

Лабораторная работа №6

Основы Информационной Безопасности

НВЕ МАНГЕ ХОСЕ ХЕРСОН МИКО; НКАбд-03-22.

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	17

Список иллюстраций

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

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
```

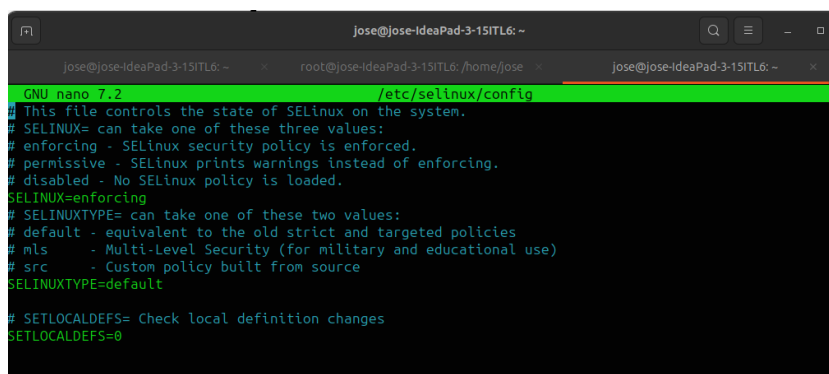
```
iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

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`).

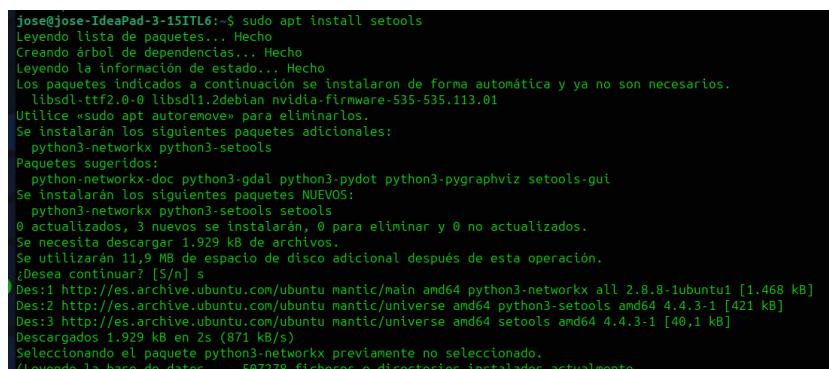
Вошла в систему с и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus** (рис. 4.1).



```
jose@jose-IdeaPad-3-15ITL6: ~  
jose@jose-IdeaPad-3-15ITL6: ~ root@jose-IdeaPad-3-15ITL6: /home/jose jose@jose-IdeaPad-3-15ITL6: ~  
GNU nano 7.2 /etc/selinux/config  
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
# enforcing - SELinux security policy is enforced.  
# permissive - SELinux prints warnings instead of enforcing.  
# disabled - No SELinux policy is loaded.  
SELINUX=enforcing  
# SELINUXTYPE= can take one of these two values:  
# default - equivalent to the old strict and targeted policies  
# mls      - Multi-Level Security (for military and educational use)  
# src      - Custom policy built from source  
SELINUXTYPE=default  
# SETLOCALDEFS= Check local definition changes  
SETLOCALDEFS=0
```

Рис. 4.1: Проверка работы SELinux

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



```
jose@jose-IdeaPad-3-15ITL6:~$ sudo apt install setools  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
libstdc++2.0-0 libstdc++12deb1 nvidia-firmware-535-535.113.01  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
python3-networkx python3-setools  
Paquetes sugeridos:  
python-networkx-doc python3-gdal python3-pydot python3-pygraphviz setools-gui  
Se instalarán los siguientes paquetes NUEVOS:  
python3-networkx python3-setools setools  
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 1.929 kB de archivos.  
Se utilizarán 11,9 MB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] s  
Des:1 http://es.archive.ubuntu.com/ubuntu mantic/main amd64 python3-networkx all 2.8.8-1ubuntu1 [1.468 kB]  
Des:2 http://es.archive.ubuntu.com/ubuntu mantic/universe amd64 python3-setools amd64 4.4.3-1 [421 kB]  
Des:3 http://es.archive.ubuntu.com/ubuntu mantic/universe amd64 setools amd64 4.4.3-1 [40,1 kB]  
Descargados 1.929 kB en 2s (871 kB/s)  
Seleccionando el paquete python3-networkx previamente no seleccionado.  
(Leyendo la base de datos ... 587278 ficheros o directorios instalados actualmente.
```

Рис. 4.2: Установка библиотеки

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

```
jose@jose-IdeaPad-3-15ITL6: ~  
jose@jose-IdeaPad-3-15ITL6: ~  
jose@jose-IdeaPad-3-15ITL6: ~  
jose@jose-IdeaPad-3-15ITL6:~$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)  
   Active: active (running) since Wed 2024-04-24 12:12:19 CEST; 5min ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Main PID: 46064 (apache2)  
     Tasks: 55 (limit: 9196)  
    Memory: 5.4M  
       CPU: 44ms  
   CGroup: /system.slice/apache2.service  
           └─46064 /usr/sbin/apache2 -k start  
             └─46065 /usr/sbin/apache2 -k start  
               └─46066 /usr/sbin/apache2 -k start  
  
abr 24 12:12:19 jose-IdeaPad-3-15ITL6 systemd[1]: Starting apache2.service - The Apache HTTP Server...  
abr 24 12:12:19 jose-IdeaPad-3-15ITL6 apachectl[46063]: AH00558: apache2: Could not reliably determine  
abr 24 12:12:19 jose-IdeaPad-3-15ITL6 systemd[1]: Started apache2.service - The Apache HTTP Server.  
ESCOC
```

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-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).

```

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
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_ssl_exec            off

```

Рис. 4.5: Текущее состояние переключателей

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

```

jose@jose-IdeaPad-3-15ITL6:~$ seinfo
Statistics for policy file: /etc/selinux/default/policy/policy.33
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135
Sensitivities:           1
Types:                   3971
Users:                   7
Booleans:                318
Allow:                   107509
Auditallow:              21
Type_trans:              9433
Type_member:             16
Role_allow:              32
Constraints:             133
MLS Constrains:          110
Permissives:             0
Defaults:                0
Allowxperm:              0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:            27
Genfscon:                95
Netifcon:                0
Permissions:             426
Categories:              1024
Attributes:              227
Roles:                   15
Cond. Expr.:             349
Neverallow:               0
Dontaudit:               17044
Type_change:              72
Range_trans:              56
Role_trans:              372
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  5
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  29
Portcon:                 487
Nodecon:                 0

```

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).

```

jose@jose-IdeaPad-3-15ITL6:~$ ls -lZ /var/www
total 4
drwxr-xr-x 2 root root ? 4096 abr 24 12:12 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).

```
jose@jose-IdeaPad-3-15ITL6:~$ ls -lZ /var/www/html
total 12
-rw-r--r-- 1 root root ? 19671 abr 24 12:12 index.html
```

Рис. 4.8: Папка html

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

```
jose@jose-IdeaPad-3-15ITL6:~$ ls -lZ /var/www/html/test.html
-rw-r--r-- 1 root root ? 31 abr 27 13:58 /var/www/html/test.html
```

Рис. 4.9: Файл html

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

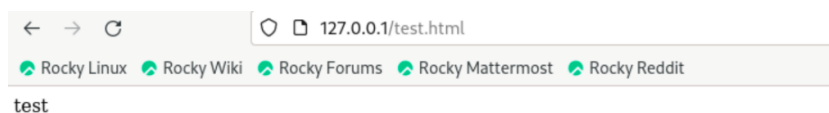


Рис. 4.10: Контекст

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

```
jose@jose-IdeaPad-3-15ITL6:~$ chcon -t samba_share_t /var/www/html/test.html
chcon: no se puede aplicar contexto parcial al fichero sin etiquetar '/var/www/html/test.html'
```

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).

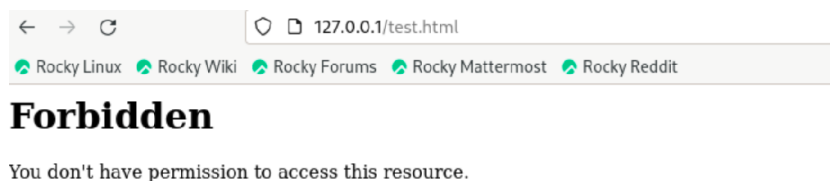


Рис. 4.12: samba_share_t

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

Веб-страница

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).

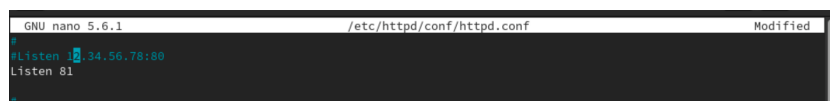


Рис. 4.14: Лог-файл

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).

```
[Fri Mar 29 15:05:46.623907 2024] [mpm_event:notice] [pid 139338:tid 139338] AH00402: caught SIGINT, shutting down gracefully
[Fri Mar 29 15:05:46.714708 2024] [core:notice] [pid 140933:tid 140933] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Mar 29 15:05:46.716284 2024] [suexec:notice] [pid 140933:tid 140933] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Mar 29 15:05:46.727697 2024] [lbmethod_heartbeat:notice] [pid 140933:tid 140933] AH02282: No slotmem from mod_heartbeat
[Fri Mar 29 15:05:46.751111 2024] [mpm_event:notice] [pid 140933:tid 140933] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Fri Mar 29 15:05:46.751223 2024] [core:notice] [pid 140933:tid 140933] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 4.15: Изменение файла

Выполнила перезапуск веб-сервера Apache. Сбой не произошёл.... 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).

```
[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. 4.16: Лог

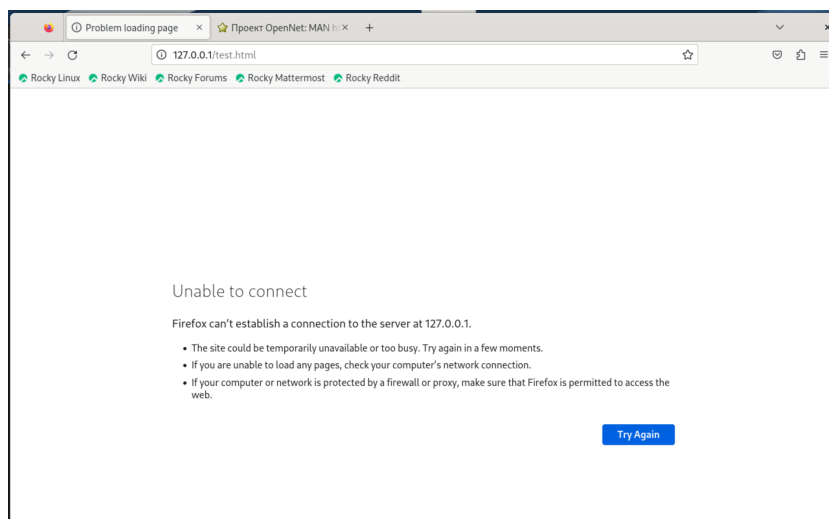


Рис. 4.17: Лог

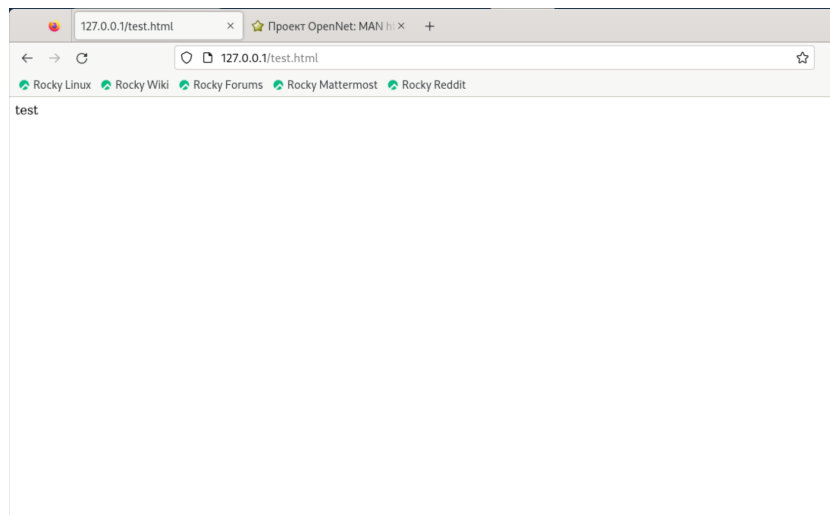


Рис. 4.18: Лог

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).

Настройка порта 81

Рис. 4.19: Настройка порта 81

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

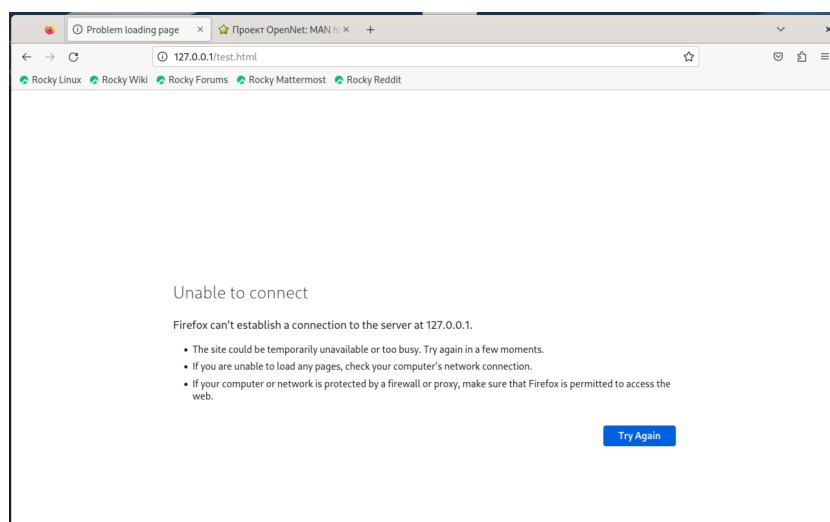


Рис. 4.20: Веб-страница

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).

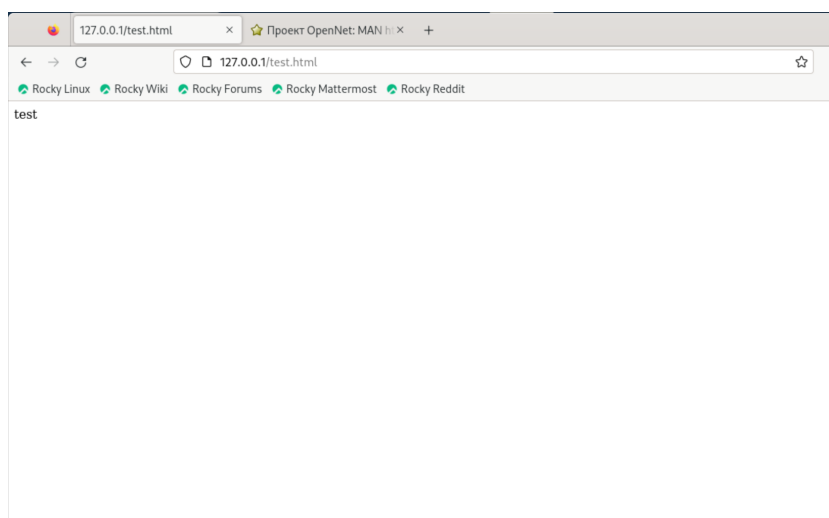


Рис. 4.21: Веб-страница

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).

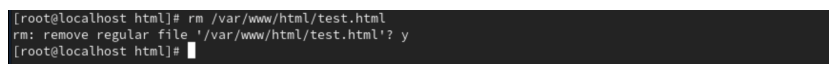


Рис. 4.22: Удаление

5 Выводы

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