Лабораторная работа №9

Управление SELinux

Руслан Алиев

19 декабря 2025

Российский университет дружбы народов, Москва, Россия

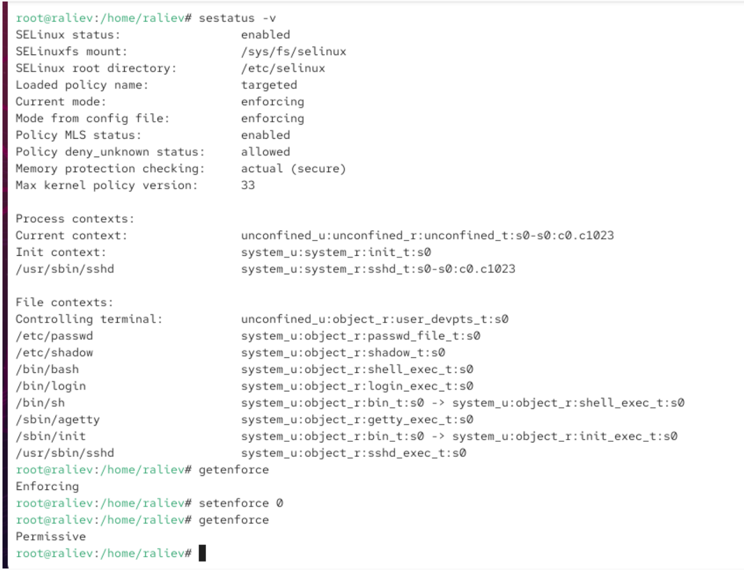
Цель работы

Основная цель

Получить навыки работы с контекстом безопасности и политиками SELinux в Linux.

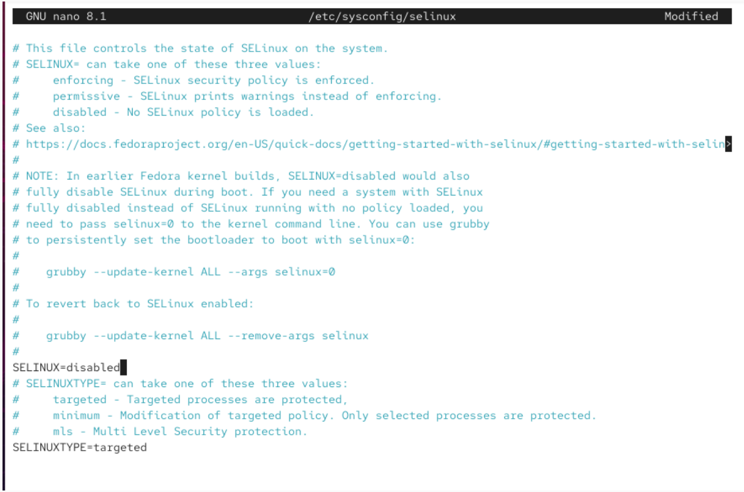
Ход выполнения работы

Проверка состояния SELinux



```
root@raliev:/home/raliev# 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@raliev:/home/raliev# getenforce
Enforcing
root@raliev:/home/raliev# setenforce 0
root@raliev:/home/raliev# getenforce
Permissive
root@raliev:/home/raliev# 
```

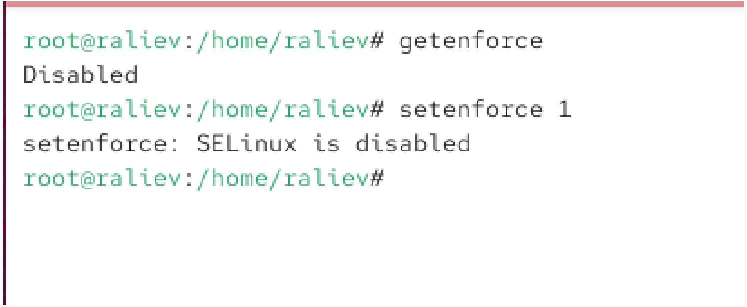
Изменение режима работы SELinux



```
 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-selin>
#
# 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: Изменение режима SELinux на Permissive

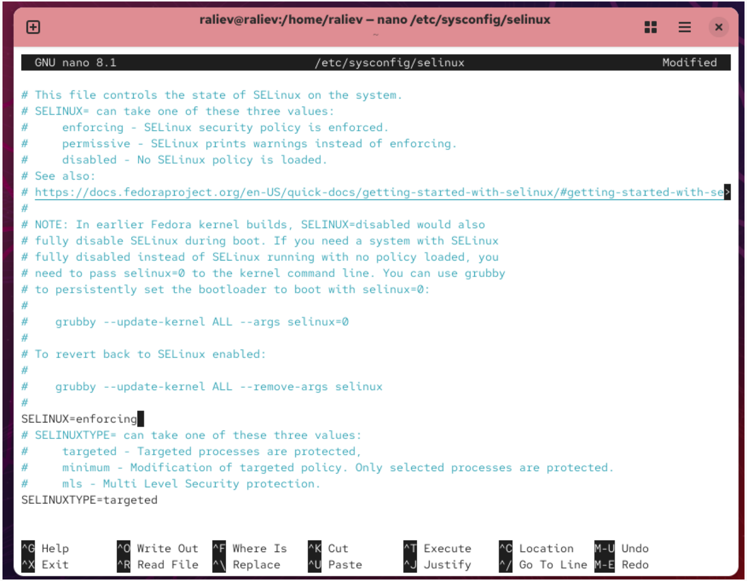
Отключение SELinux



```
root@raliev:/home/raliev# getenforce
Disabled
root@raliev:/home/raliev# setenforce 1
setenforce: SELinux is disabled
root@raliev:/home/raliev#
```

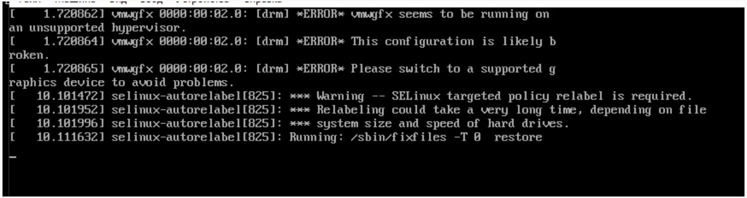
Рис. 3: Отключение SELinux в файле конфигурации

Ошибка при попытке включения после отключения



```
 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-se>
#
# 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    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

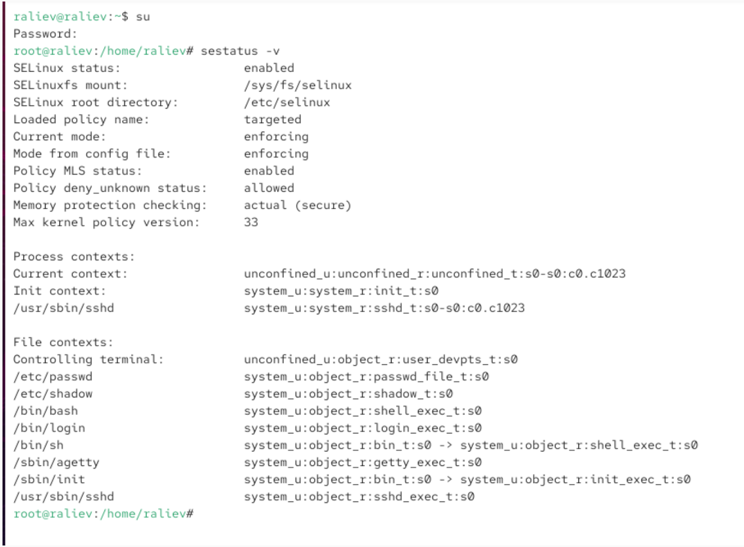
Повторное включение SELinux



```
[    1.720862] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[    1.720864] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[    1.720865] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[   10.101472] selinux-autorelabel[825]: *** Warning -- SELinux targeted policy relabel is required.
[   10.101952] selinux-autorelabel[825]: *** Relabeling could take a very long time, depending on file
[   10.101996] selinux-autorelabel[825]: *** system size and speed of hard drives.
[   10.111632] selinux-autorelabel[825]: Running: /sbin/fixfiles -T 0  restore
_
```

Рис. 5: Включение SELinux в конфигурации

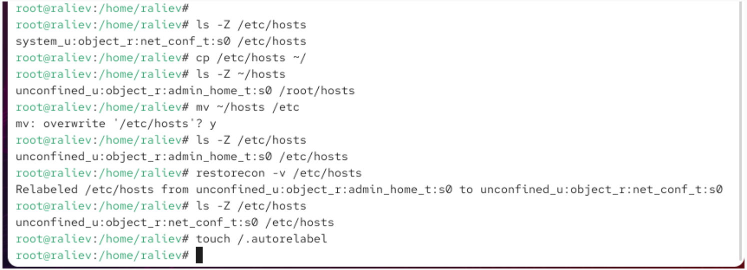
Восстановление меток SELinux



```
raliev@raliev:~$ su
Password:
root@raliev:/home/raliev# 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@raliev:/home/raliev#
```

Рис. 6: Автоматическое восстановление меток SELinux

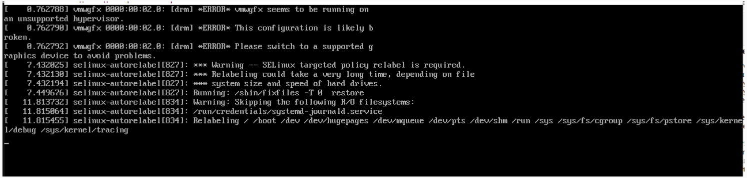
Проверка работы после перезапуска



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

Рис. 7: Проверка состояния SELinux после включения

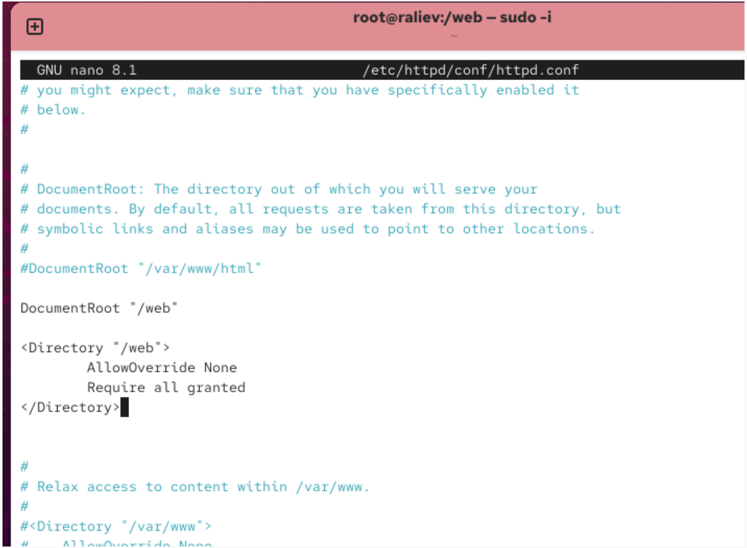
Просмотр и изменение контекста файла



```
[    0.762788] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[    0.762790] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[    0.762792] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[    7.432025] selinux-autorelabel[827]: *** Warning -- SELinux targeted policy relabel is required.
[    7.432130] selinux-autorelabel[827]: *** Relabeling could take a very long time, depending on file
[    7.432194] selinux-autorelabel[827]: *** system size and speed of hard drives.
[    7.449676] selinux-autorelabel[827]: Running: /sbin/fixfiles -T 0  restore
[   11.813732] selinux-autorelabel[834]: Warning: Skipping the following R/O filesystems:
[   11.815064] selinux-autorelabel[834]: /run/credentials/systemd-journald.service
[   11.815455] selinux-autorelabel[834]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kerne
l/debug /sys/kernel/tracing

_
```

Рис. 8: Автоматическое восстановление контекста безопасности при загрузке

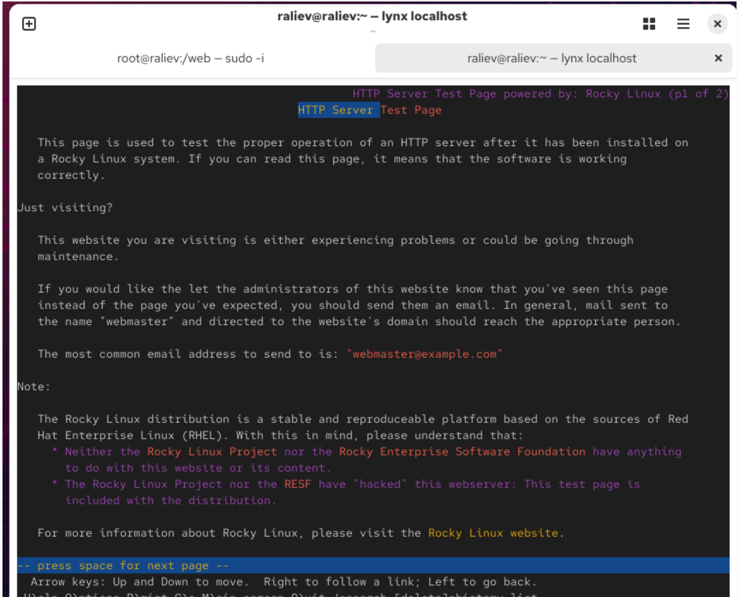
Изменение конфигурации Apache



```
 GNU nano 8.1                               /etc/httpd/conf/httpd.conf
# 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/html"

DocumentRoot "/web"

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


#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#    AllowOverride None
```

Рис. 9: Изменение файла конфигурации Apache

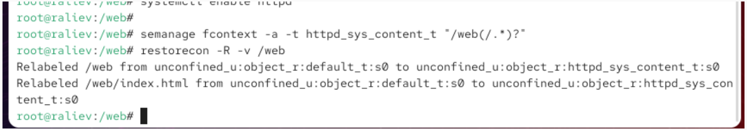
Тестовая страница Apache по умолчанию



raliev@raliev:~ — lynx localhost
root@raliev:/web — sudo -i
raliev@raliev:~ — lynx localhost

```
                                    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
```

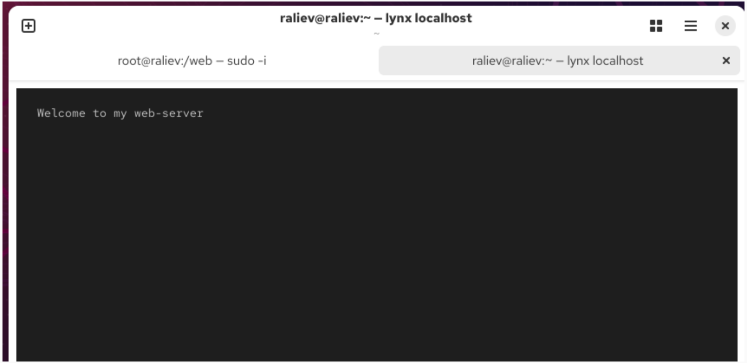
Применение контекста httpd_sys_content_t



```
root@raliev:/web# systemctl enable httpd
root@raliev:/web#
root@raliev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@raliev:/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_con
tent_t:s0
root@raliev:/web#
```

Рис. 11: Применение нового контекста безопасности к каталогу /web

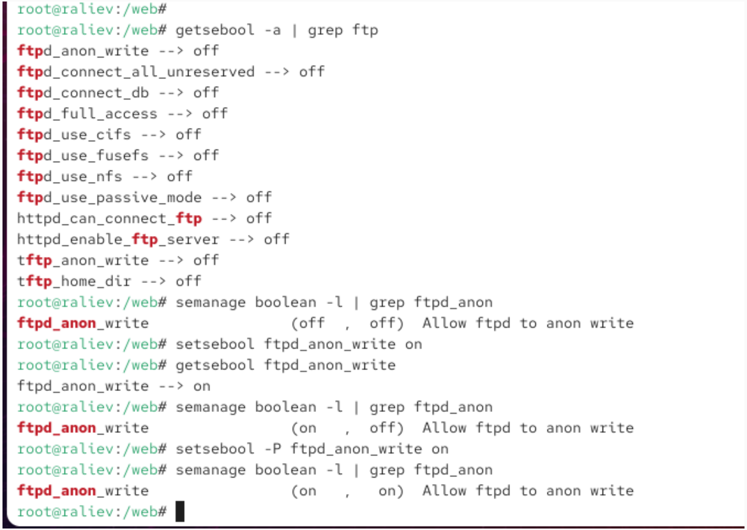
Отображение пользовательской страницы


raliev@raliev:~ – lynx localhost
root@raliev:/web – sudo -i
raliev@raliev:~ – lynx localhost

```
Welcome to my web-server
```

Рис. 12: Отображение пользовательской страницы веб-сервера

Проверка и изменение состояния ftpd_anon_write



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

Рис. 13: Просмотр и изменение переключателя ftpd_anon_write

Итоги работы

Вывод

В ходе лабораторной работы были изучены режимы работы и механизмы SELinux, методы настройки контекстов безопасности, восстановления меток, а также принципы взаимодействия SELinux с веб- и FTP-службами.
Получены практические навыки администрирования системы безопасности SELinux в Linux.