Лабараторная работа №9

Отчет

Славинский Владислав Вадимович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

Запускаем терминал в режиме суперпользователя через su - и просмотрим текущую информацию о состоянии SELinux: sestatus -v. 1) SELinux status: enabled - это строчка означает, что SELinux активирован. 2) SELinux mount - SELinux смонтирована в каталоге /sys/fs/selinux, SELinux root directory - корневой каталог конфигурации SELinux находится в /etc/selinux, 3) Loaded policy name - загружена политика безопасности типа targeted, которая защищает только определенные системные процессы, 4) Current mode: enforcing - принудительный режим работы, SELinux активно блокирует действия, нарушающие политику безопасности, 5) Mode from config file: enforcing - режим конфигурационного файла установлен как enforcing, что означает сохранение этого режима после перезагрузки, 6) Policy MLS status: enabled - поддержка многоуровневой безопасности активирована (Multi-Level-Security), 7) Policy deny_unknown status: allowed - неизвестные действия по умолчанию разрешены, 8) Memory protection checking: actual (secure) - проверка защиты памяти выполнеяется на безопасном уровне, 9) Max kernel policy version: 33 - максимальная поддерживаемая версия политики ядра 33, 10) Current context - Текущий процесс (терминал) работает в неограниченном контексте с высоким уровнем привелегий, 11) Init context - процесс init (родительский процесс системы) работает в соответствующем контексте, 12) /usr/sbin/sshd - SSH демон работает в правильном контексте безопасности для SSH службы, 13) /etc/passwd, /etc/shadow - имеют правильные контексты для файлов с паролями, 14) /bin/bash, /bin/login - имеют контексты исполняемых файлов оболочки и входа в систему, 15) /sbin/agetty, /sbin/init - имеют соответствующие контексты

для системных служб, 16) /usr/sbin/sshd - имеет правильный контекст для SSH демона. (рис. 2.1)

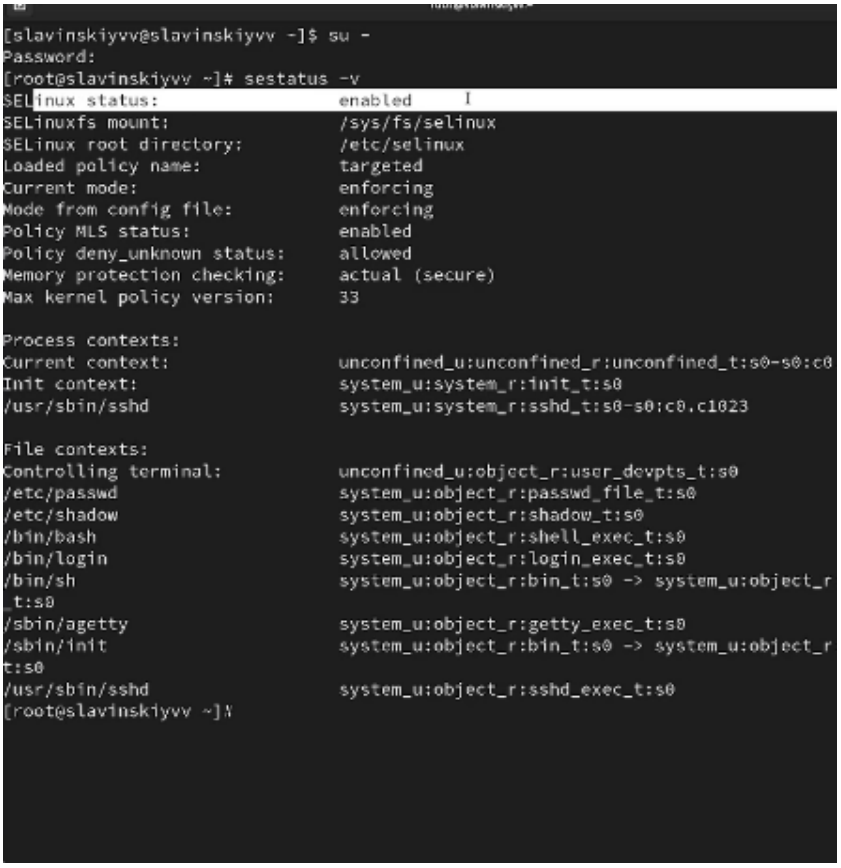

Рис. 2.1: Просмотр информации о состоянии SELinux с помощью root прав

Посмотрим, в каком режиме работает SELinux: getenforce. Видим, что работает в режиме enforcing (в режиме принудительного исполнения.(рис. 2.2)

Рис. 2.2: Режим работы SELinux

Изменим режим работы SELinux на разрешающий (Permissive): setenforce 0. Потом введем снова getenforce. (рис. 2.3)

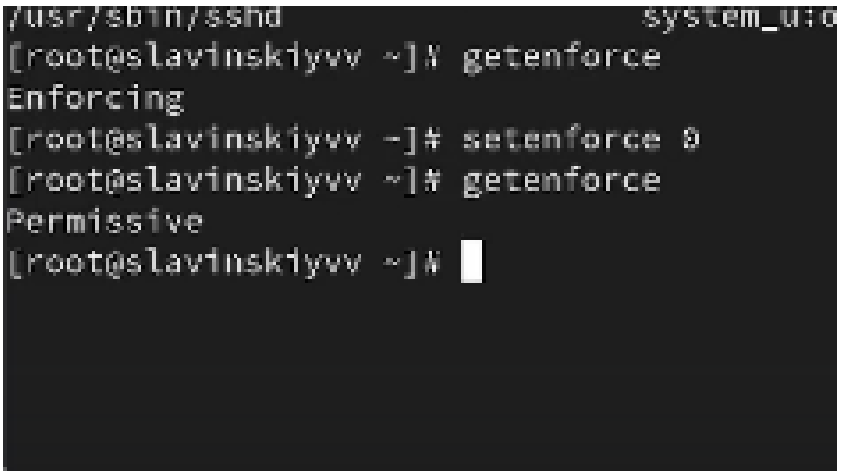

Рис. 2.3: Изменения режима работы

В файле /etc/sysconfig/selinux с помощью редактора установим SELINUX=disabled и перезапустим систему. (рис. 2.4)

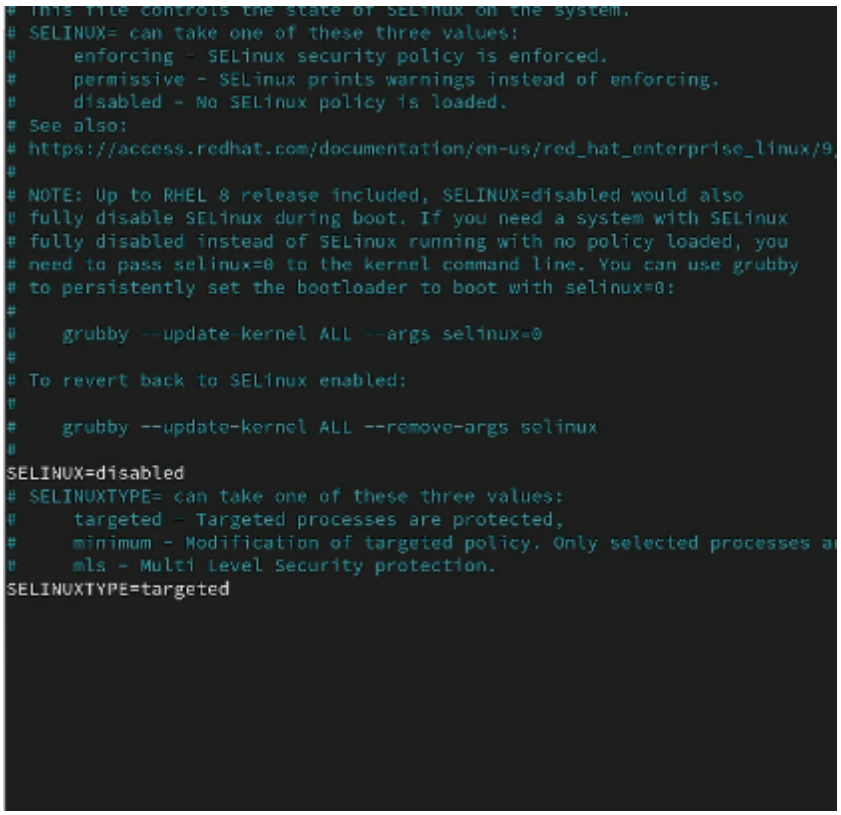

Рис. 2.4: Изменение файла и перезапуск системы

После перезагрузки запустим терминал и получим полномочия администрато-

ра.Посмотрим статус SELinux: getenforce. Мы видим, что SELinux теперь отключён. (рис. 2.5)

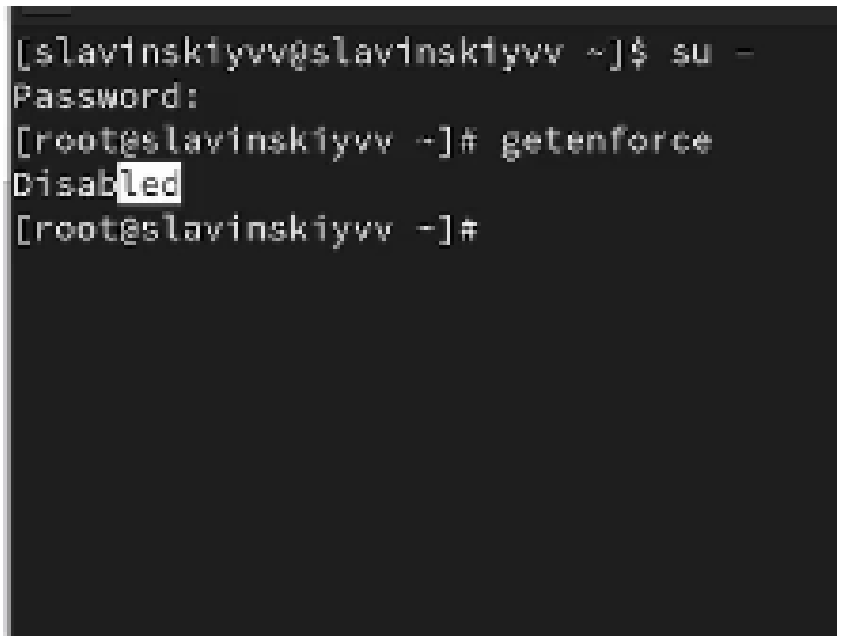

Рис. 2.5: Перезагрузки и проверка статуса SELinux

Попробуем переключить режим работы SELinux: setenforce 1. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы.(рис. 2.6)

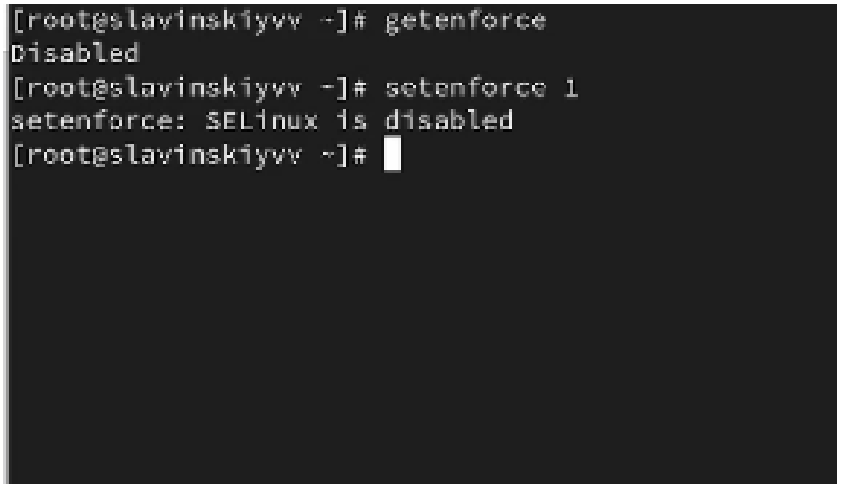

Рис. 2.6: Попытка переключить режим работы SELinux

Откроем файл /etc/sysconfig/selinux с помощью редактора и установим:

SELINUX=enforcing. Затем перезагрузим систему. (рис. 2.7)

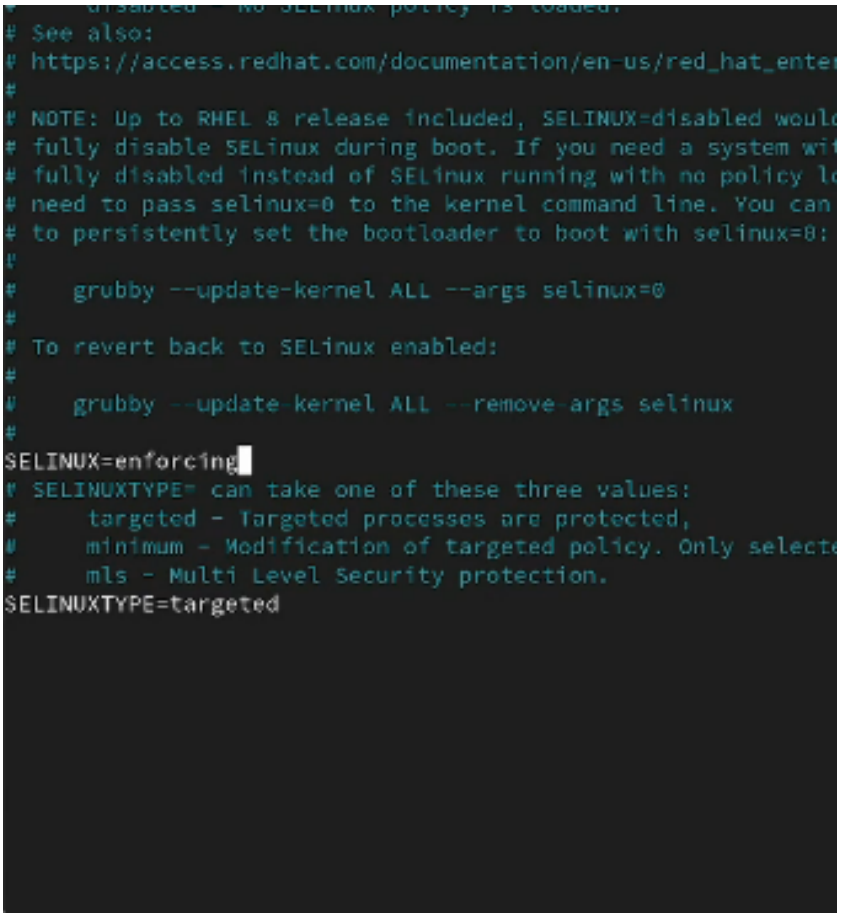

Рис. 2.7: Редактирование файла и перезагрузка системы

Во время загрузки системы мы получаем предупреждающее сообщение (Relabeling could take a very long time) о необходимости восстановления меток SELinux, это занимает некоторое время, а также труебется дополнительная перезагрузка системы. (рис. 2.8)

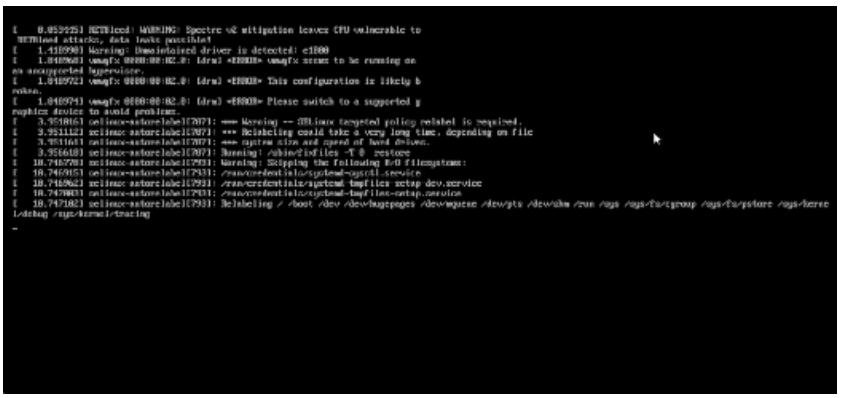

Рис. 2.8: Перезагрузка системы

После перезагрузки в терминале с полномочиями администратора просмотрим текущую информацию о состоянии SELinux: sestatus -v. Видим, что система работает в режиме enforcing.(рис. 2.9)

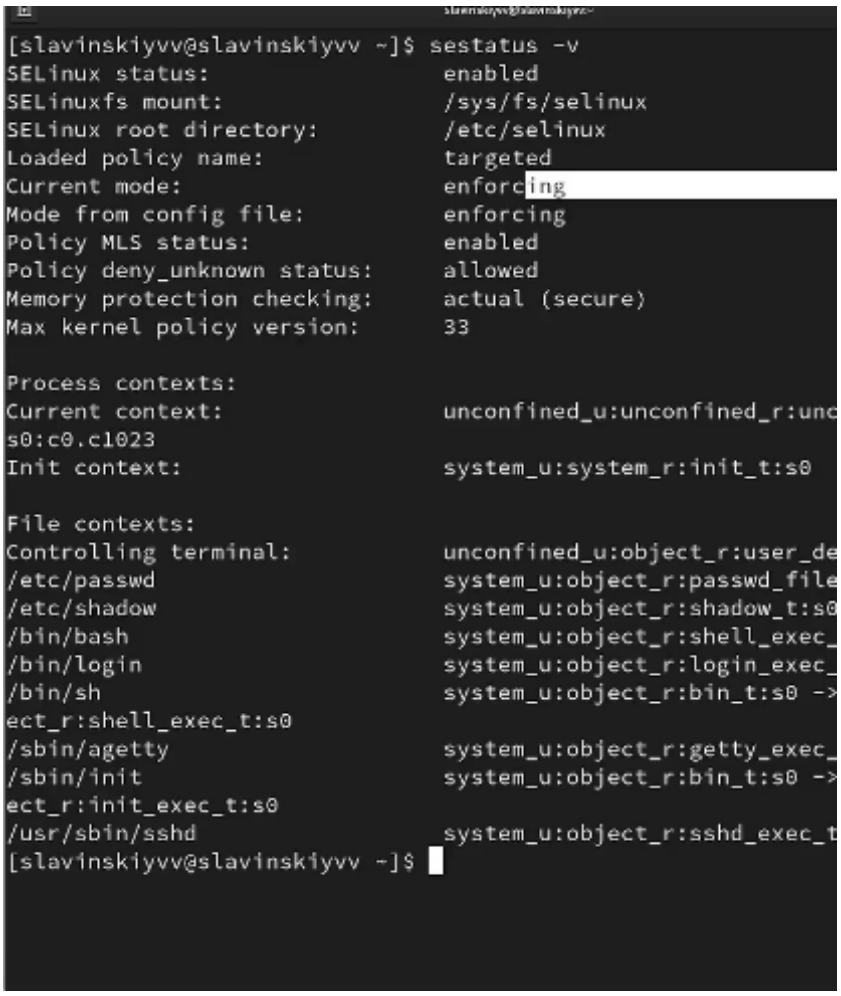

Рис. 2.9: Проверка статуса

Запустим терминал и получим полномочия администратора. Затем посмотрим контекст безопасности файла /etc/hosts: ls -Z /etc/hosts. Видим, что присутствует метка net_conf_t, что указывает на тип файла сетевой конфигурации. (рис. 2.10)

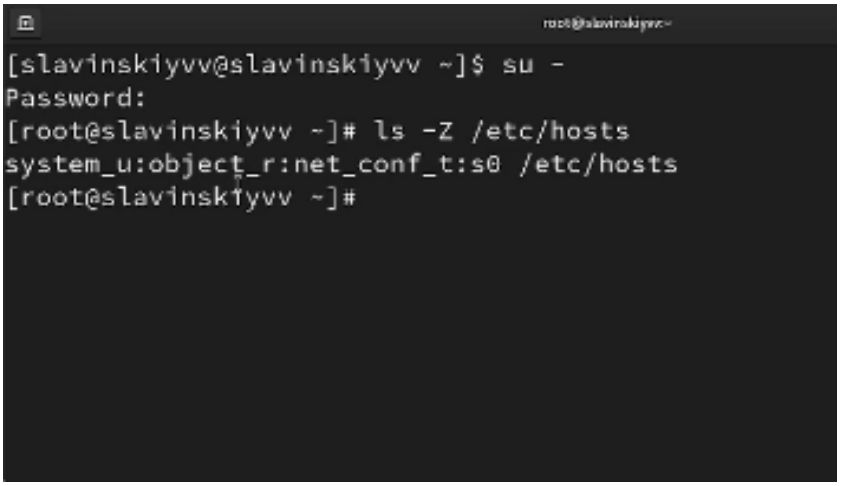

Рис. 2.10: Просмотр контекста безопасности файла

Скопируем файл /etc/hosts в домашний каталог: cp /etc/hosts ~/, проверим контекст файла ~/hosts: ls -Z ~/hosts. Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin_home_t. (рис. 2.11)

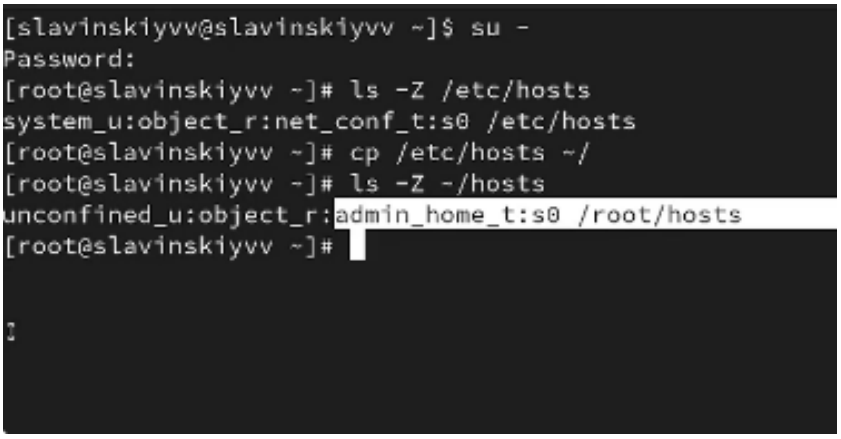

Рис. 2.11: Копирование файла в домашний каталог

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: mv ~/hosts /etc. И убедимся, что что тип контекста по-прежнему установлен на admin_home_t: ls -Z /etc/hosts. (рис. 2.12)

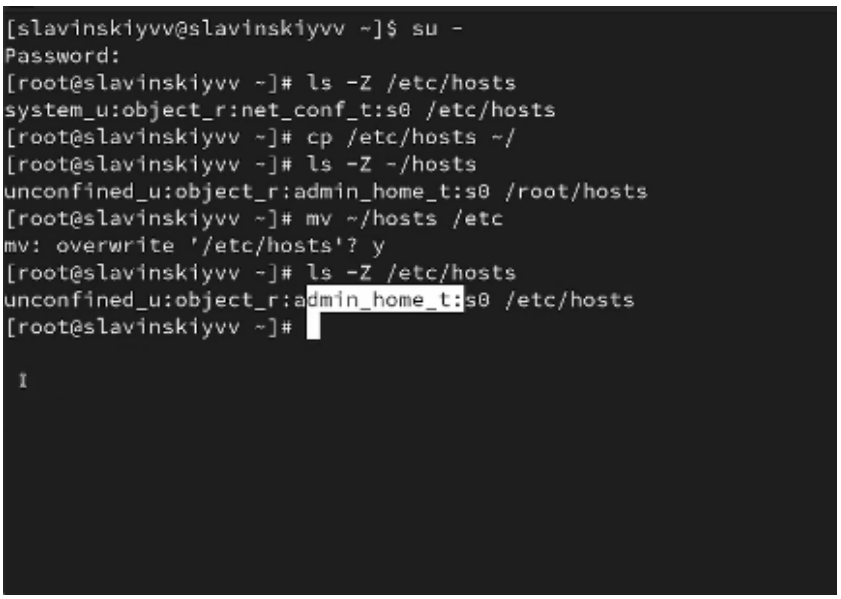

Рис. 2.12: Перезапись файла из домашнего каталога

Исправим контекст безопасности: restorecon -v /etc/hosts. Опция -v покажет нам процесс изменения. И проверим, что что тип контекста изменился: ls -Z /etc/hosts. (рис. 2.13)

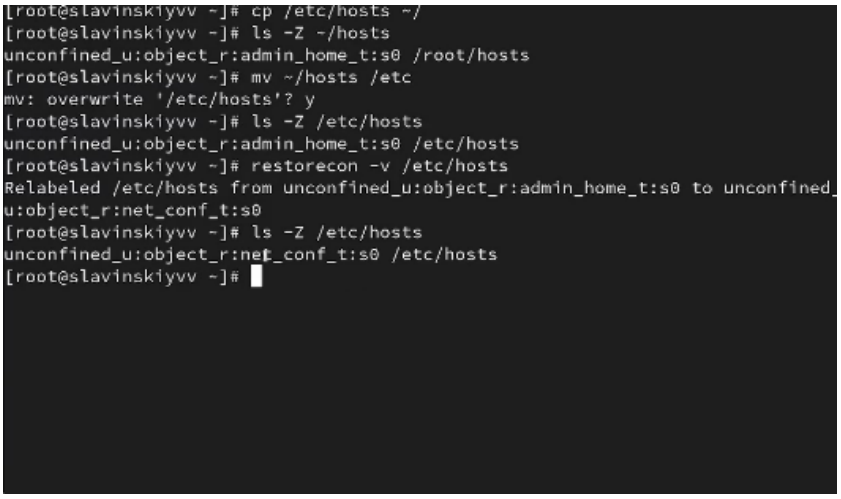

Рис. 2.13: Исправление конекста безопасности

Для массового исправления контекста безопасности на файловой системе введем touch /.autorelabel и перезагрузим систему. Во время перезапуска нажмем клавишу esc чтобы мы увидели загрузочные сообщения.(рис. 2.14)

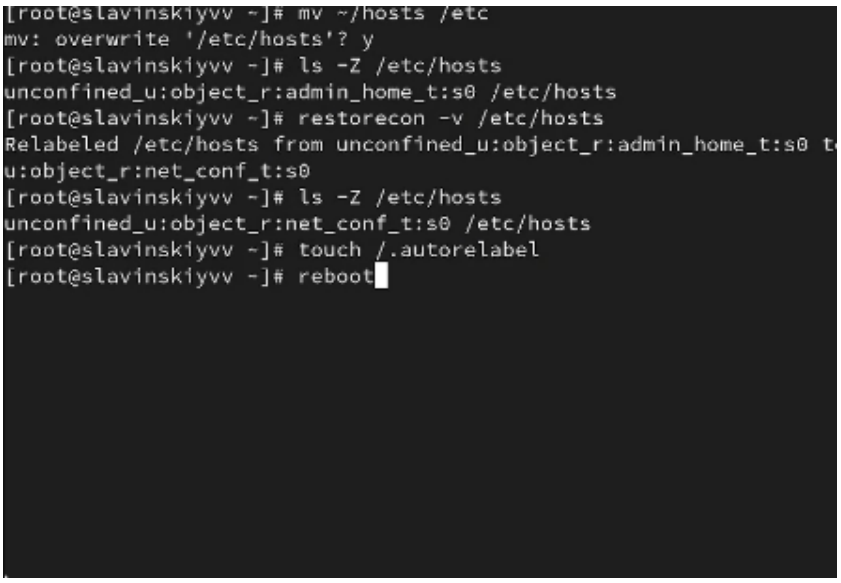

Рис. 2.14: Массовое исправление контекста безопасности

Вот какие сообщения выводятся при перезагрузке.(рис. 2.15)

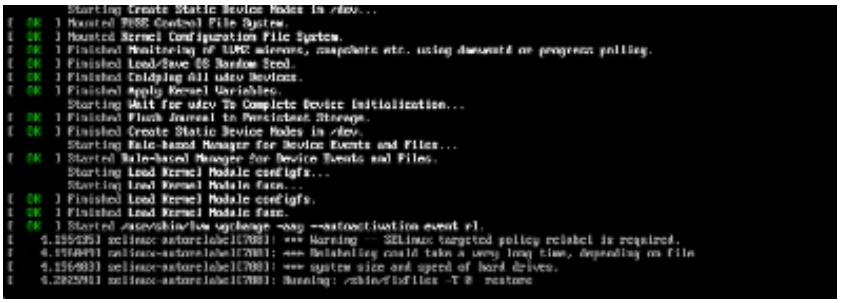

Рис. 2.15: Перемаркированные сообщения на перезагрузке

Запустим терминал в режиме администратора. Затем установим необходимое программное обеспечение: dnf -y install httpd, dnf -y install lynx.(рис. 2.16)

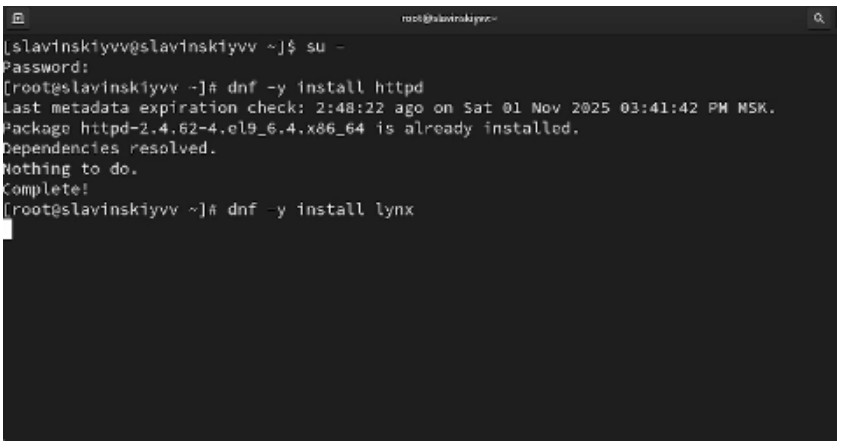

Рис. 2.16: Установка ПО

Создадим новое хранилище для файлов web-сервера: mkdir /web. Создадим файл index.html в каталоге с контентом веб-сервера: cd /web, touch index.html.(рис. 2.17)

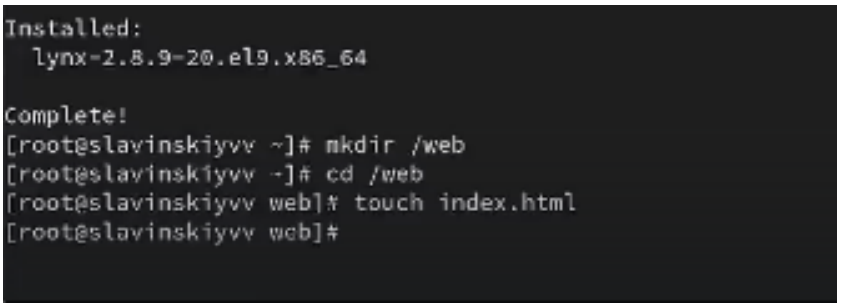

Рис. 2.17: Создание нового хранилища для файлов web-сервера

Поместим в этот файл следующий текст: Welcome to my web-server.(рис. 2.18)

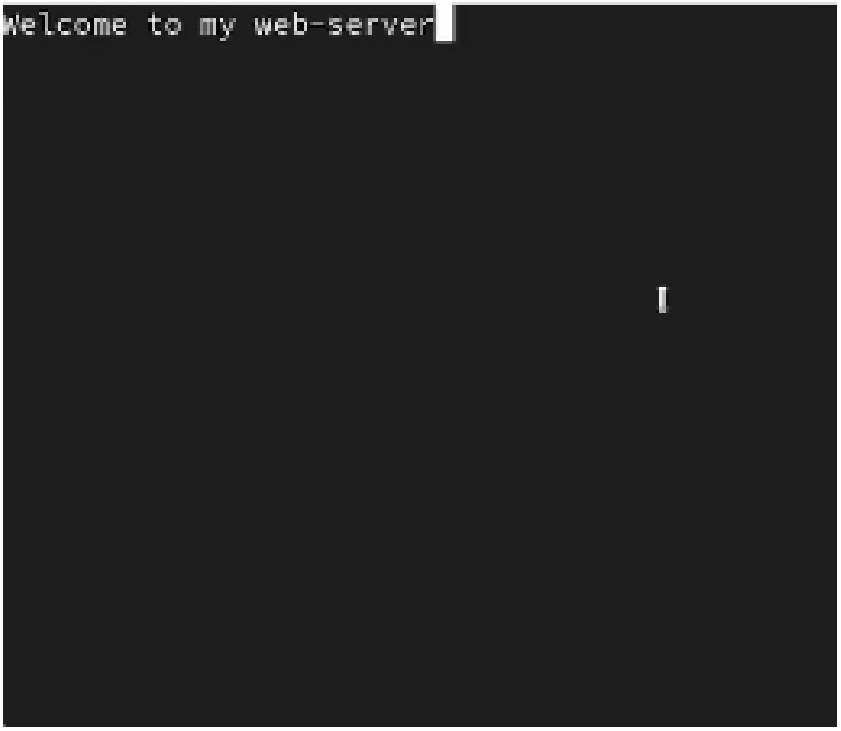

Рис. 2.18: Вставка текста

В файле /etc/httpd/conf/httpd.conf закомментируем строку DocumentRoot “/var/www/html” и ниже добавим строку DocumentRoot “/web”.(рис. 2.19)

Рис. 2.19: Редактирование файла httpd.conf

Затем в этом же файле ниже закомментируем раздел <Directory “/var/www”> AllowOverride None Require all granted и добавим следующий раздел, определяющий правила доступа: <Directory “/web”> AllowOverride None Require all granted .(рис. 2.20)

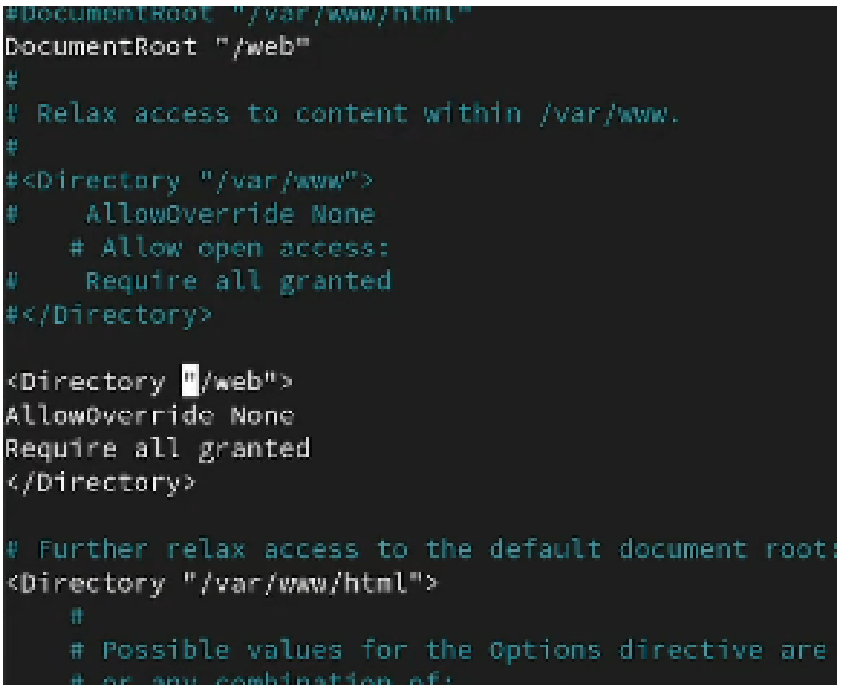

Рис. 2.20: Редактирование файла httpd.conf

Запустим веб-сервер и службу httpd: systemctl start httpd, systemctl enable httpd.(рис. 2.21)

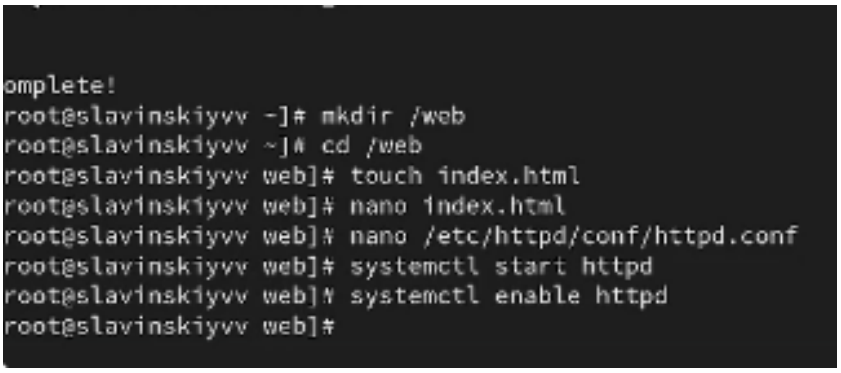

Рис. 2.21: Запуск веб-сервера и службы

В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx введем: lynx http://localhost. Мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.(рис. 2.22)

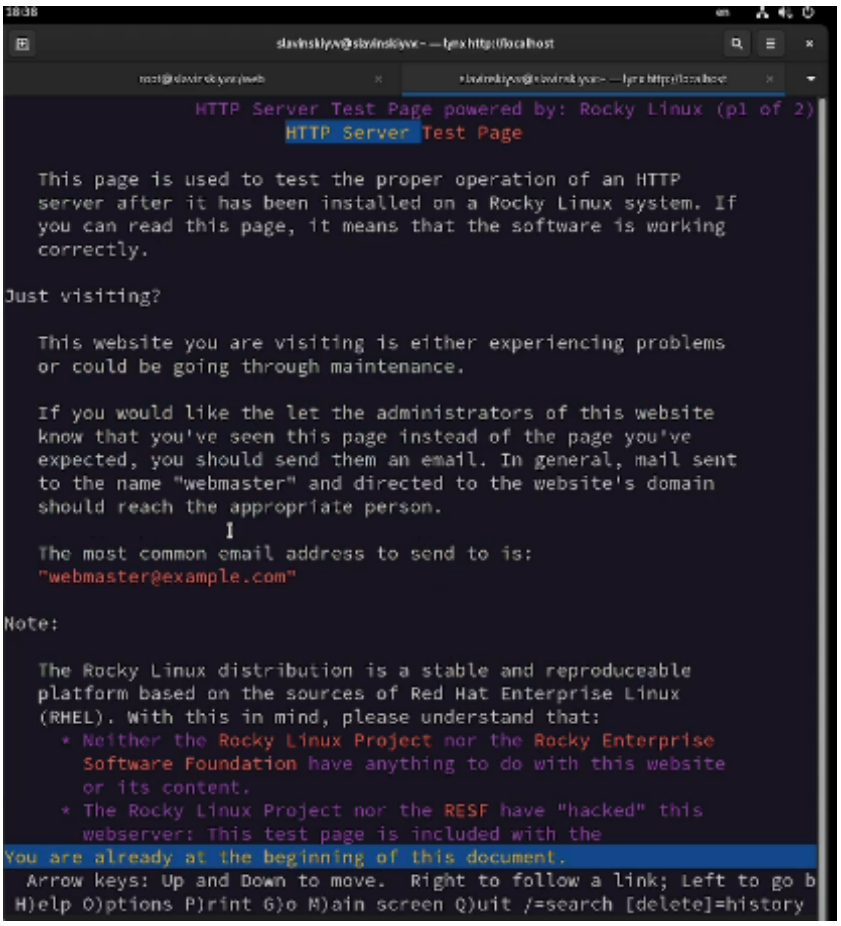

Рис. 2.22: Запуск

В терминале с полномочиями администратора применим новую метку контекста к /web: semanage fcontext -a -t httpd_sys_content_t “/web(/.*)?“.(рис. 2.23)

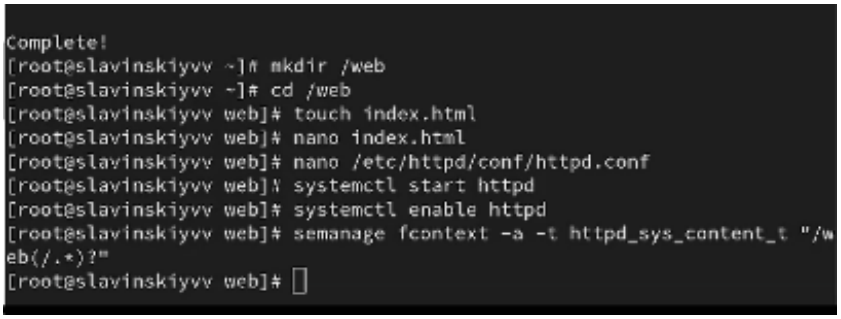

Рис. 2.23: Применение новой метки контекста

Восстановим контекст безопасности: restorecon -R -v /web.(рис. 2.24)

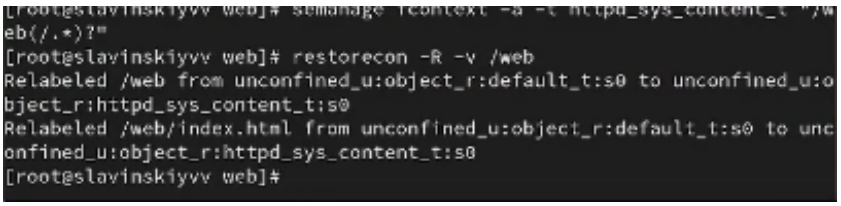

Рис. 2.24: Восстановление контекста безопасности

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу: lynx http://localhost. У нас ничего не произошло. Значит перезапускаем систему и опять обращаемся к веб-серверу. Как видим, у нас все получилось.(рис. 2.25)

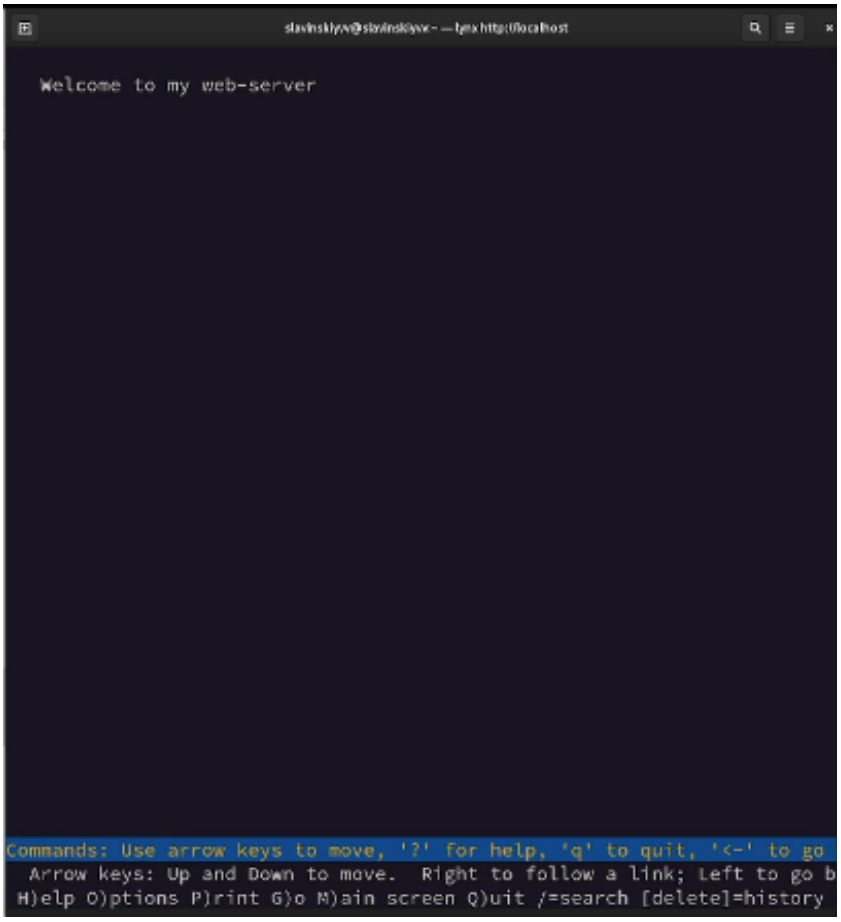

Рис. 2.25: Проверка веб-сервера

Через полномочия администратора посмотрим список переключателей SELinux для службы ftp: getsebool -a | grep ftp(рис. 2.26)

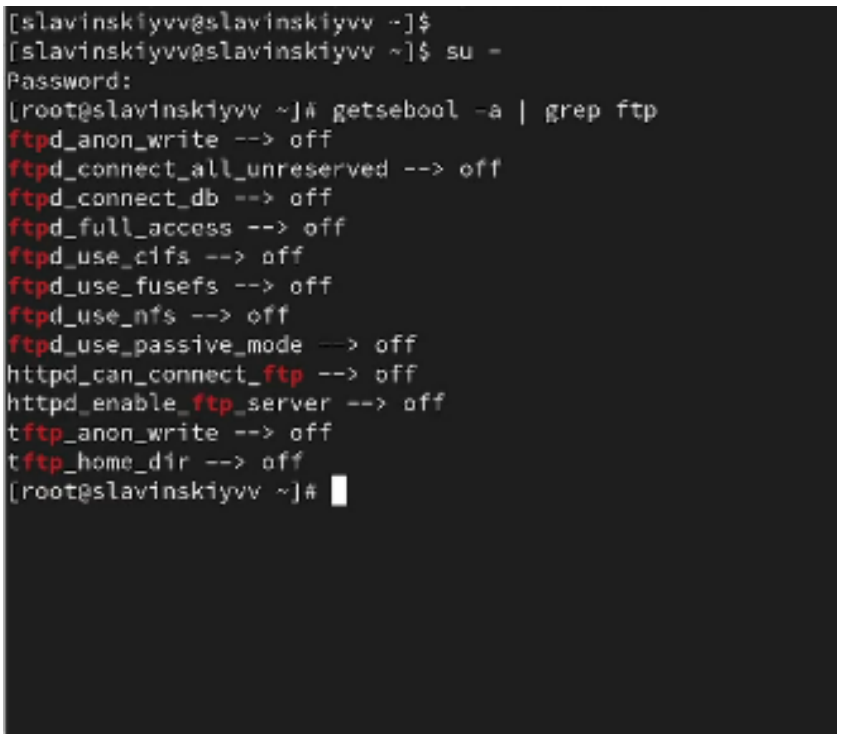

Рис. 2.26: Список переключателей SELinux

Для службы ftpd_anon посмотрим список переключателей: semanage boolean -l | grep ftpd_anon. Первое значение off - текущее состояние выполнение времени, второе значение off - постоянное состояние. Ftpd_anon_write разрешает или запрещает анонимным пользователям FTP выполнять операции записи.(рис. 2.27)

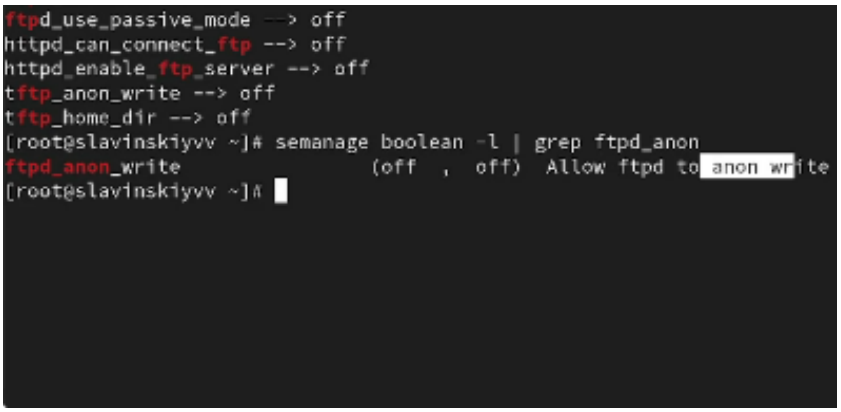

Рис. 2.27: Список переключателей

Изменим текущее значение переключателя для службы ftpd_anon_write с off на on: setsebool ftpd_anon_write on. Повторно посмотрим список переключателей SELinux для службы ftpd_anon_write: getsebool ftpd_anon_write.(рис. 2.28)

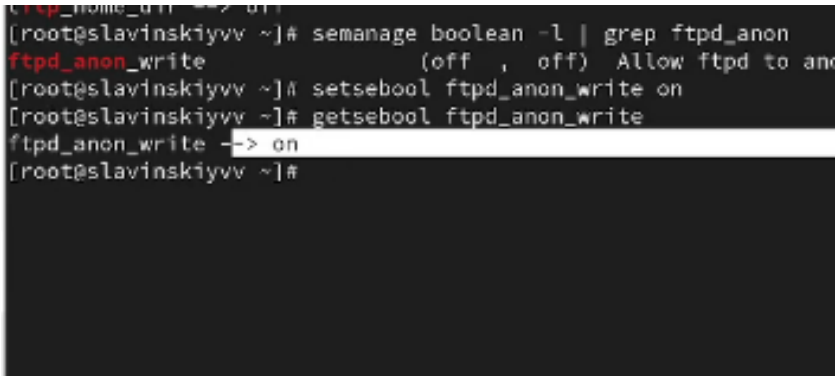

Рис. 2.28: Изменения значения переключателя

Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon. Видим, что настройка времени выполнения включена, но постоянная настройка выключена(рис. 2.29)

Рис. 2.29: Просмотр списка переключателей

Изменим постоянное значение переключателя для службы ftpd_anon_write с off на on: setsebool -P ftpd_anon_write on. Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon. Теперь у нас fttpd_anon_write полностью включен. Оба значения установлены на on: 1) включены состояние во время выполнения и постоянное состояние после перезагрузки. Теперь анонимные пользователи FTP могут выполнять операции записи на сервер. (рис. 2.30)

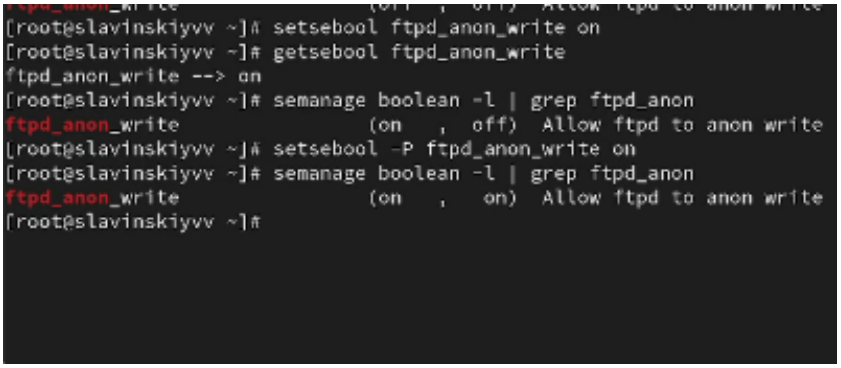

Рис. 2.30: Изменение постоянного значения переключателя

3 Выводы

В ходе выполнения лабораторной работы были получены навыки работы с контекстом безопасности и политиками SELinux.

4 Ответы на контрольные вопросы

1. setenforce 0
2. getsebool - a
3. setroubleshoot
4. semenage fcontext -a -t , restorecon -R -v
5. /etc/sysconfig/selinux
6. /var/lor/messages
7. seinfo -t | grep ftp
8. setenforce 0, если в режиме permissive проблема исчезает, то она связана с политиками SELinux. Если проблема остается, то причина в другой конфигурации