Занятие 4. Безопасность Linux серверов

Практическая работа “Настройка файлового сервера в корпоративной инфраструктуре”

Цель работы:

- Научиться настраивать сервер Samba
- Понимать как составляется конфигурационный файл Samba и его параметры
- Понять как работает Iptables

Задача:

- Получить доступ к папкам и файлам находящимся на файловом сервере Linux, клиентом Linux
- Получить доступ к папкам и файлам находящимся на файловом сервере Linux, клиентом Windows
- Добавить сервис Samba в автозагрузку OS Linux
- Настрить Samba ресурс с названием share и дать права на чтение группе пользователей users, но предоставить возможность записи для группы с именем admins, а также пользователю PT, для этого можете отредактировать файл `/etc/samba/smb.conf`.
- Настройка корзины для общего ресурса (для тех кому показалось легко 🙂)
  -- пояснить команду

`smbstatus` (*продемонстрировать, пояснить результат*)
-- записать вывод в файл .txt

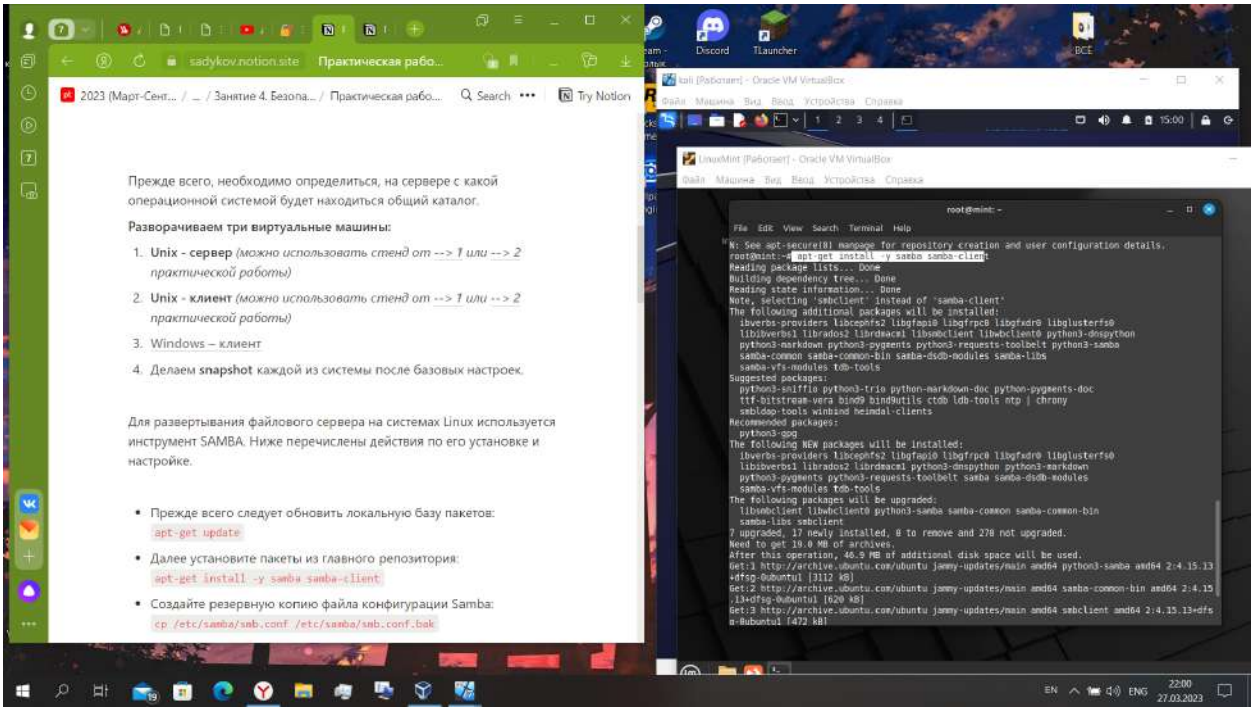

Рис. 4. 1. 1 Установка пакетов из главного репозитория

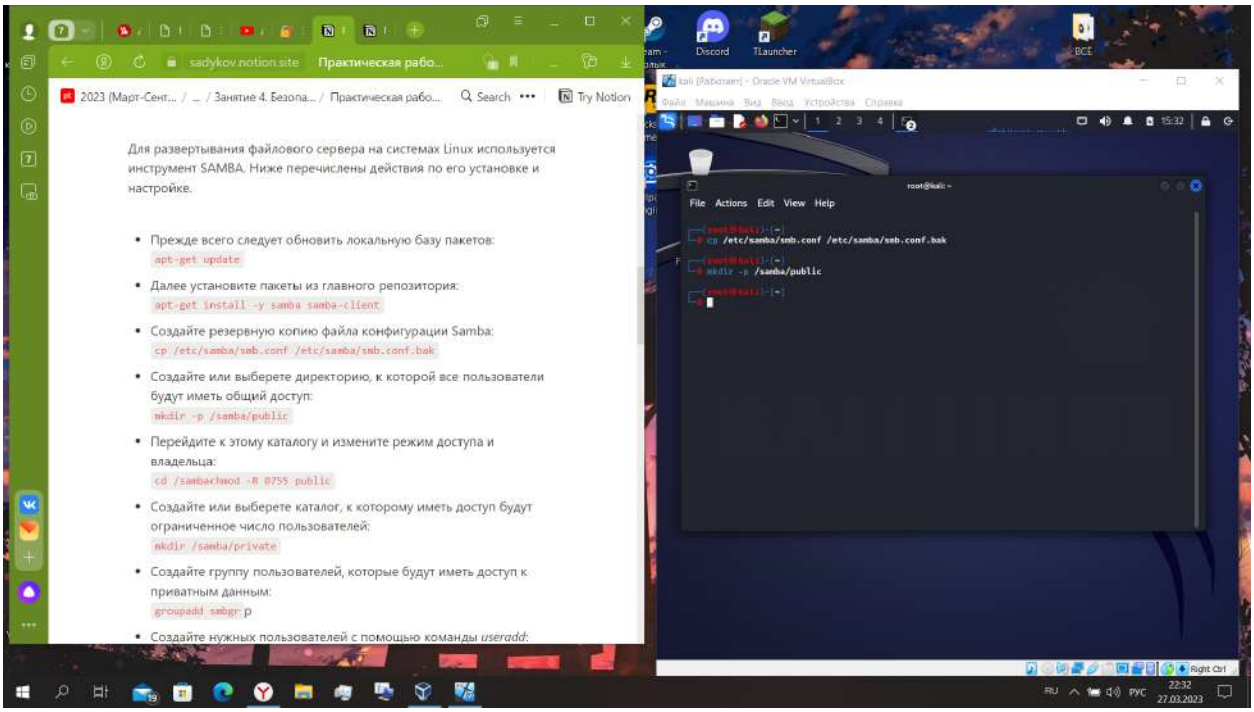

Рис. 4. 1. 2 Копия конфигурационного файла. Директория общего доступа

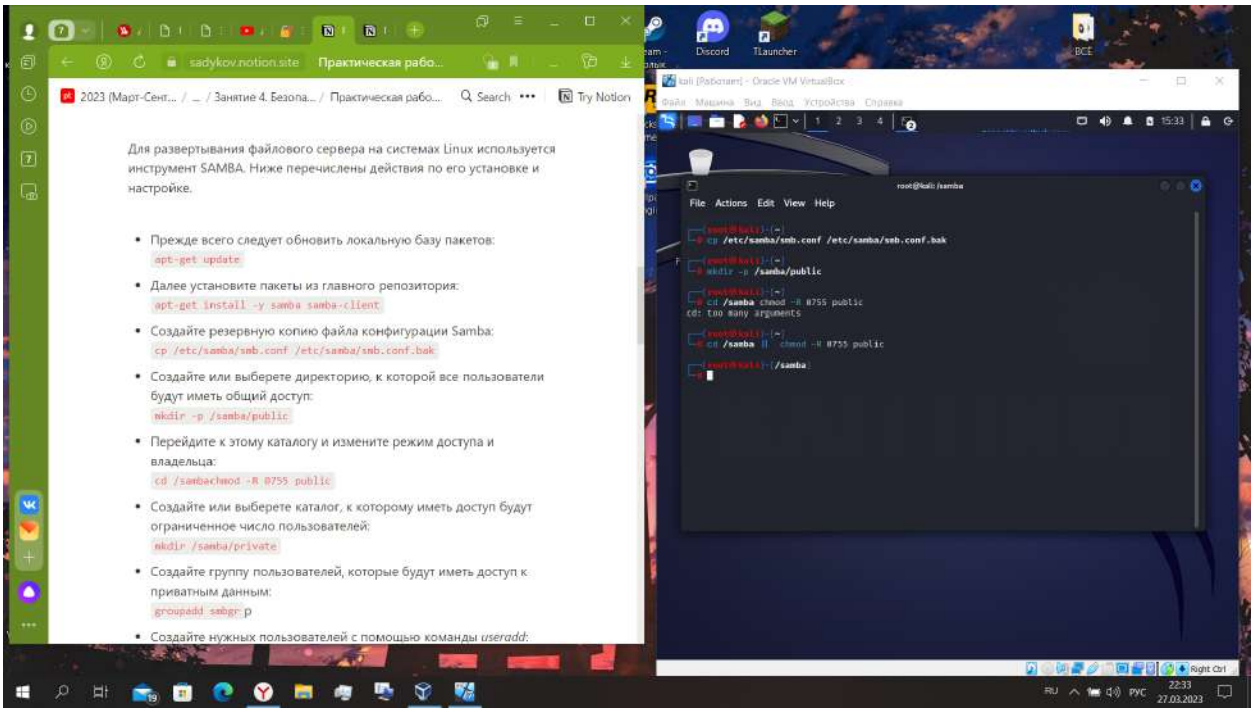

Рис. 4. 1. 3 Настройка прав доступа

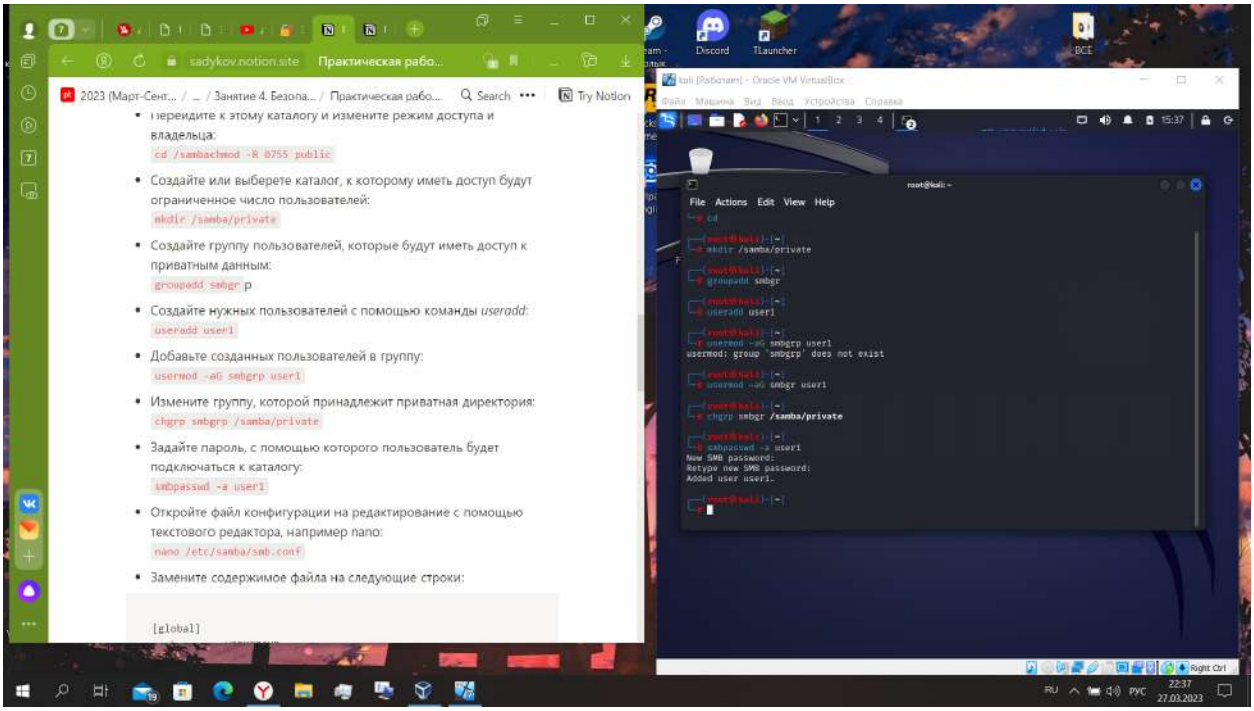

Рис. 4. 1. 4 Создание приватного каталога. Группа пользователей. Установка пароля

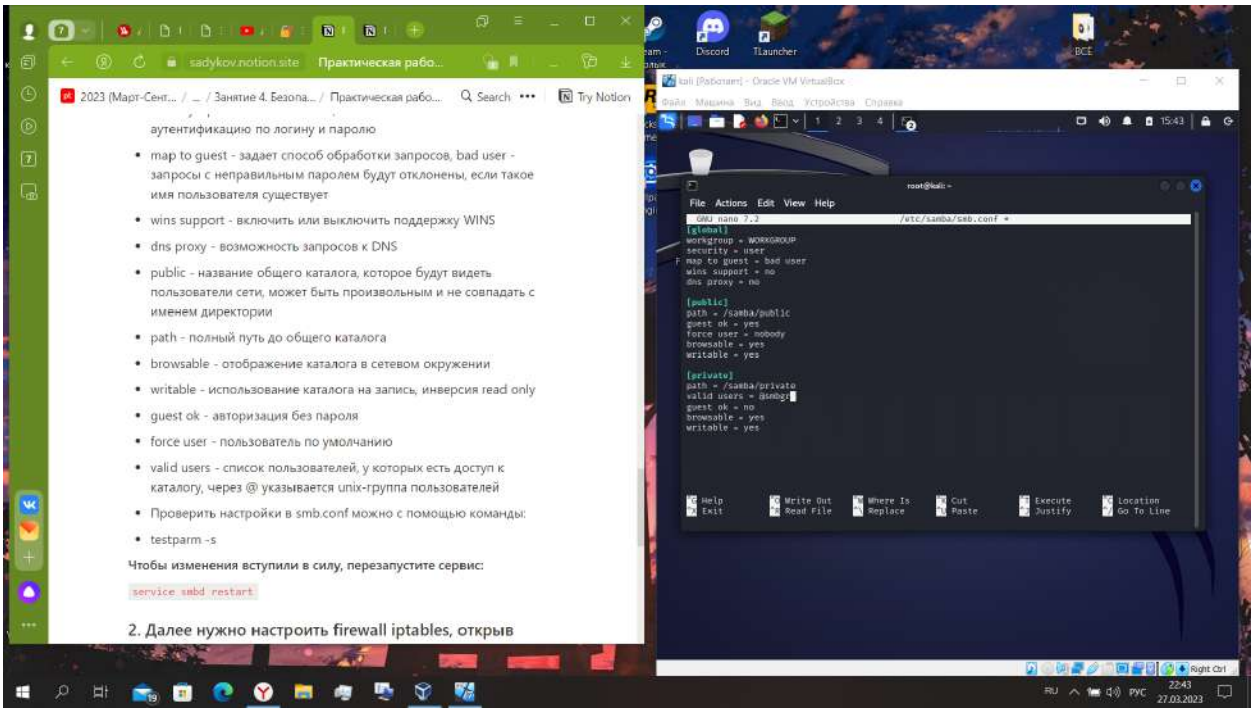

Рис. 4. 1. 5 Настройка конфигурационного файла

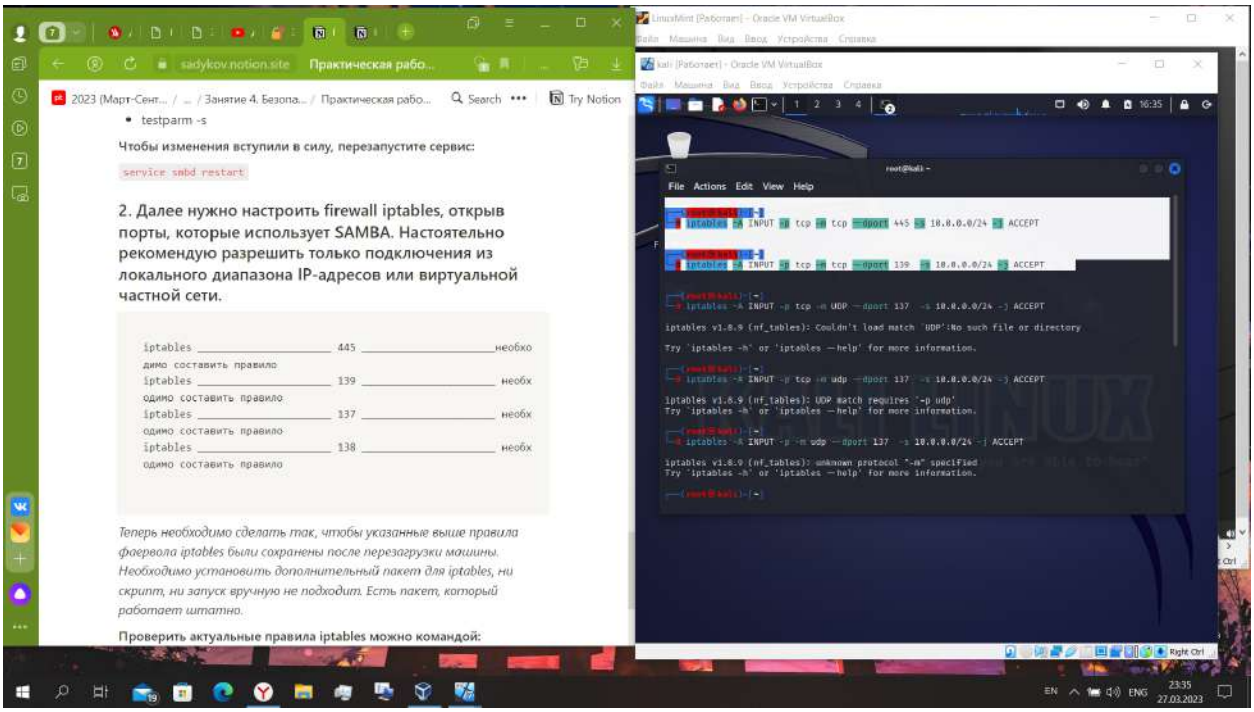

Рис. 4. 1. 6 Настройка firewall

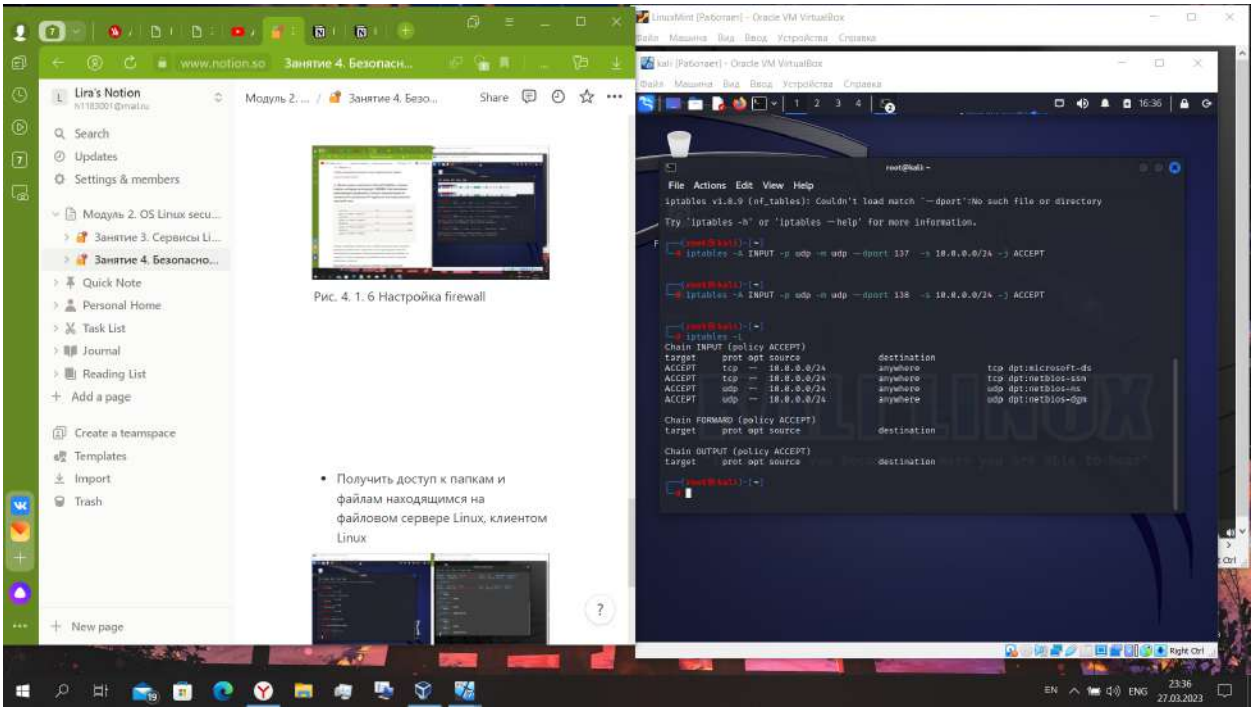

Рис. 4. 1. 7. Проверка правил. Открытие портов tcp/udp

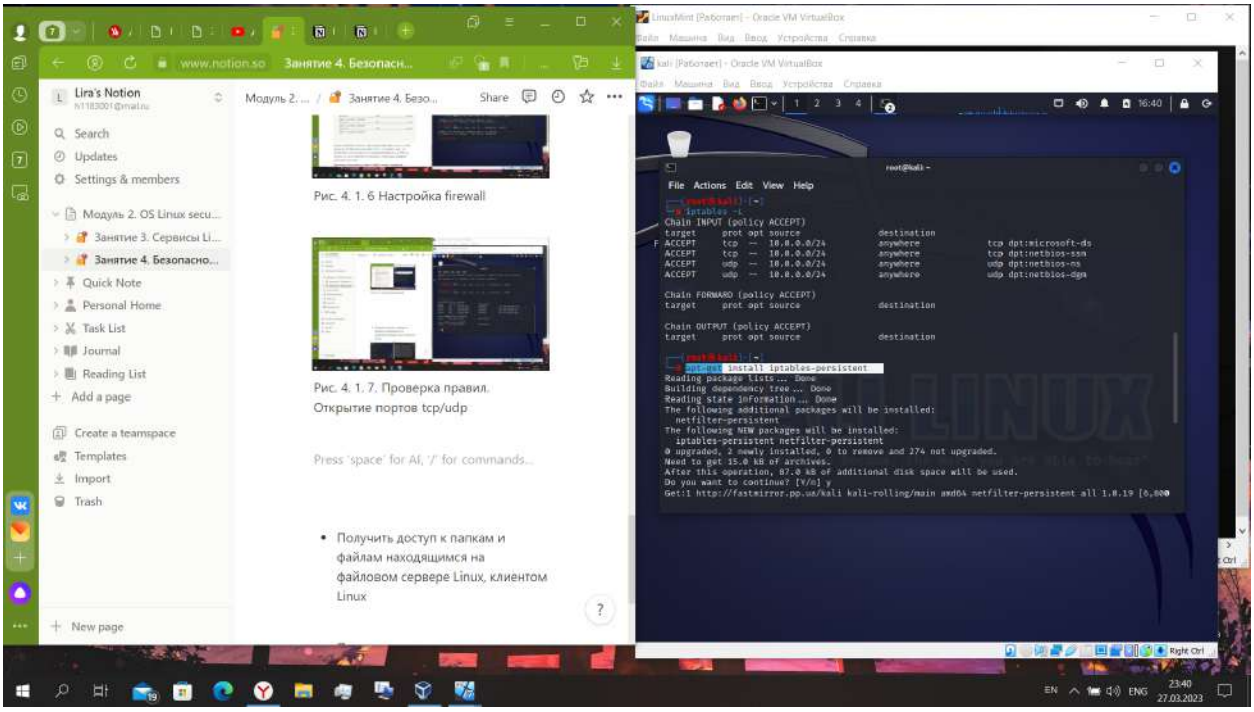

Рис. 4. 1. 8. Установка пакета для сохранения правил

- Получить доступ к папкам и файлам находящимся на файловом сервере Linux, клиентом Linux

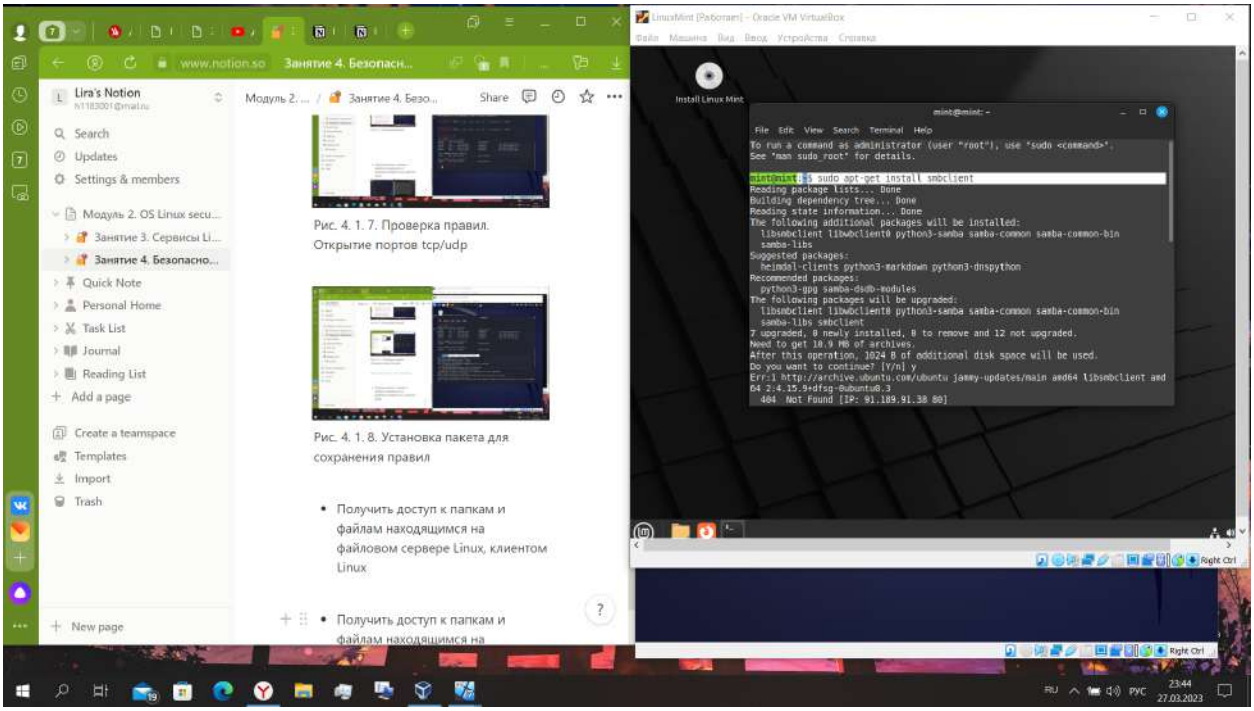

Рис. 4. 1. 9. Установка пакета для подключения к общим папкам

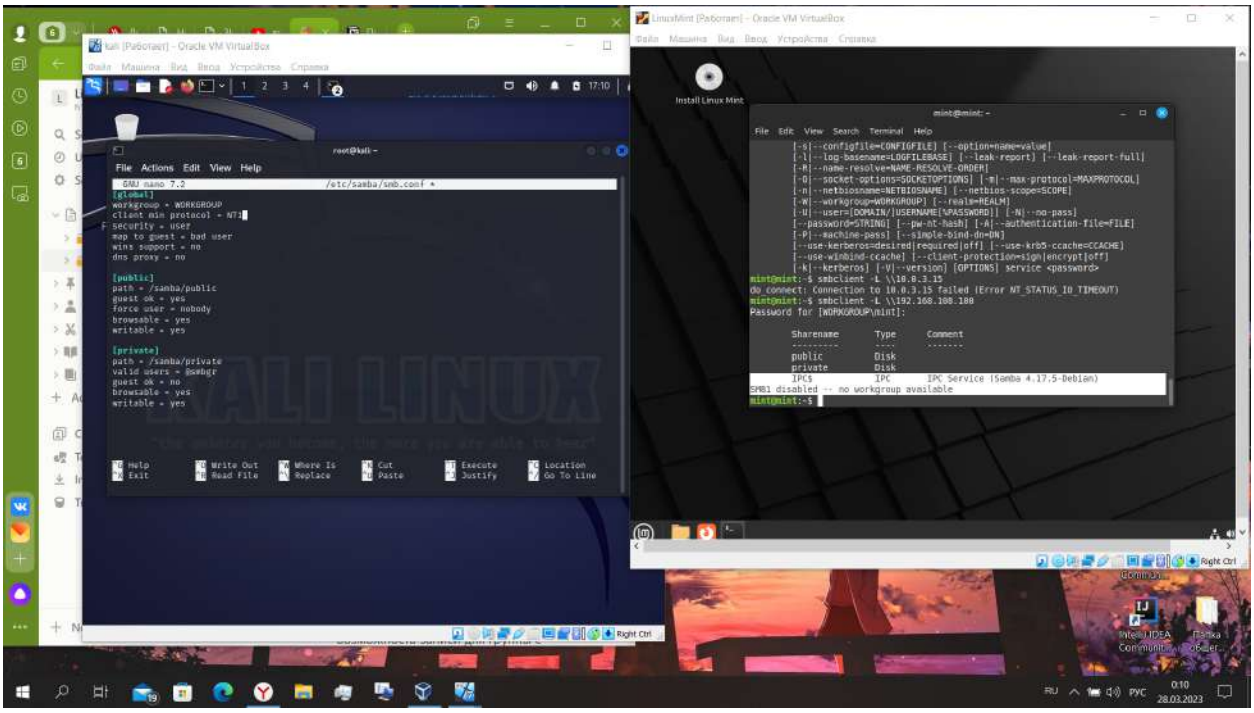

Рис. 4. 1. 10. При подключении к серверу ошибка. Меняю конфигурационный файл: включаю smb1.

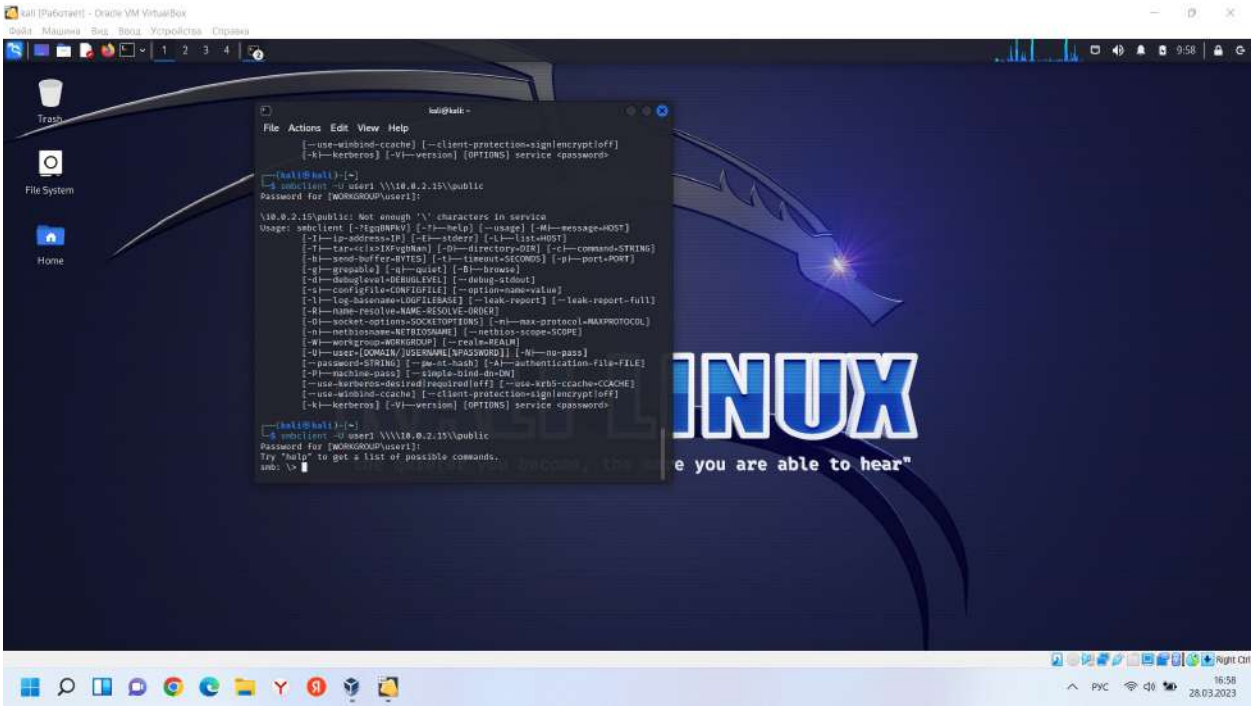

Рис. 4. 1. 11. Подключение к smb с Linux-клиента

- Получить доступ к папкам и файлам находящимся на файловом сервере Linux, клиентом Windows

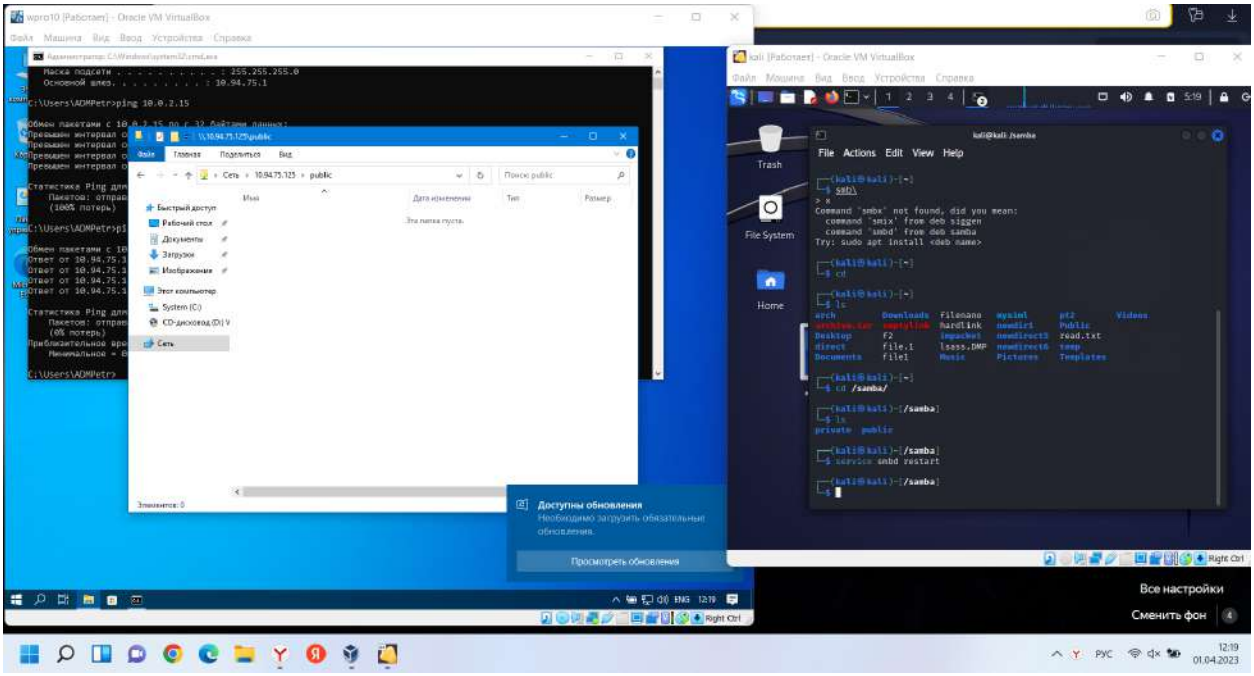

Рис. 4. 1. 12. Подключение к smb с Windows-клиента

- Добавить сервис Samba в автозагрузку OS Linux

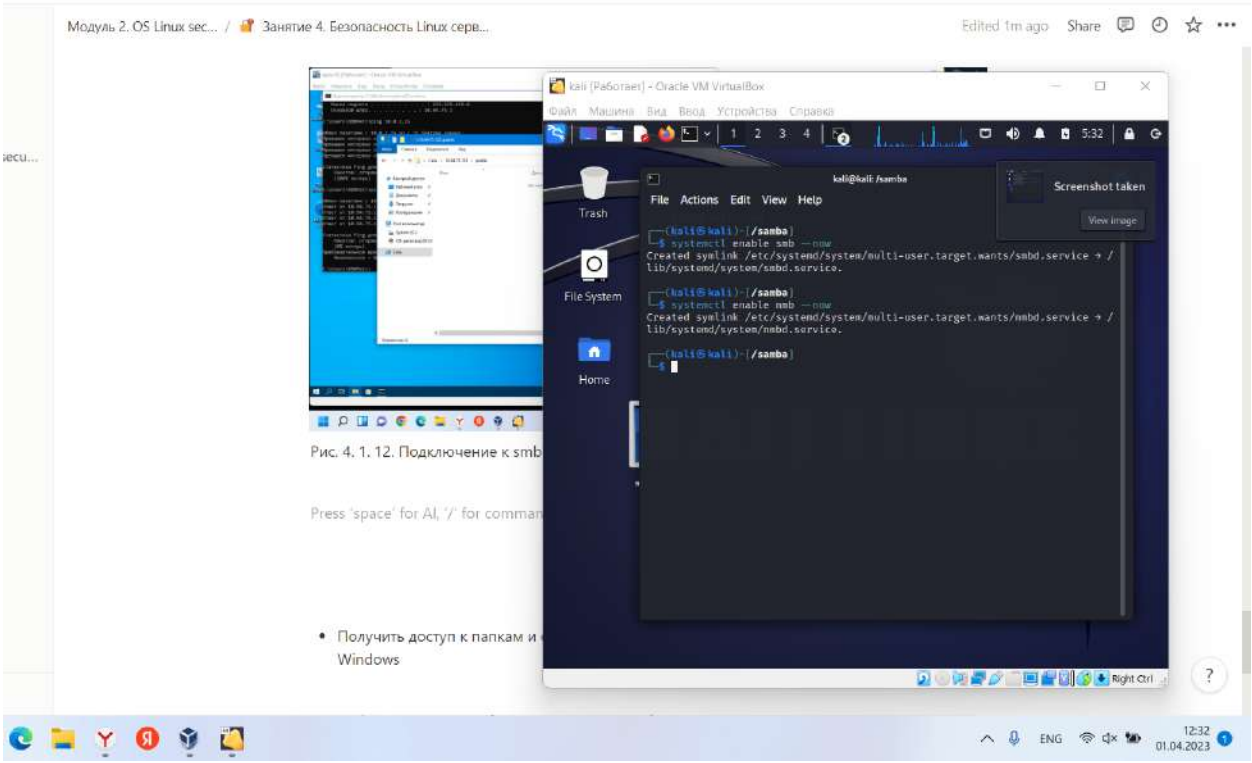

Рис. 4. 1. 13. Добавление сервисов Samba в автозагрузку

- Настроить Samba ресурс с названием share и дать права на чтение группе пользователей users, но предоставить возможность записи для группы с именем admins, а также пользователю PT, для этого можете отредактировать файл `/etc/samba/smb.conf`.

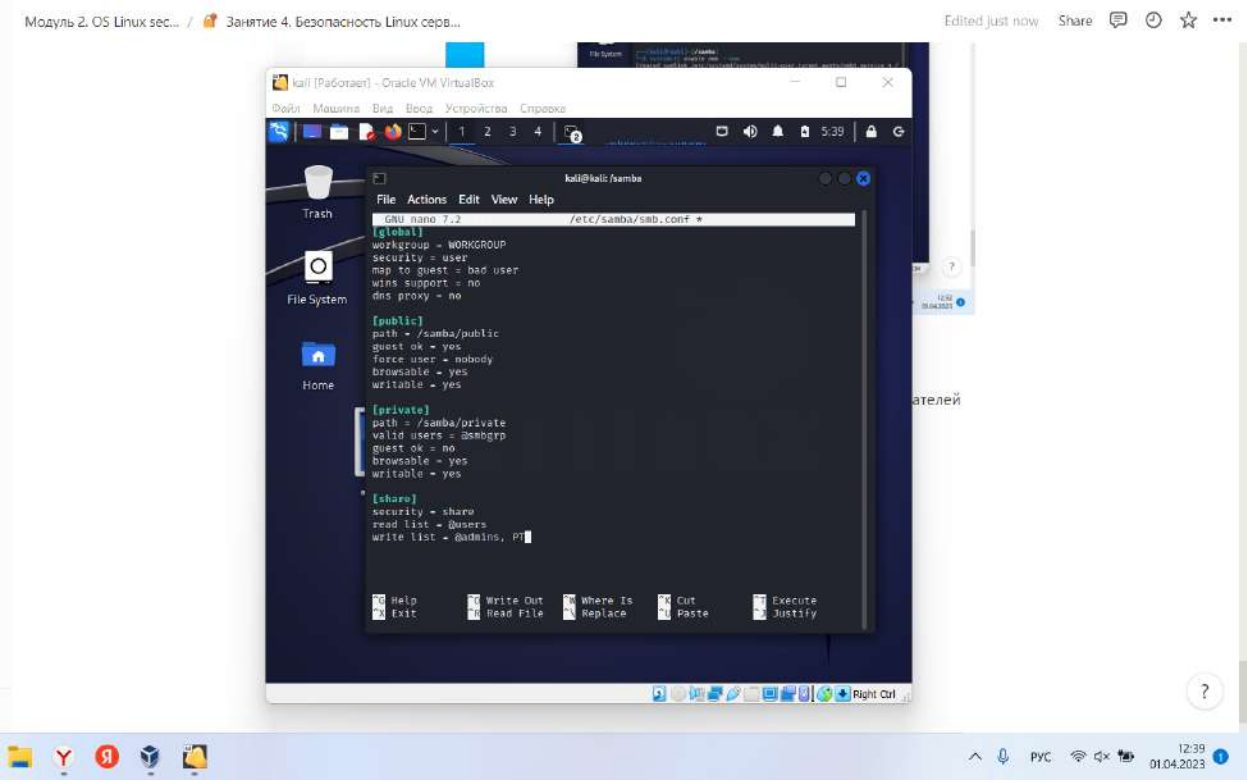

Рис. 4. 1. 14. Настройка Samba ресурса с названием share

- Настройка корзины для общего ресурса (для тех кому показалось легко 🙂)
  -- пояснить команду
  `smbstatus` (*продемонстрировать, пояснить результат*)
  -- записать вывод в файл .txt

