Отчёт по лабораторной работе №9

Управление SELinux

Агджабекова Эся Рустамовна

Содержание

Список иллюстраций

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).

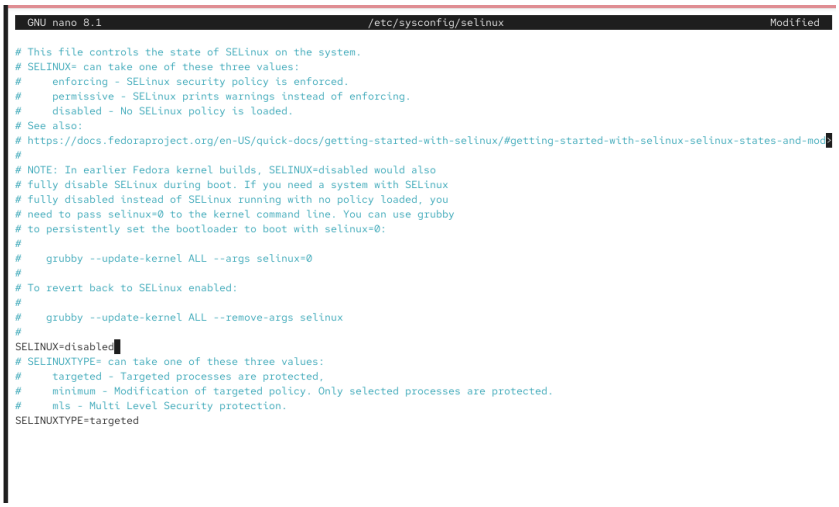

Рис. 2.2: Переключение режима SELinux в Permissive

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).

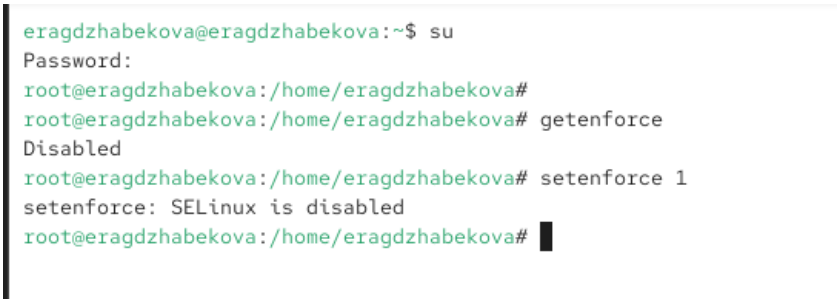

Рис. 2.3: Отключение SELinux в конфигурационном файле

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).

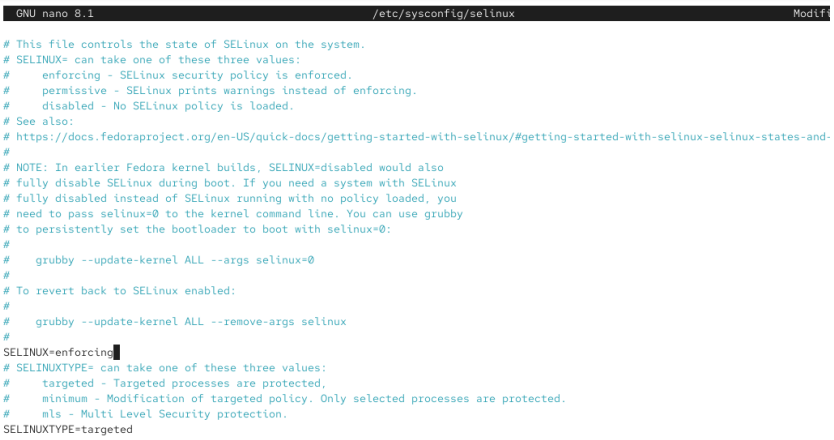

Рис. 2.4: Попытка включить SELinux после отключения

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).

