Лабораторная работа №5

Информационная безопасность

Волчок Кристина Александровна НПМбд-02-21

29 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Волчок Кристина Александровна, студентка кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- [1032215007@rudn.ru]

Вводная часть

Вводная часть

Лабораторная работа посвящена изучению механизмов дискреционного разграничения прав в операционной системе Linux. Основное внимание уделяется SetUID-, SetGID- и Sticky-битам, а также практике применения этих атрибутов для управления правами доступа в многопользовательской системе.

Актуальность

Вопросы безопасности доступа к системным ресурсам становятся всё более важными в современных информационных системах. Дискреционные механизмы разграничения прав, такие как SetUID и Sticky-биты, обеспечивают гибкое управление правами пользователей, что критически важно для предотвращения несанкционированного доступа и обеспечения целостности данных.

Объект и предмет исследования

Объектом исследования является файловая система Linux, а предметом - механизмы разграничения прав доступа с использованием SetUID-, SetGID- и Sticky-битов. Также рассматриваются вопросы взаимодействия пользователя с системой на уровне прав доступа, а именно использование дополнительных атрибутов безопасности.

Цели и задачи

Целью работы является изучение механизмов изменения идентификаторов пользователей и применения специальных битов безопасности для управления доступом к файлам и процессам. Задачи включают настройку атрибутов доступа, компиляцию программ на языке C, установку и тестирование SetUID и Sticky-битов.

Материалы и методы

Для выполнения лабораторной работы использовались стандартные утилиты Linux, такие как gcc для компиляции программ и команды chmod и chown для изменения атрибутов файлов. Применялись методы практического взаимодействия с системой, включая создание и выполнение программ на языке C, что позволило наглядно изучить работу SetUID и Sticky-битов.

Результаты

Результаты

В ходе лабораторной работы были исследованы различные сценарии установки и применения SetUID, SetGID и Sticky-битов. Было установлено, что эти атрибуты позволяют эффективно контролировать права доступа к файлам и процессам, предотвращая нежелательные действия пользователей. Sticky-бит был особенно полезен в контексте защиты общих директорий, таких как /tmp, обеспечивая ограничение на удаление файлов для пользователей, не являющихся их владельцами.

Итоговый слайд

Безопасность системы– это контроль и осознанное управление доступом.”

Главное: Дискреционные механизмы управления правами в Linux, такие как SetUID и Sticky-биты, – это мощные инструменты обеспечения безопасности. Их грамотное применение позволяет эффективно защитить систему от несанкционированного доступа и манипуляции данными.