Лабораторная работа 6

Накова Амина

2025-09-20

1. Вводная часть

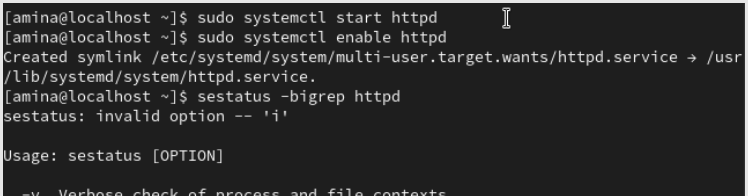
1.1 Цель работы

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

2. Ход работы

2.1 Подготовка рабочего места

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux. Предполагается использовать стандартный дистрибутив Linux CentOS с включённой политикой SELinux targeted и режимом enforcing. Для выполнения заданий требуется наличие учётной записи администратора (root) и учётной записи обычного пользователя. Постоянно работать от учётной записи root неправильно с точки зрения безопасности (рис. 1).



3. Выводы

В ходе лабораторной работы было получено практическое знакомство с технологией SELinux. Были изучены основные механизмы мандатного разграничения доступа в Linux, работа с контекстами безопасности, портами и политиками.
Исследование показало, что:

1. SELinux обеспечивает дополнительный уровень безопасности поверх стандартных прав доступа

Работа позволила получить практические навыки администрирования SELinux и понимание важности мандатного контроля доступа в современных операционных системах

3. Выводы

В ходе лабораторной работы было получено практическое знакомство с технологией SELinux. Были изучены основные механизмы мандатного разграничения доступа в Linux, работа с контекстами безопасности, портами и политиками.
Исследование показало, что:

1. SELinux обеспечивает дополнительный уровень безопасности поверх стандартных прав доступа
2. Контексты безопасности определяют, какие процессы могут обращаться к каким ресурсам

Работа позволила получить практические навыки администрирования SELinux и понимание важности мандатного контроля доступа в современных операционных системах

3. Выводы

В ходе лабораторной работы было получено практическое знакомство с технологией SELinux. Были изучены основные механизмы мандатного разграничения доступа в Linux, работа с контекстами безопасности, портами и политиками.
Исследование показало, что:

1. SELinux обеспечивает дополнительный уровень безопасности поверх стандартных прав доступа
2. Контексты безопасности определяют, какие процессы могут обращаться к каким ресурсам
3. Изменение контекста файла может заблокировать доступ к нему, даже если стандартные права доступа разрешают чтение

Работа позволила получить практические навыки администрирования SELinux и понимание важности мандатного контроля доступа в современных операционных системах

3. Выводы

В ходе лабораторной работы было получено практическое знакомство с технологией SELinux. Были изучены основные механизмы мандатного разграничения доступа в Linux, работа с контекстами безопасности, портами и политиками.

Исследование показало, что:

1. SELinux обеспечивает дополнительный уровень безопасности поверх стандартных прав доступа
2. Контексты безопасности определяют, какие процессы могут обращаться к каким ресурсам
3. Изменение контекста файла может заблокировать доступ к нему, даже если стандартные права доступа разрешают чтение
4. Для работы служб на нестандартных портах необходимо явно добавлять эти порты в политику SELinux

Работа позволила получить практические навыки администрирования SELinux и понимание важности мандатного контроля доступа в современных операционных системах