

# Лабораторная работа №6

Мандатное разграничение прав в Linux

---

Логинов Егор Игоревич

13 октября 2023

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Логинов Егор Игоревич
- студент НФИбд-01-20
- Российский университет дружбы народов
- 1032201661@pfur.ru
- <https://github.com/Y0gu4t>

## Вводная часть

---

Логические объекты файловой системы (файлы) являются носителями своеобразных меток, которые привычно называют правами доступа. Некоторые метки действительно означают право выполнения определенного действия пользователя над этим объектом. Важно изучить их для дальнейшего применения на практике.

- Атрибуты файлов
- Дистрибутив Rocky
- Дискреционное разграничение доступа

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

## Выполнение работы

---



Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted

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

Рис. 1: Конфигурация SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает

```
[yegor@yegor ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[yegor@yegor ~]$ 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:07:28 MSK; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 41219 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12196)
    Memory: 32.3M
       CPU: 147ms
    CGroup: /system.slice/httpd.service
            └─41219 /usr/sbin/httpd -DFOREGROUND
              └─41228 /usr/sbin/httpd -DFOREGROUND
                └─41229 /usr/sbin/httpd -DFOREGROUND
                  └─41230 /usr/sbin/httpd -DFOREGROUND
                    └─41231 /usr/sbin/httpd -DFOREGROUND

окт 14 15:07:22 yegor.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 15:07:28 yegor.localdomain httpd[41219]: Server configured, listening on: port 80
окт 14 15:07:28 yegor.localdomain systemd[1]: Started The Apache HTTP Server.
[yegor@yegor ~]$
```

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности

```
[yegor@yegor ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 41219 0.1 0.5 20328 11508 ? Ss 15:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41228 0.0 0.3 21664 7296 ? S 15:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41229 0.0 0.7 2521332 15012 ? Sl 15:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41230 0.0 0.5 2324660 10920 ? Sl 15:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41231 0.0 0.6 2324660 12968 ? Sl 15:07 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 yegor 41490 0.0 0.1 221688 2384 pts/0 S+ 15:08 0:00 grep --color=auto h
[yegor@yegor ~]$
```

Рис. 3: Контекст безопасности веб-сервера Apache

Посмотрим текущее состояние переключателей SELinux для Apache

```
[yegor@yegor ~]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
```

Рис. 4: Текущее состояние переключателей SELinux для Apache

Посмотрим статистику по политике с помощью команды `seinfo`

```
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:                    5100   Attributes:              258
Users:                    8      Roles:                   14
Booleans:                 353    Cond. Expr.:            384
Allow:                    65000  Neverallow:              0
Auditallow:               170    Dontaudit:              8572
Type_trans:               265341 Type_change:              87
Type_member:              35     Range_trans:            6164
Role allow:               38     Role_trans:              420
Constraints:              70     Validatetrans:          0
MLS Constrain:           72     MLS Val. Tran:          0
Permissives:              2      Polcap:                  6
Defaults:                 7      Typebounds:              0
Allowxperm:               0      Neverallowxperm:        0
Auditallowxperm:          0      Dontauditxperm:         0
Ibendportcon:             0      Ibkeycon:                0
Initial SIDes:            27     Enforc:                  25
```

Определим тип файлов и поддиректорий, находящихся в директориях `/var/www` и `/var/www/html`. Определим круг пользователей, которым разрешено создание файлов в директории `/var/www/html`

```
[yegor@yegor ~]$ ls -lZ /var/www/  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23:21 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 23:21 html  
[yegor@yegor ~]$ ls -lZ /var/www/html/  
итого 0  
[yegor@yegor ~]$
```

Рис. 6: Тип файлов и поддиректорий, находящихся в директории `/var/www`

Создадим от имени суперпользователя html-файл `/var/www/html/test.html`. Проверим контекст созданного нами файла



```
[yegor@yegor ~]$ sudo su
[root@yegor yegor]# nano /var/www/html/test.html
[root@yegor yegor]# ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 14 15:13 test.ht
[root@yegor yegor]#
```

Рис. 7: Создание файла `/var/www/html/test.html`

Как видим по умолчанию присваивается контекст `unconfined_u:object_r:httpd_sys_content_t:s0`

Обратимся к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.  
Убедимся, что файл был успешно отображён

