1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.

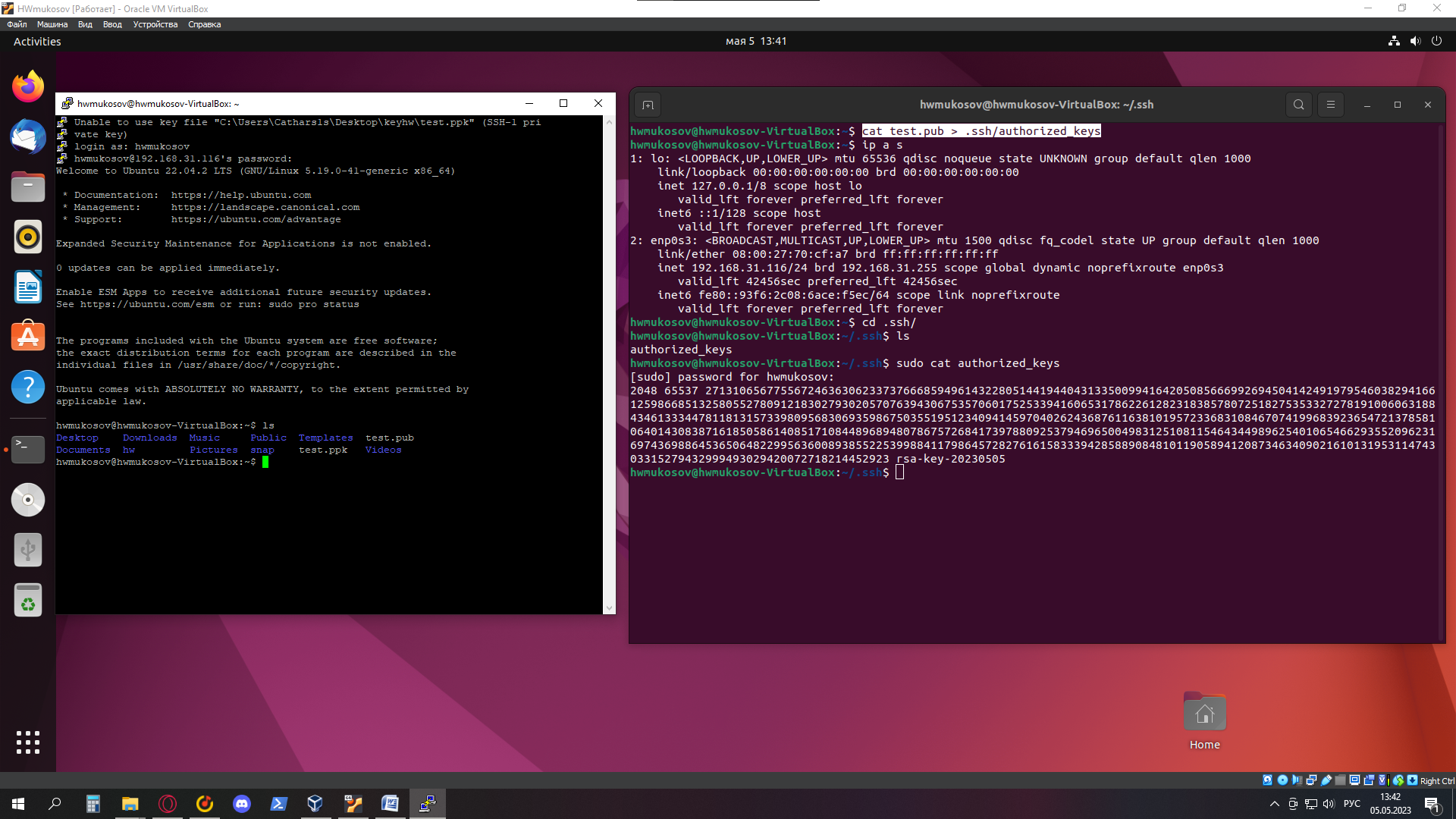
sudo apt-get install sshsudo systemctl status sshdcd /etc/ssh/sudo nano sshd\_config -----раскомментируем PubkeyAuthentication yes и строку с указанием пути к authorized\_keys > сохраняем.

**Переходим на хоста и генерируем ключи через PyTTygen. Сохраняем с именами test**

**Копируем ключи на виртуалку и записываем ключ в authorized\_keys (создаем файл через touch в .ssh/)**

cat test.pub > .ssh/authorized\_keys

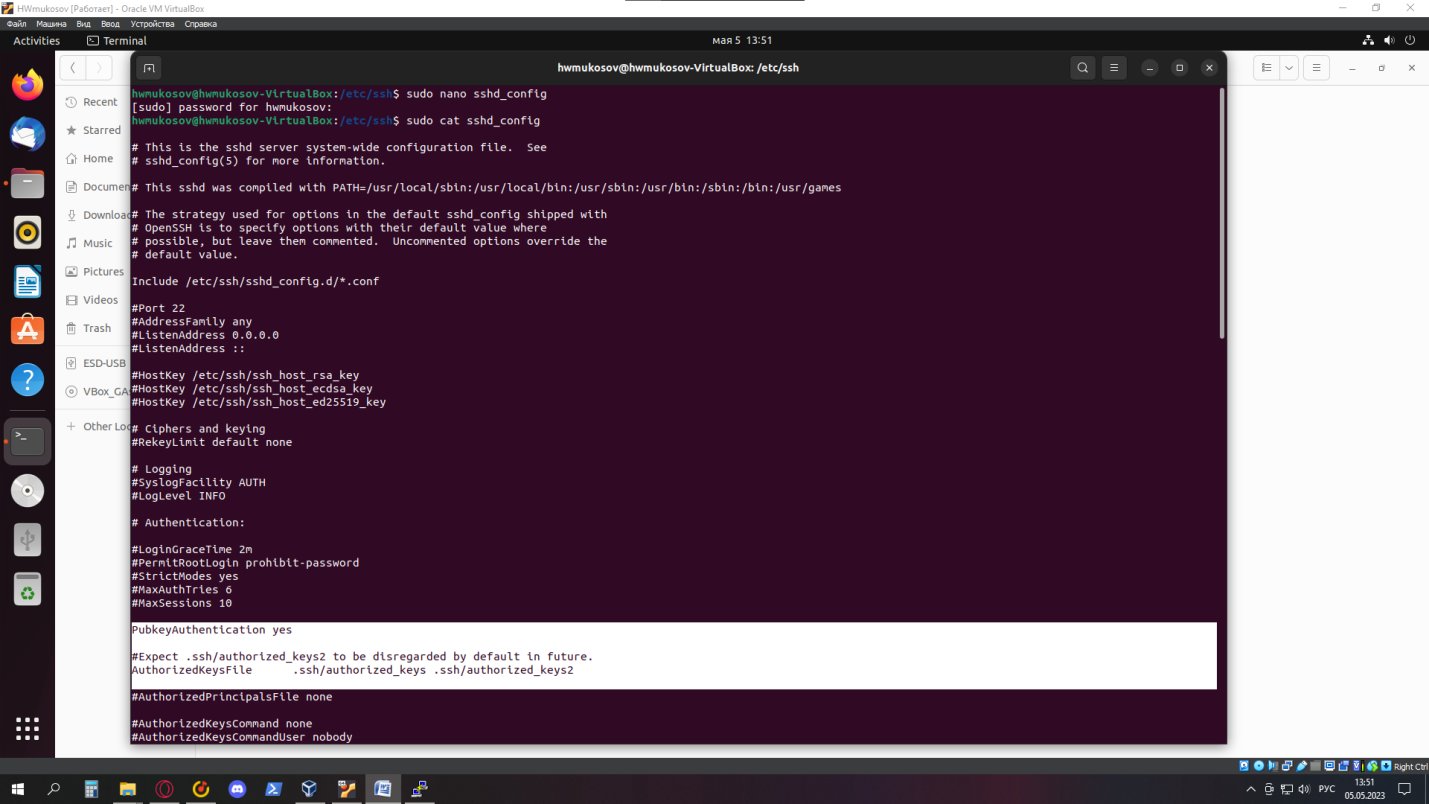
**Пробуем подключиться – успех (в моем случае). Указал в PyTTy адрес и путь до ключа.**



authorized\_keys:

2048 65537 27131065677556724636306233737666859496143228051441944043133500994164205085666992694504142491979546038294166125986685132580552780912183027930205707639430675357060175253394160653178622612823183857807251827535332727819100606318843461333447811813157339809568306935986750355195123409414597040262436876116381019572336831084670741996839236547213785810640143083871618505861408517108448968948078675726841739788092537946965004983125108115464344989625401065466293552096231697436988645365064822995636008938552253998841179864572827616158333942858890848101190589412087346340902161013195311474303315279432999493029420072718214452923 rsa-key-20230505

Sshd\_config:



Изменил только :

PubkeyAuthentication yes

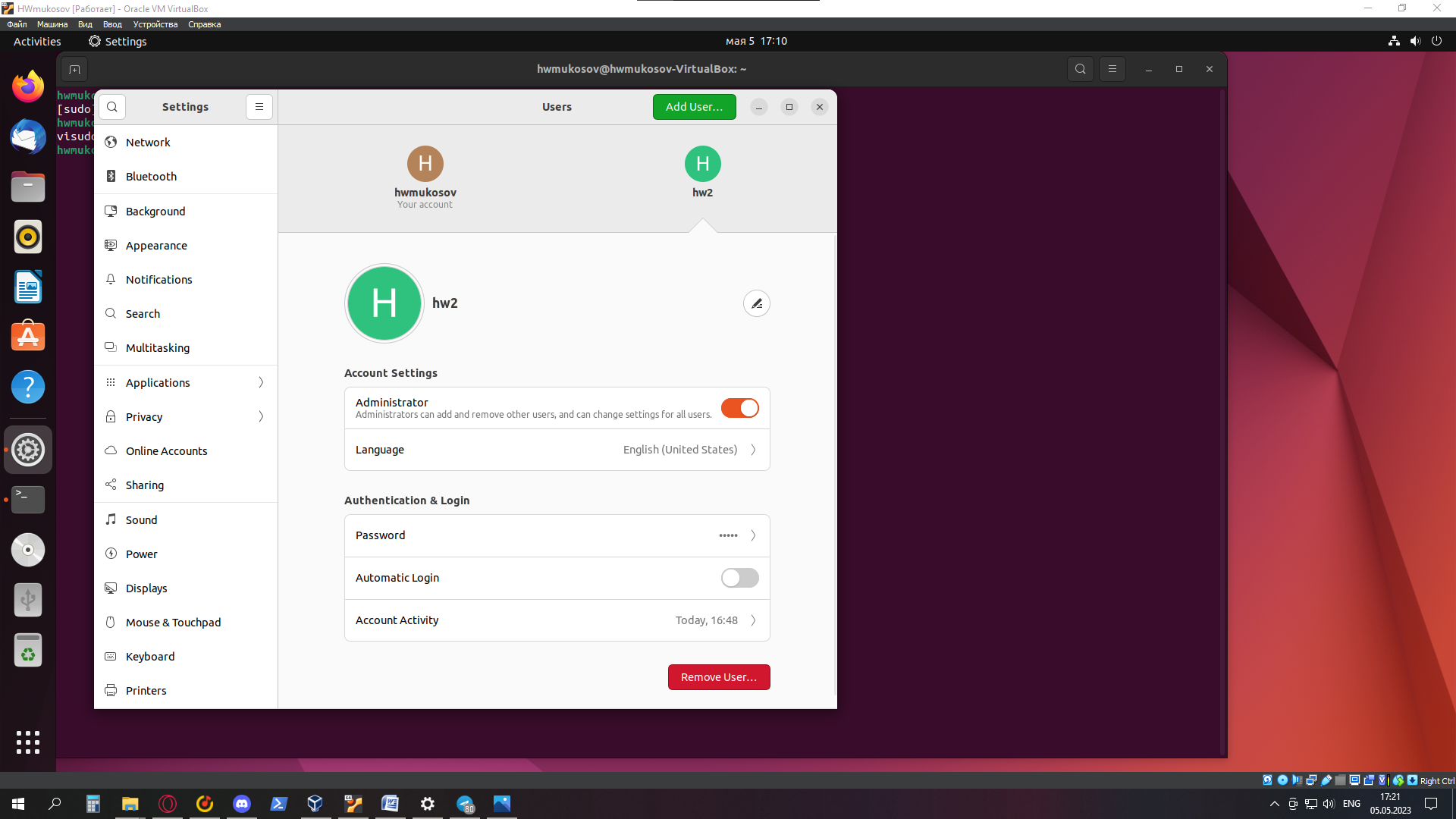
#Expect .ssh/authorized\_keys2 to be disregarded by default in future.

AuthorizedKeysFile .ssh/authorized\_keys .ssh/authorized\_keys2

1. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:
   * 1. */sbin/route*, */sbin/iptables*, */usr/bin/nmap*, */usr/sbin/hping3*
     2. *usr/bin/systemctl*
     3. *sbin/ifup*, */sbin/ifdown*

**Создаем пользователя**

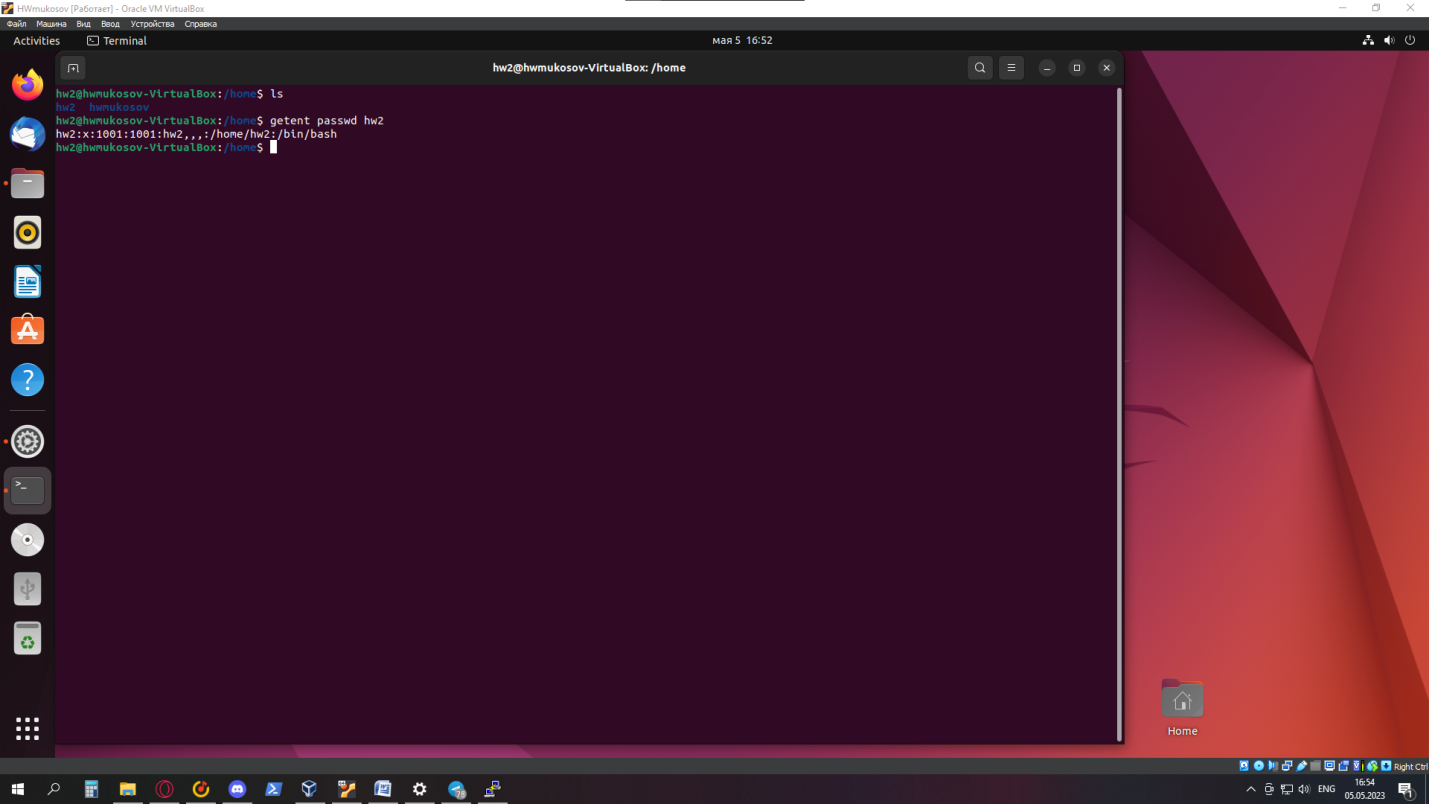
**Делал через GUI т.к. не разобрался как привязать пароль.**



**Заходим под пользователем hw2:**

-su hw2

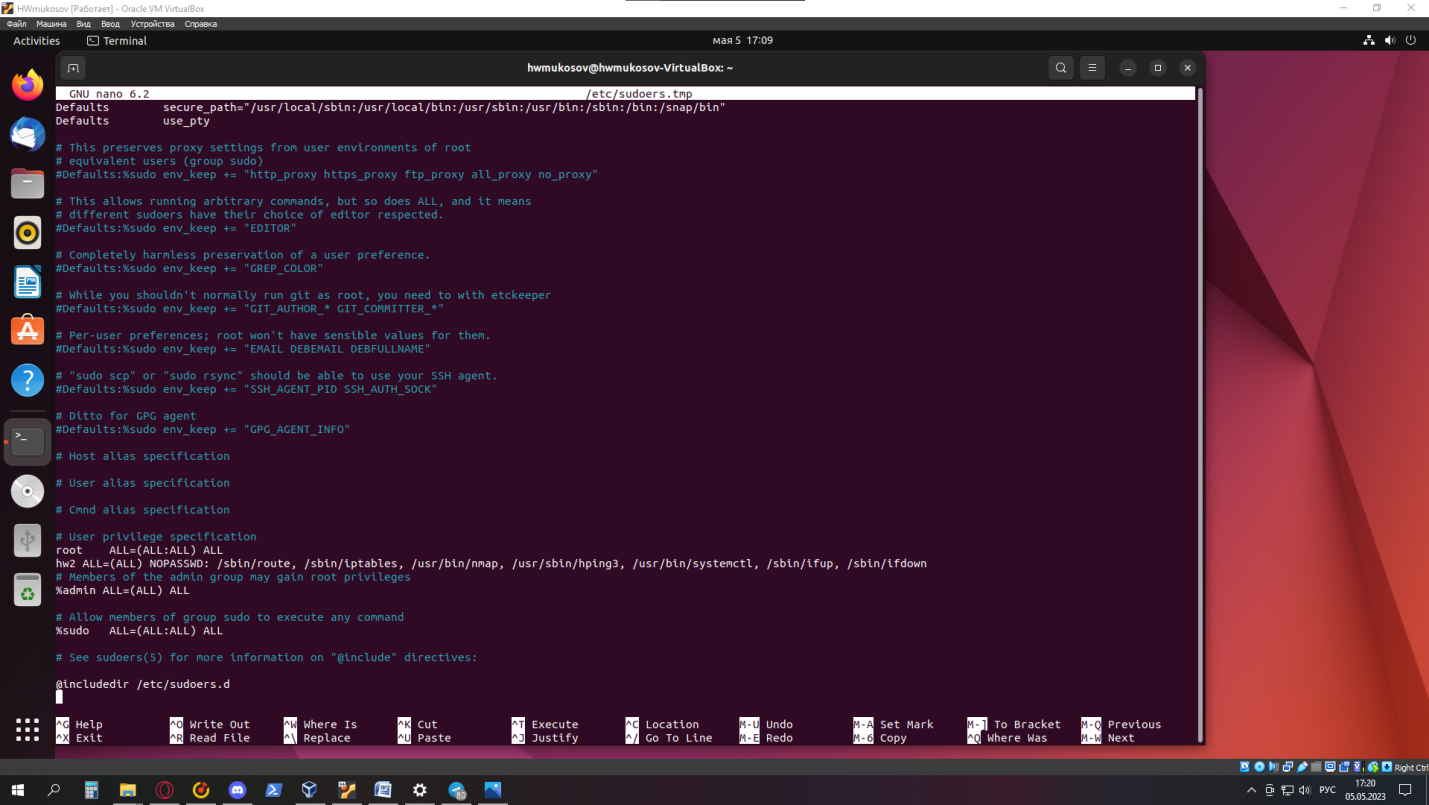
**Вводим пароль и смотрим ls и passwd**

****

**Корректируем файл sudoers**

**Добавил строку:**

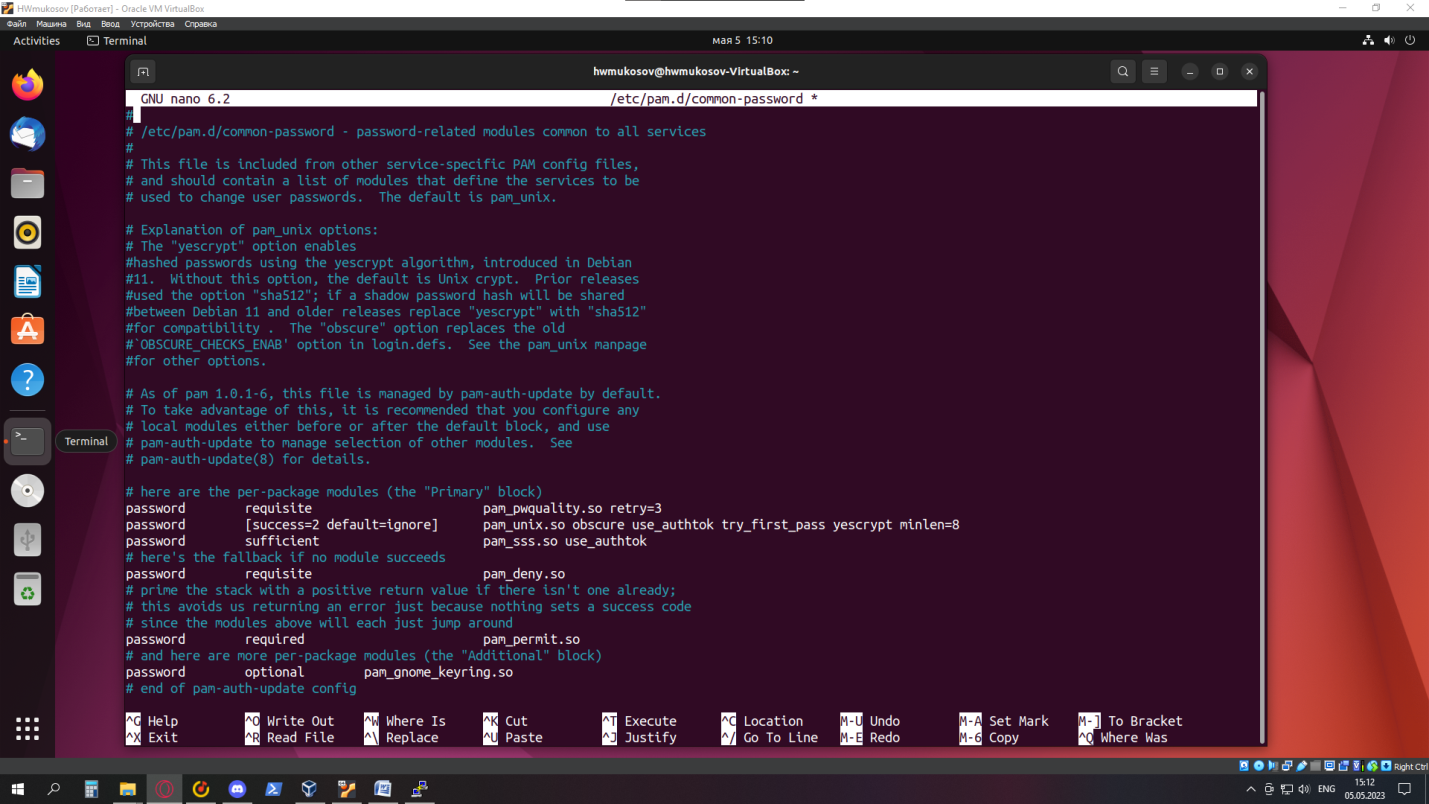
hw2 ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown



1. Установить минимальную длину пароля для пользователя в 8 символов.

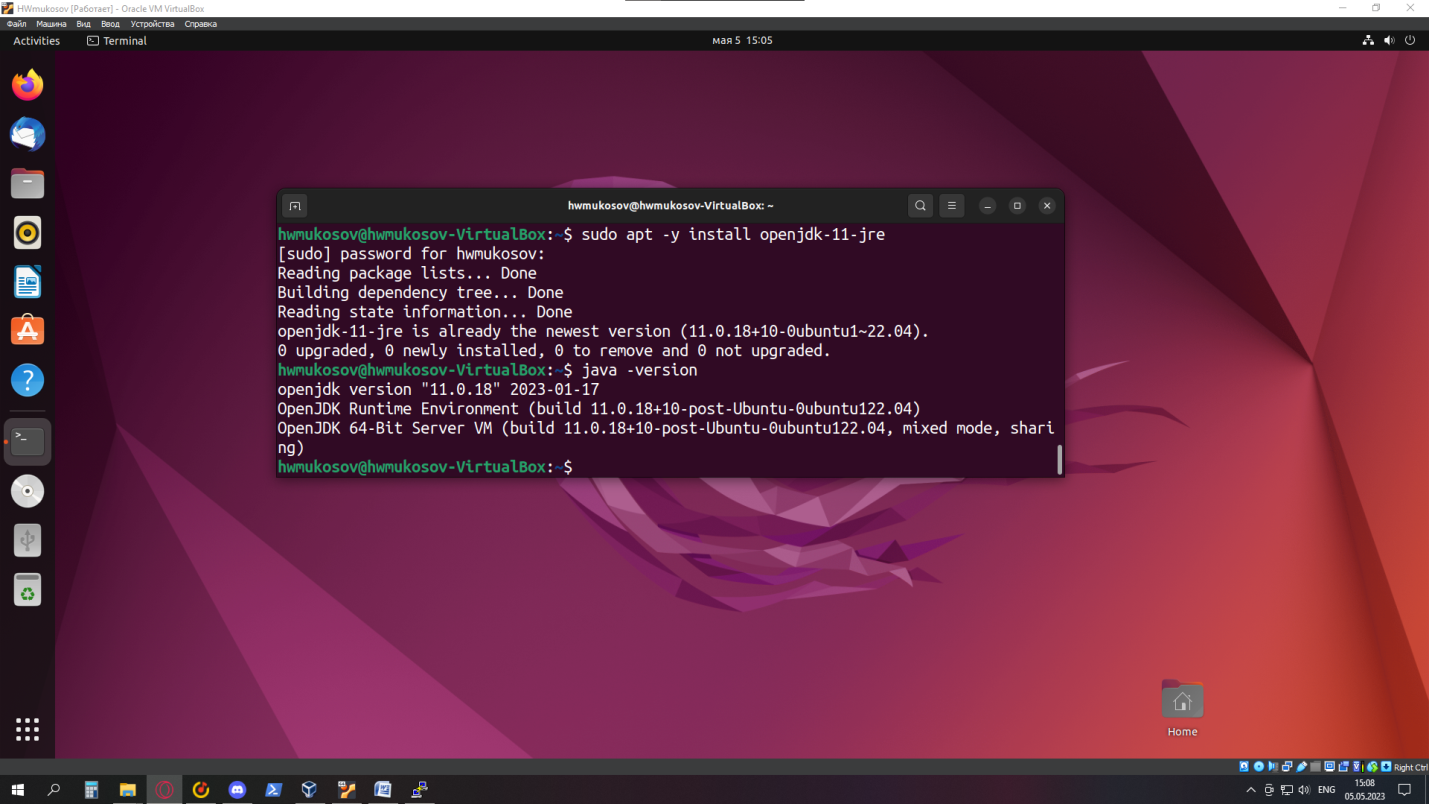
sudo nano /etc/pam.d/common-password

Добавляем в файл common-password к строке password [success=2 default=ignore] minlen=8



1. Установить на сервер пакеты Java.

sudo apt -y install openjdk-11-jre java -version



1. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.

**Устанавливаем Clamav**

sudo apt install clamav clamav-daemon clamav-freshclam

sudo freshclam

sudo systemctl start clamav-freshclam

**Готовим скрипт на скан для cron.**

**scan.sh**

#!/bin/bash

SCAN\_DIR="/"

LOG\_FILE="/var/log/clamav/scan.log"

/usr/bin/clamscan -i -r $SCAN\_DIR >> $LOG\_FILE**Настраиваем cron**

sudo apt install cron

sudo systemctl enable cron

crontab –e

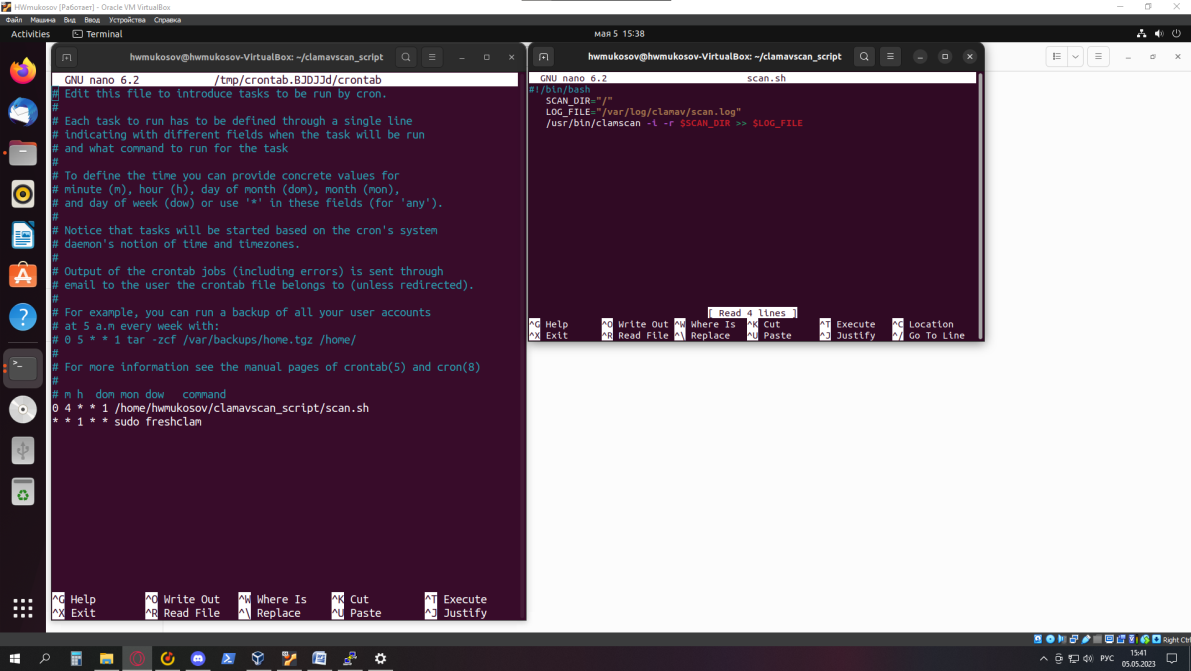
**Прописываем в таблицу задачи на запуск скрипта и обновления**

0 4 \* \* 1 /home/hwmukosov/clamavscan\_script/scan.sh

\* \* 1 \* \* sudo freshclam

**Не забываем сохранить и перезапустить cron**

sudo systemctl restart cron



6. Настроить файервол на блокирование всего входящего и выходящего трафика

sudo iptables --policy INPUT DROP && sudo iptables --policy OUTPUT DROP && sudo iptables --policy FORWARD DROP

**Смотрим таблицу iptables –L:**

Chain INPUT (policy DROP)

target prot opt source destination

Chain FORWARD (policy DROP)

target prot opt source destination

Chain OUTPUT (policy DROP)

target prot opt source destination

