МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение   
высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №1**

**«Организация удаленного доступа в ОС Linux»**

Практическая работа

по дисциплине «Современные технологии программирования»

студента 1 курса группы ПИ-б-о-233(1)

Иващенко Дениса Олеговича

направления подготовки 09.03.04 «Программная инженерия»

|  |  |  |
| --- | --- | --- |
|  |  |  |

Симферополь, 2024

**Цель:** Ознакомиться на практике со средствами удаленного управления в операционной системе Linux. Приобрести опыт и навыки управления удаленным доступом посредством ssh.

**Ход выполнения задания.**

1)Установим Ubuntu Desktop на виртуальную машину VirtualBox.

2) Установим Ubuntu Server на витуальную машину VirtualBox.

3)Перезагрузим сервер и залогинимся используя имя пользователя и пароль, которые мы указывали в процессе установки.

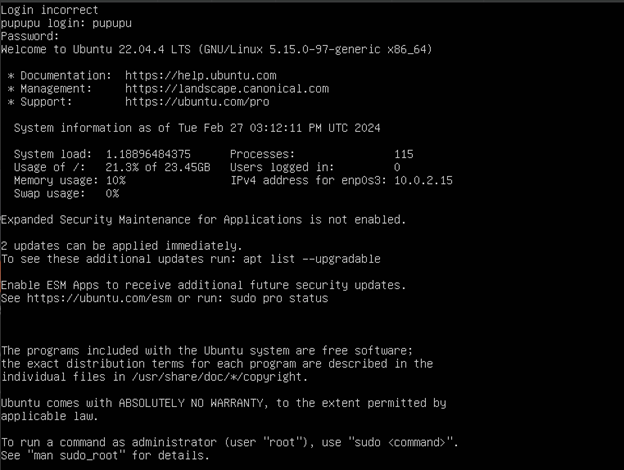


Рисунок №1 – перезагрузка сервера и вход, используя имя пользователя и пароль во время процесса установки.

4)обновим информацию о пакетах и обновим установленные пакеты до последней версии. Используем команду “sudo apt-get update && apt-get upgrade”.

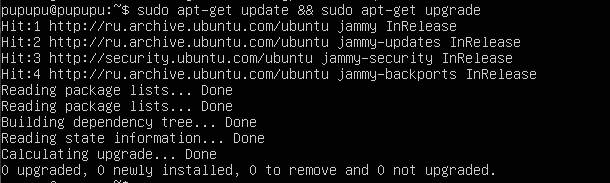


Рисунок №2 – результат команды “sudo apt-get update && apt-get upgrade”.

5)Теперь убедимся, что ssh-сервер установлен и запущен. Для этого используем команду“systemctl status ssh”.

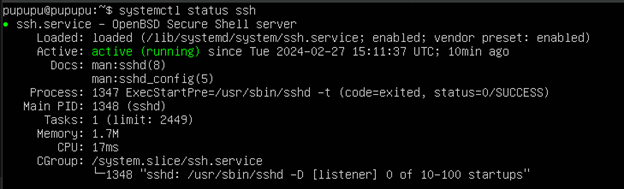


Рисунок №3 – результат команды “systemctl status ssh”.

Доступ за NAT через проброс портов

8)В VirtualBox откроем настройки машины с Ubuntu Server и на вкладке “Сеть” в настройках первого адаптера, в разделе “Дополнительно” нажмем

кнопку “Проброс портов”.

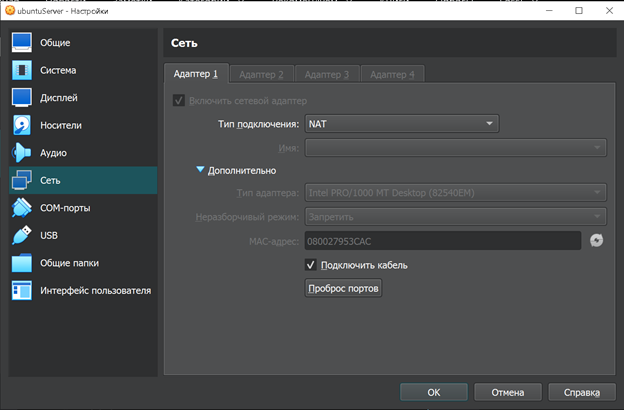


Рисунок №4 – вкладка “Сеть” в настройках Ubuntu Server-a в VirtualBox.

