

Отчёт по лабораторной работе №9

Управление SELinux

Эзиз Хатамов

Содержание

| | | |
|----------|--|-----------|
| 1 | Цель работы | 5 |
| 2 | Отчёт по выполнению работы | 6 |
| 2.1 | Управление режимами SELinux | 6 |
| 2.2 | Восстановление контекста безопасности с помощью restorecon . . | 10 |
| 2.3 | Настройка контекста безопасности для нестандартного расположе- ния файлов веб-сервера | 11 |
| 2.4 | Работа с переключателями SELinux | 14 |
| 3 | Контрольные вопросы | 16 |
| 4 | Заключение | 18 |

Список иллюстраций

| | | |
|------|---|----|
| 2.1 | Вывод команды <code>sestatus -v</code> | 7 |
| 2.2 | Переключение режима SELinux в Permissive | 8 |
| 2.3 | Изменение файла <code>/etc/sysconfig/selinux</code> — отключение SELinux . . . | 8 |
| 2.4 | SELinux отключён | 9 |
| 2.5 | Включение режима <code>enforcing</code> в конфигурационном файле | 9 |
| 2.6 | Автоматическое перемаркирование при загрузке системы | 10 |
| 2.7 | SELinux включён и работает в режиме <code>Enforcing</code> | 10 |
| 2.8 | Использование <code>restorecon</code> и автоматического перемаркирования . | 11 |
| 2.9 | Изменение конфигурации <code>DocumentRoot</code> и <code>Directory</code> | 12 |
| 2.10 | Стандартная тестовая страница Rocky Linux | 13 |
| 2.11 | Применение контекста безопасности для каталога <code>/web</code> | 13 |
| 2.12 | Отображение пользовательской страницы веб-сервера | 14 |
| 2.13 | Проверка и изменение переключателей SELinux для <code>ftpd_anon_write</code> | 15 |

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Отчёт по выполнению работы

2.1 Управление режимами SELinux

1. В терминале были получены полномочия администратора с помощью команды **su -**.
2. Для просмотра текущего состояния SELinux выполнена команда **sestatus -v**.

Вывод показал:

- **SELinux status: enabled** — SELinux включён.
- **SELinuxfs mount: /sys/fs/selinux** — точка монтирования файловой системы SELinux.
- **SELinux root directory: /etc/selinux** — каталог, где хранятся политики SELinux.
- **Loaded policy name: targeted** — используется целевая политика (защищаются только отдельные процессы).
- **Current mode: enforcing** — принудительный режим, в котором политика SELinux активно применяется.

- **Mode from config file:** enforcing — значение по умолчанию установлено в конфигурации.
- **Policy MLS status:** enabled — многоуровневая система безопасности (MLS) включена.
- **Policy deny_unknown status:** allowed — неизвестные объекты разрешены.
- **Memory protection checking:** actual (secure) — защита памяти активна.
- **Max kernel policy version:** 33 — версия политики ядра.

```

ehatamov@ehatamov:~$ su
Password:
root@ehatamov:/home/ehatamov# sestatus -v
bash: sestatus: command not found...
root@ehatamov:/home/ehatamov# 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

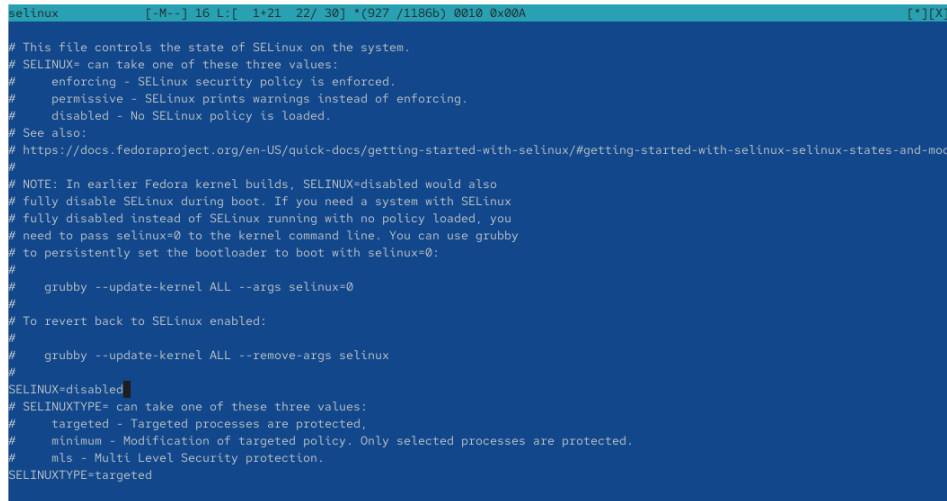
File contexts:
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
/bin/bash                     system_u:object_r:shell_exec_t:s0
/bin/login                    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@ehatamov:/home/ehatamov# getenforce
Enforcing
root@ehatamov:/home/ehatamov# setenforce 0
root@ehatamov:/home/ehatamov# getenforce
Permissive
root@ehatamov:/home/ehatamov# █

```

Рис. 2.1: Вывод команды sestatus -v

3. С помощью команды **getenforce** определён текущий режим SELinux — **Enforcing**.
4. Командой **setenforce 0** режим был изменён на **Permissive**, что подтверждено повторным вызовом **getenforce**.

В этом режиме SELinux не блокирует действия, а только регистрирует возможные нарушения.



```
selinux [~M~] 16 L:[ 1*21 22/ 30] *(927 /1186b) 0010 0x00A [*][X]
# 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-states-and-mod
#
# 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
```

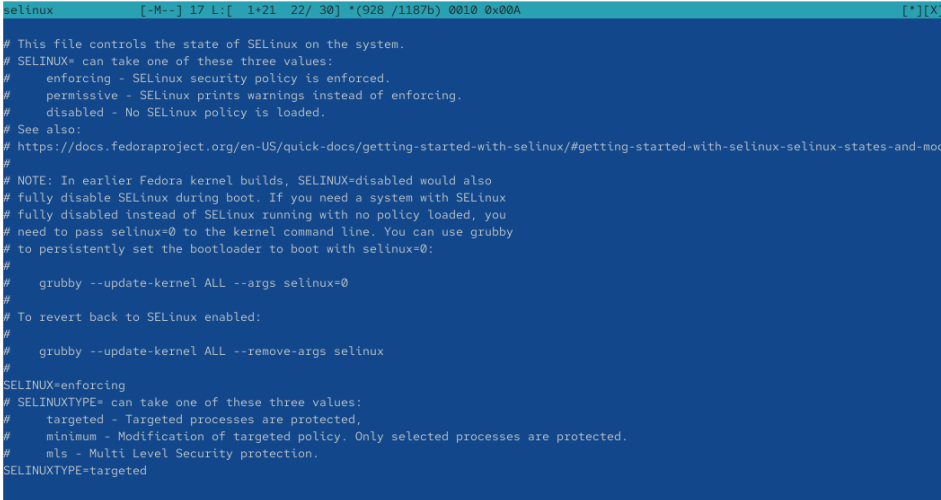
Рис. 2.2: Переключение режима SELinux в Permissive

5. В конфигурационном файле **/etc/sysconfig/selinux** параметр **SELINUX** изменён на значение **disabled**, что полностью отключает SELinux после загрузки системы.

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

Рис. 2.3: Изменение файла **/etc/sysconfig/selinux** — отключение SELinux

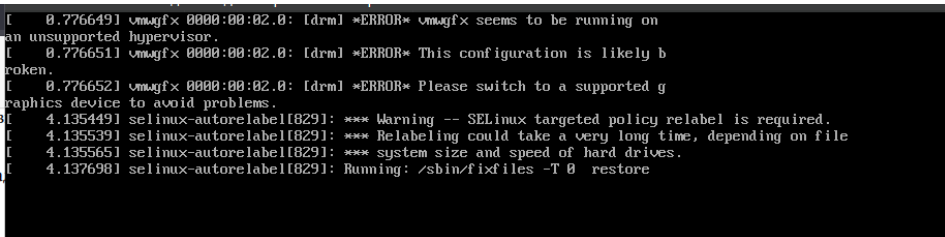
6. После перезагрузки системы выполнена команда **getenforce**, показавшая результат **Disabled**, что подтверждает успешное отключение SELinux.



```
selinux [~M--] 17 L: [ 1+21 22/ 30] *(928 /1187b) 0010 0x00A [*][X]
# 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-states-and-mod
#
# 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: SELinux отключён

7. Попытка включить SELinux командой **setenforce 1** завершилась сообщением “**SELinux is disabled**”, что подтверждает невозможность переключения между режимами без перезагрузки.
8. В файле **/etc/sysconfig/selinux** параметр был снова изменён на **SELINUX=enforcing**, после чего система перезагружена.



