Отчет по выполнению лабораторной работы

Лабораторная работа №9

Полина Витальевна Барабаш

Содержание

Список иллюстраций

Список таблиц

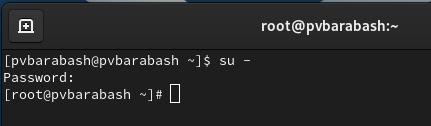
# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Выполнение лабораторной работы

**Задание 1.** Получите полномочия администратора.

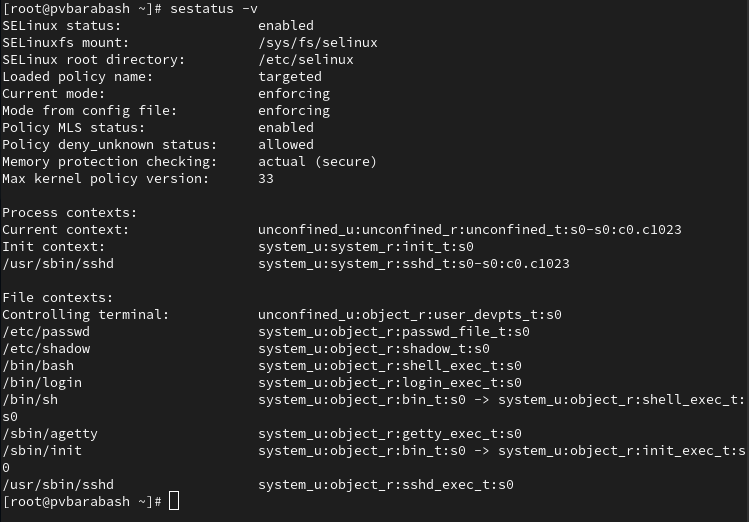
Я перешла в режим работы суперпользователя, использовав команду su - (рис. [??]).



Переход в режим суперпользователя

**Задание 2.** Просмотрите текущую информацию о состоянии SELinux.

Я ввела команду sestatus -v, чтобы посмотреть текущую информацию о состоянии SELinux (рис. [??]).

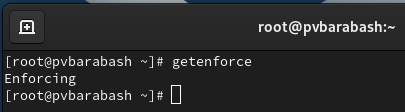


Проверка текущей информации о состоянии SELinux

**SELinux status**: показывает, включен ли SeLinux. Значение может быть “enabled” (включен) или “disabled” (выключен). **SELinux mount**: указывает, где смонтирована файловая система SELinux. **SELinux root directory**: путь к корневому каталогу конфигурации SELinux. **Loaded policy name**: название загруженной политики безопасности. **Current mode**: текущий режим работы SELinux. В данном случае “enforcing”, что означает, что политики SELinux применяются. Также могут быть значения “permissive” и “disabled”. **Mode from config file**: режим, указанных в конфигурационном файле SELinux. Это значение может совпадать с текущим режимом или отличаться. **Policy MLS status**: статус поддержки многоуровневой безопасности (MLS). Может быть “enabled” или “disabled”. **Policy deny\_unknown status**: указывает, разрешено ли отклонение неизвестных типов объектов. Значение может быть “allowed” или “denied”. **Max kernel policy version**: максимальная версия политики ядра, которая поддерживается системой.

**Задание 3.** Посмотрите, в каком режиме работает SELinux.

Я использовала команду getenforce, чтобы посмотреть, в каком режиме работает SELinux (рис. [??]).

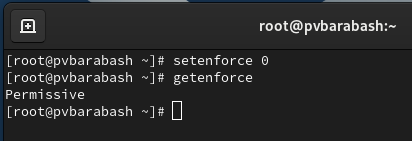


Просмотр режима работы SELinux

Как можно видеть на скриншоте, SELinux находится в режиме принудительного исполнения (Enforcing).

**Задание 4.** Измените режим работы SELinux на разрешающий (Permissive) и снова проверьте, в каком режиме работает SELinux.

Я изменила режим работы SELinux на разрешающий с помощью команды setenforce 0 и снова ввела команду getenforce (рис. [??]).

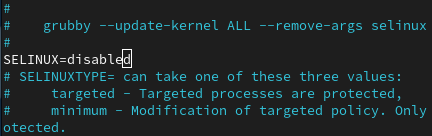


Изменение режима работы и проверка

Как можно видеть, режим работы действительно изменился на необходимый.

