Лабораторная работа №6

Мандатное разграничение прав в Linux

Петрова Мария Евгеньевна

Содержание

Цель работы 1
Теоретическое введение 1
Выполнение лабораторной работы 1
Заключение 3
Библиографическая справка 3

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Теоретическое введение

Мандатное управление доступом (Mandatory Access Control, MAC) предназначено для обеспечения большего уровня безопасности и контроля над доступом к ресурсам системы.

Мандатное разграничение доступа применяется в совокупности с дискреционным разграничением доступа. Оно определяет правила доступа на основе атрибутов объектов и субъектов, которые затем при проверке определяют разрешен ли доступ. Объект в данной модели – это то, над чем совершаются какие-либо действия, а субъект – исполнитель этого действия. Значение уровня доступа субъекта или объекта называется меткой. Метка может быть символьной или числовой. Проверка полномочий определяется при помощи сопоставления меток объекта и субъекта. Пользователи системы не могут самостоятельно определять доступ субъектов к объектам. Управление доступом субъектов к объектам осуществляют только администраторы[1].

Выполнение лабораторной работы

Перед выполнением лабораторной работы подготовим рабочее пространство и скачаем httpd

1. В конфигурационном файле задаем ServerName и отключаем пакетный фильтр

2. Войдем в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted
3. Обратимся с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает

3. Найдем веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт

4. Посмотрим текущее состояние переключателей SELinux для Apache
6. Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
7. Определимтип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html

8. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. Создадим от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html.
10. Проверим контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html

11. Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён

12. Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd

13. Измените 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.

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл.

16. Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81.
17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?
18. Проанализируйте лог-файлы.

19. Выполните команду semanage port -a -t http_port_t -p tcp 81. После этого проверьте список портов. Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache ещё раз.

21. Верните контекст httpd_sys_content__t к файлу /var/www/html/ test.html: chcon -t httpd_sys_content_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test»

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
23. Удалите привязку http_port_t к 81 порту и проверьте, что порт 81 удалён.

24. Удалите файл /var/www/html/test.html

Заключение

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Библиографическая справка

[1] Мандатное управление: https://itcloud-edu.ru/info/articles/upravlenie-dostupom-v-gnu-linux/