

Отчёт по лабораторной работе №9

Управление SELinux

Амина Аджигалиева

Содержание

1	Цель работы	5
2	Ход выполнения работы	6
2.1	Управление режимами SELinux	6
2.2	Использование restorecon для восстановления контекста безопасности	10
3	Ход выполнения работы	12
3.1	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	12
3.2	Работа с переключателями SELinux	15
4	Контрольные вопросы	17
5	Заключение	19

Список иллюстраций

2.1	Просмотр состояния SELinux с помощью sestatus	7
2.2	Отключение SELinux через конфигурационный файл	8
2.3	Проверка статуса SELinux после перезагрузки	8
2.4	Включение SELinux (режим enforcing)	9
2.5	Автоматическая перемаркировка файловой системы при загрузке	9
2.6	SELinux активен в режиме enforcing после перезагрузки	10
2.7	Восстановление контекста безопасности файла /etc/hosts	11
2.8	Автоматическая перемаркировка при перезагрузке системы . . .	11
3.1	Изменение параметров конфигурации Apache	13
3.2	Отображение стандартной страницы Rocky Linux	13
3.3	Применение контекста безопасности к каталогу /web	14
3.4	Отображение пользовательской страницы веб-сервера	14
3.5	Просмотр текущих значений переключателей FTP	15
3.6	Включение и проверка состояния переключателя ftpd_anon_write	16

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Ход выполнения работы

2.1 Управление режимами SELinux

Сначала я получила административные права с помощью команды `su`.
Затем выполнила команду `sestatus -v`, чтобы просмотреть текущее состояние системы безопасности SELinux.
Из вывода видно, что SELinux включён (`enabled`), политика загружена (`targeted`), а текущий режим — `enforcing`.
Это означает, что система применяет политики безопасности, ограничивая доступ процессов в соответствии с заданными контекстами.

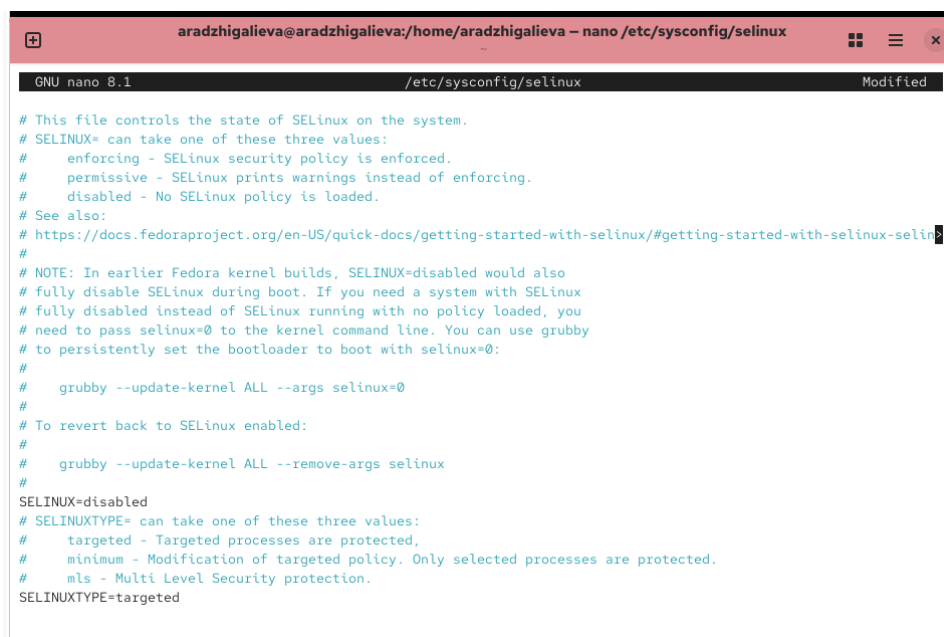
```
aradzhigalieva@aradzhigalieva:/home/aradzhigalieva# sestatus -v
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:         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@aradzhigalieva:/home/aradzhigalieva# getenforce 0
Enforcing
root@aradzhigalieva:/home/aradzhigalieva# setenforce 0
root@aradzhigalieva:/home/aradzhigalieva# getenforce
Permissive
root@aradzhigalieva:/home/aradzhigalieva#
```

Рис. 2.1: Просмотр состояния SELinux с помощью sestatus

Чтобы уточнить режим работы SELinux, я ввела команду `getenforce`. Она подтвердила, что система находится в режиме Enforcing. Далее я временно перевела SELinux в разрешающий режим (Permissive) командой `setenforce 0`, после чего снова проверила состояние через `getenforce`. Затем я открыла файл конфигурации `/etc/sysconfig/selinux` в текстовом редакторе nano и установила параметр `SELINUX=disabled`, чтобы полностью отключить SELinux после перезагрузки. На скриншоте видно, что значение параметра изменено.



```
aradzhigalieva@aradzhigalieva:/home/aradzhigalieva - nano /etc/sysconfig/selinux
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
#
# 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. 2.2: Отключение SELinux через конфигурационный файл

После перезагрузки я снова вошла под пользователем root и проверила состояние SELinux командой `getenforce`.

Вывод показал Disabled, что подтверждает успешное отключение системы без-опасности.

Попытка переключить режим с помощью `setenforce 1` завершилась сообщением об ошибке, так как при полностью отключённом SELinux это невозможно.



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

Рис. 2.3: Проверка статуса SELinux после перезагрузки

Далее я повторно отредактировала файл `/etc/sysconfig/selinux`, установив параметр `SELINUX=enforcing`, чтобы вернуть SELinux в режим принудительного контроля.



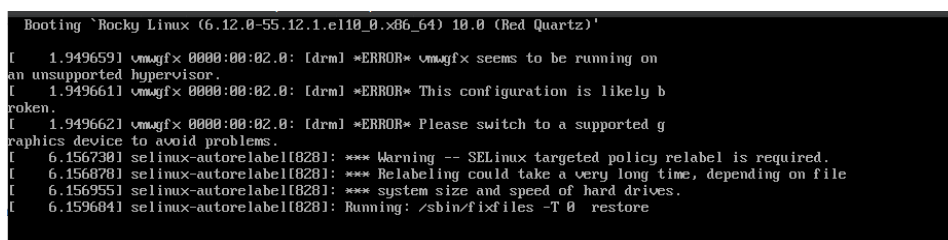
```
aradzhigalieva@aradzhigalieva:/home/aradzhigalieva - nano /etc/sysconfig/selinux
GNU nano 8.1 /etc/sysconfig/selinux Modified

# 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
#
# 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

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   ^U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  ^-E Redo
```

Рис. 2.4: Включение SELinux (режим enforcing)

После перезагрузки системы появилось предупреждающее сообщение о необходимости восстановления меток безопасности SELinux. Процесс перемаркировки файловой системы может занять продолжительное время.



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

```
[ 1.949659] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 1.949661] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 1.949662] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 6.156730] selinux-autorelabel[828]: *** Warning -- SELinux targeted policy relabel is required.
[ 6.156878] selinux-autorelabel[828]: *** Relabeling could take a very long time, depending on file
[ 6.156955] selinux-autorelabel[828]: *** system size and speed of hard drives.
[ 6.159684] selinux-autorelabel[828]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.5: Автоматическая перемаркировка файловой системы при загрузке

Когда система загрузилась, я снова проверила состояние SELinux командой `sestatus -v`. Результаты подтвердили, что SELinux снова работает в режиме enforcing, с политикой targeted.

```

aradzhigaliev@aradzhigaliev:~$ su
Password:
root@aradzhigaliev:/home/aradzhigaliev# 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@aradzhigaliev:/home/aradzhigaliev#

```

Рис. 2.6: SELinux активен в режиме enforcing после перезагрузки

2.2 Использование restorecon для восстановления контекста безопасности

Для демонстрации восстановления контекста безопасности я выполнила команду `ls -Z /etc/hosts`, чтобы просмотреть текущие метки SELinux файла `/etc/hosts`. Далее я скопировала этот файл в домашний каталог и снова проверила контекст. Он изменился на `admin_home_t`, так как копирование считается созданием нового файла.

Затем я переместила файл обратно в каталог `/etc` и убедилась, что контекст остался неправильным.

Для исправления я применила команду `restorecon -v /etc/hosts`, после чего контекст безопасности был восстановлен до исходного — `net_conf_t`.

```

root@aradzhigalieva:/home/aradzhigalieva#
root@aradzhigalieva:/home/aradzhigalieva# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@aradzhigalieva:/home/aradzhigalieva# cp /etc/hosts ~/
root@aradzhigalieva:/home/aradzhigalieva# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@aradzhigalieva:/home/aradzhigalieva# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@aradzhigalieva:/home/aradzhigalieva# ls -Z ~/hosts
ls: cannot access '/root/hosts': No such file or directory
root@aradzhigalieva:/home/aradzhigalieva# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@aradzhigalieva:/home/aradzhigalieva# 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@aradzhigalieva:/home/aradzhigalieva# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@aradzhigalieva:/home/aradzhigalieva# touch /.autorelabel
root@aradzhigalieva:/home/aradzhigalieva# █

```

Рис. 2.7: Восстановление контекста безопасности файла /etc/hosts

Чтобы выполнить массовое исправление контекстов безопасности всей файловой системы, я создала пустой файл /.autorelabel и перезагрузила систему. При загрузке снова появилось сообщение о перемаркировке файлов, подтверждающее, что SELinux выполняет автоматическое восстановление меток.

```

Файлы  Машинка  Вид  Вид  Устройство  Справка
[ 0.895157] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.895159] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.895160] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 5.266109] selinux-autorelabel[820]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.267133] selinux-autorelabel[820]: *** Relabeling could take a very long time, depending on file
[ 5.268064] selinux-autorelabel[820]: *** system size and speed of hard drives.
[ 5.269694] selinux-autorelabel[820]: Running: /sbin/fixfiles -T 0 restore

```

Рис. 2.8: Автоматическая перемаркировка при перезагрузке системы

3 Ход выполнения работы

3.1 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Сначала я получила административные права и установила необходимые пакеты для работы веб-сервера: `httpd` и `lynx`.

Затем создала новый каталог `/web`, который будет использоваться как корневая директория для веб-контента, и добавила в него файл `index.html` с текстом «Welcome to my web-server».

Далее я открыла файл конфигурации `/etc/httpd/conf/httpd.conf` и изменила параметры.

Закомментировала строку `DocumentRoot "/var/www/html"` и добавила `DocumentRoot "/web"`.

Также заменила блок `<Directory "/var/www">` на `<Directory "/web">`, разрешив доступ ко всем пользователям.

Это позволило серверу Apache использовать новую директорию в качестве источника веб-страниц.

```
GNU nano 8.1 /etc/httpd/conf/httpd.conf
#
#
# 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. 3.1: Изменение параметров конфигурации Apache

После запуска службы httpd в браузере lynx при обращении к адресу `http://localhost` появилась стандартная тестовая страница Rocky Linux, что означает успешный запуск сервера, но указанный каталог ещё не был настроен для SELinux.

```
HTTP Server Test Page powered by: Rocky Linux (pl of 2)
HTTP Server Test Page

This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky
Linux system. If you can read this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or could be going through maintenance.

If you would like the let the administrators of this website know that you've seen this page instead of
the page you've expected, you should send them an email. In general, mail sent to the name "webmaster" and
directed to the website's domain should reach the appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:

The Rocky Linux distribution is a stable and reproduceable platform based on the sources of Red Hat
Enterprise Linux (RHEL). With this in mind, please understand that:
* Neither the Rocky Linux Project nor the Rocky Enterprise Software Foundation have anything to do with
this website or its content.
* The Rocky Linux Project nor the RESF have "hacked" this webserver: This test page is included with the
distribution.

For more information about Rocky Linux, please visit the Rocky Linux website.

I am the admin, what do I do?
-- press space for next page --
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. 3.2: Отображение стандартной страницы Rocky Linux

Чтобы разрешить доступ Apache к каталогу `/web`, я применила новую метку

контекста безопасности SELinux для этого пути.

Сначала добавила контекст с помощью команды `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`, затем выполнила восстановление контекста командой `restorecon -R -v /web`.

После этого файлы в каталоге получили правильную метку безопасности `httpd_sys_content_t`.

```
root@aradzhigalieva:/web#
root@aradzhigalieva:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@aradzhigalieva:/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@aradzhigalieva:/web# █
```

Рис. 3.3: Применение контекста безопасности к каталогу /web

После внесённых изменений я снова открыла веб-сайт через `lynx` и убедилась, что теперь отображается созданная мной страница с текстом «Welcome to my web-server».

Это подтверждает, что контекст безопасности настроен корректно и сервер имеет доступ к каталогу /web.

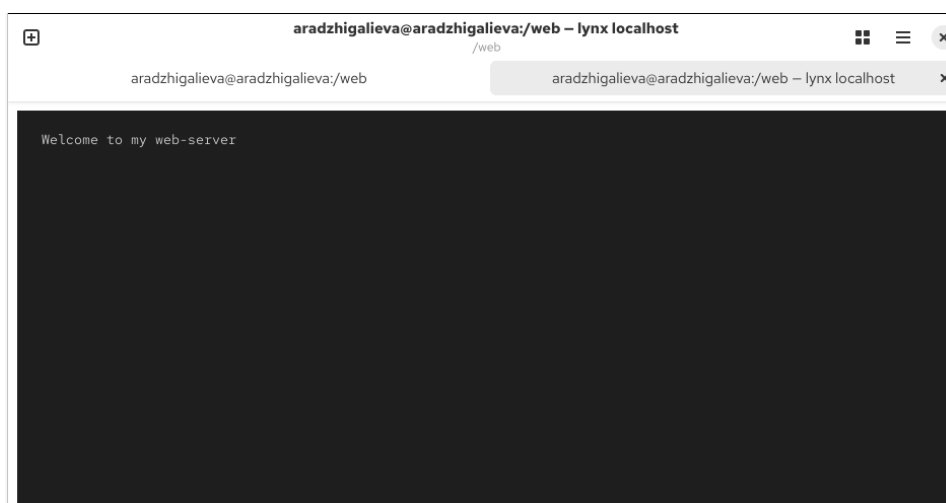


Рис. 3.4: Отображение пользовательской страницы веб-сервера

3.2 Работа с переключателями SELinux

Затем я изучила работу переключателей (boolean) SELinux для службы FTP. Сначала с помощью команды `getsebool -a | grep ftp` я просмотрела все доступные параметры.

Из вывода видно, что большинство из них имеют значение `off`, включая `ftpd_anon_write`, который отвечает за разрешение анонимной записи.

```
root@aradzhigalieva:/web#  
root@aradzhigalieva:/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
```

Рис. 3.5: Просмотр текущих значений переключателей FTP

Далее я уточнила назначение данного переключателя при помощи `semanage boolean -l | grep ftpd_anon`, после чего изменила его значение командой `setsebool ftpd_anon_write on`.

Команда `getsebool ftpd_anon_write` показала, что временная настройка переключателя включена (`on`), но постоянная — нет.

Чтобы сделать изменение постоянным, я использовала параметр `-P`:

`setsebool -P ftpd_anon_write on`.

После этого оба значения — временное и постоянное — стали равны `on`, что подтверждает успешное включение параметра.

```

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

```

Рис. 3.6: Включение и проверка состояния переключателя ftpd_anon_write

4 Контрольные вопросы

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

Для временного перевода SELinux в режим Permissive используется команда:

```
setenforce 0.
```

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

Для вывода списка всех переключателей SELinux используется команда:

```
getsebool -a.
```

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

Для удобного анализа сообщений SELinux необходимо установить пакет:

```
setroubleshoot.
```

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

Необходимо добавить и применить контекст безопасности следующими командами:

```
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?**

Для полного отключения SELinux нужно отредактировать файл:
`/etc/sysconfig/selinux`,
установив параметр `SELINUX=disabled`.

6. Где SELinux регистрирует все свои сообщения?

Сообщения SELinux записываются в системный журнал:
`/var/log/audit/audit.log`.

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

Для просмотра доступных контекстов и параметров службы ftp используется 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?

Самый простой способ — временно перевести SELinux в разрешающий режим:
`setenforce 0`.
Если после этого сервис начнёт работать корректно, значит, проблема связана с политикой SELinux.

5 Заключение

В ходе выполнения лабораторной работы я изучила механизмы управления системой безопасности SELinux и её взаимодействие с сервисами Linux.

Были рассмотрены режимы работы SELinux — enforcing, permissive и disabled, а также способы их изменения как временно, так и через конфигурационные файлы.

На практике я выполнила настройку SELinux для нестандартного каталога веб-сервера, применила корректные контексты безопасности и убедилась в правильной работе сервиса Apache.

Кроме того, я освоила использование переключателей (boolean) SELinux и научилась изменять их временно и постоянно.

Полученные знания и навыки позволяют уверенно управлять политиками безопасности SELinux, обеспечивая защиту системных служб и корректное функционирование сервисов в среде Linux.