Лабораторная работа №6

Мандатное разграничение прав в Linux

Афтаева К.В.

14 октября 2023

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Афтаева Ксения Васильевна
- студент группы НПИбд-01-20
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032201739@pfur.ru
- https://github.com/KVAftaeva/study_2023-2024_infosec

Вводная часть

Актуальность

- Система прав доступа к файлам является одной из самых важных в операционной системе Linux

Объект и предмет исследования

- ОС Linux
- технология SELinux

Цели и задачи

1. Подготовить лабораторный стенд
2. Ознакомиться с технологией SELinux
3. Выполнить задания по работе с SELinux совместно с веб-сервером Apache

Материалы и методы

- Технология SELinux

Выполнение работы

Подготовка лабораторного стенда

```
Installed:
  grub2-tools-efi-1:2.06-61.el9_2.1.rocky.0.2.x86_64       grub2-tools-extra-1:2.06-61.el9_2.1.rocky.0.2.x86_64
  kernel-5.14.0-284.30.1.el9_2.x86_64                      kernel-core-5.14.0-284.30.1.el9_2.x86_64
  kernel-devel-5.14.0-284.30.1.el9_2.x86_64                kernel-modules-5.14.0-284.30.1.el9_2.x86_64
  kernel-modules-core-5.14.0-284.30.1.el9_2.x86_64

Complete!
[root@kvaftaeva ~]# yum install httpd
Last metadata expiration check: 0:00:43 ago on Thu 12 Oct 2023 01:04:29 PM MSK.
Dependencies resolved.
================================================================================================================
 Package                    Architecture         Version                        Repository               Size
================================================================================================================
Installing:
 httpd                      x86_64               2.4.53-11.el9_2.5              appstream                47 k
Installing dependencies:
 apr                        x86_64               1.7.0-11.el9                   appstream               123 k
```

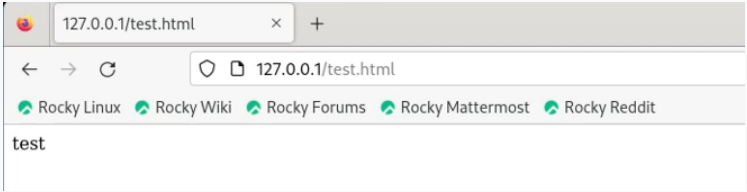
```
[root@kvaftaeva ~]# nano /etc/httpd/conf/httpd.conf
[root@kvaftaeva ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@kvaftaeva ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@kvaftaeva ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@kvaftaeva ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@kvaftaeva ~]#
```

Режим и политика SELinux

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

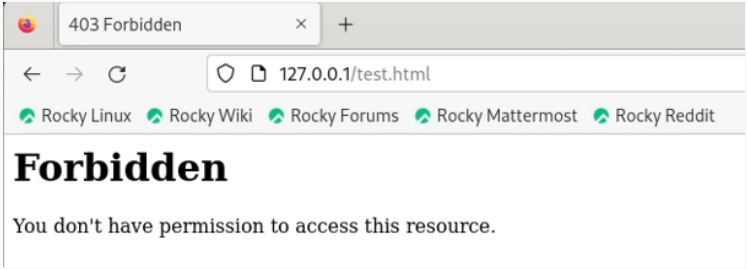
Доступ к файлу через веб-сервер

```
[kvaftaeva@kvaftaeva ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 12 13:28 test.html
[kvaftaeva@kvaftaeva ~]$
```



Отсутствие доступа к файлу через веб-сервер

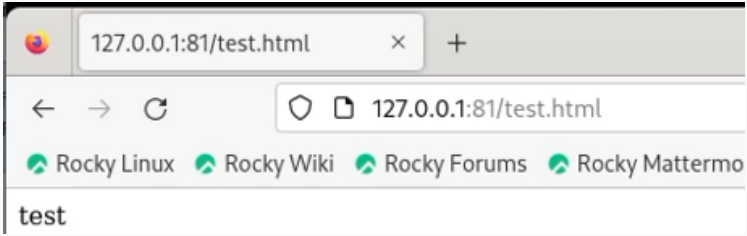
```
[root@kvaftaeva ~]# chcon -t samba_share_t /var/www/html/test.html
[root@kvaftaeva ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@kvaftaeva ~]#
```



Смена порта

```
#Listen 12.34.56.78:80
Listen 81
```

```
[root@kvaftaeva ~]# 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@kvaftaeva ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@kvaftaeva ~]# 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 Thu 2023-10-12 14:11:36 MSK; 12s ago
       Docs: man:httpd.service(8)
   Main PID: 102296 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
```



Удаление файла

```
[root@kvaftaeva ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@kvaftaeva ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@kvaftaeva ~]# ls /var/www/html
[root@kvaftaeva ~]#
```

Результаты

Результат

1. Изучена технология SELinux
2. Проверена работа SELinx на практике совместно с веб-сервером Apache

Вывод

Вывод

Я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.