

Отчёт по лабораторной работе №6

Информационная безопасность

Мандатное разграничение прав в Linux

Выполнил: Махорин Иван Сергеевич,
НПИБд-02-21, 1032211221

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Вывод	18
5	Список литературы. Библиография	19

Список иллюстраций

3.1	Проверка работы в режиме enforcing политики targeted	7
3.2	Проверка работы веб-сервера	8
3.3	Нахождение веб-сервера Apache в списке процессов и определение его контекста безопасности	8
3.4	Просмотр текущего состояния переключателей SELinux	9
3.5	Просмотр статистики по политике	10
3.6	Определение типов файлов и поддиректорий	10
3.7	Определение типов файлов и поддиректорий	11
3.8	Создание файла с содержанием	11
3.9	Проверка контекста созданного файла	12
3.10	Изучение справки и проверка контекста файла	12
3.11	Изменение контекста файла и проверка	12
3.12	Попытка получения доступа к файлу через веб-сервер	13
3.13	Просмотр log-файлов веб-сервера Apache и системного лог-файла	13
3.14	Попытка запуска веб-сервера Apache на прослушивание TCP-порта 81	14
3.15	Перезапуск веб-сервера Apache	14
3.16	Анализ лог-файлов	15
3.17	Выполнение команды и проверка списка портов	15
3.18	Возвращение контекста httpd_sys_content_t к файлу /var/www/html/test.html и попытка получения доступа к файлу через веб-сервис	16
3.19	Исправление конфигурационного файла apache	16
3.20	Удаление привязки http_port_t к 81 порту и проверка	17
3.21	Удаление файла /var/www/html/test.html	17

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 Теоретическое введение

1. **SELinux (Security-Enhanced Linux)** обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена.

SELinux имеет три основных режим работы:

- **Enforcing:** режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- **Permissive:** в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- **Disabled:** полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [1].

2. **Apache** — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA).

Для чего нужен Apache сервер:

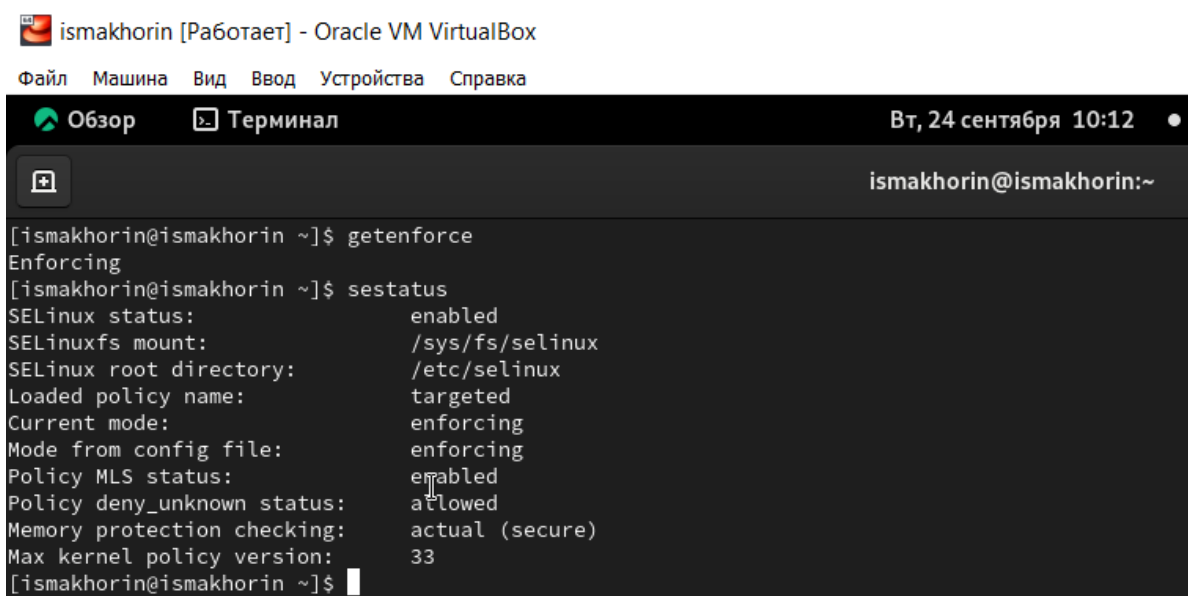
- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

Более подробно см. в [2].

3 Выполнение лабораторной работы

Войдём в систему и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`

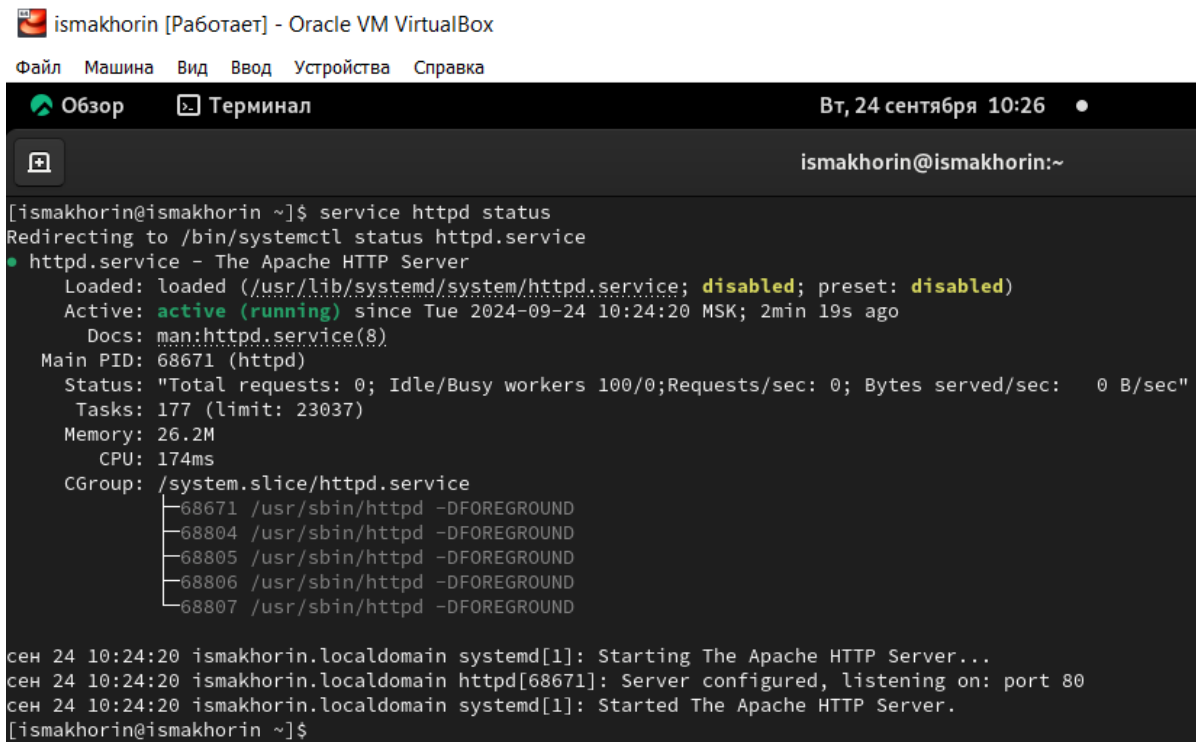


The screenshot shows a terminal window titled "ismakhorin [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar are tabs for "Обзор" and "Терминал", with the "Терминал" tab selected. The terminal shows the following commands and output:

```
[ismakhorin@ismakhorin ~]$ getenforce
Enforcing
[ismakhorin@ismakhorin ~]$ 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
[ismakhorin@ismakhorin ~]$
```

Рис. 3.1: Проверка работы в режиме enforcing политики targeted

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает

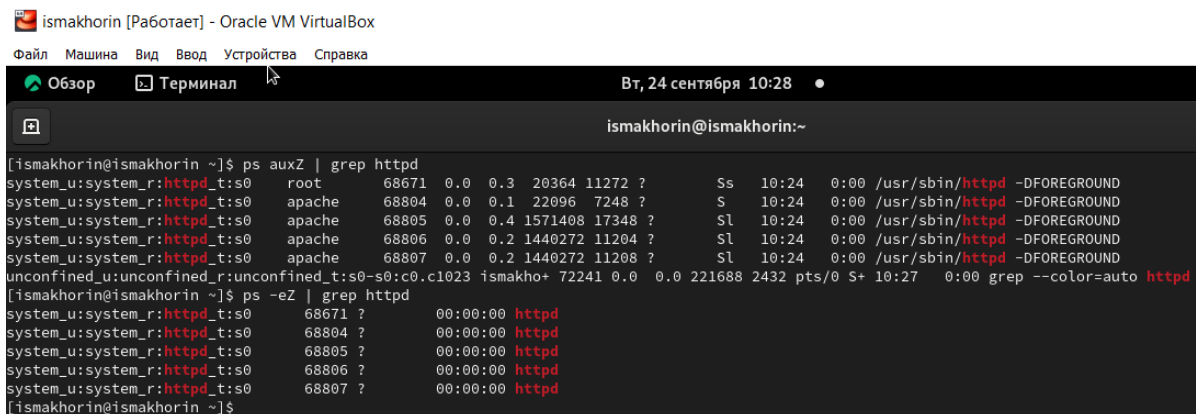


```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор Терминал Вт, 24 сентября 10:26
ismakhorin@ismakhorin:~$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
  Active: active (running) since Tue 2024-09-24 10:24:20 MSK; 2min 19s ago
  Docs: man:httpd.service(8)
  Main PID: 68671 (httpd)
  Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
  Tasks: 177 (limit: 23037)
  Memory: 26.2M
  CPU: 174ms
  CGroup: /system.slice/httpd.service
          └─68671 /usr/sbin/httpd -DFOREGROUND
            └─68804 /usr/sbin/httpd -DFOREGROUND
              └─68805 /usr/sbin/httpd -DFOREGROUND
                └─68806 /usr/sbin/httpd -DFOREGROUND
                  └─68807 /usr/sbin/httpd -DFOREGROUND

сен 24 10:24:20 ismakhorin.localdomain systemd[1]: Starting The Apache HTTP Server...
сен 24 10:24:20 ismakhorin.localdomain httpd[68671]: Server configured, listening on: port 80
сен 24 10:24:20 ismakhorin.localdomain systemd[1]: Started The Apache HTTP Server.
ismakhorin@ismakhorin ~]$
```

Рис. 3.2: Проверка работы веб-сервера

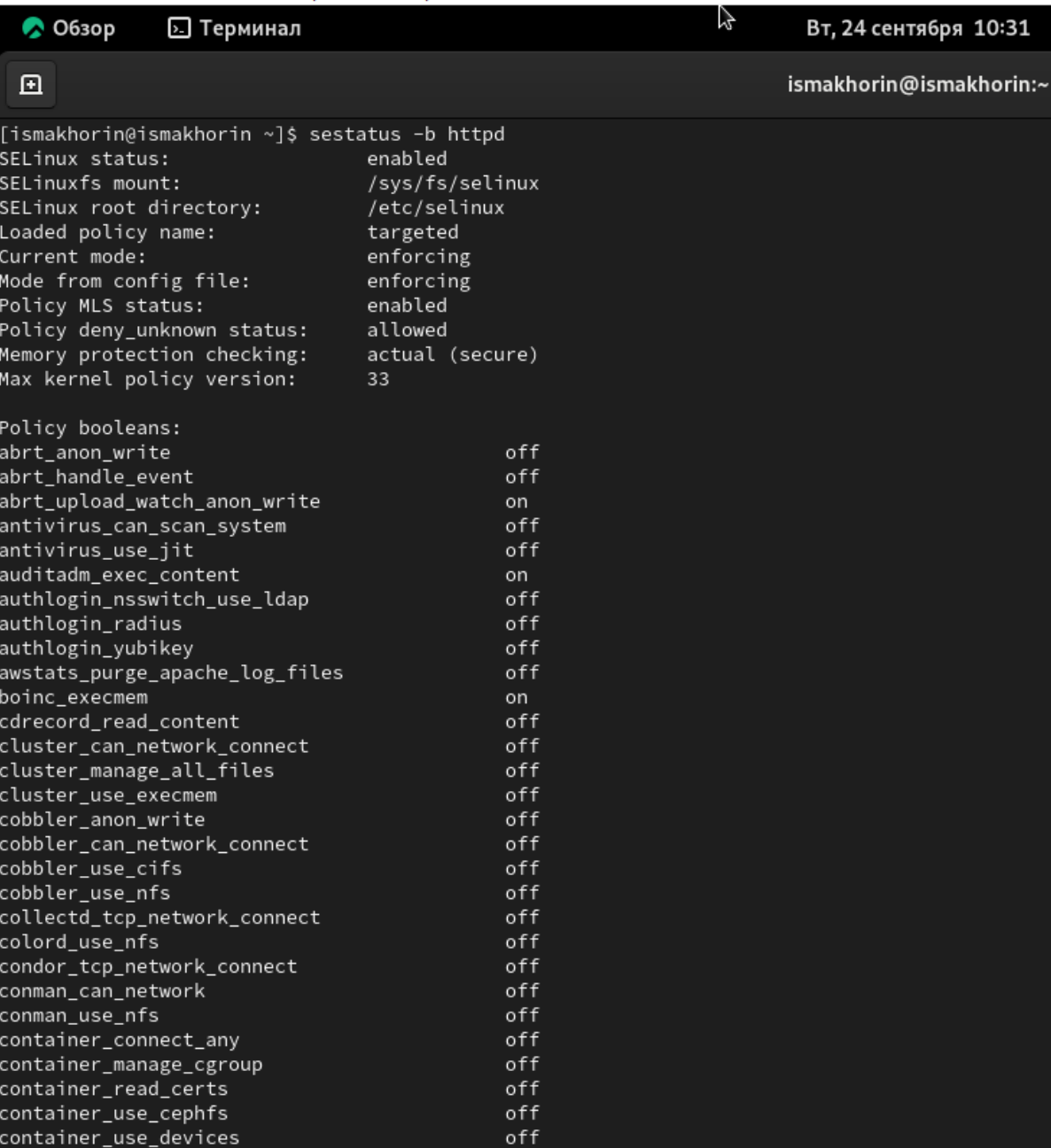
Затем найдём веб-сервер Apache в списке процессов и определим его контекст безопасности



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор Терминал Вт, 24 сентября 10:28
ismakhorin@ismakhorin:~$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 68671 0.0 0.3 20364 11272 ? Ss 10:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 68804 0.0 0.1 22096 7248 ? S 10:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 68805 0.0 0.4 1571408 17348 ? Sl 10:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 68806 0.0 0.2 1440272 11204 ? Sl 10:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 68807 0.0 0.2 1440272 11208 ? Sl 10:24 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ismakho+ 72241 0.0 0.0 221688 2432 pts/0 S+ 10:27 0:00 grep --color=auto httpd
ismakhorin@ismakhorin ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 68671 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 68804 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 68805 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 68806 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 68807 ? 00:00:00 httpd
ismakhorin@ismakhorin ~]$
```

Рис. 3.3: Нахождение веб-сервера Apache в списке процессов и определение его контекста безопасности

Посмотрим текущее состояние переключателей SELinux для Apache

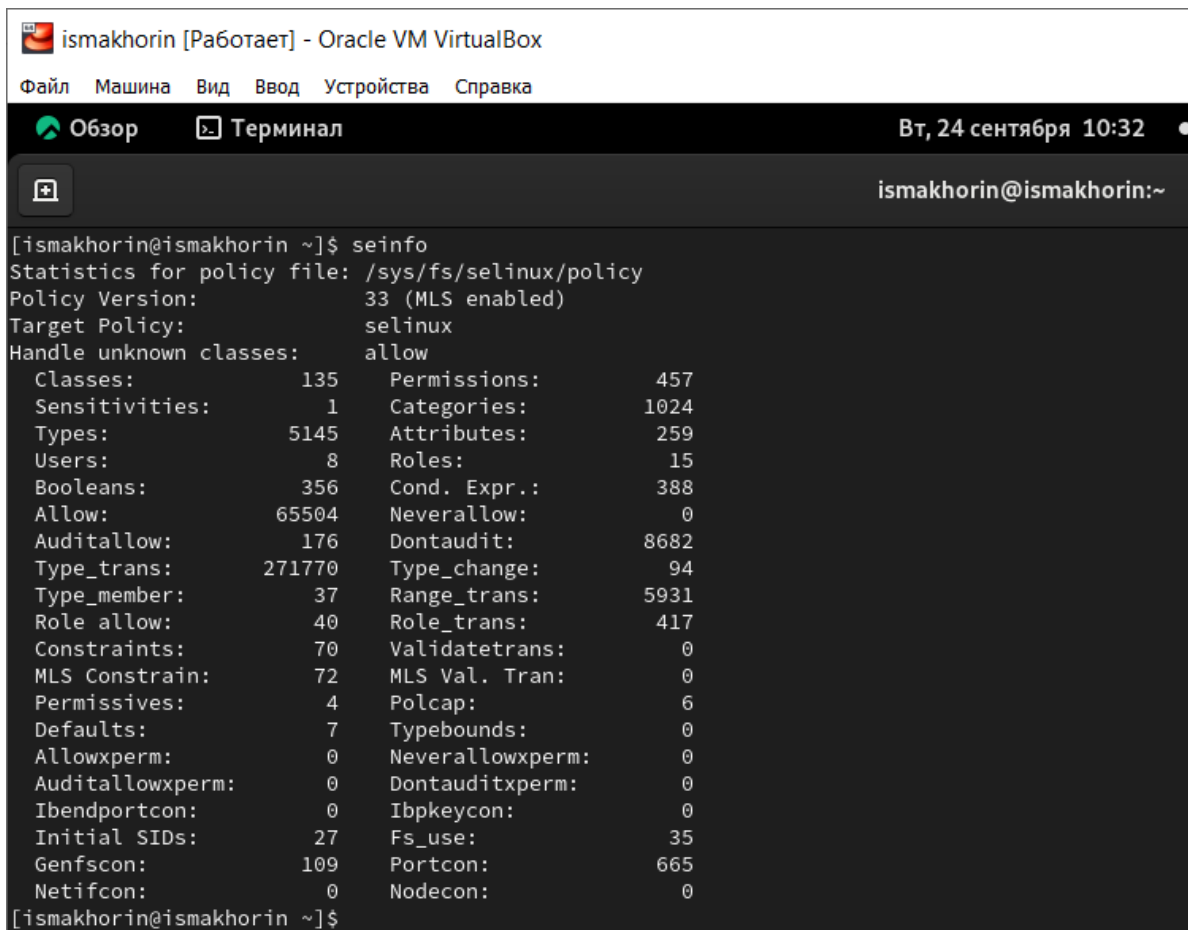


```
[ismakhorin@ismakhorin ~]$ sestatus -b httpd
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
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
cobbler_anon_write               off
cobbler_can_network_connect      off
cobbler_use_cifs                 off
cobbler_use_nfs                  off
collectd_tcp_network_connect     off
colord_use_nfs                   off
condor_tcp_network_connect       off
conman_can_network               off
conman_use_nfs                   off
container_connect_any            off
container_manage_cgroup          off
container_read_certs             off
container_use_cephfs             off
container_use_devices            off
```

Рис. 3.4: Просмотр текущего состояния переключателей SELinux

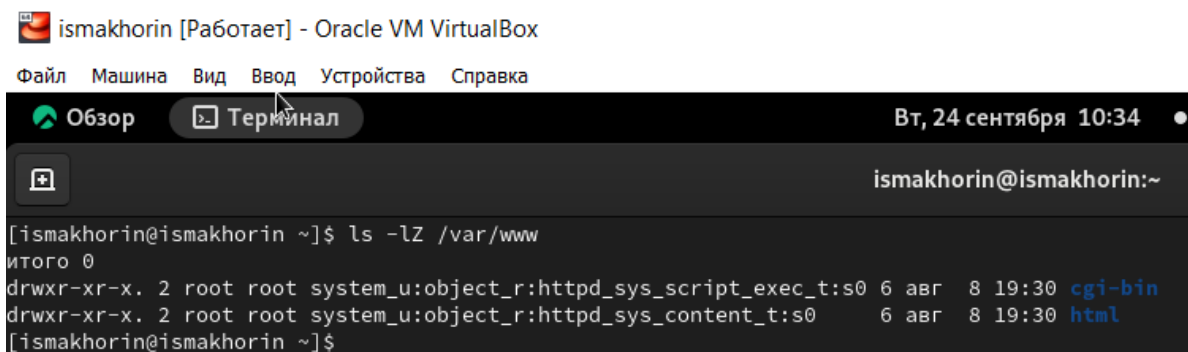
Далее посмотрим статистику по политике



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор Терминал Вт, 24 сентября 10:32
ismakhorin@ismakhorin:~$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 33 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 135 Permissions: 457
Sensitivities: 1 Categories: 1024
Types: 5145 Attributes: 259
Users: 8 Roles: 15
Booleans: 356 Cond. Expr.: 388
Allow: 65504 Neverallow: 0
Auditallow: 176 Dontaudit: 8682
Type_trans: 271770 Type_change: 94
Type_member: 37 Range_trans: 5931
Role allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constrains: 72 MLS Val. Tran: 0
Permissives: 4 Polcap: 6
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0
ismakhorin@ismakhorin ~]$
```

Рис. 3.5: Просмотр статистики по политике

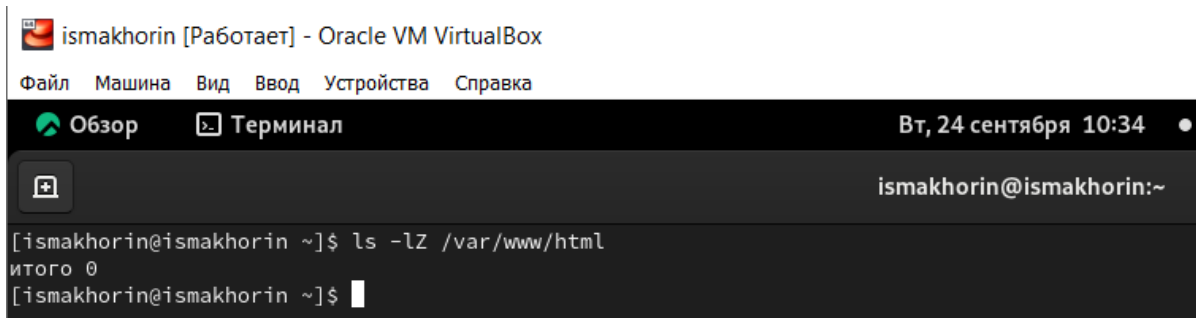
Определим тип файлов и поддиректорий, находящихся в директории /var/www



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор Терминал Вт, 24 сентября 10:34
ismakhorin@ismakhorin:~$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 8 19:30 html
ismakhorin@ismakhorin ~]$
```

Рис. 3.6: Определение типов файлов и поддиректорий

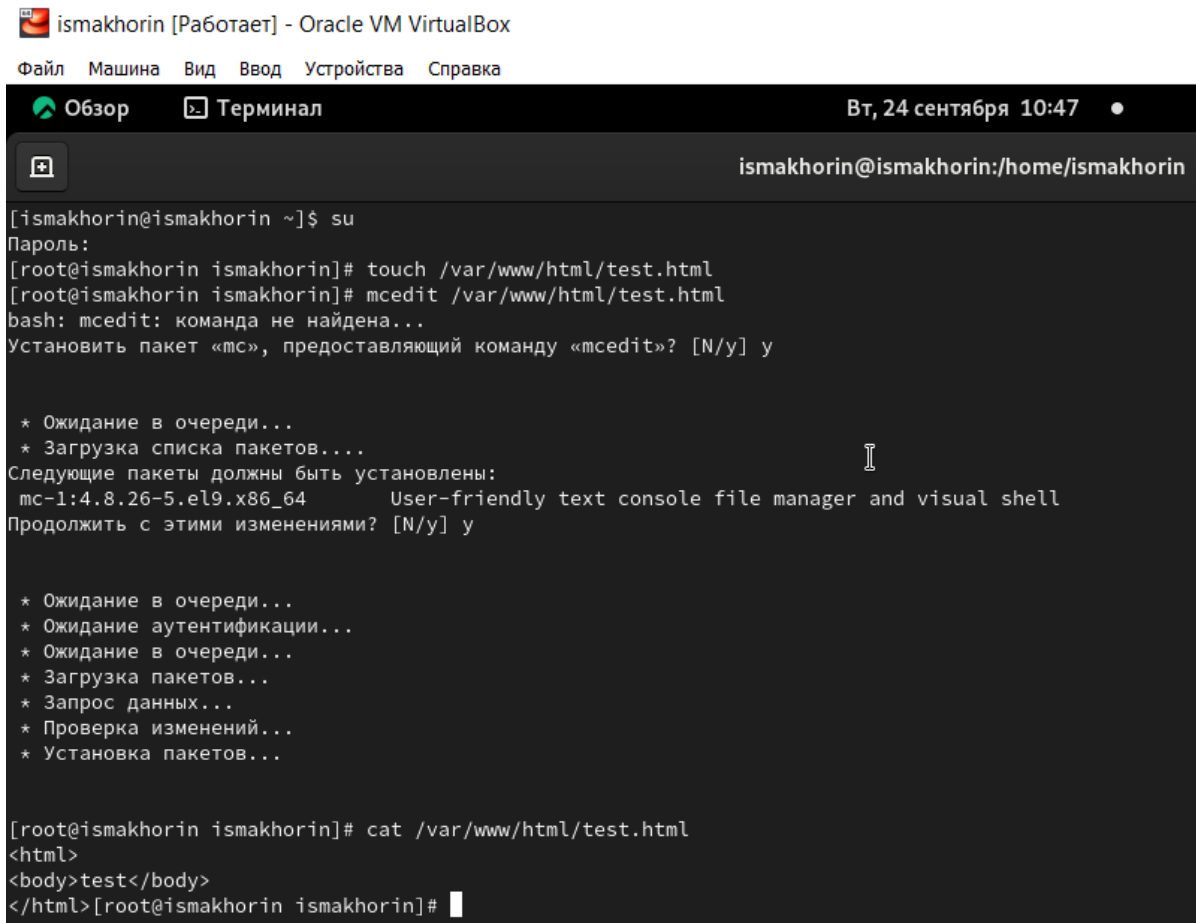
Определим тип файлов, находящихся в директории /var/www/html



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вт, 24 сентября 10:34
ismakhorin@ismakhorin:~
[ismakhorin@ismakhorin ~]$ ls -lZ /var/www/html
итого 0
[ismakhorin@ismakhorin ~]$
```

Рис. 3.7: Определение типов файлов и поддиректорий

Следующим шагом создадим от имени суперпользователя html-файл /var/www/html/test.html с содержанием “test”



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вт, 24 сентября 10:47
ismakhorin@ismakhorin:/home/ismakhorin
[ismakhorin@ismakhorin ~]$ su
Пароль:
[root@ismakhorin ismakhorin]# touch /var/www/html/test.html
[root@ismakhorin ismakhorin]# mcedit /var/www/html/test.html
bash: mcedit: команда не найдена...
Установить пакет «mc», предоставляющий команду «mcedit»? [N/y] y

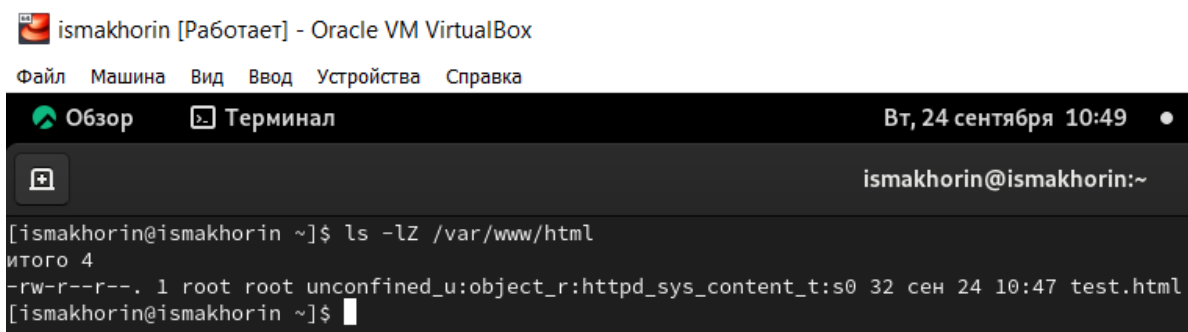
* Ожидание в очереди...
* Загрузка списка пакетов...
Следующие пакеты должны быть установлены:
mc-1:4.8.26-5.el9.x86_64      User-friendly text console file manager and visual shell
Продолжить с этими изменениями? [N/y] y

* Ожидание в очереди...
* Ожидание аутентификации...
* Ожидание в очереди...
* Загрузка пакетов...
* Запрос данных...
* Проверка изменений...
* Установка пакетов...

[root@ismakhorin ismakhorin]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>[root@ismakhorin ismakhorin]#
```

Рис. 3.8: Создание файла с содержанием

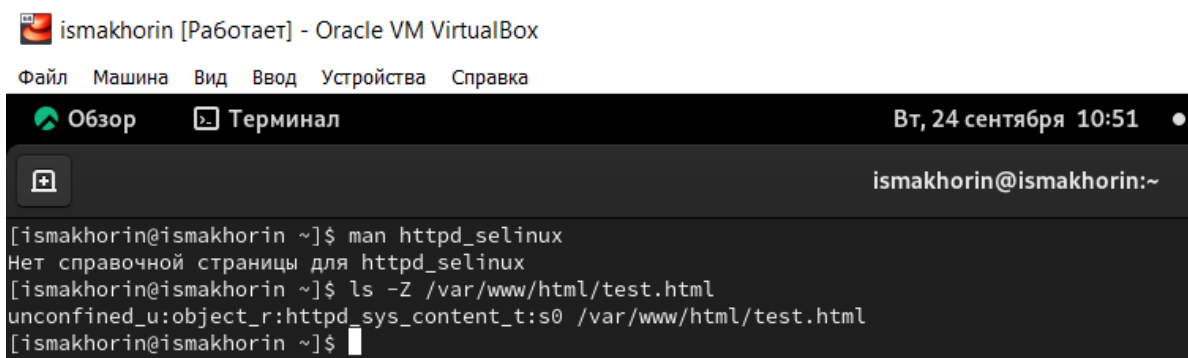
Проверим контекст созданного нами файла



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вт, 24 сентября 10:49
ismakhorin@ismakhorin:~
[ismakhorin@ismakhorin ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 32 сен 24 10:47 test.html
[ismakhorin@ismakhorin ~]$
```

Рис. 3.9: Проверка контекста созданного файла

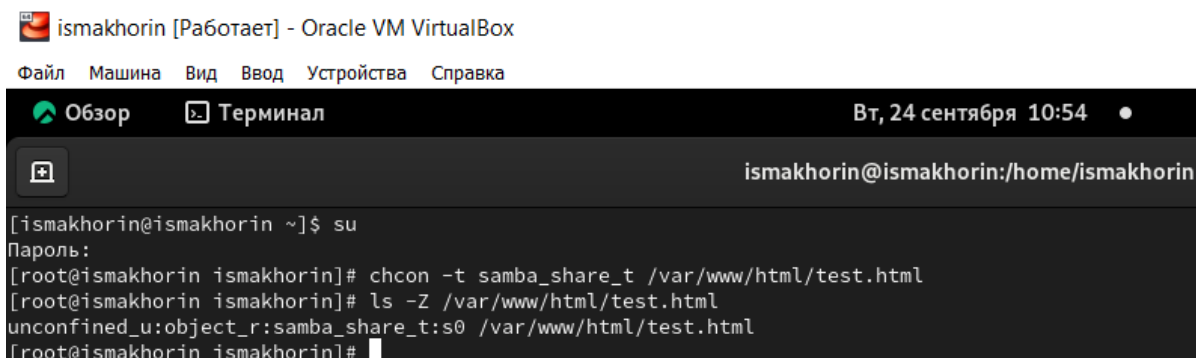
Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html` и проверим контекст файла



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вт, 24 сентября 10:51
ismakhorin@ismakhorin:~
[ismakhorin@ismakhorin ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
[ismakhorin@ismakhorin ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[ismakhorin@ismakhorin ~]$
```

Рис. 3.10: Изучение справки и проверка контекста файла

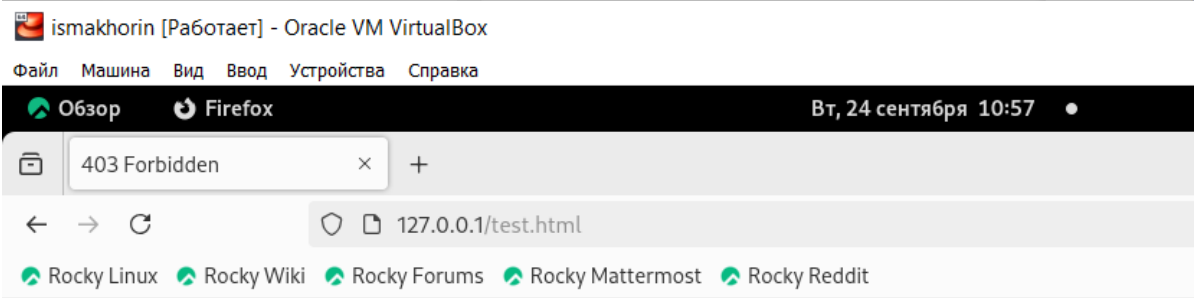
Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вт, 24 сентября 10:54
ismakhorin@ismakhorin:/home/ismakhorin
[ismakhorin@ismakhorin ~]$ su
Пароль:
[root@ismakhorin ismakhorin]# chcon -t samba_share_t /var/www/html/test.html
[root@ismakhorin ismakhorin]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@ismakhorin ismakhorin]#
```

Рис. 3.11: Изменение контекста файла и проверка

Попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`



Forbidden

You don't have permission to access this resource.

Рис. 3.12: Попытка получения доступа к файлу через веб-сервер

Просмотрим log-файлы веб-сервера Apache и системный лог-файл

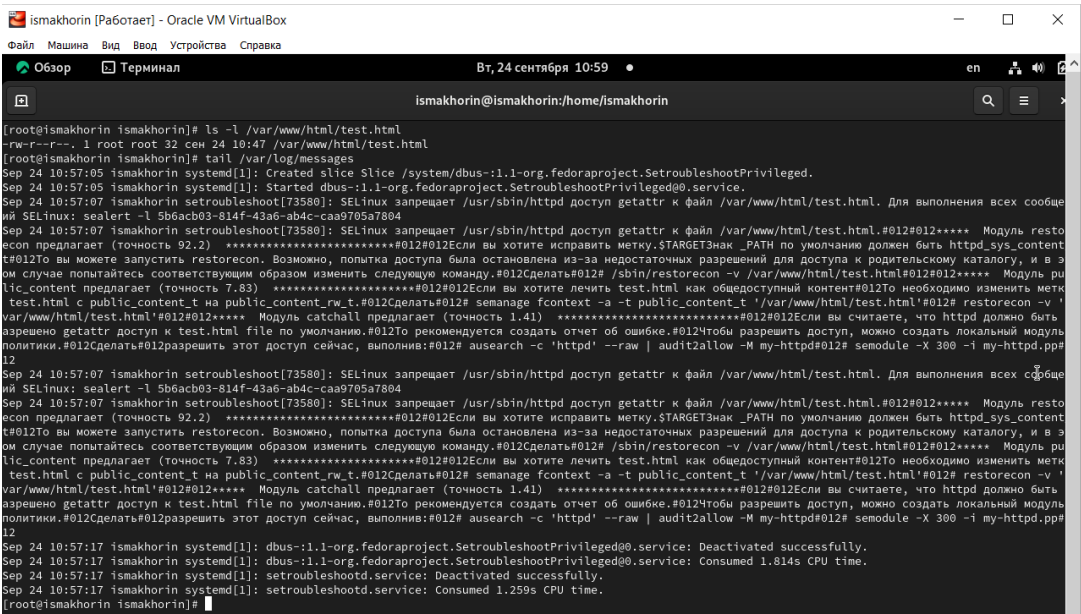
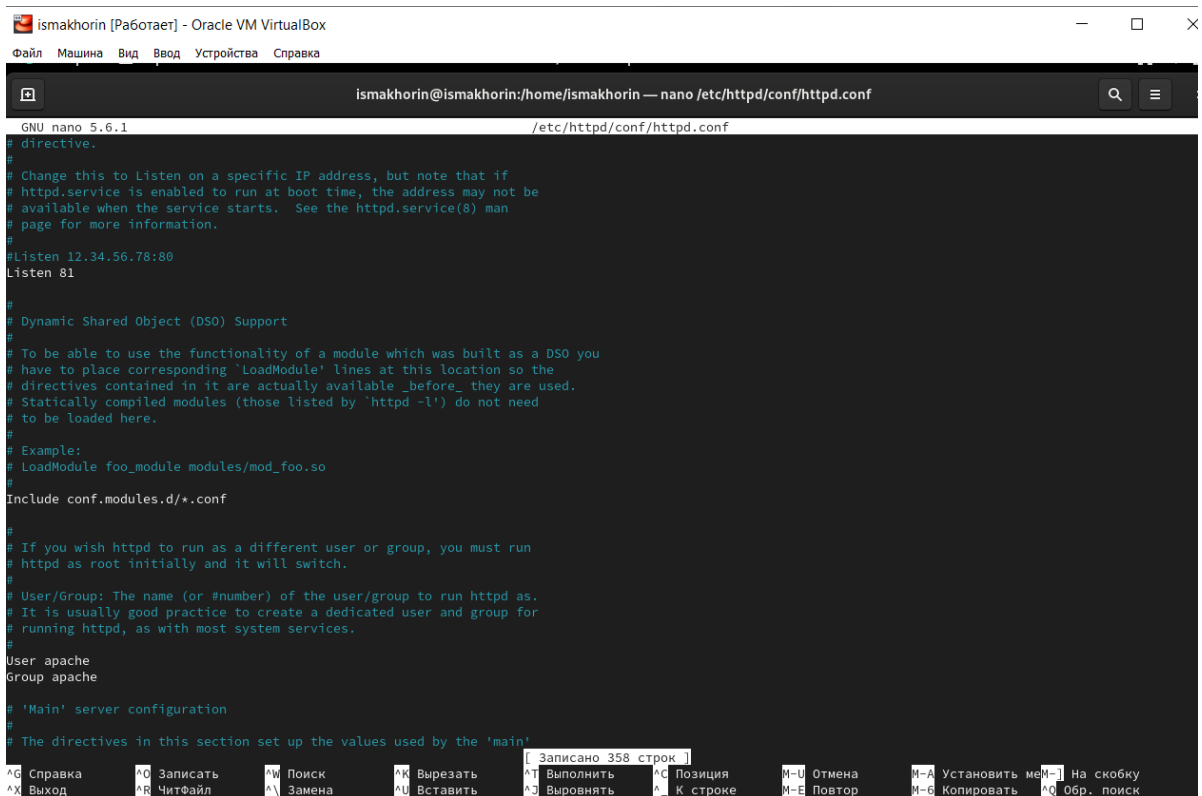


Рис. 3.13: Просмотр log-файлов веб-сервера Apache и системного лог-файла

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services)



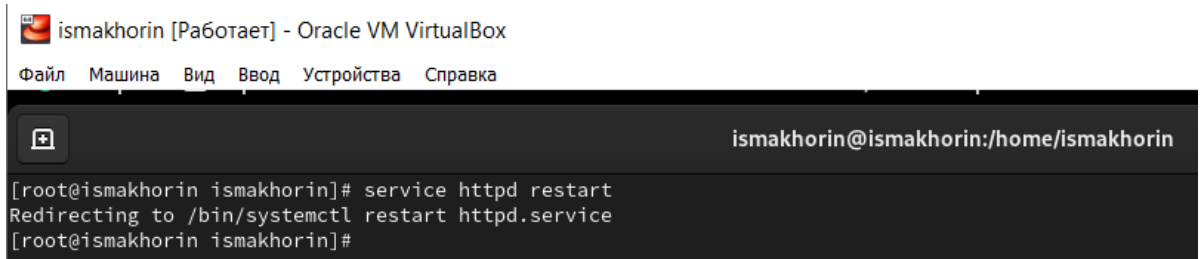
The screenshot shows a terminal window titled "ismakhorin [Работает] - Oracle VM VirtualBox". The terminal displays the nano text editor editing the file "/etc/httpd/conf/httpd.conf". The editor shows the following content:

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# 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
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User apache
Group apache
#
# 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
```

The bottom of the terminal shows a status bar with various keyboard shortcuts like "Справка", "Записать", "Поиск", etc.

Рис. 3.14: Попытка запуска веб-сервера Apache на прослушивание TCP-порта 81

Выполним перезапуск веб-сервера Apache



The screenshot shows a terminal window titled "ismakhorin [Работает] - Oracle VM VirtualBox". The terminal displays the following command and output:

```
[root@ismakhorin ismakhorin]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ismakhorin ismakhorin]#
```

Рис. 3.15: Перезапуск веб-сервера Apache

Проанализируем лог-файлы: `tail -nl /var/log/messages, /var/log/http/error_log, /var/log/http/access_log` и `/var/log/audit/audit.log`

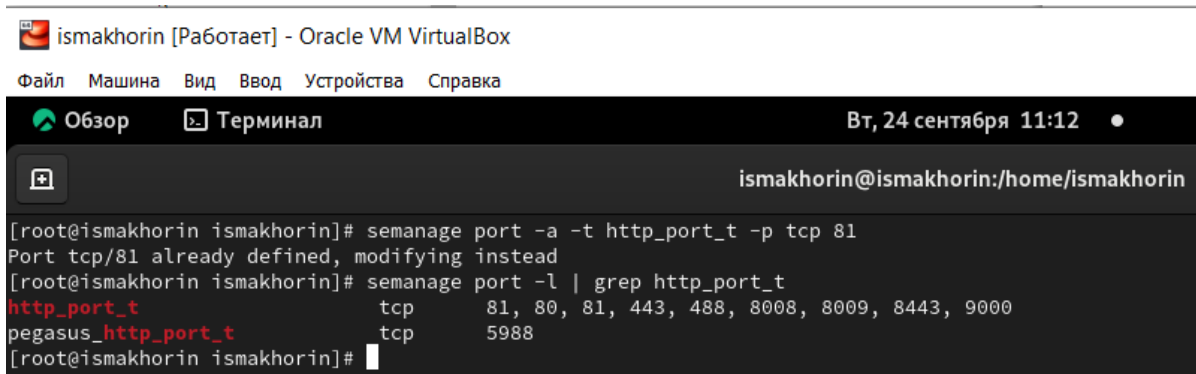


The screenshot shows a terminal window titled "ismakhorin [Работает] - Oracle VM VirtualBox". The terminal displays the output of several `tail` commands. The first command is `tail -n1 /var/log/messages`, showing a log entry for a successful HTTP POST request. The second command is `tail -n1 /var/log/httpd/error_log`, showing a core notice. The third command is `tail -n1 /var/log/httpd/access_log`, showing a GET request for `/favicon.ico`. The fourth command is `tail -n1 /var/log/audit/audit.log`, showing a systemd message.

```
[root@ismakhorin ismakhorin]# tail -n1 /var/log/messages
Sep 24 11:09:32 ismakhorin cupsd[869]: REQUEST localhost - - "POST / HTTP/1.1" 200 189 Renew-Subscription successful-ok
[root@ismakhorin ismakhorin]# tail -n1 /var/log/httpd/error_log
[Tue Sep 24 11:08:14.426292 2024] [core:notice] [pid 73990:tid 73990] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@ismakhorin ismakhorin]# tail -n1 /var/log/httpd/access_log
tail: невозможно открыть '/var/log/httpd/error_log' для чтения: Нет такого файла или каталога
[root@ismakhorin ismakhorin]# tail -n1 /var/log/audit/audit.log
type=SERVICE_START msg=audit(1727165294.431:341): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd"
xe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUDID="unset"
[root@ismakhorin ismakhorin]#
```

Рис. 3.16: Анализ лог-файлов

Выполним команду `semanage port -a -t http_port_t -p tcp 81` и после этого проверим список портов



The screenshot shows a terminal window titled "ismakhorin [Работает] - Oracle VM VirtualBox". The terminal displays the output of two `semanage` commands. The first command is `semanage port -a -t http_port_t -p tcp 81`, which returns "Port tcp/81 already defined, modifying instead". The second command is `semanage port -l | grep http_port_t`, which returns a list of ports for the `http_port_t` type.

```
[root@ismakhorin ismakhorin]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@ismakhorin ismakhorin]# semanage port -l | grep http_port_t
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@ismakhorin ismakhorin]#
```

Рис. 3.17: Выполнение команды и проверка списка портов

Вернём контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`

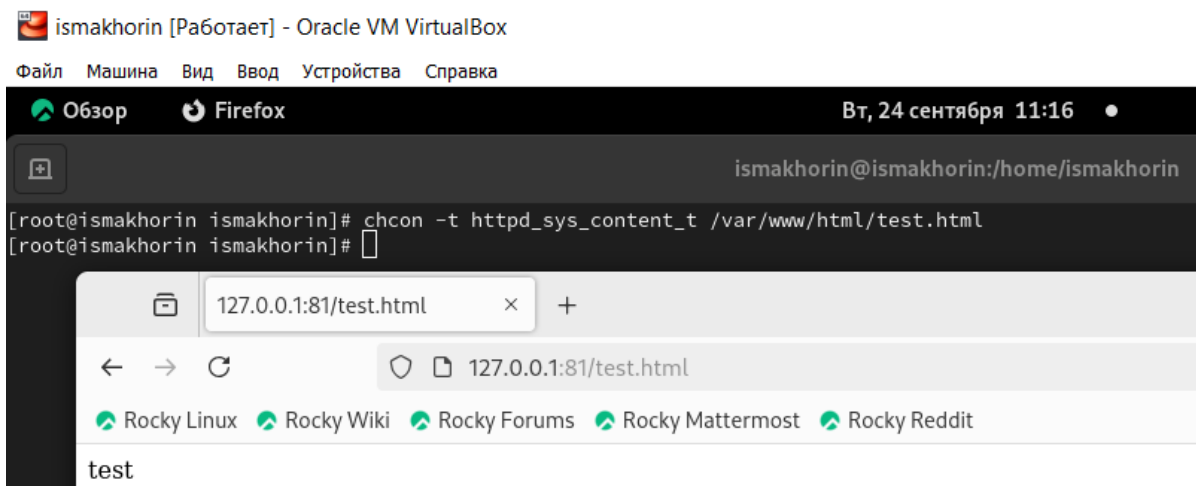


Рис. 3.18: Возвращение контекста `httpd_sys_content_t` к файлу `/var/www/html/test.html` и попытка получения доступа к файлу через веб-сервис

Исправим обратно конфигурационный файл `apache`, вернув `Listen 80`

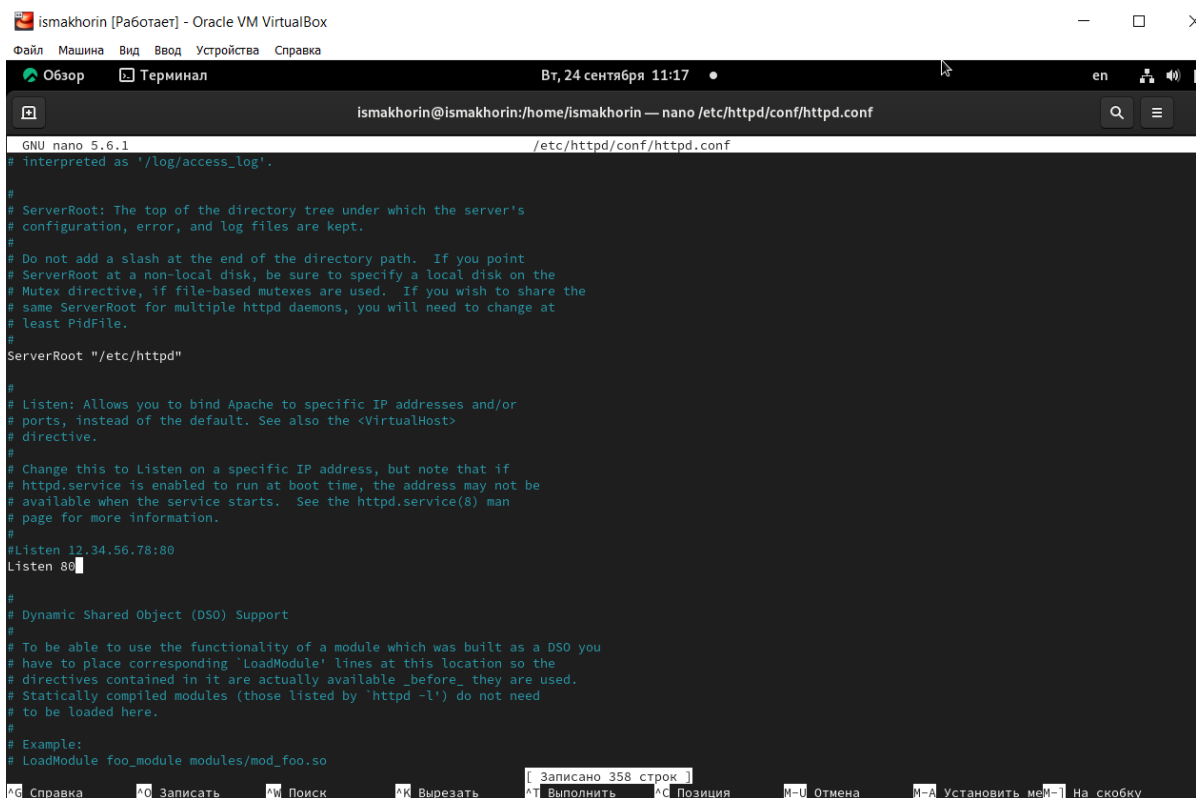
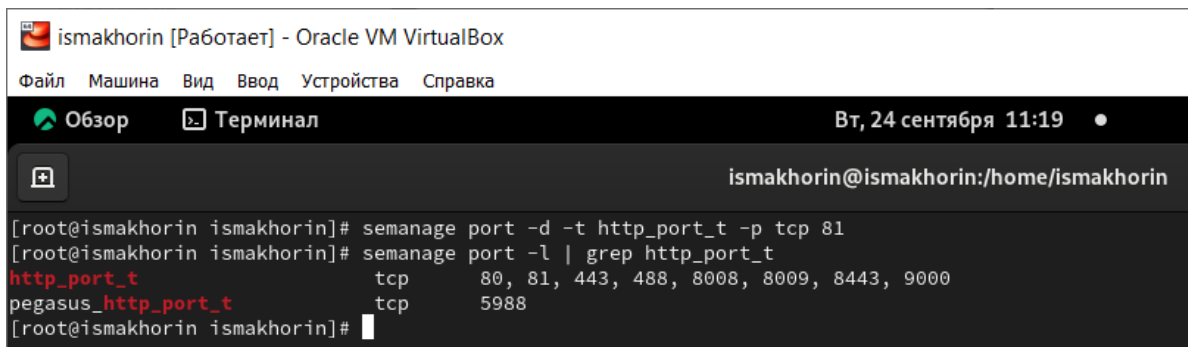


Рис. 3.19: Исправление конфигурационного файла `apache`

Удалим привязку `http_port_t` к 81 порту

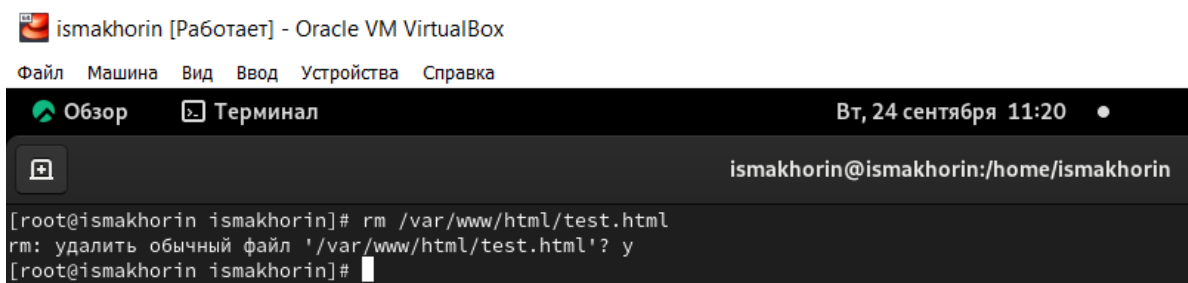


```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал
Вт, 24 сентября 11:19
ismakhorin@ismakhorin:/home/ismakhorin

[root@ismakhorin ismakhorin]# semanage port -d -t http_port_t -p tcp 81
[root@ismakhorin ismakhorin]# 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@ismakhorin ismakhorin]#
```

Рис. 3.20: Удаление привязки http_port_t к 81 порту и проверка

Удалим файл /var/www/html/test.html



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал
Вт, 24 сентября 11:20
ismakhorin@ismakhorin:/home/ismakhorin

[root@ismakhorin ismakhorin]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@ismakhorin ismakhorin]#
```

Рис. 3.21: Удаление файла /var/www/html/test.html

4 Вывод

В ходе выполнения лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.

5 Список литературы. Библиография

[1] SELinux: <https://habr.com/ru/companies/kingservers/articles/209644/>

[2] Apache: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>