Отчёт по лабораторной работе №6

*дисциплина: Информационная безопасность*

Морозова Ульяна

Содержание

# 1 Цель работы

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

# 2 Подготовка к лабораторной работе

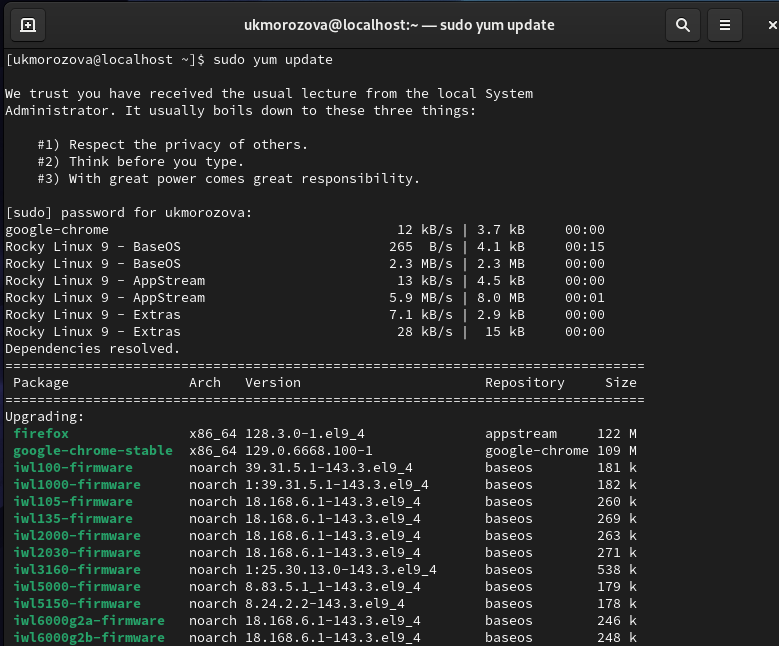


Рис. 1: Установка обновлений

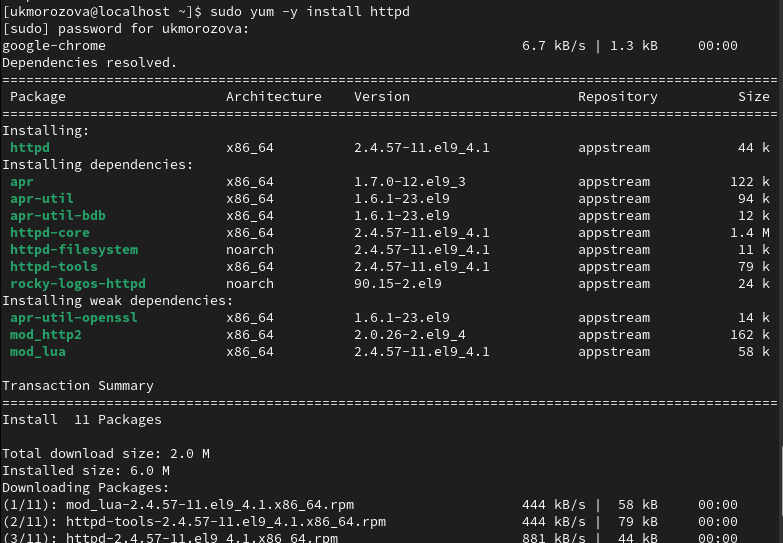


Рис. 2: Скачивание Apache

# 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. 3).

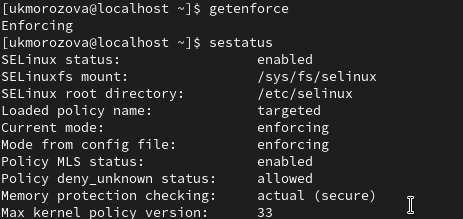


Рис. 3: getenforce и sestatus

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

service httpd status

Если не работает, запустите его так же, но с параметром start (рис. 4).

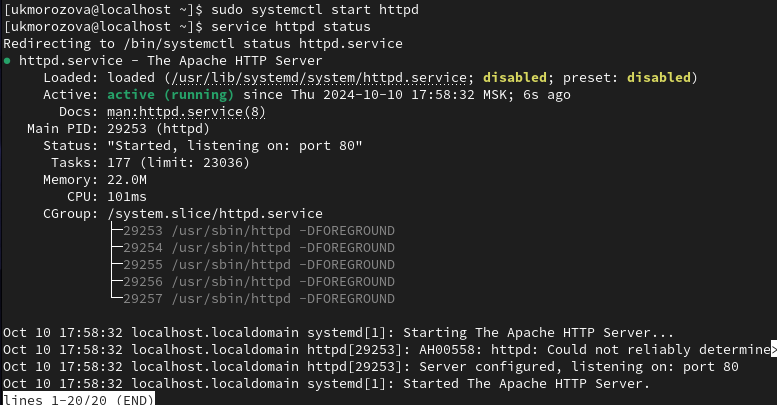


Рис. 4: httpd

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (рис. 5). Например, можно использовать команду

ps auxZ | grep httpd

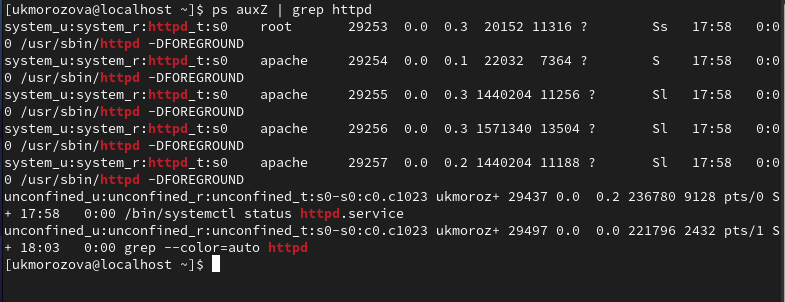


Рис. 5: веб-сервер Apache

1. Посмотрите текущее состояние переключателей SELinux для Apache спомощью команды

sestatus -bigrep httpd

Обратите внимание, что многие из них находятся в положении «off» (рис. 6).

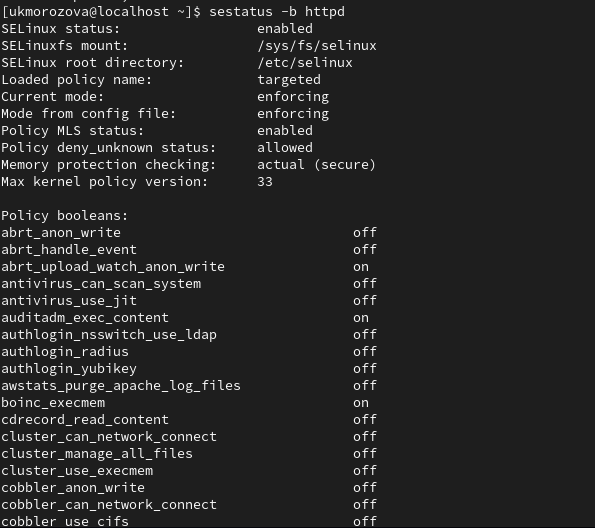


Рис. 6: переключатели SELinux

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (рис. 7).

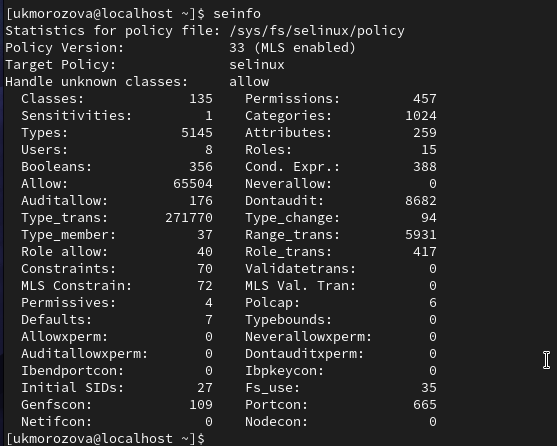


Рис. 7: seinfo

1. Определите тип файлов и поддиректорий (рис. 8), находящихся в директории /var/www, с помощью команды

ls -lZ /var/www

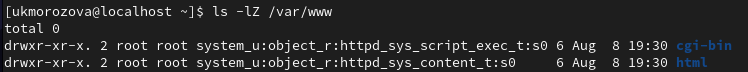


Рис. 8: /var/www

1. Определите тип файлов (рис. 9), находящихся в директории /var/www/html:

ls -lZ /var/www/html

Рис. 9: /var/www/html

Рис. 9: /var/www/html

1. Создайте от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис. 10 - рис. 11):

