Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Миличевич Александра

Содержание

[Цель работы 1](#_Toc88913918)

[Выполнение лабораторной работы 1](#_Toc88913919)

[Выводы 9](#_Toc88913920)

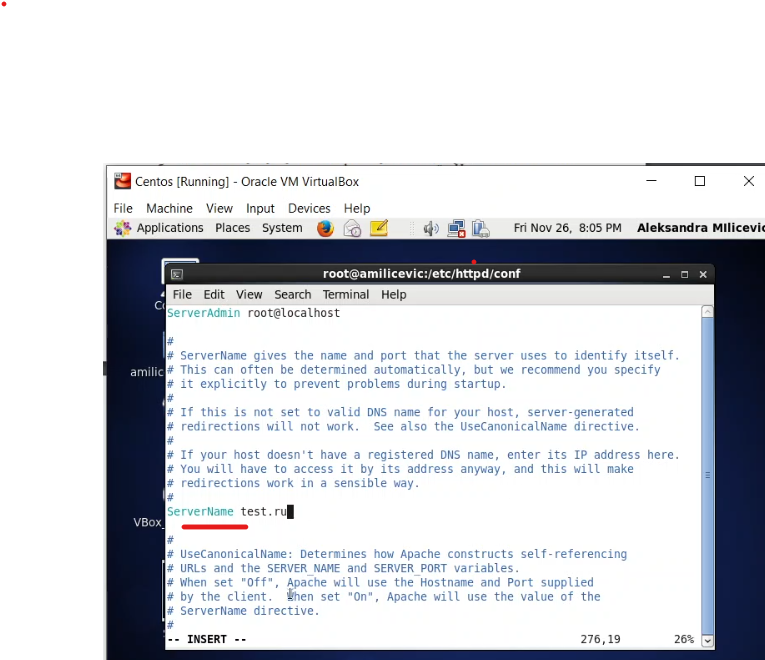
# Цель работы

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

# Выполнение лабораторной работы

\*\*Последовательность выполнения работы\*

1. SELinux — набор технологий расширения системы безопасности Linux. Сегодня основу набора составляют три технологии: мандатный контроль доступа, ролевой доступ RBAC и система типов (доменов). Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса

В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName. 

Отключила фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавила разрешающие правила.

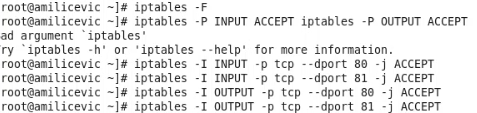


Рис. 2.

1. Вход в систему Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus

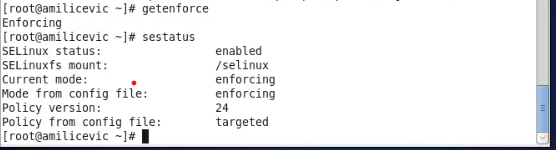


Рис. 3.

Обратилась с помощью браузера к веб-серверу, запущенному на компьютере

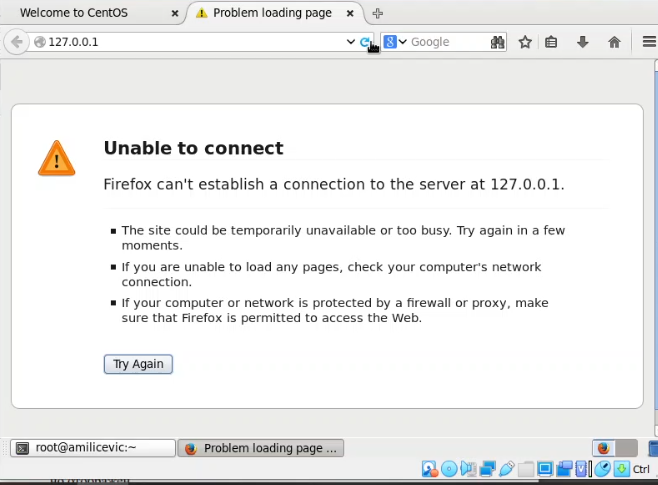
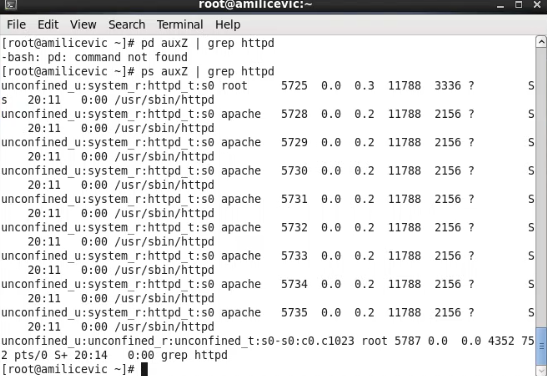
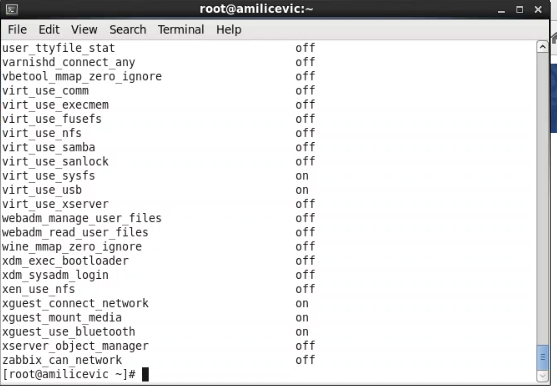


Рис. 4.

Рис. 5.

Рис. 5.

1. веб-сервер Apache Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. 

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: \*\*sestatus -bigrep httpd. 

Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: ls -lZ /var/www. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.

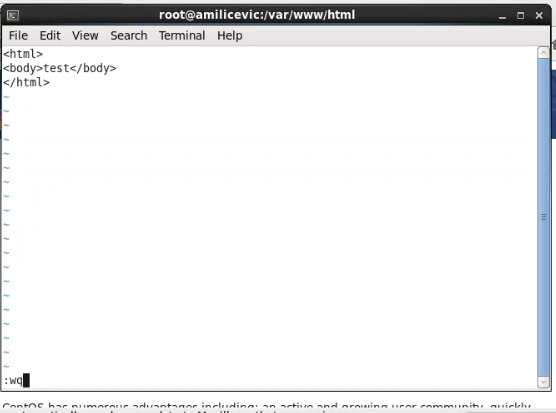
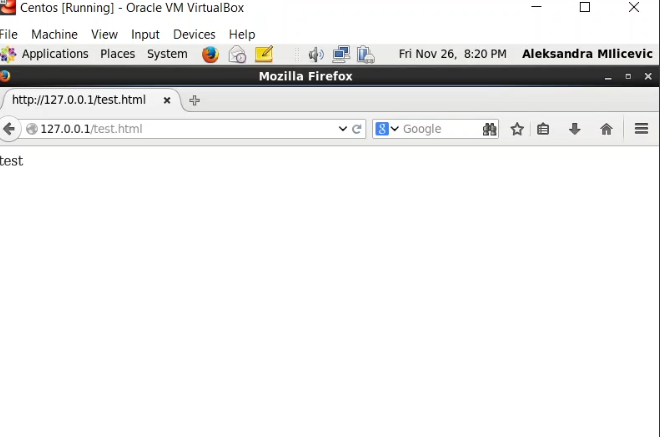


Рис. 8.

Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html



Рис. 9.

Проверила контекст созданного файла. httpd\_sys\_content\_t 

Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. файл был успешно отображён

Рис. 11.

Рис. 11.

Проверила контекст файла командой: ls -Z /var/www/html/test.html Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверила, что контекст поменялся. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение failiure.

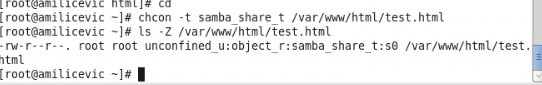


Рис. 12.

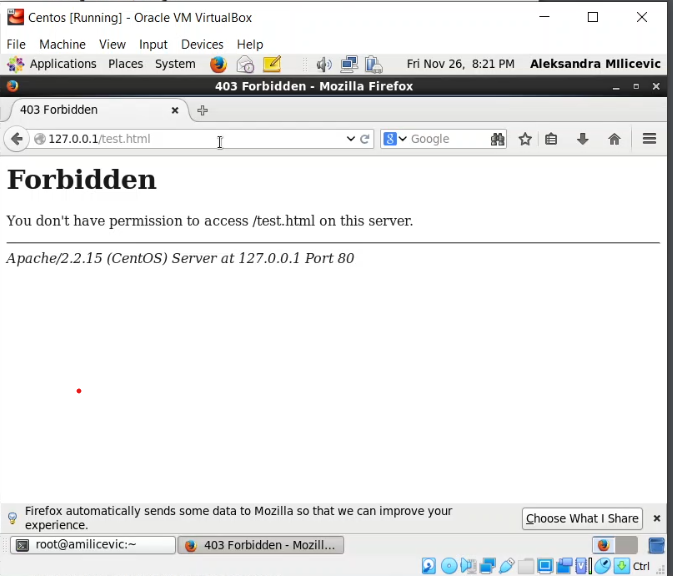


Рис. 13.

Рис. 14.

Рис. 14.

Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: tail /var/log/messages 

Рис. 16.

Рис. 16.

в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и замените её на Listen 81. Проанализиировала лог-файлы. Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log. (рис.18), (рис. 4.19), (рис.(рис. 20)

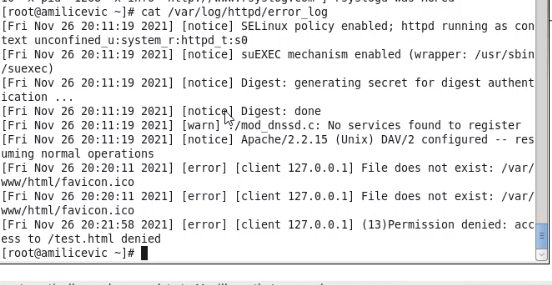
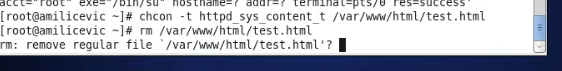


Рис. 17.

Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html. Удалила файл /var/www/html/test.html 

# Выводы

Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.