

Лабораторная Работа №6. Мандатное разграничение прав в Linux

Основы информационной безопасности

Барсегян В.Л.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

- Барсегян Вардан Левонович
- НПИбд-01-22
- Российский университет дружбы народов
- [1132222005@pfur.ru]
- <https://github.com/VARdamn/oib>

Вводная часть

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

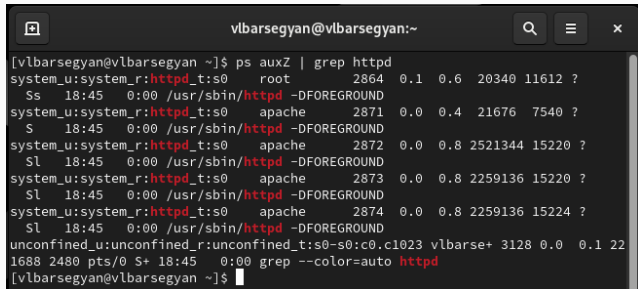
Выполнение лабораторной работы

Убеждаюсь, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus*. Запускаю веб-сервер командой *service httpd start* и проверяю его статус командой *service httpd status*

```
[vlbarsegyan@vlbarsegyan ~]$ getenforce
Enforcing
[vlbarsegyan@vlbarsegyan ~]$ 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
[vlbarsegyan@vlbarsegyan ~]$ 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)
[vlbarsegyan@vlbarsegyan ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[vlbarsegyan@vlbarsegyan ~]$ 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 Tue 2024-03-19 18:45:02 MSK; 2s ago
     Docs: man:httpd.service(8)
```

Figure 1: Запуск и проверка веб-сервера

Определяю контекст безопасности веб-сервера с помощью команды `ps auxZ | grep httpd`



```
[vlbarsegyan@vlbarsegyan ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root          2864  0.1  0.6 20340 11612 ?
  Ss  18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        2871  0.0  0.4 21676  7540 ?
  S   18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        2872  0.0  0.8 2521344 15220 ?
  Sl  18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        2873  0.0  0.8 2259136 15220 ?
  Sl  18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        2874  0.0  0.8 2259136 15224 ?
  Sl  18:45   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vlbarse+ 3128 0.0  0.1 22
1688 2480 pts/0 S+ 18:45   0:00 grep --color=auto httpd
[vlbarsegyan@vlbarsegyan ~]$
```

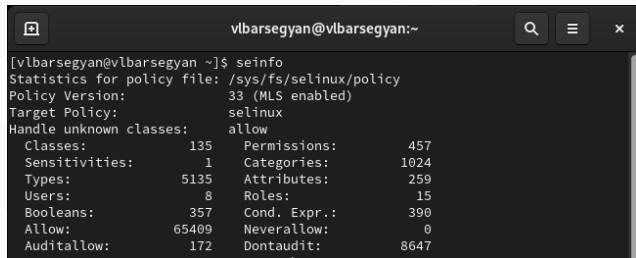
Figure 2: Контекст безопасности веб-сервера

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

```
without options, show SELinux status.  
[vlbarsegyan@vlbarsegyan ~]$ 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
```

Figure 3: Состояние переключателей SELinux

Смотрю статистику по политике с помощью команды *seinfo*

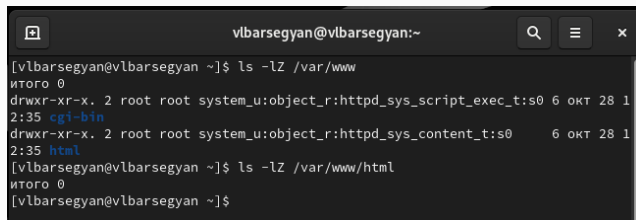


```
[vlbarsegyan@vlbarsegyan ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      135      Permissions:      457
Sensitivities: 1      Categories:      1024
Types:        5135     Attributes:       259
Users:        8       Roles:           15
Booleans:     357     Cond. Expr.:     390
Allow:        65409   Neverallow:      0
Auditallow:   172     Dontaudit:       8647
```

Figure 4: Статистика по политике

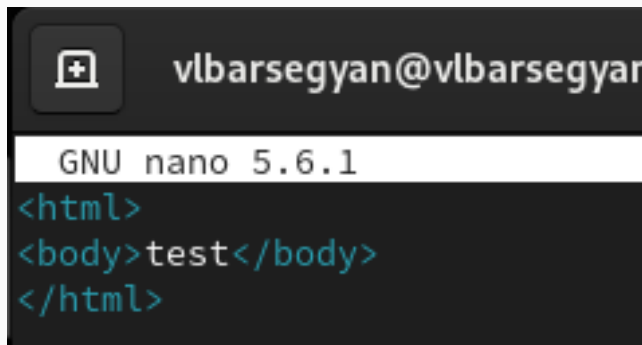
Определяю тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. Аналогично для директории `/var/www/html`



```
vlbarsegyan@vlbarsegyan:~  
[vlbarsegyan@vlbarsegyan ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 1  
2:35 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 1  
2:35 html  
[vlbarsegyan@vlbarsegyan ~]$ ls -lZ /var/www/html  
итого 0  
[vlbarsegyan@vlbarsegyan ~]$
```

Figure 5: Определение типа файлов и папок

Создаю файл `/var/www/html/test.html` и записываю следующий html-код



The image shows a terminal window with a dark background. At the top, the username and host are `vlbarsegyan@vlbarsegyan`. Below that, the prompt `GNU nano 5.6.1` is visible. The editor is displaying the following HTML code:

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

Figure 6: test.html

Проверяю контекст созданного файла командой `ps auxZ | grep test.html`

```
[root@vlbarsegyan vlbarsegyan]# nano /var/www/html/test.html
[root@vlbarsegyan vlbarsegyan]# ps auxZ | grep test.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3550 0.0  0.1 221824
2432 pts/0 S+ 18:52   0:00 grep --color=auto test.html
[root@vlbarsegyan vlbarsegyan]#
```

Figure 7: Контекст файла

Проверяю в браузере, что файл успешно отображается

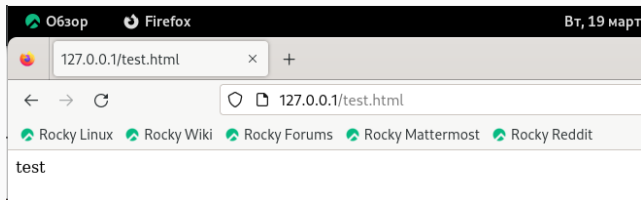
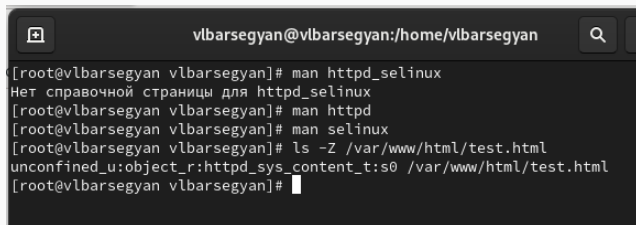


Figure 8: Проверка в браузере

Изучаю справку man по командам httpd и selinux, также проверяю контекст файла командой `ls -Z /var/www/html/test.html`



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# man httpd_selinux
Нет справочной страницы для httpd_selinux
[root@vlbarsegyan vlbarsegyan]# man httpd
[root@vlbarsegyan vlbarsegyan]# man selinux
[root@vlbarsegyan vlbarsegyan]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@vlbarsegyan vlbarsegyan]#
```

Figure 9: Изучение man, проверка контекста

Изменяю контекст файла `test.html` командой `chcon -t samba_share_t /var/www/html/test.html`. После, проверяю его и открываю веб-страницу - нет доступа

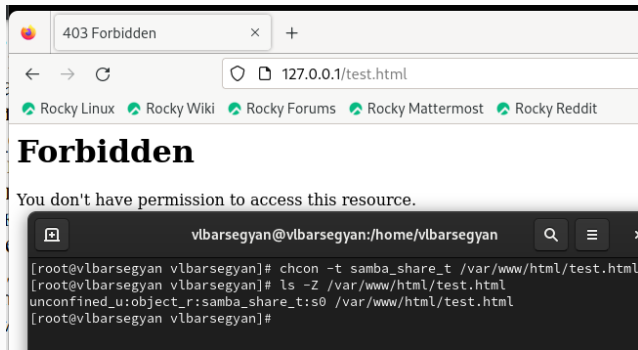


Figure 10: Изменение контекста

Просматриваю системный лог-файл командой `tail /var/log/messages`

```
ать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль  
политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -  
с 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#0  
12  
Mar 19 18:56:40 vlbarsegyan systemd[1]: dbus-:1.1-org.fedoraproject.Setroublesh  
ootPrivileged@0.service: Deactivated successfully.  
Mar 19 18:56:40 vlbarsegyan systemd[1]: dbus-:1.1-org.fedoraproject.Setroublesh  
ootPrivileged@0.service: Consumed 1.149s CPU time.  
Mar 19 18:56:40 vlbarsegyan systemd[1]: setroubleshootd.service: Deactivated su  
ccessfully.  
[root@vlbarsegyan vlbarsegyan]#
```

Figure 11: Системный лог-файл

В файле /etc/httpd/conf/httpd.conf меняю порт на 81

```
#  
# Change this to Listen on a specific IP address.  
# httpd.service is enabled to run as root, but it should be  
# available when the service starts. See http://wiki.apache.org/httpd/SELinux  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 81  
  
#  
# Dynamic Shared Object (DSO) Support  
#
```

Figure 12: Смена порта

Перезагружаю веб-сервер - получен сбой

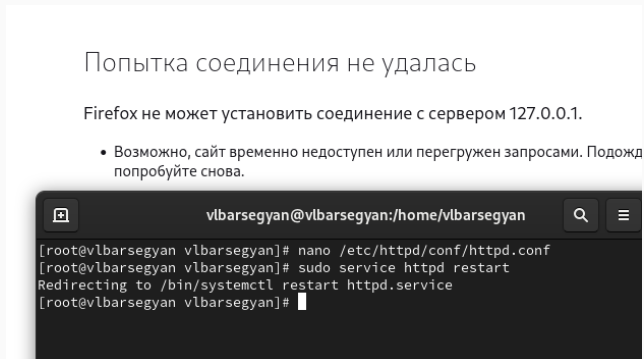
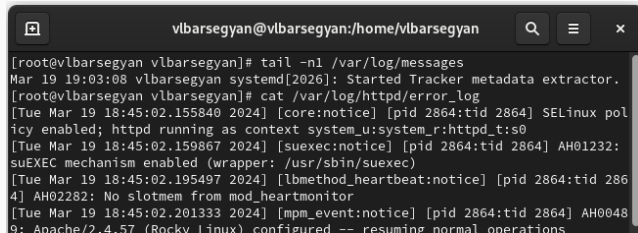


Figure 13: Сбой веб-сервера

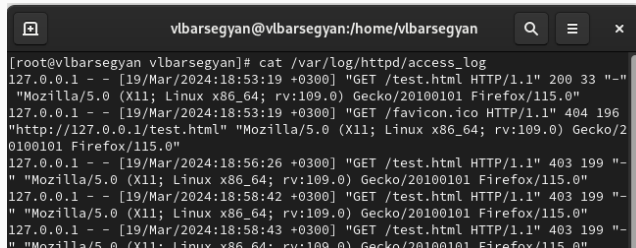
Анализирую лог-файлы командами `tail -n1 /var/log/messages` и `cat /var/log/httpd/error_log`



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# tail -n1 /var/log/messages
Mar 19 19:03:08 vlbarsegyan systemd[2026]: Started Tracker metadata extractor.
[root@vlbarsegyan vlbarsegyan]# cat /var/log/httpd/error_log
[Tue Mar 19 18:45:02.155840 2024] [core:notice] [pid 2864:tid 2864] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Tue Mar 19 18:45:02.159867 2024] [suexec:notice] [pid 2864:tid 2864] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Tue Mar 19 18:45:02.195497 2024] [lbmethod_heartbeat:notice] [pid 2864:tid 2864] AH02282: No slotmem from mod_heartbeat
[Tue Mar 19 18:45:02.201333 2024] [mpm_event:notice] [pid 2864:tid 2864] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
```

Figure 14: Проверка лог-файлов

Также проверяю лог-файл `/var/log/httpd/access_log`



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# cat /var/log/httpd/access_log
127.0.0.1 - - [19/Mar/2024:18:53:19 +0300] "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 - - [19/Mar/2024:18:53:19 +0300] "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/2
0100101 Firefox/115.0"
127.0.0.1 - - [19/Mar/2024:18:56:26 +0300] "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 - - [19/Mar/2024:18:58:42 +0300] "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 - - [19/Mar/2024:18:58:43 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

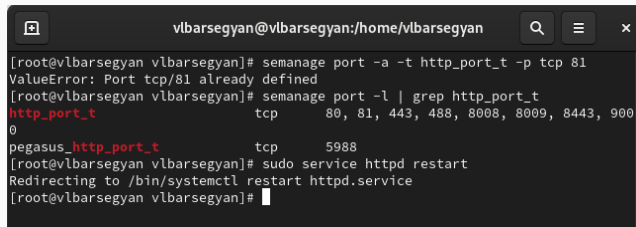
Figure 15: Проверка лог-файлов

Также проверяю лог-файл `/var/log/audit/audit.log`.

```
cat /var/log/audit/audit.log: нет такого файла или каталога
[root@vlbarsegyan vlbarsegyan]# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1708186194.512:1034): op=start ver=3.0.7 format=enr
iched kernel=5.14.0-284.11.1.el9_2.x86_64 auid=4294967295 pid=722 uid=0 ses=429
4967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1708186194.521:5): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journal-catalog-
update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal
=? res=success'UID="root" AUID="unset"
```

Figure 16: Проверка лог-файлов

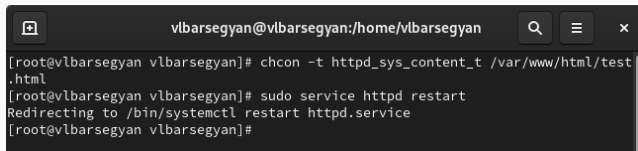
Выполняю команду `semanage port -a -t http_port_t -p tcp 81` и проверяю список портов командой `semanage port -l | grep http_port_t` - порт 81 появился в списке



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@vlbarsegyan vlbarsegyan]# 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@vlbarsegyan vlbarsegyan]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@vlbarsegyan vlbarsegyan]#
```

Figure 17: Добавление порта 81 в список

Возвращаю контекст `httpd_sys_content__t` к файлу `/var/www/html/ test.html`, введя `chcon -t httpd_sys_content_t /var/www/html/test.html`. Перезапускаю веб-сервер командой `sudo service httpd restart`

A terminal window with a dark background. The title bar shows the user 'vlbarsegyan' at host 'vlbarsegyan' in the directory '/home/vlbarsegyan'. The terminal contains the following text:

```
[root@vlbarsegyan vlbarsegyan]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vlbarsegyan vlbarsegyan]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@vlbarsegyan vlbarsegyan]#
```

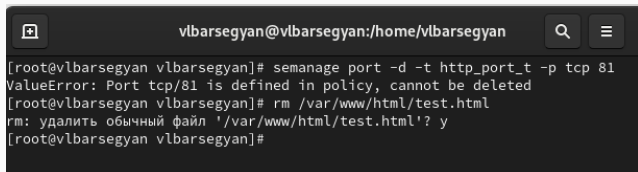
Figure 18: Возвращение контекста и перезапуск веб-сервера

Возвращаю порт 80 в конфигурационном файле

```
#  
# Change this to Listen on a $  
# httpd.service is enabled to  
# available when the service s  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 80  
  
#  
# Dynamic Shared Object (DSO)  
#
```

Figure 19: Смена порта на 80

Удаляю привязку `http_port_t` к 81 порту командой `semanage port -d -t http_port_t -p tcp 81` и удаляю файл `test.html` командой `rm /var/www/html/test.html`



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@vlbarsegyan vlbarsegyan]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@vlbarsegyan vlbarsegyan]#
```

Figure 20: Удаление привязки к 81 порту и удаление html-файла

Вывод

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux, поработал с веб-сервером Apache