Лабораторная работа №6. Мандатное разграничение прав в Linux

дисциплина: Информационная безопасность

Рыбалко Элина Павловна

Содержание

[Цель работы 1](#_Toc116768908)

[Техническое обеспечение 1](#_Toc116768909)

[Объект/Предмет исследования 1](#_Toc116768910)

[Теоретическое введение 2](#_Toc116768911)

[Выполнение лабораторной работы 2](#_Toc116768912)

[Вывод 13](#_Toc116768913)

[Список литературы 13](#_Toc116768914)

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Техническое обеспечение

Лабораторная работа подразумевает наличие на виртуальной машине VirtualBox операционной системы Linux (дистрибутив Rocky или CentOS). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (http://www.gentoo.ru/); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: /afs/dk.sci.pfu.edu.ru/common/files/iso/.

# Объект/Предмет исследования

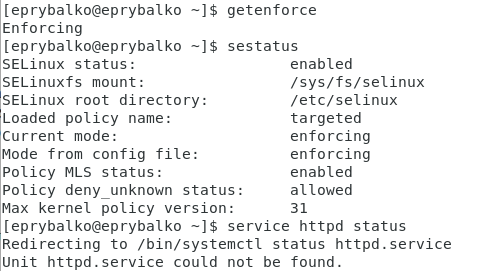
Операционная система Linux и мандатное разграничение прав.

# Теоретическое введение

В Linux дискреционные механизмы разграничения доступа (DAC, discretionary access control) являются основными и всегда активны. Их использование предполагает, что владельцы объектов правильно распоряжаются правами доступа к находящимся в их владении объектам. [[2]] (#список-литературы).

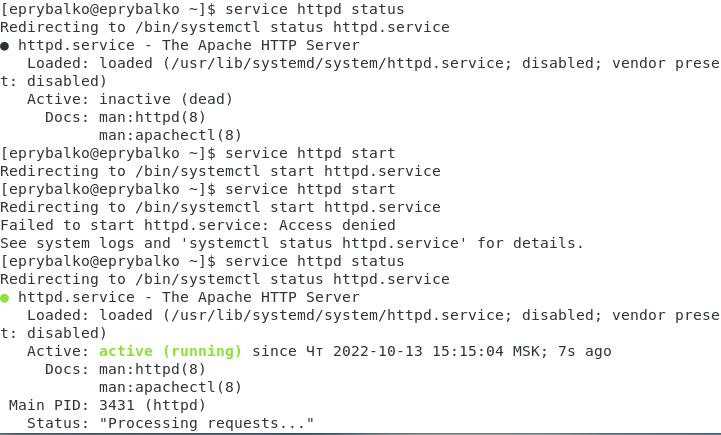
# Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (см. рис. -@fig:001).



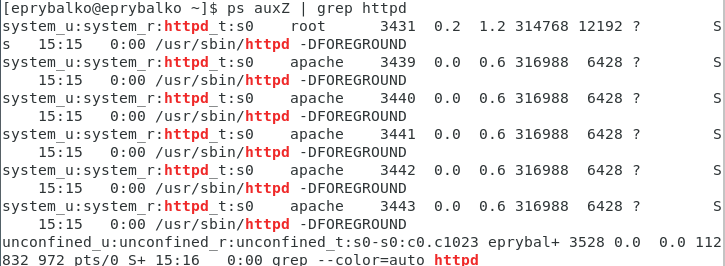
Проверка SELinux

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (см. рис. -@fig:002).



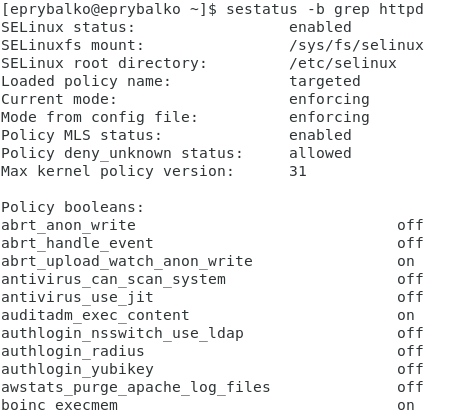
Проверка веб-сервера

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду (см. рис. -@fig:003).



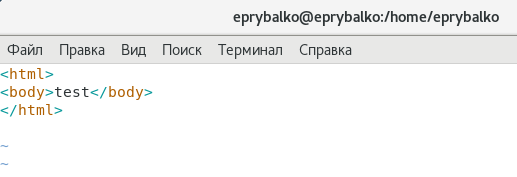
Контекст безопасности

1. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды (см. рис. -@fig:004).



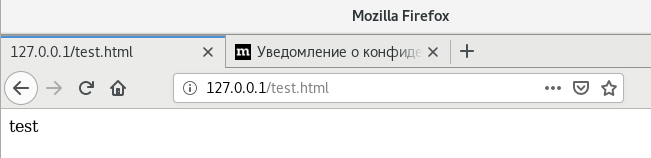
Состояние переключателей

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. (см. рис. -@fig:005).
2. Определите тип файлов и поддиректорий, находящихся в директории /var/www (см. рис. -@fig:004 и рис. -@fig:005).
3. Определите тип файлов, находящихся в директории /var/www/html (см. рис. -@fig:005).
4. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. (см. рис. -@fig:005).
5. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл (см. рис. -@fig:006).



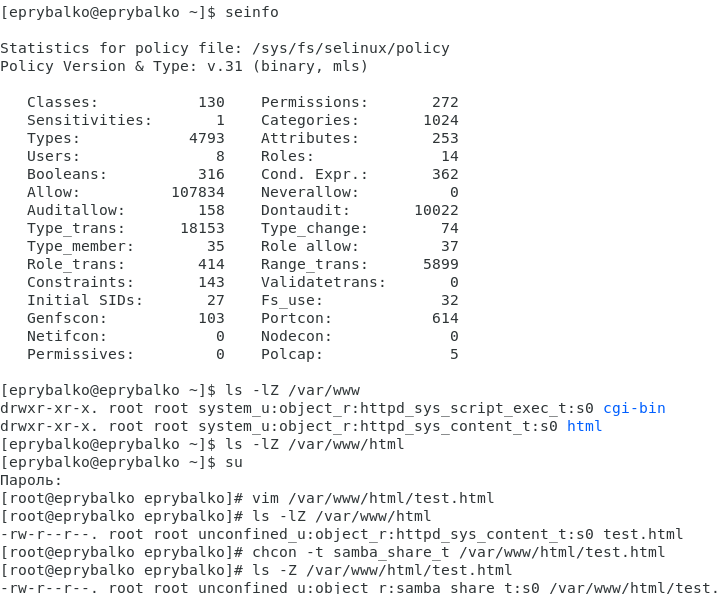
Создание файла

1. Проверьте контекст созданного вами файла (см. рис. -@fig:005).
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” (см. рис. -@fig:007).



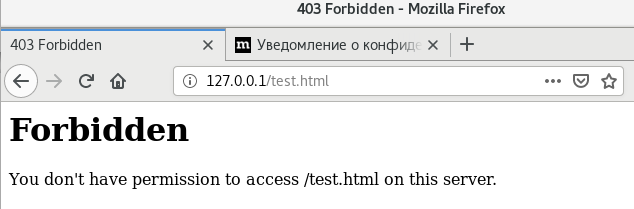
Просмотр файла через браузер

1. Изучите справку man httpd\_selinux.
2. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t (см. рис. -@fig:005).



Статистика по политике, типы файлов, просмотр и изменение контекста

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (см. рис. -@fig:008).



Попытка посмотра файла через браузер

1. Проанализируйте ситуацию. Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл (см. рис. -@fig:009, -@fig:010).

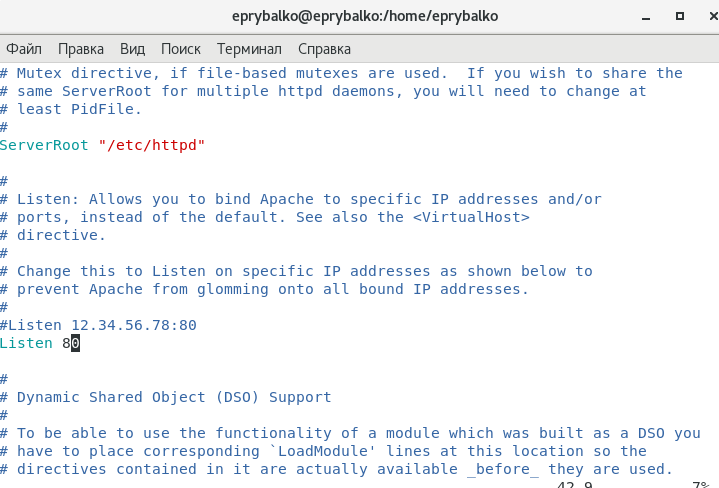


Просмотр log-файлов

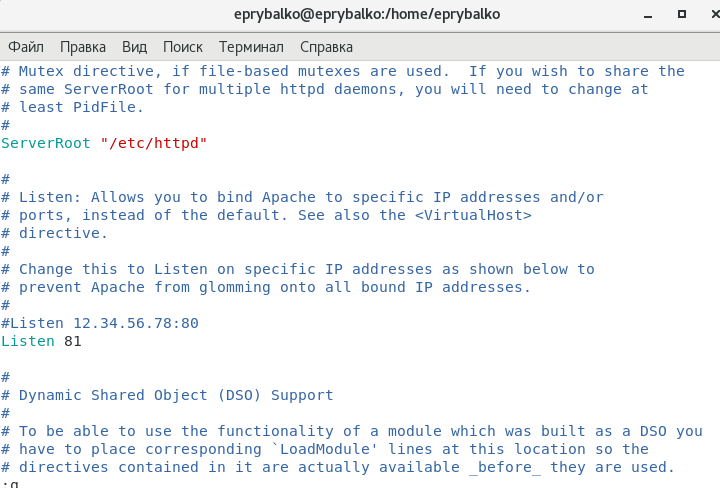


Просмотр log-файлов

1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81 (см. рис. -@fig:011 и -@fig:012).



Изменение порта

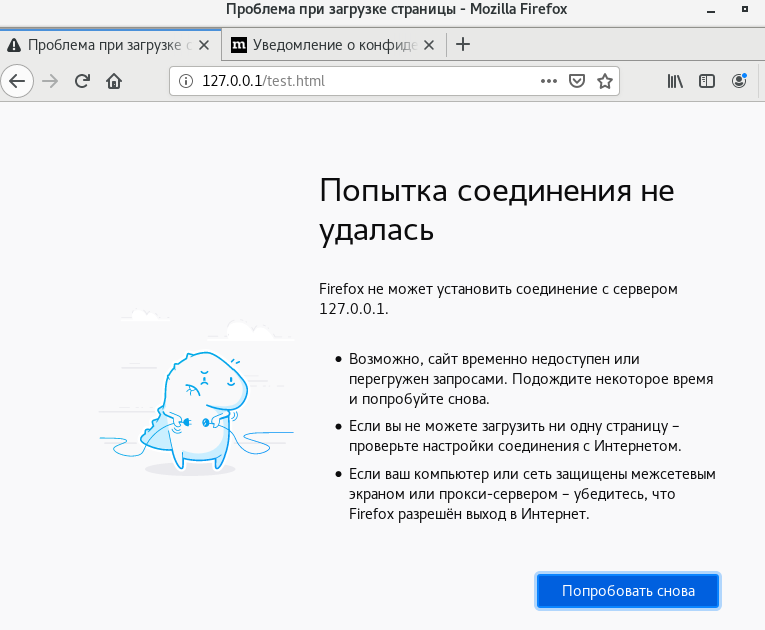


Изменение порта

1. Выполните перезапуск веб-сервера Apache. (см. рис. -@fig:013 и -@fig:014).

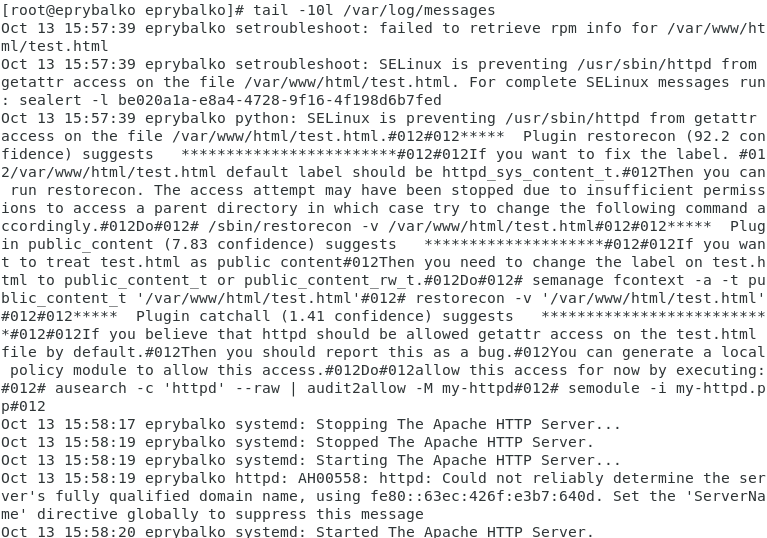
Перезапуск сервера

Перезапуск сервера

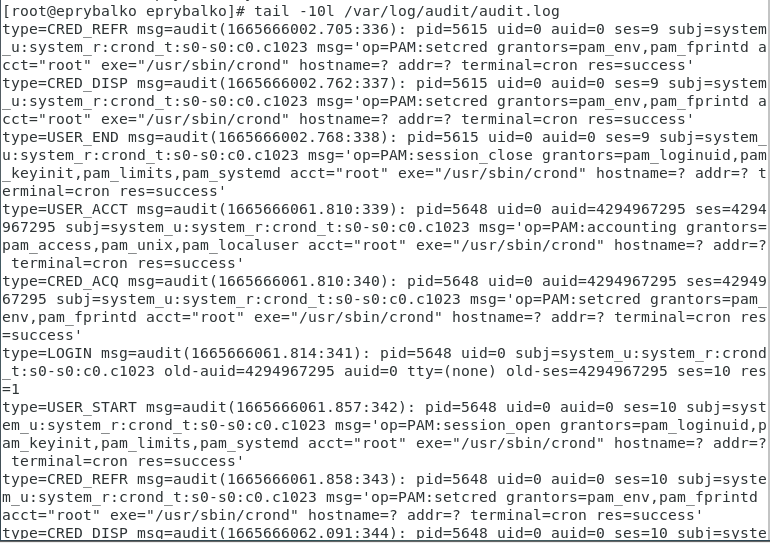


Попытка посмотра файла через браузер

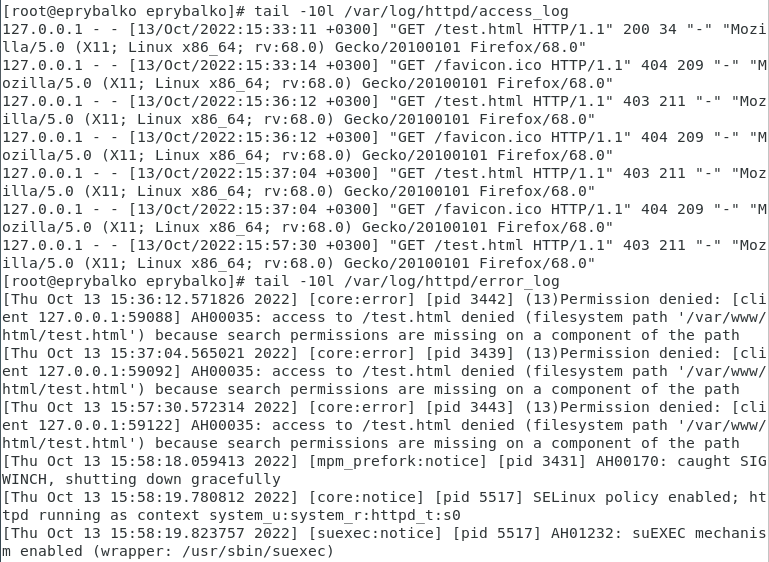
1. Проанализируйте лог-файлы (см. рис. -@fig:015, -@fig:016 и -@fig:017).



Просмотр log-файлов



Просмотр log-файлов

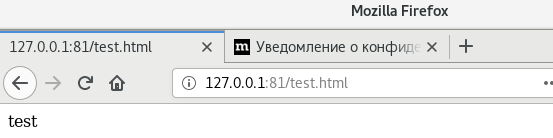


Просмотр log-файлов

1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверьте список портов командой (см. рис. -@fig:018).
2. Попробуйте запустить веб-сервер Apache ещё раз (см. рис. -@fig:018).
3. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html. После этого попробуйте получить доступ к файлу После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html (см. рис. -@fig:018 и -@fig:019).

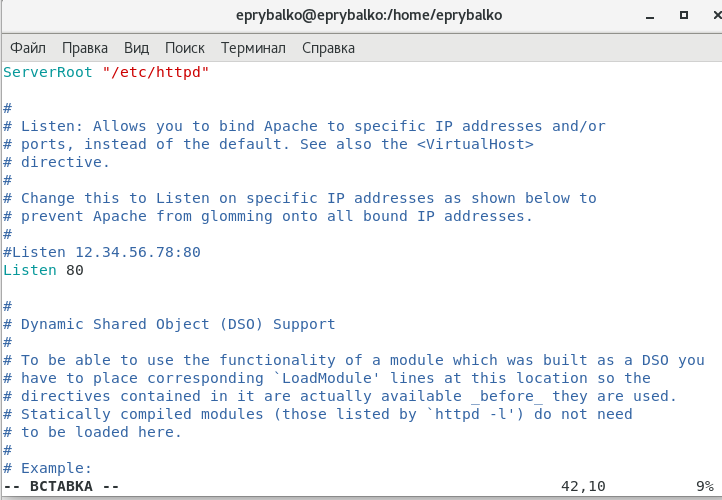


Добавление порта, перезапуск сервера и изменение контекста



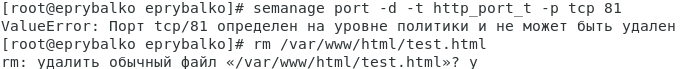
Просмотр файла через 81 порт

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80 (см. рис. -@fig:020).



Изменение файла

1. Удалите привязку http\_port\_t к 81 порту (см. рис. -@fig:021).
2. Удалите файл /var/www/html/test.html (см. рис. -@fig:021).



Удаление привязки и файла

# Вывод

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. [Лабораторная работа №6](https://docs.yandex.ru/docs/view?tm=1665700821&tld=ru&lang=ru&name=006-lab_selinux.pdf&text=6.1.%20Цели%20работы%20Развить%20навыки%20администрирования%20ОС%20Linux.%20Получить%20первое%20практическое%20знакомство%20с%20технологией%20SELinux1%20.%20Проверить%20работу%20SELinx%20на%20практике%20совместно%20с%20веб-сервером%20Apache.%206.2.%20Организация%20и%20описание%20лабораторного%20стенда%20Для%20проведения%20указанной%20лабораторной%20работы%20на%20одно%20рабочее%20место&url=https%3A%2F%2Fstud-sci.rudn.ru%2Fpluginfile.php%2F8544%2Fmod_resource%2Fcontent%2F2%2F006-lab_selinux.pdf&lr=213&mime=pdf&l10n=ru&sign=e25e3a152396f84a129b716f3d88de1e&keyno=0&serpParams=tm%3D1665700821%26tld%3Dru%26lang%3Dru%26name%3D006-lab_selinux.pdf%26text%3D6.1.%2B%25D0%25A6%25D0%25B5%25D0%25BB%25D0%25B8%2B%25D1%2580%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2582%25D1%258B%2B%25D0%25A0%25D0%25B0%25D0%25B7%25D0%25B2%25D0%25B8%25D1%2582%25D1%258C%2B%25D0%25BD%25D0%25B0%25D0%25B2%25D1%258B%25D0%25BA%25D0%25B8%2B%25D0%25B0%25D0%25B4%25D0%25BC%25D0%25B8%25D0%25BD%25D0%25B8%25D1%2581%25D1%2582%25D1%2580%25D0%25B8%25D1%2580%25D0%25BE%25D0%25B2%25D0%25B0%25D0%25BD%25D0%25B8%25D1%258F%2B%25D0%259E%25D0%25A1%2BLinux.%2B%25D0%259F%25D0%25BE%25D0%25BB%25D1%2583%25D1%2587%25D0%25B8%25D1%2582%25D1%258C%2B%25D0%25BF%25D0%25B5%25D1%2580%25D0%25B2%25D0%25BE%25D0%25B5%2B%25D0%25BF%25D1%2580%25D0%25B0%25D0%25BA%25D1%2582%25D0%25B8%25D1%2587%25D0%25B5%25D1%2581%25D0%25BA%25D0%25BE%25D0%25B5%2B%25D0%25B7%25D0%25BD%25D0%25B0%25D0%25BA%25D0%25BE%25D0%25BC%25D1%2581%25D1%2582%25D0%25B2%25D0%25BE%2B%25D1%2581%2B%25D1%2582%25D0%25B5%25D1%2585%25D0%25BD%25D0%25BE%25D0%25BB%25D0%25BE%25D0%25B3%25D0%25B8%25D0%25B5%25D0%25B9%2BSELinux1%2B.%2B%25D0%259F%25D1%2580%25D0%25BE%25D0%25B2%25D0%25B5%25D1%2580%25D0%25B8%25D1%2582%25D1%258C%2B%25D1%2580%25D0%25B0%25D0%25B1%25D0%25BE%25D1%2582%25D1%2583%2BSELinx%2B%25D0%25BD%25D0%25B0%2B%25D0%25BF%25D1%2580%25D0%25B0%25D0%25BA%25D1%2582%25D0%25B8%25D0%25BA%25D0%25B5%2B%25D1%2581%25D0%25BE%25D0%25B2%25D0%25BC%25D0%25B5%25D1%2581%25D1%2582%25D0%25BD%25D0%25BE%2B%25D1)
2. [Мандатное (принудительное) разграничение доступа Linux](https://debianinstall.ru/mandatnoe-prinuditelnoe-razgranichenie-dostupa-linux/)
3. [Руководство по формуле Cmd Markdown](https://russianblogs.com/article/26051452570/)
4. [Руководство по оформлению Markdown файлов](https://gist.github.com/Jekins/2bf2d0638163f1294637)