26: Установка httpd

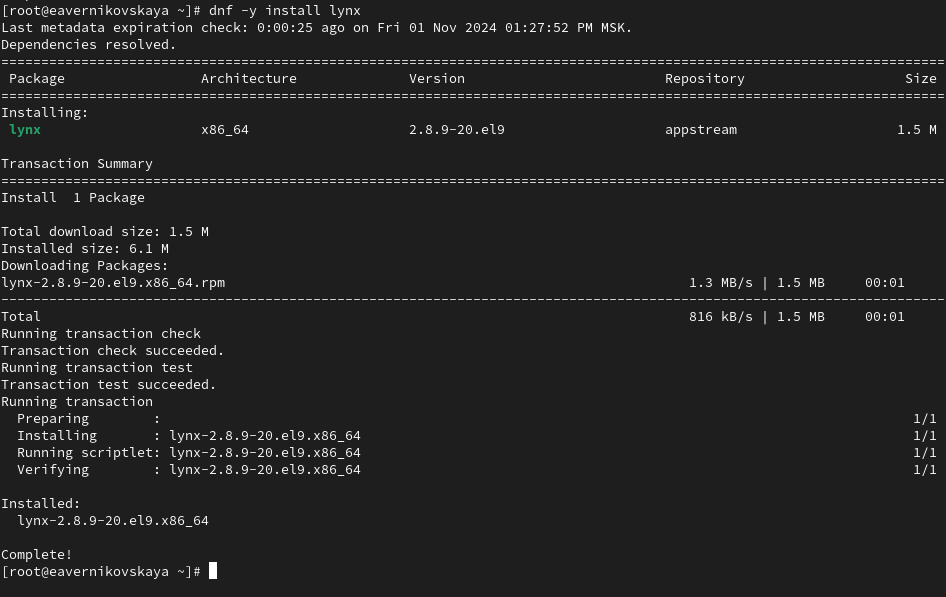


Рис. 27: Установка lynx

Создаём новое хранилище для файлов web-сервера: *mkdir /web* (рис. 28)

Создание хранилиза для файлов web-сервера

Рис. 28: Создание хранилиза для файлов web-сервера

Создаём файл index.html в каталоге с контентом веб-сервера (рис. 29)

Создание файла index.html в каталоге с контентом веб-сервера

Рис. 29: Создание файла index.html в каталоге с контентом веб-сервера

Пишем в созданном файле index.html следующий текст: Welcome to my web-server (рис. 30), (рис. 31), (рис. 32)

Открытие файла index.html

Рис. 30: Открытие файла index.html

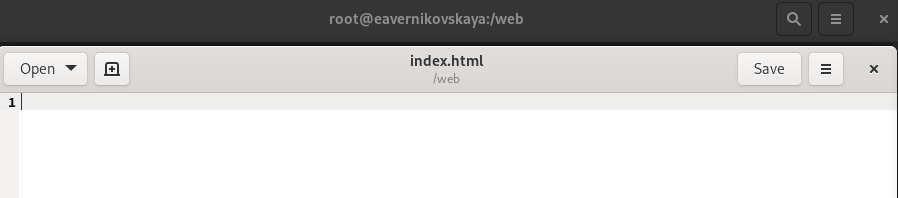


Рис. 31: Файл index.html

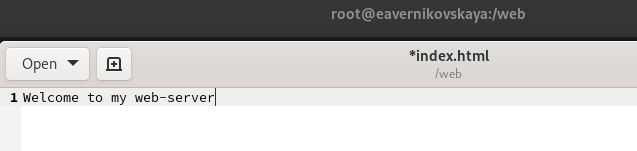


Рис. 32: Редактирование файла index.html

В файле /etc/httpd/conf/httpd.conf закомментируем строку *DocumentRoot “/var/www/html”* и ниже добавим строку *DocumentRoot “/web”* (рис. 33), (рис. 34), (рис. 35)