<html>  
<body>test</body>  
</html>

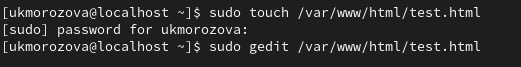


Рис. 10: Создание файла

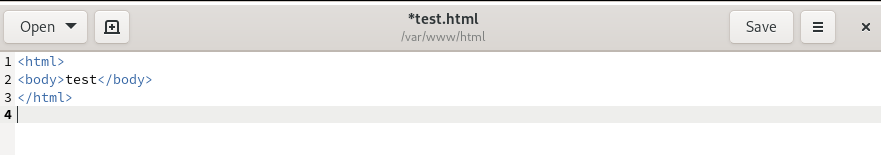


Рис. 11: test.html

1. Проверьте контекст созданного вами файла (рис. 12). Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

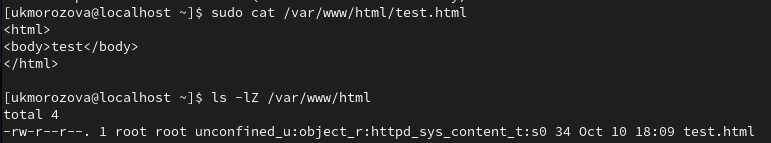


Рис. 12: контекст test.html

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 13). Убедитесь, что файл был успешно отображён.

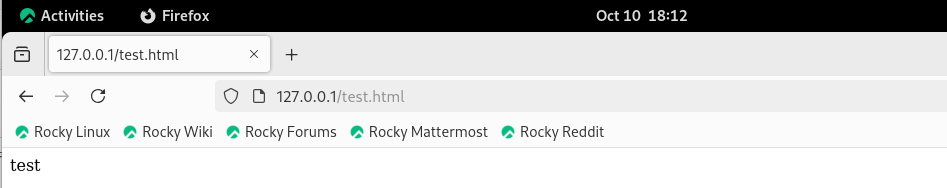


Рис. 13: test.html

1. Проверьте контекст файла командой

ls -Z /var/www/html/test.html

Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой (рис. 14), 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

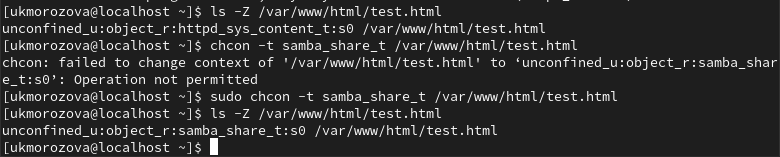


Рис. 14: Изменение контекста

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 15). Вы должны получить сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server.

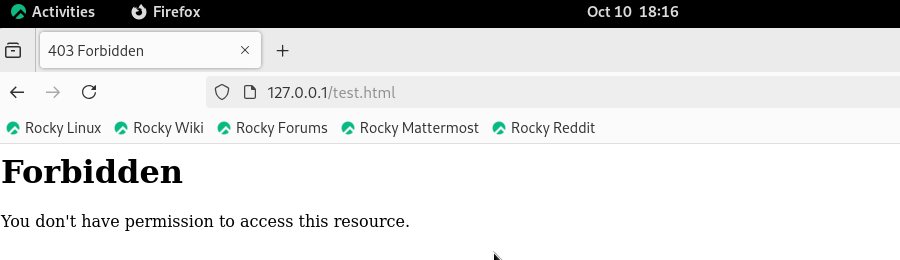


Рис. 15: Ошибка

1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

ls -l /var/www/html/test.html

Просмотрите log-файлы веб-сервера Apache (рис. 16). Также просмотрите системный лог-файл:

tail /var/log/messages

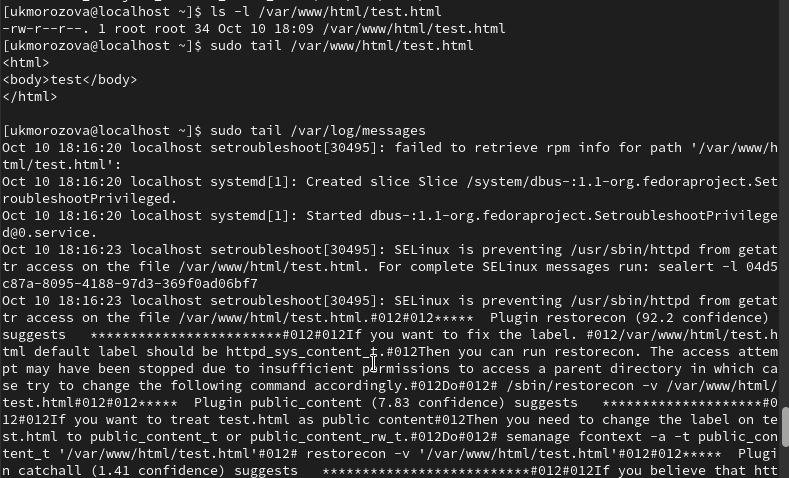


Рис. 16: log-файлы веб-сервера Apache

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. 17).

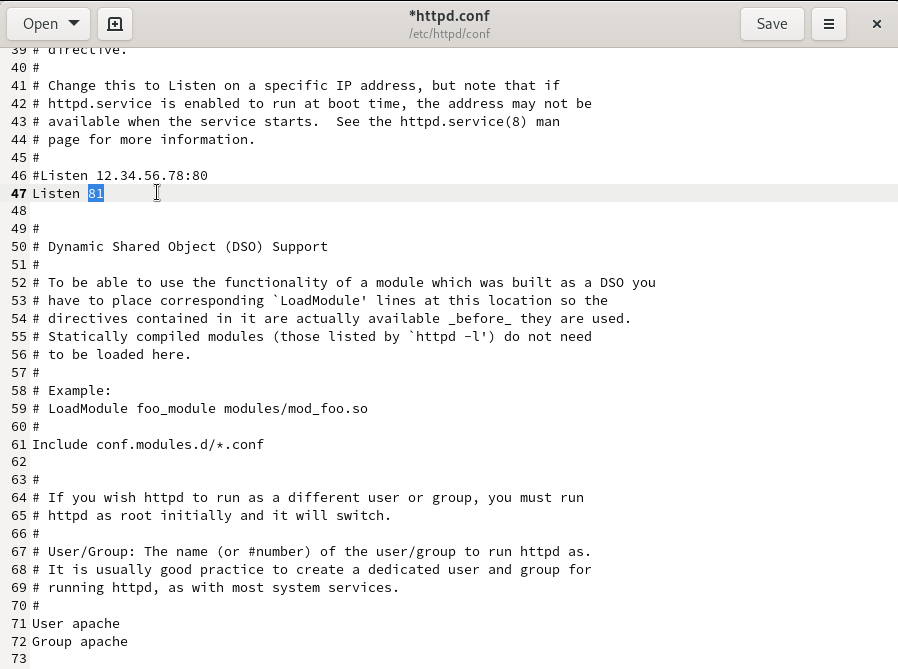


Рис. 17: Listen 81

1. Проанализируйте лог-файлы (рис. 18):

tail -nl /var/log/messages

Рис. 18: лог-файлы

Рис. 18: лог-файлы

Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи (рис. 19).

