

Лабораторная работа №6

Мандатное разграничение прав в Linux

Маслова Анастасия Сергеевна

Содержание

1	Цель работы	1
2	Выполнение лабораторной работы.....	1
3	Вывод.....	8
	Список литературы	8

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Выполнение лабораторной работы

1. Войдя в систему с полученными учётными данными, я убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис. [??]).

```
[asmaslova@asmaslova ~]$ 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
[asmaslova@asmaslova ~]$ getenforce
Enforcing
```

Выполнение команд `getenforce` и `sestatus`

2. С помощью браузера я обратилась к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает, с помощью команды `service httpd status` (рис. [??]).

```
[asmaslova@asmaslova ~]$ getenforce
Enforcing
[asmaslova@asmaslova ~]$ 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 Fri 2024-10-11 18:06:05 EDT; 14min ago
     Docs: man:httpd.service(8)
   Main PID: 41088 (httpd)
   Status: "Total requests: 4; Idle/Busy workers 100/0;Requests/sec: 0.00449; B
   Tasks: 278 (limit: 12232)
   Memory: 31.7M
   CGroup: /system.slice/httpd.service
           └─41088 /usr/sbin/httpd -DFOREGROUND
             └─41095 /usr/sbin/httpd -DFOREGROUND
               └─41096 /usr/sbin/httpd -DFOREGROUND
                 └─41097 /usr/sbin/httpd -DFOREGROUND
                   └─41098 /usr/sbin/httpd -DFOREGROUND
                     └─42107 /usr/sbin/httpd -DFOREGROUND

Oct 11 18:06:05 asmaslova.localdomain systemd[1]: Starting The Apache HTTP Serv
Oct 11 18:06:05 asmaslova.localdomain systemd[1]: Started The Apache HTTP Serv
Oct 11 18:06:05 asmaslova.localdomain httpd[41088]: Server configured, listenin
lines 1-19/19 (END)
```

Выполнение команды `service httpd status`

3. В списке процессов я нашла веб-сервер Apache и определила его контекст безопасности. Для этого я использовала команду `ps auxZ | grep httpd` (рис. [??]).

```
[asmaslova@asmaslova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 41088 0.0 0.4 265188 9820 ?
Ss 18:06 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41095 0.0 0.3 269892 7444 ?
S 18:06 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41096 0.0 0.5 1458812 10852 ?
Sl 18:06 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41097 0.0 0.5 1327684 11272 ?
Sl 18:06 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41098 0.0 0.6 1327684 13348 ?
Sl 18:06 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42107 0.0 0.5 1327684 11504 ?
Sl 18:08 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 asmaslo+ 42858 0.0 0.3 29
2060 7928 pts/0 T 18:21 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 asmaslo+ 42925 0.0 0.0 22
2012 1112 pts/0 R+ 18:24 0:00 grep --color=auto httpd
```

Выполнение команды `ps auxZ | grep httpd`

4. С помощью команды `sestatus -bigrep httpd` я посмотрела текущее состояние переключателей SELinux для Apache (рис. [??], [??]). Многие переключатели находятся в положении «off».

```
[asmaslova@asmaslova ~]$ 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_redis 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
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
```

Выполнение команды `sestatus -bigrep httpd`

```
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_redis 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
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
[asmaslova@asmaslova ~]$ =
```

Выполнение команды `sestatus -bigrep httpd`

5. С помощью команды `seinfo` я посмотрела статистику по политике, а также определила множество пользователей, ролей, типов (рис. [??]).

```
[asmaslova@asmaslova ~]$ 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:            5015     Attributes:         258
Users:            8        Roles:              15
Booleans:         349     Cond. Expr.:       399
Allow:            116257   Neverallow:         0
Auditallow:       172     Dontaudit:          10529
Type_trans:       262670  Type_change:        94
Type_member:       37     Range_trans:        5989
Role_allow:        40     Role_trans:         421
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:              34
Genfscon:          107    Portcon:             649
Netifcon:          0      Nodecon:             0
[asmaslova@asmaslova ~]$
```

Выполнение команды *seinfo*

6. С помощью команды `ls -lZ /var/www` я посмотрела тип файлов и поддиректорий, находящихся в директории `/var/www` (рис. [??]).

```
[asmaslova@asmaslova ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system u:object_r:httpd_sys_script_exec_t:s0 6 Aug 12 04:14 cgi-bin
drwxr-xr-x. 2 root root system u:object_r:httpd_sys_content_t:s0 6 Aug 12 04:14 html
[asmaslova@asmaslova ~]$
```

Выполнение команды `ls -lZ /var/www`

7. С помощью команды `ls -lZ /var/www/html` я посмотрела тип файлов, находящихся в директории `/var/www/html` (рис. [??]).

```
[asmaslova@asmaslova ~]$ ls -lZ /var/www/html
total 0
```

Выполнение команды `ls -lZ /var/www/html`

8. По выводу команды `ls -lZ /var/www` я определила круг пользователей, которым разрешено создание файлов в директории `/var/www/html` (рис. [??]).
9. От имени суперпользователя я создала html-файл `/var/www/html/test.html` следующего содержания (рис. [??]):

```
<html>
<body>test</body>
</html>
```

```
[asmaslova@asmaslova ~]$ su -
Password:
[root@asmaslova ~]# cat > /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@asmaslova ~]#
```

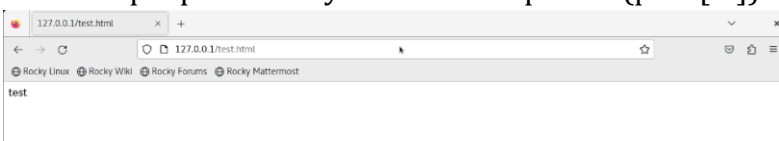
Создание html-файл /var/www/html/test.html

10. С помощью команды `ls -lZ /var/www/html/test.html` я проверила контекст созданного мною файла (рис. [??]).

```
[asmaslova@asmaslova ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 11 18:32 test.html
[asmaslova@asmaslova ~]$
```

Проверка контекста созданного мною файла

11. Введя в браузере адрес `http://127.0.0.1/test.html`, я обратилась к файлу через веб-сервер. Он был успешно отображен (рис. [??]).



Обращение к файлу через веб-сервер

12. Я попыталась изучить справку `man httpd_selinux` и выяснить, какие контексты файлов определены для `httpd`, но у меня отсутствует эта справка по неизвестным причинам, поэтому я просто решила еще раз проверить контекст файла командой `ls -Z /var/www/html/test.html` (рис. [??]).

```
[asmaslova@asmaslova ~]$ man httpd_selinux
No manual entry for httpd_selinux
[asmaslova@asmaslova ~]$ ls -Z /var/www/html
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[asmaslova@asmaslova ~]$
```

Проверка контекста файла test.html

13. После я изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` с помощью команд:

```
chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
```

После этого я проверила, что контекст поменялся (рис. [??]).

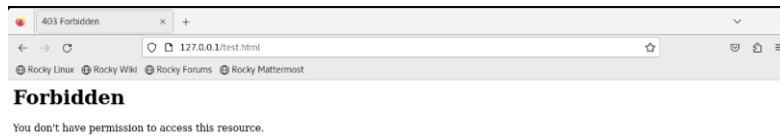
```
[asmaslova@asmaslova ~]$ su -
Password:
[root@asmaslova ~]# chcon -t samba_share_t /var/www/html/test.html
[root@asmaslova ~]# exit
logout
[asmaslova@asmaslova ~]$ ls -Z /var/www/html
unconfined_u:object_r:samba_share_t:s0 test.html
[asmaslova@asmaslova ~]$
```

Изменение контекста файла test.html

14. Введя в браузере адрес `http://127.0.0.1/test.html`, я ещё раз попробовала получить доступ к файлу через веб-сервер и получила сообщение об ошибке (рис. [??]):

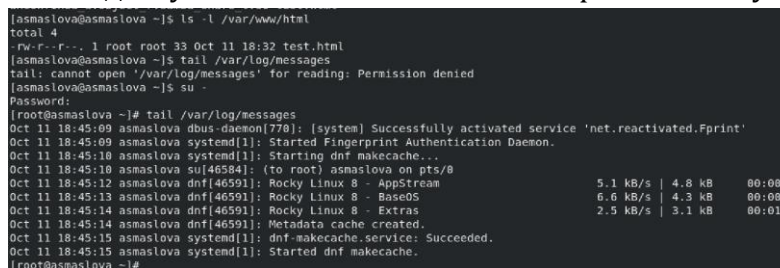
Forbidden

You don't have permission to access /test.html on this server.



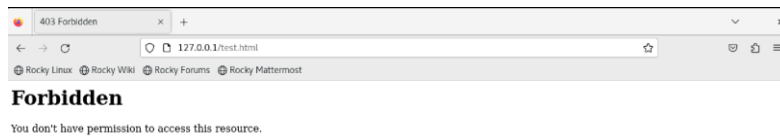
Доступ к файлу через веб-сервер

15. Я просмотрела системный лог-файл с помощью команды `tail /var/log/messages`, чтобы понять, почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю (рис. [??]).



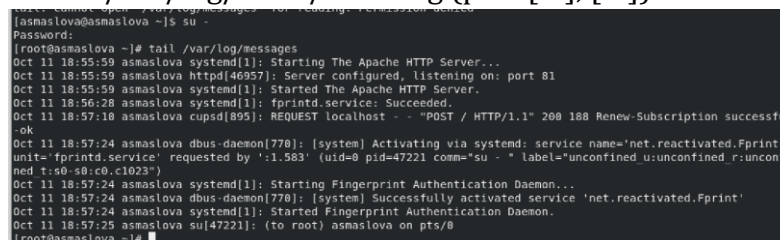
Просмотр системного лог-файла

16. Я 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` я нашла строчку `Listen 80` и заменила её на `Listen 81`.
17. Я выполнила перезапуск веб-сервера Apache, но произошел сбой (рис. [??])



Перезапуск веб-сервера Apache

18. Я проанализировала лог-файлы командой `tail -n1 /var/log/messages`, просмотрела файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` (рис. [??], [??]).



