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

- отключаем возможность аутентификации по паролю в файле sshd\_config а также UsePAM, активируем PubkeyAuthentication.

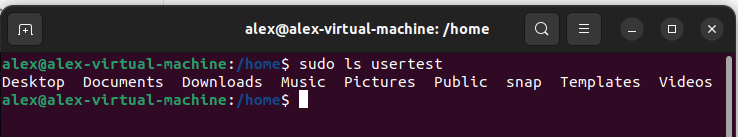
- В PuttyGen генерируем public и private key. Public перекидываем на linux машину.

Доп. Файлы в папке Task1.

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

Командой useradd создаем нового пользователя “usertets”. В sudoers прописываем запуск вышеупомянутых утилит без запроса пароля:

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



Доп. Файлы в папке Task2.

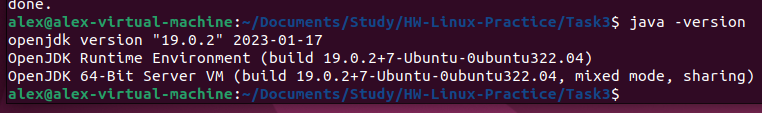
**3. Установить минимальную длину пароля для пользователя в 8 символов.**

в файле common\_password (/etc/pam.d/) в пункте password добавляем требование про минимальную длину пароля: minlen=8

Доп. Файлы в папке Task3.

**4. Установить на сервер пакеты Java.**

Командой sudo apt install openjdk-19-jre устанавливаем пакеты Java последней 19 версии:

****

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

Устанавливаем антивирус clamav – sudo apt install clamav.

В Crontab добавляем 2 команды. Одна на сканирование системы, другая на обновление антивирусной базы:

0 4 \* \* 1 /usr/bin/clamscan -r /-i --log=/var/log/clamav/weekly\_scan.log

0 0 1 \* \* /usr/bin/freshclam --quiet -l /var/log/clamav/update.log

Доп. Файлы в папке Task5.

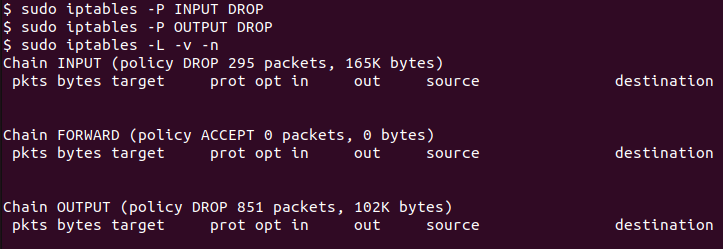
**6. Настроить файервол на блокирование всего входящего и выходящего трафика.**

Командой sudo iptables -P INPUT DROP блокируем весь входящий трафик.

Командой sudo iptables -P OUTPUT DROP блокируем весь входящий трафик.

Проверяем примененные настройки блокировки командой sudo iptables -L -v -n.

Результат:



Доп. Файлы в папке Task6.