

Отчёт по лабораторной работе №9

Управление SELinux

Агдjabекова Эся Рустамовна

Содержание

1 Цель работы	5
2 Ход выполнения работы	6
2.1 Управление режимами SELinux	6
2.2 Использование restorecon для восстановления контекста безопасности	9
2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	10
2.4 Работа с переключателями SELinux	12
3 Контрольные вопросы	14
4 Заключение	16

Список иллюстраций

2.1 Проверка текущего состояния SELinux	6
2.2 Переключение режима SELinux в Permissive	7
2.3 Отключение SELinux в конфигурационном файле	7
2.4 Попытка включить SELinux после отключения	8
2.5 Процесс relabeling при включении SELinux	8
2.6 Проверка состояния SELinux после восстановления	9
2.7 Восстановление контекста безопасности с помощью restorecon	10
2.8 Изменение конфигурационного файла httpd.conf для новой директории	11
2.9 Отображение стандартной тестовой страницы Apache	11
2.10 Применение меток безопасности для каталога /web	12
2.11 Отображение пользовательской страницы веб-сервера	12
2.12 Настройка переключателя SELinux для службы FTP	13

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Ход выполнения работы

2.1 Управление режимами SELinux

1. Запущен терминал и получены права администратора с помощью команды su.

Проверена текущая информация о состоянии SELinux командой sestatus -v (см. рис. fig. 2.1).

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

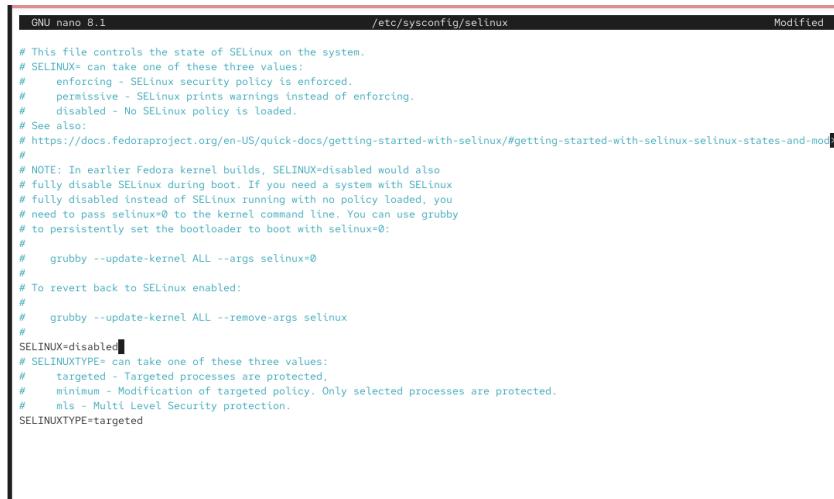
Рис. 2.1: Проверка текущего состояния SELinux

2. Определено, что SELinux включён, политика безопасности установлена в режиме enforcing, а политика по умолчанию — targeted.

Это означает, что SELinux активно контролирует доступ процессов и применяет правила безопасности к целевым службам.

3. Для проверки текущего режима работы выполнена команда getenforce, показавшая значение Enforcing.

Режим изменён на Permissive командой setenforce 0, затем снова выполнена getenforce, подтвердившая переключение режима (см. рис. fig. 2.2).



```
GNU nano 8.1 /etc/sysconfig/selinux Modified

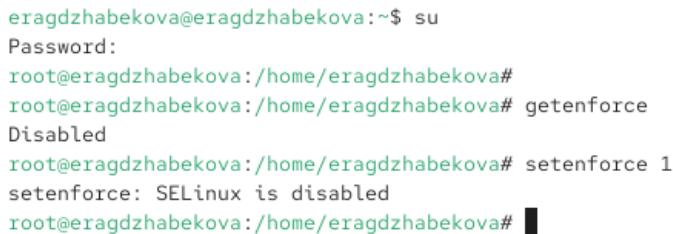
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux-states-and-mod
#
# 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 grubpy
# to persistently set the bootloader to boot with selinux=0:
#
#   grubpy --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubpy --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: Переключение режима SELinux в Permissive

4. С помощью текстового редактора nano открыт и изменён файл /etc/sysconfig/selinux.

В параметре SELINUX установлено значение disabled.

После этого система была перезагружена (см. рис. fig. 2.3).



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

Рис. 2.3: Отключение SELinux в конфигурационном файле

5. После перезапуска системы снова получены права администратора и вы-

полнена команда getenforce, показавшая, что SELinux теперь отключён.

Попытка переключить режим командой setenforce 1 завершилась сообщением, что SELinux отключён и изменить режим невозможно без перезагрузки (см. рис. fig. 2.4).

```
GNU nano 8.1          /etc/sysconfig/selinux          Modified

# 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-
#
# 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 grubpy
# to persistently set the bootloader to boot with selinux=0:
#
#   grubpy --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubpy --update-kernel ALL --remove-args selinux
#
# SELINUXTYPE=enforcing
# 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. 2.4: Попытка включить SELinux после отключения

6. Для восстановления работы SELinux файл /etc/sysconfig/selinux снова отредактирован, установлено значение enforcing.

После сохранения изменений и перезагрузки система начала процесс relabeling – восстановление контекстов безопасности (см. рис. fig. 2.5).

```
Booting 'Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'
[    0.791357] vmmqfx 0000:00:02.0: [drm] *ERROR* vmmqfx seems to be running on
an unsupported hypervisor.
[    0.791359] vmmqfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[    0.791360] vmmqfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[    4.131121] selinux-autorelabel[1789]: *** Warning -- SELinux targeted policy relabel is required.
[    4.131172] selinux-autorelabel[1789]: *** Relabeling could take a very long time, depending on file
size and speed of hard drives.
[    4.131124] selinux-autorelabel[1789]: *** system size and speed of hard drives.
[    4.134656] selinux-autorelabel[1789]: Running: /sbin/fixfiles -T 0 restore
[    7.008596] selinux-autorelabel[1787]: Warning: Skipping the following R/O filesystems:
[    7.008599] selinux-autorelabel[1787]: /run/credentials/systemd-journal.service
[    7.008591] selinux-autorelabel[1787]: Relabeling /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup
[    7.008591] /debug /sys/kernel/tracing
```

Рис. 2.5: Процесс relabeling при включении SELinux

7. После повторной загрузки в терминале проверено состояние SELinux командой sestatus -v.

Система снова работает в режиме enforcing, что подтверждает успешное восстановление политики безопасности (см. рис. fig. 2.6).

```
eragdzhabekova@eragdzhabekova:~$ su
Password:
root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova#
```

Рис. 2.6: Проверка состояния SELinux после восстановления

2.2 Использование restorecon для восстановления

контекста безопасности

1. Получены права администратора. Проверен контекст безопасности файла /etc/hosts командой ls -Z, который имел тип net_conf_t.
2. Файл /etc/hosts скопирован в домашний каталог, где его контекст изменился на admin_home_t.
3. При перемещении файла обратно в каталог /etc контекст сохранился неверным (admin_home_t).
4. Для восстановления корректного контекста выполнена команда restorecon -v /etc/hosts, после чего тип контекста вновь стал net_conf_t.

5. Для массового восстановления меток безопасности создан пустой файл `/.autorelabel`, который инициирует полное перемаркирование при следующей загрузке (см. рис. fig. 2.7).

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

Рис. 2.7: Восстановление контекста безопасности с помощью restorecon

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Запущен терминал и получены права администратора. Установлены необходимые пакеты `httpd` и `lynx`.
2. Создан каталог `/web`, предназначенный для размещения файлов веб-сервера, и внутри него создан файл `index.html` с содержимым «Welcome to my web server».
3. В конфигурационном файле `/etc/httpd/conf/httpd.conf` закомментированы строки, указывающие на стандартный каталог `/var/www/html`, и добавлены новые параметры `DocumentRoot "/web"` и раздел `Directory "/web"` с разрешенным доступом ко всем пользователям (см. рис. fig. 2.8).

```

GNU nano 8.1                               /etc/httpd/conf/httpd.conf

</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# 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. 2.8: Изменение конфигурационного файла httpd.conf для новой директории

- После сохранения изменений веб-сервер запущен и добавлен в автозагрузку.

При обращении к серверу через браузер lynx по адресу `http://localhost` отображается стандартная страница Rocky Linux (см. рис. fig. 2.9).

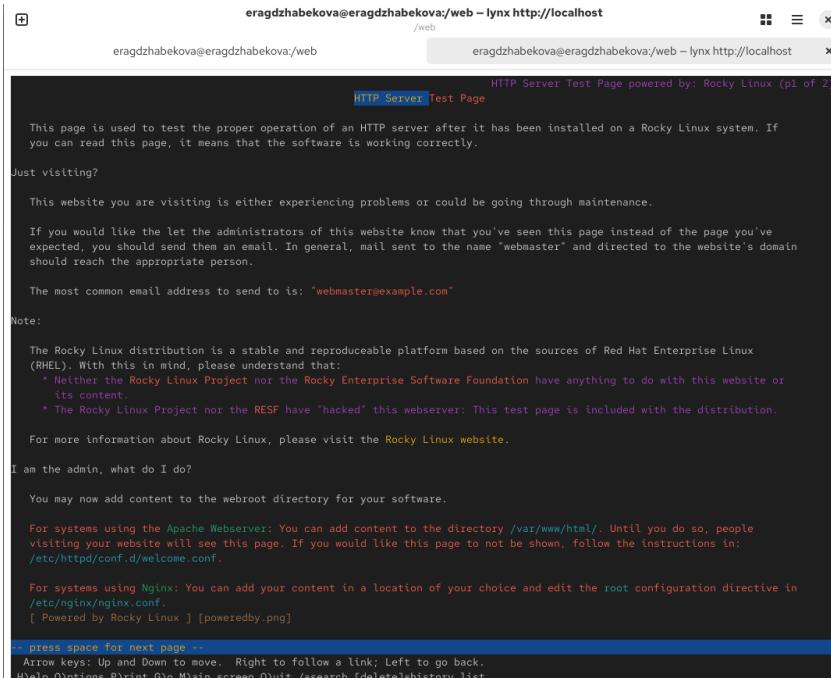


Рис. 2.9: Отображение стандартной тестовой страницы Apache

- Для корректной работы веб-сервера с новым каталогом применена новая метка контекста безопасности, после чего контексты восстановлены с помощью restorecon. Это обеспечило доступ службы httpd к файлам в каталоге /web (см. рис. fig. 2.10).

```

root@eragdzhabekova:/home/eragdzhabekova# mkdir /web
root@eragdzhabekova:/home/eragdzhabekova# cd /web
root@eragdzhabekova:/# touch index.html
root@eragdzhabekova:/# echo "Welcome to my web server" > index.html
root@eragdzhabekova:/# nano /etc/httpd/conf/httpd.conf
root@eragdzhabekova:/# 
root@eragdzhabekova:/# systemctl start httpd
root@eragdzhabekova:/# systemctl enable
Too few arguments.
root@eragdzhabekova:/# systemctl enable httpd
root@eragdzhabekova:/# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@eragdzhabekova:/# 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@eragdzhabekova:/# 

```

Рис. 2.10: Применение меток безопасности для каталога /web

- После изменения контекста и перезапуска службы веб-сервера при повторном обращении через lynx отображается созданная страница с сообщением «Welcome to my web server» (см. рис. fig. 2.11).

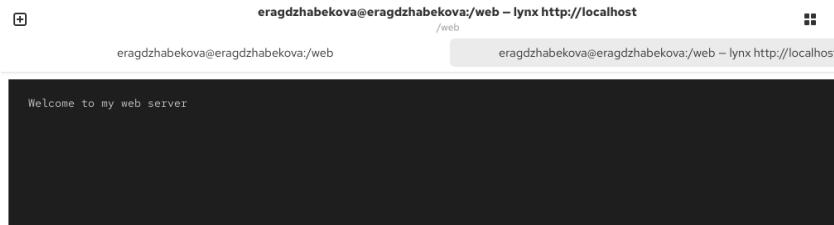


Рис. 2.11: Отображение пользовательской страницы веб-сервера

2.4 Работа с переключателями SELinux

- Получены права администратора. Выполнена проверка состояния переключателей SELinux для службы ftp, выявлено, что переключатель ftpd_anon_write имеет значение off.
- Просмотрен список доступных переключателей и их описаний, относящихся к службе ftpd_anon.

3. Для разрешения анонимной записи переключатель `ftpd_anon_write` был включён, а затем его состояние закреплено как постоянное.

4. Повторная проверка показала, что переключатель `ftpd_anon_write` теперь включён (см. fig. 2.12).

```
root@eragdzhabekova:/web# 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@eragdzhabekova:/web# semanage boolean -l | grep ftp_anon
tftp_anon_write           (off , off) Allow tftp to anon write
root@eragdzhabekova:/web# setsebool ftpd_anon_write on
root@eragdzhabekova:/web# getsebool ftpd_anon_write
ftpd_anon_write --> on
root@eragdzhabekova:/web# semanage boolean -l | grep ftp_anon
tftp_anon_write           (off , off) Allow tftp to anon write
root@eragdzhabekova:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write           (on , off) Allow ftpd to anon write
root@eragdzhabekova:/web# setsebool -P ftpd_anon_write on
root@eragdzhabekova:/web# semanage boolean -l | grep ftpd_anon
ftpd_anon_write           (on , on) Allow ftpd to anon write
root@eragdzhabekova:/web#
```

Рис. 2.12: Настройка переключателя SELinux для службы FTP

Переключатель `ftpd_anon_write` находится в состоянии `on`, что означает разрешение на запись для анонимных FTP-пользователей.

3 Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

Команда: `setenforce 0`.

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

Команда: `getsebool -a`.

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

Пакет: `setroubleshoot`.

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

Команды:

```
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?

Файл: `/etc/sysconfig/selinux`.

6. Где SELinux регистрирует все свои сообщения?

В журнале `/var/log/audit/audit.log`.

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

Команда: `semanage fcontext -l | 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?**

Временно перевести SELinux в разрешающий режим командой `setenforce 0` и проверить работу сервиса.

4 Заключение

В ходе лабораторной работы были изучены основные принципы работы SELinux и его взаимодействие с системой безопасности Linux.

В результате работы получены практические навыки администрирования и конфигурирования SELinux, необходимых для обеспечения безопасности и стабильности работы системы.