Отчет по лабораторной работе №9

Управление SELinux

Сидорова Арина Валерьевна

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Выполнение лабораторной работы

## 2.1 Управление режимами SELinux

Просмотрим текущую информацию о состоянии SELinux: sestatus -v

Посмотрим, в каком режиме работает SELinux: getenforce

Изменим режим работы SELinux на разрешающий setenforce 0 и снова введем getenforce (рис. 1)

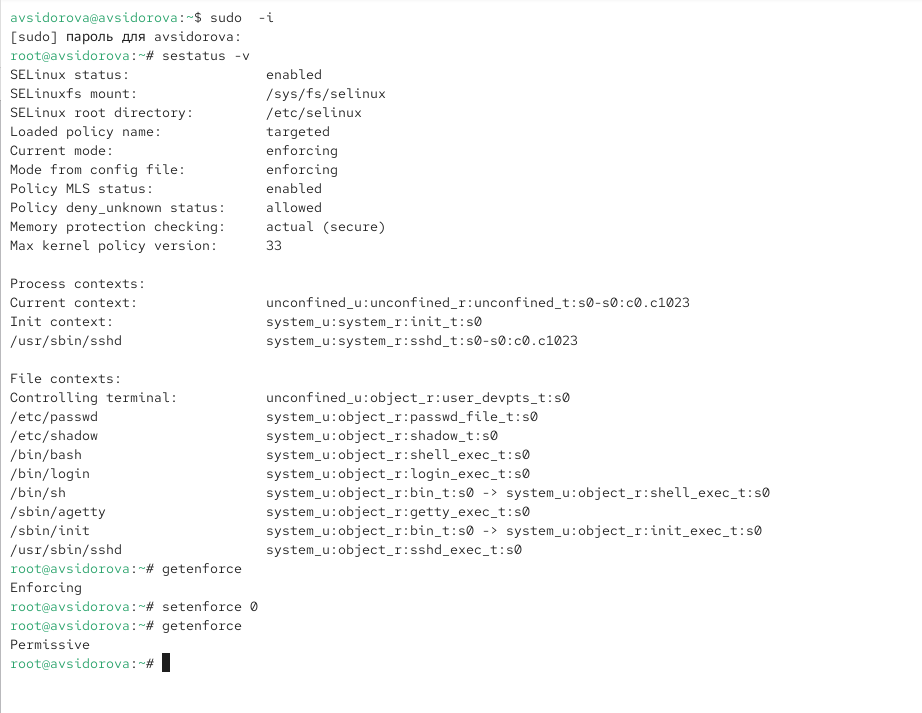


Рис. 1: getenforce

В файле /etc/sysconfig/selinux с помощью редактора установим SELINUX=disabled Перезагрузим систему (рис. 2)

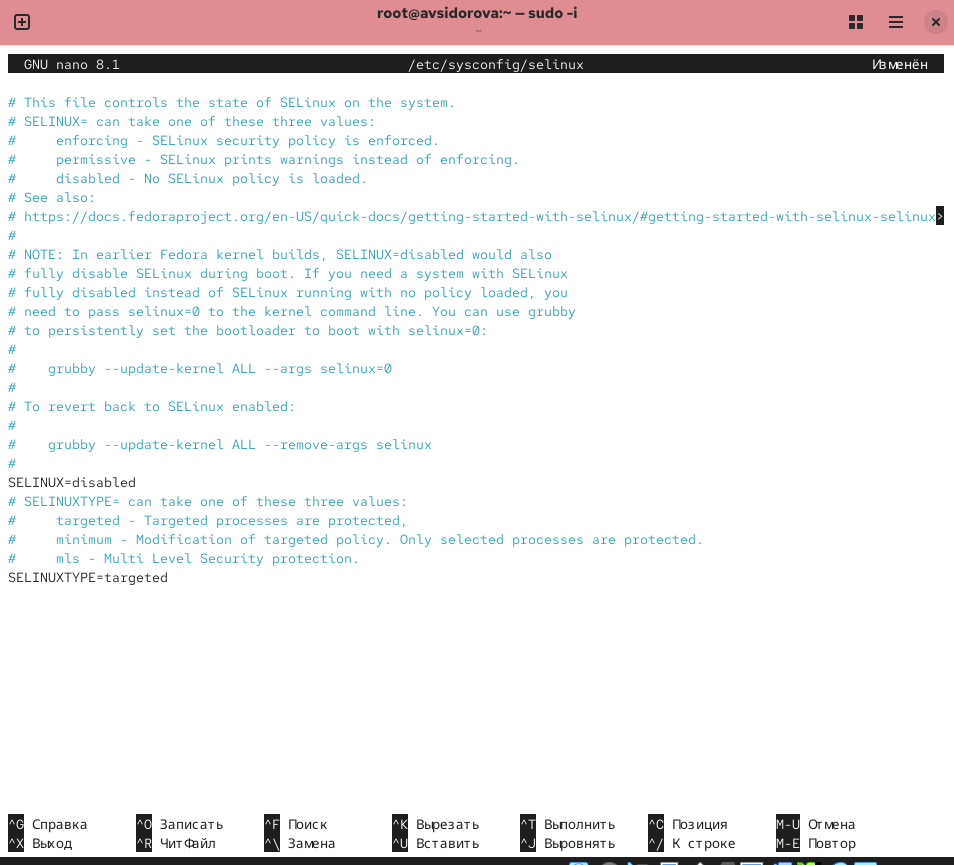


Рис. 2: SELINUX=disabled

Посмотрим статус SELinux: getenforce SELinux теперь отключён.

Попробуем переключить режим работы SELinux: setenforce 1 Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы. (рис. 3)

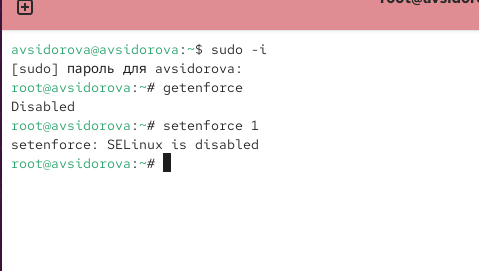


Рис. 3: SELinux теперь отключён

Откроем файл /etc/sysconfig/selinux с помощью редактора и установим: SELINUX=enforcing Перезагрузим систему. (рис. 4)

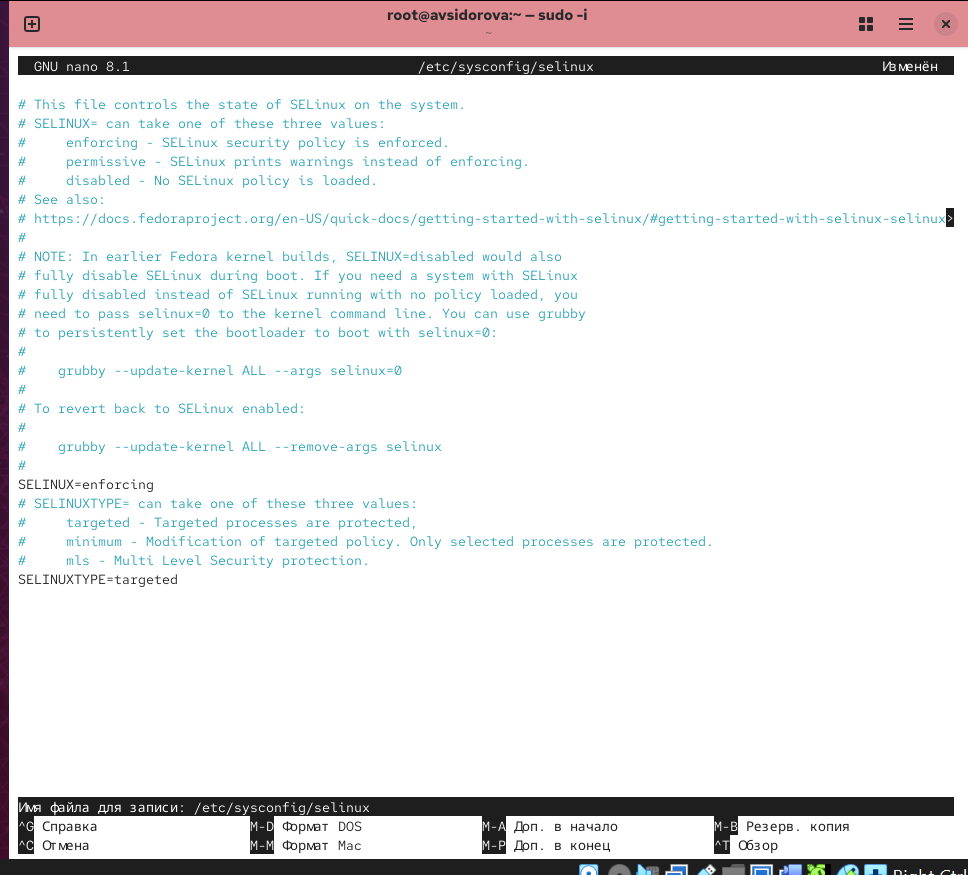


Рис. 4: SELINUX=enforcing

После перезагрузки в терминале с полномочиями администратора просмотрим текущую информацию о состоянии SELinux: sestatus -v (рис. 5)

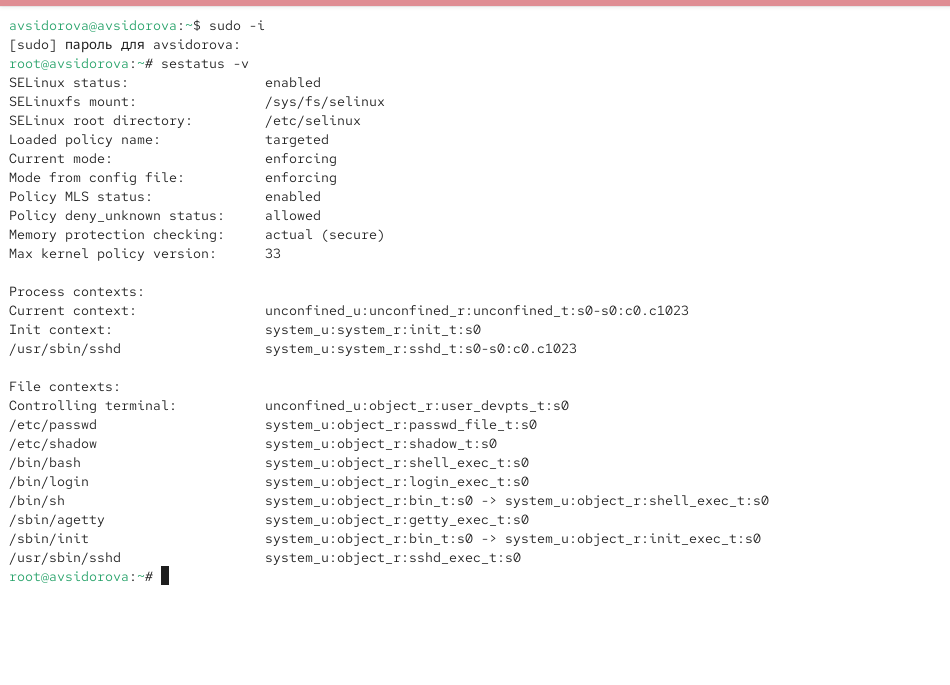


Рис. 5: sestatus -v

## 2.2 Использование restorecon для восстановления контекста безопасности

Посмотрим контекст безопасности файла /etc/hosts. У файла есть метка контекста net\_conf\_t.

Скопируем файл /etc/hosts в домашний каталог. Проверим контекст файла ~/hosts.

Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin\_home\_t.

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: mv ~/hosts /etc Убедимся, что тип контекста по-прежнему установлен на admin\_home\_t.

Исправим контекст безопасности.

Убедимся, что тип контекста изменился: ls -Z /etc/hosts

Для массового исправления контекста безопасности на файловой системе введем touch /.autorelabel (рис. 6)

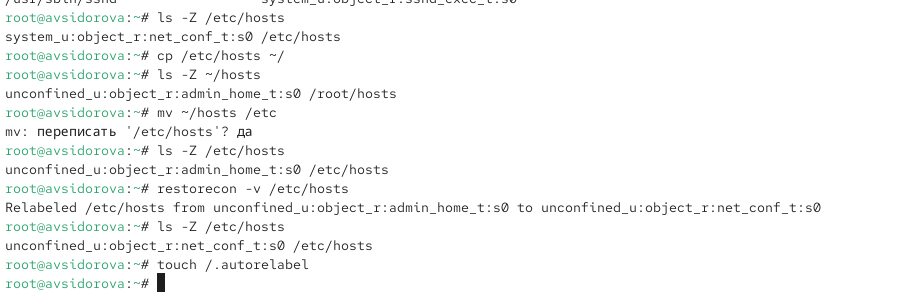


Рис. 6: Использование restorecon для восстановления контекста безопасности

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

Установим необходимое программное обеспечение (рис. 7)

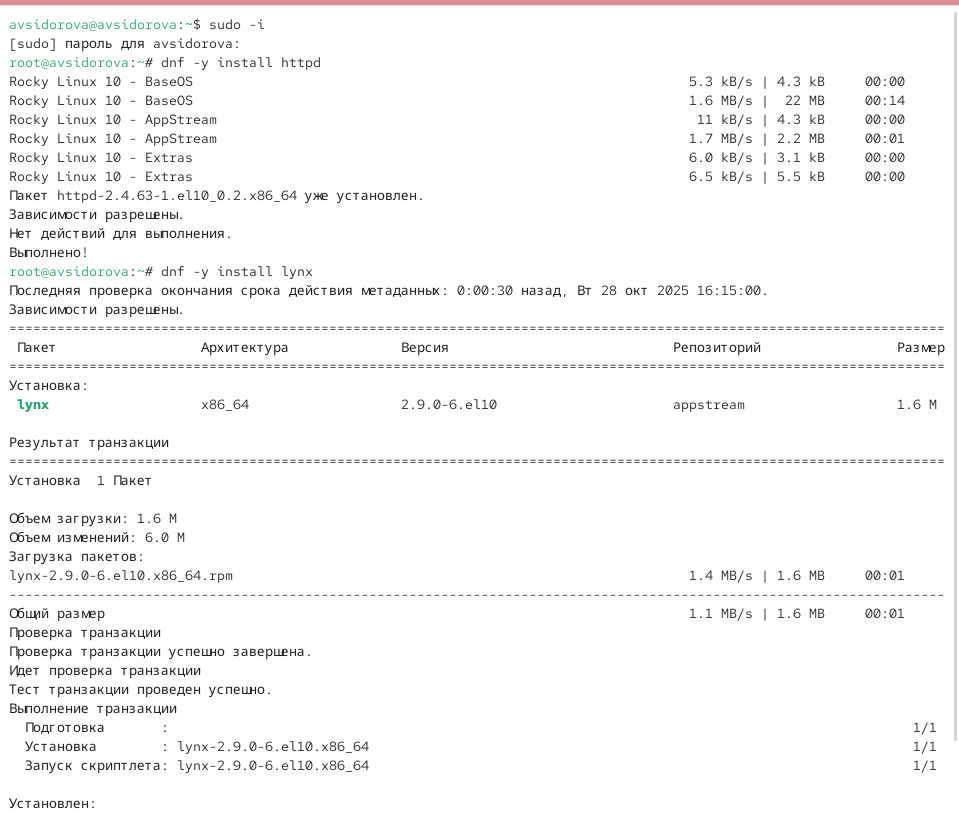


Рис. 7: Установим необходимое программное обеспечение

Создадим новое хранилище для файлов web-сервера

Создадим файл index.html в каталоге с контентом веб-сервера и поместим в файл следующий текст: Welcome to my web-server (рис. 8)



Рис. 8: mkdir /web; touch index.html

В файле /etc/httpd/conf/httpd.conf закомментируем строку DocumentRoot “/var/www/html” и ниже добавим строку DocumentRoot “/web” Затем в этом же файле ниже закомментирем раздел <Directory “/var/www”> AllowOverride None Require all granted и добавим следующий раздел, определяющий правила доступа: <Directory “/web”> AllowOverride None Require all granted (рис. 9)

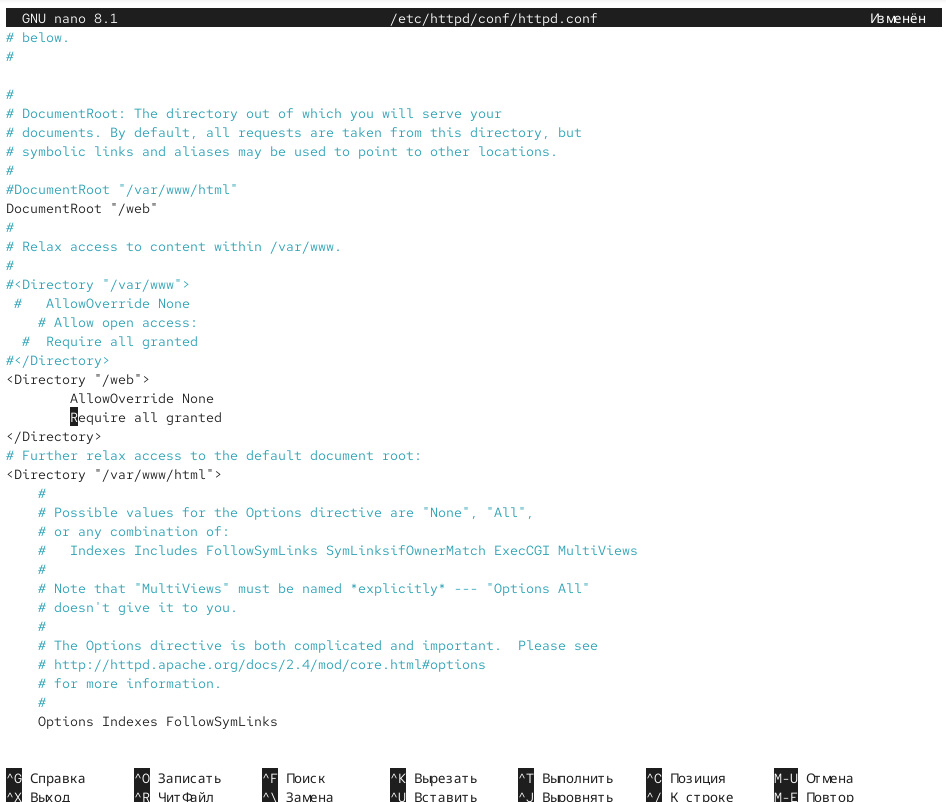


Рис. 9: Редактируем файл

Запустим веб-сервер и службу httpd: systemctl start httpd systemctl enable httpd (рис. 10)



Рис. 10: start; enable

В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: lynx http://localhost

Мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html. (рис. 11)

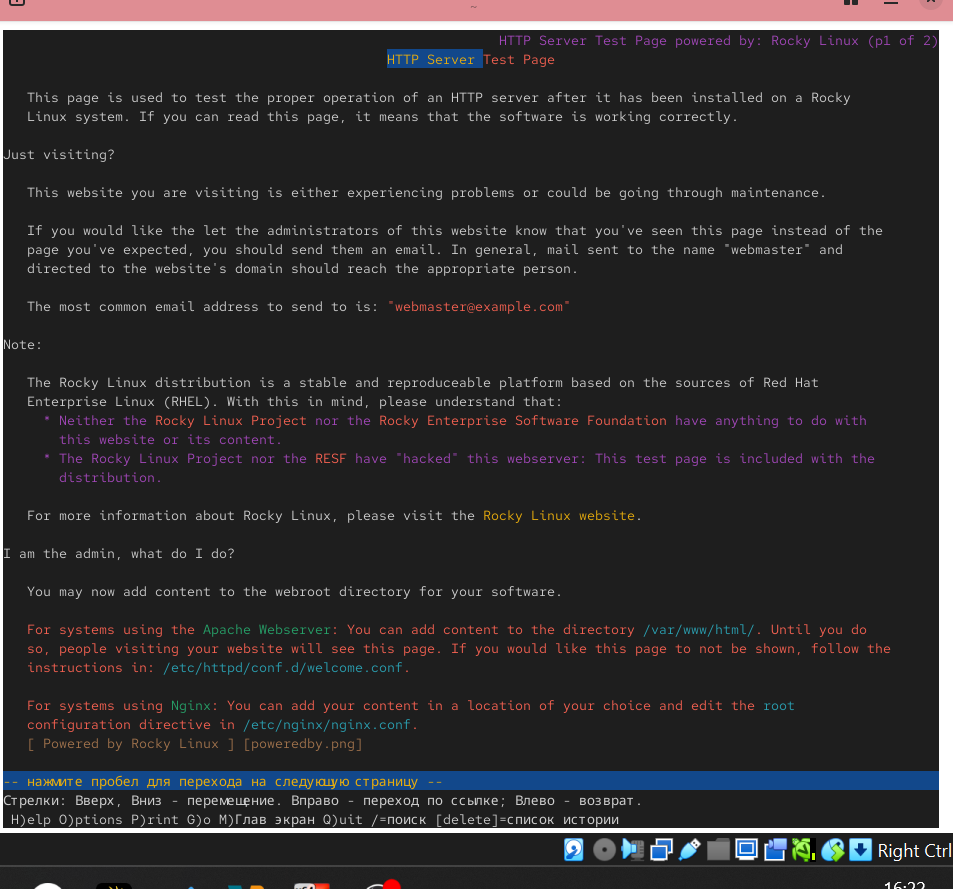


Рис. 11: веб-страница Red Hat

В терминале с полномочиями администратора применим новую метку контекста к /web: semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?”

Восстановим контекст безопасности: restorecon -R -v /web (рис. 12)

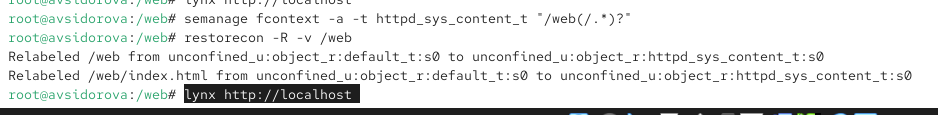


Рис. 12: Применим новую метку и восстановим контекст безопасности

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу: lynx http://localhost На экране отображена запись «Welcome to my web-server». (рис. 13)

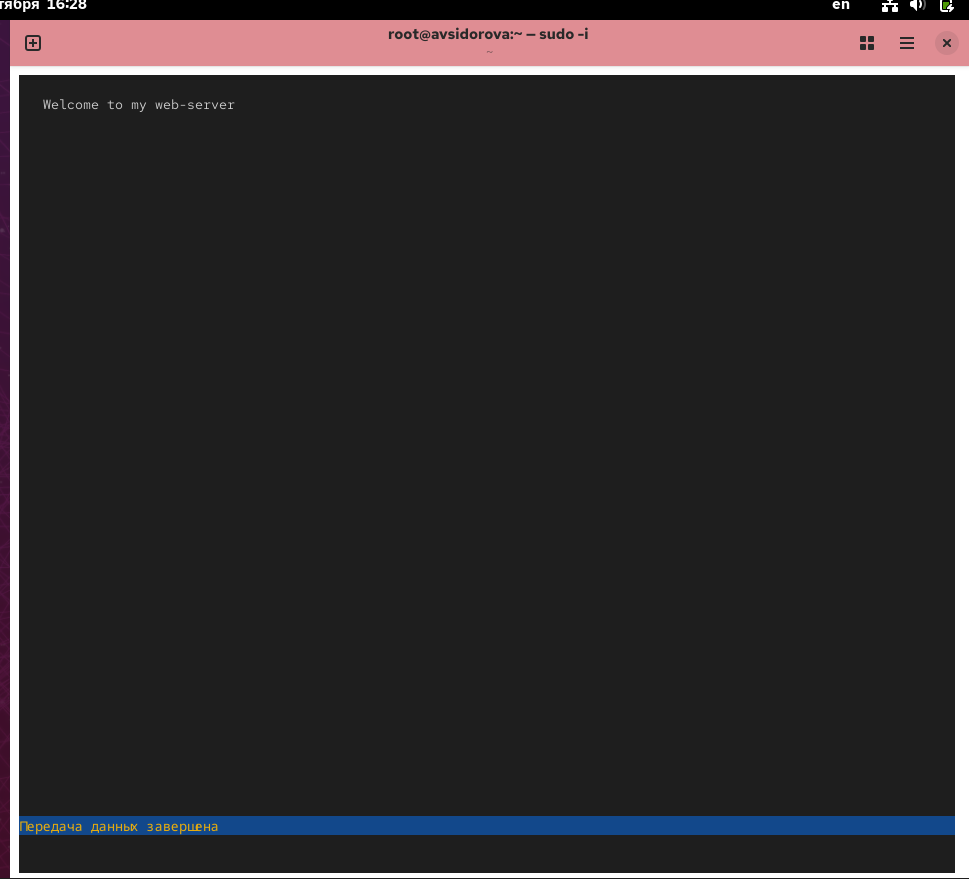


Рис. 13: Welcome to my web-server

## 2.4 Работа с переключателями SELinux

Посмотрим список переключателей SELinux для службы ftp.

Для службы ftpd\_anon посмотрим список переключателей: semanage boolean -l | grep ftpd\_anon

Изменим текущее значение переключателя для службы ftpd\_anon\_write с off на on: setsebool ftpd\_anon\_write on

Повторно посмотрм список переключателей SELinux для службы ftpd\_anon\_write: getsebool ftpd\_anon\_write

Посмотрим список переключателей: semanage boolean -l | grep ftpd\_anon Обратим внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

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 (рис. 14)

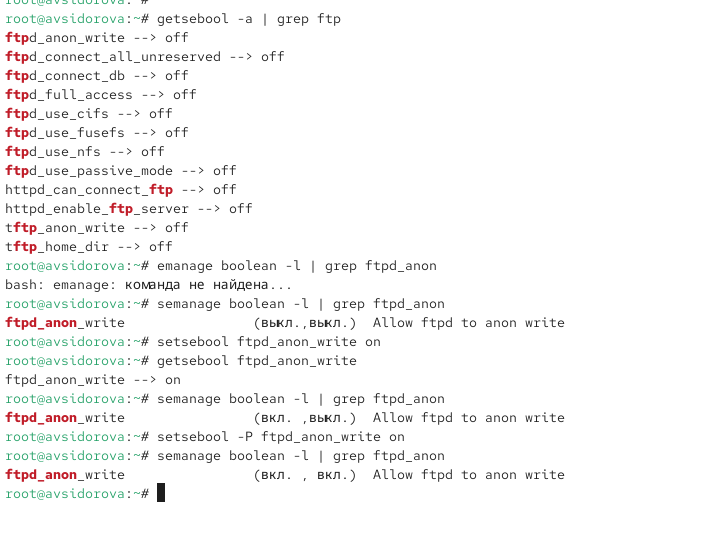


Рис. 14: Работа с переключателями SELinux

# 3 Ответы на контрольные вопросы

1. setenforce 0
2. getsebool -a
3. setroubleshoot или setroubleshoot-server
4. semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?” затем restorecon -R /web
5. /etc/selinux/config (параметр SELINUX=disabled)
6. /var/log/audit/audit.log и /var/log/messages
7. semanage boolean -l | grep ftp или getsebool -a | grep ftp
8. Временно перевести SELinux в режим Permissive (setenforce 0) и проверить работу службы

# 4 Выводы

Получили навыки работы с контекстом безопасности и политиками SELinux.