

Лабораторная работа №6

Основы Информационной Безопасности

Александрова Ульяна Вадимовна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	18

Список иллюстраций

4.1	Проверка работы SELinux	9
4.2	Установка библиотеки	10
4.3	Запустила работу Apache	10
4.4	Проверка	10
4.5	Текущее состояние переключателей	11
4.6	Статистика	12
4.7	Папка www	12
4.8	Папка html	12
4.9	Файл html	13
4.10	Контекст	13
4.11	Веб-страничка	13
4.12	samba_share_t	14
4.13	Веб-страница	14
4.14	Лог-файл	14
4.15	Изменение файла	15
4.16	Лог	15
4.17	Лог	15
4.18	Лог	15
4.19	Настройка порта 81	16
4.20	Веб-страница	16
4.21	Веб-страница	16
4.22	Удаление	17

Список таблиц

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.

2 Задание

1. Подготовить рабочую среду;
2. Выполнить основную часть работы;
3. Сделать выводы.

3 Теоретическое введение

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика `targeted` и режим `enforcing` используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл `/etc/selinux/config`, так и проверить используемый режим и политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName: ServerName test.ru`, чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола `tcp`. Отключить фильтр можно командами
`iptables -F`
`iptables -P INPUT ACCEPT`
`iptables -P OUTPUT ACCEPT`
либо добавить разрешающие правила:

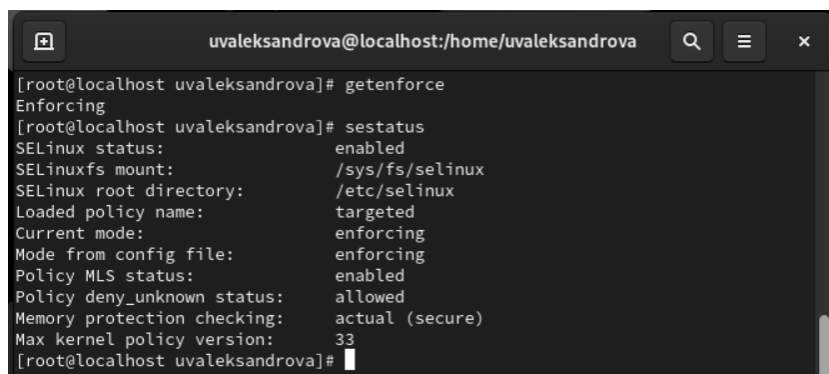
```
iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные `links`, `lynx`, `wget` и графические `konqueror`, `opera`, `firefox` или др.

4 Выполнение лабораторной работы

Перед началом работы я обновила ПО (**yum update -y**, затем установила apache (**yum install httpd -y**).

Вошла в систему с и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus** (рис. 4.1).

A screenshot of a terminal window with a dark background. The window title is 'uvaleksandrova@localhost:/home/uvaleksandrova'. The terminal shows the following commands and output:

```
[root@localhost uvaleksandrova]# getenforce
Enforcing
[root@localhost uvaleksandrova]# 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 uvaleksandrova]#
```

Рис. 4.1: Проверка работы SELinux

Чтобы работать с библиотекой httpd, скачала ее (рис. 4.2).

```
uvaleksandrova@localhost:~  
bash: httpd: command not found...  
Install package 'httpd-core' to provide command 'httpd'? [N/y] y  
  
* Waiting in queue...  
The following packages have to be installed:  
apr-1.7.0-12.el9_3.x86_64      Apache Portable Runtime library  
apr-util-1.6.1-23.el9.x86_64  Apache Portable Runtime Utility Library  
apr-util-bdb-1.6.1-23.el9.x86_64  APR utility library Berkeley DB driver  
apr-util-openssl-1.6.1-23.el9.x86_64  APR utility library OpenSSL crypto support  
httpd-core-2.4.57-5.el9.x86_64 httpd minimal core  
httpdfilesystem-2.4.57-5.el9.noarch The basic directory layout for the Apache HTTP Server  
httpd-tools-2.4.57-5.el9.x86_64 Tools for use with the Apache HTTP Server  
Proceed with changes? [N/y] y  
  
* Waiting in queue...  
* Waiting for authentication... Failed to install packages: Failed to obtain authentication.  
[uvaleksandrova@localhost ~]$
```

Рис. 4.2: Установка библиотеки

Убедилась, что веб-сервер работает при помощи утилиты **service httpd start** (рис. 4.3).

```
[root@localhost ~]# service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[root@localhost ~]# 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 Fri 2024-03-29 00:25:26 MSK; 9s ago  
     Docs: man:httpd.service(8)  
  Main PID: 139338 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"  
    Tasks: 213 (limit: 12128)  
   Memory: 26.9M  
      CPU: 75ms  
  CGroup: /system.slice/httpd.service  
          └─139338 /usr/sbin/httpd -DFOREGROUND  
            └─139339 /usr/sbin/httpd -DFOREGROUND  
              └─139343 /usr/sbin/httpd -DFOREGROUND  
                └─139345 /usr/sbin/httpd -DFOREGROUND  
                  └─139346 /usr/sbin/httpd -DFOREGROUND  
  
Mar 29 00:25:25 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...  
Mar 29 00:25:26 localhost.localdomain systemd[1]: Started The Apache HTTP Server.  
Mar 29 00:25:26 localhost.localdomain httpd[139338]: Server configured, listening on: port 80  
[root@localhost ~]#
```

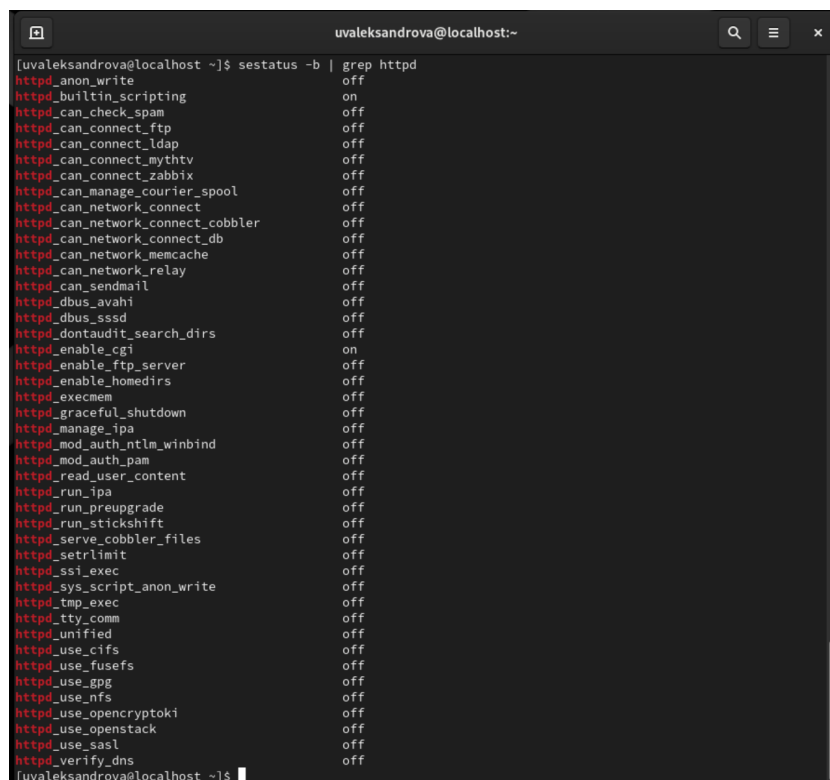
Рис. 4.3: Запустила работу Apache

Контекст безопасности - system_u:system_r (рис. 4.4).

```
[root@localhost ~]# ps -auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 139338 0.0 0.5 20128 11212 ? Ss 00:25 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 139339 0.0 0.3 21612 7248 ? S 00:25 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 139343 0.0 0.6 1210520 13020 ? Sl 00:25 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 139345 0.0 0.5 1079384 10972 ? Sl 00:25 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 139346 0.0 0.5 1079384 10972 ? Sl 00:25 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 139757 0.0 0.1 221664 2256 pts/0 S+ 12:24 0:00 grep --color=auto httpd
```

Рис. 4.4: Проверка

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -b | grep httpd** (рис. 4.5).



```
[uvaleksandrova@localhost ~]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripiting 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_avaahi 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
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openscryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
[uvaleksandrova@localhost ~]$
```

Рис. 4.5: Текущее состояние переключателей

Посмотрела статистику по политике с помощью команды **seinfo**. Типы: 5135; пользователи: 8; роли: 15 (рис. 4.6).