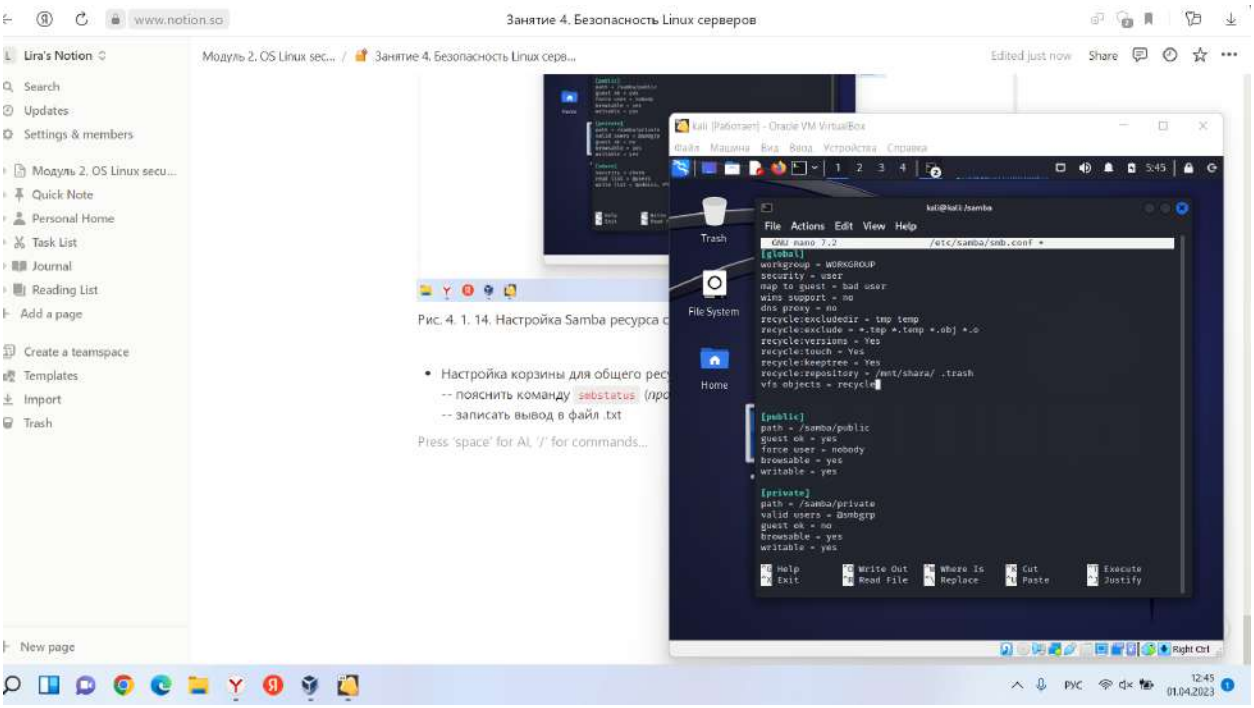

Рис. 4. 1. 15. Настройка корзины для общего ресурса

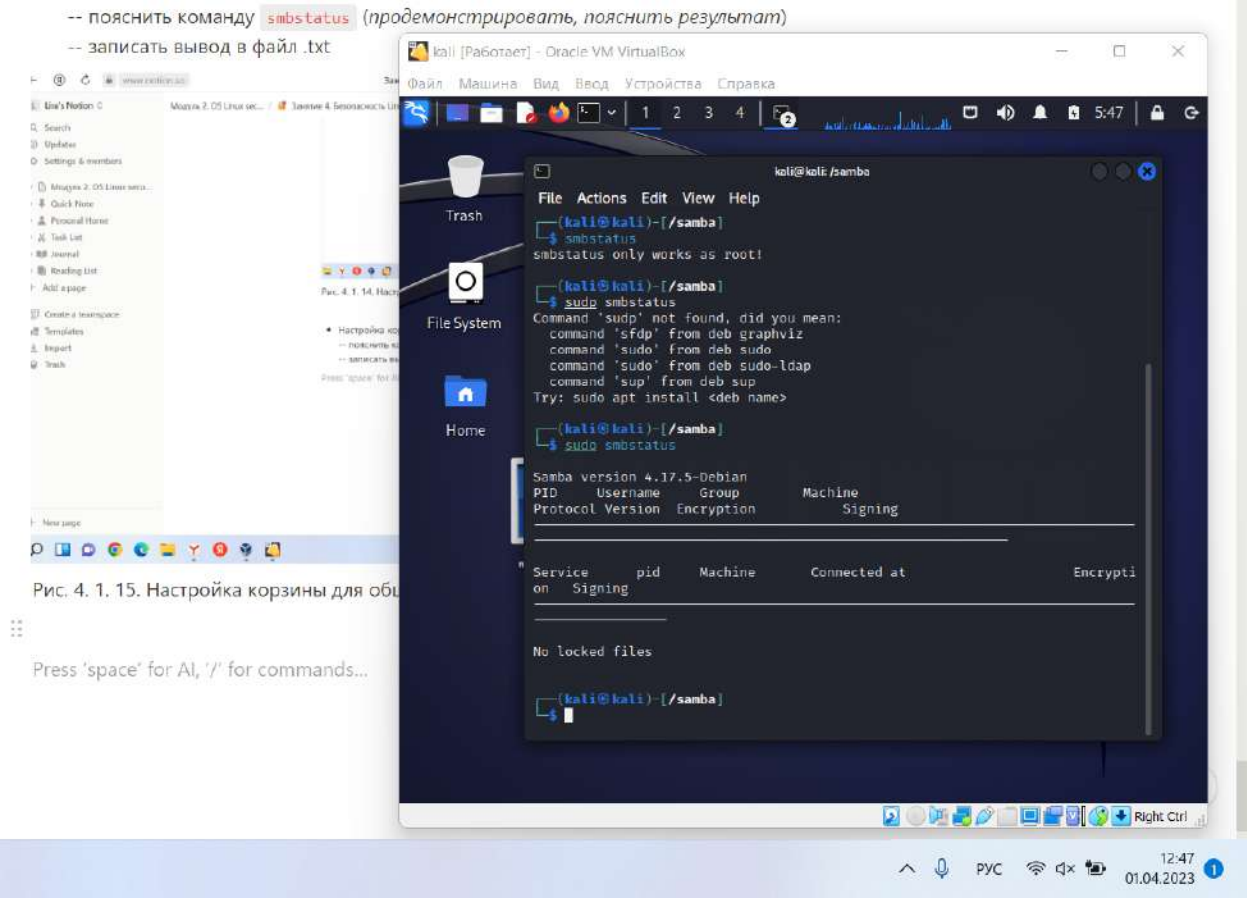

Рис. 4. 1. 16. Команда smbstatus

smbstatus - показывает параметры текущего соединение Samba

sudo smbstatus > smstatus.txt - сохраняет вывод в файл smstatus.txt

Практическая работа "Fail2Ban-SSH и Brute-force attack".

Цель работы:

- Научиться конфигурировать Fail2Ban для отражения атак brute-force attack на SSH.

Задача:

- Настроить сервер SSH
- Установить и настроить Fail2Ban
- Научиться пользоваться Hydra
- Провести с помощью Hydra brute-force attack
- Провести атаку с помощью Hydra при выключенном Fail2Ban и исключенном ip-адресе из ban листа.

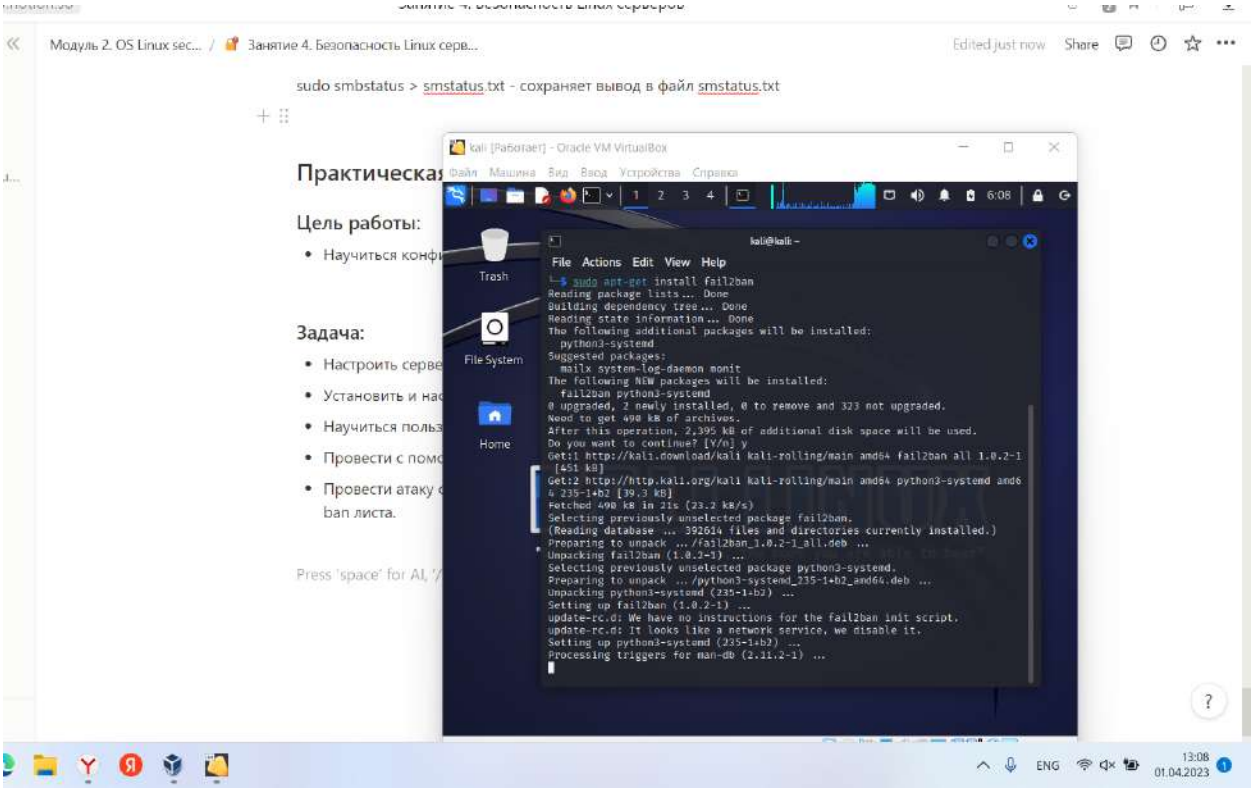

Рис. 4. 2. 1. Установка Fail2ban

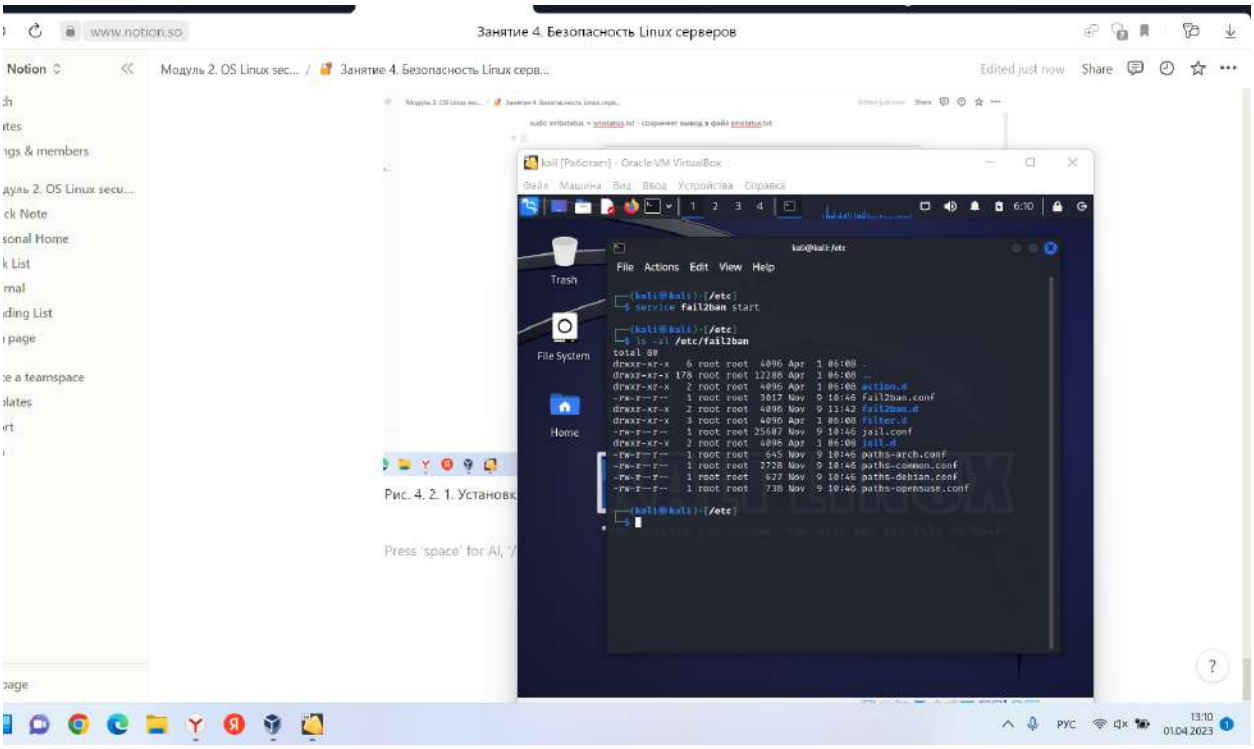

Рис. 4. 2. 2. Запуск fail2ban. Просмотр файлов конфигурации

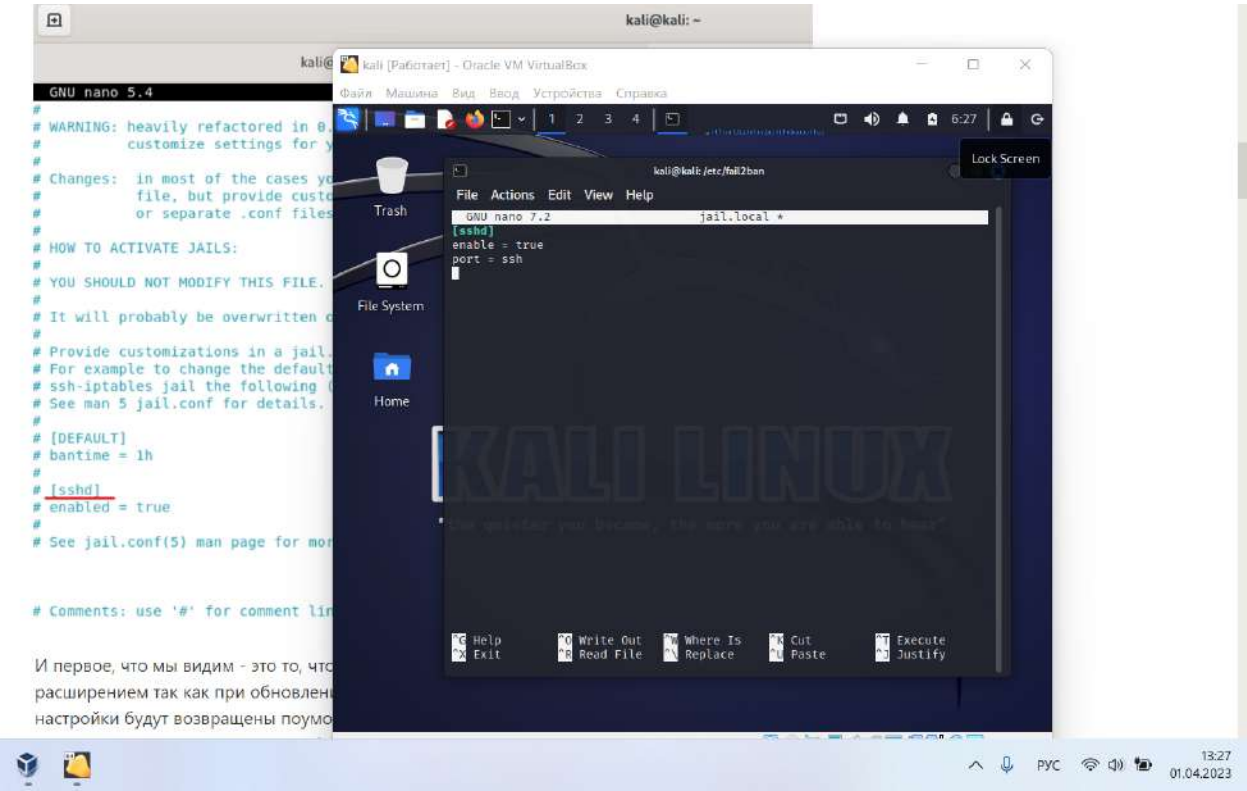

Рис. 4. 2. 3. Настройка jail.local

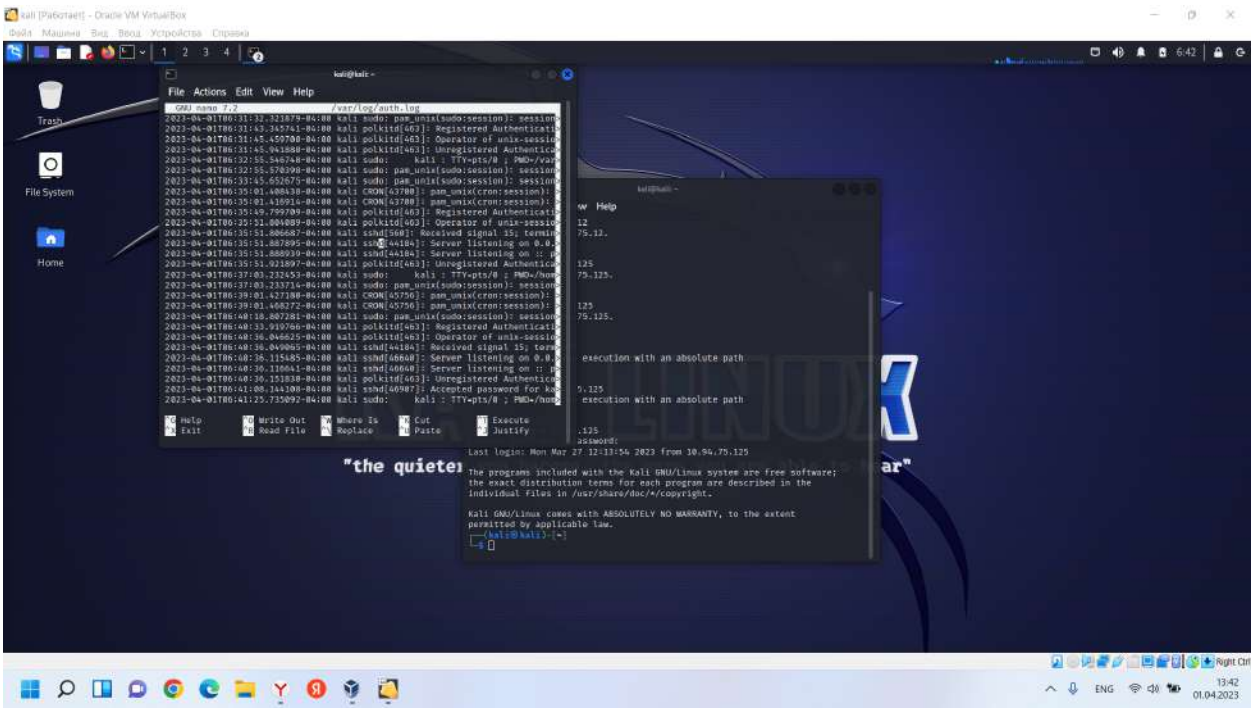

Рис. 4. 2. 4. auth.log

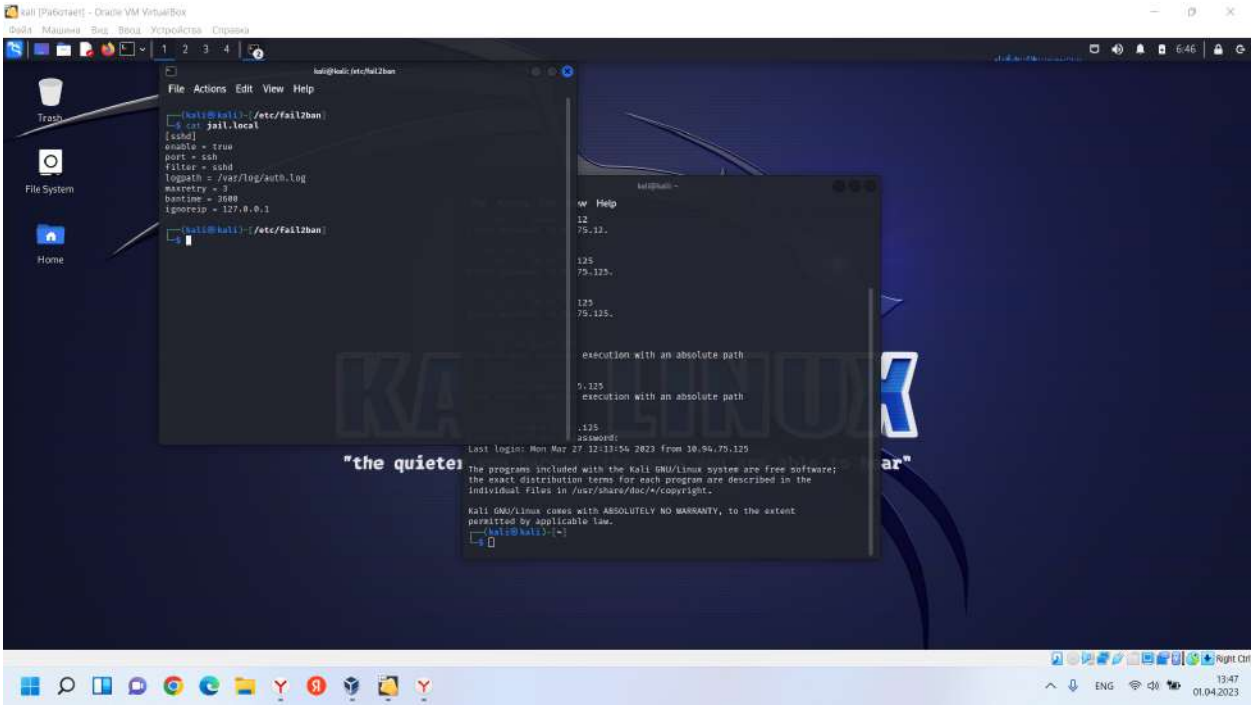

Рис. 4. 2. 3. Настройка jail.local

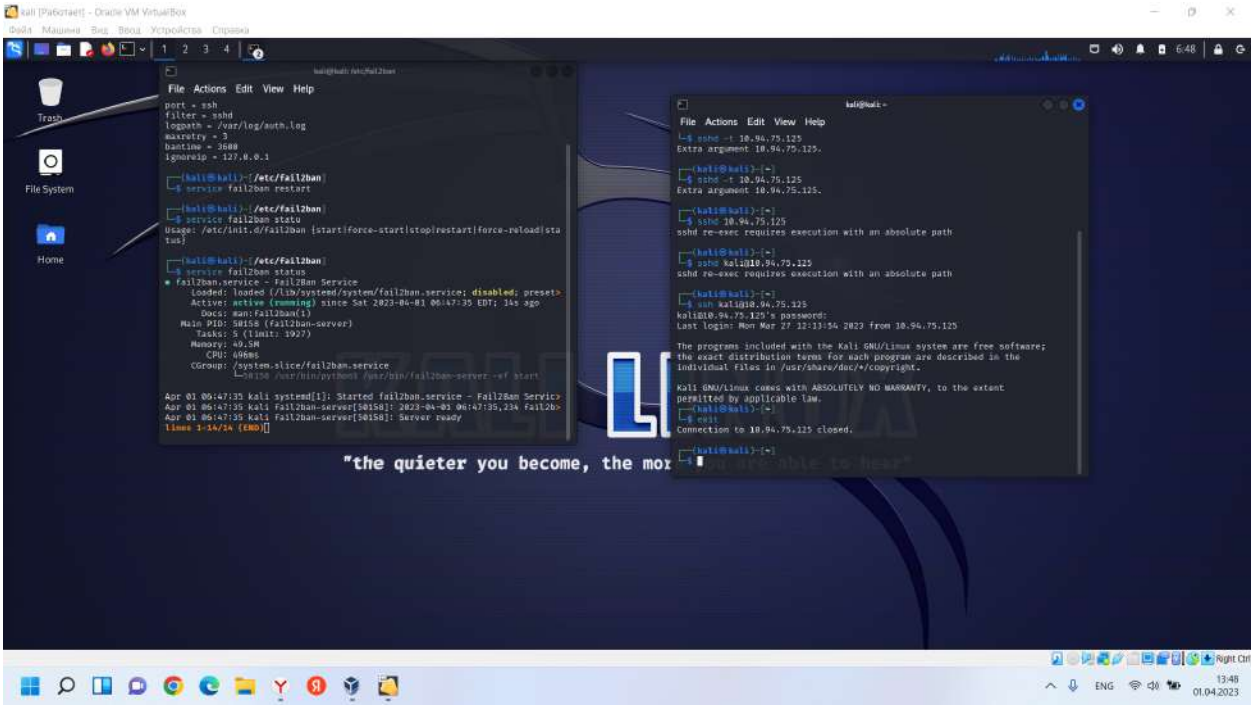

Рис. 4. 2. 4 Fail2ban активен.

Произведём подключение и потратим 3 попытки ввода правильного пароля:

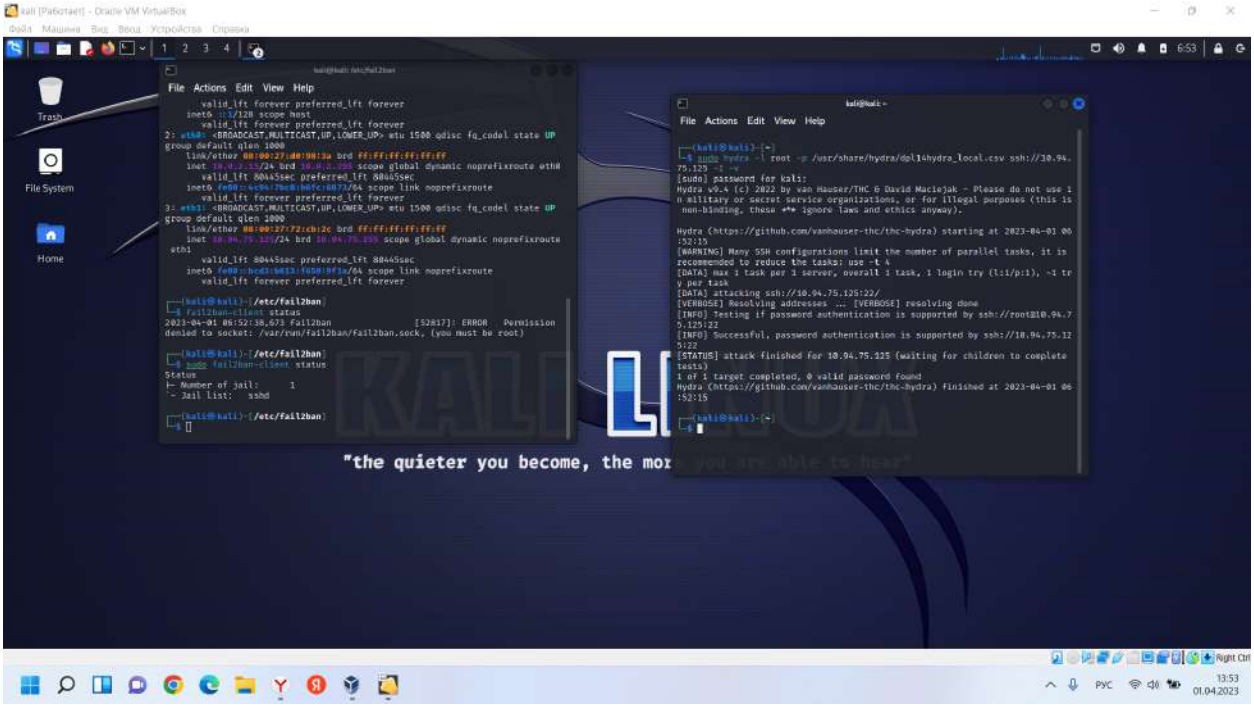

Рис. 4. 2. 5 Hydra. Журнал банов

При 4 попытки ssh-сервер блокирует соединение:

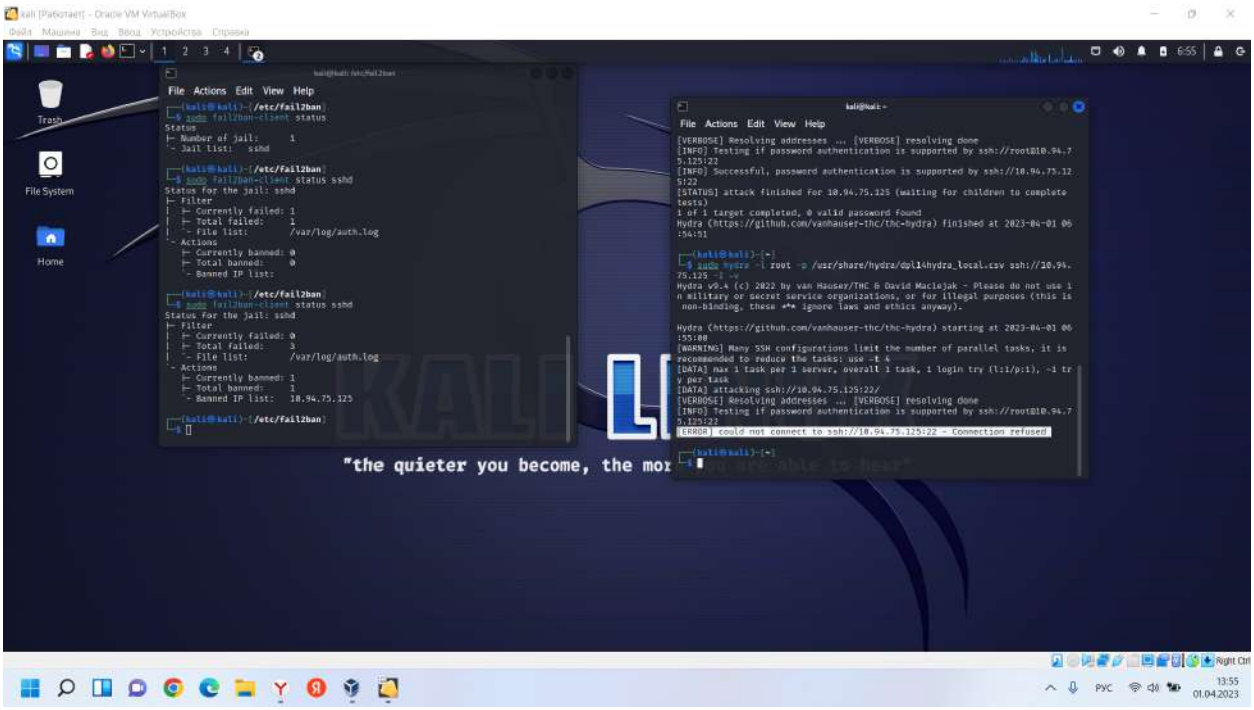

Рис. 4. 2. 6 Hydra. Журнал банов

При отключении fail2ban. Hydra начинает подбирать пароли:

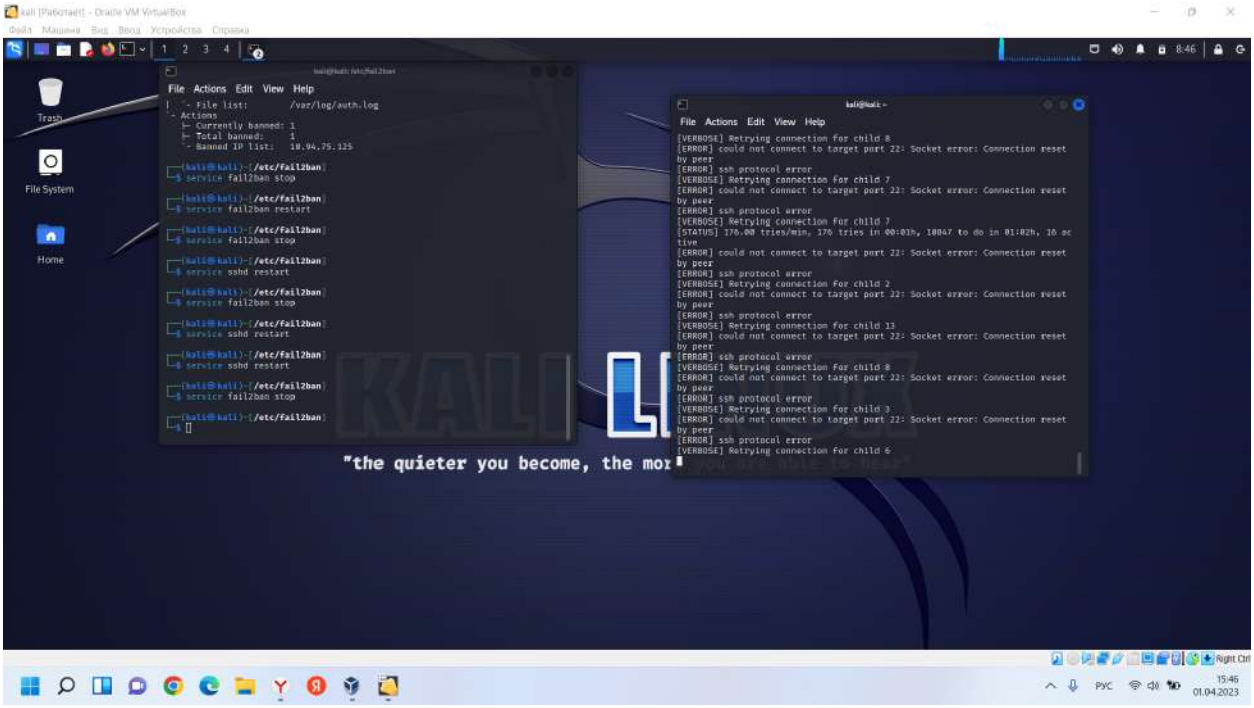

Рис. 4. 2. 7 Hydra. Подбор пароля

Практическая работа "Fail2Ban и Dos/DDoS attack" на примере nginx.

Цель работы:

1. Научиться конфигурировать Fail2Ban для отражения атак Dos/DDoS на nginx.

Задача:

- Организовать простую-тестовую атаку DoS.
- Защитить сервер от DoS/DDoS атак через встроенные возможности nginx.
- Защитить сервер от DoS/DDoS атак с помощью fail2ban при помощи iptables в автоматическом режиме.
- Защитить сервер от DoS/DDoS атак с помощью fail2ban при помощи ipset в автоматическом режиме.

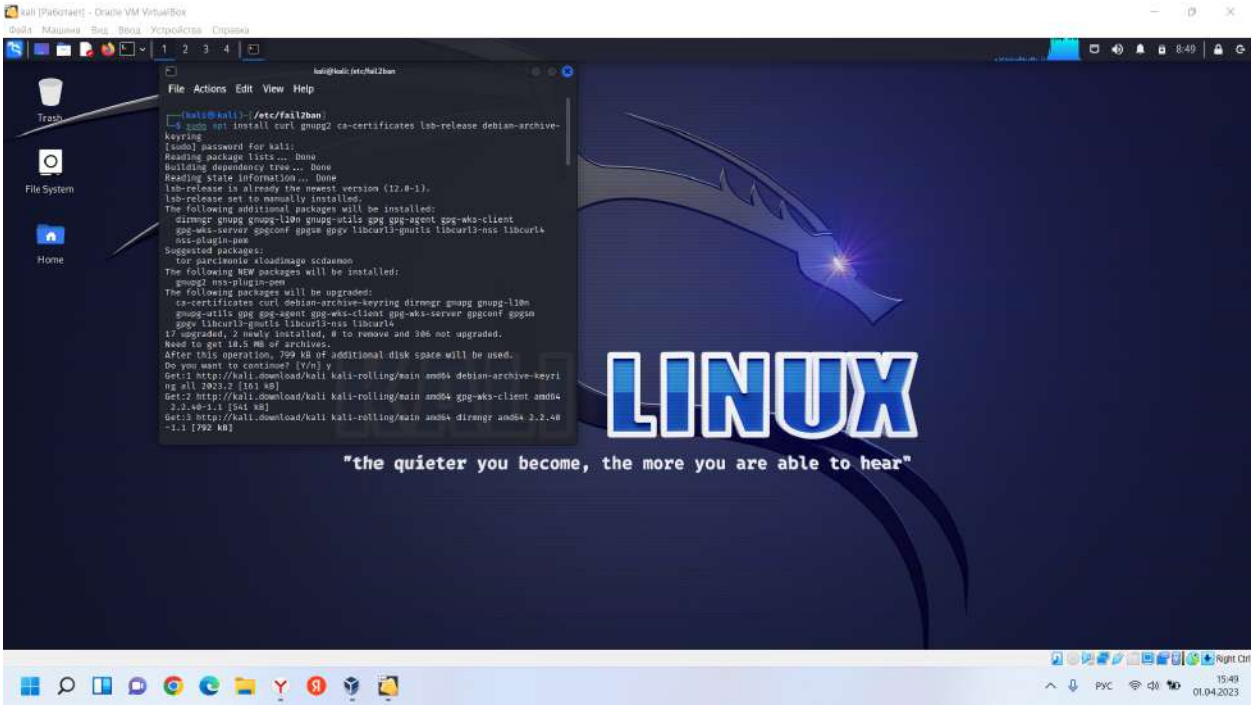

Рис. 4. 3. 1. Установка пакетов, необходимых для подключения apt-репозитория

Рис. 4. 3. 2. Импортирование официального ключа, используемого apt для проверки подлинности пакетов

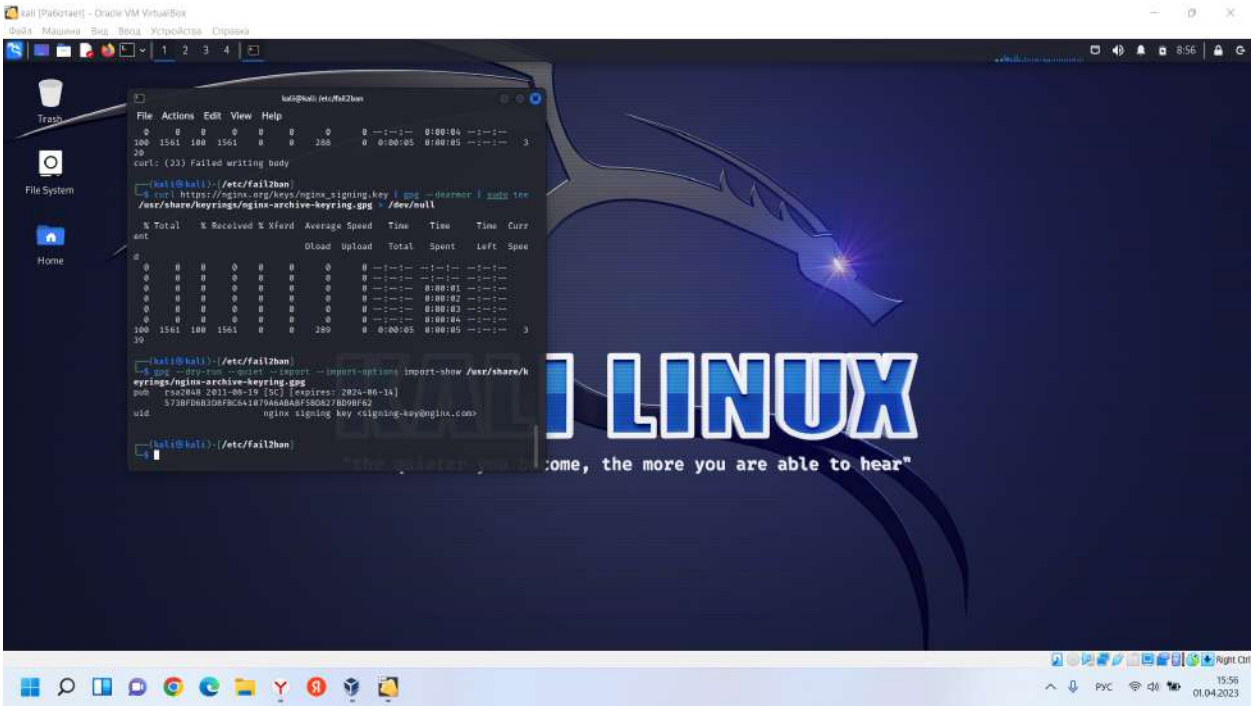

Рис. 4. 3. 3. Проверка официального ключа, используемого apt для проверки подлинности пакетов

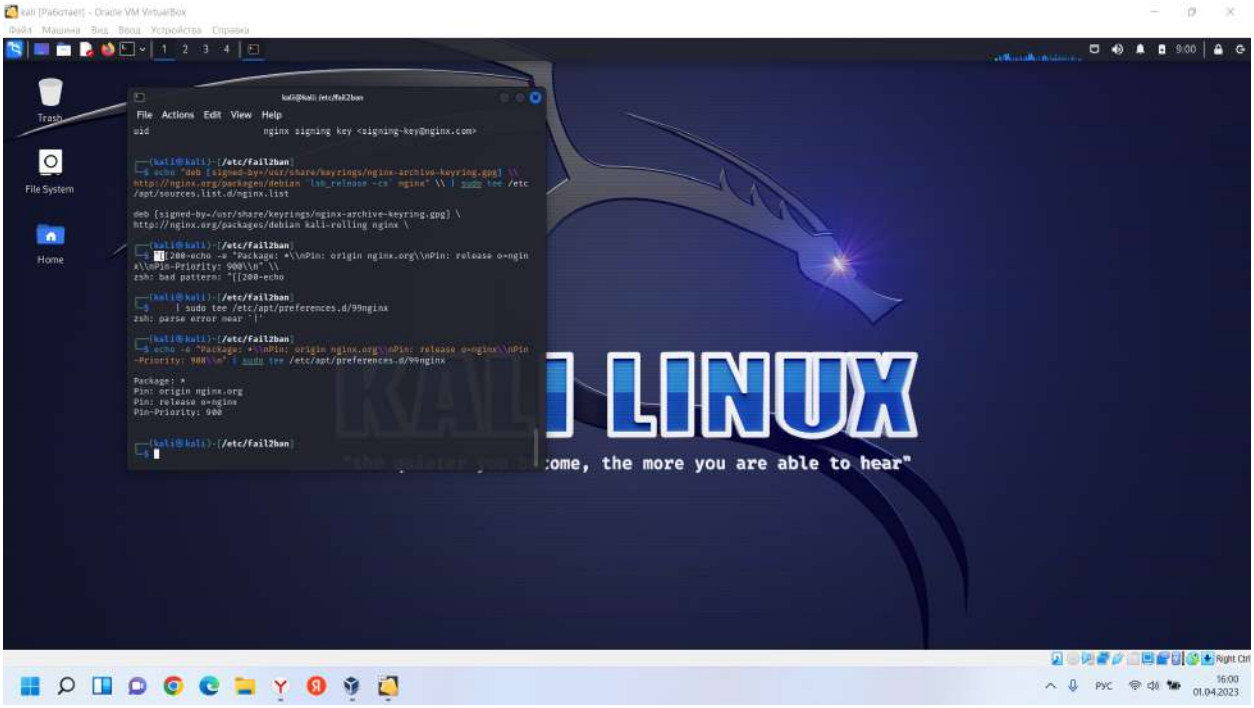

Рис. 4. 3. 4. Настройка закрепления

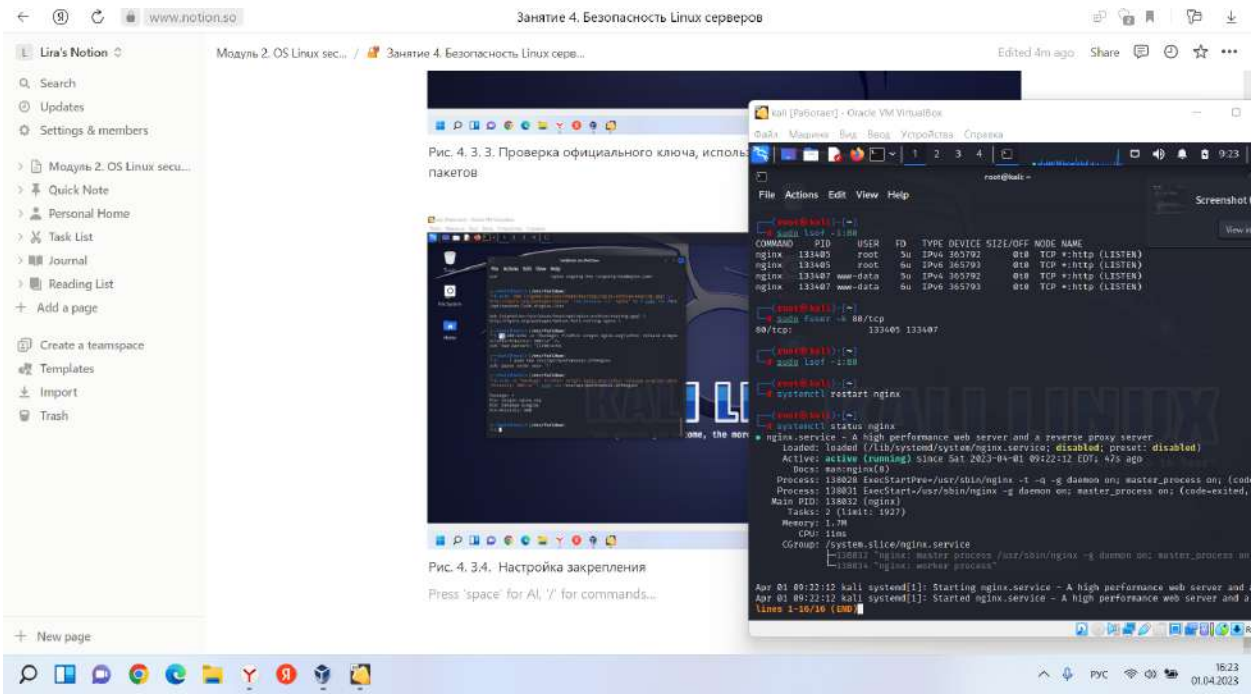

Рис. 4. 3. 5. Nginx запущен

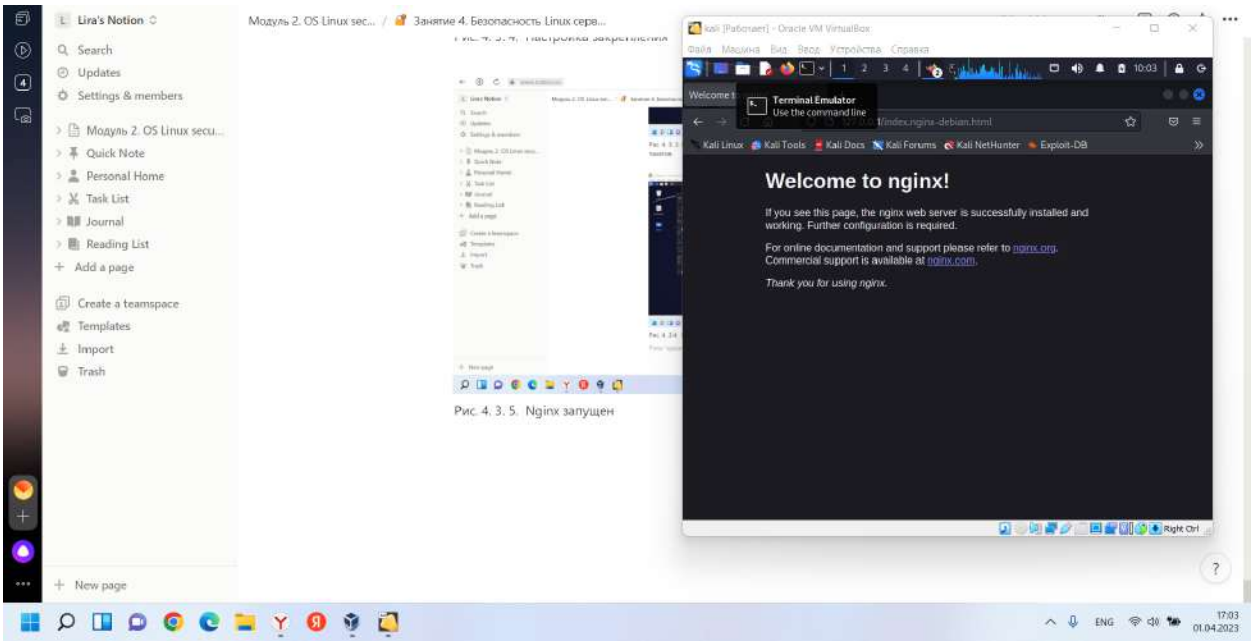

Рис. 4. 3. 5. Nginx запущен

Рис. 4. 3. 6. Стартовая страничка Nginx

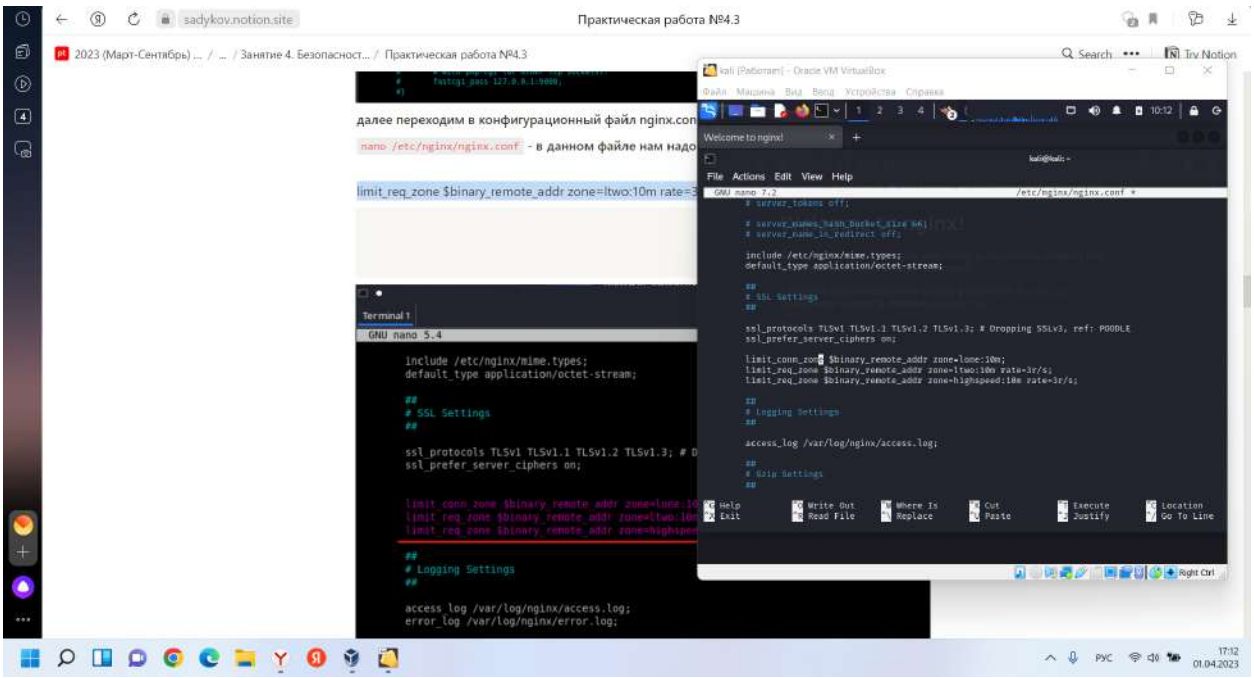

Рис. 4. 3. 7. Изменение конфигурационного файла

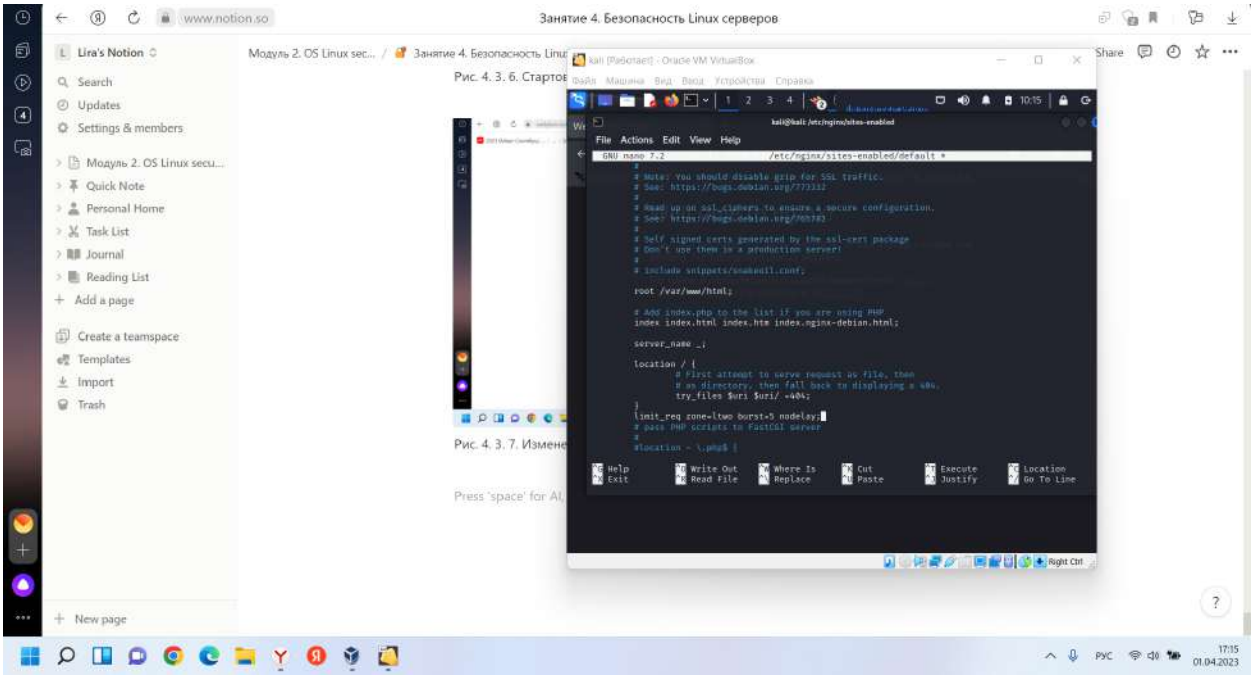

Рис. 4. 3. 8. Изменение конфигурационного файла

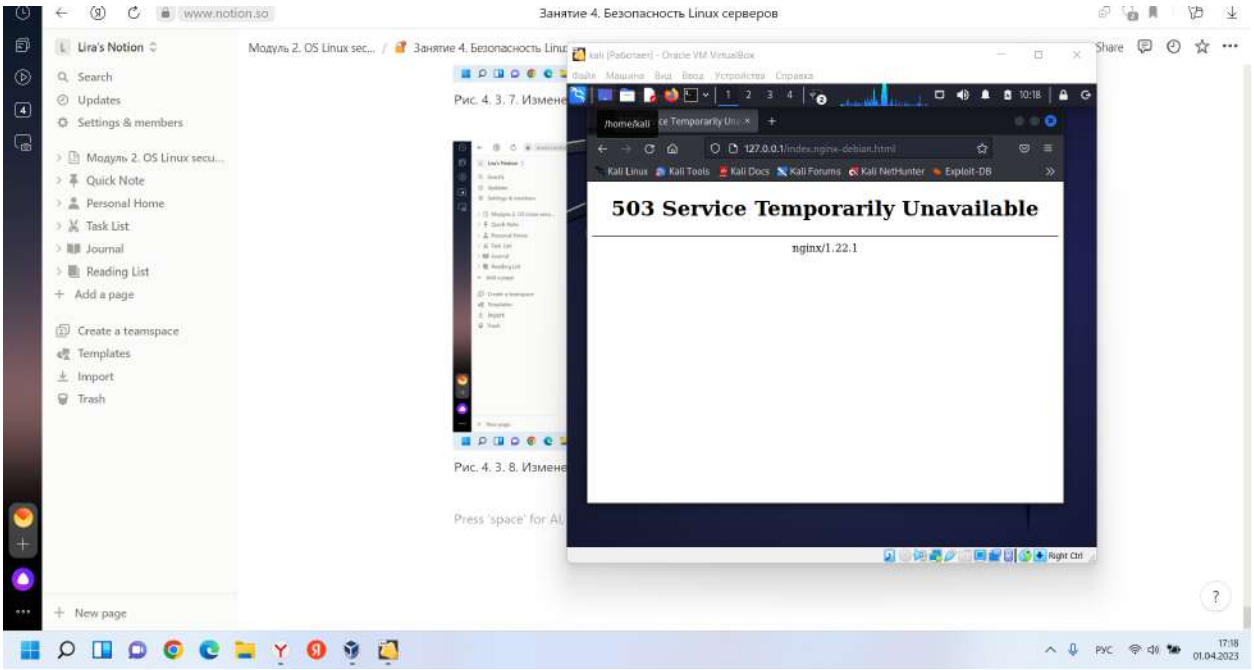

Рис. 4. 3. 9. Ошибка, вызванная многочисленными запросами

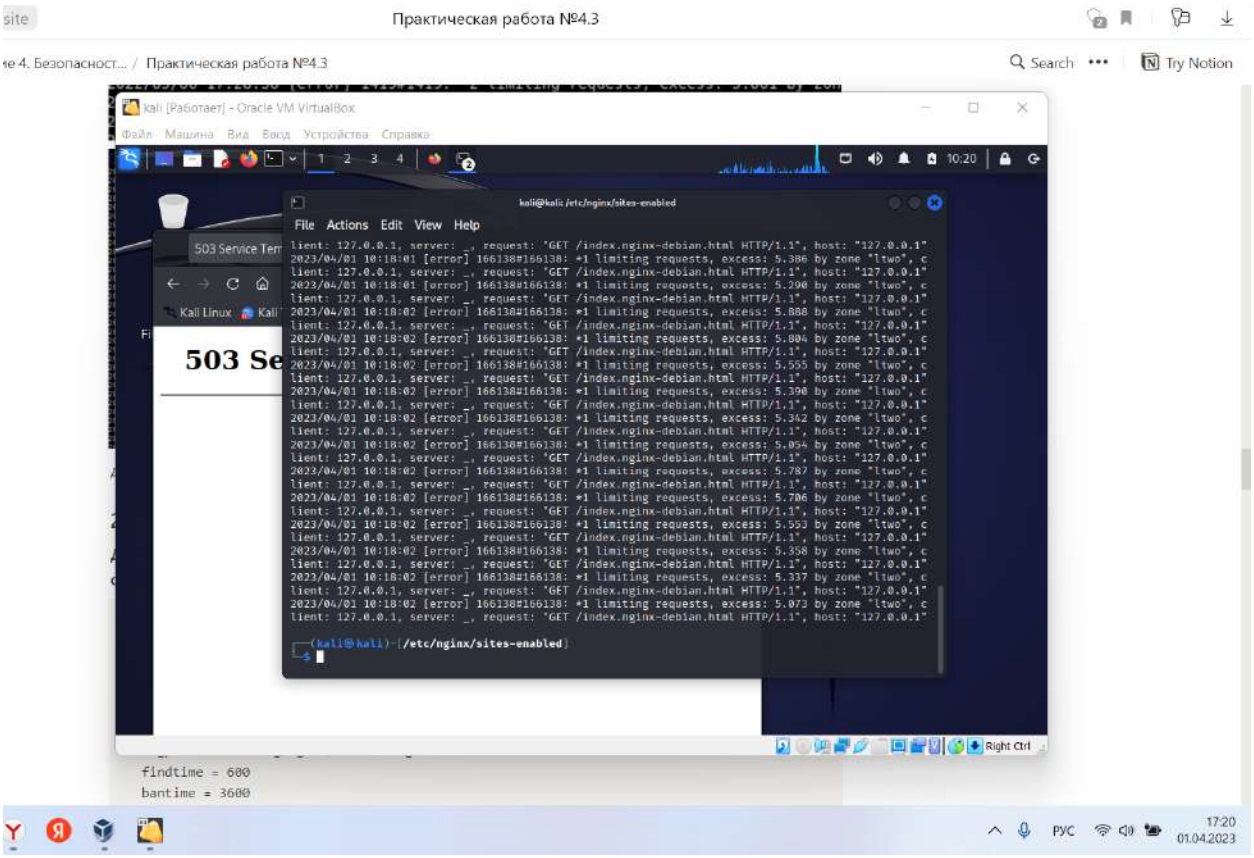

Рис. 4. 3. 10. Логи ошибок

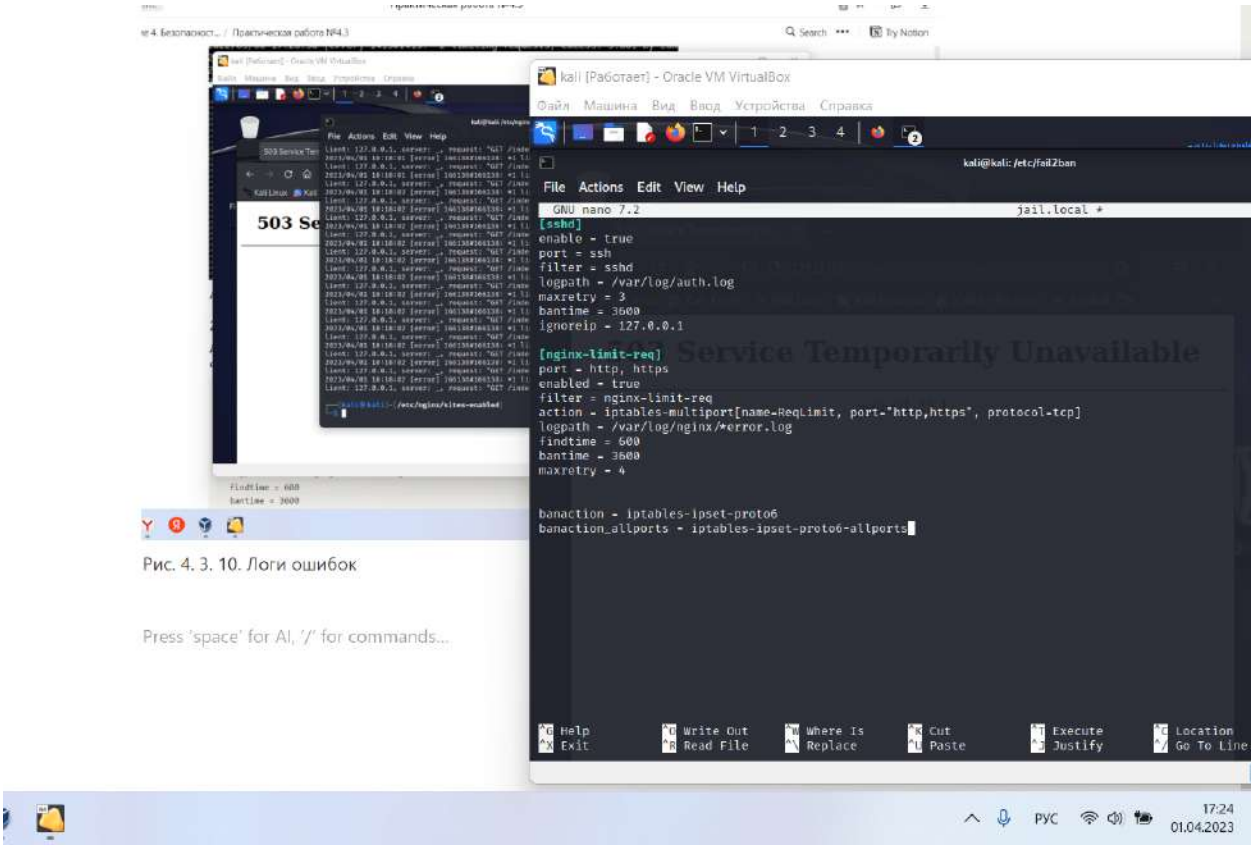

Рис. 4. 3. 10. Логи ошибок

Press 'space' for AI, '/' for commands...

Рис. 4. 3. 11. Настройка Fail2Ban

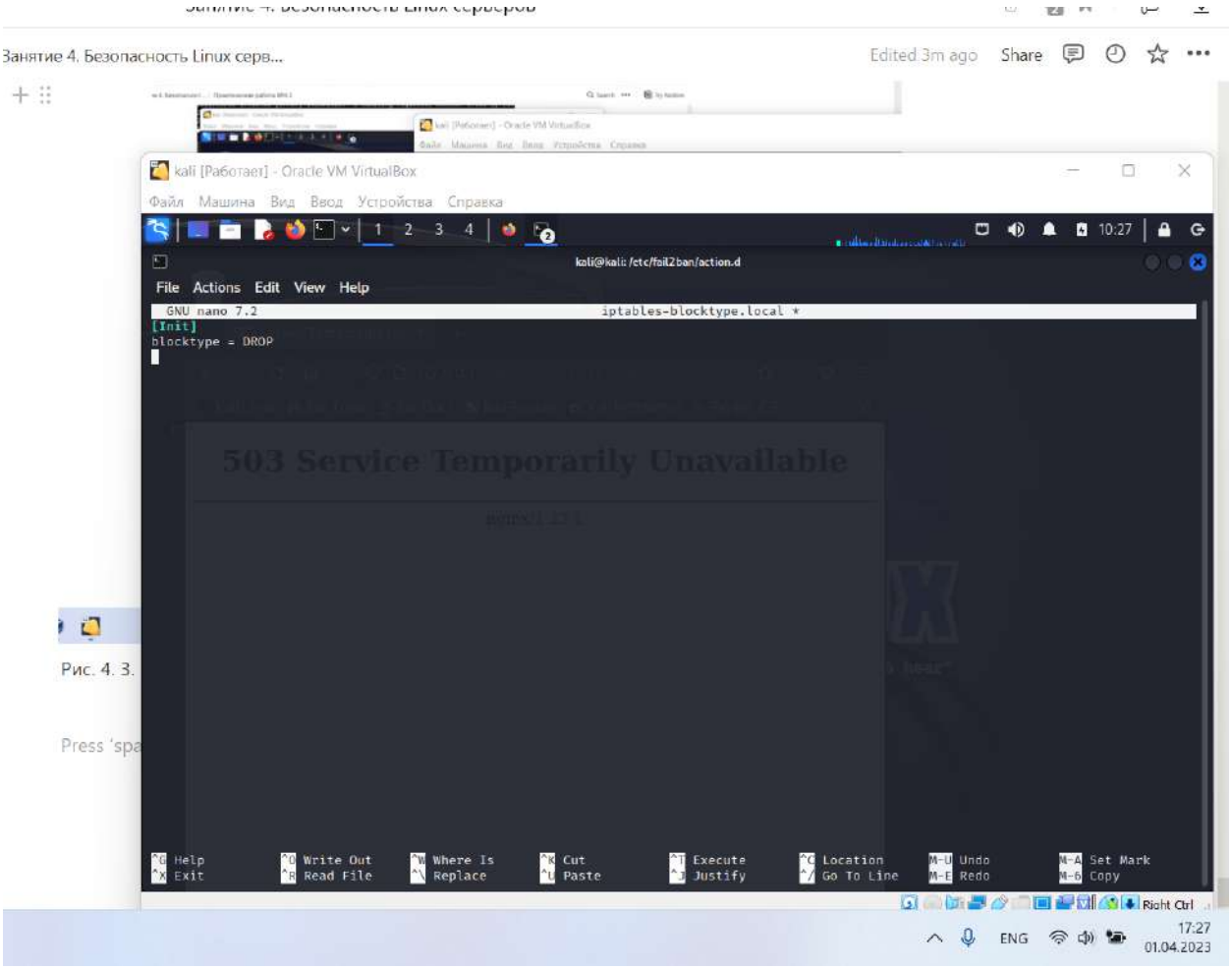

Рис. 4. 3. 12. Настройка нового конфигурационного файла

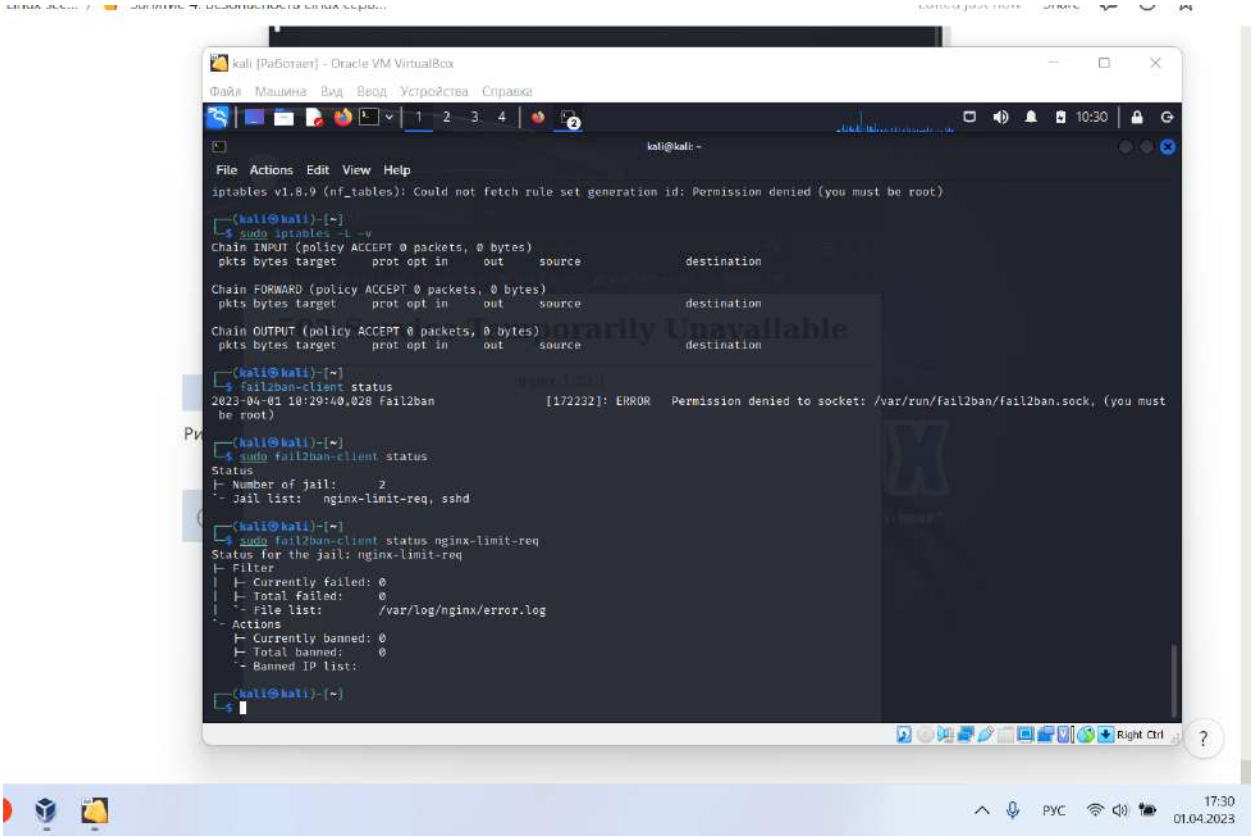

Рис. 4. 3. 13. Проверка настроек fail2ban

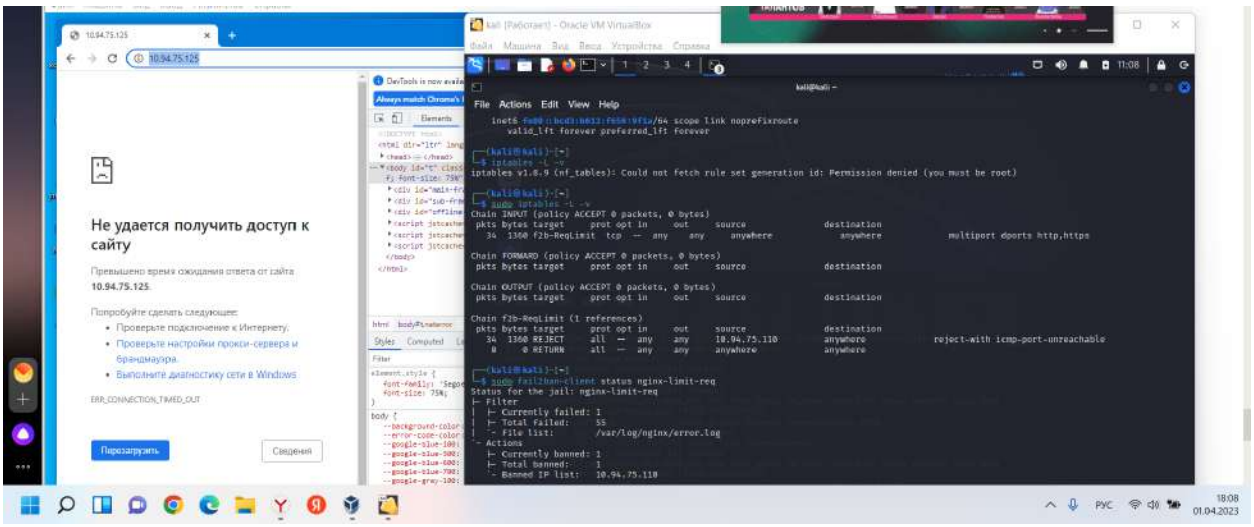

Рис. 4. 3. 14. Блокировка ip-адреса из-за многочисленных запросов