

Лабораторная работа №6

Мандатное разграничение прав в Linux

Липатникова М.С. группа НФИбд-02-19

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	14
4	Список литературы	15

List of Figures

2.1	Проверка SELinux	6
2.2	Список процессов: веб-сервер Apache	6
2.3	Переключатели для Apache	8
2.4	Статистика по политике	9
2.5	Работа в директории /var/www/html	10
2.6	Изменение контекста	11
2.7	Файл ошибок	11
2.8	Замена 80-81	12
2.9	Перезапуск сервера	12
2.10	Перезапуск сервера	12
2.11	Перезапуск сервера - работает	13
2.12	Замена 81-80	13
2.13	Удаление	13

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 Выполнение лабораторной работы

Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд: `getenforce` и `sestatus`. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: `service httpd status` (fig. 2.1).

```

[root@mslipatnikova ~]# getenforce
Enforcing
[root@mslipatnikova ~]# 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
[root@mslipatnikova ~]# 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 pre
   Active: active (running) since Wed 2022-10-12 16:09:22 MSK; 5min ago
     Docs: man:httpd.service(8)
   Main PID: 40376 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
      Tasks: 213 (limit: 12214)
     Memory: 23.1M
        CPU: 204ms
    CGroup: /system.slice/httpd.service
            └─40376 /usr/sbin/httpd -DFOREGROUND
              └─40377 /usr/sbin/httpd -DFOREGROUND
                └─40378 /usr/sbin/httpd -DFOREGROUND
                  └─40379 /usr/sbin/httpd -DFOREGROUND
                    └─40380 /usr/sbin/httpd -DFOREGROUND

Oct 12 16:09:22 mslipatnikova.localdomain systemd[1]: Starting The Apache HTTP
Oct 12 16:09:22 mslipatnikova.localdomain systemd[1]: Started The Apache HTTP S
Oct 12 16:09:22 mslipatnikova.localdomain httpd[40376]: Server configured, list
[root@mslipatnikova ~]#

```

Figure 2.1: Проверка SELinux

Нашла веб-сервер Apache в списке процессов, его контекст безопасности: httpd_t (ps -eZ | grep httpd)(fig. 2.2).

```

[root@mslipatnikova ~]# ps -eZ |grep httpd
system_u:system_r:httpd_t:s0      40376 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      40377 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      40378 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      40379 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      40380 ?        00:00:00 httpd

```

Figure 2.2: Список процессов: веб-сервер Apache

Посмотрела текущее состояние переключателей SELinux для Apache с

помощью команды: `sestatus -b | grep httpd`. Обратила внимание, что многие из них находятся в положении «off»(fig. 2.3).

```
[root@mslipatnikova ~]# 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 2.3: Переключатели для Apache

Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей (8), ролей (14), типов (5002) (fig. 2.4).

```
Installing packages...
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 Constrains:	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

Figure 2.4: Статистика по политике

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: `ls -lZ /var/www/html`. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html (root). Создала от имени суперпользователя html-файл - /var/www/html/test.html, чтобы на странице выводилось слово test. Проверила контекст созданного мной файла (httpd_sys_content_t). Обратилась к файлу

через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедилась, что файл был успешно отображён (fig. 2.5).

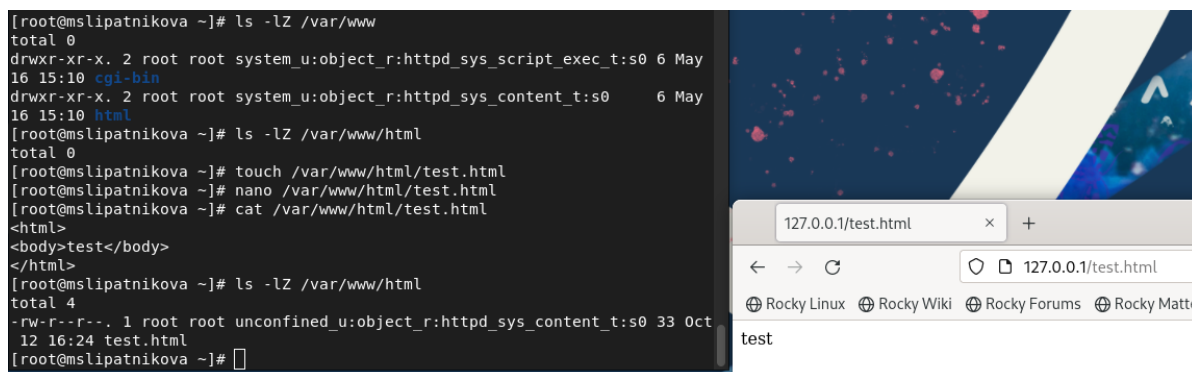


Figure 2.5: Работа в директории `/var/www/html`

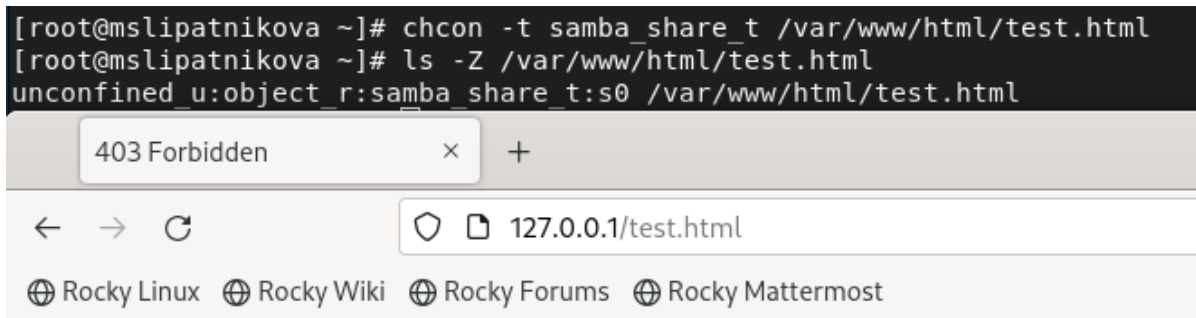
Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd`. Совпадают с типом файла `test.html`. Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на (к которому процесс `httpd` не должен иметь доступа) `samba_share_t`:

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

```
ls -Z /var/www/html/test.html
```

Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получила сообщение об ошибке: `Forbidden. You don't have permission to access /test.html on this server` (fig. 2.6).



Forbidden

You don't have permission to access this resource.

Figure 2.6: Изменение контекста

Файл не был отображён, хотя права доступа позволяют читать этот файл любому пользователю: `ls -l /var/www/html/test.html`. Это произошло, т.к. мы изменили контекст к которому процесс `httpd` не должен иметь доступа. Просмотрела `log`-файлы веб-сервера `Apache`. Также просмотрела системный `log`-файл: `tail /var/log/messages` (fig. 2.7).

```
[root@mslipatnikova ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct 12 16:24 /var/www/html/test.html
[root@mslipatnikova ~]# tail /var/log/messages
Oct 12 16:28:17 mslipatnikova systemd[1]: Started dbus-:1.10-org.fedoraproject.SetroubleshootPrivile
Oct 12 16:28:18 mslipatnikova setroubleshoot[41136]: SELinux is preventing /usr/sbin/httpd from geta
/var/www/html/test.html. For complete SELinux messages run: sealert -l 1150dbea-bae7-42dd-a52a-1771
Oct 12 16:28:18 mslipatnikova setroubleshoot[41136]: SELinux is preventing /usr/sbin/httpd from geta
/var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****
you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content t.#
```

Figure 2.7: Файл ошибок

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. 2.8). Выполнила перезапуск веб-сервера `Apache`. Сбоя не произошло. Проанализировала `log`-файлы: `tail -nl /var/log/messages` (fig. 2.9).

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

Figure 2.8: Замена 80-81

```
[root@mslipatnikova ~]# nano /etc/httpd/conf/httpd.conf
[root@mslipatnikova ~]# systemctl restart httpd
[root@mslipatnikova ~]# tail -n1 /var/log/messages
Oct 12 16:40:14 mslipatnikova httpd[41320]: Server configured, listening on: port 81
```

Figure 2.9: Перезапуск сервера

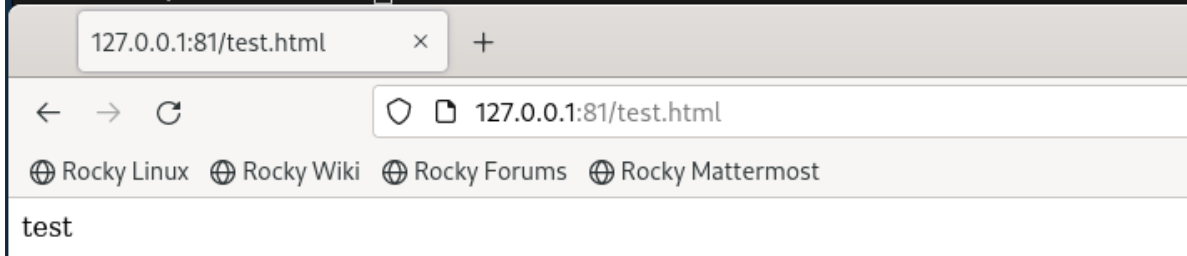
Выполнила команду: `semanage port -a -t http_port_t -p tcp 81` (уже существует). После этого проверьте список портов командой: `semanage port -l | grep http_port_t` Порт 81 есть в списке. Попробовала запустить веб-сервер Apache ещё раз. Сбоя также нет (fig. 2.10).

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

Figure 2.10: Перезапуск сервера

Вернула 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 попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Можно увидеть содержимое файла — слово «test» (fig. 2.11).

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



The screenshot shows a web browser window with a single tab titled '127.0.0.1:81/test.html'. The address bar shows '127.0.0.1:81/test.html'. Below the address bar, there are links for 'Rocky Linux', 'Rocky Wiki', 'Rocky Forums', and 'Rocky Mattermost'. The main content area of the browser displays the word 'test'.

Figure 2.11: Перезапуск сервера - работает

Исправила обратно конфигурационный файл apache, вернув Listen 80(fig. 2.12).

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80
```

Figure 2.12: Замена 81-80

Удалить привязку http_port_t к 81 порту (semanage port -d -t http_port_t -p tcp 81) не получилось, не позволяет. Удалила файл /var/www/html/test.html: rm /var/www/html/test.html(fig. 2.13).

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

Figure 2.13: Удаление

3 Вывод

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.

4 Список литературы

1. Теоретические материалы курса.