

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Кондрашина Мария Сергеевна

Содержание

| | | |
|---|--|----|
| 1 | Цель работы | 6 |
| 2 | Теоретические сведения | 7 |
| 3 | Выполнение лабораторной работы. Создание программы | 8 |
| 4 | Выводы | 22 |
| 5 | Список литературы | 23 |

List of Figures

| | | |
|------|--|----|
| 3.1 | Подготовка лабораторного стенда | 8 |
| 3.2 | Подготовка лабораторного стенда | 9 |
| 3.3 | Подготовка лабораторного стенда | 10 |
| 3.4 | Подготовка лабораторного стенда | 10 |
| 3.5 | Подготовка лабораторного стенда | 10 |
| 3.6 | Подготовка лабораторного стенда | 11 |
| 3.7 | getenforce и sestatus | 11 |
| 3.8 | Обратилась с помощью браузера к веб-серверу, запущенному на компьютере | 12 |
| 3.9 | Веб-сервер Apache в списке процессов, его контекст безопасности | 12 |
| 3.10 | Текущее состояние переключателей SELinux для Apache | 13 |
| 3.11 | Статистика по политике с помощью команды seinfo | 14 |
| 3.12 | Тип файлов и поддиректорий, находящихся в директории /var/www и /var/www/html | 15 |
| 3.13 | Создайте от имени суперпользователя html-файл /var/www/html/test.html | 15 |
| 3.14 | Создайте от имени суперпользователя html-файл /var/www/html/test.html (консоль) | 15 |
| 3.15 | Контекст созданного файла | 16 |
| 3.16 | Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html | 16 |
| 3.17 | Тип файла test.html | 16 |
| 3.18 | Изменила контекст файла test.html с httpd_sys_content_t на samba_share_t | 17 |
| 3.19 | Попробовала ещё раз получить доступ к файлу через веб-сервер . | 17 |
| 3.20 | Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл | 18 |
| 3.21 | В файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81 | 18 |
| 3.22 | Проанализировала лог-файлы /var/log/messages | 19 |
| 3.23 | Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log | 19 |
| 3.24 | Список портов | 19 |
| 3.25 | Запуск веб-сервера Apache ещё раз и возвращение контекста httpd_sys_content_t к файлу test.html | 20 |
| 3.26 | Попытка получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html | 20 |

| | |
|---|----|
| 3.27 Исправила обратно конфигурационный файл apache, вернув Listen 80 | 20 |
| 3.28 Попытка удалить привязку http_port_t к 81 порту и удаление файла test.html | 21 |

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.

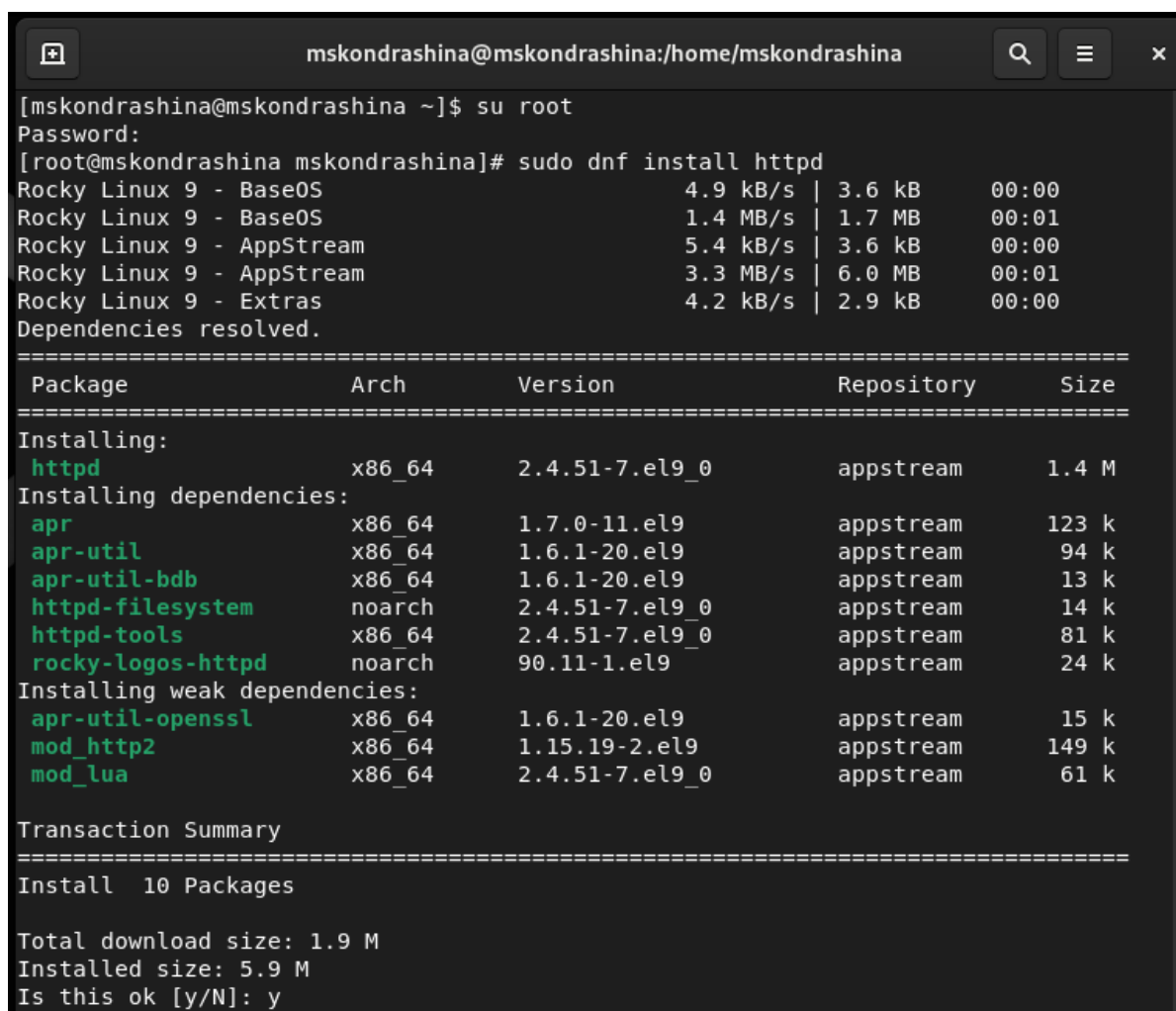
2 Теоретические сведения

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.[2]

3 Выполнение лабораторной работы.

Создание программы

1. Подготовка лабораторного стенда (fig. 3.1) -



```
[mskondrashina@mskondrashina ~]$ su root
Password:
[root@mskondrashina mskondrashina]# sudo dnf install httpd
Rocky Linux 9 - BaseOS                4.9 kB/s | 3.6 kB    00:00
Rocky Linux 9 - BaseOS                1.4 MB/s | 1.7 MB    00:01
Rocky Linux 9 - AppStream             5.4 kB/s | 3.6 kB    00:00
Rocky Linux 9 - AppStream             3.3 MB/s | 6.0 MB    00:01
Rocky Linux 9 - Extras                4.2 kB/s | 2.9 kB    00:00
Dependencies resolved.

=====
Package                Arch      Version              Repository            Size
=====
Installing:
  httpd                 x86_64    2.4.51-7.el9_0       appstream              1.4 M
Installing dependencies:
  apr                   x86_64    1.7.0-11.el9         appstream              123 k
  apr-util              x86_64    1.6.1-20.el9         appstream              94 k
  apr-util-bdb          x86_64    1.6.1-20.el9         appstream              13 k
  httpd-filesystem      noarch    2.4.51-7.el9_0       appstream              14 k
  httpd-tools           x86_64    2.4.51-7.el9_0       appstream              81 k
  rocky-logos-httpd     noarch    90.11-1.el9          appstream              24 k
Installing weak dependencies:
  apr-util-openssl      x86_64    1.6.1-20.el9         appstream              15 k
  mod_http2             x86_64    1.15.19-2.el9        appstream              149 k
  mod_lua               x86_64    2.4.51-7.el9_0       appstream              61 k

Transaction Summary
=====
Install 10 Packages

Total download size: 1.9 M
Installed size: 5.9 M
Is this ok [y/N]: y
```

