Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Асеинова Елизавета

2022 Oct 4th

Содержание

Список таблиц

Список иллюстраций

1. Цель работы

Целью данной работы является развитие навыки администрирования ОС Linux, получение первого практического знакомства с технологией SELinux1, проверка работы SELinx на практике совместно с веб-сервером Apache.[1]

2. Выполнение лабораторной работы

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

```
[root@evaseinova evaseinova]# getenforce
Enforcing
[root@evaseinova evaseinova]# 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
```

Рис. 2.1.: Вход в систему

2. Обратилась с помощью браузера к веб-серверу, и убедилась, что он работает. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. Посмотрела текущее состояние переключателей SELinux для Apache.

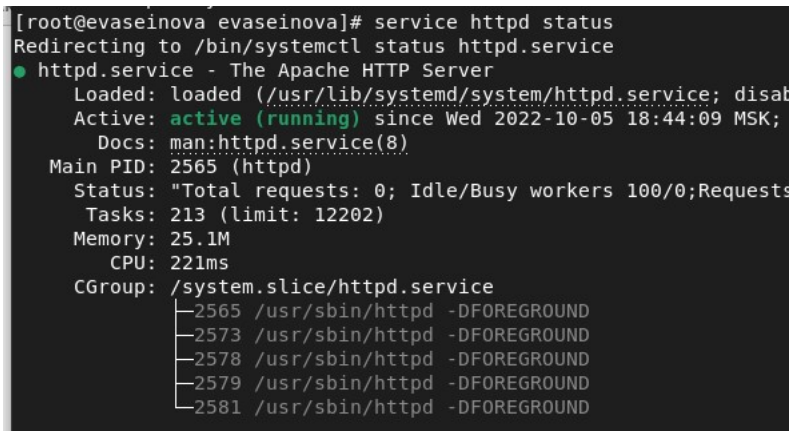

Рис. 2.2.: Обращение к серверу

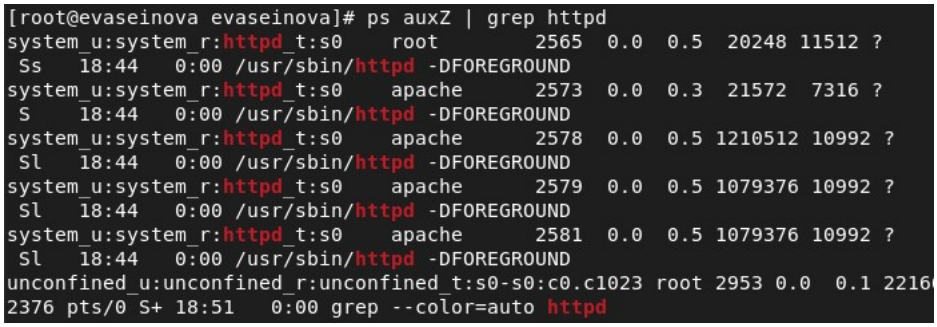

Рис. 2.3.: Apache в списке процессов

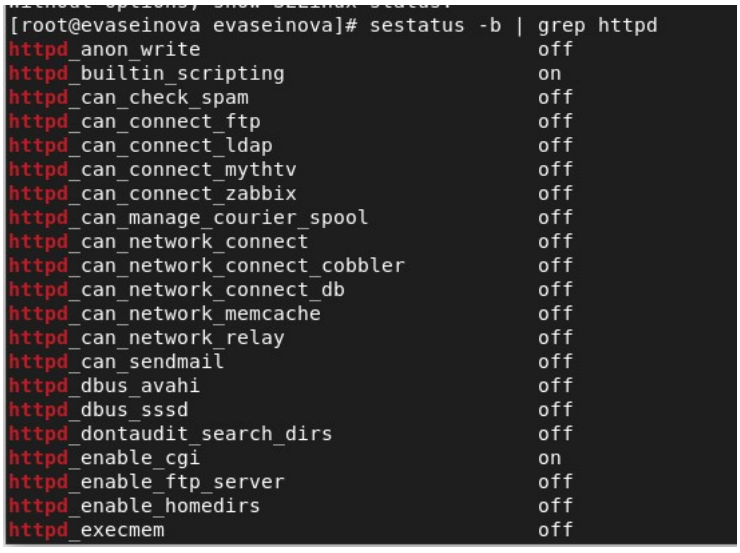

Рис. 2.4.: Переключатели

3. Посмотрела статистику по политике, также определила множество пользователей - 8, ролей - 14, типов - 4995.

```
[root@evaseinova evaseinova]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             133    Permissions:         454
  Sensitivities:         1    Categories:         1024
  Types:              4995    Attributes:          254
  Users:                 8    Roles:                14
  Booleans:            347    Cond. Expr.:         382
  Allow:             63727    Neverallow:            0
  Auditallow:          163    Dontaudit:          8391
