Лабораторная работа №6

Мандатное разграничение прав в Linux

Ли Тимофей Александрович

Содержание

Список таблиц

Список иллюстраций

Цель работы

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

Выполнение лабораторной работы

Для начала я, зайдя в root, установил apache, задал servername в конфигурационном файле и отключил пакетный фильтр. (рис. @fig:001):

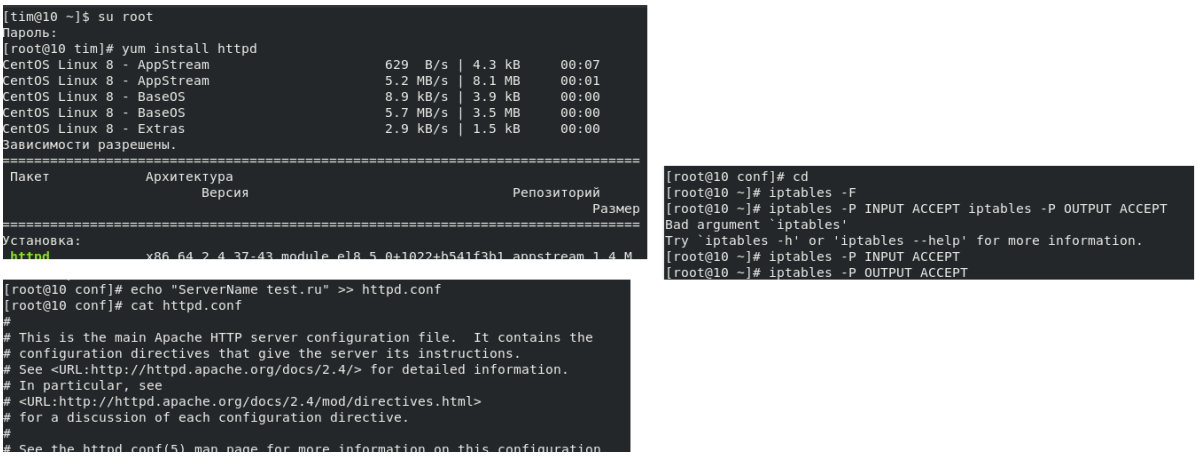

Рис. 0.1: подготовка

Убедился, что SElinux работает в нужном режиме. Нашел apache в списке процессов: (рис. @fig:002)

```
[root@10 ~]# getenforce
Enforcing
[root@10 ~]# 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@10 ~]# ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3973 0.0  0.1 12136 1160 pts/0 R+ 02:22   0:00 grep --color=auto httpd
[root@10 ~]# ps -eZ | grep httpd
[root@10 ~]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v  Verbose check of process and file contexts.
  -b  Display current state of booleans.

Without options, show SELinux status.
[root@10 ~]# sestatus | grep httpd
[root@10 ~]# seinfo
bash: seinfo: команда не найдена...
Установить пакет «setools-console», предоставляющий команду «seinfo»? [N/y] y
```

Рис. 0.2: выполненные действия

посмотрел состояние переключателей SElinux: (рис. @fig:003)

```
[root@10 ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             31 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             132    Permissions:         463
  Sensitivities:         1    Categories:         1024
  Types:              4959    Attributes:          255
  Users:                 8    Roles:                14
  Booleans:            340    Cond. Expr.:         389
  Allow:            112885    Neverallow:            0
  Auditallow:          166    Dontaudit:         10362
  Type_trans:       253398    Type_change:          87
  Type_member:          35    Range_trans:        6015
  Role allow:           38    Role_trans:          423
  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:             640
  Netifcon:              0    Nodecon:               0
[root@10 ~]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'
```

```
[root@10 ~]# sestatus -b | grep httpd
httpd_anon_write                             off
httpd_builtin_scripting                      on
httpd_can_check_spam                         off
httpd_can_connect_ftp                        off
httpd_can_connect_ldap                       off
httpd_can_connect_mythtv                     off
httpd_can_connect_zabbix                     off
httpd_can_network_connect                    off
httpd_can_network_connect_cobbler            off
httpd_can_network_connect_db                 off
httpd_can_network_memcache                   off
httpd_can_network_relay                      off
httpd_can_sendmail                           off
httpd_dbus_avahi                             off
httpd_dbus_sssd                              off
httpd_dontaudit_search_dirs                  off
httpd_enable_cgi                             on
httpd_enable_ftp_server                      off
httpd_enable_homedirs                        off
httpd_execmem                                off
httpd_graceful_shutdown                      off
httpd_manage_ipa                             off
httpd_mod_auth_ntlm_winbind                  off
httpd_mod_auth_pam                           off
httpd_read_user_content                      off
httpd_run_ipa                                off
```

Рис. 0.3: выполненные действия

Определил типы файлов и поддиректорий в www и www/html. Создал файл test.html: (рис. @fig:004)

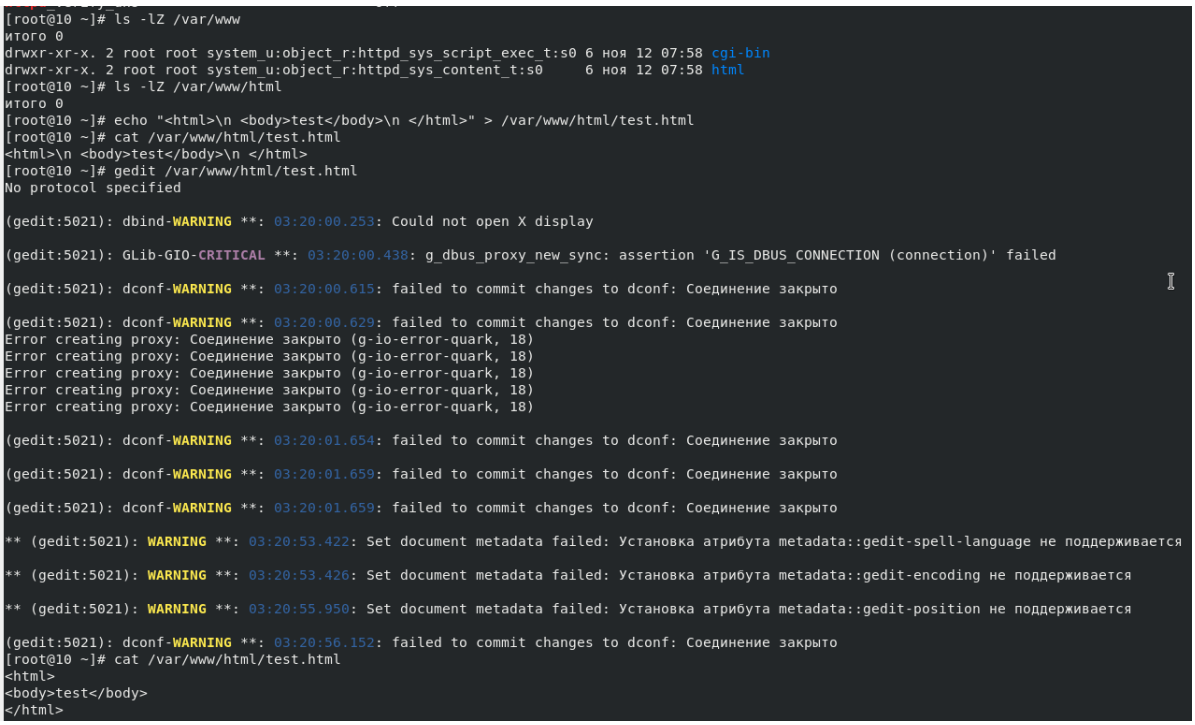

Рис. 0.4: выполненные действия

Получившийся файл: (рис. @fig:005)

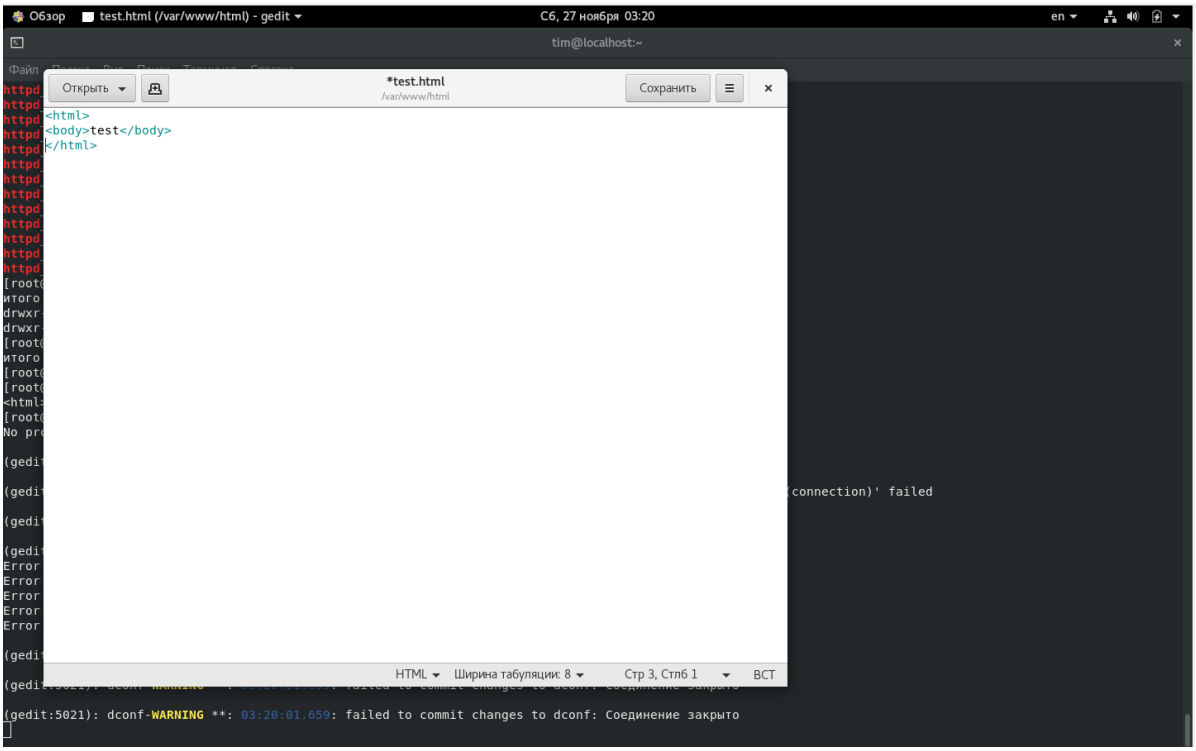

Рис. 0.5: test.html

Затем, не смог отобразить файл через браузер. Проверил контекст файла и попробовал его изменить (получил сообщение об ошибке). Посмотрел лог-файл: (рис. @fig:006)

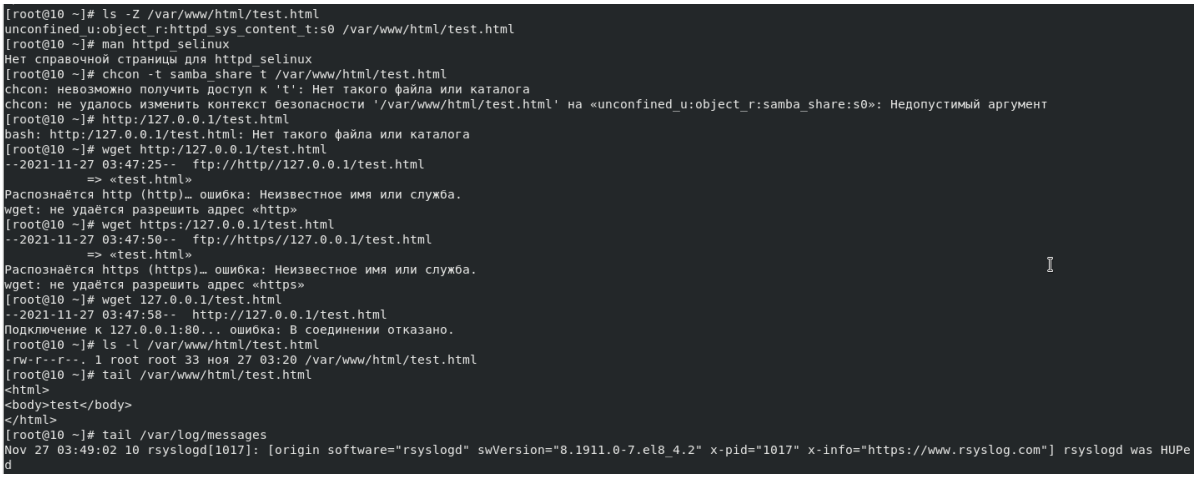

Рис. 0.6: выполненные действия

Попробовал запустить веб-сервер на прослушивание порта 81, изменив файл httpd.conf: (рис. @fig:007)

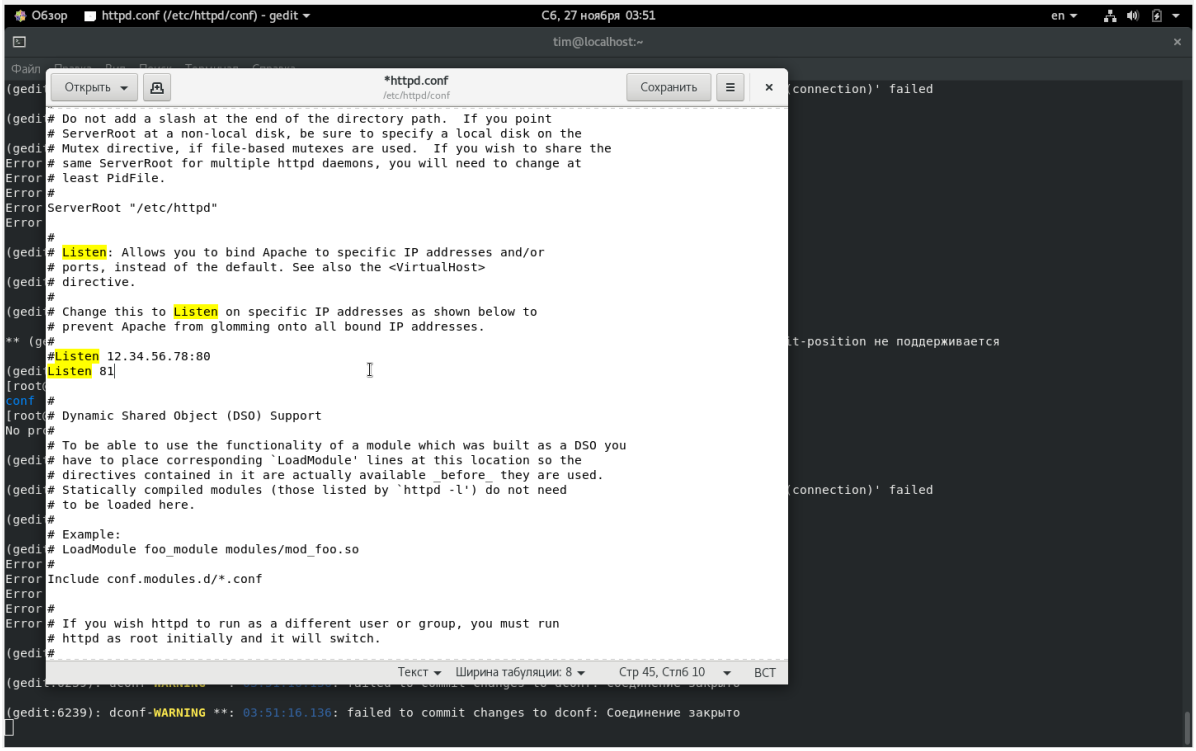

Рис. 0.7: httpd.conf

Не смог запустить веб-сервер, проанализировал лог-файлы. Выполнил команды semanage и убедился, что порт 81 есть в списках: (рис. @fig:008)

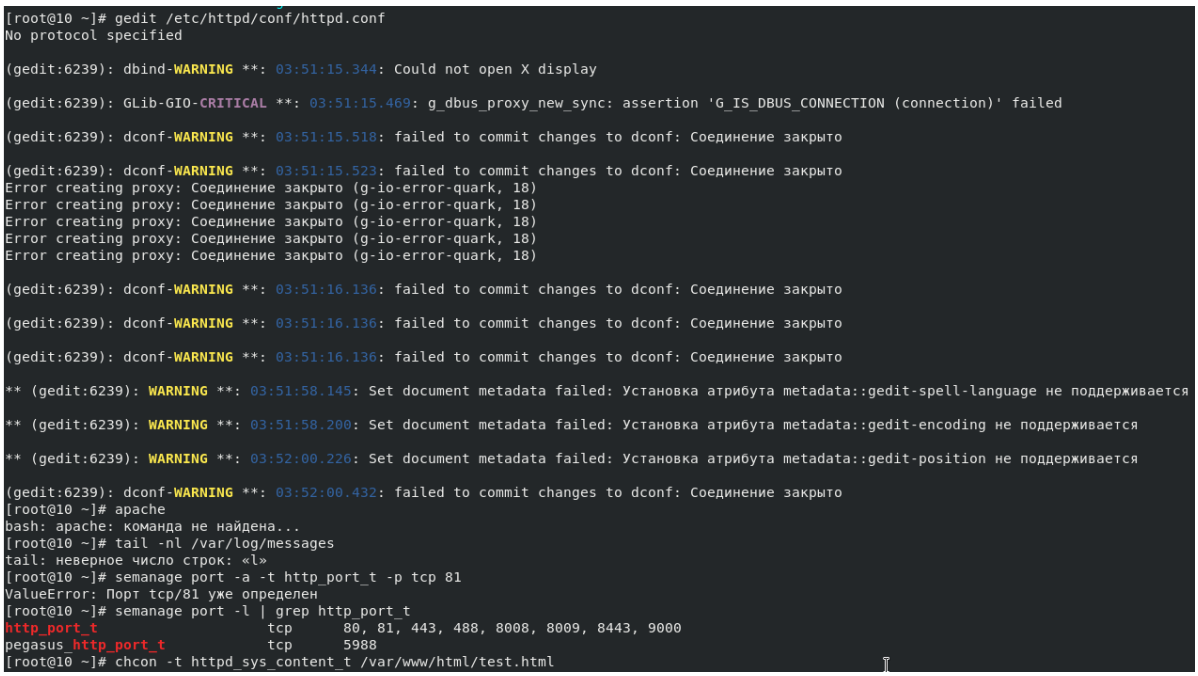

Рис. 0.8: выполненные действия

Вернул контекст файлу test.html, исправил обратно конфигурационный файл, попытался удалить привязку к порту 81 и удалил файл test.html: (рис. @fig:009)

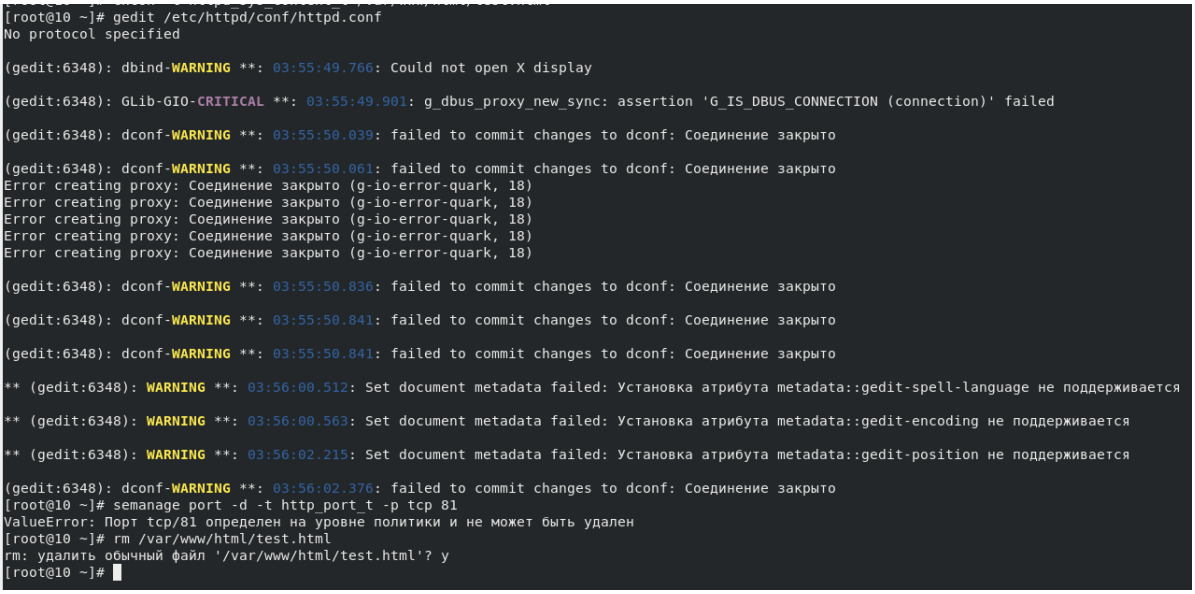

Рис. 0.9: выполненные действия

Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1. Проверил работу SELinx на практике совместно с веб-сервером Apache.