Figure 3.1: Подготовка лабораторного стенда


```

Downloading Packages:
(1/10): rocky-logos-httpd-90.11-1.el9.noarch.rp  50 kB/s | 24 kB    00:00
(2/10): mod_lua-2.4.51-7.el9_0.x86_64.rpm      125 kB/s | 61 kB    00:00
(3/10): httpd-tools-2.4.51-7.el9_0.x86_64.rpm   163 kB/s | 81 kB    00:00
(4/10): httpd-filesystem-2.4.51-7.el9_0.noarch. 280 kB/s | 14 kB    00:00
(5/10): apr-util-openssl-1.6.1-20.el9.x86_64.rp 309 kB/s | 15 kB    00:00
(6/10): apr-util-bdb-1.6.1-20.el9.x86_64.rpm   246 kB/s | 13 kB    00:00
(7/10): apr-util-1.6.1-20.el9.x86_64.rpm       1.3 MB/s | 94 kB    00:00
(8/10): mod_http2-1.15.19-2.el9.x86_64.rpm     1.6 MB/s | 149 kB   00:00
(9/10): apr-1.7.0-11.el9.x86_64.rpm           1.8 MB/s | 123 kB   00:00
(10/10): httpd-2.4.51-7.el9_0.x86_64.rpm       6.2 MB/s | 1.4 MB   00:00
-----
Total                                          1.7 MB/s | 1.9 MB   00:01
Rocky Linux 9 - AppStream                    1.7 MB/s | 1.7 kB   00:00
Importing GPG key 0x350D275D:
  Userid   : "Rocky Enterprise Software Foundation - Release key 2022 <releng@rockylinux.org>"
  Fingerprint: 21CB 256A E16F C54C 6E65 2949 702D 426D 350D 275D
  From      : /etc/pki/rpm-gpg/RPM-GPG-KEY-Rocky-9
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing    : apr-1.7.0-11.el9.x86_64        1/10
  Installing    : apr-util-bdb-1.6.1-20.el9.x86_64 2/10
  Installing    : apr-util-1.6.1-20.el9.x86_64     3/10
  Installing    : apr-util-openssl-1.6.1-20.el9.x86_64 4/10
  Installing    : httpd-tools-2.4.51-7.el9_0.x86_64 5/10
  Running scriptlet: httpd-filesystem-2.4.51-7.el9_0.noarch 6/10

```

Figure 3.2: Подготовка лабораторного стенда

```

Running scriptlet: httpd-filesystem-2.4.51-7.el9_0.noarch 6/10
useradd warning: apache's uid 48 outside of the SYS_UID_MIN 201 and SYS_UID_MAX 999
range.

Installing      : httpd-filesystem-2.4.51-7.el9_0.noarch 6/10
Installing      : rocky-logos-httpd-90.11-1.el9.noarch 7/10
Installing      : mod_lua-2.4.51-7.el9_0.x86_64 8/10
Installing      : mod_http2-1.15.19-2.el9.x86_64 9/10
Installing      : httpd-2.4.51-7.el9_0.x86_64 10/10
Running scriptlet: httpd-2.4.51-7.el9_0.x86_64 10/10
Verifying       : rocky-logos-httpd-90.11-1.el9.noarch 1/10
Verifying       : mod_lua-2.4.51-7.el9_0.x86_64 2/10
Verifying       : httpd-tools-2.4.51-7.el9_0.x86_64 3/10
Verifying       : httpd-2.4.51-7.el9_0.x86_64 4/10
Verifying       : httpd-filesystem-2.4.51-7.el9_0.noarch 5/10
Verifying       : apr-util-openssl-1.6.1-20.el9.x86_64 6/10
Verifying       : apr-util-bdb-1.6.1-20.el9.x86_64 7/10
Verifying       : apr-util-1.6.1-20.el9.x86_64 8/10
Verifying       : mod_http2-1.15.19-2.el9.x86_64 9/10
Verifying       : apr-1.7.0-11.el9.x86_64 10/10

Installed:
apr-1.7.0-11.el9.x86_64          apr-util-1.6.1-20.el9.x86_64
apr-util-bdb-1.6.1-20.el9.x86_64 apr-util-openssl-1.6.1-20.el9.x86_64
httpd-2.4.51-7.el9_0.x86_64      httpd-filesystem-2.4.51-7.el9_0.noarch
httpd-tools-2.4.51-7.el9_0.x86_64 mod_http2-1.15.19-2.el9.x86_64
mod_lua-2.4.51-7.el9_0.x86_64    rocky-logos-httpd-90.11-1.el9.noarch

Complete!
[root@mskondrashina mskondrashina]# sudo service httpd start
Redirecting to /bin/systemctl start httpd.service

```

Figure 3.3: Подготовка лабораторного стенда

```

96 # it explicitly to prevent problems during startup.
97 #
98 # If your host doesn't have a registered DNS name, enter its IP address here.
99 #
100 #ServerName test.ru
101
102 ..

```

Figure 3.4: Подготовка лабораторного стенда

```

[root@mskondrashina mskondrashina]# chmod 777 /etc/httpd/conf/httpd.conf

```

Figure 3.5: Подготовка лабораторного стенда

```

[root@mskondrashina mskondrashina]# chmod 777 /etc/httpd/conf/httpd.conf
[root@mskondrashina mskondrashina]# iptables -F
[root@mskondrashina mskondrashina]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACC
EPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@mskondrashina mskondrashina]# iptables -P INPUT ACCEPT
[root@mskondrashina mskondrashina]# iptables -P OUTPUT ACCEPT
iptables: Bad policy name. Run `dmesg' for more information.
[root@mskondrashina mskondrashina]# iptables -P OUTPUT ACCEPT

```

Figure 3.6: Подготовка лабораторного стенда

2. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`(fig. 3.7)

```

[root@mskondrashina mskondrashina]# getenforce
Enforcing
[root@mskondrashina mskondrashina]# 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

```

Figure 3.7: `getenforce` и `sestatus`

3. Обратилась с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедилась, что последний работает: (fig. 3.8)

```
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2022-10-09 21:10:40 MSK; 13min ago
     Docs: man:httpd.service(8)
  Main PID: 3260 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
    Tasks: 213 (limit: 12212)
   Memory: 23.0M
      CPU: 472ms
   CGroup: /system.slice/httpd.service
           └─3260 /usr/sbin/httpd -DFOREGROUND
             └─3261 /usr/sbin/httpd -DFOREGROUND
               └─3265 /usr/sbin/httpd -DFOREGROUND
                 └─3266 /usr/sbin/httpd -DFOREGROUND
                   └─3268 /usr/sbin/httpd -DFOREGROUND

Oct 09 21:10:39 mskondrashina.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 09 21:10:40 mskondrashina.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 09 21:10:40 mskondrashina.localdomain httpd[3260]: Server configured, listening on: port 80
~
[root@mskondrashina mskondrashina]#
```

Figure 3.8: Обратилась с помощью браузера к веб-серверу, запущенному на компьютере

4. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности и занесла эту информацию в отчёт (httpd_t). (fig. 3.9)

```
[root@mskondrashina mskondrashina]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3260 0.0 0.5 20248 11728 ? Ss 21:10 0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3261 0.0 0.3 21572 7540 ? S 21:10 0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3265 0.0 0.6 1210512 13072 ? Sl 21:10 0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3266 0.0 0.5 1079376 11024 ? Sl 21:10 0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3268 0.0 0.5 1079376 11024 ? Sl 21:10 0:00 /usr/s
bin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3887 0.0 0.1 221668 2300 pts/0 S+ 21:25 0:0
0 grep --color=auto httpd
[root@mskondrashina mskondrashina]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 3260 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3261 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3265 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3266 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3268 ? 00:00:00 httpd
[root@mskondrashina mskondrashina]#
```

Figure 3.9: Веб-сервер Apache в списке процессов, его контекст безопасности

5. Посмотрела текущее состояние переключателей SELinux для Apache. (fig. 3.10)

```

[root@mskondrashina mskondrashina]# sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting 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_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_ssi_exec off
httpd_sys_script_anon_write off

```

Figure 3.10: Текущее состояние переключателей SELinux для Apache

6. Посмотрела статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов. (fig. 3.11)

```

[root@mskondrashina mskondrashina]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          133      Permissions:        454
Sensitivities:    1        Categories:         1024
Types:            5002     Attributes:         254
Users:            8        Roles:              14
Booleans:         347     Cond. Expr.:       381
Allow:            63996    Neverallow:         0
Auditallow:       168     Dontaudit:         8417
Type_trans:       258486   Type_change:        87
Type_member:      35       Range_trans:        5960
Role_allow:       38       Role_trans:         420
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:            651
Netifcon:         0        Nodecon:            0
[root@mskondrashina mskondrashina]#

```

Figure 3.11: Статистика по политике с помощью команды seinfo

- Множество пользователей: 8
- Роли: 14
- Типы: 5002

7. Определила тип файлов и поддиректорий, находящихся в директории /var/www и /var/www/html (fig. 3.12)

```

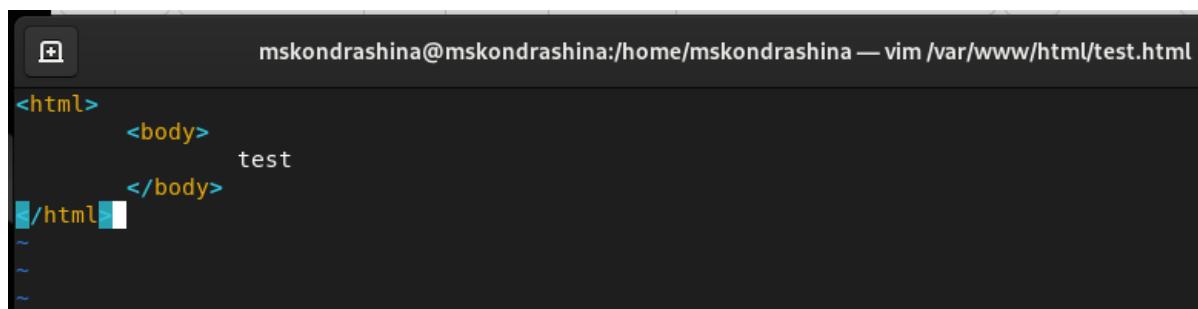
Netircon: 0 Nodecon: 0
[root@mskondrashina mskondrashina]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 c
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 h
[root@mskondrashina mskondrashina]# ls -lZ /var/www/html
total 0

```

Figure 3.12: Тип файлов и поддиректорий, находящихся в директории /var/www и /var/www/html

Круг пользователей, которым разрешено создание файлов в директории - пользователь (user)

8. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (fig. 3.13) - (fig. 3.14)

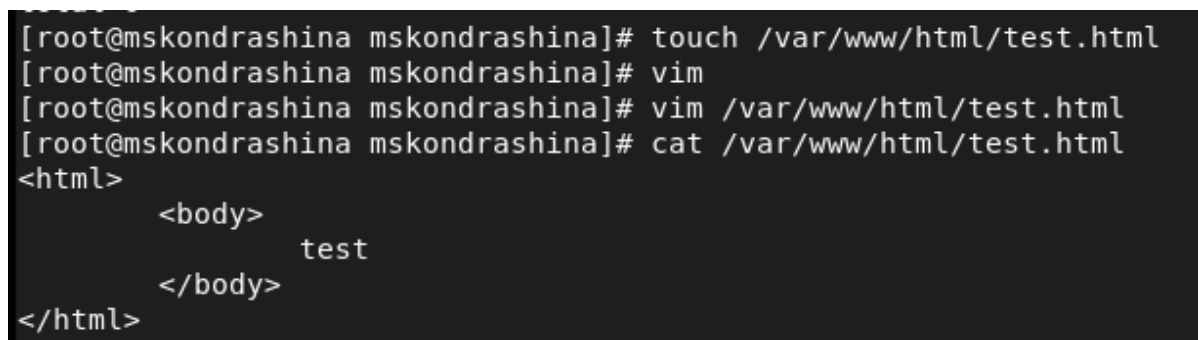


```

mskondrashina@mskondrashina:/home/mskondrashina — vim /var/www/html/test.html
<html>
    <body>
        test
    </body>
</html>

```

Figure 3.13: Создайте от имени суперпользователя html-файл /var/www/html/test.html



```

[root@mskondrashina mskondrashina]# touch /var/www/html/test.html
[root@mskondrashina mskondrashina]# vim
[root@mskondrashina mskondrashina]# vim /var/www/html/test.html
[root@mskondrashina mskondrashina]# cat /var/www/html/test.html
<html>
    <body>
        test
    </body>
</html>

