

# **Отчёт по лабораторной работе №6**

**Знакомство с SELinux**

Максим Платонов

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Подготовка . . . . .	5
2.2	Изучение механики SetUID . . . . .	5
<b>3</b>	<b>Выводы</b>	<b>13</b>
	<b>Список литературы</b>	<b>14</b>

# List of Figures

2.1	запуск http . . . . .	6
2.2	контекст безопасности http . . . . .	6
2.3	переключатели SELinux для http . . . . .	7
2.4	создание html-файла и доступ по http . . . . .	8
2.5	ошибка доступа после изменения контекста . . . . .	9
2.6	лог ошибок . . . . .	10
2.7	переключение порта . . . . .	11
2.8	доступ по http на 81 порт . . . . .	12

# 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`.

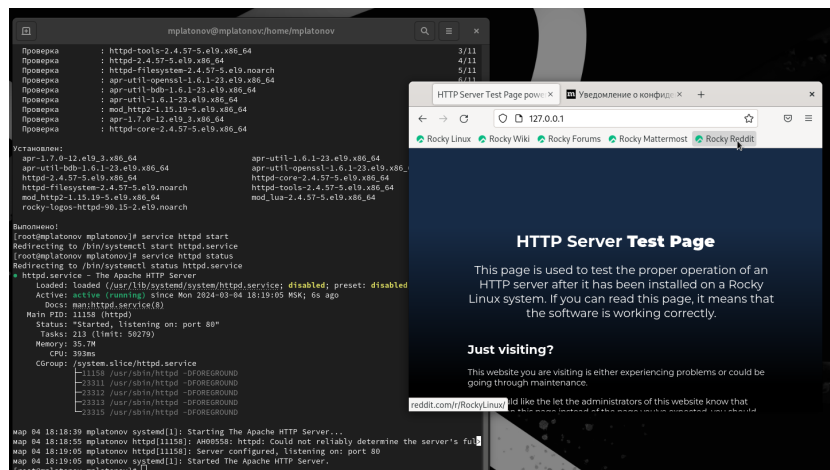


Figure 2.1: запуск http

- 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`

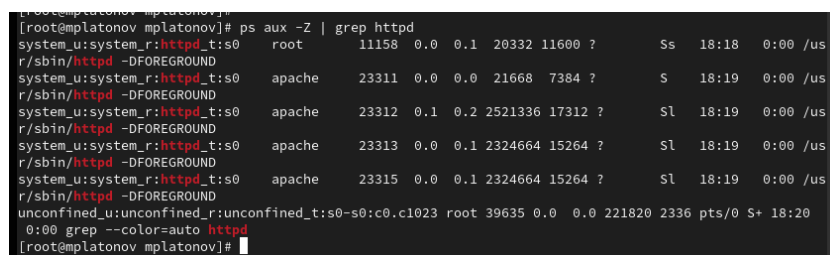


Figure 2.2: контекст безопасности http

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

```

[root@mplatonov mplatonov]#
[root@mplatonov mplatonov]# 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_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

```

Figure 2.3: 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.
- Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создавать файлы может только root.
  - 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
  - Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
  - Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

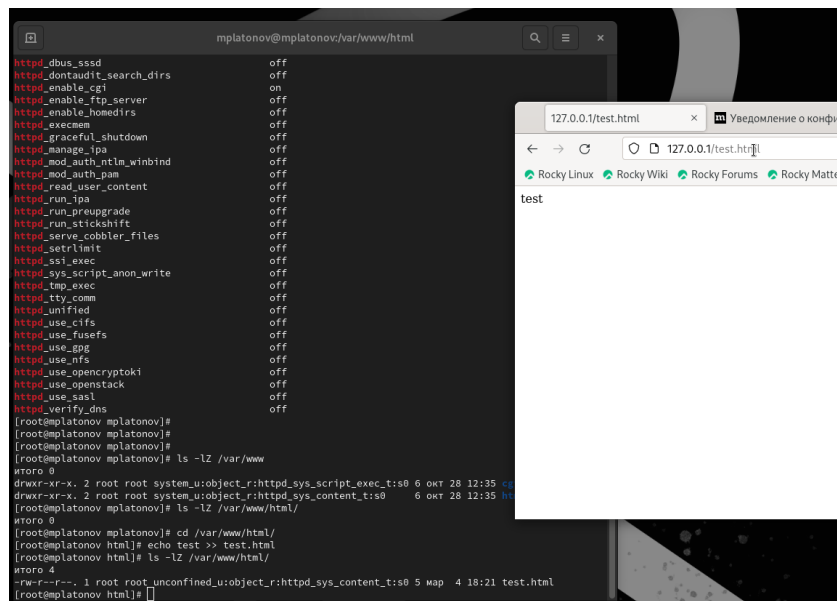


Figure 2.4: создание html-файла и доступ по http

- 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.

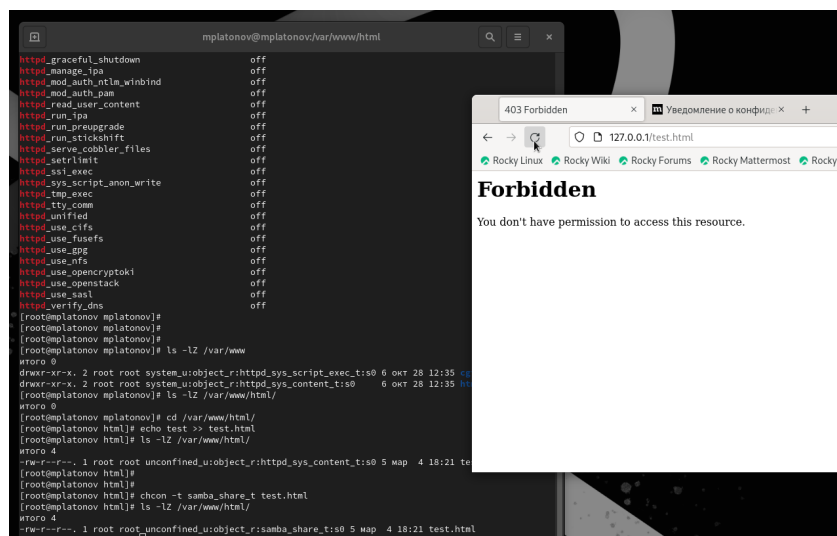
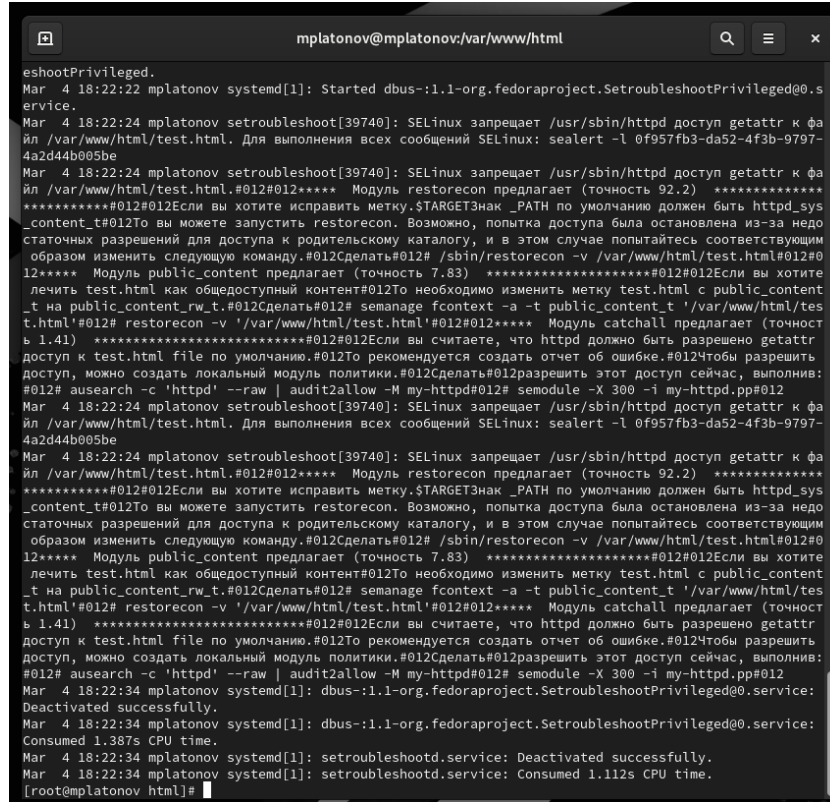


Figure 2.5: ошибка доступа после изменения контекста

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.



```
mplatonov@mplatonov:var/www/html
eshootPrivileged.
Mar  4 18:22:22 mplatonov systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.s
ervice.
Mar  4 18:22:24 mplatonov setroubleshoot[39740]: SELinux запрещает /usr/sbin/httpd доступ getattr к фа
йл /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 0f957fb3-da52-4f3b-9797-
4a2d44b005be
Mar  4 18:22:24 mplatonov setroubleshoot[39740]: SELinux запрещает /usr/sbin/httpd доступ getattr к фа
йл /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****
*****#012#012Если вы хотите исправить метку.$TARGET3знак _PATH по умолчанию должен быть httpd_sys
_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недо
статочных разрешений для доступа к родительскому каталогу, и в этом случае попытайтесь соответствующим
образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#0
12***** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите
лечить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content
_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/tes
t.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предлагает (точност
ь 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr
доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить
доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:
#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Mar  4 18:22:24 mplatonov setroubleshoot[39740]: SELinux запрещает /usr/sbin/httpd доступ getattr к фа
йл /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 0f957fb3-da52-4f3b-9797-
4a2d44b005be
Mar  4 18:22:24 mplatonov setroubleshoot[39740]: SELinux запрещает /usr/sbin/httpd доступ getattr к фа
йл /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****
*****#012#012Если вы хотите исправить метку.$TARGET3знак _PATH по умолчанию должен быть httpd_sys
_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недо
статочных разрешений для доступа к родительскому каталогу, и в этом случае попытайтесь соответствующим
образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#0
12***** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите
лечить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content
_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/tes
t.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предлагает (точност
ь 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr
доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить
доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:
#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Mar  4 18:22:34 mplatonov systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service:
Deactivated successfully.
Mar  4 18:22:34 mplatonov systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service:
Consumed 1.387s CPU time.
Mar  4 18:22:34 mplatonov systemd[1]: setroubleshootd.service: Deactivated successfully.
Mar  4 18:22:34 mplatonov systemd[1]: setroubleshootd.service: Consumed 1.112s CPU time.
[root@mplatonov html]#
```

Figure 2.6: 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.



http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test».

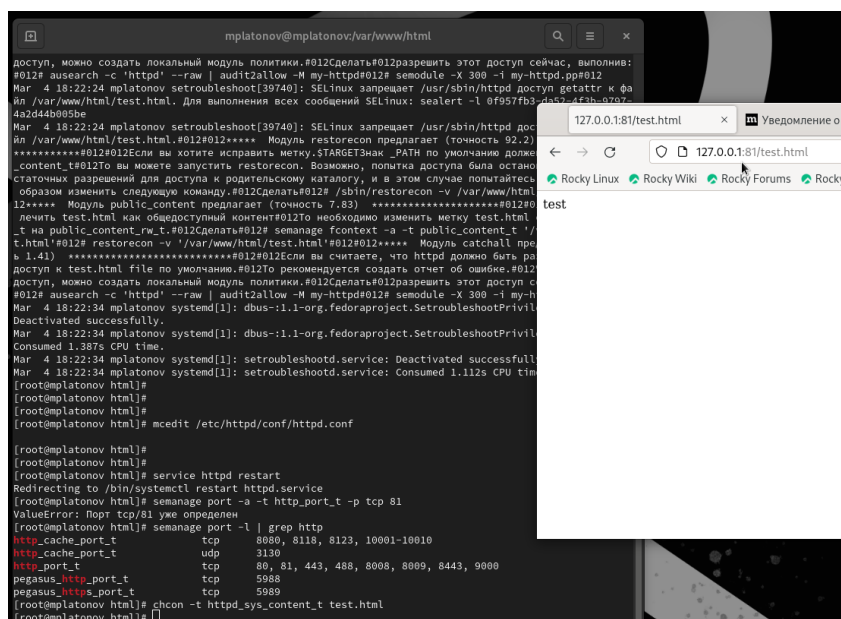


Figure 2.8: доступ по http на 81 порт

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