Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По Учебной практике №4**

Студент: Рачков Дмитрий Сергеевич

Дисциплина/Профессиональный модуль: УЧ ПР ОС

Выполнил студент

Группы: 2ОИБАС-1222

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2024г.**

**Практическая работа №4**

**«Мандатный контроль целостности в Astra Linux 1.6 / Расщепление root / информационная безопасность»**

**Цель работы:** законспектировать видеофайл.

**Мандатный контроль целостности**

Мандатный контроль целостности - это процесс проверки целостности данных, который осуществляется на основе прав доступа и прав пользователей к информационной системе. Этот вид контроля обеспечивает защиту данных от несанкционированных изменений, разрушений или копирования.

В рамках мандатного контроля целостности устанавливаются и проверяются правила и ограничения доступа для пользователей и приложений. Система контроля целостности проверяет, что данные не были изменены или повреждены без разрешения, и что только уполномоченные пользователи имеют доступ к определенным данным.

Этот вид контроля является важной частью обеспечения безопасности данных и обеспечивает сохранность информации от угроз как внутри, так и за пределами организации. Важно поддерживать мандатный контроль целостности в актуальном состоянии и регулярно анализировать его эффективность для обеспечения безопасности информационной системы.

В Astra Linux 1.6 мандатный контроль целостности может быть реализован с помощью механизма SE Linux (Security Enhanced Linux), который позволяет определить правила доступа к ресурсам системы на основе меток безопасности.

**Дискреционное ограничение доступа**

В Astra Linux используется дискреционное ограничение доступа, которое регулирует доступ пользователей к файлам.

Недостатки этого механизма: не позволяет управлять информационными потоками и контролировать утечку данных.

Дискреционное ограничение доступа - это метод управления доступом к ресурсам информационной системы, основанный на предоставлении пользователю контроля над своими собственными данными и ресурсами. Сущность дискреционного ограничения доступа заключается в том, что владелец или создатель данных определяет, кому и какие права доступа предоставляются к собственной информации.

Основные принципы дискреционного ограничения доступа:

1. Владелец информации имеет право определять, кто и как может получить доступ к его данным.

2. Пользователь, который обладает правами доступа, может делиться своими данными или ресурсами с другими пользователями в соответствии с заданными правами.

3. Дискреционное ограничение доступа основывается на концепции "need-to-know" (необходимо знать), что означает, что пользователь получает доступ только к информации, необходимой для выполнения своих обязанностей или задач.

Примером дискреционного ограничения доступа являются системы управления правами доступа (Access Control Lists - ACL), где владелец информации может устанавливать список пользователей или групп пользователей с различными уровнями доступа к файлам или папкам.

Дискреционное ограничение доступа является одним из основных методов обеспечения безопасности данных в информационных системах и позволяет управлять доступом к информации на уровне индивидуальных пользователей.

**Мандатное управление доступом**

Мандатное управление доступом работает по уровням конфиденциальности и категориям.

Реализовано в Astra Linux с помощью подсистемы безопасности Parsec.

В Astra Linux 1.6 мандатное управление доступом реализуется с помощью механизма Security Enhanced Linux (SE Linux). SE Linux предоставляет возможность добавления дополнительного уровня обеспечения безопасности, который работает на основе меток безопасности.

SE Linux позволяет администраторам системы определить политики безопасности для контроля доступа к ресурсам системы, таким как файлы, каталоги, процессы и сетевые соединения. При этом SE Linux дополнительно к основным правам доступа (режим DAC - discretionary access control) использует мандатный контроль доступа (MAC - mandatory access control), который принуждает процессы к выполнению определенных правил безопасности.

Администратор Astra Linux может настроить уровень безопасности SE Linux в соответствии с требованиями безопасности своей системы, определяя разрешенные и запрещенные действия для различных сущностей в системе. SE Linux позволяет усилить защиту от атак, включая привилегированные угрозы, эксплойты и распространение вредоносного программного обеспечения.

Для работы с мандатным управлением доступом в Astra Linux 1.6 необходимо иметь соответствующие знания по настройке SE Linux и опыт в администрировании системы.

**Примеры работы мандатного контроля целостности**

В видео демонстрируется, как работает мандатный контроль целостности на примере процессов с разными уровнями целостности.

В Linux, если взламывают иксорга и получают привилегии рута, то в Windows это не получится, так как процессы с низким уровнем целостности не могут влиять на процессы с высоким уровнем.

**Мандатный контроль целостности**

В системе действует мандатный контроль целостности, но он не применяется к файлам.

Для включения мандатного контроля целостности необходимо зайти в панель управления и включить защиту файловой системы.

**Защита файловой системы**

После включения защиты файловой системы, все файлы получают максимальный уровень контроля целостности.

Если пользователь пытается изменить файл с высоким уровнем контроля целостности, ему будет отказано в доступе.

**Мониторинг и защита от эксплоитов**

Монитор Parsec отслеживает действия пользователей с низким уровнем мандатного контроля целостности и при обнаружении создания или запуска процесса с высоким уровнем, он его прибивает.

Это усложняет эксплуатацию уязвимостей и повышает уровень безопасности системы.