```

Figure 3.14: Создайте от имени суперпользователя html-файл /var/www/html/test.html (консоль)

9. Проверила контекст созданного файла. Занесла в отчёт контекст - `httpd_sys_content_t`, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html` (fig. 3.15)

```
[root@mskondrashina mskondrashina]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 39 Oct  9 21:45 test.html
```

Figure 3.15: Контекст созданного файла

10. Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедилась, что файл был успешно отображён.(fig. 3.16)

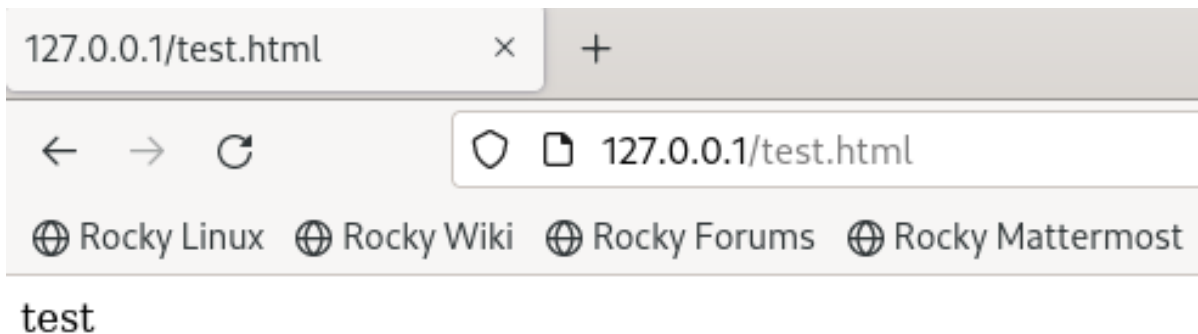


Figure 3.16: Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`

11. Тип файла `test.html` - `httpd_sys_content_t`. 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.(fig. 3.17)

```
[root@mskondrashina mskondrashina]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Figure 3.17: Тип файла `test.html`

12. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`(fig. 3.18)

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

Figure 3.18: Изменила контекст файла `test.html` с `httpd_sys_content_t` на `samba_share_t`

13. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.(fig. 3.19)

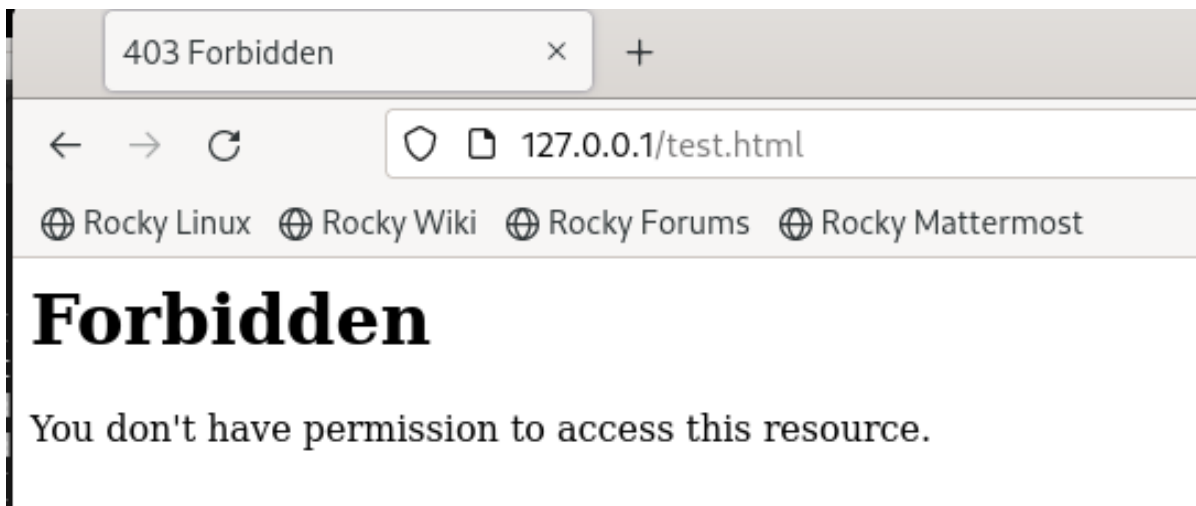


Figure 3.19: Попробовала ещё раз получить доступ к файлу через веб-сервер

14. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл(fig. 3.20)

```

[root@mskondrashina mskondrashina]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 39 Oct  9 21:45 /var/www/html/test.html
[root@mskondrashina mskondrashina]# tail /var/log/messages
Oct  9 21:56:02 mskondrashina systemd[1]: Starting dnf makecache...
Oct  9 21:56:04 mskondrashina dnf[4776]: Rocky Linux 9 - BaseOS                               3.9 kB/s | 3
.6 kB    00:00
Oct  9 21:56:05 mskondrashina dnf[4776]: Rocky Linux 9 - AppStream                         4.7 kB/s | 3
.6 kB    00:00
Oct  9 21:56:06 mskondrashina dnf[4776]: Rocky Linux 9 - Extras                         4.0 kB/s | 2
.9 kB    00:00
Oct  9 21:56:06 mskondrashina dnf[4776]: Metadata cache created.
Oct  9 21:56:06 mskondrashina systemd[1]: dnf-makecache.service: Deactivated successfully.
Oct  9 21:56:06 mskondrashina systemd[1]: Finished dnf makecache.
Oct  9 21:56:06 mskondrashina systemd[1]: dnf-makecache.service: Consumed 1.914s CPU time.
Oct  9 21:56:50 mskondrashina gnome-shell[1628]: libinput error: event2 - AT Translated Set 2 keyboa
rd: client bug: event processing lagging behind by 885ms, your system is too slow
Oct  9 21:57:00 mskondrashina kernel: sched: RT throttling activated
[root@mskondrashina mskondrashina]#

```

Figure 3.20: Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл

15. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81. (fig. 3.21)

```

45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #

```

Figure 3.21: В файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81

16. Выполнила перезапуск веб-сервера Apache. Сбой не произошёл. Проанализировала лог-файлы `tail -nl /var/log/messages`. (fig. 3.22)

Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выяснила, в каких файлах появились записи - только в /var/log/audit/audit.log. (fig. 3.23)

```
[root@mskondrashina mskondrashina]# apachectl restart
[root@mskondrashina mskondrashina]# tail /var/log/messages
Oct 9 22:02:55 mskondrashina systemd[1]: httpd.service: Consumed 1.782s CPU time.
Oct 9 22:02:55 mskondrashina systemd[1]: Starting The Apache HTTP Server...
Oct 9 22:02:56 mskondrashina systemd[1]: Started The Apache HTTP Server.
Oct 9 22:02:56 mskondrashina httpd[4918]: Server configured, listening on: port 81
Oct 9 22:03:10 mskondrashina systemd[1531]: Started dbus-:1.2-org.gnome.gedit@4.service.
Oct 9 22:03:11 mskondrashina journal[1628]: meta_window_set_stack_position_no_sync: assertion 'window->stack_position >= 0' failed
Oct 9 22:03:20 mskondrashina systemd[1531]: dbus-:1.2-org.gnome.gedit@4.service: Consumed 3.060s CPU time.
Oct 9 22:03:38 mskondrashina systemd[1531]: Started dbus-:1.2-org.gnome.gedit@5.service.
Oct 9 22:03:38 mskondrashina journal[1628]: meta_window_set_stack_position_no_sync: assertion 'window->stack_position >= 0' failed
Oct 9 22:03:45 mskondrashina systemd[1531]: dbus-:1.2-org.gnome.gedit@5.service: Consumed 1.863s CPU time.
```

Figure 3.22: Проанализировать лог-файлы /var/log/messages

```
[root@mskondrashina mskondrashina]# tail /var/log/http/error_log
tail: cannot open '/var/log/http/error_log' for reading: No such file or directory
[root@mskondrashina mskondrashina]# cat /var/log/http/error_log
cat: /var/log/http/error_log: No such file or directory
[root@mskondrashina mskondrashina]# tail /var/log/http/access_log
tail: cannot open '/var/log/http/access_log' for reading: No such file or directory
[root@mskondrashina mskondrashina]# tail /var/log/audit/audit.log
type=SYSCALL msg=audit(1665341737.565:205): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c al=7f779803de30 a2=7f7796ffcc830 a3=100 items=0 ppid=3260 p
id=3260 uid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system
_u:system_r:httpd_t:s0 keys=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache"
SGID="apache"
type=PROCTITLE msg=audit(1665341737.565:205): proctitle=2F7573722F7362696E2F687474064002044464F524547524F554E44
type=SERVICE_START msg=audit(1665341737.603:206): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedorapro
ject.Setroubleshootd@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665341739.884:207): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedorapro
ject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665341752.256:208): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproj
ect.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665341752.292:209): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproj
ect.Setroubleshootd@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665341766.326:210): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="syst
emd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665341766.327:211): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="syste
md" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665342175.517:212): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe=
"/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665342176.035:213): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe=
"/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
```

Figure 3.23: Просмотреть файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log

17. Выполнить команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверить список портов командой `semanage port -l | grep http_port_t`. Убедилась, что порт 81 появился в списке.(fig. 3.24)

```
[root@mskondrashina mskondrashina]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@mskondrashina mskondrashina]# 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
```

Figure 3.24: Список портов

18. Попробовала запустить веб-сервер Apache ещё раз, он снова запустился. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. По-

сле этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. (fig. 3.25)-(fig. 3.26)

```
[root@mskondrashina mskondrashina]# apachectl restart
[root@mskondrashina mskondrashina]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Figure 3.25: Запуск веб-сервера Apache ещё раз и возвращение контекста `httpd_sys_content_t` к файлу `test.html`

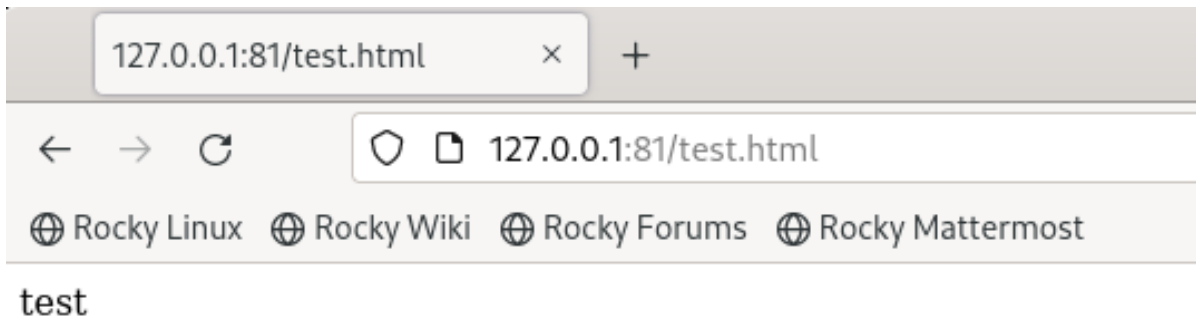


Figure 3.26: Попытка получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`

19. Исправила обратно конфигурационный файл `apache`, вернув `Listen 80`. (fig. 3.27)

```
45 #
46 #Listen 12.34.56.78:80
47 Listen 80
48
49 #
```

Figure 3.27: Исправила обратно конфигурационный файл `apache`, вернув `Listen 80`

20. Попыталась удалить привязку `http_port_t` к 81 порту, что не получилось так как 81 порт defined in policy и не может быть удален. Удалила файл `/var/www/html/test.html` (fig. 3.28)

```
[root@mskondrashina mskondrashina]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@mskondrashina mskondrashina]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@mskondrashina mskondrashina]# ls -l /var/www/html
total 0
[root@mskondrashina mskondrashina]#
```

Figure 3.28: Попытка удалить привязку `http_port_t` к 81 порту и удаление файла `test.html`

4 Выводы

Выполнила лабораторную работу №6.

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1.

Проверила работу SELinx на практике совместно с веб-сервером Apache.

5 Список литературы

1. Методические материалы курса. “Информационная безопасность компьютерных сетей” Кулябов Д. С., Королькова А. В., Геворкян М. Н.
2. <https://ru.wikipedia.org/wiki/SELinux>