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

sudo apt install ssh

sudo systemctl start ssh

**редактируем /etc/ssh/sshd\_config**

PubkeyAuthentication yes

PasswordAuthentication no

**Формируем ключ**.

su test

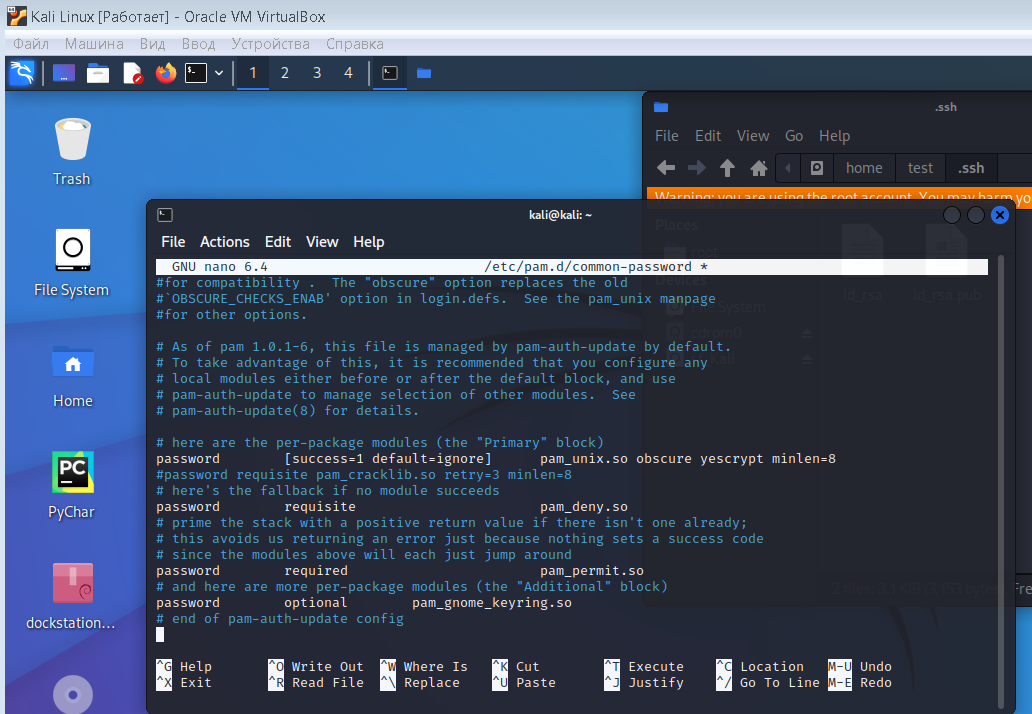
ssh-keygen

**Формируем ключи и перебрасываем публичный ключ - public\_key на сервер и записываем его содержимое в файл /home/test/.ssh/authorized\_keys**

ssh-keygen -i -f public\_key >> authorized\_keys

sudo systemctl restart ssh

<https://yadi.sk/i/e4HxKyxx9XVeZA>



# This is the sshd server system-wide configuration file. See

# sshd\_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd\_config shipped with

# OpenSSH is to specify options with their default value where

# possible, but leave them commented. Uncommented options override the

# default value.

Include /etc/ssh/sshd\_config.d/\*.conf

#Port 22

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#HostKey /etc/ssh/ssh\_host\_ed25519\_key

# Ciphers and keying

#RekeyLimit default none

# Logging

#SyslogFacility AUTH

#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

#PermitRootLogin prohibit-password

#StrictModes yes

#MaxAuthTries 6

#MaxSessions 10

PubkeyAuthentication yes

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

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

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none

#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh\_known\_hosts

#HostbasedAuthentication no

# Change to yes if you don't trust ~/.ssh/known\_hosts for

# HostbasedAuthentication

#IgnoreUserKnownHosts no

# Don't read the user's ~/.rhosts and ~/.shosts files

#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!

PasswordAuthentication no

#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with

# some PAM modules and threads)

KbdInteractiveAuthentication no

# Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

#KerberosGetAFSToken no

# GSSAPI options

#GSSAPIAuthentication no

#GSSAPICleanupCredentials yes

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,

# and session processing. If this is enabled, PAM authentication will

# be allowed through the KbdInteractiveAuthentication and

# PasswordAuthentication. Depending on your PAM configuration,

# PAM authentication via KbdInteractiveAuthentication may bypass

# the setting of "PermitRootLogin without-password".

# If you just want the PAM account and session checks to run without

# PAM authentication, then enable this but set PasswordAuthentication

# and KbdInteractiveAuthentication to 'no'.

UsePAM yes

#AllowAgentForwarding yes

#AllowTcpForwarding yes

#GatewayPorts no

X11Forwarding yes

#X11DisplayOffset 10

#X11UseLocalhost yes

#PermitTTY yes

PrintMotd no

#PrintLastLog yes

#TCPKeepAlive yes

#PermitUserEnvironment no

#Compression delayed

#ClientAliveInterval 0

#ClientAliveCountMax 3

#UseDNS no

#PidFile /run/sshd.pid

#MaxStartups 10:30:100

#PermitTunnel no

#ChrootDirectory none

#VersionAddendum none

# no default banner path

#Banner none

# Allow client to pass locale environment variables

AcceptEnv LANG LC\_\*

# override default of no subsystems

Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis

#Match User anoncvs

# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

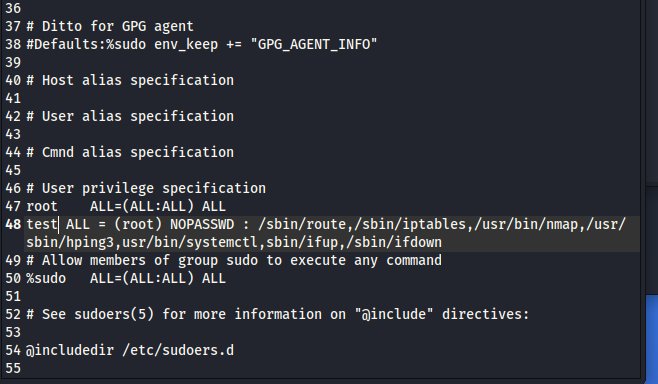
**2. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:** /sbin/route,/sbin/iptables,/usr/bin/nmap,/usr/sbin/hping3,usr/bin/systemctl,sbin/ifup,/sbin/ifdown

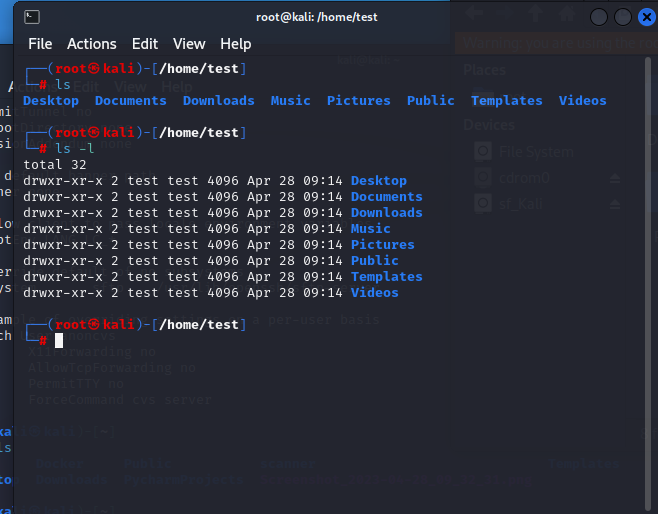
sudo useradd - m test

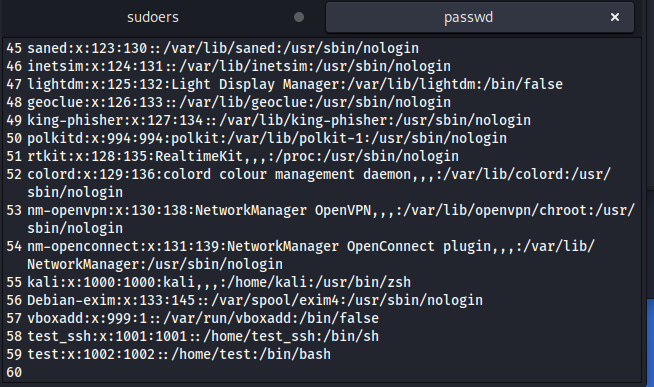
**Добавить в sudoers**

command\_allies test = /sbin/route,/sbin/iptables,/usr/bin/nmap,/usr/sbin/hping3,usr/bin/systemctl,sbin/ifup,/sbin/ifdown

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

****





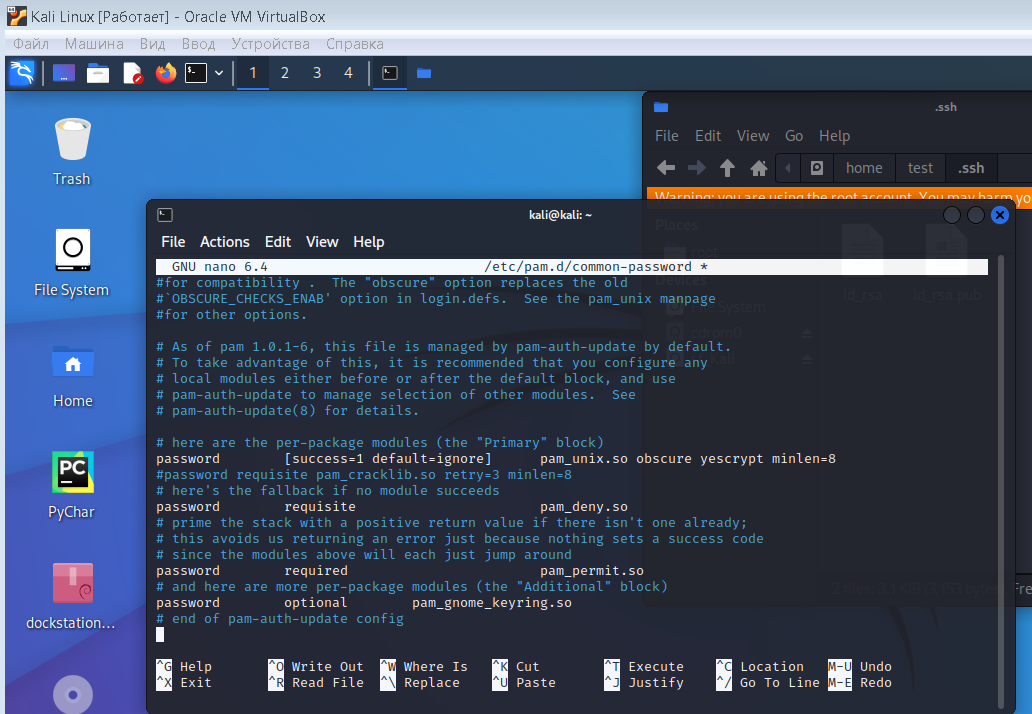
**3. Установить минимальную длину пароля для пользователя в 8 символов.**

Set linux kali to a minimum password length of 8 characters for a user

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

password requisite pam\_cracklib.so retry=3 minlen=8

Не смог разобраться почему не срабатывает это правило.



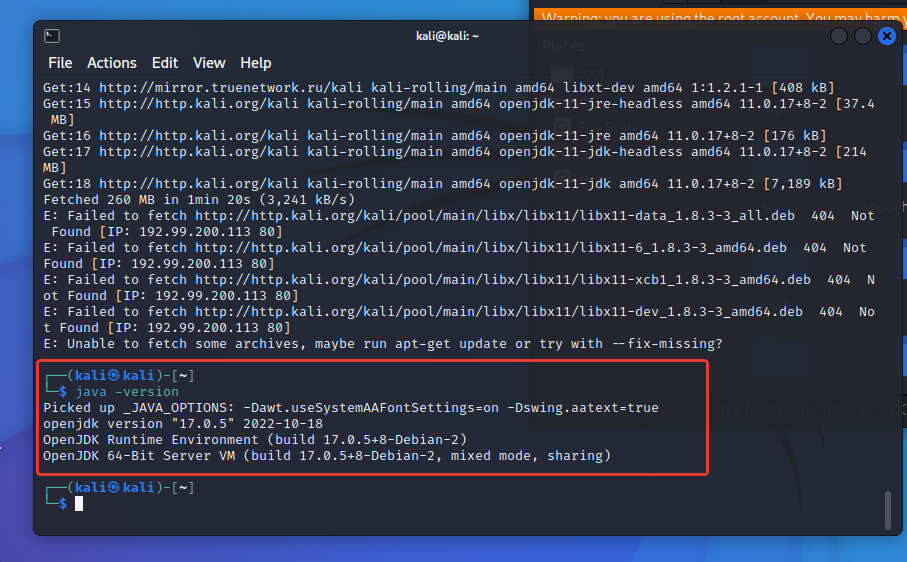
**4. Установить на сервер пакеты Java.**

**Установка пакеты Java Development Kit (JDK) и Java Runtime Environment (JRE):**

sudo apt install openjdk-11-jdk openjdk-11-jre

**Проверка**

java -version



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

**Например, создайте файл /home/user/scan.sh с содержимым:**

#!/bin/bash

# Run antivirus scan

clamscan -r / > /home/test/clamscan.log

# Update antivirus database (once a month)

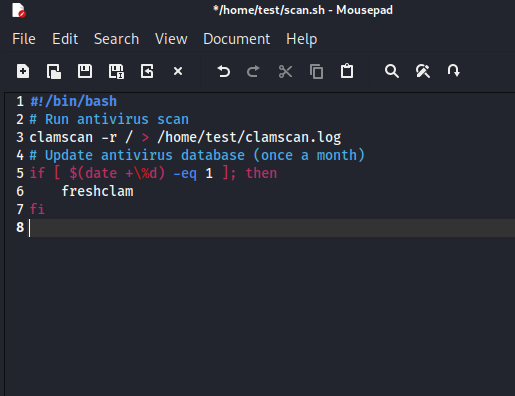
if [ $(date +\%d) -eq 1 ]; then

freshclam

fi

**Сделать файл scan.sh исполняемым:**

chmod +x /home/test/scan.sh



**файл cron для редактирования:**

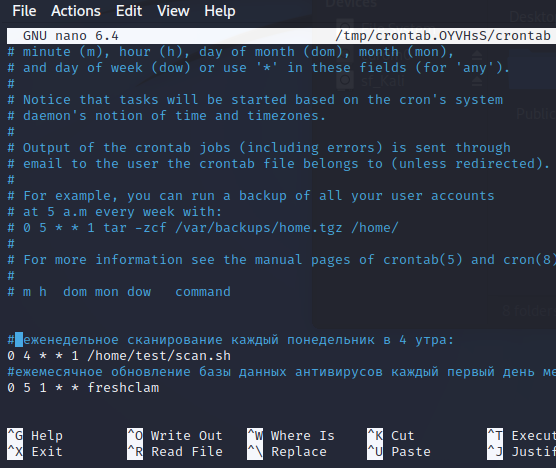
crontab -e

еженедельное сканирование каждый понедельник в 4 утра:

0 4 \* \* 1 /home/test/scan.sh

ежемесячное обновление базы данных антивирусов каждый первый день месяца в 5 утра:

0 5 1 \* \* freshclam



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

sudo iptables -P INPUT DROP

sudo iptables -P OUTPUT DROP

Вывод всех цепочек:

sudo iptables -L

<https://yadi.sk/i/ozuSFVbxitZmXQ>

