1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.
   * sudo apt-get install ssh
   * sudo nano /etc/ssh/sshd\_config
   * sudo systemctl restart sshd
   * mkdir .ssh
   * cd .ssh
   * touch authorized\_keys
   * **на хосте** ssh-keygen
   * **на хосте** scp /Users/matyu/.ssh/id\_rsa.pub dorjo@192.168.223.134:/home/dorjo/.ssh/key
   * cat key > authorized\_keys

**Содержимое файла** sshd\_config:

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

# sshd\_config(5) for more information.

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

#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

**Содержимое файла authorized\_keys:**

ssh-rsa  matyu@Dorjo

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

1. 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 -s /bin/bash -G sudo -p $(openssl passwd -1 qwerasdf) testuser
  + sudo visudo:

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

**Вывод команды ls в директории home, вывод файла passwd:**

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание

**Содержимое файла sudoers:**

#

# This file MUST be edited with the 'visudo' command as root.

#

# Please consider adding local content in /etc/sudoers.d/ instead of

# directly modifying this file.

#

# See the man page for details on how to write a sudoers file.

#

Defaults env\_reset

Defaults mail\_badpass

Defaults secure\_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

Defaults use\_pty

# This preserves proxy settings from user environments of root

# equivalent users (group sudo)

#Defaults:%sudo env\_keep += "http\_proxy https\_proxy ftp\_proxy all\_proxy no\_proxy"

# This allows running arbitrary commands, but so does ALL, and it means

# different sudoers have their choice of editor respected.

#Defaults:%sudo env\_keep += "EDITOR"

# Completely harmless preservation of a user preference.

#Defaults:%sudo env\_keep += "GREP\_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper

#Defaults:%sudo env\_keep += "GIT\_AUTHOR\_\* GIT\_COMMITTER\_\*"

# Per-user preferences; root won't have sensible values for them.

#Defaults:%sudo env\_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.

#Defaults:%sudo env\_keep += "SSH\_AGENT\_PID SSH\_AUTH\_SOCK"

# Ditto for GPG agent

#Defaults:%sudo env\_keep += "GPG\_AGENT\_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification

root ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges

%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d

testuser 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.
   * cat /etc/login.defs

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

1. Установить на сервер пакеты Java.

- **sudo apt search jre (вывод команды):**

android-platform-tools-base/jammy,jammy 2.2.2-3 all

base tools for developing applications for the Android system

default-jre/jammy 2:1.11-72build2 amd64

Standard Java or Java compatible Runtime

default-jre-headless/jammy 2:1.11-72build2 amd64

Standard Java or Java compatible Runtime (headless)

docbook-xsl/jammy,jammy 1.79.2+dfsg-1 all

stylesheets for processing DocBook XML to various output formats

java-package/jammy,jammy 0.62 all

Utility for creating Java Debian packages

jaxws/jammy,jammy 2.3.0.2-2 all

JAX-WS Reference Implementation (Command Line Tools)

libambix-utils/jammy 0.1.1-3 amd64

AMBIsonics eXchange library (utilities)

libanimal-sniffer-java/jammy,jammy 1.16-1 all

JDK/API verification tools

libcommons-exec-java/jammy,jammy 1.3-2 all

Java library to reliably execute external processes from within the JVM

libgeronimo-osgi-support-java/jammy,jammy 1.1-2 all

Java libraries providing OSGi lookup support for Geronimo projects

libhsdis0-fcml/jammy 1.2.2-2 amd64

HotSpot disassembler plugin using FCML

libhtmlcleaner-java/jammy,jammy 2.24-1 all

Java HTML Parser library

libhtmlcleaner-java-doc/jammy,jammy 2.24-1 all

Java HTML Parser library (documentation)

libjaxws-api-java/jammy,jammy 2.3.0-1.1 all

Java API for XML-Based Web Services

libjaxws-java/jammy,jammy 2.3.0.2-2 all

JAX-WS Reference Implementation (Library)

libjreen-qt5-1/jammy 1.2.0-2.1fakesync1build1 amd64

powerful Jabber/XMPP library implemented in Qt5/C++

libjreen-qt5-dbg/jammy 1.2.0-2.1fakesync1build1 amd64

powerful Jabber/XMPP library (Qt5 build) - debugging symbols

libjreen-qt5-dev/jammy 1.2.0-2.1fakesync1build1 amd64

powerful Jabber/XMPP library (Qt5 build) - development files

libjregex-java/jammy,jammy 1.2.01-2 all

regular expressions for Java

libopenjfx-java/jammy,jammy 11.0.11+0-1 all

JavaFX/OpenJFX - Rich client application platform for Java (Java libraries)

libreoffice/jammy-updates,jammy-security 1:7.3.7-0ubuntu0.22.04.3 amd64

office productivity suite (metapackage)

libsaaj-java/jammy,jammy 1.4.0-3 all

SOAP with Attachment API for Java

libtwelvemonkeys-java/jammy,jammy 3.8.1-1 all

collection of plugins and extensions for Java's ImageIO

libtwelvemonkeys-java-doc/jammy,jammy 3.8.1-1 all

Documentation for libtwelvemonkeys-java

openjdk-11-jre/jammy-updates,jammy-security 11.0.20+8-1ubuntu1~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT

openjdk-11-jre-dcevm/jammy 11.0.12+7-1 amd64

Alternative VM for OpenJDK 11 with enhanced class redefinition

openjdk-11-jre-headless/jammy-updates,jammy-security 11.0.20+8-1ubuntu1~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT (headless)

openjdk-11-jre-zero/jammy-updates,jammy-security 11.0.20+8-1ubuntu1~22.04 amd64

Alternative JVM for OpenJDK, using Zero

openjdk-17-jre/jammy-updates,jammy-security 17.0.8+7-1~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT

openjdk-17-jre-headless/jammy-updates,jammy-security 17.0.8+7-1~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT (headless)

openjdk-17-jre-zero/jammy-updates,jammy-security 17.0.8+7-1~22.04 amd64

Alternative JVM for OpenJDK, using Zero

openjdk-18-jre/jammy-updates,jammy-security 18.0.2+9-2~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT

openjdk-18-jre-headless/jammy-updates,jammy-security 18.0.2+9-2~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT (headless)

openjdk-18-jre-zero/jammy-updates,jammy-security 18.0.2+9-2~22.04 amd64

Alternative JVM for OpenJDK, using Zero

openjdk-19-jre/jammy-updates,jammy-security 19.0.2+7-0ubuntu3~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT

openjdk-19-jre-headless/jammy-updates,jammy-security 19.0.2+7-0ubuntu3~22.04 amd64

OpenJDK Java runtime, using Hotspot JIT (headless)

openjdk-19-jre-zero/jammy-updates,jammy-security 19.0.2+7-0ubuntu3~22.04 amd64

Alternative JVM for OpenJDK, using Zero

openjdk-8-jre/jammy-updates,jammy-security 8u382-ga-1~22.04.1 amd64

OpenJDK Java runtime, using Hotspot JIT

openjdk-8-jre-headless/jammy-updates,jammy-security 8u382-ga-1~22.04.1 amd64 OpenJDK Java runtime, using Hotspot JIT (headless)

openjdk-8-jre-zero/jammy-updates,jammy-security 8u382-ga-1~22.04.1 amd64

Alternative JVM for OpenJDK, using Zero

- **sudo apt install openjdk-19-jre**

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.
   * sudo apt install clamav clamav-daemon clamav-freshclam
   * sudo systemctl stop clamav-freshclam
   * sudo freshclam
   * sudo systemctl start clamav-freshclam
   * sudo systemctl enable cron

**bash script:**

#!/bin/bash

SCAN\_DIR="/"

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

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

* + crontab -e

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

1. Настроить файервол на блокирование всего входящего и выходящего трафика.
   * sudo iptables -P INPUT DROP
   * sudo iptables -P OUTPUT DROP

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание