

Отчёт по лабораторной работе №9

Управление SELinux

Максат Хемраев

Содержание

| | | |
|----------|---|-----------|
| 1 | Цель работы | 5 |
| 2 | Отчёт по выполнению работы | 6 |
| 2.1 | Управление режимами SELinux | 6 |
| 2.2 | Использование restorecon для восстановления контекста безопасности | 10 |
| 2.3 | Настройка контекста безопасности для нестандартного расположения файлов веб-сервера | 11 |
| 2.4 | Работа с переключателями SELinux | 14 |
| 3 | Контрольные вопросы | 16 |
| 3.0.1 | 1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? | 16 |
| 3.0.2 | 2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? | 16 |
| 3.0.3 | 3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? | 17 |
| 3.0.4 | 4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd_sys_content_t к каталогу /web? | 17 |
| 3.0.5 | 5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? | 17 |
| 3.0.6 | 6. Где SELinux регистрирует все свои сообщения? | 18 |
| 3.0.7 | 7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? | 18 |
| 3.0.8 | 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? | 18 |
| 4 | Заключение | 19 |

Список иллюстраций

| | | |
|------|---|----|
| 2.1 | Вывод команды <code>sestatus -v</code> | 6 |
| 2.2 | Изменение конфигурации SELinux на <code>disabled</code> | 8 |
| 2.3 | Отключённый SELinux и реакция на <code>setenforce 1</code> | 9 |
| 2.4 | Изменение конфигурации SELinux на <code>enforcing</code> | 9 |
| 2.5 | Предупреждение о релабелинге при загрузке системы | 10 |
| 2.6 | Восстановление контекста безопасности файла <code>/etc/hosts</code> | 11 |
| 2.7 | Автоматическая перемаркировка контекстов при загрузке системы | 11 |
| 2.8 | Изменение параметров конфигурации Apache | 12 |
| 2.9 | Тестовая страница Apache по умолчанию | 13 |
| 2.10 | Применение контекста безопасности к каталогу <code>/web</code> | 13 |
| 2.11 | Отображение пользовательской веб-страницы | 14 |
| 2.12 | Настройка переключателей SELinux для FTP | 15 |

Список таблиц

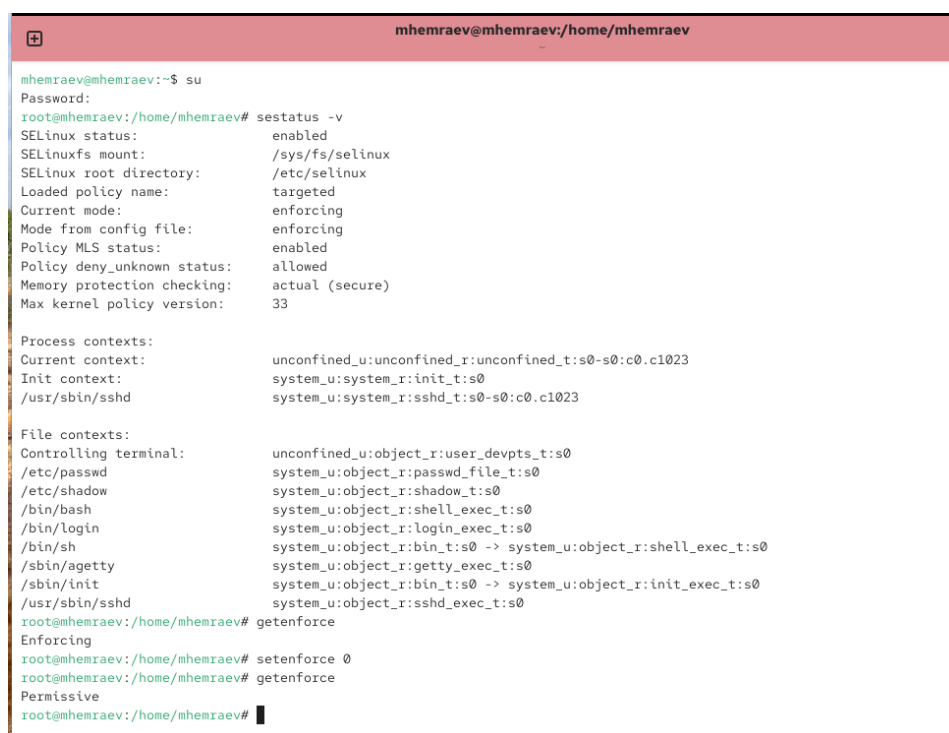
1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Отчёт по выполнению работы

2.1 Управление режимами SELinux

1. После входа в систему под пользователем **mhemraev** были получены полномочия администратора с помощью команды `su`. Затем была выполнена проверка состояния системы безопасности SELinux.



```
mhemraev@mhemraev:~/home/mhemraev
mhemraev@mhemraev:~$ su
Password:
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# getenforce
Enforcing
root@mhemraev:/home/mhemraev# setenforce 0
root@mhemraev:/home/mhemraev# getenforce
Permissive
root@mhemraev:/home/mhemraev#
```

Рис. 2.1: Вывод команды `sestatus -v`

На экране отобразились следующие параметры:

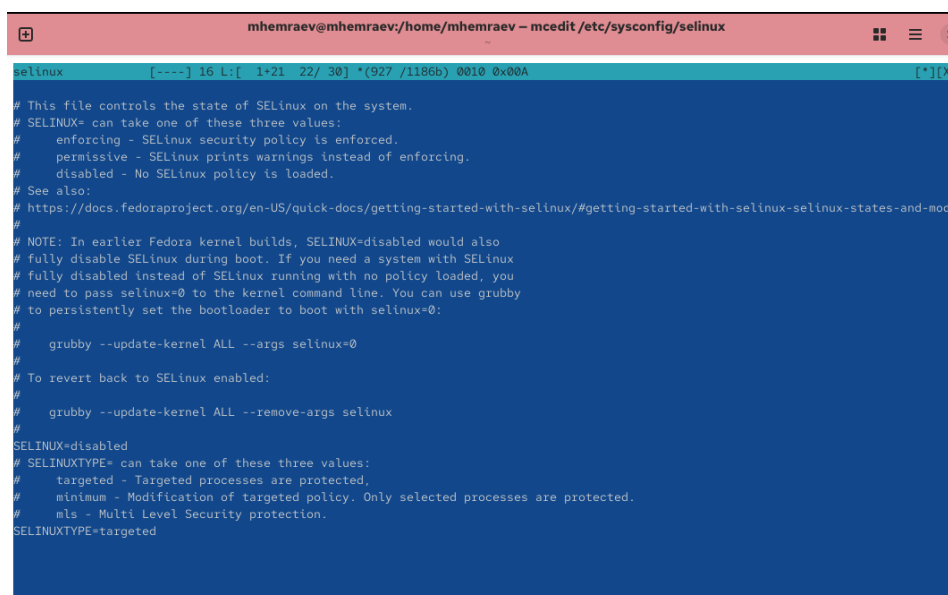
- **SELinux status: enabled** — система безопасности SELinux активна.
- **SELinuxfs mount: /sys/fs/selinux** — каталог монтирования файловой системы SELinux.
- **SELinux root directory: /etc/selinux** — расположение корневых конфигурационных файлов SELinux.
- **Loaded policy name: targeted** — активна политика типа *targeted*, при которой защите подвергаются только критические системные процессы.
- **Current mode: enforcing** — в данный момент SELinux работает в режиме принудительного контроля доступа.
- **Mode from config file: enforcing** — аналогичный режим задан в конфигурационном файле.
- **Policy MLS status: enabled** — включена поддержка многоуровневой защиты (Multi Level Security).
- **Policy deny_unknown status: allowed** — неизвестные операции разрешены.
- **Memory protection checking: actual (secure)** — защита памяти активна.

В разделе **Process contexts** приведены контексты безопасности для различных процессов, например:

- `/usr/sbin/sshd` выполняется с контекстом `system_u:system_r:sshd_t:s0-s0:c0.c1023`.

А в разделе **File contexts** указаны контексты файлов — /etc/passwd, /etc/shadow, /bin/bash и других системных компонентов.

2. Далее была выполнена проверка режима работы SELinux с помощью команды `getenforce`, подтвердившая, что система находится в режиме **Enforcing**. После этого SELinux был переведён в **Permissive**-режим, при котором нарушения политик не блокируются, а только фиксируются в журнале. Повторная проверка показала изменение режима.
3. Затем был открыт конфигурационный файл /etc/sysconfig/selinux и изменён параметр `SELINUX=disabled`. После этого система была перезагружена.



```
mhemraev@mhemraev:/home/mhemraev - mcedit /etc/sysconfig/selinux
selinux [----] 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-states-and-modes
# 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
```

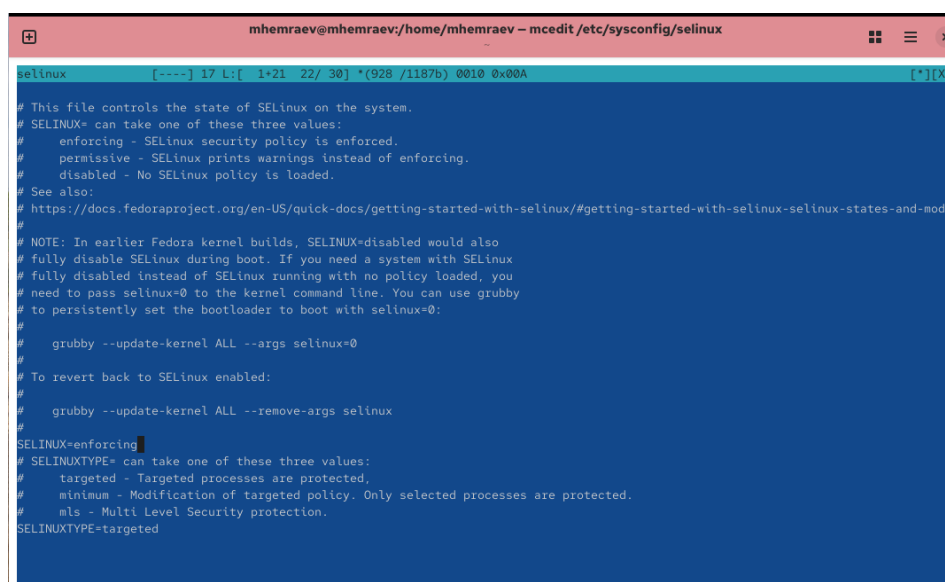
Рис. 2.2: Изменение конфигурации SELinux на disabled

4. После перезапуска проверка показала значение **Disabled**, что подтверждает полное отключение SELinux. Попытка переключить режим с помощью `setenforce 1` завершилась сообщением об ошибке, так как при отключённой системе SELinux изменение режима невозможно без перезагрузки.


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

Рис. 2.3: Отключённый SELinux и реакция на setenforce 1

5. Для восстановления контроля доступа снова был отредактирован файл `/etc/sysconfig/selinux`, в котором установлено значение `SELINUX=enforcing`.



```
mhemraev@mhemraev:/home/mhemraev - mcedit /etc/sysconfig/selinux
selinux [-----] 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-mode
# 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: Изменение конфигурации SELinux на enforcing

После очередной перезагрузки система выдала предупреждение о необходимости релабелинга (перемаркировки) контекстов SELinux. Этот процесс выполняется автоматически и может занять значительное время в зависимости от объёма данных.

```
Booting 'Rocky Linux (6.12.0-55.12.1.el10_0.x86_64) 10.0 (Red Quartz)'  
[ 0.934572] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 0.934574] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 0.934575] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 4.257749] selinux-autorelabel[781]: *** Warning -- SELinux targeted policy relabel is required.  
[ 4.258153] selinux-autorelabel[781]: *** Relabeling could take a very long time, depending on file  
[ 4.258183] selinux-autorelabel[781]: *** system size and speed of hard drives.  
[ 4.260685] selinux-autorelabel[781]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.5: Предупреждение о релабелинге при загрузке системы

6. После завершения загрузки и входа в систему проверка с помощью `sestatus -v` подтвердила, что SELinux снова работает в режиме **enforcing**, а система функционирует с активной политикой безопасности.

2.2 Использование `restorecon` для восстановления контекста безопасности

1. После получения прав администратора была выполнена проверка контекста файла `/etc/hosts`. Контекст определился как `system_u:object_r:net_conf_t:s0`.
2. Затем файл `/etc/hosts` был скопирован в домашний каталог пользователя. Новый файл получил контекст `unconfined_u:object_r:admin_home_t:s0`, поскольку копирование создаёт новый объект в домашнем каталоге.
3. Далее файл из домашнего каталога был перемещён обратно в `/etc`, что привело к сохранению контекста `admin_home_t`, не соответствующего системным стандартам.
4. Для исправления контекста была использована команда `restorecon -v /etc/hosts`. После выполнения тип контекста был возвращён к исходному значению `net_conf_t`, что соответствует корректной политике безопасности SELinux.

```

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

```

Рис. 2.6: Восстановление контекста безопасности файла /etc/hosts

- Для глобального восстановления контекстов безопасности на файловой системе была создана специальная метка /.autorelabel. После перезагрузки система автоматически начала процесс полной перемаркировки файлов, что видно по сообщениям во время загрузки.

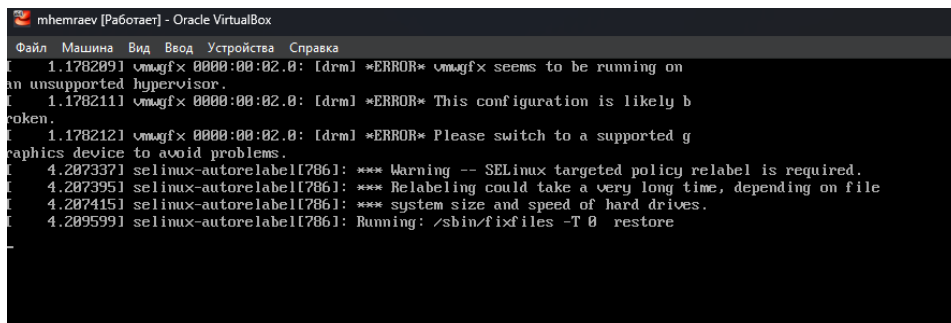
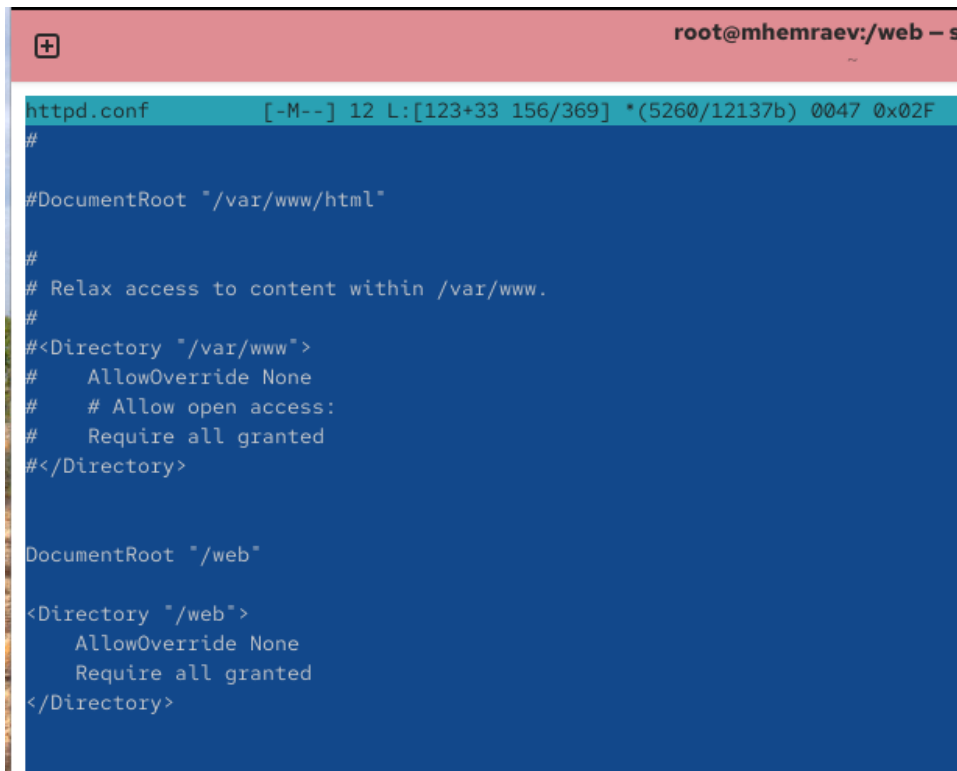


Рис. 2.7: Автоматическая перемаркировка контекстов при загрузке системы

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

- После получения прав администратора было установлено необходимое программное обеспечение — веб-сервер Apache (**httpd**) и текстовый браузер **lynx**.

2. Для хранения контента веб-сервера был создан новый каталог **/web**, внутри которого создан файл **index.html** с содержанием «Welcome to my web server».
3. В конфигурационном файле `/etc/httpd/conf/httpd.conf` была закомментирована стандартная строка
`DocumentRoot "/var/www/html"`
и добавлено новое значение
`DocumentRoot "/web"`.



```
httpd.conf [-M--] 12 L:[123+33 156/369] *(5260/12137b) 0047 0x02F
#
#DocumentRoot "/var/www/html"
#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#   AllowOverride None
#   # Allow open access:
#   Require all granted
#</Directory>

DocumentRoot "/web"

<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
```

Рис. 2.8: Изменение параметров конфигурации Apache

4. После сохранения изменений веб-сервер был запущен и добавлен в автозагрузку. Проверка в браузере **lynx** при обращении к адресу `http://localhost` показала стандартную тестовую страницу **Rocky Linux**, что свидетельствует о том, что SELinux блокирует доступ Apache к новому каталогу.

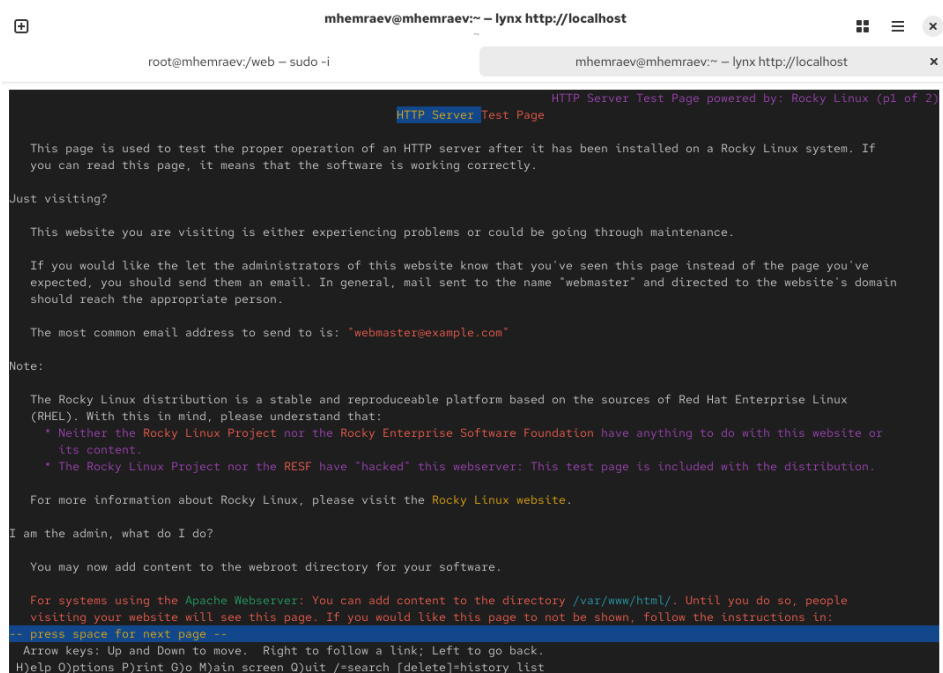


Рис. 2.9: Тестовая страница Apache по умолчанию

5. Для разрешения доступа веб-сервера к каталогу **/web** был создан новый контекст безопасности. С помощью команды `semanage fcontext` к каталогу и его содержимому была применена метка типа **httpd_sys_content_t**, предназначенная для статических веб-файлов.
6. Затем была выполнена команда `restorecon` для восстановления контекста безопасности в соответствии с новой политикой. В результате файлы в каталоге **/web** получили корректные метки безопасности.

```

root@mhemraev:~# mkdir /web
root@mhemraev:~# cd /web
root@mhemraev:/web# touch index.html
root@mhemraev:/web# echo "Welcome to my web server" > index.html
root@mhemraev:/web# mcedit /etc/httpd/conf/httpd.conf

root@mhemraev:/web#
root@mhemraev:/web# systemctl start httpd
root@mhemraev:/web# systemctl enable httpd
root@mhemraev:/web#
root@mhemraev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@mhemraev:/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@mhemraev:/web# systemctl restart httpd
root@mhemraev:/web#

```

Рис. 2.10: Применение контекста безопасности к каталогу **/web**

- После перезапуска службы **httpd** повторный запрос через **lynx** к `http://localhost` показал пользовательскую веб-страницу с сообщением «Welcome to my web server». Это подтвердило, что доступ настроен корректно, а SELinux больше не блокирует обращение Apache к пользовательскому каталогу.

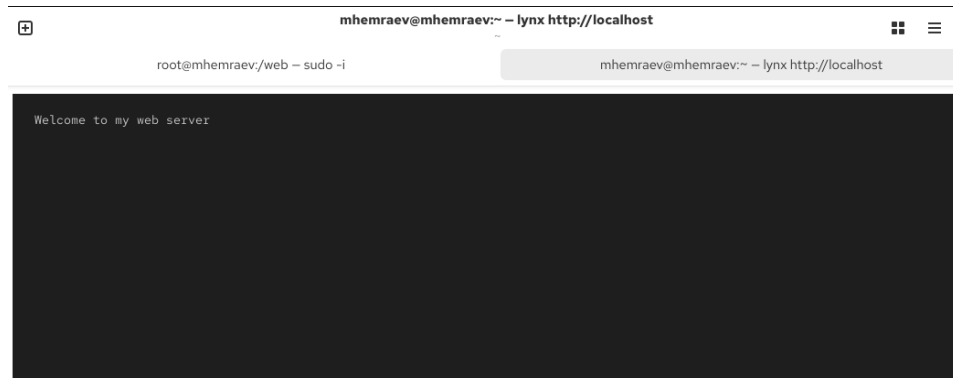


Рис. 2.11: Отображение пользовательской веб-страницы

2.4 Работа с переключателями SELinux

- После получения прав администратора был просмотрен список переключателей SELinux, связанных с протоколом FTP. Среди них параметр **ftpd_anon_write** имел значение *off*, что означает запрет на запись для анонимных пользователей.
- Для службы **ftpd_anon** был запрошен список доступных переключателей с их описанием, после чего выполнено изменение значения переключателя **ftpd_anon_write** на *on* с помощью команды `setsebool`.
- Повторная проверка показала, что временное значение переключателя изменилось на *on*, однако постоянная настройка оставалась прежней (*off*).

4. Для сохранения изменения в постоянной конфигурации был применён параметр **-P**, что позволило активировать запись для анонимных пользователей FTP на постоянной основе.
5. Финальная проверка с помощью команды `semanage boolean` подтвердила, что параметр **ftpd_anon_write** теперь имеет состояние **(on , on)** — то есть включён как во временной, так и в постоянной конфигурации SELinux.

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

Рис. 2.12: Настройка переключателей SELinux для FTP

3 Контрольные вопросы

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

- Для временного перевода SELinux в разрешающий режим используется команда:

```
setenforce 0
```

Она изменяет текущий режим на **Permissive** до следующей перезагрузки системы.

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

- Для просмотра полного списка переключателей SELinux применяется команда:

```
getsebool -a
```

Она отображает все доступные булевы параметры (boolean values) и их текущее состояние (*on* или *off*).

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

- Необходим пакет: **setroubleshoot**

Он обеспечивает расшифровку и удобное представление сообщений SELinux, поступающих в системный журнал.

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

- Необходимо выполнить две команды:

1. `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` — добавляет новое правило для каталога `/web` и его содержимого.
 2. `restorecon -R -v /web` — применяет изменения и обновляет контексты безопасности для всех файлов в каталоге.
-

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

- Нужно отредактировать файл конфигурации:

`/etc/sysconfig/selinux`

В нём следует установить параметр `SELINUX=disabled`, после чего требуется перезагрузка системы.

3.0.6 6. Где SELinux регистрирует все свои сообщения?

- Сообщения SELinux сохраняются в журнале аудита:

`/var/log/audit/audit.log`

При отсутствии этого файла информация может дублироваться в `/var/log/messages`.

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

- Для получения информации о контекстах, связанных с FTP-службой, используется команда:

`semanage fcontext -l | grep ftp`

Она выводит список всех определённых контекстов, связанных с файлами и каталогами службы FTP.

3.0.8 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 **Permissive**-режим:

`setenforce 0`

Если после этого сервис начнёт работать корректно, значит, проблема была вызвана политиками SELinux.

4 Заключение

В ходе работы были изучены принципы функционирования SELinux, отработаны практические навыки изменения режимов его работы, настройки контекстов безопасности и управления переключателями для обеспечения корректного и безопасного функционирования системных служб.