Лабораторная работа 6

Основы информационной безопасности

Симонова Полина Игоревна

2026-02-15

Содержание I

Раздел 1

1. Информация

1.1 Докладчик

Симонова Полина Игоревна; студент группы НКАбд-02-24

Раздел 2

2. Элементы презентации

2.1 Цели и задачи

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

Раздел 3

3. Выполнение лабораторной работы

3.1 1

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

```
pisimonova@pisimonova:~$ getenforce
Enforcing
pisimonova@pisimonova:~$ 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
```

3.2 2

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

```
     Active: active (running) since Sat 2026-02-14 15:57:54 MSK
; 1min 17s ago
 Invocation: d18e6a1fc1f943a3aa8967eda6c1661f
       Docs: man:httpd.service(8)
   Main PID: 14998 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Reques
ts/sec: 0; Bytes served/s
      Tasks: 177 (limit: 10544)
     Memory: 17.9M (peak: 18.1M)
        CPU: 98ms
     CGroup: /system.slice/httpd.service
             ├─14998 /usr/sbin/httpd -DFOREGROUND
             ├─15041 /usr/sbin/httpd -DFOREGROUND
             ├─15042 /usr/sbin/httpd -DFOREGROUND
             ├─15045 /usr/sbin/httpd -DFOREGROUND
             └─15046 /usr/sbin/httpd -DFOREGROUND
```

3.3 3

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

```
pisimonova@pisimonova:~$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       14998  0.0  0.3  19136  6716 ?
Ss   15:57   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15041  0.0  0.2  18792  3728 ?
S    15:57   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15042  0.0  0.3 1109220 5368 ?
Sl   15:57   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15045  0.0  0.3 978084  5356 ?
Sl   15:57   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     15046  0.0  0.3 978084  5352 ?
Sl   15:57   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 pisimon+ 15951 0.0  0.1 227
712 2168 pts/0 S+ 16:06   0:00 grep --color=auto httpd
```

Рисунок 3: Контекст безопасности Apache

3.4 4

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

```
pisimonova@pisimonova:~$ 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                           on
abrt_upload_watch_anon_write                on
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
```

В директории /var/www/html нет файлов.

```
pisimonova@pisimonova:~$ ls -lZ /var/www/html
итого 0
```

Рисунок 5: Типы файлов

3.6 6

Создать файл может только суперпользователь, поэтому от его имени создаем файл touch.html

```
pisimonova@pisimonova:~$ nano test.html
pisimonova@pisimonova:~$ sudo nano test.html
pisimonova@pisimonova:~$ sudo cat /var/www/html/test.html
pisimonova@pisimonova:~$ ls -lZ /var/www/html
итого 0
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 фев 14 16
27 test.html
pisimonova@pisimonova:~$ sudo touch /var/www/html/test.html
pisimonova@pisimonova:~$ ls
 sshgit       work          Загрузки      Общедоступные
 sshgit.pub   Видео         Изображения   'Рабочий стол'
 test.html    Документы     Музыка        Шаблоны
pisimonova@pisimonova:~$
pisimonova@pisimonova:~$ nano test.html
```

Рисунок 6: Создание файла

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

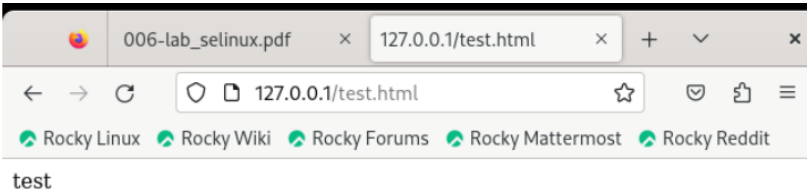

Рисунок 7: Отображение файла

3.8 8

Изменяю контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс httpd не должен иметь доступа, например, `samba_share_t`:

```
pisimonova@pisimonova:~$ sudo chcon -t samba_share_t /var/www/html/test.html

pisimonova@pisimonova:~$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 фев 14 16:36 te
st.html
```

Рисунок 8: Изменение контекста

При попытке отображения файла в браузере получаем сообщение об ошибке (рис. [-@fig:013]).

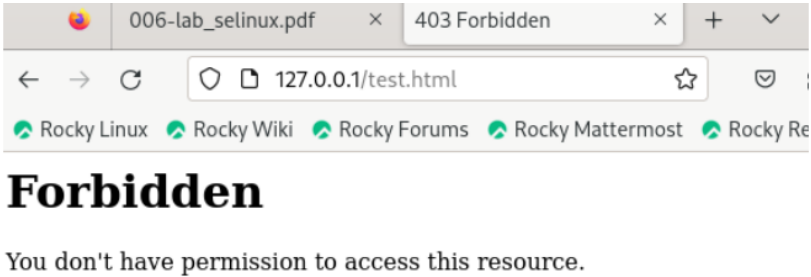

Рисунок 9: Отображение файла

Раздел 4

4. Выводы

4. Выводы

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.