

Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Купатенко Владислав Георгиевич

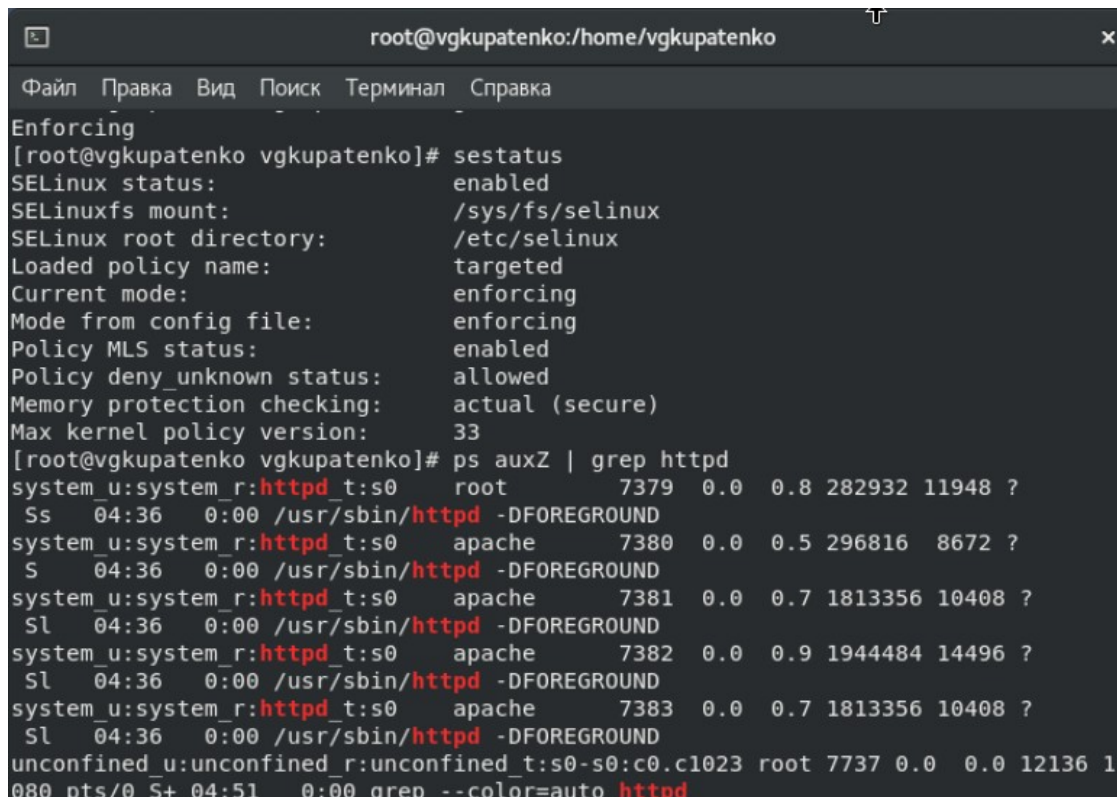
Table of Contents

Цель работы

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

Выполнение лабораторной работы

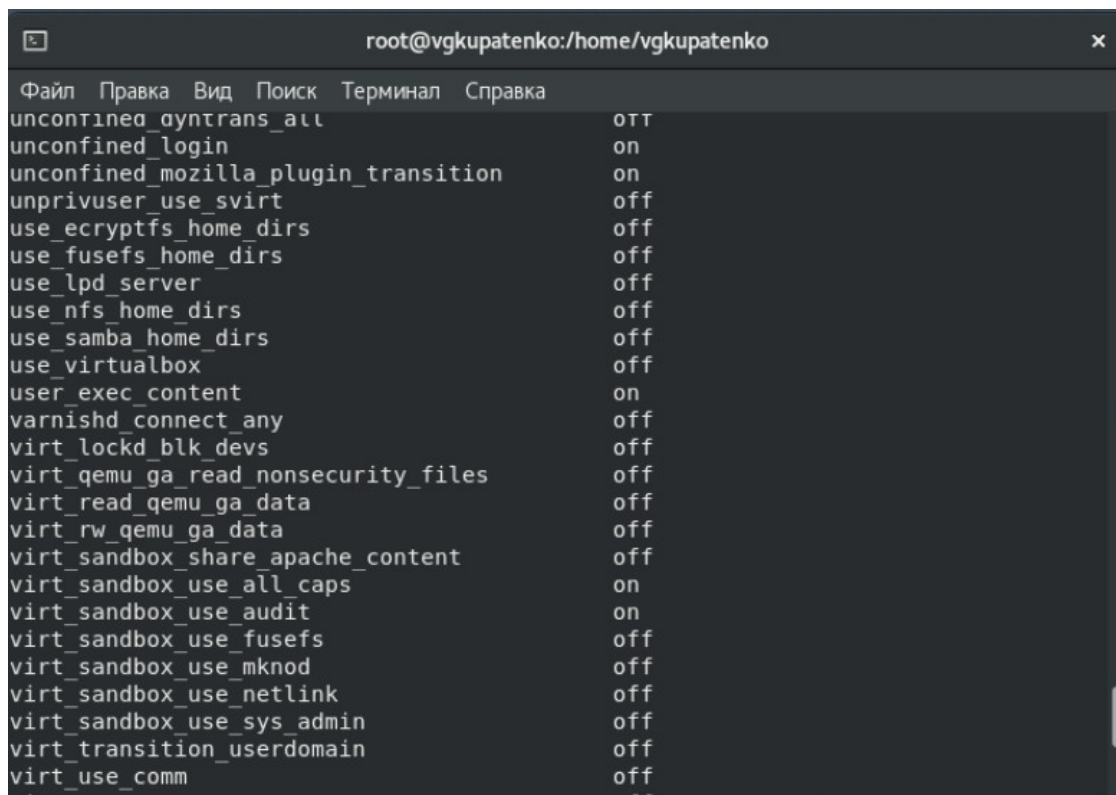
Проверил политики SELinux, статус веб-сервера, его контекст безопасности (рис.1).



```
root@vgkupatenko:/home/vgkupatenko
Файл Правка Вид Поиск Терминал Справка
Enforcing
[root@vgkupatenko vgkupatenko]# 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@vgkupatenko vgkupatenko]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      7379  0.0  0.8 282932 11948 ?
Ss  04:36   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   7380  0.0  0.5 296816  8672 ?
S   04:36   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   7381  0.0  0.7 1813356 10408 ?
Sl  04:36   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   7382  0.0  0.9 1944484 14496 ?
Sl  04:36   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   7383  0.0  0.7 1813356 10408 ?
Sl  04:36   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 7737 0.0 0.0 12136 1
080 pts/0 S+ 04:51   0:00 grep --color=auto httpd
```

Рисунок №1: Статусы

Проверил состояние переключателей SELinux (рис.2).



The screenshot shows a terminal window titled 'root@vgkupatenko:/home/vgkupatenko'. The window contains a list of SELinux processes and their status. The processes are listed on the left, and their status (on or off) is listed on the right. The status is 'on' for 'unconfined_login', 'unconfined_mozilla_plugin_transition', 'user_exec_content', 'virt_sandbox_use_all_caps', and 'virt_sandbox_use_audit'. All other processes have a status of 'off'.

Process	Status
unconfined_gyntrans_all	off
unconfined_login	on
unconfined_mozilla_plugin_transition	on
unprivuser_use_svirt	off
use_ecryptfs_home_dirs	off
use_fusefs_home_dirs	off
use_lpd_server	off
use_nfs_home_dirs	off
use_samba_home_dirs	off
use_virtualbox	off
user_exec_content	on
varnishd_connect_any	off
virt_lockd_blk_devs	off
virt_qemu_ga_read_nonsecurity_files	off
virt_read_qemu_ga_data	off
virt_rw_qemu_ga_data	off
virt_sandbox_share_apache_content	off
virt_sandbox_use_all_caps	on
virt_sandbox_use_audit	on
virt_sandbox_use_fusefs	off
virt_sandbox_use_mknod	off
virt_sandbox_use_netlink	off
virt_sandbox_use_sys_admin	off
virt_transition_userdomain	off
virt_use_comm	off

Рисунок №2: Переключатели

Статистика по политике Selinux (рис.3).

```
root@vgkupatenko:/home/vgkupatenko
Файл Правка Вид Поиск Терминал Справка
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 Constrains: 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@vgkupatenko vgkupatenko]#
```

Рисунок №3: Статистика по политике Selinux

Тип файлов и поддиректорий, круг пользователей в каталоге /var/www (рис. 4).

```
root@vgkupatenko:/home/vgkupatenko
Файл Правка Вид Поиск Терминал Справка
[root@vgkupatenko vgkupatenko]# ls -lz /var/www
ls: неверный ключ - «z»
По команде «ls --help» можно получить дополнительную информацию.
[root@vgkupatenko vgkupatenko]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 11 23
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 11 23
:58 html
[root@vgkupatenko vgkupatenko]# ls -lZ /var/www/html
итого 0
[root@vgkupatenko vgkupatenko]# ls -l /var/www/html
итого 0
[root@vgkupatenko vgkupatenko]# ls -l /var/www
итого 0
drwxr-xr-x. 2 root root 6 ноя 11 23:58 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 11 23:58 html
[root@vgkupatenko vgkupatenko]#
```

Рисунок №4: /var/www

Заполнен файл test.html (рис. 5).

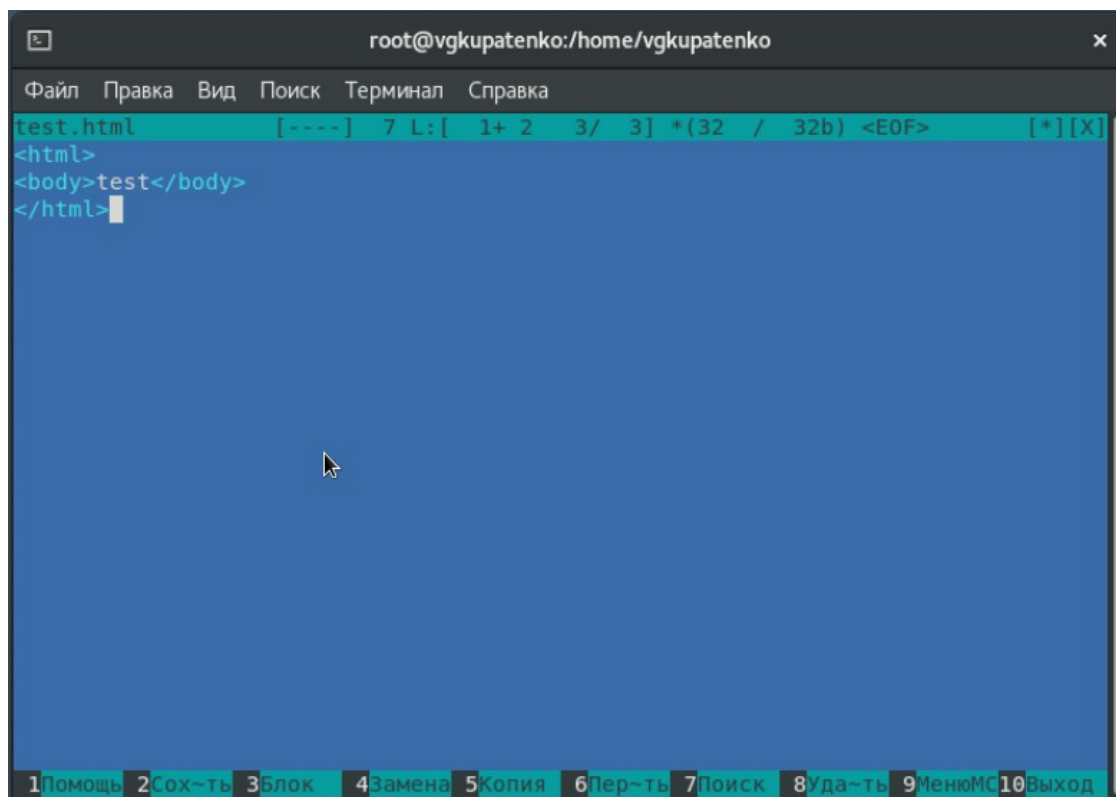
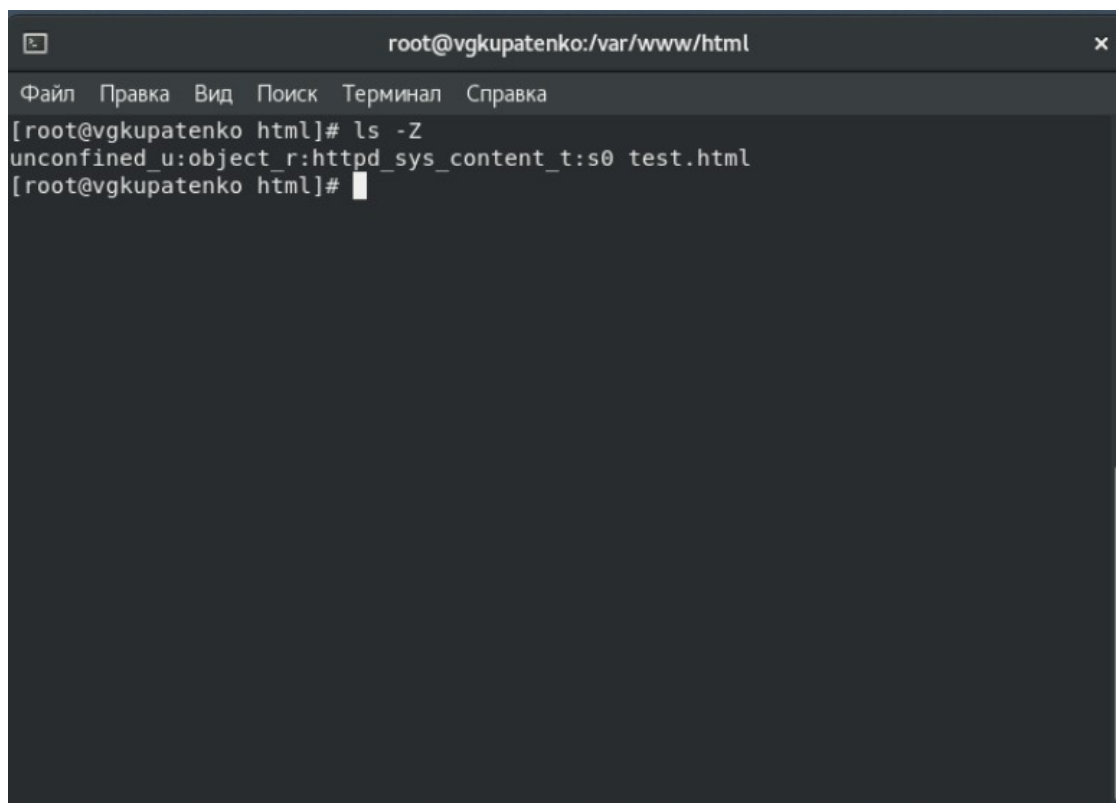


Рисунок №5: test.html

Контекст файла test.html (рис. 6).

A terminal window titled 'root@vgkupatenko:/var/www/html' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the command '[root@vgkupatenko html]# ls -Z' and its output 'unconfined_u:object_r:httpd_sys_content_t:s0 test.html'. The prompt '[root@vgkupatenko html]#' is followed by a cursor.

```
root@vgkupatenko:/var/www/html
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@vgkupatenko html]# ls -Z
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@vgkupatenko html]#
```

Рисунок №6: Контекст файла test.html

Отображение файла на веб-странице (рис. 7).

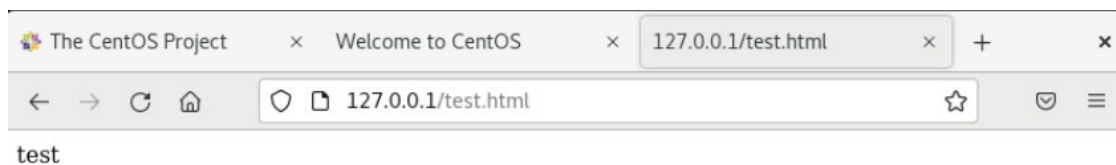


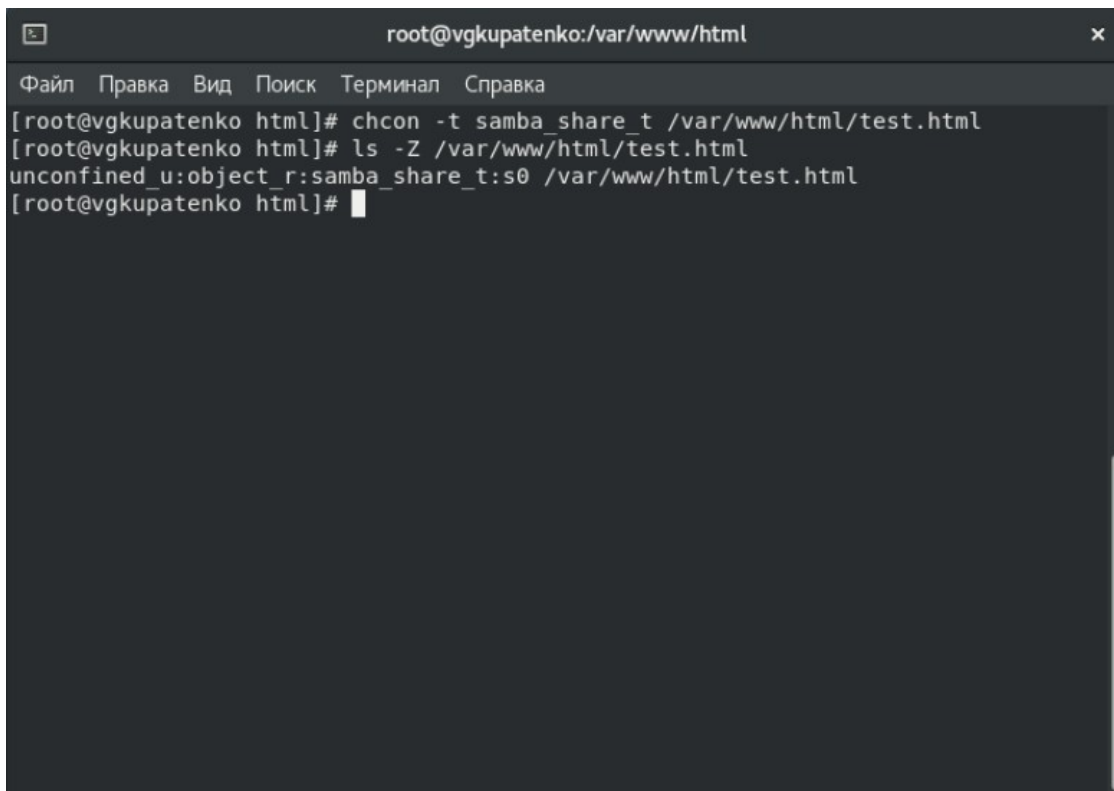
Рисунок №7: Отображение файла test.html

Мануал для httpd_selinux отсутствует (рис. 8).



Рисунок №8: man httpd_selinux

Изменение контекста файла test.html (рис. 9).



```
root@vgkupatenko:/var/www/html
Файл Правка Вид Поиск Терминал Справка
[root@vgkupatenko html]# chcon -t samba_share_t /var/www/html/test.html
[root@vgkupatenko html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@vgkupatenko html]#
```

Рисунок №9: Новый контекст файла *test.html*

Попытка открыть файл через браузер (рис. 10).



Forbidden

You don't have permission to access this resource.



Рисунок №10: Отсутствие доступа

Права доступа и лог файл сервера (рис. 11).


```
root@vgkupatenko:/var/www/html
Файл Правка Вид Поиск Терминал Справка
-rw-r--r--. 1 root root 32 ноя 27 05:03 /var/www/html/test.html
[root@vgkupatenko html]# tail /var/log/messages
Nov 27 05:13:50 vgkupatenko org.gnome.Shell.desktop[5602]: libinput error: client bug: timer event3 debounce short: scheduled expiry is in the past (-113ms), your system is too slow
Nov 27 05:13:50 vgkupatenko setroubleshoot[9407]: failed to retrieve rpm info for /var/www/html/test.html
Nov 27 05:13:50 vgkupatenko dbus-daemon[802]: [system] Activating service name='org.fedoraproject.SetroubleshootPrivileged' requested by ':1.505' (uid=979 pid=9407 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:system_r:setroubleshootd_t:s0-s0:c0.c1023") (using servicehelper)
Nov 27 05:13:51 vgkupatenko dbus-daemon[802]: [system] Successfully activated service 'org.fedoraproject.SetroubleshootPrivileged'
Nov 27 05:13:52 vgkupatenko setroubleshoot[9407]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 33f4c935-4fc1-48e5-8f57-9eea476faaa7
Nov 27 05:13:52 vgkupatenko setroubleshoot[9407]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions 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***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as
```

Рисунок №11: Лог файл messages

Изменение порта с 80 на 81 в файле конфигурации (рис. 12).

```
root@vgkupatenko:/etc/httpd/conf
Файл  Правка  Вид  Поиск  Терминал  Справка
httpd.conf  [----]  9  L:[ 29+16  45/357]  *(1919/11888b)  0010  0x00A  [*][X]
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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
1Помощь 2Сох-ть 3Блок 4Замена 5Копия 6Пер-ть 7Поиск 8Уда-ть 9МенюМС 10Выход
```

Рисунок №12: httpd.conf

Попытка открыть файл через браузер безуспешна, так как был изменен порт (рис. 13).

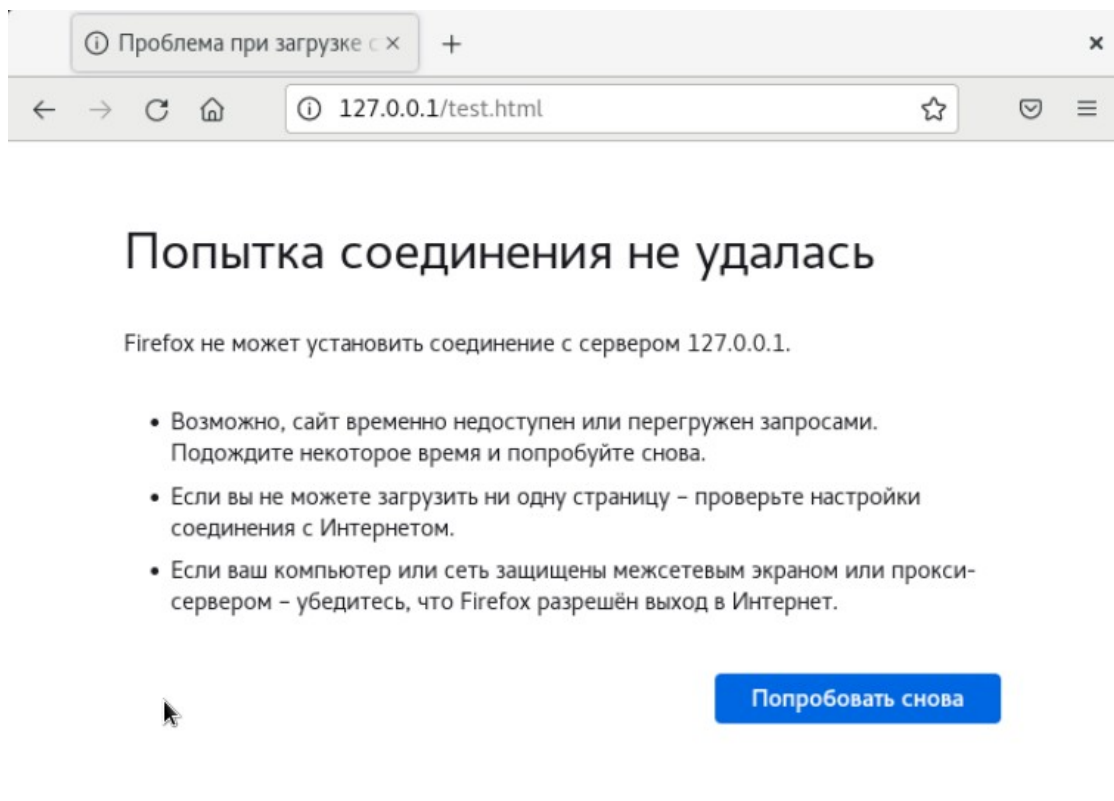
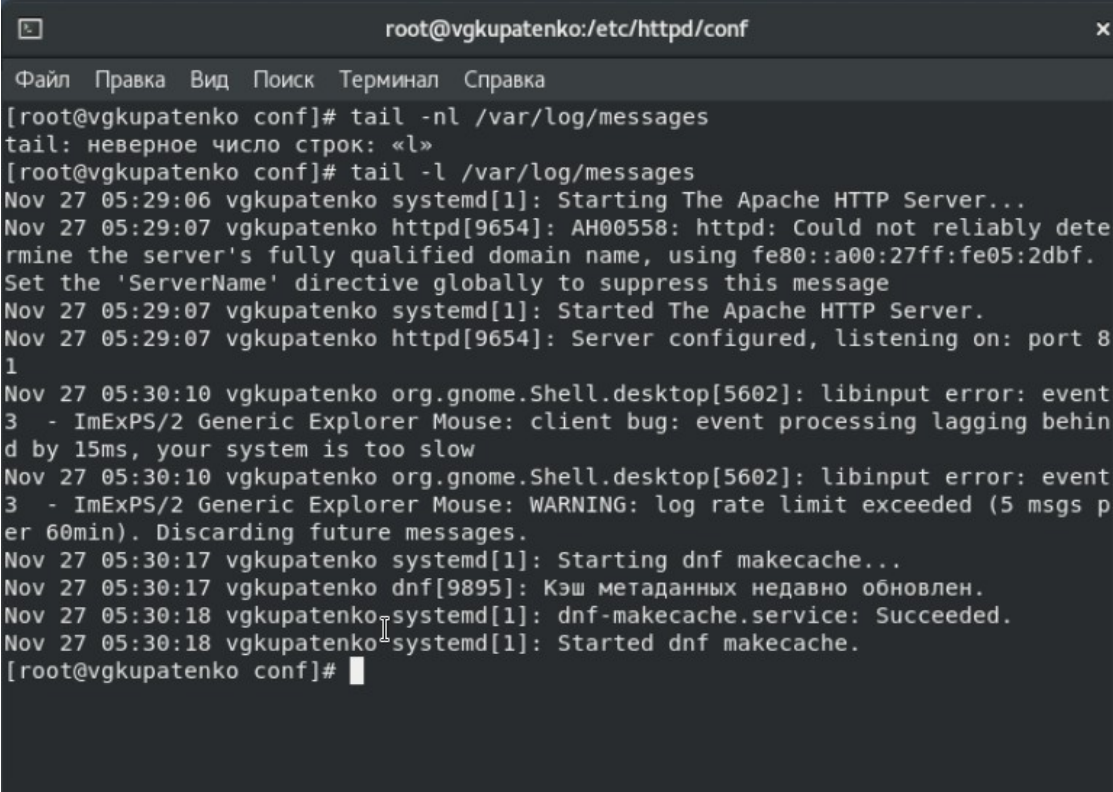


Рисунок №13: Отсутствие соединения

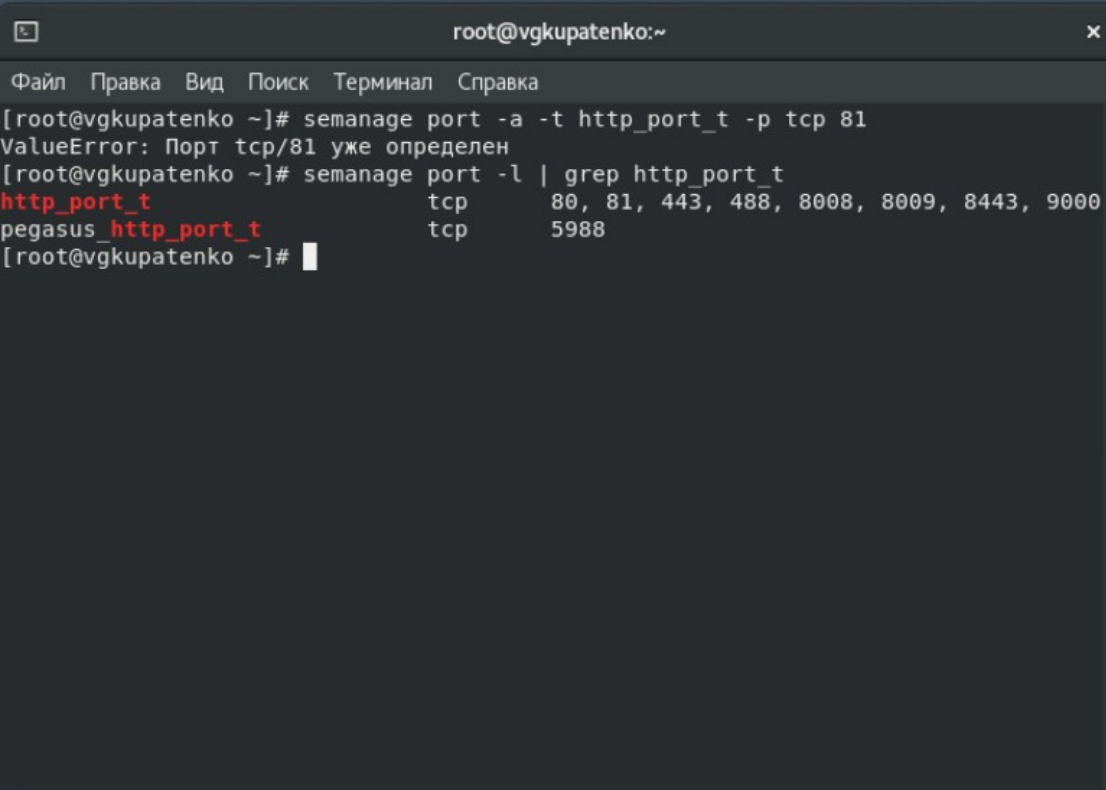
Log messages. (рис. 14).



```
root@vgkupatenko:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
[root@vgkupatenko conf]# tail -nl /var/log/messages
tail: неверное число строк: «l»
[root@vgkupatenko conf]# tail -l /var/log/messages
Nov 27 05:29:06 vgkupatenko systemd[1]: Starting The Apache HTTP Server...
Nov 27 05:29:07 vgkupatenko httpd[9654]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fe05:2dbf. Set the 'ServerName' directive globally to suppress this message
Nov 27 05:29:07 vgkupatenko systemd[1]: Started The Apache HTTP Server.
Nov 27 05:29:07 vgkupatenko httpd[9654]: Server configured, listening on: port 81
Nov 27 05:30:10 vgkupatenko org.gnome.Shell.desktop[5602]: libinput error: event 3 - ImExPS/2 Generic Explorer Mouse: client bug: event processing lagging behind by 15ms, your system is too slow
Nov 27 05:30:10 vgkupatenko org.gnome.Shell.desktop[5602]: libinput error: event 3 - ImExPS/2 Generic Explorer Mouse: WARNING: log rate limit exceeded (5 msgs per 60min). Discarding future messages.
Nov 27 05:30:17 vgkupatenko systemd[1]: Starting dnf makecache...
Nov 27 05:30:17 vgkupatenko dnf[9895]: Кэш метаданных недавно обновлен.
Nov 27 05:30:18 vgkupatenko systemd[1]: dnf-makecache.service: Succeeded.
Nov 27 05:30:18 vgkupatenko systemd[1]: Started dnf makecache.
[root@vgkupatenko conf]#
```

Рисунок №14: Лог messages.

Определение порта 81 (рис. 15).

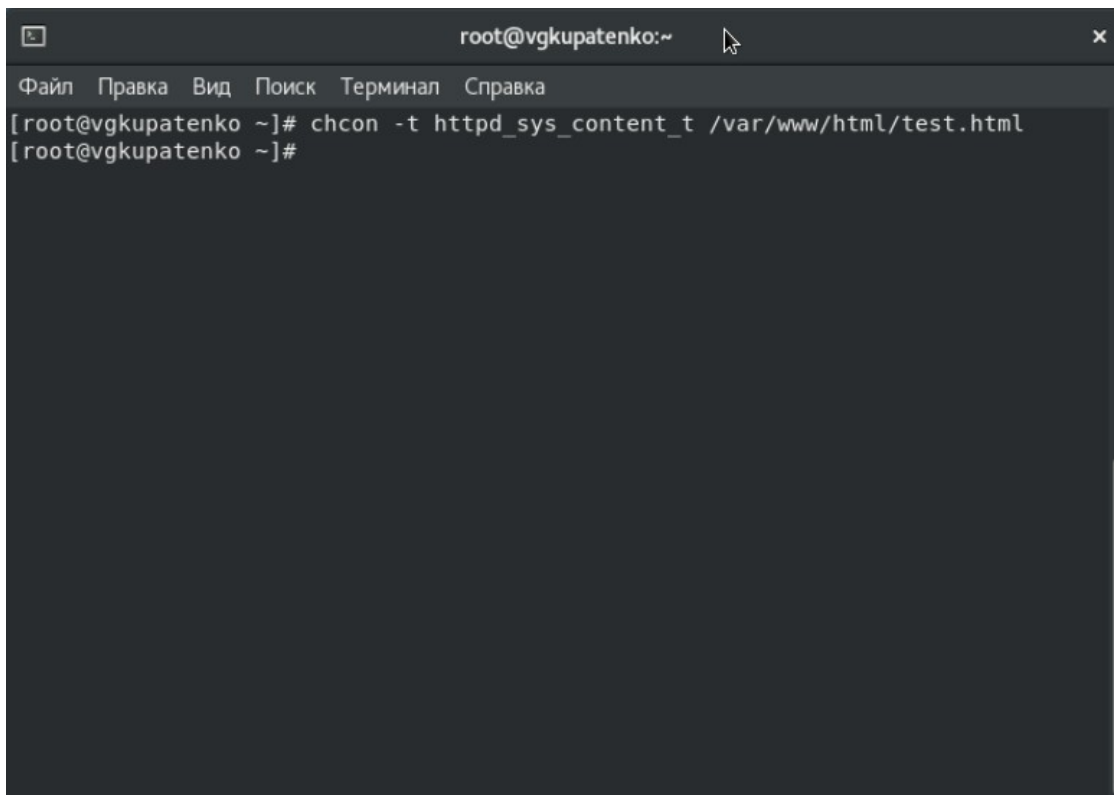


A terminal window titled "root@vgkupatenko:~" with a menu bar containing "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal shows the following commands and output:

```
[root@vgkupatenko ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@vgkupatenko ~]# 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
```

Рисунок №15: Определение порта 81

Возвращение контекста файлу test (рис. 16).



```
root@vgkupatenko:~  
Файл Правка Вид Поиск Терминал Справка  
[root@vgkupatenko ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@vgkupatenko ~]#
```

Рисунок №16: Возвращение контекста файлу test

Попытка открыть файл через браузер по порту 81 (рис. 17).

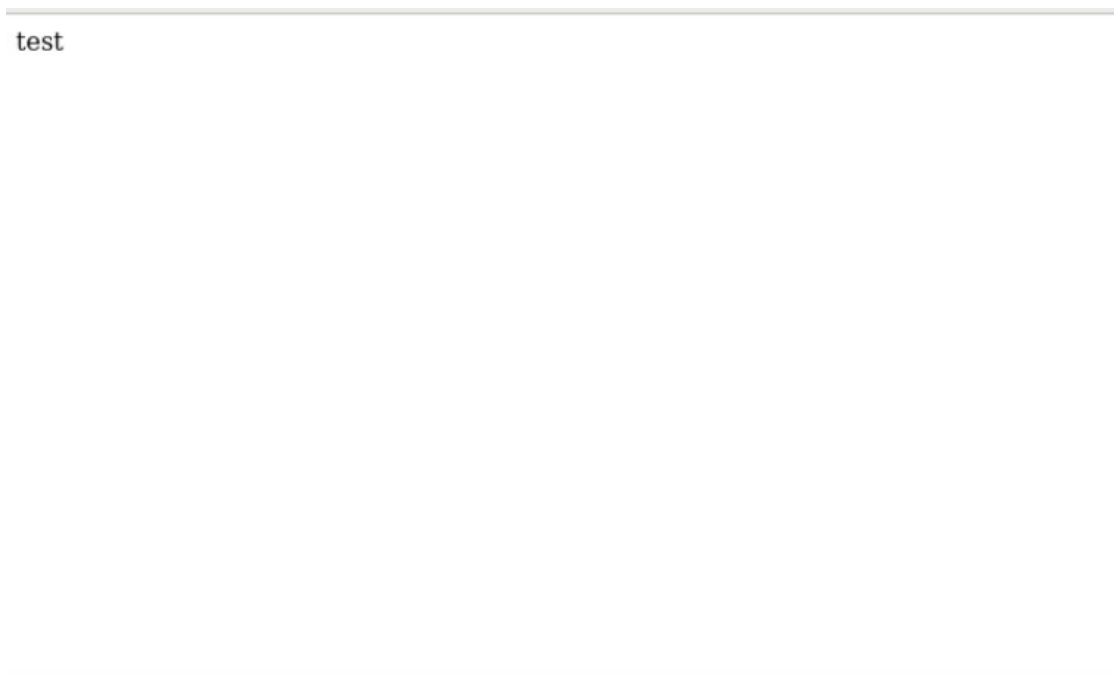
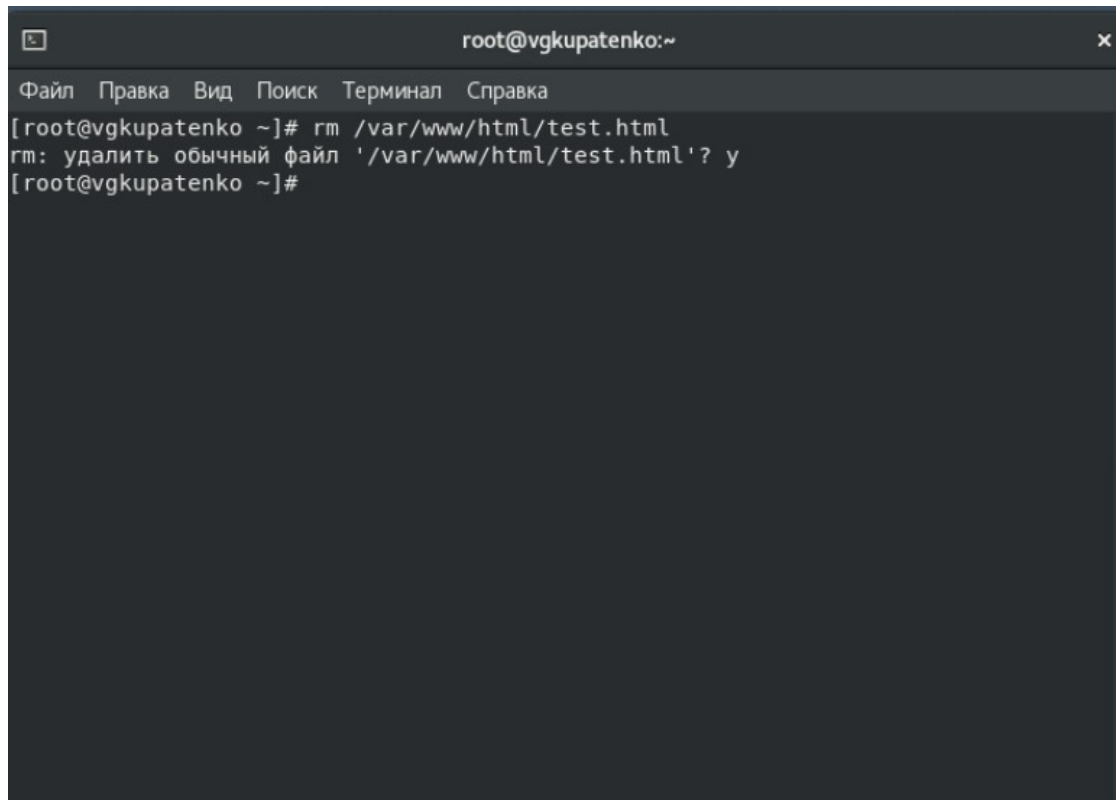


Рисунок №17: Доступ по порту 81

Файл конфигурации был изменен и приведен к порту 80. Удаление файла test.html (рис. 18).

A screenshot of a terminal window titled 'root@vgkupatenko:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the command 'rm /var/www/html/test.html' being executed. The output is 'rm: удалить обычный файл '/var/www/html/test.html'? y'. The prompt returns to '[root@vgkupatenko ~]#'.

```
root@vgkupatenko:~  
Файл Правка Вид Поиск Терминал Справка  
[root@vgkupatenko ~]# rm /var/www/html/test.html  
rm: удалить обычный файл '/var/www/html/test.html'? y  
[root@vgkupatenko ~]#
```

Рисунок №18: Удаление файла test.html

Выводы

Были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работу SELinux на практике совместно с веб-сервером Apache.