

Лабораторная работа №6

Лукьянова Ирина Владимировна, НФИбд-02-19

Содержание

| | | |
|---|--------------------------------|----|
| 1 | Цель работы | 5 |
| 2 | Выполнение лабораторной работы | 6 |
| 3 | Выводы | 16 |
| 4 | Список литературы | 17 |

List of Figures

| | | |
|------|--|----|
| 2.1 | Работа с пакетами и необходимыми параметрами | 6 |
| 2.2 | Команды getenforce и sestatus | 7 |
| 2.3 | Проверяем работу сервиса | 7 |
| 2.4 | Команда ps auxZ grep httpd | 7 |
| 2.5 | Команда sestatus -bigrep httpd | 8 |
| 2.6 | Команда seinfo | 9 |
| 2.7 | Команда ls -lZ /var/www | 9 |
| 2.8 | Команда ls -lZ /var/www/html | 9 |
| 2.9 | Файл test.html | 10 |
| 2.10 | Выполняем проверку | 10 |
| 2.11 | Обращаемся к файлу | 10 |
| 2.12 | Справка и проверка файла | 10 |
| 2.13 | Меняем контекст | 10 |
| 2.14 | Сообщение об ошибке | 11 |
| 2.15 | Просмотр лог файлов | 11 |
| 2.16 | Просмотр лог файлов | 11 |
| 2.17 | Запуск порта 81 | 12 |
| 2.18 | Проверка | 12 |
| 2.19 | Работа с лог файлами | 12 |
| 2.20 | Проверка | 13 |
| 2.21 | Проверяем список портов | 13 |
| 2.22 | Запуск веб-сервера | 13 |
| 2.23 | Доступ к файлу | 14 |
| 2.24 | Работа с конфигурацией файла | 14 |
| 2.25 | Проверка | 14 |
| 2.26 | Удаление файла | 15 |

List of Tables

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.¹

¹Мандатное разграничение прав в Linux.

2 Выполнение лабораторной работы

От имени суперпользователя устанавливаем необходимые пакеты, задаем параметр ServerName и отключаем пакетный фильтр.(рис. 2.1)

```
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerName test.ru
[root@irina conf]# iptables -F
bash: iptables: command not found...
Similar command is: 'iptables'
[root@irina conf]# cd
[root@irina ~]# iptables -F
bash: iptables: command not found...
Similar command is: 'iptables'
[root@irina ~]# iptables -F
[root@irina ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
[root@irina ~]# iptables -P INPUT ACCEPT
[root@irina ~]# iptables -P OUTPUT ACCEPT
```

Figure 2.1: Работа с пакетами и необходимыми параметрами

Входим в систему с полученными учётными данными и смотрим, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.(рис. 2.2)

```

[root@irina ~]# getenforce
Enforcing
[root@irina ~]# setstatus
bash: setstatus: command not found...
[root@irina ~]# 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@irina ~]#

```

Figure 2.2: Команды getenforce и sestatus

Обращаемся с помощью браузера к веб-серверу, запущенному на компьютере, и смотрим, что последний работает: (рис. 2.3)

```

[root@irina ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@irina ~]# 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 Sat 2022-10-01 13:16:28 MSK; 5s ago
     Docs: man:httpd.service(8)
   Main PID: 39576 (httpd)
    Status: "Started, listening on: port 80"
   Tasks: 213 (limit: 12213)
  Memory: 23.0M
    CPU: 153ms
  CGroup: /system.slice/httpd.service
          └─39576 /usr/sbin/httpd -DFOREGROUND
            └─39577 /usr/sbin/httpd -DFOREGROUND
              └─39578 /usr/sbin/httpd -DFOREGROUND
                └─39579 /usr/sbin/httpd -DFOREGROUND
                  └─39580 /usr/sbin/httpd -DFOREGROUND

Oct 01 13:16:28 irina.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 01 13:16:28 irina.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 01 13:16:28 irina.localdomain httpd[39576]: Server configured, listening on: port 80
[root@irina ~]#

```

Figure 2.3: Проверяем работу сервиса

Находим веб-сервер Apache в списке процессов, определяем его контекст безопасности: (рис. 2.4)

```

[root@irina ~]# ps auxZ | grep httpd
system u:system r:httpd_t:s0 root 39576 0.1 0.5 20064 11572 ? Ss 13:16 0:00 /usr/sbin/httpd -
DFOREGROUND
system u:system r:httpd_t:s0 apache 39577 0.0 0.3 21516 7332 ? S 13:16 0:00 /usr/sbin/httpd -
DFOREGROUND
system u:system r:httpd_t:s0 apache 39578 0.0 0.6 1210352 13144 ? Sl 13:16 0:00 /usr/sbin/httpd -
DFOREGROUND
system u:system r:httpd_t:s0 apache 39579 0.0 0.5 1079216 11096 ? Sl 13:16 0:00 /usr/sbin/httpd -
DFOREGROUND
system u:system r:httpd_t:s0 apache 39580 0.0 0.5 1079216 11104 ? Sl 13:16 0:00 /usr/sbin/httpd -
DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 root 39809 0.0 0.1 221668 2348 pts/0 S+ 13:17 0:00 grep --c
olor=auto httpd
[root@irina ~]#

```

Figure 2.4: Команда ps auxZ | grep httpd

Смотрим текущее состояние переключателей SELinux для Apache. Обращаем внимание, что многие из них находятся в положении «off».(рис. 2.5)

```
[root@irina ~]# 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
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
```

Figure 2.5: Команда sestatus -bigrep httpd

Смотрим статистику по политике, также Определяем множество пользователей, ролей, типов.(рис. 2.6).

Пользователей = 8, ролей = 14, типов = 4995


```

[root@irina ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 133
Sensitivities:           1
Types:                   4995
Users:                   8
Booleans:                347
Allow:                   63727
Auditallow:              163
Type_trans:              251060
Type_member:             35
Role_allow:              38
Constraints:             72
MLS Constrain:           72
Permissives:             0
Defaults:                7
Allowxperm:              0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:            27
Genfscon:                106
Netifcon:                0
Permissions:             454
Categories:             1024
Attributes:              254
Roles:                   14
Cond. Expr.:             382
Neverallow:              0
Dontaudit:               8391
Type_change:             87
Range_trans:             5958
Role_trans:              418
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  5
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  33
Portcon:                 651
Nodecon:                 0

```

Figure 2.6: Команда seinfo

Определяем тип файлов и поддиректорий, находящихся в директории /var/www.(рис. 2.7).

```

[root@irina ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 html

```

Figure 2.7: Команда ls -lZ /var/www

Определяем тип файлов, находящихся в директории /var/www/html (рис. 2.8)

```

[root@irina ~]# ls -lZ /var/www/html
total 0
[root@irina ~]# touch /var/www/html/test.html
[root@irina ~]#

```

Figure 2.8: Команда ls -lZ /var/www/html

От имени суперпользователя создаем файл html-файл /var/www/html/test.html следующего содержания:(рис. 2.9)

```
<html>
<body>test</body>
</html>
```

Figure 2.9: Файл test.html

Проверяем контекст созданного файла.(рис. 2.10)

```
[root@irina ~]# vi test.html
[root@irina ~]# ls -lZ /var/www/html
total 0
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 Oct  1 13:22 test.html
[root@irina ~]#
```

Figure 2.10: Выполняем проверку

Обращаемся к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Смотрим, что файл был успешно отображён.(рис. 2.11)

Firefox browser window showing the address bar with 127.0.0.1/test.html and the page content displaying "test".

Figure 2.11: Обращаемся к файлу

Изучаем справку `man httpd_selinux`, проверяем контекст файла командой `ls -lZ /var/www/html/test.html`(рис. 2.12)

```
[root@irina ~]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 36 Oct  1 13:30 /var/www/html/test.html
[root@irina ~]#
```

Figure 2.12: Справка и проверка файла

Меняем контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`:(рис. 2.13)

```
[root@irina ~]# chcon -t samba_share_t /var/www/html/test.html
[root@irina ~]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 36 Oct  1 13:30 /var/www/html/test.html
[root@irina ~]#
```

Figure 2.13: Меняем контекст

Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получаем сообщение об ошибке(рис. 2.14)

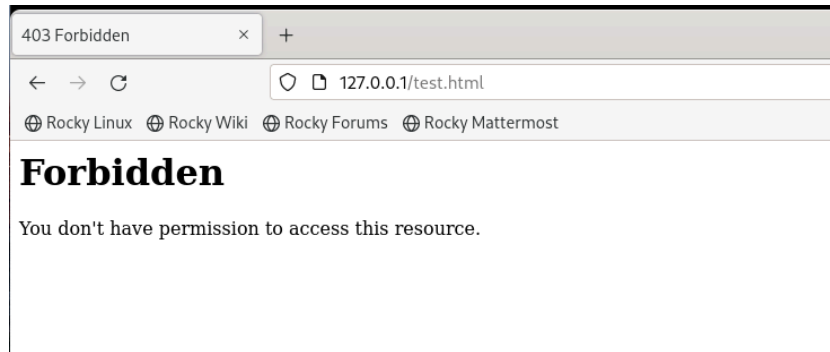


Figure 2.14: Сообщение об ошибке

Смотрим log-файлы веб-сервера Apache. Также смотрим системный лог-файл:(рис. 2.15), (рис. 2.16)

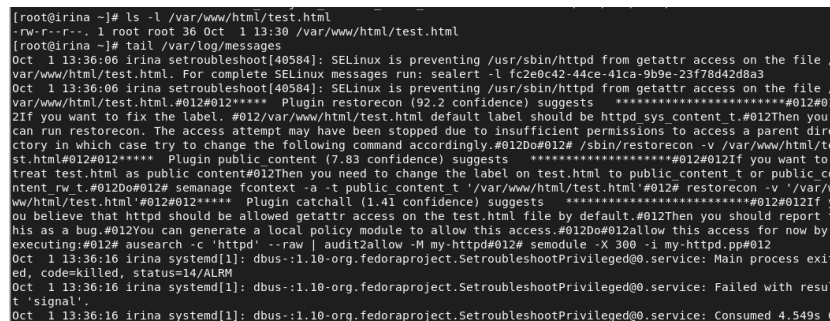


Figure 2.15: Просмотр лог файлов

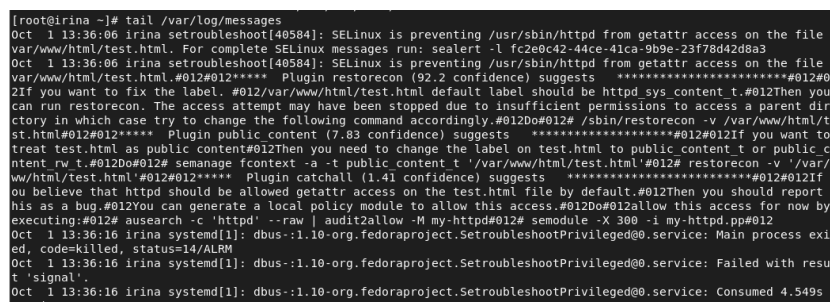


Figure 2.16: Просмотр лог файлов

Пробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 2.17)

```
httpd.conf  [-M--]  9 L: [ 27+20  47/360] *(2025/12024b) 0010 0x00A
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default.  See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts.  See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9Pull
```

Figure 2.17: Запуск порта 81

Выполняем перезапуск веб-сервера Apache. Произошёл сбой? Нет(рис. 2.18)

```
[root@irina conf]# systemctl restart httpd
[root@irina conf]#
```

Figure 2.18: Проверка

Анализируем лог-файлы. (рис. 2.19), (рис. 2.20)

```
[root@irina ~]# tail /var/log/messages
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for glibc-headers
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for glibc-devel
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for gnome-menus
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for openldap-compat
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for kernel-modules
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for kernel-core
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for kernel
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for grub2-tools-extra
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for grub2-tools-efi
Oct  1 13:49:29 irina journal[1171]: Failed to get cache filename for kernel-devel
[root@irina ~]#
```

Figure 2.19: Работа с лог файлами

```
end" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1664620576.077:206): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:ini
nit_t:s0 msg='unit=dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/syst
emd" hostname=? addr=? terminal=? res=failed'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1664620576.163:207): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:ini
nit_t:s0 msg='unit=dbus-1.10-org.fedoraproject.Setroubleshootd@0 comm="systemd" exe="/usr/lib/systemd/systemd" host
name=? addr=? terminal=? res=failed'UID="root" AUDID="unset"
type=SERVICE_START msg=audit(1664620953.804:208): pid=1171 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syst
em_r:rpm_t:s0 msg='op=install sw="mc-1.4.8.26-5.el9.x86_64" sw_type=rpm key=enforce=0 gpg_res=1 root_dir="/" comm="p
ackagekitd" exe="/usr/libexec/packagekitd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_START msg=audit(1664620953.806:209): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg='unit=run-ree9edd54ee984ab69ea4bba382b274da comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? a
ddr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_START msg=audit(1664620958.028:210): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg='unit=man-db-cache-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? r
es=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1664620958.028:211): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:ini
nit_t:s0 msg='unit=man-db-cache-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? re
s=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1664620958.040:212): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:ini
nit_t:s0 msg='unit=run-ree9edd54ee984ab69ea4bba382b274da comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? ad
dr=? terminal=? res=success'UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1664621254.652:213): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:ini
nit_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="
root" AUDID="unset"
type=SERVICE_START msg=audit(1664621255.168:214): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID
="root" AUDID="unset"
[root@irina ~]#
```

Figure 2.20: Проверка

Выполняем команду `semanage port -a -t http_port_t -p tcp 81` После этого про-
веряем список портов (рис. 2.21)

```
[root@irina ~]# 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@irina ~]# semanage port -a -t http_port_t -ptcp 81
ValueError: Port tcp/81 already defined
[root@irina ~]#
```

Figure 2.21: Проверяем список портов

Пробуем запустить веб-сервер Apache ещё раз и возвращаем контекст
`httpd_sys_content_t` к файлу `/var/www/html/test.html`(рис. 2.22)

```
[root@irina ~]# systemctl restart httpd
[root@irina ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@irina ~]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 36 Oct 1 13:30 /var/www/html/test.html
[root@irina ~]#
```

Figure 2.22: Запуск веб-сервера

Возвращаем контекст и получаем доступ к файлу через веб-сервер, введя в
браузере адрес `http://127.0.0.1:81/test.html`. Теперь увидим содержимое файла
— слово «test». (рис. 2.23)

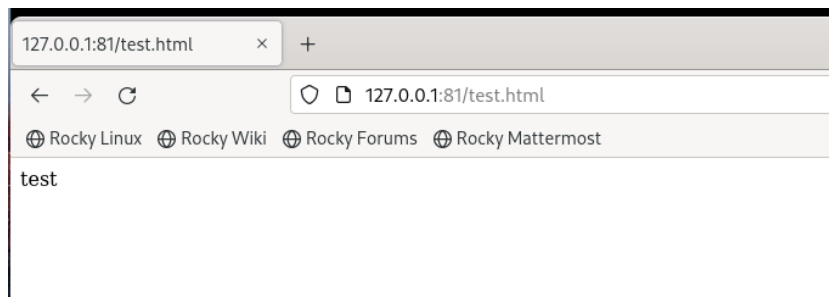


Figure 2.23: Доступ к файлу

Исправляем обратно конфигурационный файл apache, вернув Listen 80.(рис. 2.24)

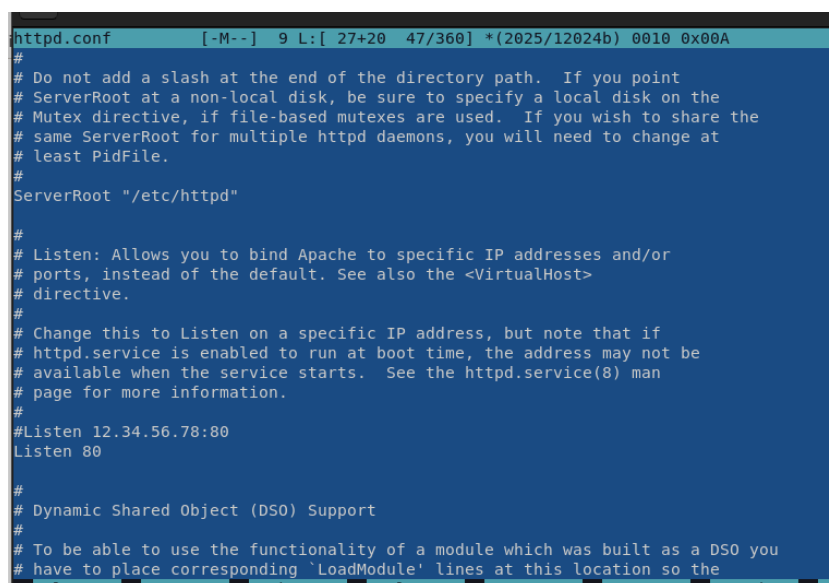


Figure 2.24: Работа с конфигурацией файла

Пытаемся удалить привязку http_port_t к 81 порту: (рис. 2.25)

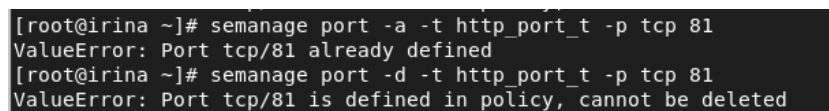


Figure 2.25: Проверка

Удаляем файл /var/www/html/test.html:(рис. 2.26)

```
[root@irina ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@irina ~]# ls -lZ /var/www/html/
total 0
[root@irina ~]# ls -lZ /var/www/
total 0
```

Figure 2.26: Удаление файла

3 Выводы

В ходе выполнения данной лабораторной работы я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

4 Список литературы

1. Мандатное разграничение прав в Linux. / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 7 с.
2. Руководство по оформлению Markdown.