Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

# 1 Цель работы

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

# 2 Подготовка к лабораторной работе

#### 2.0.0.1 Скачиваем Apache

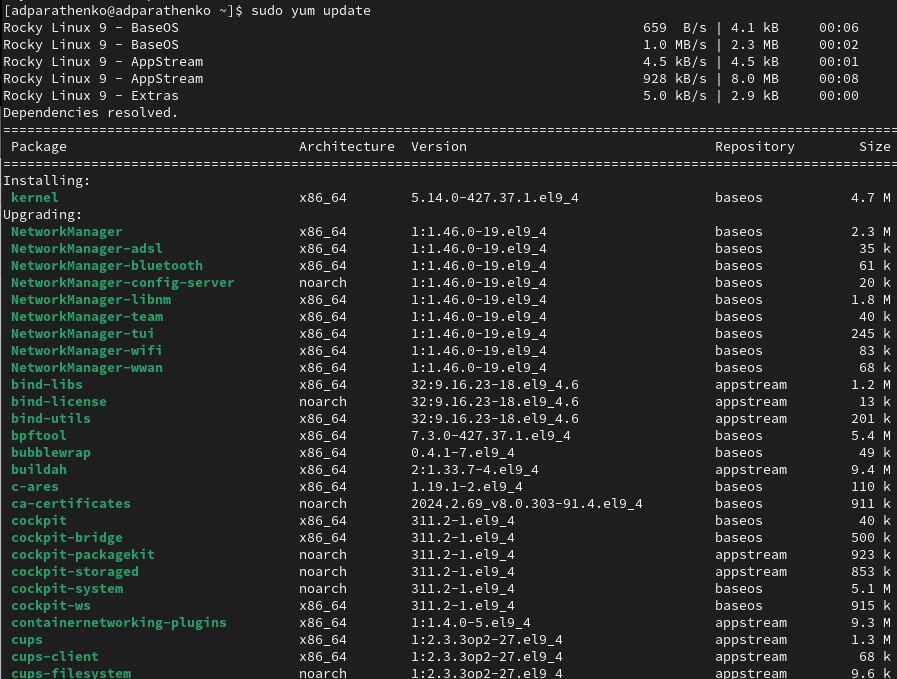


Рис. 1: Скачивание обновлений

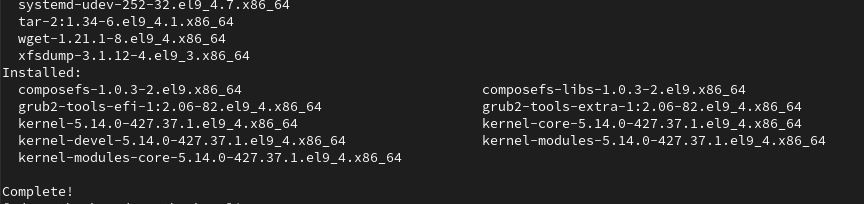


Рис. 2: Установка обновлений

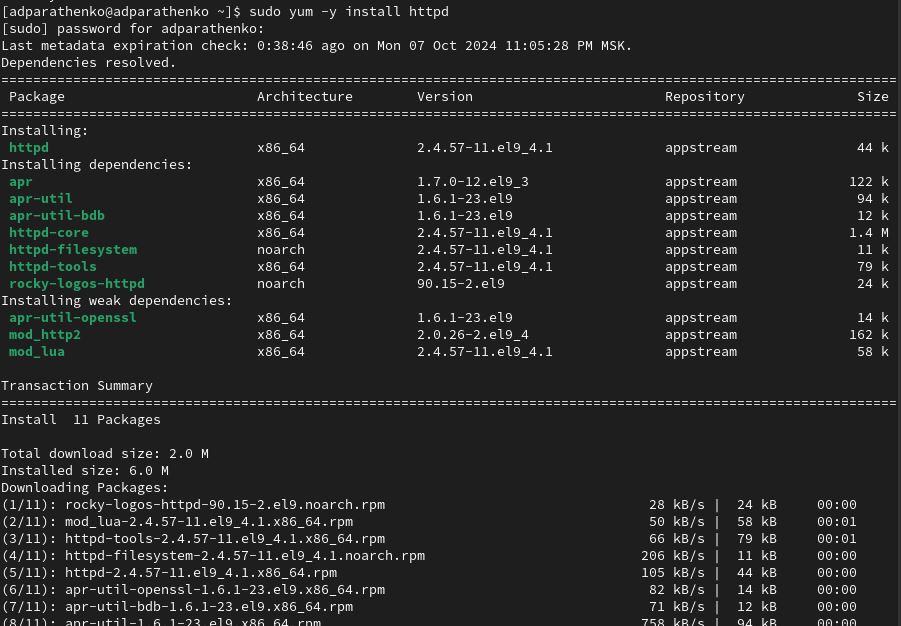


Рис. 3: Apache

# 3 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***. (рис. 4)

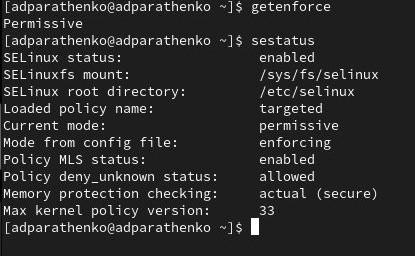


Рис. 4: SELinux режим

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: ***service httpd status*** (рис. 5)

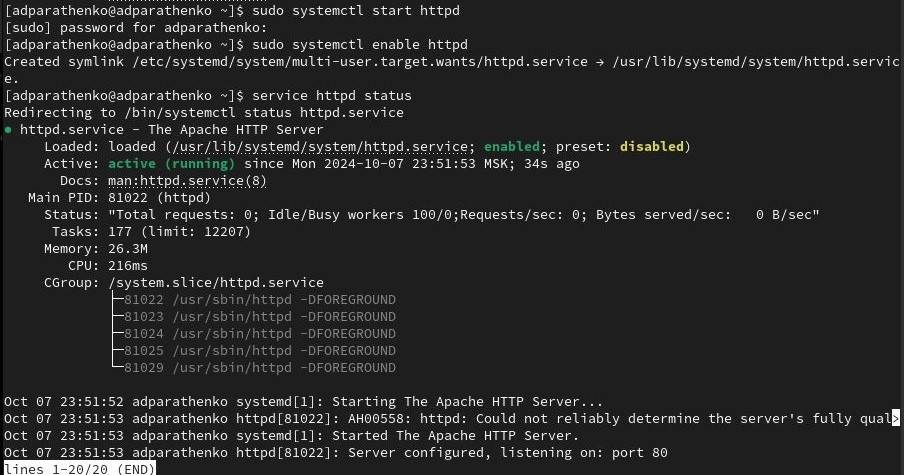


Рис. 5: service httpd status

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ***ps auxZ | grep httpd*** (рис. 6)

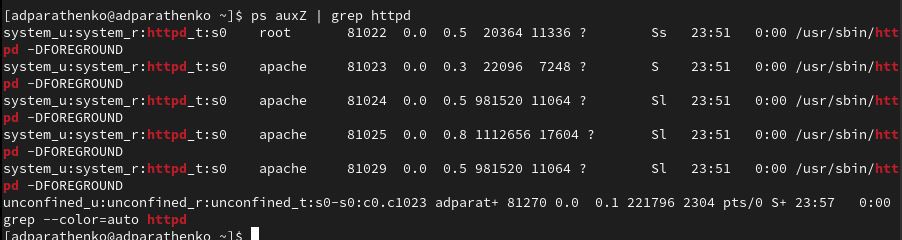


Рис. 6: ps auxZ | grep httpd

1. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды ***sestatus -bigrep httpd*** (рис. 7)



Рис. 7: sestatus -bigrep httpd

1. Посмотрите статистику по политике с помощью команды ***seinfo***, также определите множество пользователей, ролей, типов. (рис. 8)

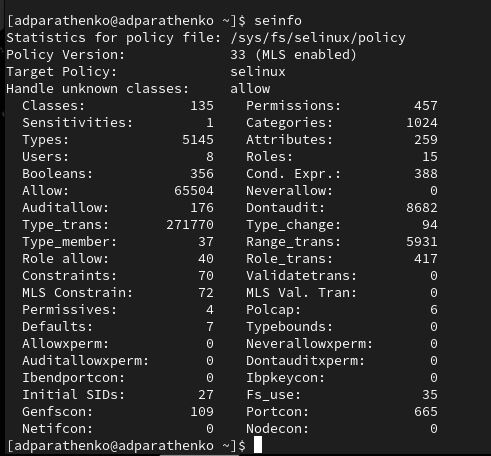


Рис. 8: seinfo

1. Определите тип файлов и поддиректорий, находящихся в директории */var/www*, с помощью команды ***ls -lZ /var/www*** (рис. 9)

