

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.

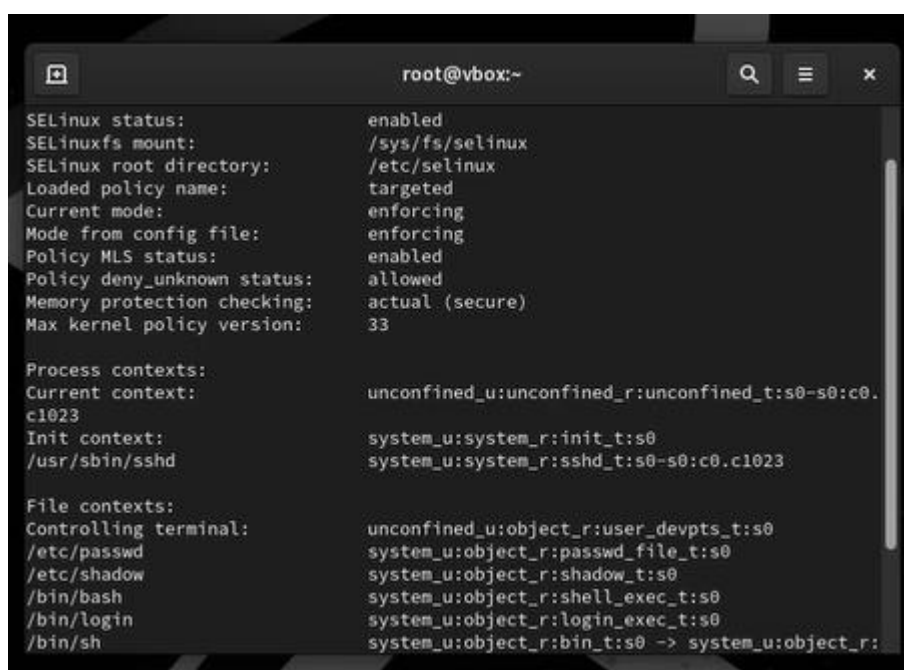
Цель работы:

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 посмотрим текущую информацию о состоянии SELinux: **sestatus -v**:



```
root@vbox:~  
SELinux status:                enabled  
SELinuxfs mount:              /sys/fs/selinux  
SELinux root directory:      /etc/selinux  
Loaded policy name:          targeted  
Current mode:                enforcing  
Mode from config file:       enforcing  
Policy MLS status:           enabled  
Policy deny_unknown status:   allowed  
Memory protection checking:   actual (secure)  
Max kernel policy version:    33  
  
Process contexts:  
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.  
c1023  
Init context:                 system_u:system_r:init_t:s0  
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023  
  
File contexts:  
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0  
/etc/passwd                   system_u:object_r:passwd_file_t:s0  
/etc/shadow                   system_u:object_r:shadow_t:s0  
/bin/bash                     system_u:object_r:shell_exec_t:s0  
/bin/login                    system_u:object_r:login_exec_t:s0  
/bin/sh                       system_u:object_r:bin_t:s0 -> system_u:object_r:
```

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`:

```
[root@vbox ~]# getenforce
Enforcing
[root@vbox ~]# setenforce 0
[root@vbox ~]# getenforce
Permissive
[root@vbox ~]# ls /etc/sysconfig/selinux
/etc/sysconfig/selinux
```

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:

```
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-selinux-states-and-modes_using_selinux#changing-selinux-states-at-boot-time_changing-selinux-states-and-modes
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

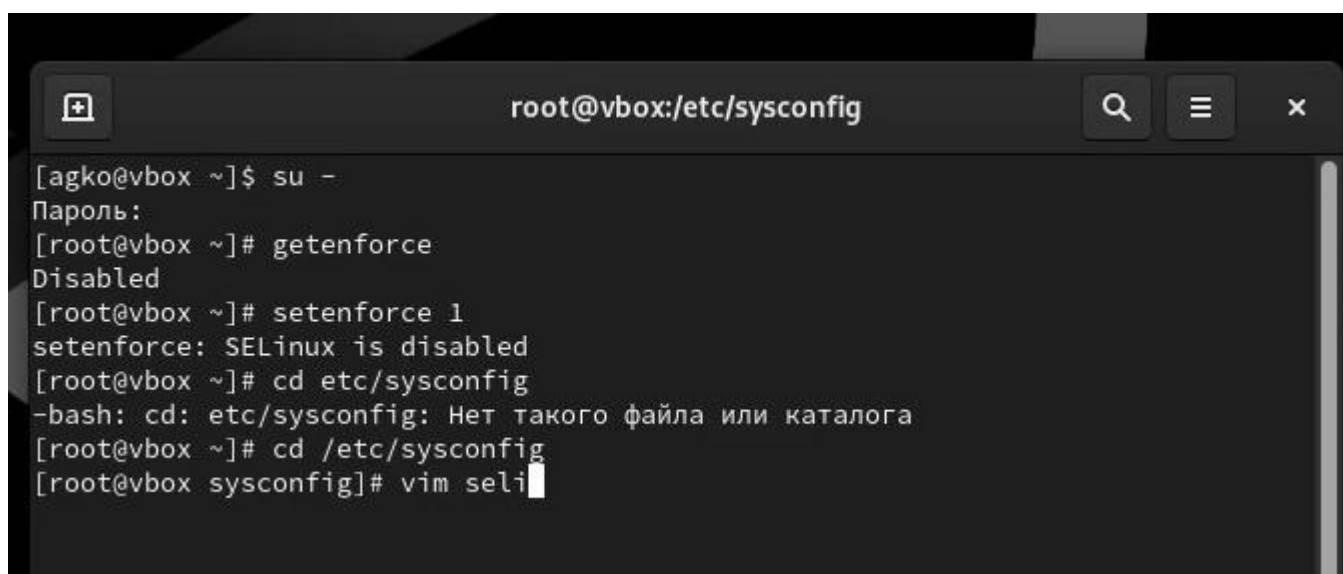
Рис.3. Установка в файле `SELINUX=disabled`, сохранение изменений.

Выполним перезагрузку системы:

```
[root@vbox ~]# reboot
```

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`:



```
root@vbox:/etc/sysconfig
[agko@vbox ~]$ su -
Пароль:
[root@vbox ~]# getenforce
Disabled
[root@vbox ~]# setenforce 1
setenforce: SELinux is disabled
[root@vbox ~]# cd etc/sysconfig
-bash: cd: etc/sysconfig: Нет такого файла или каталога
[root@vbox ~]# cd /etc/sysconfig
[root@vbox sysconfig]# vim seli
```

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:

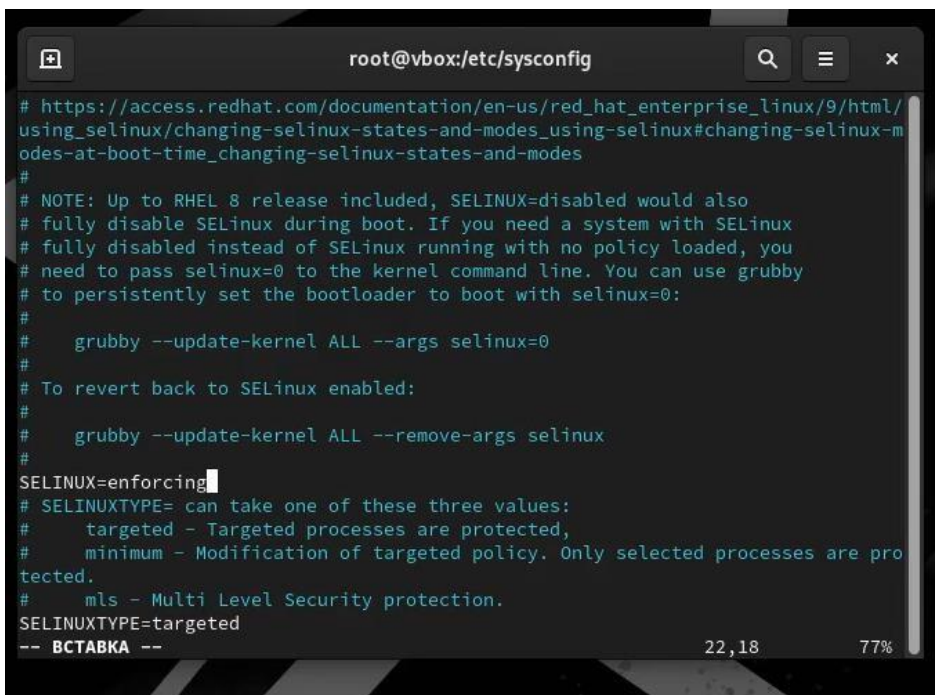


Рис. 6. Установка в файле SELINUX=enforcing, сохранение изменений.

Выполним перезагрузку системы:

```
[root@vbox ~]# reboot
```

Рис. 7. Перезагрузка системы.

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

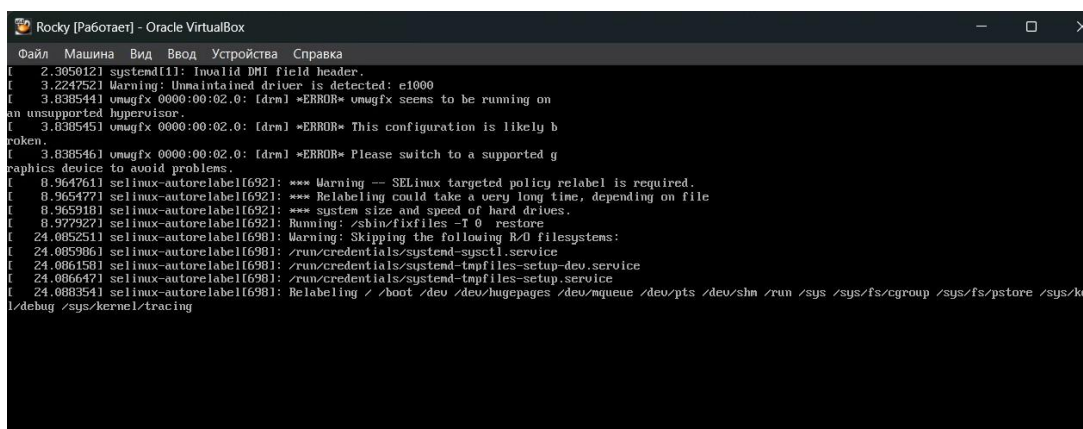
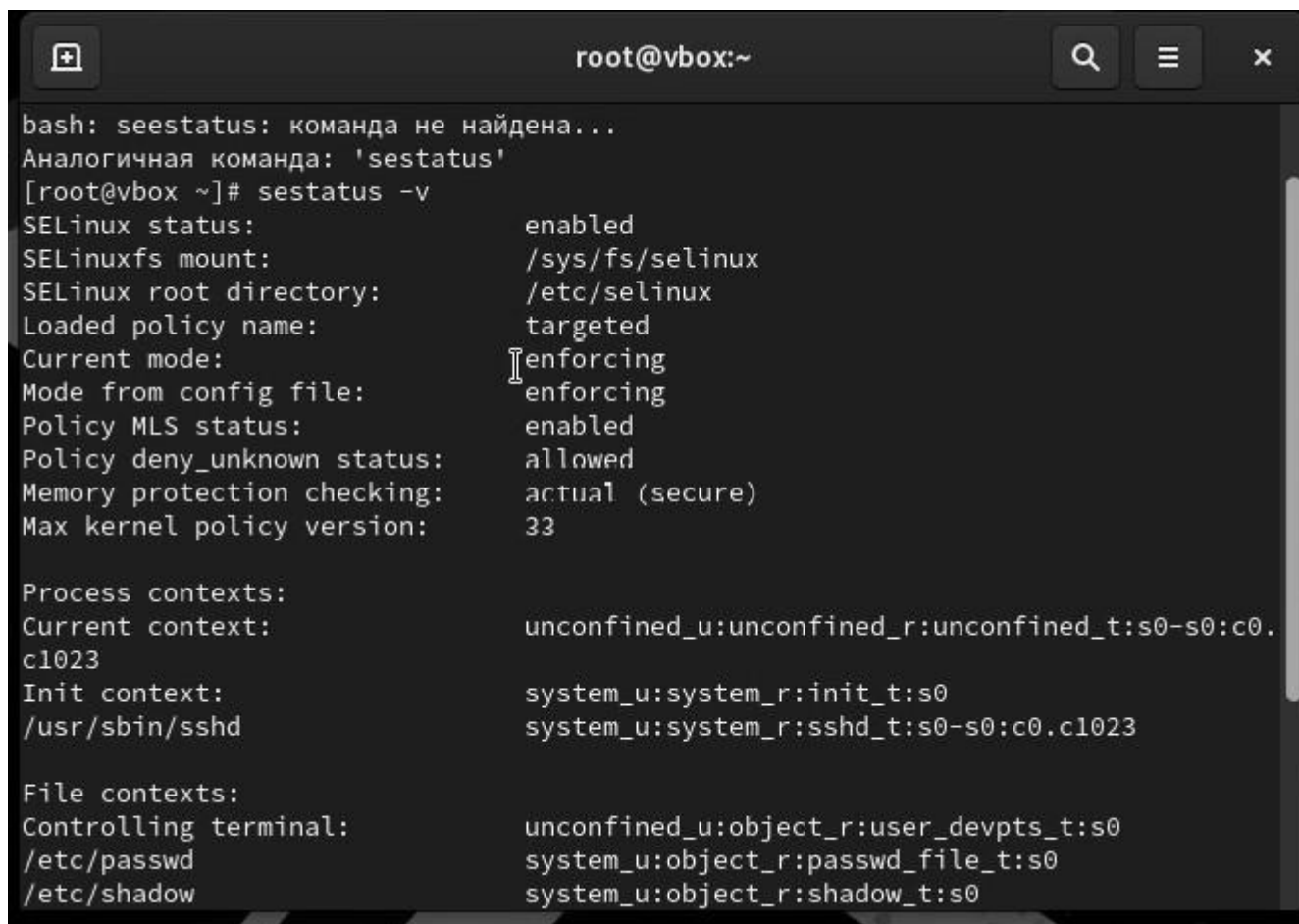


Рис. 8. Получение предупреждающего сообщения при перезагрузке системы.

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



```
root@vbox:~
bash: seestatus: команда не найдена...
Аналогичная команда: 'sestatus'
[root@vbox ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:          targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33

Process contexts:
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                 system_u:system_r:init_t:s0
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
```

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.

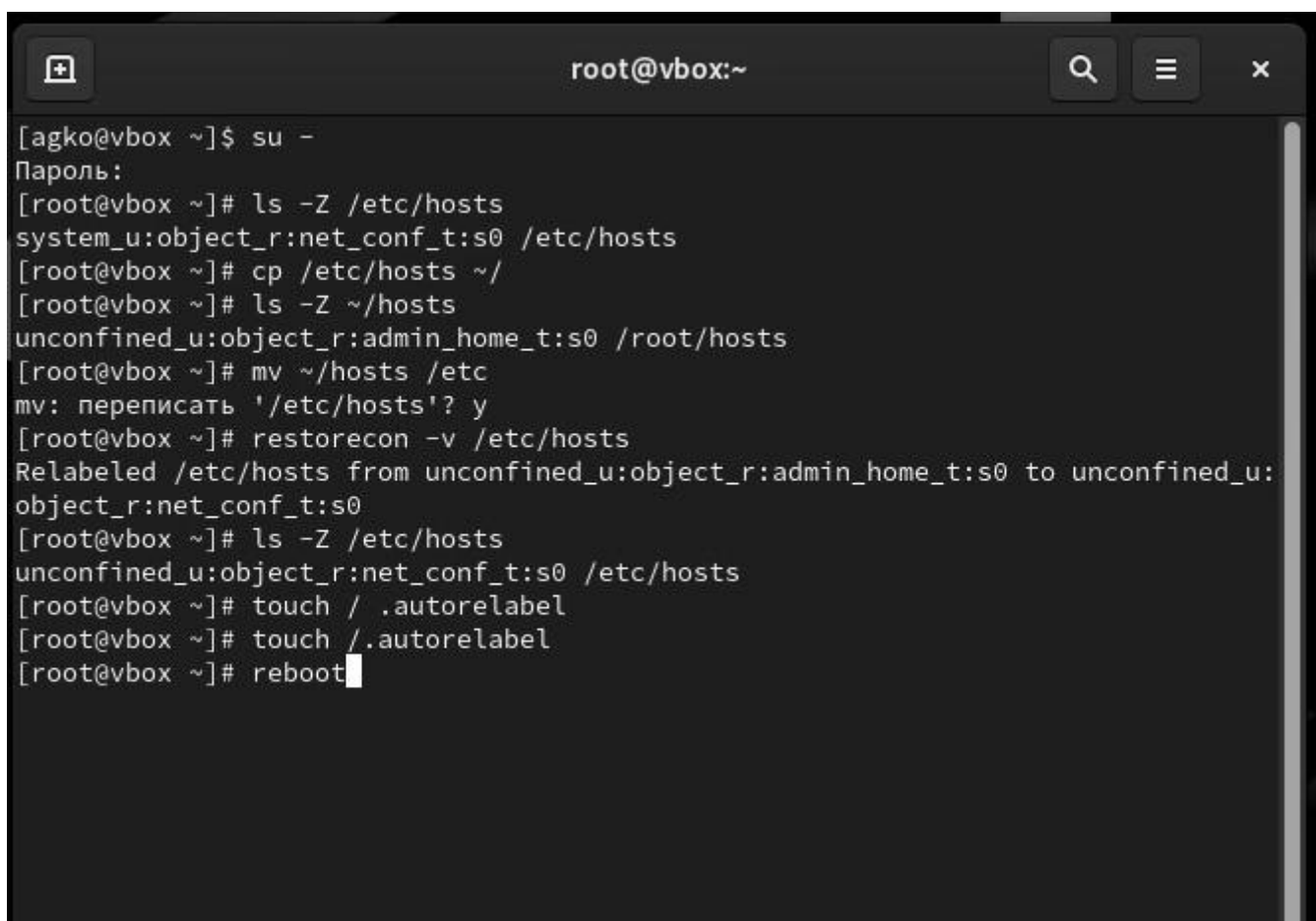
A terminal window titled 'root@vbox:~' with search, menu, and close buttons. The terminal shows a user 'agko@vbox' switching to root with 'su -'. The root user then runs 'ls -Z /etc/hosts' showing context 'system_u:object_r:net_conf_t:s0'. Then 'cp /etc/hosts ~/'. Then 'ls -Z ~/hosts' showing context 'unconfined_u:object_r:admin_home_t:s0'. Then 'mv ~/hosts /etc' with a confirmation 'y'. Then 'restorecon -v /etc/hosts' showing the relabeling from 'admin_home_t:s0' to 'net_conf_t:s0'. Then 'ls -Z /etc/hosts' showing the new context. Finally, 'touch /.autorelabel' is run twice, and the terminal ends with 'reboot'.

Рис. 10. Запуск терминала и получение полномочий администратора, просмотр контекста безопасности файла, копирование файла в домашний каталог, проверка контекста 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.

```
Starting Load Kernel Module fuse...
[ OK ] Finished Load Kernel Module fuse.
[ OK ] Finished Load Kernel Module configfs.
[ OK ] Started /usr/sbin/lvm vgchange -aay --autoactivation event rl.
[ OK ] Finished Wait for udev To Complete Device Initialization.
[ OK ] Reached target Preparation for Local File Systems.
Mounting /boot...
[ OK ] Mounted /boot.
[ OK ] Reached target Local File Systems.
Starting Tell Plymouth To Write Out Runtime Data...
Starting Automatic Boot Loader Update...
Starting Create Volatile Files and Directories...
[ OK ] Finished Automatic Boot Loader Update.
[ OK ] Finished Tell Plymouth To Write Out Runtime Data.
[ OK ] Finished Create Volatile Files and Directories.
Starting Record System Boot/Shutdown in UTMP...
[ OK ] Finished Record System Boot/Shutdown in UTMP.
[ OK ] Reached target System Initialization.
[ OK ] Started Manage Sound Card State (restore and store).
[ OK ] Reached target Sound Card.
Starting Restore /run/initramfs on shutdown...
Starting Relabel all filesystems...
[ OK ] Finished Restore /run/initramfs on shutdown.
[ 6.634732] selinux-autorelabel[752]: *** Warning -- SELinux targeted policy relabel is required.
[ 6.635495] selinux-autorelabel[752]: *** Relabeling could take a very long time, depending on file
[ 6.636268] selinux-autorelabel[752]: *** system size and speed of hard drives.
[ 6.645483] selinux-autorelabel[752]: Running: /sbin/fixfiles -T 0 restore
[ 17.053014] selinux-autorelabel[758]: Warning: Skipping the following R/O filesystems:
[ 17.053646] selinux-autorelabel[758]: /run/credentials/systemd-sysctl.service
[ 17.054237] selinux-autorelabel[758]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 17.054765] selinux-autorelabel[758]: /run/credentials/systemd-tmpfiles-setup.service
```

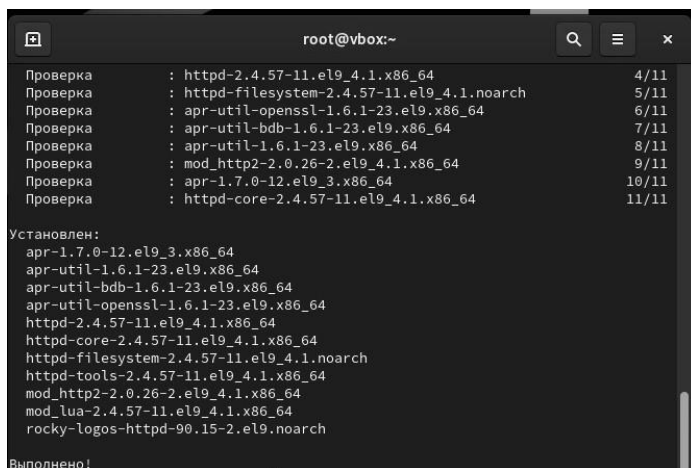
Рис. 11. Просмотр загрузочных сообщений после нажатия клавиши “Esc”.

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
```

```
root@vbox:~  
Проверка : httpd-2.4.57-11.el9_4.1.x86_64 4/11  
Проверка : httpd-filesystem-2.4.57-11.el9_4.1.noarch 5/11  
Проверка : apr-util-openssl-1.6.1-23.el9.x86_64 6/11  
Проверка : apr-util-bdb-1.6.1-23.el9.x86_64 7/11  
Проверка : apr-util-1.6.1-23.el9.x86_64 8/11  
Проверка : mod_http2-2.0.26-2.el9_4.1.x86_64 9/11  
Проверка : apr-1.7.0-12.el9_3.x86_64 10/11  
Проверка : httpd-core-2.4.57-11.el9_4.1.x86_64 11/11  
  
Установлен:  
apr-1.7.0-12.el9_3.x86_64  
apr-util-1.6.1-23.el9.x86_64  
apr-util-bdb-1.6.1-23.el9.x86_64  
apr-util-openssl-1.6.1-23.el9.x86_64  
httpd-2.4.57-11.el9_4.1.x86_64  
httpd-core-2.4.57-11.el9_4.1.x86_64  
httpd-filesystem-2.4.57-11.el9_4.1.noarch  
httpd-tools-2.4.57-11.el9_4.1.x86_64  
mod_http2-2.0.26-2.el9_4.1.x86_64  
mod_lua-2.4.57-11.el9_4.1.x86_64  
rocky-logos-httpd-90.15-2.el9.noarch  
  
Выполнено!
```

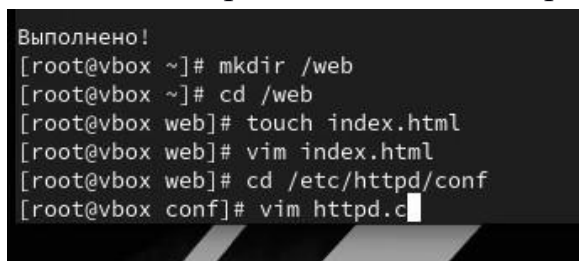
Рис. 12. Запуск терминала и получение полномочий администратора, установка необходимого программного обеспечения.

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.



```
Выполнено!  
[root@vbox ~]# mkdir /web  
[root@vbox ~]# cd /web  
[root@vbox web]# touch index.html  
[root@vbox web]# vim index.html  
[root@vbox web]# cd /etc/httpd/conf  
[root@vbox conf]# vim httpd.c
```

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**.

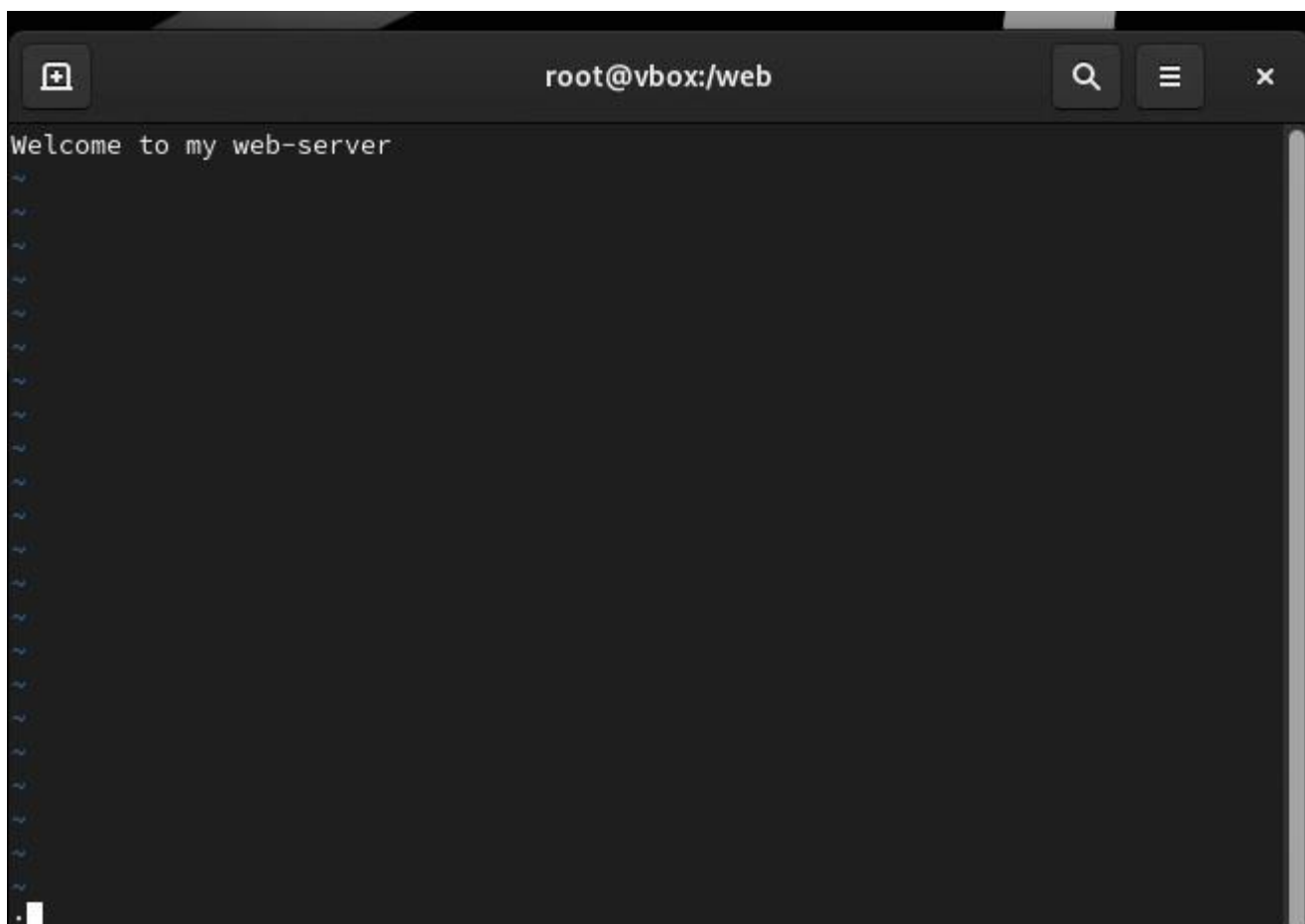


Рис. 14. Добавление текста в файл.

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:

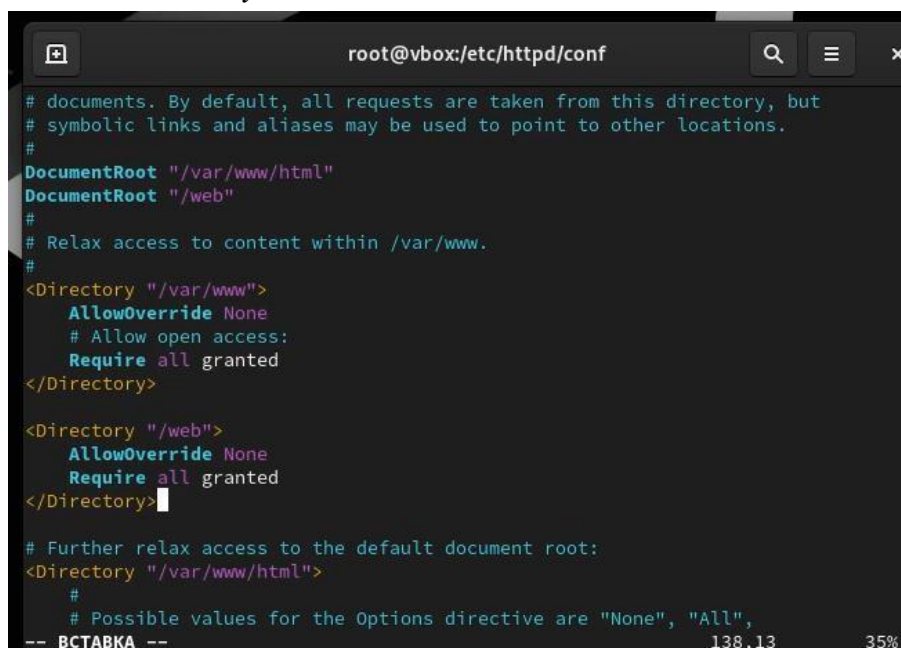
```
<Directory "/var/www">  
    AllowOverride None  
    Require all granted  
</Directory>
```

и добавим следующий раздел, определяющий правила доступа:

```
<Directory "/web">  
    AllowOverride None
```

Require all granted

</Directory>



```
root@vbox:/etc/httpd/conf
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
-- ВСТАВКА --                                     138,13      35%
```

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

```
root@vbox:/etc/httpd/conf
Подготовка      :                               1/1
Установка       : lnx-2.8.9-20.el9.x86_64      1/1
Запуск скрипта  : lnx-2.8.9-20.el9.x86_64      1/1
Проверка        : lnx-2.8.9-20.el9.x86_64      1/1

Установлен:
  lnx-2.8.9-20.el9.x86_64

Выполнено!
[root@vbox ~]# mkdir /web
[root@vbox ~]# cd /web
[root@vbox web]# touch index.html
[root@vbox web]# vim index.html
[root@vbox web]# cd /etc/httpd/conf
[root@vbox conf]# vim httpd.conf
[root@vbox conf]# systemctl start httpd
^[[A[root@vbox con
[root@vbox conf]# systemctl start httpd
[root@vbox conf]# system enable httpd
bash: system: команда не найдена...
[root@vbox conf]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr
/lib/systemd/system/httpd.service.
```

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**.

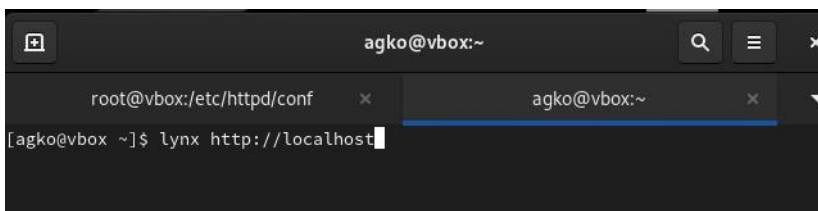


Рис. 17. Открытие терминала под учётной записью своего пользователя, обращение к веб-серверу в текстовом браузере lynx.

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”.

