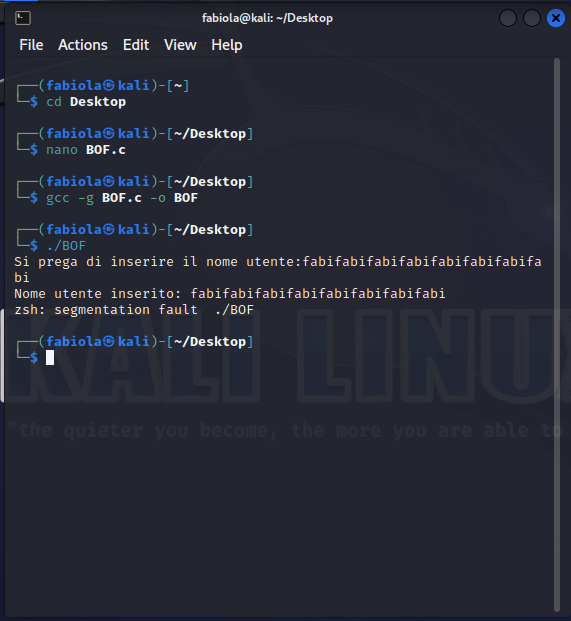
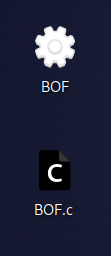
**BOF** è un acronimo che sta per "Buffer Overflow". Si tratta di una vulnerabilità di sicurezza che si verifica quando un programma, durante l'esecuzione, scrive più dati in un buffer (una zona di memoria temporanea) di quanta memoria sia stata allocata per quel buffer. Ciò può causare la sovrascrittura della memoria adiacente, che potrebbe contenere dati importanti o istruzioni di esecuzione del programma. Gli attaccanti possono sfruttare questa vulnerabilità per eseguire codice dannoso o causare il crash del programma.

Nell’esercizio di oggi vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata **«segmentation fault»**, ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere.

Per creare un nuovo documento su Kali, avviamo Kali Linux, apriamo il terminale, spostiamoci sul desktop eseguendo il comando: **cd Desktop**.

Successivamente, eseguiamo l’editor di testo nano, che ci permette o di aprire un file esistente oppure di crearne uno nuovo se il nome del file specificato non esiste. Eseguiamo quindi dal terminale il comando di seguito per creare un file BOF.c; **nano BOF.c** . Riportiamo il frammento di codice, chiudiamo e salviamo il file:

A questo punto, compiliamo il file utilizzando il comando: **gcc –g BOF.c –o BOF** . Una volta fatto, potete eseguire il programma eseguendo il comando: **./BOF**

Il programma si avvia chiedendoci di inserire un nome utente: inserendo un nome utente di 5 caratteri, il programma non ci riporta nessun problema, infatti come sappiamo il buffer accetta fino a 10 caratteri. Se inseriamo 30 caratteri il programma ci ritorna un errore, **«segmentation fault»**, ovvero errore di segmentazione. L’errore di segmentazione avviene quando un programma, come abbiamo detto in precedenza, tenta di scrivere contenuti su una porzione di memoria alla quale non ha accesso. Questo è un chiaro esempio di BOF, abbiamo inserito 30 caratteri in un buffer che ne può contenere solamente 10 e di conseguenza alcuni caratteri stanno sovrascrivendo aree di memorie inaccessibili.

Ora proviamo a riprodurre l’errore di segmentazione modificando il programma; aumentando la dimensione del vettore a 30.

Inserendo un nome utente del numero predisposto di caratteri, questo si inserirà con successo: