

# Отчёт по лабораторной работе №6

## Информационная безопасность

### Мандатное разграничение прав в Linux

Выполнил: Маляров Семён Сергеевич,  
НПИбд-01-21, 1032209505

#### Содержание

1	Цель работы.....	1
2	Теоретическое введение.....	1
3	Выполнение лабораторной работы.....	2
4	Вывод.....	3
5	Список литературы. Библиография.....	3

#### 1 Цель работы

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

#### 2 Теоретическое введение

1. **SELinux (Security-Enhanced Linux)** обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена.

*SELinux имеет три основных режим работы:*

- Enforcing: режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- Permissive: в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- Disabled: полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [1].

2. **Apache** — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA).

*Для чего нужен Apache сервер:*

- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

Более подробно см. в [2].

### 3 Выполнение лабораторной работы

Войдём в систему и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает

Затем найдём веб-сервер Apache в списке процессов и определим его контекст безопасности

Посмотрим текущее состояние переключателей SELinux для Apache

Далее посмотрим статистику по политике

Определим тип файлов и поддиректорий, находящихся в директории `/var/www`

Определим тип файлов, находящихся в директории `/var/www/html`

Следующим шагом создадим от имени суперпользователя html-файл `/var/www/html/test.html` с содержанием “test”

Проверим контекст созданного нами файла

Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html` и проверим контекст файла

Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`

Попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`

Просмотрим log-файлы веб-сервера Apache и системный лог-файл

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`)

Выполним перезапуск веб-сервера Apache

Проанализируем лог-файлы: `tail -nl /var/log/messages, /var/log/http/error_log, /var/log/http/access_log` и `/var/log/audit/audit.log`

Выполним команду `semanage port -a -t http_port_t -p tcp 81` и после этого проверим список портов

Вернём контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`

Исправим обратно конфигурационный файл `apache`, вернув `Listen 80`

Удалим привязку `http_port_t` к 81 порту

Удалим файл `/var/www/html/test.html`

## 4 Вывод

В ходе выполнения лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.

## 5 Список литературы. Библиография

[1] SELinux: <https://habr.com/ru/companies/kingservers/articles/209644/>

[2] Apache: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>