

Презентация по лабораторной работе №6

Мандатное разграничение прав в Linux

Танрибергенов Э.

2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Танрибергенов Эльдар
- студент 4 курса из группы НПИбд-02-21
- ФМиЕН, кафедра прикладной информатики и теории вероятностей
- Российский университет дружбы народов

Цели и задачи

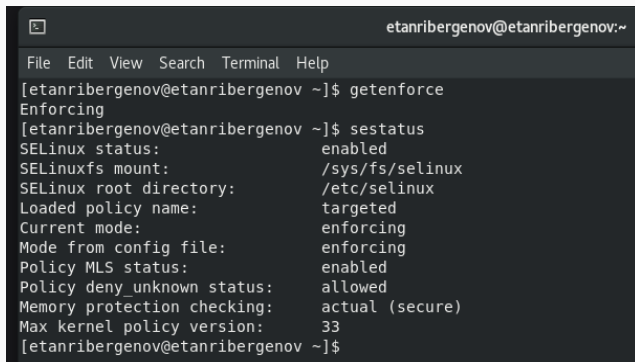
Развить навыки администрирования ОС *Linux*. Получить первое практическое знакомство с технологией *SELinux*. Проверить работу *SELinux* на практике совместно с веб-сервером *Apache*.

- Проверить работу *SELinux* на практике совместно с веб-сервером *Apache*

Результаты

Проверка работы *SELinux* на практике совместно с веб-сервером *Apache*

- команда *getenforce* - выводит режим работы *SELinux*
- команда *sestatus* - выводит статус *SELinux*

A screenshot of a terminal window with a dark background. The title bar shows a window icon and the text 'etanribergenov@etanribergenov:~'. The menu bar contains 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal text shows the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' lists various SELinux parameters and their values.

```
etanribergenov@etanribergenov:~  
File Edit View Search Terminal Help  
[etanribergenov@etanribergenov ~]$ getenforce  
Enforcing  
[etanribergenov@etanribergenov ~]$ 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  
[etanribergenov@etanribergenov ~]$
```

Рис. 1: Проверка того, что SeLinux работает в режиме enforcing политики targeted

Проверка работы *SELinux* на практике совместно с веб-сервером *Apache*

- команда *service httpd start*

```
[etanribergenov@etanribergenov ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[eetanribergenov@etanribergenov ~]$ 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; vendor preset: disabled)
   Active: active (running) since Sat 2024-11-16 12:40:10 +05; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 3520 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 37634)
   Memory: 49.8M
    CGroup: /system.slice/httpd.service
            └─3520 /usr/sbin/httpd -DFOREGROUND
              └─3536 /usr/sbin/httpd -DFOREGROUND
                └─3537 /usr/sbin/httpd -DFOREGROUND
                  └─3538 /usr/sbin/httpd -DFOREGROUND
                    └─3539 /usr/sbin/httpd -DFOREGROUND

Nov 16 12:40:09 etanribergenov.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 16 12:40:10 etanribergenov.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 16 12:40:10 etanribergenov.localdomain httpd[3520]: Server configured, listening on: port 80
[eetanribergenov@etanribergenov ~]$
```

Рис. 2: Запуск веб-сервера

- команда *ls -l var/www | grep html*
- только у суперпользователя есть разрешение на запись в директорию

```
[etanribergenov@etanribergenov ~]$ ls -l /var/www | grep html
drwxr-xr-x. 2 root root 6 Aug 12 13:14 html
[etanribergenov@etanribergenov ~]$
```

Рис. 3: Просмотр атрибутов директории для определения круга пользователей, которым разрешено создание файлов в директории

- выполнено в *Gedit*, свободном текстовом редакторе для среды *GNOME*



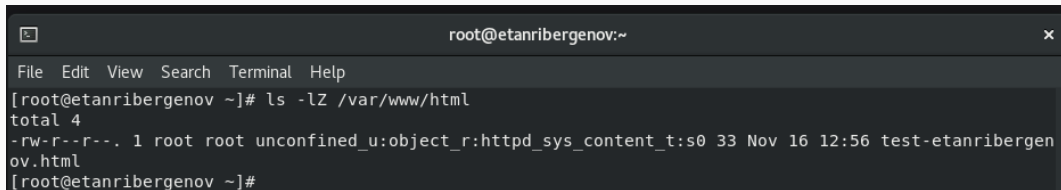
```
test-etanribergenov.html
/var/www/html

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

Рис. 4: Содержимое HTML-файла test-etanribergenov

Проверка работы *SELinux* на практике совместно с веб-сервером *Apache*

- команда *ls -Z <file>*
- контекст, присваиваемый по умолчанию вновь созданным файлам в директории */var/www/html* - *httpd_sys_content_t*.



```
root@etanribergenov:~  
File Edit View Search Terminal Help  
[root@etanribergenov ~]# ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Nov 16 12:56 test-etanribergenov.html  
[root@etanribergenov ~]#
```

Рис. 5: Проверка контекста безопасности созданного файла

- выполнено в веб-браузере *Firefox*

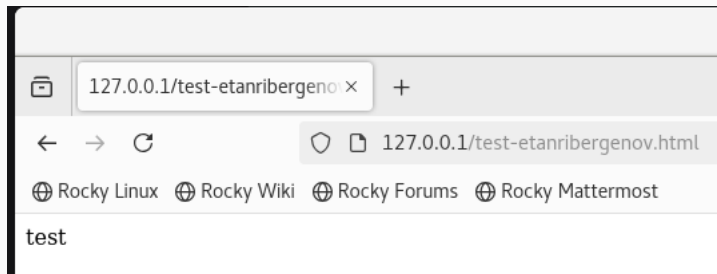


Рис. 6: Обращение к файлу через веб-сервер в браузере

- команда ***chcon -t <контекст_безопасности> <файл>*** - меняет контекст *SELinux* для файла
- ***ls -Z <file>*** - проверка контекста безопасности *SELinux*

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

Рис. 7: Изменение контекста *SELinux* для файла

- выполнено в веб-браузере *Firefox*

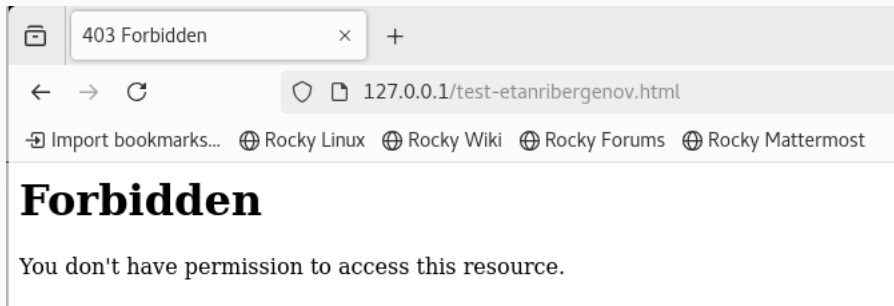
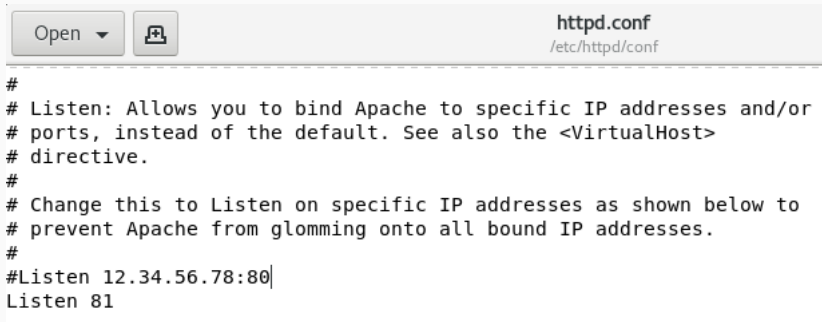


Рис. 8: Попытка получения доступа к файлу через веб-сервер в браузере

Проверка работы *SELinux* на практике совместно с веб-сервером *Apache*

- в файле конф. файле веб-сервера *Apache* */etc/httpd/httpd.conf* строка ***Listen 80*** заменена на ***Listen 81***

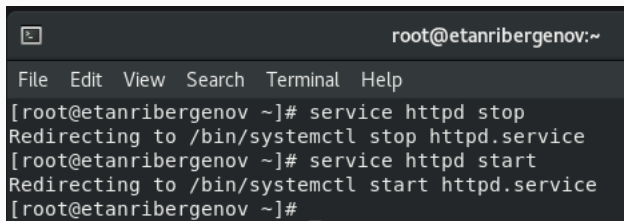


The image shows a text editor window titled 'httpd.conf' with the path '/etc/httpd/conf'. The editor contains the following text:

```
#  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default. See also the <VirtualHost>  
# 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
```

Рис. 9: Изменение порта прослушивания веб-сервера Apache

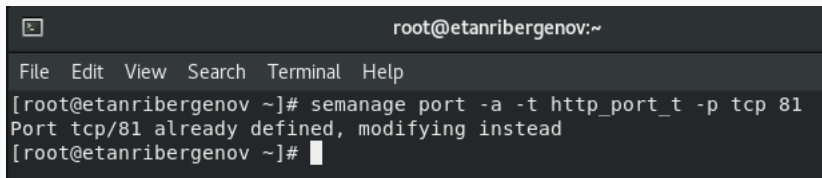
- Сбой не произошёл



```
root@etanribergenov:~  
File Edit View Search Terminal Help  
[root@etanribergenov ~]# service httpd stop  
Redirecting to /bin/systemctl stop httpd.service  
[root@etanribergenov ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@etanribergenov ~]#
```

Рис. 10: Выполнение перезапуска веб-сервера

- команда *semanage port -a -t http_port_t -p tcp 81*



```
root@etanribergenov:~  
File Edit View Search Terminal Help  
[root@etanribergenov ~]# semanage port -a -t http_port_t -p tcp 81  
Port tcp/81 already defined, modifying instead  
[root@etanribergenov ~]#
```

Рис. 11: Добавление tcp-порта 81 в список портов SELinux для веб-сервера

- команда *semanage port -l | grep http_port_t*

```
[root@etanribergenov ~]# semanage port -l | grep http_port_t
http_port_t            tcp      81, 80, 81, 443, 488, 8008, 8009, 8443,
9000
pegasus_http_port_t    tcp      5988
[root@etanribergenov ~]#
```

Рис. 12: Просмотр списка портов SELinux для веб-сервера

```
[root@etanribergenov ~]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@etanribergenov ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@etanribergenov ~]#
```

Рис. 13: Перезапуск веб-сервера Apache

- команда *chcon -t <контекст_безопасности> <файл>*

```
[root@etanribergenov ~]# chcon -t httpd_sys_content_t /var/www/html/test-etanribergenov.html  
[root@etanribergenov ~]#
```

Рис. 14: Возвращение контекста SELinux к файлу

- выполнено в веб-браузере *Firefox*

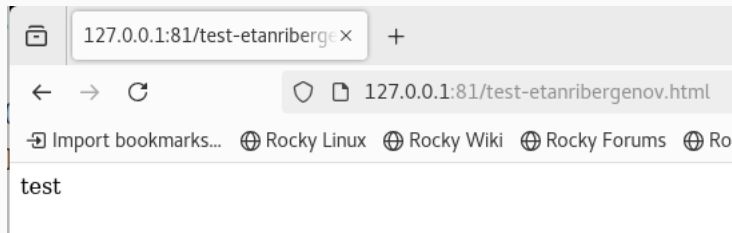


Рис. 15: Получение доступа к файлу через веб-сервер в браузере

Вывод

В результате выполнения работы я развил навыки администрирования ОС *Linux*. Получил первое практическое знакомство с технологией *SELinux*. Проверил работу *SELinux* на практике совместно с веб-сервером *Apache*.