

# Отчёт по лабораторной работе №6

## Знакомство с SELinux

Овезов Мерген

### Содержание

## 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

### 2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

### 2.2 Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`.

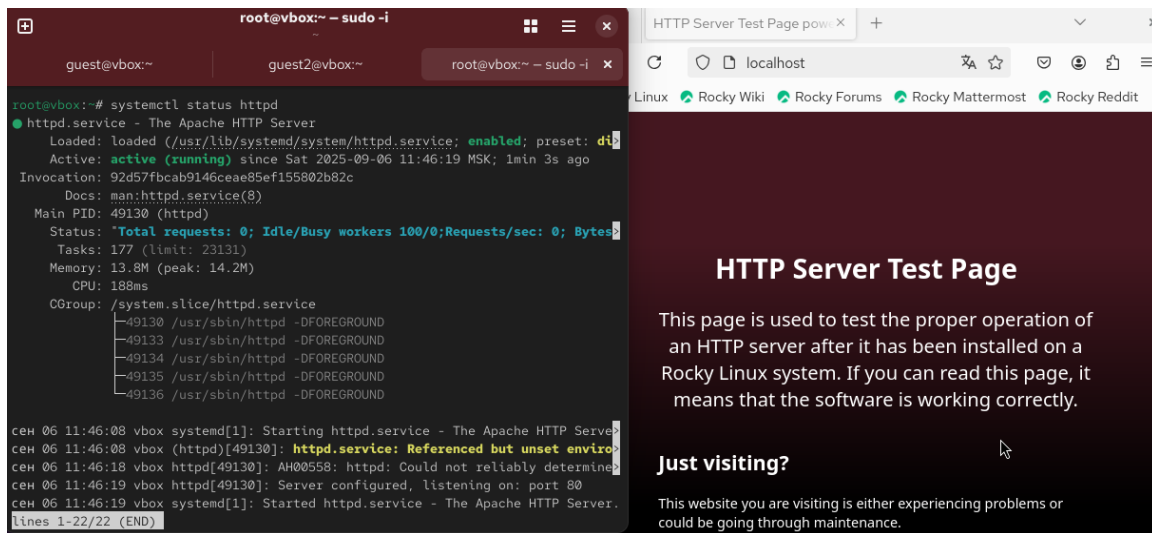


Figure 1: запуск http

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`

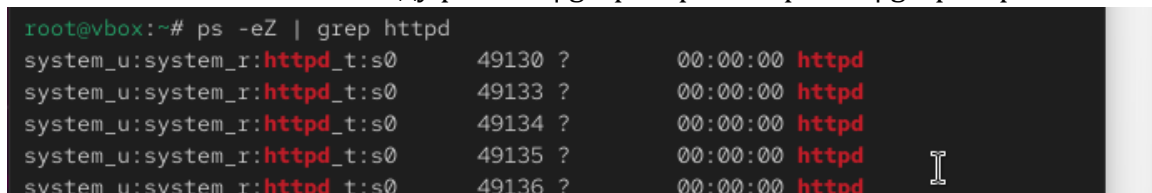


Figure 2: контекст безопасности http

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».

```

root@vbox:~# sestatus -b | grep httpd
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_redis         off
httpd_can_network_relay         off
httpd_can_sendmail              off
httpd_dbus_avahi                off
httpd_dbus_sssd                 off

```

Figure 3: переключатели SELinux для http

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. В директории изначально нет файлов.
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Создавать файлы может только `root`.
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: `Test`
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

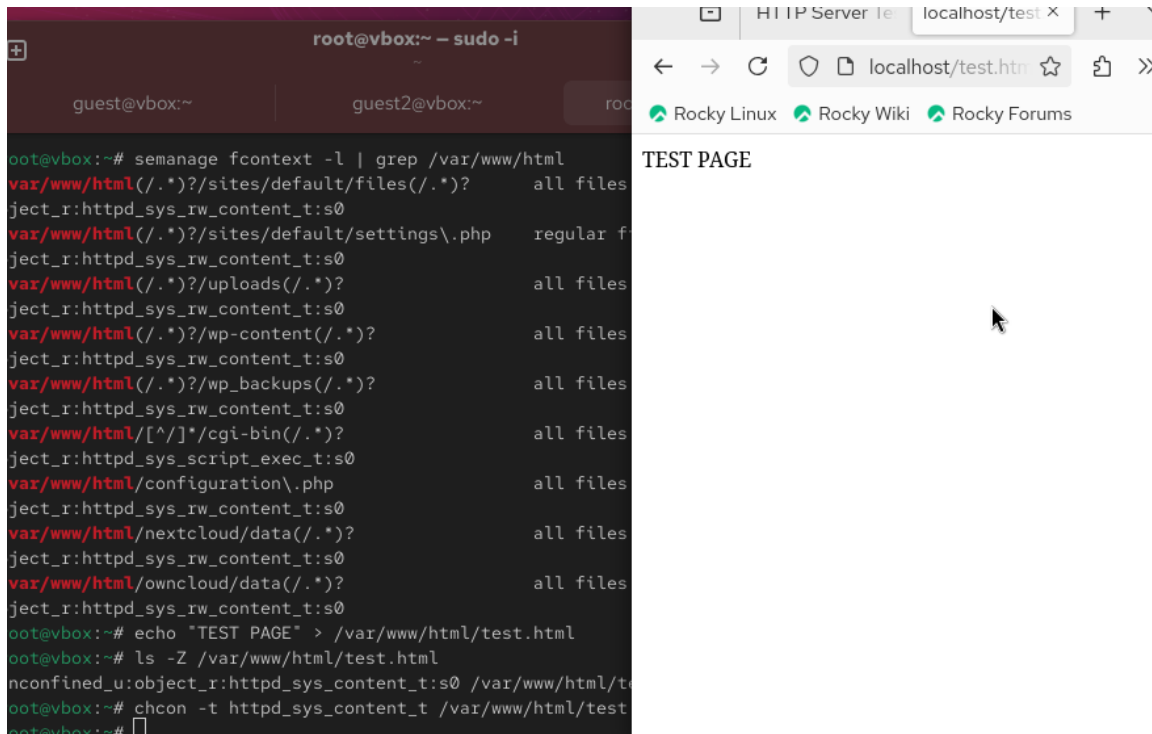


Figure 4: создание html-файла и доступ по http

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.
13. Измените контекст файла `/var/www/html/test.html` с `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` После этого проверьте, что контекст поменялся.
14. 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.` При изменении контекста файл стал считаться чужим для `http` и программа не может его прочитать.

