Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Бармина Ольга Константиновна

2022 Sep 22th

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@localhost okbarmina]# getenforce
Enforcing
[root@localhost okbarmina]# 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
[root@localhost okbarmina]#
```

Рис. 2.1.: рис 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.

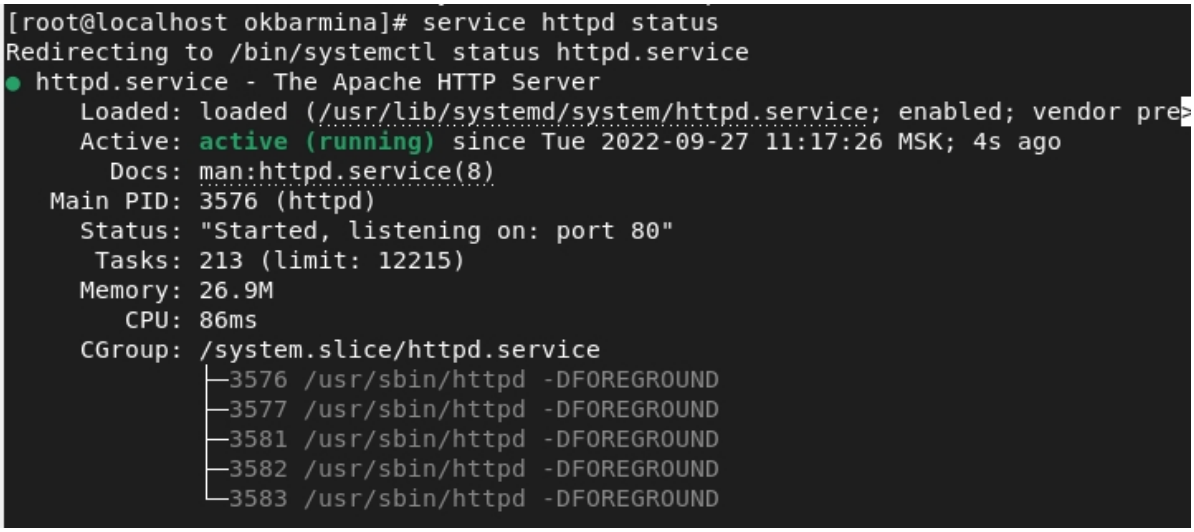

Рис. 2.2.: рис 2. обращение к серверу

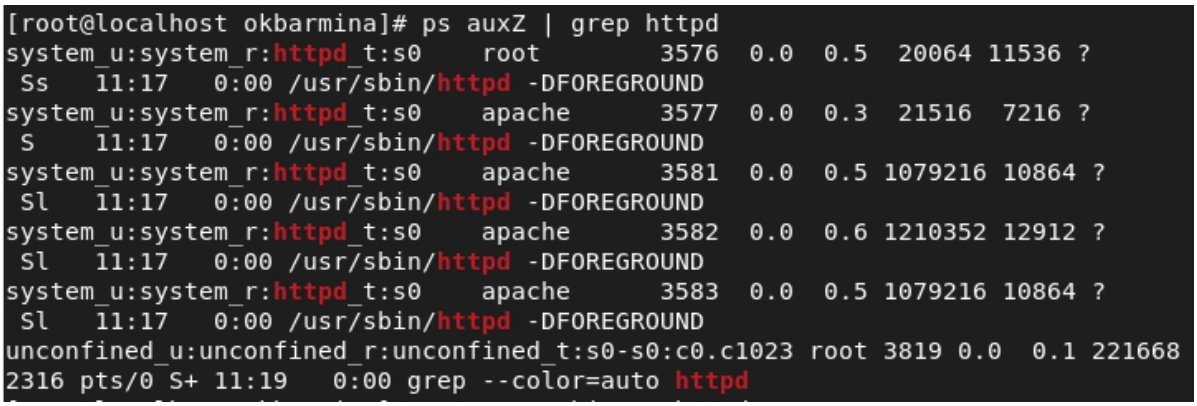

Рис. 2.3.: рис 3. состояние переключателей

3. Посмотрела статистику по политике, также определила множество пользователей, ролей, типов.

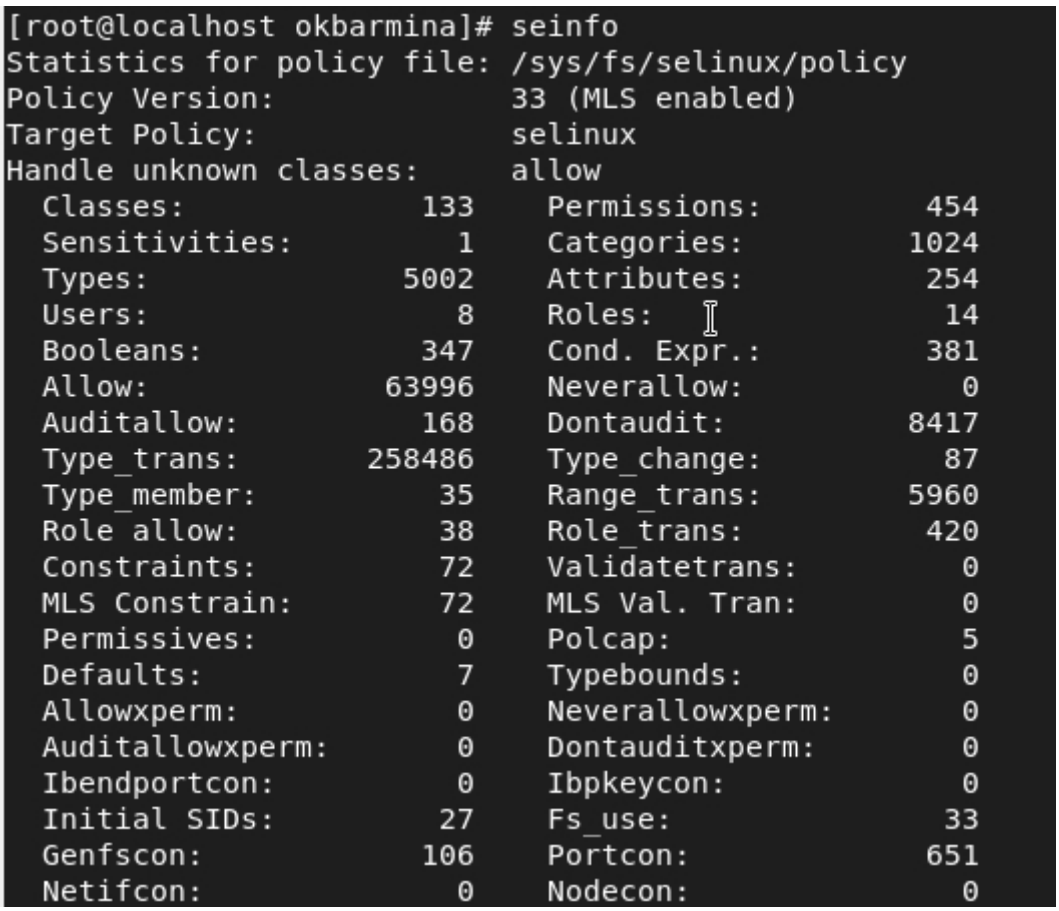

Рис. 2.4.: рис 4. статистика

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.

Рис. 2.5.: рис 5. 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.

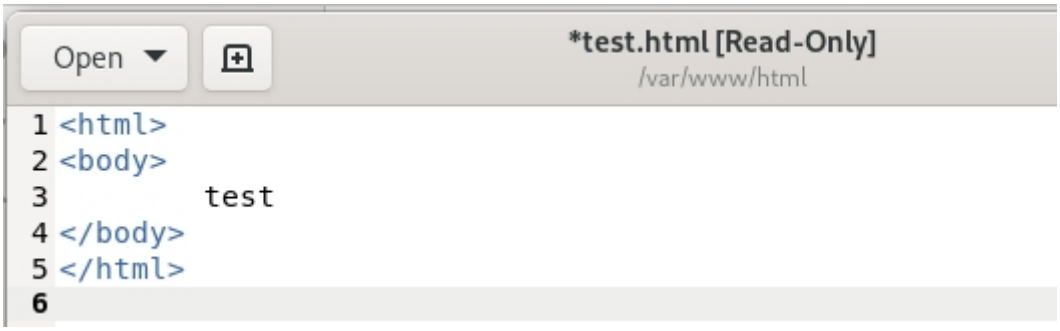

Рис. 2.6.: рис 6. html файл

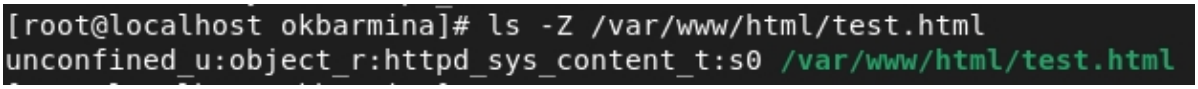

Рис. 2.7.: рис 7. контекст

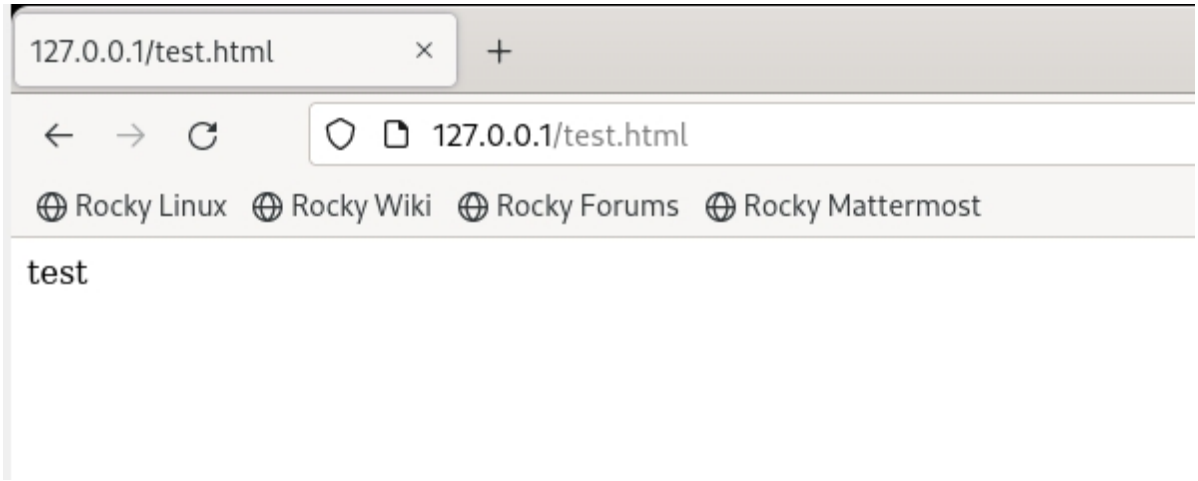

Рис. 2.8.: рис 8. отображение в браузере

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

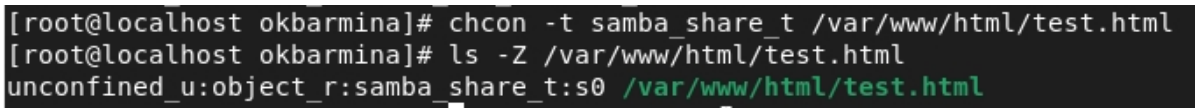

Рис. 2.9.: рис 9. изменение контекста

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

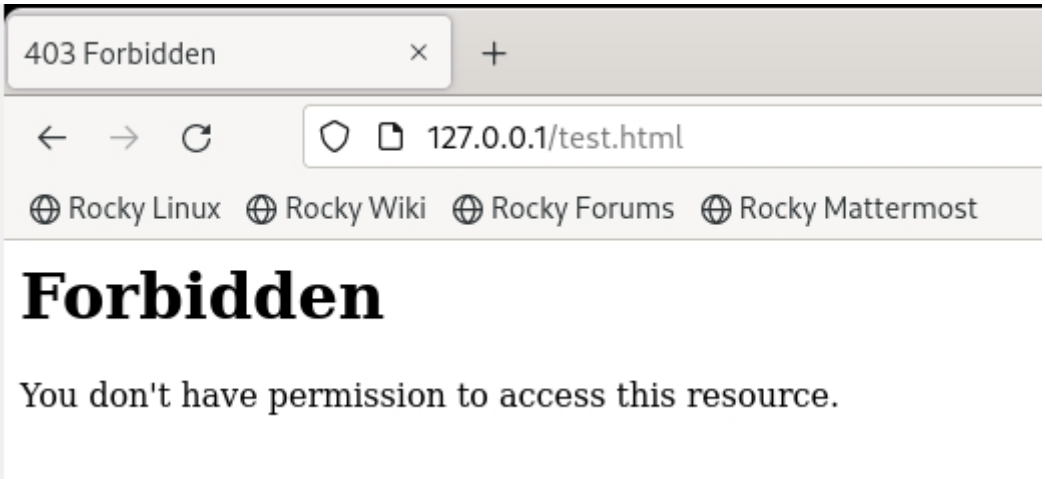

Рис. 2.10.: рис 10. отказ в доступе

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

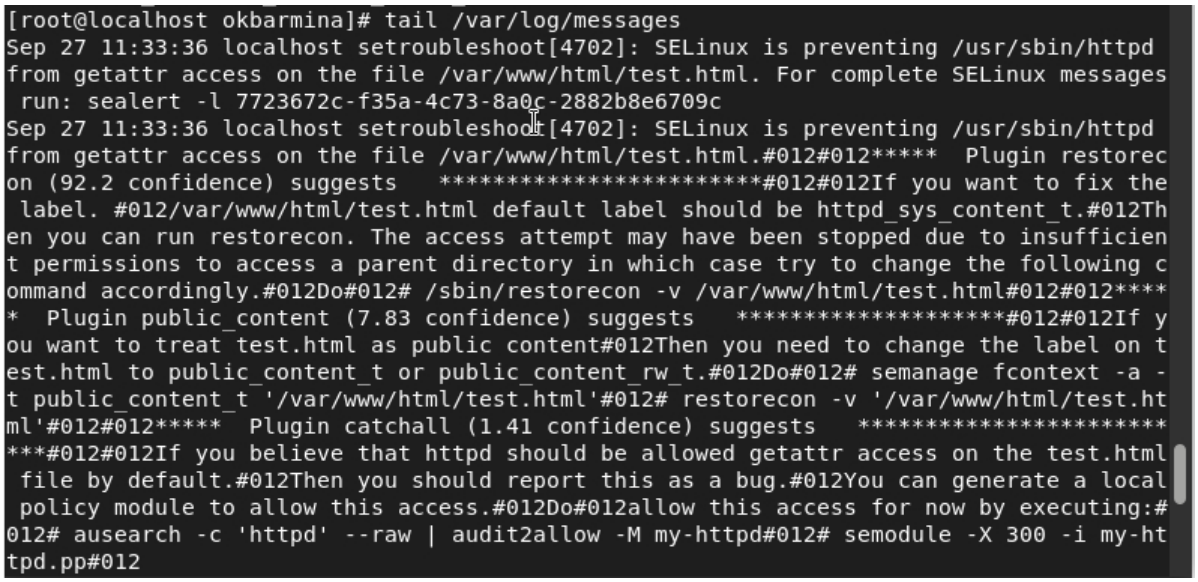

Рис. 2.11.: рис 11. лог-файлы

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

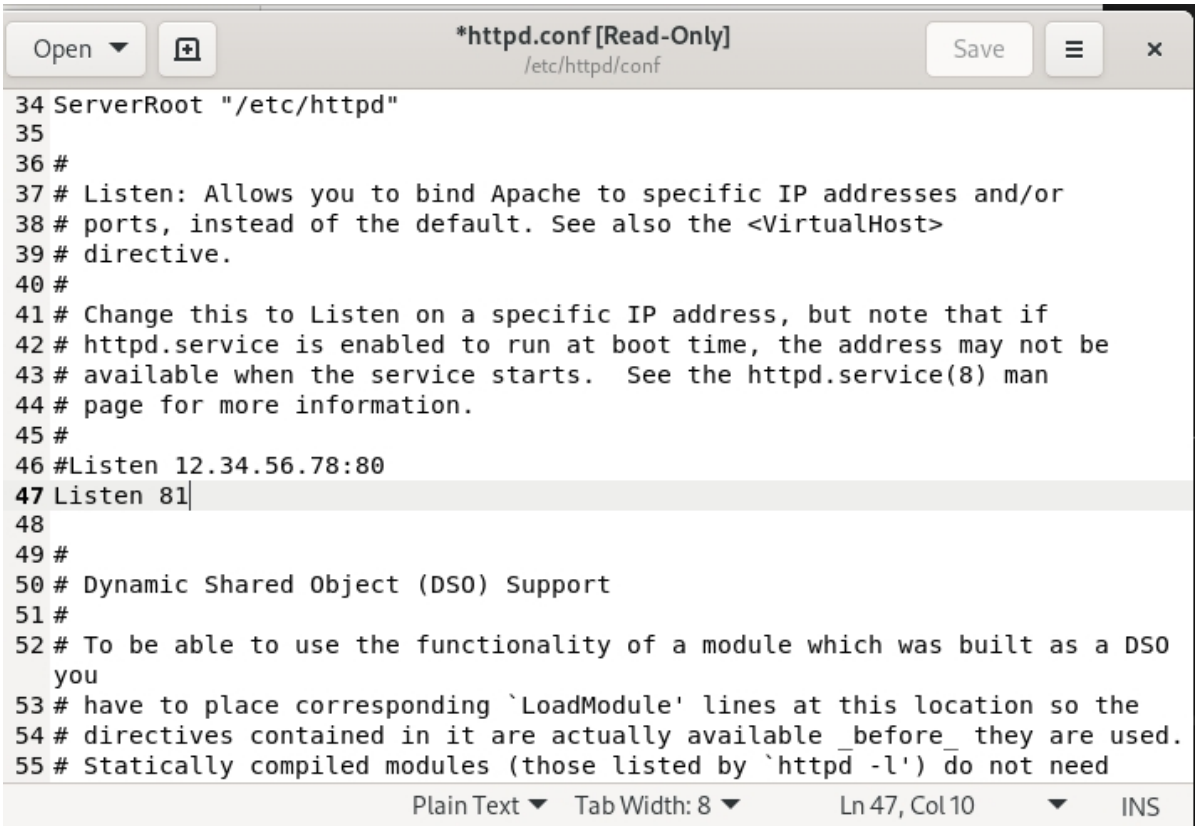

Рис. 2.12.: рис 12. изменение порта

10. Просмотрела log-файлы веб-сервера Apache.

```
[root@localhost okbarmina]# tail /var/log/http/error_log
tail: cannot open '/var/log/http/error_log' for reading: No such file or directory
[root@localhost okbarmina]# tail /var/log/http/access_log
tail: cannot open '/var/log/http/access_log' for reading: No such file or directory
[root@localhost okbarmina]# tail /var/log/audit/audit.log
type=AVC msg=audit(1664267877.485:245): avc:  denied  { getattr } for  pid=3582 comm="
httpd" path="/var/www/html/test.html" dev="dm-0" ino=101151653 scontext=system_u:syste
m_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=
0
type=SYSCALL msg=audit(1664267877.485:245): arch=c000003e syscall=262 success=no exit=
-13 a0=ffffff9c a1=7fafd0043a30 a2=7fafca7f3830 a3=0 items=0 ppid=3576 pid=3582 auid=4
294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) s
es=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key
=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apa
che" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1664267877.485:245): proctitle=2F7573722F7362696E2F6874747064
002D44464F524547524F554E44
type=AVC msg=audit(1664267877.486:246): avc:  denied  { getattr } for  pid=3582 comm="
httpd" path="/var/www/html/test.html" dev="dm-0" ino=101151653 scontext=system_u:syste
m_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=
0
```

Рис. 2.13.: рис 13. лог файлы

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

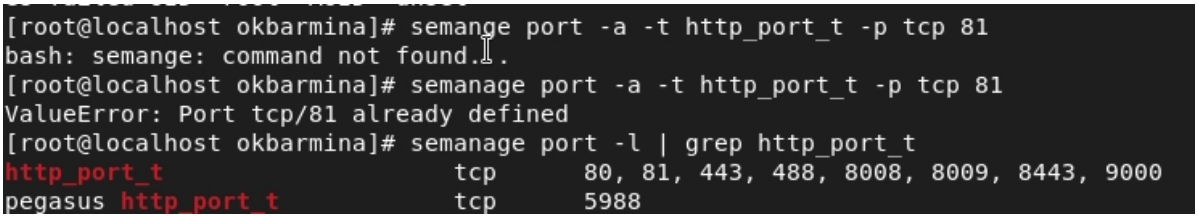

Рис. 2.14.: рис 14. подключение порта

12. Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html. Исправила обратно конфигурационный файл apache, удалила привязку http_port_t к 81 порту, удалила файл /var/www/html/test.html.

Рис. 2.15.: рис 15. возвращение параметров

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