```
[ 0.776649] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.776651] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.776652] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 4.135449] selinux-autorelabel[829]: *** Warning -- SELinux targeted policy relabel is required.
[ 4.135539] selinux-autorelabel[829]: *** Relabeling could take a very long time, depending on file
[ 4.135565] selinux-autorelabel[829]: *** system size and speed of hard drives.
[ 4.137698] selinux-autorelabel[829]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.5: Включение режима enforcing в конфигурационном файле

9. При загрузке системы появилось предупреждение “**SELinux targeted policy relabel is required**” — система автоматически перемаркировала файлы для восстановления корректных контекстов безопасности.

```

root@ehatamov: /home/ehatamov#
root@ehatamov:/home/ehatamov# 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@ehatamov:/home/ehatamov# █

```

Рис. 2.6: Автоматическое перемаркирование при загрузке системы

10. После завершения загрузки команда **sestatus -v** подтвердила, что SELinux снова работает в режиме **Enforcing**.

```

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

```

Рис. 2.7: SELinux включён и работает в режиме Enforcing

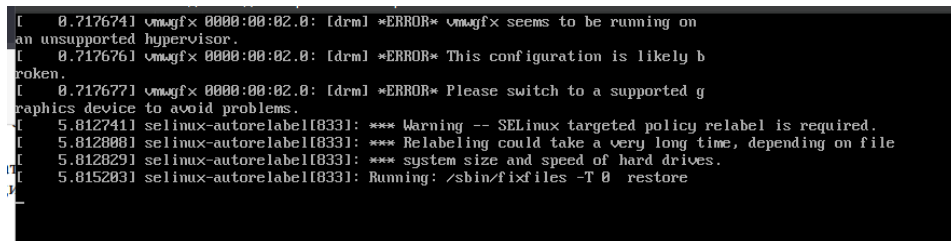
2.2 Восстановление контекста безопасности с помощью restorecon

1. В терминале с полномочиями администратора просмотрен контекст безопасности файла **/etc/hosts** с помощью команды **ls -Z /etc/hosts**.

Тип контекста — **net_conf_t**.

2. Файл **/etc/hosts** был скопирован в домашний каталог, где его контекст изменился на **admin_home_t**, так как копирование создаёт новый файл.
3. После возврата файла в каталог **/etc** командой **mv ~/hosts /etc**, его контекст остался **admin_home_t**, что неверно.
4. Для восстановления корректного контекста применена команда **restorecon -v /etc/hosts**, после чего контекст был успешно изменён обратно на **net_conf_t**.
5. Для массового восстановления контекстов была создана специальная метка командой **touch /.autorelabel**.

После перезагрузки система автоматически перемаркировала файлы, что отразилось в загрузочных сообщениях.



```
[ 0.717674] vmxgf 0000:00:02.0: [drm] *ERROR* vmxgf seems to be running on
an unsupported hypervisor.
[ 0.717676] vmxgf 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.717677] vmxgf 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 5.812741] selinux-autorelabel[8331]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.812808] selinux-autorelabel[8331]: *** Relabeling could take a very long time, depending on file
[ 5.812829] selinux-autorelabel[8331]: *** system size and speed of hard drives.
[ 5.815203] selinux-autorelabel[8331]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.8: Использование **restorecon** и автоматического перемаркирования

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

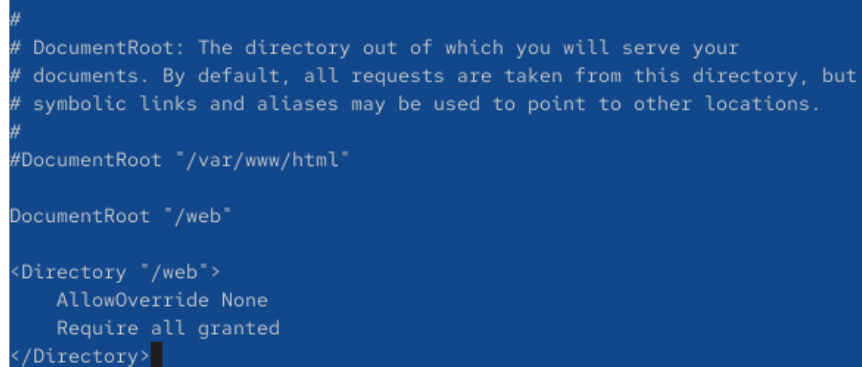
1. В терминале были получены полномочия администратора и установлены необходимые пакеты **httpd** и **lynx**. Это обеспечило возможность запуска веб-сервера Apache и проверки его работы через текстовый браузер.

2. Создан каталог /web, предназначенный для хранения файлов веб-сервера, и в нём создан файл index.html со строкой: Welcome to my web-server.
3. В конфигурационном файле /etc/httpd/conf/httpd.conf была закомментирована стандартная строка DocumentRoot "/var/www/html" и добавлена новая строка DocumentRoot "/web". Также был изменён раздел Directory, определяющий политику доступа:

AllowOverride None

Require all granted

Это разрешает доступ ко всем ресурсам каталога /web без ограничений.



```
#  
# 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. 2.9: Изменение конфигурации DocumentRoot и Directory

4. После перезапуска службы httpd при обращении к веб-серверу через lynx <http://localhost> отобразилась стандартная страница теста Rocky Linux. Это свидетельствует о том, что SELinux заблокировал доступ к новому каталогу /web.

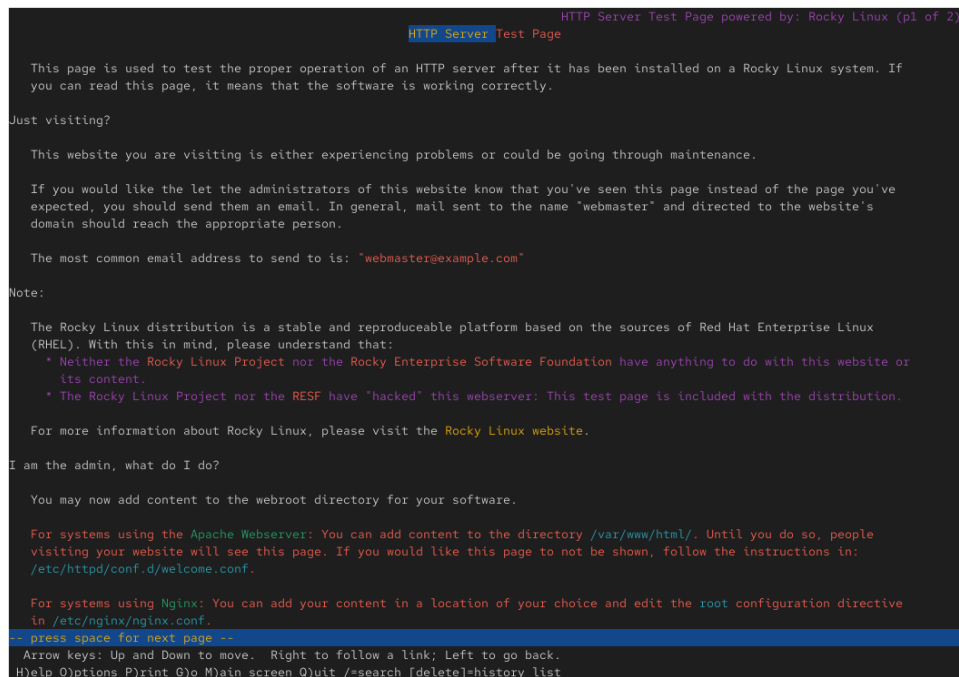


Рис. 2.10: Стандартная тестовая страница Rocky Linux

5. Для устранения этой проблемы новому каталогу был присвоен корректный контекст безопасности. Сначала добавлено новое правило контекста для каталога /web с типом httpd_sys_content_t, затем выполнено восстановление контекста. В результате каталогу /web и файлу index.html был назначен правильный тип безопасности, что позволило веб-серверу обращаться к содержимому.

```

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

```

Рис. 2.11: Применение контекста безопасности для каталога /web

6. После повторного обращения к серверу через браузер lynx страница успешно отобразила текст: Welcome to my web-server. Это подтверждает правильную настройку контекста безопасности.

