Выполните настройку по чек-листу:

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

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

Установить минимальную длину пароля для пользователя в 8 символов.

Установить на сервер пакеты Java.

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

Настроить файервол на блокирование всего входящего и выходящего трафика.

Пункт 1

sudo apt update

sudo apt-get install ssh

sudo apt install openssh-server

sudo systemctl enable sshd

systemctl status sshd

ssh-keygen

Generating public/private rsa key pair.

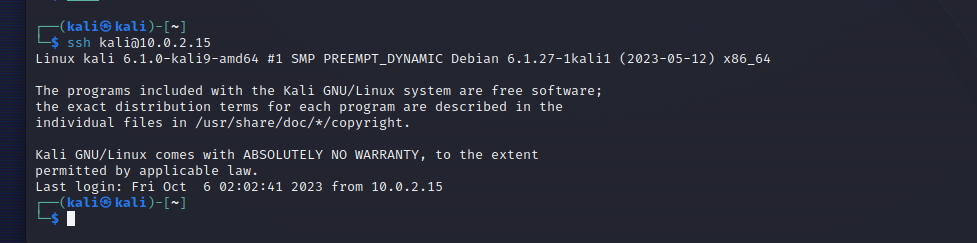
Enter file in which to save the key (/home/kali/.ssh/id\_rsa): ssh\_key

ssh kali@10.0.2.15

cat ~/.ssh/authorized\_keys

sudo sed -i 's/PasswordAuthentication yes/PasswordAuthentication no/g' /etc/ssh/sshd\_config

sudo service ssh restart



Cодержимое конфигурационного файла sshd

# 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 prohibit-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

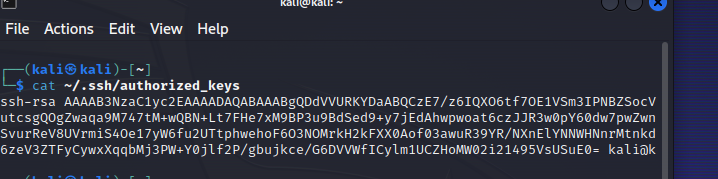
# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

Cодержимое файла authorized\_keys



Пункт 2

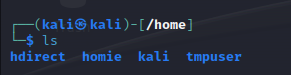
sudo useradd -m hdirect

sudo passwd hdirect

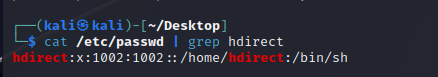
sudo visudo -f /etc/sudoers

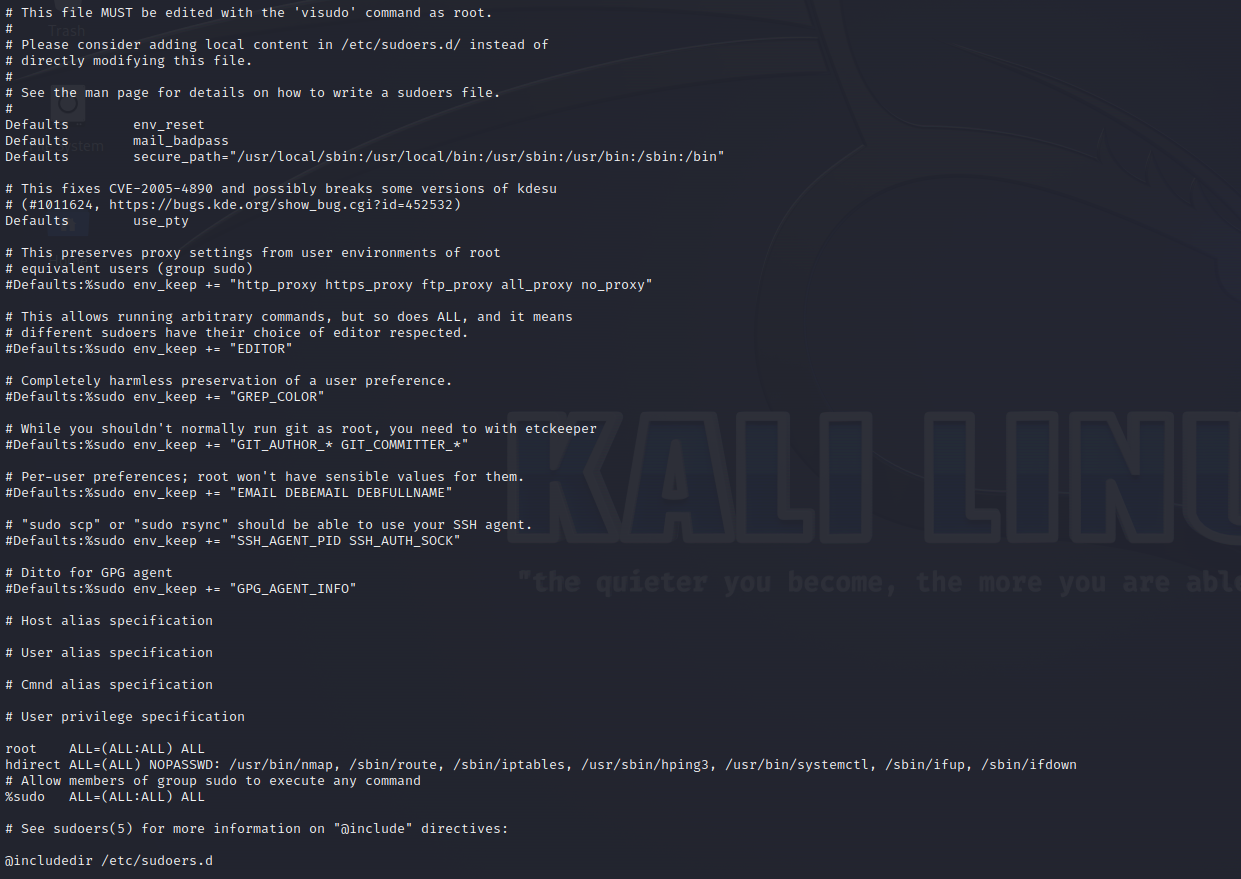
hdirect ALL=(ALL) NOPASSWD: /usr/bin/nmap, /sbin/route, /sbin/iptables, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown

вывод команды ls в директории home



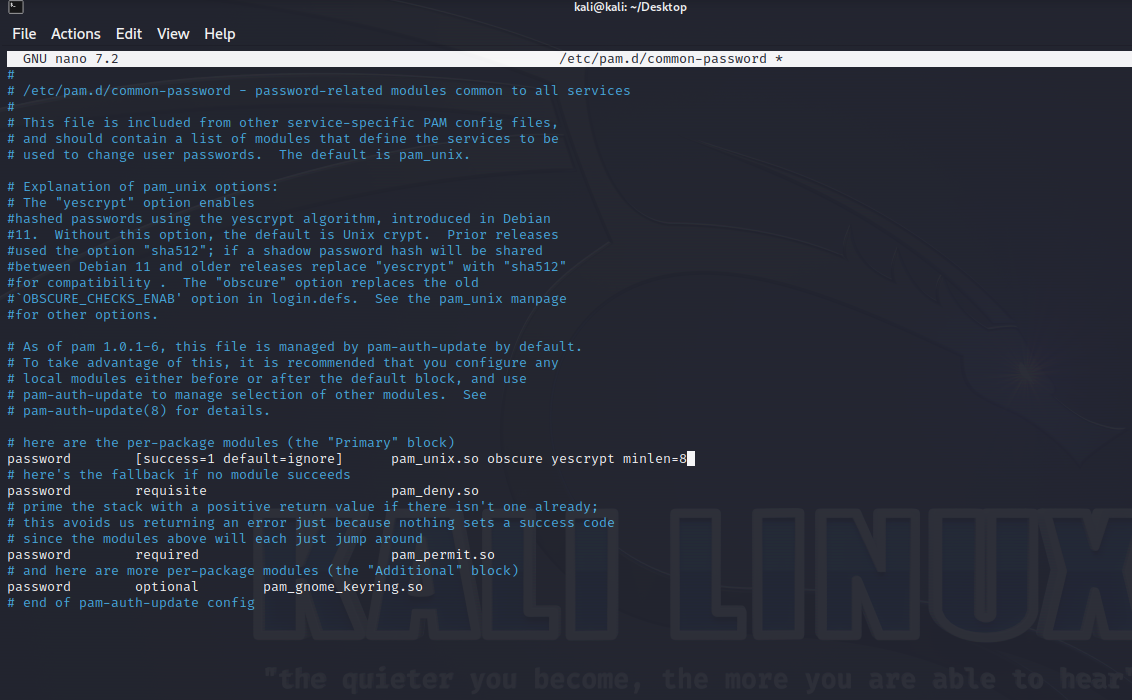
вывод файла passwd

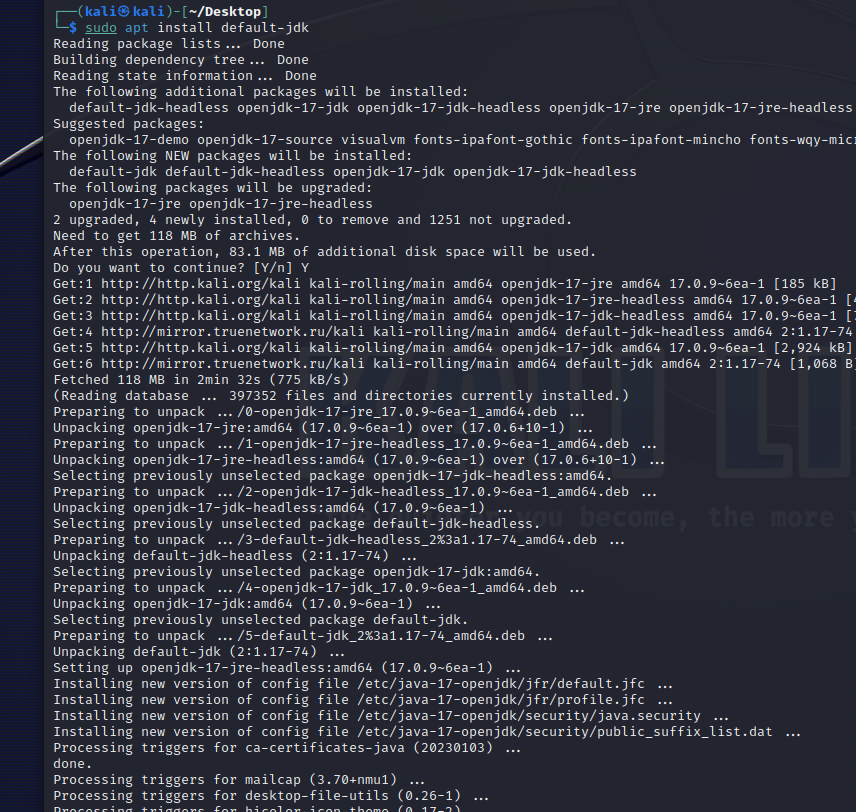


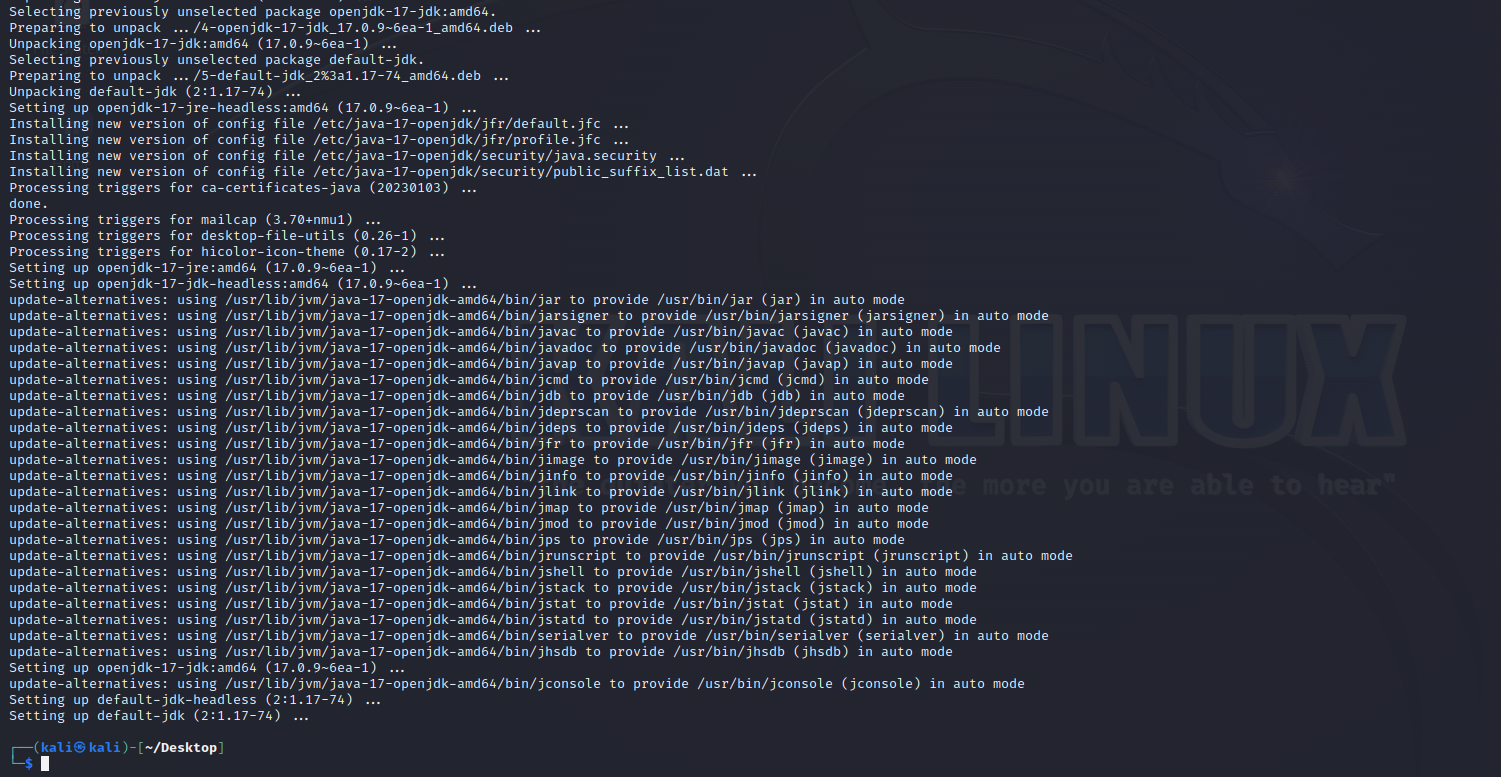
содержимое файла sudoers

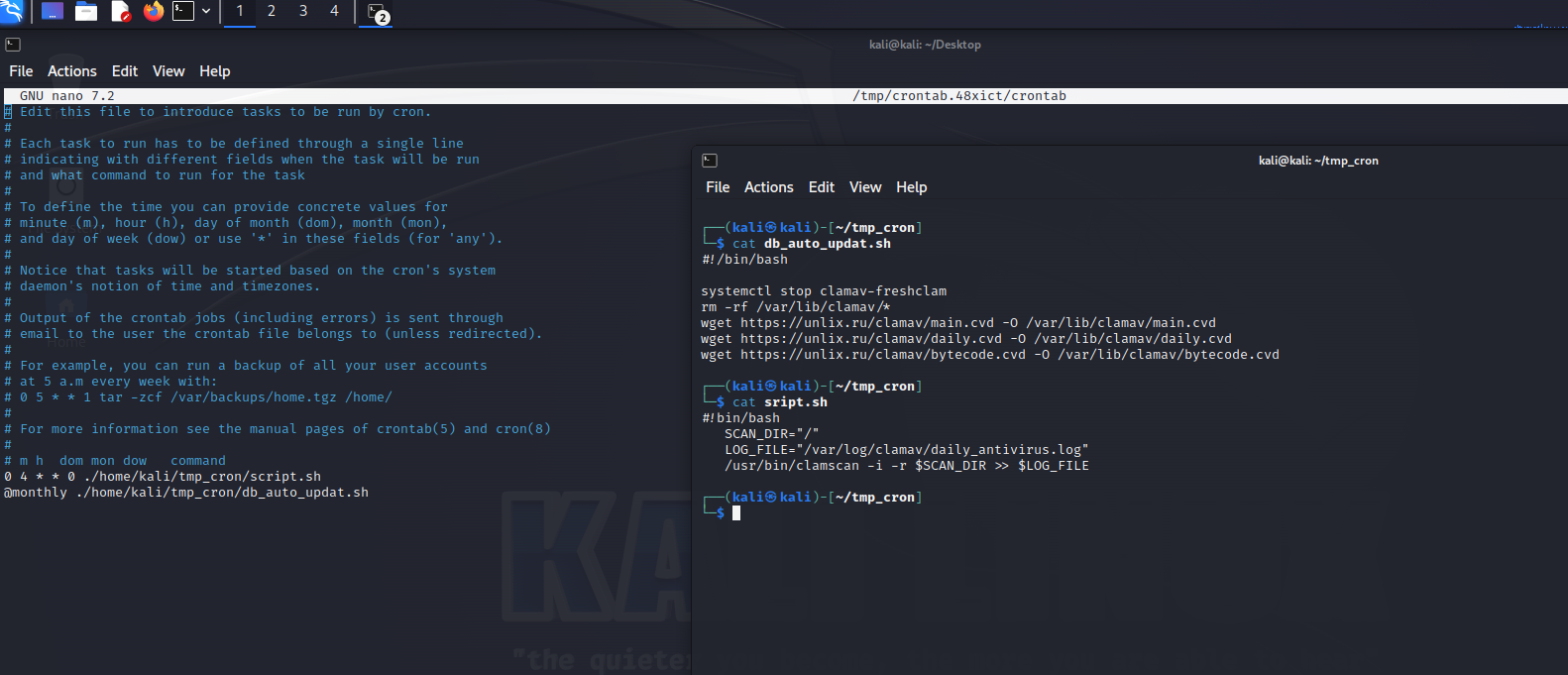
Пункт 3

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



Пункт 4



Пункт 5

Пункт 6

sudo iptables -A INPUT -j REJECT

sudo iptables -A OUTPUT -j REJECT

