Отчёта по лабораторной работе №9

Отчет

Зубов Иван Александрович

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Задание

1. Продемонстрируйте навыки по управлению режимами SELinux
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux
3. Настройте контекст безопасности для нестандартного расположения файлов вебслужбы
4. Продемонстрируйте навыки работы с переключателями SELinux

# 3 Выполнение лабораторной работы

## 3.1 Управление режимами SELinux

Получаем полномочия администратора и смотрим текущую информацию о состоянии SELinux

Построчное пояснение информации на экране

SELinux status: enabled — SELinux включен в системе. SELinuxfs mount — точка монтирования виртуальной ФС SELinux. SELinux root directory — корневая директория конфигурации SELinux. Loaded policy name: targeted — загружена политика «targeted» (ограничивает только определённые сервисы). Current mode: enforcing — текущий режим: принудительный (правила применяются). Mode from config file: enforcing — режим из конфигурационного файла тоже «enforcing». Policy MLS status: enabled — поддержка Multi-Level Security включена. Policy deny\_unknown status: allowed — неизвестные действия по умолчанию разрешены. Memory protection checking — проверка защиты памяти активна. Max kernel policy version — максимальная версия политики, поддерживаемая ядром.

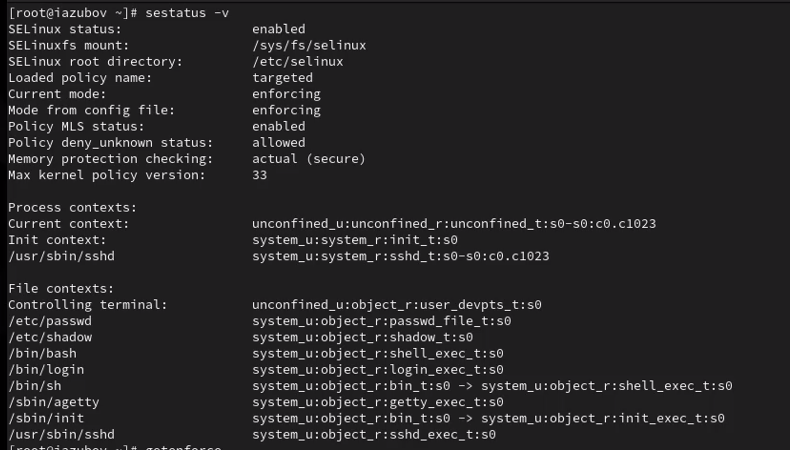


Рис. 1: Смотрим информацию

Посмотрим, в каком режиме работает SELinux и изменим режим работы SELinux на разрешающий (Permissive)



Рис. 2: Изменяем режим

Редактируем файл /etc/sysconfig/selinux и перезагружаем систему

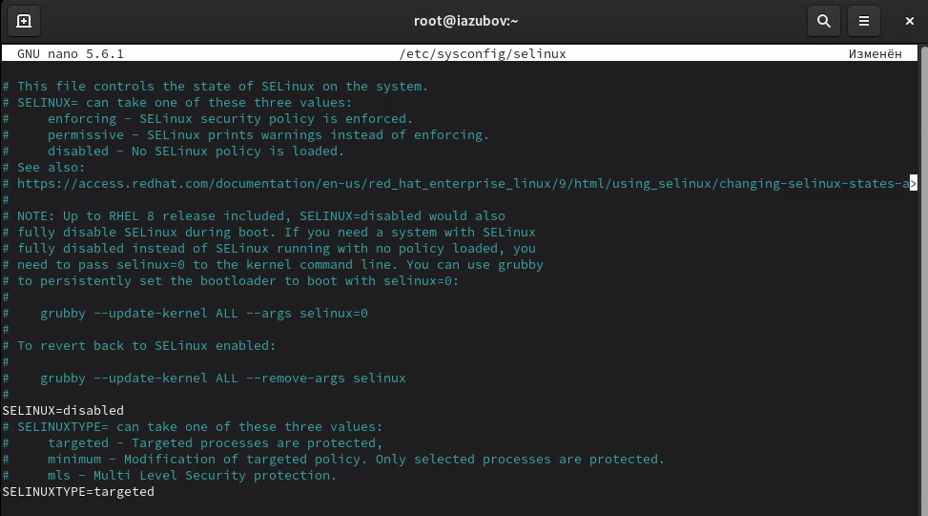
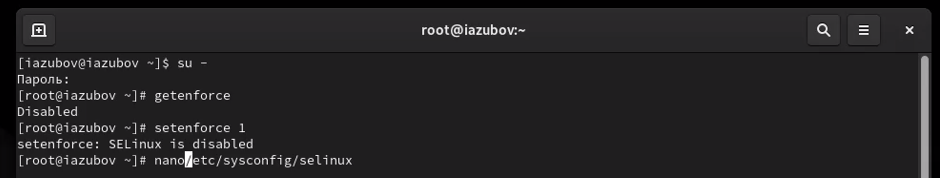