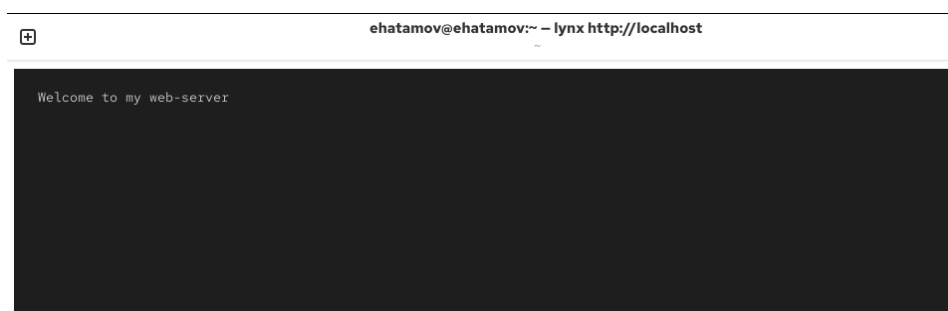


Рис. 2.12: Отображение пользовательской страницы веб-сервера

2.4 Работа с переключателями SELinux

1. После получения прав администратора был выполнен просмотр всех переключателей SELinux, связанных со службой ftp. Из вывода видно, что параметр `ftpd_anon_write` имеет значение `off`, что означает запрет на анонимную запись.
2. Для получения более подробной информации использовалась команда для вывода всех доступных переключателей `ftpd_anon`, что показало их текущее состояние и назначение — `Allow ftpd to anon write`.
3. Значение переключателя `ftpd_anon_write` было изменено на `on`. После проверки состояние изменилось на активное, что означает включение временной настройки.
4. Для сохранения изменения между перезагрузками параметр был установлен с постоянным флагом. Повторная проверка подтвердила, что `ftpd_anon_write` теперь активен как во временной, так и в постоянной конфигурации.

```

ehatamov@ehatamov:~$ lynx http://localhost
ehatamov@ehatamov:~$
ehatamov@ehatamov:~$ su
Password:
root@ehatamov:/home/ehatamov#
root@ehatamov:/home/ehatamov# 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@ehatamov:/home/ehatamov# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@ehatamov:/home/ehatamov# setsebool ftpd_anon_write on
root@ehatamov:/home/ehatamov# getsebool ftpd_anon_write
ftpd_anon_write --> on
root@ehatamov:/home/ehatamov# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
root@ehatamov:/home/ehatamov# setsebool -P ftpd_anon_write on
root@ehatamov:/home/ehatamov# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
root@ehatamov:/home/ehatamov# █

```

Рис. 2.13: Проверка и изменение переключателей SELinux для ftpd_anon_write

3 Контрольные вопросы

1. **Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**
 - `setenforce 0` — временно переводит SELinux в разрешающий режим (**Permissive**) без перезагрузки системы.
2. **Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**
 - `getsebool -a` — отображает список всех доступных переключателей SELinux и их текущие состояния.
3. **Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**
 - Пакет **setroubleshoot** — обеспечивает расшифровку и понятное представление сообщений SELinux в системных журналах.
4. **Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?**
 - `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` — добавляет правило для каталога `/web`.
 - `restorecon -R -v /web` — применяет новое правило и изменяет контекст безопасности каталога и его содержимого.

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

- `/etc/sysconfig/selinux` — конфигурационный файл, где параметр **SELINUX** устанавливается в значение **disabled**.

6. Где SELinux регистрирует все свои сообщения?

- Все сообщения SELinux записываются в файл `/var/log/audit/audit.log`.

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

- `semanage fcontext -l | grep ftp` — показывает все доступные типы контекстов, связанные со службой 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?

- `setenforce 0` — временно перевести SELinux в разрешающий режим (**Permissive**) и проверить, устранится ли проблема. Если сервис заработал, причина связана с политикой SELinux.

4 Заключение

В ходе лабораторной работы были изучены принципы работы механизма SELinux, его режимы функционирования (**Enforcing**, **Permissive**, **Disabled**) и способы их изменения. На практике была выполнена настройка контекста безопасности для нестандартного каталога веб-сервера, что позволило обеспечить корректное взаимодействие Apache с системой безопасности.