

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Косолапов Степан Эдуардович НПИбд-01-20

Содержание

| | | |
|----------|--------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Выполнение работы | 6 |
| 3 | Выводы | 15 |

Список иллюстраций

| | | |
|----------|--|----|
| figno:1 | getenforce и sestatus | 6 |
| figno:2 | Главная страница apache | 7 |
| figno:3 | Контекст безопасности процессов httpd | 7 |
| figno:4 | Переключатели selinux для httpd | 8 |
| figno:5 | Статистика по политике | 9 |
| figno:6 | Данные о содержимом /var/www/ | 9 |
| figno:7 | test.html | 10 |
| figno:8 | Контекст test.html | 10 |
| figno:9 | test.html в браузере | 10 |
| figno:10 | Меню контекста | 11 |
| figno:11 | Ошибка при попытке доступа к файлу с другим контекстом | 11 |
| figno:12 | Системные логи | 12 |
| figno:13 | Логи apache | 12 |
| figno:14 | Настройка listen 81 | 12 |
| figno:15 | Запуск httpd с портом 81 | 13 |
| figno:16 | Системные логи при прослушивании 81 порта httpd | 13 |
| figno:17 | Повторение действий для порта 82 | 14 |
| figno:18 | Удаление test.html и порта 82 из http_port_t | 14 |

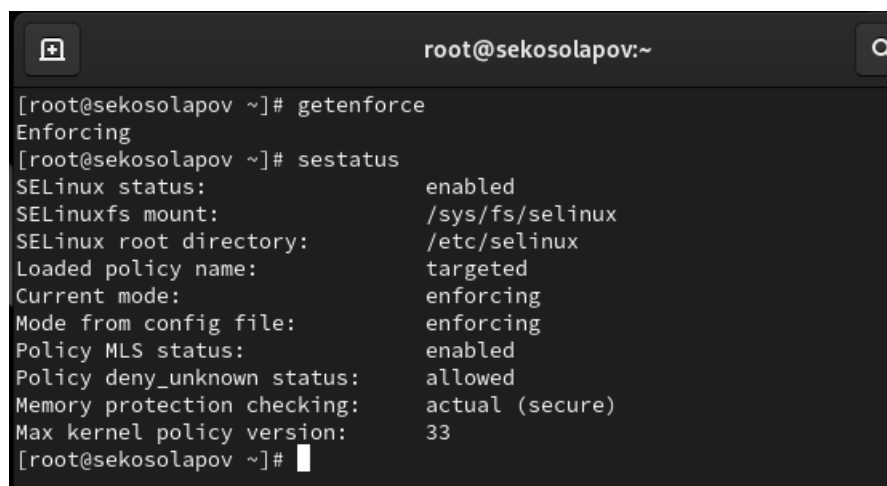
Список таблиц

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 работы

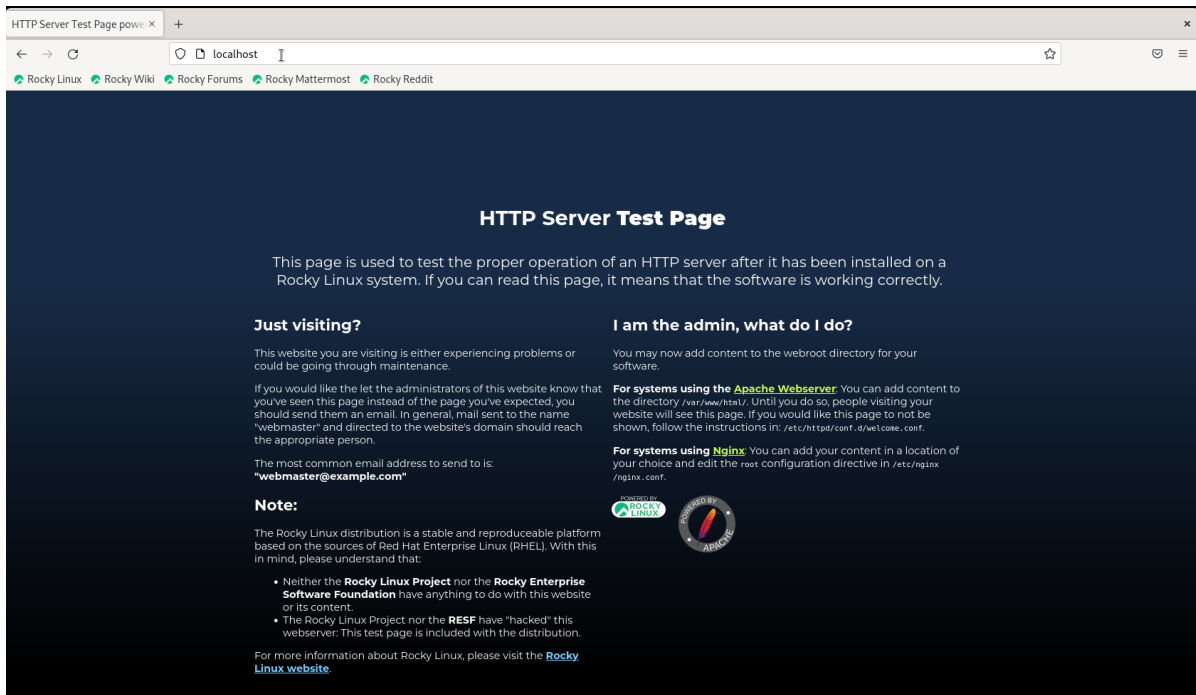
1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

A terminal window titled 'root@sekosolapov:~' with a search icon in the top right. The terminal shows the execution of 'getenforce' and 'sestatus' commands. 'getenforce' returns 'Enforcing'. 'sestatus' displays various SELinux configuration details.

```
[root@sekosolapov ~]# getenforce
Enforcing
[root@sekosolapov ~]# 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@sekosolapov ~]#
```

getenforce и sestatus

2. Обращаемся с помощью браузера к веб-серверу, запущенному на компьютере, и видим, что сервер работает



тестовая страница apache

- Находим веб-сервер Apache в списке процессов, определяем его контекст безопасности - `system_u:system_r:htpd_t:s0`

```

root@sekosolapov:~
[root@sekosolapov ~]# ps auxZ | grep httpd
system_u:system_r:htpd_t:s0 root      39952  0.0  0.1 20116 11604 ?        Ss   19:52   0:00 /usr/sbin/htpd -DFOREGROUND
system_u:system_r:htpd_t:s0 apache  39954  0.0  0.0 21600 7440 ?        S    19:52   0:00 /usr/sbin/htpd -DFOREGROUND
system_u:system_r:htpd_t:s0 apache  39955  0.3  0.2 2455692 23404 ?        Sl   19:52   0:00 /usr/sbin/htpd -DFOREGROUND
system_u:system_r:htpd_t:s0 apache  39956  0.2  0.2 2324556 17256 ?        Sl   19:52   0:00 /usr/sbin/htpd -DFOREGROUND
system_u:system_r:htpd_t:s0 apache  39957  0.2  0.2 2324556 17256 ?        Sl   19:52   0:00 /usr/sbin/htpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 root  40598  0.0  0.0 221796 2376 pts/0    S+   19:56   0:00 grep --color=auto httpd
[root@sekosolapov ~]#

```

контекст безопасности процессов httpd

- Смотрим текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`

```
root
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
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
```

переключатели selinux для httpd

5. Смотрим статистику по политике с помощью команды seinfo. Количество пользователей - 8, ролей - 14, типов - 5100.


```
root@sekosolapov:~  
[root@sekosolapov ~]# seinfo  
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: 65009 Neverallow: 0  
Auditallow: 170 Dontaudit: 8572  
Type_trans: 265337 Type_change: 87  
Type_member: 35 Range_trans: 6164  
Role allow: 38 Role_trans: 420  
Constraints: 70 Validatetrans: 0  
MLS Constrains: 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  
[root@sekosolapov ~]#
```

статистика по политике

6. Определяем тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` - это типы `httpd_sys_script_exec_t` для `cgi-bin` и `httpd_sys_content_t` для `html`
7. Файлов в директории /var/www/html пока что нет.
8. Определяем круг пользователей, которым разрешено создание файлов в директории /var/www/html с помощью той же команды `ls`, видим, что доступ на создание есть только у `root`.

```
[root@sekosolapov ~]# 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
```

данные о содержимом /var/www/

9. Создаём от имени суперпользователя html-файл /var/www/html/test.html

```
root@sekosolapov:~  
<html>  
  <body>  
    test  
  </body>  
</html>  
~
```

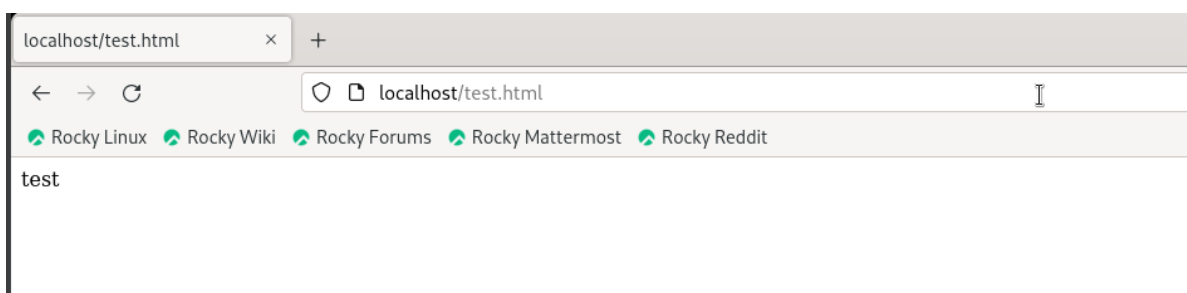
test.html

10. Проверяем контекст созданного нами файла - `unconfined_u:object_r:httpd_sys_content_t:s0` - это контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.

```
[root@sekosolapov ~]# vim /var/www/html/test.html  
[root@sekosolapov ~]# ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 38 Oct 14 20:02 test.html  
[root@sekosolapov ~]# ls --lcontext /var/www/html/  
ls: unrecognized option '--lcontext'  
Try 'ls --help' for more information.  
[root@sekosolapov ~]# ls -l --context /var/www/html/  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 38 Oct 14 20:02 test.html  
[root@sekosolapov ~]#
```

контекст test.html

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



test.html в браузере

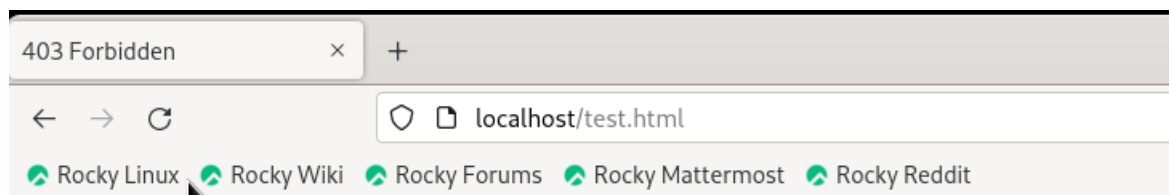
12. Изучить справку `man httpd_selinux` у нас не получилось, т.к такой справки не было обнаружено, поэтому обратились в интернет за этой справкой.

13. Изменяем контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html`

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

смена контекста

14. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Мы получаем сообщение об ошибке: `Forbidden` `You don't have permission to access this resource.`



Forbidden

You don't have permission to access this resource.

ошибка при попытке доступа к файлу с другим контекстом

15. В данной ситуации у сервиса `httpd` не было доступа до файла из-за изменённого контекста.

Смотрим логи и видим, что действительно не было доступа у самого процесса до файла `test.html`


```
[root@sekosolapov ~]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@sekosolapov ~]# 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)

Oct 14 20:22:42 sekosolapov.localdomain systemd[1]: Stopping The Apache HTTP Server...
Oct 14 20:22:43 sekosolapov.localdomain systemd[1]: httpd.service: Deactivated successfully.
Oct 14 20:22:43 sekosolapov.localdomain systemd[1]: Stopped The Apache HTTP Server.
Oct 14 20:22:43 sekosolapov.localdomain systemd[1]: httpd.service: Consumed 12.857s CPU time.
Oct 14 20:22:43 sekosolapov.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 20:22:43 sekosolapov.localdomain httpd[41448]: Server configured, listening on: port 81
Oct 14 20:22:43 sekosolapov.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 20:23:26 sekosolapov.localdomain systemd[1]: Stopping The Apache HTTP Server...
Oct 14 20:23:27 sekosolapov.localdomain systemd[1]: httpd.service: Deactivated successfully.
Oct 14 20:23:27 sekosolapov.localdomain systemd[1]: Stopped The Apache HTTP Server.
[root@sekosolapov ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@sekosolapov ~]# 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 20:23:33 MSK; 2s ago
     Docs: man:httpd.service(8)
  Main PID: 41697 (httpd)
    Status: "Started, listening on: port 81"
    Tasks: 213 (limit: 50441)
   Memory: 45.0M
      CPU: 207ms
   CGroup: /system.slice/httpd.service
           └─41697 /usr/sbin/httpd -DFOREGROUND
             └─41698 /usr/sbin/httpd -DFOREGROUND
               └─41699 /usr/sbin/httpd -DFOREGROUND
                 └─41700 /usr/sbin/httpd -DFOREGROUND
                   └─41701 /usr/sbin/httpd -DFOREGROUND

Oct 14 20:23:33 sekosolapov.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 14 20:23:33 sekosolapov.localdomain httpd[41697]: Server configured, listening on: port 81
Oct 14 20:23:33 sekosolapov.localdomain systemd[1]: Started The Apache HTTP Server.
[root@sekosolapov ~]#
```