Рис. 3: Редактируем файл

Посмотрим статус SELinux и увидим,что он отключен. Переключаем режим работы Дальше откроем файл /etc/sysconfig/selinux с помощью редактора и установим: SELINUX=enforcing Перезагружаем систему Во время перезагрузки мы получили предупреждающее сообщение и убедились потом ,что система работает в принудительном режиме 

## 3.2 Использование restorecon для восстановления контекста безопасности

Посмотрите контекст безопасности файла /etc/hosts Скопируйте файл /etc/hosts в домашний каталог и проверим контекст файла ~/hosts



Рис. 4: Проверяем контексты файлов

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc и изменяем тип контекста

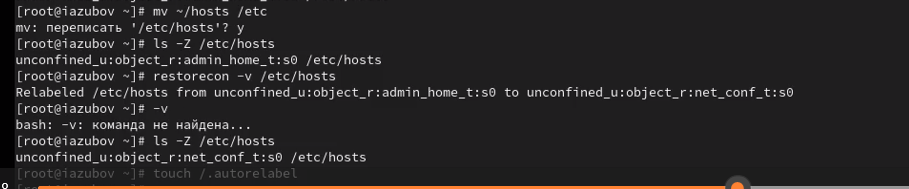


Рис. 5: Изменяем тип контекста

## 3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Устанавливаем программное обеспечение

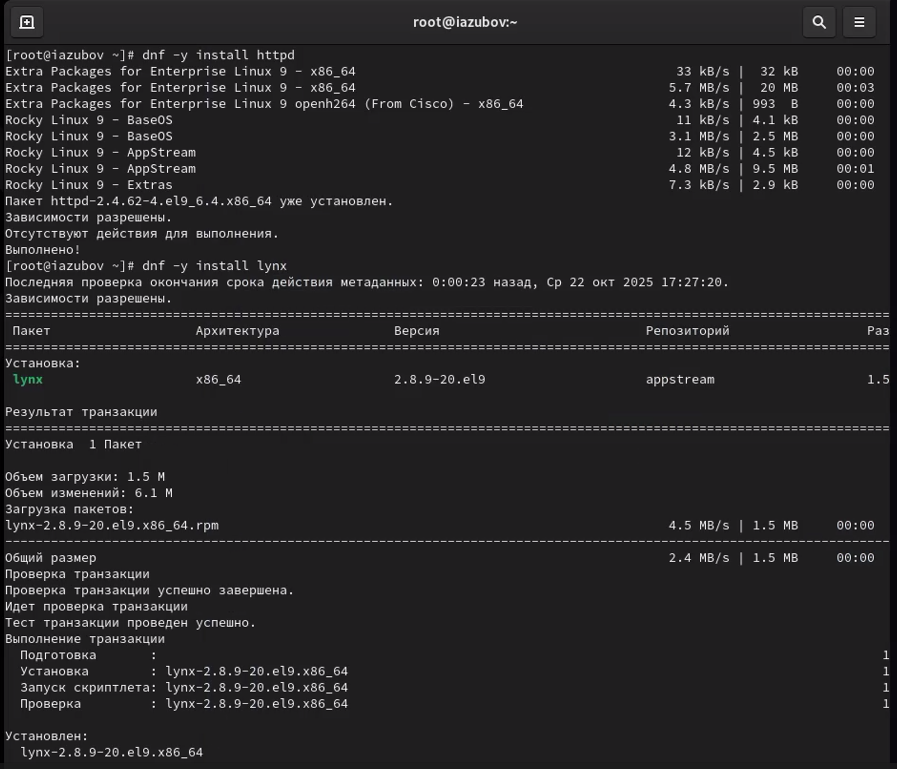


Рис. 6: Установка ПО

Создаем новое хранилище для файлов web-сервера и файл



Рис. 7: Создаем каталог и файл

С помощью редактора nano редактируем файл index.html

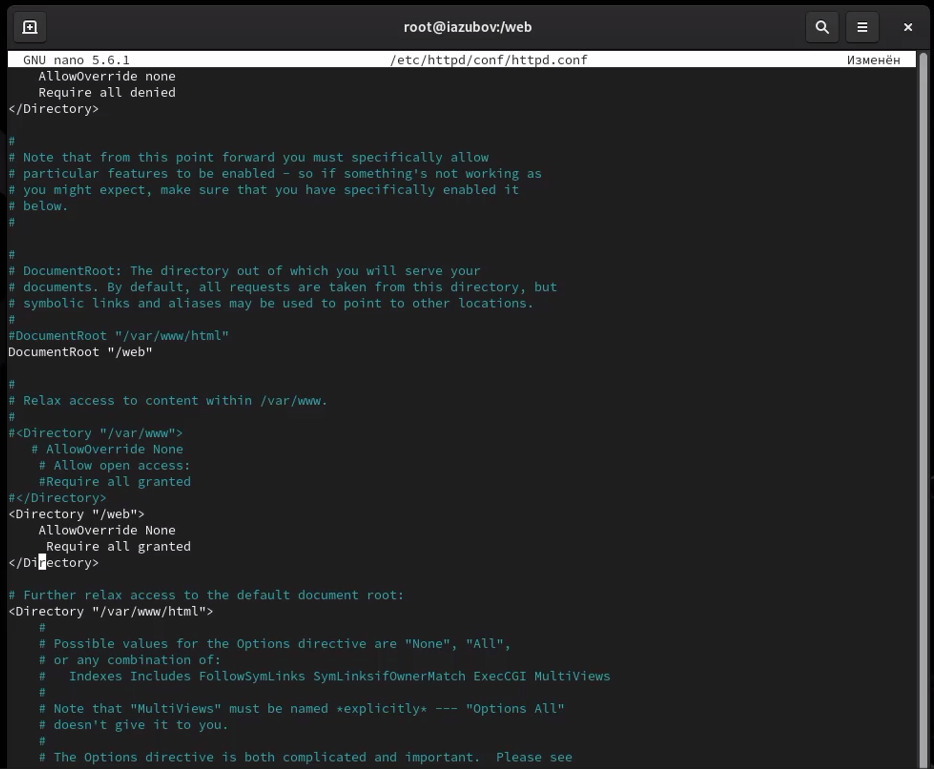


Рис. 8: Редактируем файл

Запускаем веб сервер и службу httpd Запускаем веб страница. Она будет просто по умолчанию

