**Пункт 1.**

Для установки SSH сначала сделал:

sudo apt update

Затем произвел установку:

sudo apt-get install ssh

После этого прописал автоматический старт при запуске машины:

sudo systemctl enable ssh

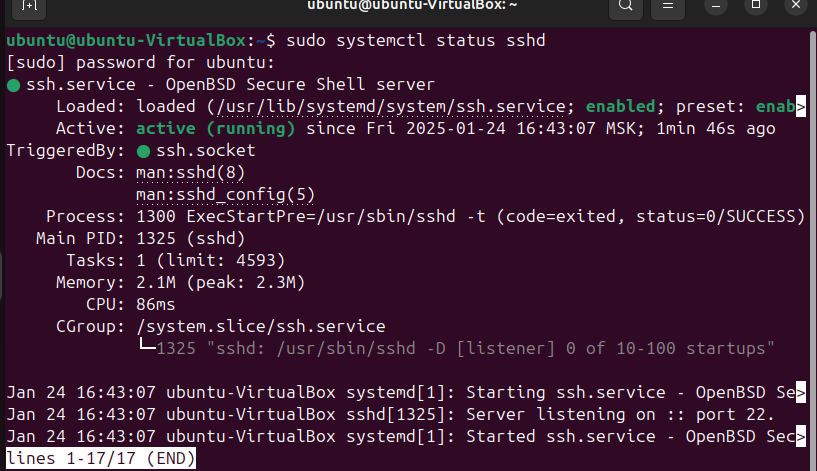
Перезагрузил машину:

systemctl reboot

Проверил, что SSH работает:

sudo systemctl status sshd

Получил результат:



Производим настройку для соединения по связке ключей public:private для подключения к SSH.

cd /etc

cd ssh

sudo nano sshd\_config

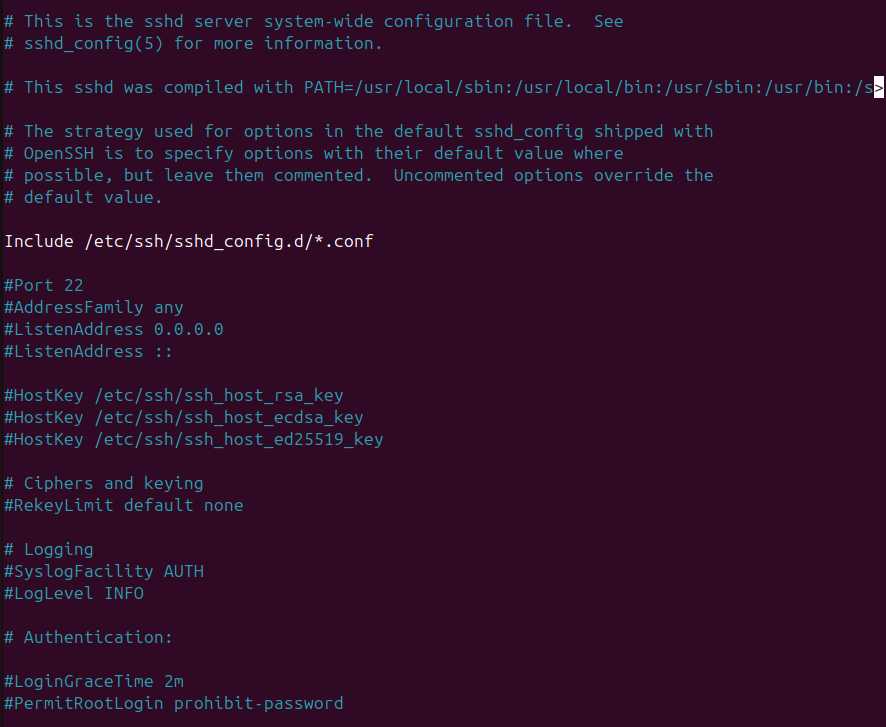
В файле ставим запрет на соединение при помощи пароля

