Отчет по лабораторной работе №6

Астафьева Анна Андреевна НПИбд-01-18[1]

Информационная Безопасность–2021, 27 ноября, 2021, Москва, Россия

[1]Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

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

Задание к лабораторной работе

Лабораторная работа подразумевает выполнение последовательно необходимых действий, чтобы развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Процесс выполнения лабораторной работы

Процесс выполнения

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus
2. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что веб-сервер работает.
3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности.

Процесс выполнения

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -bigrep httpd. Обратила внимание, что многие из них находятся в положении «off».

5. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей(8), ролей(14), типов(4793). Определила тип файлов и поддиректорий, находящихся в директории /var/www. Определила тип файлов, находящихся в директории /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.

Процесс выполнения

6. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html.
7. Проверила контекст созданного файла. httpd_sys_content_t.
8. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён.
9. Проверила контекст файла.

Процесс выполнения

10. Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t.

11. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение об ошибке.

12. Проанализировала ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл.

Процесс выполнения

13. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и замените её на Listen 81.

14. Проанализиировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log.

15. Выполнила команду: semanage port -a -t http_port_t -p tcp 81. После этого проверила список портов командой: semanage port -l | grep http_port_t. Убедилась, что порт 81 появился в списке.

Процесс выполнения

16. Вернула контекст httpd_sys_content__t к файлу /var/www/html/test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Увидела содержимое файла — слово «test».
17. Исправила обратно конфигурационный файл apache, вернув Listen 80.
18. Удалила привязку http_port_t к 81 порту.
19. Удалила файл /var/www/html/test.html.

Выводы по проделанной работе

Вывод

На основе проделанной работы развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.