Презентация по лабораторной работе №6

Основы информационной безопасности

Чувакина М. В.

28 апреля 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Чувакина Мария Владимировна
- студентка группы НКАбд-03-23
- Российский университет дружбы народов
- 1132236055@rudn.ru
- https://mvchuvakina.github.io/ru/

Цель

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx 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

проверка режима работы SELinux

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`

Проверка работы Apache

Рис. 2: Проверка работы Apache

Выполнение лабораторной работы

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

Контекст безопасности Apache

Рис. 3: Контекст безопасности Apache

Выполнение лабораторной работы

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

Состояние переключателей SELinux

Рис. 4: Состояние переключателей SELinux

Выполнение лабораторной работы

Просмотрела статистику по политике с помощью команды `seinfo`. Множество пользователей - 8, ролей - 39, типов - 5135.

Выполнение лабораторной работы

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

Выполнение лабораторной работы

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

Выполнение лабораторной работы

Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t

Выполнение лабораторной работы

Обращаюсь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён

Выполнение лабораторной работы

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

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.

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.

Выполнение лабораторной работы

Выполняю перезапуск веб-сервера Apache. Произошёл сбой

Выполнение лабораторной работы

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

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

Выполнение лабораторной работы

Перезапускаю сервер Apache

Выполнение лабораторной работы

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

Выполнение лабораторной работы

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

Выполнение лабораторной работы

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

Вывод

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.

:::