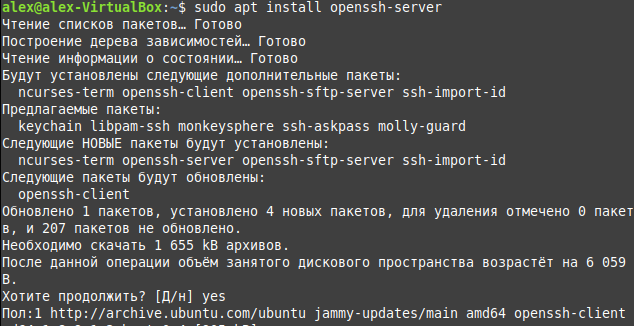
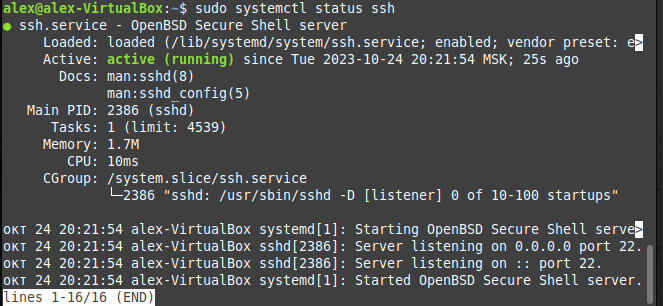
Лабораторная 5

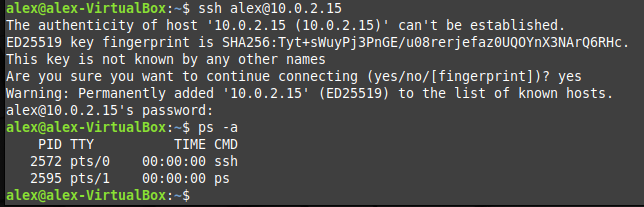
Основное задание

1. Убедитесь, что на виртуальной машине установлен и запущен SSH-сервер.

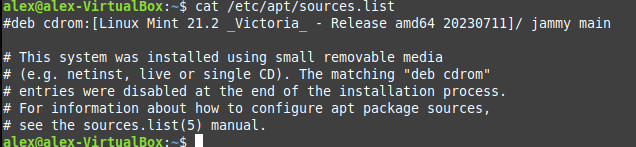




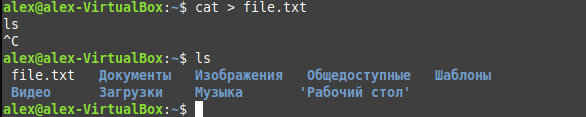
1. подключаемся по SSH на нужный IP к виртуальной машине и далее работаем с системой только через SSH



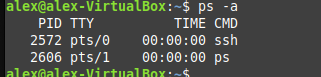
1. Отображаем содержимое /etc/apt/sources.list, используя команду cat



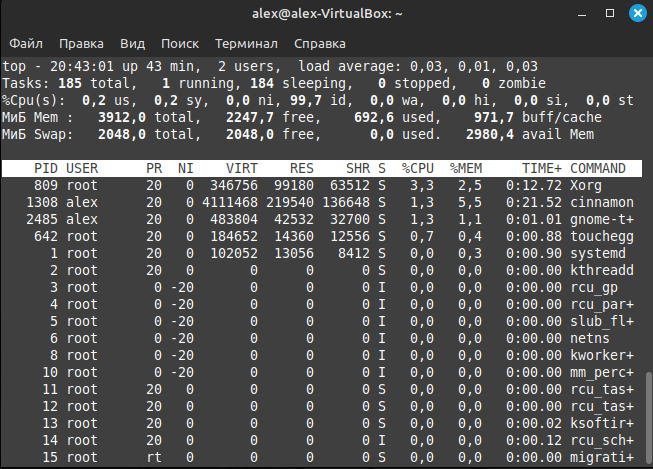
1. С её же помощью и символа “>” создаем файл в домашней директории пользователя.



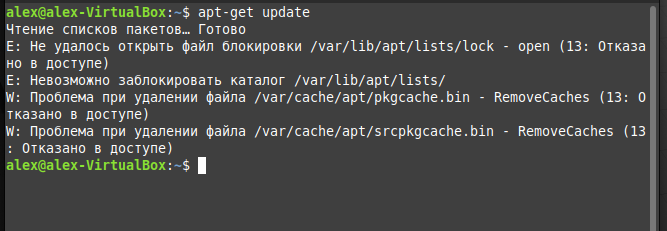
1. Отображаем список процессов.



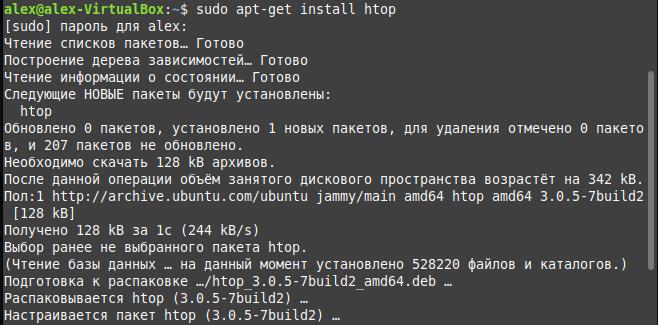
1. Запускаем мониторинг ресурсов системы.



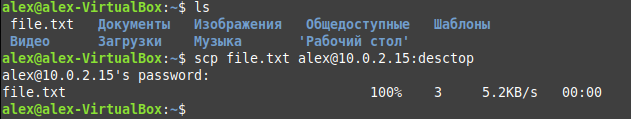
1. Обновляем кэш менеджера пакетов apt-get.



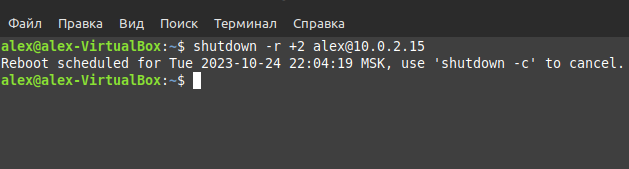
1. Установите удаленно какой-либо пакет из репозитория на ваш выбор.



1. Выполните копирование файла по протоколу SSH с одного компьютера на другой.



1. Перезагрузить удаленный сервер через SSH.





Контрольные вопросы

1. Для чего нужен протокол SSH?

Протокол SSH (Secure Shell) используется для безопасного удаленного доступа к компьютерам и управления удаленными ресурсами. Он обеспечивает шифрование данных и аутентификацию, что делает его надежным инструментом для удаленного администрирования серверов.

1. Почему этот протокол называют защищенным?

Протокол SSH считается защищенным, потому что он обеспечивает шифрование данных, предотвращает перехват и подделку информации во время передачи. Кроме того, SSH использует методы аутентификации для проверки личности пользователей, обеспечивая высокий уровень безопасности при удаленном доступе.

1. Какая информация нужна для того, чтобы подключиться к удаленной машине?

- IP-адрес или доменное имя удаленной машины.

- Имя пользователя на удаленной машине.

- Пароль (или ключи SSH, если используются).

1. Из чего состоит пара ключей?

Пара ключей SSH состоит из двух ключей: открытого и закрытого. Открытый ключ (public key) предоставляется удаленному серверу, а закрытый ключ (private key) хранится только на вашей локальной машине. Эта пара ключей используется для аутентификации и обеспечения безопасности при подключении по SSH.

1. Каковы рекомендуемые действия по безопасному использованию SSH?

- Использование ключей SSH для аутентификации вместо пароля.

- Ограничение доступа к SSH только с известных IP-адресов.

- Регулярное обновление и поддержание SSH-сервера.

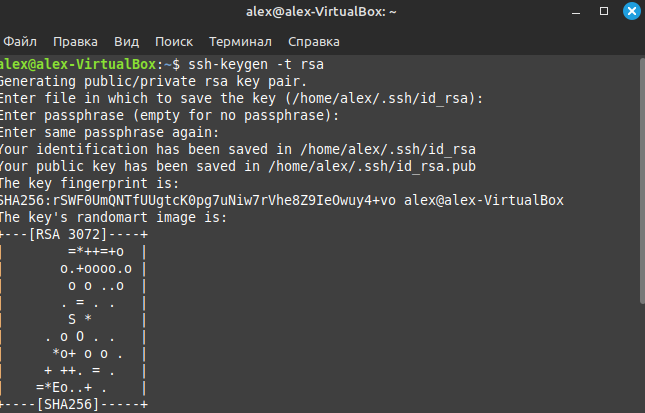
- Использование дополнительных слоев безопасности, таких как файрвол и сетевые меры безопасности.

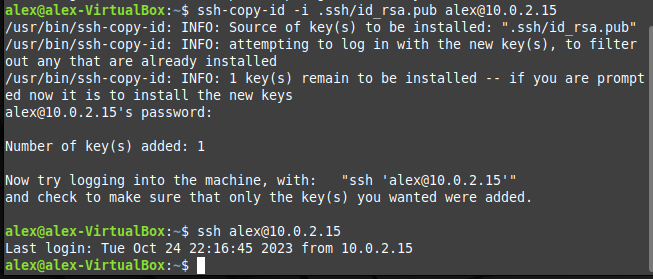
1. Как установить и настроить пакета OpenSSH в Linux и Windows?

В Linux установить пакет OpenSSH через менеджер пакетов (`apt`, `yum`, `zypper`, и т. д.), а в Windows, это может быть настроено через "Параметры" > "Приложения" > "Дополнительные параметры Windows"

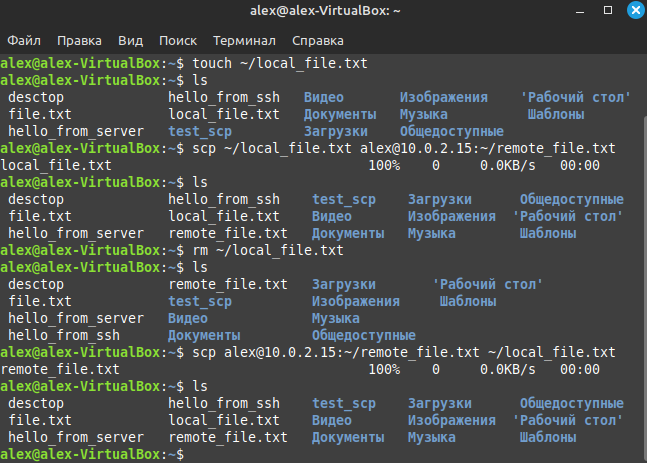
Задания для самостоятельного выполнения

1. Выполните настройку Вашего и виртуального компьютеров так, чтобы возможно было входить с одного на другой по открытому ключу, без явного запроса пароля, по протоколу SSH.

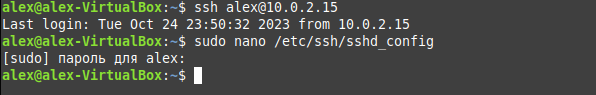


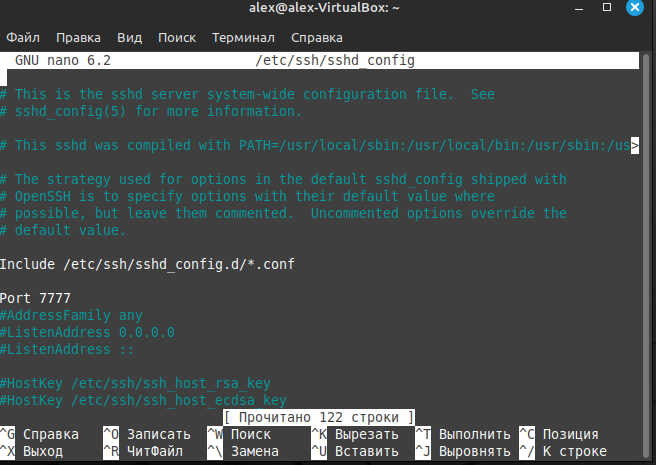


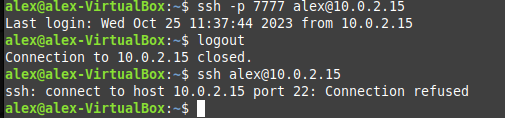
1. Создайте файл в домашней директории локальной машины. Скопируйте его на удаленную машину при помощи утилиты scp. Удалите исходный файл. Скопируйте файл обратно.



1. Измените порт по умолчанию на удаленной машине для сервера SSH. Перезапустите сервер. Проверьте корректность подключения.







1. Сохраните свое подключение на локальной машине при помощи конфигурационного файла. Проверьте работоспособность подключения по имени.
2. (\*) Проанализировать сравнительную скорость ssh-соединения, выполнив следующие замеры:
   1. Выполнить передачу файла через FTP с помощью утилиты wget. Проанализировать проходящие пакеты с помощью утилиты tcpdump(-ХХ). Запомнить скорость передачи.
   2. Выполнить передачу через ssh. Проанализировать проходящие пакеты с помощью утилиты tcpdump(-ХХ). Запомнить скорость передачи. Сравнить передаваемые пакеты и скорости передачи данных.
   3. Включить сжатие ssh и повторить замер скорости. В каждом тесте анализировать результаты для файла состоящего из нулей и для файла состоящего из случайных последовательностей (dd if= /dev/urandom of=file ds=1M count=10), для текстового конфигурационного файла или бинарного файла.