

Лабораторная работа №6

Мандатное разграничение прав

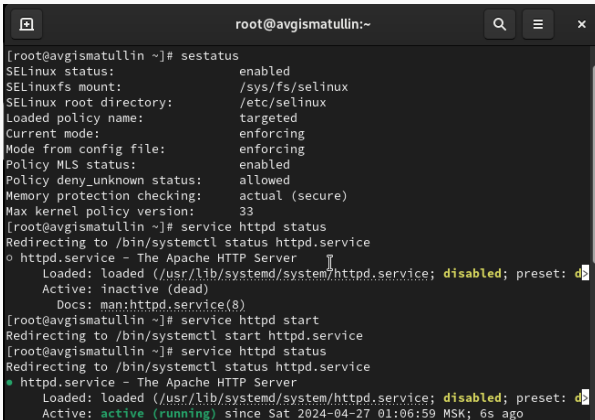
Гисматуллин А.В.

Российский университет дружбы народов, Москва, Россия

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.
- Проверить работу SELinx на практике совместно с веб-сервером Apache.

Процесс выполнения лабораторной работы

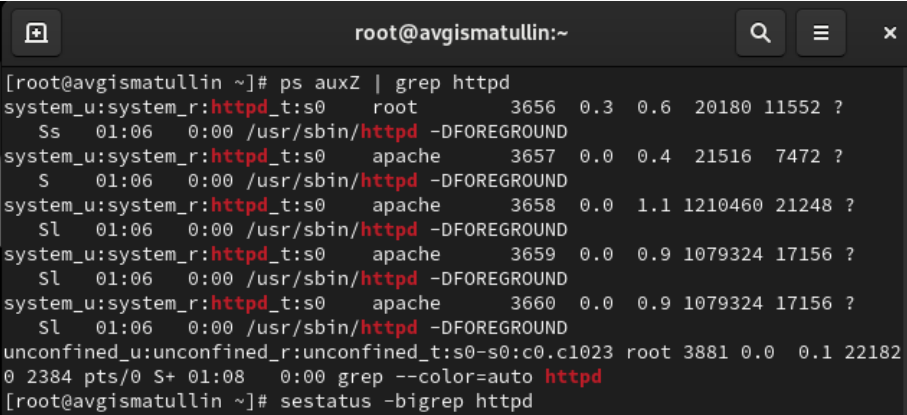
Проверка сервера

A terminal window titled 'root@avgismatullin:~' with search, menu, and close icons in the title bar. The terminal shows the output of 'sestatus' and 'service httpd status' commands. The SELinux status is enabled with various configurations. The httpd service is initially shown as 'disabled' and 'inactive (dead)'. After running 'service httpd start', the status is updated to 'active (running)' since Saturday, 2024-04-27 01:06:59 MSK.

```
root@avgismatullin:~  
[root@avgismatullin ~]# 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@avgismatullin ~]# 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: disabled)  
   Active: inactive (dead)  
   Docs: man:httpd.service(8)  
[root@avgismatullin ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@avgismatullin ~]# 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: disabled)  
   Active: active (running) since Sat 2024-04-27 01:06:59 MSK; 6s ago
```

Рис. 1: Командная строка. Проверка работоспособности сервера

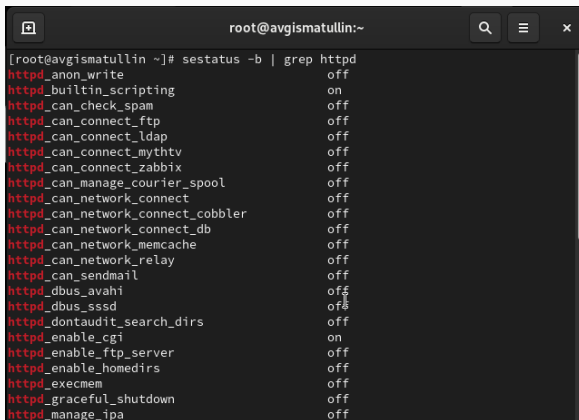
Проверка сервера



```
root@avgismatullin:~  
[root@avgismatullin ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 3656 0.3 0.6 20180 11552 ?  
Ss 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3657 0.0 0.4 21516 7472 ?  
S 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3658 0.0 1.1 1210460 21248 ?  
Sl 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3659 0.0 0.9 1079324 17156 ?  
Sl 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3660 0.0 0.9 1079324 17156 ?  
Sl 01:06 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3881 0.0 0.1 22182  
0 2384 pts/0 S+ 01:08 0:00 grep --color=auto httpd  
[root@avgismatullin ~]# sestatus -bigrep httpd
```

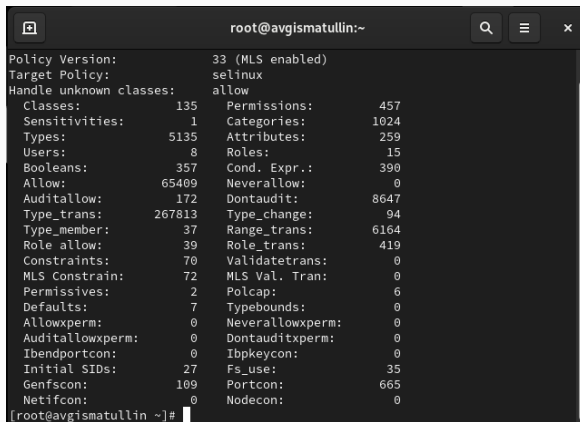
Рис. 2: Командная строка. Веб-сервер запущен в процессе

Проверка сервера



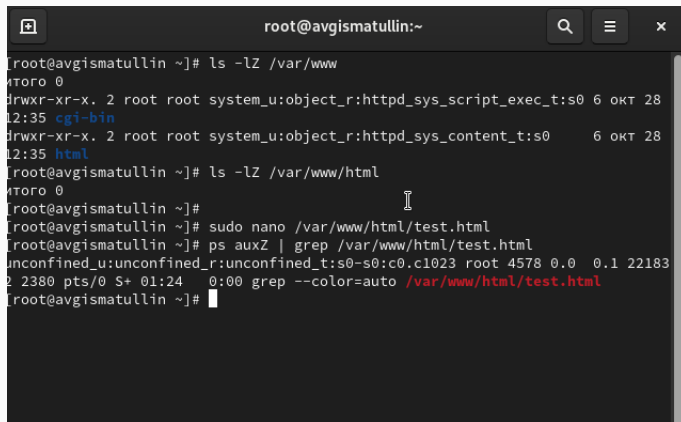
```
root@avgismatullin:~  
[root@avgismatullin ~]# sestatus -b | grep httpd  
httpd_anon_write off  
httpd_builtin_scripting on  
httpd_can_check_spam off  
httpd_can_connect_ftp off  
httpd_can_connect_ldap off  
httpd_can_connect_mythtv off  
httpd_can_connect_zabbix off  
httpd_can_manage_courier_spool 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
```

Рис. 3: Командная строка. Текущее состояние переключателей

A terminal window titled 'root@avgismatullin:~' displays the output of the 'seinfo' command. The output is organized into two columns. The left column lists various SELinux components and their counts, while the right column lists permissions and their counts. The terminal has a dark background with light-colored text. At the bottom, the prompt '[root@avgismatullin ~]#' is visible.

```
Policy Version:          33 (MLS enabled)
Target Policy:          selinux
Handle unknown classes: allow
Classes:                135
Sensitivities:          1
Types:                  5135
Users:                  8
Booleans:               357
Allow:                  65409
Auditallow:             172
Type_trans:             267813
Type_member:            37
Role_allow:             39
Constraints:            70
MLS Constrains:         72
Permissives:            2
Defaults:               7
Allowxperm:             0
Auditallowxperm:        0
Ibendportcon:           0
Initial SIDs:           27
Genfscon:               109
Netifcon:               0
Permissions:            457
Categories:             1024
Attributes:             259
Roles:                  15
Cond. Expr.:           390
Neverallow:             0
Dontaudit:             8647
Type_change:            94
Range_trans:            6164
Role_trans:             419
Validatetrans:          0
MLS Val. Tran:          0
Polcap:                 6
Typebounds:             0
Neverallowxperm:        0
Dontauditxperm:         0
Ibpkeycon:              0
Fs_use:                 35
Portcon:                665
Nodecon:                0
```

Рис. 4: Командная строка. Статистика о политике



```
root@avgismatullin:~  
[root@avgismatullin ~]# ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28  
12:35 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28  
12:35 html  
[root@avgismatullin ~]# ls -lZ /var/www/html  
итого 0  
[root@avgismatullin ~]#  
[root@avgismatullin ~]# sudo nano /var/www/html/test.html  
[root@avgismatullin ~]# ps auxZ | grep /var/www/html/test.html  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4578 0.0 0.1 22183  
2 2380 pts/0 S+ 01:24 0:00 grep --color=auto /var/www/html/test.html  
[root@avgismatullin ~]#
```

Рис. 5: Командная строка. Информация о директории и файле

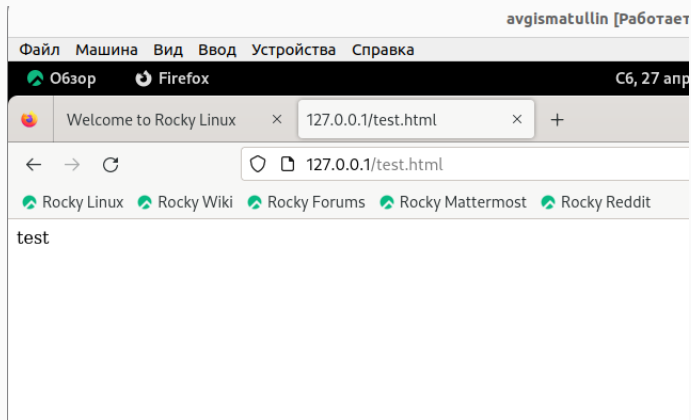
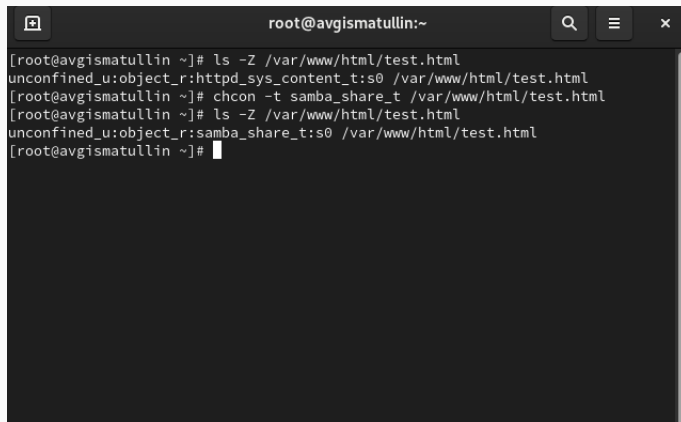


Рис. 6: Браузер. Проверка отображения файла

Изменение контекста

A terminal window titled 'root@avgismatullin:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
[root@avgismatullin ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@avgismatullin ~]# chcon -t samba_share_t /var/www/html/test.html
[root@avgismatullin ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@avgismatullin ~]#
```

Рис. 7: Командная строка. Изменение контекста файла

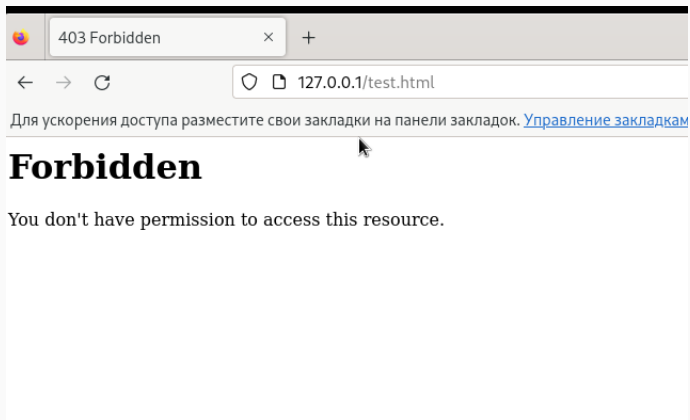
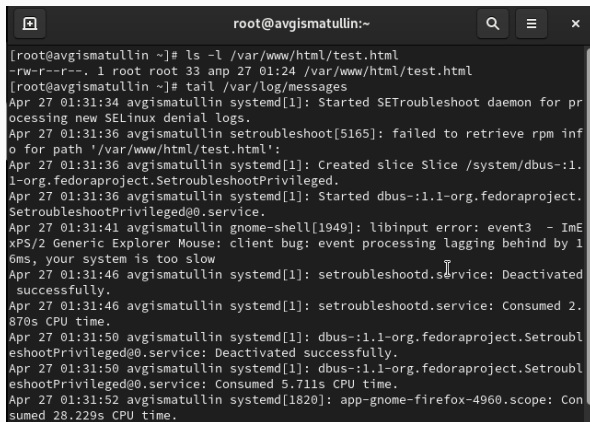


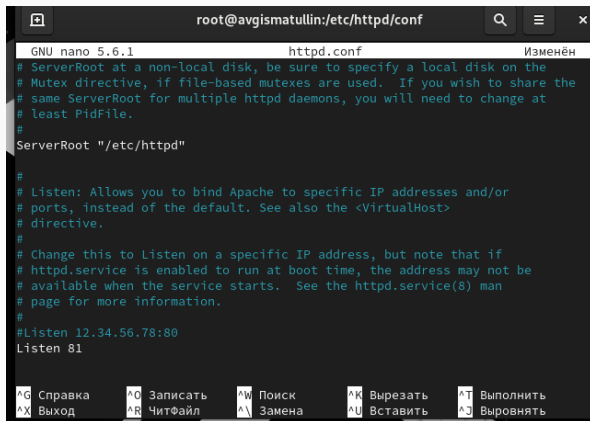
Рис. 8: Браузер. Попытка посетить сайт

A terminal window titled 'root@avgismatullin:~' with search, menu, and close icons. It shows the output of 'ls -l /var/www/html/test.html' and 'tail /var/log/messages'. The log messages show SELinux denial logs, systemd service status for setroubleshootd, and dbus service status.

```
[root@avgismatullin ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 anp 27 01:24 /var/www/html/test.html
[root@avgismatullin ~]# tail /var/log/messages
Apr 27 01:31:34 avgismatullin systemd[1]: Started SETroubleshoot daemon for pr
ocessing new SELinux denial logs.
Apr 27 01:31:36 avgismatullin setroubleshoot[5165]: failed to retrieve rpm inf
o for path '/var/www/html/test.html':
Apr 27 01:31:36 avgismatullin systemd[1]: Created slice Slice /system/dbus-:1.
1-org.fedoraproject.SetroubleshootPrivileged.
Apr 27 01:31:36 avgismatullin systemd[1]: Started dbus-:1.1-org.fedoraproject.
SetroubleshootPrivileged@0.service.
Apr 27 01:31:41 avgismatullin gnome-shell[1949]: libinput error: event3 - ImE
xPS/2 Generic Explorer Mouse: client bug: event processing lagging behind by 1
6ms, your system is too slow
Apr 27 01:31:46 avgismatullin systemd[1]: setroubleshootd.service: Deactivated
successfully.
Apr 27 01:31:46 avgismatullin systemd[1]: setroubleshootd.service: Consumed 2.
870s CPU time.
Apr 27 01:31:50 avgismatullin systemd[1]: dbus-:1.1-org.fedoraproject.Setroubl
eshootPrivileged@0.service: Deactivated successfully.
Apr 27 01:31:50 avgismatullin systemd[1]: dbus-:1.1-org.fedoraproject.Setroubl
eshootPrivileged@0.service: Consumed 5.711s CPU time.
Apr 27 01:31:52 avgismatullin systemd[1820]: app-gnome-firefox-4960.scope: Con
sumed 28.229s CPU time.
```

Рис. 9: Командная строка. Просмотр ошибок

Изменения файла



```
root@avgismatullin:/etc/httpd/conf
GNU nano 5.6.1 httpd.conf Изменён
# 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

^G Справка  ^O Записать  ^W Поиск    ^K Вырезать ^T Выполнить
^X Выход    ^R ЧитФайл  ^\ Замена  ^U Вставить ^J Выводить
```

Рис. 10: Командная строка. Изменение конфигурационного файла

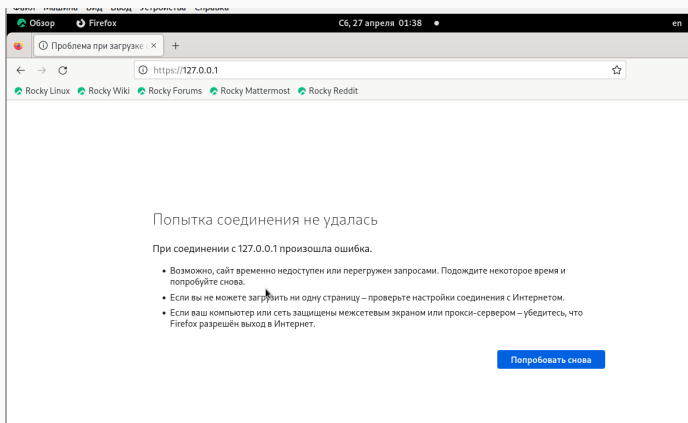



Рис. 11: Браузер. Попытка соединения

Просмотр ошибок

```
[root@avgismatullin conf]# sudo cat /var/log/httpd/access_log
127.0.0.1 - - [27/Apr/2024:01:15:22 +0300] "GET / HTTP/1.1" 403 7620 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:15:27 +0300] "GET /icons/poweredby.png HTTP/1.1"
200 15443 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:15:27 +0300] "GET /poweredby.png HTTP/1.1" 200 5714 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:15:28 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:26:01 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [27/Apr/2024:01:31:30 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@avgismatullin conf]#
```

Рис. 12: Командная строка. Просмотр ошибок

Проверка изменений



```
root@avgismatullin:/etc/httpd/conf

[root@avgismatullin conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@avgismatullin conf]# semanage port -l | grep httpd_port_t
[root@avgismatullin 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@avgismatullin conf]# service httpd reload
Redirecting to /bin/systemctl reload httpd.service
[root@avgismatullin conf]#
```

Рис. 13: Командная строка. Проверка изменений

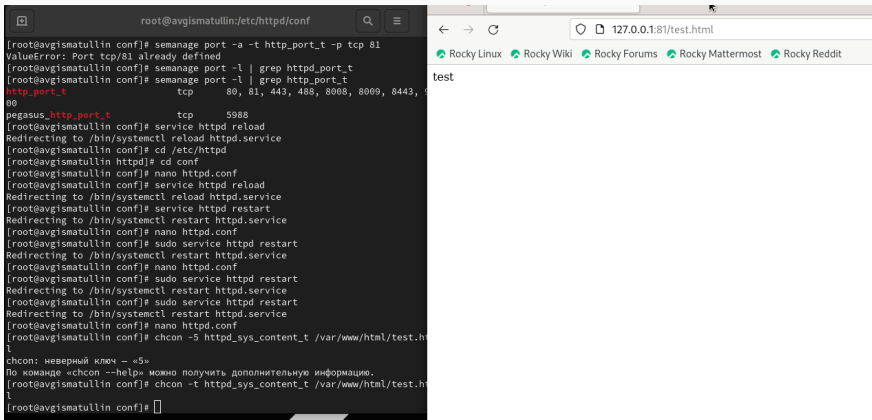
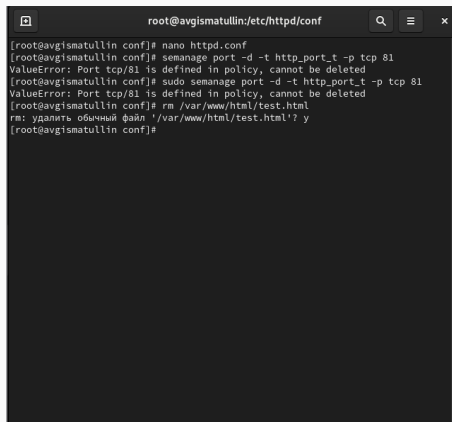


Рис. 14: Командная строка. Повторный запуск сервера



```
root@avgismatullin:/etc/httpd/conf
[root@avgismatullin conf]# nano httpd.conf
[root@avgismatullin conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@avgismatullin conf]# sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@avgismatullin conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html': y
[root@avgismatullin conf]#
```

Рис. 15: Командная строка. Удаление

Выводы по проделанной работе

Выводы по проделанной работе

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, а также проверена работа SELinux на практике совместно с веб-сервером Apache.