Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Тимур Дмитриевич Калинин

Содержание

List of Figures

List of Tables

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 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 (Рис. 2.1)

Figure 2.1: Статус selinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (Рис. 2.2). Если не работает, запустите его так же, но с параметром start (Рис. 2.3)

Figure 2.2: Статус веб-сервера

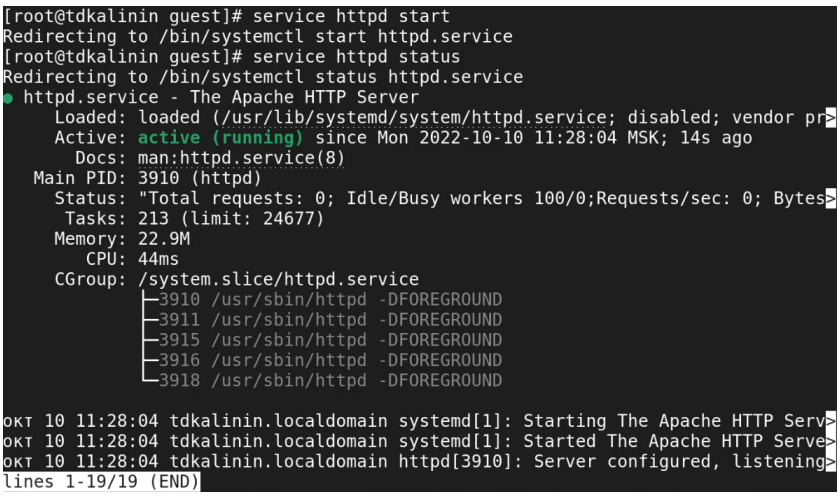

Figure 2.3: Запуск веб-сервера

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (Рис. 2.4).

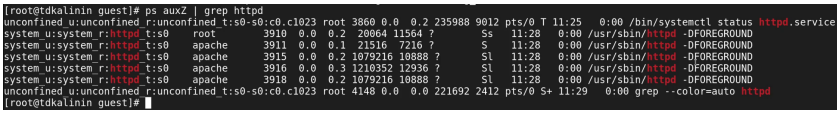

Figure 2.4: Контекст службы Apache

4. Посмотрите текущее состояние переключателей SELinux для Apache. Обратите внимание, что многие из них находятся в положении «off» (Рис. 2.5).

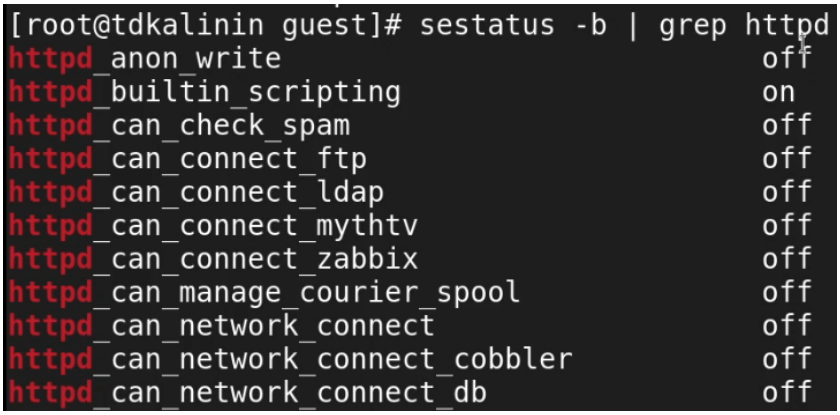

Figure 2.5: Состояние переключателей SELinux для Apache

5. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (Рис. 2.6).

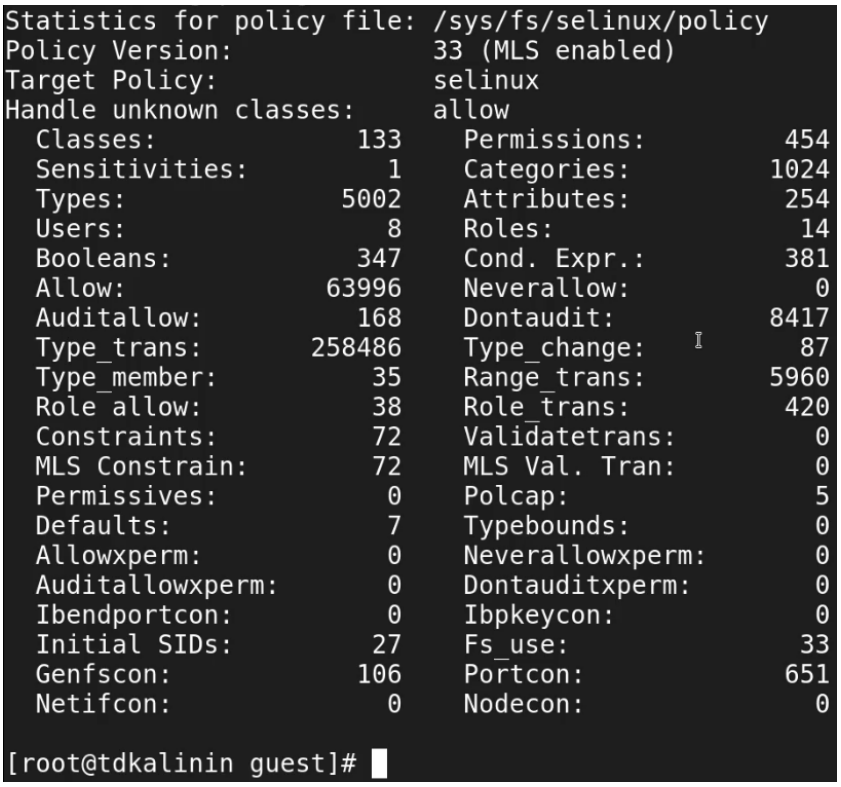

Figure 2.6: Статистика по политике

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www (Рис. 2.7):

Figure 2.7: Тип файлов и директорий в /var/www

7. Определите тип файлов, находящихся в директории /var/www/html (Рис. 2.8):

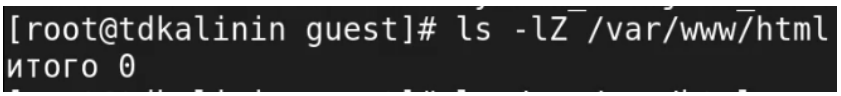

Figure 2.8: Тип файлов в /var/www/html

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Как видим, создание файлов разрешено только владельцу каталога.

9. 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 (Рис. 2.9):

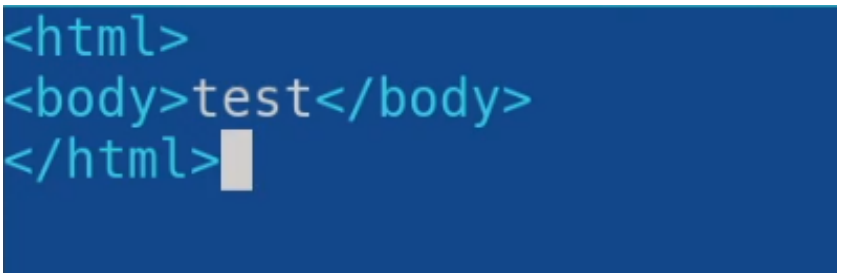

Figure 2.9: Содержание test.html

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (Рис. 2.10).

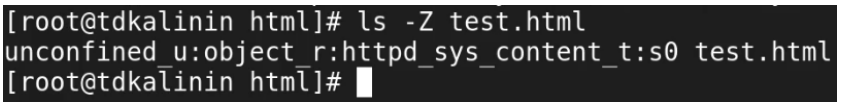

Figure 2.10: Контекст test.html

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён (Рис. 2.11).

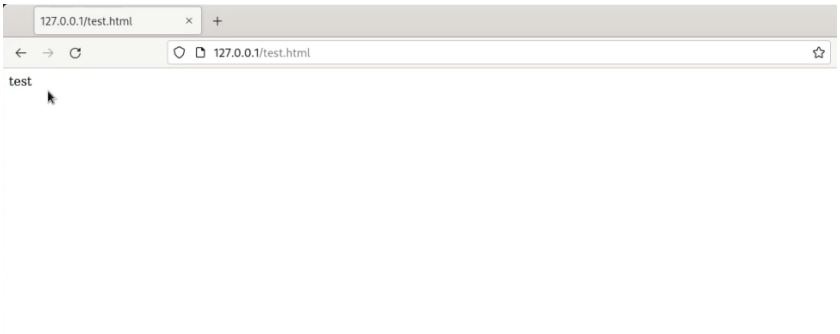

Figure 2.11: Обращение к файлу через веб-сервер

12. Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd (Рис. 2.12). Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z (Рис. 2.13).

Figure 2.12: Обращение к файлу через веб-сервер

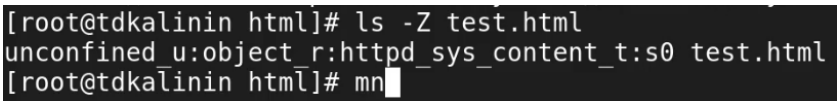

Figure 2.13: Контекст файла

13. 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. После этого проверьте, что контекст поменялся (Рис. 2.14).

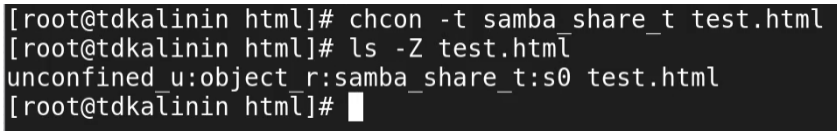

Figure 2.14: Изменение контекста

14. 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 (Рис. 2.15):

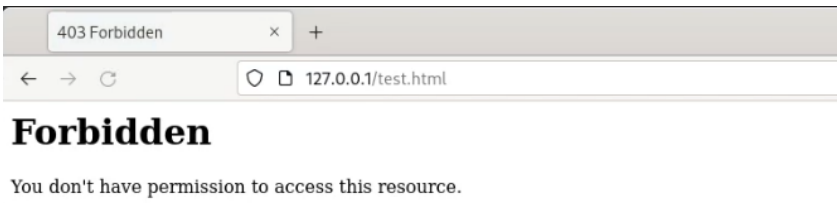

Figure 2.15: Проверка доступа через веб-сервер

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Потому что у процесса, который пытается запросить доступ к файлу, нет к нему доступа из-за метки.

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл (Рис. 2.16):

```
Oct 10 12:19:03 tdkalinin setroubleshoot[5573]: SELinux запрещает /usr/s
bin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения
всех сообщений SELinux: sealert -l d584e6c0-90fd-41af-9e8c-9402f50ee1d6
```

Figure 2.16: Системный лог-файл

Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно (Рис. 2.17).

```
type=AVC msg=audit(1665393541.398:219): avc:  denied  { getattr } for  p
id=3918 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=68945
126 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r
:samba_share_t:s0 tclass=file permissive=0
```

Figure 2.17: Файл /var/log/audit/audit.log

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 100 (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 100 (Рис. 2.18).

Figure 2.18: Прослушивание 100 порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой произошел из-за того, что у процесса нет доступа к 100 порту протокола TCP, так как он ограничивается selinux (Рис. 2.19).

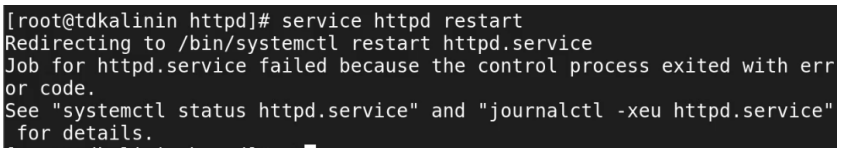

Figure 2.19: Сбой перезапуска

18. Проанализируйте лог-файлы (Рис. 2.20):

Figure 2.20: Содержимое системного лог-файла

Просмотрите файлы /var/log/http/error_log (Рис. 2.21), /var/log/http/access_log (Рис. 2.22) и /var/log/audit/audit.log (Рис. 2.23) и выясните, в каких файлах появились записи.

