

Отчёт

по лабораторной работе 6

Кочетов Андрей Владимирович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	14

List of Figures

3.1	рис.1. Режимы	7
3.2	рис.2. Запуск сервера	7
3.3	рис.3. Процессы	8
3.4	рис.4. Состояние	8
3.5	рис.5. Статистика и типы файлов	9
3.6	рис.6. Создание файла	9
3.7	рис.7. Файл	10
3.8	рис.8. Смена контекста и тест веб-сервера	10
3.9	рис.9. Анализ	11
3.10	рис.10. Смена порта	11
3.11	рис.11. Сбой сервера	11
3.12	рис.12. Логи	12
3.13	рис.13. Semaпage	12
3.14	рис.14. Работа с командами	13
3.15	рис.15. Удаление	13

List of Tables

1 Цель работы

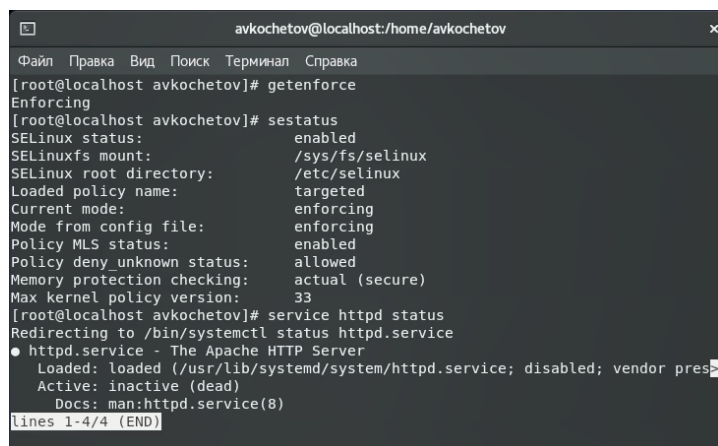
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Задание

Работа с сервером arach и настройка портов.

3 Выполнение лабораторной работы

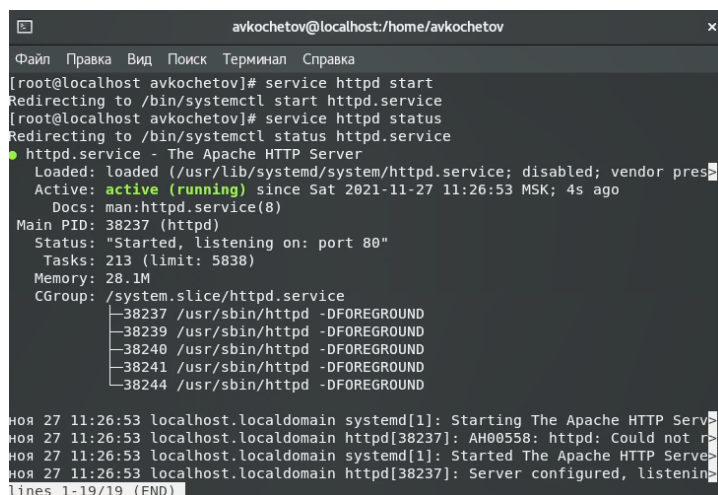
1. Проверил режим работы SELinux при помощи 2 команд(рис.1).



```
avkochetov@localhost:/home/avkochetov
[root@localhost avkochetov]# getenforce
Enforcing
[root@localhost avkochetov]# 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@localhost avkochetov]# 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 pres
   Active: inactive (dead)
   Docs: man:httpd.service(8)
lines 1-4/4 (END)
```

Figure 3.1: рис.1. Режимы

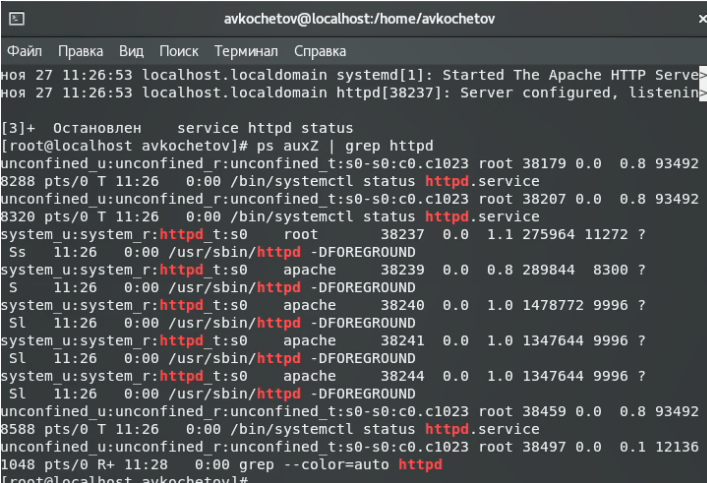
2. Запустил сервер и проверил его работоспособность(рис.2).



```
avkochetov@localhost:/home/avkochetov
[root@localhost avkochetov]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost avkochetov]# 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 pres
   Active: active (running) since Sat 2021-11-27 11:26:53 MSK; 4s ago
   Docs: man:httpd.service(8)
   Main PID: 38237 (httpd)
   Status: "Started, listening on: port 80"
   Tasks: 213 (limit: 5838)
   Memory: 28.1M
   CGroup: /system.slice/httpd.service
           └─38237 /usr/sbin/httpd -DFOREGROUND
             └─38239 /usr/sbin/httpd -DFOREGROUND
               └─38240 /usr/sbin/httpd -DFOREGROUND
                 └─38241 /usr/sbin/httpd -DFOREGROUND
                   └─38244 /usr/sbin/httpd -DFOREGROUND
ноя 27 11:26:53 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv
ноя 27 11:26:53 localhost.localdomain httpd[38237]: AH00558: httpd: Could not r
ноя 27 11:26:53 localhost.localdomain systemd[1]: Started The Apache HTTP Serv
ноя 27 11:26:53 localhost.localdomain httpd[38237]: Server configured, listeni
lines 1-19/19 (END)
```

Figure 3.2: рис.2. Запуск сервера

3. Нашел веб-сервер Apache в списке процессов(рис.3).

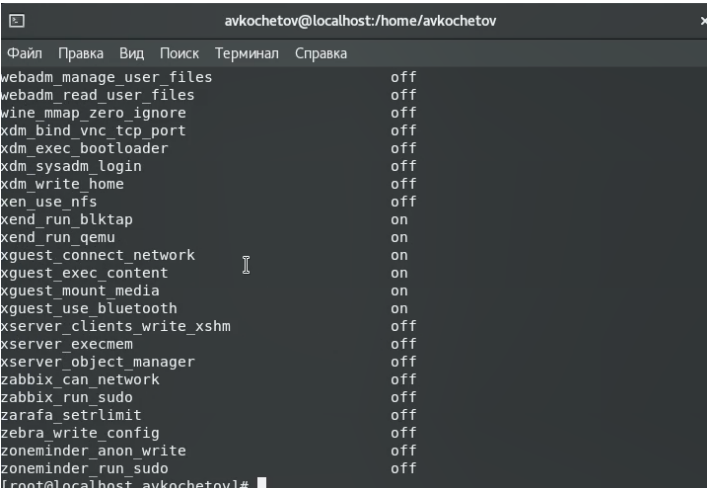


```
avkochetov@localhost:/home/avkochetov
Файл Правка Вид Поиск Терминал Справка
ноя 27 11:26:53 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 27 11:26:53 localhost.localdomain httpd[38237]: Server configured, listening.

[3]+ Остановлен service httpd status
[root@localhost avkochetov]# ps auxZ | grep httpd
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 38179 0.0 0.8 93492
8288 pts/0 T 11:26 0:00 /bin/systemctl status httpd.service
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 38207 0.0 0.8 93492
8320 pts/0 T 11:26 0:00 /bin/systemctl status httpd.service
system u:system r:httpd_t:s0 root 38237 0.0 1.1 275964 11272 ?
Ss 11:26 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd_t:s0 apache 38239 0.0 0.8 289844 8300 ?
S 11:26 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd_t:s0 apache 38240 0.0 1.0 1478772 9996 ?
Sl 11:26 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd_t:s0 apache 38241 0.0 1.0 1347644 9996 ?
Sl 11:26 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd_t:s0 apache 38244 0.0 1.0 1347644 9996 ?
Sl 11:26 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 38459 0.0 0.8 93492
8588 pts/0 T 11:26 0:00 /bin/systemctl status httpd.service
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 38497 0.0 0.1 12136
1048 pts/0 R+ 11:28 0:00 grep --color=auto httpd
[root@localhost avkochetov]#
```

Figure 3.3: рис.3. Процессы

4. Посмотрел текущее состояние переключателей SELinux для Apache(рис.4).



```
avkochetov@localhost:/home/avkochetov
Файл Правка Вид Поиск Терминал Справка
webadm_manage_user_files off
webadm_read_user_files off
wine_mmap_zero_ignore off
xdm_bind_vnc_tcp_port off
xdm_exec_bootloader off
xdm_sysadm_login off
xdm_write_home off
xen_use_nfs off
xend_run_blktp on
xend_run_qemu on
xguest_connect_network on
xguest_exec_content on
xguest_mount_media on
xguest_use_bluetooth on
xserver_clients_write_xshm off
xserver_execmem off
xserver_object_manager off
zabbix_can_network off
zabbix_run_sudo off
zarafa_setrlimit off
zebra_write_config off
zoneminder_anon_write off
zoneminder_run_sudo off
[root@localhost avkochetov]#
```

Figure 3.4: рис.4. Состояние

5. Посмотрел статистику по политике, тип файлов и поддиректорий и тип файлов, находящихся в другой директории(рис.5).


```

avkochetov@localhost:/home/avkochetov
Файл Правка Вид Поиск Терминал Справка
Auditallow: 166 Dontaudit: 10362
Type_trans: 252747 Type_change: 87
Type_member: 35 Range_trans: 6015
Role_allow: 37 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: 33
Genfscon: 106 Portcon: 640
Netifcon: 0 Nodecon: 0

[root@localhost avkochetov]# ls -lZ /var/www
итого 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@localhost avkochetov]# ls -lZ /var/www/html
итого 0
[root@localhost avkochetov]#

```

Figure 3.5: рис.5. Статистика и типы файлов

6. Создал html-файл, проверил контекст файла(рис.6).

```

avkochetov@localhost:/home/avkochetov
Файл Правка Вид Поиск Терминал Справка
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 33
Genfscon: 106 Portcon: 640
Netifcon: 0 Nodecon: 0

[root@localhost avkochetov]# ls -lZ /var/www
итого 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@localhost avkochetov]# ls -lZ /var/www/html
итого 0
[root@localhost avkochetov]# nano /var/www/html/test.html
[root@localhost avkochetov]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@localhost avkochetov]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 1
1:37 test.html
[root@localhost avkochetov]#

```

Figure 3.6: рис.6. Создание файла

7. Обратился к файлу через веб-сервер(рис.7).

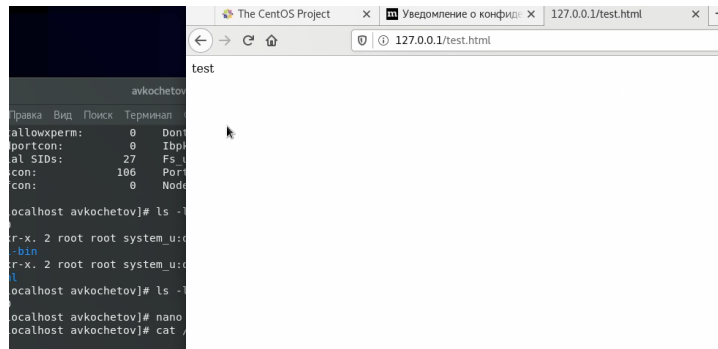


Figure 3.7: рис.7. Файл

8. Проверил контекст командой `ls -Z`, изменил контекст на другой, убедился в смене и проверил работоспособность веб-сервера (рис.8).

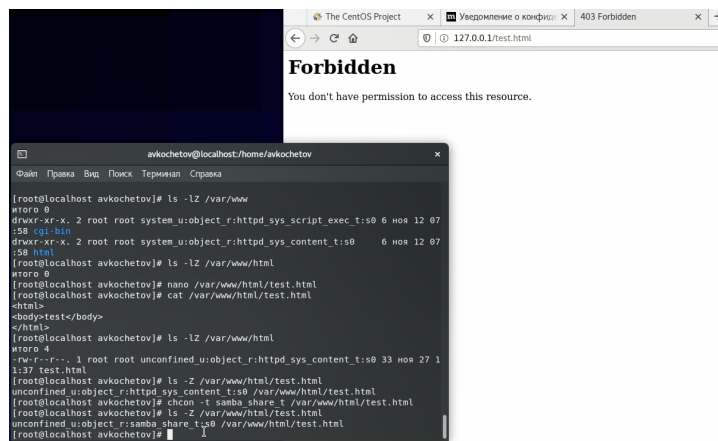


Figure 3.8: рис.8. Смена контекста и тест веб-сервера

9. Проанализировал ситуацию и посмотрел логи(рис.9).

```
avkochetov@localhost:/home/avkochetov
Файл Правка Вид Поиск Терминал Справка
/htpdd from getattr access on the file /var/www/html/test.html.#012#012***** Pl
ugin restorecon (92.2 confidence) suggests *****#012#012If
you want to fix the label. #012/var/www/html/test.html default label should be h
ttpd 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 whi
ch case try to change the following command accordingly.#012Do#012# /sbin/restor
econ -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confid
ence) suggests *****#012#012If you want to treat test.html as p
ublic content#012Then you need to change the label on test.html to public conten
t t or public_content_rw t.#012Do#012# semanage fcontext -a -t public_content_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 default.#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# semodul
e -X 300 -i my-httpd.pp#012
Nov 27 11:44:33 localhost org.gnome.Shell.desktop[2003]: libinput error: client
bug: timer event3 debounce: scheduled expiry is in the past (-10ms), your system
is too slow
Nov 27 11:44:33 localhost org.gnome.Shell.desktop[2003]: libinput error: client
bug: timer event3 debounce short: scheduled expiry is in the past (-23ms), your
system is too slow
[root@localhost avkochetov]# tail /var/log/audit/audit.log
```

Figure 3.9: рис.9. Анализ

10. Сменил порт на TCP-порт 81(рис.10).

```
# Interpreted as '/log/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# 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 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
```

Figure 3.10: рис.10. Смена порта

11. Выполнил перезапуск сервера и увидел сбой(рис.11).

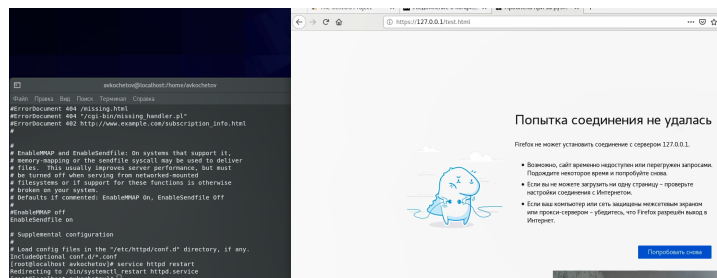
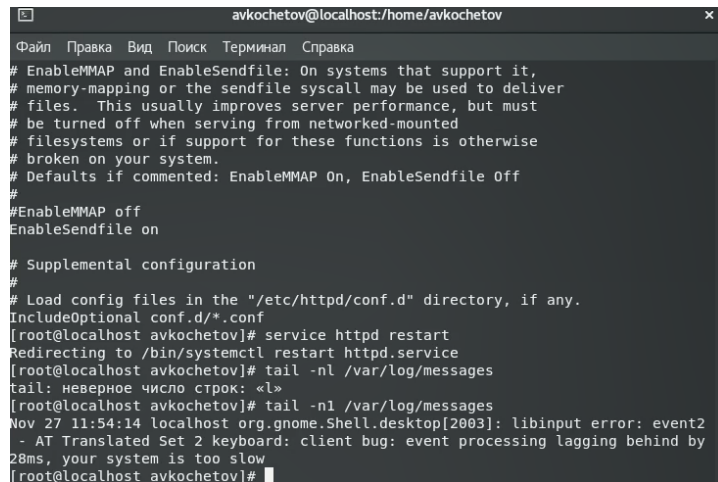


Figure 3.11: рис.11. Сбой сервера

12. Проанализировал log-файлы(рис.12).

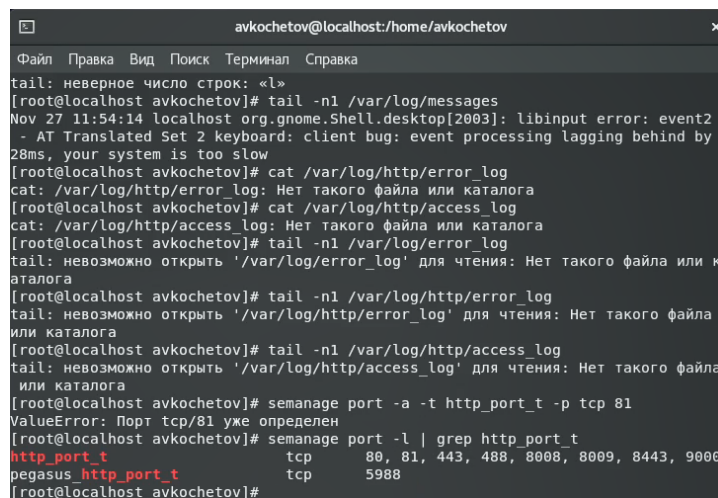


```
avkochetov@localhost:/home/avkochetov
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
[root@localhost avkochetov]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost avkochetov]# tail -nl /var/log/messages
tail: неверное число строк: «1»
[root@localhost avkochetov]# tail -nl /var/log/messages
Nov 27 11:54:14 localhost org.gnome.Shell.desktop[2003]: libinput error: event2
- AT Translated Set 2 keyboard: client bug: event processing lagging behind by
28ms, your system is too slow
[root@localhost avkochetov]#
```

Figure 3.12: рис.12. Логи

13. Выполнил программу semanage и проверил список портов, где увидел порт 81 в списке(рис.13).



```
avkochetov@localhost:/home/avkochetov
tail: неверное число строк: «1»
[root@localhost avkochetov]# tail -nl /var/log/messages
Nov 27 11:54:14 localhost org.gnome.Shell.desktop[2003]: libinput error: event2
- AT Translated Set 2 keyboard: client bug: event processing lagging behind by
28ms, your system is too slow
[root@localhost avkochetov]# cat /var/log/http/error_log
cat: /var/log/http/error_log: Нет такого файла или каталога
[root@localhost avkochetov]# cat /var/log/http/access_log
cat: /var/log/http/access_log: Нет такого файла или каталога
[root@localhost avkochetov]# tail -nl /var/log/error_log
tail: невозможно открыть '/var/log/error_log' для чтения: Нет такого файла или каталога
[root@localhost avkochetov]# tail -nl /var/log/http/error_log
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
[root@localhost avkochetov]# tail -nl /var/log/http/access_log
tail: невозможно открыть '/var/log/http/access_log' для чтения: Нет такого файла или каталога
[root@localhost avkochetov]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@localhost avkochetov]# 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@localhost avkochetov]#
```

Figure 3.13: рис.13. Semanage

14. Снова зашел на сервер и увидел, что он работает. Вернул контекст и listen 80, и удалил привязку к 81(рис.14).

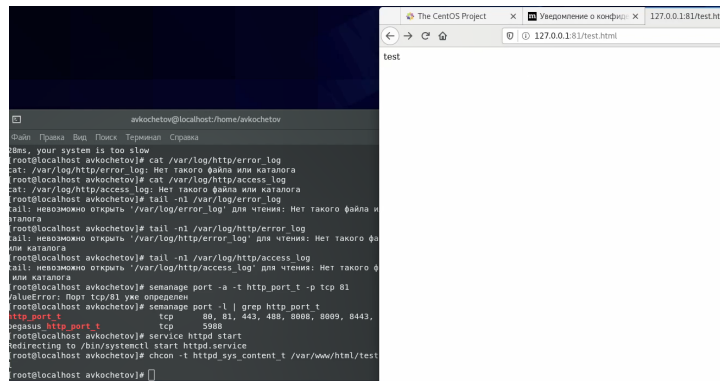


Figure 3.14: рис.14. Работа с командами

15. Удалил файл test.html(рис.15).

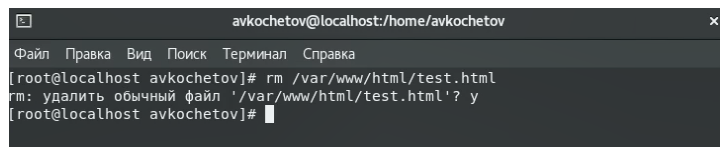


Figure 3.15: рис.15. Удаление

4 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux¹. Проверил работу SELinx на практике совместно с веб-сервером Apache.