Лабораторная работа №6

Основы информационной безопасности

Разанацуа Сара Естэлл

Цель

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

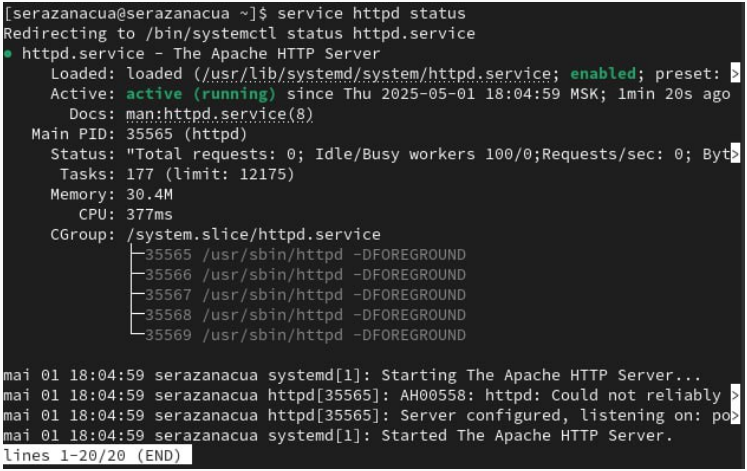
Вошла в систему под своей учетной записью. Убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

```
[serazanacua@serazanacua ~]$ getenforce
Enforcing
[serazanacua@serazanacua ~]$ 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
[serazanacua@serazanacua ~]$
```

Рис. 1: проверка режима работы SELinux

Процесс выполнения

Запускаю сервер apache, далее обращаюсь с помощью браузера к веб-серверу, запущенному на компьютере, он работает, что видно из вывода команды `service httpd status`.



Процесс выполнения

- С помощью команды `ps auxZ | grep httpd` нашла веб-сервер Apache в списке процессов. Его контекст безопасности - httpd_t.

```
[serazanacua@serazanacua ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       35565  0.0  0.5  21232 11444 ?
   Ss   18:04   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     35566  0.0  0.3  22964  7404 ?
   S    18:04   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     35567  0.1  0.7 2358704 15424 ?
   Sl   18:04   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     35568  0.1  0.8 2162032 17576 ?
   Sl   18:04   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     35569  0.1  0.5 2162032 11064 ?
   Sl   18:04   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 serazan+ 35851 0.0  0.1
221676 2432 pts/0 S+ 18:09   0:00 grep --color=auto httpd
[serazanacua@serazanacua ~]$
```

Рис. 3: Контекст безопасности Apache

Процесс выполнения

- Просмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`.

```
[serazanacua@serazanacua ~]$ 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.
[serazanacua@serazanacua ~]$ 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
```

Процесс выполнения

- Просмотрела статистику по политике с помощью команды `seinfo`. Множество пользователей - 8, ролей - 39, типов - 5135.

```
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:              5169    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            358    Cond. Expr.:         390
  Allow:             65633    Neverallow:            0
  Auditallow:          176    Dontaudit:          8703
  Type_trans:       271851    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           1    Polcap:                6
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
```

- Типы поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` следующие: владелец - root, права на изменения только у владельца. Файлов в директории нет.

```
[serazanacua@serazanacua ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 22 janv
. 03:25 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 22 janv
. 03:25 html
[serazanacua@serazanacua ~]$
```

Рис. 6: Типы поддиректорий

Процесс выполнения

- Создать файл может только суперпользователь, поэтому от его имени создаем файл touch.html со следующим содержанием:

```
[serazanacua@serazanacua ~]$ sudo touch /var/www/html/test.html
[serazanacua@serazanacua ~]$ sudo nano /var/www/html/test.html
[serazanacua@serazanacua ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[serazanacua@serazanacua ~]$
```

Рис. 7: Создание файла

- Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t.

```
[serazanacua@serazanacua ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33  1 mai
   18:22 test.html
[serazanacua@serazanacua ~]$
```

Рис. 8: Контекст файла

- Обращаюсь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён (.

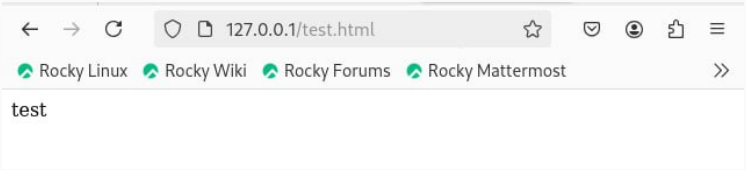


Рис. 9: Отображение файла

- При попытке отображения файла в браузере получаем сообщение об ошибке.

Рис. 10: Отображение файла

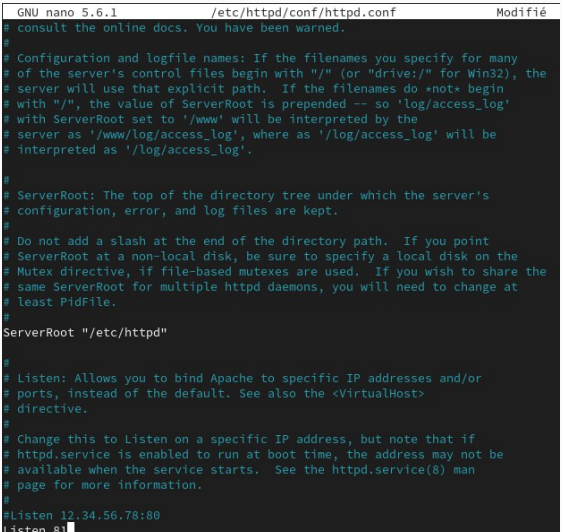
- Чтобы запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services) открываю файл /etc/httpd/httpd.conf для изменения.

```
[serazanacua@serazanacua ~]$ sudo nano /etc/httpd/conf/httpd.conf
[serazanacua@serazanacua ~]$
```

Рис. 11: Изменение файла

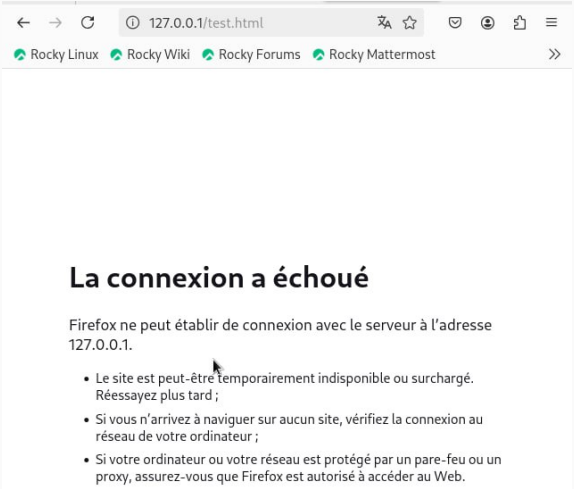
Процесс выполнения

- Нахожу строчку Listen 80 и заменяю её на Listen 81.



Процесс выполнения

- Выполняю перезапуск веб-сервера Apache. Произошёл сбой, потому что порт 80 для локальной сети, а 81 нет.



Процесс выполнения

- Перезапускаю сервер Apache.

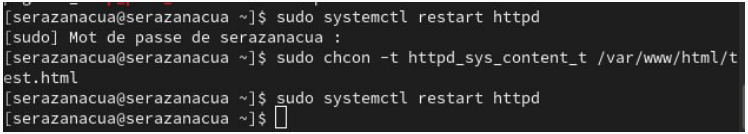


Рис. 14: Перезапуск сервера

- Теперь он работает, ведь мы внесли порт 81 в список портов `httpd_port_t`.

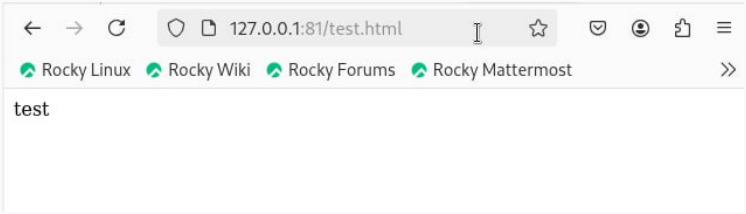


Рис. 15: Проверка сервера

- Возвращаю в файле /etc/httpd/httpd.conf порт 80, вместо 81. Проверяю, что порт 81 удален, это правда.

```
[serazanacua@serazanacua ~]$ sudo nano /etc/httpd/conf/httpd.conf
[serazanacua@serazanacua ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Le port tcp/81 est défini dans la politique, il ne peut être suppr
imé
[serazanacua@serazanacua ~]$ semanage port -d -t http_port_t -p tcp 81
ValueError: La stratégie SELinux n'est pas gérée ou la base n'est pas accessib
le.
[serazanacua@serazanacua ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Le port tcp/81 est défini dans la politique, il ne peut être suppr
imé
[serazanacua@serazanacua ~]$
```

Рис. 16: Проверка порта 81

Вывод

- В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.

Спасибо за внимания