

Лабораторная работа №6

Мандатное разграничение прав в Linux

Тасыбаева Наталья Сергеевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	13
4	Список используемой литературы	14

Список иллюстраций

2.1	Запуск сервера	6
2.2	Параметр ServerName	6
2.3	Команды getenforce и sestatus. Запуск apache	7
2.4	Контекст безопасности и Состояние переключателей SELinux . . .	8
2.5	Статистика по политике	9
2.6	Типы файлов и поддиректории	10
2.7	Запуск в браузере	10
2.8	Изменение контекста безопасности	10
2.9	Запуск в браузере с ошибкой	11
2.10	Лог файлы	11
2.11	Настройки	11
2.12	Запуск в браузере	12
2.13	Открытие файла	12

Список таблиц

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 Выполнение лабораторной работы

1. Установила веб-сервис apache для дальнейшей работы (рис. 2.1).

```
Installed:
  apr-1.7.0-11.el9.x86_64
  apr-util-1.6.1-20.el9_2.1.x86_64
  apr-util-bdb-1.6.1-20.el9_2.1.x86_64
  apr-util-openssl-1.6.1-20.el9_2.1.x86_64
  httpd-2.4.53-11.el9_2.5.x86_64
  httpd-core-2.4.53-11.el9_2.5.x86_64
  httpd-filesystem-2.4.53-11.el9_2.5.noarch
  httpd-tools-2.4.53-11.el9_2.5.x86_64
  mod_http2-1.15.19-4.el9_2.4.x86_64
  mod_lua-2.4.53-11.el9_2.5.x86_64
  rocky-logos-httpd-90.14-1.el9.noarch

Complete!
[nstasihbaeva@nstasihbaeva ~]$ cat etc/httpd/httpd.conf
```

Рис. 2.1: Запуск сервера

2. В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName (рис. 2.2).

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru
```

Рис. 2.2: Параметр ServerName

3. Вошла в систему с полученными учётными данными и убедилась, что

SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Запустила веб-сервис (рис. 2.3).

```
[nstashbaeva@nstashbaeva ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
○ httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: man:httpd.service(8)
[nstashbaeva@nstashbaeva ~]$ getenforce
Enforcing
[nstashbaeva@nstashbaeva ~]$ 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
[nstashbaeva@nstashbaeva ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[nstashbaeva@nstashbaeva ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2023-10-14 15:37:49 MSK; 13s ago
   Docs: man:httpd.service(8)
  Main PID: 42349 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 213 (limit: 12224)
    Memory: 23.3M
       CPU: 447ms
    CGroup: /system.slice/httpd.service
            └─42349 /usr/sbin/httpd -DFOREGROUND
              └─42357 /usr/sbin/httpd -DFOREGROUND
                └─42361 /usr/sbin/httpd -DFOREGROUND
                  └─42362 /usr/sbin/httpd -DFOREGROUND
                    └─42365 /usr/sbin/httpd -DFOREGROUND

Oct 14 15:37:48 nstashbaeva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 15:37:49 nstashbaeva.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 15:37:49 nstashbaeva.localdomain httpd[42349]: Server configured, listening on: port 80
[nstashbaeva@nstashbaeva ~]$
```

Рис. 2.3: Команды `getenforce` и `sestatus`. Запуск `apache`

4. Определила его контекст безопасности. Посмотрела текущее состояние переключателей SELinux (рис. 2.4)

```
Oct 14 15:37:49 nstasihbaeva.localdomain httpd[42349]: server configured, listening on: port 80
[nstasihbaeva@nstasihbaeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 42349 0.1 0.5 20116 11328 ? Ss 15:37 0:00 /usr/sbin/httpd
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42357 0.0 0.3 21600 7244 ? S 15:37 0:00 /usr/sbin/httpd
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42361 0.0 0.6 1210508 12880 ? Sl 15:37 0:00 /usr/sbin/httpd
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42362 0.5 0.5 1079372 10832 ? Sl 15:37 0:00 /usr/sbin/httpd
httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42365 0.0 0.5 1079372 10832 ? Sl 15:37 0:00 /usr/sbin/httpd
httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 nstasih+ 42622 0.0 0.1 221664 2184 pts/0 S+ 15:38 0:0
0 grep --color=auto httpd
[nstasihbaeva@nstasihbaeva ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

-v Verbose check of process and file contexts.
-b Display current state of booleans.

Without options, show SELinux status.
[nstasihbaeva@nstasihbaeva ~]$ 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_avaahi off
httpd_dbus_sss 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_...
```

Рис. 2.4: Контекст безопасности и Состояние переключателей SELinux

5. Посмотрела статистику по политике с помощью команды seinfo (рис. 2.5)


```
* Installing packages...
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          135      Permissions:        457
Sensitivities:    1        Categories:         1024
Types:            5100     Attributes:         258
Users:            8        Roles:              14
Booleans:         353     Cond. Expr.:       384
Allow:            65000    Neverallow:         0
Auditallow:       170     Dontaudit:          8572
Type_trans:       265341   Type_change:        87
Type_member:      35       Range_trans:        6164
Role allow:       38       Role_trans:         420
Constraints:      70       Validatetrans:      0
MLS Constrain:    72       MLS Val. Tran:      0
Permissives:      2        Polcap:             6
Defaults:         7        Typebounds:         0
Allowxperm:       0        Neverallowxperm:    0
Auditallowxperm:  0        Dontauditxperm:     0
Ibendportcon:     0        Ibpkeycon:          0
Initial SIDs:     27       Fs_use:             35
Genfscon:         109     Portcon:            660
Netifcon:         0        Nodecon:            0

[nstasihbaeva@nstasihbaeva ~]$
```

Рис. 2.5: Статистика по политике

6. Определила тип файлов и поддиректорий, находящихся в директории /var/www, определила тип файлов, находящихся в директории /var/www/html, определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создала от имени супер-пользователя html-файл test.html. Проверила контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. Обратился к файлу через веб-сервер (рис. 2.6, 2.7)

```

[nstasihbaeva@nstasihbaeva ~]$ 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 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 23:21 html
[nstasihbaeva@nstasihbaeva ~]$ ls -lZ /var/www/html
total 0
[nstasihbaeva@nstasihbaeva ~]$ cd /var/www
[nstasihbaeva@nstasihbaeva www]$ cd html
[nstasihbaeva@nstasihbaeva html]$ ls -lZ
total 0
[nstasihbaeva@nstasihbaeva html]$ ls -l
total 0
[nstasihbaeva@nstasihbaeva html]$ cd ../
[nstasihbaeva@nstasihbaeva www]$ ls -l
total 0
drwxr-xr-x. 2 root root 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root 6 May 16 23:21 html
[nstasihbaeva@nstasihbaeva www]$ sudo -i
[sudo] password for nstasihbaeva:
[root@nstasihbaeva ~]# cd /var/www/html
[root@nstasihbaeva html]# touch test.html
[root@nstasihbaeva html]# vi test.html
[root@nstasihbaeva html]# cat test.html
<html>
<body>test</body>
</html>

[root@nstasihbaeva html]# ls -l
total 4
-rw-r--r--. 1 root root 34 Oct 14 15:49 test.html
[root@nstasihbaeva html]# ls -lZ
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 14 15:49 test.html
[root@nstasihbaeva html]#

```

Рис. 2.6: Типы файлов и поддиректории

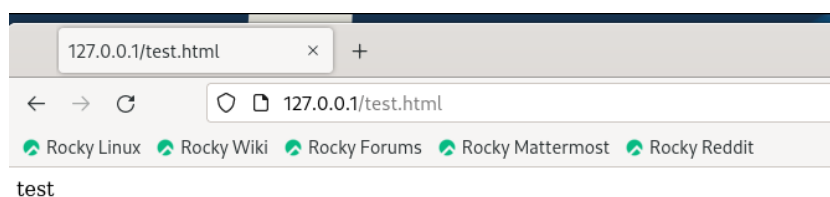


Рис. 2.7: Запуск в браузере

7. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, попробовала ещё раз получить доступ к файлу через веб-сервер (рис. 2.8, 2.9).

```

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

```

Рис. 2.8: Изменение контекста безопасности

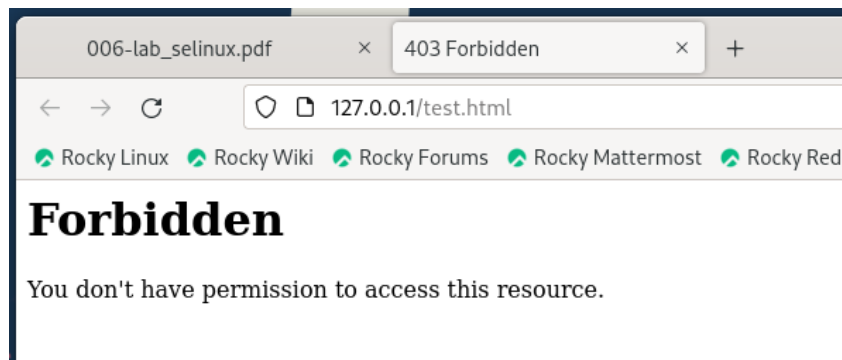


Рис. 2.9: Запуск в браузере с ошибкой

9. Просмотрела log-файлы веб-сервера Apache (рис. 2.10)

```
root@instashbaeva:~# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 34 Oct 14 15:49 /var/www/html/test.html
root@instashbaeva:~# cat /var/log/messages
Oct 14 16:18:28 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-507ms), your system is too slow
Oct 14 16:18:31 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2499ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-4271ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-4272ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-3217ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-3184ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2965ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2809ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2813ms), your system is too slow
Oct 14 16:18:32 instashbaeva gnome-shell[2656]: libinput error: client bug: timer event3 debounce: scheduled expiry is in the past (-2366ms), your system is too slow
root@instashbaeva:~# cd /etc/httpd/conf/
root@instashbaeva:~# vi httpd.conf
root@instashbaeva:~# cat httpd.conf
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information.
# In particular, see http://httpd.apache.org/docs/2.4/mod/mod\_ssl.html.
```

Рис. 2.10: Лог файлы

10. Открыл файл через 81 порт (рис. 2.11, ??, ??)

```
root@instashbaeva:~# cd httpd
root@instashbaeva:~# ls
error_log
root@instashbaeva:~# cat error_log
[Sat Oct 14 15:17:48.958000 2023] [core:notice] [pid 42340:tid 42340] SELinux policy enabled: httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 15:17:48.958000 2023] [suexec:notice] [pid 42340:tid 42340] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 14 15:17:49.934000 2023] [lbmethod:heartbeat:notice] [pid 42340:tid 42340] AH02282: No slotmem from mod_heartbeat
[Sat Oct 14 15:17:49.934000 2023] [mpm_event:notice] [pid 42340:tid 42340] AH00489: Apache/2.4.54 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 14 15:17:49.934000 2023] [core:notice] [pid 42340:tid 42340] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 14 15:17:49.934000 2023] [core:error] [pid 42340:tid 42340] (13)Permission denied: client 127.0.0.1:57952 AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because it is not a component of the path
[Sat Oct 14 15:18:04.121500 2023] [mpm_event:notice] [pid 42340:tid 42340] AH00492: caught SIGCHLD, shutting down gracefully
[Sat Oct 14 15:18:04.323000 2023] [core:notice] [pid 43872:tid 43872] SELinux policy enabled: httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 15:18:04.323000 2023] [suexec:notice] [pid 43872:tid 43872] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 14 15:18:04.323000 2023] [lbmethod:heartbeat:notice] [pid 43872:tid 43872] AH02282: No slotmem from mod_heartbeat
[Sat Oct 14 15:18:04.323000 2023] [mpm_event:notice] [pid 43872:tid 43872] AH00489: Apache/2.4.54 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 14 15:18:04.323000 2023] [core:notice] [pid 43872:tid 43872] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
root@instashbaeva:~# cat access_log
127.0.0.1 - [14/Oct/2023:15:18:37 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - [14/Oct/2023:15:18:37 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
root@instashbaeva:~# semanage port -a -t http_port_t -p 81
semanage: error: unrecognized arguments: -p 81
root@instashbaeva:~# semanage port -a | grep http_port_t
tcp      80, 81, 443, 488, 8089, 8009, 8443, 9000
root@instashbaeva:~# systemctl restart httpd.service
Redirecting to /bin/systemctl restart httpd.service
root@instashbaeva:~# systemctl status httpd.service
Redirecting to /bin/systemctl status httpd.service
httpd.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
Active: active (running) since Sat 2023-10-14 15:18:21 MSK; 11s ago
Docs: man:httpd.service(8)
Main PID: 43872 (httpd)
Status: 'Total requests: 0 | Idle/Busy workers 180/0|Requests/sec: 0 |Bytes served/sec: 0 B/sec'
```

Рис. 2.11: Настройки

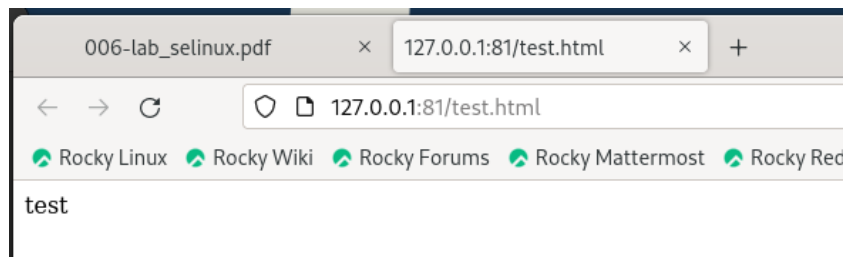


Рис. 2.12: Запуск в браузере

```
Oct 14 16:36:17 nstasihbaeva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 16:36:17 nstasihbaeva.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 16:36:17 nstasihbaeva.localdomain httpd[44186]: Server configured, listening on: port 81
[root@nstasihbaeva httpd]# cd
[root@nstasihbaeva ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@nstasihbaeva ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@nstasihbaeva ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 14 15:49 /var/www/html/test.html
[root@nstasihbaeva ~]# cd /etc/httpd/conf/
[root@nstasihbaeva conf]# vi httpd.conf
[root@nstasihbaeva conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@nstasihbaeva conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@nstasihbaeva conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@nstasihbaeva conf]# 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@nstasihbaeva conf]# cd
[root@nstasihbaeva ~]# cd /var/www/html
[root@nstasihbaeva html]# rm test.html
rm: remove regular file 'test.html'? y
[root@nstasihbaeva html]# ls
[root@nstasihbaeva html]#
```

Рис. 2.13: Открытие файла

3 Выводы

Я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux, а также проверила работу SELinux на практике совместно с веб-сервером Apache.

4 Список используемой литературы