

# **Отчёт по лабораторной работе 6**

**Мандатное разграничение прав в Linux**

Максимова Ксения НБИбд-02-18

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>6</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>21</b>
	<b>Список литературы</b>	<b>22</b>

# List of Figures

4.1	Рис 1.Режиме enforcing . . . . .	8
4.2	Рис 2.Проверка . . . . .	9
4.3	Рис 3.Список процессов . . . . .	10
4.4	Рис 4.Текущее состояние . . . . .	11
4.5	Рис 5.Статистика . . . . .	12
4.6	Рис 6.Директория “/var/www” . . . . .	13
4.7	Рис 7.Директория “/var/www/html” . . . . .	14
4.8	Рис 7.Директория “/var/www/html” . . . . .	15
4.9	Рис 8.html-файл . . . . .	15
4.10	Рис 8.html-файл . . . . .	16
4.11	Рис 9.Файл . . . . .	17
4.12	Рис 10.Контексты файлов . . . . .	18
4.13	Рис 11.Изменение контекста файла . . . . .	19
4.14	Рис 12.Изменение контекста файла . . . . .	20

# 1 Цель работы

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

## 2 Задание

Установить веб-сервер Apache и проверить на нем работу SELinux.

### 3 Теоретическое введение

SELinux (Security-Enhanced Linux) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа[1]. В SELinux права доступа определяются самой системой при помощи специально определенных политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux. Иными словами, через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа[1].

Основные понятия [1]

1. Домен — это некоторый набор действий, которые может производить один процесс. Главным образом это действия, необходимые процессу для выполнения определенной задачи.
2. Роль — это совокупность нескольких доменов.
3. Контекст безопасности — это совокупность всех атрибутов, которые связаны с объектами и субъектами.
4. Политика безопасности — это набор заданных правил, который регулирует взаимодействие ролей, доменов.

Security Enhanced Linux может работать различными способами[2]:

- Enforcing: SELinux запрещает доступ на основе правил политики SELinux, набора руководящих принципов, которые управляют механизмом безопасности.

- Permissive: SELinux не запрещает доступ, но в журнале регистрируются отказы для действий, которые были бы запрещены при запуске в принудительном режиме.
- Disabled: Полное отключение системы принудительного контроля доступа

SELinux предоставляет следующие модели управления доступом[3]:

1. Type Enforcement (TE): основной механизм контроля доступа, используемый в целевых политиках. Позволяет детально, на самом низком уровне управлять разрешениями. Самый гибкий, но и самый трудоемкий для системного администратора механизм.
2. Role-Based Access Control (RBAC): в этой модели права доступа реализуются в качестве ролей. Ролью называется разрешения на выполнение определенных действий одним или несколькими элементами системы над другими частями системы. По-сути, RBAC является дальнейшим развитием TE.
3. Multi-Level Security (MLS): многоуровневая модель безопасности, в которой всем объектам системы присваивается определенный уровень доступа. Разрешение или запрет доступа определяется только соотношением этих уровней.

## 4 Выполнение лабораторной работы

1. Убедитесь, что SELinux работает в режиме enforcing политики targeted.

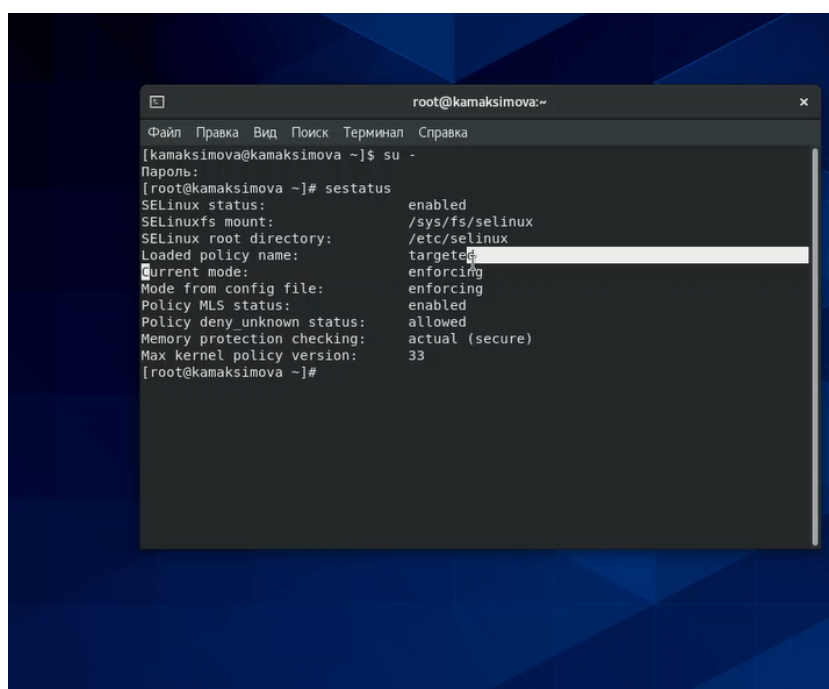
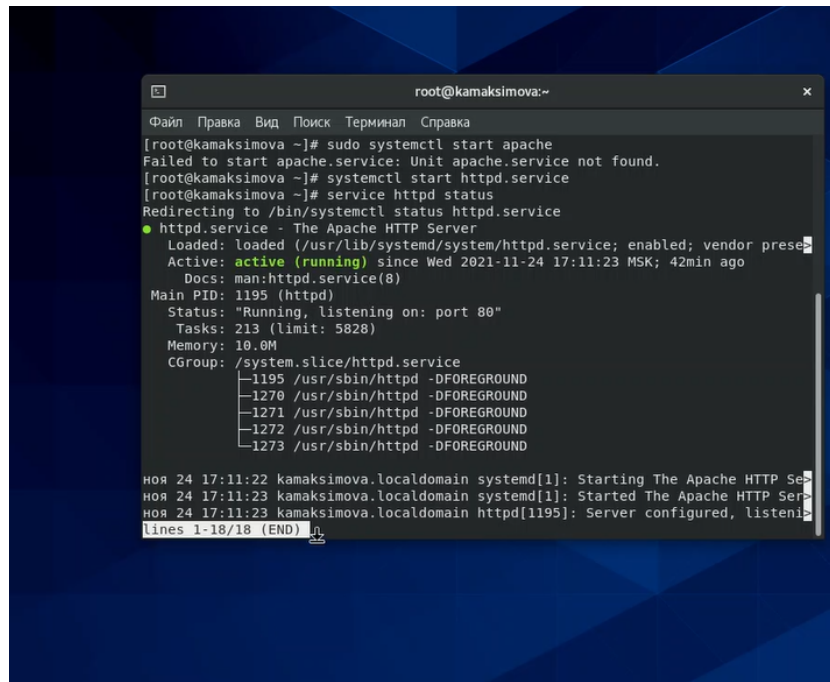


Figure 4.1: Рис 1.Режиме enforcing

Рисунок 1

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает.



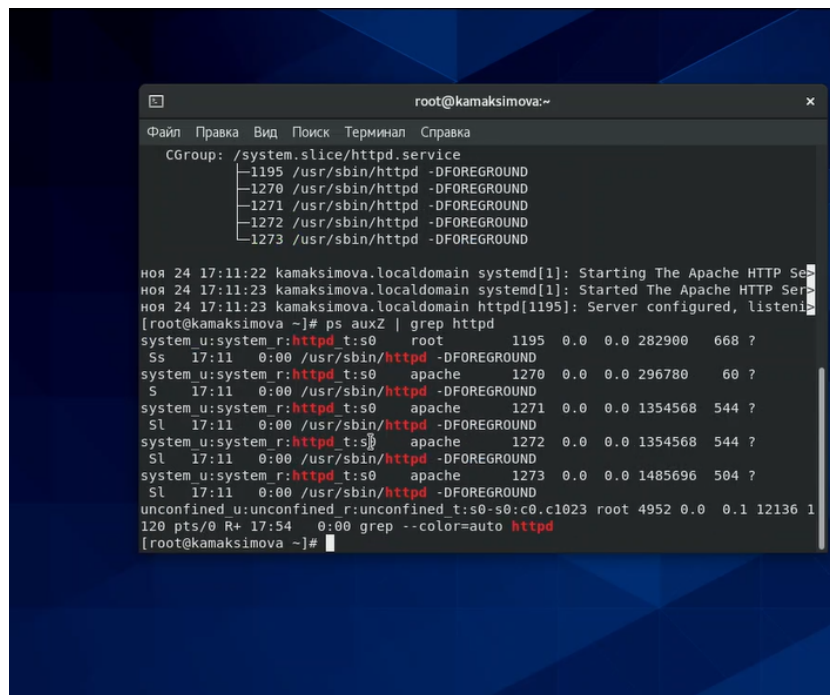


```
root@kamaksimova:~  
Файл Правка Вид Поиск Терминал Справка  
[root@kamaksimova ~]# sudo systemctl start apache  
Failed to start apache.service: Unit apache.service not found.  
[root@kamaksimova ~]# systemctl start httpd.service  
[root@kamaksimova ~]# service httpd status  
Redirecting to /bin/systemctl status httpd.service  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese  
   Active: active (running) since Wed 2021-11-24 17:11:23 MSK; 42min ago  
     Docs: man:httpd.service(8)  
  Main PID: 1195 (httpd)  
    Status: "Running, listening on: port 80"  
   Tasks: 213 (limit: 5828)  
  Memory: 10.0M  
    CGroup: /system.slice/httpd.service  
            └─1195 /usr/sbin/httpd -DFOREGROUND  
              └─1270 /usr/sbin/httpd -DFOREGROUND  
                └─1271 /usr/sbin/httpd -DFOREGROUND  
                  └─1272 /usr/sbin/httpd -DFOREGROUND  
                    └─1273 /usr/sbin/httpd -DFOREGROUND  
  
ноя 24 17:11:22 kamaksimova.localdomain systemd[1]: Starting The Apache HTTP Ser  
ноя 24 17:11:23 kamaksimova.localdomain systemd[1]: Started The Apache HTTP Ser  
ноя 24 17:11:23 kamaksimova.localdomain httpd[1195]: Server configured, listeni  
lines 1-18/18 (END) ↵
```

Figure 4.2: Рис 2.Проверка

Рисунок 2

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности.



```
root@kamaksimova:~  
Файл Правка Вид Поиск Терминал Справка  
CGroup: /system.slice/httpd.service  
├─1195 /usr/sbin/httpd -DFOREGROUND  
├─1270 /usr/sbin/httpd -DFOREGROUND  
├─1271 /usr/sbin/httpd -DFOREGROUND  
├─1272 /usr/sbin/httpd -DFOREGROUND  
└─1273 /usr/sbin/httpd -DFOREGROUND  
ноя 24 17:11:22 kamaksimova.localdomain systemd[1]: Starting The Apache HTTP Se  
ноя 24 17:11:23 kamaksimova.localdomain systemd[1]: Started The Apache HTTP Ser  
ноя 24 17:11:23 kamaksimova.localdomain httpd[1195]: Server configured, listeni  
[root@kamaksimova ~]# ps auxZ | grep httpd  
system u:system r:httpd t:s0 root 1195 0.0 0.0 282900 668 ?  
Ss 17:11 0:00 /usr/sbin/httpd -DFOREGROUND  
system u:system r:httpd t:s0 apache 1270 0.0 0.0 296780 60 ?  
S 17:11 0:00 /usr/sbin/httpd -DFOREGROUND  
system u:system r:httpd t:s0 apache 1271 0.0 0.0 1354568 544 ?  
Sl 17:11 0:00 /usr/sbin/httpd -DFOREGROUND  
system u:system r:httpd t:s0 apache 1272 0.0 0.0 1354568 544 ?  
Sl 17:11 0:00 /usr/sbin/httpd -DFOREGROUND  
system u:system r:httpd t:s0 apache 1273 0.0 0.0 1485696 504 ?  
Sl 17:11 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 4952 0.0 0.1 12136 1  
120 pts/0 R+ 17:54 0:00 grep --color=auto httpd  
[root@kamaksimova ~]#
```

Figure 4.3: Рис 3.Список процессов

Рисунок 3

4. Посмотрите текущее состояние переключателей SELinux для Apache

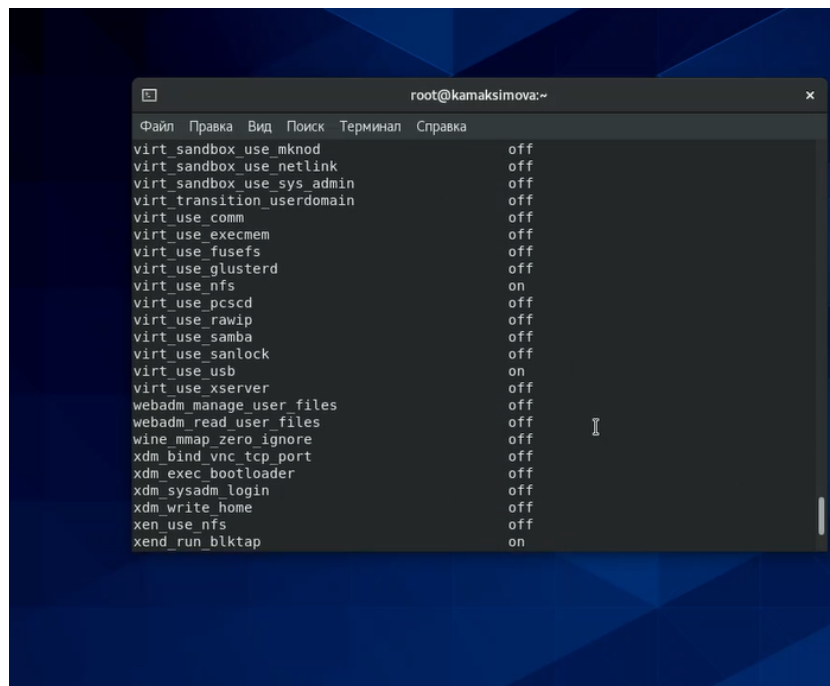


Figure 4.4: Рис 4.Текущее состояние

Рисунок 4

Многие из них находятся в положении «off».

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

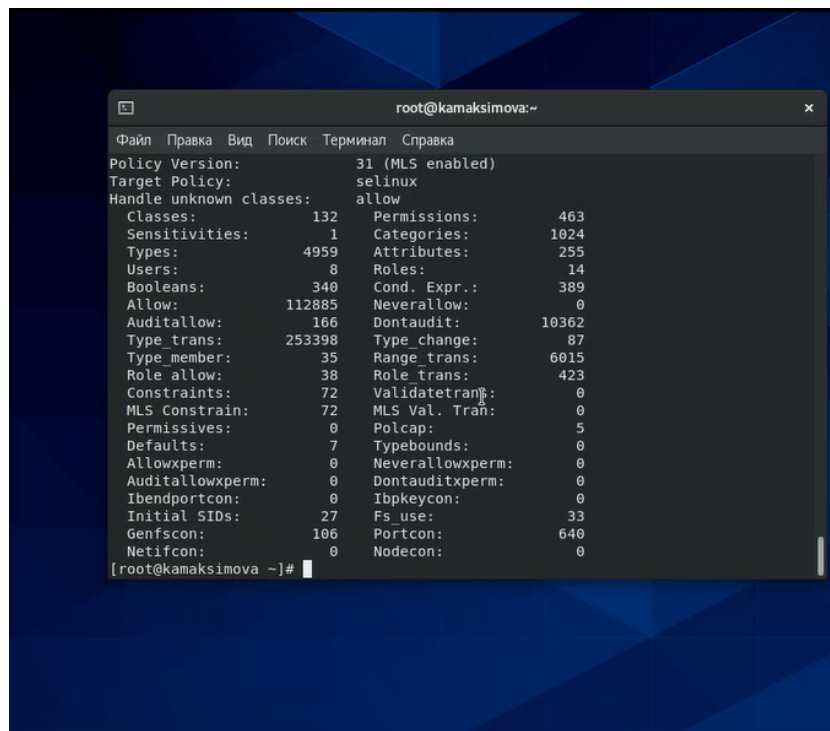


Figure 4.5: Рис 5.Статистика

Рисунок 5

6. Определите тип файлов и поддиректорий, находящихся в директории “/var/www”.

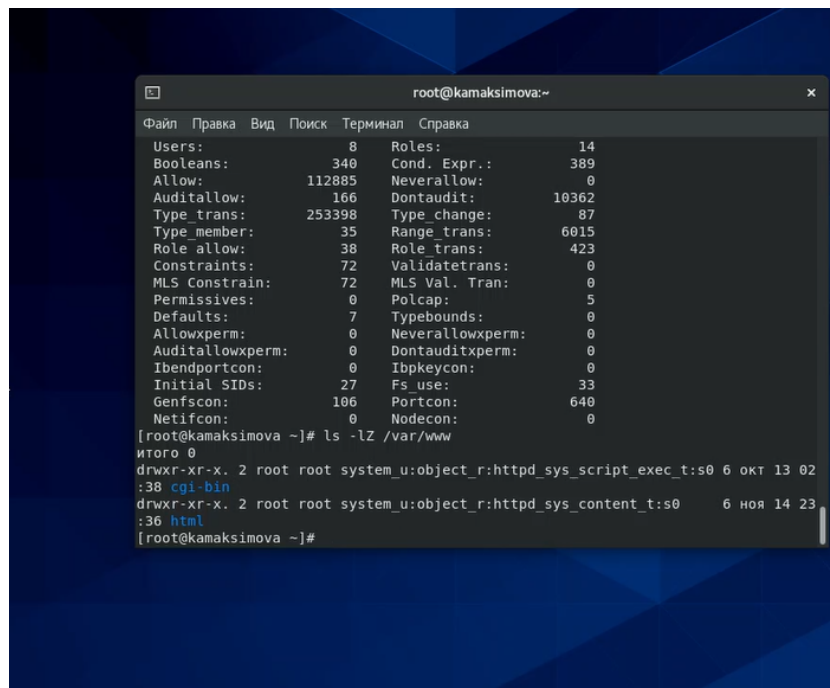


Figure 4.6: Рис 6.Директория “/var/www”

Рисунок 6

7. Определите тип файлов, находящихся в директории “/var/www/html”

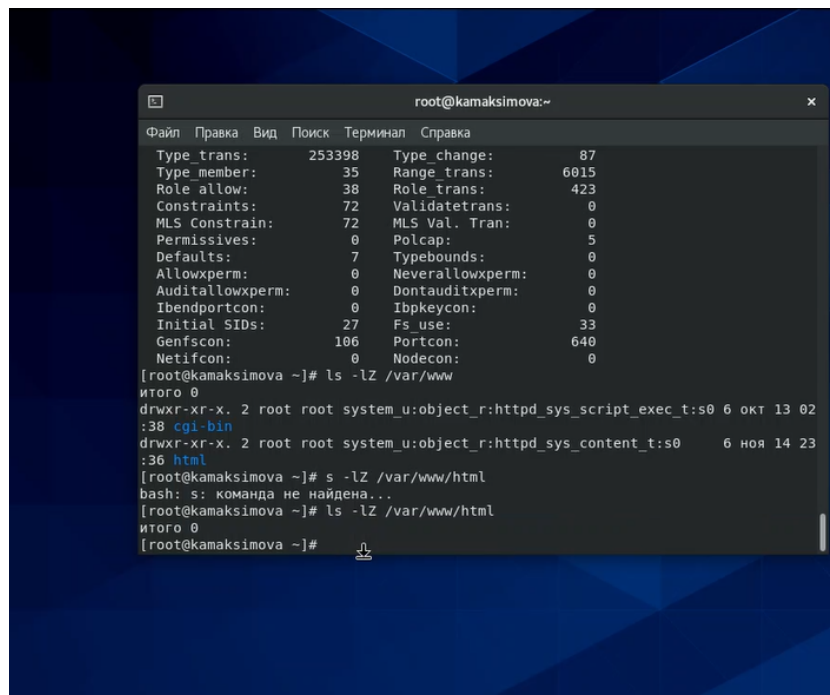


Figure 4.7: Рис 7.Директория “/var/www/html”

Рисунок 7

8. Определите круг пользователей, которым разрешено создание файлов в директории “/var/www/html”

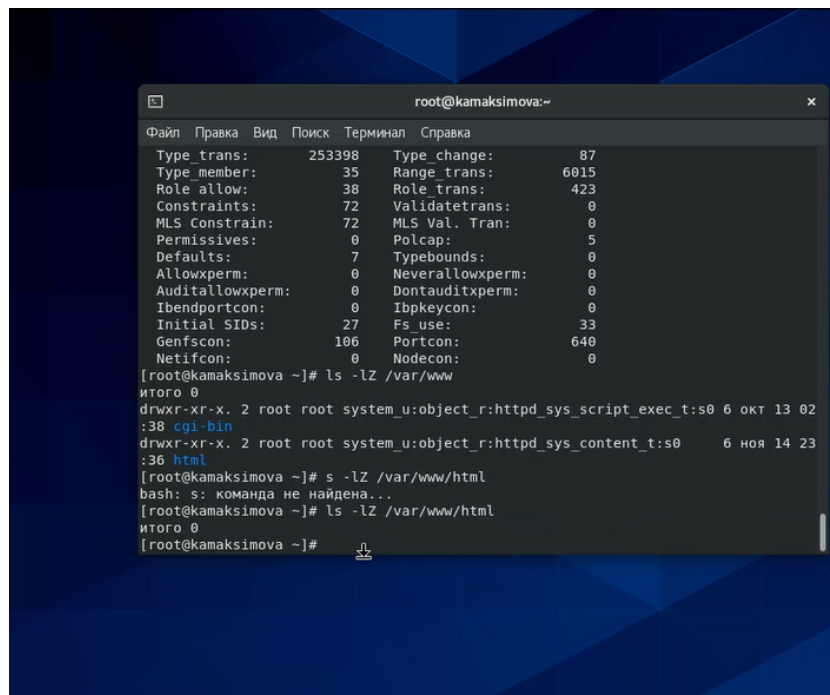


Figure 4.8: Рис 7.Директория “/var/www/html”

Рисунок 7

9. Создайте от имени суперпользователя html-файл

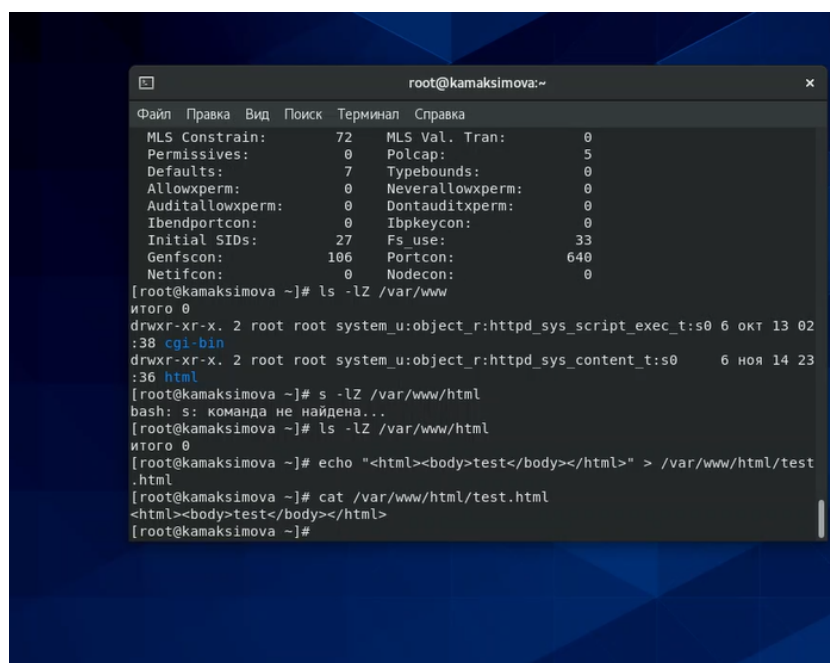
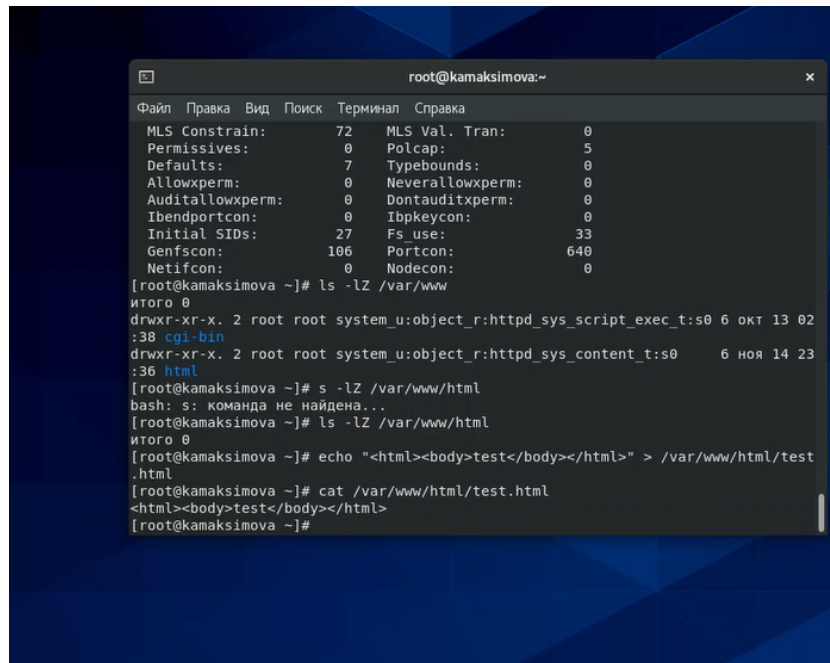


Figure 4.9: Рис 8.html-файл

Рисунок 8

10. Проверьте контекст созданного вами файла.



```
root@kamaksimova:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
MLS Constrain: 72    MLS Val. Tran: 0  
Permissives: 0     Polcap: 5  
Defaults: 7      Typebounds: 0  
Allowxperm: 0    Neverallowxperm: 0  
Auditallowxperm: 0  Dontauditxperm: 0  
Ibendportcon: 0   Ibpkeycon: 0  
Initial SIDs: 27   Fs_use: 33  
Genfscon: 106     Portcon: 640  
Netifcon: 0       Nodecon: 0  
[root@kamaksimova ~]# ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 13 02  
:38 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 14 23  
:36 html  
[root@kamaksimova ~]# s -lZ /var/www/html  
bash: s: команда не найдена...  
[root@kamaksimova ~]# ls -lZ /var/www/html  
итого 0  
[root@kamaksimova ~]# echo "<html><body>test</body></html>" > /var/www/html/test  
.html  
[root@kamaksimova ~]# cat /var/www/html/test.html  
<html><body>test</body></html>  
[root@kamaksimova ~]#
```

Figure 4.10: Рис 8.html-файл

Рисунок 8

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”



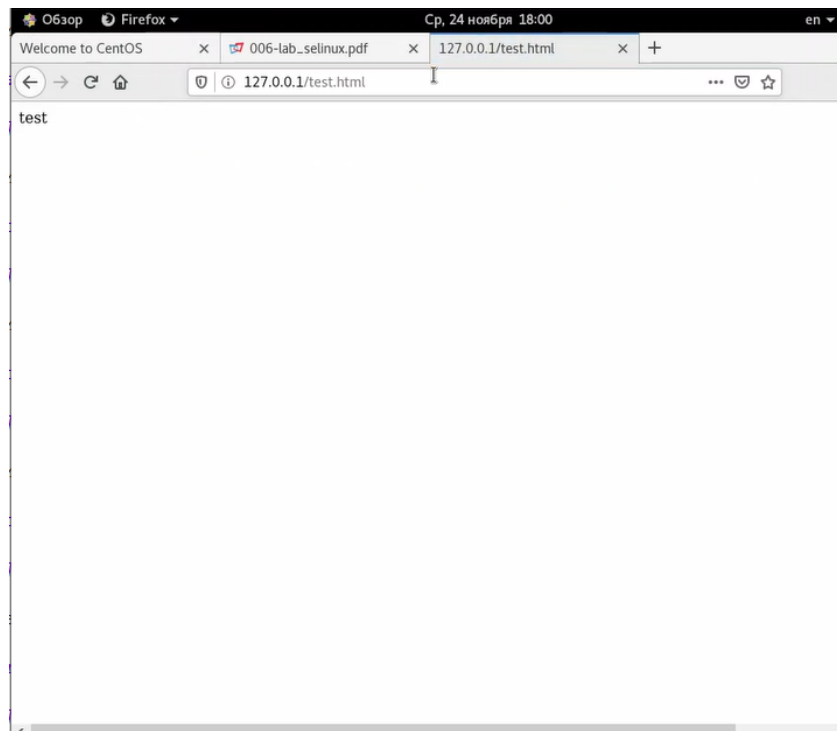


Figure 4.11: Рис 9.Файл

Рисунок 9

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`.

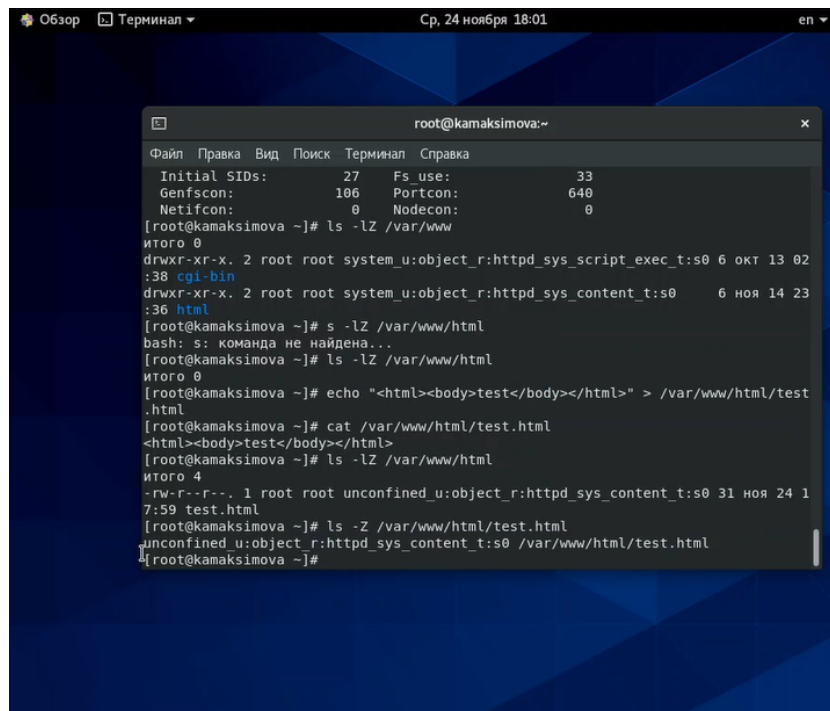
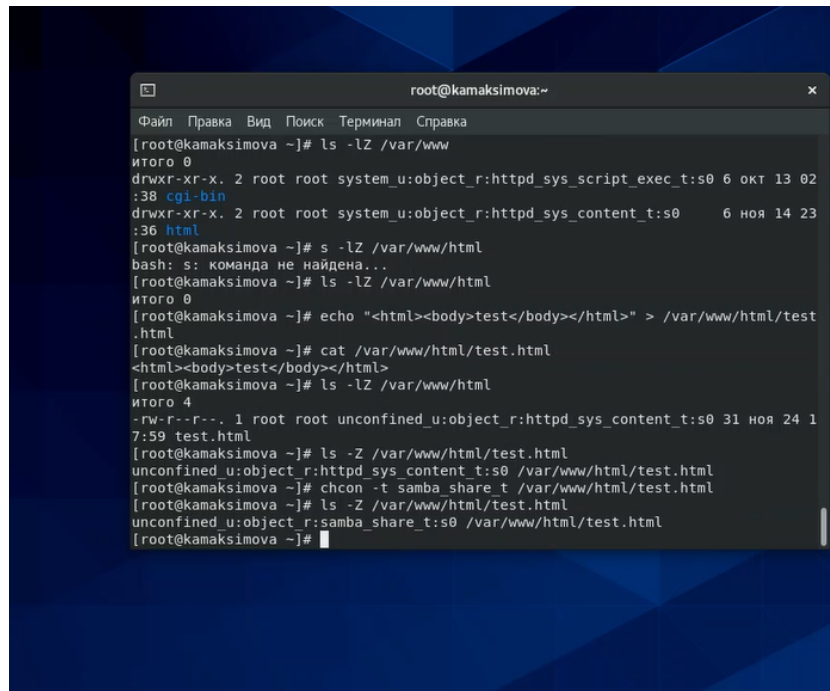


Figure 4.12: Рис 10.Контексты файлов

Рисунок 10

13. Измените контекст файла `"/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`



```
root@kamaksimova:~  
Файл Правка Вид Поиск Терминал Справка  
[root@kamaksimova ~]# ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 13 02  
:38 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 14 23  
:36 html  
[root@kamaksimova ~]# s -lZ /var/www/html  
bash: s: команда не найдена...  
[root@kamaksimova ~]# ls -lZ /var/www/html  
итого 0  
[root@kamaksimova ~]# echo "<html><body>test</body></html>" > /var/www/html/test  
.html  
[root@kamaksimova ~]# cat /var/www/html/test.html  
<html><body>test</body></html>  
[root@kamaksimova ~]# ls -lZ /var/www/html  
итого 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 31 ноя 24 1  
7:59 test.html  
[root@kamaksimova ~]# ls -lZ /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[root@kamaksimova ~]# chcon -t samba_share_t /var/www/html/test.html  
[root@kamaksimova ~]# ls -lZ /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@kamaksimova ~]#
```

Figure 4.13: Рис 11.Изменение контекста файла

Рисунок 11

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер.

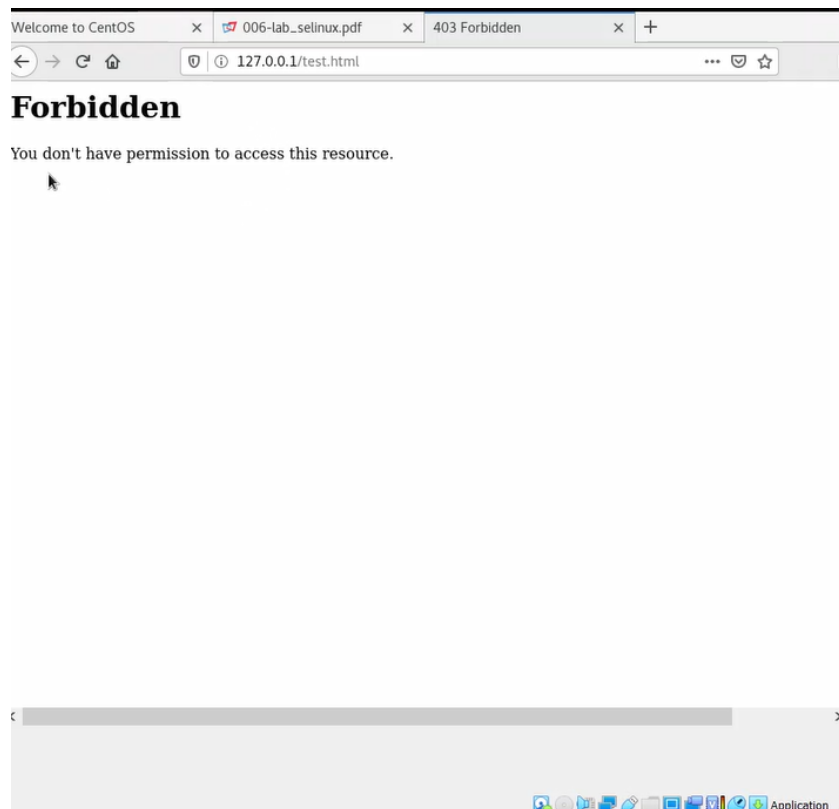


Figure 4.14: Рис 12.Изменение контекста файла

Рисунок 12

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

## 5 Выводы

Получены практические навыки администрирования ОС Linux, а так же получено практическое знакомство с технологией SELinux совместно с веб-сервером Apache.

# Список литературы

1. SELinux

2. Реализация мандатного контроля доступа с помощью SELinux или AppArmor в Linux

3. SELinux – описание и особенности работы с системой