

Отчёт по лабораторной работе №9

Управление SELinux

Тукаев Тимур

Содержание

1 Цель работы	5
2 Выполнение	6
2.1 Управление режимами SELinux	6
2.2 Использование restorecon для восстановления контекста безопасности	10
2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	11
2.4 Работа с переключателями SELinux	13
3 Контрольные вопросы	15
4 Заключение	16

Список иллюстраций

2.1	Переход в режим суперпользователя и просмотр состояния SELinux	6
2.2	Редактирование файла конфигурации SELinux	7
2.3	Проверка отключённого состояния SELinux	8
2.4	Повторное включение SELinux через конфигурационный файл . .	8
2.5	Сообщение о восстановлении меток безопасности при загрузке . .	9
2.6	Подтверждение восстановления работы SELinux в режиме enforcing	9
2.7	Использование restorecon и autorelabel для восстановления контек- стов безопасности	10
2.8	Создание каталога и файла веб-страницы	11
2.9	Редактирование конфигурационного файла httpd.conf	11
2.10	Отображение стандартной страницы Rocky Linux	12
2.11	Применение контекста безопасности к каталогу /web	13
2.12	Проверка работы веб-сервера с новым контентом	13
2.13	Настройка переключателя SELinux для службы FTP	14

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение

2.1 Управление режимами SELinux

- Получены права администратора с помощью команды su.

После ввода пароля произведён переход в контекст суперпользователя.

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# 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
/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
root@titukaev:/home/titukaev# getenforce
Enforcing
root@titukaev:/home/titukaev# setenforce 0
root@titukaev:/home/titukaev# getenforce
Permissive
root@titukaev:/home/titukaev#
```

Рис. 2.1: Переход в режим суперпользователя и просмотр состояния SELinux

Команда `sestatus -v` показала, что SELinux включён (enabled) и работает в режиме принудительного контроля доступа (enforcing).

Из вывода видно, что используется политика *targeted*, конфигурация загружена из файла `/etc/selinux/config`, а все процессы и файлы имеют назначенные контексты безопасности.

2. Проверено текущее состояние SELinux командой `getenforce`.

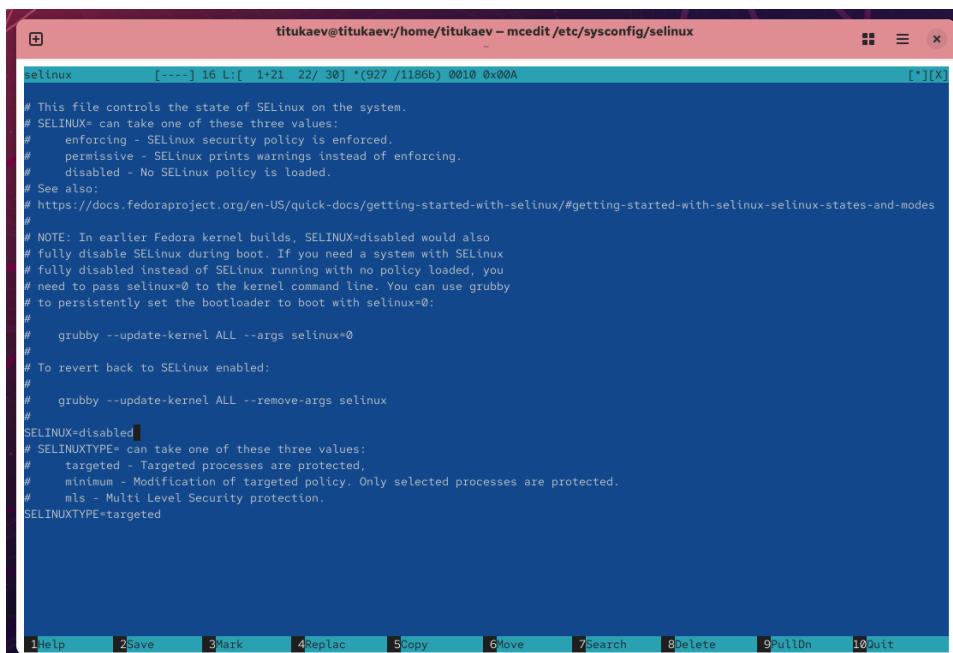
Система находится в режиме Enforcing.

3. Режим SELinux изменён на разрешающий (Permissive) с помощью `setenforce 0`.

После проверки через `getenforce` подтверждено, что режим изменился.

В этом режиме SELinux не блокирует действия, но фиксирует их в логах.

4. Открыт файл `/etc/sysconfig/selinux` и изменено значение параметра `SELINUX` на `disabled`, что полностью отключает SELinux после перезагрузки.



```
titukaev@titukaev:~ - mcedit /etc/sysconfig/selinux
[---] 16 L:[ 1+21 22/ 30 ] *(927 /1186b) $010 0x00A [*][X]

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux-states-and-modes
#
# NOTE: In earlier Fedora kernel builds, 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 grub2
# to persistently set the bootloader to boot with selinux=0:
#
#   grub2 --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grub2 --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. 2.2: Редактирование файла конфигурации SELinux

5. После перезагрузки системы и повторного входа с правами администратора проверено состояние SELinux командой `getenforce`.

Вывод `Disabled` подтверждает, что SELinux отключён.

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# getenforce
Disabled
root@titukaev:/home/titukaev# setenforce 1
setenforce: SELinux is disabled
root@titukaev:/home/titukaev#
```

Рис. 2.3: Проверка отключённого состояния SELinux

6. Попытка включить SELinux без перезагрузки (`setenforce 1`) завершилась сообщением «SELinux is disabled».

Это подтверждает, что смена режима невозможна при полном отключении механизма.

7. В файле `/etc/sysconfig/selinux` параметр изменён обратно на `SELINUX=enforcing`.

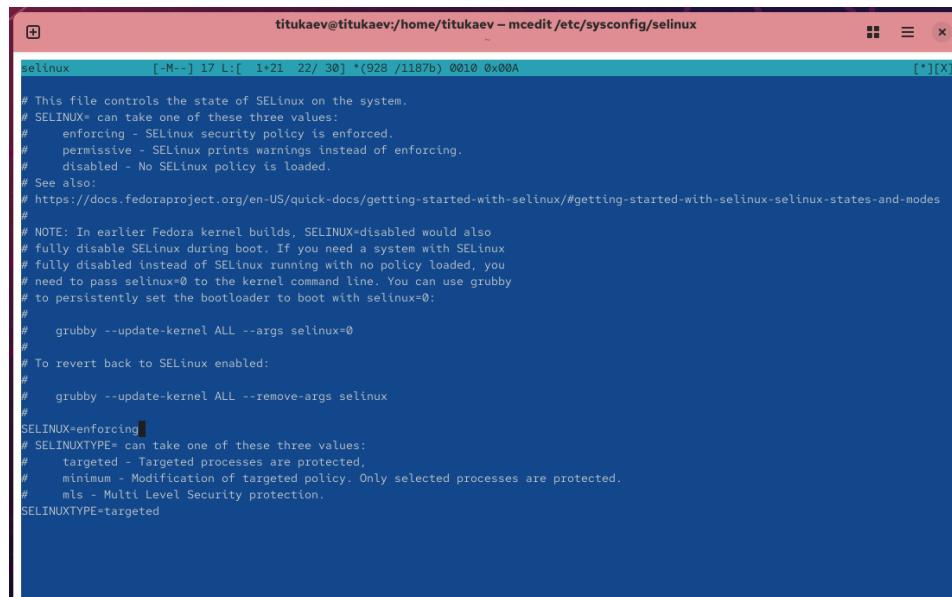


Рис. 2.4: Повторное включение SELinux через конфигурационный файл

8. После перезагрузки система выдала предупреждение о необходимости восстановления меток безопасности (relabeling) для корректного применения

политик SELinux.

```
Booting `Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'

[ 1.785036] vmmqfx 0000:00:02.0: [drm] *ERROR* vmmqfx seems to be running on
an unsupported hypervisor
[ 1.785038] vmmqfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.785039] vmmqfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 10.881428] selinux-autorelabel[858]: *** Warning -- SELinux targeted policy relabel is required.
[ 10.881513] selinux-autorelabel[858]: *** Relabeling could take a very long time, depending on file
[ 10.881664] selinux-autorelabel[858]: *** system size and speed of hard drives.
[ 10.892671] selinux-autorelabel[858]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.5: Сообщение о восстановлении меток безопасности при загрузке

9. После завершения relabeling и загрузки ОС повторно выполнена проверка состояния SELinux через `sestatus -v`.

Система снова работает в режиме enforcing.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# 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
/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
root@titukaev:/home/titukaev#
```

Рис. 2.6: Подтверждение восстановления работы SELinux в режиме enforcing

2.2 Использование restorecon для восстановления контекста безопасности

- Проверен контекст безопасности файла `/etc/hosts` с помощью `ls -Z /etc/hosts`.

Файл имеет контекст `net_conf_t`.

- Файл скопирован в домашний каталог командой `cp /etc/hosts ~/`.
При копировании контекст изменился на `admin_home_t`, так как файл создан в пользовательской области.
- При попытке заменить оригинальный файл `/etc/hosts` командой `mv ~/hosts /etc` контекст остался `admin_home_t`, что не соответствует системному стандарту.
- Для восстановления корректного контекста использована команда `restorecon -v /etc/hosts`.

Она автоматически вернула файлу правильный контекст `net_conf_t`.

- Проверка подтвердила успешное восстановление.

Для массового исправления контекстов безопасности создан файл `/.autorelabel`.

После перезагрузки система автоматически перемарковала все файлы.

```
root@titukaev:/home/titukaev# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@titukaev:/home/titukaev# cp /etc/hosts ~/
root@titukaev:/home/titukaev# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@titukaev:/home/titukaev# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@titukaev:/home/titukaev# touch /.autorelabel
root@titukaev:/home/titukaev#
```

Рис. 2.7: Использование `restorecon` и `autorelabel` для восстановления контекстов безопасности

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

- Получены права администратора с помощью команды su.

Установлены необходимые пакеты `httpd` и `lynx` для запуска веб-сервера и проверки его работы в текстовом браузере.

- Создан новый каталог `/web` для хранения файлов веб-сервера.

В нём создан файл `index.html` с содержимым:

```
[ 0.691821] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.691823] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.691824] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 9.150172] selinux-autorelabel[857]: *** Warning -- SELinux targeted policy relabel is required.
[ 9.150236] selinux-autorelabel[857]: *** Relabeling could take a very long time, depending on file
[ 9.150261] selinux-autorelabel[857]: *** system size and speed of hard drives.
[ 9.162208] selinux-autorelabel[857]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.8: Создание каталога и файла веб-страницы

- В файле `/etc/httpd/conf/httpd.conf` закомментирована строка `DocumentRoot "/var/www/html"` и добавлена новая — `DocumentRoot "/web"`.

Также изменён раздел `<Directory>` для указания новых прав доступа.

```
# 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"

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

Рис. 2.9: Редактирование конфигурационного файла `httpd.conf`

4. Служба `httpd` запущена и добавлена в автозагрузку.

После запуска при обращении к серверу через `lynx http://localhost` открылась стандартная тестовая страница Rocky Linux, что говорит о том, что контекст безопасности SELinux пока не позволяет серверу обращаться к новому каталогу `/web`.

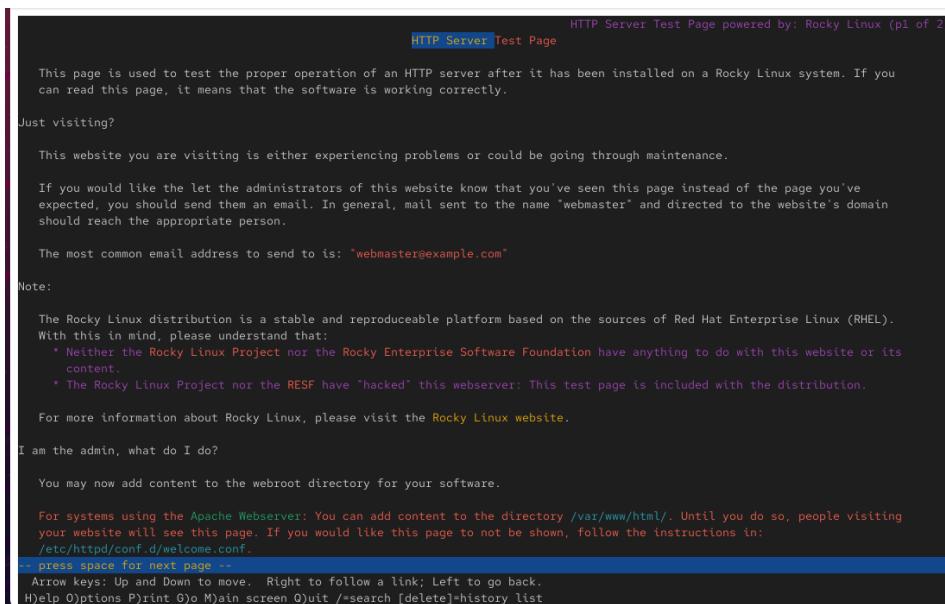


Рис. 2.10: Отображение стандартной страницы Rocky Linux

5. Для корректного доступа веб-сервера к каталогу `/web` назначен соответствующий контекст безопасности SELinux:

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

а затем выполнено восстановление контекста `restorecon -R -v /web`.

После изменения контекста система сообщила, что файлы были успешно перелabelированы.

```

Installed:
lynx-2.9.0-6.el10.x86_64

Complete!
root@titukaev:/home/titukaev# mkdir /web
root@titukaev:/home/titukaev# cd /web
root@titukaev:/web# touch index.html
root@titukaev:/web# echo "Welcome yo my web-server" > index.html
root@titukaev:/web# mcedit /etc/httpd/conf/httpd.conf

root@titukaev:/web# systemctl start httpd
root@titukaev:/web# systemctl enable httpd
root@titukaev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@titukaev:/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
root@titukaev:/web#

```

Рис. 2.11: Применение контекста безопасности к каталогу /web

- При повторном обращении к серверу через браузер lynx отображается созданная страница с текстом «Welcome to my web-server», что подтверждает правильную настройку SELinux для нестандартного каталога веб-контента.



Рис. 2.12: Проверка работы веб-сервера с новым контентом

2.4 Работа с переключателями SELinux

- Получены права администратора и просмотрены текущие параметры SELinux для служб, связанных с FTP, с помощью команды `getsebool -a | grep ftp`.
Определено, что переключатель `ftpd_anon_write` имеет состояние `off`.
- С помощью команды `semanage boolean -l | grep ftpd_anon` получена информация о назначении данного переключателя — он отвечает за разрешение

ние анонимной записи через FTP.

3. Временное включение параметра выполнено командой `setsebool ftpd_anon_write on`.

После проверки через `getsebool ftpd_anon_write` его значение изменилось на `on`.

4. Для сохранения изменения после перезагрузки параметр был включён постоянно командой `setsebool -P ftpd_anon_write on`.

Повторная проверка показала, что теперь флаг `ftpd_anon_write` включён как во временном, так и в постоянном состоянии.

```
titukaev@titukaev:~$  
titukaev@titukaev:~$ su  
Password:  
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# 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  
ftpd_anon_write --> off  
ftpd_home_dir --> off  
root@titukaev:/home/titukaev# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (off , off) Allow ftpd to anon write  
root@titukaev:/home/titukaev# setsebool ftpd_anon_write on  
root@titukaev:/home/titukaev# getsebool ftpd_anon_write  
ftpd_anon_write --> on  
root@titukaev:/home/titukaev# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (on , off) Allow ftpd to anon write  
root@titukaev:/home/titukaev# setsebool -P ftpd_anon_write on  
root@titukaev:/home/titukaev# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (on , on) Allow ftpd to anon write  
root@titukaev:/home/titukaev#
```

Рис. 2.13: Настройка переключателя SELinux для службы FTP

3 Контрольные вопросы

1. Для временного перевода SELinux в разрешающий режим используется команда `setenforce 0`.
2. Для просмотра списка всех доступных переключателей SELinux применяется команда `getsebool -a`.
3. Для получения человекочитаемых сообщений журнала SELinux необходимо установить пакет `setroubleshoot`.
4. Для применения типа контекста `httpd_sys_content_t` к каталогу `/web` выполняются команды:
`semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`
и
`restorecon -R -v /web.`
5. Чтобы полностью отключить SELinux, необходимо изменить параметр `SELINUX=disabled` в файле `/etc/sysconfig/selinux`.
6. SELinux регистрирует свои сообщения в файле `/var/log/audit/audit.log`.
7. Для получения информации о доступных типах контекстов для службы FTP используется команда `semanage fcontext -l | grep ftp`.
8. Чтобы определить, связано ли поведение сервиса с SELinux, можно воспользоваться утилитой `setroubleshoot` или командой `sealert -a /var/log/audit/audit.log`, которая анализирует журнал аудита и выдаёт рекомендации.

4 Заключение

В ходе лабораторной работы были изучены механизмы управления системой безопасности SELinux и её взаимодействие с сервисами Linux.

Были рассмотрены режимы работы SELinux – принудительный (Enforcing), разрешающий (Permissive) и отключённый (Disabled).

В процессе выполнения лабораторных заданий освоены приёмы изменения режима работы SELinux, редактирования конфигурационного файла `/etc/sysconfig/selinux`, а также восстановления контекстов безопасности с помощью команд `restorecon` и `semanage`.

Особое внимание уделено настройке контекстов безопасности для нестандартного расположения веб-контента и управлению переключателями SELinux.

Полученные навыки позволяют администратору корректно конфигурировать систему доступа и обеспечивать безопасную работу сервисов в среде Linux.