Оглавление

[Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля. 2](#_Toc192852339)

[Создать нового пользователя с домашней директорией 7](#_Toc192852340)

[Установить минимальную длину пароля для пользователя в 8 символов. 11](#_Toc192852341)

[Установить на сервер пакеты Java. 13](#_Toc192852342)

[Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов. 15](#_Toc192852343)

[Настроить файервол на блокирование всего входящего и выходящего трафика. 16](#_Toc192852344)

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

Команду / набор команд / текст, которыми вы пользовались для выполнения задания.

Скриншот результата работы / получившегося файла.

Предоставьте всё содержимое конфигурационного файла sshd и содержимое файла authorized\_keys.

1. **sudo apt update**
2. **sudo apt install openssh-server**
3. **nano /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

# When systemd socket activation is used (the default), the socket

# configuration must be re-generated after changing Port, AddressFamily, or

# ListenAddress.

#

# For changes to take effect, run:

#

# systemctl daemon-reload

# systemctl restart ssh.socket

#

#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

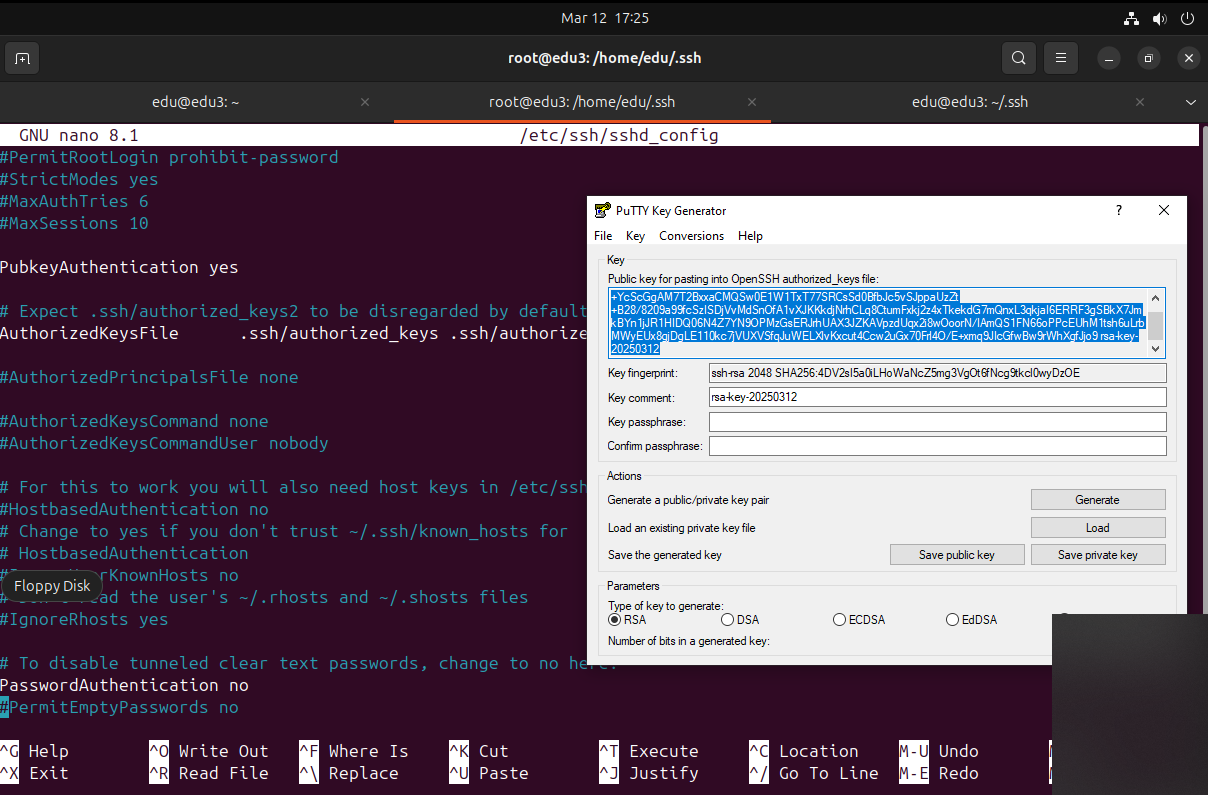
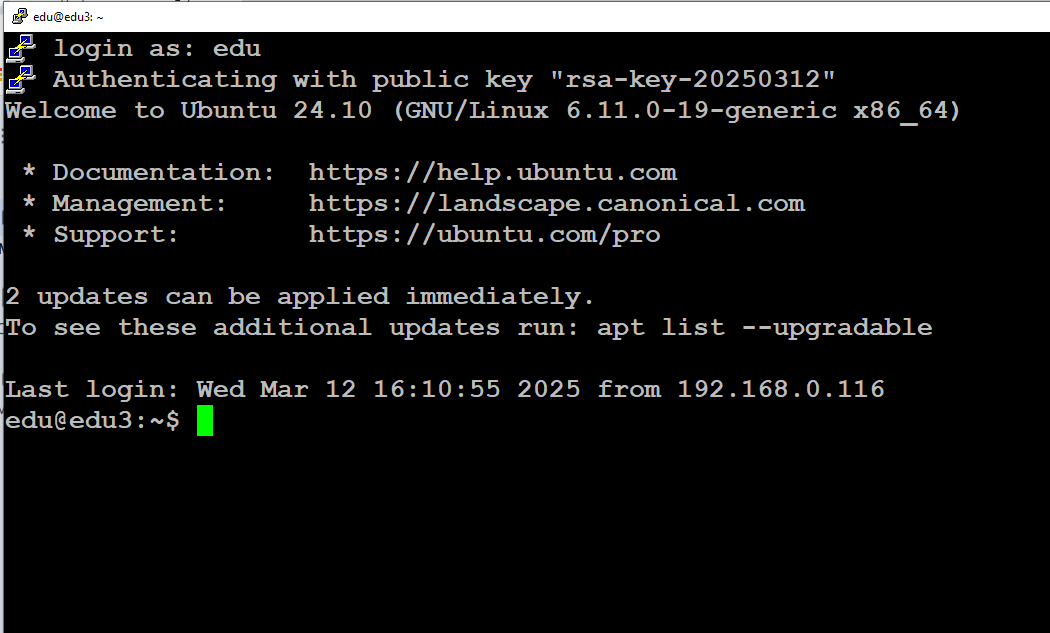
#Match User anoncvs

# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

1. **sudo service ssh restart**
2. **Генерим ключи**
3. 
4. **edu@edu3:~/.ssh$ nano authorized\_keys**
5. **ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCtyXST6pFTUET6X7AgO9KDhXPo17B2wFQ+YcScGgAM7T2BxxaCMQSw0E1W1TxT77SRCsSd0BfbJc5vSJppaUzZt+B28/8209a99fcSzISDjVvMdSnOfA1vXJKKkdjNrhCLq8CtumFxkj2z4xTkekdG7mQnxL3qkjaI6ERRF3gSBkX7JmkBYn1jJR1HIDQ06N4Z7YN9OPMzGsERJrhUAX3JZKAVpzdUqx2i8wOoorN/IAmQS1FN66oPPcEUhM1tsh6uLrbMWyEUx8gjDgLE110kc7jVUXVSfqJuWELXlvKxcut4Ccw2uGx70Frl4O/E+xmq9JIcGfwBw9rWhXgfJjo9 rsa-key-20250312**
6. **sudo service ssh restart**
7. **Подключаемся**
8. 

# Создать нового пользователя с домашней директорией

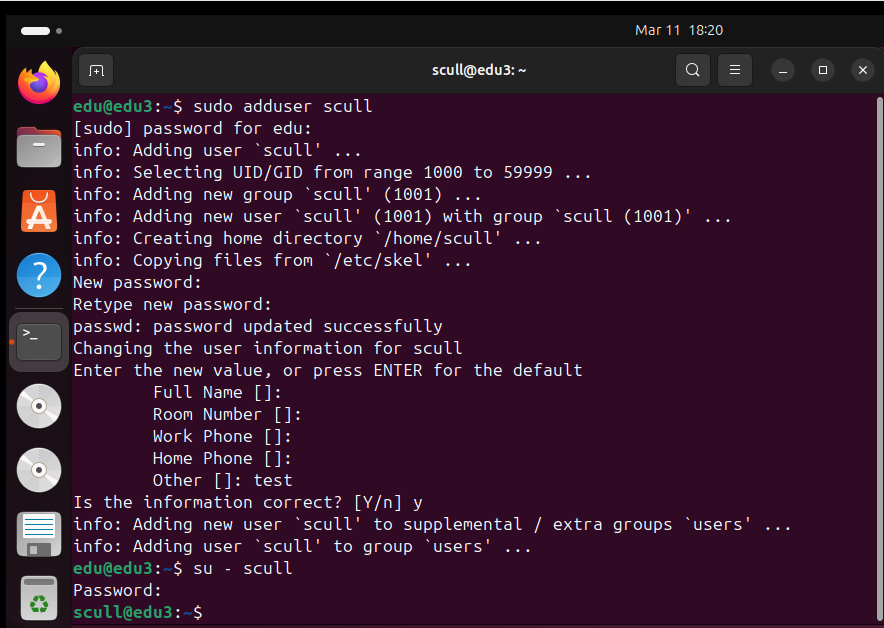
и выдать ему возможность запускать следующие утилиты без требования пароля

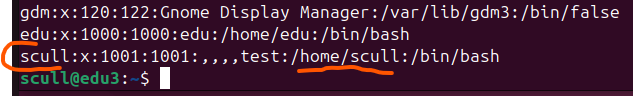
/sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3

usr/bin/systemctl

sbin/ifup, /sbin/ifdown

предоставьте вывод команды ls в директории home, вывод файла passwd, содержимое файла sudoers.

1. **Создание пользователя. sudo adduser scull**
2. 
3. **Вывод файла passwd: cat /etc/passwd**



1. **sudo visudo**
2. **Добавляем для scull: scull ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown**
3. **Cодержимое файла sudoers**

root@edu3:/home# cat /etc/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"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu

# (#1011624, https://bugs.kde.org/show\_bug.cgi?id=452532)

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

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

# Members of the admin group may gain root privileges

%admin ALL=(ALL) ALL

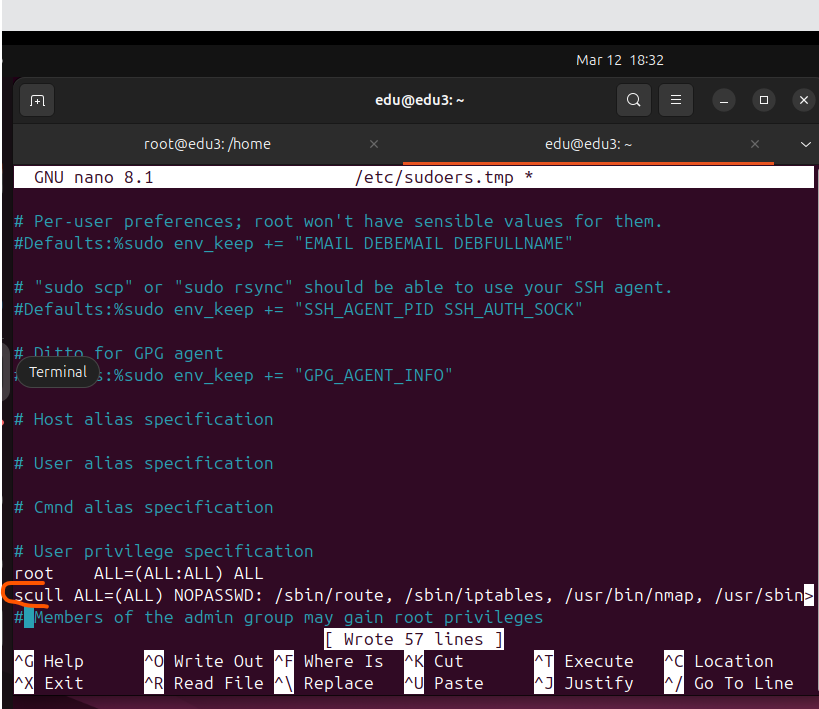
# Allow members of group sudo to execute any command

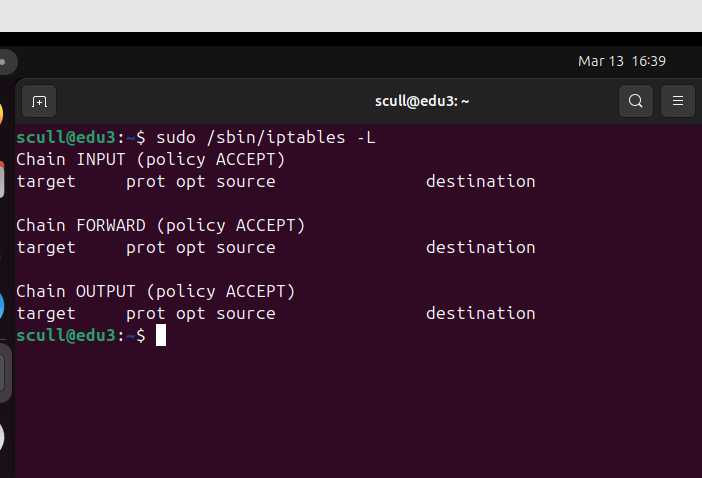
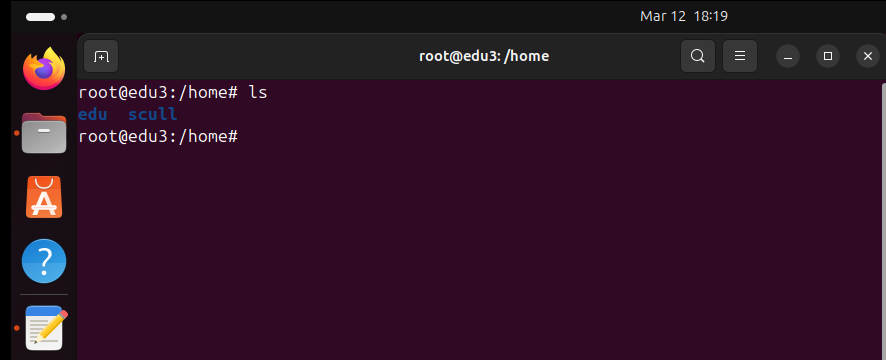
%sudo ALL=(ALL:ALL) ALL

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

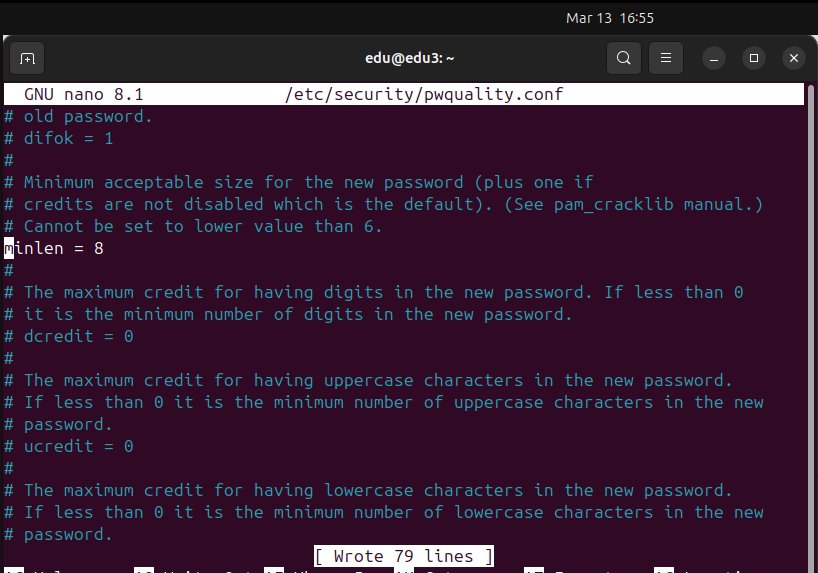
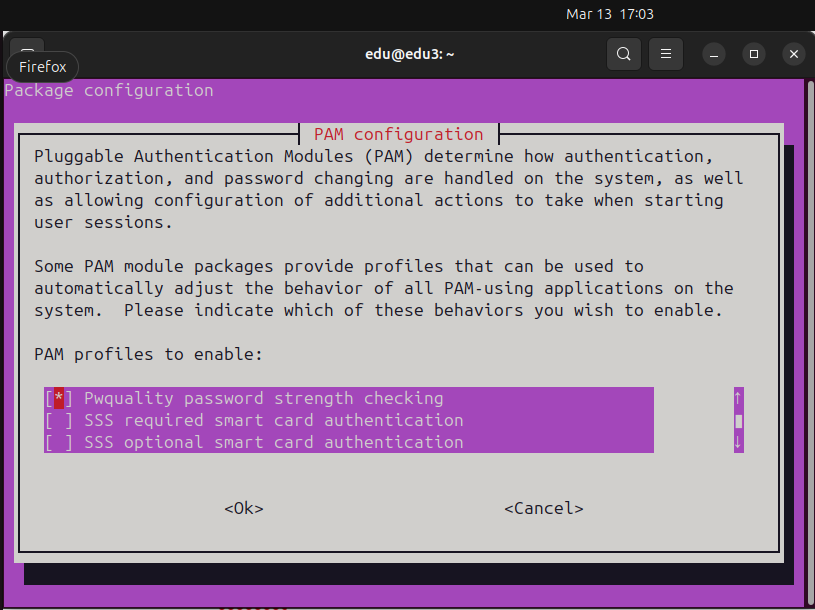
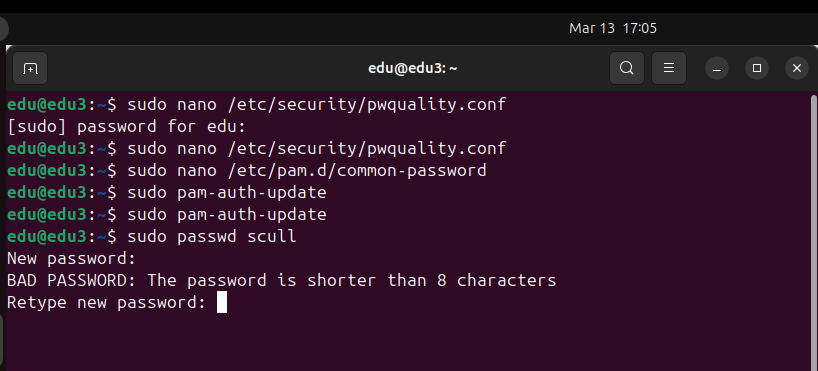
@includedir /etc/sudoers.d

root@edu3:/home#



1. **Проверяем исполнения команды без пароля**
2. 
3. **вывод команды ls в директории home**
4. 

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

1. sudo nano /etc/security/pwquality.conf
2. 
3. **sudo pam-auth-update**
4. 
5. Проверка sudo passwd scull
6. 
7. содержимое файла common-passwords.
8. sudo cat /etc/pam.d/common-password

#

# /etc/pam.d/common-password - password-related modules common to all services

#

# This file is included from other service-specific PAM config files,

# and should contain a list of modules that define the services to be

# used to change user passwords. The default is pam\_unix.

# Explanation of pam\_unix options:

# The "yescrypt" option enables

#hashed passwords using the yescrypt algorithm, introduced in Debian

#11. Without this option, the default is Unix crypt. Prior releases

#used the option "sha512"; if a shadow password hash will be shared

#between Debian 11 and older releases replace "yescrypt" with "sha512"

#for compatibility . The "obscure" option replaces the old

#`OBSCURE\_CHECKS\_ENAB' option in login.defs. See the pam\_unix manpage

#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.

# To take advantage of this, it is recommended that you configure any

# local modules either before or after the default block, and use

# pam-auth-update to manage selection of other modules. See

# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)

password requisite pam\_pwquality.so retry=3

password [success=2 default=ignore] pam\_unix.so obscure use\_authtok try\_first\_pass yescrypt

password sufficient pam\_sss.so use\_authtok

# here's the fallback if no module succeeds

password requisite pam\_deny.so

# prime the stack with a positive return value if there isn't one already;

# this avoids us returning an error just because nothing sets a success code

# since the modules above will each just jump around

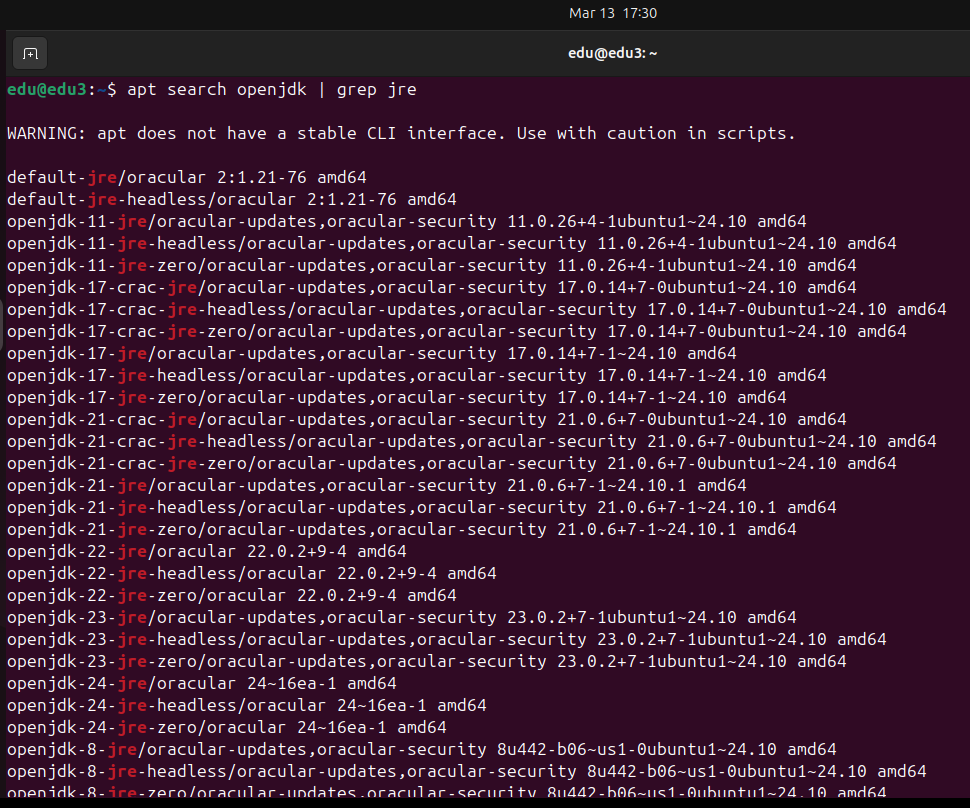
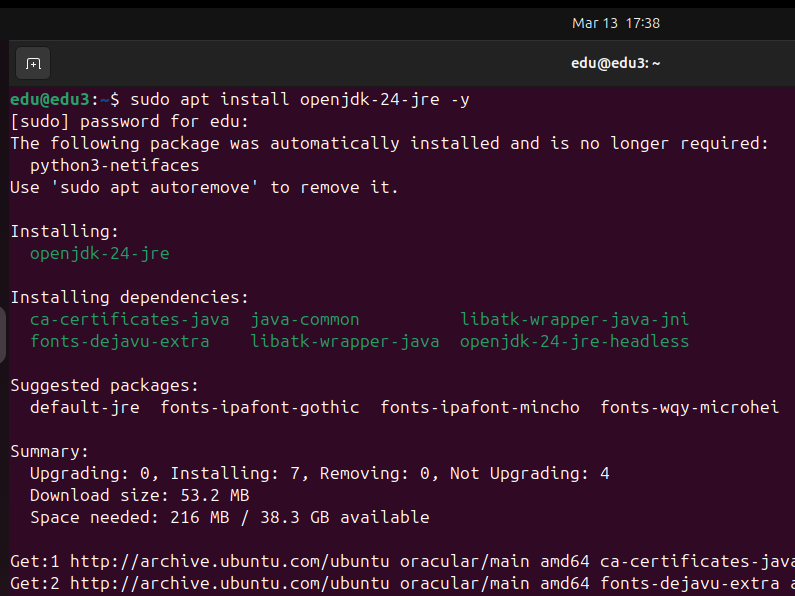
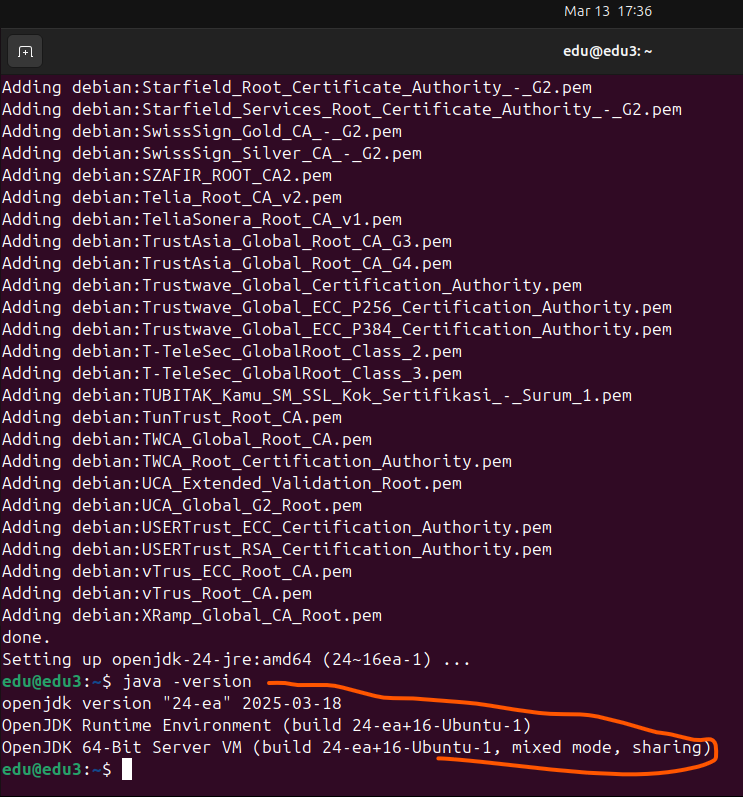
password required pam\_permit.so

# and here are more per-package modules (the "Additional" block)

password optional pam\_gnome\_keyring.so

# end of pam-auth-update config

## Установить на сервер пакеты Java.

1. **Узнаём последнюю версию apt search openjdk | grep jre**
2. 
3. **sudo apt install openjdk-24-jre –y**
4. ****
5. **java –version**
6. ****

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

* По пункту 5 предоставьте тексты задач cron, содержимое файла crontab (скрипт Bash — пожеланию)

1. **sudo nano /usr/local/bin/daily\_antivirus.sh**
2. **#!/bin/bash**

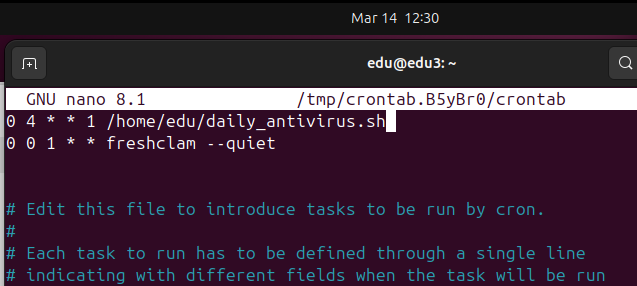
**LOG\_FILE="/var/log/clamav/daily\_antivirus.log"**

**SCAN\_DIR="/"**

**echo "Starting ClamAV scan at $(date)" >> $LOG\_FILE**

**clamscan -r --bell -i $SCAN\_DIR >> $LOG\_FILE**

**echo "Finished ClamAV scan at $(date)" >> $LOG\_FILE**

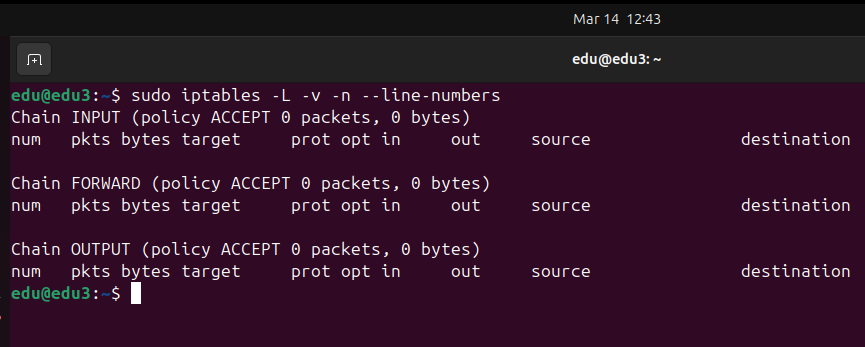
1. **sudo chmod +x /home/edu/daily\_antivirus.sh**
2. ****
3. **sudo crontab -e**

0 4 \* \* 1 /home/edu/daily\_antivirus.sh

0 0 1 \* \* freshclam --quiet

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

вывод всех цепочек и правил iptables

* 1. **sudo iptables -L -v -n --line-numbers**
  2. 
  3. **sudo apt update**
  4. **sudo apt install ufw**
  5. **sudo ufw status**
  6. **sudo ufw enable**
  7. **sudo ufw default deny incoming**
  8. **sudo ufw default deny outgoing**
  9. **sudo iptables -L -v -n --line-numbers**

**Chain INPUT (policy DROP** 15 packets, 9564 bytes)

num pkts bytes target prot opt in out source destination

1 653 59450 ufw-before-logging-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

2 653 59450 ufw-before-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

3 260 29134 ufw-after-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

4 21 10024 ufw-after-logging-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

5 21 10024 ufw-reject-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

6 21 10024 ufw-track-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

**Chain FORWARD (policy DROP** 0 packets, 0 bytes)

num pkts bytes target prot opt in out source destination

1 0 0 ufw-before-logging-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

2 0 0 ufw-before-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

3 0 0 ufw-after-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

4 0 0 ufw-after-logging-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

5 0 0 ufw-reject-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

6 0 0 ufw-track-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

**Chain OUTPUT (policy DROP** 0 packets, 0 bytes)

num pkts bytes target prot opt in out source destination

1 0 0 ufw-before-logging-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

2 0 0 ufw-before-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

3 0 0 ufw-after-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

4 0 0 ufw-after-logging-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

5 0 0 ufw-reject-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

6 0 0 ufw-track-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-after-forward (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-after-input (1 references)

num pkts bytes target prot opt in out source destination

1 153 11934 ufw-skip-to-policy-input 17 -- \* \* 0.0.0.0/0 0.0.0.0/0 udp dpt:137

2 1 229 ufw-skip-to-policy-input 17 -- \* \* 0.0.0.0/0 0.0.0.0/0 udp dpt:138

3 0 0 ufw-skip-to-policy-input 6 -- \* \* 0.0.0.0/0 0.0.0.0/0 tcp dpt:139

4 0 0 ufw-skip-to-policy-input 6 -- \* \* 0.0.0.0/0 0.0.0.0/0 tcp dpt:445

5 0 0 ufw-skip-to-policy-input 17 -- \* \* 0.0.0.0/0 0.0.0.0/0 udp dpt:67

6 0 0 ufw-skip-to-policy-input 17 -- \* \* 0.0.0.0/0 0.0.0.0/0 udp dpt:68

7 4 176 ufw-skip-to-policy-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ADDRTYPE match dst-type BROADCAST

Chain ufw-after-logging-forward (1 references)

num pkts bytes target prot opt in out source destination

1 0 0 LOG 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 10 LOG flags 0 level 4 prefix "[UFW BLOCK] "

Chain ufw-after-logging-input (1 references)

num pkts bytes target prot opt in out source destination

1 11 6844 LOG 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 10 LOG flags 0 level 4 prefix "[UFW BLOCK] "

Chain ufw-after-logging-output (1 references)

num pkts bytes target prot opt in out source destination

1 0 0 LOG 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 10 LOG flags 0 level 4 prefix "[UFW BLOCK] "

Chain ufw-after-output (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-before-forward (1 references)

num pkts bytes target prot opt in out source destination

1 0 0 ACCEPT 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED

2 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 3

3 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 11

4 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 12

5 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 8

6 0 0 ufw-user-forward 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-before-input (1 references)

num pkts bytes target prot opt in out source destination

1 0 0 ACCEPT 0 -- lo \* 0.0.0.0/0 0.0.0.0/0

2 0 0 ACCEPT 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED

3 0 0 ufw-logging-deny 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate INVALID

4 0 0 DROP 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate INVALID

5 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 3

6 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 11

7 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 12

8 0 0 ACCEPT 1 -- \* \* 0.0.0.0/0 0.0.0.0/0 icmptype 8

9 0 0 ACCEPT 17 -- \* \* 0.0.0.0/0 0.0.0.0/0 udp spt:67 dpt:68

10 441 42714 ufw-not-local 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

11 248 16831 ACCEPT 17 -- \* \* 0.0.0.0/0 224.0.0.251 udp dpt:5353

12 20 3980 ACCEPT 17 -- \* \* 0.0.0.0/0 239.255.255.250 udp dpt:1900

13 173 21903 ufw-user-input 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-before-logging-forward (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-before-logging-input (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-before-logging-output (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-before-output (1 references)

num pkts bytes target prot opt in out source destination

1 0 0 ACCEPT 0 -- \* lo 0.0.0.0/0 0.0.0.0/0

2 0 0 ACCEPT 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED

3 0 0 ufw-user-output 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-logging-allow (0 references)

num pkts bytes target prot opt in out source destination

1 0 0 LOG 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 10 LOG flags 0 level 4 prefix "[UFW ALLOW] "

Chain ufw-logging-deny (2 references)

num pkts bytes target prot opt in out source destination

1 0 0 RETURN 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ctstate INVALID limit: avg 3/min burst 10

2 0 0 LOG 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 10 LOG flags 0 level 4 prefix "[UFW BLOCK] "

Chain ufw-not-local (1 references)

num pkts bytes target prot opt in out source destination

1 1 44 RETURN 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ADDRTYPE match dst-type LOCAL

2 282 30331 RETURN 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ADDRTYPE match dst-type MULTICAST

3 158 12339 RETURN 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 ADDRTYPE match dst-type BROADCAST

4 0 0 ufw-logging-deny 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 10

5 0 0 DROP 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-reject-forward (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-reject-input (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-reject-output (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-skip-to-policy-forward (0 references)

num pkts bytes target prot opt in out source destination

1 0 0 DROP 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-skip-to-policy-input (7 references)

num pkts bytes target prot opt in out source destination

1 158 12339 DROP 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-skip-to-policy-output (0 references)

num pkts bytes target prot opt in out source destination

1 0 0 DROP 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-track-forward (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-track-input (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-track-output (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-user-forward (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-user-input (1 references)

num pkts bytes target prot opt in out source destination

Chain ufw-user-limit (0 references)

num pkts bytes target prot opt in out source destination

1 0 0 LOG 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 limit: avg 3/min burst 5 LOG flags 0 level 4 prefix "[UFW LIMIT BLOCK] "

2 0 0 REJECT 0 -- \* \* 0.0.0.0/0 0.0.0.0/0 reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)

num pkts bytes target prot opt in out source destination

1 0 0 ACCEPT 0 -- \* \* 0.0.0.0/0 0.0.0.0/0

Chain ufw-user-logging-forward (0 references)

num pkts bytes target prot opt in out source destination

Chain ufw-user-logging-input (0 references)

num pkts bytes target prot opt in out source destination

Chain ufw-user-logging-output (0 references)

num pkts bytes target prot opt in out source destination

Chain ufw-user-output (1 references)

num pkts bytes target prot opt in out source destination