

Презентация по лабораторной работе №6

Основы информационной безопасности

Дворкина Е. В

22 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Дворкина Ева Владимировна
- студентка группы НКАбд-01-22
- Российский университет дружбы народов
- <https://vk.com/yuri.kamori>

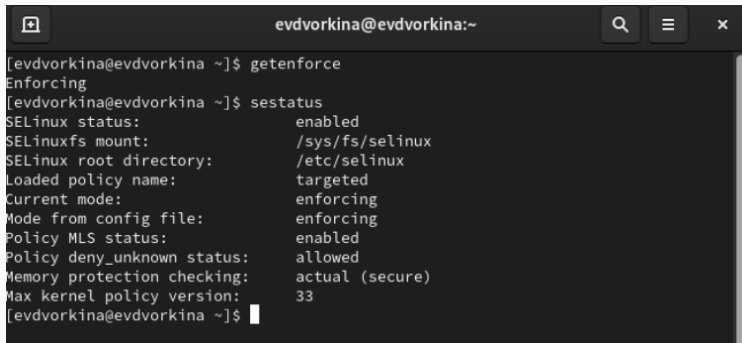


Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

Выполнение лабораторной работы

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

A terminal window titled 'evdvorkina@evdvorkina:~' with search, menu, and close icons in the title bar. It shows the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' is as follows:

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

Рис. 1: проверка режима работы SELinux

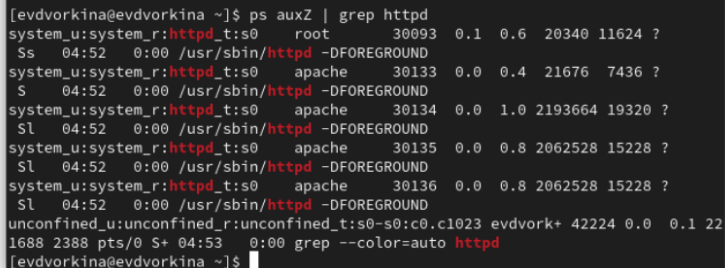
Выполнение лабораторной работы

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

```
[evdvorkina@evdvorkina ~]$ sudo systemctl start httpd
[evdvorkina@evdvorkina ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[evdvorkina@evdvorkina ~]$ 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 2024-04-20 04:52:10 MSK; 31s ago
     Docs: man:httpd.service(8)
  Main PID: 30093 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
    Tasks: 213 (limit: 10899)
   Memory: 37.9M
      CPU: 301ms
    CGroup: /system.slice/httpd.service
            └─30093 /usr/sbin/httpd -DFOREGROUND
              └─30133 /usr/sbin/httpd -DFOREGROUND
                └─30134 /usr/sbin/httpd -DFOREGROUND
                  └─30135 /usr/sbin/httpd -DFOREGROUND
                    └─30136 /usr/sbin/httpd -DFOREGROUND
```

Выполнение лабораторной работы

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



```
[evdvorkina@evdvorkina ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      30093  0.1  0.6  20340 11624 ?
Ss   04:52   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    30133  0.0  0.4   21676  7436 ?
S    04:52   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    30134  0.0  1.0 2193664 19320 ?
Sl   04:52   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    30135  0.0  0.8 2062528 15228 ?
Sl   04:52   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    30136  0.0  0.8 2062528 15228 ?
Sl   04:52   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 evdvork+ 42224 0.0  0.1 22
1688 2388 pts/0 S+  04:53   0:00 grep --color=auto httpd
[evdvorkina@evdvorkina ~]$
```

Рис. 3: Контекст безопасности Apache

Выполнение лабораторной работы

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

```
[evdvorkina@evdvorkina ~]$ 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
```

Выполнение лабораторной работы

Просмотрела 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:                    5135     Attributes:               259
Users:                    8         Roles:                    15
Booleans:                 357      Cond. Expr.:             390
Allow:                    65409    Neverallow:               0
Auditallow:               172      Dontaudit:               8647
Type_trans:               267813   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 SIDes:             27      Enforce:                   25
```

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

```
[evdvorkina@evdvorkina ~]$ 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 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 12:35 html
```

Рис. 6: Типы поддиректорий

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

```
[evdvorkina@evdvorkina ~]$ sudo touch /var/www/html/test.html
[sudo] пароль для evdvorkina:
[evdvorkina@evdvorkina ~]$ sudo nano /var/www/html/test.html
[evdvorkina@evdvorkina ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

Рис. 7: Создание файла

Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t

```
[evdvorkina@evdvorkina ~]$ ls -lZ /var/www/html/  
итого 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 anp 20 05:01 test.html  
[evdvorkina@evdvorkina ~]$
```

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

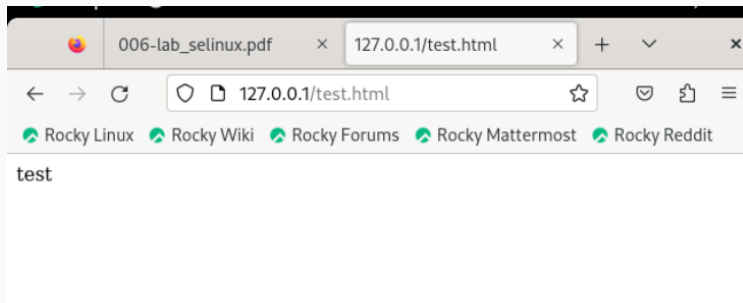
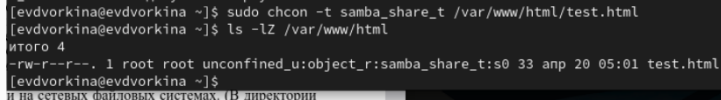


Рис. 9: Отображение файла

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



```
[evdvorkina@evdvorkina ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[evdvorkina@evdvorkina ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 anp 20 05:01 test.html
[evdvorkina@evdvorkina ~]$
```

и на сетевых файловых системах. (В директории

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.

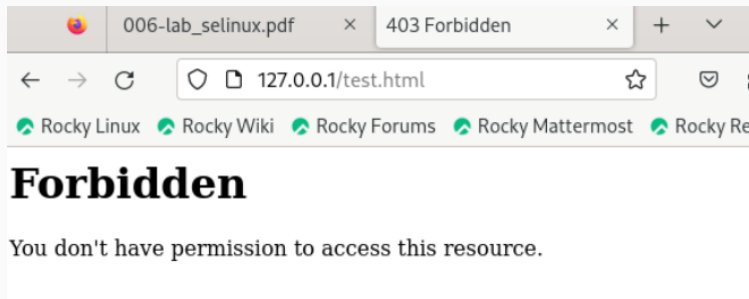


Рис. 11: Отображение файла

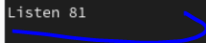
Выполнение лабораторной работы

Чтобы запустить веб-сервер Apache на прослушивание TCP-порта 81 открываю файл /etc/httpd/httpd.conf для изменения. Нахожу строчку Listen 80 и заменяю её на Listen 81.

```
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

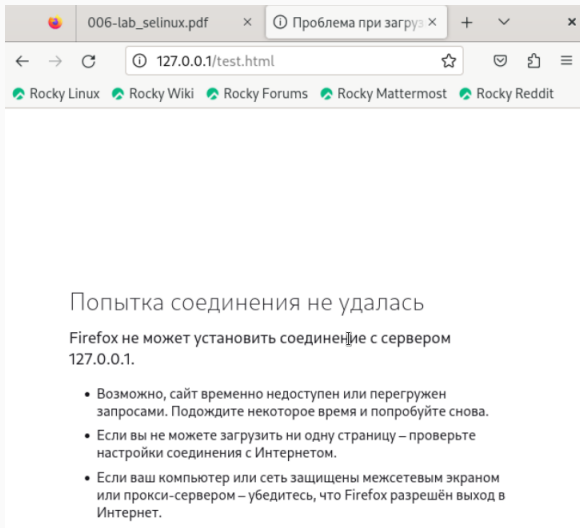
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support
#
```



Выполнение лабораторной работы

Выполняю перезапуск веб-сервера Apache. Произошёл сбой



Выполнение лабораторной работы

Просмотрите файлы `/var/log/httpd/error_log`, `/var/log/httpd/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи. Запись появилась в файле `error_log`

```
/var/log/httpd/error_log
[evdvorkina@evdvorkina ~]$ sudo cat /var/log/httpd/error_log
[Sat Apr 20 04:52:10.304359 2024] [core:notice] [pid 30093:tid 30093] SELinux
policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Apr 20 04:52:10.307330 2024] [suexec:notice] [pid 30093:tid 30093] AH0123
2: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using fe80::a00:27ff:fe98:bdea%enp0s3. Set the 'ServerName' directive
globally to suppress this message
[Sat Apr 20 04:52:10.371973 2024] [lbmethod_heartbeat:notice] [pid 30093:tid 3
0093] AH02282: No slotmem from mod_heartbeat
[Sat Apr 20 04:52:10.389422 2024] [mpm_event:notice] [pid 30093:tid 30093] AH0
0489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Apr 20 04:52:10.389524 2024] [core:notice] [pid 30093:tid 30093] AH00094:
Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Apr 20 05:09:47.974451 2024] [core:error] [pid 30136:tid 30312] (13)Permi
ssion denied: [client 127.0.0.1:44098] AH00035: access to /test.html denied (f
ilesystem path '/var/www/html/test.html') because search permissions are missi
ng on a component of the path
[Sat Apr 20 05:15:41.743945 2024] [core:error] [pid 30134:tid 30322] (13)Permi
ssion denied: [client 127.0.0.1:58006] AH00035: access to /test.html denied (f
ilesystem path '/var/www/html/test.html') because search permissions are missi
ng on a component of the path
```

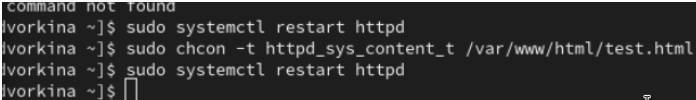
Выполнение лабораторной работы

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

```
[evdvorkina@evdvorkina ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[evdvorkina@evdvorkina ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[evdvorkina@evdvorkina ~]$ sudo 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
[evdvorkina@evdvorkina ~]$
```

Рис. 15: Проверка портов

Перезапускаю сервер Apache

A terminal window with a dark background and light-colored text. The text shows a sequence of commands and their outputs. The first line shows an error message. The subsequent lines show the user 'lvorkina' in the directory '~' executing 'sudo systemctl restart httpd', 'sudo chcon -t httpd_sys_content_t /var/www/html/test.html', and another 'sudo systemctl restart httpd'. The prompt returns to '~\$' after each command.

```
command not found
lvorkina ~]$ sudo systemctl restart httpd
lvorkina ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
lvorkina ~]$ sudo systemctl restart httpd
lvorkina ~]$
```

Рис. 16: Перезапуск сервера

Выполнение лабораторной работы

Теперь он работает, ведь мы внесли порт 81 в список портов `httpd_port_t`

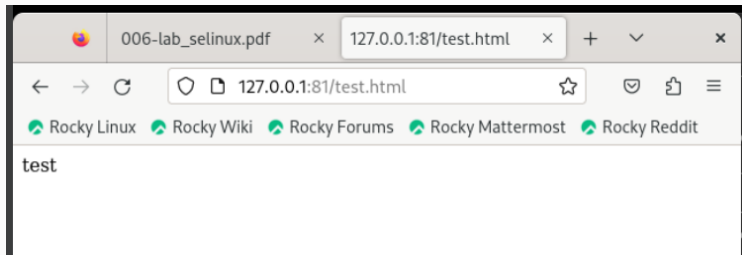


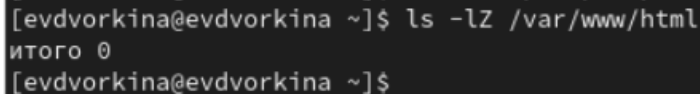
Рис. 17: Проверка сервера

Возвращаю в файле `/etc/httpd/httpd.conf` порт 80, вместо 81. Проверяю, что порт 81 удален, это правда.

```
[evdvorkina@evdvorkina ~]$ sudo nano /etc/httpd/conf/httpd.conf
[evdvorkina@evdvorkina ~]$ semanage port -d -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[evdvorkina@evdvorkina ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[evdvorkina@evdvorkina ~]$
```

Рис. 18: Проверка порта 81

Далее удаляю файл test.html, проверяю, что он удален

A terminal window with a dark background and light gray text. The prompt is [evdvorkina@evdvorkina ~]\$. The command ls -lZ /var/www/html is entered. The output shows a list of files and directories, followed by 'итого 0' (total 0). The prompt [evdvorkina@evdvorkina ~]\$ is shown again.

```
[evdvorkina@evdvorkina ~]$ ls -lZ /var/www/html
итого 0
[evdvorkina@evdvorkina ~]$
```

Рис. 19: 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.

...