Отчет по лабораторной работе №6

Лабораторная работа №6: Мандатное разграничение прав в Linux

Голова Варвара Алексеевна, НФИбд-03-18

2021, 25 November

Содержание

List of Figures

1 Цель работы

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

2 Выполнение работы

2.1 SELinux

Убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

```
[vgolova@vagolova ~]$ getenforce
Enforcing
[vgolova@vagolova ~]$ 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
```

Figure 2.1: SELinux

2.2 Веб-сервер

Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает, предварительно запустив его.

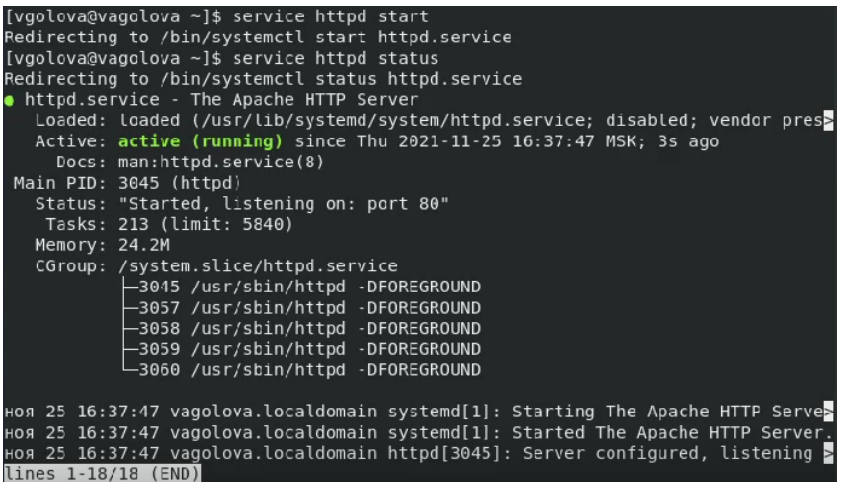

Figure 2.2: Веб-сервер

2.3 Веб-сервер Apache

Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности - unconfined_u, unconfined_r, unconfined_t.

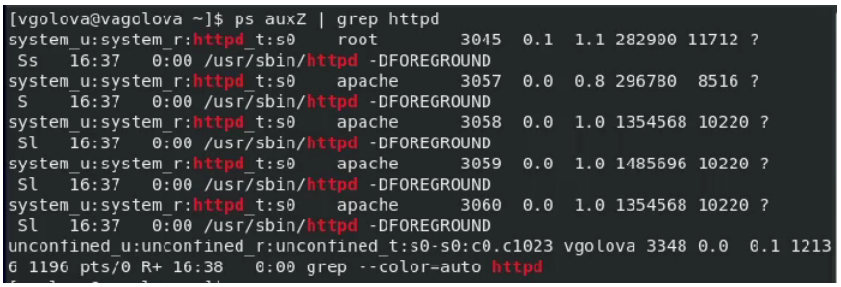

Figure 2.3: Apache

2.4 Текущее состояние переключателей

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd. Обратила внимание, что многие из них находятся в положении «off».

```
webadm_manage_user_files                    off
webadm_read_user_files                      off
wine_mmap_zero_ignore                       off
xdm_bind_vnc_tcp_port                       off
xdm_exec_bootloader                         off
xdm_sysadm_login                            off
xdm_write_home                              off
xen_use_nfs                                 off
xend_run_blktap                             on
xend_run_qemu                               on
xguest_connect_network                      on
xguest_exec_content                         on
xguest_mount_media                          on
xguest_use_bluetooth                        on
xserver_clients_write_xshm                  off
xserver_execmem                             off
xserver_object_manager                      off
zabbix_can_network                          off
zabbix_run_sudo                             off
zarafa_setrlimit                            off
zebra_write_config                          off
zoneminder_anon_write                       off
zoneminder_run_sudo                         off
[vgolova@vagolova ~]$
```

Figure 2.4: Многие находятся в положении “off”

2.5 Статистика

Посмотрела статистику по политике с помощью команды seinfo.

```
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
```

Figure 2.5: Статистика

2.6 Директория

Определила тип файлов и поддиректорий, находящихся в директории /var/www.

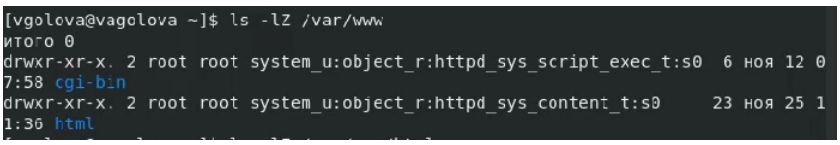

Figure 2.6: Директория

2.7 Test.html

Создала от имени суперпользователя html-файл /var/www/html/test.html.

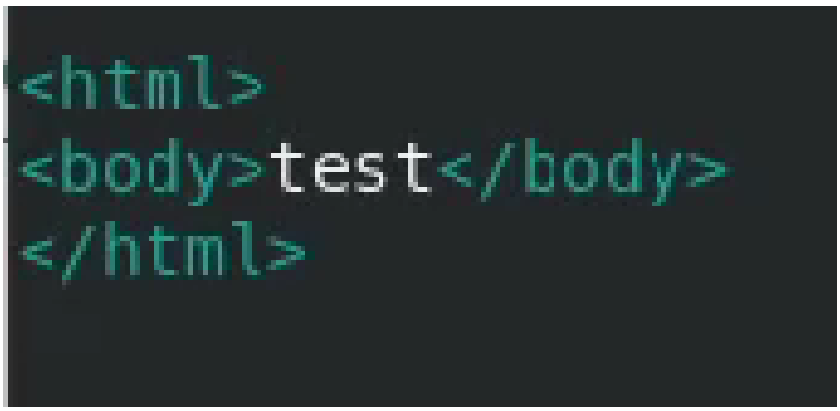

Figure 2.7: Содержимое файла

2.8 Контекст файла

Проверила контекст созданного мной файла - httpd_sys_content_t.

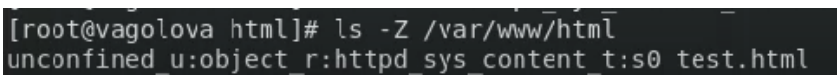

Figure 2.8: Контекст

2.9 Отображение в браузере

Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён.

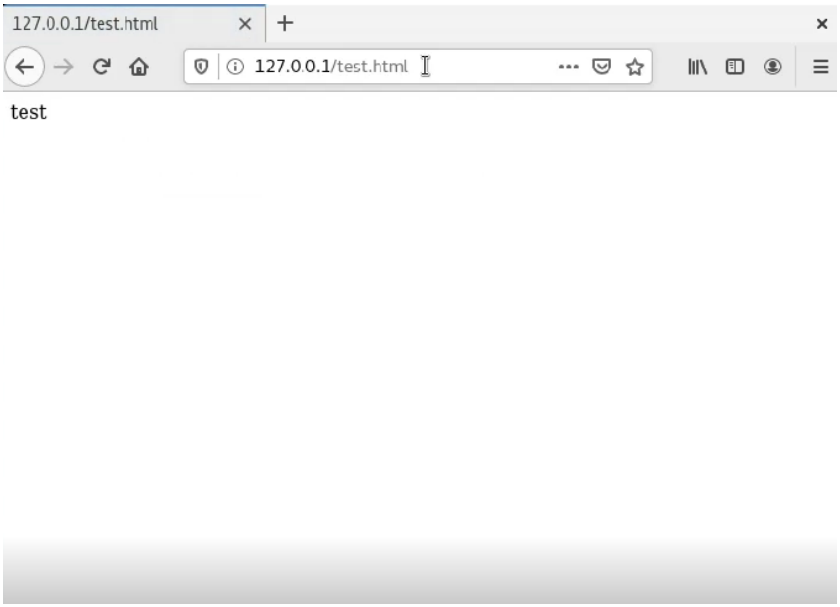

Figure 2.9: Отображение

2.10 Изменение контекста

Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t.

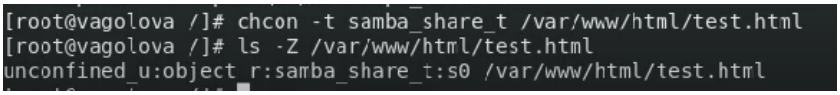

Figure 2.10: Контекст

2.11 Веб-сервер

Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение об ошибке.

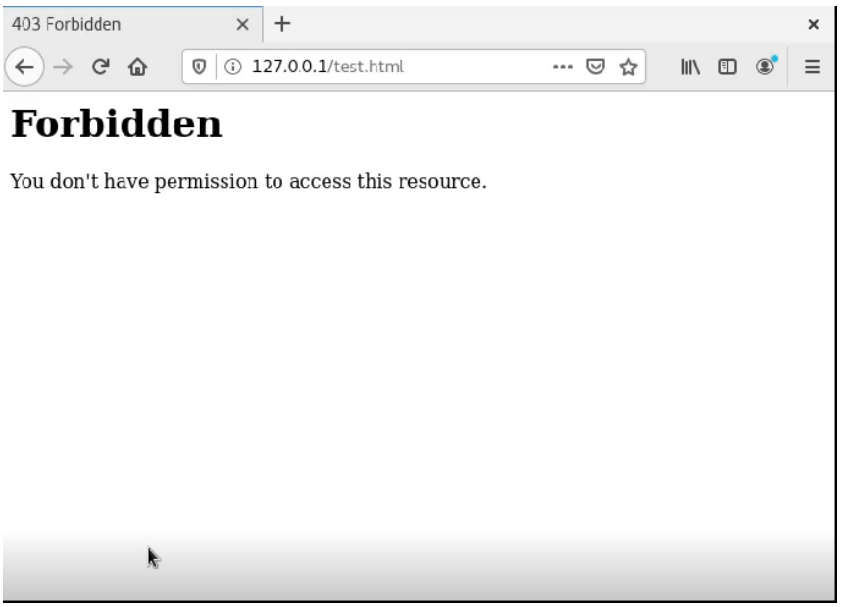

Figure 2.11: Сообщение об ошибке

2.12 Log-файлы

Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл.

Log-файлы

2.13 TCP-порт

Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81.

Figure 2.12: TCP-порт

2.14 Отображение в браузере

Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Доступ был получен.

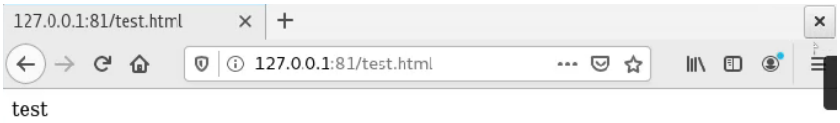

Figure 2.13: Отображение в браузере

2.15 TCP-порт

Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту и проверила, что порт 81 удалён. Затем удалила файл /var/www/html/test.html.

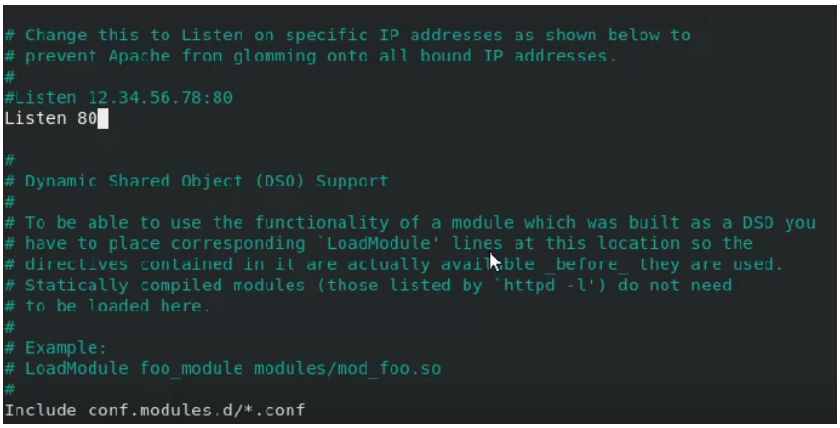

Figure 2.14: TCP-порт

3 Выводы

Я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.