

Лабораторная работа №6

Мандатное разграничение прав в Linux

Хусаинова Д.А. Группа НПИбд-02-21

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinx на практике совместно с веб-сервером Apache.

1. **SELinux (Security-Enhanced Linux)** обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена.

SELinux имеет три основных режим работы:

- Enforcing: режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Теоретическое введение 2/2

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA).

Для чего нужен Apache сервер:

- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Выполнение лабораторной работы

getenforce и sestatus

```
[dakhusainova@dakhusainova ~]$ getenforce
Enforcing
[dakhusainova@dakhusainova ~]$ 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
[dakhusainova@dakhusainova ~]$
```

Рис. 1: getenforce и sestatus

status

```
[dakhusainova@dakhusainova ~]$ sudo systemctl start httpd
[dakhusainova@dakhusainova ~]$ 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; vendor preset: enabled)
   Active: active (running) since Thu 2024-10-10 18:59:27 MSK; 1min 15s ago
     Docs: man:httpd.service(8)
   Main PID: 3387 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests served 0/0"
   Tasks: 177 (limit: 12195)
   Memory: 22.3M
     CPU: 72ms
   CGroup: /system.slice/httpd.service
           └─3387 /usr/sbin/httpd -DFOREGROUND
             └─3388 /usr/sbin/httpd -DFOREGROUND
               └─3392 /usr/sbin/httpd -DFOREGROUND
                 └─3393 /usr/sbin/httpd -DFOREGROUND
                   └─3394 /usr/sbin/httpd -DFOREGROUND

Oct 10 18:59:25 dakhusainova.localdomain systemd[1]: Starting httpd.service: The Apache HTTP Server:
Oct 10 18:59:27 dakhusainova.localdomain systemd[1]: Started httpd.service: The Apache HTTP Server:
Oct 10 18:59:27 dakhusainova.localdomain httpd[3387]: Server configured for IPv6
lines 1-19/19 (END)...skipping...
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-10-10 18:59:27 MSK; 1min 15s ago
     Docs: man:httpd.service(8)
   Main PID: 3387 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests served 0/0"
   Tasks: 177 (limit: 12195)
   Memory: 22.3M
     CPU: 72ms
```

ps auxZ | grep httpd and sestatus

```
[dakhusainova@dakhusainova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root          3387  0.0  0.5 203
64 11528 ?                Ss   18:59   0:00 /usr/sbin/httpd -DFOREGROUN
D
system_u:system_r:httpd_t:s0      apache        3388  0.0  0.3 220
96 7144 ?                S    18:59   0:00 /usr/sbin/httpd -DFOREGROUN
D
system_u:system_r:httpd_t:s0      apache        3392  0.0  0.5 9815
20 11092 ?               Sl   18:59   0:00 /usr/sbin/httpd -DFOREGROUN
D
system_u:system_r:httpd_t:s0      apache        3393  0.0  0.5 9815
20 11096 ?               Sl   18:59   0:00 /usr/sbin/httpd -DFOREGROUN
D
system_u:system_r:httpd_t:s0      apache        3394  0.0  0.6 1112
656 13288 ?              Sl   18:59   0:00 /usr/sbin/httpd -DFOREGROUN
D
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dakhusa+
3760 0.0  0.1 221664 2176 pts/0 S+ 19:01   0:00 grep --color=au
to httpd
[dakhusainova@dakhusainova ~]$ 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.
[dakhusainova@dakhusainova ~]$
```


Определение типа файлов

```
[dakhusainova@dakhusainova ~]$ 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:        5145     Attributes:       259
Users:        8       Roles:           15
Booleans:     356     Cond. Expr.:     388
Allow:        65500   Neverallow:      0
Auditallow:   176     Dontaudit:       8682
Type_trans:   271770  Type_change:     94
Type_member:  37      Range_trans:     5931
Role allow:   40      Role_trans:      417
Constraints:  70      Validatetrans:   0
MLS Constrai: 72     MLS Val. Tran:   0
Permissives:  4      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:         665
Netifcon:     0      Nodecon:         0

[dakhusainova@dakhusainova ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec
_t:s0 6 Aug  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s
0 6 Aug  8 19:30 html
[dakhusainova@dakhusainova ~]$ ls -lZ /var/www/html
total 0
```

создание файла

```
[dakhusainova@dakhusainova ~]$ sudo nano /var/www/html/test.html
[dakhusainova@dakhusainova ~]$ sudo cat /var/www/html/test.html<html>
<body>
test
</body>
</html>
[dakhusainova@dakhusainova ~]$
```

Рис. 5: создание файла

```
[dakhusainova@dakhusainova ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 35 0
ct 10 19:07 test.html
[dakhusainova@dakhusainova ~]$
```

Рис. 6: проверка контекста

обращение к файлу

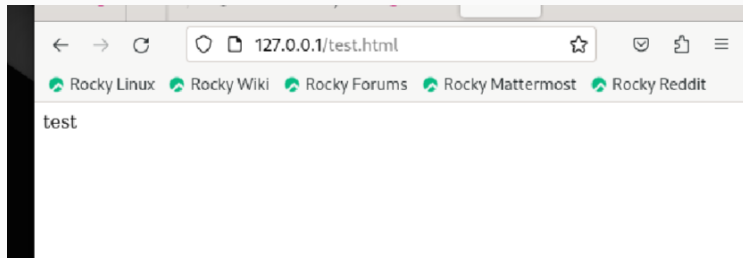


Рис. 7: обращение к файлу

man httpd_selinux

```
dakhusainova@dakhusainova:~ — info httpd selinux
HTTPD(8)                                httpd                                HTTPD(8)

NAME
    httpd - Apache Hypertext Transfer Protocol Server

SYNOPSIS
    httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c di-
    rective ] [ -D parameter ] [ -e level ] [ -E file ] [ -k
    start|restart|graceful|stop|graceful-stop ] [ -h ] [ -l ] [ -L ]
    [ -S ] [ -t ] [ -v ] [ -V ] [ -X ] [ -M ] [ -T ]

    On Windows systems, the following additional arguments are
    available:

    httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]

SUMMARY
    httpd is the Apache HyperText Transfer Protocol (HTTP) server
    program. It is designed to be run as a standalone daemon
    process. When used like this it will create a pool of child
    processes or threads to handle requests.

    In general, httpd should not be invoked directly, but rather
    should be invoked via apachectl on Unix-based systems or as a
    service on Windows NT, 2000 and XP and as a console application
    on Windows 9x and ME.

OPTIONS
    -d serverroot
        Set the initial value for the ServerRoot directive to
        serverroot. This can be overridden by the ServerRoot di-
        rective in the configuration file. The default is
        /etc/httpd.

    -f config
        Uses the directives in the file config on startup. If
        -----Info: (*manpages*)httpd, 119 lines --Top-----
```

проверка контекста файла

```
[dakhusainova@dakhusainova ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[dakhusainova@dakhusainova ~]$
```

Рис. 9: проверка контекста файла

Изменение контекста файла

```
rw-r--r--. 1 root root 35 Oct 10 19:07 /var/www/html/test.html
[dakhusainova@dakhusainova ~]$ sudo chcon -t samba_share_t /var/www/html/
test.html
[dakhusainova@dakhusainova ~]$ ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 35 Oct 10
19:07 /var/www/html/test.html
[dakhusainova@dakhusainova ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 35 Oct 10 19:07 /var/www/html/test.html
[dakhusainova@dakhusainova ~]$
```

Рис. 10: Изменение контекста файла

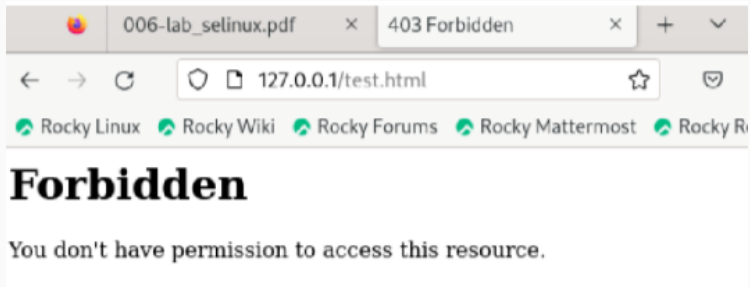


Рис. 11: You don't have permission to access

просмотр логов

```
[dakhusainova@dakhusainova ~]$ sudo tail /var/log/messages
Oct 10 19:21:46 dakhusainova systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.
Oct 10 19:21:46 dakhusainova setroubleshoot[4506]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 10 19:21:46 dakhusainova systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 10 19:21:46 dakhusainova systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 10 19:21:47 dakhusainova setroubleshoot[4506]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 68690a52-e372-4bef-8939-553277261788
Oct 10 19:21:47 dakhusainova setroubleshoot[4506]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 10 19:21:47 dakhusainova setroubleshoot[4506]: SELinux is preventing
```

замена порта

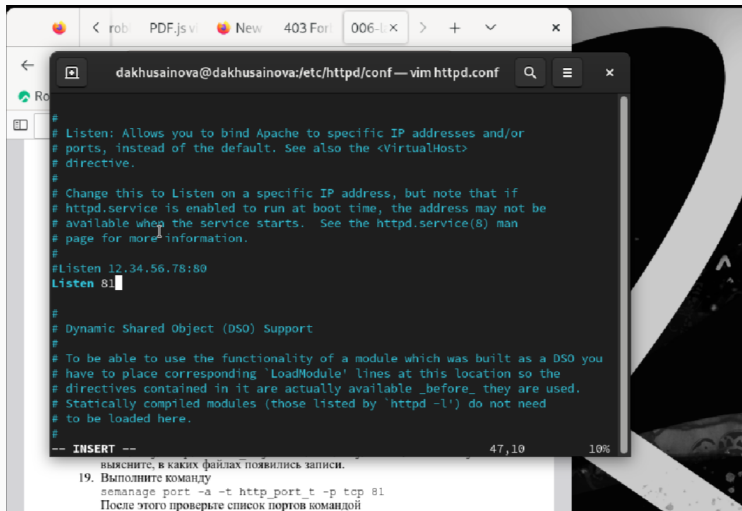


Рис. 13: замена порта

```
[dakhusainova@dakhusainova conf]$ sudo semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9
pegasus_http_port_t tcp      5988
[dakhusainova@dakhusainova conf]$
```

Рис. 14: сбой

удаление файла

```
[dakhusainova@dakhusainova conf]$ sudo rm /var/www/html/test.html  
[dakhusainova@dakhusainova conf]$
```

Рис. 15: удаление файла

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.

Список литературы. Библиография

[0] Методические материалы курса

[1] Права доступа:

<https://codechick.io/tutorials/unix-linux/unix-linux-permissions>