  Type_trans:       251060    Type_change:          87
  Type_member:          35    Range_trans:        5958
  Role allow:           38    Role_trans:          418
  Constraints:          72    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           0    Polcap:                5
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               33
  Genfscon:            106    Portcon:             651
```

Рис. 2.5.: Статистика

4. Определила тип файлов и поддиректорий, находящихся в директории /var/www. Определила тип файлов, находящихся в директории /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[root@evaseinova evaseinova]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0
:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0
:10 html
[root@evaseinova evaseinova]# ls -lZ /var/www/html
total 0
```

Рис. 2.6.: Тип файлов

5. Создала от имени суперпользователя html-файл. Проверила контекст созданного файла. Обратилась к файлу через веб-сервер. Убедилась, что файл был успешно отображён.

```
[root@evaseinova evaseinova]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

Рис. 2.7.: Html файл

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

Рис. 2.8.: Контекст

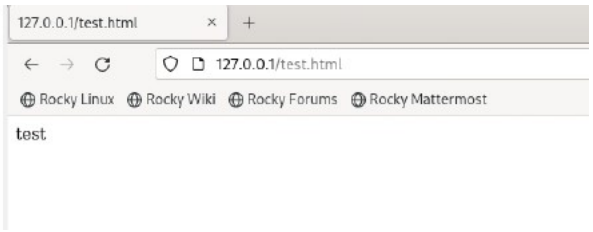

Рис. 2.9.: Отображение в браузере

6. Изменила контекст файла /var/www/html/test.html на samba_share_t.

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

Рис. 2.10.: Изменение контекста

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

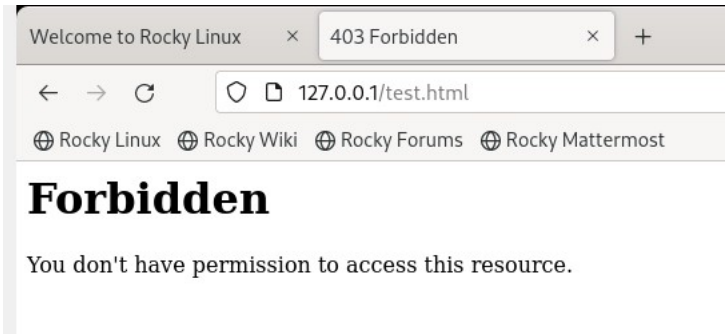

Рис. 2.11.: Отказ в доступе

8. Просмотрела log-файлы веб-сервера Apache и системный лог-файл.

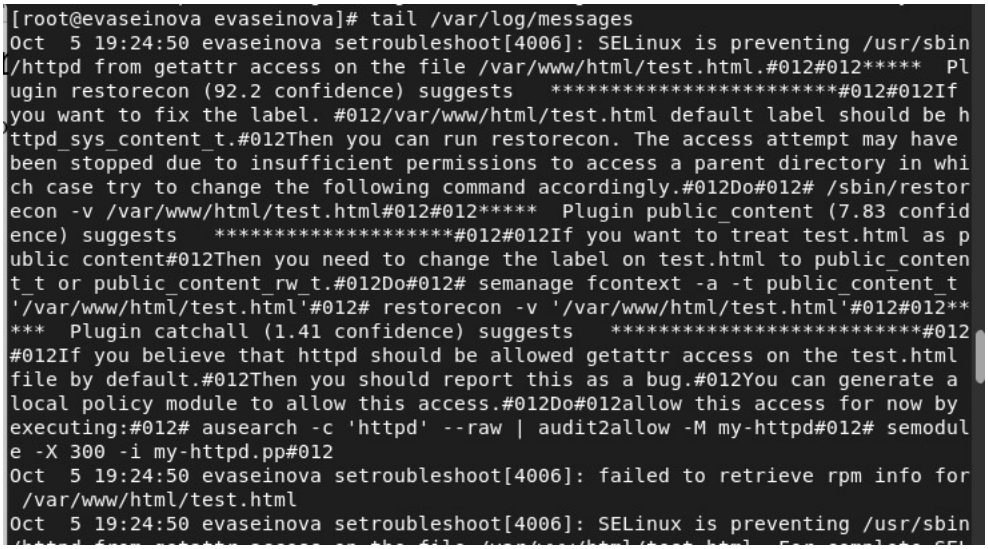

Рис. 2.12.: Лог-файлы

9. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Выполнила перезапуск веб-сервера Apache.

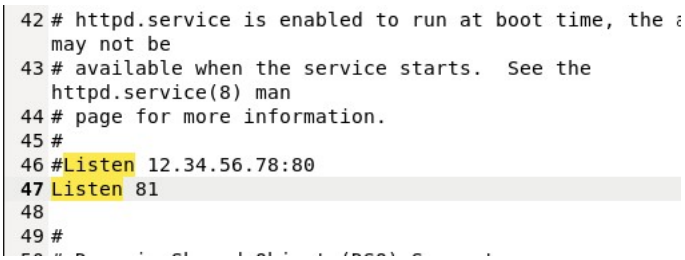

Рис. 2.13.: Изменение порта

10. Просмотрела log-файлы веб-сервера Apache.

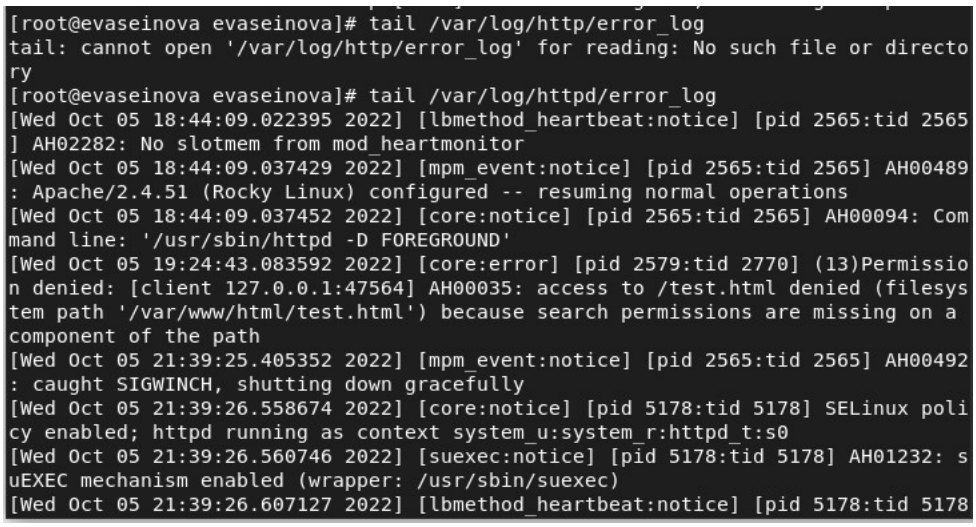

Рис. 2.14.: Лог файлы

11. Выполнила команду semanage port -a -t http_port_t -p tcp 81. Попробовала запустить веб-сервер Apache ещё раз.

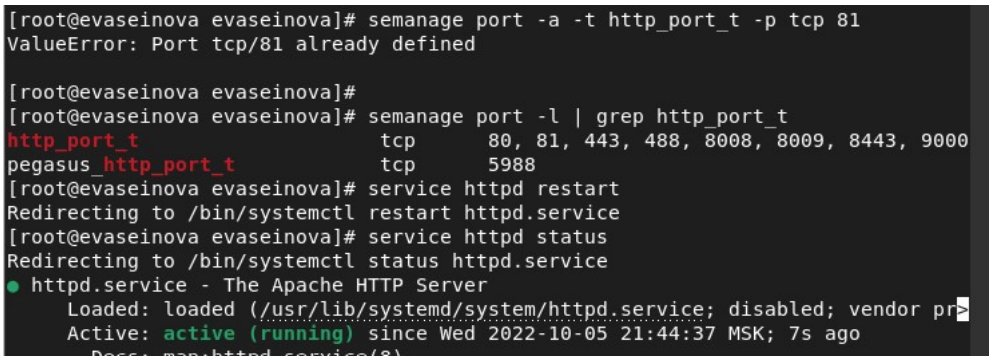

Рис. 2.15.: Подключение порта

12. Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html и открыла его в браузере.

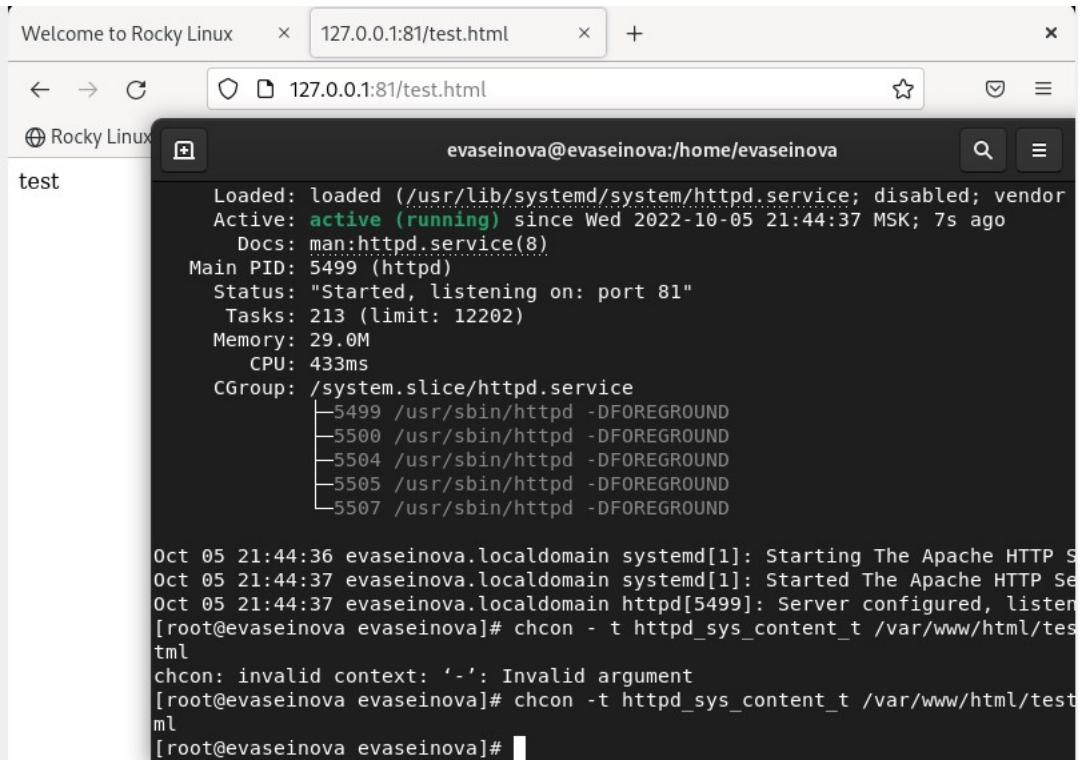

Рис. 2.16.: Возвращение параметров

13. Исправила обратно конфигурационный файл apache, удалила привязку http_port_t к 81 порту, удалила файл /var/www/html/test.html.

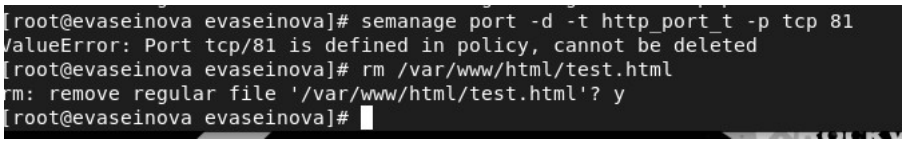

Рис. 2.17.: Удаление файла

3. Выводы

В ходе работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux1, проверили работу SELinx на практике совместно с веб-сервером Apache.

4. Список литературы

1. Методические материалы курса