

Отчёт по лабораторной работе №9

Управление SELinux

Лабси Мохаммед

Содержание

1	Цель работы	5
2	Выполнение работы	6
2.1	Просмотр состояния SELinux	6
2.2	Проверка и изменение режима SELinux	7
2.3	Отключение SELinux через конфигурационный файл	8
2.4	Включение SELinux и возврат в режим Enforcing	9
2.5	Восстановление контекста безопасности файлов	11
2.6	Настройка контекста безопасности для нестандартного расположе- ния файлов веб-сервера	12
2.7	Работа с переключателями SELinux	14
3	Контрольные вопросы	16
4	Заключение	18

Список иллюстраций

2.1	Проверка состояния SELinux	7
2.2	Изменение режима работы SELinux	7
2.3	Редактирование конфигурации SELinux (отключение)	8
2.4	SELinux отключён	9
2.5	Редактирование конфигурации SELinux (включение)	9
2.6	Переразметка меток безопасности при загрузке	10
2.7	Проверка состояния SELinux после включения	10
2.8	Восстановление контекста безопасности файла /etc/hosts	11
2.9	Автоматическая перемаркировка файловой системы при загрузке	11
2.10	Изменение конфигурации веб-сервера	12
2.11	Тестовая страница Rocky Linux	13
2.12	Назначение контекста безопасности каталогу /web	13
2.13	Доступ к пользовательской веб-странице	14
2.14	Работа с переключателями SELinux для FTP	15

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение работы

2.1 Просмотр состояния SELinux

Для начала были получены права администратора с помощью команды `su`. После ввода пароля выполнена команда `sestatus -v`.

Вывод команды показывает подробную информацию о состоянии SELinux:

- SELinux status: enabled — система безопасности SELinux включена;
- SELinuxfs mount: /sys/fs/selinux — точка монтирования файловой системы SELinux;
- SELinux root directory: /etc/selinux — корневой каталог конфигурации SELinux;
- Loaded policy name: targeted — используется политика, защищающая только определённые процессы;
- Current mode: enforcing — политика SELinux активно применяется;
- Mode from config file: enforcing — тот же режим задан в конфигурации;
- Policy MLS status: enabled — поддержка многоуровневой безопасности включена;
- Policy deny_unknown status: allowed — неизвестные объекты разрешены;
- Memory protection checking: actual (secure) — контроль памяти активен;
- Process contexts и File contexts — показывают контексты безопасности активных процессов и файлов.

```

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

```

Рис. 2.1: Проверка состояния SELinux

2.2 Проверка и изменение режима SELinux

Режим SELinux был проверен с помощью команды `getenforce`.

По умолчанию система находилась в состоянии Enforcing (принудительное исполнение политики).

Затем режим был изменён на разрешающий Permissive.