Открытие файла etc/httpd/conf/httpd.conf

Рис. 33: Открытие файла etc/httpd/conf/httpd.conf

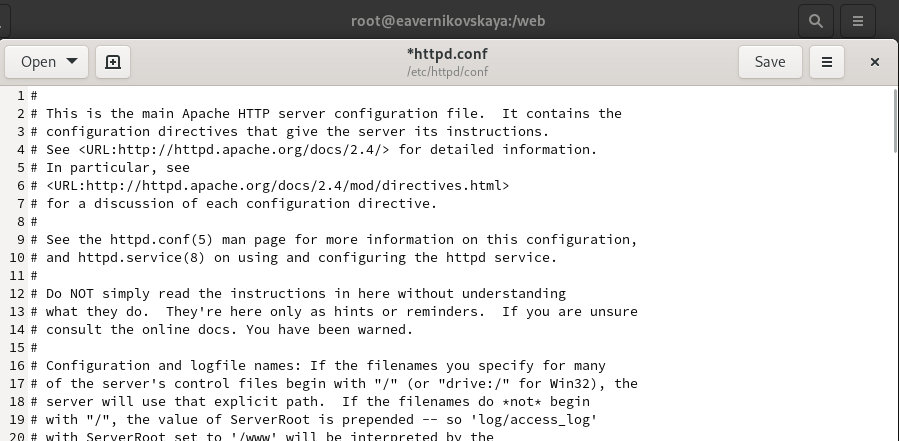


Рис. 34: Файл etc/httpd/conf/httpd.conf

Редактирование файла etc/httpd/conf/httpd.conf (1)

Рис. 35: Редактирование файла etc/httpd/conf/httpd.conf (1)

Затем в этом же файле ниже закомментируем раздел

<Directory "/var/www">  
 AllowOverride None  
 Require all granted  
</Directory>

и добавим следующий раздел, определяющий правила доступа: (рис. 36)

<Directory "/web">  
 AllowOverride None  
 Require all granted  
</Directory>

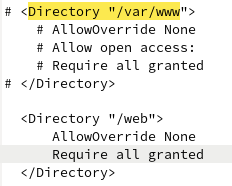


Рис. 36: Редактирование файла etc/httpd/conf/httpd.conf (2)

Запускаем веб-сервер и службу httpd (рис. 37)

Запуск веб-сервера и службы httpd

Рис. 37: Запуск веб-сервера и службы httpd

В терминале под учётной записью нашего пользователя обращаемся к веб-серверу в текстовом браузере lynx: *lynx http://localhost* (рис. 38)

lynx http://localhost (1)

Рис. 38: lynx http://localhost (1)

После этого мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html (для выхода из lynx нажмается q) (рис. 39)

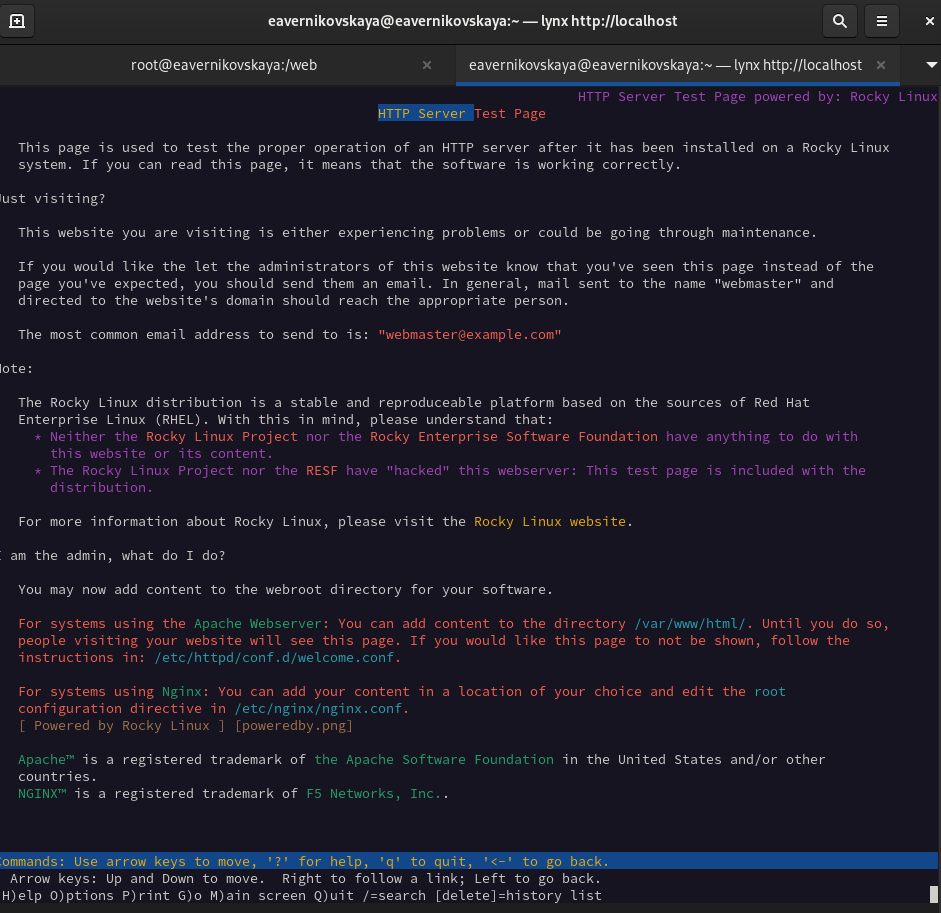


Рис. 39: Веб-страница Red Hat по умолчанию

В терминале с полномочиями администратора применяем новую метку контекста к /web: semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?” (рис. 40)

Применение новой метку контекста к /web

Рис. 40: Применение новой метку контекста к /web

Восстановим контекст безопасности: *restorecon -R -v /web* (рис. 41)

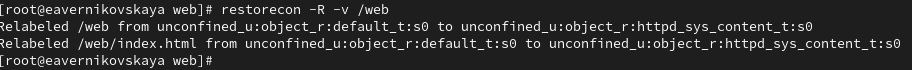


Рис. 41: Восстановление контекста безопасности

В терминале под учётной записью нашего пользователя снова обращаемся к веб-серверу: *lynx http://localhost*. Теперь мы получили доступ к своей пользовательской веб-странице. На экране есть запись «Welcome to my web-server» (рис. 42), (рис. 43)

lynx http://localhost (2)

Рис. 42: lynx http://localhost (2)

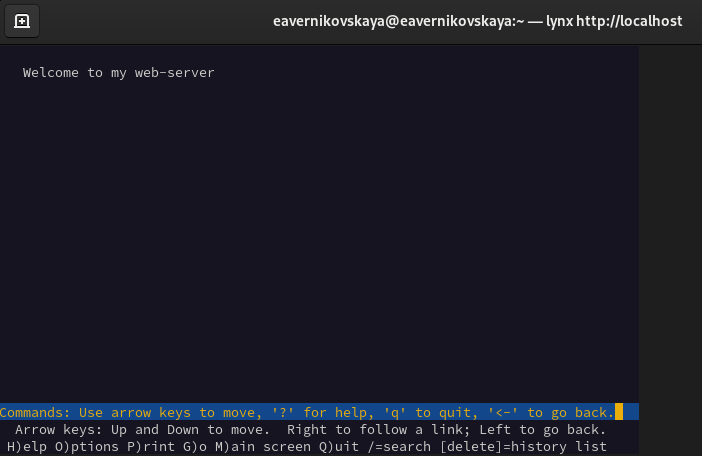


Рис. 43: Наша пользовательская веб-страница

## 3.4 Работа с переключателями SELinux

Посмотрим список переключателей SELinux для службы ftp: *getsebool -a | grep ftp*. Мы увидим переключатель ftpd\_anon\_write с текущим значением off (рис. 44)

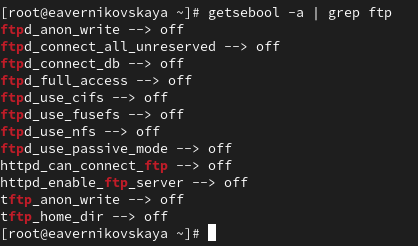


Рис. 44: Список переключателей SELinux для службы ftp

Для службы ftpd\_anon посмотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен: *semanage boolean -l | grep ftpd anon* (рис. 45)

Список переключателей c пояснением для службы ftpd_anon

Рис. 45: Список переключателей c пояснением для службы ftpd\_anon

Изменим текущее значение переключателя для службы ftpd\_anon\_write с off на on: *setsebool ftpd\_anon\_write on* (рис. 46)

Изменение текущего значения переключателя службы ftpd_anon_write с off на on

Рис. 46: Изменение текущего значения переключателя службы ftpd\_anon\_write с off на on

Повторно смотрим список переключателей SELinux для службы ftpd\_anon\_write: *getsebool ftpd\_anon\_write* (рис. 47)

Список переключателей SELinux для службы ftpd_anon_write

Рис. 47: Список переключателей SELinux для службы ftpd\_anon\_write

Псмотрим список переключателей с пояснением: *semanage boolean -l | grep ftpd\_anon*. Мы видим, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена (рис. 48)

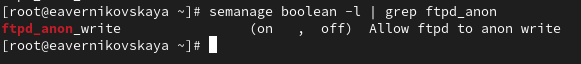


Рис. 48: Список переключателей с пояснением для службы ftpd\_anon\_write (1)

Изменим постоянное значение переключателя для службы ftpd\_anon\_write с off на on: *setsebool -P ftpd\_anon\_write on* (рис. 49)

Изменение постоянного значения переключателя для службы ftpd_anon_write с off на on

Рис. 49: Изменение постоянного значения переключателя для службы ftpd\_anon\_write с off на on

Снова посмотрим список переключателей: *semanage boolean -l | grep ftpd\_anon*. Теперь постоянная настройка включена (рис. 50)

Список переключателей с пояснением для службы ftpd_anon_write (2)

Рис. 50: Список переключателей с пояснением для службы ftpd\_anon\_write (2)

# 4 Контрольные вопросы + ответы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

setenforce 0 (рис. 51)

Вопрос №1

Рис. 51: Вопрос №1

1. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

getsebool -a (рис. 52)

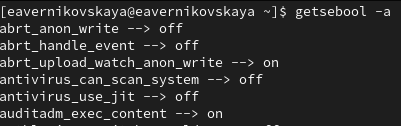


Рис. 52: Вопрос №2

1. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

audit2allow

1. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd\_sys\_content\_t к каталогу /web?

semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?” restorecon -R -v /web (рис. 53), (рис. 54)

Вопрос №4 (1)

Рис. 53: Вопрос №4 (1)

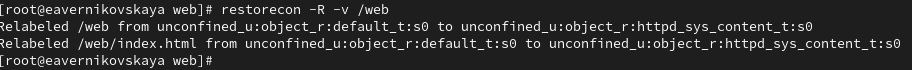


Рис. 54: Вопрос №4 (2)

1. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

/etc/sysconfig/selinux (рис. 55), (рис. 56)

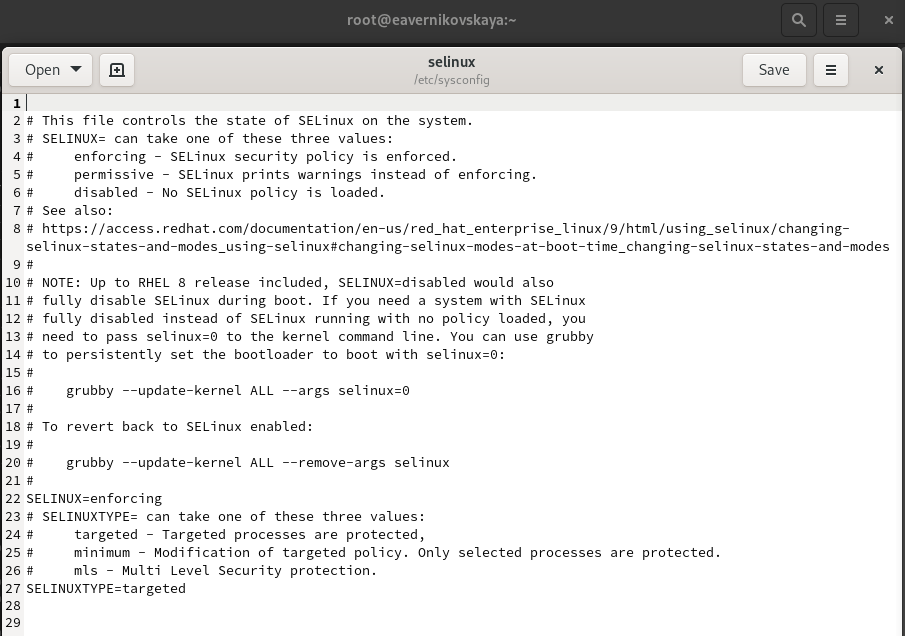


Рис. 55: Вопрос №5 (1)

Вопрос №5 (2)

Рис. 56: Вопрос №5 (2)

1. Где SELinux регистрирует все свои сообщения?

в /var/log/audit/audit.log (рис. 57)

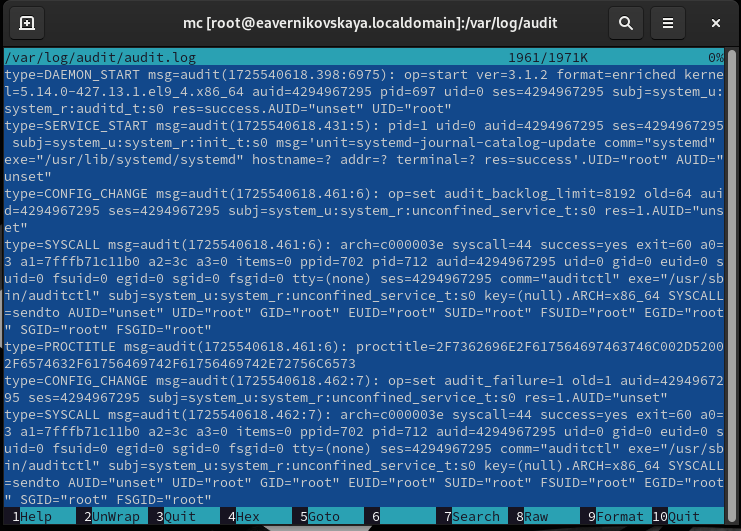


Рис. 57: Вопрос №6

1. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

getsebool -a | grep ftp (рис. 58)

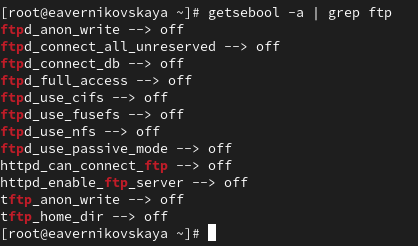


Рис. 58: Вопрос №7

1. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

Просмотреть контекст безопасности процессора ps -eZ или id -Z

# 5 Выводы

В ходе выполнения лабораторной работы мы получили навыки и работы с контекстом безопасности и политиками SELinux

# 6 Список литературы

1. Лаборатораня работа №9 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/2400723/mod\_resource/content/4/010-selinux.pdf