Введение

Повышение уровня безопасности в Linux достигается за счет устранения рисков, связанных с настройками по умолчанию. К ним относятся излишние права доступа для домашнего каталога, потенциально опасный удаленный вход для суперпользователя и отсутствие контроля над сетевыми подключениями.

Данное руководство предлагает три конкретных действия для формирования базовой политики безопасности:

1. Защита домашнего каталога путем изменения прав доступа.
2. Запрет входа по SSH под учетной записью root.
3. Установка и настройка брандмауэра для фильтрации входящего и исходящего трафика.

Выполнение этих шагов позволит создать надежный фундамент для защиты вашей системы и данных.

1. Защитите свой домашний каталог

По умолчанию ваш домашний каталог доступен другим пользователям системы. Это означает, что кто-то, войдя с гостевой учётной записью, может получить доступ к вашим личным файлам.

Чтобы сделать каталог доступным только вам, выполните в терминале команду, которая устанавливает права доступа, разрешающие полный доступ только владельцу (вам), блокируя просмотр содержимого для всех остальных. Пример представлен на рисунке 1.

Рисунок 1 – Защита домашнего каталога

2. Отключите вход по SSH от имени root

Разрешение на вход по SSH под учётной записью root представляет угрозу безопасности. Злоумышленник может подобрать простой пароль и получить полный контроль над системой. Рекомендуется отключить эту возможность.

Перед выполнением убедитесь, что на вашем компьютере установлен и запущен SSH-сервер. Если при попытке подключения вы получаете ошибку connection refused, значит, сервер не установлен, и этот шаг можно пропустить. Пример представлен на рисунке 2.

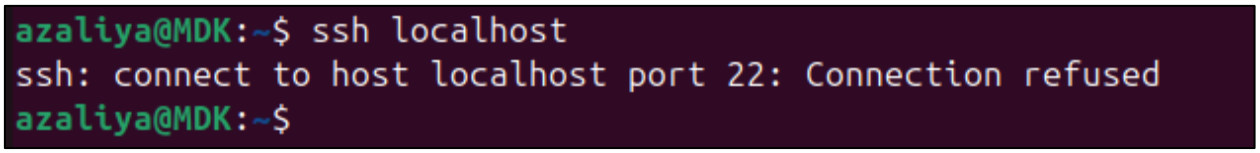

Рисунок 2 – Проверка SSH-сервера

3. Установите и настройте брандмауэр

Если на вашем компьютере запущены серверные службы (например, веб-сервер или база данных), брандмауэр предотвратит несанкционированные подключения к ним извне. Для Ubuntu рекомендуется использовать gufw, так как он разработан специально для этой системы.

Настройка:

1. Установите gufw. Пример представлен на рисунке 3.1.

```
azaliya@MDK:~$ sudo apt install gufw
[sudo] пароль для azaliya:
Чтение списков пакетов… Готово
Построение дерева зависимостей… Готово
Чтение информации о состоянии… Готово
Следующие НОВЫЕ пакеты будут установлены:
  gufw
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 80 пакетов
 не обновлено.
Необходимо скачать 944 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 3 748 kB.
Пол:1 http://ru.archive.ubuntu.com/ubuntu noble/universe amd64 gufw all 24.04.0-2 [944 kB]
Получено 944 kB за 1с (1 222 kB/s)
Выбор ранее не выбранного пакета gufw.
(Чтение базы данных … на данный момент установлено 150409 файлов и каталогов.)
Подготовка к распаковке …/gufw_24.04.0-2_all.deb …
Распаковывается gufw (24.04.0-2) …
Настраивается пакет gufw (24.04.0-2) …
Обрабатываются триггеры для desktop-file-utils (0.27-2build1) …
Обрабатываются триггеры для hicolor-icon-theme (0.17-2) …
Обрабатываются триггеры для gnome-menus (3.36.0-1.1ubuntu3) …
Обрабатываются триггеры для man-db (2.12.0-4build2) …
azaliya@MDK:~$
```

Рисунок 3.1 – Установка gufw

2. Запустите программу и активируйте защиту. Пример представлен на рисунке 3.2.

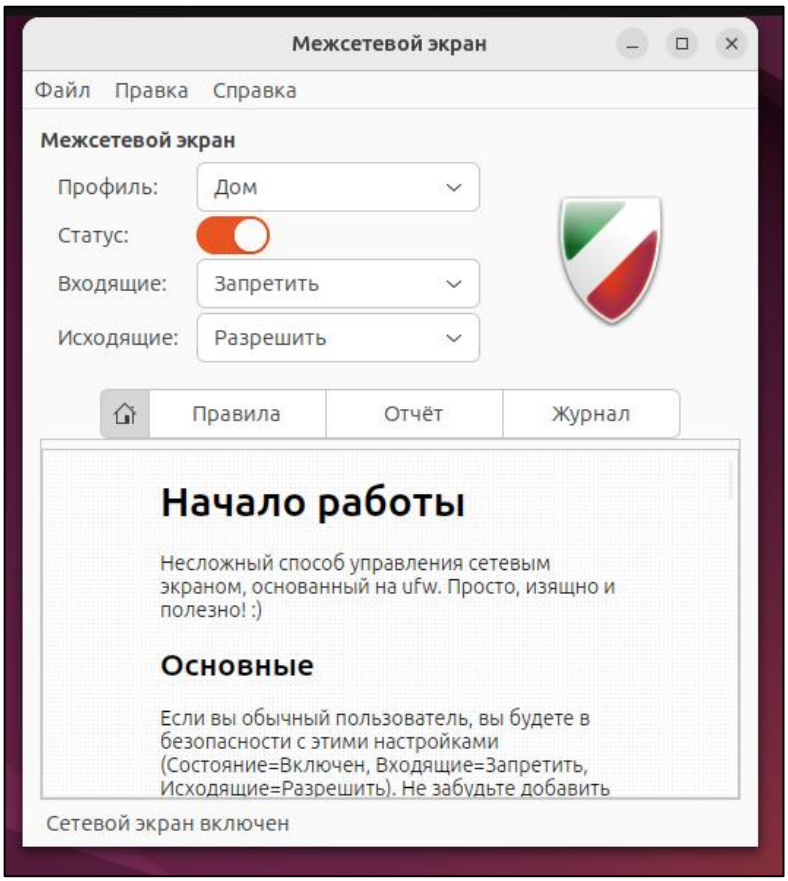

Рисунок 3.2 – Главное окно Брандмауэра

3. Вручную разрешите только те порты, которые необходимы для работы доверенных программ (например, для браузера).

Пример настройки правил:

После включения строгой блокировки весь интернет-трафик, включая DNS-запросы, будет заблокирован. Пример представлен на рисунке 3.3.

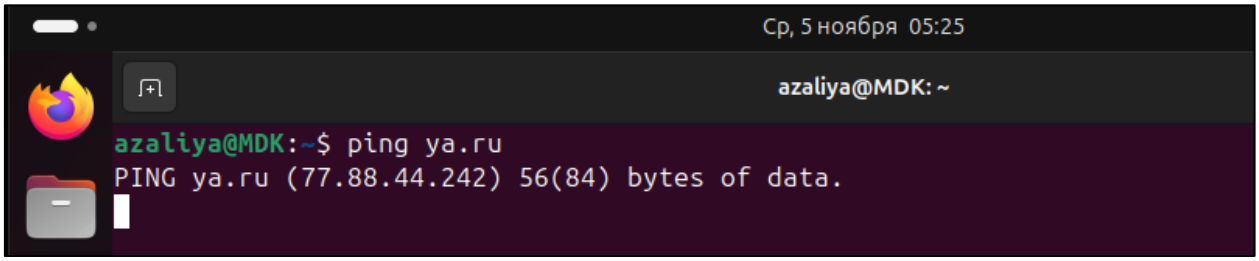

Рисунок 3.3 – Проверка блокирования интернет-трафика

Чтобы это исправить:

– добавьте новое правило;

– выберите политику «Разрешить» для DNS-трафика. Пример представлен на рисунке 3.4;

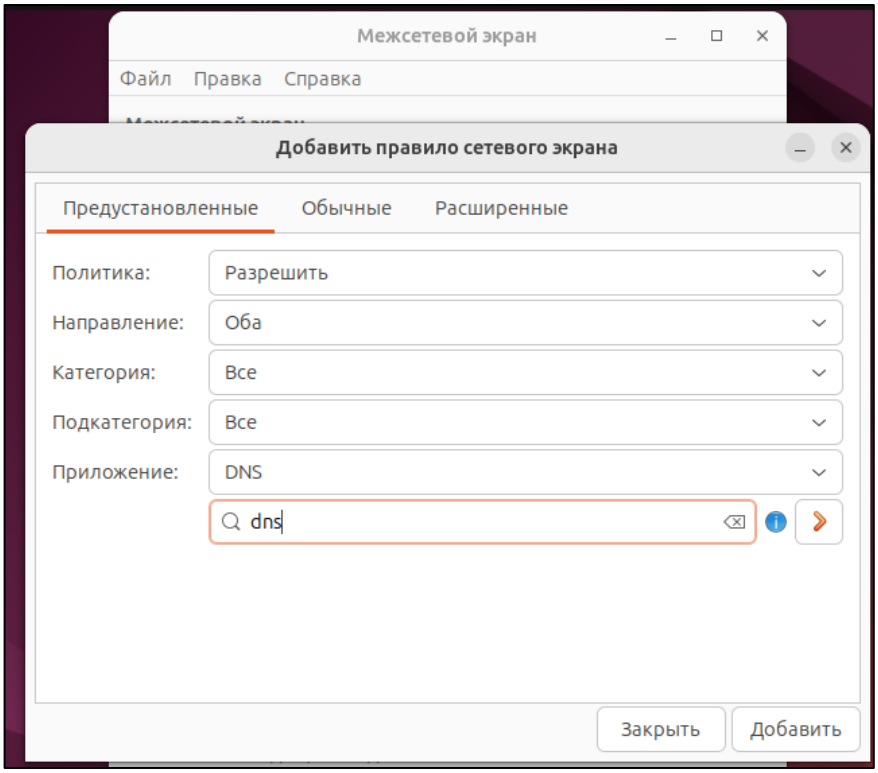

Рисунок 3.4 – Настройки правил для DNS-трафика

– после добавления правила проверьте, восстановился ли доступ к интернету. Пример представлен на рисунке 3.5.

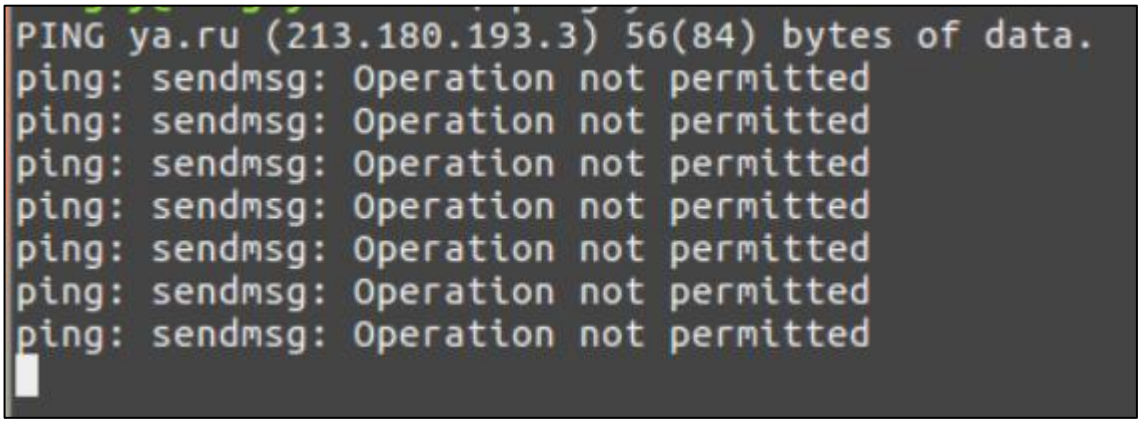

Рисунок 3.5 – Проверка восстановленного доступа к интернету

Вывод

В результате выполнения этого руководства вы реализовали три ключевых принципа безопасности: минимальные привилегии, отключение неиспользуемых сервисов и контроль сетевого трафика. Теперь ваш домашний каталог приватнен, удаленный доступ для суперпользователя заблокирован, а брандмауэр фильтрует все соединения.

Однако не стоит останавливаться на достигнутом. Безопасность – это комплексный подход.

Рекомендуется продолжить укрепление системы: регулярно обновлять пакеты, использовать надежные пароли и ключи SSH, а также ознакомиться с более продвинутыми инструментами, такими как SELinux или AppArmor. Начав с этих основ, вы заложили прочную основу для создания по-настоящему защищенной системы.