перезапуск httpd с портом 81

18. Анализируем лог-файлы: `tail -n1 /var/log/messages`, и видим, что проблем не возникло. После просмотра `semanage port -l | grep http_port_t`, замечаем, что 81 порт уже добавлен.

```
[root@sekosolapov ~]# tail -n10 /var/log/messages
Oct 14 20:25:36 sekosolapov gnome-shell[1769]: Window manager warning: W1 appears to be one of the offending windows with a timestamp of 2586211. Working around...
Oct 14 20:25:36 sekosolapov gnome-shell[1769]: Window manager warning: last_user_time (2586278) is greater than comparison timestamp (2586242). This most likely represents a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 14 20:25:36 sekosolapov gnome-shell[1769]: Window manager warning: W1 appears to be one of the offending windows with a timestamp of 2586278. Working around...
Oct 14 20:25:51 sekosolapov systemd[1]: Stopping The Apache HTTP Server...
Oct 14 20:25:52 sekosolapov systemd[1]: httpd.service: Deactivated successfully.
Oct 14 20:25:52 sekosolapov systemd[1]: Stopped The Apache HTTP Server.
Oct 14 20:25:52 sekosolapov systemd[1]: httpd.service: Consumed 1.307s CPU time.
Oct 14 20:25:52 sekosolapov systemd[1]: Starting The Apache HTTP Server...
Oct 14 20:25:52 sekosolapov systemd[1]: Started The Apache HTTP Server.
Oct 14 20:25:52 sekosolapov httpd[41971]: Server configured, listening on: port 81
[root@sekosolapov ~]# 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@sekosolapov ~]#
```

системные логи при прослушивании 81 порта httpd

19. Пробуем провести все действия с портом 82. Добавляем его в `/etc/httpd/conf/httpd.conf` и перезапускаем httpd сервис. Видим ошибку, все из-за того, то не добавлен

порт в http_port_t. Добавляем командой semanage port -a -t http_port_t -p tcp 82.

После этого пробуем перезапустить httpd и все проходит на этот раз без ошибок.

Возвращаем контекст файлу test.html и у нас получается достучаться теперь к этому файлу, все работает.

```
[root@sekosolapov ~]# 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@sekosolapov ~]# semanage port -a -t http_port_t -p tcp 82
[root@sekosolapov ~]# semanage port -l | grep http_port_t
http_port_t          tcp      82, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@sekosolapov ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@sekosolapov ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@sekosolapov ~]# wget localhost:81/test.html
--2023-10-14 20:31:29-- http://localhost:81/test.html
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:81... failed: Connection refused.
Connecting to localhost (localhost)|127.0.0.1|:81... failed: Connection refused.
[root@sekosolapov ~]# wget localhost:82/test.html
--2023-10-14 20:31:35-- http://localhost:82/test.html
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:82... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38 [text/html]
Saving to: 'test.html'

test.html          100%[=====]
2023-10-14 20:31:35 (5.67 MB/s) - 'test.html' saved [38/38]

[root@sekosolapov ~]# wget localhost:82/test.html | cat
```

повторение действий для порта 82

20. Удаляем файл test.html и удаляем связь порта 82 из http_port_t.

```
[root@sekosolapov ~]# semanage port -d -t http_port_t -p tcp 82
[root@sekosolapov ~]# 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@sekosolapov ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@sekosolapov ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'?
[root@sekosolapov ~]#
```

удаление test.html и порта 82 из http_port_t

3 Выводы

В данной работе мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.