

# Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Поленикова Анна Алексеевна

# Содержание

Цель работы	4
Выполнение лабораторной работы	5
Вывод	11

## Список иллюстраций

0.1	Проверка работы SELinux и веб-сервера . . . . .	5
0.2	Веб-сервер Apache в списке процессов . . . . .	6
0.3	Состояние переключателей SELinux для Apache . . . . .	6
0.4	Статистика . . . . .	7
0.5	Тип файлов и поддиректорий в директориях /var/www и /var/www/html . . . . .	7
0.6	Создание html-файла /var/www/html/test.html . . . . .	8
0.7	Обращение к файлу test.html через веб-сервер . . . . .	8
0.8	Контекст файла test.html . . . . .	8
0.9	log-файлы веб-сервера Apache и системный log-файл . . . . .	9
0.10	Запуск веб-сервера Apache на прослушивание TCP-порта 81 . . . . .	9
0.11	Вывод списка портов . . . . .	10
0.12	Возвращение контекста httpd_sys_content_t файлу test.html . . . . .	10

## Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

# Выполнение лабораторной работы

1. Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Обратилась к веб-серверу, запущенному на компьютере, и убедилась, что последний работает с помощью команды `service httpd status`.

```
[aaapolnikova@aaapolnikova ~]$ getenforce
Enforcing
[aaapolnikova@aaapolnikova ~]$ 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
[aaapolnikova@aaapolnikova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese
   Active: active (running) since Sat 2021-11-27 16:56:19 MSK; 22min ago
     Docs: man:httpd.service(8)
   Main PID: 34336 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 4809)
    Memory: 10.0M
   CGroup: /system.slice/httpd.service
           └─34336 /usr/sbin/httpd -DFOREGROUND
             └─34343 /usr/sbin/httpd -DFOREGROUND
               └─34344 /usr/sbin/httpd -DFOREGROUND
                 └─34345 /usr/sbin/httpd -DFOREGROUND
                   └─34346 /usr/sbin/httpd -DFOREGROUND
lines 1-14/14 (END)
```

Рис. 0.1: Проверка работы SELinux и веб-сервера

2. Нашла веб-сервер Apache в списке процессов и определила его контекст безопасности, используя команду `ps auxZ | grep httpd`.

```
[aapolenikova@aapolenikova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      34336  0.0  0.0 282912  708 ?
      Ss  16:56   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  34343  0.0  0.0 296796  152 ?
      S   16:56   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  34344  0.0  0.0 1354584  780 ?
      Sl  16:56   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  34345  0.0  0.0 1354584  760 ?
      Sl  16:56   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  34346  0.0  0.0 1485712  760 ?
      Sl  16:56   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aapolen+ 35935 0.0
0.1 221928 1192 pts/0 S+ 17:22   0:00 grep --color=auto httpd
```

Рис. 0.2: Веб-сервер Apache в списке процессов

3. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`. Многие из них находятся в положении «off».

```
[aapolenikova@aapolenikova ~]$ 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_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
```

Рис. 0.3: Состояние переключателей SELinux для Apache

4. Посмотрела статистику по политике с помощью команды `seinfo` и определила

множество пользователей, ролей, типов.

```
[aapolenikova@aapolenikova ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      132      Permissions:      464
Sensitivities: 1        Categories:       1024
Types:        4936     Attributes:       252
Users:        8        Roles:           14
Booleans:     335      Cond. Expr.:     380
Allow:        110637   Neverallow:      0
Auditallow:   163      Dontaudit:       10251
Type_trans:   243882   Type_change:     87
Type_member:  35       Range_trans:     5781
Role_allow:   37       Role_trans:      420
Constraints:  72       Validatetrans:   0
MLS Constrai: 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:          34
Genfscon:     107      Portcon:         642
Netifcon:     0        Codecon:         0
```

Рис. 0.4: Статистика

5. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`. Определила тип файлов, находящихся в директории /var/www/html с помощью команды `ls -lZ /var/www/html`. Создание файлов в директории /var/www/html разрешено только root пользователю.

```
[aapolenikova@aapolenikova ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58
cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58
html
[aapolenikova@aapolenikova ~]$ ls -lZ /var/www/html
итого 0
```

Рис. 0.5: Тип файлов и поддиректорий в директориях /var/www и /var/www/html

6. Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

test

```
[aapolenikova@aapolenikova ~]$ su
Пароль:
[root@aapolenikova aapolenikova]# touch /var/www/html/test.html
[root@aapolenikova aapolenikova]# echo "test" >> /var/www/html/test.html
```

Рис. 0.6: Создание html-файла /var/www/html/test.html

7. Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.  
Файл был успешно отображён.

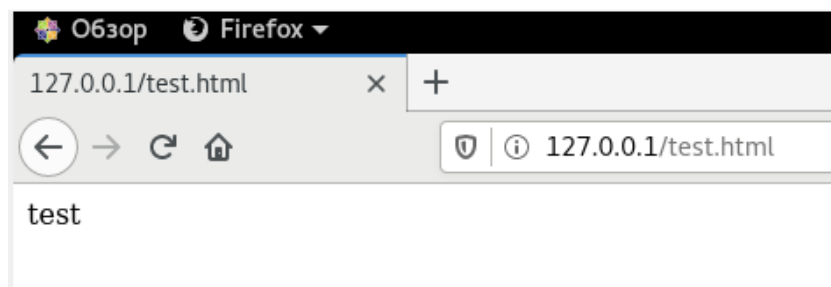


Рис. 0.7: Обращение к файлу test.html через веб-сервер

8. Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd`. Проверила контекст файла `ls -Z /var/www/html/test.html`. При выполнении команды был получен контекст `httpd_sys_content_t`, который позволяет процессу `httpd` получить доступ к файлу. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` с помощью команды `chcon -t samba_share_t /var/www/html/test.html` и проверила, что контекст поменялся с помощью команды `ls -Z /var/www/html/test.html`.

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

Рис. 0.8: Контекст файла test.html

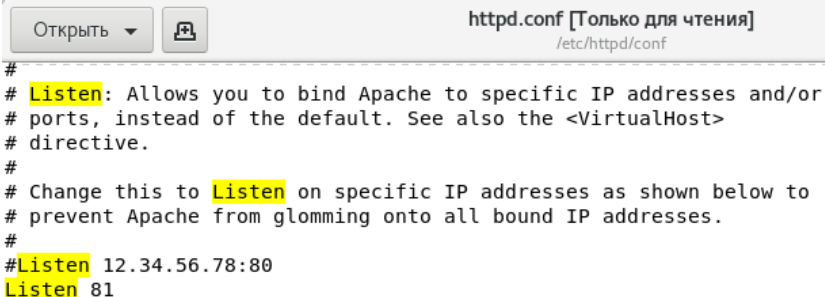


9. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. При выполнении команды получила сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`
10. Просмотрела log-файлы веб-сервера Apache с помощью команды `ls -l /var/www/html/test.html`. Также просмотрела системный лог-файл командой `tail /var/log/messages`.

```
[root@aapolenikova aapolenikova]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 5 ноя 27 17:50 /var/www/html/test.html
[root@aapolenikova aapolenikova]# tail /var/log/messages
Nov 27 18:09:05 aapolenikova setroubleshoot[38227]: failed to retrieve rpm info for
/var/www/html/test.html
Nov 27 18:09:06 aapolenikova dbus-daemon[849]: [system] Activating service name='org
.fedoraproject.SetroubleshootPrivileged' requested by ':1.721' (uid=978 pid=38227 co
mm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:system_r:set
roubleshootd t:s0-s0:c0.c1023") (using servicehelper)
Nov 27 18:09:07 aapolenikova dbus-daemon[849]: [system] Successfully activated servi
ce 'org.fedoraproject.SetroubleshootPrivileged'
Nov 27 18:09:10 aapolenikova setroubleshoot[38227]: SELinux is preventing /usr/sbin/
httpd from getattr access on the file /var/www/html/test.html. For complete SELinux
messages run: sealert -l 6b7609af-0046-4693-9d3a-f1c6e8747dd8
Nov 27 18:09:10 aapolenikova setroubleshoot[38227]: SELinux is preventing /usr/sbin/
httpd from getattr access on 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_sys cont
ent t.#012Then you can run restorecon. The access attempt may have been stopped due
to insufficient permissions to access a parent directory in which case try to change
the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/tes
t.html#012#012***** Plugin public content (7.83 confidence) suggests *****
```

Рис. 0.9: log-файлы веб-сервера Apache и системный log-файл

11. 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`.



```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 0.10: Запуск веб-сервера Apache на прослушивание TCP-порта 81

12. Выполнила перезапуск веб-сервера Apache, при этом сбоя не произошло, поскольку порт 81 уже был определен.
13. Проанализировала лог-файлы с помощью команды `tail -nl /var/log/messages`. Просмотрела файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`.
14. Выполнила команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверила список портов командой `semanage port -l | grep http_port_t`. Порт 81 в списке.

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

Рис. 0.11: Вывод списка портов

15. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` командой `chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.

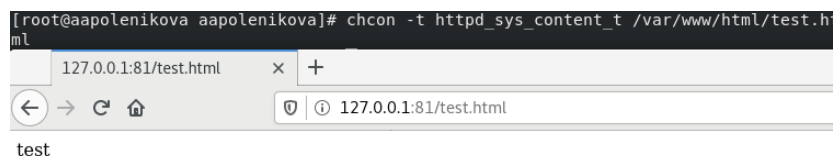


Рис. 0.12: Возвращение контекста `httpd_sys_content_t` файлу `test.html`

16. Исправила обратно конфигурационный файл `apache`, вернув `Listen 80`.
17. Удалила привязку `http_port_t` к 81 порту командой `semanage port -d -t http_port_t -p tcp 81`.
18. Удалила файл `/var/www/html/test.html` командой `rm /var/www/html/test.html`.

## Вывод

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