Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Артамонов Тимофей Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Теоретическое введение

В SELinux права доступа определяются самой системой при помощи специально определённых политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux: через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила SELinux «прозрачны» для приложений, и не требуется никакой их модификации. В состав некоторых дистрибутивов входят готовые политики, в которых права могут определяться на основе совпадения типов процесса (субъекта) и файла (объекта) — это основной механизм SELinux. Две других формы контроля доступа — доступ на основе ролей и на основе многоуровневой системы безопасности. [1]

3 Выполнение лабораторной работы

Убедимся, что SELinux работает в режиме enforcing политики targeted. (рис. 3.1)

```
[teartamonov@teartamonov conf]$ getenforce
Enforcing
[teartamonov@teartamonov conf]$ 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
[teartamonov@teartamonov conf]$
```

Рис. 3.1: Все верно

Обратимся к веб-серверу и убедимся, что он работает. (рис. 3.2)

```
[teartamonov@teartamonov conf]$ 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: di>
     Active: active (running) since Sun 2024-09-0[ 12:16:01 MSK; 16min ago
       Docs: man:httpd.service(8)
   Main PID: 41566 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
      Tasks: 177 (limit: 12190)
     Memory: 38.4M
        CPU: 4.044s
     CGroup: /system.slice/httpd.service
             ├─41566 /usr/sbin/httpd -DFOREGROUND
             ├─41567 /usr/sbin/httpd -DFOREGROUND
             ├─41568 /usr/sbin/httpd -DFOREGROUND
             ├─41569 /usr/sbin/httpd -DFOREGROUND
             └─41570 /usr/sbin/httpd -DFOREGROUND

сен 08 12:15:41 teartamonov systemd[1]: Starting The Apache HTTP Server...
сен 08 12:15:51 teartamonov httpd[41566]: AH00558: httpd: Could not reliably de>
сен 08 12:16:01 teartamonov httpd[41566]: Server configured, listening on: port>
сен 08 12:16:01 teartamonov systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

Рис. 3.2: Веб-сервер работает

Найдем apache в списке процессов. (рис. 3.3)

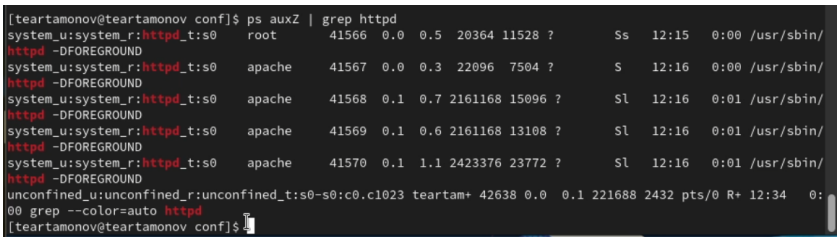

Рис. 3.3: Нашли с помощью команды ps auxZ | grep httpd

Посмотрим статистику по политике. (рис. 3.4)

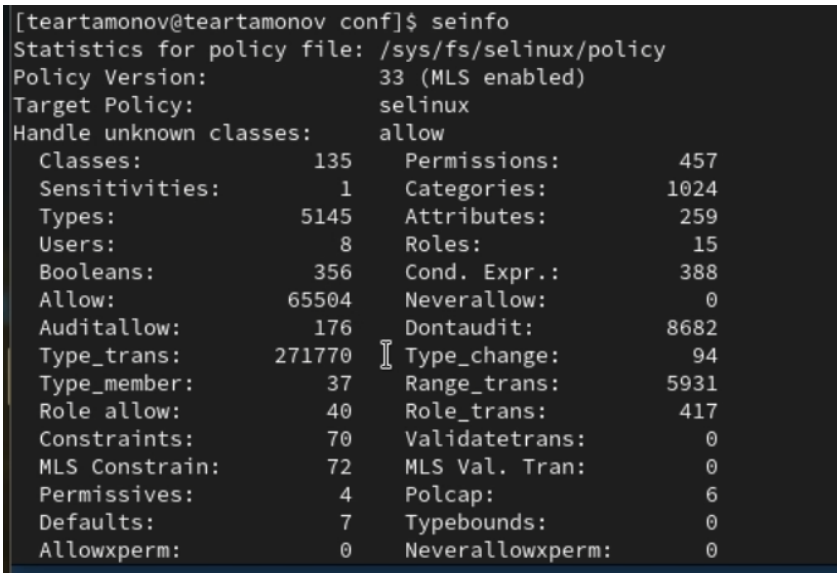

Рис. 3.4: Видно количество разных сущностей, например, пользователей

Определим тип файлов и директорий в /var/www. (рис. 3.5)

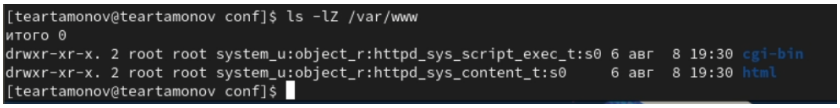

Рис. 3.5: httpd_sys_script_exec_t и httpd_sys_content_t

Посмотрим список пользователей. (рис. 3.6)

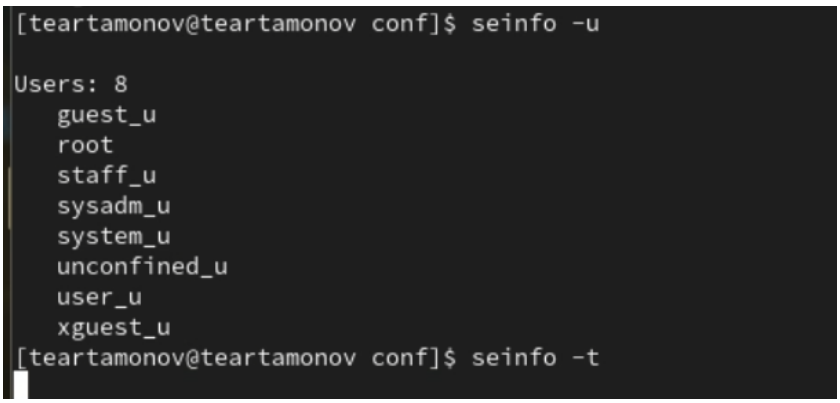

Рис. 3.6: Список пользователей

Создадим от имени root файл в /var/www/html. (рис. 3.7)

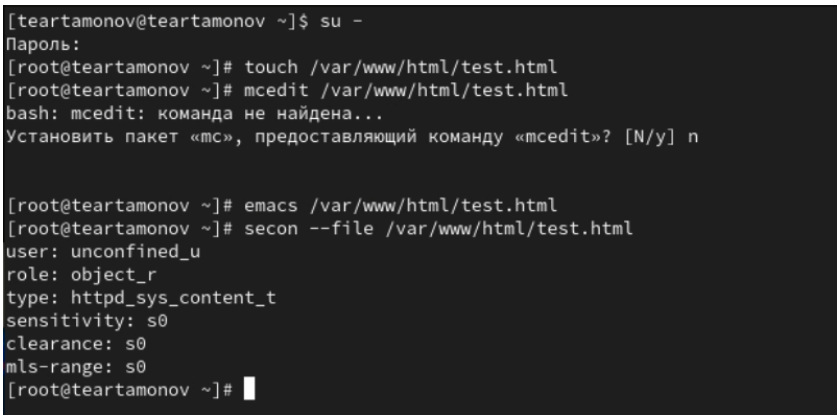

Рис. 3.7: Успешно

Попробуем посмотреть файл в браузере. (рис. 3.8)

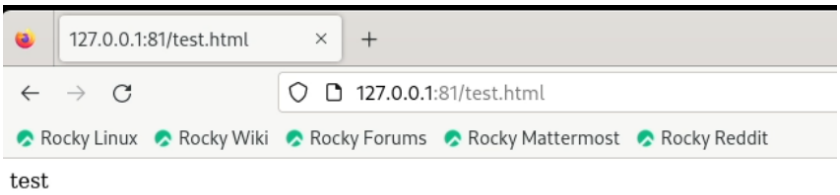

Рис. 3.8: Успешно

Изменим контекст файла. (рис. 3.9)

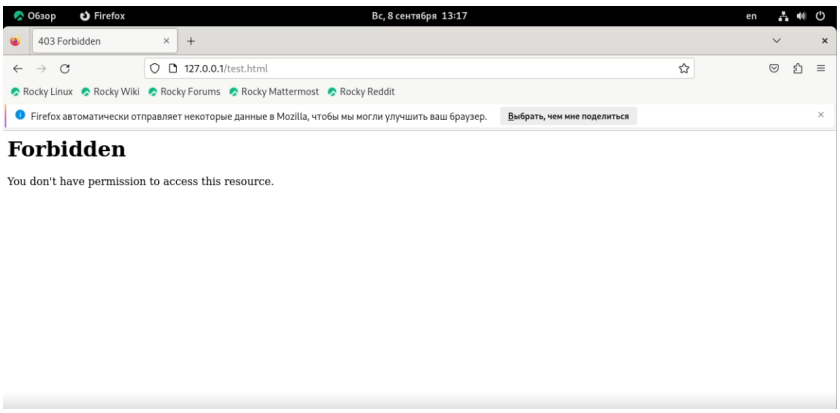

Рис. 3.9: Успешно, теперь файл не отображается

Добавим на прослушивание порт 81. (рис. 3.10)

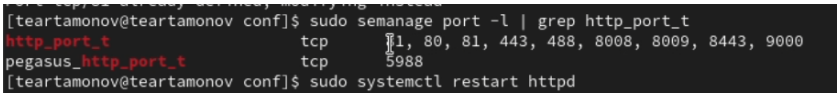

Рис. 3.10: Успешно, теперь происходит сбой, если не добовать 81 порт в список

Вернем все как было. (рис. 3.11)

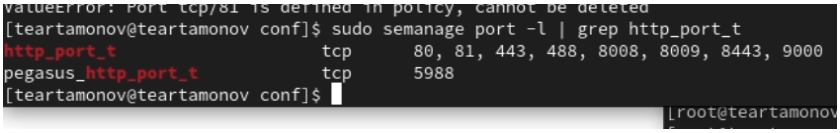

Рис. 3.11: Успешно

4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. SELinux [Электронный ресурс]. Wikimedia Foundation, 2024. URL: https://ru.wikipedia.org/wiki/SELinux.