

# Мандатное разграничение прав в Linux.

---

Алхимова Дарья Сергеевна НБИ-01-19<sup>1</sup>

12 октября, 2022

<sup>1</sup>Российский Университет Дружбы Народов

## Докладчик

- Алхимова Дарья Сергеевна
- студентка 4 курса
- группы НБИбд-01-19
- Российский университет дружбы народов
- 1032191645@rudn.ru

Целью данной работы является приобретение навыков администрирования ОС Linux, получение первого практического знакомства с технологией SELinux1 и проверка работы SELinx на практике совместно с веб-сервером Apache.

## Прверила работу SELinux

Вошла в систему и вызвала команды `getenforce` и `sestatus`

```
[root@dsalkhimova dsalkhimova]# getenforce
Enforcing
[root@dsalkhimova dsalkhimova]# 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:          disabled
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
[root@dsalkhimova dsalkhimova]# █
```

**Рис. 1:** Проверка работы SELinux

# Выполнение лабораторной работы

## Определила контекст безопасности Apache

Использовала команду `ps auxZ | grep httpd`.

```
[root@dsalkhimova dsalkhimova]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 16166 0.1 0.6 314768 6388 ? Ss 20:59 0
:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16171 0.0 0.5 316988 5792 ? S 20:59 0
:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16172 0.0 0.5 316988 5468 ? S 20:59 0
:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16173 0.0 0.5 316988 5468 ? S 20:59 0
:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16174 0.0 0.5 316988 5468 ? S 20:59 0
:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16175 0.0 0.5 316988 5468 ? S 20:59 0
:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16274 0.0 0.5 316988 5468 ? S 21:01 0
:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 16840 0.0 0.0 112808 968 pts/0 R+
21:26 0:00 grep --color=auto httpd
[root@dsalkhimova dsalkhimova]#
```

Рис. 2: Контекст Apache

# Выполнение лабораторной работы

## Посмотрела статистику по политике

Использовала команду seinfo

```
zoneminder_run_sudo                                     off
[root@dsalkhimova dsalkhimova]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1        Categories:       1024
Types:            4793     Attributes:        253
Users:            8        Roles:            14
Booleans:         316     Cond. Expr.:      362
Allow:            107834   Neverallow:        0
Auditallow:       158     Dontaudit:         10022
Type_trans:       18153   Type_change:       74
Type_member:      35      Role_allow:        37
Role_trans:       414     Range_trans:       5899
Constraints:      143     Validatetrans:     0
Initial SIDs:     27      Fs_use:            32
Genfscon:         103     Portcon:           614
Netifcon:         0       Nodecon:           0
```

**Рис. 3:** Статистика по политике

## Определила тип файлов и поддиректорий /var/www

Использовала команду `ls -lZ /var/www`. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[root@dsalkhimova dsalkhimova]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@dsalkhimova dsalkhimova]# ls -lZ /var/www/html
[root@dsalkhimova dsalkhimova]#
```

**Рис. 4:** Типы файлов, поддиректорий и права для /www и /html

## Создала html-файл test.html

Файл следующего содержания:

```
<html>
```

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

```
</html>
```

```
[root@dsalkhimova dsalkhimova]# touch /var/www/html/test.html  
[root@dsalkhimova dsalkhimova]# nano /var/www/html/test.html
```

**Рис. 5:** Создание файла test.html



## Проверила контекст созданного файла

Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html - httpd\_sys\_content\_t

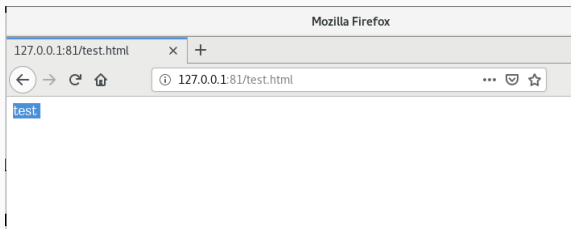
```
[root@dsalkhimova dsalkhimova]# ls -lZ /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

**Рис. 6:** Контекст файла test.html

# Выполнение лабораторной работы

**Обратилась к файлу через веб-сервер**

Ввела адрес `http://127.0.0.1/test.html`



**Рис. 7:** Открытие test.html через браузер

## Изменила контекст файла

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

```
[root@dsalkhimova dsalkhimova]# chcon -t samba_share_t /var/www/html/test.html
[root@dsalkhimova dsalkhimova]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

**Рис. 8:** Смена контекста файла test.html

# Выполнение лабораторной работы

Повторно обратилась к файлу через веб-сервер  
Получила сообщение об ошибке

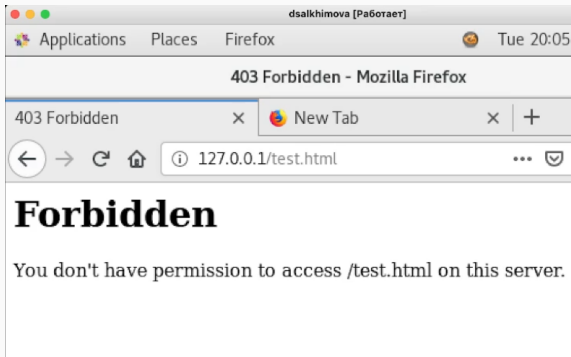
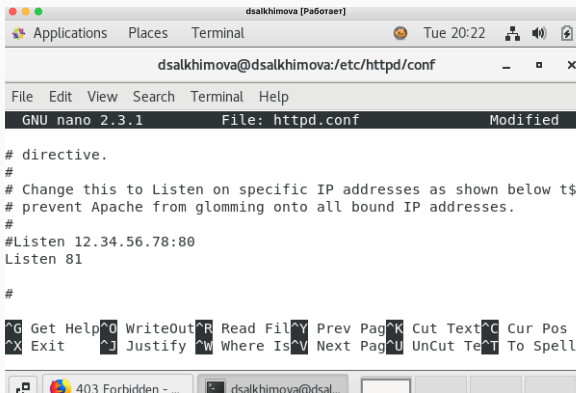


Рис. 9: Повторное открытие test.html через браузер

# Выполнение лабораторной работы

## Запустила веб-сервер Apache на прослушивание TCP-порта 81

Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81



```
dsalkhimova [Работаer]
Applications Places Terminal Tue 20:22
dsalkhimova@dsalkhimova:/etc/httpd/conf
File Edit View Search Terminal Help
GNU nano 2.3.1 File: httpd.conf Modified

# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
#

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Te ^T To Spell
```

Рис. 10: httpd.conf после исправления

## Выполнила перезапуск веб-сервера Apache

```
[dsalkhimova@dsalkhimova root]$ service httpd restart  
Redirecting to /bin/systemctl restart httpd.service
```

**Рис. 11:** Перезапуск Apache

## Добавила порт 81

Выполнила команду `semanage port -a -t http_port_t -tcp 81` и проверила список портов командой `semanage port -l | grep http_port_t`

```
[root@dsalkhimova dsalkhimova]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@dsalkhimova dsalkhimova]# 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
```

**Рис. 12:** Добавление и просмотр наличия 81 порта

## Попробовала запустить веб-сервер Apache ещё раз

```
[root@dsalkhimova dsalkhimova]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service
```

**Рис. 13:** Запуск Apache



**Вернула исходный контекст файлу test.html**

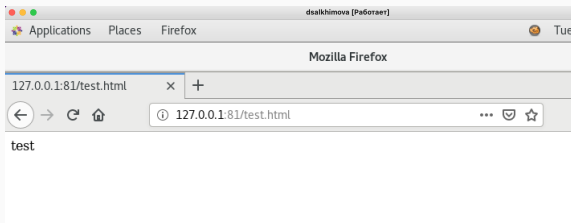
Использовала `chcon -t httpd_sys_content_t /var/www/html/test.html`

```
[root@dsalkhimova dsalkhimova]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dsalkhimova dsalkhimova]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@dsalkhimova dsalkhimova]# █
```

**Рис. 14:** Возвращение контекста файлу test.html

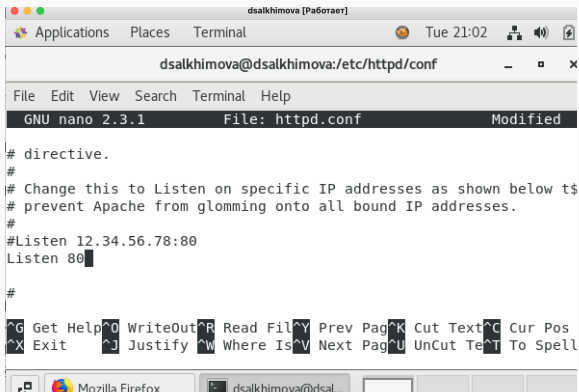
**Снова попробовала получить доступ к файлу через веб-сервер**

Ввела в браузере адрес `http://127.0.0.1:81/test.html`.



**Рис. 15:** Открытие файла test.html через браузер

## Исправила обратно конфигурационный файл Apache



```
dsalkhimova [Работаer]
Applications Places Terminal Tue 21:02
dsalkhimova@dsalkhimova:/etc/httpd/conf
File Edit View Search Terminal Help
GNU nano 2.3.1 File: httpd.conf Modified
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Te ^T To Spell
```

**Рис. 16:** Возвращение настроек на 80 порт httpd.conf

**Пропробовала удалить привязку http\_port\_t к 81 порту**  
Операция запрещена, поэтому порт 81 остался в списке.

```
[root@dsalkhimova conf]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

**Рис. 17:** Попытка удаления 81 порта

## Удалила файл test.html

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

```
[root@dsalkhimova dsalkhimova]# rm /var/www/html/test.html  
rm: remove regular file '/var/www/html/test.html'? y
```

**Рис. 18:** Удаление файла test.html

В процессе выполнения данной лабораторной работы я приобрела навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.