

Лабораторная работа №6

Информационная безопасность

Леонтьева К. А., НПМбд-01-19

3 октября 2022

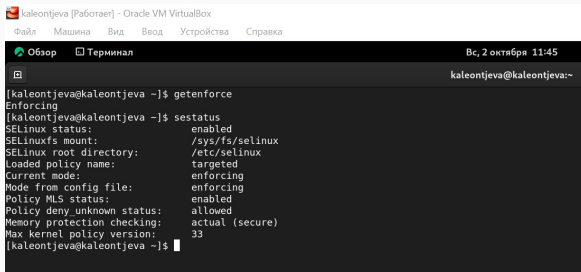
Российский университет дружбы народов

Москва, Россия

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

- 1) Проверить корректность работы SELinux, запустить веб-сервер Apache
- 2) Создать файл test.html
- 3) Обратиться к файлу через веб-сервер при разном контексте и порте

- Проверила, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”

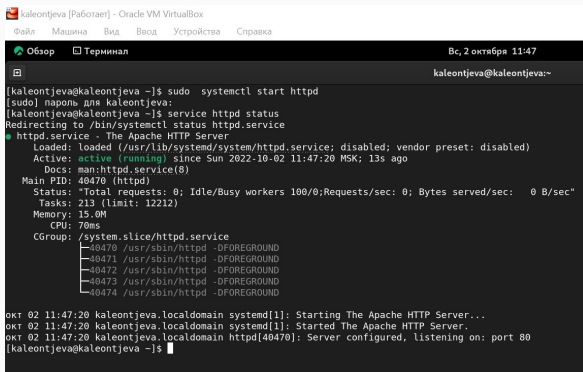
A screenshot of a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar are tabs for "Обзор" and "Терминал", with "Терминал" being the active tab. The terminal shows the output of two commands: "getenforce" and "sestatus". The "getenforce" command returns "Enforcing". The "sestatus" command returns a detailed status report: 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), and Max kernel policy version: 33.

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

Figure 1: Рис.1: Проверка режима enforcing политики targeted

Ход выполнения лабораторной работы

- Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает с помощью команды “service httpd status”



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 11:47
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ sudo systemctl start httpd
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ 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 Sun 2022-10-02 11:47:20 MSK; 13s ago
     Docs: man:httpd.service(8)
   Main PID: 40470 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 12212)
   Memory: 15.0M
      CPU: 70ms
   CGroup: /system.slice/httpd.service
           └─40470 /usr/sbin/httpd -DFOREGROUND
             └─40471 /usr/sbin/httpd -DFOREGROUND
               └─40472 /usr/sbin/httpd -DFOREGROUND
                 └─40473 /usr/sbin/httpd -DFOREGROUND
                   └─40474 /usr/sbin/httpd -DFOREGROUND

окт 02 11:47:20 kaleontjeva.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 02 11:47:20 kaleontjeva.localdomain systemd[1]: Started The Apache HTTP Server.
окт 02 11:47:20 kaleontjeva.localdomain httpd[40470]: Server configured, listening on: port 80
[kaleontjeva@kaleontjeva ~]$
```

Figure 2: Рис.2: Проверка работы веб-сервера

Ход выполнения лабораторной работы

- От имени суперпользователя создала файл test.html. Обратилась к нему через веб-сервер, введя адрес “http://127.0.0.1/test.html”.

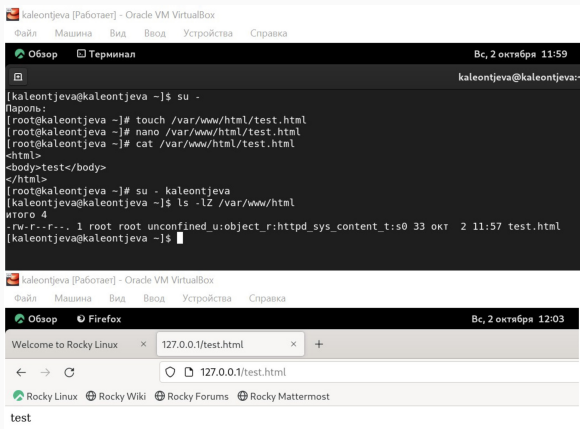


Figure 3: Рис.3: Создание файла и его просмотр в веб-сервере

Ход выполнения лабораторной работы

- Изменила контекст файла на samba_share_t. Попробовала получить доступ к файлу через веб-сервер и получила сообщение об ошибке

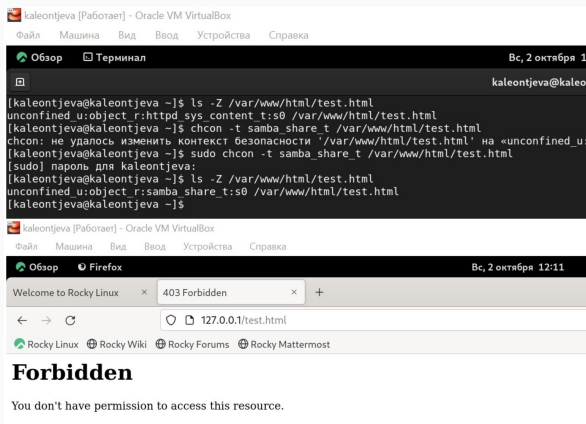
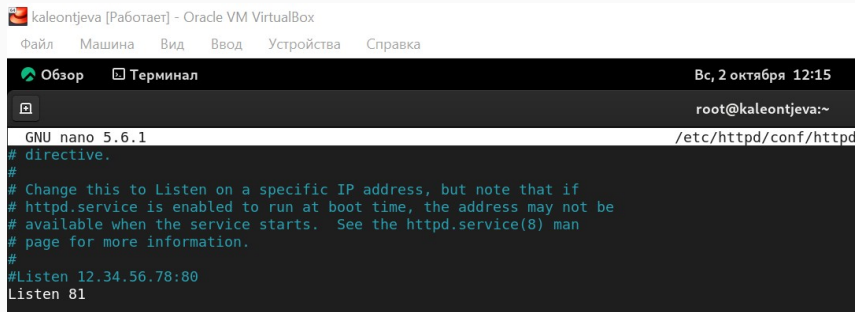


Figure 4: Рис.4: Изменение контекста и просмотр файла в веб-сервере

Ход выполнения лабораторной работы

- В файле `/etc/httpd/conf/httpd.conf` заменила строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81



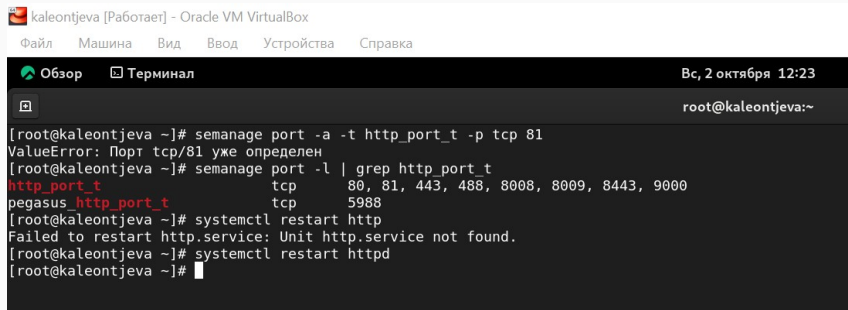
The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal interface includes a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar, there are tabs for "Обзор" and "Терминал", with the current time "Вс, 2 октября 12:15" displayed on the right. The terminal prompt is "root@kaleontjeva:~". The user has opened the file `/etc/httpd/conf/httpd.conf` using the nano text editor (GNU nano 5.6.1). The visible content of the file includes comments about listening on a specific IP address and the directive `#Listen 12.34.56.78:80`. The user has replaced this line with `Listen 81`.

```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 12:15
root@kaleontjeva:~
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

Figure 5: Рис.5: Установка веб-сервера Apache на прослушивание TCP-порта 81

- Выполнила команду “semanage port -a -t http_port_t -p tcp 81” и убедилась, что порт TCP-81 установлен. Проверила список доступных портов



The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[root@kaleontjeva ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kaleontjeva ~]# 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
[root@kaleontjeva ~]# systemctl restart http
Failed to restart http.service: Unit http.service not found.
[root@kaleontjeva ~]# systemctl restart httpd
[root@kaleontjeva ~]#
```

Figure 6: Рис.6: Проверка установки порта 81

Ход выполнения лабораторной работы

- Вернула контекст “httpd_sys_content_t” файлу test.html и попробовала получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”

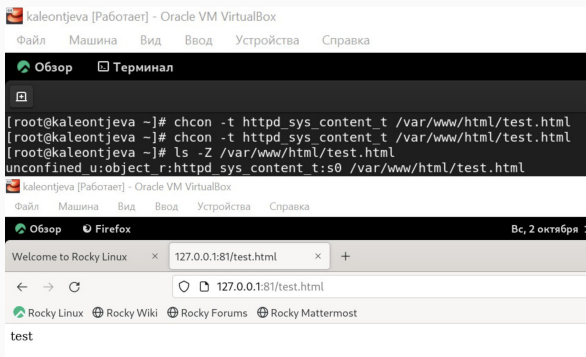


Figure 7: Рис.7: Возвращение исходного контекста файлу и просмотр файла в веб-сервере

- В ходе выполнения данной лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.