

Отчёт по лабораторной работе №9

Управление SELinux

Щемелев Илья Владимирович

Содержание

| | |
|---------------------------------------------------------------------------------------------------|-----------|
| 1 Цель работы | 5 |
| 2 Ход выполнения | 6 |
| 2.1 Управление режимами SELinux | 6 |
| 2.2 Использование restorecon для восстановления контекста безопасности | 12 |
| 2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера | 14 |
| 2.4 Работа с переключателями SELinux | 19 |
| 3 Контрольные вопросы | 21 |
| 4 Заключение | 23 |

Список иллюстраций

| | |
|------------------------------------------------------------------|----|
| 2.1 Проверка состояния SELinux | 8 |
| 2.2 Отключение SELinux в конфигурации | 9 |
| 2.3 Попытка включения SELinux без перезагрузки | 10 |
| 2.4 Возврат режима Enforcing | 11 |
| 2.5 Проверка SELinux после перемаркировки | 12 |
| 2.6 Контекст файла /etc/hosts | 13 |
| 2.7 Сообщения перемаркировки во время загрузки | 14 |
| 2.8 Изменение конфигурации httpd | 16 |
| 2.9 Тестовая страница Apache по умолчанию | 17 |
| 2.10 Применение контекста безопасности к каталогу /web | 18 |
| 2.11 Отображение пользовательской веб-страницы | 18 |
| 2.12 Список FTP-переключателей SELinux | 19 |

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Ход выполнения

2.1 Управление режимами SELinux

1. Запущен терминал и получены полномочия администратора с помощью команды `su -`.

Это позволило выполнять действия, требующие прав суперпользователя, и управлять настройками безопасности системы.

2. Для получения подробной информации о текущем состоянии SELinux выполнена команда `sestatus -v`.

В результате на экран выведены следующие сведения (пояснение построчно):

- **SELinux status: enabled** – SELinux включён и функционирует.
- **SELinuxfs mount: /sys/fs/selinux** – служебная файловая система SELinux смонтирована по указанному пути.
- **SELinux root directory: /etc/selinux** – каталог, содержащий конфигурацию SELinux.
- **Loaded policy name: targeted** – загружена политика типа *targeted* (защищаются ключевые службы/процессы).
- **Current mode: enforcing** – активен принудительный режим применения политики (нарушения блокируются).
- **Mode from config file: enforcing** – в конфигурации также установлен режим *enforcing*.

- **Policy MLS status: enabled** — поддержка MLS (многоуровневая защита) активна.
- **Policy deny_unknown status: allowed** — неизвестные действия не запрещаются автоматически (разрешены).
- **Memory protection checking: actual (secure)** — включена проверка механизмов защиты памяти.
- **Max kernel policy version: 33** — максимальная версия политики, поддерживаемая ядром.

Далее выводится раздел контекстов:

- **Process contexts** — контексты безопасности для процессов.
 - **Current context: unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023** — текущий пользовательский сеанс выполняется в домене *unconfined_t* (ограничения SELinux минимальны).
 - **Init context: system_u:system_r:init_t:s0** — контекст процесса инициализации.
 - **/usr/sbin/sshd: system_u:system_r:sshd_t:s0-s0:c0.c1023** — SSH-сервер работает в домене *sshd_t* (типичный защищаемый домен targeted-политики).
- **File contexts** — контексты безопасности для файлов/объектов.
 - **Controlling terminal: unconfined_u:object_r:user_devpts_t:s0** — контекст псевдотерминала пользователя.
 - **/etc/passwd: system_u:object_r:passwd_file_t:s0** — файл паролей имеет тип *passwd_file_t*.
 - **/etc/shadow: system_u:object_r:shadow_t:s0** — файл хэшей паролей имеет тип *shadow_t*.
 - **/bin/bash: system_u:object_r:shell_exec_t:s0** — исполняемый файл оболочки имеет тип *shell_exec_t*.
 - **/bin/login: system_u:object_r:login_exec_t:s0** — исполняемый файл *login* имеет тип *login_exec_t*.

- **/bin/sh → system_u:object_r:shell_exec_t:s0** – для sh указан тип исполняемого файла оболочки.
- **/sbin/agetty: system_u:object_r:getty_exec_t:s0** – getty имеет тип *getty_exec_t*.
- **/sbin/init → system_u:object_r:init_exec_t:s0** – init имеет тип *init_exec_t*.
- **/usr/sbin/sshd: system_u:object_r:sshd_exec_t:s0** – бинарный файл sshd имеет тип *sshd_exec_t*.

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

Рис. 2.1: Проверка состояния SELinux

3. Для определения режима работы SELinux выполнена команда `getenforce`.

В ответ получено значение **Enforcing** (Enforcing), что означает принуди-

тельное применение политики.

4. Выполнено переключение SELinux в разрешающий режим командой `setenforce 0`.

После этого повторно введена команда `getenforce`, получено значение **Permissive**.

В режиме permissive нарушения не блокируются, а только фиксируются в журналах.

5. Для полного отключения SELinux выполнено редактирование файла `/etc/sysconfig/selinux` в редакторе nano.

Установлено значение параметра:

- `SELINUX=disabled`

После сохранения изменений выполнена перезагрузка системы.

```
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=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 в конфигурации

6. После перезагрузки снова запущен терминал и получены права администратора.

7. Выполнена проверка статуса командой `getenforce`.

Получено значение **Disabled**, что означает, что SELinux полностью отключён.

8. Выполнена попытка переключить режим SELinux командой `setenforce 1`.

Система вывела сообщение об ошибке, указывающее, что SELinux отключён. Это подтверждает невозможность переключения режимов при отключённом SELinux без перезагрузки системы.

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

Рис. 2.3: Попытка включения SELinux без перезагрузки

9. Файл `/etc/sysconfig/selinux` снова открыт и параметр изменён на:

- `SELINUX=enforcing`

После сохранения изменений выполнена перезагрузка.

```
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
```

Рис. 2.4: Возврат режима Enforcing

10. Во время загрузки появилось предупреждение о необходимости восстановления меток SELinux.

Система запустила перемаркировку файловой системы (relabelling), что может занимать продолжительное время и сопровождаться дополнительной перезагрузкой.

11. После загрузки системы снова выполнена команда `sestatus -v`.

Полученная информация подтвердила, что SELinux включён и работает в режиме **enforcing**.

```
ivschemelev@ivschemelev:~$ su
Password:
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# █
```

Рис. 2.5: Проверка SELinux после перемаркировки

2.2 Использование restorecon для восстановления

контекста безопасности

1. Запущен терминал и получены полномочия администратора.
2. Просмотрен контекст безопасности файла `/etc/hosts` с помощью команды `ls -Z /etc/hosts`.

В результате установлено, что файл имеет контекст типа **net_conf_t**, соответствующий сетевым конфигурационным файлам.

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

Рис. 2.6: Контекст файла /etc/hosts

3. Файл /etc/hosts скопирован в домашний каталог командой `cp /etc/hosts ~/`.

После копирования проверен контекст файла ~/hosts командой `ls -Z ~/hosts`.

Контекст изменился на **admin_home_t**, так как копирование в домашний каталог создаёт новый файл с типичным домашним контекстом.

4. Выполнена попытка заменить существующий файл /etc/hosts перемещением файла из домашнего каталога: `mv ~/hosts /etc`.

Операция подтверждена пользователем.

5. Проверено, что после перемещения файл /etc/hosts сохранил неверный контекст **admin_home_t**, что подтверждено выводом команды `ls -Z /etc/hosts`.

6. Для восстановления корректного контекста выполнена команда `restorecon -v /etc/hosts`.

Опция `-v` вывела информацию о процессе исправления контекста.

7. Повторно проверен контекст командой `ls -Z /etc/hosts`.

Установлено, что тип контекста изменился на корректный **net_conf_t**.

8. Для массового исправления контекстов безопасности на файловой системе создан файл /.autorelabel командой touch /.autorelabel, после чего выполнена перезагрузка системы.

Во время загрузки были отображены сообщения о выполнении автоматической перемаркировки файловой системы.

```
[ OK ] Starting systemd-tmpfiles-setup.service - Create System Files and Directories...
[ OK ] 1 Finished plymouth-read-write.service - Tell Plymouth To Write Out Runtime Data.
[ OK ] 1 Finished systemd-tmpfiles-setup.service - Create System Files and Directories.
      Starting systemd-update-utmp.service - Record System Boot/Shutdown in UTMP...
[ OK ] 1 Finished systemd-update-utmp.service - Record System Boot/Shutdown in UTMP.
[ OK ] 1 Reached target sysinit.target - System Initialization.
[ OK ] 1 Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] 1 Reached target sound.target - Sound Card.
      Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
      Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] 1 Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
6.407416] selinux-autorelabel[1035]: *** Warning -- SELinux targeted policy relabel is required.
6.407591] selinux-autorelabel[1035]: *** Relabeling could take a very long time, depending on file
6.407752] selinux-autorelabel[1035]: *** system size and speed of hard drives.
6.409882] selinux-autorelabel[1035]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.7: Сообщения перемаркировки во время загрузки

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Запущен терминал и получены полномочия администратора, что позволило выполнять установку программного обеспечения и изменять системные конфигурационные файлы.
2. Установлено необходимое программное обеспечение для работы веб-сервера и проверки его функционирования:
 - веб-сервер Apache HTTP Server (httpd);
 - текстовый веб-браузер lynx.
3. Создан новый каталог /web, который будет использоваться в качестве хранилища файлов веб-сервера.

Данный каталог выбран намеренно, чтобы продемонстрировать работу SELinux с нестандартным расположением веб-контента.

4. В каталоге /web создан файл index.html.

В файл помещён текст:

- **Welcome to my web-server**

Этот файл используется в качестве тестовой веб-страницы.

5. Выполнено редактирование конфигурационного файла веб-сервера /etc/httpd/conf/httpd.conf.

В ходе настройки:

- строка DocumentRoot "/var/www/html" закомментирована;
- добавлена новая строка DocumentRoot "/web", указывающая на нестандартный каталог с веб-контентом;
- закомментирован стандартный блок <Directory "/var/www"> ... </Directory>;
- добавлен новый блок:
 - <Directory "/web">
 - AllowOverride None
 - Require all granted
 - </Directory>

Данные изменения определяют правила доступа и разрешают веб-серверу обслуживать содержимое каталога /web.

```
GNU nano 8.1                               /etc/httpd/conf/httpd.conf
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# 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/"
#
DocumentRoot "/web"
<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
```

Рис. 2.8: Изменение конфигурации httpd

6. Веб-сервер запущен и добавлен в автозагрузку службы systemd.

При первоначальном обращении к веб-серверу отображается стандартная тестовая страница Rocky Linux, что указывает на то, что SELinux блокирует доступ к файлам в каталоге /web из-за некорректного контекста безопасности.

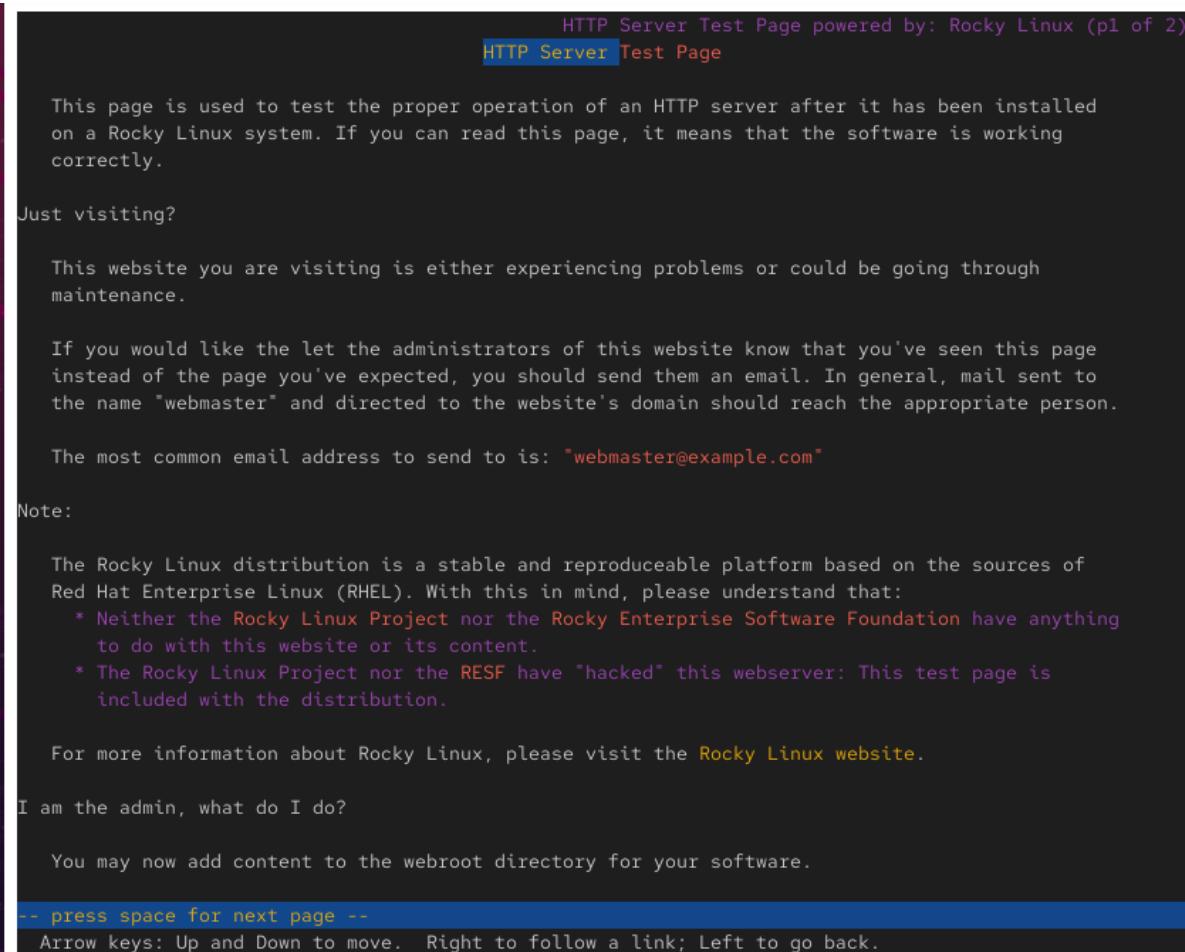


Рис. 2.9: Тестовая страница Apache по умолчанию

7. Под пользовательской учётной записью выполнено обращение к веб-серверу с помощью текстового браузера lynx по адресу `http://localhost`. Вместо пользовательской страницы отображена стандартная тестовая страница, что подтверждает ограничение доступа со стороны SELinux.
8. Для разрешения доступа веб-сервера к каталогу `/web` добавлено новое правило контекста безопасности SELinux.
Для каталога `/web` и всех вложенных файлов установлен тип контекста **httpd_sys_content_t**, предназначенный для веб-контента Apache.
9. Выполнено восстановление контекста безопасности каталога `/web` и всех файлов внутри него.

В процессе восстановления отображены сообщения о смене контекста для каталога /web и файла index.html.

```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# mkdir /web
root@ivschemelev:/home/ivschemelev# cd /web
root@ivschemelev:/web# touch index.html
root@ivschemelev:/web# echo "Welcome to my web-server" > index.html
root@ivschemelev:/web# nano /etc/httpd/conf/httpd.conf
root@ivschemelev:/web#
root@ivschemelev:/web# systemctl start httpd
root@ivschemelev:/web# systemctl enable httpd
Failed to enable unit: Unit httpd.service does not exist
root@ivschemelev:/web# systemctl enable httpd
root@ivschemelev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@ivschemelev:/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@ivschemelev:/web# systemctl restart httpd
root@ivschemelev:/web#
```

Рис. 2.10: Применение контекста безопасности к каталогу /web

10. Повторно выполнено обращение к веб-серверу с помощью браузера lynx.

В результате успешно отображена пользовательская веб-страница с текстом **Welcome to my web-server**, что подтверждает корректную настройку SELinux для нестандартного расположения веб-контента.

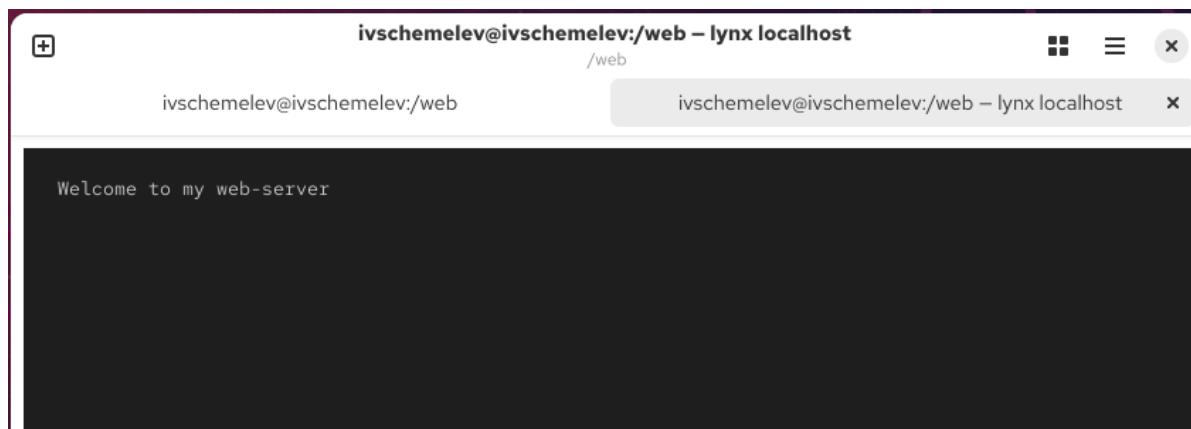


Рис. 2.11: Отображение пользовательской веб-страницы

2.4 Работа с переключателями SELinux

1. Запущен терминал и получены полномочия администратора.
2. Просмотрен список переключателей SELinux, относящихся к службе FTP.
В списке обнаружен переключатель **ftpd_anon_write**, имеющий текущее значение **off**, что означает запрет анонимной записи для FTP-службы.

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

Рис. 2.12: Список FTP-переключателей SELinux

3. Получен расширенный список переключателей для службы **ftpd_anon** с пояснениями.

Установлено, что:

- переключатель **ftpd_anon_write** разрешает или запрещает анонимную запись через FTP;
- временное и постоянное значения переключателя различаются.

4. Текущее (временное) значение переключателя **ftpd_anon_write** изменено

с **off** на **on**.

Это разрешило анонимную запись для FTP-службы до следующей перезагрузки системы.

5. Повторная проверка состояния переключателя показала, что **ftpd_anon_write** находится в состоянии **on** для текущего сеанса.
6. Повторно просмотрен список переключателей с пояснениями.

Установлено, что:

- временное значение переключателя включено;
- постоянное значение по-прежнему остаётся выключенным.

7. Выполнено включение постоянного значения переключателя **ftpd_anon_write**. Данное изменение сохраняется после перезагрузки системы.
8. После повторного просмотра списка переключателей установлено, что:

- временное значение переключателя **ftpd_anon_write – on**;
- постоянное значение переключателя **ftpd_anon_write – on**.

3 Контрольные вопросы

1. Для временного перевода SELinux в разрешающий режим используется команда:
 - **setenforce 0** — переводит SELinux в режим *Permissive*, при котором нарушения политики не блокируются, а только регистрируются в журналах.

Проверить текущий режим можно с помощью команды **getenforce**.
2. Для получения списка всех доступных переключателей SELinux применяется команда:
 - **getsebool -a** — выводит полный список всех SELinux boolean-переключателей и их текущие значения (on/off).
3. Для получения легко читаемых сообщений SELinux в журнале аудита необходимо установить пакет:
 - **setroubleshoot-server** — данный пакет анализирует события SELinux и формирует понятные диагностические сообщения, упрощающие поиск и устранение проблем.
4. Для применения типа контекста **httpd_sys_content_t** к каталогу `/web` необходимо выполнить следующие действия:
 - добавить правило для нового контекста безопасности, указывающее, что каталог `/web` и все вложенные файлы относятся к веб-контенту;
 - восстановить контексты безопасности для каталога `/web`.

Эти действия обеспечивают корректный доступ веб-сервера Apache к файлам, расположенным вне стандартного каталога `/var/www`.

5. Для полного отключения SELinux необходимо изменить конфигурационный файл:

- **/etc/sysconfig/selinux**

В данном файле параметру `SELINUX` должно быть присвоено значение `disabled`.

Изменения вступают в силу только после перезагрузки системы.

6. SELinux регистрирует все свои сообщения в журнале аудита:

- **/var/log/audit/audit.log**

Именно в этом файле содержится подробная информация обо всех разрешённых и запрещённых действиях, связанных с политиками SELinux.

7. Для получения подробной информации о доступных типах контекстов и переключателях, относящихся к службе FTP, используется команда:

- **semanage boolean -l | grep ftp**

Она выводит список boolean-переключателей SELinux для FTP-службы с пояснением их назначения и текущего состояния.

8. Если сервис работает некорректно и требуется определить, связано ли это с SELinux, самым простым способом является:

- временный перевод SELinux в режим *Permissive*.

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

Дополнительно для анализа причин можно изучить журнал аудита SELinux.

4 Заключение

В ходе выполнения лабораторной работы были изучены принципы работы механизма SELinux, способы управления его режимами и средствами контроля доступа. Были освоены методы временного и постоянного изменения режима работы SELinux, а также процедуры восстановления контекстов безопасности. Практически продемонстрирована настройка SELinux для обеспечения корректной работы веб-сервера с нестандартным расположением файлов и использование переключателей безопасности (boolean). Полученные результаты подтверждают, что корректная настройка SELinux позволяет повысить уровень безопасности системы без нарушения работоспособности сервисов.