**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №9**

*дисциплина: Основы администрирования операционных систем*

Студент: Ко Антон Геннадьевич Студ. билет № 1132221551 Группа: НПИбд-02-23

**МОСКВА**

2024 г.

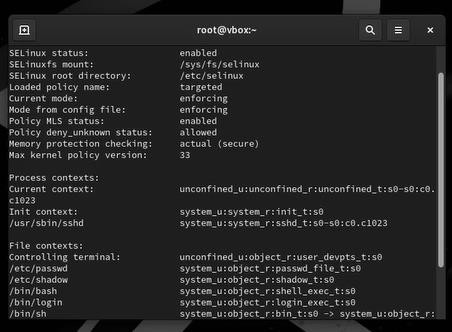
# Цель работы:

Целью данной работы является получение навыков работы с контекстом безопасности и политиками SELinux.

**Выполнение работы:**

**Управление режимами SELinux:**

Запустим терминал и получим полномочия администратора: **su -**. Затем просмотрим текущую информацию о состоянии SELinux: **sestatus -v**:



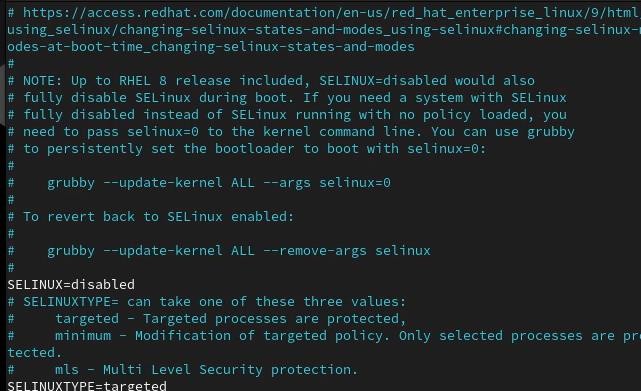
**Рис.1.** Запуск терминала и получение полномочий администратора, просмотр текущей информации о состоянии SELinux.

Посмотрим, в каком режиме работает SELinux: **getenforce**. По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing). Изменим режим работы SELinux на разрешающий (Permissive): **setenforce 0** и

снова введём **getenforce**. Откроем файл /etc/sysconfig/selinux с помощью текстового редактора mcedit:

**Рис. 2.** Просмотр режима работы SELinux, изменение режима работы и проверка, открытие файла в текстовом редакторе.

В открытом в редакторе файле /etc/sysconfig/selinux установим SELINUX=disabled. После чего сохраним изменения:

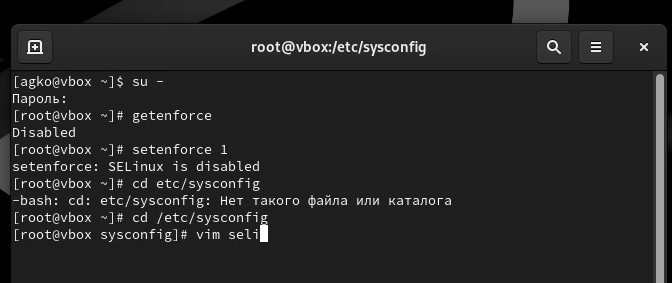


**Рис.3.** Установка в файле SELINUX=disabled, сохранение изменений.

Выполним перезагрузку системы:

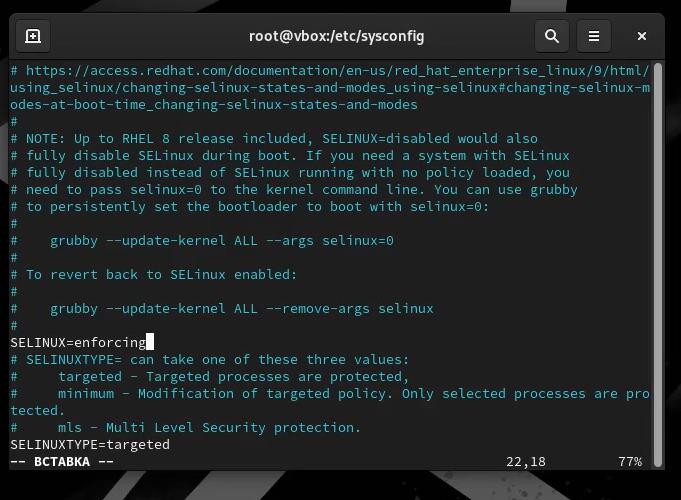


**Рис.4.** Перезагрузка системы.

После перезагрузки запустим терминал и получим полномочия администратора. Далее посмотрим статус SELinux: **getenforce**. Мы видим, что SELinux теперь отключён. Попробуем переключить режим работы SELinux: **setenforce 1**. Система пишет, что SELinux отключён, так как мы не можете переключаться между отключённым и принудительным режимом без перезагрузки системы. Откроем файл /etc/sysconfig/selinux с помощью текстового редактора mcedit:

**Рис. 5.** Запуск терминала и получение полномочий администратора, просмотр статуса SELinux, попытка переключения режима работы, открытие файла в текстовом редакторе.

В открытом в редакторе файле /etc/sysconfig/selinux установим SELINUX=enforcing. После чего сохраним изменения:



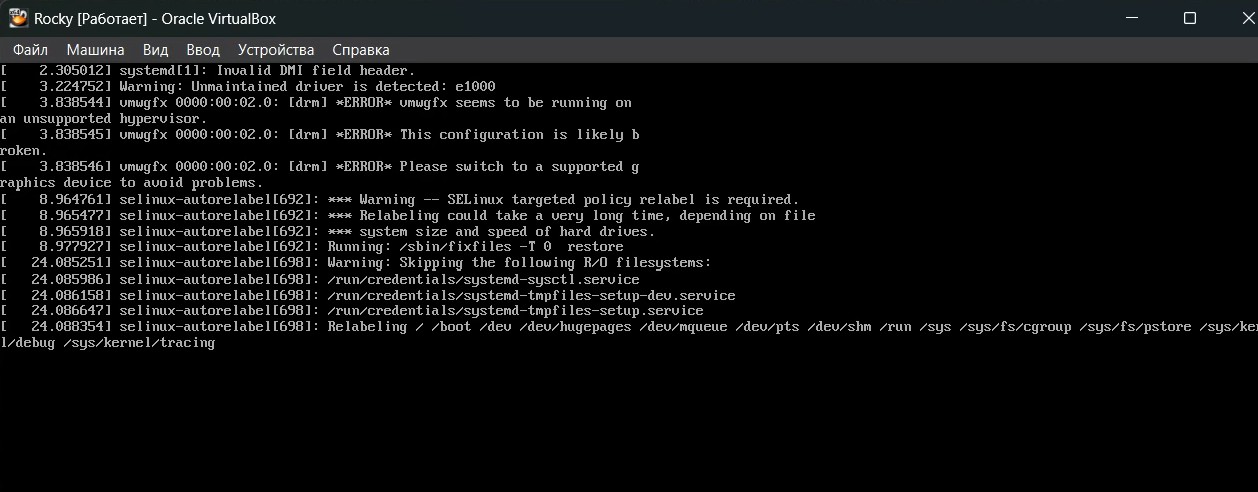
**Рис. 6.** Установка в файле SELINUX=enforcing, сохранение изменений.

Выполним перезагрузку системы:



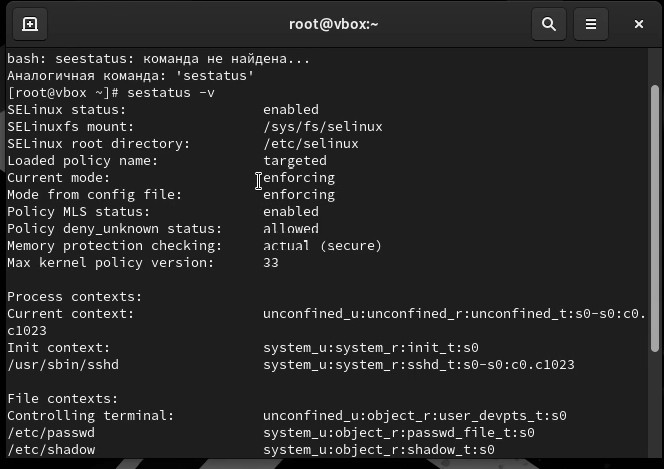
**Рис. 7.** Перезагрузка системы.

Во время загрузки системы мы получили предупреждающее сообщение о необходимости восстановления меток SELinux:



**Рис. 8.** Получение предупреждающего сообщения при перезагрузке системы.

После перезагрузки в терминале с полномочиями администратора просмотрим текущую информацию о состоянии SELinux: **sestatus -v.** Убедимся, что система работает в принудительном режиме (enforcing) использования SELinux:



**Рис. 9.** Запуск терминала и получение полномочий администратора, просмотр текущей информации о состоянии SELinux.

# Использование restorecon для восстановления контекста безопасности:

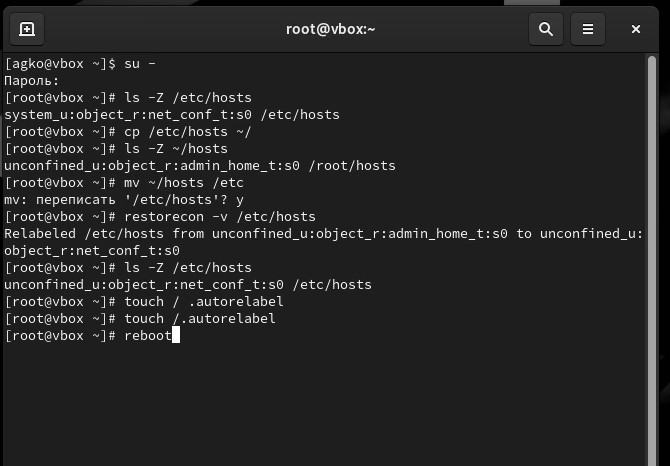
Запустим терминал и получим полномочия администратора. Просмотрим контекст безопасности файла /etc/hosts: **ls -Z /etc/hosts**. Мы видим, что у файла есть метка контекста *net\_conf\_t*. Скопируем файл /etc/hosts в домашний каталог: **cp /etc/hosts ~/**. Затем проверим контекст файла ~/hosts: **ls -Z ~/hosts**. Поскольку

копирование считается созданием нового файла, то параметр контекста в файле

~/hosts, расположенном в домашнем каталоге, стал *admin\_home\_t*. Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: **mv**

**~/hosts /etc** и подтвердим, что мы хотим сделать это. После чего нам нужно убедиться, что тип контекста по-прежнему установлен на *admin\_home\_t*: **ls -Z**

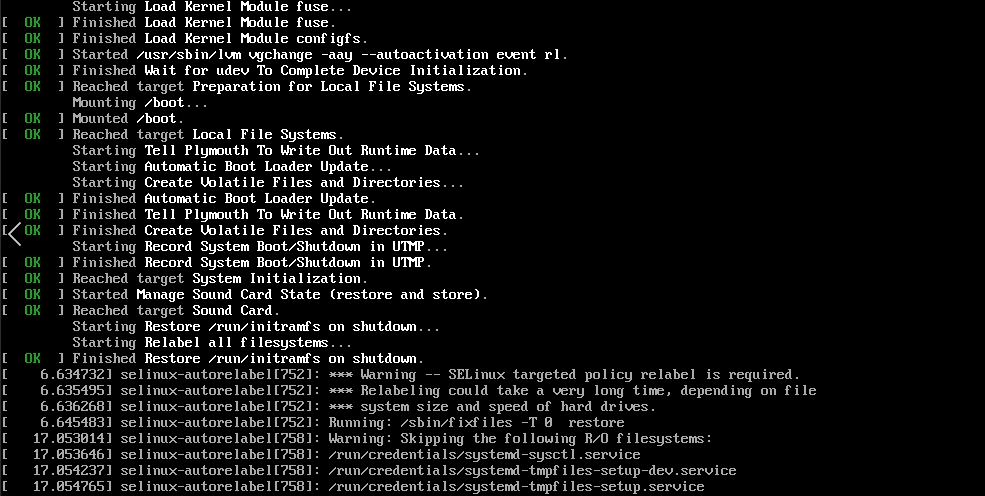
**/etc/hosts**. Исправим контекст безопасности: **restorecon -v /etc/hosts**. Опция -v покажет процесс изменения. Убедимся, что тип контекста изменился: **ls -Z**

**/etc/hosts**. Для массового исправления контекста безопасности на файловой системе введём **touch /.autorelabel** и перезагрузим систему.

**Рис. 10.** Запуск терминала и получение полномочий администратора, просмотр контекста безопасности файла, копирование файла в домашний каталог, проверка контекст файла, попытка перезаписи файла и подтверждение, проверка типа контекста, исправление контекста безопасности, проверка изменения типа контекста, добавление массового исправления контекста

безопасности на файловой системе. Перезагрузка системы.

Во время перезапуска не забываем нажать клавишу Esc на клавиатуре, чтобы мы видели загрузочные сообщения. Мы видим, что файловая система автоматически перемаркирована.

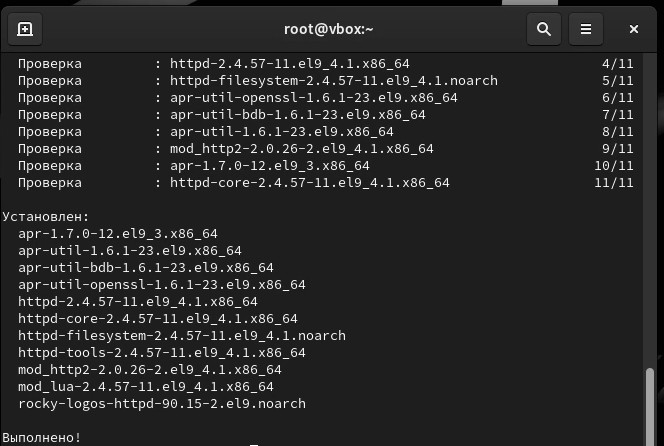


**Рис. 11.** Просмотр загрузочных сообщений после нажатия клавиши “Esc”.

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

Запустим терминал и получим полномочия администратора. После чего установим необходимое программное обеспечение:

# dnf -y install httpd dnf -y install lynx

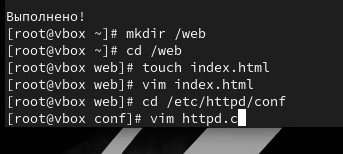


**Рис. 12.** Запуск терминала и получение полномочий администратора, установка необходимого программного обеспечения.

Создадим новое хранилище для файлов web-сервера: **mkdir /web**. Далее создаём файл index.html в каталоге с контентом веб-сервера:

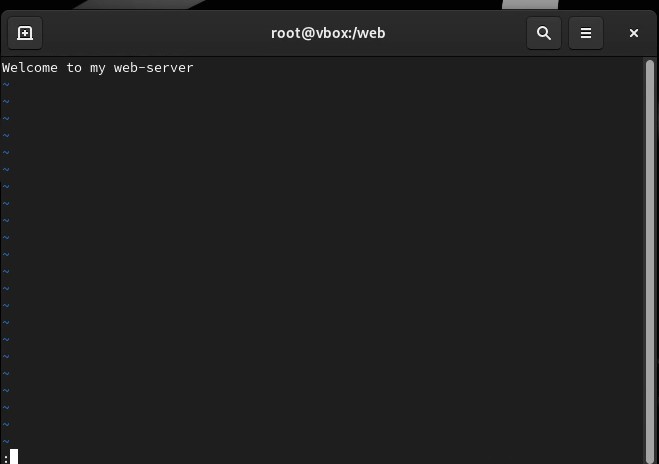
# cd /web

**touch index.html**

Файл открываем в текстовом редакторе mcedit для помещения в него текста.

**Рис. 13.** Создание нового хранилища (для файлов web-сервера) и файла в этом хранилище, открытие файла в текстовом редакторе.

Поместим в файл следующий текст: **Welcome to my web-server**.

**Рис. 14.** Добавление текста в файл.

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 закомментируем раздел:

*<Directory “/var/www”>*

*AllowOverride None Require all granted*

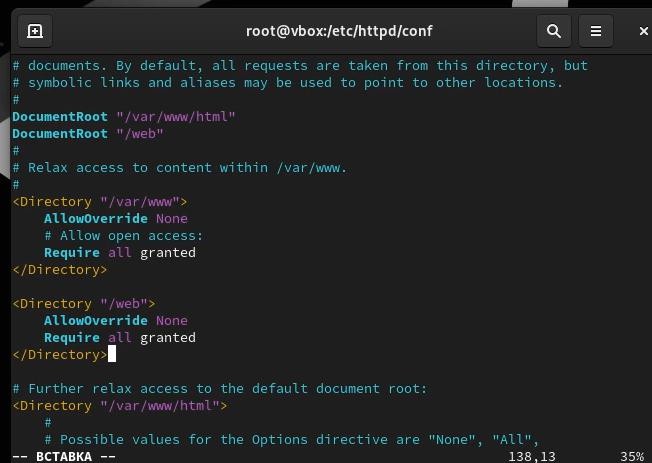
*</Directory>*

и добавим следующий раздел, определяющий правила доступа:

*<Directory “/web”>*

*AllowOverride None*

*Require all granted*

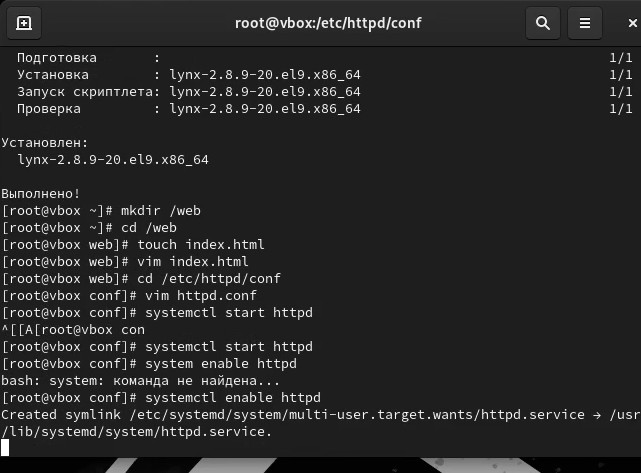
*</Directory>*

**Рис. 15.** Комментирование строки и добавление ниже другой.

Комментирование раздела и добавление следующего, определяющего правила доступа.

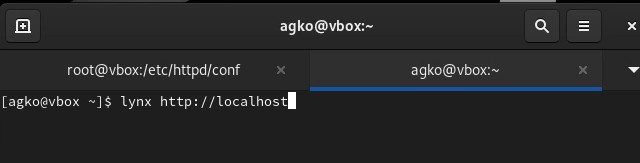
Запустим веб-сервер и службу httpd:

# systemctl start httpd systemctl enable httpd



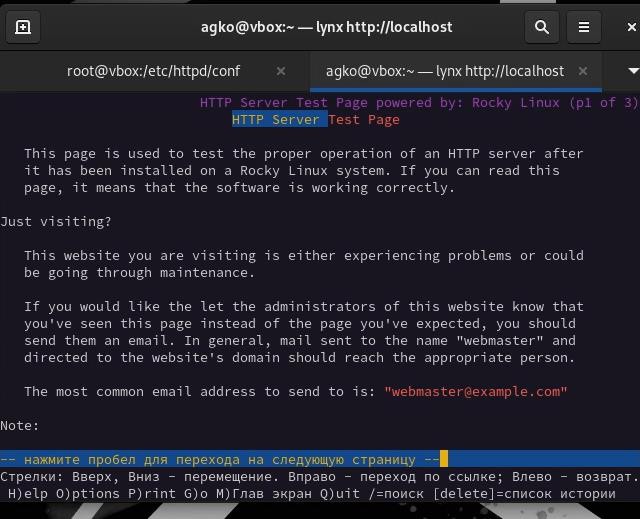
**Рис. 16.** Запуск веб-сервера и службы httpd.

В терминале под учётной записью своего пользователя обратимся к веб-серверу в текстовом браузере lynx: **lynx** [**http://localhost**.](http://localhost/)

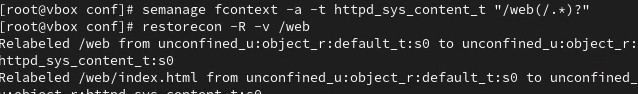


**Рис. 17.** Открытие терминала под учётной записью своего пользователя, обращение к веб-серверу в текстовом браузере lynx.

После открытия мы видим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html. Для выхода из lynx нажмём “**q**”.

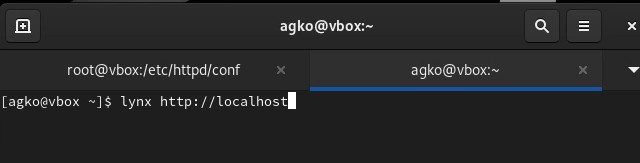


**Рис. 18.** Открытие веб-страницы Red Hat по умолчанию, выход из lynx.

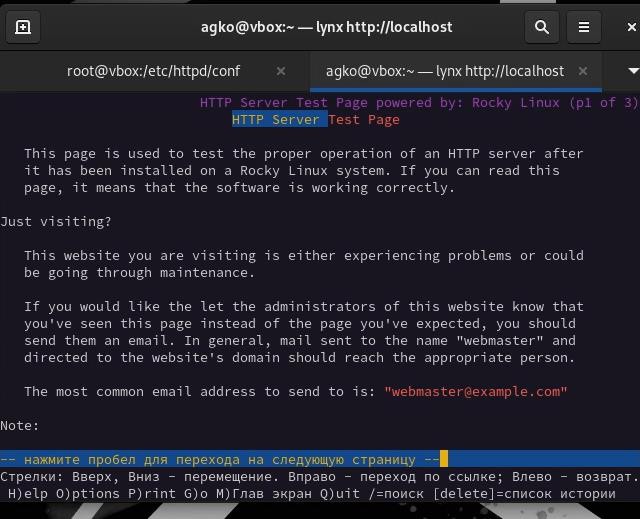
В терминале с полномочиями администратора применим новую метку контекста к /web: **semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?"** и восстановим контекст безопасности: **restorecon -R -v /web.** Теперь установим SELinux в режим принудительного исполнения: **setenforce 1**. После чего перезагрузим систему.

**Рис. 19.** Применение новой метки контекста к /web, восстановление контекста безопасности.

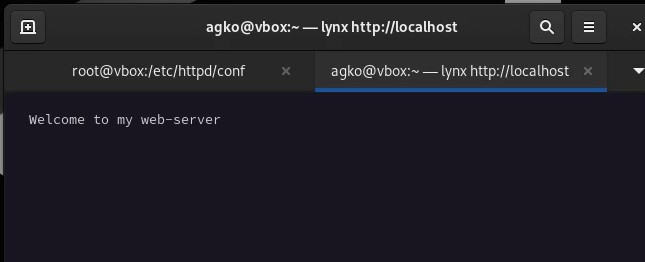
В терминале под учётной записью своего пользователя снова обратимся к веб-серверу: **lynx** [**http://localhost**.](http://localhost/) Т.к. получить доступ к серверу не получилось, нужно перезапустить систему



**Рис. 20.** Открытие терминала под учётной записью своего пользователя, повторное обращение к веб-серверу в текстовом браузере lynx.



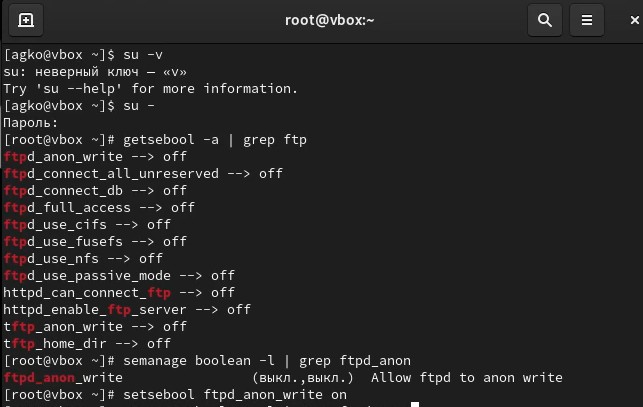
**Рис. 21.** Открытие веб-страницы Red Hat по умолчанию, выход из lynx.



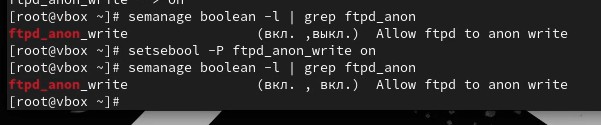
**Рис. 23.** Получение доступа к своей пользовательской веб-странице.

# Работа с переключателями SELinux:

Запустим терминал и получим полномочия администратора. Посмотрим список переключателей SELinux для службы ftp: **getsebool -a | grep ftp**. Мы видим переключатель *ftpd\_anon\_write* с текущим значением *off*. Для службы *ftpd\_anon* посмотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен: **semanage boolean -l | grep ftpd\_anon**. Теперь 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**. Посмотрим список переключателей с пояснением: **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\_writ*e с *off* на *on*: **setsebool -P ftpd\_anon\_write on** и посмотрим список переключателей: **semanage boolean -l | grep ftpd\_anon** (переключатель имеет состояние *on*).

**Рис. 24.** Запуск терминала и получение полномочий администратора, просмотр списка переключателей SELinux для службы ftp, просмотр списка переключателей с пояснением, изменение текущего значение переключателя

**для службы *ftpd\_anon\_write* с *off* на *on.*

**Рис. 25.** Повторный просмотр списка переключателей SELinux для службы *ftpd\_anon\_write,* просмотр списка переключателей с пояснением, изменение постоянного значение переключателя для службы *ftpd\_anon\_writ*e с *off* на *on* и

просмотр списка переключателей.

# Ответы на 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? getsebol -a
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? audit2allow
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 -v /web

1. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? /etc/sysconfig/selinux
2. Где SELinux регистрирует все свои сообщения? По умолчанию в

/var/log/audit/audit.log

1. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? getsebool -a | grep ftp
2. 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? Просмотреть контекст безопасности процессора ps -eZ или id -Z

# Вывод:

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