

# **Отчёт по лабораторной работе №6**

**Основы информационной безопасности**

Надежда Александровна Рогожина

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теоретическое введение</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>4</b>	<b>Выводы</b>	<b>22</b>
	<b>Список литературы</b>	<b>23</b>

## Список иллюстраций

3.1	Статус SELinux . . . . .	8
3.2	service httpd status . . . . .	9
3.3	обе команды . . . . .	9
3.4	Состояние переключателей SELinux . . . . .	10
3.5	Статистика по политике . . . . .	11
3.6	Тип файлов и поддиректорий . . . . .	11
3.7	Поддиректории . . . . .	12
3.8	Создание файла . . . . .	12
3.9	test.ru . . . . .	13
3.10	изменение контекста . . . . .	14
3.11	попытка №1 . . . . .	14
3.12	выполнение команды . . . . .	14
3.13	Системный лог-файл . . . . .	15
3.14	audit.log . . . . .	15
3.15	Listen 80 -> Listen 81 . . . . .	16
3.16	restart . . . . .	16
3.17	Попытка №2 . . . . .	17
3.18	tail -nl /var/log/messages . . . . .	17
3.19	/var/log/http/error_log . . . . .	18
3.20	/var/log/http/access_log . . . . .	18
3.21	var/log/audit/audit.log . . . . .	18
3.22	semanage . . . . .	19
3.23	semanage grep . . . . .	19
3.24	Попытка №3 . . . . .	19
3.25	test.ru . . . . .	20
3.26	change back . . . . .	20
3.27	rm test.html . . . . .	21

# Список таблиц

2.1	Описание основных терминов SELinux . . . . .	7
-----	--	---

# 1 Цель работы

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.
- Проверить работу SELinx на практике совместно с веб-сервером Apache.

## 2 Теоретическое введение

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена.

Для того, чтобы понять, в чем состоит практическая ценность SELinux, рассмотрим несколько примеров, когда стандартная система контроля доступа недостаточна. Если SELinux отключен, то вам доступна только классическая дискреционная система контроля доступа, которая включает в себя DAC (избирательное управление доступом) или ACL(списки контроля доступа). То есть речь идет о манипулировании правами на запись, чтение и исполнение на уровне пользователей и групп пользователей, чего в некоторых случаях может быть совершенно недостаточно. Например:

- Администратор не может в полной мере контролировать действия пользователя. Например, пользователь вполне способен дать всем остальным пользователям права на чтение собственных конфиденциальных файлов, таких как ключи SSH.
- Процессы могут изменять настройки безопасности. Например, файлы, содержащие в себе почту пользователя должны быть доступны для чтения только одному конкретному пользователю, но почтовый клиент вполне мо-

жет изменить права доступа так, что эти файлы будут доступны для чтения всем.

- Процессы наследуют права пользователя, который их запустил. Например, зараженная трояном версия браузера Firefox в состоянии читать SSH-ключи пользователя, хотя не имеет для того никаких оснований.

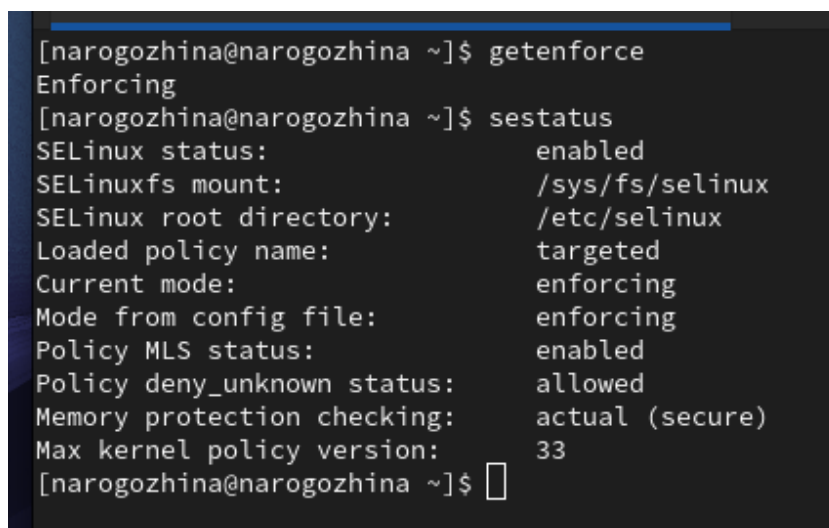
По сути, в традиционной модели избирательного управления доступом (DAC), хорошо реализованы только два уровня доступа — пользователь и суперпользователь. Нет простого метода, который позволил бы устанавливать для каждого пользователя необходимый минимум привилегий. В табл. [2.1] приведено краткое описание основных терминов SELinux.

Таблица 2.1: Описание основных терминов SELinux

Термин	Описание
Домен	Список действий, которые может выполнять процесс. Обычно в качестве домена определяется минимально-возможный набор действий, при помощи которых процесс способен функционировать. Таким образом, если процесс дискредитирован, злоумышленнику не удастся нанести большого вреда.
Роль	Список доменов, которые могут быть применены. Если какого-то домена нет в списке доменов какой-то роли, то действия из этого домена не могут быть применены.
Тип	Набор действий, которые допустимы по отношению к объекту. Тип отличается от домена тем, что он может применяться к пайпам, каталогам и файлам, в то время как домен применяется к процессам.
Контекст безопасности	Все атрибуты SELinux — роли, типы и домены.

### 3 Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис. [3.1]).

A screenshot of a terminal window with a dark background and light-colored text. The prompt is [narogozhina@narogozhina ~]\$. The first command entered is getenforce, which returns Enforcing. The second command is sestatus, which returns a detailed status report for SELinux. The report shows that SELinux is enabled, the mount point is /sys/fs/selinux, the root directory is /etc/selinux, the loaded policy is targeted, and the current mode is enforcing. Other details include the mode from the config file (enforcing), MLS status (enabled), deny\_unknown status (allowed), memory protection checking (actual (secure)), and the max kernel policy version (33).

```
[narogozhina@narogozhina ~]$ getenforce
Enforcing
[narogozhina@narogozhina ~]$ sestatus
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
[narogozhina@narogozhina ~]$
```

Рис. 3.1: Статус SELinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает `service httpd status` (рис. [3.2]).



```
se[narogozhina@narogozhina ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sun 2024-04-21 10:36:09 MSK; 1h 19min ago
     Docs: man:httpd.service(8)
   Main PID: 1266 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
   Tasks: 213 (limit: 10978)
  Memory: 17.0M
    CPU: 1.982s
   CGroup: /system.slice/httpd.service
           └─1266 /usr/sbin/httpd -DFOREGROUND
             └─1356 /usr/sbin/httpd -DFOREGROUND
               └─1361 /usr/sbin/httpd -DFOREGROUND
                 └─1366 /usr/sbin/httpd -DFOREGROUND
                   └─1367 /usr/sbin/httpd -DFOREGROUND

Apr 21 10:36:08 narogozhina.localdomain systemd[1]: Starting The Apache HTTP Server...
Apr 21 10:36:09 narogozhina.localdomain systemd[1]: Started The Apache HTTP Server.
Apr 21 10:36:09 narogozhina.localdomain httpd[1266]: Server configured, listening on: port 80
lines 1-19/19 (END)
```

Рис. 3.2: service httpd status

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd` (рис. [3.3]).

```
[narogozhina@narogozhina ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 1266 0.0 0.2 20340 5328 ? Ss 10:36 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1266 0.0 0.1 21676 3560 ? S 10:36 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1361 0.0 0.2 1079488 4068 ? Sl 10:36 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1366 0.0 0.3 1079488 6180 ? Sl 10:36 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1367 0.0 0.1 1210624 3628 ? Sl 10:36 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 narogozh 4839 0.0 0.4 236232 8928 pts/0 S+ 11:55 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 narogozh 4075 0.0 0.1 221796 2212 pts/2 S+ 11:56 0:00 grep --color=auto httpd

[narogozhina@narogozhina ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 1266 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 1356 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 1361 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 1366 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 1367 ? 00:00:00 httpd
[narogozhina@narogozhina ~]$
```

Рис. 3.3: обе команды

4. Посмотрите текущее состояние переключателей SELinux для Apache (рис. [3.4]).

```

[narogozhina@narogozhina ~]$ getsebool -a | grep httpd
httpd_anon_write --> off
httpd_builtinscripting --> on
httpd_can_check_spam --> off
httpd_can_connect_ftp --> off
httpd_can_connect_ldap --> off
httpd_can_connect_mythtv --> off
httpd_can_connect_zabbix --> off
httpd_can_manage_courier_spool --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_memcache --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> off
httpd_dbus_sssd --> off
httpd_dontaudit_search_dirs --> off
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> off
httpd_execmem --> off
httpd_graceful_shutdown --> off
httpd_manage_ipa --> off
httpd_mod_auth_ntlm_winbind --> off
httpd_mod_auth_pam --> off
httpd_read_user_content --> off
httpd_run_ipa --> off
httpd_run_preupgrade --> off
httpd_run_stickshift --> off
httpd_serve_cobbler_files --> off
httpd_setrlimit --> off
httpd_ssi_exec --> off
httpd_sys_script_anon_write --> off
httpd_tmp_exec --> off
httpd_tty_comm --> off
httpd_unified --> off
httpd_use_cifs --> off
httpd_use_fusefs --> off
httpd_use_gpg --> off
httpd_use_nfs --> off
httpd_use_opencryptoki --> off
httpd_use_openstack --> off
httpd_use_sasl --> off
httpd_verify_dns --> off
[narogozhina@narogozhina ~]$ █

```

Рис. 3.4: Состояние переключателей SELinux

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (рис. [3.5]).

```

[narogozhina@narogozhina ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135
Sensitivities:           1
Types:                   5135
Users:                   8
Booleans:                357
Allow:                   65409
Auditallow:              172
Type_trans:              267813
Type_member:             37
Role allow:              39
Constraints:             70
MLS Constrain:           72
Permissives:             2
Defaults:                7
Allowxperm:              0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:            27
Genfscon:                109
Netifcon:                0
Permissions:             457
Categories:              1024
Attributes:              259
Roles:                   15
Cond. Expr.:             390
Neverallow:              0
Dontaudit:               8647
Type_change:             94
Range_trans:             6164
Role_trans:              419
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  6
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  35
Portcon:                 665
Nodecon:                 0
[narogozhina@narogozhina ~]$

```

Рис. 3.5: Статистика по политике

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. [3.6]).

```

[narogozhina@narogozhina ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Oct 28 12:35 html
[narogozhina@narogozhina ~]$

```

Рис. 3.6: Тип файлов и поддиректорий

7. Определите тип файлов, находящихся в директории /var/www/html `ls -lZ /var/www/html` (рис. [3.7]).

```
[narogozhina@narogozhina ~]$ ls -lZ /var/www/html
total 0
[narogozhina@narogozhina ~]$
```

Рис. 3.7: Поддиректории

8. Создание файлов в директории `/var/www/html` разрешено только владельцу данной директории.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) `html`-файл `/var/www/html/test.html` следующего содержания:

```
<html>
<body>test</body>
</html>
```

(рис. [3.8]).

```
[root@narogozhina conf]# touch /var/www/html/test.html
[root@narogozhina conf]# gedit /var/www/html/test.html

(gedit:4631): dconf-WARNING **: 12:02:13.508: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:4631): dconf-WARNING **: 12:02:13.518: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:4631): dconf-WARNING **: 12:02:13.628: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:4631): dconf-WARNING **: 12:02:13.627: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:4631): dconf-WARNING **: 12:02:13.627: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:4631): WARNING **: 12:02:21.480: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:4631): WARNING **: 12:02:21.480: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:4631): WARNING **: 12:02:24.722: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:4631): dconf-WARNING **: 12:02:24.740: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
[root@narogozhina conf]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@narogozhina conf]#
```

Рис. 3.8: Создание файла

10. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён (рис. [3.9]).

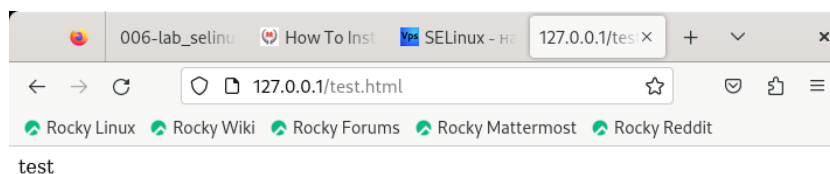


Рис. 3.9: test.ru

11. Тип файла `test.html`: `unconfined_u:object_r:httpd_sys_content_t:s0`

12. Измените контекст файла `/var/www/html/test.html` `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`:

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```

(рис. [3.10]).

```
[root@narogozhina conf]# chcon -t samba_share_t /var/www/html/test.html
[root@narogozhina conf]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@narogozhina conf]#
```

Рис. 3.10: изменение контекста

13. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке:

Forbidden

You don't have permission to access /test.html on this server.

(рис. [3.11]).

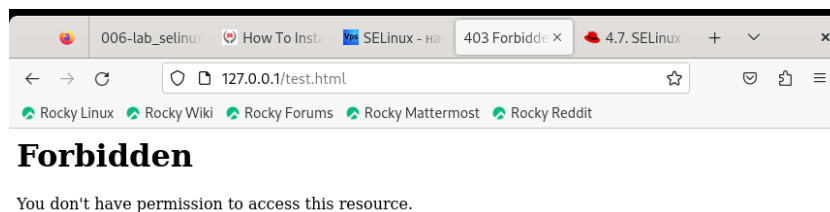


Рис. 3.11: попытка №1

15. `ls -l /var/www/html/test.html` (рис. [3.12]).

```
[root@narogozhina conf]# ls -l /vat/www/html/test.html
ls: cannot access '/vat/www/html/test.html': No such file or directory
[root@narogozhina conf]#
```

Рис. 3.12: выполнение команды

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл (рис. [3.13]).

```
[root@narogozhina conf]# tail -n 10 /var/log/messages
Apr 21 12:09:45 narogozhina systemd[1]: Started SEtroubleshoot daemon for processing new SELinux denial logs.
Apr 21 12:09:45 narogozhina setroubleshoot[5021]: failed to retrieve rpm info for path '/var/www/html/test.html':
Apr 21 12:09:46 narogozhina systemd[1]: Created slice Slice /system/dbus-1.1-org.fedoraproject.SetroubleshootPrivileged.
Apr 21 12:09:46 narogozhina systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Apr 21 12:09:47 narogozhina setroubleshoot[5021]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/h
tml/test.html. For complete SELinux messages run: sealert -l cdb20800e-bdf1-450f-af0b-ee5d71986043
Apr 21 12:09:47 narogozhina setroubleshoot[5021]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/h
tml/test.html.#012#012**** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the
label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attemp
t may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following com
mand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Plugin public_content (7.83 confidence) sug
gests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.
html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012
# restorecon -v '/var/www/html/test.html'#012#012**** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this a
s a bug.#012You can generate a local policy module to allow this access.#012Do#012# allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr 21 12:09:47 narogozhina setroubleshoot[5021]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/h
tml/test.html. For complete SELinux messages run: sealert -l cdb20800e-bdf1-450f-af0b-ee5d71986043
Apr 21 12:09:47 narogozhina setroubleshoot[5021]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/h
tml/test.html.#012#012**** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the
label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attemp
t may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following com
mand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Plugin public_content (7.83 confidence) sug
gests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.
html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012
# restorecon -v '/var/www/html/test.html'#012#012**** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this a
s a bug.#012You can generate a local policy module to allow this access.#012Do#012# allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr 21 12:09:57 narogozhina systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Apr 21 12:09:57 narogozhina systemd[1]: setroubleshootd.service: Deactivated successfully.
[root@narogozhina conf]#
```

Рис. 3.13: Системный лог-файл

Если в системе окажутся запущенными процессы setroubleshootd и auditd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно (рис. [3.14]).

```
[root@narogozhina conf]# tail -n 10 /var/log/audit/audit.log
type=AVC msg=audit(1713690584.916:178): avc: denied { getattr } for pid=1366 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=
68529495 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1713690584.916:178): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c al=7f551400038 a2=7f55247f7b0 a3=0
items=0 ppid=1266 pid=1366 uid=0 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 com=
"httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUDID="unset" UID="apache" GID="apac
he" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1713690584.916:178): proctitle=2F7573722F73626962F6874747064802D44464F524547524F554E44
type=AVC msg=audit(1713690584.916:179): avc: denied { getattr } for pid=1366 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=
68529495 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1713690584.916:179): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c al=7f5514007140 a2=7f55247f7b0 a3=10
0 items=0 ppid=1266 pid=1366 uid=0 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 com
="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUDID="unset" UID="apache" GID="ap
ache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1713690584.916:179): proctitle=2F7573722F73626962F6874747064802D44464F524547524F554E44
type=SERVICE_START msg=audit(1713690585.678:180): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=se
troubleshootd comm='systemd' exe='/usr/lib/systemd/systemd' hostname=? addr=? terminal=? res=success'UID='root' AUDID='unset'
type=SERVICE_START msg=audit(1713690586.029:181): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=dbu
s-1.1-org.fedoraproject.SetroubleshootPrivileged@0 comm='systemd' exe='/usr/lib/systemd/systemd' hostname=? addr=? terminal=? res=success'
UID='root' AUDID='unset'
type=SERVICE_STOP msg=audit(1713690597.497:182): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=dbus
-1.1-org.fedoraproject.SetroubleshootPrivileged@0 comm='systemd' exe='/usr/lib/systemd/systemd' hostname=? addr=? terminal=? res=success'U
ID='root' AUDID='unset'
type=SERVICE_STOP msg=audit(1713690597.578:183): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg="unit=setr
oubleshootd comm='systemd' exe='/usr/lib/systemd/systemd' hostname=? addr=? terminal=? res=success'UID='root' AUDID='unset'
[root@narogozhina conf]#
```

Рис. 3.14: audit.log

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81 (рис. [3.15]).

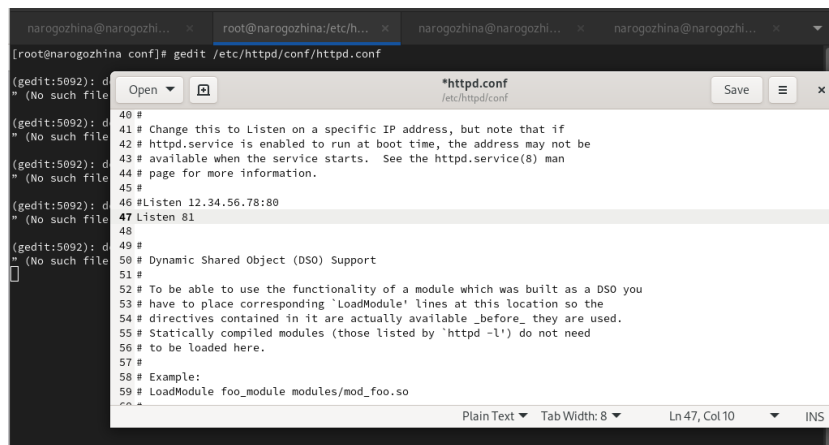


Рис. 3.15: Listen 80 -> Listen 81

17. Выполните перезапуск веб-сервера Apache (рис. [3.16]).

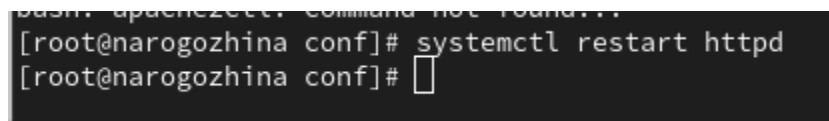
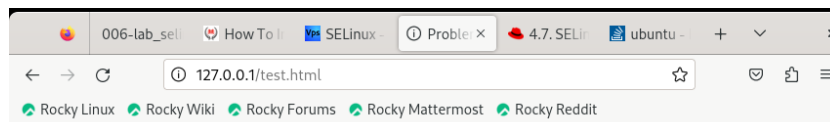


Рис. 3.16: restart

При попытке переподключиться - произошел сбой, т.к. мы подключаемся по другому tcp серверу (рис. [3.17]).





## Unable to connect

Firefox can't establish a connection to the server at 127.0.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

Рис. 3.17: Попытка №2

18. Проанализируйте лог-файлы: `tail -nl /var/log/messages`(рис. [3.18]).

