

## Лабораторная работа 6

Терентьев Егор Дмитриевич, НФИбд-01-19

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Информационная безопасность

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Терентьев Егор Дмитриевич

Группа: НФИбд-01-19

МОСКВА

2022 г.

# **Прагматика выполнения лабораторной работы**

# Прагматика выполнения лабораторной работы

- ▶ Администрирования ОС Linux:
  1. Работа с SELinux
  2. Работа с веб-сервером Apache

## Цель работы

## Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux 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



1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted

```
[root@edterentjev ~]# getenforce
Enforcing
[root@edterentjev ~]# 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
```

Figure 1: getenforce

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

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

```
[root@edterentjev /]# 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 pr>
   Active: active (running) since Wed 2022-10-12 15:34:11 MSK; 10min ago
     Docs: man:httpd.service(8)
   Main PID: 40253 (httpd)
    Status: "Total requests: 4; Idle/Busy workers 100/0;Requests/sec: 0.00646;>
     Tasks: 213 (limit: 24684)
    Memory: 27.1M
       CPU: 316ms
    CGroup: /system.slice/httpd.service
           └─40253 /usr/sbin/httpd -DFOREGROUND
             └─40254 /usr/sbin/httpd -DFOREGROUND
               └─40259 /usr/sbin/httpd -DFOREGROUND
                 └─40260 /usr/sbin/httpd -DFOREGROUND
                   └─40261 /usr/sbin/httpd -DFOREGROUND

Oct 12 15:34:11 edterentjev.localdomain systemd[1]: Starting The Apache HTTP Se>
Oct 12 15:34:11 edterentjev.localdomain systemd[1]: Started The Apache HTTP Ser>
Oct 12 15:34:11 edterentjev.localdomain httpd[40253]: Server configured, listen>
[root@edterentjev /]#
```

Figure 2: service\_httpd\_status

3. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

3. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```
Target Policy:                selinux
Handle unknown classes:      allow
Classes:                      133
Sensitivities:                1
Types:                        5002
Users:                        8
Booleans:                     347
Allow:                        63996
Auditallow:                   168
Type_trans:                   258486
Type_member:                  35
Role_allow:                   38
Constraints:                  72
MLS Constrain:                72
Permissives:                  0
Defaults:                     7
Allowxperm:                   0
Auditallowxperm:              0
Ibendportcon:                 0
Permissions:                  454
Categories:                   1024
Attributes:                   254
Roles:                        14
Cond. Expr.:                  381
Neverallow:                   0
Dontaudit:                    8417
Type_change:                  87
Range_trans:                  5960
Role_trans:                   420
Validatetrans:                0
MLS Val. Tran:                0
Polcap:                       5
Typebounds:                   0
Neverallowxperm:              0
Dontauditxperm:               0
Ibpkeycon:                    0
```

4. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл

4. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл

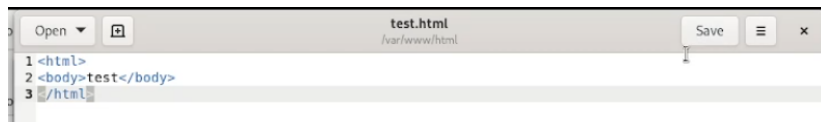


Figure 4: html\_file

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



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

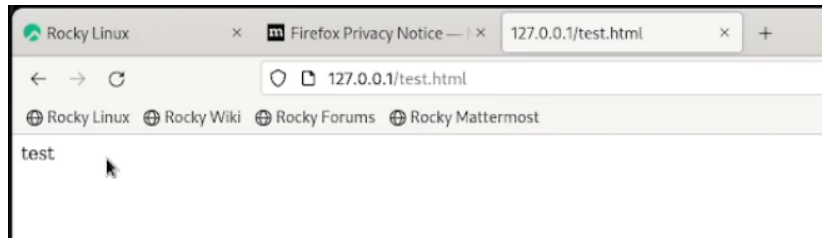
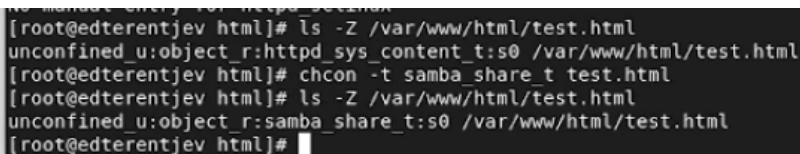


Figure 5: test\_file\_on\_site

6. Проверить контекст файла и измените  
контекст файла

## 6. Проверить контекст файла и измените контекст файла

меняю с httpd\_sys\_content\_t на samba\_share\_t

A terminal window showing the process of changing the SELinux context of a file. The user is root at a machine named edterentjev. They first run 'ls -Z /var/www/html/test.html' and see the context 'unconfined\_u:object\_r:httpd\_sys\_content\_t:s0'. Then they run 'chcon -t samba\_share\_t test.html'. Finally, they run 'ls -Z /var/www/html/test.html' again and see the context 'unconfined\_u:object\_r:samba\_share\_t:s0'.

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

Figure 6: samba\_share\_t

7. Попробуйте ещё раз получить доступ к файлу через веб-сервер.

7. Попробуйте ещё раз получить доступ к файлу через веб-сервер.

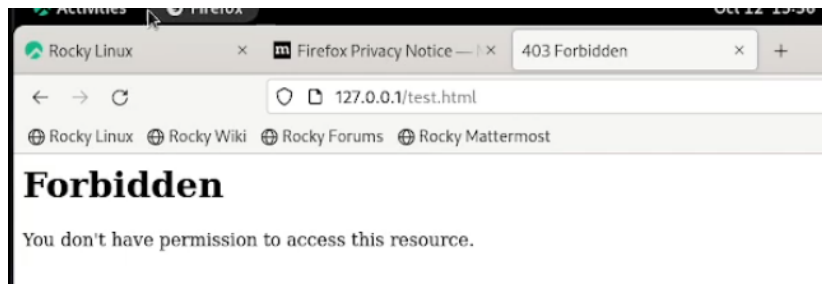


Figure 7: error

8. Попробуйте запустить веб-сервер  
Apache на прослушивание TCP-порта 81 и  
делаем привязку

## 8. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 и делаем привязку

```
[edterentjev@edterentjev ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[edterentjev@edterentjev ~]$ semanage port -l | grep http_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
[edterentjev@edterentjev ~]$ 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
[edterentjev@edterentjev ~]$
```

Figure 8: semanage\_port

9. Удалите привязку `http_port_t` к 81 порту и проверьте, что порт 81 удалён. (Удалить привязку невозможно)



9. Удалите привязку `http_port_t` к 81 порту и проверьте, что порт 81 удалён. (Удалить привязку невозможно)

```
[edterentjev@edterentjev conf]$ sudo semanage port -d -t http_port_t -p tcp 81
/valueError: Port tcp/81 is defined in policy, cannot be deleted
[edterentjev@edterentjev conf]$ sudo semanage port -a -p tcp 81 -t http_port_t
/valueError: Port tcp/81 already defined
[edterentjev@edterentjev conf]$ sudo semanage port -d -p tcp 81 -t http_port_t
/valueError: Port tcp/81 is defined in policy, cannot be deleted
[edterentjev@edterentjev conf]$ rm /var/www/html/test.html
rm: remove write-protected regular file '/var/www/html/test.html'? y
rm: cannot remove '/var/www/html/test.html': Permission denied
[edterentjev@edterentjev conf]$
```

Figure 9: `semanage_rm`

## Выводы

## Выводы

В результате выполнения работы я развитл навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux, а также проверил работу SELinx на практике совместно с веб-сервером Apache.