```
uvaleksandrova@localhost: /home/uvaleksandrova
[uvaleksandrova@localhost ~]$ su root
Password:
[root@localhost uvaleksandrova]# seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] y

* Waiting in queue...
The following packages have to be installed:
setools-console-4.4.3-1.el9.x86_64 Policy analysis command-line tools for SELinux
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...
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: 5135 Attributes: 259
Users: 8 Roles: 15
Booleans: 357 Cond. Expr.: 390
Allow: 65380 Neverallow: 0
Auditallow: 172 Dontaudit: 8647
Type_trans: 267809 Type_change: 94
Type_member: 37 Range_trans: 6164
Role_allow: 39 Role_trans: 419
Constraints: 70 Validatetrans: 0
MLS Constrains: 72 MLS Val. Tran: 0
Permissives: 2 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
[root@localhost uvaleksandrova]#
```

Рис. 4.6: Статистика

Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www** (папки). Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html (суперпользователю) (рис. 4.7).

```
[root@localhost uvaleksandrova]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12:35 html
```

Рис. 4.7: Папка www

Определила тип файлов, находящихся в директории /var/www/html утилитой **ls -lZ /var/www/html** (не отобразилось ничего) (рис. 4.8).

```
[root@localhost uvaleksandrova]# ls -lZ /var/www/html
total 0
```

Рис. 4.8: Папка html

Создала html-файл /var/www/html/test.html (рис. 4.9).

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

Рис. 4.9: Файл html

Проверила контекст созданного файла (httpd_sys_content_t) (рис. 4.10).

```
[uvaleksandrova@localhost html]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 4.10: Контекст

Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Файл был успешно отображён (рис. 4.11).

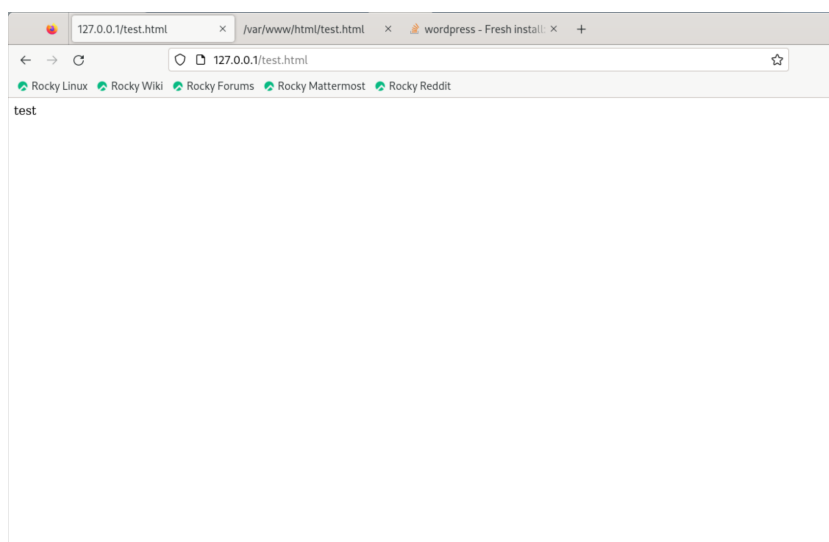


Рис. 4.11: Веб-страничка

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` с помощью утилиты `chcon -t samba_share_t /var/www/html/test.html`. Контекст поменялся (рис. 4.12).

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

Рис. 4.12: samba_share_t

Попробовала ещё раз получить доступ к файлу через веб-сервер. Ошибка :((рис. 4.13).

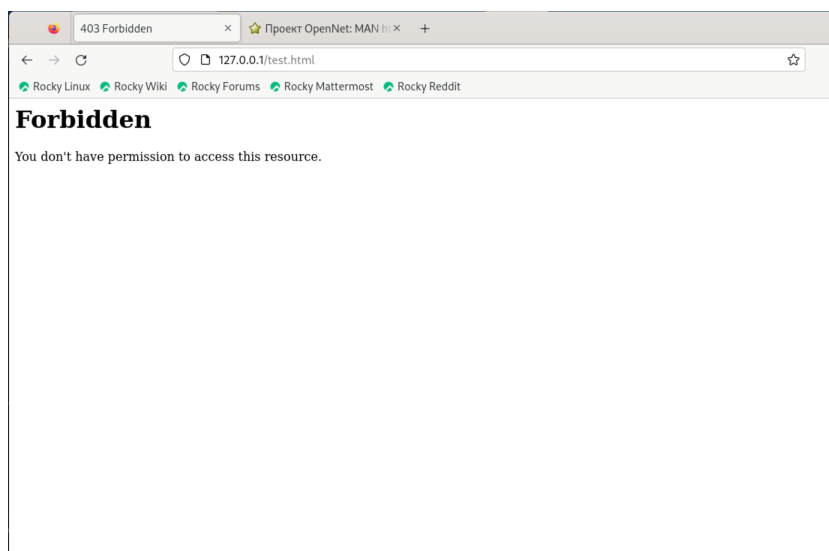


Рис. 4.13: Веб-страница

Проанализировала ситуацию. Файл не отображается, так как этот тип не позволяет процессу httpd получить доступ к файлу. Также просмотрела системный лог-файл `tail /var/log/messages` (рис. 4.14).

```
Mar 29 14:54:55 localhost setroubleshoot[140747]: SELinux is preventing /usr/sbin/httpd from getattr access o
n 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_s
ys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient pe
rmissions to access a parent directory in which case try to change the following command accordingly.#012Do#0
12# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggest
s *****#012#012If you want to treat test.html as public content#012Then you need to change t
he label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_c
ontent_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 g
etattr 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# semodule -X 300 -i my-httpd.pp#012
Mar 29 14:55:05 localhost systemd[1]: dbus-1.1-0-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactiv
ated successfully.
Mar 29 14:55:05 localhost systemd[1]: dbus-1.1-0-org.fedoraproject.SetroubleshootPrivileged@0.service: Consume
d 1.553s CPU time.
Mar 29 14:55:05 localhost systemd[1]: setroubleshootd.service: Deactivated successfully.
Mar 29 14:55:05 localhost systemd[1]: setroubleshootd.service: Consumed 1.155s CPU time.
[root@localhost html]#
```

Рис. 4.14: Лог-файл

Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81.

Для этого в файле /etc/httpd/httpd.conf поменяла строчку Listen 80 на Listen 81 (рис. 4.15).

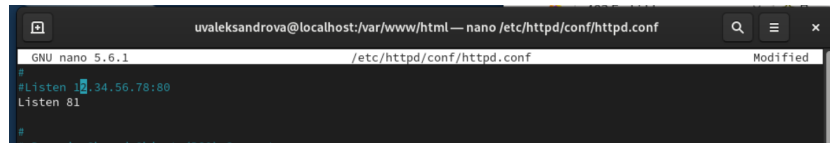


Рис. 4.15: Изменение файла

Выполнила перезапуск веб-сервера Apache. Сбой не произошел.... Проанализировала лог-файлы tail -nl /var/log/messages, /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log (рис. 4.16), (рис. 4.17), (рис. 4.18).

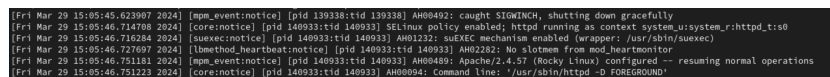


Рис. 4.16: Лог

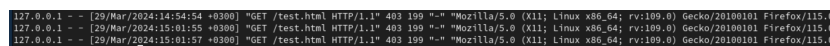


Рис. 4.17: Лог

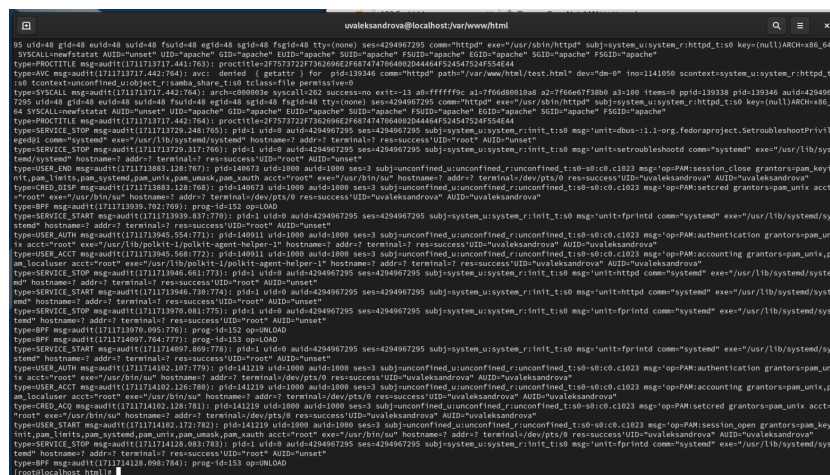


Рис. 4.18: Лог

Выполнила команду semanage port -a -t http_port_t -p tcp 81, проверила список портов командой semanage port -l | grep http_port_t (рис. 4.19).

```
uvaleksandrova@localhost:/var/www/html
[root@localhost html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost html]# 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 html]#
```

Рис. 4.19: Настройка порта 81

Попробовала запустить веб-сервер Apache ещё раз. Не сработало.... (рис. 4.20).

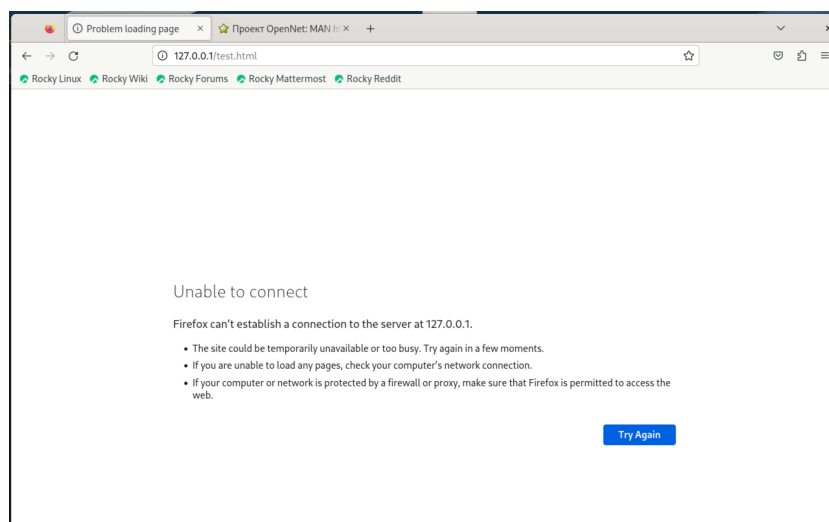


Рис. 4.20: Веб-страница

Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`.

После этого попробовала получить доступ к файлу через веб-сервер (рис. 4.21).

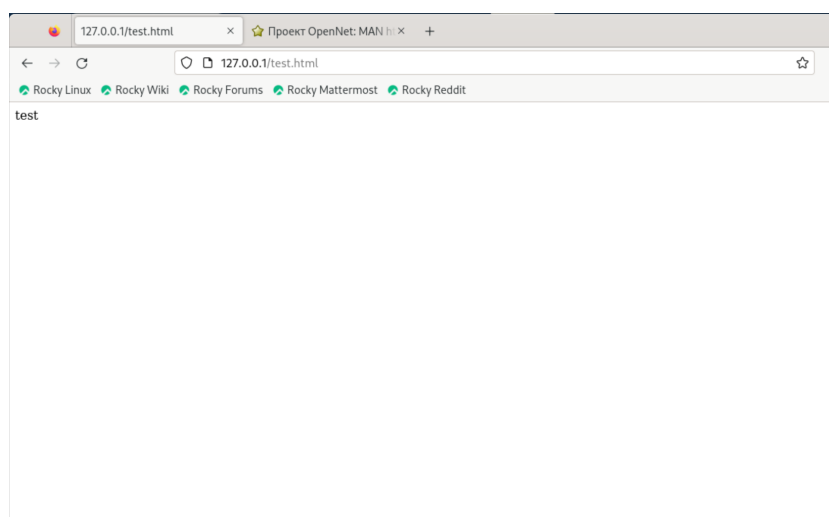
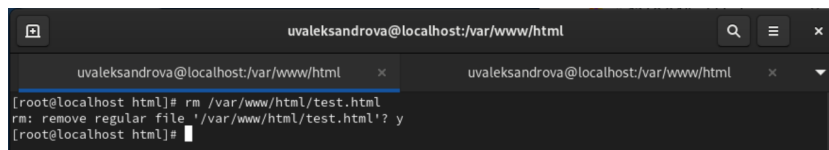


Рис. 4.21: Веб-страница

Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту, но появилась ошибка, что этот порт удалить невозможно, даже через суперпользователя.

Удалила файл /var/www/html/test.html (рис. 4.22).

A screenshot of a terminal window with a dark background. The title bar shows the user 'uvaleksandrova' at 'localhost:/var/www/html'. There are two tabs open, both with the same title. The terminal content shows a root user at a localhost prompt in an 'html' directory. The user enters the command 'rm /var/www/html/test.html'. The system responds with 'rm: remove regular file '/var/www/html/test.html'? y'. The user then enters 'y' to confirm the deletion. The prompt returns to the root user at the localhost in the 'html' directory.

```
uvaleksandrova@localhost:/var/www/html
uvaleksandrova@localhost:/var/www/html
[root@localhost html]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@localhost html]#
```

Рис. 4.22: Удаление

5 Выводы

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux.