

# **Отчет по лабораторной работе № 6**

**Дисциплина: основы информационной безопасности**

Казазаев Даниил Михайлович

# Содержание

1	Цель работы	4
2	Выполнение лабораторной работы.	5
3	Вывод	13

## Список иллюстраций

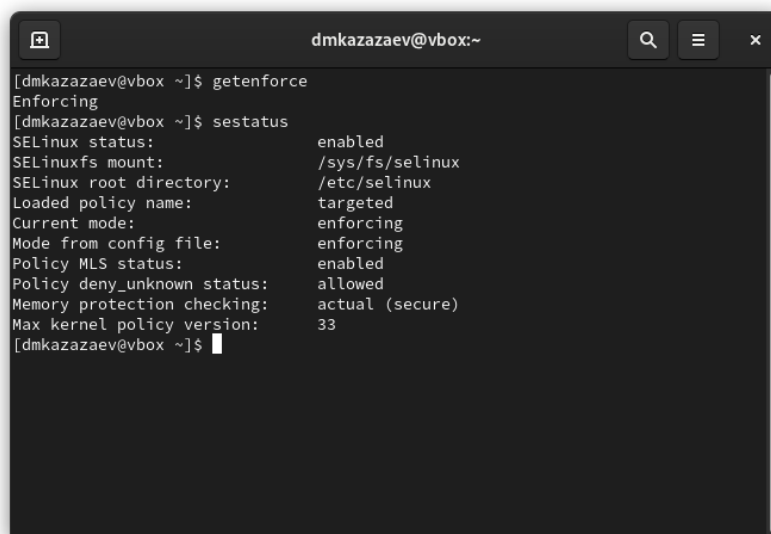
2.1	Информация о SELinux . . . . .	5
2.2	Проверка и запуск Apache . . . . .	6
2.3	Контекст безопасности . . . . .	6
2.4	Контекст безопасности . . . . .	7
2.5	Состояние переключателей . . . . .	7
2.6	Статистика по политике . . . . .	8
2.7	Контекст файлов в директории . . . . .	8
2.8	Создание html файла . . . . .	8
2.9	Код программы . . . . .	9
2.10	Контекст нового файла . . . . .	9
2.11	Запущенный тестовый файл . . . . .	9
2.12	Справка по контекстам . . . . .	10
2.13	Контекст созданного файла . . . . .	10
2.14	Меняю контекст . . . . .	10
2.15	Запуск файла с новым контекстом . . . . .	11
2.16	Проверка прав доступа . . . . .	11
2.17	Смена ТСП-порта . . . . .	11
2.18	Добавление и проверка . . . . .	12
2.19	Удаление и проверка . . . . .	12
2.20	Удаление и проверка . . . . .	12

# 1 Цель работы

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

## 2 Выполнение лабораторной работы.

После запуска проверяю, работает-ли SELinux. (рис. 2.1)

A terminal window titled 'dmkazazaev@vbox:~' with search, menu, and close buttons in the title bar. The terminal shows the command 'getenforce' being executed, returning 'Enforcing'. Then, the command 'sestatus' is executed, displaying a detailed status report for SELinux.

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

Рис. 2.1: Информация о SELinux

Проверяю запущен-ли Apache. Так как он не запущен, запускаю его. (рис. 2.2)

```
dmkazazaev@vbox:~$ sestatus
Enforcing
[dmkazazaev@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
[dmkazazaev@vbox ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
o httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset:
   Active: inactive (dead)
   Docs: man:httpd.service(8)

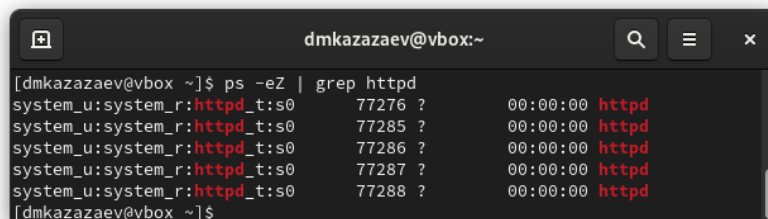
[2]+  Остановлен service httpd status
[dmkazazaev@vbox ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[dmkazazaev@vbox ~]$
```

Рис. 2.2: Проверка и запуск Apache

Смотрю контекст безопасности веб-сервера Apache.(рис. 2.3)

```
[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 ~]$
```

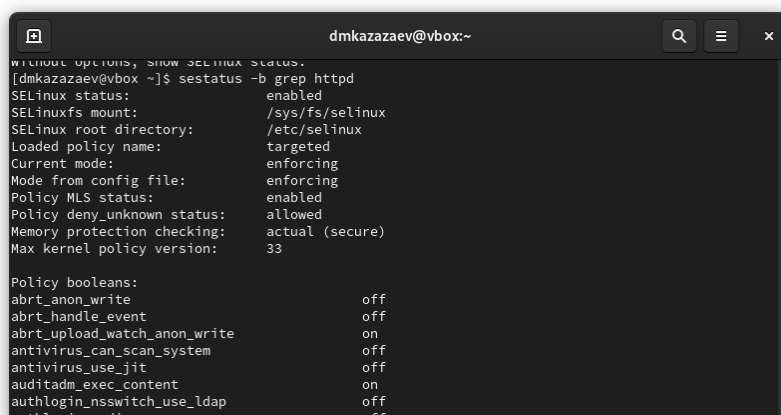
Рис. 2.3: Контекст безопасности



```
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. 2.4: Контекст безопасности

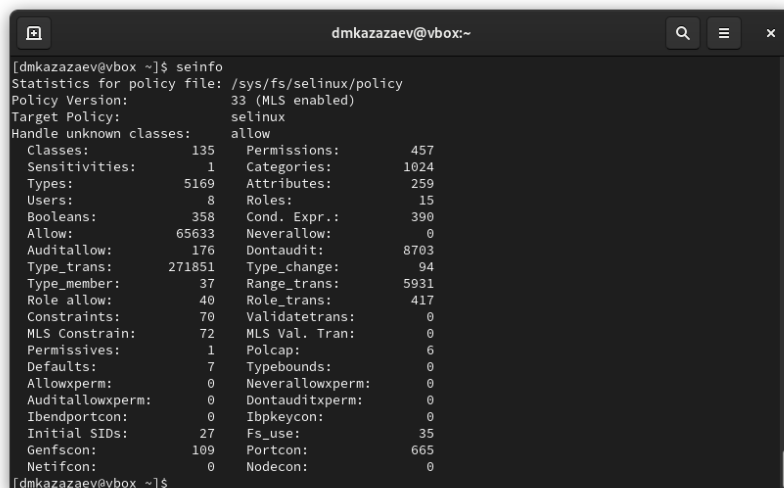
Смотрю состояние переключателей SELinux.(рис. 2.5)



```
dmkazazaev@vbox:~  
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. 2.5: Состояние переключателей

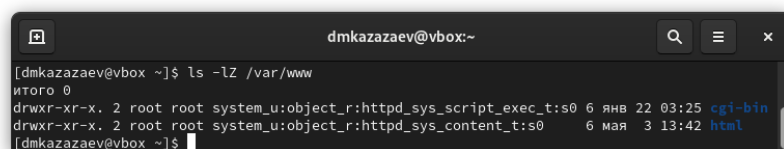
Смотрю статистику по политике SELinux.(рис. 2.6)



```
dmkazazaev@vbox:~$ seinfo
[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_Constrain: 72 MLS_Val. Tran: 0
Permissives: 1 Polcap: 6
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial_SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0
[dmkazazaev@vbox ~]$
```

Рис. 2.6: Статистика по политеке

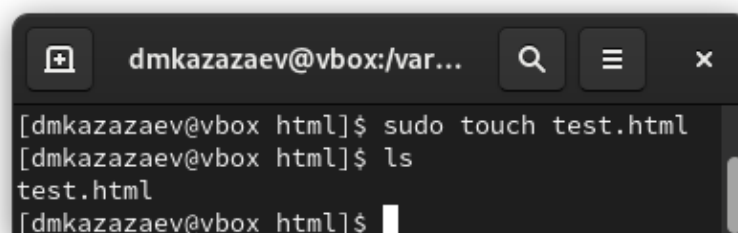
Смотрю, какие типы файлов есть в директории /var/www и права доступа к этим файлам.(рис. 2.7)



```
dmkazazaev@vbox:~$ ls -lZ /var/www
[dmkazazaev@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
[dmkazazaev@vbox ~]$
```

Рис. 2.7: Контекст файлов в директории

Создаю html файл в /var/www/html.(рис. 2.8)



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

Рис. 2.8: Создание html файла

Переношу простую программу в созданный файл.(рис. 2.9)



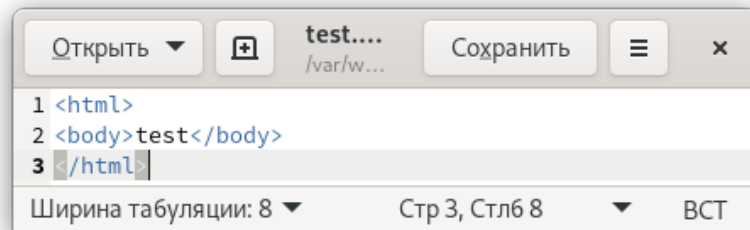


Рис. 2.9: Код программы

Проверяю контекст нового файла.(рис. 2.10)

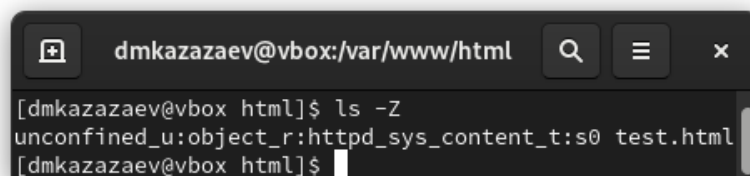


Рис. 2.10: Контекст нового файла

По умолчанию присваивается контекст вида unconfident\_u:object\_r:httpd\_sys\_content\_t  
Запускаю тестовый файл в веб-сервисе. (рис. 2.11)

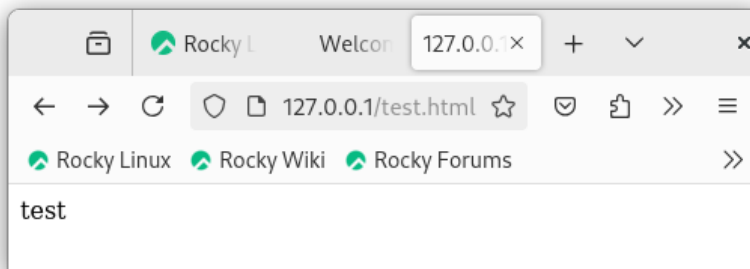


Рис. 2.11: Запущенный тестовый файл

Изучаю, какие контексты могут быть присвоены файлам. (рис. 2.12)

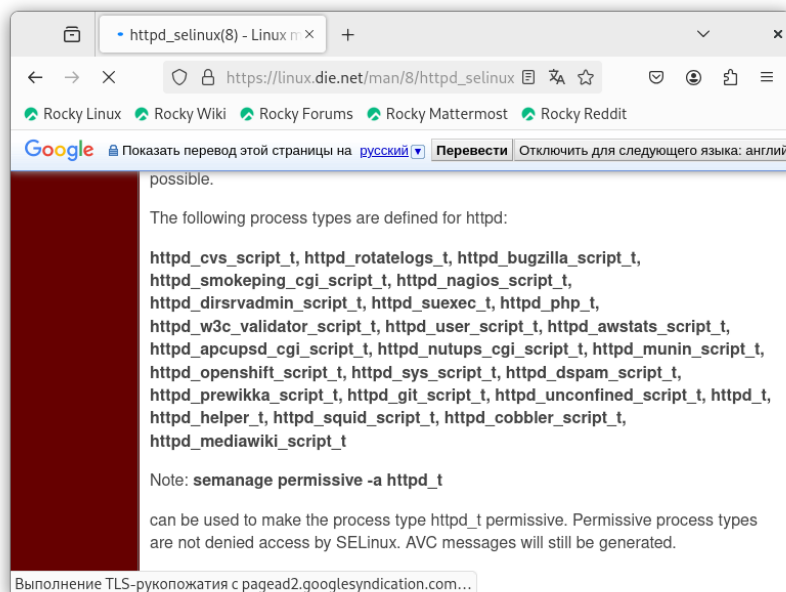


Рис. 2.12: Справка по контекстам

Детальнее изучаю контекст созданного файла. (рис. 2.13)

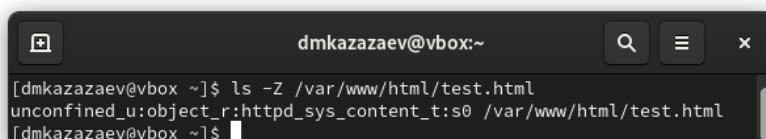


Рис. 2.13: Контекст созданного файла

Меняю контекст файла на samba\_share\_t. (рис. 2.14)

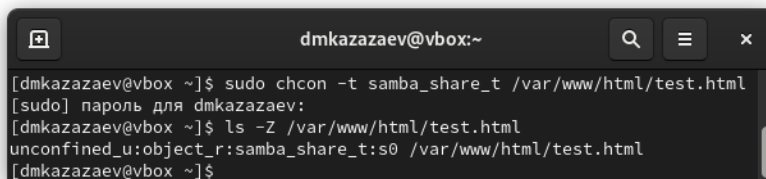


Рис. 2.14: Меняю контекст

После сменя контекста перезапускаю веб-сервис. При попытке запуска файла выводится ошибка прав доступа. (рис. 2.15)

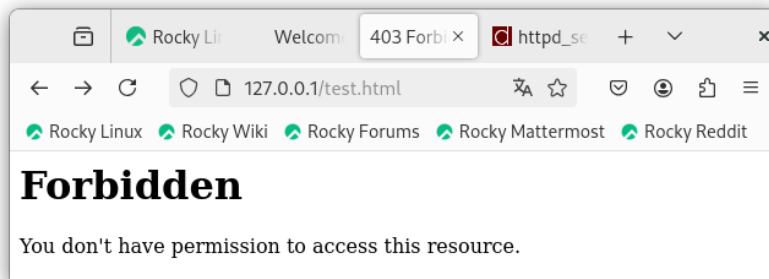


Рис. 2.15: Запуск файла с новым контекстом

Недостаток доступа обусловлен тем, что новый контекст непубличный. Проверяю права доступа html файла. (рис. 2.16)

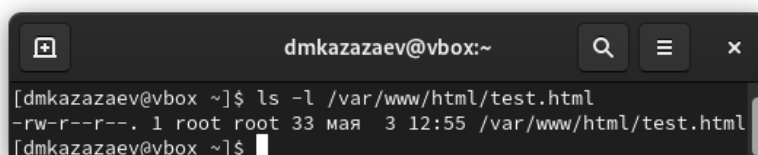


Рис. 2.16: Проверка прав доступа

В конфиг файле Apache меняю прослушивание TCP-порта на 81. (рис. 2.17)

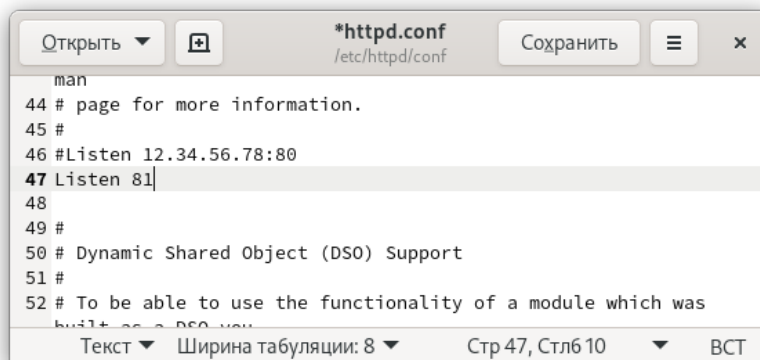
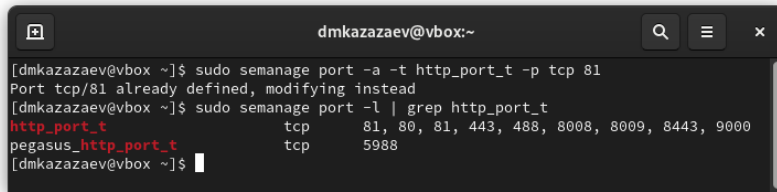


Рис. 2.17: Смена TCP-порта

Добавляю новый TCP-порт. (рис. 2.18)

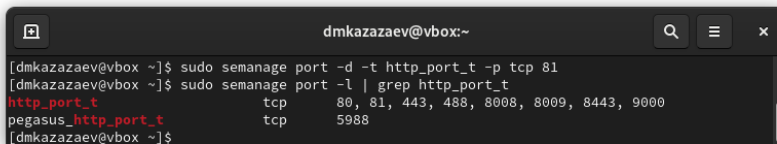


```
dmkazazaev@vbox:~  
[dmkazazaev@vbox ~]$ sudo semanage port -a -t http_port_t -p tcp 81  
Port tcp/81 already defined, modifying instead  
[dmkazazaev@vbox ~]$ sudo semanage port -l | grep http_port_t  
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus_http_port_t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

Рис. 2.18: Добавление и проверка

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

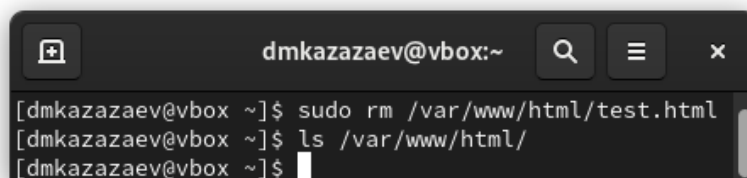
Удаляю новый порт. (рис. 2.19)



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

Рис. 2.19: Удаление и проверка

Удаляю созданный в ходе лабораторной работы html файл. (рис. 2.20)



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

Рис. 2.20: Удаление и проверка

## **3 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.