

Лабораторная работа №6

Информационная безопасность

Николаев Д. И.

8 октября 2023

Российский университет дружбы народов, Москва, Россия

Прагматика выполнения

- Повышение навыков администрирования ОС Linux;
- Знакомство с технологией SELinux и проверка ее работы на практике совместно с веб-сервером Apache;
- Применение полученных знаний на практике в дальнейшем.

Цели

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

Задачи

1. Ознакомиться с технологией SELinux;
2. Проверить работу SELinux в связке с веб-сервером Apache.

Выполнение работы

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

Рис. 1: Режим работы SELinux

```
[dinikolaev@dinikolaev ~]$ 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 2023-10-07 22:32:51 MSK; 2min 12s ago
     Docs: man:httpd.service(8)
   Main PID: 42745 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 213 (limit: 5689)
    Memory: 38.2M
       CPU: 134ms
    CGroup: /system.slice/httpd.service
            └─42745 /usr/sbin/httpd -DFOREGROUND
              └─42753 /usr/sbin/httpd -DFOREGROUND
                └─42754 /usr/sbin/httpd -DFOREGROUND
                  └─42755 /usr/sbin/httpd -DFOREGROUND
                    └─42756 /usr/sbin/httpd -DFOREGROUND

окт 07 22:32:51 dinikolaev systemd[1]: Starting The Apache HTTP Server...
окт 07 22:32:51 dinikolaev systemd[1]: Started The Apache HTTP Server.
окт 07 22:32:51 dinikolaev httpd[42745]: Server configured, listening on: port 80
[dinikolaev@dinikolaev ~]$
```

Рис. 2: Обращение к веб-серверу

Проверка контекста безопасности

```
[dinikolaev@dinikolaev ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 42684 0.0 0.9 236232 8808 pts/0 T 22:31
0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 42699 0.0 0.9 236232 8864 pts/0 T 22:32
0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0 root 42745 0.0 1.0 20128 9748 ? Ss 22:32 0:00 /usr
/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42753 0.0 0.5 21612 5772 ? S 22:32 0:00 /usr
/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42754 0.0 1.4 1079384 13824 ? Sl 22:32 0:00 /usr
/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42755 0.0 1.6 1210520 15772 ? Sl 22:32 0:00 /usr
/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42756 0.0 1.4 1079384 13912 ? Sl 22:32 0:00 /usr
/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 43031 0.0 0.9 236232 9080 pts/0 T 22:33
0:00 /bin/systemctl status httpd.service start
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 43140 0.0 0.2 221688 2332 pts/0 S+ 22:3
6 0:00 grep --color=auto httpd
[dinikolaev@dinikolaev ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 42745 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42753 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42754 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42755 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42756 ? 00:00:00 httpd
[dinikolaev@dinikolaev ~]$
```

Рис. 3: Проверка контекста безопасности процессов

```
[dinikolaev@dinikolaev ~]$ 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:                    65380    Neverallow:               0
Auditallow:               172      Dontaudit:                8647
Type_trans:               267809   Type_change:              94
Type_member:               37       Range_trans:              6164
Role allow:               39        Role_trans:               419
Constraints:              70        Validatetrans:            0
MLS Constrain:            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:                   665
Netifcon:                 0         Nodecon:                   0

[dinikolaev@dinikolaev ~]$
```

```
[dinikolaev@dinikolaev ~]$ ps auxZ | grep html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 43656 0.0  0.2 221688 2332 pts/0 S+ 22:4
8   0:00 grep --color=auto html
[dinikolaev@dinikolaev ~]$ ps auxZ | grep test.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 43666 0.0  0.2 221824 2316 pts/0 S+ 22:4
9   0:00 grep --color=auto test.html
[dinikolaev@dinikolaev ~]$ ps auxZ | grep www
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dinikol+ 43672 0.0  0.2 221688 2332 pts/0 S+ 22:4
9   0:00 grep --color=auto www
[dinikolaev@dinikolaev ~]$ ps -eZ | grep html
[dinikolaev@dinikolaev ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 окт  7 22:46 test.html
[dinikolaev@dinikolaev ~]$
```

Рис. 5: Проверка контекста созданного файла

Обращение к файлу через браузер

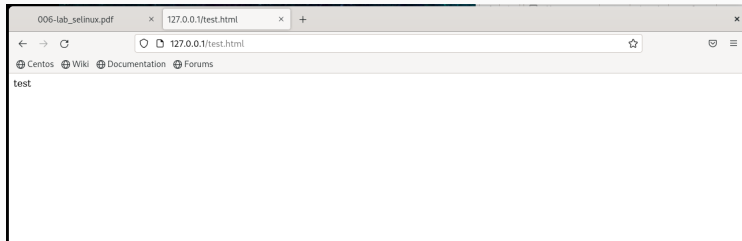


Рис. 6: Обращение к файлу через веб-сервер

```
[dinikolaev@dinikolaev ~]$ su
Пароль:
[root@dinikolaev dinikolaev]# chcon -t samba_share_t /var/www/html/test.html
[root@dinikolaev dinikolaev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@dinikolaev dinikolaev]#
```

Рис. 7: Смена контекста файла

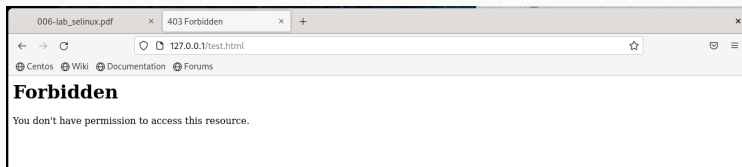


Рис. 8: Попытка получения доступа к файлу через веб-сервер

```
[dinikolaev@dinikolaev ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[dinikolaev@dinikolaev ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 окт  7 22:46 /var/www/html/test.html
[dinikolaev@dinikolaev ~]$ tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[dinikolaev@dinikolaev ~]$ sudo tail /var/log/messages
[sudo] пароль для dinikolaev:
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for webkit2gtk3-jsc
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-core
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-modules
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-modules-core
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-devel
Oct  7 23:12:07 dinikolaev systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service:
Deactivated successfully.
Oct  7 23:12:07 dinikolaev systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct  7 23:14:32 dinikolaev systemd[1]: Starting Fingerprint Authentication Daemon...
Oct  7 23:14:32 dinikolaev systemd[1]: Started Fingerprint Authentication Daemon.
```

Рис. 9: Последние сообщения log-файла

Перезапуск веб-сервера Apache

```
[dinikolaev@dinikolaev ~]$ sudo systemctl restart httpd
[sudo] пароль для dinikolaev:
[dinikolaev@dinikolaev ~]$ sudo netstat -tlnp | grep httpd
tcp6      0      0 :::81                :::*                  LISTEN      8814/httpd

[dinikolaev@dinikolaev ~]$ sudo ss -tlnp | grep httpd
LISTEN 0      511      *:81                 *:.*                  users:((("httpd",pid=8821,fd=4),("httpd",pid=8820,fd=4),("httpd",pid=8816,fd=4),("httpd",pid=8814,fd=4))
[dinikolaev@dinikolaev ~]$ 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 Sun 2023-10-08 01:33:23 MSK; 52s ago
     Docs: man:httpd.service(8)
   Main PID: 8814 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
     Tasks: 213 (limit: 4460)
    Memory: 33.3M
       CPU: 67ms
   CGroup: /system.slice/httpd.service
           └─8814 /usr/sbin/httpd -DFOREGROUND
             └─8815 /usr/sbin/httpd -DFOREGROUND
               └─8816 /usr/sbin/httpd -DFOREGROUND
                 └─8820 /usr/sbin/httpd -DFOREGROUND
                   └─8821 /usr/sbin/httpd -DFOREGROUND

окт 08 01:33:23 dinikolaev systemd[1]: Starting The Apache HTTP Server...
окт 08 01:33:23 dinikolaev systemd[1]: Started The Apache HTTP Server.
окт 08 01:33:23 dinikolaev httpd[8814]: Server configured, listening on: port 81
lines 1-19/19 (END)
```

Рис. 10: Перезапуск веб-сервера Apache

Попытка подключения через браузер

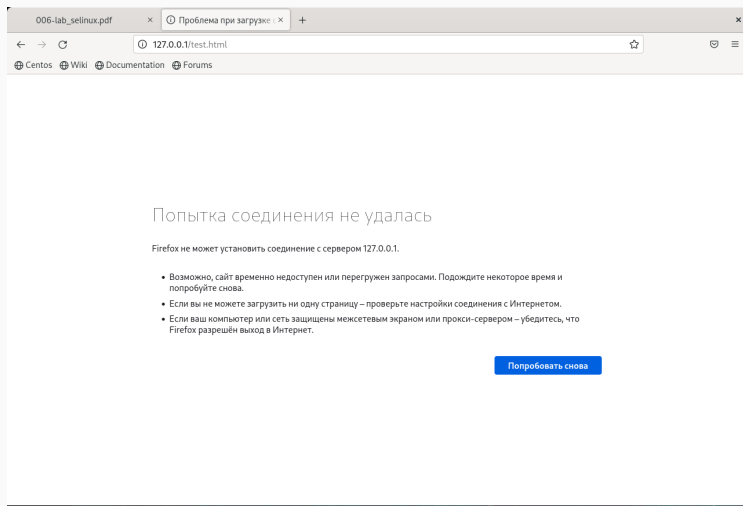


Рис. 11: Попытка подключения к веб-серверу через браузер

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

Рис. 12: Установка 81 порта и проверка списка всех портов

```
[dinikolaev@dinikolaev ~]$ su
Пароль:
[root@dinikolaev dinikolaev]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dinikolaev dinikolaev]#
```

Рис. 13: Возвращение контекста httpd_sys_content_t нашему файлу

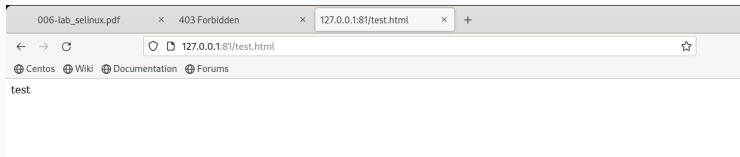


Рис. 14: Получение доступа к файлу через браузер

Попытка удаления привязки к 81 порту

```
[root@dinikolaev dinikolaev]# vim /etc/httpd/conf/httpd.conf
[root@dinikolaev dinikolaev]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@dinikolaev dinikolaev]# systemctl restart httpd
[root@dinikolaev dinikolaev]# netstat -tln | grep httpd
tcp6      0      0 :::80          :::*           LISTEN     10024/httpd
[root@dinikolaev dinikolaev]# ss -tln | grep httpd
LISTEN 0      511      *:80          :::*           users:(("httpd",pid=10031,fd=4),("httpd",pid=10030,fd=4),
"httpd",pid=10029,fd=4),("httpd",pid=10024,fd=4))
[root@dinikolaev dinikolaev]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@dinikolaev dinikolaev]# 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@dinikolaev dinikolaev]#
```

Рис. 15: Попытка удаления привязки к 81 порту

```
[dinikolaev@dinikolaev ~]$ sudo rm /var/www/html/test.html
[sudo] пароль для dinikolaev:
[dinikolaev@dinikolaev ~]$
```

Рис. 16: Удаление файла test.html

Результаты

По результатам работы, я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux и проверил работу SELinux на практике совместно с веб-сервером Apache.