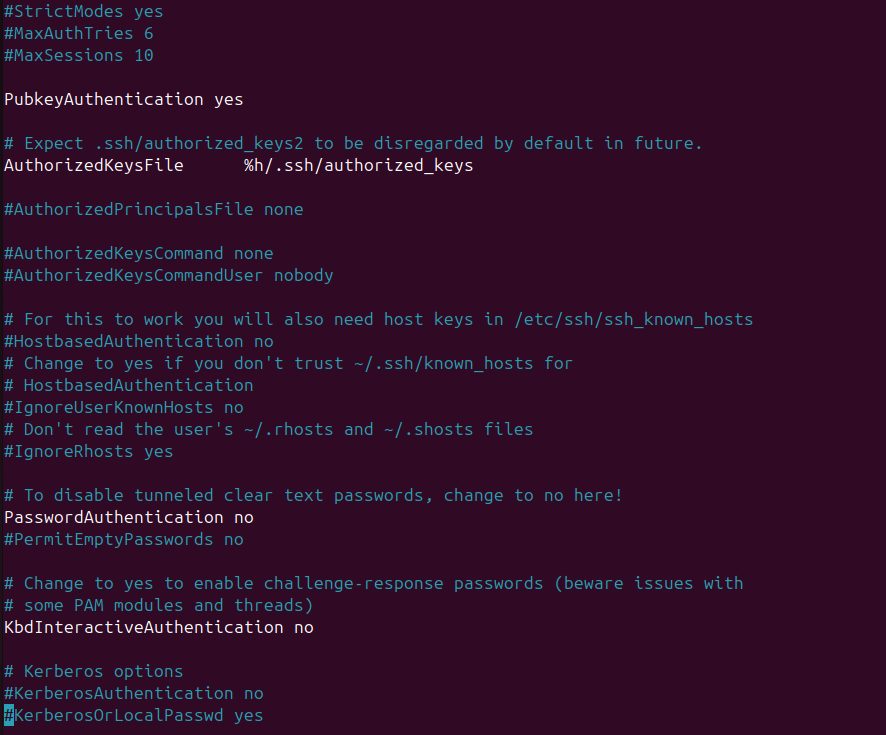
PasswordAuthentication no

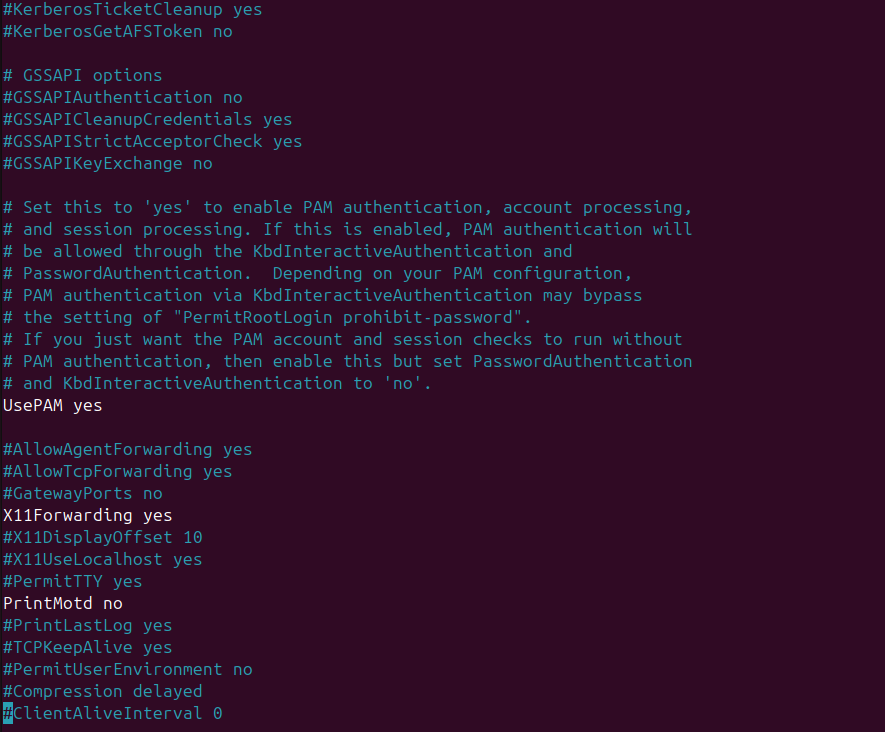
За тем раскомментируем строчку и разрешаем соединение по публичному ключу

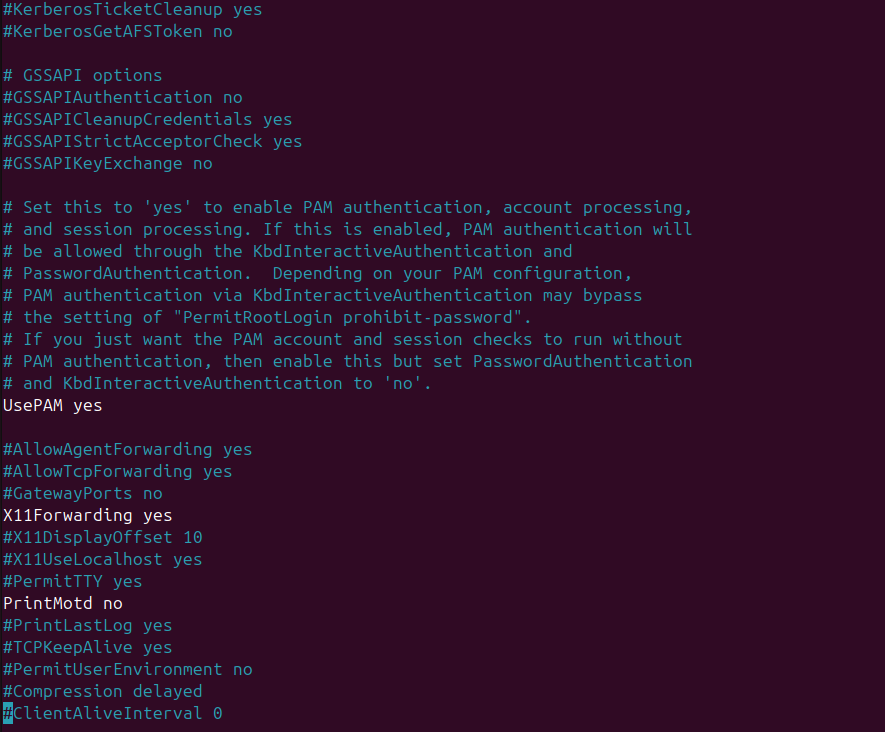
PubkeyAuthentication yes

Таким образом все содержимое файла:









Далее при помощи PuTTYgen генерируем публичный и приватный ключи (процесс подробно описан в уроке про SSH). Публичный ключ сохраняем под именем test.pub, приватный privat.ppk.

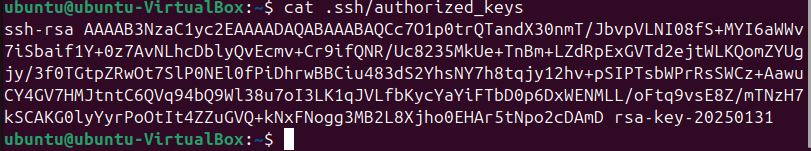
В ubuntu:

sudo nano .ssh/authorized\_keys

В данный файл сохраняем скопированное содержимое публичного ключа (test.pub) и проверяем его содержимое:

cat .ssh/authorized\_keys

Видим:



Перезапускаем сервис ssh

sudo systemctl restart sshd

Проверяем его статус, чтобы убедиться, что он активен

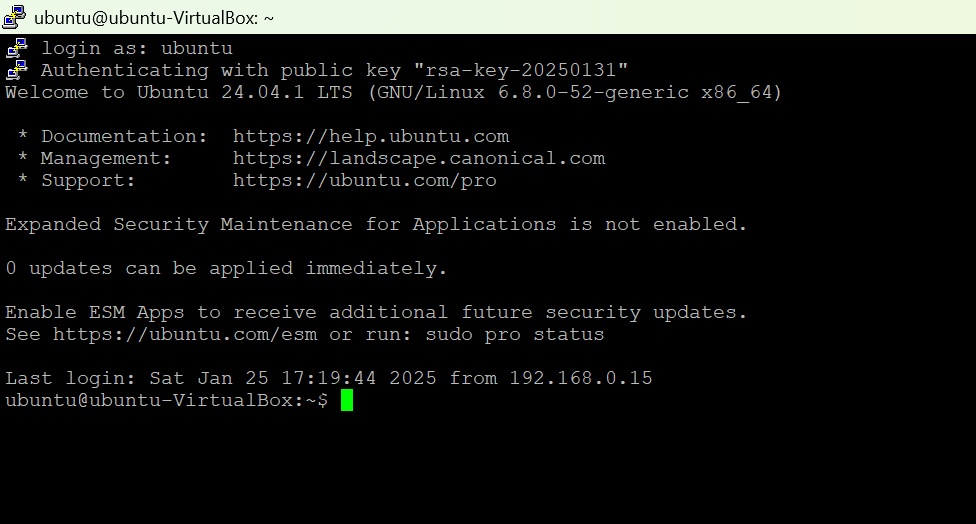
sudo systemctl status sshd

Проверяем свой текущий ip адрес ubuntu

ip -br a

Текущий ip 10.8.12.155

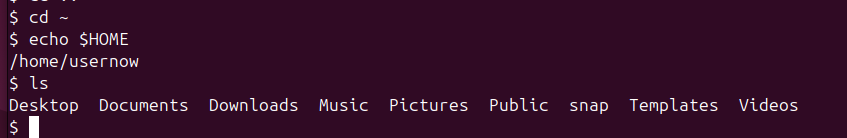
Производим соединение хоста и сервера ubuntu через Putty:



**Пункт 2.**

sudo useradd -m usernow создать пользователя с домашней директорией и логином usernow

sudo passwd usernow прописать пароль для пользователя usernow





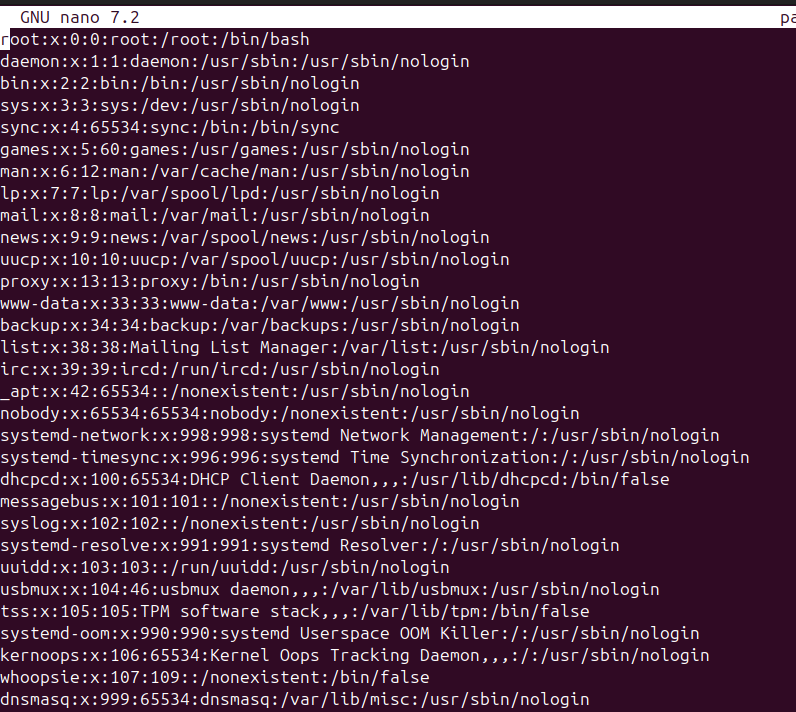
cd /etc перешли в директорию /etc

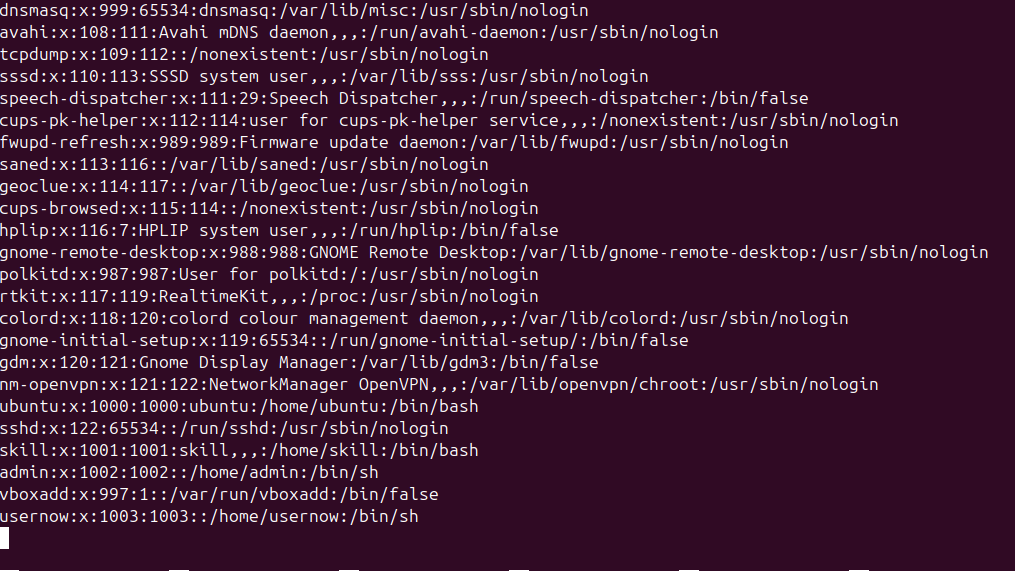
sudo nano sudoers редактируем файл sudoers

Вносим

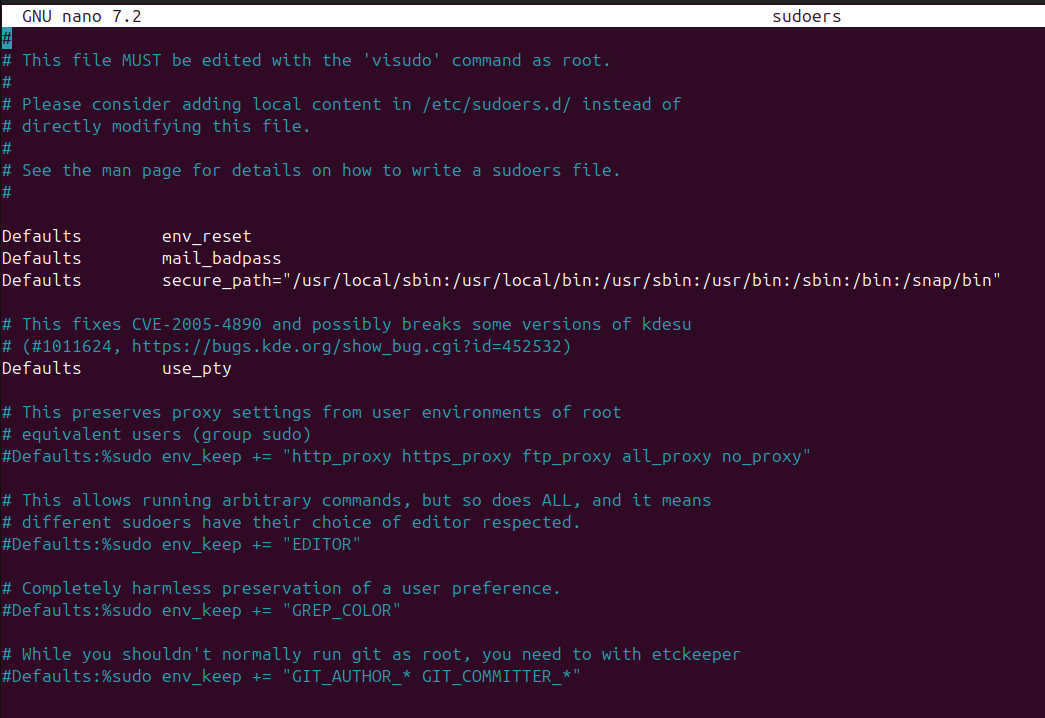
usernow ALL=(ALL) NOPASSWD : /usr/sbin/route, /usr/sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /usr/sbin/ifup, /usr/sbin/ifdown

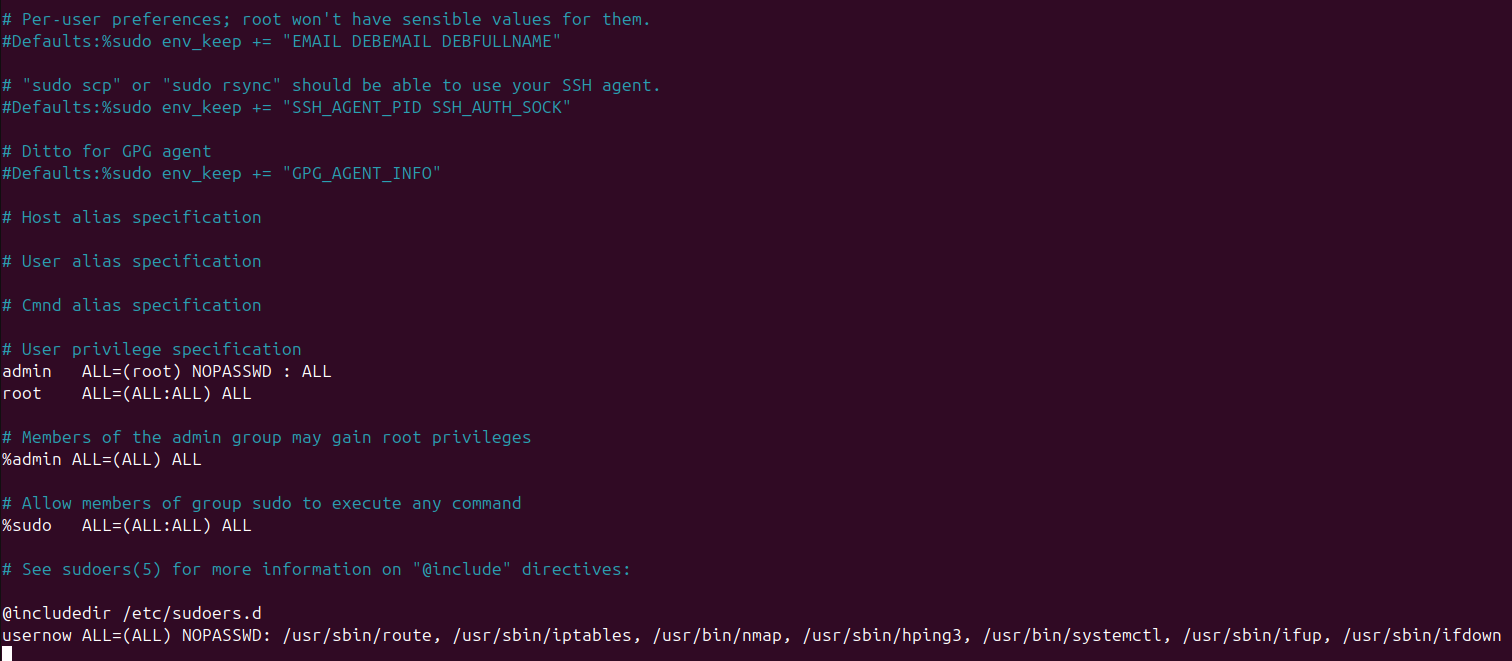
Содержимое файла passwd:





Содержимое файла sudoers:





**Пункт 3.**

Открываем файл common-password

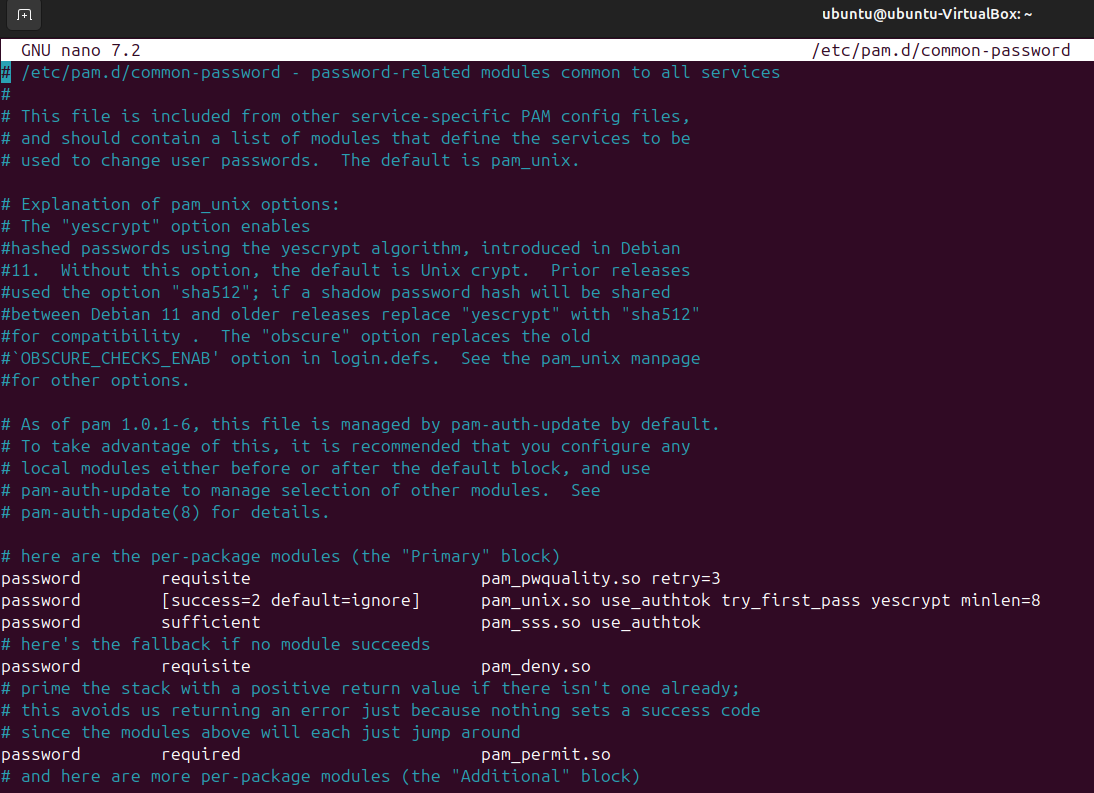
sudo nano /etc/pam.d/common-password

Из строки

password [success=2 default=ignore] pam\_unix.so obscure use\_authtok try\_first\_pass yescrypt

убираем функцию obscure (доп проверки на сложность пароля) и добавляем minlen = 8 для установления минимальной длины пароля.

Таким образом содержимое файла common-password:





**Пункт 4.**

Обновляем список пакетов и саму систему

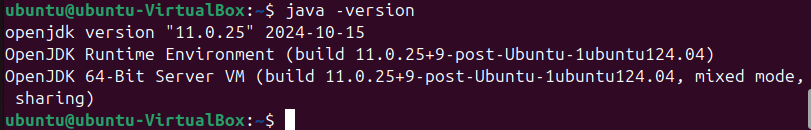
sudo apt update && sudo apt upgrade -y

Устанавливаем OpenJDK (Java)

sudo apt install -y openjdk-11-jdk

Проверяем установленную версию Java

java -version



JDK по умолчанию содержит в себе редакцию JRE.

**Пункт 5.**

Устанавливается антивирус ClamAV для Linux

sudo apt install -y clamav clamav-daemon

Обновляем антивирусные базы данных вручную

sudo freshclam

Для настройки автоматического обновления раз в месяц, открываем crontab для редактирования:

crontab -e

Добавляем строчку для обновления базы данных антивируса в 3:00 утра первого числа каждого месяца:

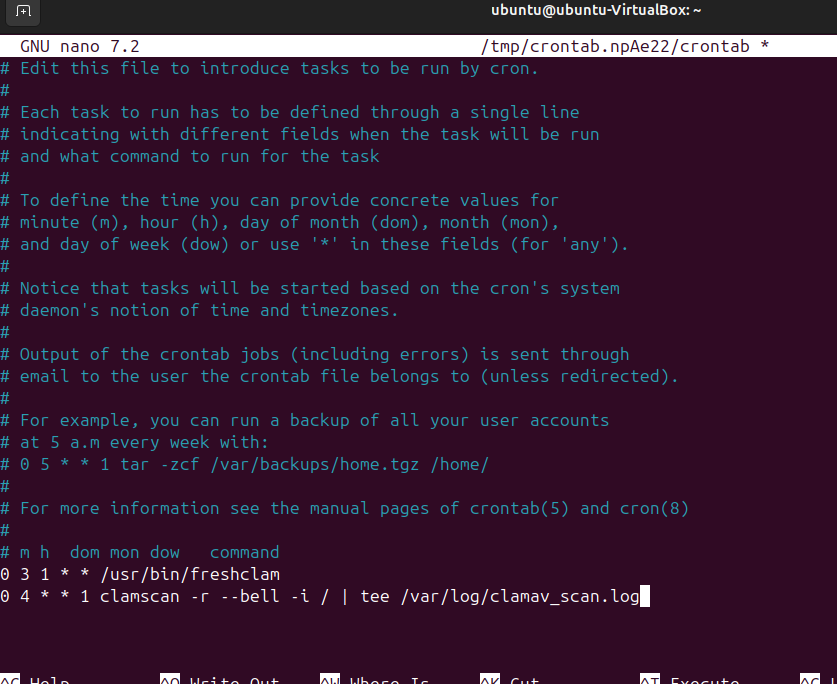
0 3 1 \* \* /usr/bin/freshclam

Для настройки автоматического сканирования каждый понедельник в 4 утра добавляем строчку:

0 4 \* \* 1 clamscan -r --bell -i / | tee /var/log/clamav\_scan.log

Результаты сканирования будут сохраняться в /var/log/clamav\_scan.log.

Содержимое файла crontab:



**Пункт 6.**

Проверяем установлен ли у нас файервол:

sudo ufw status

Получаем ответ:

Status: inactive

То есть он есть, но не активен.

Удаляем все существующие правила файервола, чтобы начать с чистого листа:

sudo ufw reset

Устанавливаем политику блокировки всего входящего и исходящего трафика по умолчанию:

sudo ufw default deny incoming

sudo ufw default deny outgoing

Разрешаем выходящий трафик для DNS (порт 53) и HTTP (порт 80) для обновления антивируса

sudo ufw allow out 53

sudo ufw allow out 80

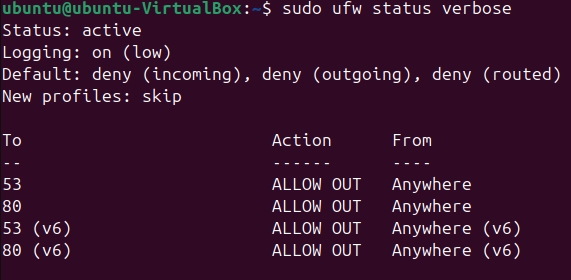
Активирует файервол с заданными правилами:

sudo ufw enable

Проверяем текущие настройки файервола

sudo ufw status verbose

Ответ:



Вывод всех цепочек и правил iptables:

