

Лабораторная №6

Основы информационной безопасности

Банникова Екатерина Алексеевна

Российский университет дружбы народов, Москва, Россия

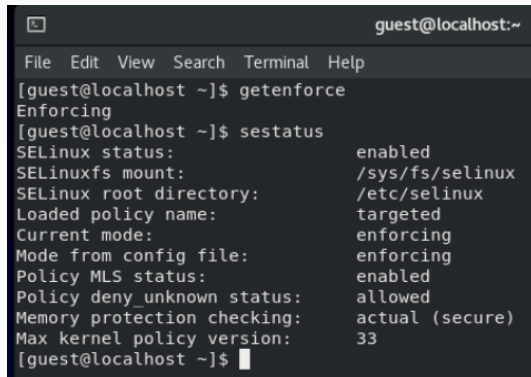
НПМбд-01-19

Мандатное разграничение прав в Linux

- Получить практические навыки администрирования
- Ознакомиться с технологией SELinux1

1. Запустить веб-сервер Apache
2. Создать файл test.html
3. Изменить контексты и порт прослушивания

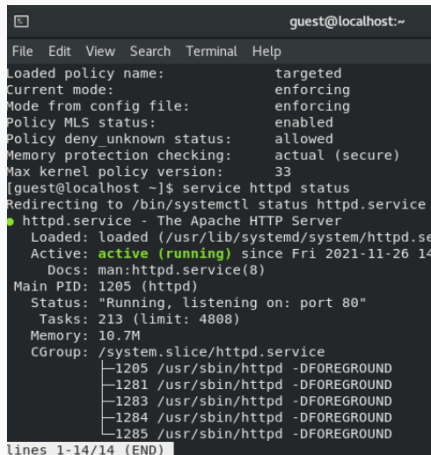
Вход в систему с полученными учётными данными. Проверка, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

A terminal window titled 'guest@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The user has entered two commands: 'getenforce' and 'sestatus'. The output of 'getenforce' is 'Enforcing'. The output of 'sestatus' is a multi-line status report.

```
guest@localhost:~  
File Edit View Search Terminal Help  
[guest@localhost ~]$ getenforce  
Enforcing  
[guest@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  
[guest@localhost ~]$
```

Figure 1: `getenforce` и `sestatus`

Обращение с помощью браузера к веб-серверу



```
guest@localhost:~  
File Edit View Search Terminal Help  
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  
[guest@localhost ~]$ service httpd status  
Redirecting to /bin/systemctl status httpd.service  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; vendor preset: enabled)  
   Active: active (running) since Fri 2021-11-26 14:00:00 MSK; 1min 12s ago  
     Docs: man:httpd.service(8)  
  Main PID: 1205 (httpd)  
    Status: "Running, listening on: port 80"  
   Tasks: 213 (limit: 4808)  
  Memory: 10.7M  
    CGroup: /system.slice/httpd.service  
            └─1205 /usr/sbin/httpd -DFOREGROUND  
              └─1281 /usr/sbin/httpd -DFOREGROUND  
                └─1283 /usr/sbin/httpd -DFOREGROUND  
                  └─1284 /usr/sbin/httpd -DFOREGROUND  
                    └─1285 /usr/sbin/httpd -DFOREGROUND  
lines 1-14/14 (END)
```

Figure 2: Работающий сервер

Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`

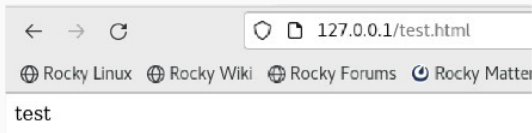


Figure 3: Просмотр файла в веб-браузере

Меняем контекст файла text.html. Перезагружаем страницу в веб-браузере.

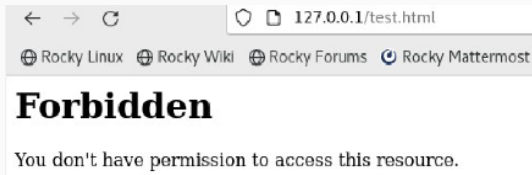


Figure 4: Сообщение об ошибке

Установила веб-сервер Apache на прослушивание TCP-порта 81, изменяя строку Listen

```
#  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default. See also the <VirtualHost>  
# directive.  
#  
# Change this to Listen on specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
#  
#Listen 12.34.56.78:80  
Listen 0.0.0.0:81
```

Figure 5: Прослушивание

Установила порт и посмотрела список доступных

```
http_port_t      tcp      80, 81, 443, 488, 8088, 8009, 8443, 9000  
pegasus_http_port_t tcp      5988
```

Figure 6: Удаление Sticky-бита

Просматриваем файл test.html в веб-браузере



Figure 7: Отсутствие Sticky-бита

- Развила навыки администрирования ОС Linux.
- Проверила работу SELinux на практике совместно с веб-сервером Apache.