

# **Отчёт по лабораторной работе №6**

Серегин Денис Алексеевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>14</b>

## Список иллюстраций

2.1	Режим и политика SELinux . . . . .	6
2.2	Стандартная страница Apache . . . . .	7
2.3	Процесс веб-сервера Apache . . . . .	7
2.4	Состояния переключателей Apache . . . . .	8
2.5	Статистика по политике безопасности Apache . . . . .	9
2.6	Типы файлов . . . . .	9
2.7	Типы файлов . . . . .	10
2.8	Стандартная страница Apache . . . . .	10
2.9	Файл test.html . . . . .	10
2.10	Контекст файла . . . . .	10
2.11	Отображение файла . . . . .	11
2.12	Контекст файла . . . . .	11
2.13	Ошибка доступа . . . . .	11
2.14	Логи веб-сервера . . . . .	12
2.15	Ошибка соединения с сервером . . . . .	12
2.16	Логи Apache . . . . .	12
2.17	Добавления порта 81 в разрешенные . . . . .	13

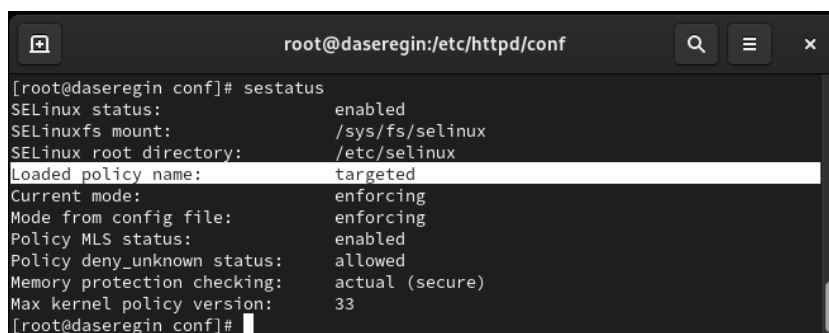
## **Список таблиц**

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

0. Перед выполнением лабораторной работы я подготовил виртуальную машину в соответствии с указаниями к лабораторной работе
1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. (рис. 2.1)

A screenshot of a terminal window with a dark background. The title bar shows 'root@daseregin:/etc/httpd/conf'. The terminal content shows the command 'sestatus' and its output. The output indicates that SELinux is enabled, the loaded policy is 'targeted', and the current mode is 'enforcing'.

```
root@daseregin:/etc/httpd/conf
[root@daseregin conf]# 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
[root@daseregin conf]#
```

Рис. 2.1: Режим и политика SELinux

2. Проверил работу веб-сервера с помощью браузера, убедившись, что он успешно работает. (рис. 2.2)

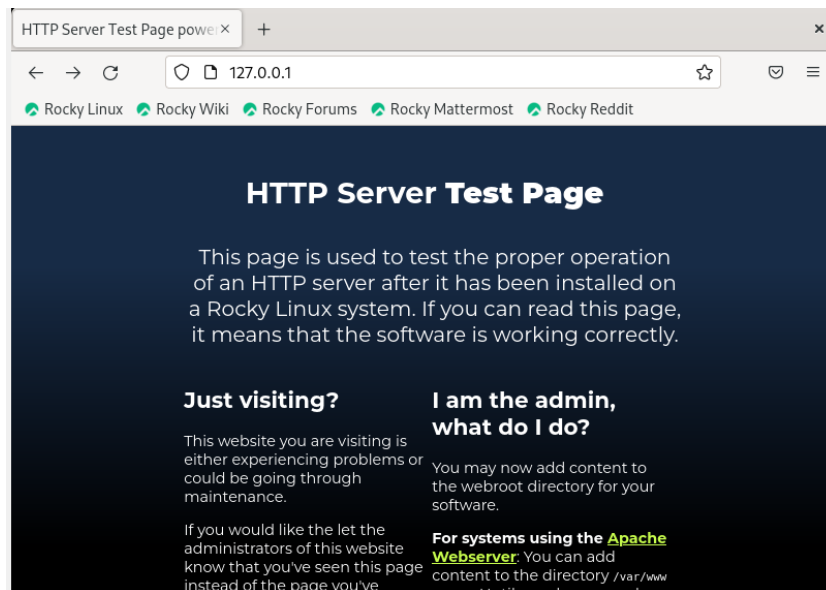


Рис. 2.2: Стандартная страница Apache

### 3. Нашел процесс веб-сервера Apache в списке процессов. (рис. 2.3)

```
[root@daseregin init.d]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 40639 0.0 0.5 20116 11360 ?
Ss 21:20 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40640 0.0 0.3 21600 7380 ?
S 21:20 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40641 0.0 0.6 1210508 13008 ?
Sl 21:20 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40642 0.0 0.5 1079372 10960 ?
Sl 21:20 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40643 0.0 0.5 1079372 10960 ?
Sl 21:20 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 41120 0.0 0.1 221796
2296 pts/0 S+ 21:25 0:00 grep --color=auto httpd
[root@daseregin init.d]#
```

Рис. 2.3: Процесс веб-сервера Apache

### 4. Проверил текущее состояние переключателей SELinux для Apache с использованием команды `sestatus -bigrep httpd`. (рис. 2.4)

```
[root@daseregin init.d]# sestatus -b | grep http
httpd_anon_write off
httpd_builtin_scripting 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
```

Рис. 2.4: Состояния переключателей Apache

5. Получил статистику по политике с помощью команды `seinfo` и определил множество пользователей, ролей и типов. (рис. 2.5)



```
[root@daseregin init.d]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          135      Permissions:        457
Sensitivities:    1        Categories:         1024
Types:            5100     Attributes:         258
Users:            8        Roles:              14
Booleans:         353     Cond. Expr.:       384
Allow:            65000    Neverallow:         0
Auditallow:       170     Dontaudit:          8572
Type_trans:       265341  Type_change:        87
Type_member:      35      Range_trans:        6164
Role allow:       38      Role_trans:         420
Constraints:      70     Validatetrans:      0
MLS Constrain:    72     MLS Val. Tran:      0
Permissives:      2      Polcap:             6
Defaults:         7      Typebounds:         0
Allowxperm:       0      Neverallowxperm:    0
Auditallowxperm:  0      Dontauditxperm:     0
Ibendportcon:     0      Ibpkeycon:          0
Initial SIDs:     27     Fs_use:             35
Genfscon:         109    Portcon:            660
Netifcon:         0      Nodecon:            0
```

Рис. 2.5: Статистика по политику безопасности Apache

6. Определил тип файлов и поддиректорий в директории /var/www с помощью команды `ls -lZ /var/www`. (рис. 2.6)

```
[root@daseregin init.d]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:
21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 23:
21 html
```

Рис. 2.6: Типы файлов

7. Определил тип файлов в директории /var/www/html с помощью команды `ls -lZ /var/www/html`. Как видим папка пуста. (рис. 2.7)

```
[root@daseregin init.d]# ls -lZ /var/www/html
total 0
```

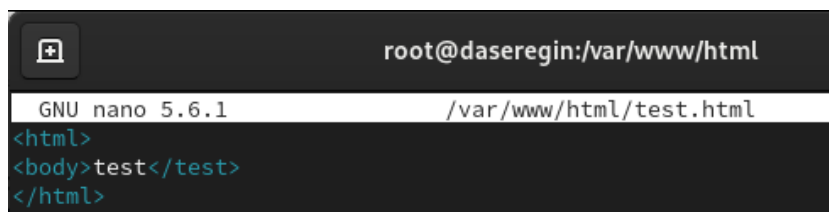
Рис. 2.7: Типы файлов

8. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 2.8)

```
[root@daseregin html]# ls -ld /var/www/html
drwxr-xr-x. 2 root root 6 May 16 23:21 /var/www/html
```

Рис. 2.8: Стандартная страница Apache

9. Создал от имени суперпользователя файл /var/www/html/test.html с указанным содержанием. (рис. 2.9)



```
root@daseregin:/var/www/html
GNU nano 5.6.1 /var/www/html/test.html
<html>
<body>test</test>
</html>
```

Рис. 2.9: Файл test.html

10. Проверил контекст созданного файла, внес контекст, присваиваемый по умолчанию новым файлам в директории /var/www/html (рис. 2.10)

```
[root@daseregin html]# ls -ld /var/www/html
drwxr-xr-x. 2 root root 6 May 16 23:21 /var/www/html
[root@daseregin html]# nano /var/www/html/test.html
[root@daseregin html]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 14 21
:36 /var/www/html/test.html
[root@daseregin html]#
```

Рис. 2.10: Контекст файла

11. Обратился к файлу через веб-сервер, введя в браузере соответствующий адрес, и убедился, что файл был успешно отображён. (рис. 2.11)

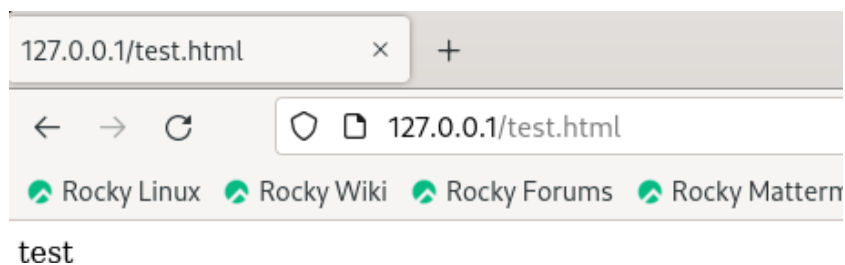


Рис. 2.11: Отображение файла

12. Изучил справку `man httpd_selinux` и сопоставил контексты файлов для `httpd`. Проверил контекст файла с помощью команды `ls -Z /var/www/html/test.html`. (рис. 2.12)

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

Рис. 2.12: Контекст файла

13. Изменил контекст файла `/var/www/html/test.html` на другой, к которому процессу `httpd` не должен иметь доступа, и проверил изменение контекста.
14. Попытался снова получить доступ к файлу через веб-сервер и убедился, что была выдана ошибка “Forbidden”. (рис. 2.13)

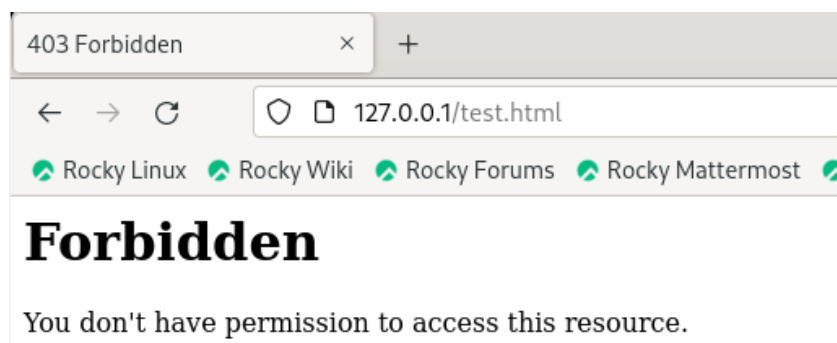


Рис. 2.13: Ошибка доступа

15. Проанализировал ситуацию и выяснил, что файл не был отображен, несмотря на права доступа, изучив логи веб-сервера и системные логи. (рис. 2.14)

```
Oct 14 21:41:00 daseregin systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 14 21:41:00 daseregin systemd[1]: setroubleshootd.service: Consumed 1.530s CPU time.
```

Рис. 2.14: Логи веб-сервера

16. Попытался запустить веб-сервер Apache на прослушивание TCP-порта 81 и выяснил, что возник сбой. Так как порт не является стандартным. (рис. 2.15)

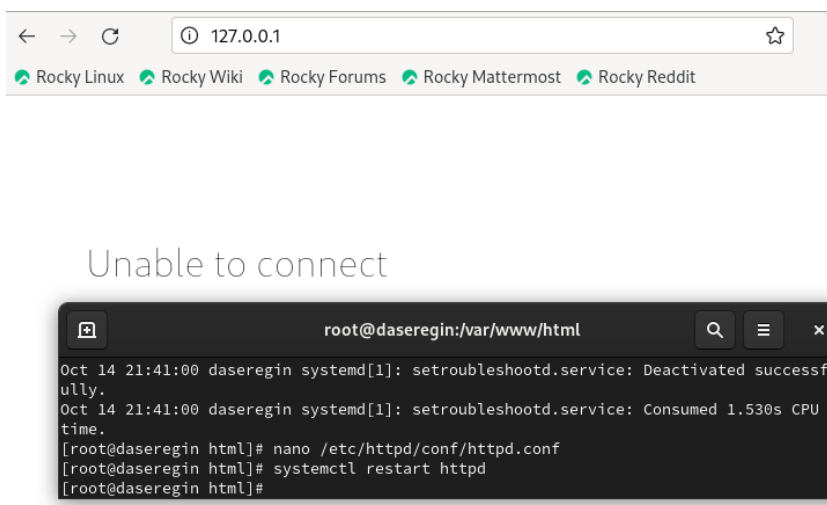


Рис. 2.15: Ошибка соединения с сервером

17. Проанализировал логи и выяснил причину сбоя при попытке изменения порта прослушивания. (рис. 2.16)

```
Oct 14 21:46:01 daseregin systemd[1]: Stopping The Apache HTTP Server...
Oct 14 21:46:02 daseregin systemd[1]: httpd.service: Deactivated successfully.
Oct 14 21:46:02 daseregin systemd[1]: Stopped The Apache HTTP Server.
Oct 14 21:46:02 daseregin systemd[1]: httpd.service: Consumed 1.242s CPU time.
Oct 14 21:46:02 daseregin systemd[1]: Starting The Apache HTTP Server...
Oct 14 21:46:02 daseregin systemd[1]: Started The Apache HTTP Server.
Oct 14 21:46:02 daseregin httpd[42141]: Server configured, listening on: port 81
```

Рис. 2.16: Логи Apache

18. Проанализировал логи веб-сервера Apache и системные логи, определив, где появились новые записи.

19. Выполнил команду `semanage port -a -t http_port_t -p tcp 81` и убедился, что порт 81 добавлен. (рис. 2.17)

```
[root@daseregin html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@daseregin html]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
```

Рис. 2.17: Добавления порта 81 в разрешенные

20. Попытался снова запустить веб-сервер Apache и убедился, что он запустился успешно.

Затем привёл всё к исходному состоянию следующими действиями:

21. Вернул контекст файла `/var/www/html/test.html` к исходному, предварительно изменив его на `samba_share_t`.
22. Изменил обратно конфигурационный файл Apache, вернув порт прослушивания к 80.
23. Удалил привязку `http_port_t` к порту 81.
24. Удалил файл `/var/www/html/test.html`.

## **3 Выводы**

В результате выполнения работы я развил свои навыки администрирования Linux, смог настроить SELinux, а также поработать с веб-сервисом Apache.