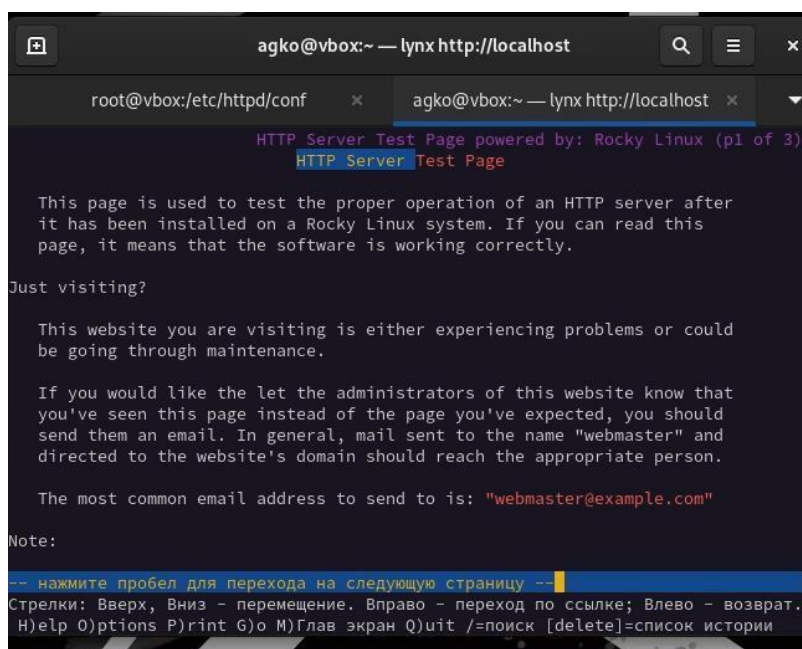


Рис. 18. Открытие веб-страницы Red Hat по умолчанию, выход из lynx.

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.

```
[root@vbox conf]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@vbox conf]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:
httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_
```

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**. Т.к. получить доступ к серверу не получилось, нужно перезапустить систему

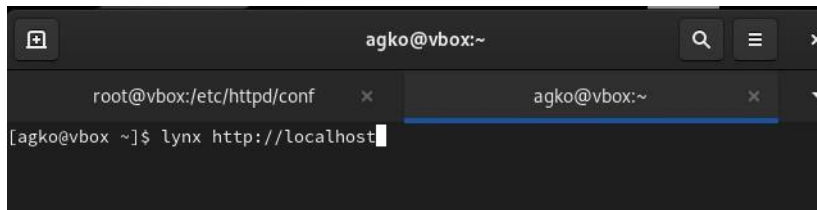


Рис. 20. Открытие терминала под учётной записью своего пользователя, повторное обращение к веб-серверу в текстовом браузере lynx.

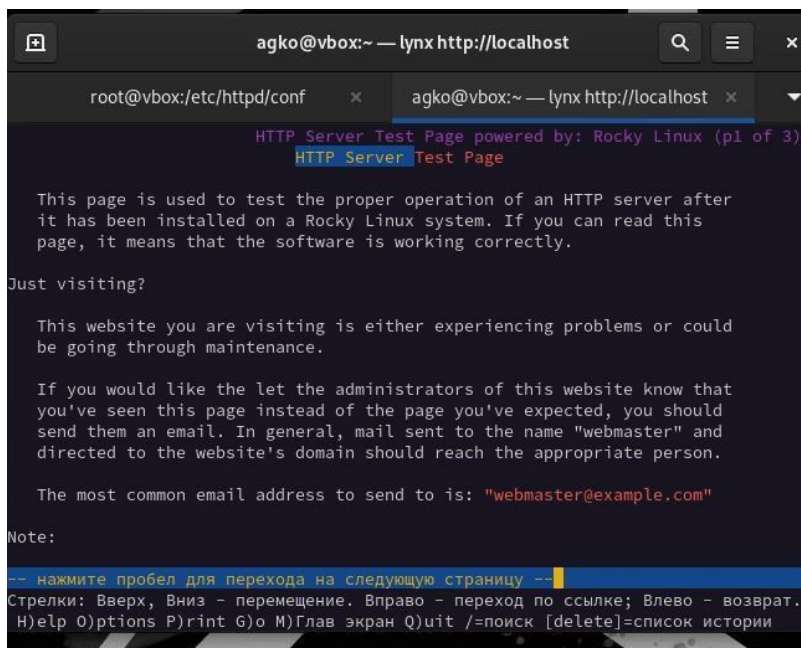


Рис. 21. Открытие веб-страницы Red Hat по умолчанию, выход из lynx.

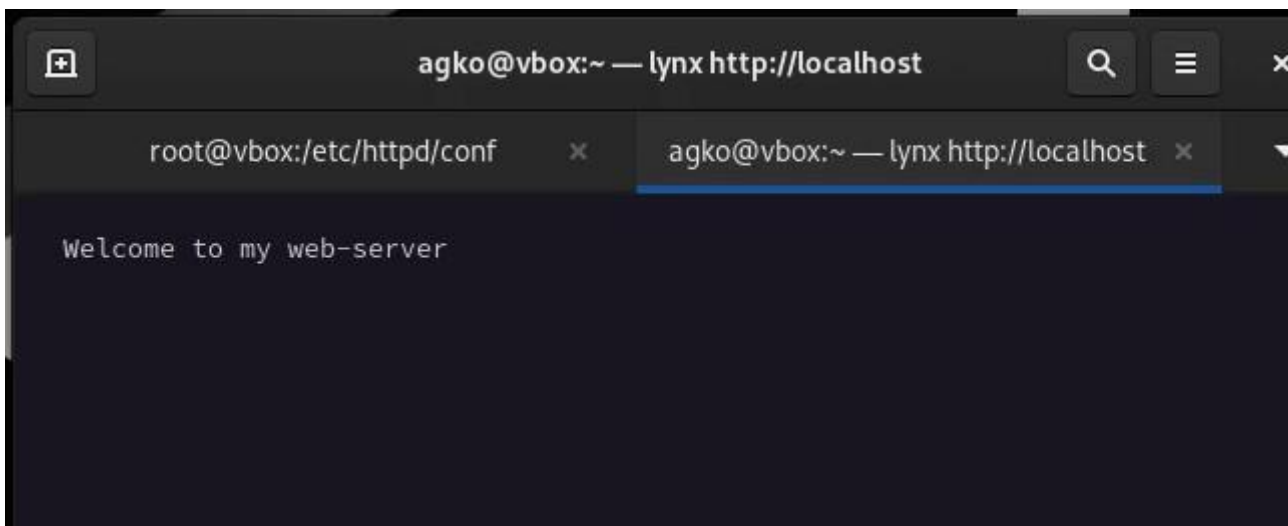
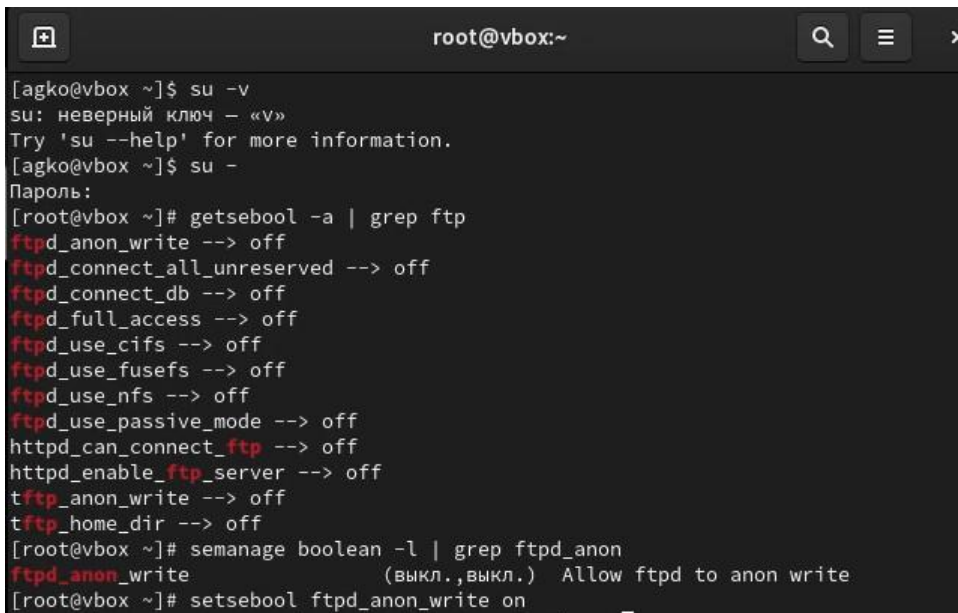


Рис. 23. Получение доступа к своей пользовательской веб-странице.

Работа с переключателями SELinux:

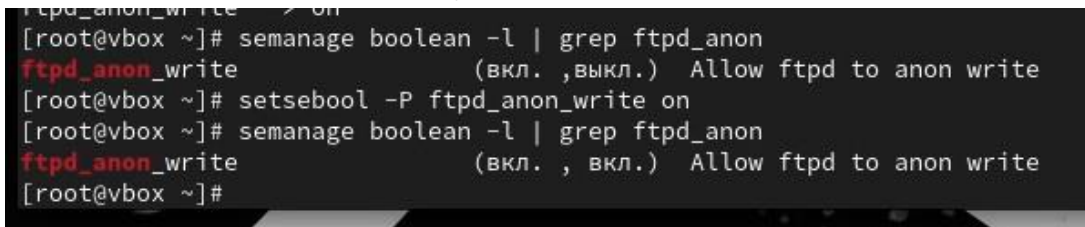
Запустим терминал и получим полномочия администратора. Посмотрим список переключателей SELinux для службы `ftp`: **`getsebool -a | grep ftp`**. Мы видим переключатель `ftpd_anon_write` с текущим значением `off`. Для службы `ftpd_anon` посмотрим список переключателей с пояснением, за что отвечает каждый 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_write* с *off* на *on*: **setsebool -P ftpd_anon_write on** и посмотрим список переключателей: **semanage boolean -l | grep ftpd_anon** (переключатель имеет состояние *on*).



```
root@vbox:~
[agko@vbox ~]$ su -v
su: неверный ключ - «v»
Try 'su --help' for more information.
[agko@vbox ~]$ su -
Пароль:
[root@vbox ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@vbox ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@vbox ~]# setsebool ftpd_anon_write 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*.



```
[root@vbox ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. ,выкл.) Allow ftpd to anon write
[root@vbox ~]# setsebool -P ftpd_anon_write on
[root@vbox ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@vbox ~]#
```

Рис. 25. Повторный просмотр списка переключателей SELinux для службы *ftpd_anon_write*, просмотр списка переключателей с пояснением, изменение постоянного значения переключателя для службы *ftpd_anon_write* 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? `getsebool -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
```

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? `/etc/sysconfig/selinux`

6. Где SELinux регистрирует все свои сообщения? По умолчанию в `/var/log/audit/audit.log`

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? `getsebool -a | 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? 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.