

Презентация по лабораторной работе №6

Коновалова Татьяна Борисовна

9 Октября 2023

РУДН, Москва, Россия

Презентация по лабораторной работы №6

Мандатное разграничение прав в Linux

Цель лабораторной работы

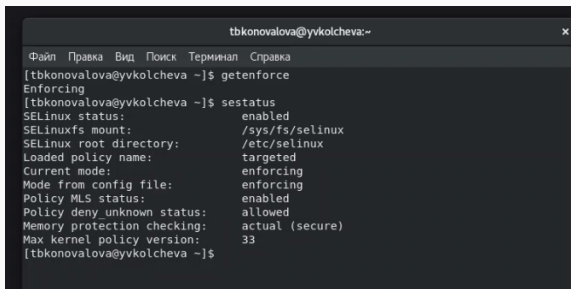
- Получить практические навыки администрирования
- Ознакомиться с технологией SELinux

Задачи лабораторной работы

- Найти веб-сервер Apache в списке процессов, определить его контекст безопасности и занести эту информацию в отчёт.
- Посмотреть текущее состояние переключателей SELinux для Apache;
- Изучить справку `man httpd_selinux`

Ход лабораторной работы

С помощью команд `getenforce` и `sestatus` убедилась, что SELinux работает в режиме enforcing политики targeted



```
tbkonovalova@yvkolcheva:~  
Файл Правка Вид Поиск Терминал Справка  
[tbkonovalova@yvkolcheva ~]$ getenforce  
Enforcing  
[tbkonovalova@yvkolcheva ~]$ 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  
[tbkonovalova@yvkolcheva ~]$
```

Рис. 1: `getenforce` и `sestatus`

Веб-сервер Apache

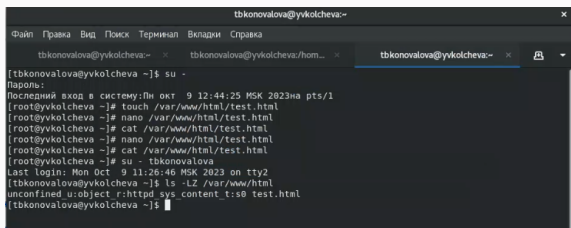
Проверила работу веб-сервера Apache командой `sevrice httpd status`.

```
Выполнено!  
[root@yvkolcheva tbkonovalova]# systemctl start httpd  
[root@yvkolcheva tbkonovalova]# 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: disabled)  
   Active: active (running) since Mon 2023-10-09 12:46:28 MSK; 5s ago  
     Docs: man:httpd.service(8)  
  Main PID: 16417 (httpd)  
    Status: "Started, listening on: port 80"  
    Tasks: 213 (limit: 11025)  
   Memory: 20.7M  
    CGroup: /system.slice/httpd.service  
            └─16417 /usr/sbin/httpd -DFOREGROUND  
              └─21577 /usr/sbin/httpd -DFOREGROUND  
                └─21578 /usr/sbin/httpd -DFOREGROUND  
                  └─21579 /usr/sbin/httpd -DFOREGROUND  
                    └─21580 /usr/sbin/httpd -DFOREGROUND  
  
окт 09 12:46:22 yvkolcheva.myquest.virtualbox.org systemd[1]: Starting The Apache HTTP Server...  
окт 09 12:46:28 yvkolcheva.myquest.virtualbox.org systemd[1]: Started The Apache HTTP Server...  
окт 09 12:46:31 yvkolcheva.myquest.virtualbox.org httpd[16417]: Server configured, listening on: port 80  
lines 1-18/18 (END)
```

Рис. 2: Проверка работы сервера

Создание основного файла

Создала файл /var/www/html/test.html от имени суперпользователя



```
tbkonovalova@yvkolcheva:~  
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка  
tbkonovalova@yvkolcheva:~  tbkonovalova@yvkolcheva:/hom...  tbkonovalova@yvkolcheva:~  
[tbkonovalova@yvkolcheva ~]$ su -  
Пароль:  
Последний вход в систему: Пн окт  9 12:44:25 MSK 2023 на pts/1  
[root@yvkolcheva ~]# touch /var/www/html/test.html  
[root@yvkolcheva ~]# nano /var/www/html/test.html  
[root@yvkolcheva ~]# cat /var/www/html/test.html  
[root@yvkolcheva ~]# nano /var/www/html/test.html  
[root@yvkolcheva ~]# cat /var/www/html/test.html  
[root@yvkolcheva ~]# su - tbkonovalova  
Last login: Mon Oct  9 11:26:46 MSK 2023 on tty2  
tbkonovalova@yvkolcheva ~]$ ls -LZ /var/www/html  
unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[tbkonovalova@yvkolcheva ~]$
```

Рис. 3: Файл test.html

Просмотр файла в веб-браузере

Просмотрела созданный файл в веб-браузере, открыв ссылку 127.0.0.1/test.html.

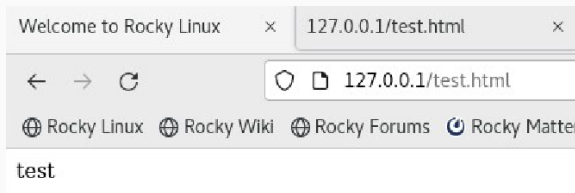


Рис. 4: Обращение к файлу через веб-сервер

Изменила контекст файла test.html командой chcon.

```
[tbkonovalova@yvkolcheva ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[tbkonovalova@yvkolcheva ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted
[tbkonovalova@yvkolcheva ~]$ su
Password:
[root@yvkolcheva tbkonovalova]# chcon -t samba_share_t /var/www/html/test.html
[root@yvkolcheva tbkonovalova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yvkolcheva tbkonovalova]#
```

Рис. 5: Изменение контекста файла

Перезагрузила страницу в веб-браузере. Теперь я получила ошибку доступа.

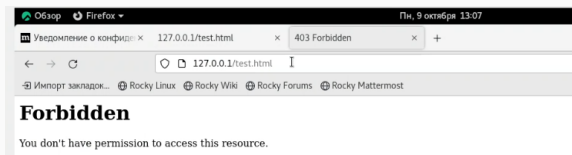
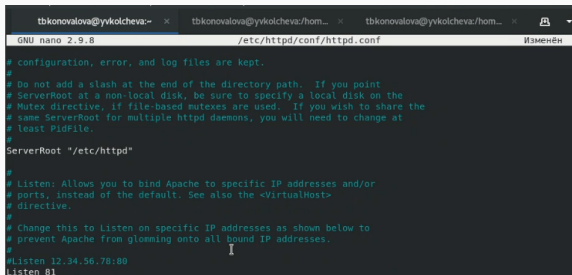


Рис. 6: Ошибка доступа при открытии файла через веб-сервер

Смена порта

В конфигурационном файле поменяла порт, через который происходит прослушивание. Для этого изменила строку “Listen”.



```
tbkonovalova@yvkolcheva:~ x tbkonovalova@yvkolcheva:/hom... x tbkonovalova@yvkolcheva:/hom... x Изменён
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf

# 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
```

Рис. 7: Прослушивание 81 порта

Установила порт и посмотрела список доступных можно с помощью команды `semanage`.

```
[root@yvkolcheva tbkonovalova]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 уже определен
[root@yvkolcheva tbkonovalova]# semanage -l | grep http_port_t
semanage: error: the following arguments are required: subcommand
[root@yvkolcheva tbkonovalova]# 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@yvkolcheva tbkonovalova]# systemctl restart httpd
[root@yvkolcheva tbkonovalova]#
```

Рис. 8: Установка порта

Повторный просмотр в веб-браузере

Просмотрела файл test.html в веб-браузере, открыв ссылку 127.0.0.1:81/test.html.

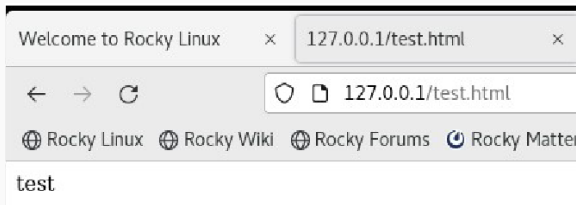


Рис. 9: Повторный просмотр файла в веб-браузере

Получила практические навыки администрирования в ОС Linux и ознакомилась с технологией SELinux совместно с веб-сервером Apache.

СПИСОК ЛИТЕРАТУРЫ

1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>

2.Теоретические знания, приведённые в Лабораторной работе №6 -

https://esystem.rudn.ru/pluginfile.php/2090131/mod_resource/content/1/lab_selinux.pdf

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

1.[Электронный ресурс] - доступ:

<https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>

Спасибо за внимание!