

Знакомство с SELinux

Турсунов Баходурхон Азимджонович

15 октября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

SELinux или Security Enhanced Linux — это улучшенный механизм управления доступом, разработанный Агентством национальной безопасности США (АНБ США) для предотвращения злонамеренных вторжений. Он реализует принудительную (или мандатную) модель управления доступом (англ. Mandatory Access Control, MAC) поверх существующей дискреционной (или избирательной) модели (англ. Discretionary Access Control, DAC), то есть разрешений на чтение, запись, выполнение.

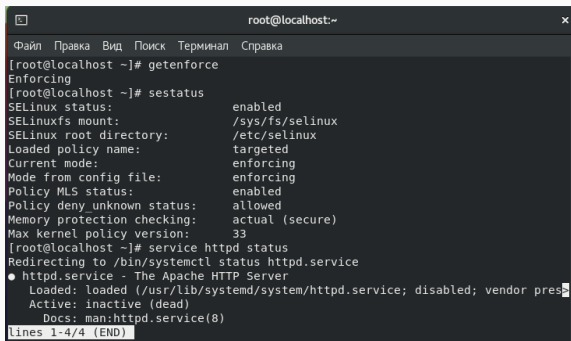
Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

Цель лабораторной работы

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

Выполнение лабораторной работы

Запуск HTTP-сервера



```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[root@localhost ~]# getenforce  
Enforcing  
[root@localhost ~]# 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  
[root@localhost ~]# 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: enabled)  
   Active: inactive (dead)  
   Docs: man:httpd.service(8)  
lines 1-4/4 (END)
```

Figure 1: запуск http

Создание HTML-файла



Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

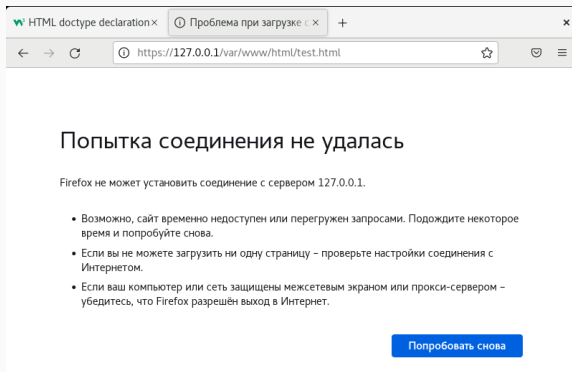


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста без-опасности

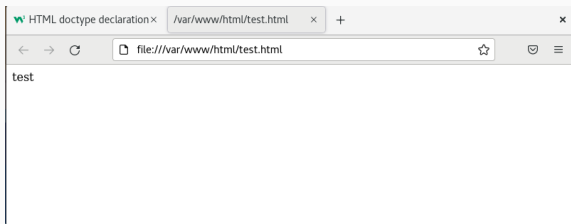


Figure 4: открытие с помощью Chrome

Выводы

Результаты выполнения лабораторной работы

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией SELinux.