Повторная проверка показала, что SELinux работает в режиме Permissive.

```

/usr/sbin/sshd                 system_u:object_r:sshd_ex
root@mlabsi:/home/mlabsi#
root@mlabsi:/home/mlabsi# getenforce
Enforcing
root@mlabsi:/home/mlabsi# setenforce 0
root@mlabsi:/home/mlabsi# getenforce
Permissive
root@mlabsi:/home/mlabsi#

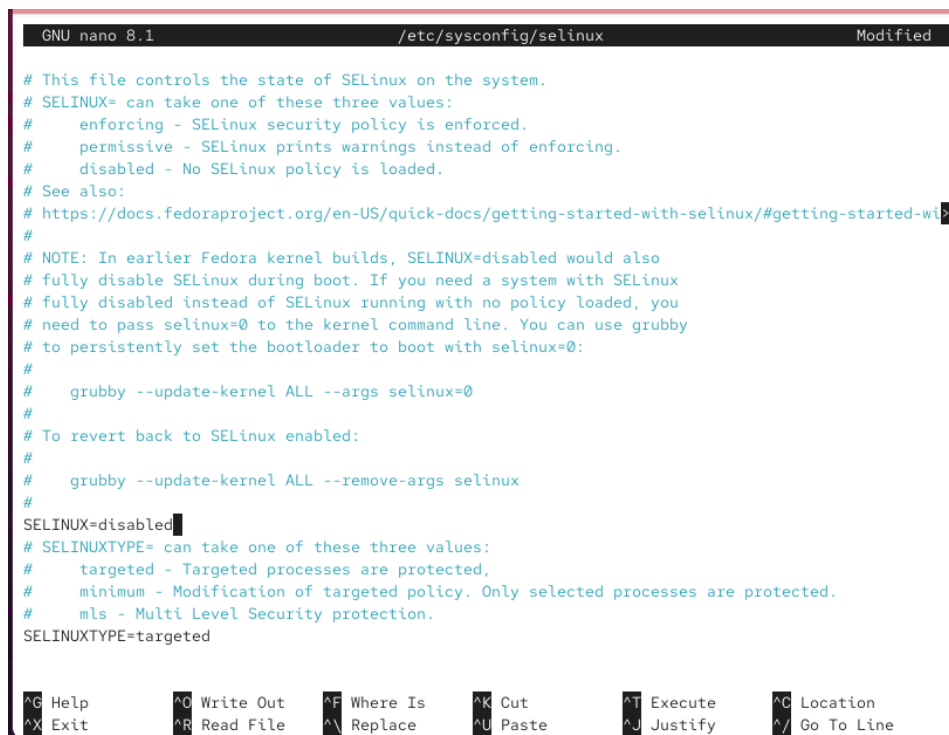
```

Рис. 2.2: Изменение режима работы SELinux

2.3 Отключение SELinux через конфигурационный файл

Для полного отключения SELinux был отредактирован файл конфигурации /etc/sysconfig/selinux.

В нём параметр SELINUX был изменён на disabled и сохранены изменения.



```
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-wi
#
# 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

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

Рис. 2.3: Редактирование конфигурации SELinux (отключение)

После перезагрузки проверка состояния показала, что SELinux отключён. Попытка включить SELinux без перезагрузки завершилась сообщением, что SELinux is disabled.


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

Рис. 2.4: SELinux отключён

2.4 Включение SELinux и возврат в режим Enforcing

Для повторного включения SELinux параметр SELINUX в файле `/etc/sysconfig/selinux` был изменён на `enforcing`.



```
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
#
# 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
^X Exit      ^R Read File ^V Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Рис. 2.5: Редактирование конфигурации SELinux (включение)

После перезагрузки система вывела предупреждение о необходимости переразметки меток безопасности (relabeling), что может занять некоторое время.

```
Booting `Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)`
[ 0.864878] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.864880] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.864881] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 7.478621] selinux-autorelabel[1819]: *** Warning -- SELinux targeted policy relabel is required.
[ 7.478714] selinux-autorelabel[1819]: *** Relabeling could take a very long time, depending on file
[ 7.478750] selinux-autorelabel[1819]: *** system size and speed of hard drives.
[ 7.478788] selinux-autorelabel[1819]: Running: /sbin/fixfiles -T 0 restore
[ 12.253822] selinux-autorelabel[1826]: Warning: Skipping the following R/O filesystems:
[ 12.253644] selinux-autorelabel[1826]: /run/credentials/systemd-journald.service
[ 12.256677] selinux-autorelabel[1826]: Relabeling /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys
l/debug /sys/kernel/tracing
```

Рис. 2.6: Переразметка меток безопасности при загрузке

После завершения перезагрузки команда `sestatus -v` показала, что SELinux снова работает в режиме enforcing.

```
m1absi@m1absi:~$ su
Password:
root@m1absi:/home/m1absi# 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/getty 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@m1absi:/home/m1absi#
```

Рис. 2.7: Проверка состояния SELinux после включения

2.5 Восстановление контекста безопасности файлов

Для примера использовался системный файл /etc/hosts.

