Отчет по лабораторной работе №6

по дисциплине: Информационная безопасность

Ким Михаил Алексеевич

Содержание

Список иллюстраций

1 Цель работы

Развитие навыков администрирования ОС Linux. Получение первого практического знакомства с технологией SELinux. Проверка работы SELinx на практике совместно с веб-сервером Apache.

2 Задание

1. Произвести эксперименты с дополнительными атрибутами прав доступа.

3 Теоретическое введение

- Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями [1].
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами [2].
- В UNIX-системах, кроме стандартных прав доступа, существуют также дополнительные или специальные атрибуты файлов, которые поддерживает файловая система [3].
- SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра [4].
- Apache («Апачи», Apache HTTP Server) — это открытое кросс-платформенное программное обеспечение для размещения и поддержки веб-сервера [5].

4 Выполнение лабораторной работы

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 4.1).

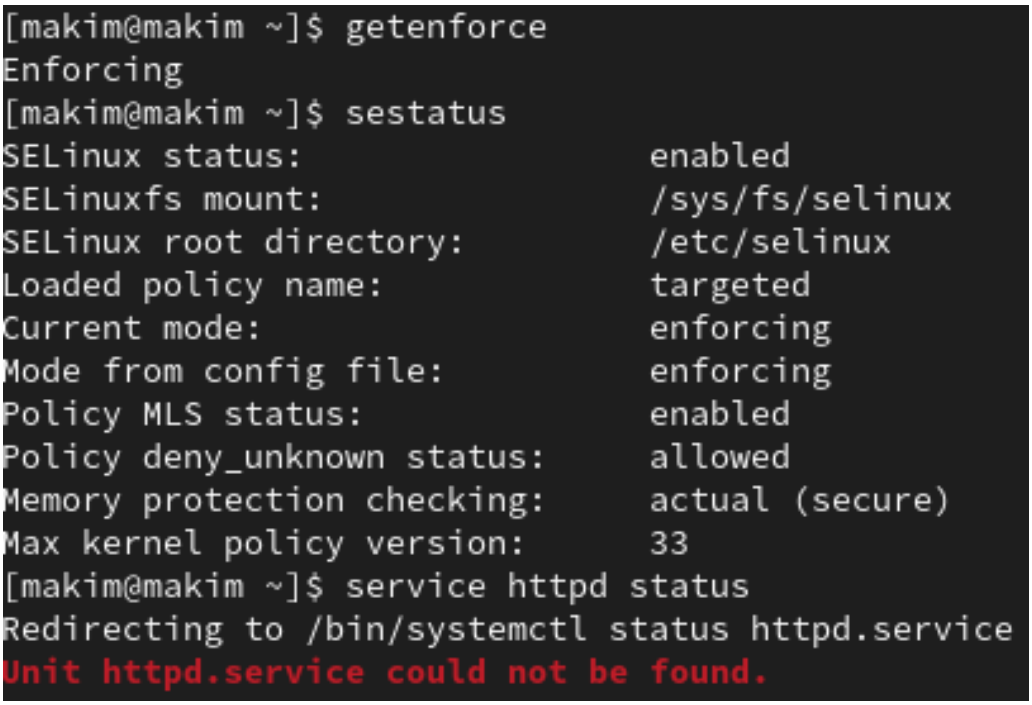

Рис. 4.1: Проверка getenforce и sestatus

2. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает: `service httpd status`. Предварительно установим пакет: `sudo yum install httpd`. Если не работает, запустим его так же, но с параметром `start`. (рис. 4.2, 4.3).

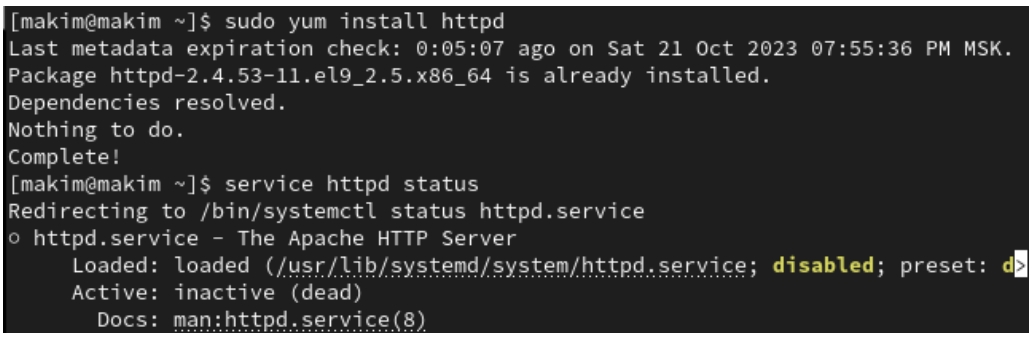

Рис. 4.2: Установка и проверка статуса httpd

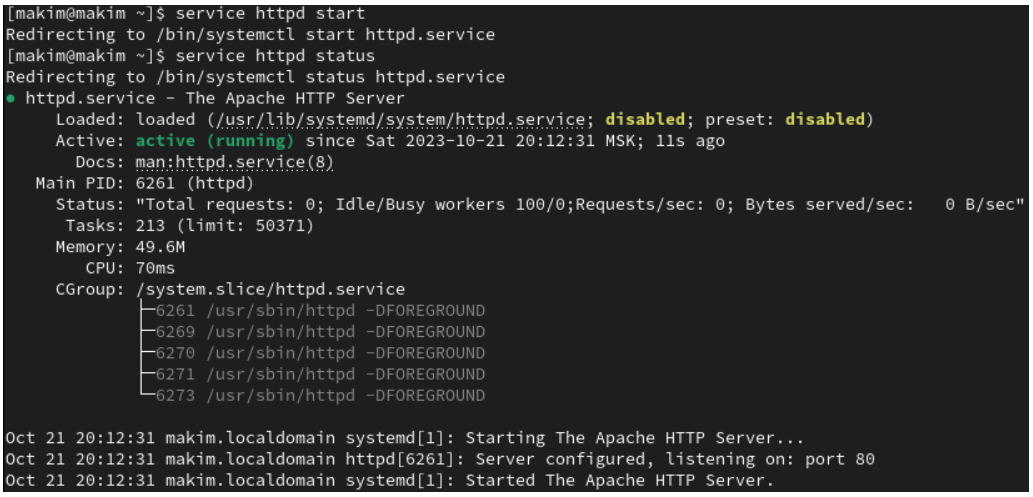

Рис. 4.3: Запуск httpd

3. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности и занесем эту информацию в отчёт. Например, можно использовать команды: `ps auxZ | grep httpd`, `ps -eZ | grep httpd` (рис. 4.4).

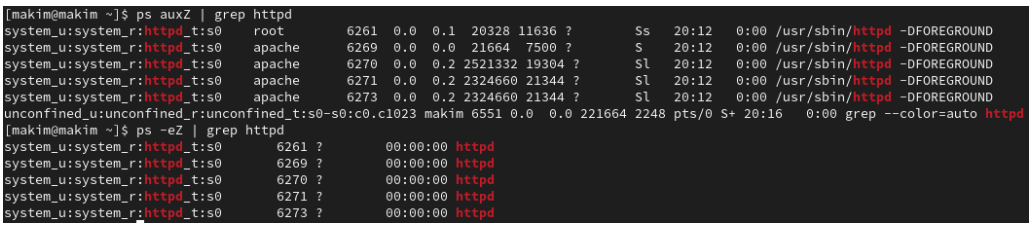

Рис. 4.4: Контекст безопасности httpd

4. Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис. 4.5).

```
[makim@makim ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                             off
abrt_handle_event                           off
abrt_upload_watch_anon_write                on
antivirus_can_scan_system                   off
antivirus_use_jit                           off
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
awstats_purge_apache_log_files              off
boinc_execmem                               on
cdrecord_read_content                       off
cluster_can_network_connect                 off
cluster_manage_all_files                    off
cluster_use_execmem                         off
cobbler_anon_write                          off
cobbler_can_network_connect                 off
cobbler_use_cifs                            off
cobbler_use_nfs                             off
collectd_tcp_network_connect                off
colord_use_nfs                              off
condor_tcp_network_connect                  off
conman_can_network                          off
conman_use_nfs                              off
container_connect_any                       off
container_manage_cgroup                     off
container_use_cephfs                        off
container_use_devices                       off
container_use_ecryptfs                      off
cron_can_relabel                            off
cron_system_cronjob_use_shares              off
cron_userdomain_transition                  on
cups_execmem                                off
cvs_read_shadow                             off
daemons_dontaudit_scheduling                on
daemons_dump_core                           off
daemons_enable_cluster_mode                 off
daemons_use_tcp_wrapper                     off
daemons_use_tty                             off
```

Рис. 4.5: Текущее состояние переключателей SELinux для Apache

5. Посмотрим статистику по политике с помощью команды seinfo (предварительно установив необходимый пакет), также определим множество пользователей, ролей, типов. (рис. 4.6).

```
[makim@makim ~]$ seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] y


 * Waiting in queue...
The following packages have to be installed:
 setools-console-4.4.1-1.el9.x86_64     Policy analysis command-line tools for SELinux
Proceed with changes? [N/y] y


 * Waiting in queue...
 * Waiting for authentication...
 * Waiting in queue...
 * Downloading packages...
 * Requesting data...
 * Testing changes...
 * Installing packages...
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              5100    Attributes:          258
  Users:                 8    Roles:                14
  Booleans:            353    Cond. Expr.:         384
  Allow:             65008    Neverallow:            0
  Auditallow:          170    Dontaudit:          8572
  Type_trans:       265344    Type_change:          87
  Type_member:          35    Range_trans:        6164
  Role allow:           38    Role_trans:          420
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           2    Polcap:                6
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               35
  Genfscon:            109    Portcon:             660
  Netifcon:              0    Nodecon:               0

[makim@makim ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              5100    Attributes:          258
  Users:                 8    Roles:                14
  Booleans:            353    Cond. Expr.:         384
  Allow:             65008    Neverallow:            0
  Auditallow:          170    Dontaudit:          8572
  Type_trans:       265344    Type_change:          87
  Type_member:          35    Range_trans:        6164
  Role allow:           38    Role_trans:          420
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           2    Polcap:                6
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               35
  Genfscon:            109    Portcon:             660
  Netifcon:              0    Nodecon:               0
```

Рис. 4.6: Статистика по политике

6. Определим тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. Определим тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`: `ll /var/www/html`. Создадим от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания (рис. 4.7): `html <html> <body>test</body> </html>`

Рис. 4.7: Определение параметров и создание простого html-файла

7. Проверим контекст созданного файла: `ls -Z /var/www/html`.(рис. 4.8).

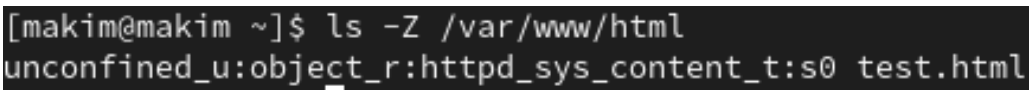

Рис. 4.8: Контекст созданного файла

8. Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл был успешно отображён. (рис. 4.9).

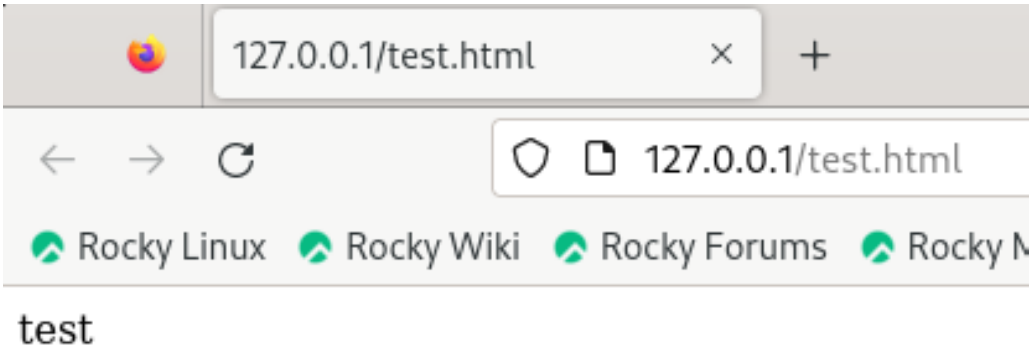

Рис. 4.9: Отображение файла test.html

9. Проверим контекст файла командой: `ls -Z /var/www/html/test.html` (рис. 4.10).

```
[makim@makim ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 4.10: Проверка контекста файла test.html

10. Изменим 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`: `chcon -t samba_share_t /var/www/html/test.html`, `ls -Z /var/www/html/test.html`. После этого проверим, что контекст поменялся. При попытку получить доступ к файлу получаем сообщение об ошибке (рис. 4.11).

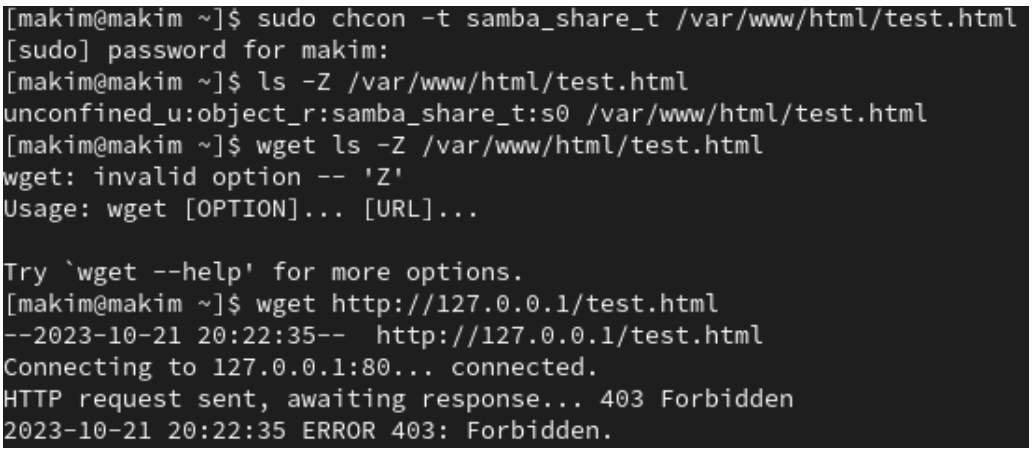

Рис. 4.11: Изменение контекста файла test.html. Попытка получения доступа

11. Просмотрим log-файлы (рис. 4.12).

Рис. 4.12: Log-файлы

12. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`). Для этого в

файле `/etc/httpd/httpd.conf` найдем строчку `Listen 80` и заменим её на `Listen 81` (рис. 4.13).

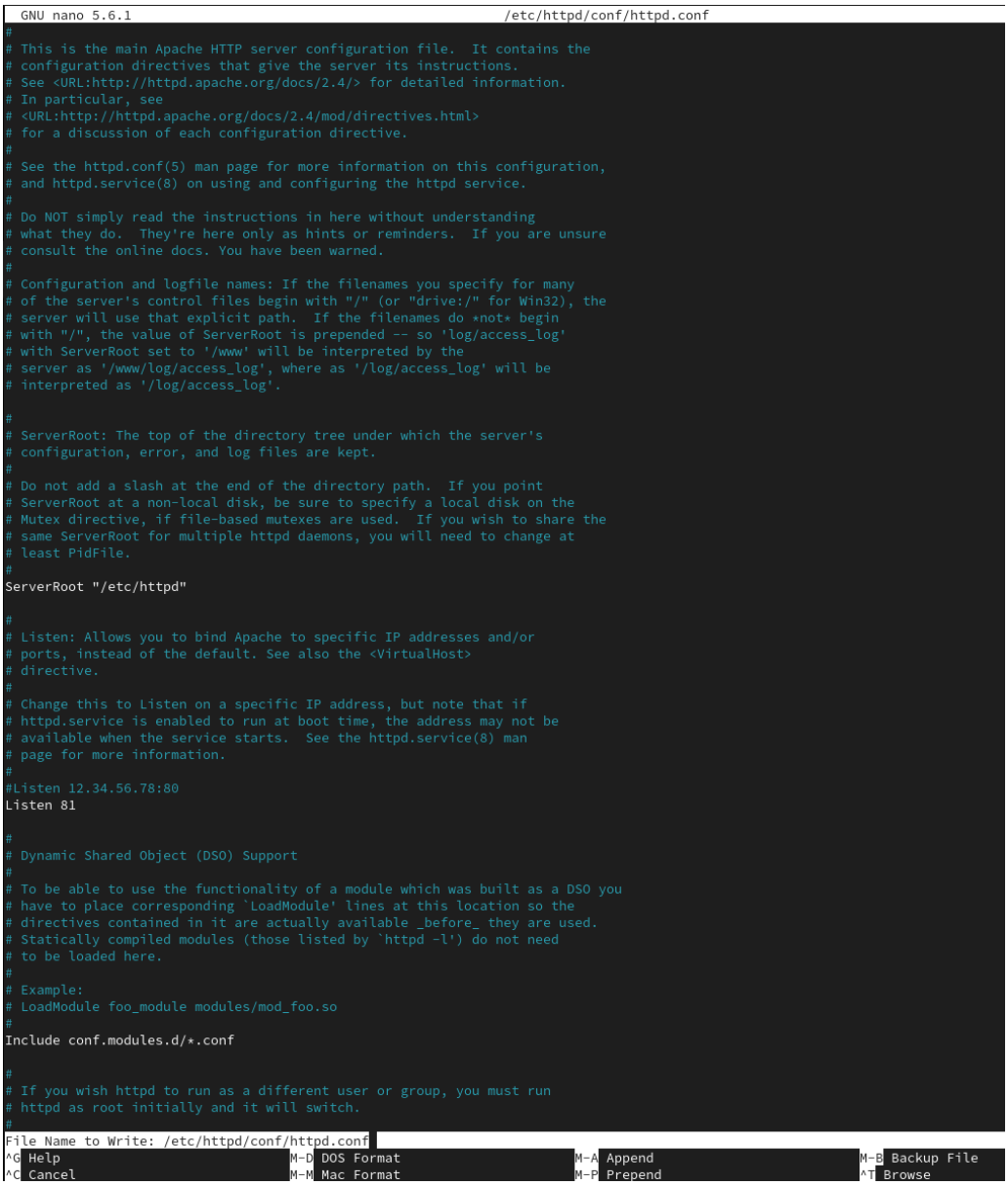

Рис. 4.13: Запуск веб-сервера Apacht на TCP-порт 81

13. Запустить веб-сервер удалось, т.к. TCP-порт 81 уже находится в списке прослушиваемых портов (рис. 4.14).

Рис. 4.14: Список прослушиваемых портов

14. Вернем контекст httpd_sys_content__t к файлу /var/www/html/ test.html: chcon -t httpd_sys_content_t /var/www/html/test.html. После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. (рис. 4.15, 4.16).

Рис. 4.15: Обратное изменение контекста файла

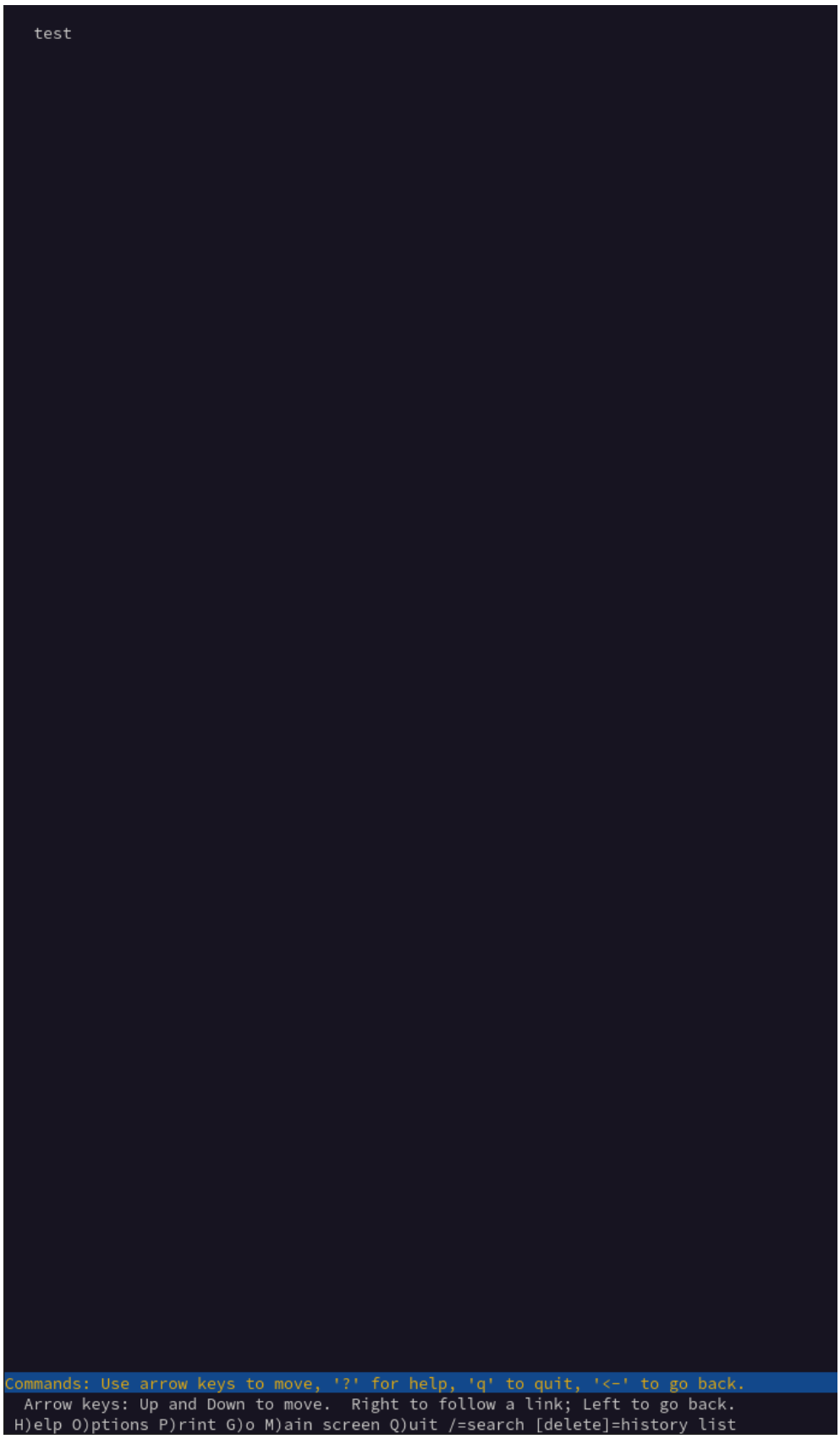

Рис. 4.16: Файл открывается

15. Исправим обратно конфигурационный файл apache, вернув Listen 80. (рис. 4.17).

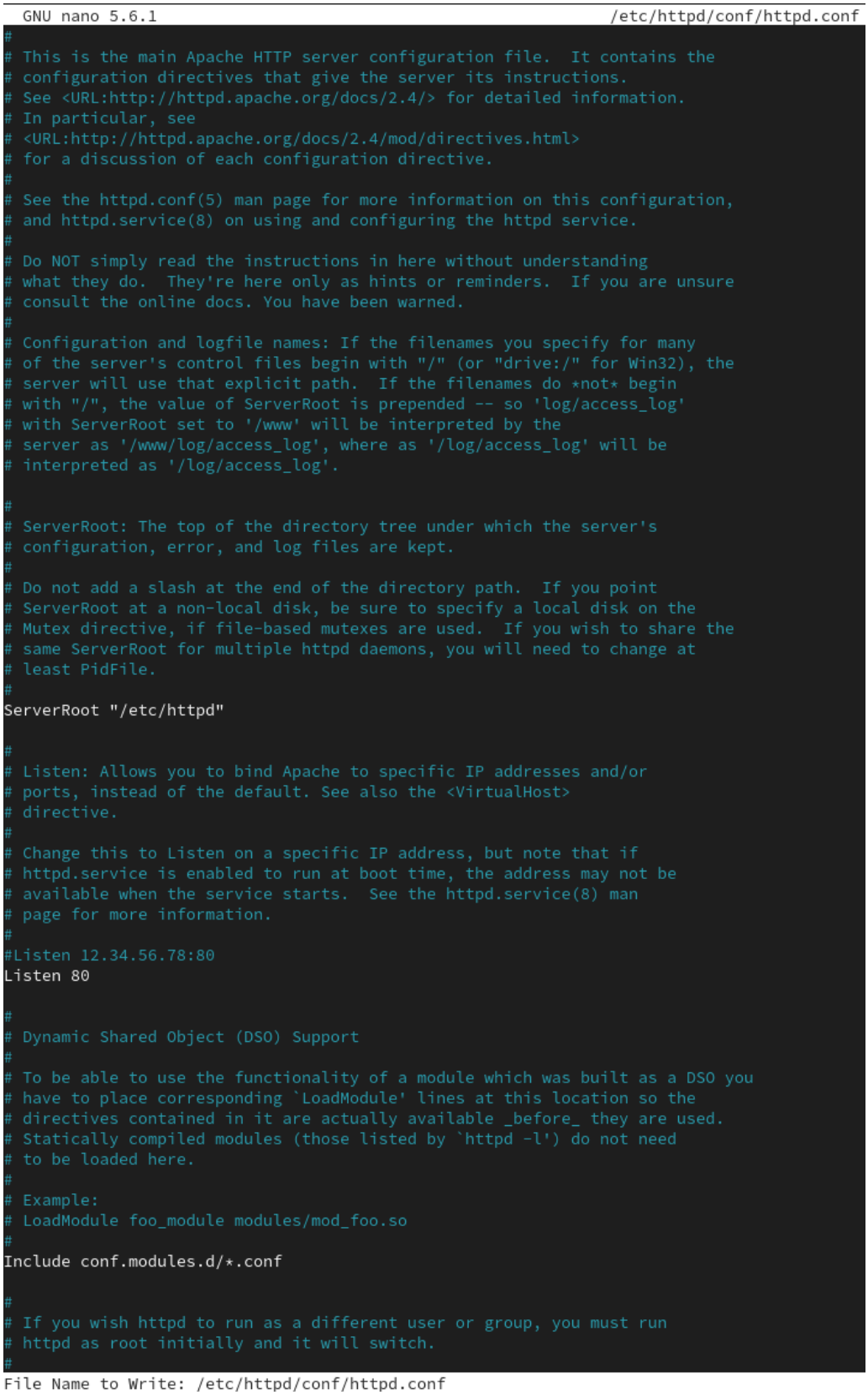

Рис. 4.17: Обратное изменение порта

16. Удалить привязку http_port_t к 81 порту невозможно из-за политики (рис. 4.18).

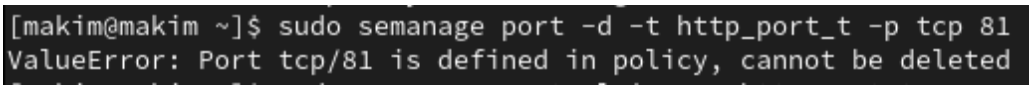

Рис. 4.18: Попытка удаления привязки TCP-порта 81

17. Удалим файл `/var/www/html/test.html`: `rm /var/www/html/test.html` (рис. 4.19).

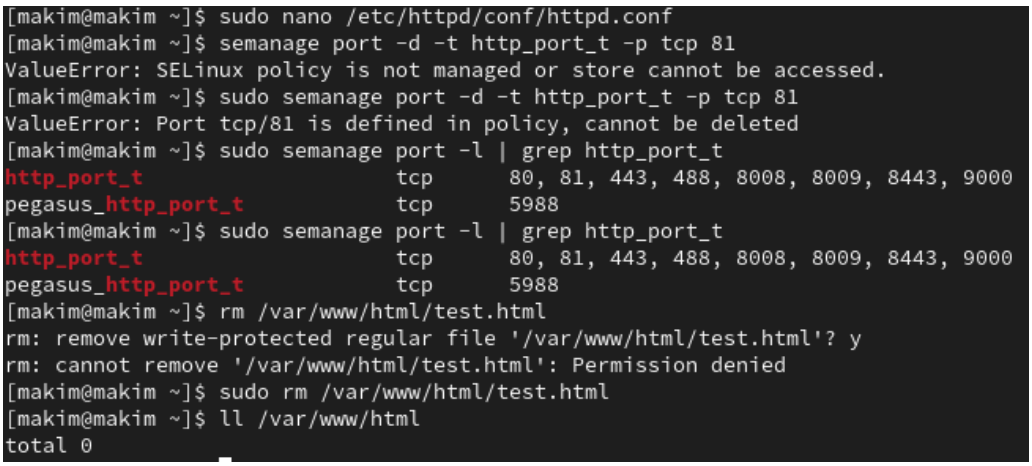

Рис. 4.19: Удаление файла text.html

5 Анализ результатов

Работа выполнена без каких-либо проблем. Работа с терминалом ОС Rocky Linux в данном случае нареканий не вызвала.

6 Выводы

Развиты навыки администрирования ОС Linux. Полученое первое практическое знакомство с технологией SELinux. Проверена работа SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. Терминал Linux [Электронный ресурс]. URL: %7Bhttps://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/%7D.
2. Права доступа [Электронный ресурс]. URL: https://codechick.io/tutorials/unix-linux/unix-linux-permissions.
3. Дополнительные атрибуты файлов [Электронный ресурс]. Enchanted Technology, 2022. URL: https://wiki.enchtex.info/doc/linux_file_attributes.
4. SELinux – описание и особенности работы с системой. Часть 1 [Электронный ресурс]. Habr, 2014. URL: https://habr.com/ru/companies/kingservers/articles/209644/.
5. Apache [Электронный ресурс]. Skillfactory Media, 2023. URL: https://blog.skillfactory.ru/glossary/apache/.