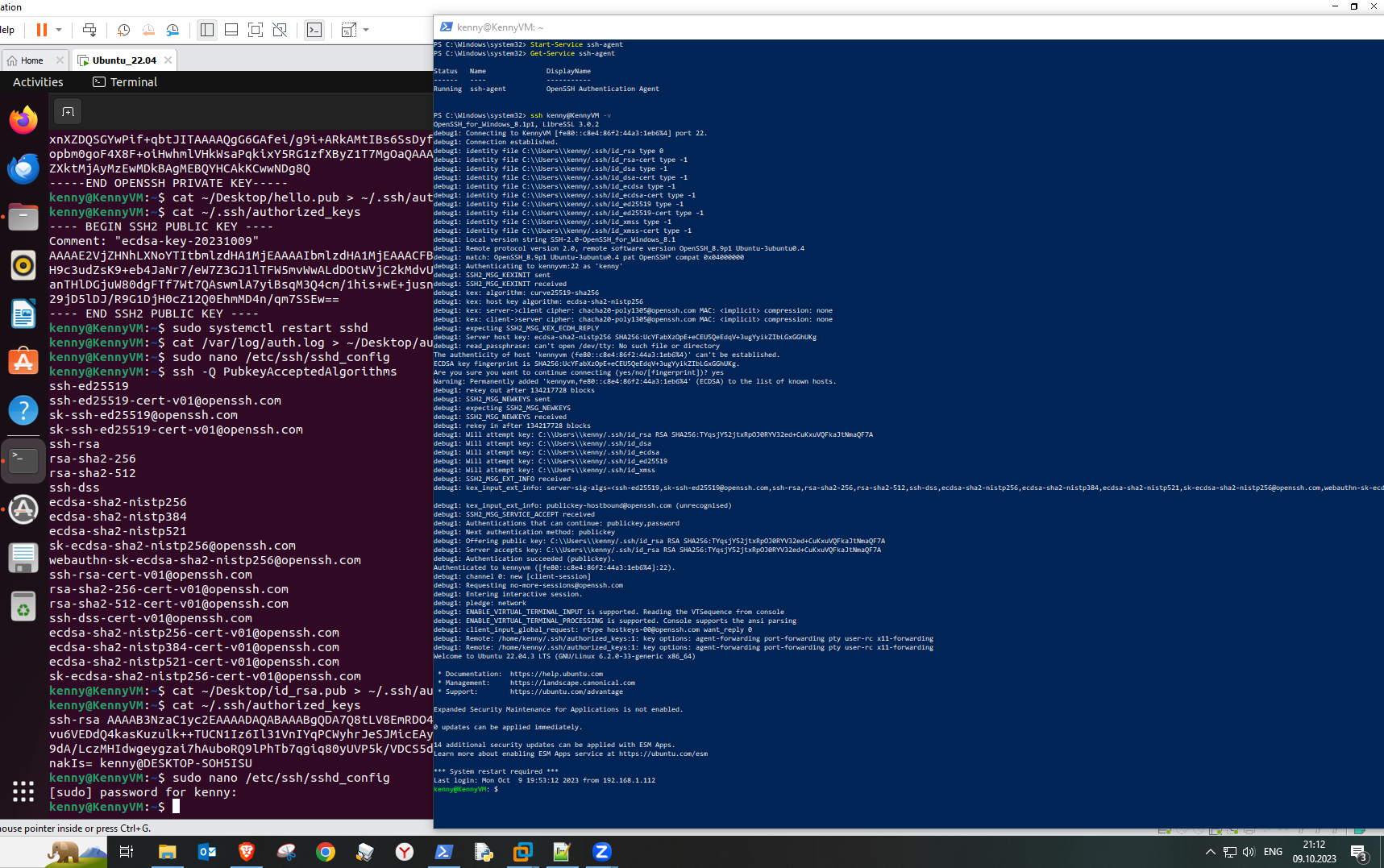
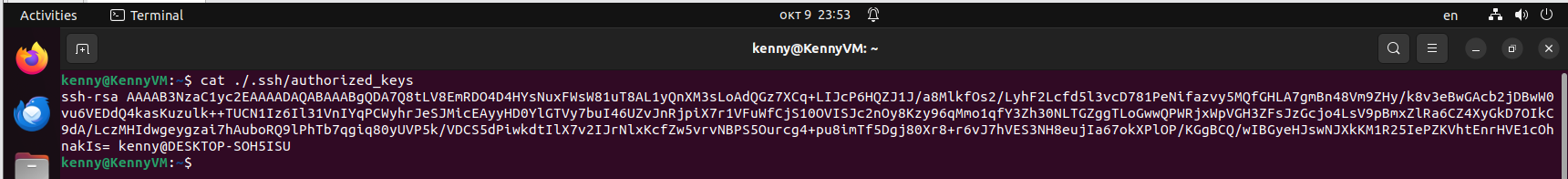
1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.

# Подключение к SSH-серверу, установленному на KennyVM (Ubuntu 22.04 192.168.1.97) осуществлялось с помощью OpenVPN (хост на Windows 10; 192.168.1.112), ключ ssh-rsa генерировался на хосте с помощью ssh-keygen на хосте.



Скрин 1 (Аутентификация на SSH-сервере с RSA-ключом)



Скрин 2 (Содержимое ~/.ssh/authorized\_keys)

Содержимое файла /etc/ssh/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 DEBUG3

# Authentication:

#LoginGraceTime 2m

#PermitRootLogin prohibit-password

#StrictModes yes

#MaxAuthTries 6

#MaxSessions 10

PubkeyAuthentication yes

HostKeyAlgorithms +ssh-rsa

PubkeyAcceptedKeyTypes +ssh-rsa

PubkeyAcceptedAlgorithms +ssh-rsa

# 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

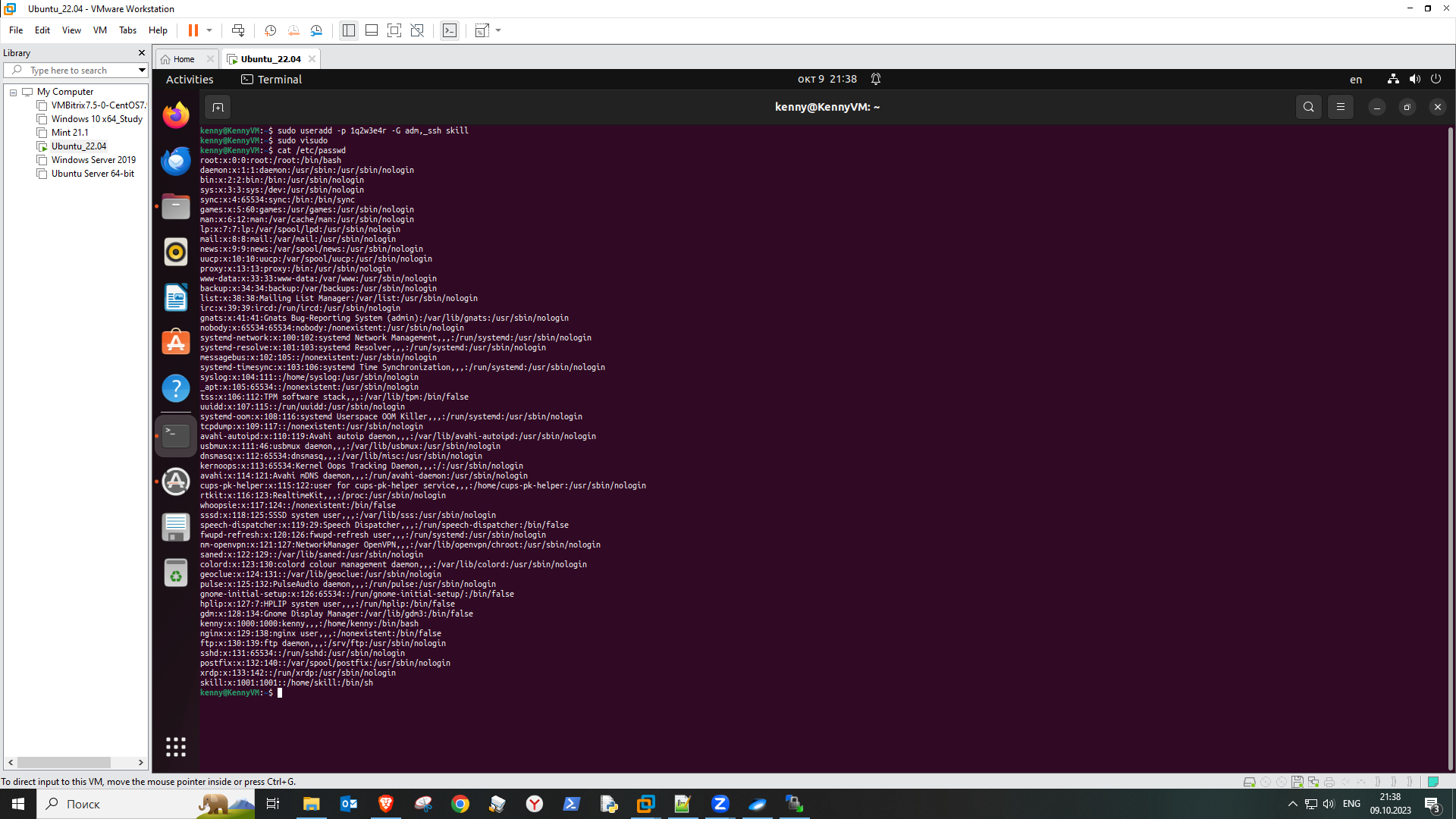
# PermitTTY no

# ForceCommand cvs server

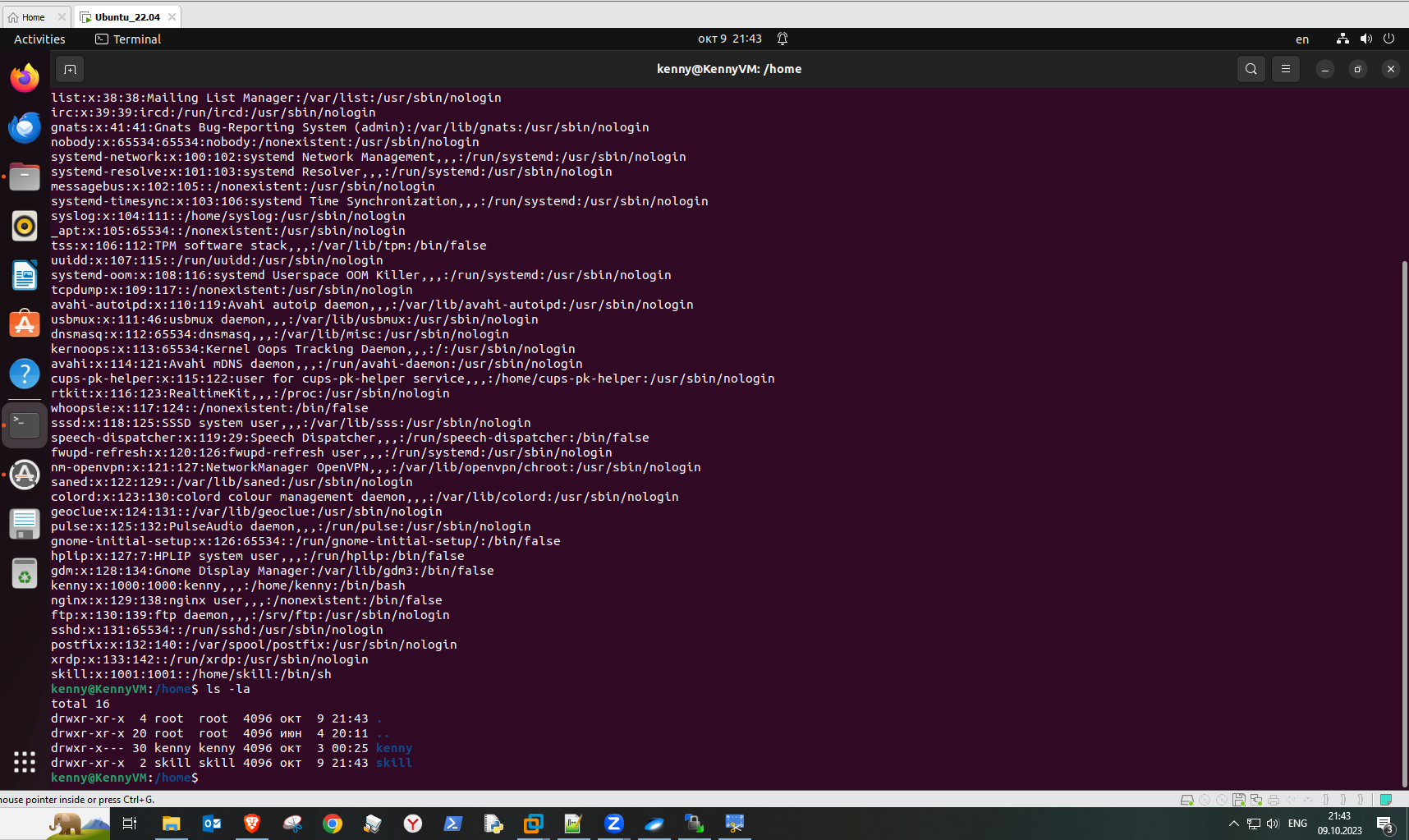
1. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:
   * 1. */sbin/route*, */sbin/iptables*, */usr/bin/nmap*, */usr/sbin/hping3*
     2. *usr/bin/systemctl*
     3. *sbin/ifup*, */sbin/ifdown*

# Командой sudo useradd –p 1q2w3e4r –G adm,\_ssh skill был создан новый пользователь «skill»

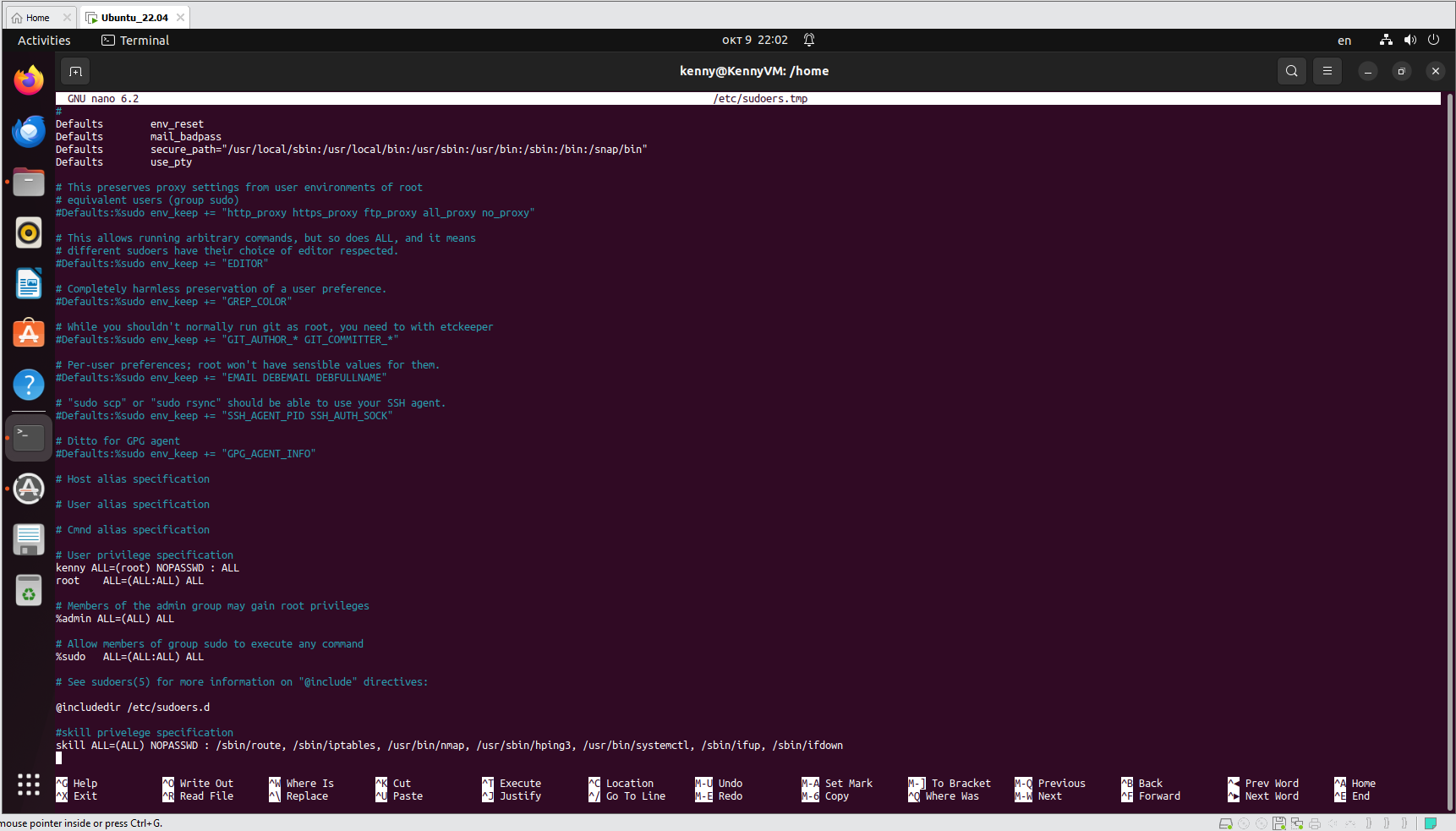
Путем внесения изменений в sudoers разрешен запуск утилит без требования пароля для пользователя «skill»



Скрин 3 (создание пользователя, вывод содержимого файла /etc/passwd)



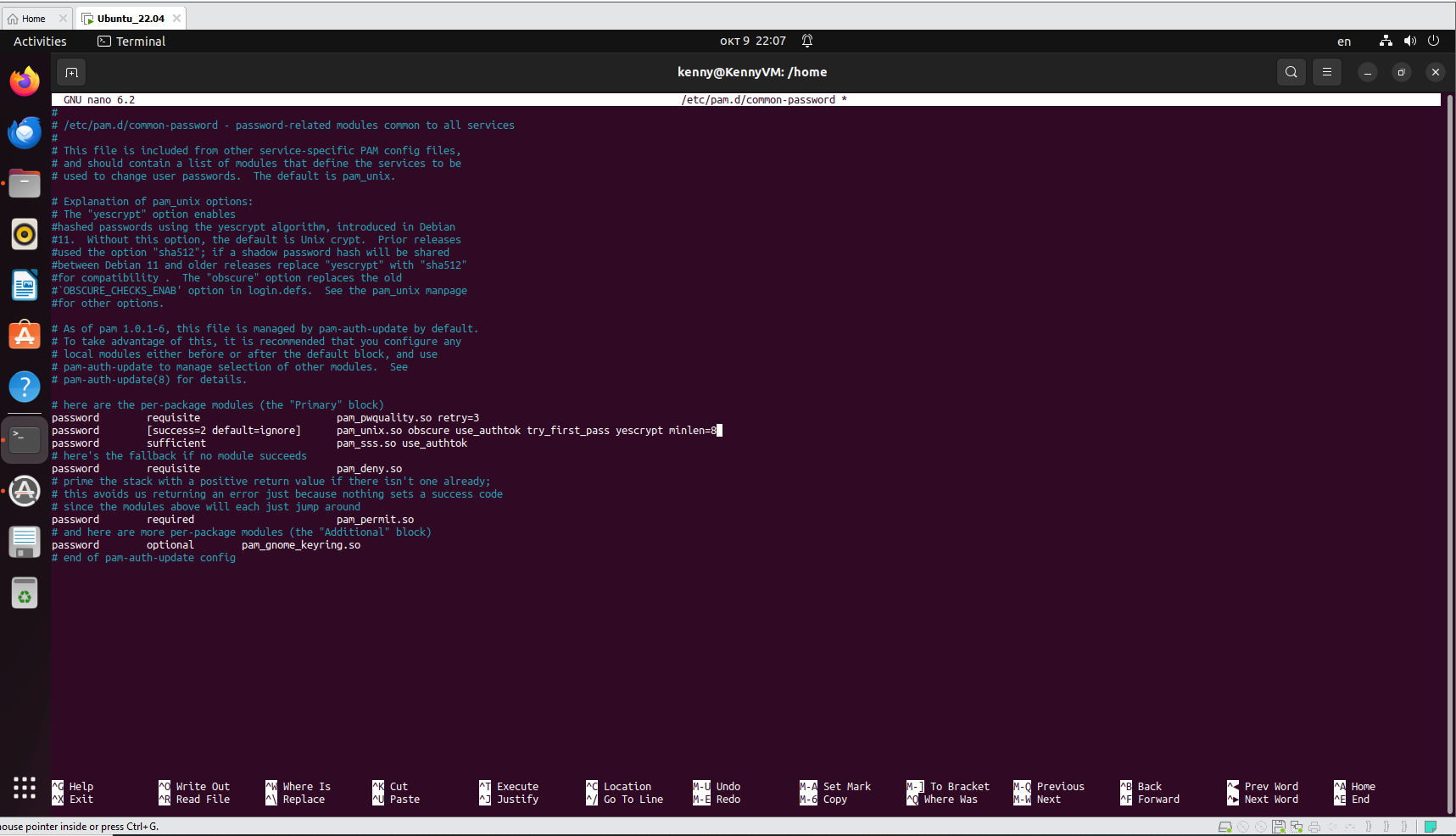
Скрин 4 (вывод команды ls –la каталога /home)



Скрин 5 (изменения в sudoers (sudo visudo))

1. Установить минимальную длину пароля для пользователя в 8 символов.

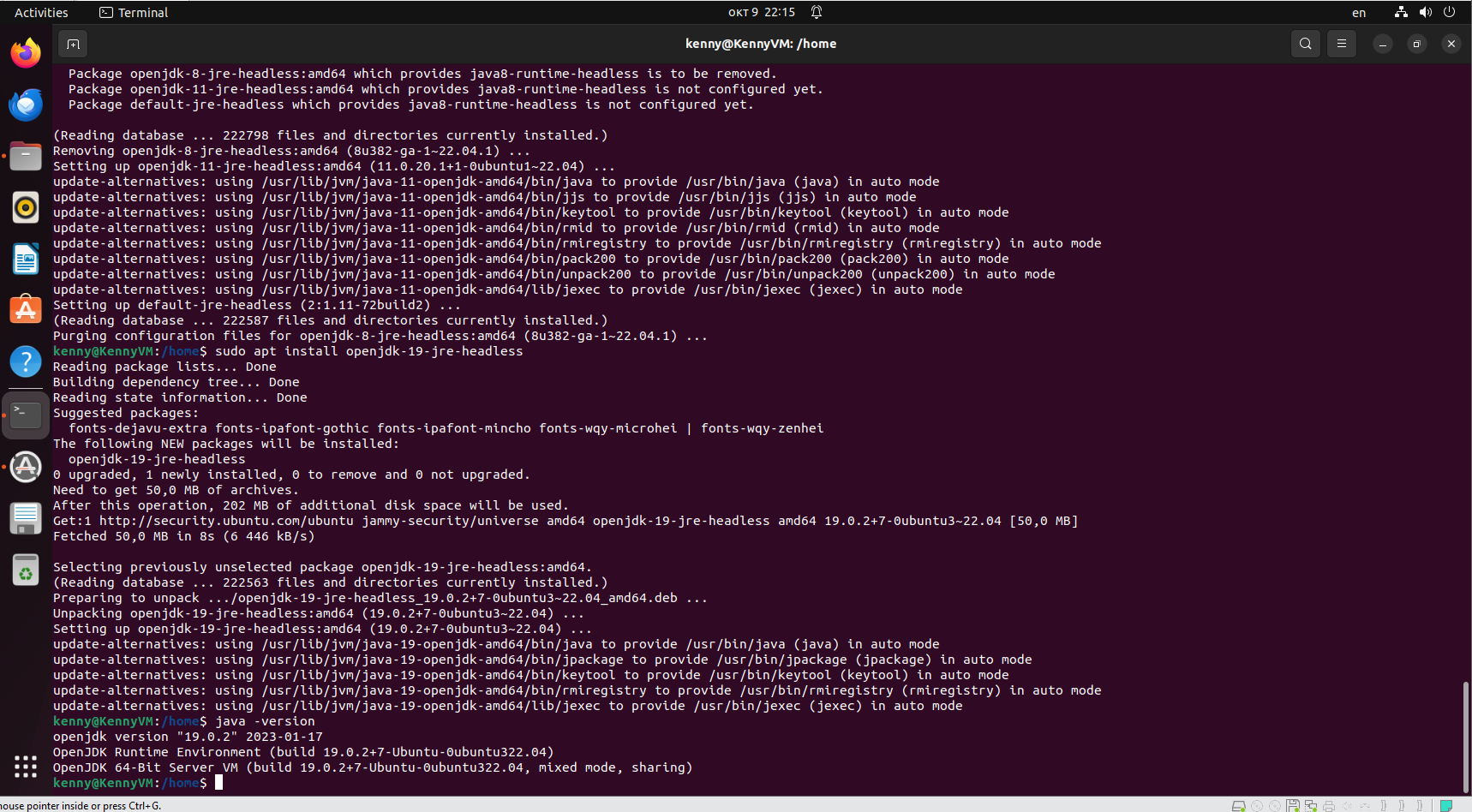
# Внесены изменения в файле /etc/pam.d/common-password (добавлен параметр minlen=8)



Скрин 6 (изменения в файле /etc/pam.d/common-password)

1. Установить на сервер пакеты Java.

# Командой sudo apt install openjdk-19-jre-headless произведена установка OpenJDK 19.0.2 и openJDK Runtime Environment



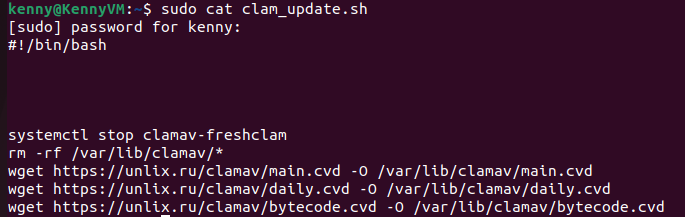
Скрин 7 (вывод команды java –version)

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

# 1. Установка ClamAV (sudo apt install clamav clamav-daemon)

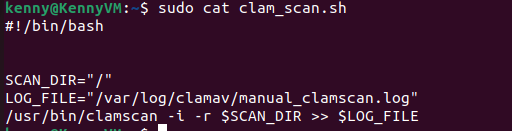
2. Остановка сервиса обновления (sudo systemctl stop clamav-freshclam)

3. Создание bash-скрипта для обновления БД ClamAV с сервера в РФ



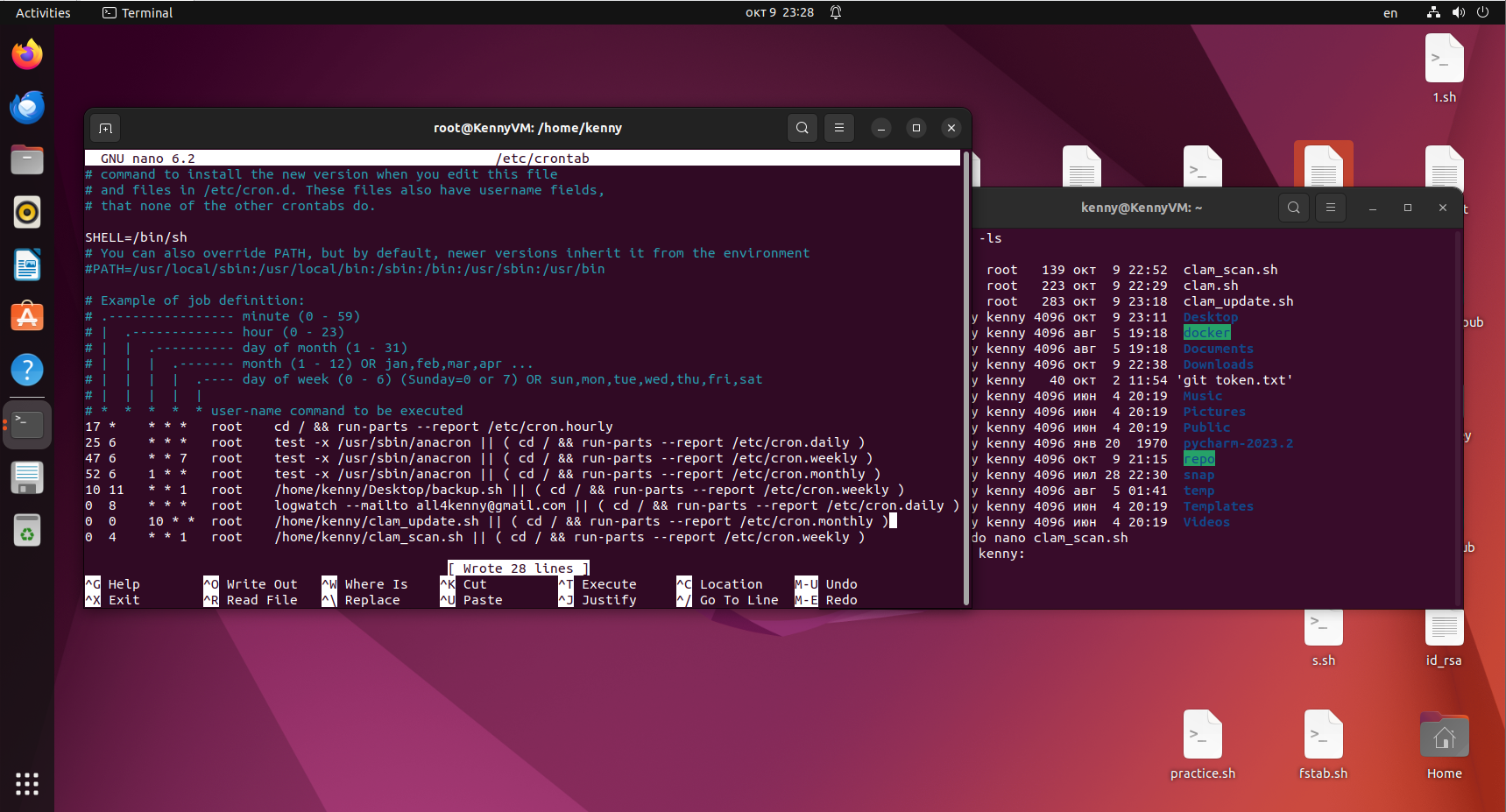
Скрин 8 (скрипт обновления баз антивируса)

4. Создание bash-скрипта для проверки всей ОС с логированием



Скрин 9 (скрипт проверки всей ОС)

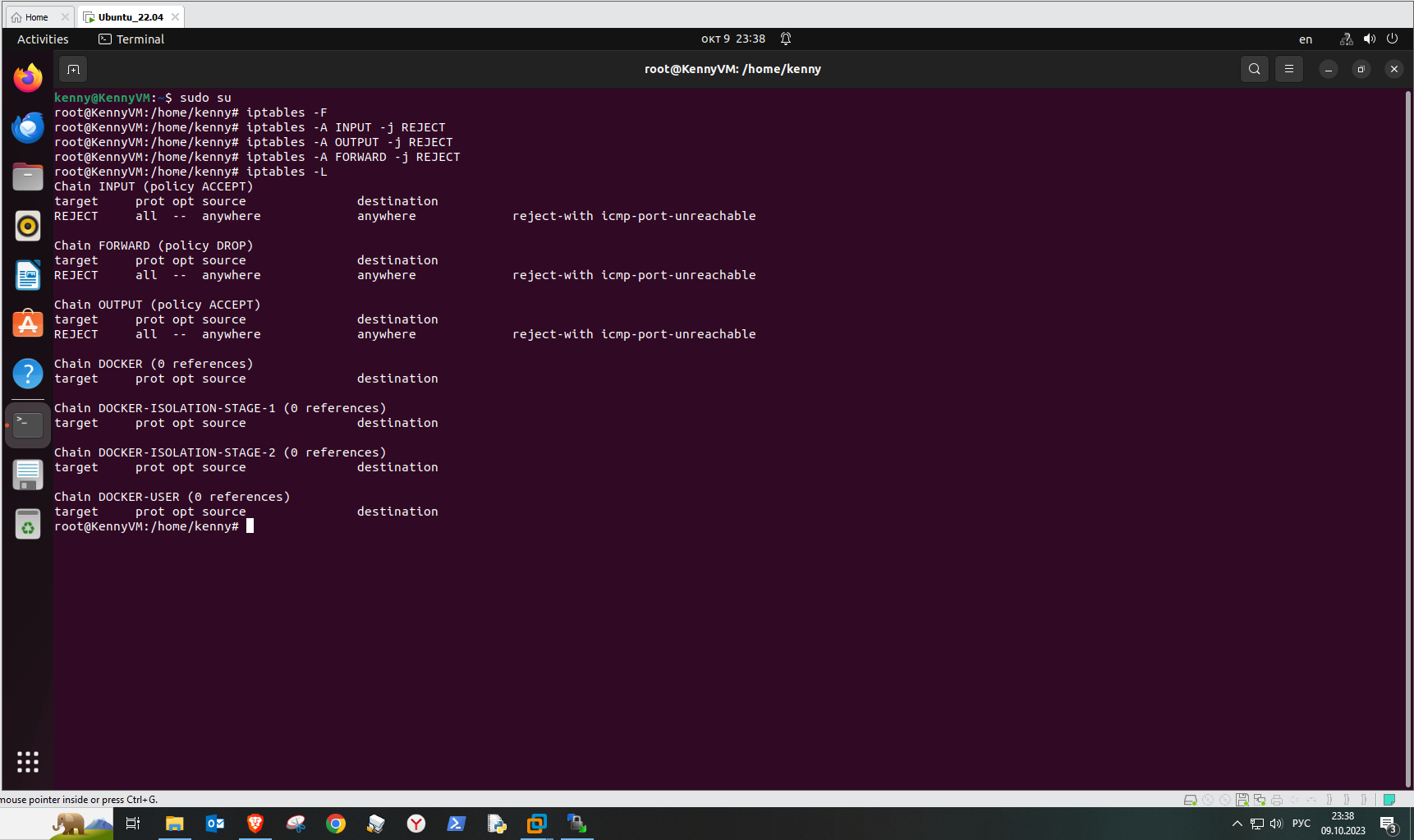
5. Создание задач в /etc/crontab для запуска скрипта сканирования в 4 утра каждый понедельник и запуска скрипта обновления каждый 10 день месяца



Скрин 10 (Содержимое /etc/crontab)

1. Настроить файервол на блокирование всего входящего и выходящего трафика.

# В iptables созданы правила для цепочек INPUT, OUTPUT и FORWARD с действием REJECT



Скрин 11 (вывод всех цепочек и правил iptables)