Figure 2.21: Содержимое /var/log/http/error_log

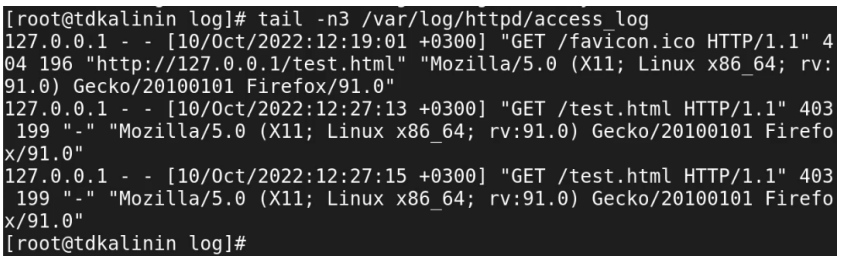

Figure 2.22: Содержимое /var/log/http/access_log

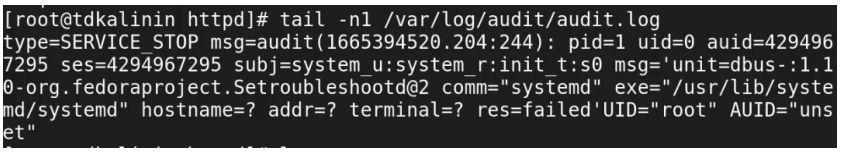

Figure 2.23: Содержимое /var/log/audit/audit.log

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов (Рис. 2.24)

Figure 2.24: Добавление порта 100 для httpd

Убедитесь, что порт 100 появился в списке.

20. Попробуйте запустить веб-сервер Apache ещё раз (Рис. 2.25). Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? Потому что в этот раз у процесса веб-сервера был доступ к порту 100.

Figure 2.25: Перезапуск Apache

21. Верните контекст httpd_sys_content__t к файлу /var/www/html/ test.html (Рис. 2.26):

```
[root@tdkalinin log]# chcon -t httpd_sys_content_t /var/www/html/test.ht
ml
[root@tdkalinin log]#
```

Figure 2.26: Возвращение контекста

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test» (Рис. 2.27).

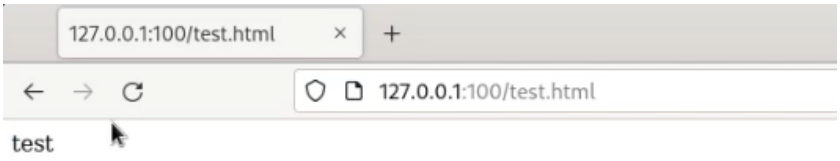

Figure 2.27: Доступ через браузер

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80 (Рис. 2.28).

```
#Listen 12.34.56.78:80
Listen 80
```

Figure 2.28: Исправление конфигурационного файла

23. Удалите привязку http_port_t к 100 порту и проверьте, что порт 100 удалён (Рис. 2.29).

```
[root@tdkalinin conf]# semanage port -d -t http_port_t -p tcp 100

[root@tdkalinin log]#
```

Figure 2.29: Удаление 100 порта

24. Удалите файл /var/www/html/test.html (Рис. 2.30):

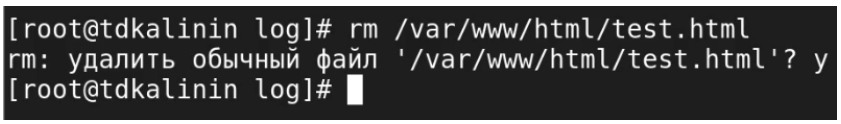

Figure 2.30: Удаление test.html

3 Выводы

Мы развили навыки администрирования ОС Linux и получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

4 Библиография

1. Лабораторная работа №6. - 5 с. URL: https://esystem.rudn.ru/pluginfile.php/1651891/mod_resource/content/2/006-lab_selinux.pdf