

Лабораторная работа № 6. Мандаторное разграничение прав в Linux.

Лёшьен Стефани, НФИбд-02-19

Содержание

1	Цель работы	5
2	Последовательность выполнения работы	6
3	Выводы	12
4	Библиография	13

List of Figures

2.1	Установка веб-сервер Apache	6
2.2	Отключили пакетный фильтр	7
2.3	service httpd start	8
2.4	Нашли веб-сервер Apache в списке процессов	8
2.5	Многие переключателей находятся в положении «off»	9
2.6	Создали от имени суперпользователя html-файл	9
2.7	html-файл test.html	10
2.8	html-файл в веб-сервер	10
2.9	Изменили контекст файла на samba_share_t	11
2.10	Проверили список портов	11
2.11	Удалили файл /var/www/html/test.html	11

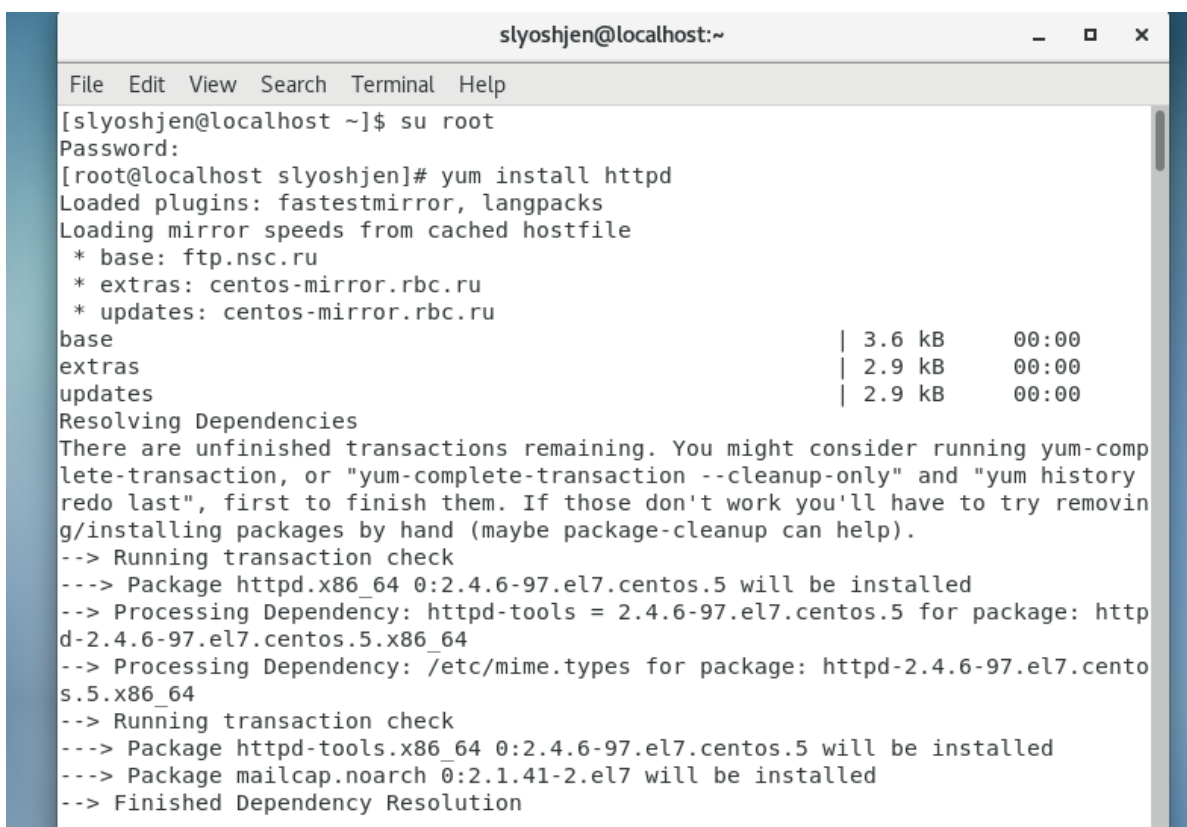
List of Tables

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 Последовательность выполнения работы

1. От имени пользователя root установили веб-сервер Apache с помощью команды `yum install httpd`.



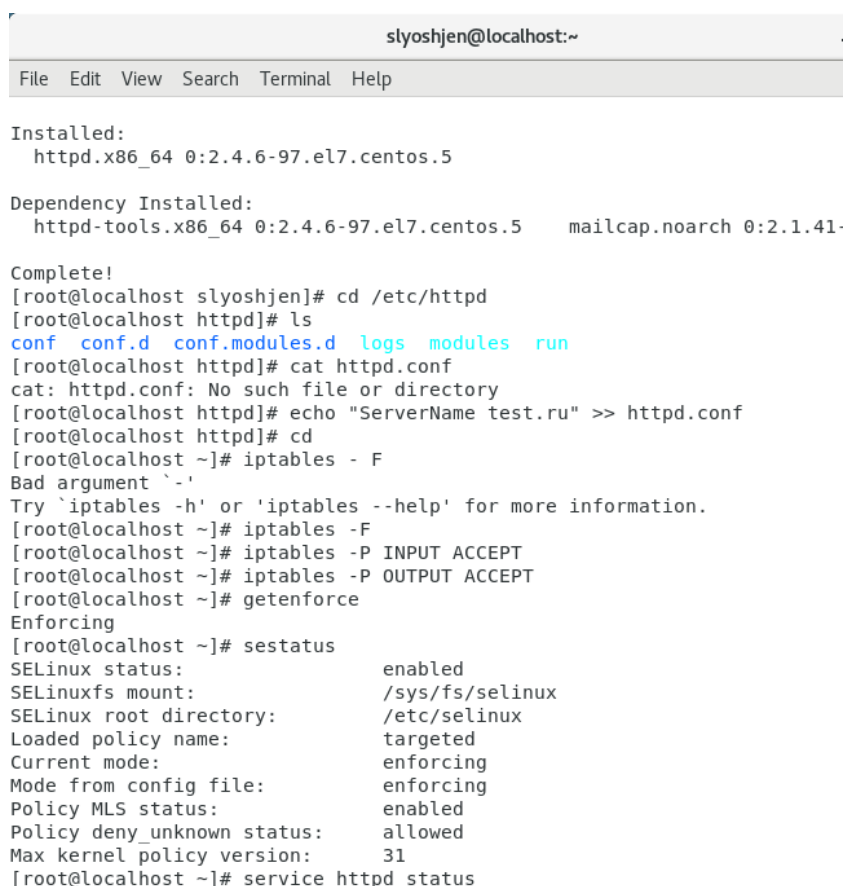
```
slyoshjen@localhost:~  
File Edit View Search Terminal Help  
[slyoshjen@localhost ~]$ su root  
Password:  
[root@localhost slyoshjen]# yum install httpd  
Loaded plugins: fastestmirror, langpacks  
Loading mirror speeds from cached hostfile  
* base: ftp.nsc.ru  
* extras: centos-mirror.rbc.ru  
* updates: centos-mirror.rbc.ru  
base | 3.6 kB 00:00  
extras | 2.9 kB 00:00  
updates | 2.9 kB 00:00  
Resolving Dependencies  
There are unfinished transactions remaining. You might consider running yum-complete-transaction, or "yum-complete-transaction --cleanup-only" and "yum history redo last", first to finish them. If those don't work you'll have to try removing/installing packages by hand (maybe package-cleanup can help).  
--> Running transaction check  
---> Package httpd.x86_64 0:2.4.6-97.el7.centos.5 will be installed  
--> Processing Dependency: httpd-tools = 2.4.6-97.el7.centos.5 for package: httpd-2.4.6-97.el7.centos.5.x86_64  
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.6-97.el7.centos.5.x86_64  
--> Running transaction check  
---> Package httpd-tools.x86_64 0:2.4.6-97.el7.centos.5 will be installed  
---> Package mailcap.noarch 0:2.1.41-2.el7 will be installed  
--> Finished Dependency Resolution
```

Figure 2.1: Установка веб-сервер Apache

2. В конфигурационном файле `/etc/httpd/httpd.conf` задали параметр `ServerName`: `ServerName test.ru` Для чтобы при запуске веб-сервера не

выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе. Также отключили пакетный фильтр командами : `iptables -F`
`iptables -P INPUT ACCEPT` `iptables -P OUTPUT ACCEPT`

Убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.



```
slyoshjen@localhost:~  
File Edit View Search Terminal Help  
  
Installed:  
  httpd.x86_64 0:2.4.6-97.el7.centos.5  
  
Dependency Installed:  
  httpd-tools.x86_64 0:2.4.6-97.el7.centos.5  mailcap.noarch 0:2.1.41-  
  
Complete!  
[root@localhost slyoshjen]# cd /etc/httpd  
[root@localhost httpd]# ls  
conf  conf.d  conf.modules.d  logs  modules  run  
[root@localhost httpd]# cat httpd.conf  
cat: httpd.conf: No such file or directory  
[root@localhost httpd]# echo "ServerName test.ru" >> httpd.conf  
[root@localhost httpd]# cd  
[root@localhost ~]# iptables - F  
Bad argument '-'  
Try 'iptables -h' or 'iptables --help' for more information.  
[root@localhost ~]# iptables -F  
[root@localhost ~]# iptables -P INPUT ACCEPT  
[root@localhost ~]# iptables -P OUTPUT ACCEPT  
[root@localhost ~]# getenforce  
Enforcing  
[root@localhost ~]# 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@localhost ~]# service httpd status
```

Figure 2.2: Отключили пакетный фильтр

3. Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает: `service httpd start`

```
[root@localhost ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
  Docs: man:httpd(8)
        man:apachectl(8)
[root@localhost ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
  Active: active (running) since Sat 2022-10-15 14:37:54 EDT; 46s ago
  Docs: man:httpd(8)
        man:apachectl(8)
Main PID: 9209 (httpd)
Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
Tasks: 6
CGroup: /system.slice/httpd.service
├─9209 /usr/sbin/httpd -DFOREGROUND
├─9212 /usr/sbin/httpd -DFOREGROUND
├─9213 /usr/sbin/httpd -DFOREGROUND
├─9214 /usr/sbin/httpd -DFOREGROUND
├─9215 /usr/sbin/httpd -DFOREGROUND
└─9216 /usr/sbin/httpd -DFOREGROUND

Oct 15 14:37:54 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 15 14:37:54 localhost.localdomain httpd[9209]: AH00558: httpd: Could not reliably determi...ge
Oct 15 14:37:54 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]#
```

Figure 2.3: service httpd start

4. Нашли веб-сервер Apache в списке процессов : `ps auxZ | grep httpd` или `ps -eZ | grep httpd`. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Многие переключателей находятся в положении «off»

```
[root@localhost ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 9209 0.0 0.4 224084 5032 ? Ss 14:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9212 0.0 0.3 226168 3104 ? S 14:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9213 0.0 0.3 226168 3104 ? S 14:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9214 0.0 0.3 226168 3104 ? S 14:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9215 0.0 0.3 226168 3104 ? S 14:37 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 9216 0.0 0.3 226168 3104 ? S 14:37 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 9322 0.0 0.0 112812 980 pts/0 R+ 14:42 0:00 grep --color=auto httpd

[root@localhost ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 9209 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 9212 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 9213 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 9214 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 9215 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 9216 ? 00:00:00 httpd
[root@localhost ~]# 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.
```

Figure 2.4: Нашли веб-сервер Apache в списке процессов


```
slyoshjen@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# 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_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 on  
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
```

Figure 2.5: Многие переключателей находятся в положении «off»

5. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` и определили тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

test

```
slyoshjen@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# ls -lZ /var/www  
lrwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin  
lrwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html  
[root@localhost ~]# ls -lZ /var/www/html  
[root@localhost ~]# echo "<html>\n <body>test</body>\n </html>"> /var/www/html/test.html  
[root@localhost ~]# cat /var/www/html/test.html  
<html>\n <body>test</body>\n </html>  
[root@localhost ~]# gedit /var/www/html/test.html
```

Figure 2.6: Создали от имени суперпользователя html-файл

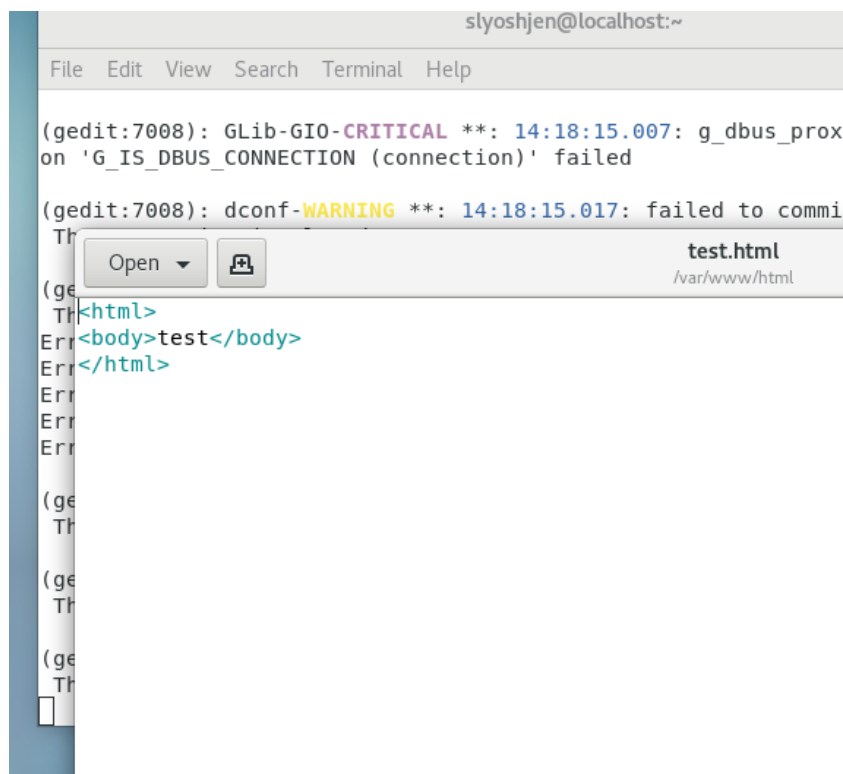


Figure 2.7: html-файл test.html

6. Обратились к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.
Файл успешно отображён.

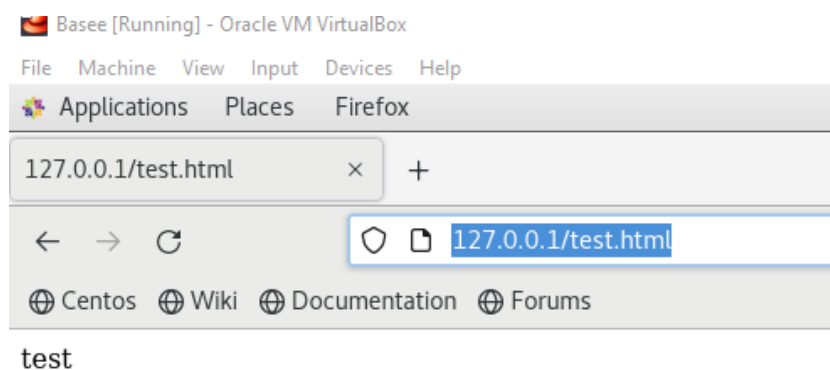


Figure 2.8: html-файл в веб-сервер

7. Проверили контекст файла можно командой `ls -Z`. Изменили контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которо-

му процесс httpd не должен иметь доступа, например, на samba_share_t.

```
[root@localhost ~]# ls -Z /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@localhost ~]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost ~]# ls -Z /var/www/html/test.html
-rw-r--r-- root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost ~]#
```

Figure 2.9: Изменили контекст файла на samba_share_t

8. Попробовали ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Мы получили сообщение об ошибке.
9. Просмотрели системный лог-файл `tail /var/log/messages` и выполнили команду : `semanage port -a -t http_port_t -p tcp 81` После этого проверили список портов командой: `semanage port -l | grep http_port_t` Порт 81 появился в списке.

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

Figure 2.10: Проверили список портов

10. Вернули контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. После этого мы получили доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Мы увидели содержимое файла — слово «test».
11. Удалили привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверили, что порт 81 удалён. Удалили файл `/var/www/html/test.html`

```
[root@localhost ~]# semanage port -d -t http_port_t -p tcp 81
usage: semanage port [-h] [-n] [-N] [-S STORE] [ --add -t TYPE -p PROTOCOL -r RANGE ( port_name | port_range ) ] --delete -p PROTOCOL ( port_name | port_range ) | --deleteall | --extract | --list -C | --modify -t TYPE -p PROTOCOL -r RANGE ( port_name | port_range ) ]
semanage port: error: argument -t/--type: expected one argument
[root@localhost ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@localhost ~]#
```

Figure 2.11: Удалили файл `/var/www/html/test.html`

3 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux¹. Проверили работу SELinx на практике совместно с веб-сервером Apache.

4 Библиография

1. Методические материалы курса