

# Лабораторная работа № 6

Основы информационной безопасности

---

Казазаев Д. М.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Казазаев Даниил Михайлович
- Студент бакалавриата
- Российский университет дружбы народов
- [1132231427@rudn.ru]
- [https://github.com/KazazaevDaniil/study\\_2024-2025\\_infosec-intro](https://github.com/KazazaevDaniil/study_2024-2025_infosec-intro)

## Вводная часть

---

Развитие навыков администрирования ОС Linux. Получение практических навыков в работе с технологией SELinux. Проверка работы SELinux совместно с Apache.

Для выполнения лабораторной работы мы воспользуемся виртуальной машиной Oracle VM Virtual Box. Лабораторные работы выполняются на домашнем оборудовании.

- Этапы работы
  - 1. Выполнение лабораторной работы.

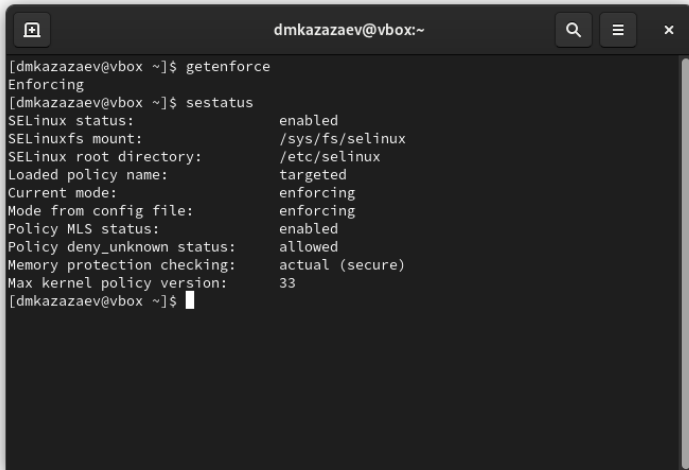
Выполнение лабораторной работы.

---



## Выполнение лабораторной работы.

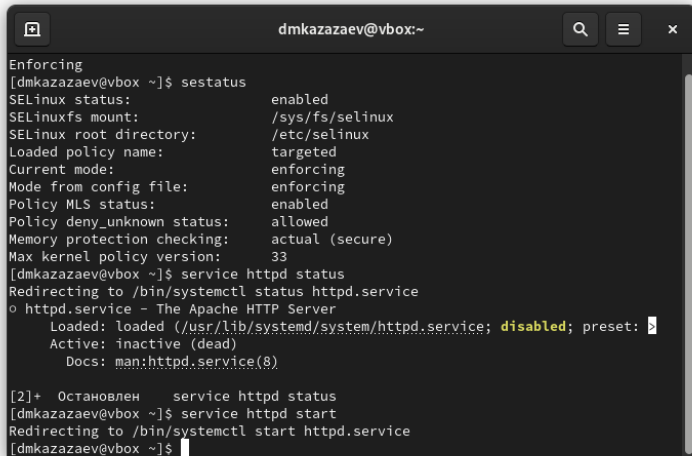
После запуска проверяю, работает-ли SELinux. (рис. 1)

A terminal window titled 'dmkazazae@vbox:~' with search, menu, and close buttons in the title bar. The terminal shows the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' shows SELinux is enabled, in enforcing mode, with various configuration details.

```
[dmkazazae@vbox ~]$ getenforce
Enforcing
[dmkazazae@vbox ~]$ 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
[dmkazazae@vbox ~]$
```

## Выполнение лабораторной работы.

Проверяю запущен-ли Apache. Так как он не запущен, запускаю его. (рис. 2)

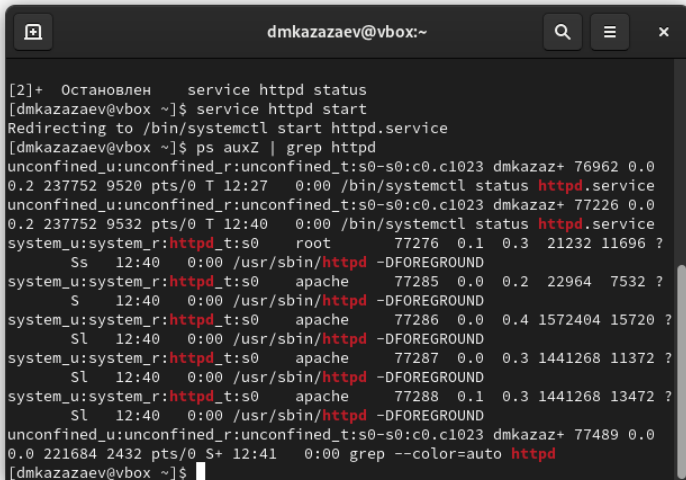
A terminal window titled 'dmkazazae@vbox:~' with search, menu, and close icons in the title bar. The terminal shows the output of 'sestatus' and 'service httpd status'. The SELinux status is enforcing. The Apache service is loaded but inactive (dead) and is disabled. The user then runs 'service httpd start' to start the service.

```
Enforcing
[dmkazazae@vbox ~]$ 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
[dmkazazae@vbox ~]$ 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: ▸)
   Active: inactive (dead)
   Docs: man:httpd.service(8)

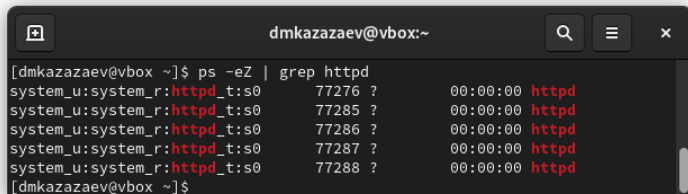
[2]+  Остановлен    service httpd status
[dmkazazae@vbox ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[dmkazazae@vbox ~]$
```

## Выполнение лабораторной работы.

Смотрю контекст безопасности веб-сервера Apache.(рис. 3)



```
dmkazazaev@vbox:~  
[2]+  Остановлен    service httpd status  
[dmkazazaev@vbox ~]$ service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[dmkazazaev@vbox ~]$ ps auxZ | grep httpd  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dmkazaz+ 76962 0.0  
0.2 237752 9520 pts/0 T 12:27  0:00 /bin/systemctl status httpd.service  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dmkazaz+ 77226 0.0  
0.2 237752 9532 pts/0 T 12:40  0:00 /bin/systemctl status httpd.service  
system_u:system_r:httpd_t:s0    root      77276  0.1  0.3  21232 11696 ?  
    Ss  12:40  0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0    apache   77285  0.0  0.2  22964  7532 ?  
    S  12:40  0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0    apache   77286  0.0  0.4 1572404 15720 ?  
    Sl 12:40  0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0    apache   77287  0.0  0.3 1441268 11372 ?  
    Sl 12:40  0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0    apache   77288  0.1  0.3 1441268 13472 ?  
    Sl 12:40  0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dmkazaz+ 77489 0.0  
0.0 221684 2432 pts/0 S+ 12:41  0:00 grep --color=auto httpd  
[dmkazazaev@vbox ~]$
```