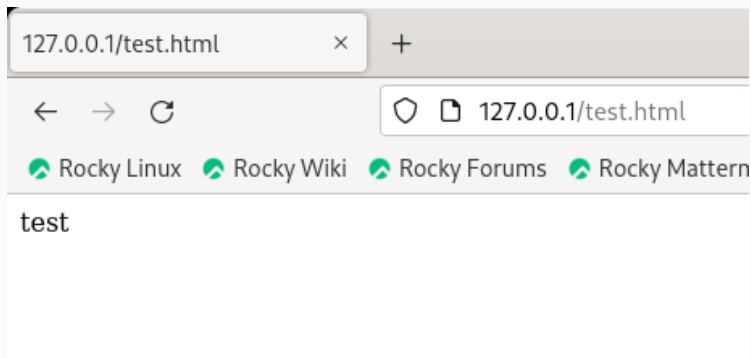



Рис. 8: Файл test.html в браузере




Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html`



```
[root@yegor yegor]# man selinux
[root@yegor yegor]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@yegor yegor]#
```

Рис. 9: Вызов справки

Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`



```
[root@yegor yegor]# chcon -t samba_share_t /var/www/html/test.html
[root@yegor yegor]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yegor yegor]#
```

Рис. 10: Изменение контекста

Попробуем ещё раз получить доступ к файлу через веб-сервер

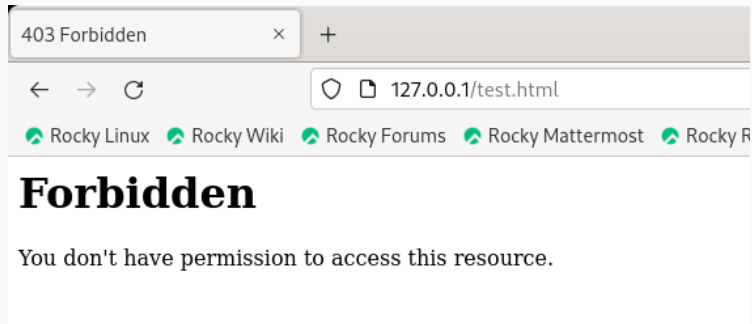
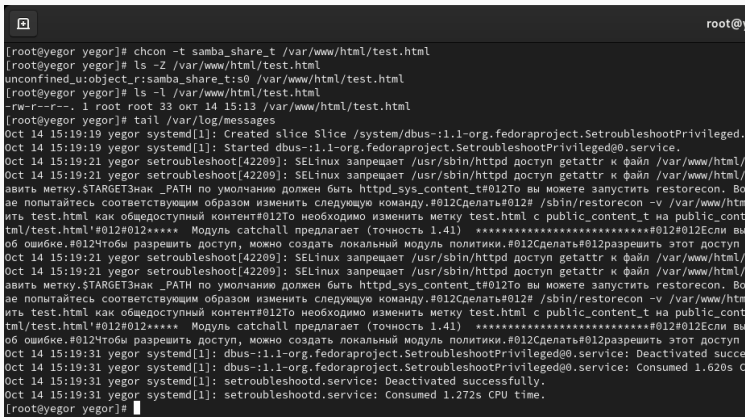


Рис. 11: Файл test.html в браузере после изменения контекста

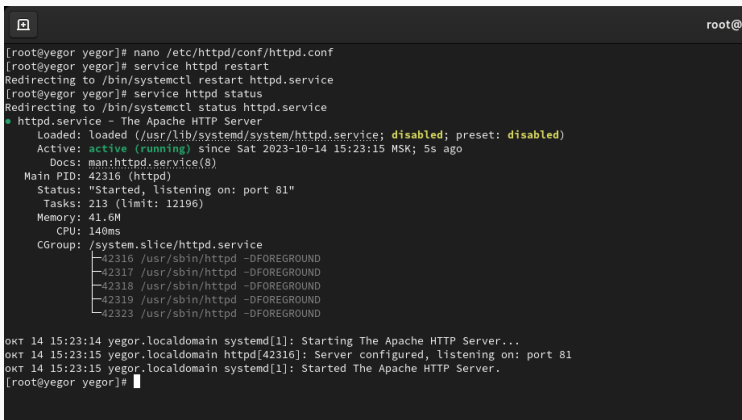
Посмотрим log-файлы веб-сервера Apache и системный лог-файл

A terminal window with a dark background and light text. The prompt is 'root@yegor'. The user enters several commands: 'chcon -t samba\_share\_t /var/www/html/test.html', 'ls -Z /var/www/html/test.html', 'ls -l /var/www/html/test.html', and 'tail /var/log/messages'. The output shows SELinux audit messages from 'setroubleshoot[42209]' regarding permissions for httpd and the 'restorecon' command being run. The terminal also shows systemd logs for the 'setroubleshootd.service' being deactivated and consumed CPU time.

```
root@yegor
[root@yegor yegor]# chcon -t samba_share_t /var/www/html/test.html
[root@yegor yegor]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yegor yegor]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 14 15:13 /var/www/html/test.html
[root@yegor yegor]# tail /var/log/messages
Oct 14 15:19:19 yegor systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 14 15:19:19 yegor systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
авить метку.$TARGET3знак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Bo
ae попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/hm
ить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_cont
tml/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы
об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
авить метку.$TARGET3знак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Bo
ae попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/hm
ить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_cont
tml/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы
об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ
Oct 14 15:19:31 yegor systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated succe
Oct 14 15:19:31 yegor systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.620s C
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Consumed 1.272s CPU time.
[root@yegor yegor]#
```

Рис. 12: Содержимое логов

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Выполним перезапуск веб-сервера. Сбоя не произошло

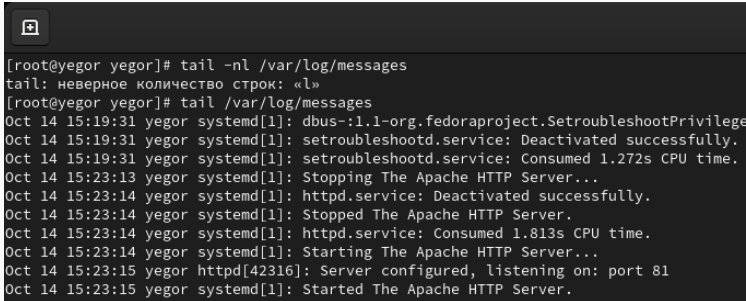
A terminal window with a dark background and light text. The prompt is root@yegor. The user enters 'nano /etc/httpd/conf/httpd.conf'. Then 'service httpd restart', which shows a redirection to 'systemctl restart httpd.service'. Then 'service httpd status', which shows a redirection to 'systemctl status httpd.service'. The status output shows 'httpd.service - The Apache HTTP Server' is loaded and active (running) since Sat 2023-10-14 15:23:15 MSK; 5s ago. It is listening on port 81. Below this, it lists the CGroup and the processes: 42316, 42317, 42318, 42319, and 42323, all running /usr/sbin/httpd -DFOREGROUND. At the bottom, there are three log messages from systemd: 'Starting The Apache HTTP Server...', 'Server configured, listening on: port 81', and 'Started The Apache HTTP Server.'.

```
root@yegor yegor# nano /etc/httpd/conf/httpd.conf
root@yegor yegor# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
root@yegor yegor# 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; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:23:15 MSK; 5s ago
     Docs: man:httpd.service(8)
   Main PID: 42316 (httpd)
    Status: "Started, listening on: port 81"
     Tasks: 213 (limit: 12196)
    Memory: 41.6M
       CPU: 140ms
   CGroup: /system.slice/httpd.service
           └─42316 /usr/sbin/httpd -DFOREGROUND
             └─42317 /usr/sbin/httpd -DFOREGROUND
               └─42318 /usr/sbin/httpd -DFOREGROUND
                 └─42319 /usr/sbin/httpd -DFOREGROUND
                   └─42323 /usr/sbin/httpd -DFOREGROUND

окт 14 15:23:14 yegor.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 15:23:15 yegor.localdomain httpd[42316]: Server configured, listening on: port 81
окт 14 15:23:15 yegor.localdomain systemd[1]: Started The Apache HTTP Server.
root@yegor yegor#
```

