

Лабораторная работа №9

Управление SELinux

Ко Антон Геннадьевич

1132221551

НПИБД-02-23

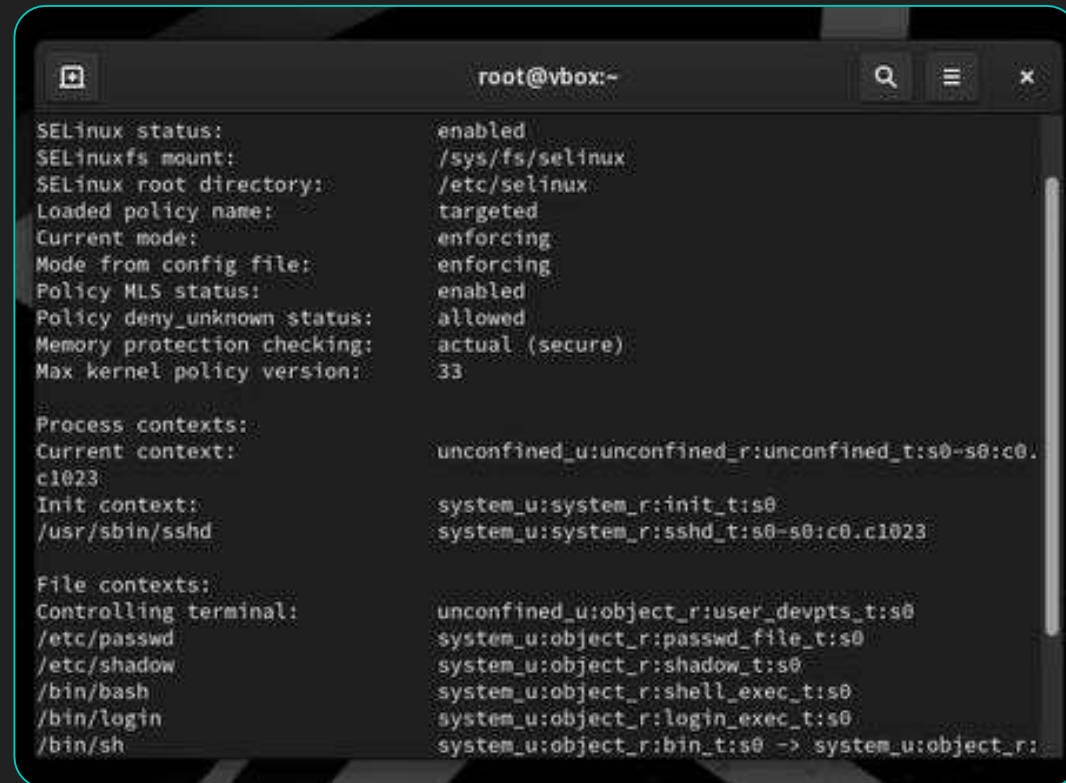
Цель работы:

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

Управление режимами SELinux:

Просмотр информации о состоянии SELinux

○Рис. 1.1. Запуск терминала и получение полномочий администратора, просмотр текущей информации о состоянии SELinux.



```
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:
```

Режимы работы SELinux

○ **Рис. 1.2.** Просмотр режима работы SELinux, изменение режима работы и проверка, открытие файла в текстовом редакторе.

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

SELINUX=disabled

○Рис. 1.3. Установка в файле SELINUX=disabled, сохранение изменений.

```
# 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
```

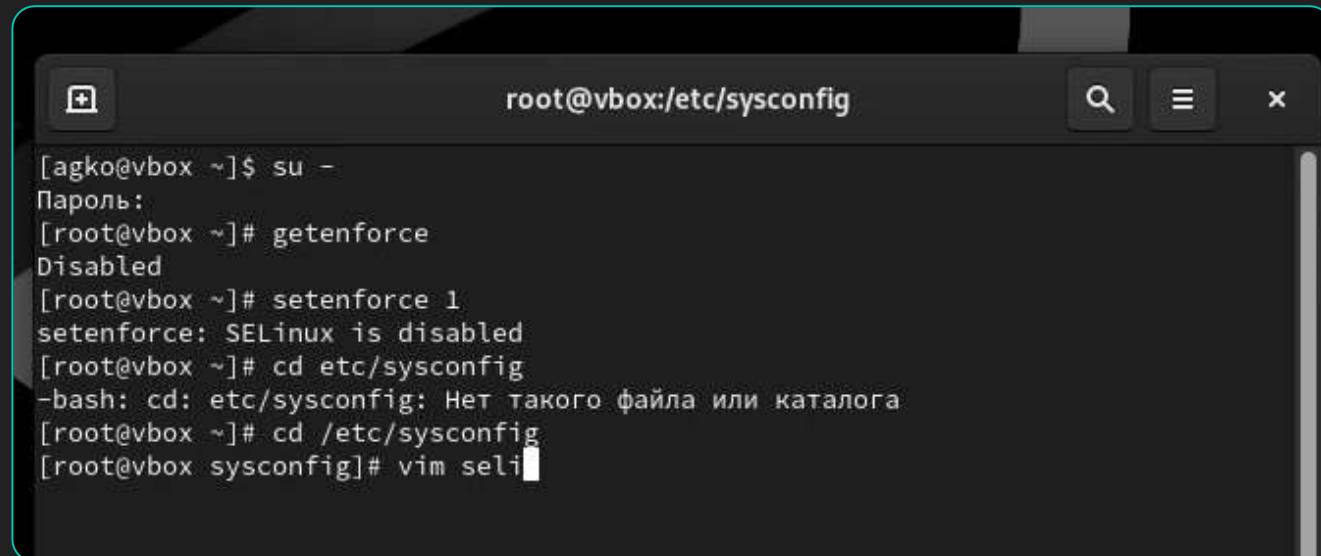
Перезагрузка системы

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

Рис. 1.4. Перезагрузка системы.

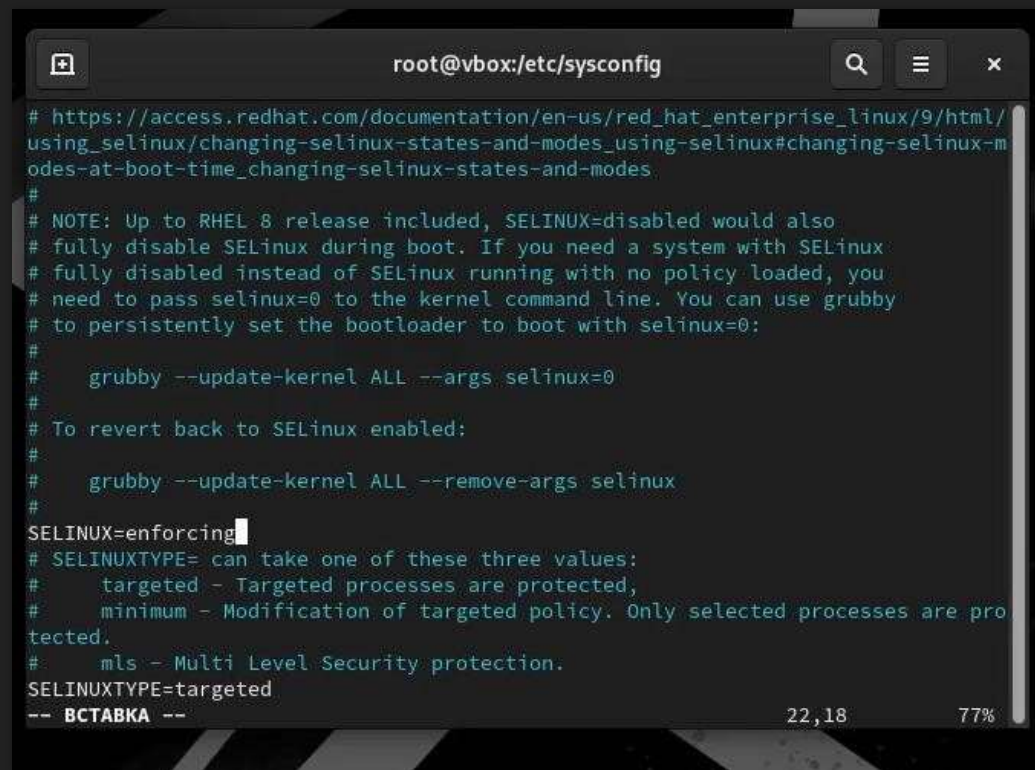
Статус SELinux, попытка переключения режима работы

○Рис. 1.5. Запуск терминала и получение полномочий администратора, просмотр статуса SELinux, попытка переключения режима работы, открытие файла в текстовом редакторе.

A screenshot of a terminal window with a dark background. The window title bar shows 'root@vbox:/etc/sysconfig' and standard window controls. The terminal output shows a user switching to root, checking SELinux status (Disabled), attempting to force it on (setenforce 1), which fails with the message 'setenforce: SELinux is disabled'. The user then attempts to change to the directory /etc/sysconfig, which fails with the message '-bash: cd: etc/sysconfig: Нет такого файла или каталога'. Finally, the user attempts to open a file named 'seli' in the 'sysconfig' directory using the 'vim' editor.

```
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
```


SELINUX=enforcing



```
root@vbox:/etc/sysconfig
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/
using_selinux/changing-selinux-states-and-modes_using_selinux#changing-selinux-m
odes-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=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are pro
tected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
-- ВСТАВКА -- 22,18 77%
```

Рис. 1.6. Установка в файле SELINUX=enforcing, сохранение изменений.

Перезагрузка системы



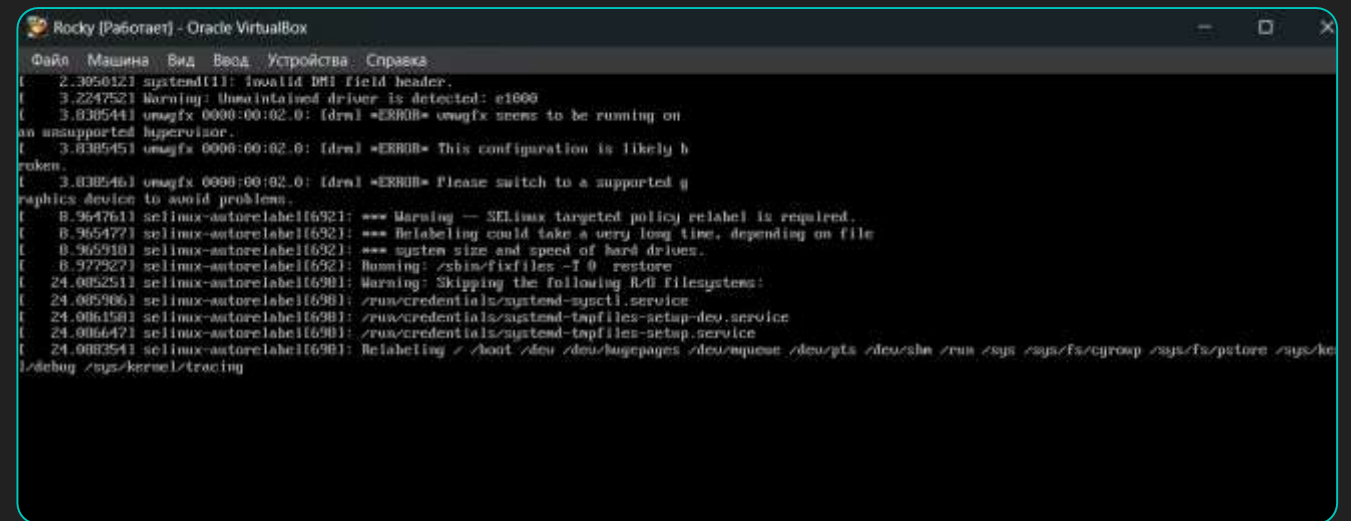
```
[root@vbox ~]# reboot
```

A screenshot of a terminal window with a black background and white text. The prompt is [root@vbox ~]# and the command being entered is reboot. A white cursor is visible at the end of the command.

Рис. 1.7. Перезагрузка системы.

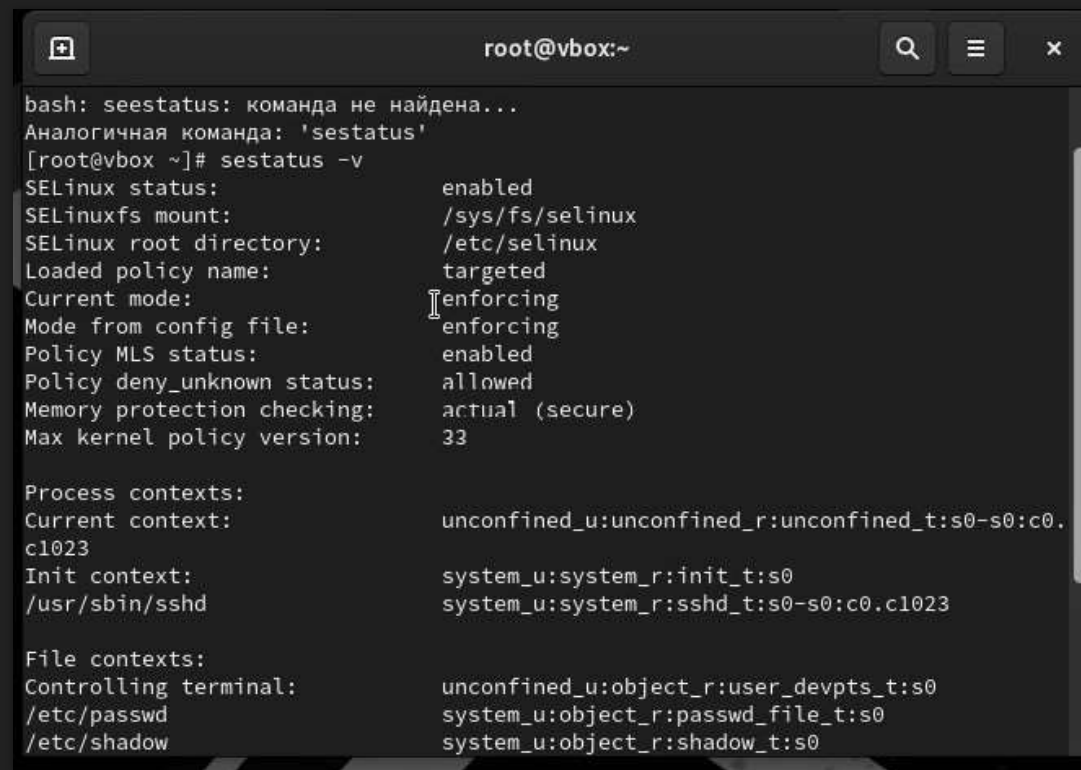
Предупреждающее сообщение

Орис. 1.8. Получение предупреждающего сообщения при перезагрузке системы.



```
Rocky [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[ 2.305012] systemd[1]: Invalid DMI field header.
[ 3.224752] Warning: Unmaintained driver is detected: e1000
[ 3.838544] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 3.838545] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 3.838546] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 6.964761] selinux-autorelabel[692]: *** Warning -- SELinux targeted policy relabel is required.
[ 6.964777] selinux-autorelabel[692]: *** Relabeling could take a very long time, depending on file
[ 6.965910] selinux-autorelabel[692]: *** system size and speed of hard drives.
[ 6.977927] selinux-autorelabel[692]: Running: /sbin/fixfiles -f 0 restore
[ 24.005251] selinux-autorelabel[690]: Warning: Skipping the following R/O filesystems:
[ 24.005906] selinux-autorelabel[690]: /run/credentials/systemd-sysctl.service
[ 24.006158] selinux-autorelabel[690]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 24.006471] selinux-autorelabel[690]: /run/credentials/systemd-tmpfiles-setup.service
[ 24.008354] selinux-autorelabel[690]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kc
l/debug /sys/kernel/tracing
```

Текущее состояние SELinux

A terminal window titled 'root@vbox:~' with search, menu, and close icons in the title bar. The terminal shows the command 'sestatus -v' and its output, which details the SELinux configuration and current state.

```
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

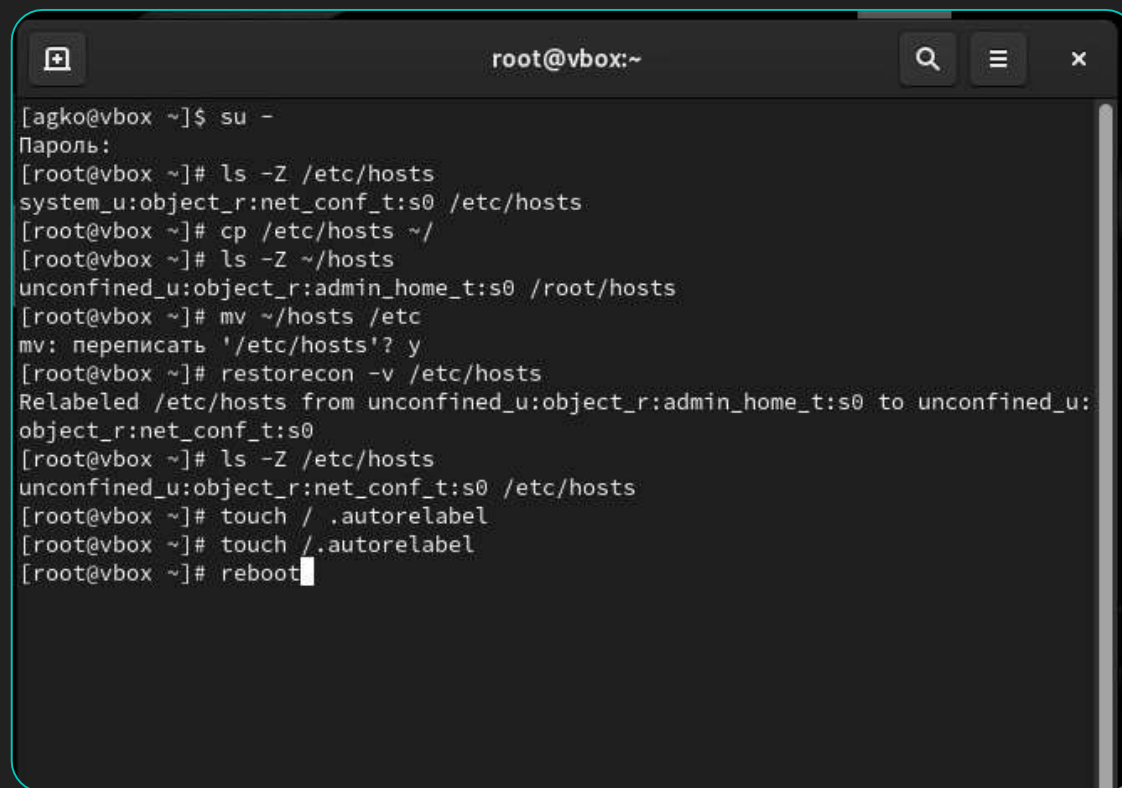
File contexts:
Controlling terminal:          unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                    system_u:object_r:passwd_file_t:s0
/etc/shadow                    system_u:object_r:shadow_t:s0
```

Рис. 1.9. Запуск терминала и получение полномочий администратора, просмотр текущей информации о состоянии SELinux.

Использование `restorecon` для восстановления контекста безопасности

Просмотр контекстов

○ **Рис. 2.1.** 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.



```
root@vbox:~  
[agko@vbox ~]$ su -  
Пароль:  
[root@vbox ~]# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[root@vbox ~]# cp /etc/hosts ~/  
[root@vbox ~]# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
[root@vbox ~]# mv ~/hosts /etc  
mv: переписать '/etc/hosts'? y  
[root@vbox ~]# restorecon -v /etc/hosts  
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:  
object_r:net_conf_t:s0  
[root@vbox ~]# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
[root@vbox ~]# touch /.autorelabel  
[root@vbox ~]# touch /.autorelabel  
[root@vbox ~]# reboot
```

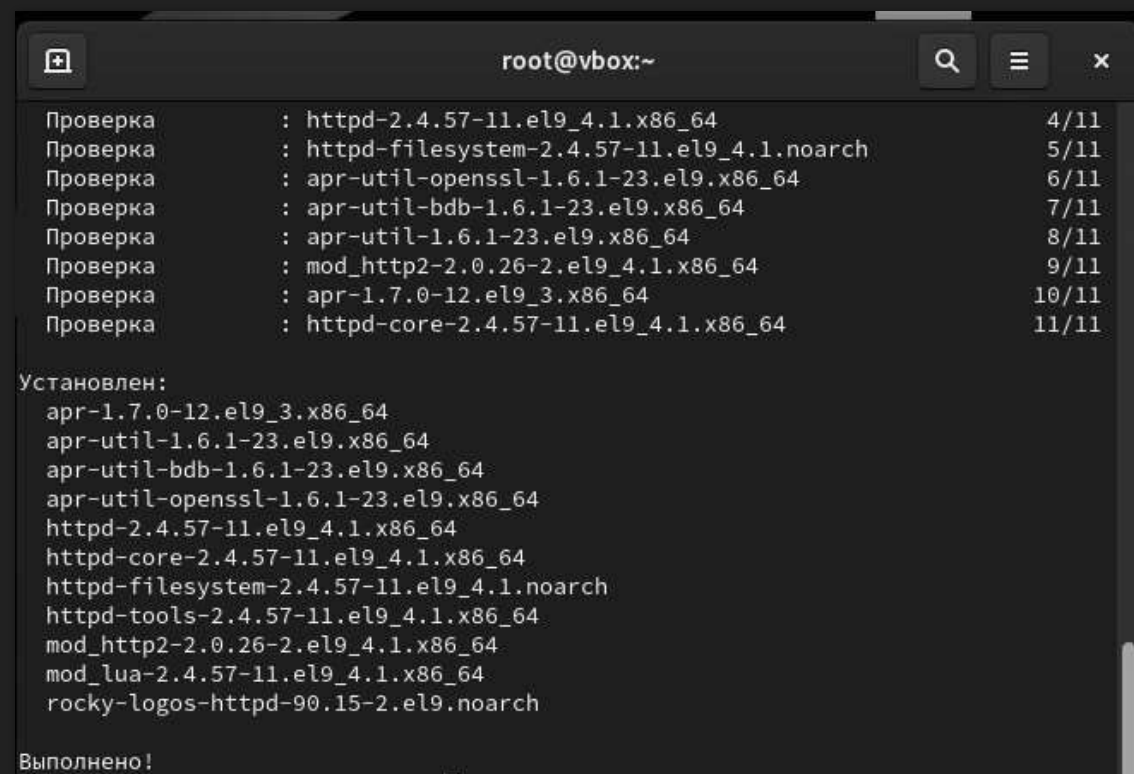

Загрузочные сообщения

Орис. 2.2. Просмотр загрузочных сообщений после нажатия клавиши “Esc”.

```
Starting Load Kernel Module fuse...
[ OK ] Finished Load Kernel Module fuse.
[ OK ] Finished Load Kernel Module configs.
[ 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
```


Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Установка необходимого программного обеспечения



```
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. 3.1. Запуск терминала и получение полномочий администратора, установка необходимого программного обеспечения.

Создание нового хранилища и файла

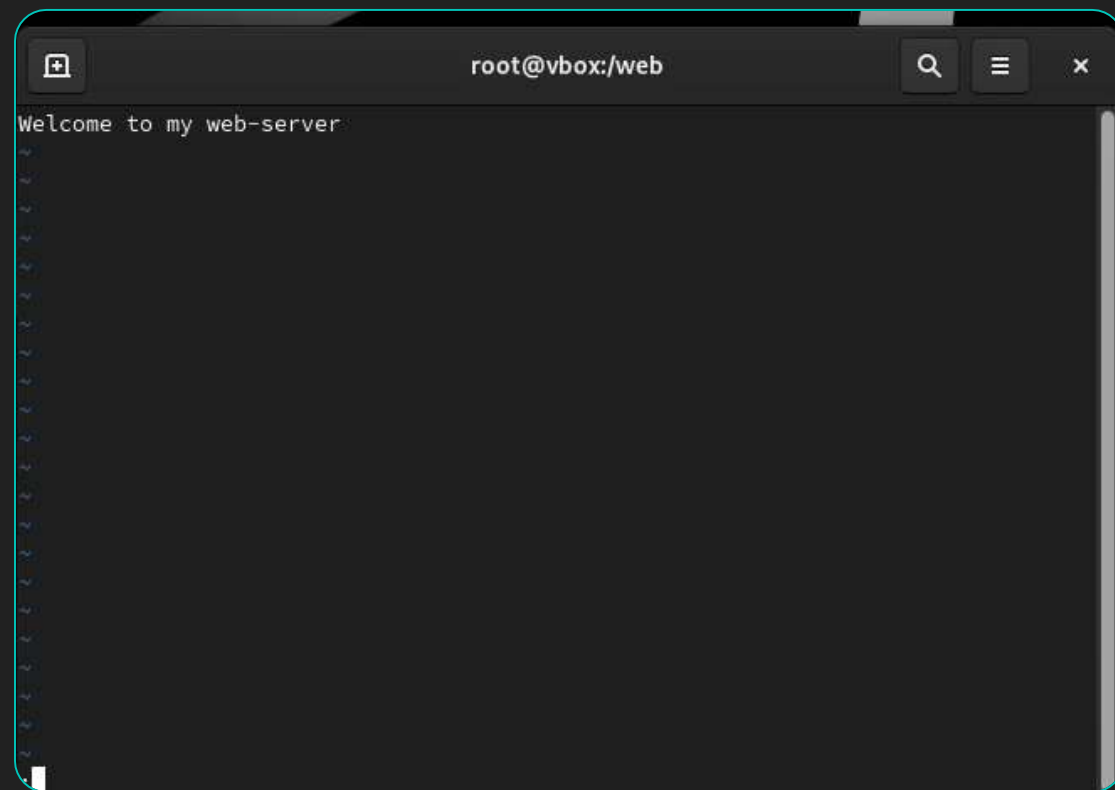
○ **Рис. 3.2.** Создание нового хранилища (для файлов web-сервера) и файла в этом хранилище, открытие файла в текстовом редакторе.

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
```

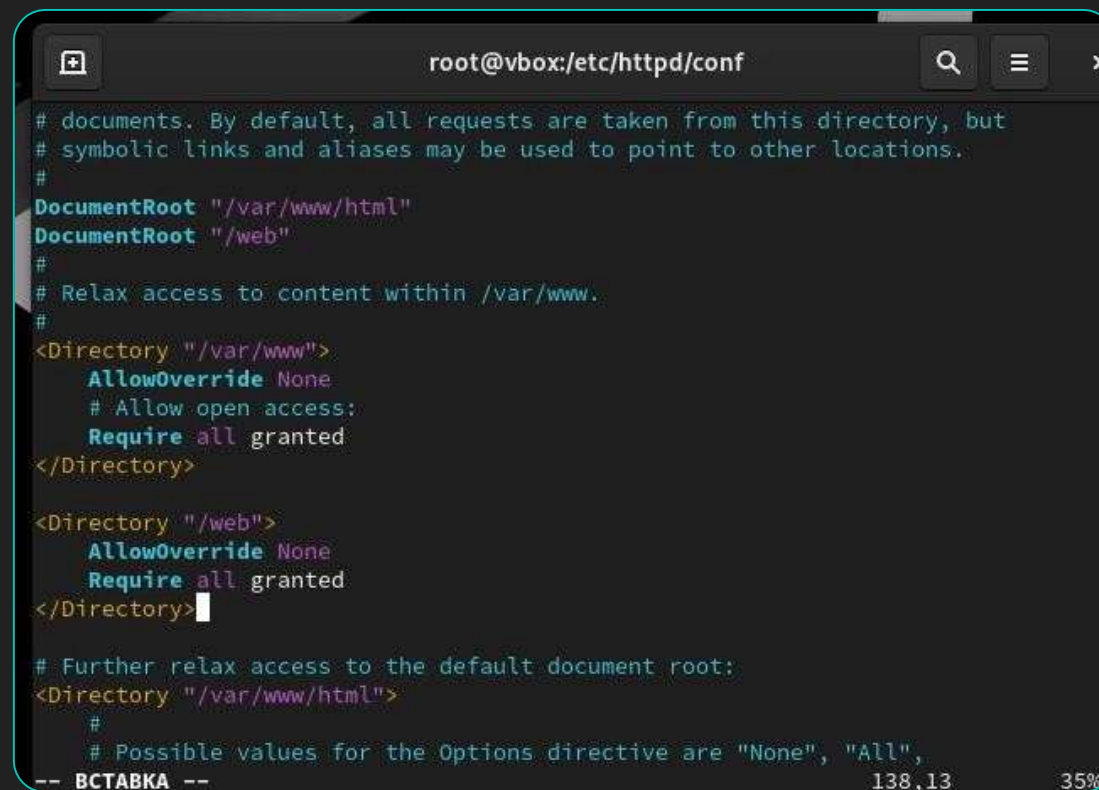
Добавление текста в файл

Рис. 3.3. Добавление текста в файл.



Комментирование строк и добавление новых

○Рис. 3.4. Комментирование строки и добавление ниже другой. Комментирование раздела и добавление следующего, определяющего правила доступа.



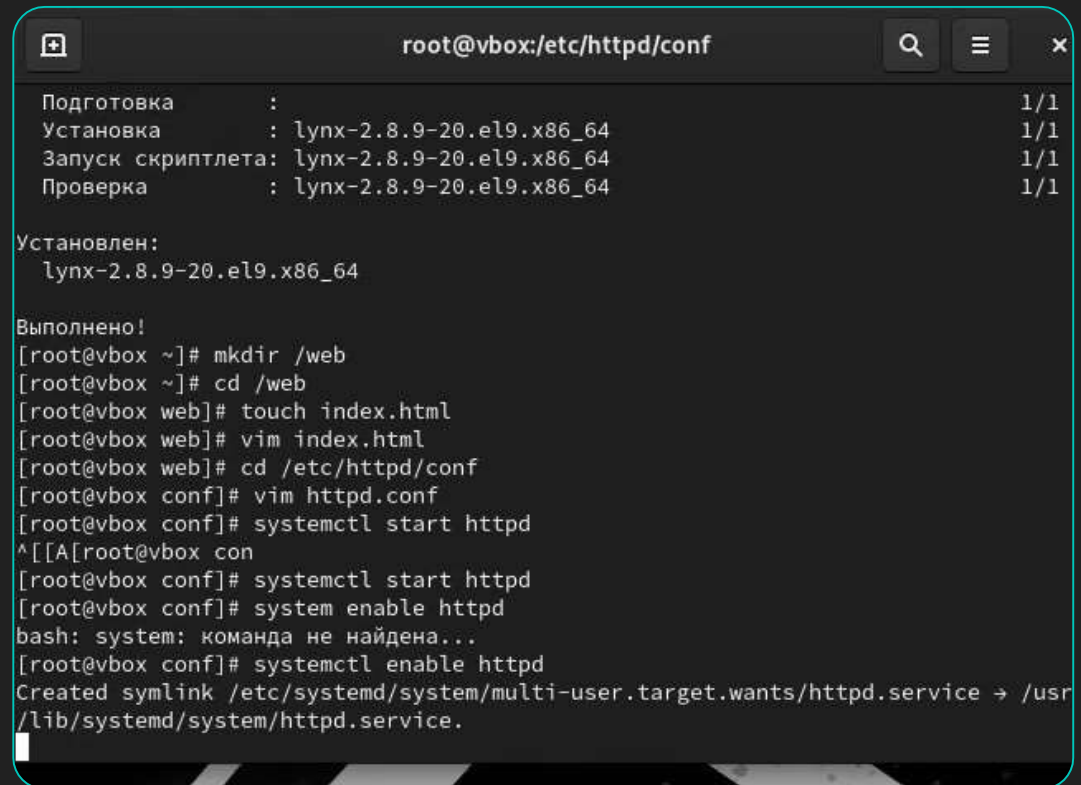
```
root@vbox:/etc/httpd/conf
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride 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%
```

Запуск веб-сервера и службы httpd

○Рис. 3.5. Запуск веб-сервера и службы httpd.



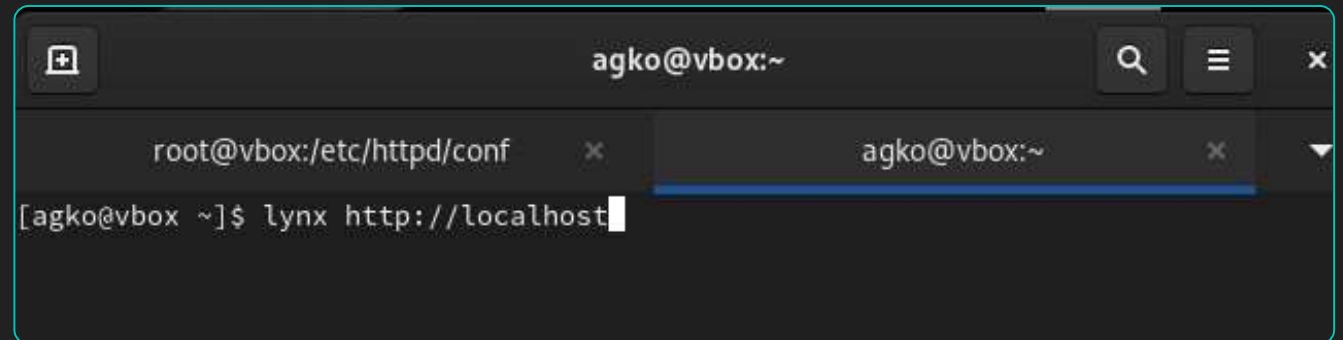
```
root@vbox:/etc/httpd/conf
Подготовка      :                               1/1
Установка       : lynx-2.8.9-20.el9.x86_64      1/1
Запуск скрипта  : lynx-2.8.9-20.el9.x86_64      1/1
Проверка        : lynx-2.8.9-20.el9.x86_64      1/1

Установлен:
  lynx-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.
```


Обращение к веб-серверу

○Рис. 3.6. Открытие терминала под учётной записью своего пользователя, обращение к веб-серверу в текстовом браузере lynx.



Веб-страница Red Hat



Рис. 3.7. Открытие веб-страницы Red Hat по умолчанию, выход из lynx.

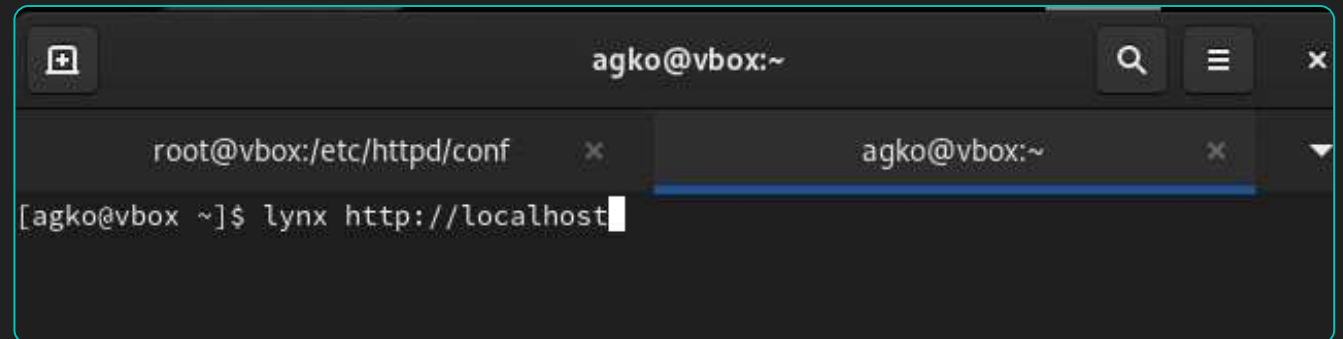
Разрешающий режим

```
[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_  
object_r:httpd_sys_content_t:s0
```

Рис. 3.8. Переключение SELinux в разрешающий режим и последующая перезагрузка системы.

Обращение к веб-серверу

○Рис. 3.9. Открытие терминала под учётной записью своего пользователя, повторное обращение к веб-серверу в текстовом браузере lynx.



Пользовательская веб-страница

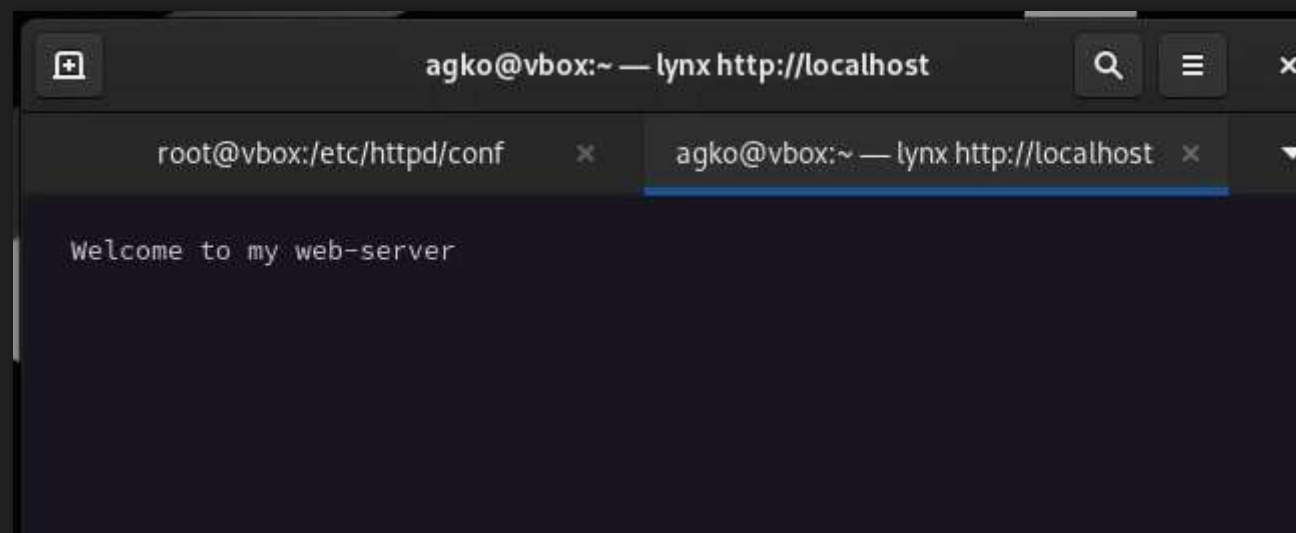


Рис. 3.10. Получение доступа к своей пользовательской веб-странице, выход из lynx.

Работа с переключателями SELinux

Работа с переключателями

○ **Рис. 4.** 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`, повторный просмотр списка переключателей SELinux для службы `ftpd_anon_write`, просмотр списка переключателей с пояснением, изменение постоянного значение переключателя для службы `ftpd_anon_write` с `off` на `on` и просмотр списка переключателей.

```
[agko@vbox ~]$ su -v
su: неверный логин - «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_hone_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
```

```
ftpd_anon_write --> on
[root@vbox ~]# semanage boo
ftpd_anon_write
[root@vbox ~]# setsebool -P
[root@vbox ~]# semanage boo
ftpd_anon_write
[root@vbox ~]#
```

Вывод

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

Спасибо за внимание!