

# **Отчет по лабораторной работе №6**

**Мандатное разграничение прав в Linux**

Динькиев Валерий

# Содержание

1	Цель работы	4
2	Подготовка лабораторного стенда:	5
3	Выполнение лабораторной работы	7
4	Выводы	16

# List of Figures

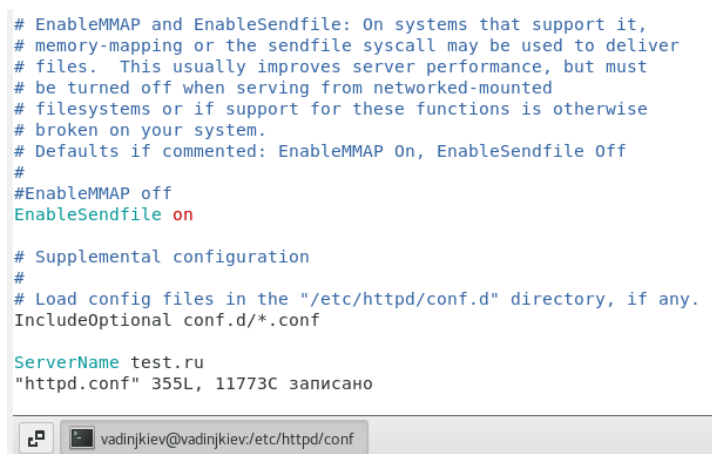
2.1	Параметр ServerName . . . . .	5
2.2	Отключение фильтра . . . . .	5
2.3	Отключение фильтра . . . . .	6
2.4	Добавление разрешающих правил . . . . .	6
3.1	Проверка через браузер . . . . .	8
3.2	Проверка статуса . . . . .	8
3.3	веб-сервер Apache . . . . .	8
3.4	Просмотр переключателей SELinux для Apache . . . . .	9
3.5	Статистика . . . . .	10
3.6	Статистика . . . . .	10
3.7	Создание файла . . . . .	11
3.8	Проверка . . . . .	11
3.9	Получение доступа к файлу через браузер . . . . .	11
3.10	Изменение контекста, проверка . . . . .	11
3.11	Получение доступа к файлу через браузер . . . . .	12
3.12	Изменение порта 80 на 81 . . . . .	12
3.13	Анализ лог-файла . . . . .	13
3.14	Просмотр файла /var/log/http/error_log . . . . .	13
3.15	Просмотр файла /var/log/http/access_log . . . . .	13
3.16	Просмотр файла var/log/audit/audit.log . . . . .	13
3.17	Выполнение и проверка . . . . .	14
3.18	Возвращение контекста . . . . .	14
3.19	Получение доступа к файлу через браузер . . . . .	14
3.20	Исправленный файл apache . . . . .	14
3.21	Удаление привязки к 81 порту . . . . .	14
3.22	Удаление файла /var/www/html/test.html . . . . .	15

# 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 Подготовка лабораторного стенда:

1. В конфигурационном файле `/etc/httpd/httpd.conf` задал параметр `ServerName`. (рис. 2.1).



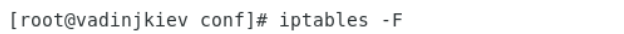
```
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# 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

ServerName test.ru
"httpd.conf" 355L, 11773C записано
```

Figure 2.1: Параметр `ServerName`

2. Также проследил, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключил фильтр командами: `iptables -F`, `iptables -P INPUT ACCEPT`, `iptables -P OUTPUT ACCEPT`. Так же добавил разрешающие правила. (рис. 2.2), (рис. 2.3), (рис. 2.4).



```
[root@vadinjkiiev conf]# iptables -F
```

Figure 2.2: Отключение фильтра

```
[root@vadinjkiev conf]# iptables -P INPUT ACCEPT
[root@vadinjkiev conf]# iptables -P OUTPUT ACCEPT
[root@vadinjkiev conf]# █
```

Figure 2.3: Отключение фильтра

```
[root@vadinjkiev conf]# iptables -P INPUT ACCEPT
[root@vadinjkiev conf]# iptables -P OUTPUT ACCEPT
[root@vadinjkiev conf]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@vadinjkiev conf]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@vadinjkiev conf]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@vadinjkiev conf]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@vadinjkiev conf]# █
```

Figure 2.4: Добавление разрешающих правил

### 3 Выполнение лабораторной работы

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. ??).

```
[root@vadinjkiev conf]# getenforce
Enforcing
[root@vadinjkiev conf]# 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
Max kernel policy version:    31
[root@vadinjkiev conf]# █
```

2. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: `service httpd status` (рис. 3.1), (рис. 3.2).

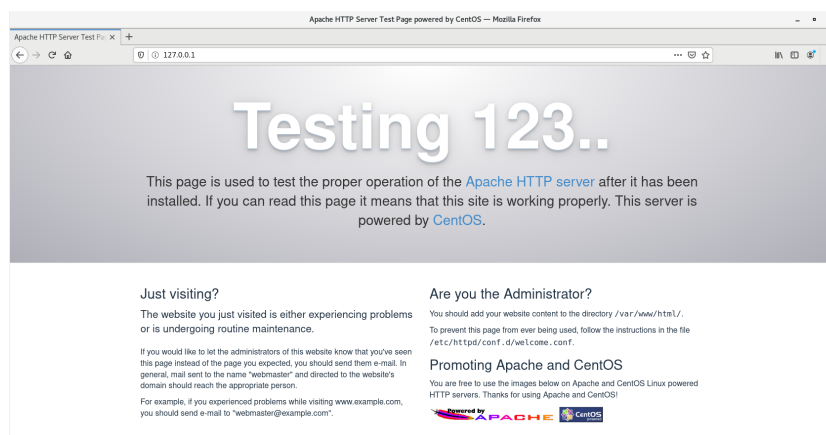


Figure 3.1: Проверка через браузер

```
[root@vadinjkiy conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3182  0.0  0.0 230448  628 ?        Ss   03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3185  0.0  0.0 232524  836 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3186  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3187  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3188  0.0  0.1 232660  1992 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3189  0.0  0.1 232660  1812 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4405  0.0  0.2 232524  2304 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4406  0.0  0.2 232524  2344 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4438  0.0  0.0 112832  976 pts/0  S+  03:42   0:00 grep --color=auto httpd
[root@vadinjkiy conf]#
```

Figure 3.2: Проверка статуса

3. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности. (рис. 3.3).

```
[root@vadinjkiy conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3182  0.0  0.0 230448  628 ?        Ss   03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3185  0.0  0.0 232524  836 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3186  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3187  0.0  0.0 232524  172 ?        S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3188  0.0  0.1 232660  1992 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3189  0.0  0.1 232660  1812 ?       S    03:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4405  0.0  0.2 232524  2304 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4406  0.0  0.2 232524  2344 ?       S    03:41   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4438  0.0  0.0 112832  976 pts/0  S+  03:42   0:00 grep --color=auto httpd
[root@vadinjkiy conf]#
```

Figure 3.3: веб-сервер Apache

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратил внимание, что многие из них находятся в положении «off». (рис. 3.4).



```
[root@vadinjkiev conf]# 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
Max kernel policy version:      31

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
condor_tcp_network_connect       off
conman_can_network               off
conman_use_nfs                   off
container_connect_any            off
cron_can_relabel                 off
cron_system_cronjob_use_shares   off
cron_userdomain_transition       on
cups_execmem                     off
cvs_read_shadow                  off
daemons_dump_core                off
daemons_enable_cluster_mode     off
daemons_use_tcp_wrapper         off
daemons_use_tty                 off
dbadm_exec_content               on
```

Figure 3.4: Просмотр переключателей SELinux для Apache

5. Посмотрел статистику по политике с помощью команды seinfo, также определил множество пользователей(8), ролей(14), типов(4793) (рис. 3.5).

```

[root@vadinjkiev conf]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1        Categories:       1024
Types:            4793     Attributes:        253
Users:            8        Roles:            14
Booleans:         316     Cond. Expr.:      362
Allow:            107834   Neverallow:        0
Auditallow:       158     Dontaudit:         10022
Type_trans:       18153   Type_change:       74
Type_member:      35      Role_allow:        37
Role_trans:       414     Range_trans:       5899
Constraints:      143     Validatetrans:     0
Initial SIDs:     27      Fs_use:            32
Genfscon:         103     Portcon:           614
Netifcon:         0       Nodecon:           0
Permissives:      0       Polcap:            5

[root@vadinjkiev conf]# █

```

Figure 3.5: Статистика

6. Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: `ls -lZ /var/www`.
7. Определил тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`.
8. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 3.6).

```

[root@vadinjkiev conf]# ls -lZ /var/www

drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@vadinjkiev conf]#
[root@vadinjkiev conf]# ls -lZ /var/www/html
[root@vadinjkiev conf]# ls -l /var/www
итого 0
drwxr-xr-x. 2 root root 6 ноя 10 17:27 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 10 17:27 html
[root@vadinjkiev conf]# █

```

Figure 3.6: Статистика

9. Создал от имени суперпользователя (так как в дистрибутиве после

установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 3.7).



Figure 3.7: Создание файла

10. Проверил контекст созданного файла. httpd\_sys\_content\_t (рис. 3.8).

```
[root@vadinjkiev html]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@vadinjkiev html]#
```

Figure 3.8: Проверка

11. Обратился к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедился, что файл был успешно отображён. (рис. 3.9).

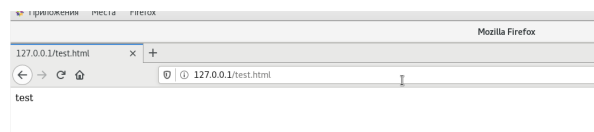


Figure 3.9: Получение доступа к файлу через браузер

12. Проверил контекст файла командой: `ls -lZ /var/www/html/test.html` (рис. 3.10).

13. Изменил контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверил, что контекст поменялся. (рис. 3.10).

```
[root@vadinjkiev html]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@vadinjkiev html]# chcon -t samba_share_t /var/www/html/test.html
[root@vadinjkiev html]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@vadinjkiev html]#
```

Figure 3.10: Изменение контекста, проверка

14. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получил сообщение об ошибке. (рис. 3.11).



Figure 3.11: Получение доступа к файлу через браузер

15. Проанализировал ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: `tail /var/log/messages` (рис. ??).



16. Попробовал 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` нашел строчку `Listen 80` и заменил её на `Listen 81` (рис. 3.12).

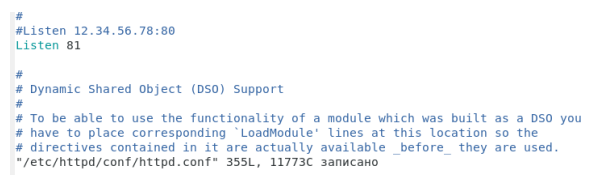


Figure 3.12: Изменение порта 80 на 81

17. Проанализировал лог-файлы. Просмотрел файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`. (рис. 3.13), (рис. 3.14), (рис. 3.15), (рис. 3.16).

Figure 3.13: Анализ лог-файла

Figure 3.14: Просмотр файла /var/log/http/error\_log

Figure 3.15: Просмотр файла /var/log/http/access\_log

Figure 3.16: Просмотр файла `var/log/audit/audit.log`

13

```
[root@vadinjkiy httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 уже определен
[root@vadinjkiy httpd]# 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@vadinjkiy httpd]#
```

Figure 3.17: Выполнение и проверка

19. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test». (рис. 3.18), (рис. 3.19).

```
[root@vadinjkiy httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vadinjkiy httpd]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 ноя 27 03:53 /var/www/html/test.html
[root@vadinjkiy httpd]# ls -lZ /var/www/html/test.html
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@vadinjkiy httpd]#
```

Figure 3.18: Возвращение контекста



Figure 3.19: Получение доступа к файлу через браузер

20. Исправил обратно конфигурационный файл `apache`, вернув `Listen80`. (рис. 3.20).



Figure 3.20: Исправленный файл `apache`

21. Удалил привязку `http_port_t` к 81 порту. (рис. 3.21).

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

Figure 3.21: Удаление привязки к 81 порту

22. Удалил файл /var/www/html/test.html. (рис. 3.22).

```
[root@vadinjkiev httpd]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@vadinjkiev httpd]#
```

Figure 3.22: Удаление файла /var/www/html/test.html

## 4 Выводы

На основе проделанной работы развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.