Лабораторная работа No 6.

Тагиев Байрам Алтай оглы

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

# 2 Выполнение лабораторной работы

## 2.1 Подготовка лабораторного стенда

1. Установить Apache2 при помощи dnf.

dnf install httpd

1. В конфигурационном файле httpd.conf прописать параметр ServerName ([1](#fig:001)).

Figure 1: ServerName

Figure 1: ServerName

1. Отключить пакетный фильтр при помощи iptables ([2](#fig:002)).

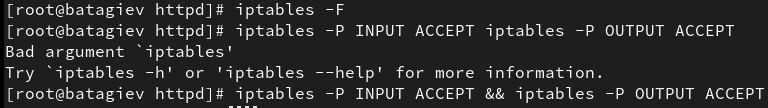


Figure 2: iptables

## 2.2 Выполнение

1. Проверим правильность работы SELinux. Должен быть выставлен режим enforcing политики targeted ([3](#fig:003)).

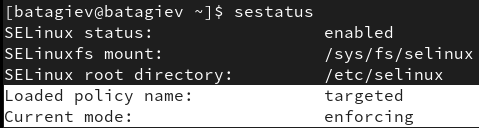


Figure 3: sestatus

1. Запустим Apache веб-сервер ([4](#fig:004)).

Figure 4: httpd

Figure 4: httpd

1. В списке процессов найдем httpd ([5](#fig:005)). На этот процесс выставлен следующий контекст безопасности (первый столбец изображения [1]).

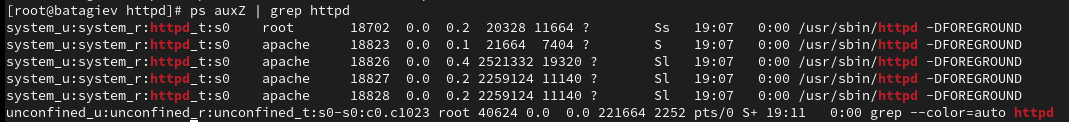


Figure 5: Контекст безопасности

1. Посмотрим текущее состояние переключателей SELinux для Apache2 ([6](#fig:006)).

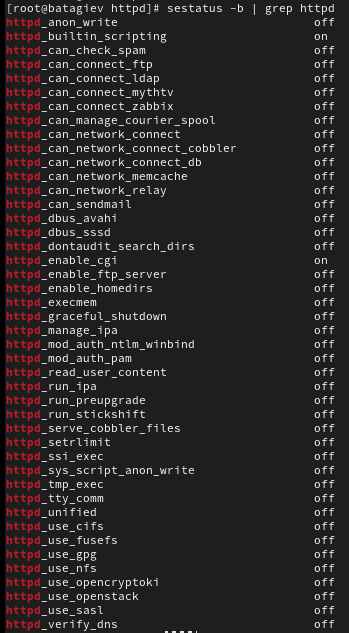


Figure 6: переключатели SELinux

1. Также посмотрим текущую статистику по политике ([7](#fig:007)).

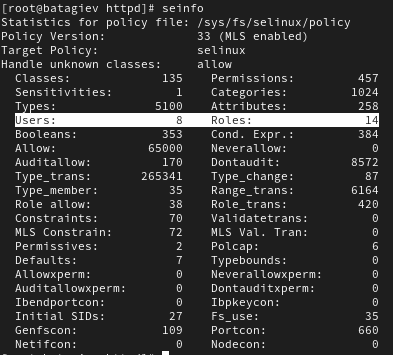


Figure 7: Статистика по политике

1. Посмотрим текущий контекст безопасности для файлов и поддиректорий в директории /var/www ([8](#fig:008)).

* Установлен контекст httpd\_sys\_script\_exec\_t для cgi-скриптов, чтобы был разрешен им доступ ко всем sys-типам.
* Установлен контекст httpd\_sys\_content\_t для содержимого, которое должно быть доступно для всех скриптов httpd и для самого демона.

Figure 8: Контекст безопасности

Figure 8: Контекст безопасности

1. В директории /var/www/html пусто.

Figure 9: /var/www/html

Figure 9: /var/www/html

1. В директории /var/www/html создавать папки может только root (право w есть только у него).
2. Создадим файл /var/www/html/test.html ([10](#fig:010)).

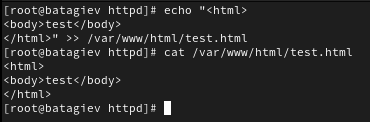


Figure 10: test.html

1. Проверим контекст созданного нами файла ([11](#fig:011)).

Figure 11: test.html

Figure 11: test.html

1. Перейдем в браузер и в нем проверим доступность данного файла ([12](#fig:012)).

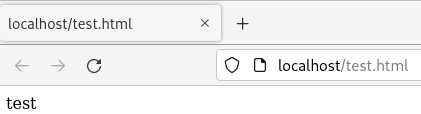


Figure 12: Проверка

1. Изменим конекст файла, чтобы Apache не смог получить доступ ([13](#fig:013)).

Figure 13: test.html

Figure 13: test.html

1. Проверим, что доступ к файлу стал не доступен ([14](#fig:014)).

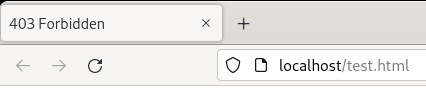


Figure 14: Проверка

1. Посмотрим логи от веб-сервера Apache ([15](#fig:015)).

Figure 15: /var/log/messages

Figure 15: /var/log/messages

Также проверим audit.log ([16](#fig:0151)).

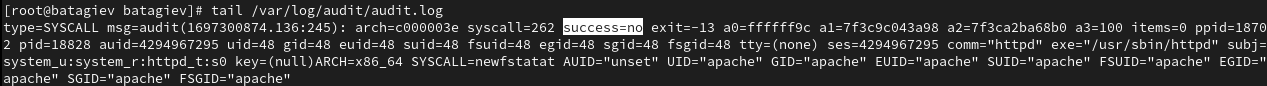


Figure 16: /var/log/audit/audit.log

1. Поменяем порт, на котором работает Apache.

Figure 17: Порт 81

Figure 17: Порт 81

1. Перезапустим веб-сервер (успешно).

Figure 18: Перезапуск

Figure 18: Перезапуск

1. В логах наблюдаем запуск сервера на 81 порту.

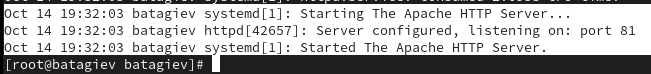


Figure 19: /var/log/messages

1. Добавим порт в semanage для http\_port\_t и проверим его добавление

Figure 20: Добавление

Figure 20: Добавление

Figure 21: Проверка

Figure 21: Проверка

1. Ввернем контекст файлу test.html.
2. Удалим привязку порта.
3. Удалим файл test.html.

# 3 Выводы

В результате выполнения работы я выполнил цели работы.

1. SELinux/Tutorials/Linux services and the system u SELinux user - Gentoo wiki — wiki.gentoo.org. <https://wiki.gentoo.org/wiki/SELinux/Tutorials/Linux_services_and_the_system_u_SELinux_user>.