

**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: Накова Амина Михайловна

Студ. билет № 1132232887

Группа: НПИбд-02-23

**МОСКВА**

2025 г.

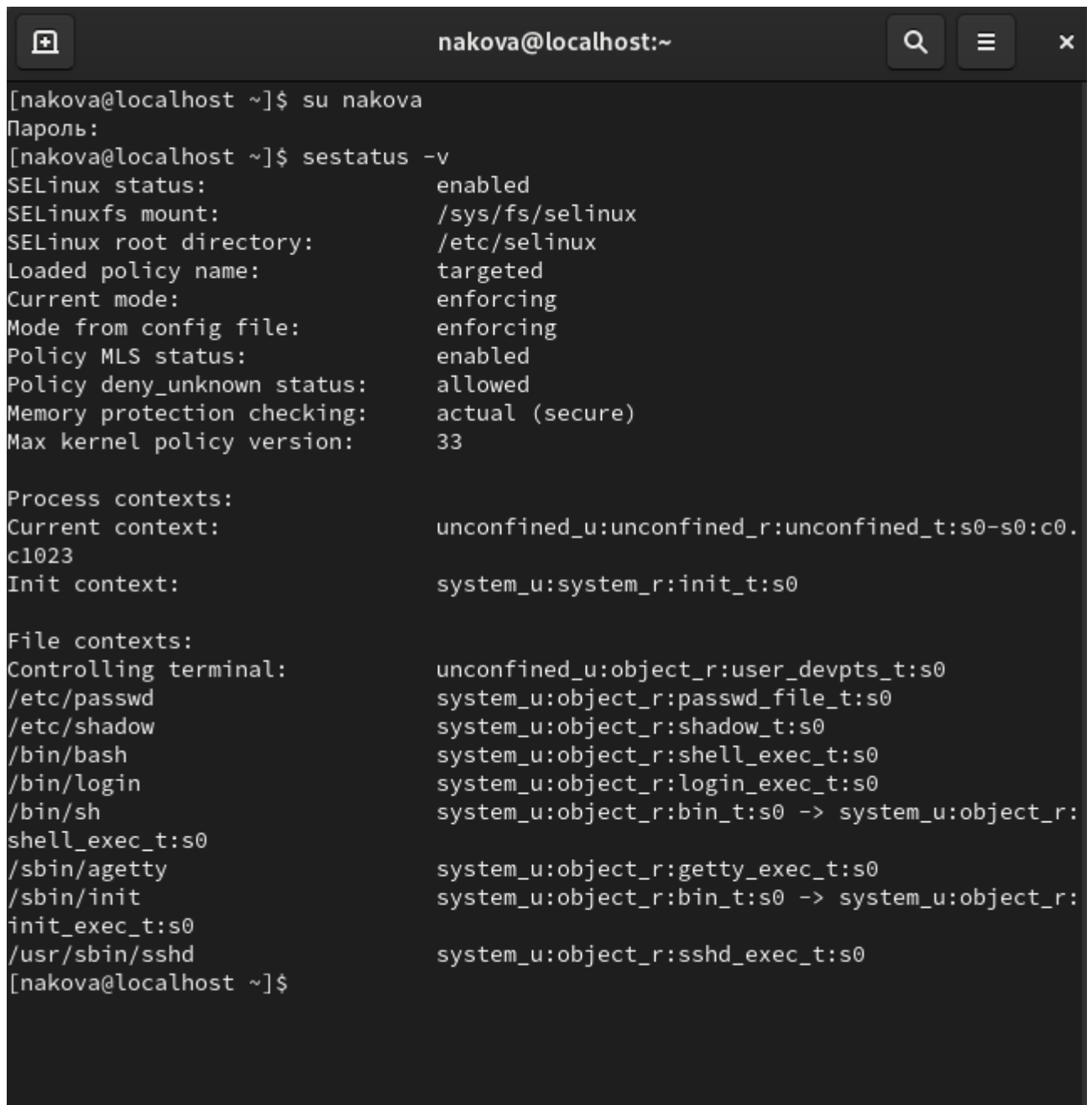
### **Цель работы:**

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** (Рис. 1.1):

A terminal window titled 'nakova@localhost:~' with search, menu, and close icons in the title bar. The terminal shows the user switching to 'nakova' and running 'sestatus -v'. The output displays SELinux status (enabled), mount point (/sys/fs/selinux), root directory (/etc/selinux), policy name (targeted), and current mode (enforcing). It also lists process contexts for the current user and the init process. Finally, it lists file contexts for various system files and directories, showing their SELinux labels.

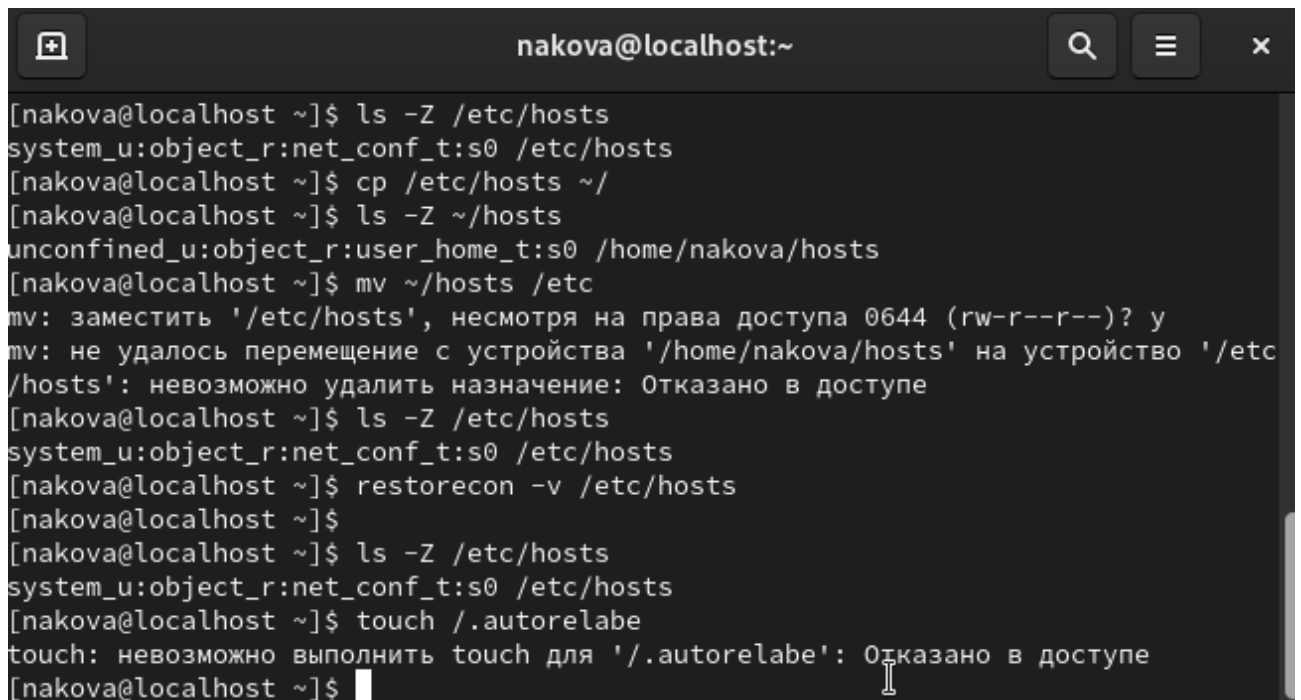
```
[nakova@localhost ~]$ su nakova
Пароль:
[nakova@localhost ~]$ sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config 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

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:
shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:
init_exec_t:s0
/usr/sbin/sshd                system_u:object_r:sshd_exec_t:s0
[nakova@localhost ~]$
```

**Рис. 1.1.** 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. 1.2):

A terminal window titled 'nakova@localhost:~' with search, menu, and close icons in the title bar. The terminal shows a series of commands and their outputs related to SELinux. The user attempts to move a file from /home/nakova/hosts to /etc/hosts, but fails due to SELinux permissions. The user then runs 'restorecon' and 'touch' commands, which also fail due to SELinux. The terminal output is as follows:

```
[nakova@localhost ~]$ ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[nakova@localhost ~]$ cp /etc/hosts ~/
[nakova@localhost ~]$ ls -Z ~/hosts
unconfined_u:object_r:user_home_t:s0 /home/nakova/hosts
[nakova@localhost ~]$ mv ~/hosts /etc
mv: заместить '/etc/hosts', несмотря на права доступа 0644 (rw-r--r--)? y
mv: не удалось перемещение с устройства '/home/nakova/hosts' на устройство '/etc/hosts': невозможно удалить назначение: Отказано в доступе
[nakova@localhost ~]$ ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[nakova@localhost ~]$ restorecon -v /etc/hosts
[nakova@localhost ~]$
[nakova@localhost ~]$ ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[nakova@localhost ~]$ touch /.autorelabel
touch: невозможно выполнить touch для '/.autorelabel': Отказано в доступе
[nakova@localhost ~]$
```

**Рис. 1.2.** 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. 1.3):

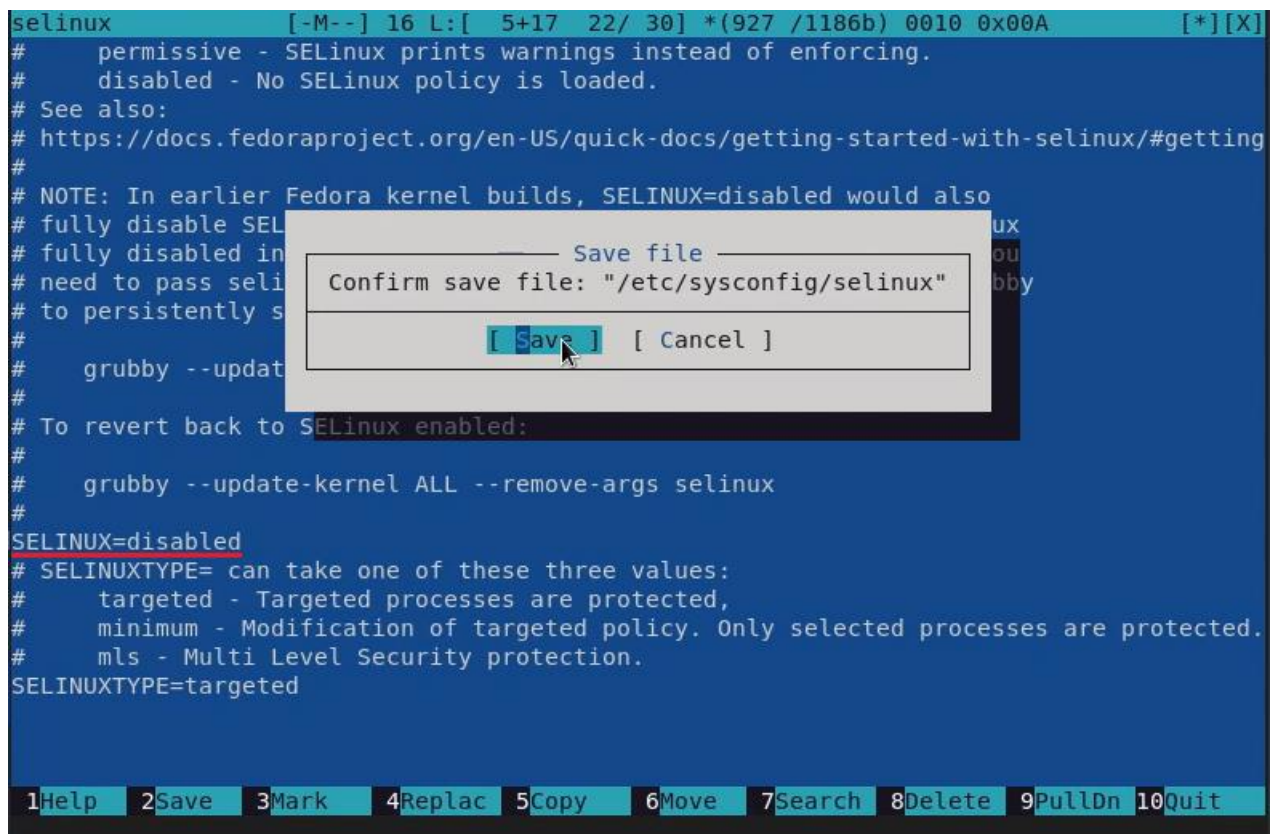


Рис. 1.3. Установка в файле SELINUX=disabled, сохранение изменений.

Выполним перезагрузку системы (Рис. 1.4):



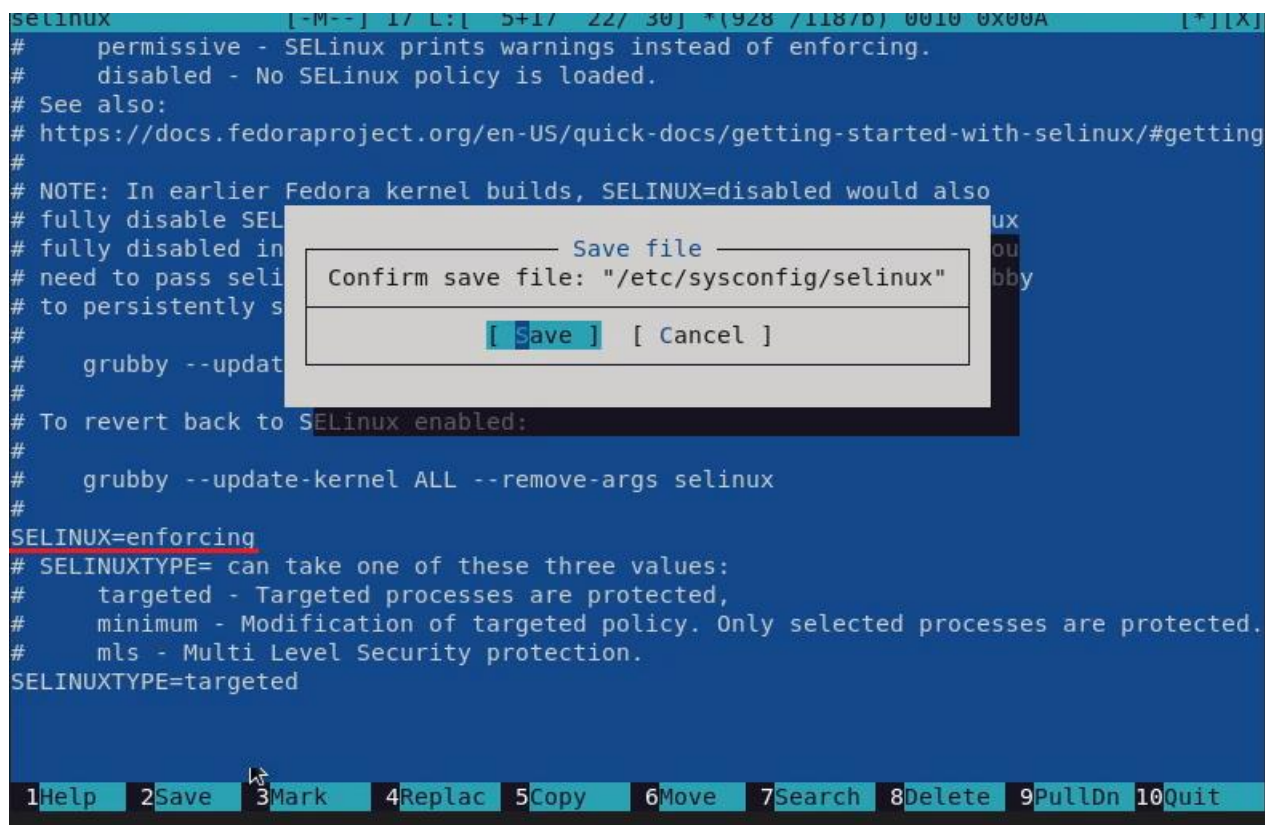
Рис. 1.4. Перезагрузка системы.

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. 1.5):

```
is disabled
# mcedit /etc/sysconfig/selinux
```

**Рис. 1.5.** 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. 1.6):



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

Выполним перезагрузку системы (Рис. 1.7):


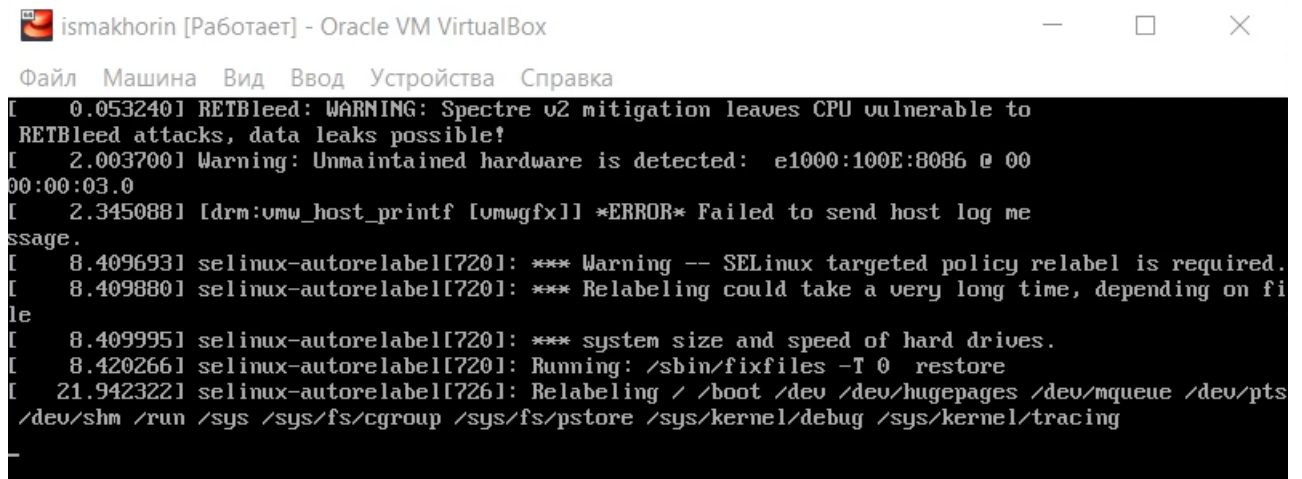


Рис. 1.7. Перезагрузка системы.

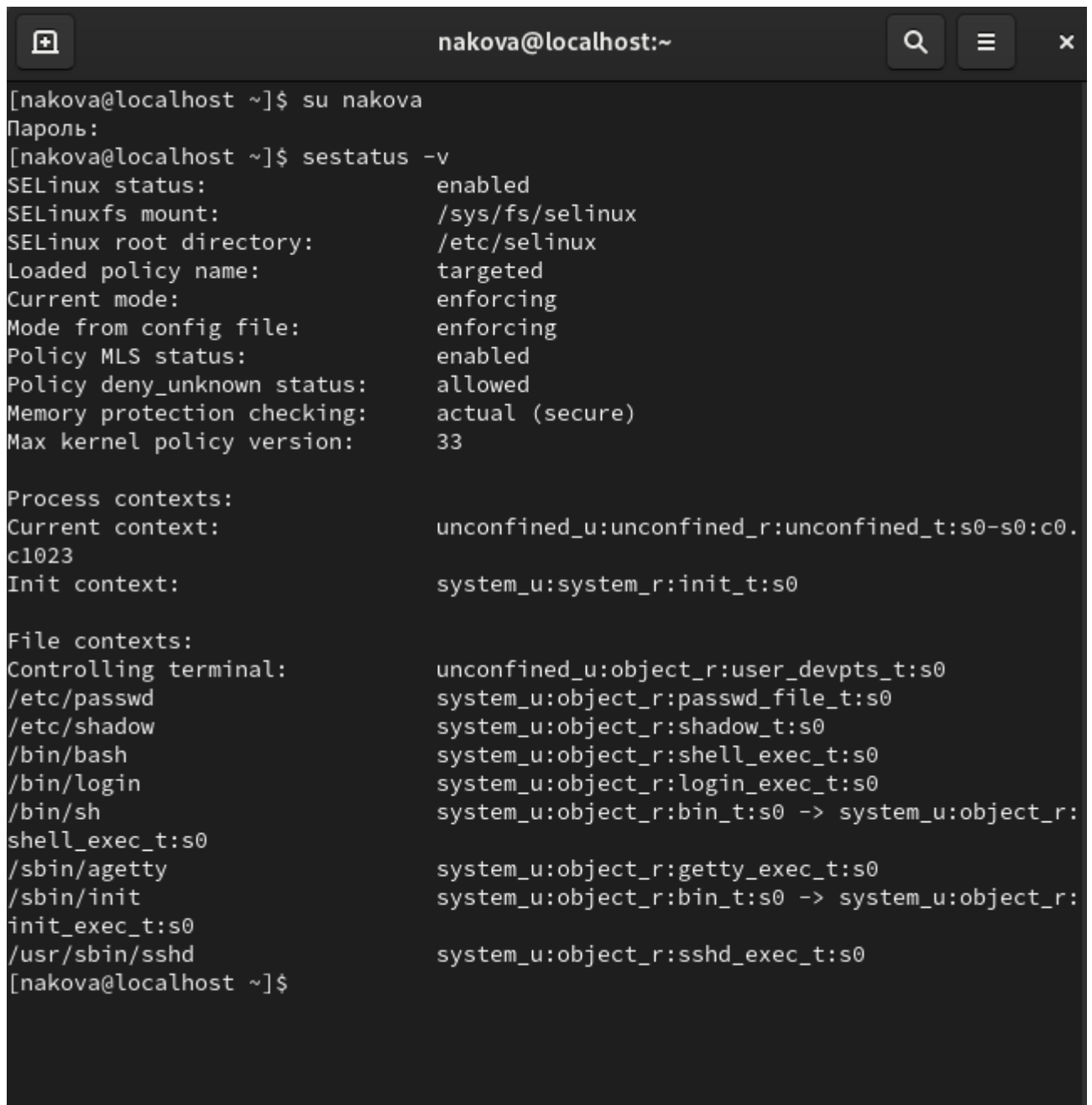
Во время загрузки системы мы получили предупреждающее сообщение о необходимости восстановления меток SELinux (Рис. 1.8):



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[ 0.053240] RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to
RETbleed attacks, data leaks possible!
[ 2.003700] Warning: Unmaintained hardware is detected: e1000:100E:8086 @ 00
00:00:03.0
[ 2.345088] [drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send host log me
ssage.
[ 8.409693] selinux-autorelabel[720]: *** Warning -- SELinux targeted policy relabel is required.
[ 8.409880] selinux-autorelabel[720]: *** Relabeling could take a very long time, depending on fi
le
[ 8.409995] selinux-autorelabel[720]: *** system size and speed of hard drives.
[ 8.420266] selinux-autorelabel[720]: Running: /sbin/fixfiles -T 0 restore
[ 21.942322] selinux-autorelabel[726]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts
/dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kernel/debug /sys/kernel/tracing
```

Рис. 1.8. 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 (Рис. 1.9):

A terminal window titled 'nakova@localhost:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
[nakova@localhost ~]$ su nakova
Пароль:
[nakova@localhost ~]$ 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

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:
shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:
init_exec_t:s0
/usr/sbin/sshd                system_u:object_r:sshd_exec_t:s0
[nakova@localhost ~]$
```

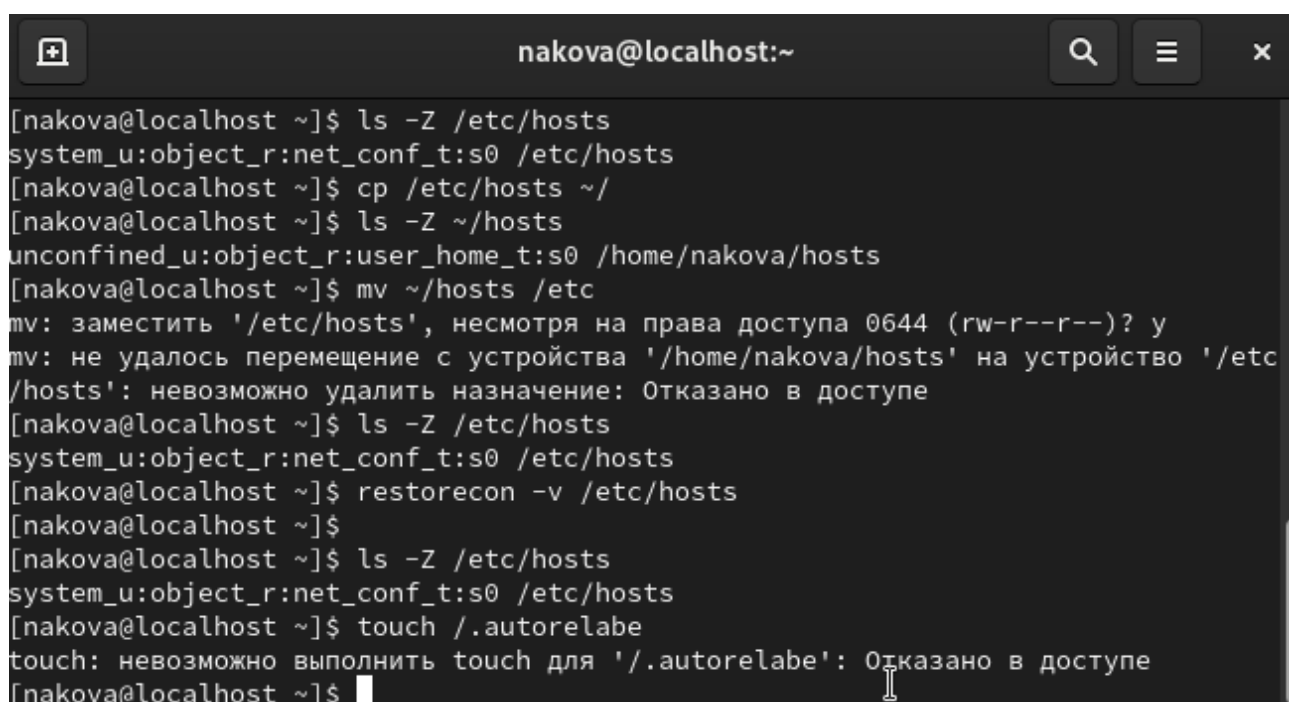
**Рис. 1.9.** Запуск терминала и получение полномочий администратора, просмотр текущей информации о состоянии SELinux.

### **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



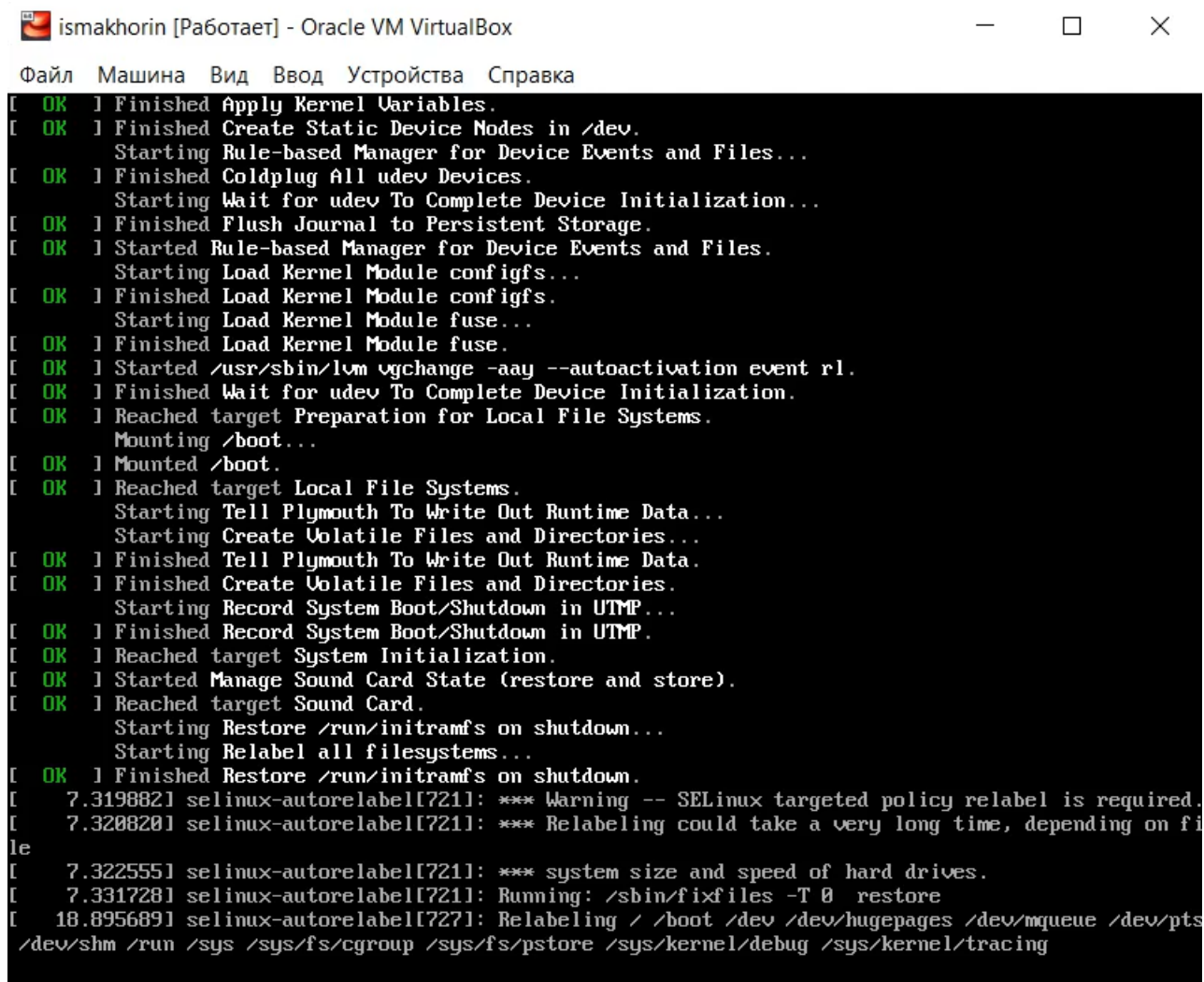
копирование считается созданием нового файла, то параметр контекста в файле `~/hosts`, расположенном в домашнем каталоге, стал `admin_home_t`. Попытаемся перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc`: **`mv ~/hosts /etc`** и подтвердим, что мы хотим сделать это. После 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. 2.1).



```
nakova@localhost:~  
[nakova@localhost ~]$ ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[nakova@localhost ~]$ cp /etc/hosts ~/  
[nakova@localhost ~]$ ls -Z ~/hosts  
unconfined_u:object_r:user_home_t:s0 /home/nakova/hosts  
[nakova@localhost ~]$ mv ~/hosts /etc  
mv: заместить '/etc/hosts', несмотря на права доступа 0644 (rw-r--r--)? у  
mv: не удалось перемещение с устройства '/home/nakova/hosts' на устройство '/etc/  
/hosts': невозможно удалить назначение: Отказано в доступе  
[nakova@localhost ~]$ ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[nakova@localhost ~]$ restorecon -v /etc/hosts  
[nakova@localhost ~]$  
[nakova@localhost ~]$ ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[nakova@localhost ~]$ touch /.autorelabel  
touch: невозможно выполнить touch для '/.autorelabel': Отказано в доступе  
[nakova@localhost ~]$
```

**Рис. 2.1.** 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 (Рис. 2.2).



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[ OK ] Finished Apply Kernel Variables.
[ OK ] Finished Create Static Device Nodes in /dev.
Starting Rule-based Manager for Device Events and Files...
[ OK ] Finished Coldplug All udev Devices.
Starting Wait for udev To Complete Device Initialization...
[ OK ] Finished Flush Journal to Persistent Storage.
[ OK ] Started Rule-based Manager for Device Events and Files.
Starting Load Kernel Module configs...
[ OK ] Finished Load Kernel Module configs.
Starting Load Kernel Module fuse...
[ OK ] Finished Load Kernel Module fuse.
[ 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 Create Volatile Files and Directories...
[ 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.
[ 7.319882] selinux-autorelabel[721]: *** Warning -- SELinux targeted policy relabel is required.
[ 7.320820] selinux-autorelabel[721]: *** Relabeling could take a very long time, depending on fi
le
[ 7.322555] selinux-autorelabel[721]: *** system size and speed of hard drives.
[ 7.331728] selinux-autorelabel[721]: Running: /sbin/fixfiles -T 0 restore
[ 18.895689] selinux-autorelabel[727]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts
/dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kernel/debug /sys/kernel/tracing
```

Рис. 2.2. 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 (Рис. 3.1):

```
dnf -y install httpd
```

```
dnf -y install lynx
```

```
Dependencies resolved.
=====
Package           Architecture      Version           Repository        Size
=====
Installing:
lynx               x86_64            2.8.9-19.el9      appstream         1.5 M
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-19.el9.x86_64.rpm                2.2 MB/s | 1.5 MB    00:00
-----
Total                                         1.2 MB/s | 1.5 MB    00:01
Running transaction check
Transaction check succeeded.
```

**Рис. 3.1.** 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. 3.2).

```
cd /web
# touch index.html
# mcedit index.html
```

**Рис. 3.2.** 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. 3.3).

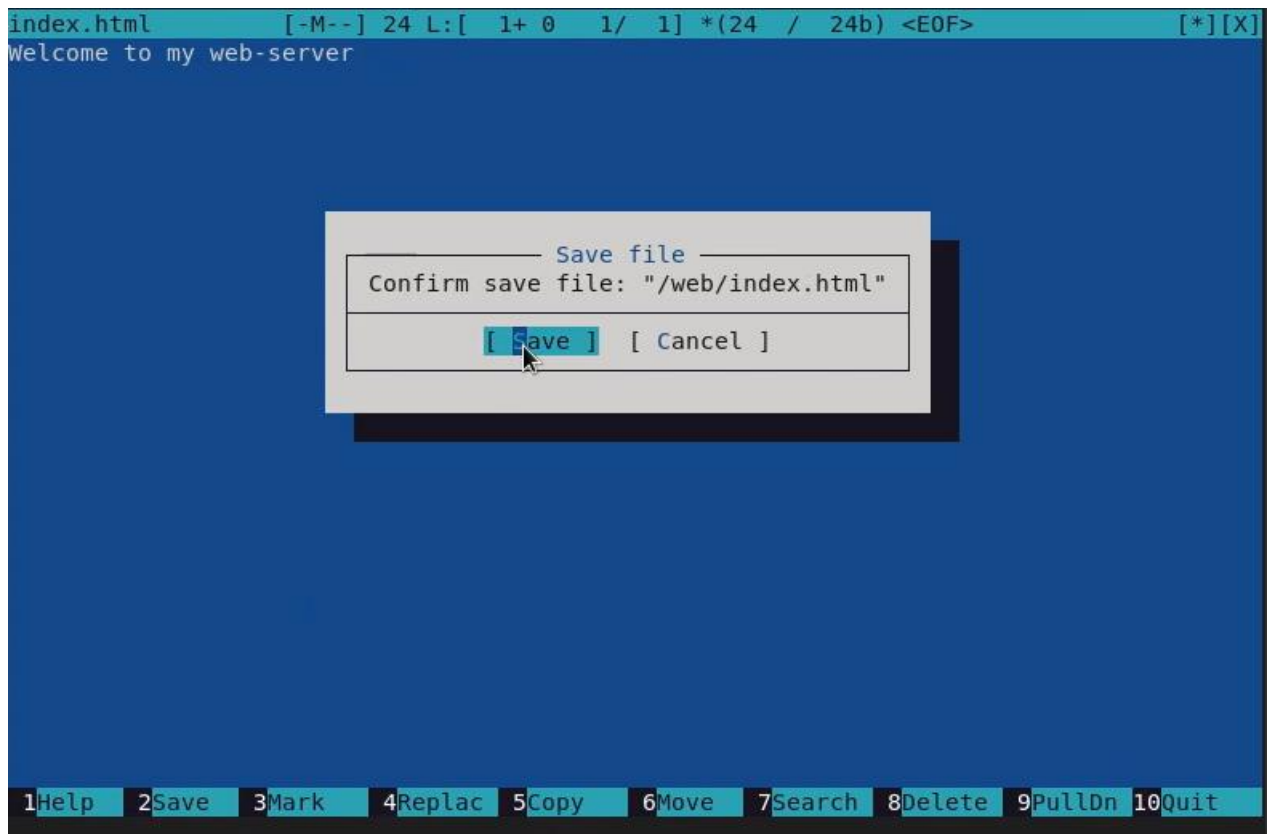


Рис. 3.3. Добавление текста в файл.

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>
```

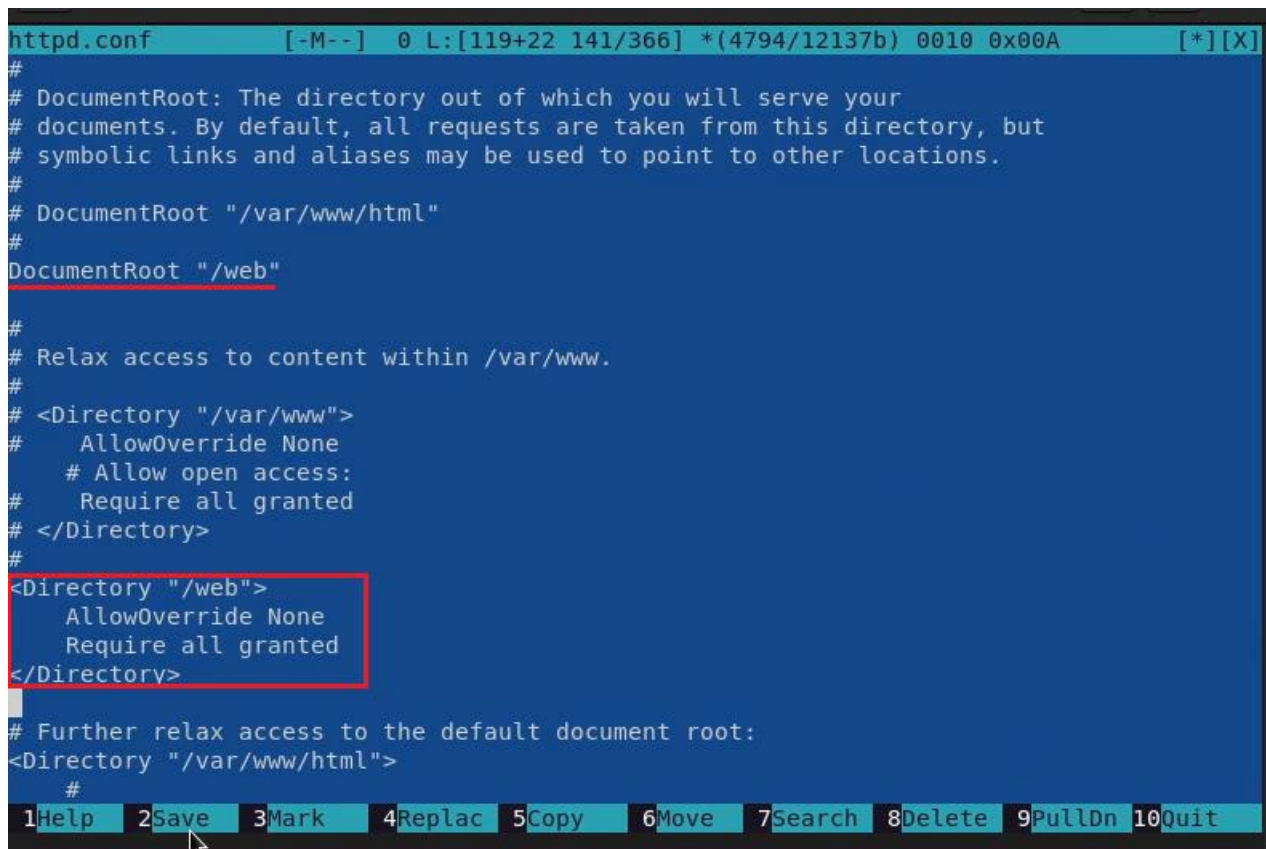
и добавим следующий раздел, определяющий правила доступа (Рис. 3.4):

```
<Directory "/web">
```

```
    AllowOverride None
```

```
    Require all granted
```

`</Directory>`



```
httpd.conf [-M--] 0 L:[119+22 141/366] *(4794/12137b) 0010 0x00A [*][X]
#
# DocumentRoot: The directory out of which you will serve your
# 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">
    #
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

**Рис. 3.4.** Комментирование строки и добавление ниже другой.

Комментирование раздела и добавление следующего, определяющего правила доступа.

Запустим веб-сервер и службу httpd (Рис. 3.5).:

**systemctl start httpd**

**systemctl enable httpd**



```
systemctl start httpd
systemctl enable httpd
```

### Рис. 3.5. 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. 3.6).


A terminal window with a dark background. The prompt '\$' is followed by the text 'lynx http://localhost' and a cursor is at the end of the line.

Рис. 3.6. 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. 3.7).

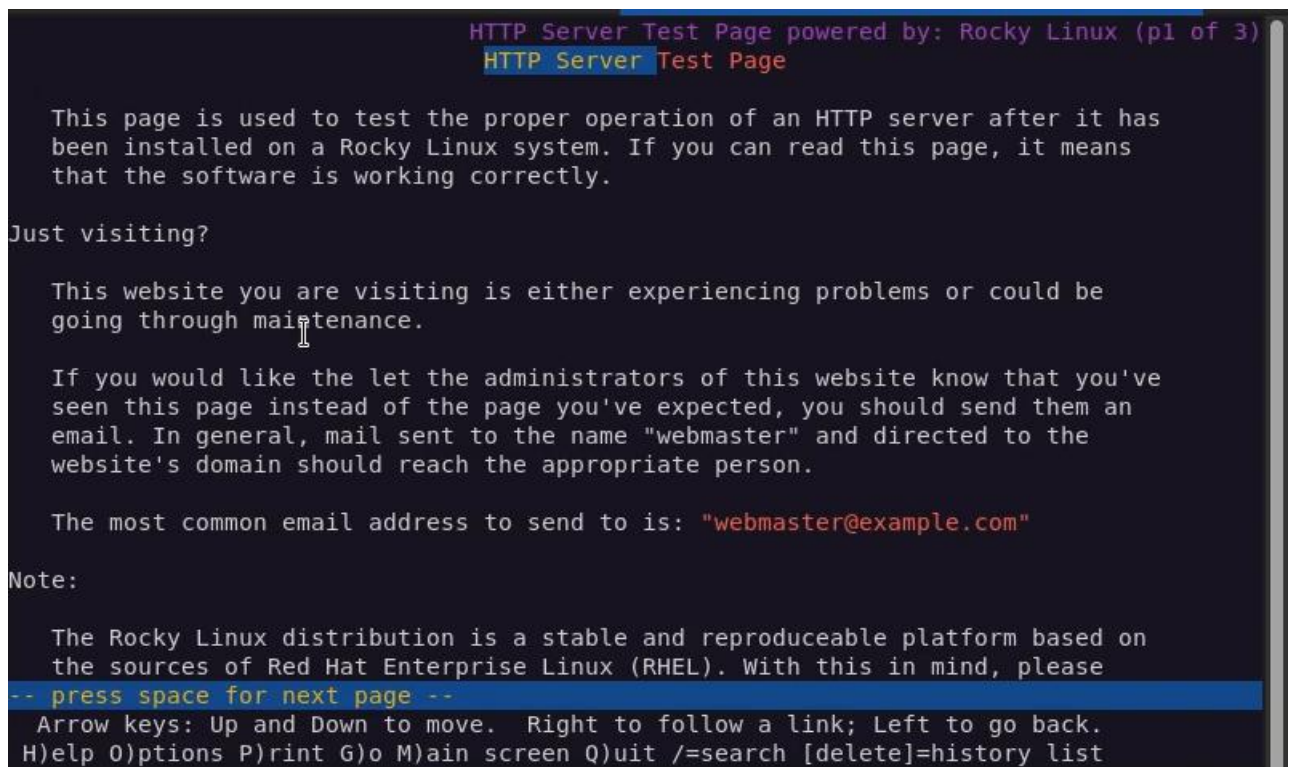
A screenshot of a terminal window showing the Lynx web browser. The title bar at the top says 'HTTP Server Test Page powered by: Rocky Linux (p1 of 3)'. The main content area displays the 'HTTP Server Test Page' with a message about testing the HTTP server operation. It asks 'Just visiting?' and provides instructions on how to contact the webmaster. At the bottom, there is a 'Note' section about the Rocky Linux distribution. A blue highlight bar is visible at the bottom of the terminal window, containing the text '-- press space for next page --'. The bottom of the terminal shows navigation instructions: 'Arrow keys: Up and Down to move. Right to follow a link; Left to go back. H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list'.

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

В терминале с полномочиями администратора переключите SELinux в разрешающий режим: **setenforce 0** и выполняем перезагрузку системы (Рис. 3.8).



```
# setenforce 0
# reboot
```

A terminal window with a dark background. The first line shows the command `# setenforce 0` and the second line shows `# reboot` followed by a cursor.

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

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу: **lynx http://localhost** (Рис. 3.9).



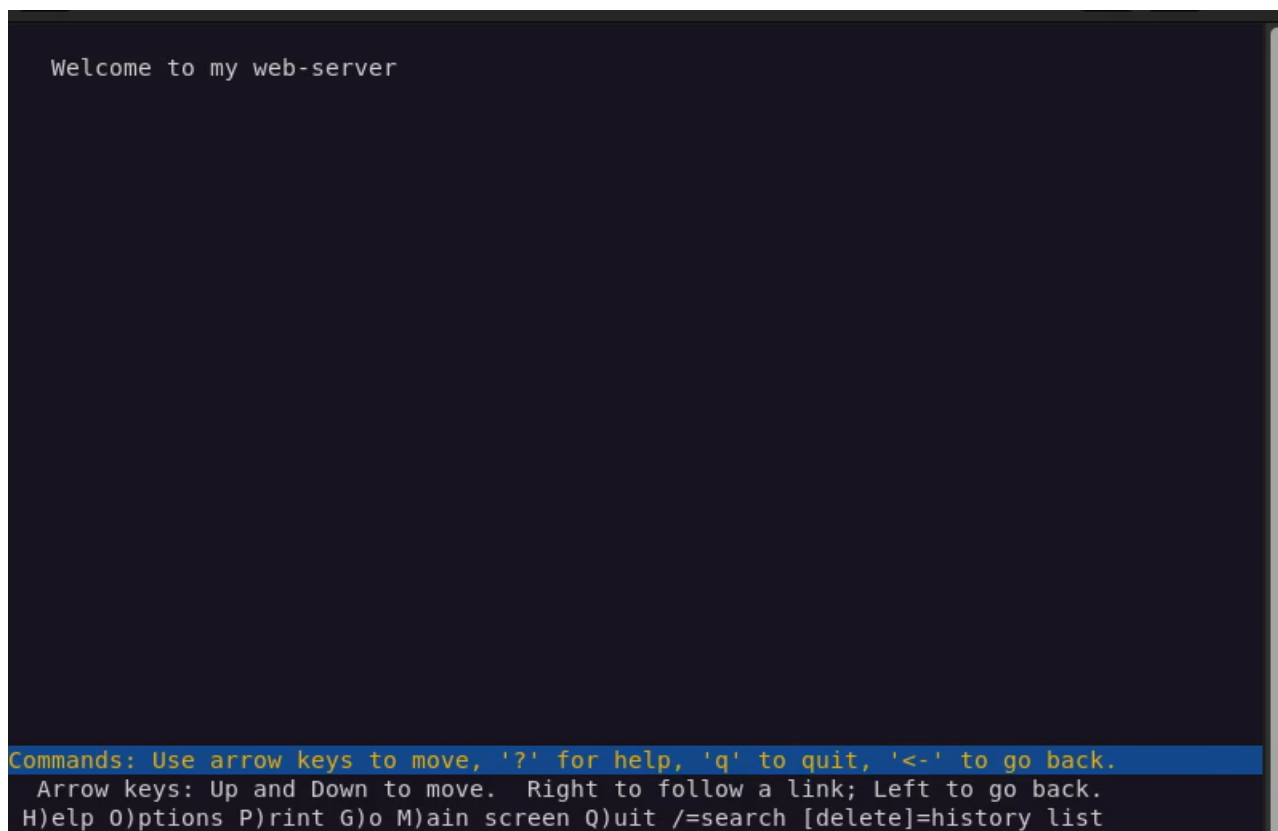
```
$ lynx http://localhost
```

A terminal window with a dark background. The prompt is `$` and the command `lynx http://localhost` has been entered, with a cursor at the end.

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

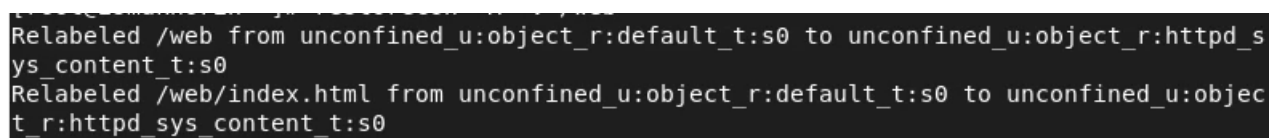
Теперь мы получили доступ к своей пользовательской веб-странице. Это показывает, что SELinux делает что-то для блокировки доступа. Выйдем из lynx (Рис. 3.10).





**Рис. 3.10.** Получение доступа к своей пользовательской веб-странице, 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** (Рис. 3.11). Теперь установим SELinux в режим принудительного исполнения: **setenforce 1**. После чего перезагрузим систему (Рис. 3.12).



**Рис. 3.11.** Применение новой метки контекста к /web, восстановление контекста безопасности.



```
# setenforce 1
# reboot
```

**Рис. 3.12.** Установка SELinux в режим принудительного исполнения, перезагрузка системы.

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу (Рис. 3.13): **lynx http://localhost**. Теперь мы получили доступ к своей пользовательской веб-странице (Рис. 3.14).

```
$ lynx http://localhost
$
```

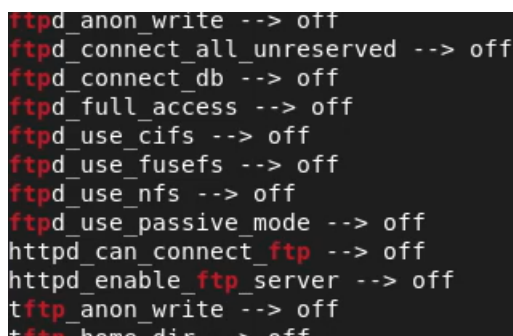
**Рис. 3.13.** Открытие терминала под учётной записью своего пользователя, повторное обращение к веб-серверу в текстовом браузере lynx.



**Рис. 3.14.** 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`) (Рис. 4).



```
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
+ftpd_anon_write --> off
+ftpd_home_dir --> off
```

**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 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**

```
~]# setenforce 0
```

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? **getsebool -a**

```
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
colord_use_nfs --> off
condor_tcp_network_connect --> off
conman_can_network --> off
conman_use_nfs --> off
container_connect_any --> off
container_manage_cgroup --> off
```

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? **audit2allow**

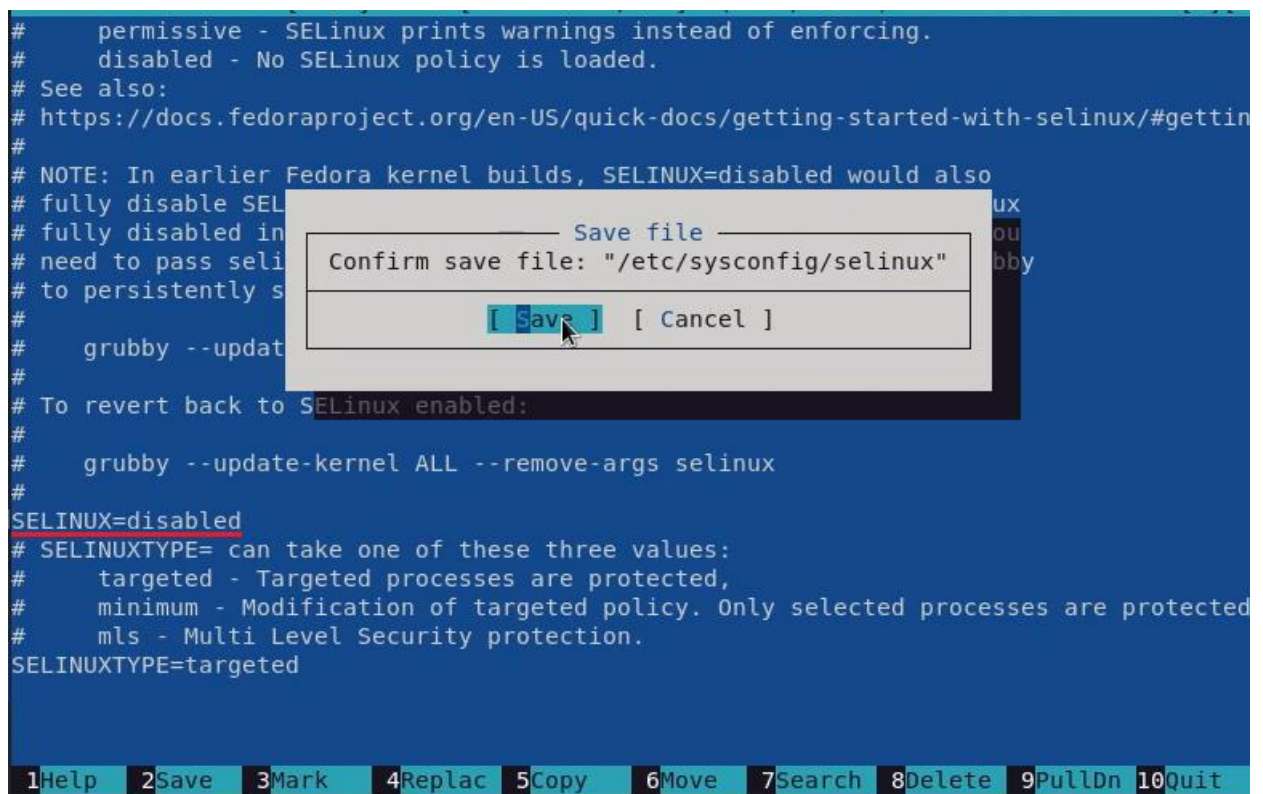
4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

```
restorecon -R -v /web
```

```
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_u:object_r:httpd_sys_content_t:s0
```

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`

```

audit.log      [----]  0 L:[ 1+ 0    1/6931] *(0    /1577473b) 0116 0x074    [*][X]
type=DAEMON START msg=audit(1668207101.317:1741): op=start ver=3.0.7 format=enriched ke
type=SERVICE_START msg=audit(1668207101.346:5): pid=1 uid=0 auid=4294967295 ses=4294967
type=CONFIG_CHANGE msg=audit(1668207101.373:6): op=set audit_backlog_limit=8192 old=64
type=SYSCALL msg=audit(1668207101.373:6): arch=c000003e syscall=44 success=yes exit=60
type=PROCTITLE msg=audit(1668207101.373:6): proctitle=2F7362696E2F617564697463746C002D5
type=CONFIG_CHANGE msg=audit(1668207101.373:7): op=set audit_failure=1 old=1 auid=42949
type=SYSCALL msg=audit(1668207101.373:7): arch=c000003e syscall=44 success=yes exit=60
type=PROCTITLE msg=audit(1668207101.373:7): proctitle=2F7362696E2F617564697463746C002D5
type=CONFIG_CHANGE msg=audit(1668207101.373:8): op=set audit_backlog_wait_time=60000 ol
type=SYSCALL msg=audit(1668207101.373:8): arch=c000003e syscall=44 success=yes exit=60
type=PROCTITLE msg=audit(1668207101.373:8): proctitle=2F7362696E2F617564697463746C002D5
type=SERVICE_START msg=audit(1668207101.375:9): pid=1 uid=0 auid=4294967295 ses=4294967
type=SYSTEM_BOOT msg=audit(1668207101.387:10): pid=734 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207101.390:11): pid=1 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207101.770:12): pid=1 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207101.781:13): pid=1 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207101.798:14): pid=1 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207101.800:15): pid=1 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207101.807:16): pid=1 uid=0 auid=4294967295 ses=429496
type=BPF msg=audit(1668207101.980:17): prog-id=28 op=LOAD
type=BPF msg=audit(1668207101.984:18): prog-id=29 op=LOAD
type=BPF msg=audit(1668207101.985:19): prog-id=30 op=LOAD
type=BPF msg=audit(1668207102.010:20): prog-id=31 op=LOAD
type=BPF msg=audit(1668207102.015:21): prog-id=32 op=LOAD
type=SERVICE_START msg=audit(1668207102.042:22): pid=1 uid=0 auid=4294967295 ses=429496
type=SERVICE_START msg=audit(1668207102.053:23): pid=1 uid=0 auid=4294967295 ses=429496
1Help  2Save  3Mark  4Replac  5Copy  6Move  7Search  8Delete  9PullDn 10Quit

```

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? **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
tftpd_anon_write --> off
tftpd_home_dir --> off

```

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.