При проверке его контекста была получена метка system_u:object_r:net_conf_t:s0.

После копирования файла в домашний каталог его контекст изменился на admin_home_t, поскольку копирование создает новый объект.

При перемещении файла обратно в /etc контекст остался прежним — admin_home_t.

Для восстановления корректного контекста была использована команда restorecon -v /etc/hosts, после чего контекст вернулся к исходному — net_conf_t.

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

Рис. 2.8: Восстановление контекста безопасности файла /etc/hosts

Для массового восстановления контекста безопасности на всей файловой системе была создана команда touch /.autorelabel.

После перезагрузки система автоматически провела процесс перемаркировки (relabeling).

```
[ 1.771095] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 1.771097] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 1.771098] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 9.770446] selinux-autorelabel[817]: *** Warning -- SELinux targeted policy relabel is required.  
[ 9.770504] selinux-autorelabel[817]: *** Relabeling could take a very long time, depending on file  
[ 9.770525] selinux-autorelabel[817]: *** system size and speed of hard drives.  
[ 9.786460] selinux-autorelabel[817]: Running: /sbin/fixfiles -T 0 restore  
[ 13.794642] selinux-autorelabel[824]: Warning: Skipping the following ERO filesystems:  
[ 13.794703] selinux-autorelabel[824]: /run/credentials/systemd-journald.service  
[ 13.794735] selinux-autorelabel[824]: Relabeling /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cg  
l/debug /sys/kernel/tracing
```

Рис. 2.9: Автоматическая перемаркировка файловой системы при загрузке

2.6 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

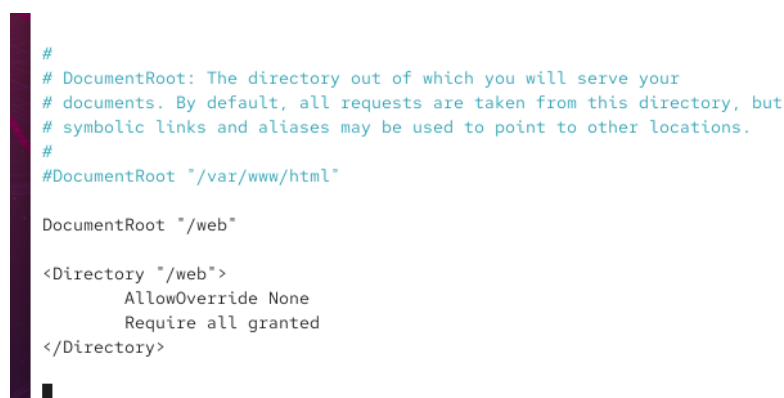
Для начала были установлены необходимые пакеты `httpd` и `lynx`.

Создан новый каталог для веб-контента `/web` и файл `index.html` с текстом «Welcome to my web-server».

В конфигурационном файле `/etc/httpd/conf/httpd.conf` были внесены изменения:

строка `DocumentRoot "/var/www/html"` закомментирована и заменена на `DocumentRoot "/web"`.

Также добавлен новый раздел с правами 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. 2.10: Изменение конфигурации веб-сервера

