

Отчёт по лабораторной работе 9

Управление SELinux

Вишняков Родион Сергеевич

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Вывод	16
4	Контрольные вопросы	17

Список иллюстраций

2.1	root	6
2.2	SELinux	6
2.3	SELinux	7
2.4	Изменение редактора	7
2.5	SELinux	7
2.6	SELinux	8
2.7	Изменение редактора	8
2.8	SELinux	9
2.9	Контекст безопасности файла	9
2.10	Создание файла сценария	9
2.11	Файл hosts	9
2.12	admin_home_t	10
2.13	Контекст безопасности	10
2.14	Тип контекста	10
2.15	Массовое исправления контекста	10
2.16	root	11
2.17	Необходимое программное обеспечение	11
2.18	Новое хранилище	11
2.19	index.html	12
2.20	/etc/httpd/conf/httpd.conf	12
2.21	Служба httpd и веб-сервер	12
2.22	lynx	13
2.23	Новая метку контекста к /web	13
2.24	Контекст безопасности	13
2.25	Веб-сервер	13
2.26	Список переключателей SELinux	14
2.27	Список переключателей с пояснением	14
2.28	Значение переключателя	14
2.29	Список переключателей SELinux	14
2.30	Постоянное значение переключателя	15
2.31	Список переключателей	15

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

Получаем полномочия администратора

```
rodvish@rodvishh:~$ sudo -i
[sudo] пароль для rodvish:
root@rodvishh:~#
```

Рис. 2.1: root

Просмотрели текущую информацию о состоянии SELinux

```
root@rodvishh:~# 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@rodvishh:~#
```

Рис. 2.2: SELinux

Посмотрели, в каком режиме работает SELinux

```

root@rodvishh:~# getenforce
Enforcing
root@rodvishh:~#

```

Рис. 2.3: SELinux

В файле /etc/sysconfig/selinux с помощью редактора установили заданное значение

```

GNU nano 8.1 /etc/sysc
# 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
#
# 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. 2.4: Изменение редактора

Посмотрели статус SELinux

```

root@rodvishh:~# getenforce
Disabled
root@rodvishh:~#

```

Рис. 2.5: SELinux

Попробовали переключить режим работы SELinux

```
root@rodvishh:~# setenforce 1
setenforce: SELinux is disabled
root@rodvishh:~#
```

Рис. 2.6: SELinux

В файле /etc/sysconfig/selinux с помощью редактора установили заданное значение

```
GNU nano 8.1
# 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/
#
# 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
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

^G Справка      ^O Записать     ^F Поиск       ^K Вырезать    ^T Выполнить
^X Выход        ^R ЧитФайл     ^\ Замена      ^U Вставить    ^J Вывод
```

Рис. 2.7: Изменение редактора

Просмотрели текущую информацию о состоянии SELinux


```

root@rodvishh:~# 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@rodvishh:~#

```

Рис. 2.8: SELinux

Посмотрели контекст безопасности файла /etc/hosts

```

root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#

```

Рис. 2.9: Контекст безопасности файла

Скопировали файл /etc/hosts в домашний каталог и проверили контекст файла ~/hosts

```

root@rodvishh:~# cp /etc/hosts ~/
root@rodvishh:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@rodvishh:~#

```

Рис. 2.10: Создание файла сценария

Попытались перезаписать существующий файл hosts из домашнего каталога в каталог /etc

```

root@rodvishh:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'?
root@rodvishh:~#

```

Рис. 2.11: Файл hosts

Убедились, что тип контекста по-прежнему установлен на admin_home_t

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 2.12: admin_home_t

Исправили контекст безопасности

```
root@rodvishh:~# restorecon -v /etc/hosts
root@rodvishh:~#
```

Рис. 2.13: Контекст безопасности

Убедились, что тип контекста изменился

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 2.14: Тип контекста

Для массового исправления контекста безопасности на файловой системе ввели

```
root@rodvishh:~# touch /.autorelabel
root@rodvishh:~#
```

Рис. 2.15: Массовое исправления контекста

Получаем полномочия администратора

```
rodvish@rodvishh:~$ sudo -i
[sudo] пароль для rodvish:
Попробуйте ещё раз.
[sudo] пароль для rodvish:
root@rodvishh:~#
```

Рис. 2.16: root

Устанавливаем необходимое программное обеспечение

```
rodvishh@rodvishh:~$ dnf -y install httpd
Rocky Linux 10 - BaseOS                               8.4 kB/s | 4.3 kB  00:00
Rocky Linux 10 - BaseOS                               4.8 MB/s | 22 MB  00:04
Rocky Linux 10 - AppStream                             8.3 kB/s | 4.3 kB  00:00
Rocky Linux 10 - AppStream                           286 kB/s | 2.2 MB  00:11
Rocky Linux 10 - CRB                                   7.6 kB/s | 4.3 kB  00:00
Rocky Linux 10 - CRB                                   38 kB/s | 531 kB  00:17
Rocky Linux 10 - Extras                               105 B/s | 3.1 kB  00:19
Rocky Linux 10 - Extras                               18 kB/s | 5.5 kB  00:00
Package httpd-2.4.63-1.el10.0.2.x86_64 уже установлен.
Зависимости разрешены.
Нет действий для выполнения.
Выполнено.
rodvishh@rodvishh:~$ dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:20 назад, СО 01 ноя 2025 14:53:33.
Зависимости разрешены.
-----
Пакет      Архитектура      Версия      Репозиторий      Размер
-----
Установка:
lynx       x86_64            2.9.0-6.el10      appstream         1.6 М
-----
Результат транзакции
-----
Установка: 1 Пакет
-----
Объем загрузки: 1.6 М
Объем изменений: 5.0 М
Загрузка пакетов:
lynx-2.9.0-6.el10.x86_64.rpm                               215 kB/s | 1.6 MB  00:07
-----
Общий размер
Проверка транзакции
Проверка транзакции успешно завершена.
Удаление транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
Подготовка
Установка: lynx-2.9.0-6.el10.x86_64                      1/1
Загрузка сертификата: lynx-2.9.0-6.el10.x86_64             1/1
```

Рис. 2.17: Необходимое программное обеспечение

Создали новое хранилище для файлов web-сервера

```
root@rodvishh:~# mkdir /web
root@rodvishh:~#
```

Рис. 2.18: Новое хранилище

Создали файл index.html в каталоге с контентом веб-сервера и поместили в файл следующий текст

```
root@rodvishh:~# cd /web
root@rodvishh:/web# touch index.html
root@rodvishh:/web# echo "Welcome to my web-server" > /web/index.html
root@rodvishh:/web#
```

Рис. 2.19: index.html

Продельваем различные действия со строками в файле /etc/httpd/conf/httpd.conf

```
#
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#    AllowOverride None
#    Allow open access:
#    Require all granted
#</Directory>
<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
# Further relax access to the default document
```

Рис. 2.20: /etc/httpd/conf/httpd.conf

Запустили веб-сервер и службу httpd

```
root@rodvishh:/web# systemctl start httpd
root@rodvishh:/web# systemctl enable httpd
root@rodvishh:/web#
```

Рис. 2.21: Служба httpd и веб-сервер

Обратились к веб-серверу в текстовом браузере lynx

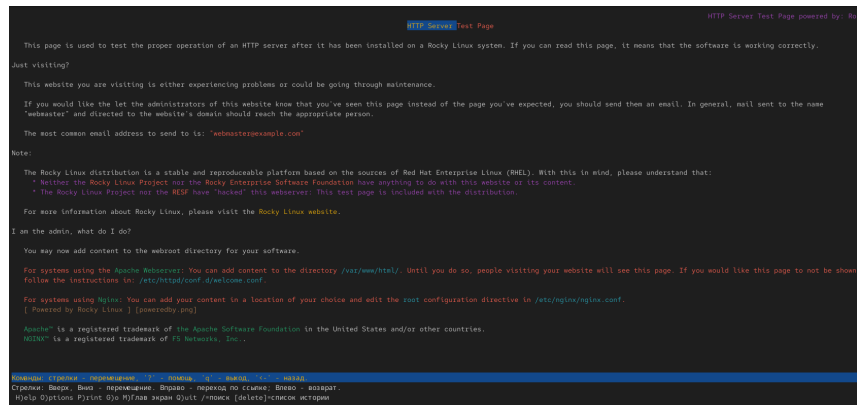


Рис. 2.22: lynx

В терминале с полномочиями администратора применили новую метку контекста к /web

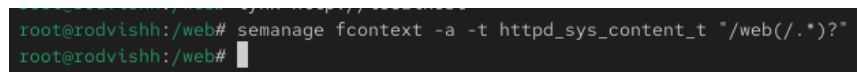


Рис. 2.23: Новая метку контекста к /web

Восстановили контекст безопасности

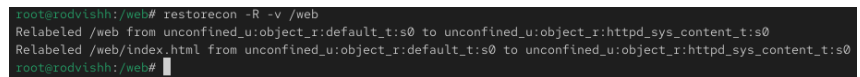


Рис. 2.24: Контекст безопасности

Снова обращаемся к веб-серверу

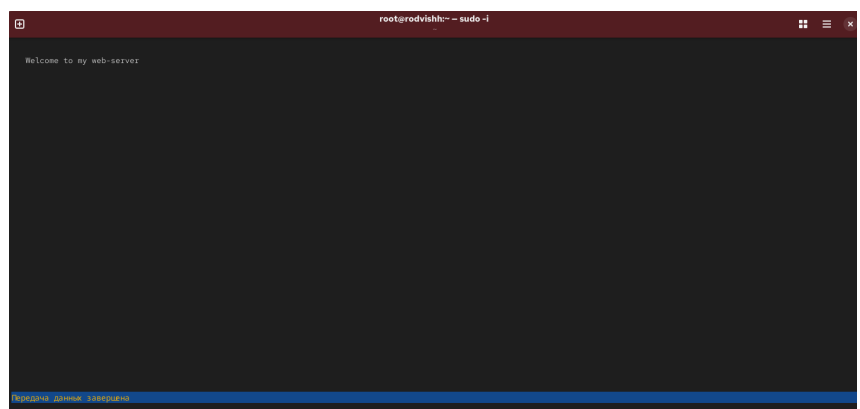


Рис. 2.25: Веб-сервер

Посмотрели список переключателей SELinux для службы ftp

```

root@rodvishh:~# 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@rodvishh:~#

```

Рис. 2.26: Список переключателей SELinux

Посмотрели список переключателей с пояснением

```

root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
root@rodvishh:~#

```

Рис. 2.27: Список переключателей с пояснением

Изменили текущее значение переключателя для службы ftpd_anon_write с off на on

```

root@rodvishh:~# setsebool ftpd_anon_write on
root@rodvishh:~#

```

Рис. 2.28: Значение переключателя

Повторно посмотрели список переключателей SELinux для службы ftpd_anon_write

```

root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. ,выкл.) Allow ftpd to anon write
root@rodvishh:~#

```

Рис. 2.29: Список переключателей SELinux

Изменили постоянное значение переключателя для службы ftpd_anon_write с off на on

```
root@rodvishh:~# setsebool -P ftpd_anon_write on
```

Рис. 2.30: Постоянное значение переключателя

Посмотрели список переключателей

```
root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (вкл. , вкл.) Allow ftpd to anon write
root@rodvishh:~#
```

Рис. 2.31: Список переключателей

3 Вывод

Мы получили навыки работы с контекстом безопасности и политиками SELinux.

4 Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? Ответ: Команда `setenforce 0`.
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? Ответ: Команда `getsebool -a`.
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? Ответ: Имя пакета `setroubleshoot`.
4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`? Ответ: Команда `chcon -t httpd_sys_content_t /web` или команды `semanage fcontext -a -t httpd_sys_content_t '/web(/.*)?'` и затем `restorecon -Rv /web`.
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? Ответ: Файл `/etc/selinux/config`.
6. Где SELinux регистрирует все свои сообщения? Ответ: В журнале аудита `/var/log/audit/audit.log` и в системном журнале `/var/log/messages`.
7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию? Ответ: Команда `sepolicy ftp` или `semanage boolean -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? Ответ: Временно перевести SELinux в разрешающий режим с помощью команды `setenforce 0` и проверить, исчезла ли проблема.