#### **Задание 1: Регулярное обновление системы**

1. **Открыть терминал**:  
   Выполните команды:  
   sudo apt update

sudo apt upgrade -y

1. Перезагрузите систему:  
   sudo reboot

**Вопросы для самопроверки:**

* Использованные команды: sudo apt update, sudo apt upgrade.
* Вывод команд покажет, были ли установлены обновления (информация о новых версиях пакетов).

#### **Задание 2: Создание и управление сильными паролями**

**Изменение пароля пользователя**:  
  
1. passwd - Введите сложный пароль (буквы разного регистра, цифры, специальные символы).

**2. Установка менеджера паролей** (пример с **KeePass**):  
  
sudo apt install keepassxc

keepassxc

Создайте файл базы данных, установите мастер-пароль.

**Вопросы для самопроверки:**

* Критерии для пароля: длина > 12 символов, буквы, цифры, символы, без повторяющихся шаблонов.
* Выбранный менеджер паролей (например, KeePass) настроен для хранения паролей в защищённой базе.

##################################################################

$ passwd

Changing password for user.

Current password: \*\*\*\*\*\*\*\*

New password: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Retype new password: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

passwd: password updated successfully

$ sudo apt update && sudo apt install keepassxc -y

Reading package lists... Done

Building dependency tree... Done

The following additional packages will be installed:

libargon2 libqt5concurrent5 libqt5svg5

The following NEW packages will be installed:

keepassxc libargon2 libqt5concurrent5 libqt5svg5

0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.

Need to get 10.2 MB of archives.

After this operation, 29.7 MB of additional disk space will be used.

Do you want to continue? [Y/n] Y

...

$ keepassxc

**GUI действия:**

1. В графическом интерфейсе KeePassXC выберите **"Create New Database"**.
2. Установите **мастер-пароль**, например: S3cur3!P@ssw0rd2024.
3. Сохраните базу данных с именем Passwords.kdbx.

######################################################################

#### **Задание 3: Ограничение прав доступа**

**Создание нового пользователя**:  
  
1. sudo adduser newuser - Следуйте инструкциям, не добавляйте пользователя в административные группы.

**2. Ограничение прав доступа к домашней директории**:  
  
 sudo chmod 700 /home/newuser

**Вопросы для самопроверки:**

* Права доступа для нового пользователя ограничены с помощью chmod.
* Назначенные права: только владелец имеет доступ (700).

#### **Задание 4: Аудит и мониторинг системы**

1. **Установка и запуск auditd**:  
   sudo apt install auditd

sudo service auditd start

1. **Настройка правил аудита** в /etc/audit/audit.rules (пример):  
    -w /etc/passwd -p wa -k passwd\_changes

Примените правила:  
 sudo systemctl restart auditd

1. **Просмотр логов аудита**:  
   sudo ausearch -i

**Вопросы для самопроверки:**

* Настроены правила для мониторинга изменений в системных файлах.
* Логи показывают действия, например, изменение /etc/passwd.

###########################################################

$ sudo apt update && sudo apt install auditd -y

Reading package lists... Done

Building dependency tree... Done

The following additional packages will be installed:

auditd-tools

The following NEW packages will be installed:

auditd auditd-tools

...

$ sudo service auditd start

$ sudo service auditd status

● auditd.service - Security Auditing Service

Loaded: loaded (/lib/systemd/system/auditd.service;

#############################################################

#### **Задание 5: Настройка файервола и антивируса**

1. **Настройка ufw**:  
     
   sudo apt install ufw

sudo ufw enable

sudo ufw allow ssh

sudo ufw allow http

sudo ufw allow https

1. **Установка и использование ClamAV**:  
     
   sudo apt install clamav

sudo freshclam

sudo clamscan -r /home

**Вопросы для самопроверки:**

* Настроены правила файервола для SSH, HTTP, HTTPS.
* Установлена антивирусная программа ClamAV, проведено сканирование.

#### **Задание 6: Шифрование данных**

1. **Установка GnuPG**:  
    sudo apt install gnupg
2. **Создание ключа**:  
    gpg --gen-key
3. **Шифрование файла**:  
    gpg -c filename
4. **Расшифровка файла**:  
    gpg filename.gpg

**Вопросы для самопроверки:**

* Ключ для шифрования создан с помощью gpg --gen-key.
* Команды: gpg -c для шифрования, gpg для расшифровки.

#######################################################################

$ sudo apt install gnupg -y

Reading package lists... Done

Building dependency tree... Done

The following NEW packages will be installed:

gnupg

0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.

Need to get 2,493 kB of archives.

After this operation, 6,738 kB of additional disk space will be used.

Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 gnupg all 2.2.19-3ubuntu2 [2,493 kB]

Fetched 2,493 kB in 1s (4,069 kB/s)

Selecting previously unselected package gnupg.

(Reading database ... 209715 files and directories currently installed.)

Preparing to unpack .../gnupg\_2.2.19-3ubuntu2\_all.deb ...

Unpacking gnupg (2.2.19-3ubuntu2) ...

Setting up gnupg (2.2.19-3ubuntu2) ...

Processing triggers for man-db (2.9.1-1) ...

$ gpg --gen-key

gpg (GnuPG) 2.2.19; Copyright (C) 2020 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:

(1) RSA and RSA (default)

(2) DSA and Elgamal

(3) DSA (sign only)

(4) RSA (sign only)

Your selection? 1

RSA keys may be between 1024 and 4096 bits long.

What keysize do you want? (3072) 4096

Requested keysize is 4096 bits

Please specify how long the key should be valid.

0 = key does not expire

<n> = key expires in n days

<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0) 0

Key does not expire at all

Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: John Doe

Email address: johndoe@example.com

Comment: Testing GPG Encryption

You selected this USER-ID:

"John Doe (Testing GPG Encryption) <johndoe@example.com>"

Change (N)ame, (C)omment, (E)mail, or (O)kay/(Q)uit? O

We need a passphrase to protect your key.

Enter passphrase: \*\*\*\*\*\*\*\*

Repeat passphrase: \*\*\*\*\*\*\*\*

gpg: key ABCD1234EF567890 marked as ultimately trusted

gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-revocs.d/ABCD1234EF567890.rev'

public and secret key created and signed.

$ echo "Это секретная информация" > secret.txt

$ gpg -c secret.txt

Enter passphrase: \*\*\*\*\*\*\*\*

Repeat passphrase: \*\*\*\*\*\*\*\*

$ ls

secret.txt secret.txt.gpg

$ rm secret.txt

$ gpg secret.txt.gpg

Enter passphrase: \*\*\*\*\*\*\*\*

$ ls

secret.txt secret.txt.gpg

$ cat secret.txt

Это секретная информация

######################################################################

#### **Задание 7: Резервное копирование данных**

1. **Установка rsync**:  
    sudo apt install rsync
2. **Создание скрипта для резервного копирования**:  
    rsync -av --delete /home/user/ /backup/home/user/
3. **Настройка cron для автоматизации**:  
    crontab -e

Добавьте строку:  
 0 2 \* \* \* /usr/bin/rsync -av --delete /home/user/ /backup/home/user/

**Вопросы для самопроверки:**

* Использован инструмент rsync.
* Настроен cron для ежедневного выполнения резервного копирования в 02:00.