9.1)В появившемся окне нажмем иконку с “+” и введем требуемую информацию: адрес хоста можно поставить стандартный – 127.0.0.1; порт хоста – 22(порт по умолчанию для подключения по ssh); порт гостя – 22(по умолчанию); адрес гостя – это ip-адрес виртуальной машины,здесь мы используем команду“ip a”.

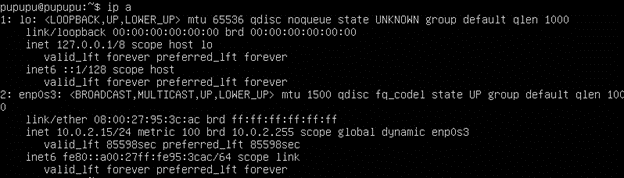


Рисунок №5 – результат команды “ip a”.

9.2)Вот, что у нас получилось в изменениях настроек.

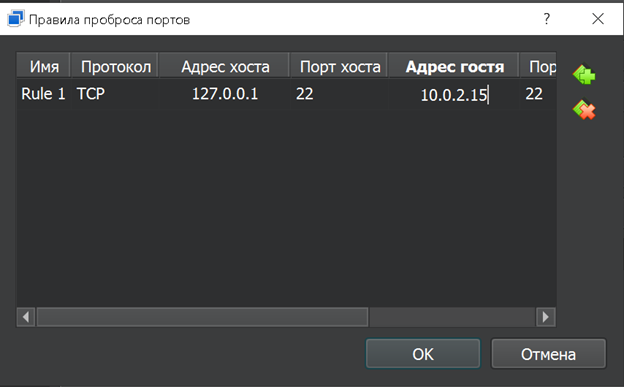


Рисунок №6 – результат настроек.

10)сейчас мы будем подключаться к серверу из хостовой системы по ssh. В данной ситуации мы используем команду ssh [pupupu@127.0.0.1](mailto:pupupu@127.0.0.1)

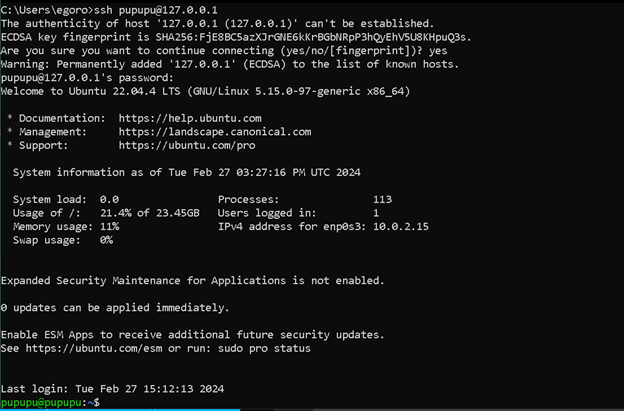


Рисунок №7 – подключение к серверу из хост. системы по ssh

13)Чтобы отключиться от сервера в хостовой системе используем команду “exit”.

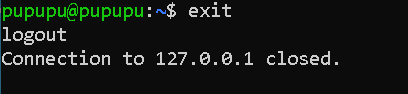


Рисунок №8 – результат команды “exit”.

Доступ к серверу в сети без NAT

14)Теперь зайдем в “Настройки” Ubuntu Server-a в VirtualBox. Зайдем в раздел “Cеть” и поменяем “Тип подключения” на “Сетевой мост”.

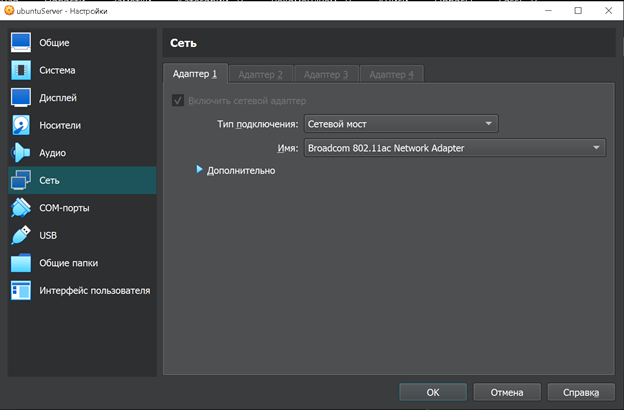


Рисунок №9 – тип подключения (Сетевой мост).

15)посмотрим список сетевых интерфейсов с помощью команды “ip a”.

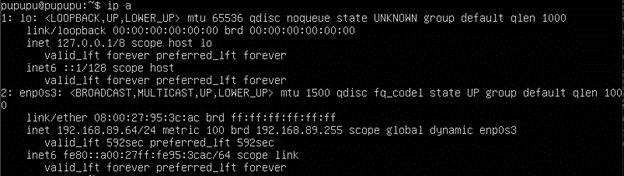


Рисунок №10 – результат команды “ip a”.

16)проверим, что сервер доступен из хостовой ОС при помощи утилиты ping : ping 192.168.89.64(ip-адрес)

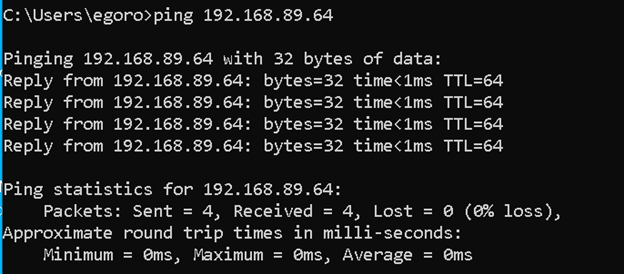


Рисунок №11 – результат “ping”

17)теперь проверим подключение с помощью ssh.

ssh [pupupu@192.168.89.64](mailto:pupupu@192.168.89.64)

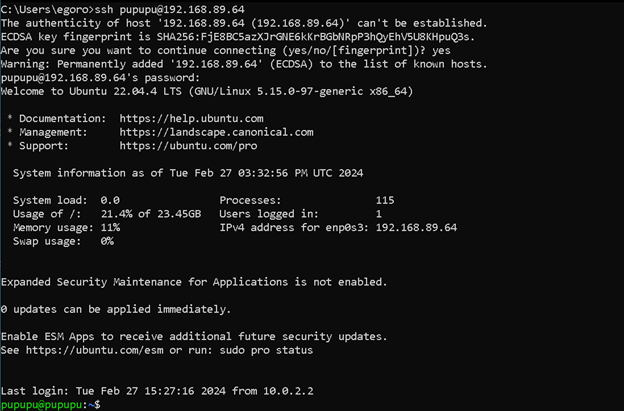


Рисунок №12 – результат подключения к серверу из хост. системы по ssh.

18)выполним команду “ls”



Рисунок №13 – результат команды “ls”

20)На сервере создадим папку “info” в домашнем каталоге.

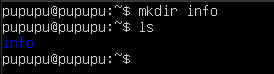


Рисунок №13 – создали папку “info” и проверили есть ли она.

21)На хостовой машине создадим файл “get\_info.py” со следующим содержимым.

import platform

print(platform.uname())

22)используя утилиту scp копируем “get\_info.py” с хостовой машины на сервер в каталог “info”Для этого пропишем следующее: scp get\_info.py [pupupu@192.168.89.64:/home/pupupu/info/](mailto:pupupu@192.168.89.64:/home/pupupu/info/)



Рисунок №14 – результат команды scp

24) проверим появился ли файл “get\_info.py” на сервере(зайдем в папку “cd info” и пропишем команду “ls”).



Рисунок №15 – проверили, что существует такой файл на сервере.

25)переходим в каталог “info” и запускаем скрипт, при этом результат его работы перенаправим в файл “log.txt”.

python3 get\_info.py > log.txt



26)Выполним копирование файлов с сервера на хостовую систему. В данной ситуации используем “scp -r [pupupu@192.168.89.64:/home/pupupu/info](mailto:pupupu@192.168.89.64:/home/pupupu/info) .”.Перейдем до рабочего стола, чтобы папка появилась на рабочем столе.



Рисунок №16 – результат команды “scp”.

27)Откроем файл “log.txt” и посмотрим содержимое.

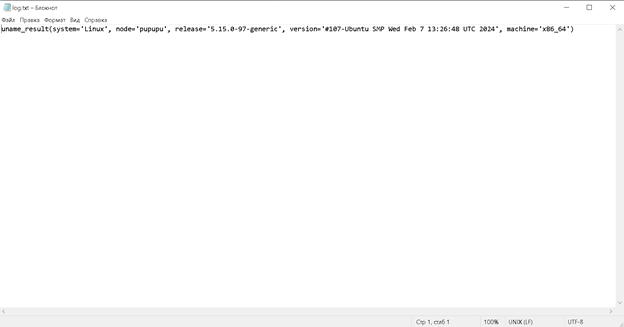


Рисунок №17 – просмотр содержимого файла “log.txt”

Обмен файлами с сервером в интерактивном режиме (sftp)

28) На хостовой машине модифицируем файл “get\_info.py”

import platform

uname = platform.uname()

print(f"System: {uname.system}")

print(f"Node Name: {uname.node}")

print(f"Release: {uname.release}")

print(f"Version: {uname.version}")

print(f"Machine: {uname.machine}")

print(f"Processor: {uname.processor}")

29)Подключимся к серверу при помощи утилиты sftp для интерактивного обмена файлами с сервером.

sftp [pupupu@192.168.89.64](mailto:pupupu@192.168.89.64)

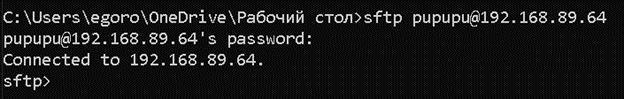


Рисунок №18 – результат команды sftp

30)Введем команду “help”.

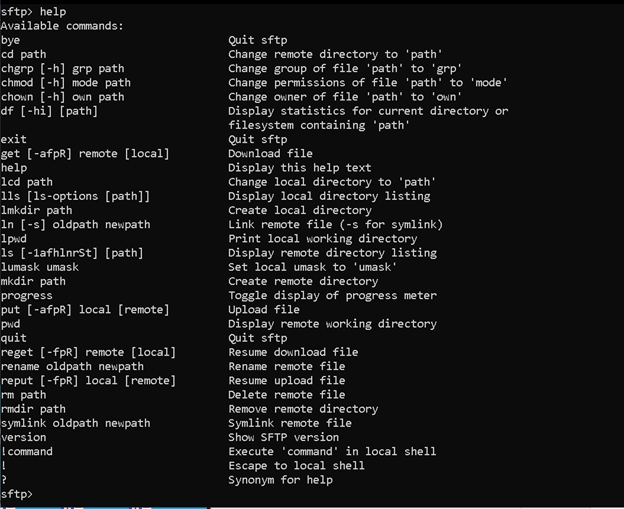


Рисунок №19 – результат команды “help”.

31)Используем команду “put”, чтобы скопировать локальный файл “get\_info.py” на сервер.

put get\_info.py /home/pupupu/info



Рисунок №20 – результат команды “put”.

32) запустим его через ssh-терминал



Рисунок №21 – результат команды python3 get\_info.py > log.txt

33)Используем команду “get” в терминале с запущенным sftp, чтобы забрать с сервера файл “log.txt” с выводом программы.

get /home/pupupu/info/log.txt



Рисунок №22 – результат команды “get”

34)Завершаем сеанс командой “exit”.



Рисунок №23 – результат команды “exit”.

Обмен файлами в графическом режиме (sftp)

35)Запустим виртуальную машину с Ubuntu Desktop

36)В настройках VirtualBox, для этой машины, установим “Тип подключения” – “Сетевой мост”.

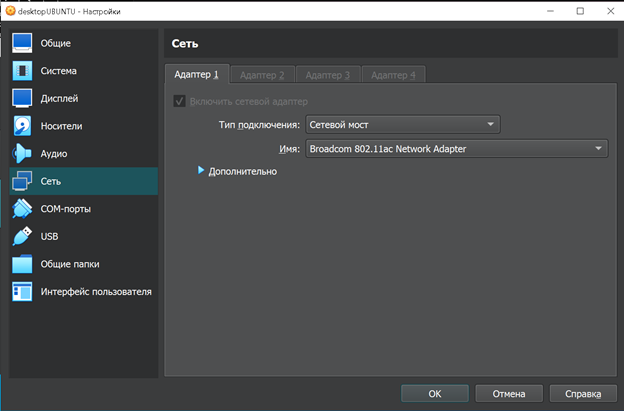


Рисунок №24 – настройки

37)встроенный файловый менеджер Ubuntu Desktop может без проблем подключится к удаленному серверу и с удаленными файлами можно будет работать также, как и со своими собственными:

sftp://pupupu@192.168.89.64/~

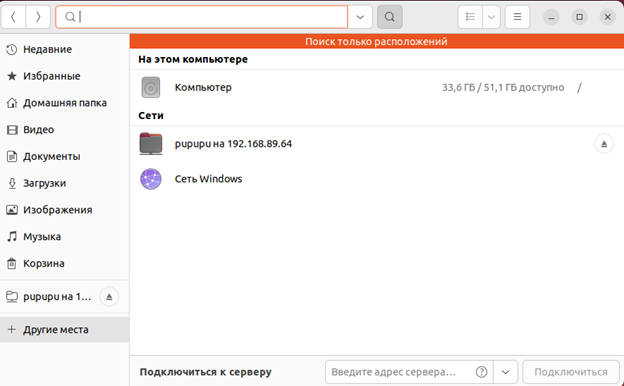


Рисунок №25 – результат “sftp://pupupu@192.168.89.64/~”

38)установим программу WinSCP, заполнив поля, у нас выходит следующее окно, после подключения.

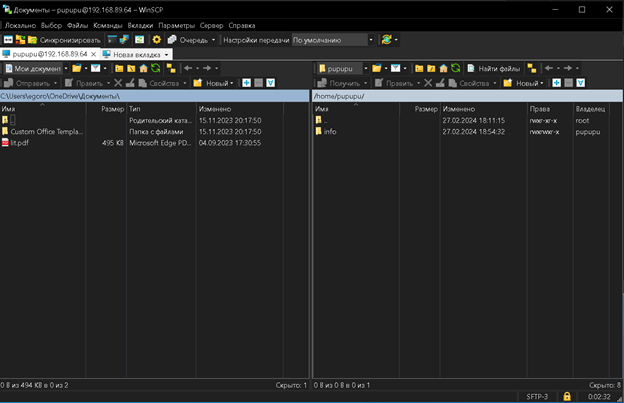


Рисунок №26 – WinSCP

41)Запустим виртуальную машину с Ubuntu Server-ом.

42)Из хостовой машины подключимся к серверу по ssh.

43)выполним базовые настройки безопасности ssh-сервера. Для этого отредактируем конфигурационный файл “/etc/ssh/sshd\_config” и его мы открываем через sudo nano.Заменяем строку “#Post 22” на “Port 6543”.

Добавляем строку “Protocol 2”.Заменяем строку “PermitRootLogin prohibit-password” на “PermitRootLogin no”. Заменяем строку “#PermitEmptyPasswords no” на “PermitEmptyPasswords no”.

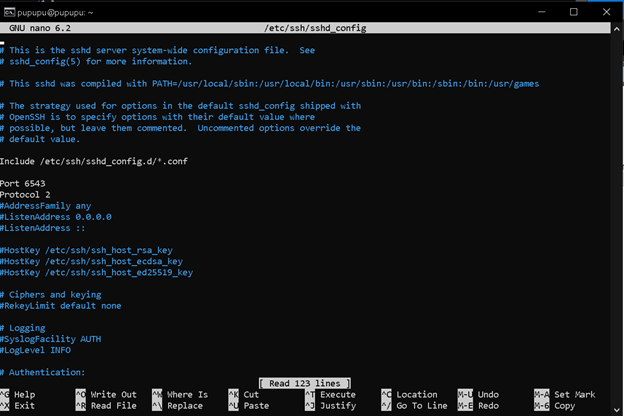


Рисунок №27 – замена строк в “/etc/ssh/sshd\_config”.

После внесенных изменений мы выходим и сохраняем файл. Теперь проверим с помощью команды “sudo sshd -t”.



Рисунок №28 – результат команды “sudo sshd -t”.

45)Теперь настроим доступ для нашей админской машины. Для начала ограничим доступ для админского аккаунта только своим ip-адресом Это можно делать, т.к. по условию у нас фиксированный ip и он внезапно не изменится. Если это произойдёт, мы потеряем удалённый доступ к машине.

Для этого снова откройте файл "/etc/ssh/sshd\_config" и добавим строку:

AllowUsers = [pupupu@192.168.89.64](mailto:pupupu@192.168.89.64)

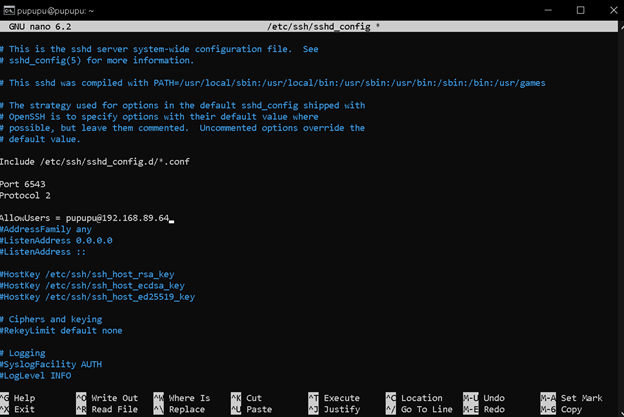


Рисунок №29 – добавили строку AllowUsers

46)Завершаем подключение к серверу, а затем пробуем подключаться к нему по новому порту.

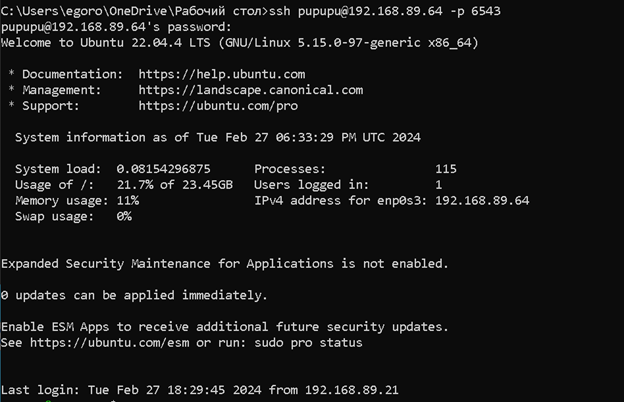


Рисунок №30 – подключение по новому порту

47)Дальше настроим доступ для админского хоста 192.168.89.64 по ключу, а не по паролю.

47.1)генерируем rsa ключ длинной 4096 бит.

Ssh-kegen -t rsa -b 4096

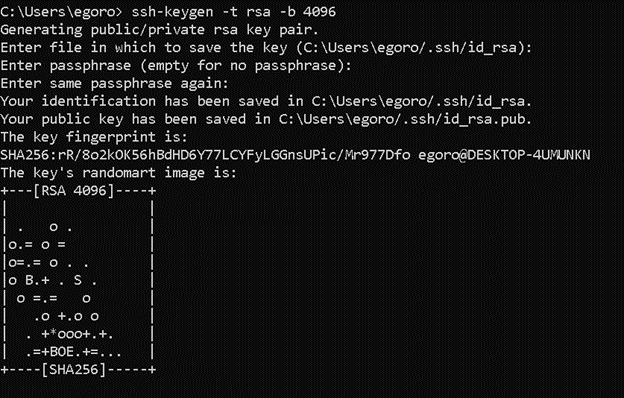


Рисунок №31 – результат генерирование ключа

47.2)передаем серверу публичный ключ в каталог ~/.ssh/.

Используем следующую команду “scp -P 6543 id\_rsa.pub [pupupu@192.168.89.64:.ssh/](mailto:pupupu@192.168.89.64:.ssh/)”.



Рисунок №32 – результат команды “scp”.

47.3)добавляем ключ в файл ~/.ssh/authorized\_keys, чтобы серввер знал о его существовании. Используем следующую команду “cat ~/.ssh/id\_rsa.pub >> /.ssh/authorized\_keys”.



Рисунок №33 – результат команды “cat”

49)теперь попробуем зайти на сервер по ключу, а не паролю. Используем следующую команду: “scp -P 6543 id\_rsa.pub pupupu@192.168.89.64:.ssh/”.

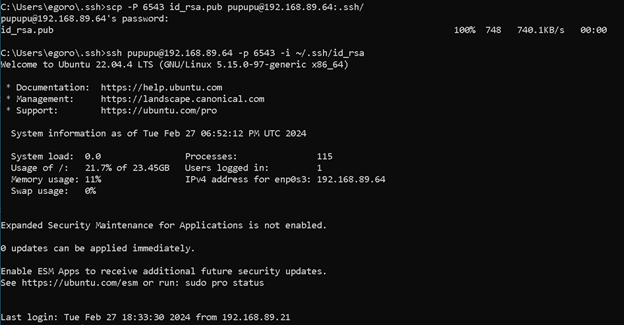
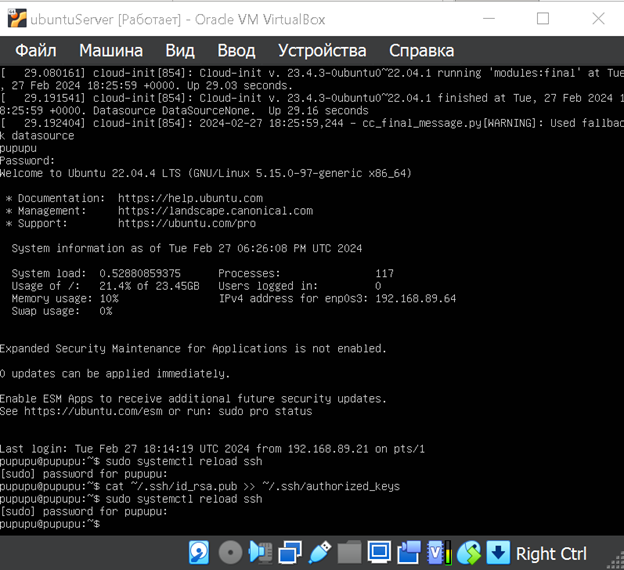
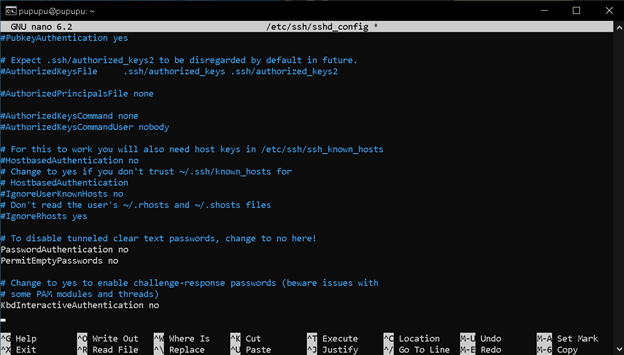


Рисунок №34 – мы вошли на сервер по ключу.

51)Отключим возможность авторизации по паролю. Для этого мы открываем файл “/etc/ssh/sshd\_config” и заменяем “PasswordAuthentication yes” на “PasswordAuthentication no”. Сохранм файл и перезапустим службу ssh: sudo systemctl reload ssh.



Рисунки №35,№36 – реализация вышеописанных действий

52) Создадим нового пользователя с помощью команды: “sudo adduser proger”.

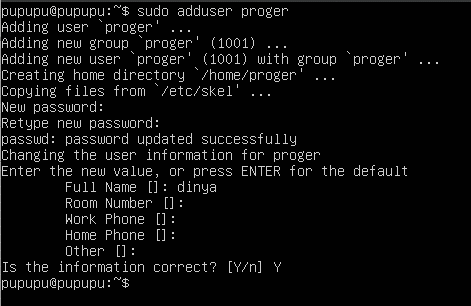


Рисунок №37 – результат команды “sudo adduser proger”.

54)Сделаем для пользователя “proger” исключение и разрешим ему достпу по паролю. Для этого к строке “AllowUsers = [pupupu@192.168.89.64](mailto:pupupu@192.168.89.64)” добавим “proger”. Посел этого в конце страницы добавим следующее

“Match User proger

PasswordAuthentication yes”.

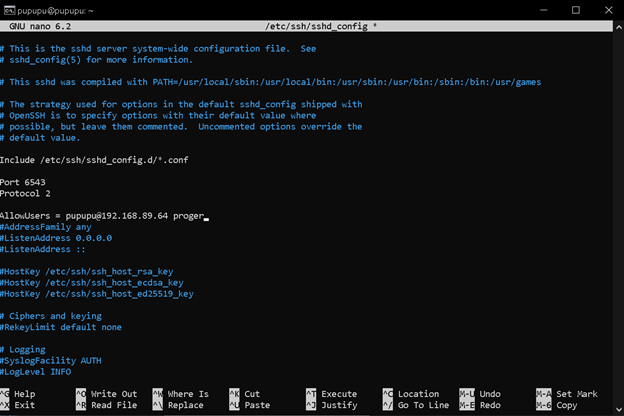


Рисунок №38 – результат изменений строк.

55) Сохранив файл, проверим наличие ошибок через тестовый запуск “sudo sshd -t” и перезапустим службу.

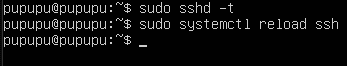


Рисунок №39 – результат команды sudo sshd -t.

56) Выполним подключение к серверу под пользователем “proger”.

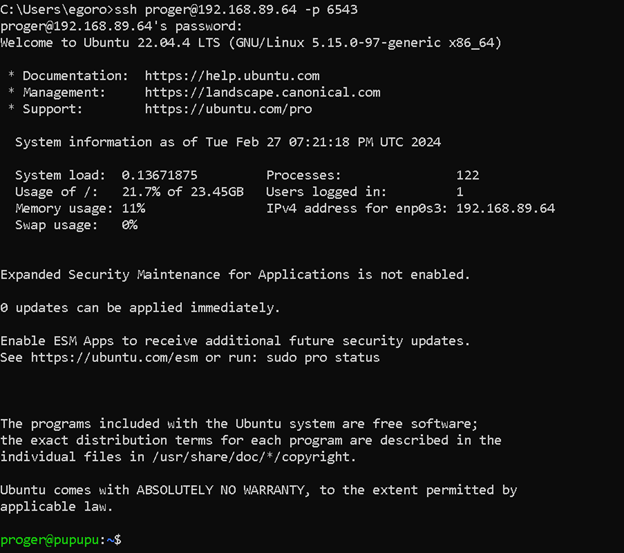


Рисунок №40 – результат подключения.

57)Теперь клонируем в свой домашний каталог репозиторий <https://github.com/VladimirChabanov/google.git>. Используем команду “git clone”.

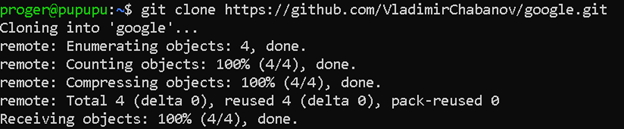
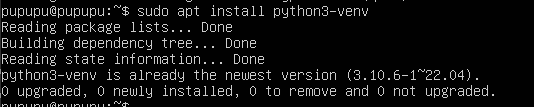


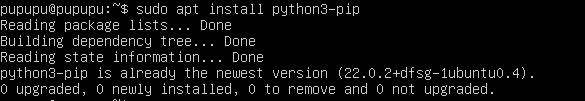
Рисунок №41 – результат команды “git clone”.

58)Под админом выполним установку pip,venv

Sudo apt install python3-pip

Sudo apt install python3-venv





Рисунки №42,№43 – результаты команд.

59) Под пользователем “proger” создадим в клонированном репозитории виртуальное окружение, активируем его, скачаем зависимости перечисленные в файле “requirements.txt” и запустим скрипт “main.py”. Чтобы проверить его работоспособность выполним любой запрос.

Cd google

Python3 -m venv venv

Source venv/bin/activate

Pip install -r requirements.txt

Python main.py

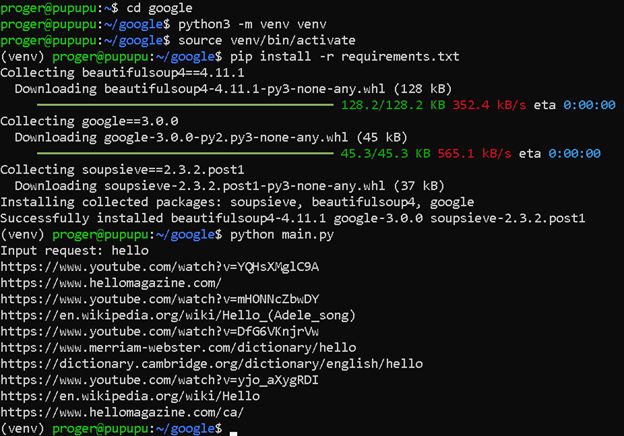


Рисунок №44 – резуьтат команд

**Ответы на вопросы.**

1)Что такое SSH и для чего используется?

SSH (Secure Shell) - это криптографический сетевой протокол, который используется для защищенного удаленного доступа к компьютерам через незащищенную сеть. SSH обеспечивает шифрование данных, аутентификацию и защиту от атак во время передачи данных между клиентом и сервером.

SSH часто используется администраторами систем для удаленного управления серверами и другими устройствами, также для передачи файлов через SCP или SFTP. SSH также позволяет создавать защищенные туннели для безопасной передачи данных между удаленными узлами сети.

2) Где можно поменять значение порта для SSH-сервера и какое там указано значение по умолчанию?

Значение порта для SSH-сервера можно изменить в конфигурационном файле SSH-сервера. Обычно это файл “/etc/.shh/sshd\_config”. Порт, который стоит по умолчанию равен 22.

3) Что нужно сделать, чтобы заблокировать доступ по SSH только одному конкретному пользователю?

Для начала, нам нужно открыть файл “/etc/.ssh/sshd\_config”, в котором мы находим строчку DenyUsers, если ее нет, то мы ее создаем, то есть прописываем. В этой самой строчке мы и пишем имя пользователя.

4)Какой ключ (публичный или приватный) нужно отправить на сервер, если мы хотим настроить доступ к этому серверу по ключу?

Если мы хотим настроить доступ к серверу по ключу, то мы должны отправить на сервер публичный ключ.

5) Как при помощи утилиты scp скопировать содержимое каталога "www" расположенного в текущей папке на удалённый хост "site" в каталог "/var/www/" от имени пользователя "admin"? При условии, что ssh-порт стандартный, а ключ для авторизации расположен по пути ~/.ssh/id\_rsa.

Мы можем прописать команду “scp -r -I ~/.ssh/id\_rsa ./www admin@site:/var/www/”.

**Вывод:** сегодня на практической работе я ознакомился на практике со средствами удаленного управления в операционной системе Linux. Приобрел опыт и навыки управления удаленным доступом посредством ssh.