Лабораторная работа №6

Основы Информационной Безопасности

Дьяконова Софья Александровна

Содержание

Цель работы

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

Задание

1. Подготовить рабочую среду;
2. Выполнить основную часть работы;
3. Сделать выводы.

Теоретическое введение

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика targeted и режим enforcing используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл /etc/selinux/config, так и проверить используемый режим и политику.

3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName: ServerName test.ru, чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами
   iptables -F
   iptables -P INPUT ACCEPT
   iptables -P OUTPUT ACCEPT
   либо добавить разрешающие правила:
   iptables -I INPUT -p tcp –dport 80 -j ACCEPT
   iptables -I INPUT -p tcp –dport 81 -j ACCEPT
   iptables -I OUTPUT -p tcp –sport 80 -j ACCEPT
   iptables -I OUTPUT -p tcp –sport 81 -j ACCEPT

6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные links, lynx, wget и графические konqueror, opera, firefox или др.

Выполнение лабораторной работы

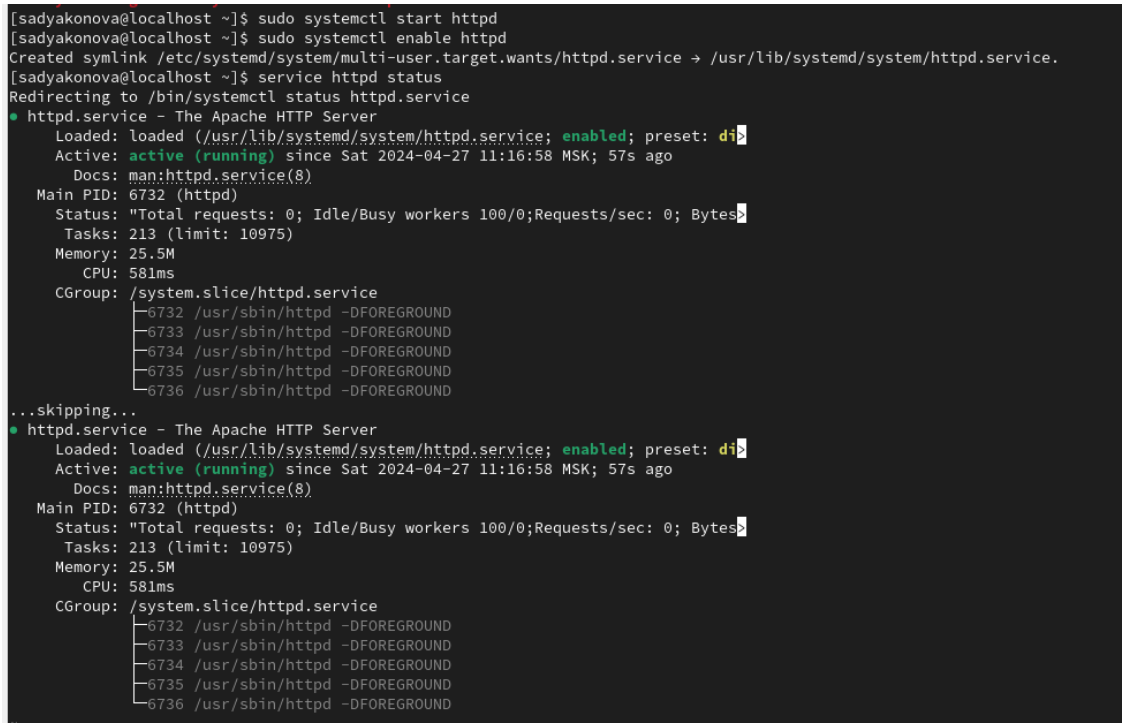
Вошла в систему с и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce и sestatus** (рис. [-@fig:001]).

```
[sadyakonova@localhost ~]$ getenforce
Enforcing
[sadyakonova@localhost ~]$ 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
```

Проверка работы SELinux

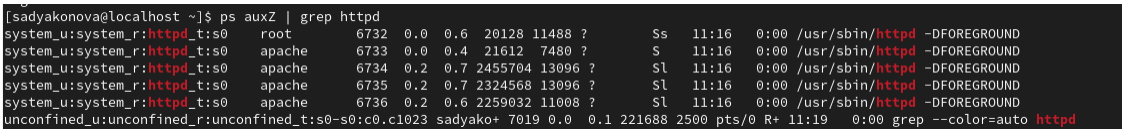
Чтобы работать с библиотекой httpd, скачала ее.

Убедилась, что веб-сервер работает при помощи утилиты **service httpd start** (рис. [-@fig:002]).



Проверка работы

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -b | grep httpd** (рис. [-@fig:003]), (рис. [-@fig:004]).



Состояние переключателей

```
[sadyakonova@localhost ~]$ 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
```

Состояние переключателей

Посмотрела статистику по политике с помощью команды seinfo. Типы: 5135; пользователи: 8; роли: 15 (рис. [-@fig:005]).

```
[root@localhost sadyakonova]# 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:              5135    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            357    Cond. Expr.:         390
  Allow:             65409    Neverallow:            0
  Auditallow:          172    Dontaudit:          8647
  Type_trans:       267813    Type_change:          94
  Type_member:          37    Range_trans:        6164
  Role allow:           39    Role_trans:          419
  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:             665
  Netifcon:              0    Nodecon:               0
[root@localhost sadyakonova]#
```

Статистика

Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www** (папки). Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html (суперпользователю) (рис. [-@fig:006]).

```
[root@localhost sadyakonova]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 окт 28 12:35 html
[root@localhost sadyakonova]# ls -lZ /var/www/html
итого 0
```