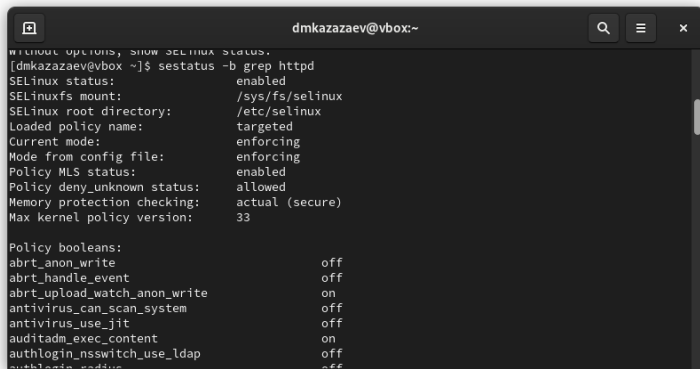


```
dmkazazaev@vbox:~  
[dmkazazaev@vbox ~]$ ps -eZ | grep httpd  
system_u:system_r:httpd_t:s0      77276 ?        00:00:00 httpd  
system_u:system_r:httpd_t:s0      77285 ?        00:00:00 httpd  
system_u:system_r:httpd_t:s0      77286 ?        00:00:00 httpd  
system_u:system_r:httpd_t:s0      77287 ?        00:00:00 httpd  
system_u:system_r:httpd_t:s0      77288 ?        00:00:00 httpd  
[dmkazazaev@vbox ~]$
```

Рис. 4: Контекст безопасности

## Выполнение лабораторной работы.

Смотрю состояние переключателей SELinux.(рис. 5)



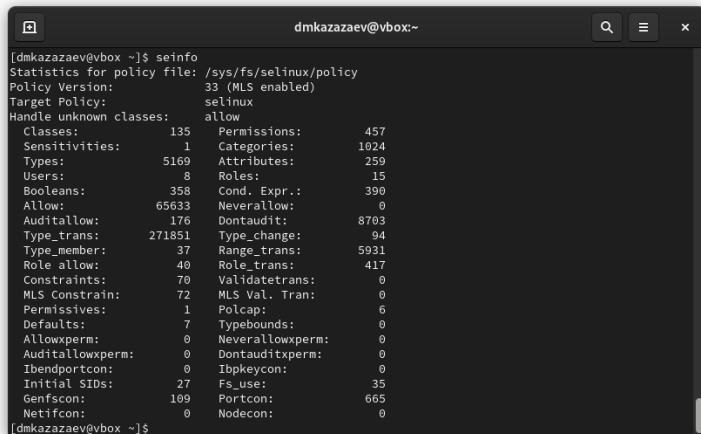
```
without options, show SELinux status.
[dmkazazaev@vbox ~]$ sestatus -b grep httpd
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
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                off
abrt_upload_watch_anon_write    on
antivirus_can_scan_system       off
antivirus_use_jit               off
auditadm_exec_content           on
authlogin_nsswitch_use_ldap     off
authlogin_radius                off
```

Рис. 5: Состояние переключателей

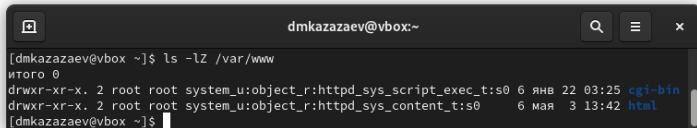
## Выполнение лабораторной работы.

Смотрю статистику по политике SELinux.(рис. 6)



```
dmkazazaev@vbox:~  
[dmkazazaev@vbox ~]$ 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: 5169 Attributes: 259  
Users: 8 Roles: 15  
Booleans: 358 Cond. Expr.: 390  
Allow: 65633 Neverallow: 0  
Auditallow: 176 Dontaudit: 8703  
Type_trans: 271851 Type_change: 94  
Type_member: 37 Range_trans: 5931  
Role allow: 40 Role_trans: 417  
Constraints: 70 Validatetrans: 0  
MLS Constrains: 72 MLS Val. Tran: 0  
Permissives: 1 Polcap: 6  
Defaults: 7 Typebounds: 0  
Allowxperm: 0 Neverallowxperm: 0  
Auditallowxperm: 0 Dontauditxperm: 0  
Ibendportcon: 0 Ibkeycon: 0  
Initial SIDs: 27 Fs_use: 35  
Genfscon: 109 Portcon: 665  
Netifcon: 0 Nodecon: 0  
[dmkazazaev@vbox ~]$
```

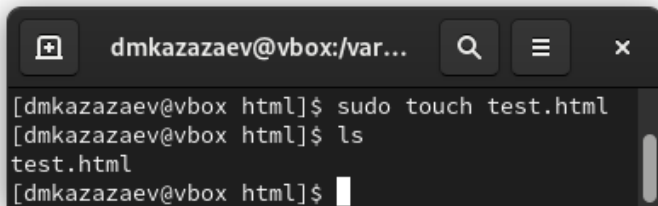
Смотрю, какие типы файлов есть в директории `/var/www` и права доступа к этим файлам.(рис. 7)



```
dmkazazae@vbox:~  
[dmkazazae@vbox ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 янв 22 03:25 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 3 13:42 html  
[dmkazazae@vbox ~]$
```

Рис. 7: Контекст файлов в директории

Создаю html файл в /var/www/html.(рис. 8)

A terminal window with a dark background. The title bar shows a plus icon, the text 'dmkazazaev@vbox:/var...', a search icon, a menu icon, and a close icon. The terminal content shows the user 'dmkazazaev' in the directory 'html' executing 'sudo touch test.html', then 'ls', which lists 'test.html', and finally a new prompt line.

```
[dmkazazaev@vbox html]$ sudo touch test.html  
[dmkazazaev@vbox html]$ ls  
test.html  
[dmkazazaev@vbox html]$
```

Рис. 8: Создание html файла



Переношу простую программу в созданный файл.(рис. 9)

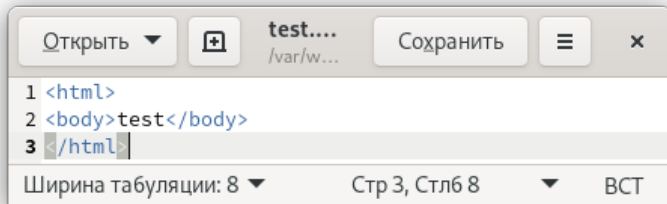
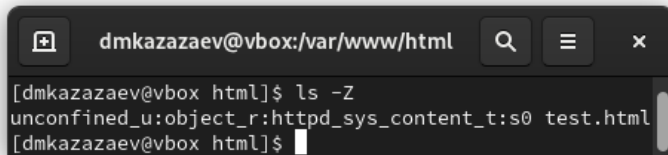


Рис. 9: Код программы

Проверяю контекст нового файла.(рис. 10)

A terminal window with a dark background. The title bar shows a window icon, the text 'dmkazazaev@vbox:/var/www/html', a search icon, a menu icon, and a close icon. The terminal content shows the command 'ls -Z' being executed, resulting in the output 'unconfined\_u:object\_r:httpd\_sys\_content\_t:s0 test.html'. The prompt is '[dmkazazaev@vbox html]\$' followed by a cursor.

```
[dmkazazaev@vbox html]$ ls -Z
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[dmkazazaev@vbox html]$
```

Рис. 10: Контекст нового файла

По умолчанию присваивается контекст вида

```
unconfident_u:object_r:httpd_sys_content_t:s0
```

Запускаю тестовый файл в веб-сервисе. (рис. 11)

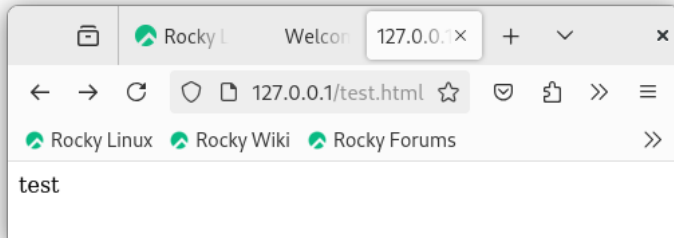
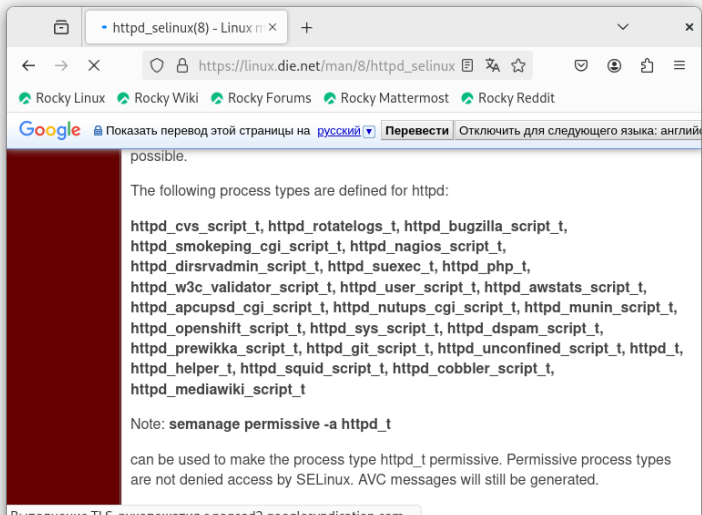


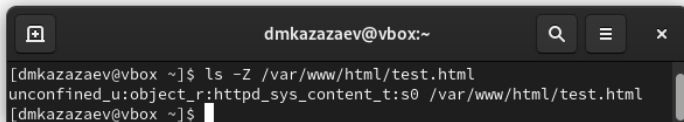
Рис. 11: Запущенный тестовый файл

## Выполнение лабораторной работы.

Изучаю, какие контексты могут быть присвоенный файлам. (рис. 12)



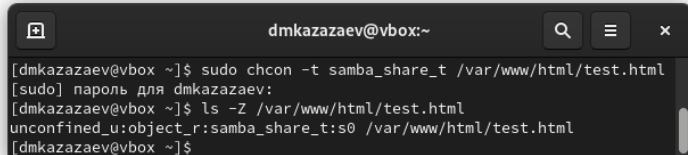
Детальнее изучаю контекст созданного файла. (рис. 13)

A terminal window with a dark background. The title bar shows 'dmkazazae@vbox:~' and standard window controls. The terminal content shows a command to list file details for a specific HTML file, followed by the output showing the SELinux context.

```
dmkazazae@vbox:~  
[dmkazazae@vbox ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[dmkazazae@vbox ~]$
```

Рис. 13: Контекст созданного файла

Меняю контекст файла на `samba_share_t`. (рис. 14)



```
dmkazazaev@vbox:~  
[dmkazazaev@vbox ~]$ sudo chcon -t samba_share_t /var/www/html/test.html  
[sudo] пароль для dmkazazaev:  
[dmkazazaev@vbox ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[dmkazazaev@vbox ~]$
```

Рис. 14: Меняю контекст

## Выполнение лабораторной работы.

После смены контекста перезапускаю веб-сервис. При попытке запуска файла выводится ошибка прав доступа. (рис. 15)

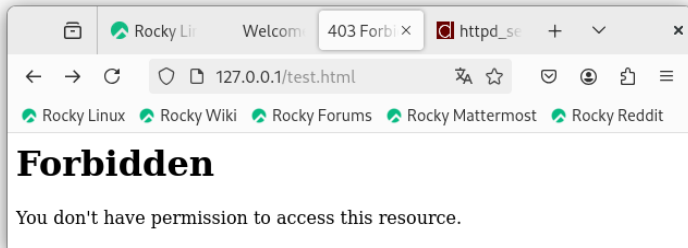
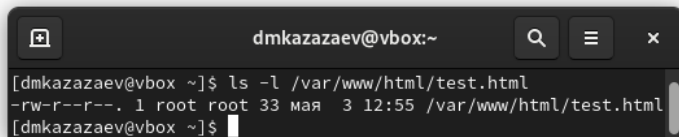


Рис. 15: Запуск файла с новым контекстом



Недостаток доступа обусловлен тем, что новый контекст не публичный.

Проверяю права доступа html файла. (рис. 16)



```
dmkazazaev@vbox:~  
[dmkazazaev@vbox ~]$ ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 мая  3 12:55 /var/www/html/test.html  
[dmkazazaev@vbox ~]$
```

Рис. 16: Проверка прав доступа

## Выполнение лабораторной работы.

В конфиг файле Apache меняю прослушивание TCP-порта на 81. (рис. 17)

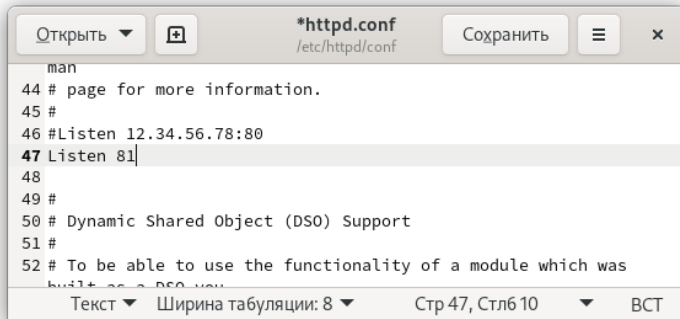
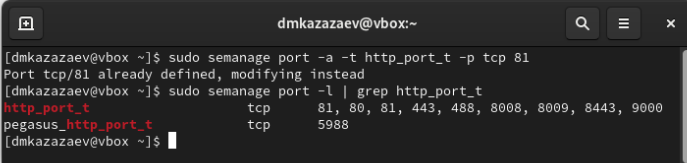


Рис. 17: Смена TCP-порта

Добавляю новый TCP-порт. (рис. 18)

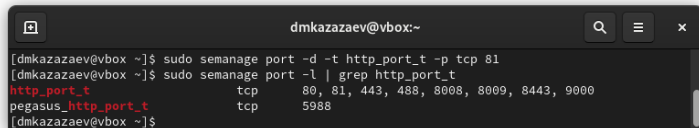


```
dmkazazaev@vbox:~  
[dmkazazaev@vbox ~]$ sudo semanage port -a -t http_port_t -p tcp 81  
Port tcp/81 already defined, modifying instead  
[dmkazazaev@vbox ~]$ sudo semanage port -l | grep http_port_t  
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus_http_port_t  tcp      5988  
[dmkazazaev@vbox ~]$
```

Рис. 18: Добавление и проверка

После добавление 81-го порта сайт должен был запускаться, но у меня этого не произошло.

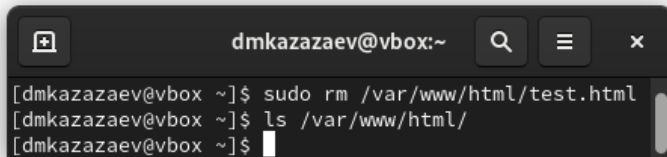
Удаляю новый порт. (рис. 19)



```
dmkazazae@vbox:~  
[dmkazazae@vbox ~]$ sudo semanage port -d -t http_port_t -p tcp 81  
[dmkazazae@vbox ~]$ 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  
[dmkazazae@vbox ~]$
```

Рис. 19: Удаление и проверка

Удаляю созданный в ходе лабораторной работы html файл. (рис. 20)

A terminal window with a dark background. The title bar shows a window icon, the text 'dmkazazaev@vbox:~', a search icon, a menu icon, and a close icon. The terminal content shows three lines of commands and their outputs: the first line is 'sudo rm /var/www/html/test.html', the second line is 'ls /var/www/html/' followed by a blank line, and the third line is a prompt with a cursor.

```
[dmkazazaev@vbox ~]$ sudo rm /var/www/html/test.html  
[dmkazazaev@vbox ~]$ ls /var/www/html/  
[dmkazazaev@vbox ~]$
```

Рис. 20: Удаление и проверка

## Вывод

---



В ходе лабораторной работы я познакомился с администрированием ОС Linux. Получил практические навыки в работе с технологией SELinux. Проверил работу SELinux совместно с Apache.