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

Установка: sudo apt-get install ssh

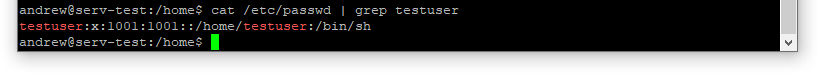
Изменение конфигурации SSH: sudo nano /etc/ssh/sshd\_config

Раскоментировал строку PubkeyAuthentication yes

Ссылка на файл [sshd\_config](https://github.com/Budogun/Sec_of_Linux/blob/main/sshd_config)

Перенес сгенерированный публичный ключ на сервер и прописал его в [authorized\_keys](https://github.com/Budogun/Sec_of_Linux/blob/main/authorized_keys) ( 🡨ссылка на файл)командой cat public\_key > authorized\_keys

Перезапустил демона sshd: sudo systemctl restart sshd

1. **Создать нового пользователя с домашней директорией:**
   * Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

     Автоматически созданное описаниеsudo useradd -m testuser
   * Файл [sudoers](https://github.com/Budogun/Sec_of_Linux/blob/main/sudoers) (разрешить запускать утилиты без ввода пароля sudo)
   * Минимальная длинна пароля 8 символов – в файле /etc/pam.d/common-password в строке password [success=1 default=ignore] pam\_unix.so yescrypt minlen=8 убрали параметр obscure и дописали minlen=8
   * Ссылка на файл [common-password](https://github.com/Budogun/Sec_of_Linux/blob/main/common-password)
2. **Установить на сервер пакеты Java.**
   * Изображение выглядит как текст, программное обеспечение, снимок экрана, Мультимедийное программное обеспечение

     Автоматически созданное описаниеsudo apt -y install openjdk-11-jre
3. **Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.**
   * Скрипт сканирования daily\_antivirus.sh:

#!/bin/bash

SCAN\_DIR="/"

LOG\_FILE="/var/log/clamav/daily\_antivirus.log"

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

* + Задачи в cron:

0 4 \* \* 1 /home/andrew/daily\_antivirus.sh #запуск скрипта на сканирование

0 0 1 \* \* /usr/bin/freshclam # обновление раз в месяц

1. **Настроить файервол на блокирование всего входящего и выходящего трафика.**
   * Установка iptables:

sudo apt-get install iptables

Правила блокировки:

sudo iptables --policy INPUT DROP # запрет входящего трафика

sudo iptables --policy OUTPUT DROP #запрет исходящего трафика

