Отчёт по лабораторной работе №9

Управление SELinux

Ришард Когенгар

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Ход выполнения

2.1 Управление режимами SELinux

1. После загрузки операционной системы был запущен терминал и получены полномочия администратора.
   Получение прав суперпользователя необходимо для выполнения операций администрирования SELinux, так как управление режимами работы и конфигурацией системы безопасности доступно только пользователю root.

2. Для просмотра текущего состояния SELinux была выполнена команда `sestatus -v`.
   На экране была выведена подробная информация о состоянии системы безопасности:

   - SELinux status: enabled — механизм SELinux включён и функционирует.
   - SELinuxfs mount: /sys/fs/selinux — файловая система SELinux успешно смонтирована.
   - SELinux root directory: /etc/selinux — каталог с конфигурационными файлами SELinux.
   - Loaded policy name: targeted — используется целевая политика, защищающая основные системные службы.
   - Current mode: enforcing — SELinux работает в режиме принудительного исполнения политик.
   - Mode from config file: enforcing — в конфигурационном файле также указан режим enforcing.

- Policy MLS status: enabled — поддержка многоуровневой модели безопасности активна.
- Policy deny_unknown status: allowed — неизвестные действия разрешены, если не запрещены политикой.
- Memory protection checking: actual (secure) — активна проверка защиты памяти.
- Max kernel policy version: 33 — версия политики SELinux, поддерживаемая ядром.

Дополнительно отображены контексты процессов и системных файлов, включая init, sshd, /etc/passwd и /etc/shadow.

```
root@rishardkogengar:~# 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@rishardkogengar:~# getenforce
Enforcing
root@rishardkogengar:~# setenforce 0
root@rishardkogengar:~# getenforce
Permissive
root@rishardkogengar:~#
```

Рис. 2.1: Проверка состояния SELinux

3. Для определения текущего режима работы SELinux была использована команда `getenforce`.

   В ответ было получено значение Enforcing, что подтверждает работу SELinux в режиме строгого контроля.

4. Далее SELinux был временно переведён в разрешающий режим.

   После выполнения команды смены режима и повторной проверки было установлено, что система перешла в состояние Permissive.

   В данном режиме SELinux не блокирует операции, нарушающие политики, а только фиксирует их в журналах.

```
root@rishardkogengar:~# 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@rishardkogengar:~# getenforce
Enforcing
root@rishardkogengar:~# setenforce 0
root@rishardkogengar:~# getenforce
Permissive
root@rishardkogengar:~#
```

Рис. 2.2: Переключение SELinux в режим Permissive

5. Для полного отключения SELinux был отредактирован конфигурационный

файл `/etc/sysconfig/selinux`.

Параметр SELINUX был установлен в значение disabled.

После сохранения изменений система была перезагружена.

```
# 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-se
#
# 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 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
```

Рис. 2.3: Отключение SELinux через конфигурационный файл

6. После перезагрузки системы снова был открыт терминал и получены права администратора.

   Проверка состояния SELinux показала значение Disabled, что подтверждает его полное отключение.

Рис. 2.4: SELinux отключён

7. Была предпринята попытка переключить режим SELinux.
   Система выдала сообщение о том, что SELinux отключён, и отказалась менять режим.
   Это подтверждает невозможность переключения режимов без перезагрузки, если SELinux был отключён на уровне конфигурации.

8. Для повторного включения SELinux файл `/etc/sysconfig/selinux` был вновь отредактирован.
   Параметр SELINUX был установлен в значение enforcing.
   После этого система была перезагружена.

```
# 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-selin
#
# 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 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 protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 2.5: Включение SELinux в режиме enforcing

9. Во время загрузки системы было выведено предупреждение о необходимости восстановления меток безопасности SELinux.

   Служба selinux-autorelabel автоматически запустила процесс перемаркировки файловой системы, который может занимать продолжительное время.

```
[  OK  ] Reached target sysinit.target - System Initialization.
[  OK  ] Started alsa-state.service - Manage Sound Card State (restore and store).
[  OK  ] Reached target sound.target - Sound Card.
         Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
         Starting selinux-autorelabel.service - Relabel all filesystems...
[  OK  ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[    8.151261] selinux-autorelabel[1046]: *** Warning -- SELinux targeted policy relabel is required.
[    8.152701] selinux-autorelabel[1046]: *** Relabeling could take a very long time, depending on file
[    8.154380] selinux-autorelabel[1046]: *** system size and speed of hard drives.
[    8.159105] selinux-autorelabel[1046]: Running: /sbin/fixfiles -T 0  restore
```

Рис. 2.6: Процесс автоматической перемаркировки SELinux

10. После завершения загрузки была повторно выполнена проверка состояния SELinux.

    Было подтверждено, что система работает в режиме enforcing, а политика безопасности успешно загружена.

```
rishard@rishardkogengar:~$ su
Password:
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Рис. 2.7: SELinux работает в режиме enforcing

2.2 Использование restorecon для восстановления контекста безопасности

1. В терминале с правами администратора был проверен контекст безопасности файла `/etc/hosts`.

   Было установлено, что файл имеет корректный тип контекста net_conf_t.

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

Рис. 2.8: Контекст безопасности файла /etc/hosts

2. Файл `/etc/hosts` был скопирован в домашний каталог пользователя.
   Проверка контекста показала, что файл `~/hosts` получил тип admin_home_t, так как копирование рассматривается системой как создание нового файла.

3. Далее файл из домашнего каталога был перемещён обратно в каталог `/etc` с подтверждением перезаписи.
   Проверка показала, что контекст безопасности остался неверным и по-прежнему соответствует admin_home_t.

4. Для восстановления корректного контекста безопасности была использована утилита restorecon.
   В процессе выполнения было выведено сообщение об изменении контекста файла.

5. Повторная проверка подтвердила, что файл `/etc/hosts` снова имеет корректный контекст net_conf_t.

6. Для массового восстановления контекстов безопасности файловой системы был создан файл `.autorelabel` в корневом каталоге.
   После перезагрузки системы была автоматически выполнена полная перемаркировка файлов, что отображалось в загрузочных сообщениях.

Рис. 2.9: Процесс автоматической перемаркировки SELinux

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Был запущен терминал и получены полномочия администратора.
   Это необходимо для установки программного обеспечения, изменения конфигурации веб-сервера и управления политиками SELinux.

2. В системе было установлено необходимое программное обеспечение: веб-сервер Apache (httpd) и текстовый браузер lynx.
   Установка данных пакетов позволяет развернуть локальный HTTP-сервер и проверить его работу из консоли.

3. Для размещения файлов веб-сервера был создан новый каталог `/web`.
   Данный каталог используется в качестве альтернативного корневого каталога (DocumentRoot) для Apache.

4. В каталоге `/web` был создан файл `index.html`.
   В файл был помещён текст `Welcome to my web-server`, который должен отображаться при обращении к веб-серверу.

5. Был отредактирован конфигурационный файл `/etc/httpd/conf/httpd.conf`.
   Стандартная директива `DocumentRoot "/var/www/html"` была закомментирована, после чего ниже добавлена директива `DocumentRoot "/web"`.

Также был закомментирован стандартный раздел `<Directory "/var/www">`, определяющий правила доступа, и добавлен новый раздел `<Directory "/web">`, разрешающий доступ ко всем файлам в данном каталоге.

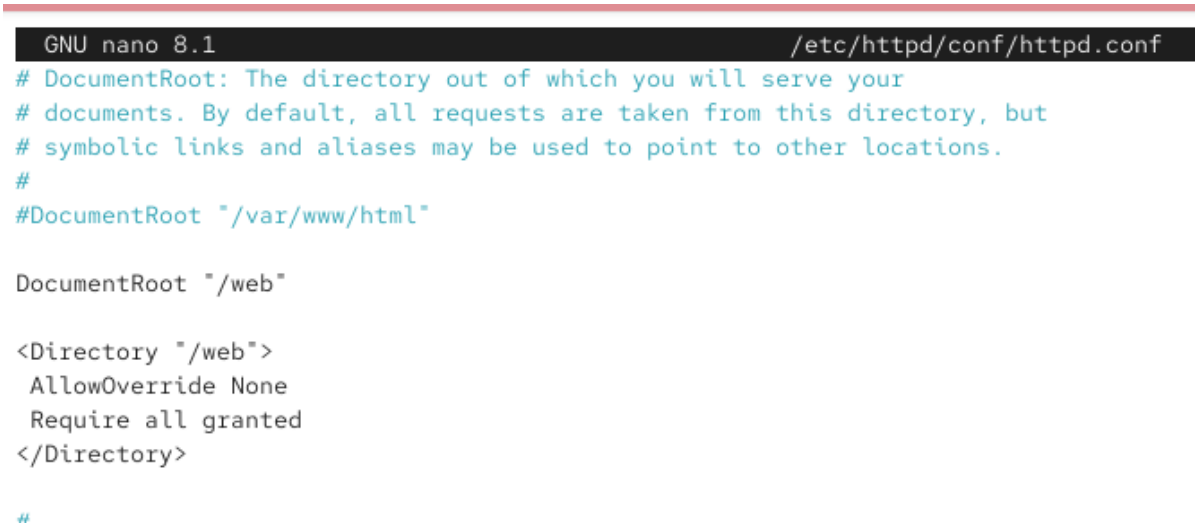

Рис. 2.10: Изменение конфигурации Apache

6. После изменения конфигурации веб-сервер Apache был запущен и добавлен в автозагрузку системы.
   Это обеспечивает автоматический запуск службы httpd при каждом старте системы.

7. Под учётной записью обычного пользователя был выполнен запрос к веб-серверу с помощью текстового браузера lynx.
   В результате была отображена стандартная тестовая страница Rocky Linux, а не содержимое созданного файла `index.html`.
   Это свидетельствует о том, что SELinux блокирует доступ Apache к каталогу `/web` из-за отсутствия корректного контекста безопасности.

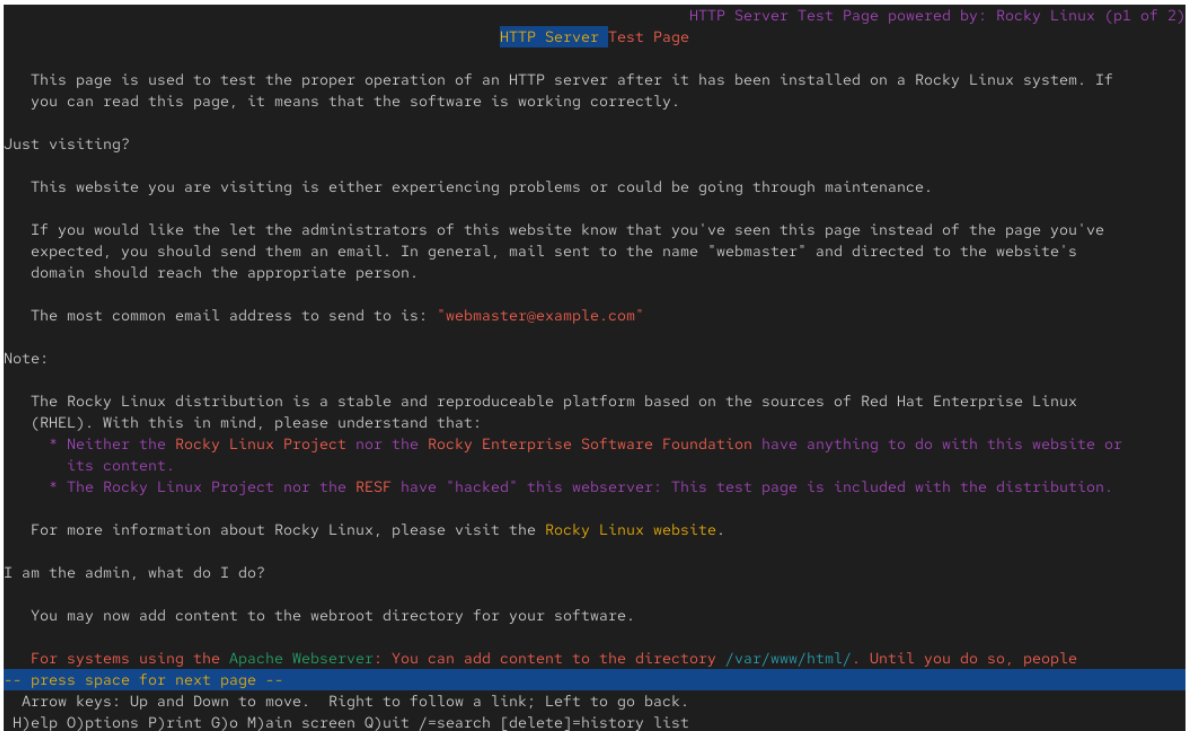

Рис. 2.11: Стандартная страница Apache

8. Для разрешения доступа веб-серверу к нестандартному каталогу была добавлена новая запись контекста безопасности SELinux.
   Для каталога `/web` и всех его вложенных файлов был назначен тип контекста `httpd_sys_content_t`, используемый для статического контента Apache.

9. После назначения нового контекста была выполнена операция восстановления меток безопасности для каталога `/web`.
   В процессе было отображено сообщение о смене контекста каталога и файла `index.html`.

```
root@rishardkogengar:/web#
root@rishardkogengar:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@rishardkogengar:/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@rishardkogengar:/web# systemctl restart httpd
root@rishardkogengar:/web#
```

Рис. 2.12: Назначение и восстановление контекста SELinux

10. После этого под учётной записью пользователя был повторно выполнен

запрос к веб-серверу с помощью lynx.

В результате на экране была успешно отображена пользовательская веб-страница с текстом `Welcome to my web-server`, что подтверждает корректную настройку контекста безопасности.

