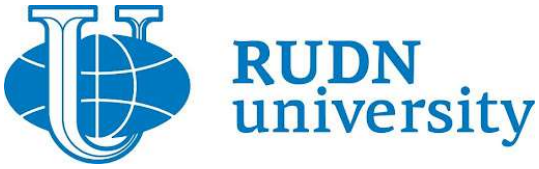
Лабораторная работа №6

Мандатное разграничение прав в Linux

Доборщук В.В., НФИбд-01-18



27 ноября 2021

Содержание

Список иллюстраций

Цель работы

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

Задачи:

— познакомиться с SELinux;
— проверить работу с SELinux с веб-сервером Apache;

Теоретическое введение

Для выполнения данной лабораторной работы мы использовали данные источники, в виде описания лабораторной работы, а также свободные источники в интернете.

Выполнение лабораторной работы

Предварительно подготовили стенд и установили сервер Apache.

```
[vdoborschuk@localhost ~]$ getenforce
Enforcing
[vdoborschuk@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
[vdoborschuk@localhost ~]$ sudo service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 23:05:10 MSK; 7min ago
     Docs: man:httpd.service(8)
 Main PID: 14884 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 11260)
   Memory: 33.0M
   CGroup: /system.slice/httpd.service
           ├─14884 /usr/sbin/httpd -DFOREGROUND
           ├─15060 /usr/sbin/httpd -DFOREGROUND
           ├─15061 /usr/sbin/httpd -DFOREGROUND
           ├─15062 /usr/sbin/httpd -DFOREGROUND
           └─15063 /usr/sbin/httpd -DFOREGROUND

ноя 27 23:05:10 localhost.vdoborschuk systemd[1]: Starting The Apache HTTP Server...
ноя 27 23:05:10 localhost.vdoborschuk systemd[1]: Started The Apache HTTP Server.
ноя 27 23:05:10 localhost.vdoborschuk httpd[14884]: Server configured, listening on: port 80
[vdoborschuk@localhost ~]$
```

Рис. 1: Проверка `sestatus` и Apache-сервера

```
[vdoborschuk@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       14884  0.0  0.6 282928 11960 ?        Ss   23:05   0:00 /usr/sbin/ht
tpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15060  0.0  0.4 296812  8668 ?        S    23:05   0:00 /usr/sbin/ht
tpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15061  0.0  0.8 1354600 16500 ?       Sl   23:05   0:00 /usr/sbin/ht
tpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15062  0.0  0.7 1485728 14460 ?       Sl   23:05   0:00 /usr/sbin/ht
tpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15063  0.0  0.8 1354600 16500 ?       Sl   23:05   0:00 /usr/sbin/ht
tpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vdobors+ 33314 0.0  0.0 12136 1132 pts/0 S+ 23:13   0:00
grep --color=auto httpd
[vdoborschuk@localhost ~]$
```

Рис. 2: Определение сервера Apache в списке процессов

Не удалось определить текущее состояние переключателей SELinux, т.к. не поддерживается `-bigrep` аргумент.

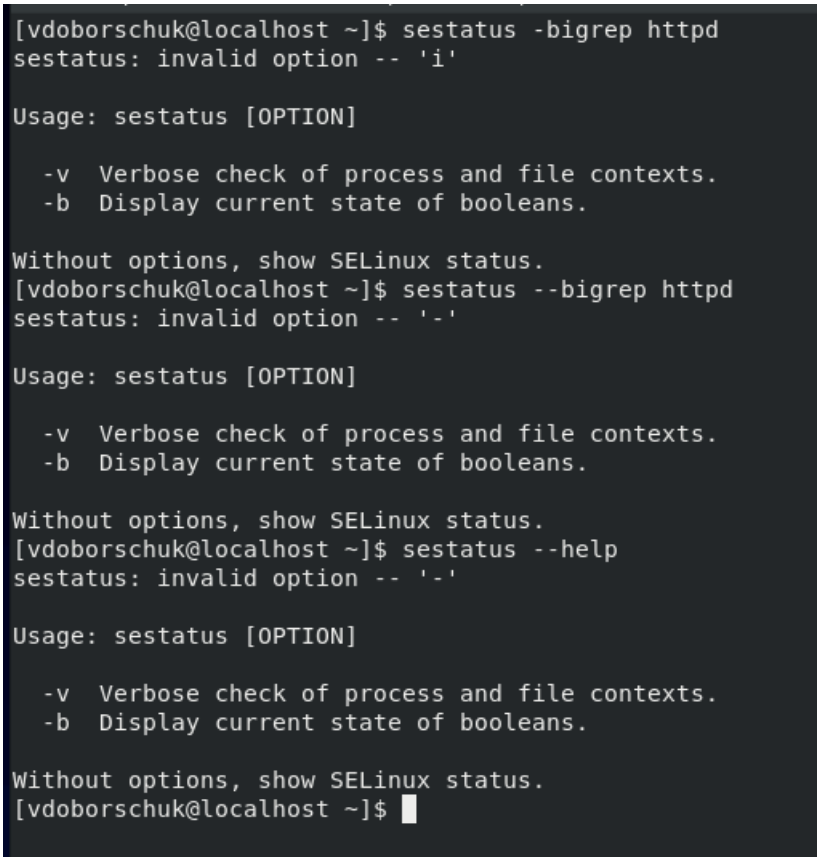


Рис. 3: `sestatus -bigrep httpd`

```
[vdoborschuk@localhost ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             31 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             132    Permissions:         464
  Sensitivities:         1    Categories:         1024
  Types:              4961    Attributes:          255
  Users:                 8    Roles:                14
  Booleans:            338    Cond. Expr.:         386
  Allow:            112594    Neverallow:            0
  Auditallow:          166    Dontaudit:         10358
  Type_trans:       252747    Type_change:          87
  Type_member:          35    Range_trans:        5781
  Role allow:           38    Role_trans:          421
  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:               34
  Genfscon:            107    Portcon:             642
  Netifcon:              0    Nodecon:               0
[vdoborschuk@localhost ~]$
```

Рис. 4: Статистика `seinfo`

Определили тип файлов директорий /var/www/...

```
[vdoborschuk@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 ноя 12 07:58 html
[vdoborschuk@localhost ~]$ ls -lZ /var/www/html
итого 0
[vdoborschuk@localhost ~]$
```

Рис. 5: Директории `/var/www/`

```
[vdoborschuk@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 ноя 12 07:58 html
[vdoborschuk@localhost ~]$ ls -lZ /var/www/html
итого 0
[vdoborschuk@localhost ~]$ sudo vi /var/www/html/test.html
[vdoborschuk@localhost ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 23:16 test.html
[vdoborschuk@localhost ~]$
```

Рис. 6: Создание `test.html`

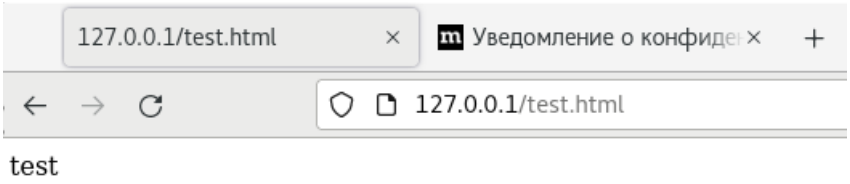


Рис. 7: Проверка в браузере по 127.0.0.1

Далее не удалось изучить справку, т.к. `man` по предложенной инструкции не существует.

```
[vdoborschuk@localhost ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
[vdoborschuk@localhost ~]$ ls -Z /var/www/html/test
ls: невозможно получить доступ к '/var/www/html/test': Нет такого файла или каталога
[vdoborschuk@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

Рис. 8: Проверка контекста `test.html`

Рис. 9: Изменение контекста `test.html`

Рис. 10: Проверка измененного контекста в браузере

Далее, проанализировали log-файлы, убедившись, что при таком контексте мы не сможем получить информацию из `test.html` через браузер.

Рис. 11: Анализ log-файлов

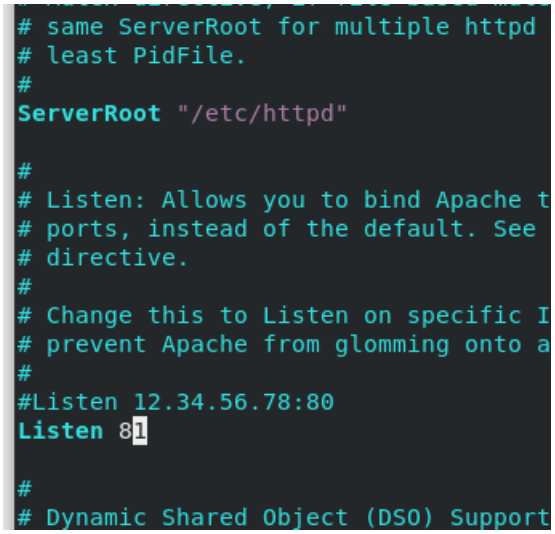


Рис. 12: Измененение TCP-порта

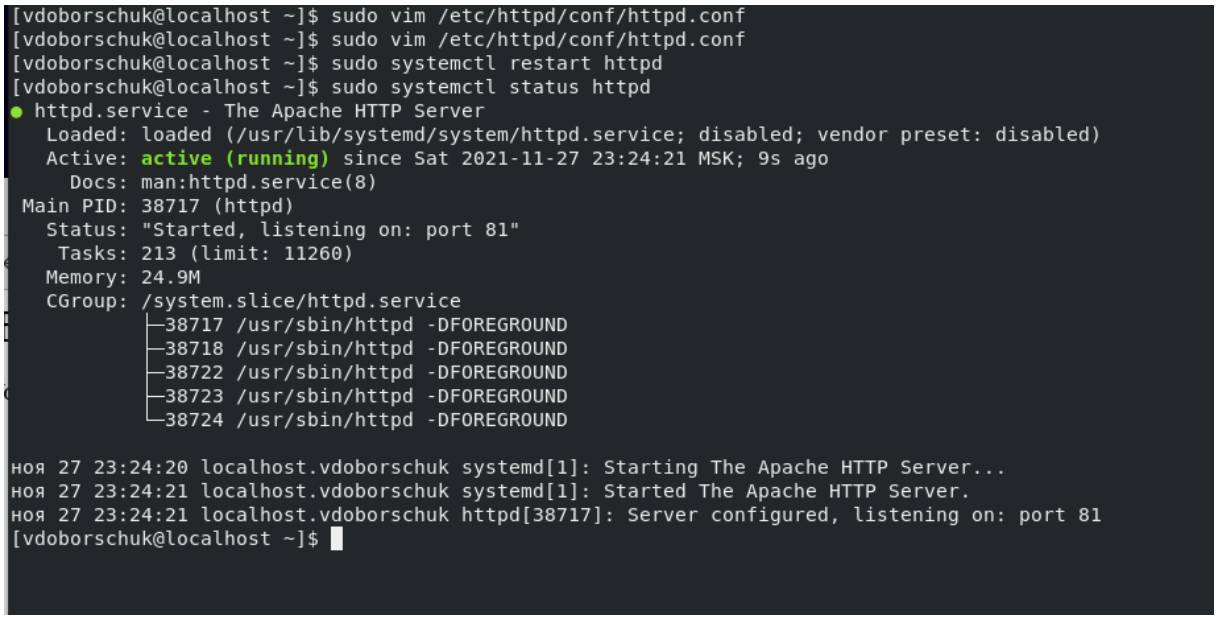


Рис. 13: Успешный перезапуск Apache

Нам не потребовалось проверять лог-файлы, все прошло успешно.

```
[vdoborschuk@localhost ~]$ semanage port -a -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[vdoborschuk@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[vdoborschuk@localhost ~]$ sudo semanage port -l | grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[vdoborschuk@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

Рис. 14: Назначение порта по semanage и изменение контекста

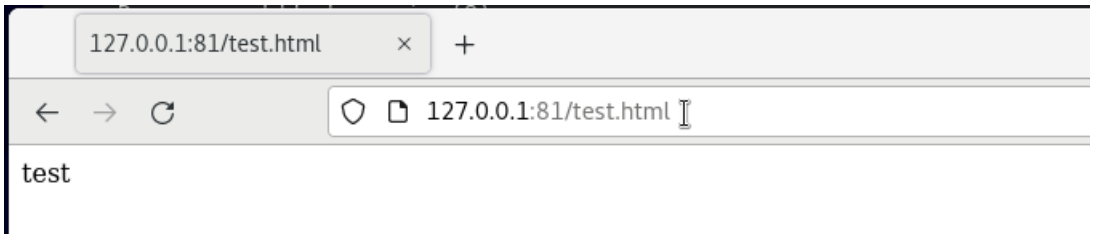


Рис. 15: Проверка измененного контекста в браузере (успешно)

```
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[vdoborschuk@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[vdoborschuk@localhost ~]$ sudo vi /etc/httpd/conf/httpd.conf
[vdoborschuk@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[vdoborschuk@localhost ~]$ sudo rm /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

Рис. 16: Возврат к основным конфигурациям

Заключение

В результате выполнения работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.