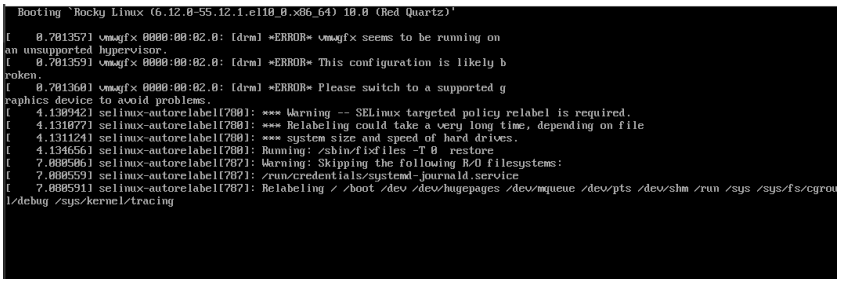

Рис. 2.5: Процесс relabeling при включении SELinux

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).

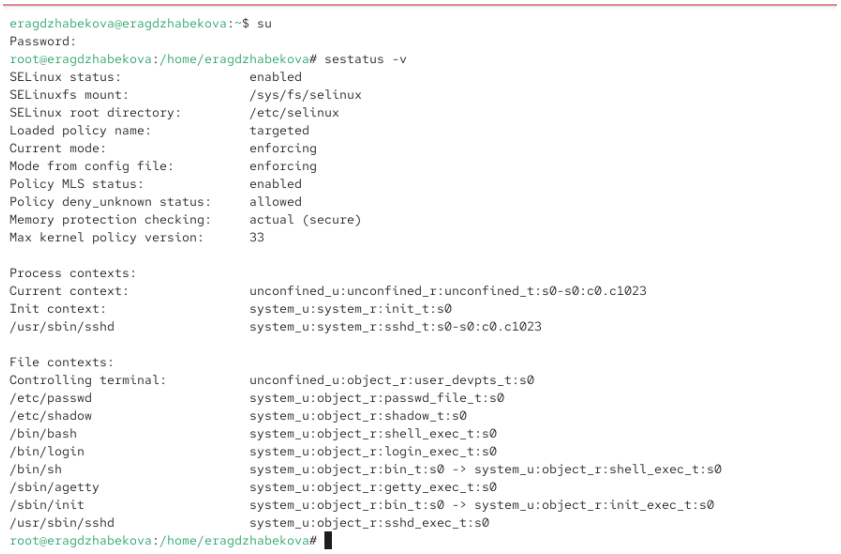

Рис. 2.6: Проверка состояния SELinux после восстановления

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).

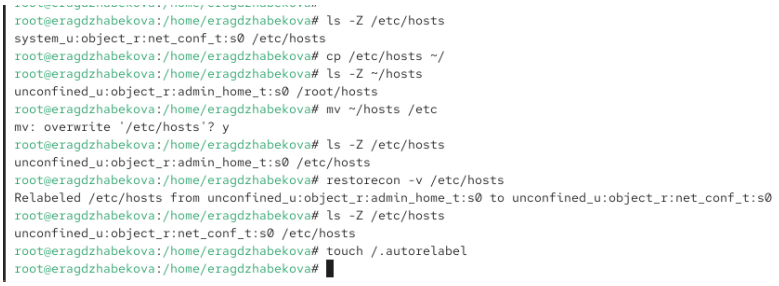

Рис. 2.7: Восстановление контекста безопасности с помощью restorecon

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 разрешённым доступом ко всем пользователям (см. рис. fig. 2.8).