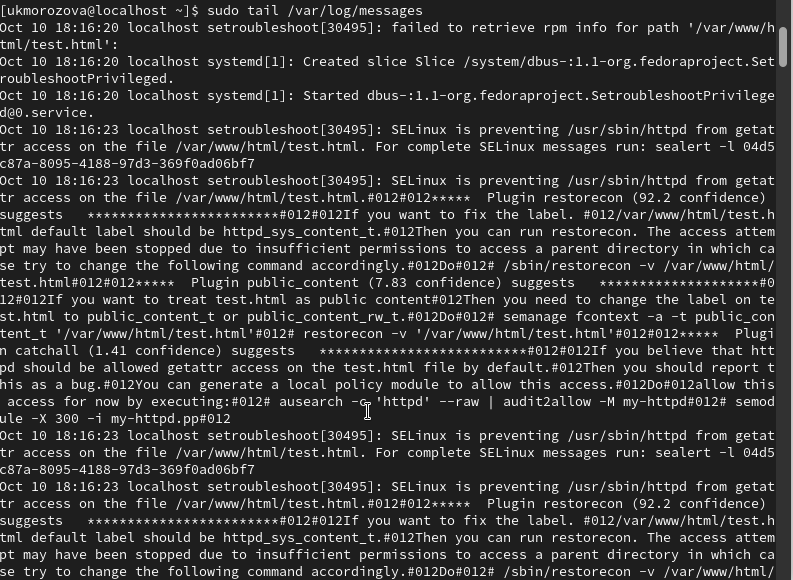


Рис. 19: error\_log

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

Убедитесь, что порт 81 появился в списке (рис. 20).

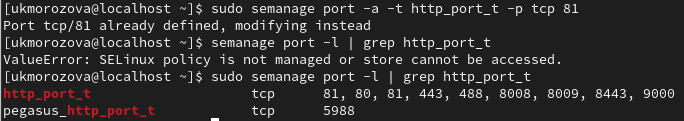


Рис. 20: semanage port

1. 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. Вы должны увидеть содержимое файла — слово «test» (рис. 21).

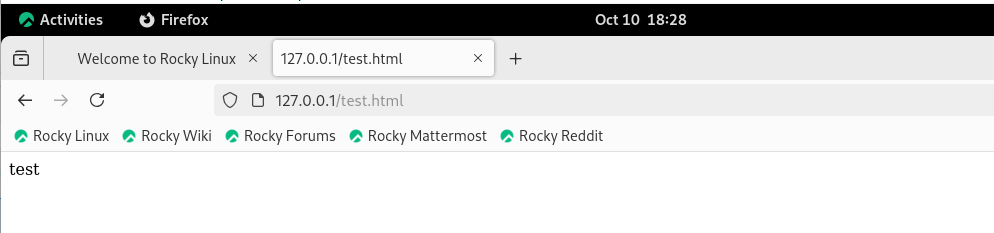


Рис. 21: веб-сервер Apache

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80 (рис. 22).

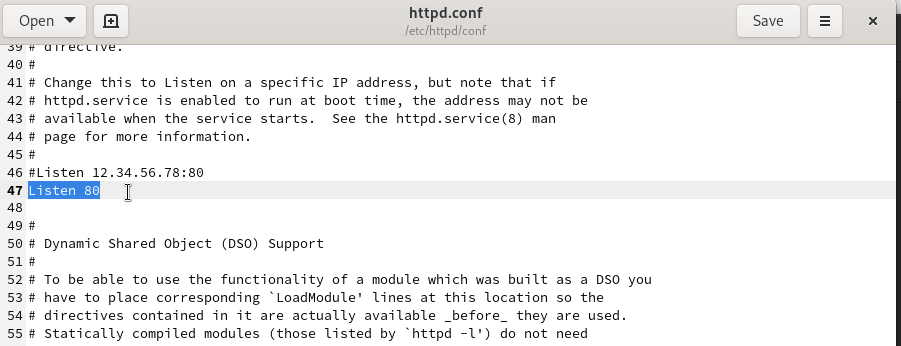


Рис. 22: Listen 80

1. 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. 23).

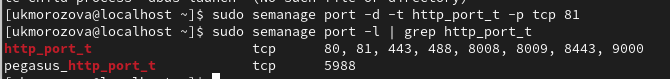


Рис. 23: порт 81

1. Удалите файл /var/www/html/test.html (рис. 24):

rm /var/www/html/test.html

Рис. 24: Удаление файла

Рис. 24: Удаление файла

# 4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы