

# Лабораторная работа №6. Мандатное разграничение прав в Linux

Дисциплина: Основы информационной безопасности

---

Ганина Т. С.

27 апреля 2024

Группа НКАбд-01-22

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Ганина Таисия
- Студентка 2 курса, НКАбд-01-22
- Направление “Компьютерные и информационные науки”
- Российский университет дружбы народов
- Гитхаб
- <https://tsganina.github.io/>

## Вводная часть

---

- Работа с атрибутами файлов

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinux на практике совместно с веб-сервером Apache.

## Выполнение лабораторной работы

---

Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает с помощью команды “service httpd status”

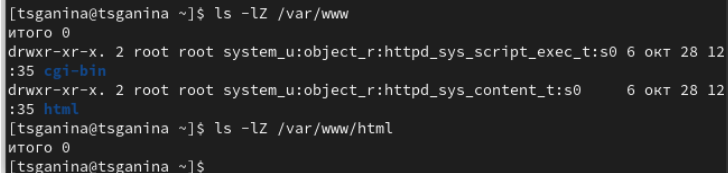
```
tsganina@tsganina:~ — /bin/systemctl status httpd.service

[tsganina@tsganina ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[tsganina@tsganina ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: d
  Active: active (running) since Sat 2024-04-27 20:33:32 MSK; 42s ago
  Docs: man:httpd.service(8)
  Main PID: 100666 (httpd)
  Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
  Tasks: 213 (limit: 12109)
  Memory: 50.0M
  CPU: 341ms
  CGroup: /system.slice/httpd.service
          └─100666 /usr/sbin/httpd -DFOREGROUND
            └─100677 /usr/sbin/httpd -DFOREGROUND
              └─100678 /usr/sbin/httpd -DFOREGROUND
                └─100679 /usr/sbin/httpd -DFOREGROUND
                  └─100680 /usr/sbin/httpd -DFOREGROUND

anp 27 20:33:32 tsganina.localdomain systemd[1]: Starting The Apache HTTP Serve
anp 27 20:33:32 tsganina.localdomain httpd[100666]: Server configured, listenin
anp 27 20:33:32 tsganina.localdomain systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
```



С помощью команды “ls -lZ /var/www” посмотрели файлы и поддиректории, находящиеся в директории /var/www



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

Рис. 2: (Просмотр файлов и поддиректорий в директории /var/www)

От имени суперпользователя создали html-файл `/var/www/html/test.html`. Контекст созданного файла - `httpd_sys_content_t`

```
[root@tsganina tsganina]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@tsganina tsganina]# exit
exit
[tsganina@tsganina ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 anp 27 2
0:44 test.html
[tsganina@tsganina ~]$
```

Рис. 3: (Создание файла `/var/www/html/test.html`)

Обратились к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”.  
Файл был успешно отображен

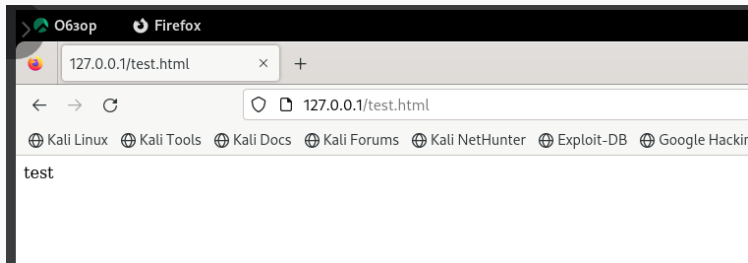


Рис. 4: (Обращение к файлу через веб-сервер)

```
[tsganina@tsganina ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
[tsganina@tsganina ~]$ man httpd
[tsganina@tsganina ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»: Операция не позволена
[tsganina@tsganina ~]$ su
Пароль:
[root@tsganina tsganina]# chcon -t samba_share_t /var/www/html/test.html
[root@tsganina tsganina]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 апр 27 20:44 /
var/www/html/test.html
[root@tsganina tsganina]#
```

Рис. 5: (Изменение контекста)

Попробовали еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получили сообщение об ошибке (т.к. к установленному ранее контексту процесс httpd не имеет доступа)

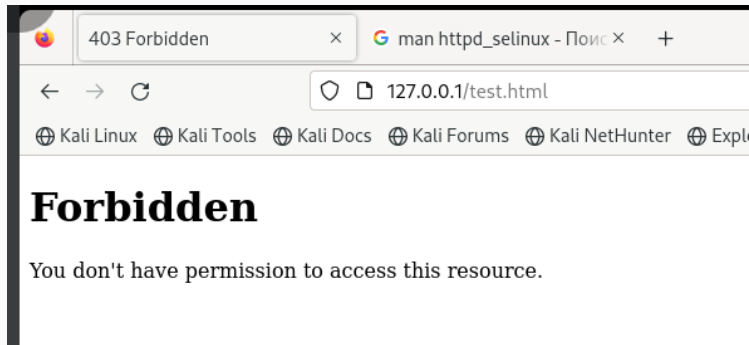
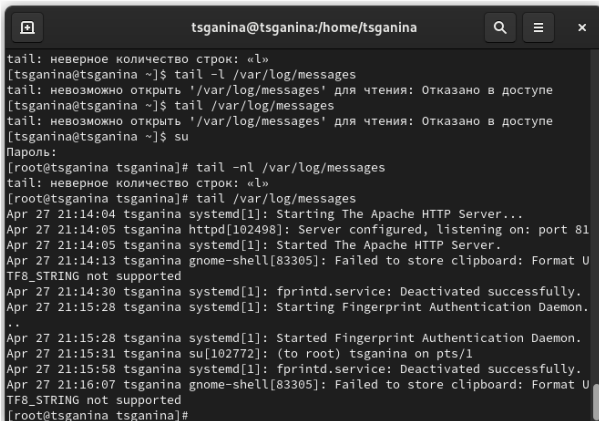


Рис. 6: (Обращение к файлу через веб-сервер)

Просмотрели системный лог-файл веб-сервера Apache командой “`sudo tail /var/log/messages`”, отображающий ошибки

A terminal window titled 'tsganina@tsganina:/home/tsganina' with search, menu, and close icons. The terminal shows a series of commands and their outputs. The user first tries to run 'tail -l /var/log/messages' as a regular user, which fails with an error about the number of lines and a permission denied message. Then, the user switches to root using 'su'. As root, the user runs 'tail -nl /var/log/messages', which successfully displays the last lines of the log file. The log entries show the Apache HTTP server starting, systemd messages, and a failed attempt to store clipboard data.

```
tsganina@tsganina:/home/tsganina
tail: неверное количество строк: «l»
[tsganina@tsganina ~]$ tail -l /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[tsganina@tsganina ~]$ tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[tsganina@tsganina ~]$ su
Пароль:
[root@tsganina tsganina]# tail -nl /var/log/messages
tail: неверное количество строк: «l»
[root@tsganina tsganina]# tail /var/log/messages
Apr 27 21:14:04 tsganina systemd[1]: Starting The Apache HTTP Server...
Apr 27 21:14:05 tsganina httpd[102498]: Server configured, listening on: port 81
Apr 27 21:14:05 tsganina systemd[1]: Started The Apache HTTP Server.
Apr 27 21:14:13 tsganina gnome-shell[83305]: Failed to store clipboard: Format UTF8_STRING not supported
Apr 27 21:14:30 tsganina systemd[1]: fprintd.service: Deactivated successfully.
Apr 27 21:15:28 tsganina systemd[1]: Starting Fingerprint Authentication Daemon.
..
Apr 27 21:15:28 tsganina systemd[1]: Started Fingerprint Authentication Daemon.
Apr 27 21:15:31 tsganina su[102772]: (to root) tsganina on pts/1
Apr 27 21:15:58 tsganina systemd[1]: fprintd.service: Deactivated successfully.
Apr 27 21:16:07 tsganina gnome-shell[83305]: Failed to store clipboard: Format UTF8_STRING not supported
[root@tsganina tsganina]#
```

Рис. 7: (Просмотр log-файла)

Вернули контекст “httpd\_sys\_content\_t” файлу “/var/www/html/test.html” командой “chcon -t httpd\_sys\_content\_t /var/www/html/test.html” и после этого попробовали получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидели содержимое файла - слово “test”

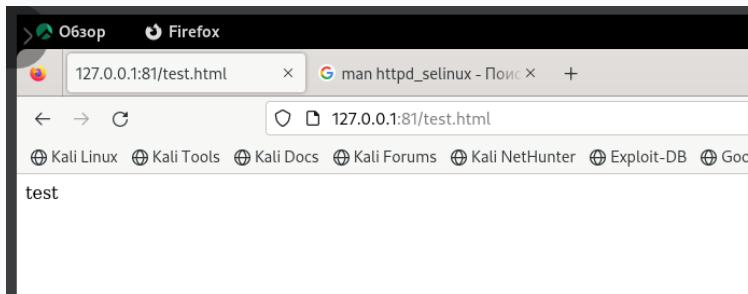


Рис. 8: (Обращение к файлу через веб-сервер)

Удалили файл “/var/www/html/test.html” командой “rm /var/www/html/test.html”

```
[tsganina@tsganina ~]$ semanage port -d -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[tsganina@tsganina ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[tsganina@tsganina ~]$ sudo rm /var/www/html/test.html
[tsganina@tsganina ~]$
```

Рис. 9: (Возвращение Listen 80 и попытка удалить порт 81)



## Результаты

---

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.