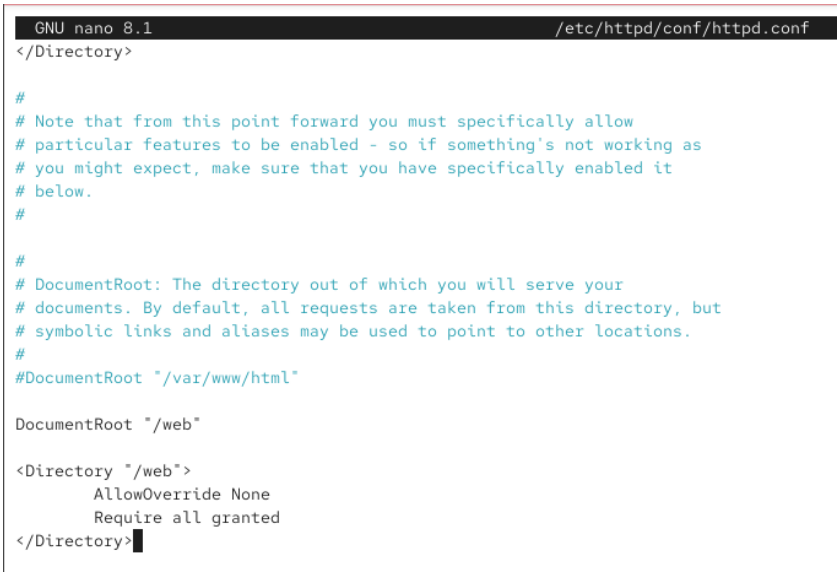

Рис. 2.8: Изменение конфигурационного файла httpd.conf для новой директории

4. 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).

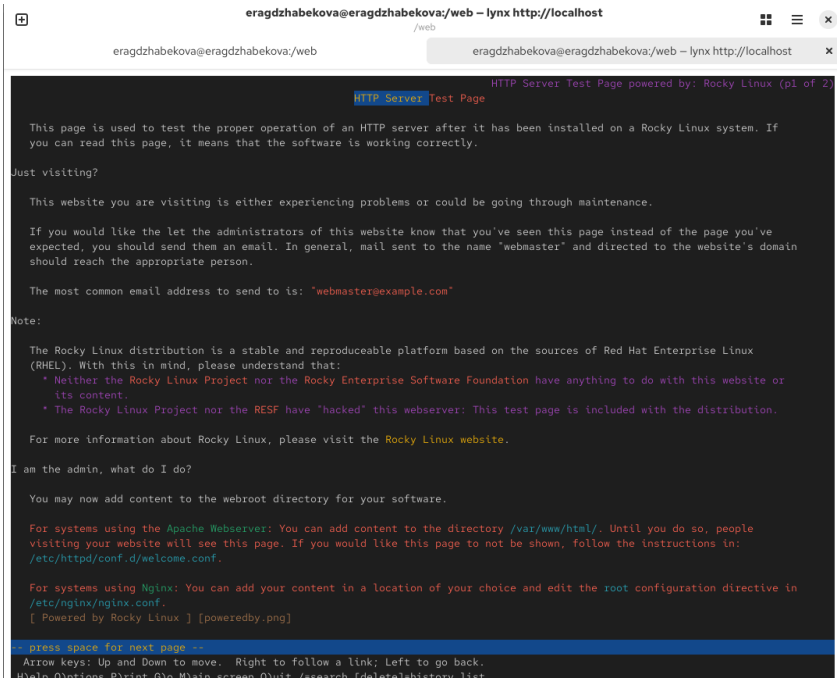

Рис. 2.9: Отображение стандартной тестовой страницы Apache

5. 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).

Рис. 2.10: Применение меток безопасности для каталога /web

6. 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).

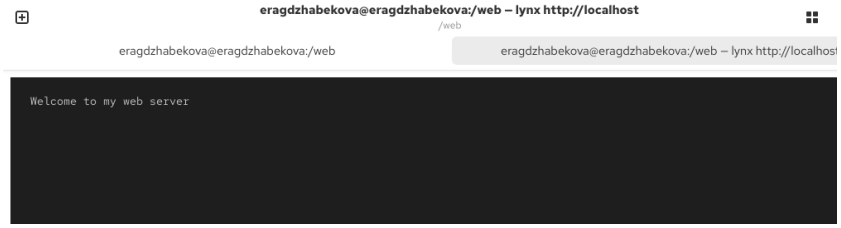

Рис. 2.11: Отображение пользовательской страницы веб-сервера

2.4 Работа с переключателями SELinux

1. Получены права администратора. Выполнена проверка состояния переключателей SELinux для службы ftp, выявлено, что переключатель ftpd_anon_write имеет значение off.

2. 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. рис. fig. 2.12).

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.