

Презентация по лабораторной работе №6.

Основы информационной безопасности.

Рогожина Н.А.

21 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

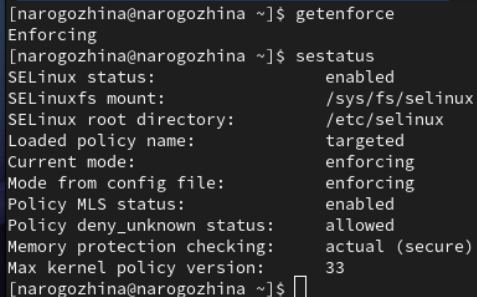
- Рогожина Надежда Александровна
- Студентка 2го курса, НКАбд-02-22
- Компьютерные и информационные науки
- Российский университет дружбы народов
- Github

Цели работы

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.
- Проверить работу SELinx на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

A terminal window with a dark background and light blue text. The prompt is [narogozhina@narogozhina ~]\$. The first command is getenforce, which returns Enforcing. The second command is sestatus, which returns a detailed status report for SELinux.

```
[narogozhina@narogozhina ~]$ getenforce
Enforcing
[narogozhina@narogozhina ~]$ 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
[narogozhina@narogozhina ~]$
```

Рис. 1: Статус SELinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает `service httpd status`.

```
se[narogozhina@narogozhina ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sun 2024-04-21 10:36:09 MSK; 1h 19min ago
     Docs: man:httpd.service(8)
   Main PID: 1266 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: >
     Tasks: 213 (limit: 10978)
   Memory: 17.0M
     CPU: 1.982s
   CGroup: /system.slice/httpd.service
           └─1266 /usr/sbin/httpd -DFOREGROUND
             └─1356 /usr/sbin/httpd -DFOREGROUND
               └─1361 /usr/sbin/httpd -DFOREGROUND
                 └─1366 /usr/sbin/httpd -DFOREGROUND
                   └─1367 /usr/sbin/httpd -DFOREGROUND

Apr 21 10:36:08 narogozhina.localdomain systemd[1]: Starting The Apache HTTP Server...
Apr 21 10:36:09 narogozhina.localdomain systemd[1]: Started The Apache HTTP Server.
Apr 21 10:36:09 narogozhina.localdomain httpd[1266]: Server configured, listening on: port 80
lines 1-19/19 (END)
```

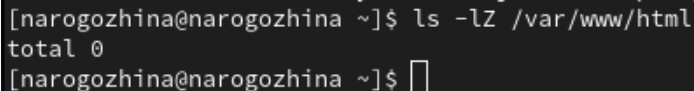
Рис. 2: service httpd status

3. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`.

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

Рис. 3: Тип файлов и поддиректорий

4. Определите тип файлов, находящихся в директории `/var/www/html` `ls -lZ /var/www/html`. Создание файлов в директории `/var/www/html` разрешено только владельцу данной директории.



```
[narogozhina@narogozhina ~]$ ls -lZ /var/www/html
total 0
[narogozhina@narogozhina ~]$
```

Рис. 4: Поддиректории

5. 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:

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

Создание тестового файла

```
[root@narogozhina conf]# touch /var/www/html/test.html
[root@narogozhina conf]# gedit /var/www/html/test.html

(gedit:4631): dconf-WARNING **: 12:02:13.508: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:4631): dconf-WARNING **: 12:02:13.514: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:4631): dconf-WARNING **: 12:02:13.826: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:4631): dconf-WARNING **: 12:02:13.827: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

(gedit:4631): dconf-WARNING **: 12:02:13.827: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

** (gedit:4631): WARNING **: 12:02:21.489: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

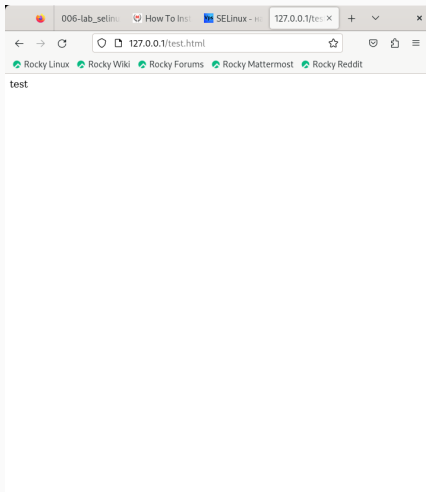
** (gedit:4631): WARNING **: 12:02:21.489: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:4631): WARNING **: 12:02:24.722: Set document metadata failed: Setting attribute metadata::gedit-position not supported

(gedit:4631): dconf-WARNING **: 12:02:24.740: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
[root@narogozhina conf]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@narogozhina conf]#
```

Рис. 5: Создание файла

6. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.
Убедитесь, что файл был успешно отображён.



Контекст файла `test.html`: `unconfined_u:object_r:httpd_sys_content_t:s0`

7. 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
```

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

Рис. 7: изменение контекста

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.`

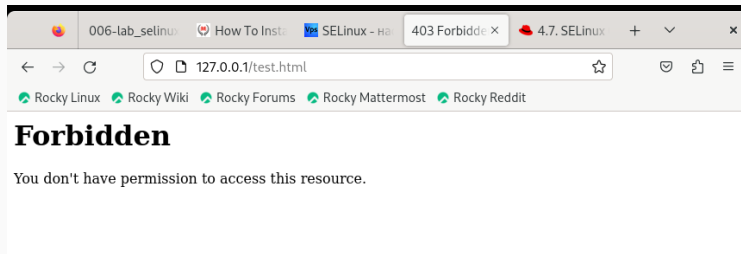


Рис. 8: попытка №1

```
[root@narogozhina conf]# ls -l /vat/www/html/test.html
ls: cannot access '/vat/www/html/test.html': No such file or directory
[root@narogozhina conf]#
```

Рис. 9: выполнение команды

Переписывание порта

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`.

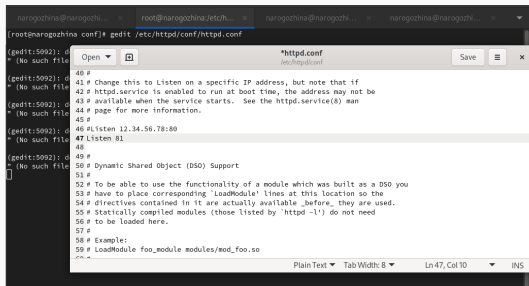


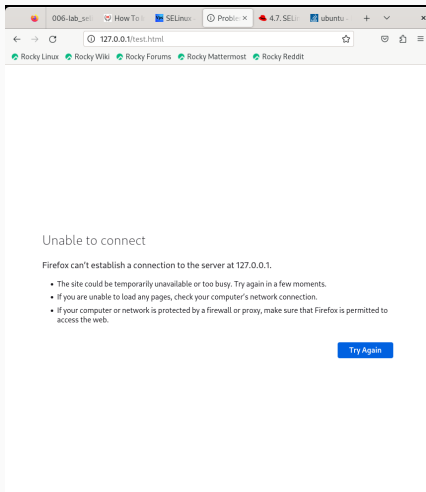
Рис. 10: Listen 80 -> Listen 81

```
bash: apachectl: command not found...  
[root@narogozhina conf]# systemctl restart httpd  
[root@narogozhina conf]#
```

Рис. 11: restart

Попытка подключения

При попытке переподключиться - произошел сбой, т.к. мы подключаемся по другому tcp серверу.



```
[narogozhina@narogozhina ~]$ sudo semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[narogozhina@narogozhina ~]$
```

Рис. 13: semanage

```
datacenter: SELinux policy is not managed or store cannot be accessed.  
[narogozhina@narogozhina ~]$ sudo 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  
[narogozhina@narogozhina ~]$
```

Рис. 14: semanage grep

Порт 81 появился в списке.

Попытка переподключения

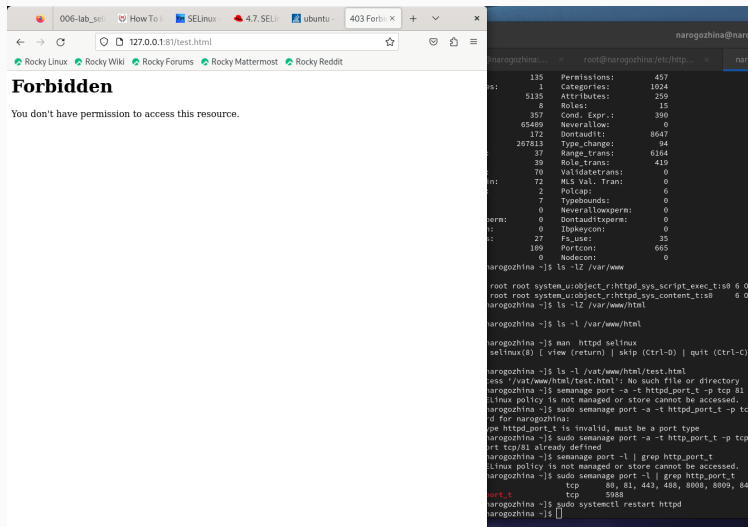


Рис. 15: Попытка №3

Выводы

В ходе лабораторной работы мы развили навыки администрирования ОС Linux, получить первое практическое знакомство с технологией SELinux¹, а также проверили работу SELinux на практике совместно с веб-сервером Apache.