Выполнение команды `tail -n1 /var/Log/messages`

```
[root@asmaslova ~]# cat /var/log/httpd/access_log
127.0.0.1 - - [11/Oct/2024:18:08:49 -0400] "GET / HTTP/1.1" 403 7620 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:08:50 -0400] "GET /poweredby.png HTTP/1.1" 200 5714 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:08:50 -0400] "GET /icons/poweredby.png HTTP/1.1" 200 15443 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:08:50 -0400] "GET /favicon.ico HTTP/1.1" 404 196 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:35:23 -0400] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:35:24 -0400] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:43:41 -0400] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [11/Oct/2024:18:54:16 -0400] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

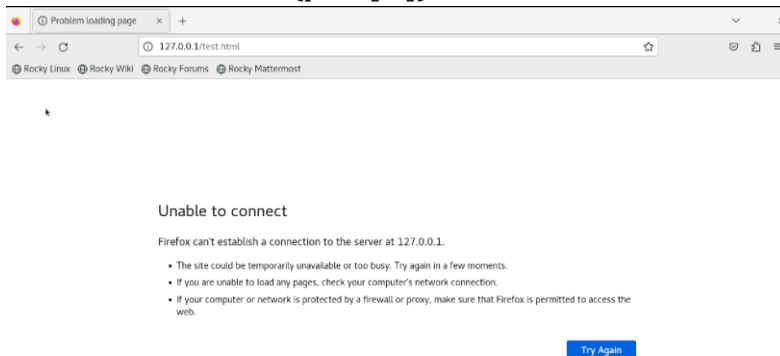
Просмотр файла /var/log/httpd/access_log

19. Я выполнила команду `semanage port -a -t http_port_t -p tcp 81`, после чего проверила список портов командой `semanage port -l | grep http_port_t` (рис. [??]).

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

Выполнение команды `semanage port -a -t http_port_t -p tcp 81` и проверка списка портов

20. Я попробовала запустить веб-сервер Apache ещё раз, но он как в прошлый раз не работал, так и сейчас не работает, просто теперь с другим системным сообщением (рис. [??]).



Запуск веб-сервера Apache

21. Я 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` (рис. [??]). После этого я попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`, и увидела содержимое файла — слово «test» (рис. [??]).

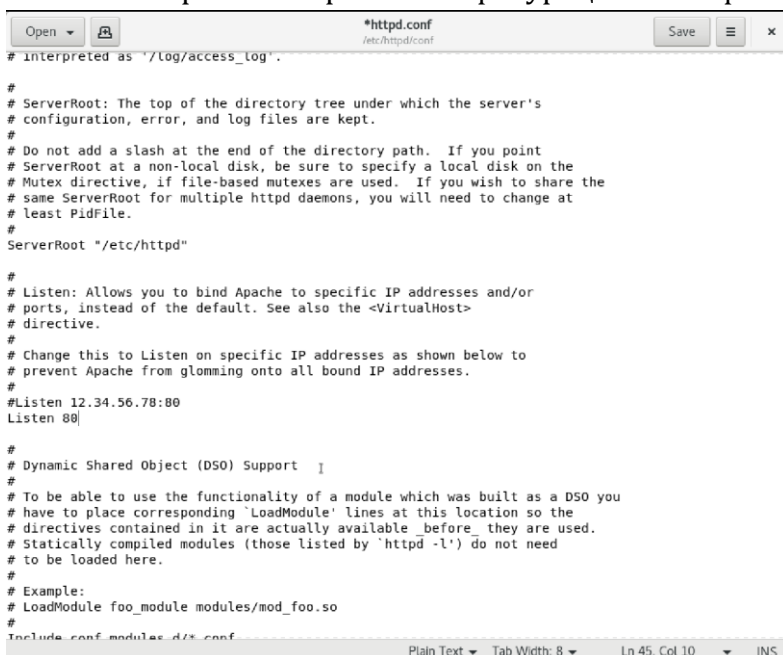
```
[root@asmaslova ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@asmaslova ~]#
```

Возвращение контекста `httpd_sys_content_t` к файлу `/var/www/html/test.html`



Получение доступа к файлу через веб-сервер

22. Я исправила обратно конфигурационный файл apache, вернув Listen 80 (рис. [??]).



```
# Interpreted as '/log/access_log'.

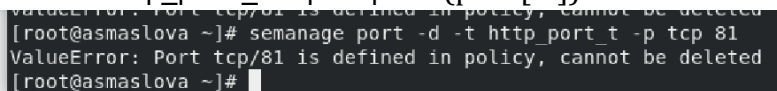
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# 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 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/* conf
```

Исправление конфигурационного файла apache

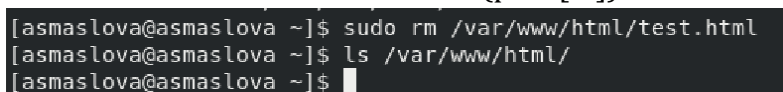
23. Я удалила привязку http_port_t к 81 порту командой semanage port -d -t http_port_t -p tcp 81 (рис. [??]).



```
[root@asmaslova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@asmaslova ~]#
```

Удаление привязки http_port_t к 81 порту

24. В конце я удалила файл /var/www/html/test.html командой rm /var/www/html/test.html (рис. [??]).



```
[asmaslova@asmaslova ~]$ sudo rm /var/www/html/test.html
[asmaslova@asmaslova ~]$ ls /var/www/html/
[asmaslova@asmaslova ~]$
```

Удаление файла /var/www/html/test.html

3 Вывод

В ходе лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux1 и проверила работу SELinx на практике совместно с веб-сервером Apache.

Список литературы