

Лабораторная работа №6

Основы информационной безопасности

Мурашов И. В., НКАбд-03-23

3 мая 2025

Российский университет дружбы народов, Москва, Россия

- Мурашов Иван Вячеславович
- Студент, 2 курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132236018@rudn.ru
- <https://neve7mind.github.io>

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

Выполнение лабораторной работы

Выполнение лабораторной работы

SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`

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

Выполнение лабораторной работы

Запускаю сервер apache, далее обращаюсь с помощью браузера к веб-серверу, запущенному на компьютере, он работает, что видно из вывода команды `service httpd status`

```
[ivmurashov@ivmurashov ~]$ sudo systemctl start httpd
[sudo] password for ivmurashov:
[ivmurashov@ivmurashov ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ivmurashov@ivmurashov ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-05-03 00:23:55 MSK; 40s ago
     Docs: man:httpd.service(8)
  Main PID: 7378 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 177 (limit: 29427)
   Memory: 32.5M
      CPU: 453ms
  CGroup: /system.slice/httpd.service
          └─7378 /usr/sbin/httpd -DFOREGROUND
             └─7379 /usr/sbin/httpd -DFOREGROUND
                └─7380 /usr/sbin/httpd -DFOREGROUND
                   └─7381 /usr/sbin/httpd -DFOREGROUND
                      └─7382 /usr/sbin/httpd -DFOREGROUND

May 03 00:23:55 ivmurashov.localdomain systemd[1]: Starting The Apache HTTP Server: httpd.
May 03 00:23:55 ivmurashov.localdomain httpd[7378]: Server configured, listening on *
May 03 00:23:55 ivmurashov.localdomain systemd[1]: Started The Apache HTTP Server: httpd.
lines 1-19/19 (END)...skipping...
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-05-03 00:23:55 MSK; 40s ago
     Docs: man:httpd.service(8)
  Main PID: 7378 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 177 (limit: 29427)
   Memory: 32.5M
```

С помощью команды `ps auxZ | grep httpd` нахожу веб-сервер Apache в списке процессов. Его контекст безопасности - `httpd_t`

```
[ivmurashov@ivmurashov ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      7378  0.0  0.2 21232 11472 ?        Ss   00:23   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  7379  0.0  0.1 22964  7556 ?        S    00:23   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  7380  0.1  0.3 2358708 17356 ?        Sl   00:23   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  7381  0.1  0.2 2162036 10976 ?        Sl   00:23   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  7382  0.1  0.2 2162036 13244 ?        Sl   00:23   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 ivmuras+ 7721  0.0  0.0 221660 2304 pts/0 R+  00:26   0:00 grep --color=auto httpd
```

Рис. 3: Контекст безопасности Apache

Выполнение лабораторной работы

Просматриваю текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`

```
[ivmurashov@ivmurashov ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap     off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content          off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write             off
```


Выполнение лабораторной работы

Просматриваю статистику по политике с помощью команды `seinfo`.
Множество пользователей - 8, ролей - 39, типов - 5135.

```
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:                    5187     Attributes:               259
Users:                    8         Roles:                    15
Booleans:                 358      Cond. Expr.:             390
Allow:                    66245     Neverallow:               0
Auditallow:               178      Dontaudit:                8723
Type_trans:               274461    Type_change:              94
Type_member:              37        Range_trans:              5931
Role allow:               40        Role_trans:               417
Constraints:              70        Validatetrans:            0
MLS Constrain:           72        MLS Val. Tran:            0
Permissives:              6         Polcap:                   6
Defaults:                 7         Typebounds:               0
Allowxperm:               0         Neverallowxperm:          0
Auditallowxperm:          0         Dontauditxperm:           0
```

Типы поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` следующие: владелец - `root`, права на изменения только у владельца. Файлов в директории нет

```
[ivmurashov@ivmurashov ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Jan 22 03:25 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Jan 22 03:25 html
```

Рис. 6: Типы поддиректорий

Выполнение лабораторной работы

Создать файл может только суперпользователь, поэтому от его имени создаём файл touch.html со следующим содержанием:

```
[ivmurashov@ivmurashov ~]$ sudo touch /var/www/html/test.html
[sudo] password for ivmurashov:
[ivmurashov@ivmurashov ~]$ sudo nano /var/www/html/test.html
[ivmurashov@ivmurashov ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</xhtml>
[ivmurashov@ivmurashov ~]$ sudo nano /var/www/html/test.html
[ivmurashov@ivmurashov ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[ivmurashov@ivmurashov ~]$
```

Рис. 7: Создание файла

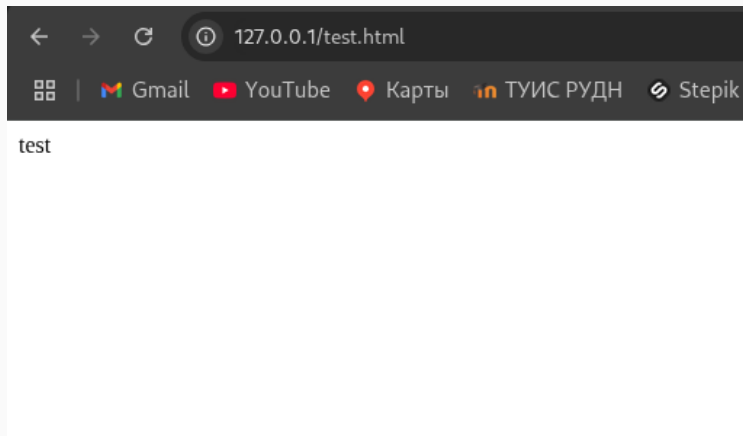
Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t

```
[ivmurashov@ivmurashov ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 May  3 00:31 test.html
[ivmurashov@ivmurashov ~]$
```

Рис. 8: Контекст файла

Выполнение лабораторной работы

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



Изменяю 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` Контекст действительно поменялся

```
[ivmurashov@ivmurashov ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[ivmurashov@ivmurashov ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 May  3 00:31 test.html
[ivmurashov@ivmurashov ~]$
```

Рис. 10: Изменение контекста

Выполнение лабораторной работы

При попытке отображения файла в браузере получаем сообщение об ошибке файл не был отображён, хотя права доступа позволяют читать этот файл любому пользователю, потому что установлен контекст, к которому процесс `httpd` не должен иметь доступа.

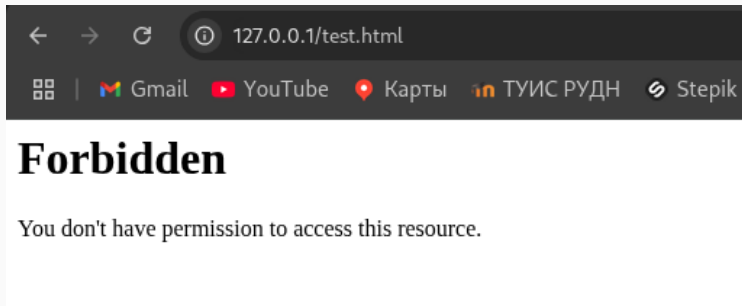


Рис. 11: Отображение файла

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.