Мандатное разграничение прав в Linux

Максимова Ксения НБИбд-02-18[1]

24 ноября, 2021, Москва, Россия

[1]Российский Университет Дружбы Народов

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.

Введение

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена.

Основные понятия

1.Домен — это некоторый набор действий, которые может производить один процесс. Главным образом это действия, необходимые процессу для выполнения определенной задачи.

2. Роль — это совокупность нескольких доменов.

3. Контекст безопасности — это совокупность всех атрибутов, которые связаны с объектами и субъектами.

4. Политика безопасности — это набор заданных правил, который регулирует взаимодействие ролей, доменов.

Способы работы

-Enforcing: SELinux запрещает доступ на основе правил политики SELinux, набора руководящих принципов, которые управляют механизмом безопасности.
-Permissive: SELinux не запрещает доступ, но в журнале регистрируются отказы для действий, которые были бы запрещены при запуске в принудительном режиме.
- Disabled: Полное отключение системы принудительного контроля доступа

Модели управления доступом

1.Type Enforcement (TE): основной механизм контроля доступа, используемый в целевых политиках. Позволяет детально, на самом низком уровне управлять разрешениями. Самый гибкий, но и самый трудоемкий для системного администратора механизм.
2.Role-Based Access Control (RBAC): в этой модели права доступа реализуются в качестве ролей. Ролью называется разрешения на выполнение определенных действий одним или несколькими элементами системы над другими частями системы. По-сути, RBAC является дальнейшим развитием TE.
3.Multi-Level Security (MLS): многоуровневая модель безопасности, в которой всем объектам системы присваивается определенный уровень доступа. Разрешение или запрет доступа определяется только соотношением этих уровней.

Результат лабораторной работы

Получены практические навыки администрирования ОС Linux, а так же получено практическое знакомство с технологией SELinux совместно с веб-сервером Apache.