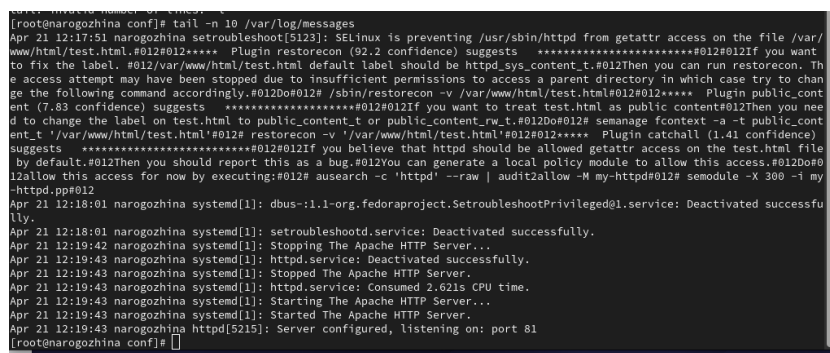


Рис. 3.18: `tail -nl /var/log/messages`

Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи (рис. [3.19], рис. [3.20], рис. [3.21]).

```
[root@narogzhina conf]# tail -n 10 /var/log/http/error_log
[Sun Apr 21 10:36:09.081700 2024] [mpm_event:notice] [pid 1266:tid 1266] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sun Apr 21 10:36:09.081729 2024] [core:notice] [pid 1266:tid 1266] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sun Apr 21 12:09:44.918477 2024] [core:error] [pid 1366:tid 1571] (13)Permission denied: [client 127.0.0.1:59596] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Sun Apr 21 12:17:49.022919 2024] [core:error] [pid 1366:tid 1568] (13)Permission denied: [client 127.0.0.1:57538] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Sun Apr 21 12:19:42.353556 2024] [mpm_event:notice] [pid 1266:tid 1266] AH00492: caught SIGWINCH, shutting down gracefully
[Sun Apr 21 12:19:43.582202 2024] [core:notice] [pid 5215:tid 5215] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sun Apr 21 12:19:43.584699 2024] [suexec:notice] [pid 5215:tid 5215] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sun Apr 21 12:19:43.603671 2024] [lbmethod_heartbeat:notice] [pid 5215:tid 5215] AH02282: No slotmem from mod_heartbeat
[Sun Apr 21 12:19:43.613173 2024] [mpm_event:notice] [pid 5215:tid 5215] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sun Apr 21 12:19:43.613203 2024] [core:notice] [pid 5215:tid 5215] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@narogzhina conf]#
```

Рис. 3.19: /var/log/http/error\_log

```
[root@narogzhina conf]# tail -n 10 /var/log/http/access_log
127.0.0.1 - - [21/Apr/2024:10:34:50 +0300] "GET / HTTP/1.1" 403 7620 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:10:34:50 +0300] "GET /icons/poweredby.png HTTP/1.1" 200 15443 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:10:34:50 +0300] "GET /poweredby.png HTTP/1.1" 200 5714 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:10:34:50 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:12:02:54 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:12:03:59 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:12:09:44 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [21/Apr/2024:12:17:49 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@narogzhina conf]#
```

Рис. 3.20: /var/log/http/access\_log

```
[root@narogzhina conf]# tail -n 10 /var/log/audit/audit.log
type=PROCTITLE msg=audit(1713691069.621:184): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=AVC msg=audit(1713691069.621:185): avc: denied { getattr } for pid=1366 comm="httpd" path="/var/www/html/test.html" dev="dm-0" tno=68529495 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permission=0
type=SYSCALL msg=audit(1713691069.621:185): arch=C000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f5510005128 a2=7f5525fa8b0 a3=100 items=0 ppid=1266 pid=1366 uid=0 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUDID="unset" UID="apache"
type=PROCTITLE msg=audit(1713691069.621:185): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1713691070.084:186): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_START msg=audit(1713691070.366:187): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-1.12-0.fedoraproject.SetroubleshootPrivileged1 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1713691081.765:188): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-1.12-0.fedoraproject.SetroubleshootPrivileged1 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1713691081.833:189): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1713691183.453:190): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_START msg=audit(1713691183.605:191): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
[root@narogzhina conf]#
```

Рис. 3.21: var/log/audit/audit.log

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` (рис. [3.22]).

```
[narogozhina@narogozhina ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[narogozhina@narogozhina ~]$
```

Рис. 3.22: semanage

После этого проверьте список портов командой `semanage port -l | grep http_port_t` (рис. [3.23]).

```
[narogozhina@narogozhina ~]$ sudo semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
[narogozhina@narogozhina ~]$
```

Рис. 3.23: semanage grep

Порт 81 появился в списке.

20. Попробуйте запустить веб-сервер Apache ещё раз (рис. [3.24]).

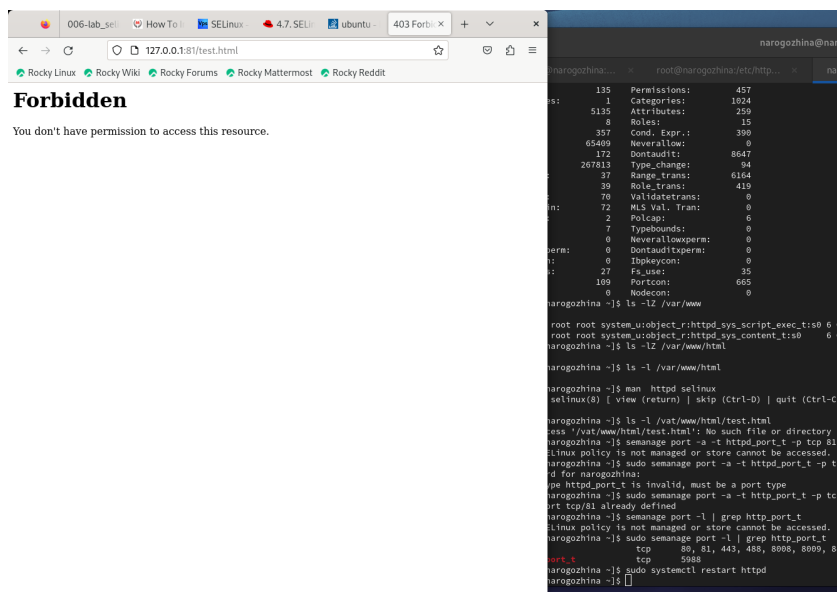


Рис. 3.24: Попытка №3

Сейчас мы подключаемся к серверу, который знаком нашей программе, и поэтому подключение у нас прошло. Да, доступа у нас нет, но тем не менее, сервер запустился, а не выдал ошибку.

21. Верните контекст `httpd_sys_content__t` к файлу `/var/www/html/test.html`:

```
chcon -t httpd_sys_content_t /var/www/html/test.html
```

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test». (рис. [3.25]).

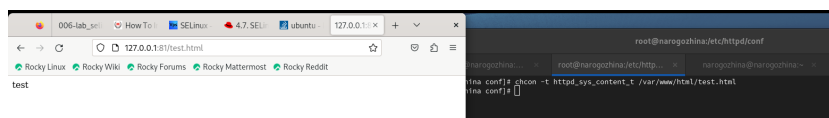


Рис. 3.25: test.ru

22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80` (рис. [3.26]).

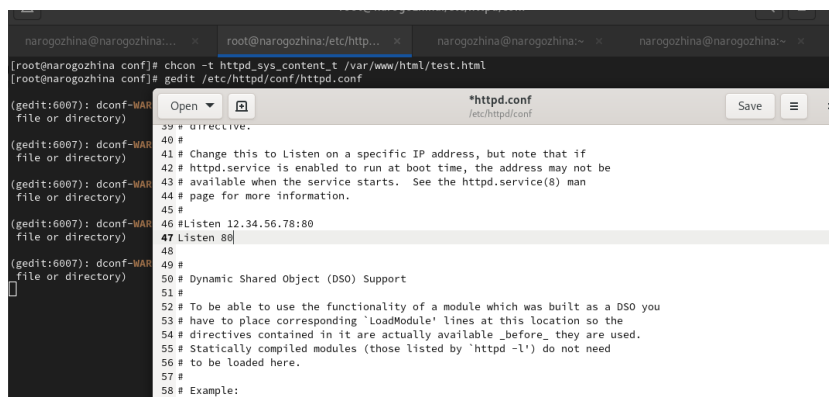


Рис. 3.26: change back

23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.

24. Удалите файл `/var/www/html/test.html`:

```
rm /var/www/html/test.html
```

(рис. [3.27]).

```
[root@narogozhina conf]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
[root@narogozhina conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@narogozhina conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@narogozhina conf]# semanage port -m -t http_port_t -p tcp 81
[root@narogozhina conf]# semanage port -l | grep http_port_t
http_port_t      tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
[root@narogozhina conf]# semanage port -d -t http_port_t -p tcp 81
[root@narogozhina conf]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
[root@narogozhina conf]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@narogozhina conf]# ls -l /var/www/html
total 0
[root@narogozhina conf]#
```

Рис. 3.27: rm test.html

## 4 Выводы

В ходе лабораторной работы мы развили навыки администрирования ОС Linux, получить первое практическое знакомство с технологией SELinux<sup>1</sup>, а также проверили работу SELinx на практике совместно с веб-сервером Apache.

## **Список литературы**