### РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

#### ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Поляков Арсений Андреевич

Группа: НФИбд-01-19

МОСКВА 2022 г.

## Цель работы

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с вебсервером Apache.

# Выполнение лабораторной работы

1. Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**.

```
[a.polyakov@a ~]$ getenforce
Enforcing
[a.polyakov@a ~]$ 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
                                enabled
Policy MLS status:
                                allowed
Policy deny unknown status:
Memory protection checking:
                                actual (secure)
Max kernel policy version:
                                33
```

2. Запустили веб-сервер и обратились к нему с помощью команды: service httpd status

```
[a.polyakov@a ~]$ 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; vendor pre>
    Active: active (running) since Wed 2022-10-12 18:57:48 MSK; 19min ago
      Docs: man:httpd.service(8)
  Main PID: 95236 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes>
     Tasks: 213 (limit: 18634)
    Memory: 23.3M
       CPU: 410ms
    CGroup: /system.slice/httpd.service
             —95236 /usr/sbin/httpd -DFOREGROUND
             —95237 /usr/sbin/httpd -DFOREGROUND
             —95238 /usr/sbin/httpd -DFOREGROUND
             —95242 /usr/sbin/httpd -DFOREGROUND
             └95243 /usr/sbin/httpd -DFOREGROUND
```

3. Найшли веб-сервер Apache в списке процессов с помощью команды **ps auxZ** | **grep httpd**. Контекст безопасности - unconfined\_u:unconfined\_r:unconfined\_t.

```
[a.polyakov@a ~]$ ps auxZ | grep httpd
system u:system r:httpd t:s0
                                          95236 0.0 0.3 20248 11900 ?
                                root
     18:57
             0:00 /usr/sbin/
                              tpd -DFOREGROUND
                                                 0.0 0.2 21572 7396 ?
system u:system r:ht1
                               apache
                     pd t:s0
                                          95237
             0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0
                               apache
                                          95238
                                                 0.0 0.3 1079376 11120 ?
     18:57
             0:00 /usr/sbin/ht
                                  -DFOREGROUND
system u:system r:httpd t:s0
                               apache
                                                0.0 0.4 1210512 13168 ?
                                          95242
     18:57
             0:00 /usr/sbin/
                                   -DFOREGROUND
                                                 0.0 0.3 1079376 11120 ?
system u:system r:httpd t:s0
                               apache
                                          95243
    18:57
             0:00 /usr/sbin/httpd
                                  -DFOREGROUND
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 a.polya+ 96362 0.0 0.0 22
```

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды .

```
[a.polyakov@a ~]$ ps -eZ | grep httpd
system u:system r:
                      pd t:s0
                                   95236 ?
                                                   00:00:00
system u:system r:
                         t:s0
                                   95237 ?
                                                   00:00:00
system u:system r:
                         t:s0
                                   95238 ?
                                                   00:00:00
'system u:system r:|
                                   95242 ?
                                                   00:00:00
                         t:s0
system u:system r:h
                         t:s0
                                   95243 ?
                                                   00:00:00
```

5. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **Is -IZ /var/www**.

```
[a.polyakov@a ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root_root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 html
```

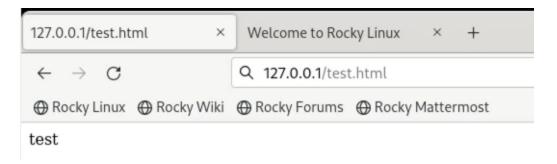
6. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:



7. Проверили контекст созданного файла - httpd\_sys\_content\_t.

```
[a.polyakov@a ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined u:object r:httpd_sys_content_t:s0 33 Oct 12 19:27 test.html
```

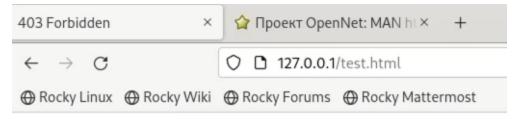
8. Обратитились к файлу через веб-сервер, введя в браузере адрес <a href="http://127.0.0.1/test.html">http://127.0.0.1/test.html</a> и убедились, что файл был успешно отображён.



9. Изменили контекст файла И проверили, что контекст поменялся.

```
[a.polyakov@a ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[a.polyakov@a ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Oct 12 19:27 test.html
```

10. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. В результате получили ошибку.



#### Forbidden

You don't have permission to access this resource.

11. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf находим строчку Listen 80 и заменяем её на Listen 81.

```
46 #Listen 12.34.56.78:80
47 Listen 81
```

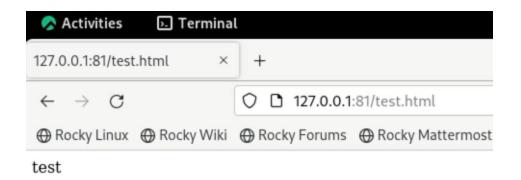
- 12. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
- 13. Выполним команду semanage port -a -t http\_port\_t -p tcp 81. Вылетает ValueError в связи с тем, что порт уже определен. После этого проверим список портов командой semanage port -l | grep http\_port\_t и убедились, что порт 81 появился в списке.

```
[a.polyakov@a ~]$ sudo semanage port -a -p tcp 81 -t http_port_t
ValueError: Port tcp/81 already defined
[a.polyakov@a ~]$ sudo semanage port -l | grep http_port_t
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443
pegasus_http_port_t tcp 5988
```

14. Вернули контекст httpd\_sys\_content\_t к файлу /var/www/html/test.html: chcon - t httpd\_sys\_content\_t /var/www/html/test.html

```
[a.polyakov@a ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.htm
```

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. В результате увидели содержимое файла — слово «test».



15. Исправим обратно конфигурационный файл apache, вернув Listen 80.

```
46 #Listen 12.34.56.78:80
47 Listen 80
```

16. Удалим привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверим, что порт 81 удалён. Данная команда не была выполнена.

```
[a.polyakov@a ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

17. Удалим файл /var/www/html/test.html: rm /var/www/html/test.html.

```
[a.polyakov@a ~]$ sudo rm /var/www/html/test.html
[a.polyakov@a ~]$ ls /var/www/html
[a.polyakov@a ~]$ ls -l /var/www/html
total 0
```

## Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.