Настройка политики безопасности Linux

1 Настройка общей памяти

По умолчанию весь объем общей памяти /run/shm доступен для чтения и записи с возможностью выполнения программ. Это считается брешью в безопасности и многие эксплойты используют /run/shm для атак на запущенные сервисы. Для большинства настольных, а особенно серверных устройств рекомендуется монтировать этот файл в режиме только для чтения.

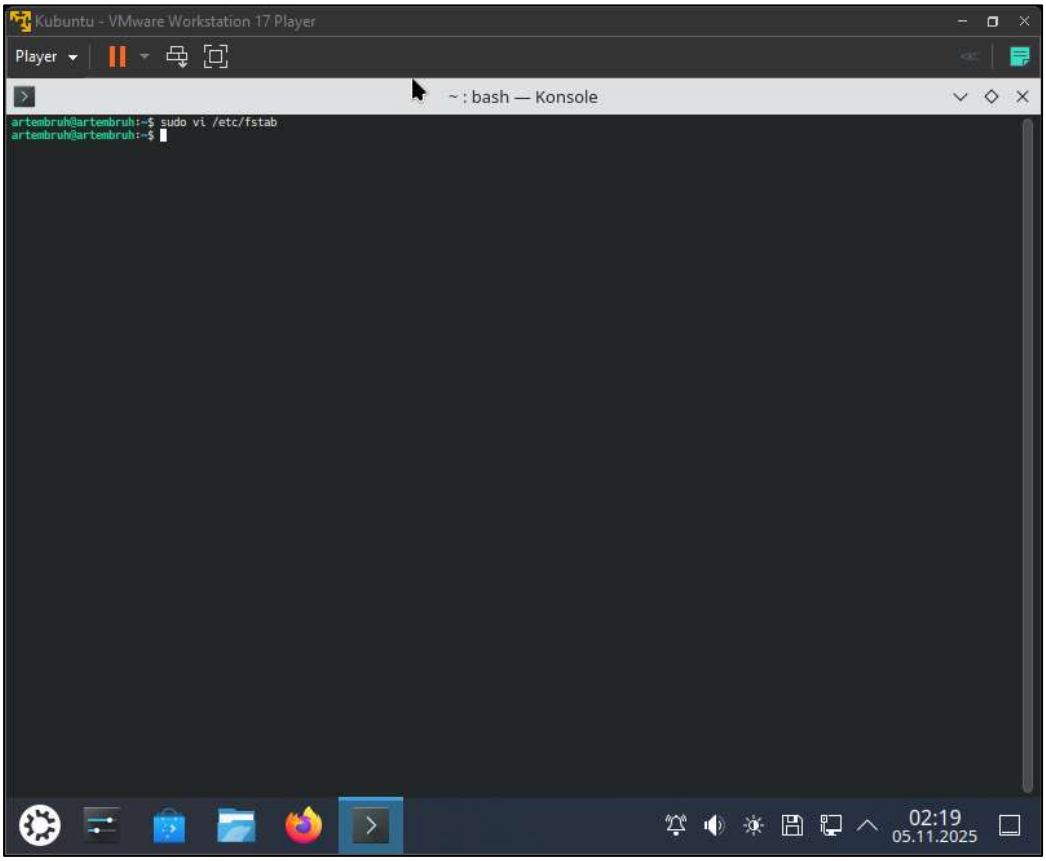

Рисунок 1 – Открываем папку fstab через терминал

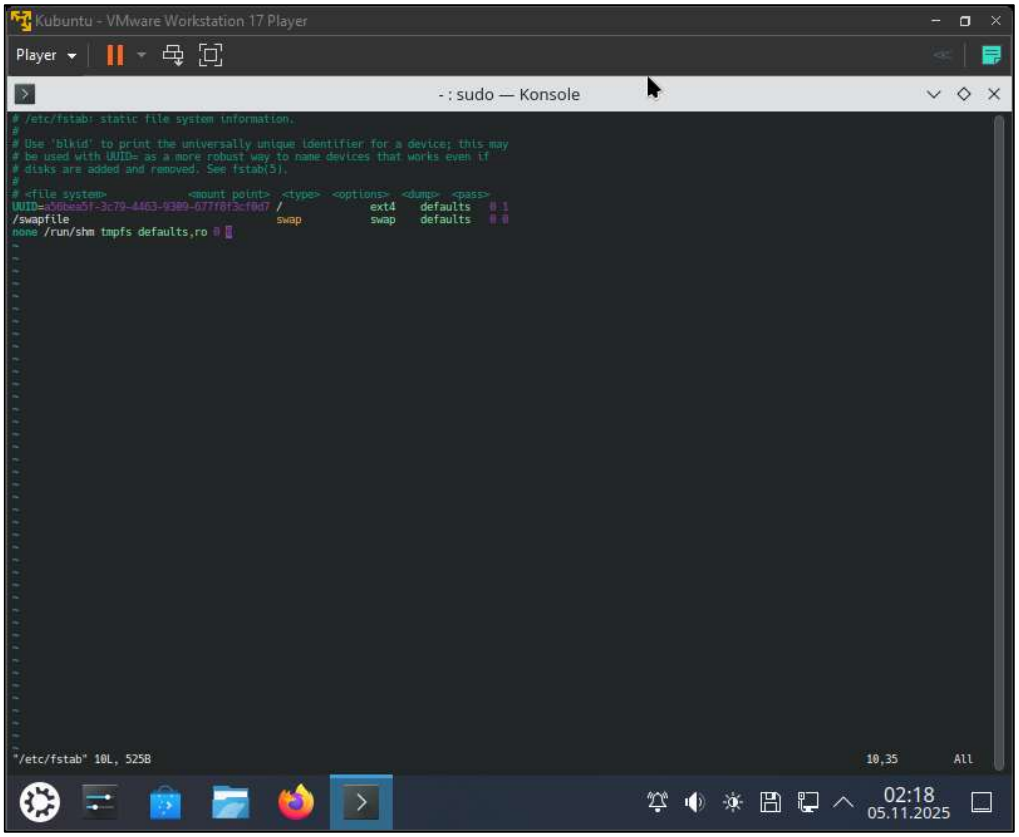

Рисунок 2 – Папка fstab через терминал

2 Настройка Брандмауэра

По умолчанию UFW в Ubuntu может быть отключен. Чтобы включить его, выполните следующие команды в терминале. Включаем брандмауэр Uncomplicated Firewall, и проверяем статус. Разрешаем доступ через порт 80 с протоколом tcp. Запрещаем доступ через порт 22.

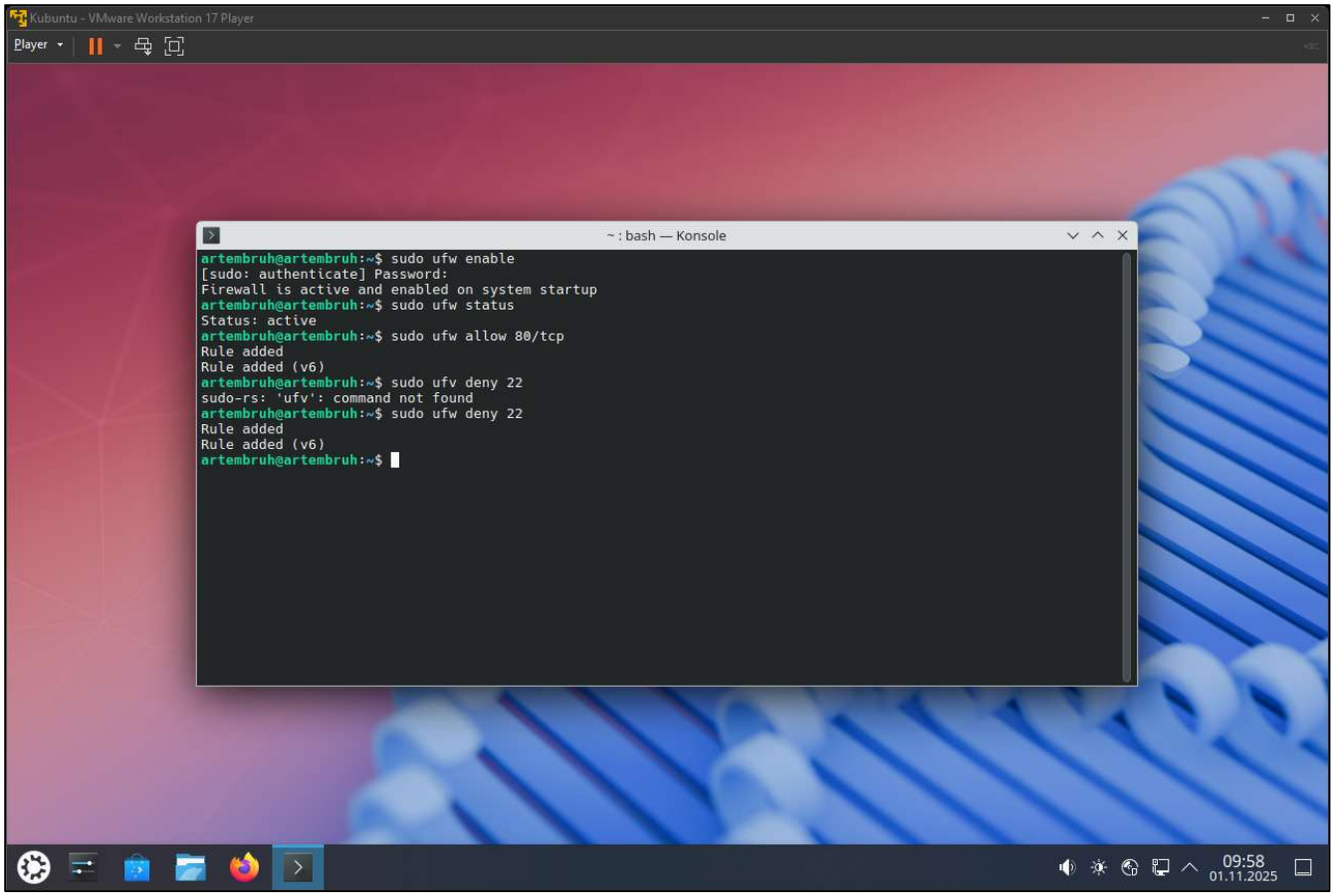

Рисунок 3 – Включаем Брандмауэр

3 Настройка доступа к общему каталогу

Ваш домашний каталог по умолчанию будет доступен каждому пользователю в системе. Так что если у вас есть гостевая учетная запись, то гость сможет получить полный доступ ко всем вашим личным файлам и документам. Но вы можете сделать его доступным только вам.

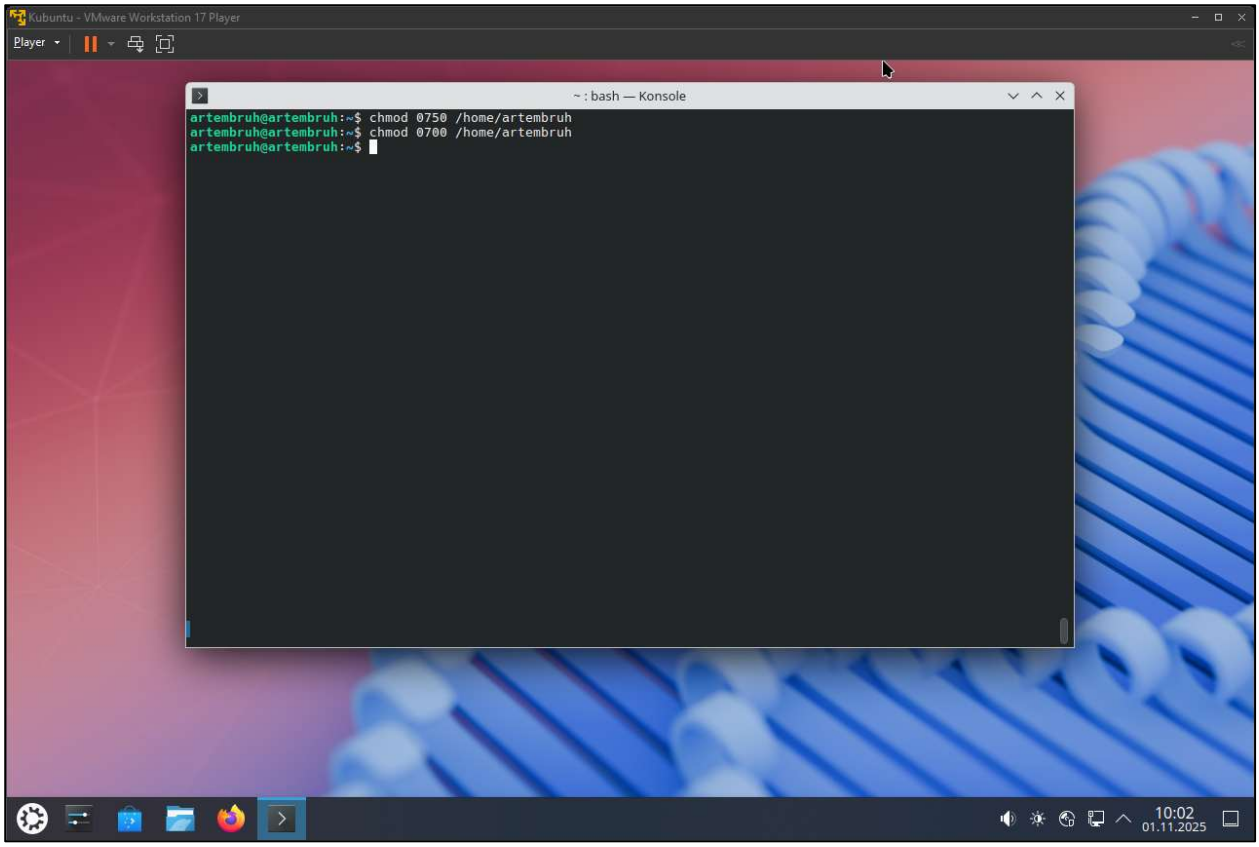

Рисунок 4 – Ограничиваем доступ к домашнему каталогу

4 Проверка на наличие руткитов и вредоносного ПО

Устанавливаем rkhunter для проверки на наличие руткитов и вредоносного ПО.

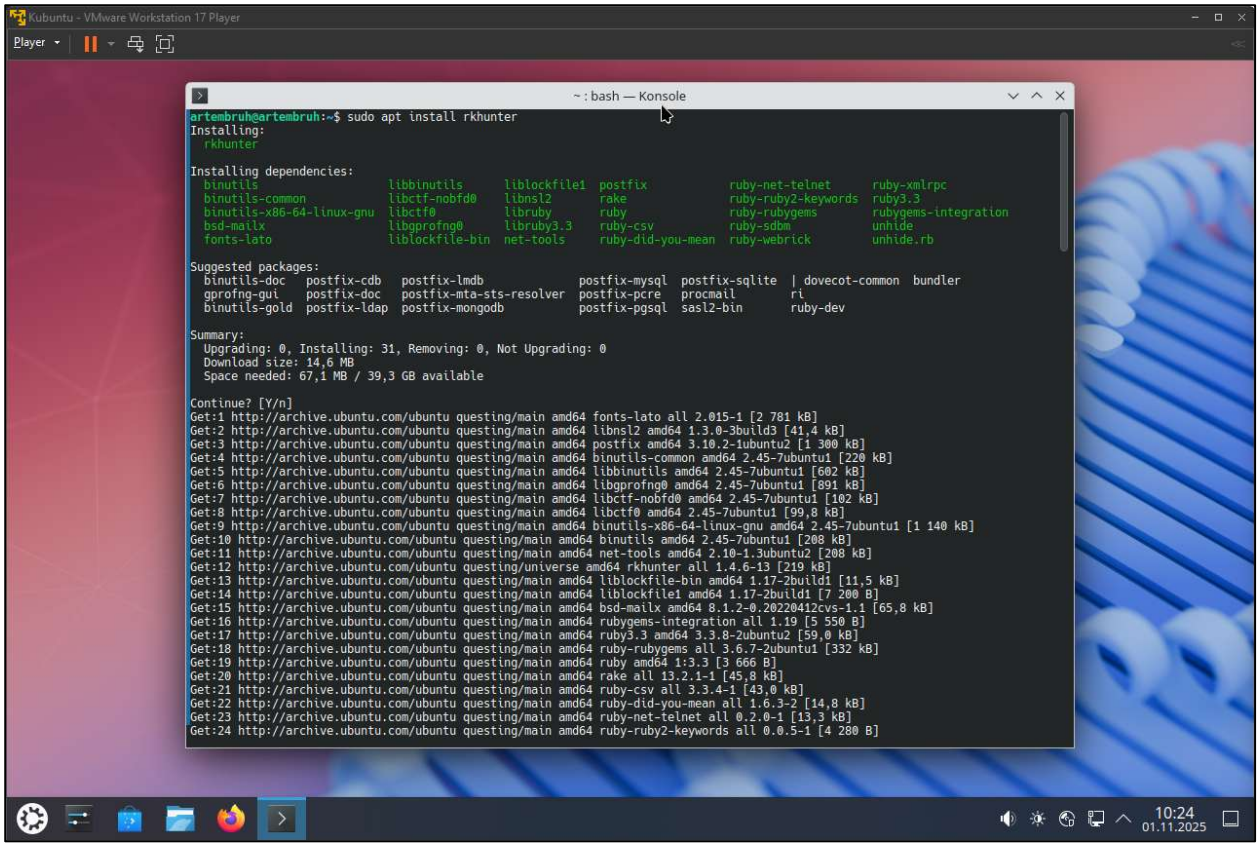

Рисунок 5 – Установка rkhunter

После установки выполните обновление баз данных и сканирование

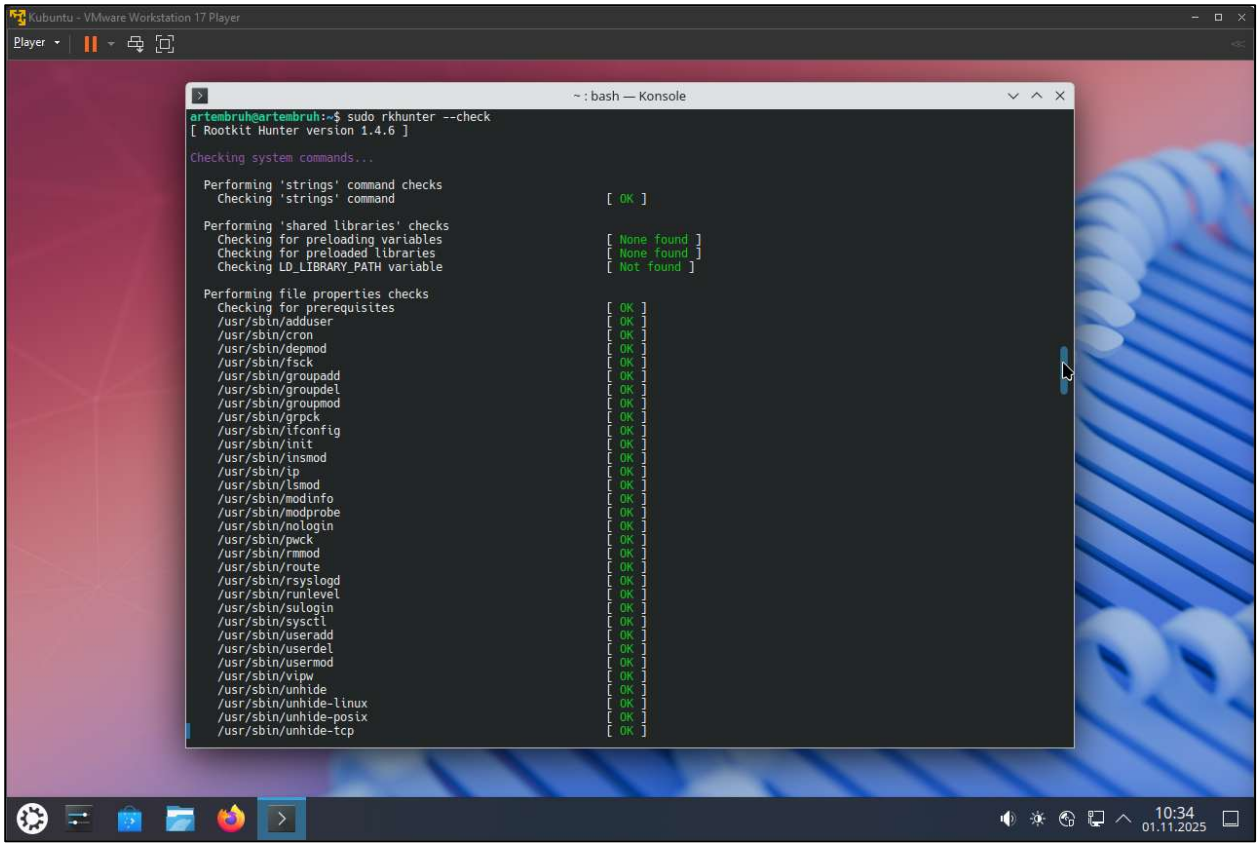

Рисунок 5 – Обновление баз данных и сканирование

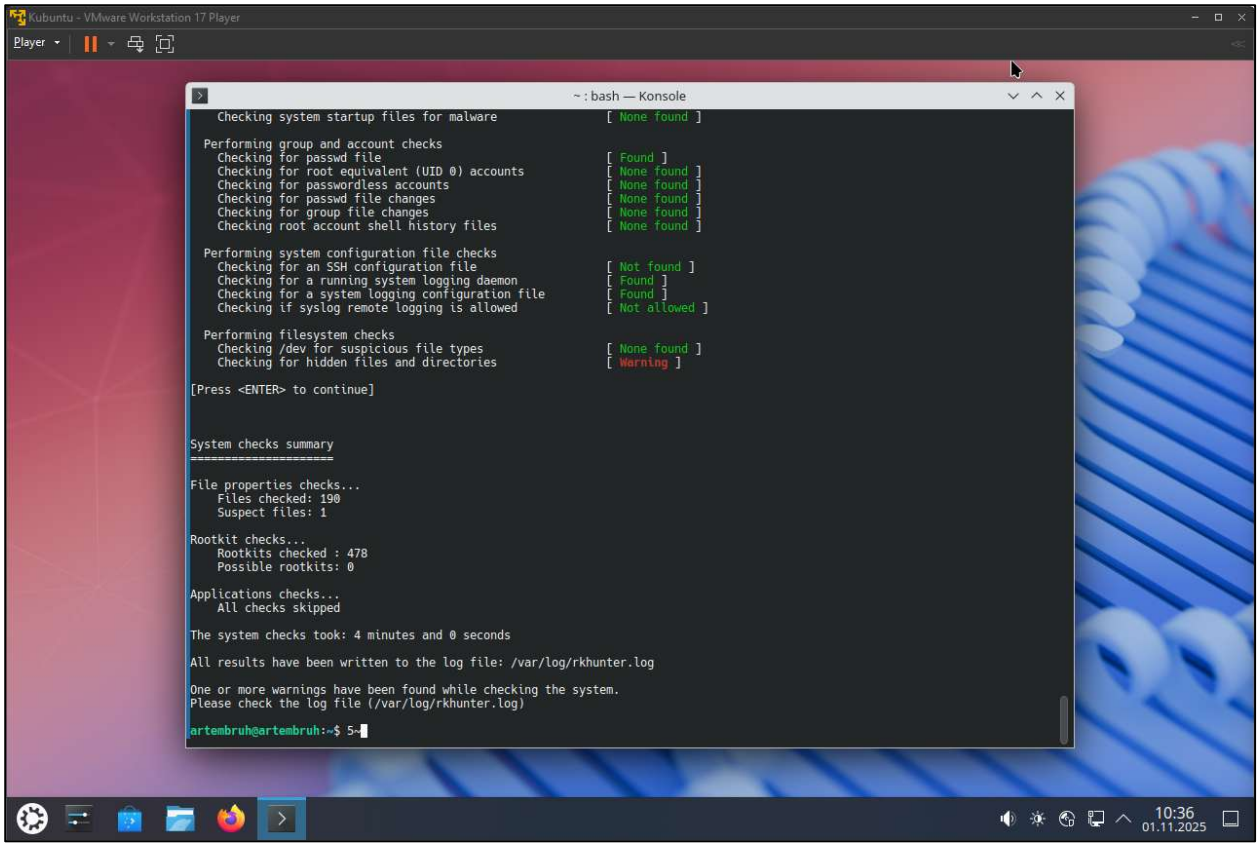

Рисунок 6 – Результат сканирования

Вывод

Безопасность Kubuntu — это комплексный процесс, который требует регулярного внимания и действий. Настройка UFW позволяет эффективно защитить систему от несанкционированного сетевого доступа. Ограничение доступа к домашней папке позволит защитить файлы от посторонних пользователей.