**Задание 5.** В файле /etc/sysconfig/selinux с помощью редактора установите SELINUX=disabled. Перезагрузите систему.

Я использовала редактор vim, чтобы изменить файл (рис. [??]).

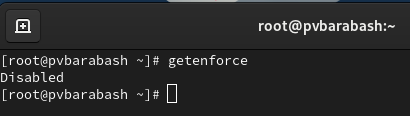


Изменение настроек в файле

Затем я перезапустила систему с помощью команды reboot.

**Задание 6.** После перезагрузки запустите терминал и получите полномочия администратора. Посмотрите статус SELinux.

После перезагрузки я запустила терминал и получила полномочия администратора. Затем я посмотрела статус SELinux с помощью всё той же команды getenforce (рис. [??]).

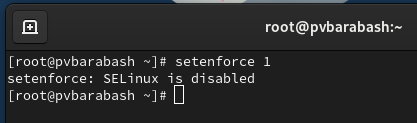


Проверка статуса после изменения настроек в файле

Действительно, статус изменен на disabled.

**Задание 7.** Попробуйте переключить режим работы SELinux.

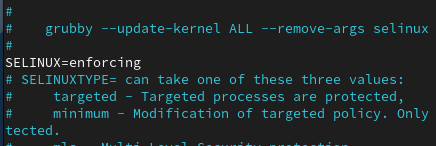
Я использовала команду setenforce 1, но получила сообщение, что SELinux is disabled (рис. [??]).



Попытка переключить режим работы SELinux

**Задание 8.** Откройте файл /etc/sysconfig/selinux с помощью редактора и установите: SELINUX=enforcing. Перезагрузите систему.

Я снова открыла файл в редакторе vim и изменила настройки на enforcing (рис. [??]).

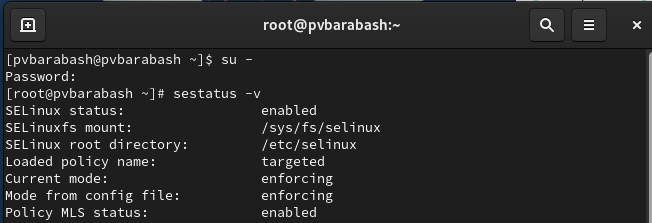


Обратное изменение настроек в файле

Затем я перезагрузила систему.

**Задание 9.** После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux.

Я снова получила полномочия администратора и посмотрела текущую информацию о состоянии SELinux с помощью команды sestatus -v (рис. [??]).

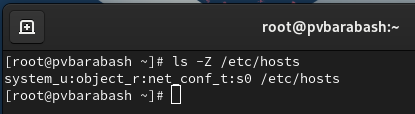


Повторная проверка статуса SELinux

Я убедилась, что система работает в принудительном режиме (enforcing) использования SELinux.

**Задание 10.** Запустите терминал и получите полномочия администратора. Посмотрите контекст безопасности файла /etc/hosts.

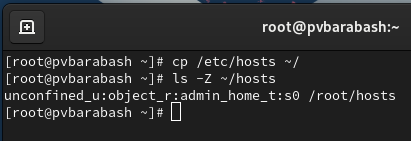
Я использовала команду ls -Z /etc/hosts и увидела, что у файла есть метка контекста net\_conf\_t (рис. [??]).



Просмотр контекста безопасности файла

**Задание 11.** Скопируйте файл /etc/hosts в домашний каталог. Проверьте контекст файла ~/hosts

Я скопировала файл /etc/hosts в домашний каталог с помощью команды cp. Затем я проверила контекст скопированного файла (рис. [??]).

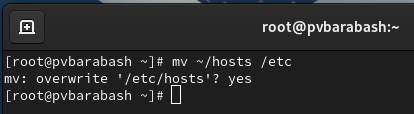


Проверка контекста безопасности скопированного файла

Как можно видеть, у этого файла метка контекста стала admin\_home\_t.

**Задание 12.** Попытайтесь перезаписать существующий файл hosts из домашнего каталога в каталог /etc. И подтвердите, что вы хотите сделать это.

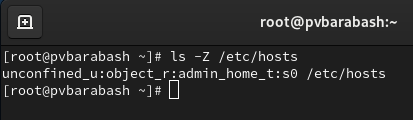
Я использовала команду mv ~/hosts /etc и подтвердила, что хочу переместить файл (рис. [??]).



Перемещение скопированного файла в исходную папку

**Задание 13.** Убедитесь, что тип контекста по-прежнему установлен на admin\_home\_t.

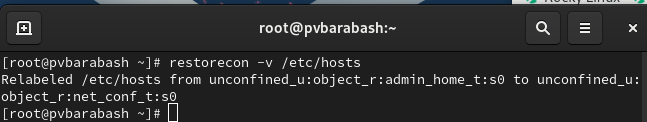
Я использовала команды ls -Z /etc/hosts и убедилась, что тип контекста по-прежнему установлен на admin\_home\_t (рис. [??]).



Проверка метки контекста перемещенного файла

**Задание 14.** Исправьте контекст безопасности.

Я выполнила команду restorecon -v /etc/hosts, чтобы исправить контекст безопасности (рис. [??]).

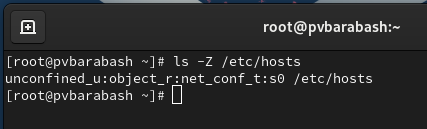


Исправление контекста безопасности

Благодаря опции -v, мы получили сообщение об исправлении.

**Задание 15.** Убедитесь, что тип контекста изменился.

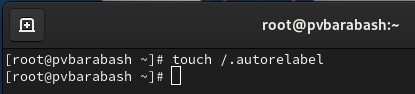
Я вновь ввела команду ls -Z /etc/hosts и убедилась, что тип контекста изменился (рис. [??]).



Проверка изменений типа контекста безопасности

**Задание 16.** Для массового исправления контекста безопасности на файловой системе введите touch /.autorelabel и перезагрузите систему. Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения. Вы увидите, что файловая система автоматически перемаркирована.

Я ввела приведенную команду (рис. [??]).

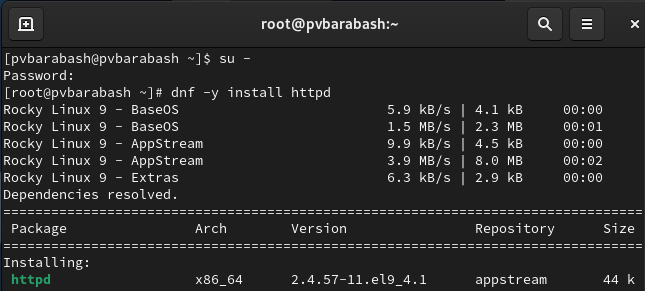


Создание файла .autorelabel

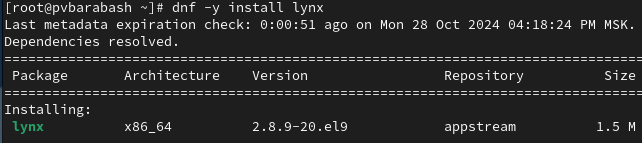
Затем перезапустила систему. И при перезагрузке нажала Esc и действительно увидела, что файловая система перемаркировалась.

**Задание 17.** Получите права администратора. Установите необходимое программное обеспечение: dnf -y install httpd и dnf -y install lynx.

Я получила права администратора, а затем использовала обе приведенные команды, чтобы установить необходимое ПО (рис. [??]) и (рис. [??]).



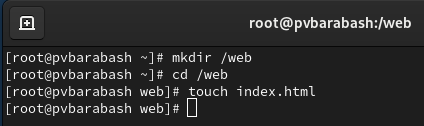
Установка httpd



Установка lynx

**Задание 18.** Создайте новое хранилище для файлов web-сервера. Создайте файл index.html в каталоге с контентом веб-сервера.

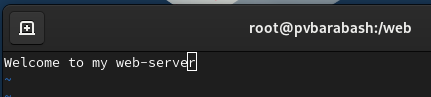
Я создала каталог /web с помощью команды mkdir. Затем перешла в этот каталог с помощью команды cd и создала внутри файл index.html с помощью команды touch (рис. [??]).



Создание каталога и файла

**Задание 19.** Поместите в файл следующий текст: Welcome to my web-server.

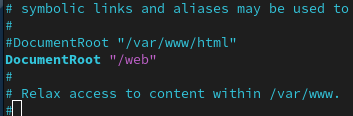
Я открыла файл index.html в vim и добавила туда нужную фразу (рис. [??]).



Добавление нужной фразы в файл

**Задание 20.** В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot “/var/www/html” и ниже добавьте строку DocumentRoot “/web”.

Я открыла файл /etc/httpd/conf/httpd.conf с помощью редактора vim, затем я закомментировала нужную строку и добавила данную (рис. [??])



Комментирование и добавление строк

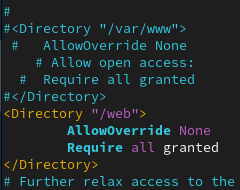
**Задание 21.** Затем в этом же файле ниже закомментируйте раздел

<Directory “/var/www”> AllowOverride None Require all granted

и добавьте следующий раздел, определяющий правила доступа:

<Directory “/web”> AllowOverride None Require all granted

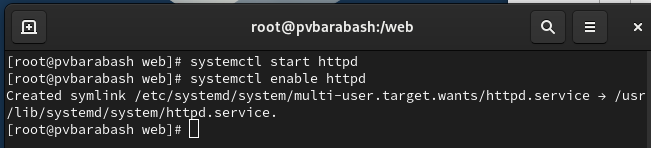
Все в том же открытом в vim файле я закомментировала нужный раздел и добавила данных (рис. [??]).



Комментирование и добавление разделов

**Задание 22.** Запустите веб-сервер и службу httpd.

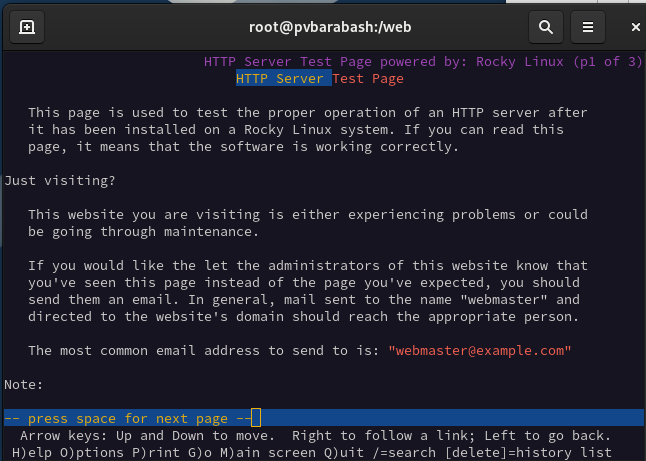
Я использовала команды systemctl start httpd и systemctl enable httpd, чтобы запустить веб-сервер и службу httpd (рис. [??]).



Запуск веб-сервера и службы httpd

**Задание 23.** Запустите веб-сервер в текстовом браузере lynx.

Я запустила веб-сервер в текстовом браузере lynx с помощью команды lynx http://localhost (рис. [??]).

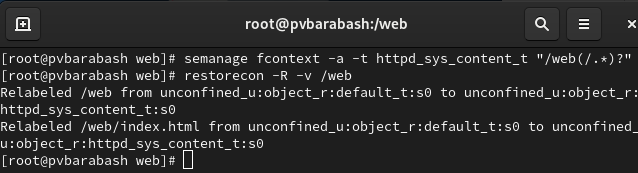


Запуск веб-сервера в текстовом браузере

Я увидела веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.

**Задание 24.** В терминале с полномочиями администратора примените новую метку контекста к /web: semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?“. Восстановите контекст безопасности.

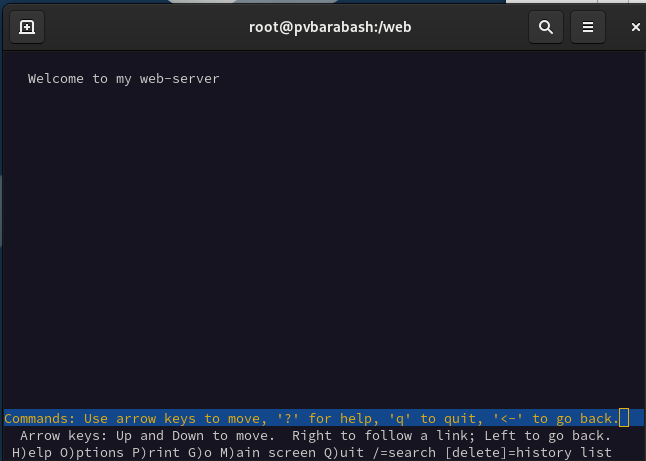
Я использовала приведенную команду, затем я использовала команду restorecon -R -v /web, чтобы восстановить контекст безопасности (рис. [??]).



Применение новой метки контекста к /web и восстановление контекста безопасности

**Задание 25.** Снова обратитесь к веб-серверу.

Я использовала команду lynx http://localhost, чтобы вновь открыть страницу в текстовом браузере (рис. [??]).

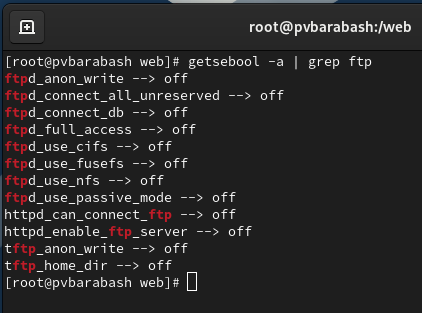


Повторное открытие веб-сервера в текстовом браузере

Теперь действительно появилась запись из нашего файла index.html.

**Задание 26.** Посмотрите список переключателей SELinux для службы ftp.

Я использовала команду getsebool -a | grep ftp, чтобы посмотреть список переключателей SELinux для службы ftp (рис. [??]).

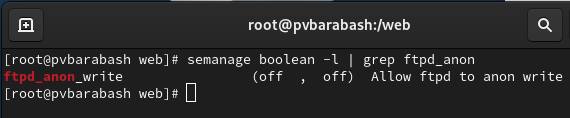


Просмотр списка переключателей SELinux для службы ftp

Я увидела переключатель ftpd\_anon\_write с текущим значением off.

**Задание 27.** Для службы ftpd\_anon посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен.

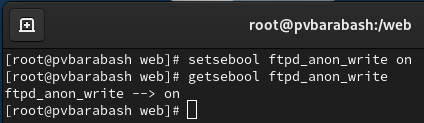
Я ввела команду semanage boolean -l | grep ftpd\_anon, чтобы посмотреть список переключателей с пояснением (рис. [??]).



Просмотр списка переключателей с пояснением

**Задание 28.** Измените текущее значение переключателя для службы ftpd\_anon\_write с off на on. Повторно посмотрите список переключателей SELinux для службы ftpd\_anon\_write.

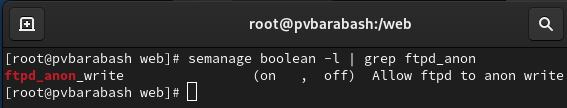
Я использовала команду setsebool ftpd\_anon\_write on, чтобы изменить текущее значение переключателя для службы ftpd\_anon\_write с off на on. Затем я проверила командой getsebool ftpd\_anon\_write, что действительно текущее состояние переключателя изменилось (рис. [??]).



Изменение переключателя для службы и проверка изменения

**Задание 29.** Посмотрите список переключателей с пояснением.

Я вновь посмотрела список переключателей с пояснением (рис. [??]).

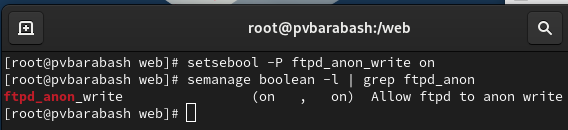


Просмотр списка переключателей с пояснением

Я обратила внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

**Задание 30.** Измените постоянное значение переключателя для службы ftpd\_anon\_write с off на on. Посмотрите список переключателей.

Я ввела команду setsebool -P ftpd\_anon\_write on, чтобы изменить постоянное значение переключателя службы ftpd\_anon\_write с off на on. А затем посмотрела список переключателей (рис. [??]).



Изменение постоянного значения переключателя для службы и просмотр списка переключателей

Теперь и текущее значение переключателя, и постоянное включено.

# 3 Ответы на контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? Команду setenforce 0.
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? Команду getsebool -a.
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? Пакет называется policycoreutils.
4. 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(/.\*)?”
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? Файл конфигурации находится по пути: /etc/selinux/config. Нужно изменить параметр SELINUX= на disabled.
6. Где SELinux регистрирует все свои сообщения? SELinux регистрирует свои сообщения в журнале /var/log/audit/audit.log и в системном журнале (/var/log/messages или /var/log/syslog в зависимости от дистрибутива).
7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? seinfo –type=ftp или sesearch –allow -s ftp\_t -t
8. 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? Ввести команду ausearch -m avc -ts recent. Эта команда покажет последние сообщения AVC (Access Vector Cache), которые могут указать, блокирует ли SELinux доступ сервису.

# 4 Выводы

Я получила навыки работы с контекстом безопасности и политиками SELinux.