После запуска веб-сервера и обращения к адресу `http://localhost` отображалась стандартная тестовая страница Rocky Linux, что указывает на отсутствие доступа к пользовательскому каталогу.

```
HTTP Server Test Page powered by: Rocky Linux (p1 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.
-- 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. 2.11: Тестовая страница Rocky Linux

Для решения этой проблемы был задан новый контекст безопасности каталогу /web.

Выполнена команда semanage fcontext для назначения типа httpd_sys_content_t и восстановлен контекст при помощи restorecon.

В результате каталог /web и файл index.html получили корректные метки безопасности.

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

Рис. 2.12: Назначение контекста безопасности каталогу /web

После этого при повторном обращении к серверу в браузере lynx отображается страница с пользовательским сообщением «Welcome to my web server».

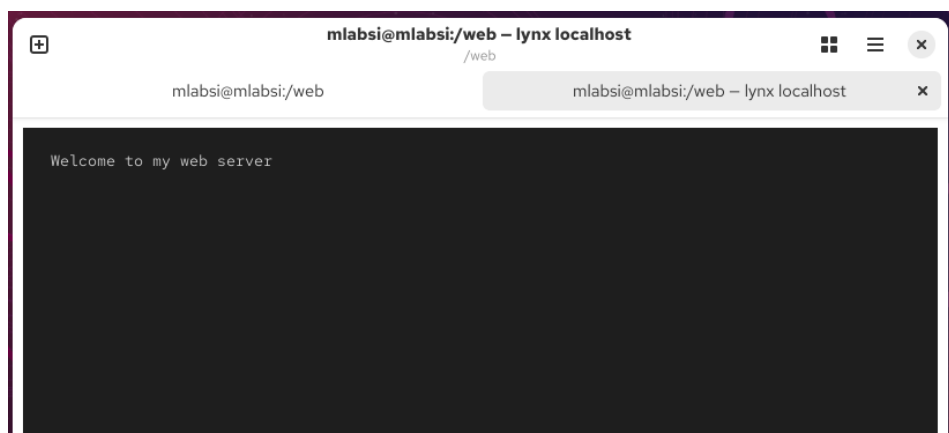


Рис. 2.13: Доступ к пользовательской веб-странице

2.7 Работа с переключателями SELinux

Для анализа переключателей SELinux, связанных с FTP-службой, была выполнена команда `getsebool -a | grep ftp`.

В списке найден параметр `ftpd_anon_write`, отвечающий за возможность анонимной записи через FTP, который по умолчанию имел состояние `off`.

Затем была выполнена команда `semanage boolean -l | grep ftpd_anon` для отображения описания параметра и его текущего состояния.

Параметр `ftpd_anon_write` был временно включён при помощи `setsebool ftpd_anon_write on`.

Проверка показала, что состояние изменилось на `on`, однако настройка постоянной (`persistent`) конфигурации осталась выключенной.

Для включения постоянной настройки был применён ключ `-P`

Повторная проверка с помощью `semanage boolean -l | grep ftpd_anon` показала, что переключатель `ftpd_anon_write` теперь включён как временно, так и постоянно (`on , on`).

```

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

```

Рис. 2.14: Работа с переключателями SELinux для FTP

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.

После этого можно проверить состояние командой **getenforce**.

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

Для вывода полного списка переключателей SELinux используется команда **getsebool -a**.

Она отображает все логические параметры (boolean) и их текущее состояние.

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

Для интерпретации сообщений SELinux используется пакет **setroubleshoot**.

Он позволяет получать понятные уведомления о причинах блокировок и рекомендациях по их устранению.

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

Необходимо выполнить следующие команды:

- **`**semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"**`** — добавляет

правило для назначения типа контекста.

- **restorecon -R -v /web** — применяет изменения и обновляет контекст безопасности каталога.

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

Для полного отключения SELinux необходимо отредактировать файл **/etc/sysconfig/selinux**,
изменив строку **SELINUX=enforcing** на **SELINUX=disabled**.

6. **Где SELinux регистрирует все свои сообщения?**

Журнал событий SELinux записывается в файл **/var/log/audit/audit.log**.
Если служба аудита недоступна, сообщения также могут появляться в **/var/log/messages**.

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

Для просмотра контекстов и разрешённых типов, связанных с FTP, используется команда

semanage fcontext -l | grep ftp.

Она показывает все файлы и каталоги, имеющие контексты, применяемые к FTP-службе.

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 и проверить, изменилось ли поведение сервиса.

Если после этого сервис начал работать корректно, значит, причина связана с политикой SELinux.

4 Заключение

В ходе работы были изучены принципы управления безопасностью с помощью SELinux, включая изменение режимов работы, настройку контекстов безопасности и использование переключателей политик.