

Лабораторная работа № 6

Мандатное разграничение прав в Linux

Аксёнова Алина Владимировна

Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Ход работы	8
Выводы	17
Библиографический список	18

List of Figures

0.1	Проверка режима и политики SELinux	8
0.2	Проверка статуса веб-сервера	9
0.3	Определение контекста безопасности	9
0.4	Состояние переключателей	10
0.5	Статистика по политике	10
0.6	Определяем типы	11
0.7	Создание html-файла	11
0.8	Проверка контекста файла	11
0.9	Обращение через веб-сервер	12
0.10	Тип файла	12
0.11	Изменение контекста	12
0.12	Повторный просмотр файла в браузере	12
0.13	Запуск веб-сервера	13
0.14	Анализ лог-файлов	14
0.15	Запуск веб-сервера	14
0.16	Доступ к файлу	15
0.17	Исправление конфигурационного файла	15
0.18	Удаление привезки и файла html	16

List of Tables

Цель работы

Развить навыки администрирования ОС Linux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Задание

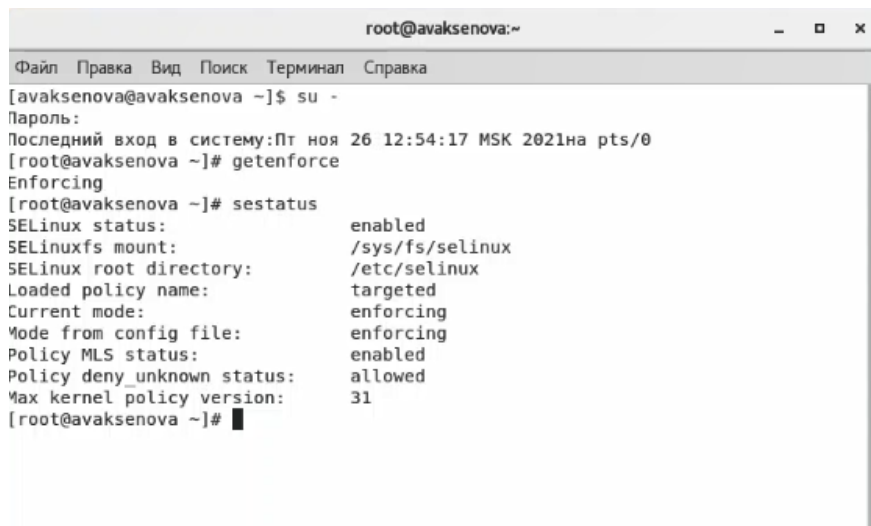
Получить первое практическое знакомство с технологией SELinux

Теоретическое введение

Для разграничения доступа субъектов — программ к объектам — файлам дерева каталогов используют так называемый мандатный (от англ, mandatory — обязательный или принудительный) подход (MAC, mandatory access control), предполагающий следование обязательным правилам доступа к файлам, назначаемым администраторами системы. Правила доступа строятся на основе знания о внутреннем устройстве программ и представляют собой описание набора минимально необходимых условий их целевого функционирования. Таким образом, в мандатных правилах, ограничивающих доступ к SSH-ключам пользователя, только программе ssh должен быть разрешен доступ для непосредственного выполнения своих прямых функций, а программам firefox и skype в доступе к SSH-ключам должно быть отказано.

Ход работы

1. Входим в систему и убеждаемся, что SELinux работает в режиме enforcing политики targeted. (Рис. 0.1).

A screenshot of a terminal window titled 'root@avaksenova:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the following commands and output:

```
[avaksenova@avaksenova ~]$ su -
Пароль:
Последний вход в систему: Пт ноя 26 12:54:17 MSK 2021 на pts/0
[root@avaksenova ~]# getenforce
Enforcing
[root@avaksenova ~]# 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
Max kernel policy version:     31
[root@avaksenova ~]#
```

Figure 0.1: Проверка режима и политики SELinux

2. Проверяем работу веб-сервера. (Рис. 0.2).


```
root@avaksenova:~  
Файл Правка Вид Поиск Терминал Справка  
[root@avaksenova ~]# 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; vendor preset  
: disabled)  
   Active: active (running) since Пт 2021-11-26 15:43:59 MSK; 15min ago  
     Docs: man:httpd(8)  
           man:apachectl(8)  
  Main PID: 1164 (httpd)  
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/s  
ec"  
    Tasks: 6  
   CGroup: /system.slice/httpd.service  
           └─1164 /usr/sbin/httpd -DFOREGROUND  
             └─1263 /usr/sbin/httpd -DFOREGROUND  
               └─1264 /usr/sbin/httpd -DFOREGROUND  
                 └─1265 /usr/sbin/httpd -DFOREGROUND  
                   └─1266 /usr/sbin/httpd -DFOREGROUND  
                     └─1267 /usr/sbin/httpd -DFOREGROUND  
  
ноя 26 15:43:56 avaksenova.localdomain systemd[1]: Starting The Apache HTT...  
ноя 26 15:43:59 avaksenova.localdomain systemd[1]: Started The Apache HTTP...  
Hint: Some lines were ellipsized, use -l to show in full.  
[root@avaksenova ~]#
```

Figure 0.2: Проверка статуса веб-сервера

3. Определяем контекст безопасности веб-сервера.(Рис. 0.3).

```
[root@avaksenova ~]# ps -eZ | grep httpd  
system_u:system_r:httpd_t:s0 1164 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 1263 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 1264 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 1265 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 1266 ? 00:00:00 httpd  
system_u:system_r:httpd_t:s0 1267 ? 00:00:00 httpd
```

Figure 0.3: Определение контекста безопасности

4. Теперь посмотрим текущее состояние SELinux переключателей. Как можно заметить, практически все переключатели выключены. (Рис. 0.4).

```
Without options, show SELinux status.
[root@avaksenova ~]# 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_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avaahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
```

Figure 0.4: Состояние переключателей

5. Посмотрели статистику по политике. Кроме того, определили множество пользователей, ролей, типов (Рис. 0.5).

```
[root@avaksenova ~]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1       Categories:       1024
Types:            4793     Attributes:        253
Users:            8       Roles:            14
Booleans:         316     Cond. Expr.:      362
Allow:            107834   Neverallow:        0
Auditallow:       158     Dontaudit:         10022
Type_trans:       18153   Type_change:       74
Type_member:      35      Role_allow:        37
Role_trans:       414     Range_trans:       5899
Constraints:      143     Validatetrans:     0
Initial SIDs:     27      Fs_use:            32
Genfscon:         103     Portcon:           614
Netifcon:         0       Nodecon:           0
Permissives:      0       Polcap:            5
```

Figure 0.5: Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории `/var/www`. Тип файлов, находящихся в директории `/var/www/html`, определить не удалось, т.к. директория не содержит файлов. Кроме того, определили круг пользователей, которым разрешено создание файлов в данной директории. Оказалось, что только суперпользователь имеет такое право. (Рис. 0.6).

```

[root@avaksenova ~]# ls -lZ /var/www
lrwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
lrwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@avaksenova ~]# ls -lZ /var/www/html

```

Figure 0.6: Определяем типы

7. Создали от имени суперпользователя html-файл. (Рис. 0.7).



Figure 0.7: Создание html-файла

8. Проверили контекст созданного файла и обратились к файлу через веб-сервер (Рис. 0.8, -fig. 0.9)].

Figure 0.8: Проверка контекста файла

Figure 0.8: Проверка контекста файла

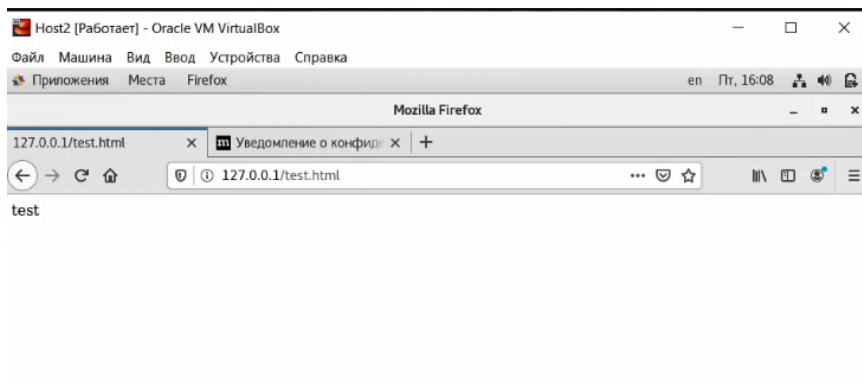


Figure 0.9: Обращение через веб-сервер

9. Изучили справку `man httpd_sys_content_t` и сопоставили их с типом файла `test`. (Рис. 0.10).

```
httpd_sys_content_t
- Set files with the httpd_sys_content_t type, if you want to treat the files as httpd sys content.
```

Figure 0.10: Тип файла

10. Изменили контекст файла на `samba_share_t` и проверили, что контекст поменялся. После этого в браузере получили сообщение об ошибке. Это произошло, поскольку SELinux запретил доступ к файлу (Рис. 0.11, 0.12).

```
[root@avaksenova ~]# chcon -t samba_share_t /var/www/html/test.html
[root@avaksenova ~]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 0.11: Изменение контекста

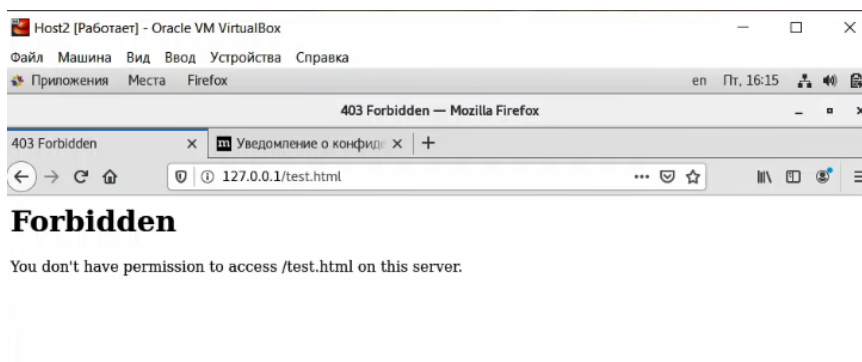
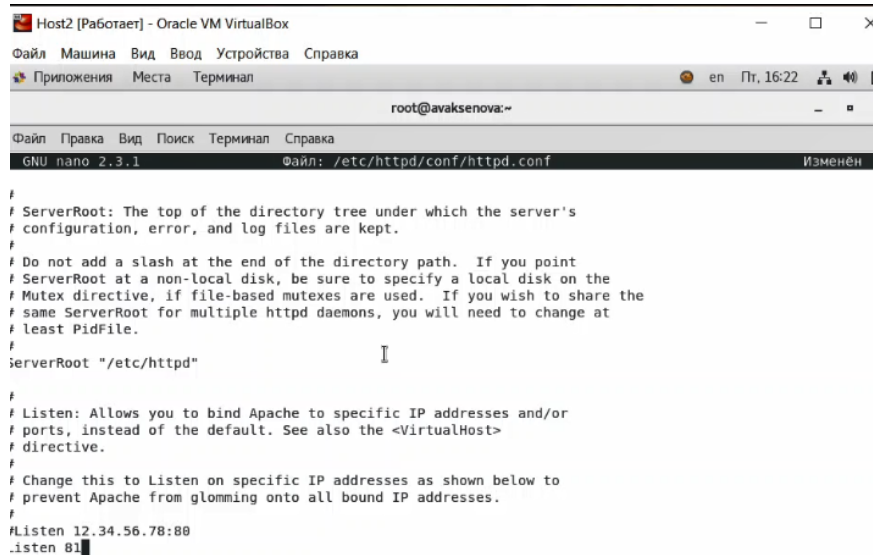


Figure 0.12: Повторный просмотр файла в браузере

11. Запустили веб-сервер Apache на прослушивание TCP-порта 81. После чего перезапустили веб-сервер и проанализировали log-файлы. Также проверили список портов (Рис. 0.13, 0.14).



```
Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал
root@avaksenova:~
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.3.1 Файл: /etc/httpd/conf/httpd.conf Изменён

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
Listen 12.34.56.78:80
Listen 81
```

Figure 0.13: Запуск веб-сервера

```

Redirecting to /bin/systemctl restart httpd.service
[root@avaksenova ~]# 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; vendor
   Active: active (running) since Пт 2021-11-26 16:22:34 MSK; 19s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 4601 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=
 Main PID: 4605 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─4605 /usr/sbin/httpd -DFOREGROUND
              └─4606 /usr/sbin/httpd -DFOREGROUND
                └─4607 /usr/sbin/httpd -DFOREGROUND
                  └─4608 /usr/sbin/httpd -DFOREGROUND
                    └─4609 /usr/sbin/httpd -DFOREGROUND
                      └─4610 /usr/sbin/httpd -DFOREGROUND

ноя 26 16:22:33 avaksenova.localdomain systemd[1]: Starting The Apache HTTP
ноя 26 16:22:34 avaksenova.localdomain systemd[1]: Started The Apache HTTP
[root@avaksenova ~]# tail -nl /var/log/messages
tail: l: неверное число строк
[root@avaksenova ~]# tail -nl /var/log/messages
Nov 26 16:22:34 avaksenova systemd: Started The Apache HTTP Server.
[root@avaksenova ~]# /var/log/http/error_log
-bash: /var/log/http/error_log: Нет такого файла или каталога
[root@avaksenova ~]# nano /var/log/http/error_log
[root@avaksenova ~]# nano /var/log/http/access_log
[root@avaksenova ~]# nano /var/log/audit/audit.log
[root@avaksenova ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,
                ermissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@avaksenova ~]# emanage port -l | grep http_port_t
bash: emanage: команда не найдена...
[root@avaksenova ~]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443
pegasus_http_port_t tcp      5988
[root@avaksenova ~]#

```

Figure 0.14: Анализ лог-файлов

12. Снова запустили веб-сервер Apache и вернули контекст `httpd_sys_content__t` к файлу, а затем попробовали получить доступ к файлу через браузер. В результате увидели содержимое файла (Рис. 0.15, 0.16).

```

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

```

Figure 0.15: Запуск веб-сервера

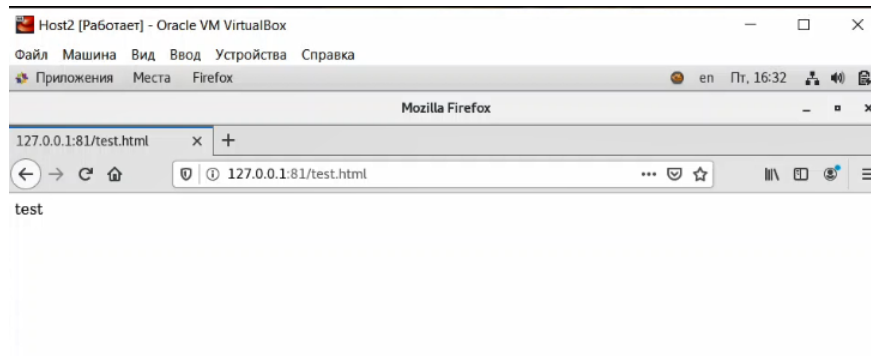


Figure 0.16: Доступ к файлу

13. Исправили обратно конфигурационный файл apache, вернув Listen 80 и попытались удалить привязку `http_port_t` к 81 порту. Вылезла ошибка, поскольку порт 81 определен на уровне политики. После этого удилили html-файл (Рис. 0.17, 0.18).

```
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot to 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
```

Figure 0.17: Исправление конфигурационного файла

```
[root@avaksenova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@avaksenova ~]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@avaksenova ~]#
```

Figure 0.18: Удаление привезки и файла html

Выводы

В результате выполнения данной работы была изучена технология SELinux, а также проверена работа SELinux с веб-сервером Apache.

Библиографический список

- [illegible]