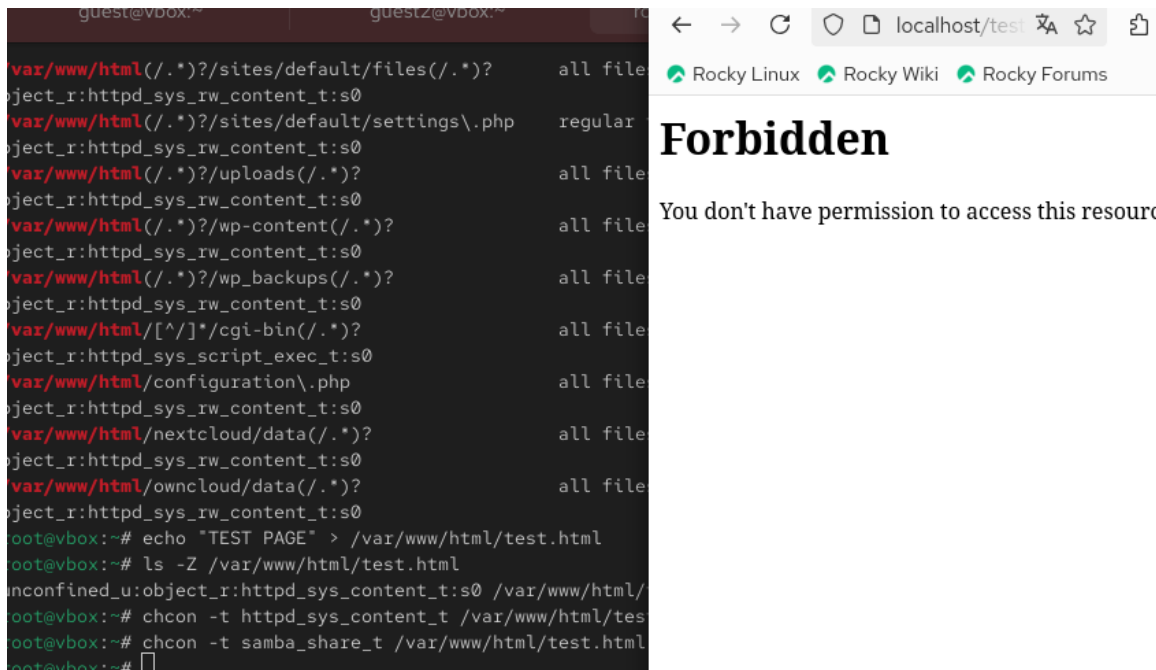


Figure 5: ошибка доступа после изменения контекста

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

```
root@vbox:~# chcon -t httpd_sys_content_t /var/www/html/test.html
root@vbox:~# cat /var/log/audit/audit.log | grep test.html
type=AVC msg=audit(1757149461.910:3473): avc: denied { getattr } for pid=49134 comm="httpd" path="/var/www/html/t
t=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=AVC msg=audit(1757149461.912:3474): avc: denied { getattr } for pid=49134 comm="httpd" path="/var/www/html/t
t=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
root@vbox:~# cat /var/log/httpd/error_log
[Sat Sep 06 11:46:18.482893 2025] [suexec:notice] [pid 49130:tid 49130] AH01232: suEXEC mechanism enabled (wrapper:
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fe05:321
globally to suppress this message
[Sat Sep 06 11:46:19.360110 2025] [lbmethod_heartbeat:notice] [pid 49130:tid 49130] AH02282: No slotmem from mod_he
[Sat Sep 06 11:46:19.362035 2025] [systemd:notice] [pid 49130:tid 49130] SELinux policy enabled; httpd running as co
[Sat Sep 06 11:46:19.368307 2025] [mpm_event:notice] [pid 49130:tid 49130] AH00489: Apache/2.4.63 (Rocky Linux) conf
[Sat Sep 06 11:46:19.368349 2025] [core:notice] [pid 49130:tid 49130] AH00094: Command line: '/usr/sbin/httpd -D FOR
[Sat Sep 06 11:48:19.370283 2025] [autoindex:error] [pid 49135:tid 49273] [client 127.0.0.1:59648] AH01276: Cannot s
g DirectoryIndex (index.html) found, and server-generated directory index forbidden by Options directive
[Sat Sep 06 12:04:21.913311 2025] [core:error] [pid 49134:tid 49186] (13)Permission denied: [client 127.0.0.1:52948]
lesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
root@vbox:~# cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Нет такого файла или каталога
root@vbox:~# cat /var/log/httpd/access_log
127.0.0.1 - - [06/Sep/2025:11:48:19 +0300] "GET / HTTP/1.1" 403 7620 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
127.0.0.1 - - [06/Sep/2025:11:48:19 +0300] "GET /icons/poweredby.png HTTP/1.1" 200 15443 "http://localhost/" "Mozill
/20100101 Firefox/128.0"
127.0.0.1 - - [06/Sep/2025:11:48:19 +0300] "GET /poweredby.png HTTP/1.1" 200 5714 "http://localhost/" "Mozilla/5.0 (
01 Firefox/128.0"
127.0.0.1 - - [06/Sep/2025:11:48:19 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://localhost/" "Mozilla/5.0 (X11
Firefox/128.0"
127.0.0.1 - - [06/Sep/2025:11:59:15 +0300] "GET /test.html HTTP/1.1" 200 10 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
127.0.0.1 - - [06/Sep/2025:11:59:15 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://localhost/test.html" "Mozilla
20100101 Firefox/128.0"
127.0.0.1 - - [06/Sep/2025:12:02:57 +0300] "GET /test.html HTTP/1.1" 200 10 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
127.0.0.1 - - [06/Sep/2025:12:04:21 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
127.0.0.1 - - [06/Sep/2025:12:05:15 +0300] "GET /test.html HTTP/1.1" 200 10 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
root@vbox:~#
```

Figure 6: лог ошибок

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.

```
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
```

Figure 7: переключение порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные
18. Проанализируйте лог-файлы: `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.
19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache ещё раз.
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».

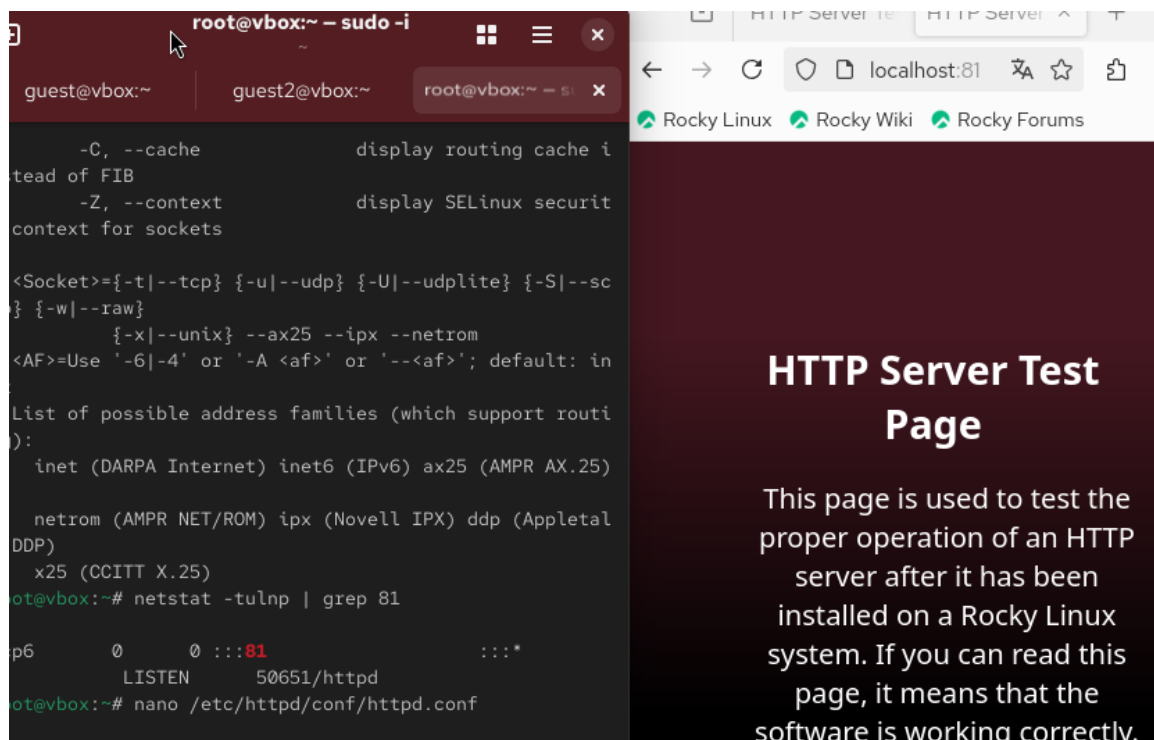


Figure 8: доступ по http на 81 порту

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
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

### 3 Выводы

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.

### Список литературы

1. SELinux в CentOS
2. Веб-сервер Apache