Тип файлов, круг пользователей

Создала html-файл /var/www/html/test.html (рис. [-@fig:007]).

```
[sadyakonova@localhost ~]$ sudo touch /var/www/html/test.html
[sudo] пароль для sadyakonova:
[sadyakonova@localhost ~]$ sudo nano /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

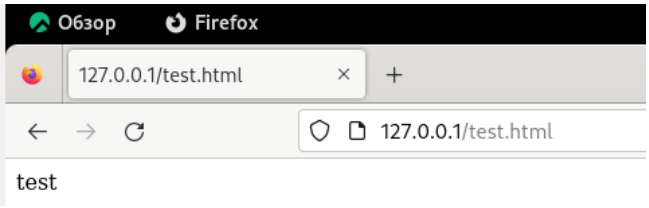
Файл

Проверила контекст созданного файла (httpd_sys_content_t) (рис. [-@fig:008]).

```
[sadyakonova@localhost ~]$ ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 апр 27 11:26 test.html
```

Контекст файла

Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён (рис. [-@fig:009]).



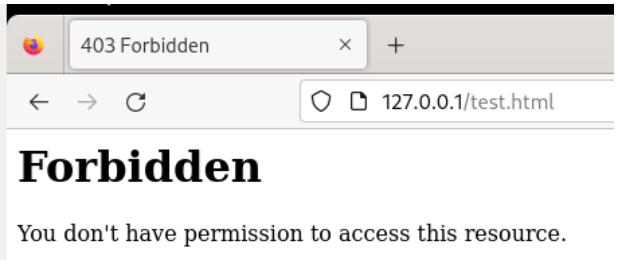
Состояние переключателей

Тип httpd_sys_content_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер. Изменила контекст файла /var/www/html/test.html с **httpd_sys_content_t** на **samba_share_t** с помощью утилиты **chcon -t samba_share_t /var/www/html/test.html**. Контекст поменялся (рис. [-@fig:010]).

```
[sadyakonova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для sadyakonova:
[sadyakonova@localhost ~]$ sudo ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 апр 27 11:26 /var/www/html/test.html
```

Изменение контекста

Попробовала ещё раз получить доступ к файлу через веб-сервер. Ошибка :(((рис. [-@fig:011]).



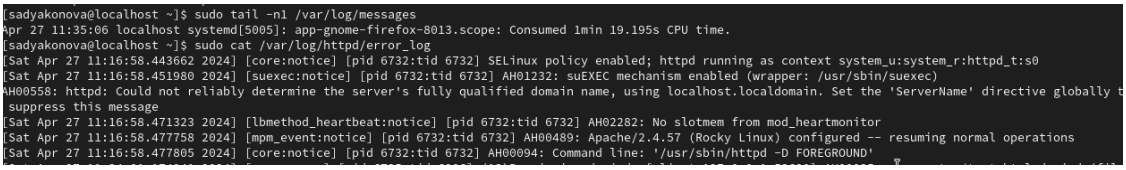
Отказ в доступе

Проанализировала ситуацию. Файл не отображается, так как этот тип не позволяет процессу httpd получить доступ к файлу. Также просмотрела системный лог-файл tail /var/log/messages (рис. [-@fig:012]).

Лог-файл

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

Выполнила перезапуск веб-сервера Apache. Сбой не произошел…. Проанализировала лог-файлы tail -nl /var/log/messages, /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log (рис. [-@fig:013]) .

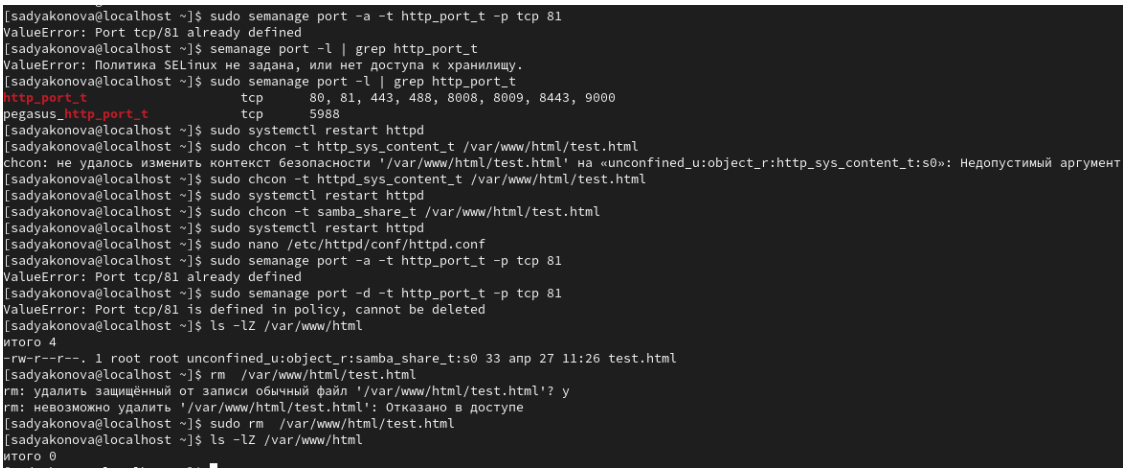


Перезапуск сервера

Выполнила команду **semanage port -a -t http_port_t -p tcp 81**, проверила список портов командой **semanage port -l | grep http_port_t** (рис. [-@fig:014]).

Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html.
После этого попробовала получить доступ к файлу через веб-сервер (рис. [-@fig:014]).

Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту, но появилась ошибка, что этот порт удалить невозможно, даже через суперпользователя.
Удалила файл /var/www/html/test.html (рис. [-@fig:014]).



Конец)

Выводы

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux.