

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Волков Тимофей Евгеньевич

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	17

List of Tables

List of Figures

2.1	Начало работ с apache	7
2.2	Состояние переключателей	7
2.3	Статистика по политике	8
2.4	Тип файлов и поддиректорий	9
2.5	Файл test.html	9
2.6	Проверка контекста	10
2.7	Вывод файла	10
2.8	Справка по apache	11
2.9	Изменение контекста файла	11
2.10	Ошибка доступа	12
2.11	log-файлы	13
2.12	Перезапуск веб-сервера Apache	14
2.13	Подготовка к запуску файла test.html	15
2.14	Вывод файла	15
2.15	Возврат к начальным настройкам	16

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 Выполнение лабораторной работы

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (fig. 2.1).

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

```
service httpd status
```

Если не работает, запустите его так же, но с параметром `start` (fig. 2.1).

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (fig. 2.1). Например, можно использовать команду

```
ps auxZ | grep httpd
```

Контекст безопасности - `system_u:system_r:httpd_t`

```
tevolkov@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@tevolkov ~]# getenforce  
Enforcing  
[root@tevolkov ~]# 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  
[root@tevolkov ~]# 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; vendor preset: disabled)  
   Active: inactive (dead)  
     Docs: man:httpd.service(8)  
  
[1]+ Остановлен service httpd status  
[root@tevolkov ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@tevolkov ~]# ps auxZ | grep httpd  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 6519 0.0 0.3 82136 7856 pts  
/0 T 13:50 0:00 /bin/systemctl status httpd.service  
system_u:system_r:httpd_t:s0 root 6550 0.1 0.5 273848 11212 ? Ss 1  
13:50 0:00 /usr/sbin/httpd -DFOREGROUND
```

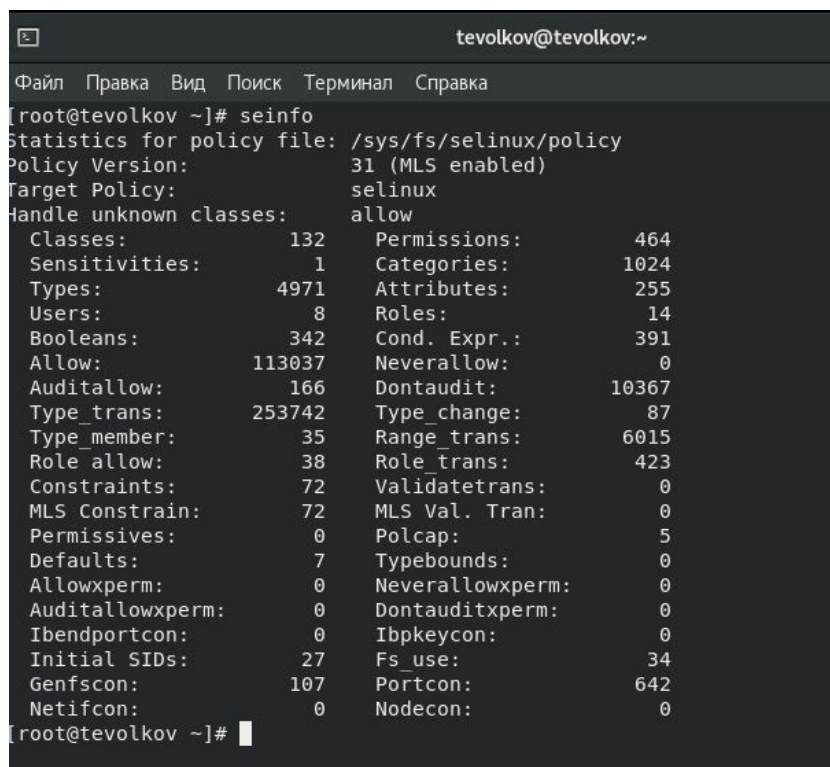
Figure 2.1: Начало работ с apache

Посмотрите текущее состояние переключателей SELinux для Apache (fig. 2.2) с помощью команды `sestatus -b httpd`

```
Обзор Терминал Пт, 19 ноября 14:10 en  
tevolkov@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@tevolkov ~]# sestatus -b 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  
authlogin_yubikey off  
awstats_purge_apache_log_files off  
boinc_execmem on  
cdrecord_read_content off  
cluster_can_network_connect off  
cluster_manage_all_files off  
cluster_use_execmem off
```

Figure 2.2: Состояние переключателей

Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (fig. 2.3).



```
tevolkov@tevolkov:~
Файл Правка Вид Поиск Терминал Справка
[root@tevolkov ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 31 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 132 Permissions: 464
Sensitivities: 1 Categories: 1024
Types: 4971 Attributes: 255
Users: 8 Roles: 14
Booleans: 342 Cond. Expr.: 391
Allow: 113037 Neverallow: 0
Auditallow: 166 Dontaudit: 10367
Type_trans: 253742 Type_change: 87
Type_member: 35 Range_trans: 6015
Role_allow: 38 Role_trans: 423
Constraints: 72 Validatetrans: 0
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: 34
Genfscon: 107 Portcon: 642
Netifcon: 0 Nodecon: 0
[root@tevolkov ~]#
```

Figure 2.3: Статистика по политике

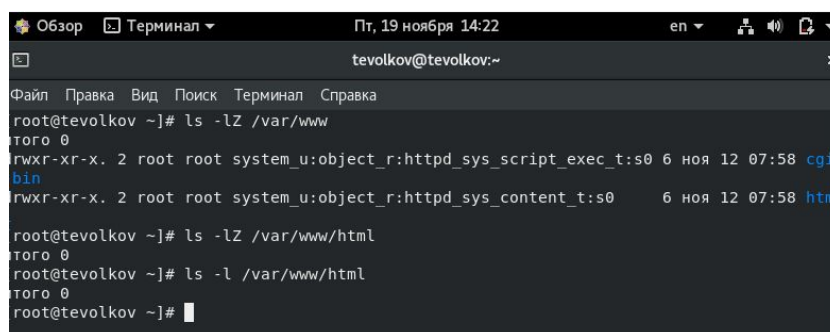
Определите тип файлов и поддиректорий, находящихся в директории `/var/www` (fig. 2.4), с помощью команды

```
ls -lZ /var/www
```

Определите тип файлов, находящихся в директории `/var/www/html` (fig. 2.4):

```
ls -lZ /var/www/html
```

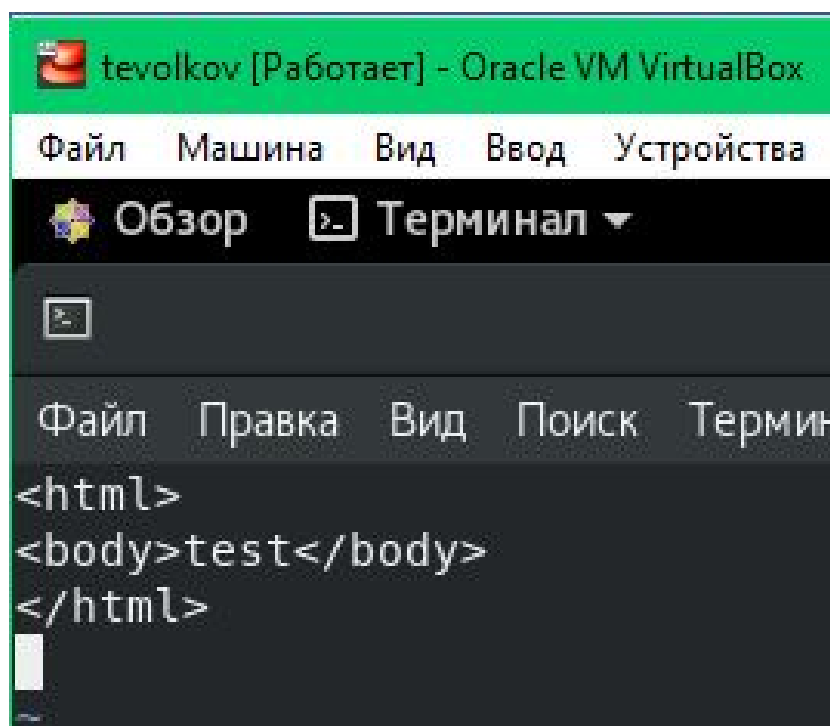
Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Позволено только владельцу.



```
tevolkov@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
root@tevolkov ~]# ls -lZ /var/www  
total 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi  
bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58 html  
  
root@tevolkov ~]# ls -lZ /var/www/html  
total 0  
root@tevolkov ~]# ls -l /var/www/html  
total 0  
root@tevolkov ~]#
```

Figure 2.4: Тип файлов и поддиректорий

Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания (fig. 2.5):



```
tevolkov [Работает] - Oracle VM VirtualBox  
Файл Машина Вид Ввод Устройства  
Обзор Терминал  
Файл Правка Вид Поиск Термин  
<html>  
<body>test</body>  
</html>
```

Figure 2.5: Файл test.html

Проверьте контекст созданного вами файла.
`unconfined_u:object_r:httpd_sys_content_t` - контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html` (fig. 2.6).

```
[root@tevolkov ~]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 19 14:28 test.html
[root@tevolkov ~]#
```

Figure 2.6: Проверка контекста

Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён (fig. 2.7).

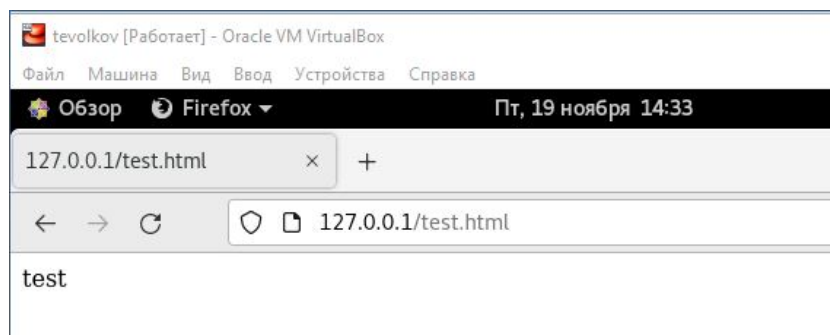
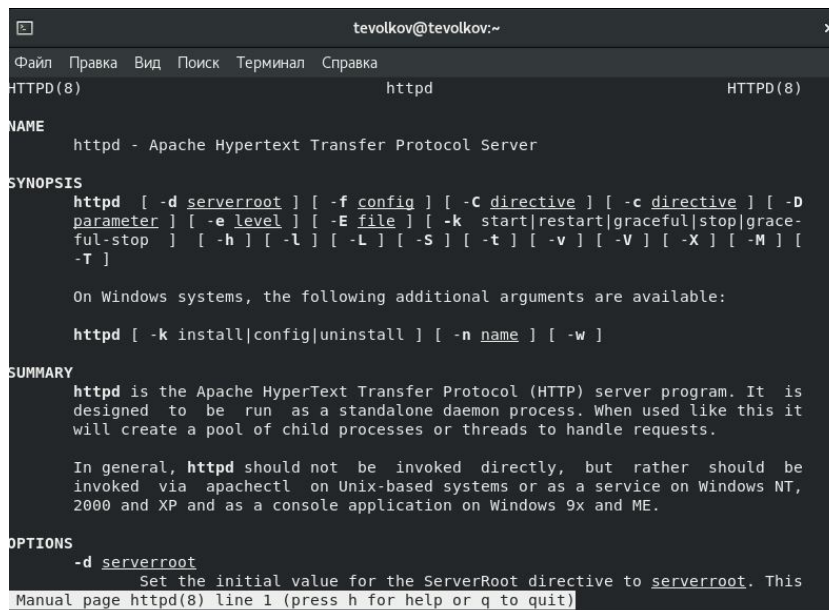


Figure 2.7: Вывод файла

Изучите справку `man httpd` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Контексты совпадают. Проверить контекст файла можно командой `ls -Z` (fig. 2.8).

`ls -Z /var/www/html/test.html`



```
tevolkov@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
HTTPD(8) httpd HTTPD(8)  
NAME  
httpd - Apache Hypertext Transfer Protocol Server  
SYNOPSIS  
httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ] [ -D  
parameter ] [ -e level ] [ -E file ] [ -k start|restart|graceful|stop|grace-  
ful-stop ] [ -h ] [ -l ] [ -L ] [ -S ] [ -t ] [ -v ] [ -V ] [ -X ] [ -M ] [ -T ]  
  
On Windows systems, the following additional arguments are available:  
  
httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]  
SUMMARY  
httpd is the Apache HyperText Transfer Protocol (HTTP) server program. It is  
designed to be run as a standalone daemon process. When used like this it  
will create a pool of child processes or threads to handle requests.  
  
In general, httpd should not be invoked directly, but rather should be  
invoked via apachectl on Unix-based systems or as a service on Windows NT,  
2000 and XP and as a console application on Windows 9x and ME.  
OPTIONS  
-d serverroot  
Set the initial value for the ServerRoot directive to serverroot. This  
Manual page httpd(8) line 1 (press h for help or q to quit)
```

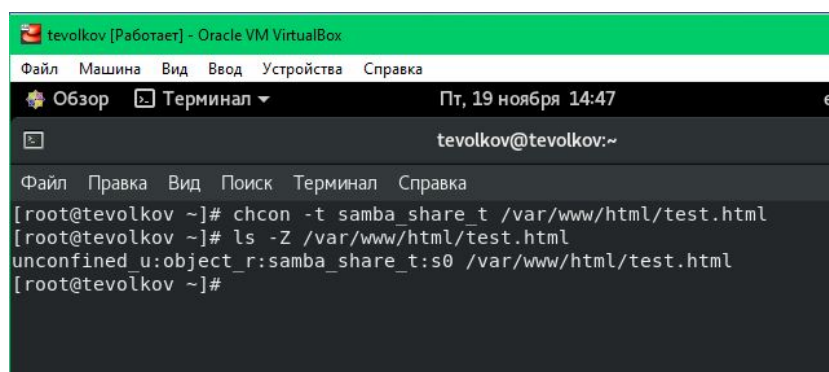
Figure 2.8: Справка по apache

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` (fig. 2.9):

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```

После этого проверьте, что контекст поменялся.



```
tevolkov [Работает] - Oracle VM VirtualBox  
Файл Машина Вид Ввод Устройства Справка  
Обзор Терминал Пт, 19 ноября 14:47  
tevolkov@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@tevolkov ~]# chcon -t samba_share_t /var/www/html/test.html  
[root@tevolkov ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@tevolkov ~]#
```

Figure 2.9: Изменение контекста файла

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке (fig.

2.10).

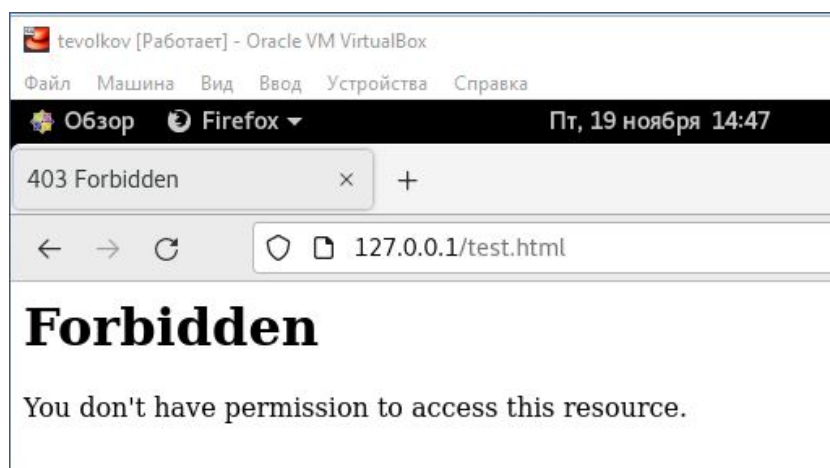
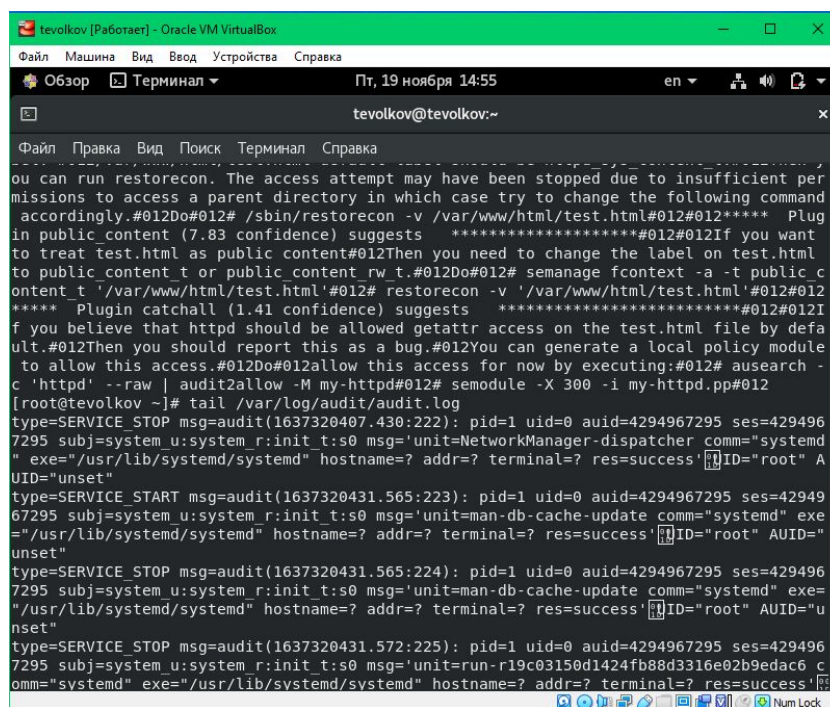


Figure 2.10: Ошибка доступа

Файл не был отображён так как у `httpd` не было доступа к изменённому контексту. Просмотрите `log`-файлы веб-сервера `Apache`. Также просмотрите системный `лог-файл` (fig. 2.11):

```
tail /var/log/messages
```

Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log` (fig. 2.11).

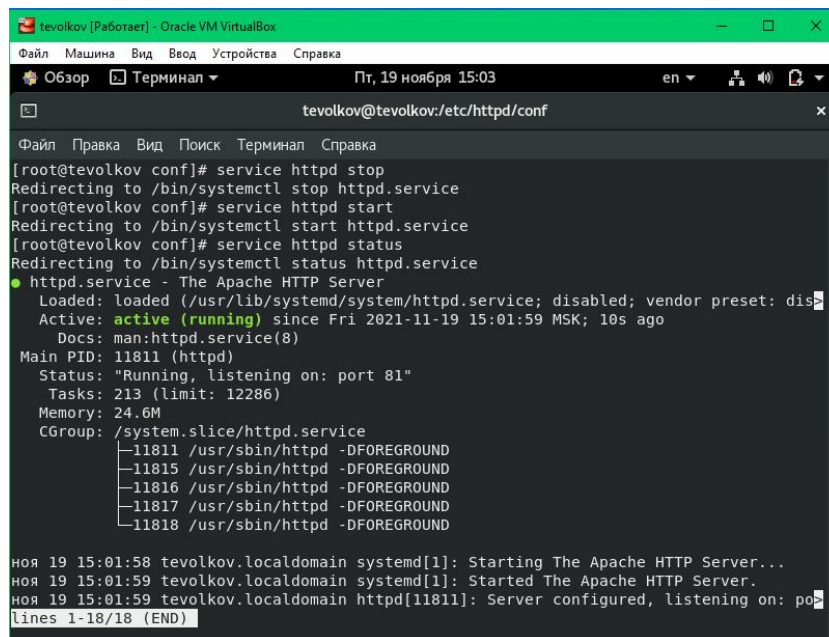


```
tevolkov@tevolkov:~  
-----  
ou can run restorecon. The access attempt may have been stopped due to insufficient per  
missions to access a parent directory in which case try to change the following command  
accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Plug  
in public_content (7.83 confidence) suggests *****#012#012If you want  
to treat test.html as public content#012Then you need to change the label on test.html  
to public content t or public content rw t.#012Do#012# semanage fcontext -a -t public c  
ontent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012  
**** Plugin catchall (1.41 confidence) suggests *****#012#012If  
you believe that httpd should be allowed getattr access on the test.html file by defa  
ult.#012Then you should report this as a bug.#012You can generate a local policy module  
to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -  
c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012  
[root@tevolkov ~]# tail /var/log/audit/audit.log  
type=SERVICE_STOP msg=audit(1637320407.430:222): pid=1 uid=0 auid=4294967295 ses=429496  
7295 subj=system_u:system_r:init_t:s0 msg='unit=NetworkManager-dispatcher comm="systemd"  
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'ID="root" A  
UID="unset"  
type=SERVICE_START msg=audit(1637320431.565:223): pid=1 uid=0 auid=4294967295 ses=42949  
67295 subj=system_u:system_r:init_t:s0 msg='unit=man-db-cache-update comm="systemd" exe  
="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'ID="root" AUID="u  
nset"  
type=SERVICE_STOP msg=audit(1637320431.565:224): pid=1 uid=0 auid=4294967295 ses=429496  
7295 subj=system_u:system_r:init_t:s0 msg='unit=man-db-cache-update comm="systemd" exe  
="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'ID="root" AUID="u  
nset"  
type=SERVICE_STOP msg=audit(1637320431.572:225): pid=1 uid=0 auid=4294967295 ses=429496  
7295 subj=system_u:system_r:init_t:s0 msg='unit=run-r19c03150d1424fb88d3316e02b9edac6 c  
omm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
```

Figure 2.11: log-файлы

Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

Выполните перезапуск веб-сервера Apache (fig. 2.12).



```
tevolkov@tevolkov:/etc/httpd/conf
[root@tevolkov conf]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@tevolkov conf]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@tevolkov conf]# 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; vendor preset: disabled)
   Active: active (running) since Fri 2021-11-19 15:01:59 MSK; 10s ago
     Docs: man:httpd.service(8)
   Main PID: 11811 (httpd)
    Status: "Running, listening on: port 81"
     Tasks: 213 (limit: 12286)
    Memory: 24.6M
    CGroup: /system.slice/httpd.service
            └─11811 /usr/sbin/httpd -DFOREGROUND
              └─11815 /usr/sbin/httpd -DFOREGROUND
                └─11816 /usr/sbin/httpd -DFOREGROUND
                  └─11817 /usr/sbin/httpd -DFOREGROUND
                    └─11818 /usr/sbin/httpd -DFOREGROUND

ноя 19 15:01:58 tevolkov.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 19 15:01:59 tevolkov.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 19 15:01:59 tevolkov.localdomain httpd[11811]: Server configured, listening on: po
lines 1-18/18 (END)
```

Figure 2.12: Перезапуск веб-сервера Apache

Выполните команду

```
semanage port -a -t http_port_t -p tcp 81
```

После этого проверьте список портов командой

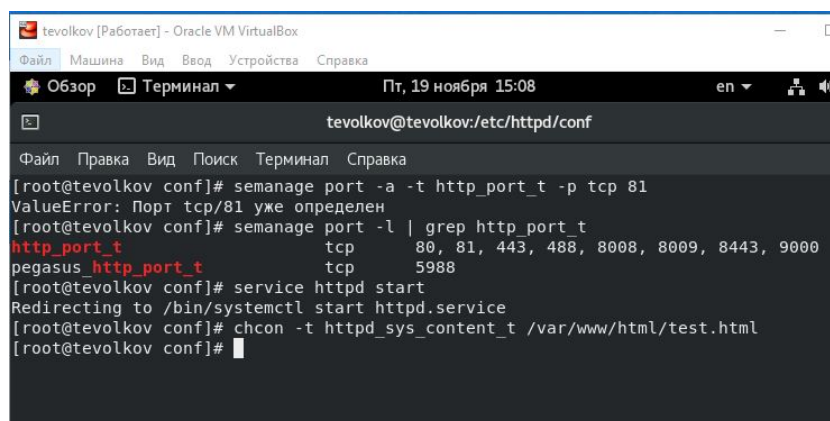
```
semanage port -l | grep http_port_t
```

Убедитесь, что порт 81 появился в списке (fig. 2.13).

Попробуйте запустить веб-сервер Apache ещё раз (fig. 2.13).

Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` (fig. 2.13):

```
chcon -t httpd_sys_content_t /var/www/html/test.html
```



```
tevolkov [Работает] - Oracle VM VirtualBox
Файл | Машина | Вид | Ввод | Устройства | Справка
Обзор Терминал ▼ Пт, 19 ноября 15:08 en
tevolkov@tevolkov:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
[root@tevolkov conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@tevolkov conf]# 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@tevolkov conf]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@tevolkov conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@tevolkov conf]#
```

Figure 2.13: Подготовка к запуску файла test.html

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html` (fig. 2.14).

Вы должны увидеть содержимое файла — слово «test»

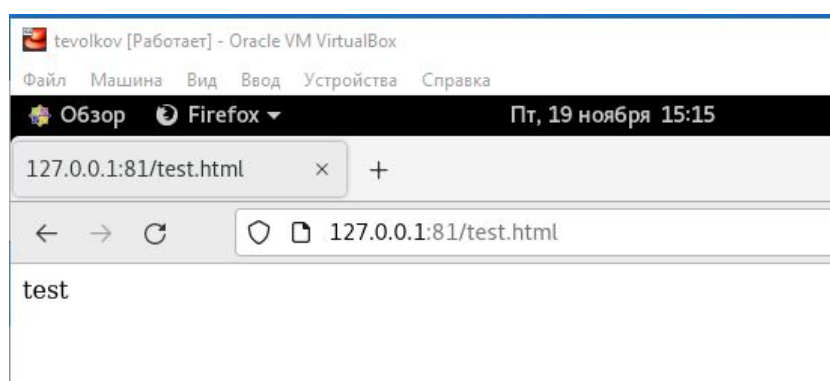
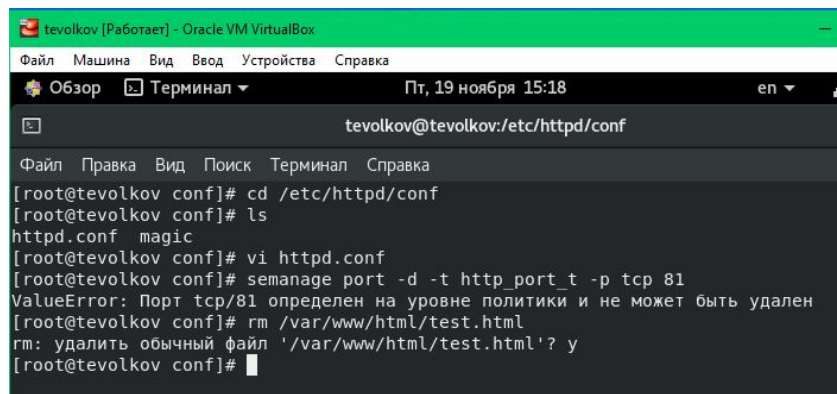


Figure 2.14: Вывод файла

Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.

Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81`

Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`



```
tevolkov [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал
Пт, 19 ноября 15:18  en
tevolkov@tevolkov:/etc/httpd/conf
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@tevolkov conf]# cd /etc/httpd/conf
[root@tevolkov conf]# ls
httpd.conf  magic
[root@tevolkov conf]# vi httpd.conf
[root@tevolkov conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@tevolkov conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@tevolkov conf]#
```

Figure 2.15: Возврат к начальным настройкам

3 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.