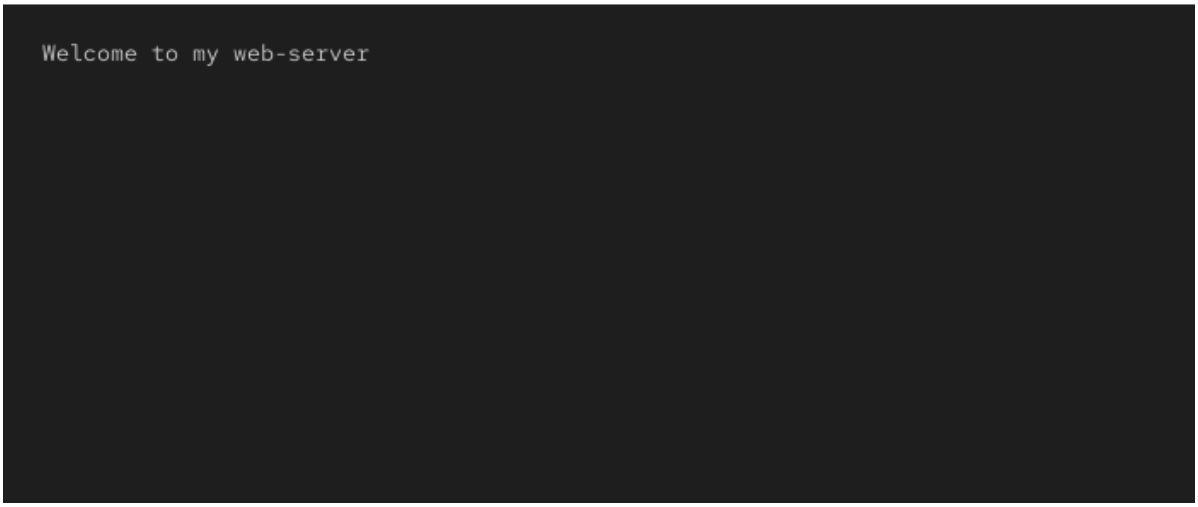

Рис. 2.13: Пользовательская веб-страница

2.4 Работа с переключателями SELinux

1. В терминале с правами администратора был просмотрен список переключателей SELinux, относящихся к службе FTP.

   Был обнаружен переключатель `ftpd_anon_write`, имеющий значение off, что означает запрет анонимной записи через FTP.

2. Далее был выведен список переключателей службы `ftpd_anon` с пояснениями.

   Было установлено, что параметр `ftpd_anon_write` отвечает за разрешение анонимной записи и по умолчанию отключён как во временной, так и в постоянной конфигурации.

3. Значение переключателя `ftpd_anon_write` было изменено с off на on для текущего сеанса работы системы.

После этого проверка показала, что переключатель включён, однако постоянное значение по-прежнему остаётся отключённым.

4. Для сохранения изменения после перезагрузки системы переключатель `ftpd_anon_write` был включён в постоянной конфигурации.
   Это обеспечивает сохранение разрешения анонимной записи для FTP-службы даже после перезапуска системы.

5. Повторная проверка списка переключателей показала, что `ftpd_anon_write` имеет состояние on как для временной, так и для постоянной настройки.
   Это означает, что анонимная запись через FTP разрешена и настройка сохранена на постоянной основе.

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

Рис. 2.14: Работа с переключателями SELinux

2.5 Вывод

В ходе работы были изучены механизмы настройки SELinux для доступа к нестандартным каталогам веб-сервера и управления логическими переключателями безопасности. Настройка контекстов и переключателей позволила обеспечить корректную работу служб без отключения SELinux, сохранив требуемый уровень защиты системы.

3 Контрольные вопросы

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

Для временного перевода SELinux в разрешающий режим используется команда

`setenforce 0`

Данная команда переключает SELinux в режим Permissive до следующей перезагрузки системы или изменения режима обратно.

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

Для просмотра всех доступных переключателей SELinux применяется команда `getsebool -a`

Она выводит полный список boolean-переключателей и их текущие значения.

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

Для получения человекочитаемых сообщений SELinux необходимо установить пакет

`setroubleshoot-server`

Он позволяет анализировать события SELinux и формировать подробные пояснения к ним.

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

Для применения корректного контекста безопасности к каталогу `/web` необхо-

димо: - добавить правило контекста для каталога и его содержимого; - восстановить контексты безопасности на файловой системе.

Используются команды `semanage fcontext` и `restorecon`.

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

Для полного отключения SELinux необходимо изменить конфигурационный файл

`/etc/sysconfig/selinux`

В данном файле параметр `SELINUX` устанавливается в значение `disabled`.

6. Где SELinux регистрирует все свои сообщения?

Все сообщения SELinux регистрируются в журнале аудита системы, который хранится в файле

`/var/log/audit/audit.log`

Дополнительно сообщения могут дублироваться в системный журнал.

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

Для получения подробной информации о переключателях и параметрах SELinux, связанных со службой FTP, используется команда

```
semanage boolean -l | grep ftp
```

Она отображает описание каждого переключателя и его текущее состояние.

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?

Самый простой способ — временно перевести SELinux в разрешающий режим с помощью `setenforce 0`.

Если после этого сервис начинает работать корректно, значит проблема связана с политиками SELinux.