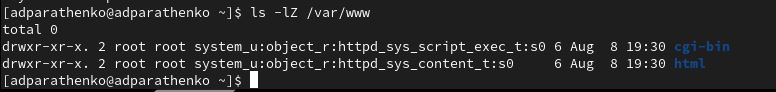


Рис. 9: seinfo

1. Определите тип файлов, находящихся в директории */var/www/html*: ***ls -lZ /var/www/html***. Директория пуста. (рис. 10)

Рис. 10: seinfo

Рис. 10: seinfo

1. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл */var/www/html/test.html* (рис. 11) - (рис. 12)

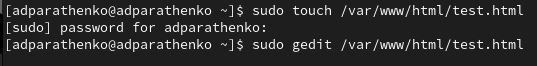


Рис. 11: Создание файла test.html



Рис. 12: Файл test.html

1. Проверьте контекст созданного вами файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории */var/www/html* это ***httpd\_sys\_content*** (рис. 13)

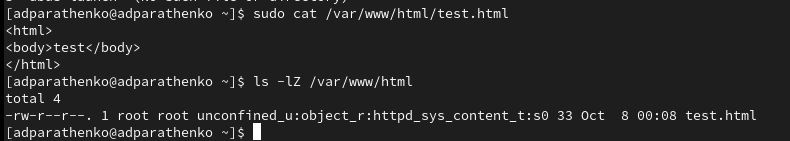


Рис. 13: /var/www/html

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес *http://127.0.0.1/test.html*. Файл был успешно отображён. (рис. 14)

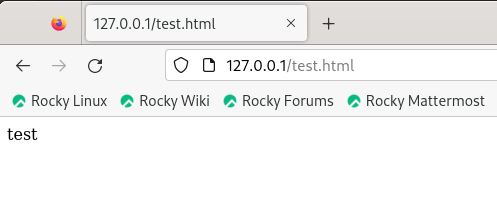


Рис. 14: Веб-сервер test.html

1. Изучите справку ***man httpd\_selinux***. (рис. 15)

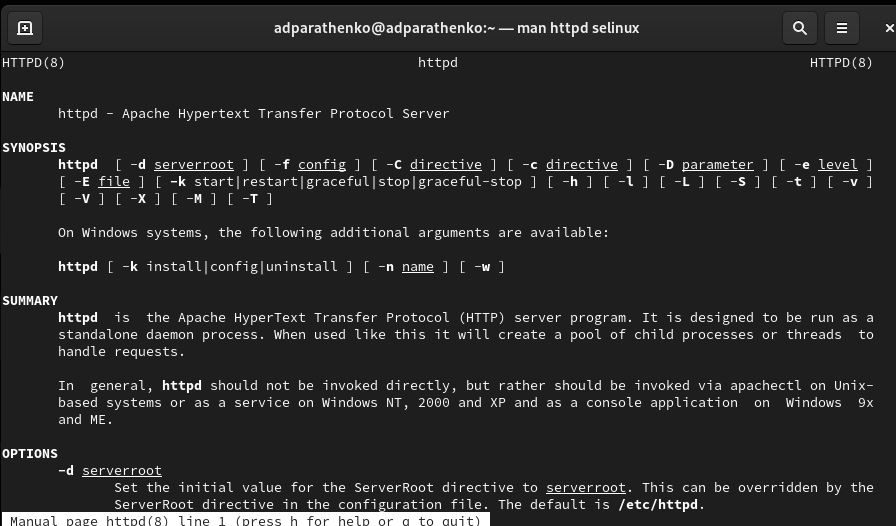


Рис. 15: man httpd\_selinux

1. Проверить контекст файла можно командой ***ls -Z. ls -Z /var/www/html/test.html*** 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*: ***chcon -t samba\_share\_t /var/www/html/test.html*** ***ls -Z /var/www/html/test.html*** (рис. 16)

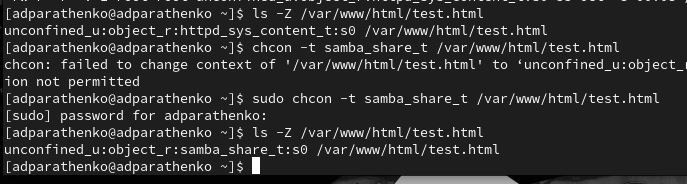


Рис. 16: man httpd\_selinux

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес *http://127.0.0.1/test.html*. Получили сообщение об ошибке. (рис. 17)

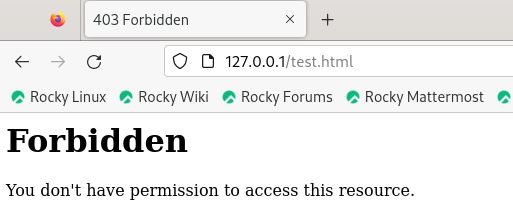


Рис. 17: Ошибка

1. Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: ***tail /var/log/messages*** (рис. 18)

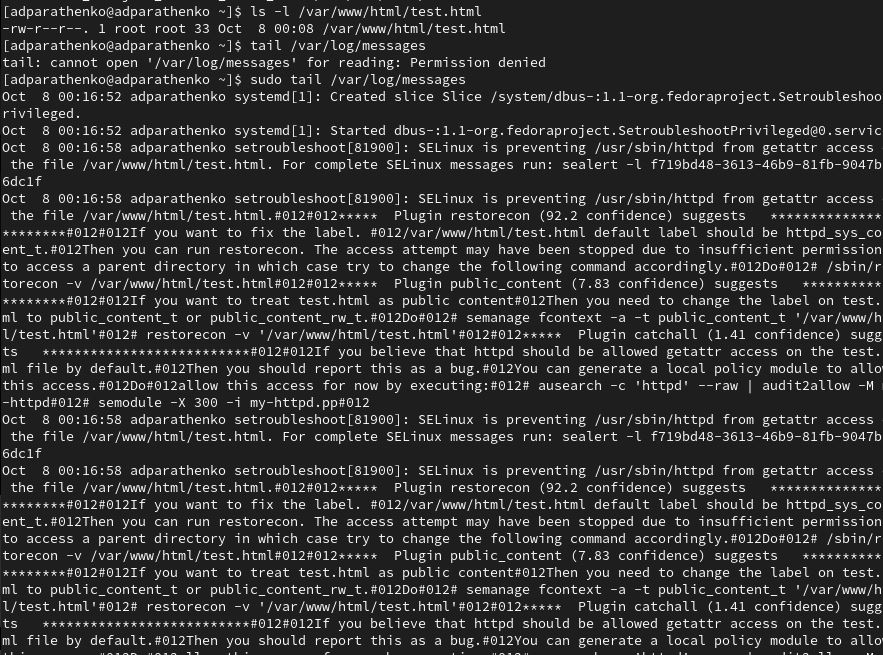


Рис. 18: tail /var/log/messages

1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле */etc/httpd/httpd.conf* найдите строчку *Listen 80* и замените её на *Listen 81*. (рис. 19)

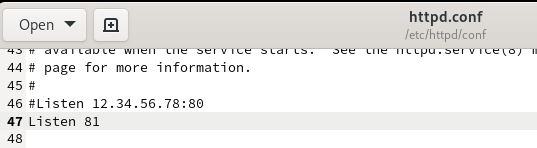


Рис. 19: Listen 81

1. Выполните перезапуск веб-сервера Apache. Произошел сбой. (рис. 20)

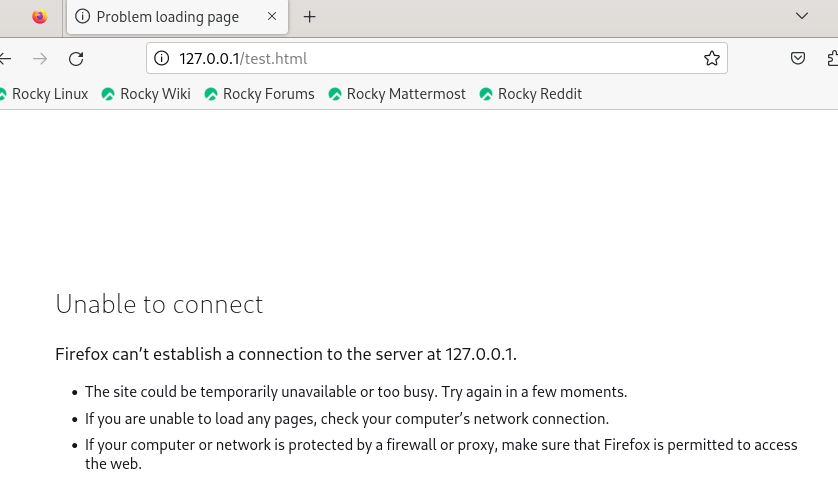


Рис. 20: Сбой порта 81

1. Проанализируйте лог-файлы: ***tail -nl /var/log/messages***. (рис. 21)

Рис. 21: /var/log/messages

Рис. 21: /var/log/messages

1. Просмотрите файлы */var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log*. (рис. 22)

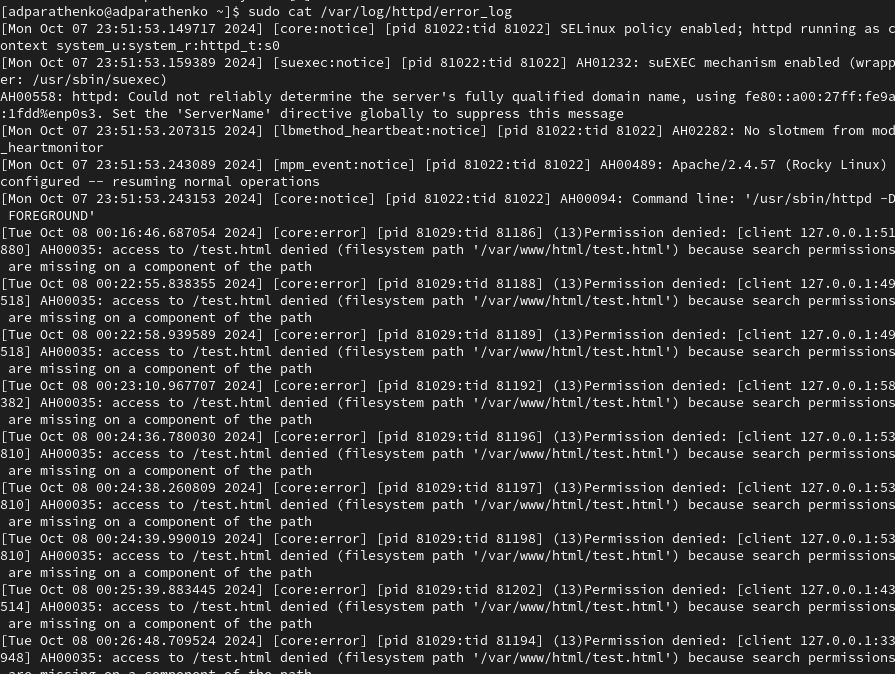


Рис. 22: /var/log/http/error\_log

1. Выполните команду ***semanage port -a -t http\_port\_t -р tcp 81***. После этого проверьте список портов командой ***semanage port -l | grep http\_port\_t***. Порт 81 появился в списке. (рис. 23)

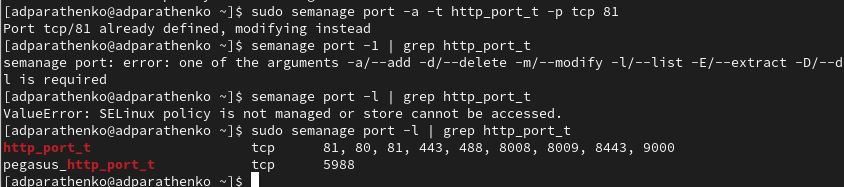


Рис. 23: Порт 81

1. Попробуйте запустить веб-сервер Apache ещё раз. Сейчас запустился. Верните контекст \*\*httpd\_sys\_cоntent\_\_t\*\* к файлу */var/www/html/test.html*: ***chcon -t httpd\_sys\_content\_t /var/www/html/test.html*** После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес *http://127.0.0.1:81/test.html*. Видим содержимое файла. (рис. 24)

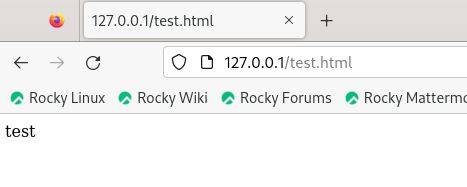


Рис. 24: httpd\_sys\_cоntent\_\_t

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80. Удалите привязку *http\_port\_t* к 81 порту: ***semanage port -d -t http\_port\_t -p tcp 81*** и проверьте, что порт 81 удалён. (рис. 25)

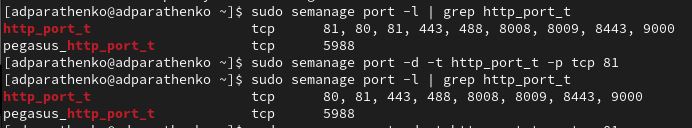


Рис. 25: httpd\_sys\_cоntent\_\_t

1. Удалите файл */var/www/html/test.html*: ***rm /var/www/html/test.html*** (рис. 26)

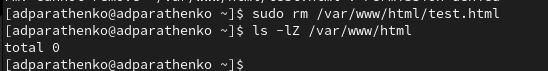


Рис. 26: httpd\_sys\_cоntent\_\_t

# 4 Вывод

В результате выполнения работы мы получили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux1, а также проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. https://esystem.rudn.ru/pluginfile.php/2357155/mod\_resource/content/2/006-lab\_selinux.pdf