Рис. 13: Изменение содержимого файла /etc/httpd/httpd.conf

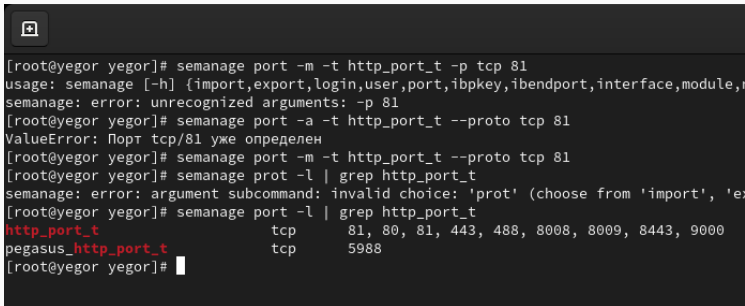
Проанализируем лог-файлы

A terminal window with a dark background and a light-colored border. The title bar is dark with a small icon on the left. The terminal text shows a sequence of commands and system messages. The first command is 'tail -nl /var/log/messages', which results in an error message. The second command is 'tail /var/log/messages', which displays a series of log entries from the system journal, including messages about dbus, setroubleshootd, and the Apache HTTP server.

```
[root@yegor yegor]# tail -nl /var/log/messages
tail: неверное количество строк: «1»
[root@yegor yegor]# tail /var/log/messages
Oct 14 15:19:31 yegor systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivilege
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Consumed 1.272s CPU time.
Oct 14 15:23:13 yegor systemd[1]: Stopping The Apache HTTP Server...
Oct 14 15:23:14 yegor systemd[1]: httpd.service: Deactivated successfully.
Oct 14 15:23:14 yegor systemd[1]: Stopped The Apache HTTP Server.
Oct 14 15:23:14 yegor systemd[1]: httpd.service: Consumed 1.813s CPU time.
Oct 14 15:23:14 yegor systemd[1]: Starting The Apache HTTP Server...
Oct 14 15:23:15 yegor httpd[42316]: Server configured, listening on: port 81
Oct 14 15:23:15 yegor systemd[1]: Started The Apache HTTP Server.
```

Рис. 14: Лог-файл tail -nl /var/log/messages

Выполним команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов командой `semanage port -l | grep http_port_t`. Убедимся, что порт 81 есть в списке.



```
[root@yegor yegor]# semmanage port -m -t http_port_t -p tcp 81
usage: semmanage [-h] {import,export,login,user,port,ibpkey,ibendport,interface,module,r
semanage: error: unrecognized arguments: -p 81
[root@yegor yegor]# semmanage port -a -t http_port_t --proto tcp 81
ValueError: Порт tcp/81 уже определен
[root@yegor yegor]# semmanage port -m -t http_port_t --proto tcp 81
[root@yegor yegor]# semmanage prot -l | grep http_port_t
semanage: error: argument subcommand: invalid choice: 'prot' (choose from 'import', 'ex
[root@yegor yegor]# semmanage port -l | grep http_port_t
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@yegor yegor]#
```

Рис. 15: Попытка добавления порта 81 в список и вывод списка допустимых портов


Попробуем запустить веб-сервер Apache ещё раз. Вернем контекст `httpd_sys_content__t` к файлу `/var/www/html/ test.html`. Попробуем получить доступ к файлу через веб-сервер

```
[root@yegor yegor]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@yegor yegor]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@yegor yegor]# 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; preset: disabled)
  Active: active (running) since Sat 2023-10-14 15:33:03 MSK; 4s ago
  Docs: man:httpd.service(8)
  Main PID: 42710 (httpd)
  Status: "Started, listening on: port 81"
  Tasks: 213 (limit: 12196)
  Memory: 35.6M
  CPU: 108ms
  CGroup: /system.slice/httpd.service
          └─42710 /usr/sbin/httpd -DFOREGROUND
            └─42711 /usr/sbin/httpd -DFOREGROUND
              └─42712 /usr/sbin/httpd -DFOREGROUND
                └─42713 /usr/sbin/httpd -DFOREGROUND
                  └─42714 /usr/sbin/httpd -DFOREGROUND

окт 14 15:33:03 yegor.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 15:33:03 yegor.localdomain httpd[42710]: Server configured, listening on: port 81
окт 14 15:33:03 yegor.localdomain systemd[1]: Started The Apache HTTP Server.
[root@yegor yegor]#
```



Исправим обратно конфигурационный файл apache, вернув Listen 80. Попробуем удалить привязку http\_port\_t к 81. Удалим файл /var/www/html/test.html



```
[root@yegor yegor]# nano /etc/httpd/conf/httpd.conf
[root@yegor yegor]# semanage port -d -t http_port_t -p tcp 81
[root@yegor yegor]# 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@yegor yegor]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@yegor yegor]#
```

Рис. 17: Попытка удаления привязки к порту 81

- В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux
- Получено первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверена работа SELinx на практике совместно с веб-сервером Apache