

Лабораторная работа №9

Управление SELinux

Хохлачева Полина Дмитриевна

Российский университет дружбы народов, Москва, Россия

Информация

- Хохлачева Полина Дмитриевна
- Российский университет дружбы народов
- Номер студенческого билета- 1132242473
- [1132242473@pfur.ru]

Вводная часть

Получить навыки работы с контекстом безопасности и политиками SELinux.

Выполнение лабораторной работы

Выполнение лабораторной работы

Получаем полномочия администратора, смотрим текущую информацию о состоянии, изменение режим работы(рис. (fig:001?)).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# 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
```

Выполнение лабораторной работы

Установка с помощью редактора (рис. (fig:002?)).

```
GNU nano 5.6.1 /etc/sysconfig/selinux

# 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://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html
#
# NOTE: Up to RHEL 8 release included, 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 pr
#   mls - Multi Level Security protection.
```

Выполнение лабораторной работы

Получаем полномочия администратора, просматриваем контекст безопасности файла, копируем файл в домашний каталог, переписываем существующий файл, исправляем контекст безопасности, убеждаемся в этом(рис. (fig:003?)).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@khokhlacheva ~]# cp /etc/hosts ~/
[root@khokhlacheva ~]# ls -Z ~/hosts
? /root/hosts
[root@khokhlacheva ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'?
[root@khokhlacheva ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@khokhlacheva ~]# restorecon -v /etc/hosts
[root@khokhlacheva ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@khokhlacheva ~]#
```

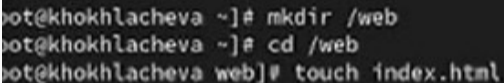
Выполнение лабораторной работы

Устанавливаем необходимое программное обеспечение(рис. (fig:004?)).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               8.8 kB/s | 4.1 kB    00:00
Rocky Linux 9 - BaseOS                               999 kB/s | 2.5 MB    00:02
Rocky Linux 9 - AppStream                             13 kB/s | 4.5 kB    00:00
Rocky Linux 9 - AppStream                             2.2 MB/s | 9.5 MB    00:04
Rocky Linux 9 - Extras                               8.7 kB/s | 2.9 kB    00:00
Пакет httpd-2.4.62-4.el9_6.4.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@khokhlacheva ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:17 назад, Пт 31 окт
2025 23:29:33.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий  Размер
=====
Установка:
lynx      x86_64      2.8.9-20.el9  appstream    1.5 M
=====
Результат транзакции
=====
Установка  1 Пакет

Объем загрузки: 1.5 M
Объем изменений: 6.1 M
Загрузка пакетов:
lynx-2.8.9-20.el9.x86_64.rpm                2.0 MB/s | 1.5 MB    00:00
-----
Общий размер                                1.3 MB/s | 1.5 MB    00:01
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
```

Создаём новое хранилище, создаём файл в каталоге с контентом веб-сервера(рис. (fig:005?)).



```
oot@khokhlacheva ~]# mkdir /web  
oot@khokhlacheva ~]# cd /web  
oot@khokhlacheva web]# touch index.html
```

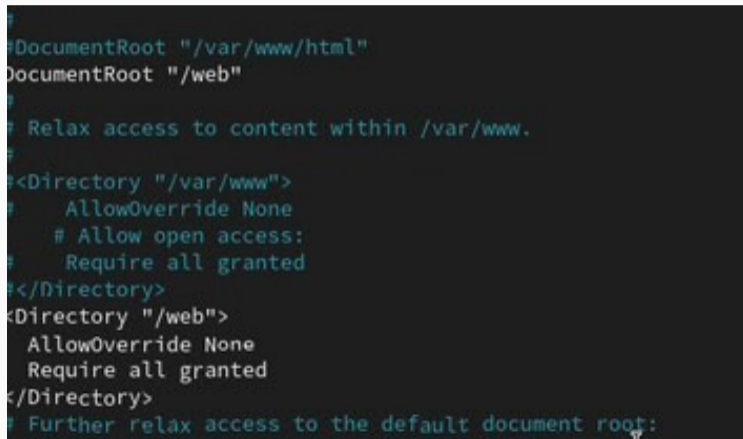
Рис. 5: Создаём

Помещаем следующий текст(рис. (fig:006?)).

```
oot@khokhlacheva web]# systemctl start httpd
oot@khokhlacheva web]# systemctl enable httpd
oot@khokhlacheva web]# su khokhlacheva
hokhlacheva@khokhlacheva web]$ lynx http://localhost
```

Рис. 6: Помещаем

Запускаем веб-сервер(рис. (fig:007?)).



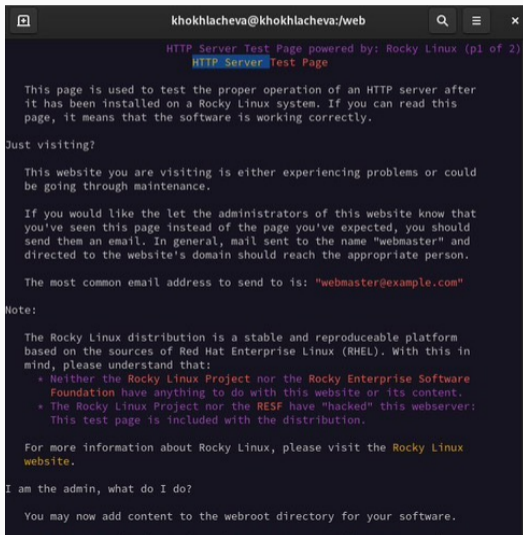
```
#DocumentRoot "/var/www/html"
DocumentRoot "/web"

#
# 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 root:
```

Рис. 7: Запускаем

Выполнение лабораторной работы

Комментируем строки и добавляем следующие отделы(рис. (fig:008?)).



```
khokhlacheva@khokhlacheva:/web
HTTP Server Test Page powered by: Rocky Linux (pl 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.

I am the admin, what do I do?

You may now add content to the webroot directory for your software.
```

Снова обращаемся к веб-серверу(рис. (fig:009?)).

```
[khokhlacheva@khokhlacheva ~]$ su -  
Пароль:  
[root@khokhlacheva ~]# getsebool -a | grep ftp  
getsebool: SELinux is disabled  
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write  
[root@khokhlacheva ~]# setsebool ftpd_anon_write on  
Could not change active booleans: Invalid boolean  
[root@khokhlacheva ~]# getsebool ftpd_anon_write  
getsebool: SELinux is disabled  
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write  
[root@khokhlacheva ~]# setsebool -P ftpd_anon_write on  
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write  
[root@khokhlacheva ~]#
```

Рис. 9: Обращаемся

Выполнение лабораторной работы

Получаем полномочия администратора, смотрим список переключателей, изменяем текущее значение переключателя для службы, повторно смотрим список, изменяем постоянное значение и снова смотрим список(рис. (fig:010?)).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# getsebool -a | grep ftp
getsebool: SELinux is disabled
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@khokhlacheva ~]# setsebool ftpd_anon_write on
Could not change active booleans: Invalid boolean
[root@khokhlacheva ~]# getsebool ftpd_anon_write
getsebool: SELinux is disabled
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@khokhlacheva ~]# setsebool -P ftpd_anon_write on
[root@khokhlacheva ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@khokhlacheva ~]#
```

Рис. 10: Смотрим, изменяем

Выводы

Мы получили навыки работы с контекстом безопасности и политиками SELinux.