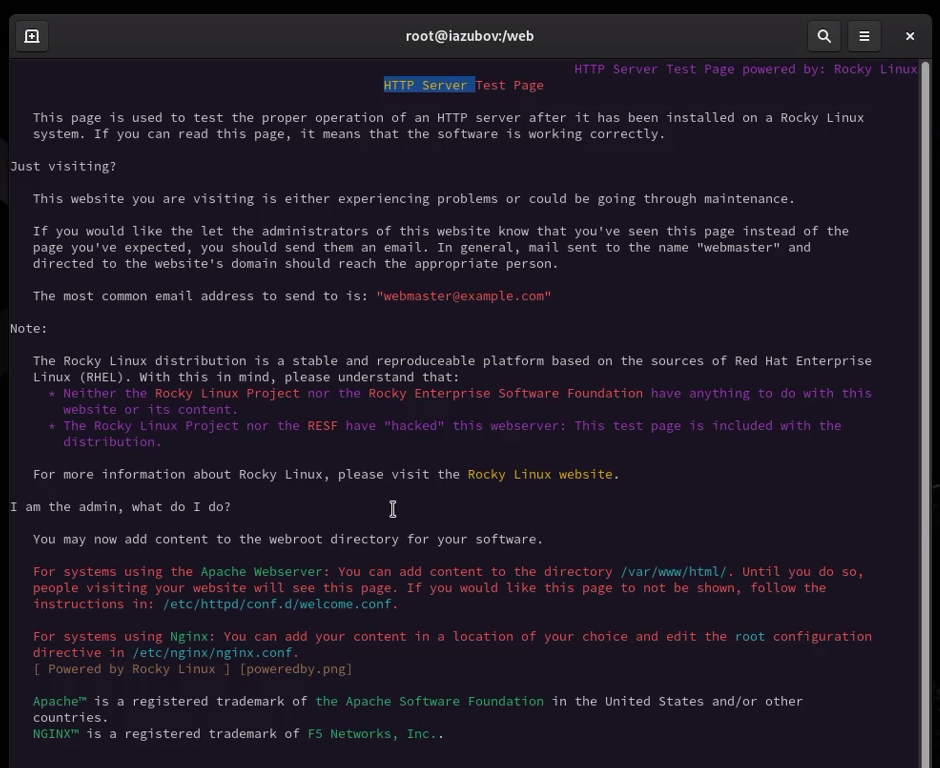


Рис. 9: Запускаем службу

В терминале применим новую метку контекста к /web и восстановим контекст безопасности

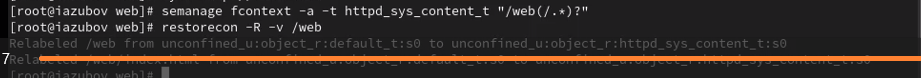


Рис. 10: Применяем новую метку контекста и восстановим метку безопасности

Запускаем наш веб сервер

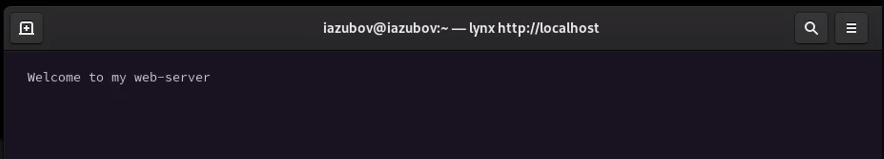


Рис. 11: Welcome to my web-server

## 3.4 Работа с переключателями SELinux

Смотрим списки переключателей и изменяем их

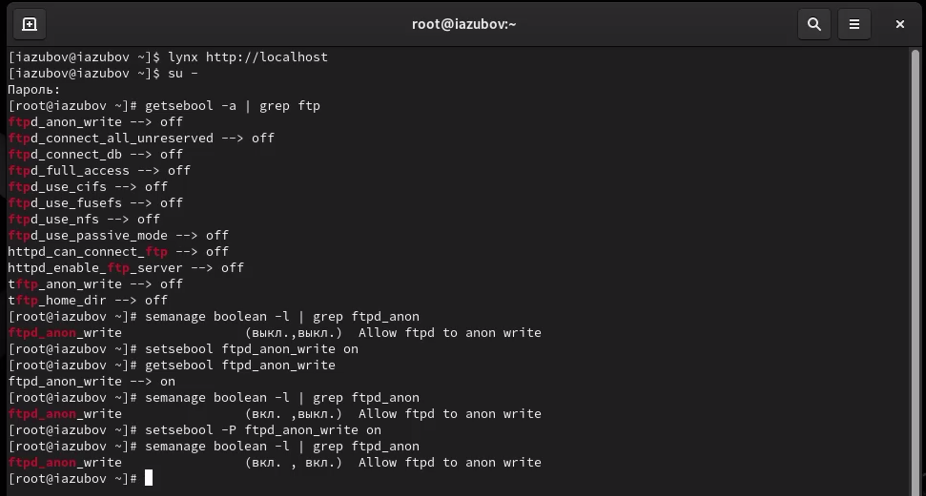


Рис. 12: Работа с переключателями

# 4 Выводы

Я получил навыки работы с контекстом безопасности и политиками SELinux.

# 5 Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? setenforce 0
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? getsebool -a
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? selinux-policy-doc
4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd\_sys\_content\_t к каталогу /web? semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?” restorecon -R /web
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? /etc/selinux/config (изменить SELINUX=disabled
6. Где SELinux регистрирует все свои сообщения? /var/log/messages
7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?seinfo -t | grep ftp
8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать? Временно перевести SELinux в режим setenforce Permissive и проверить работу сервиса