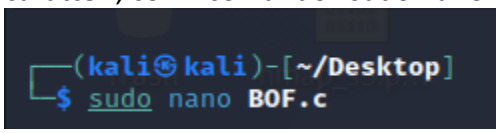
BUFFER OVERFLOW

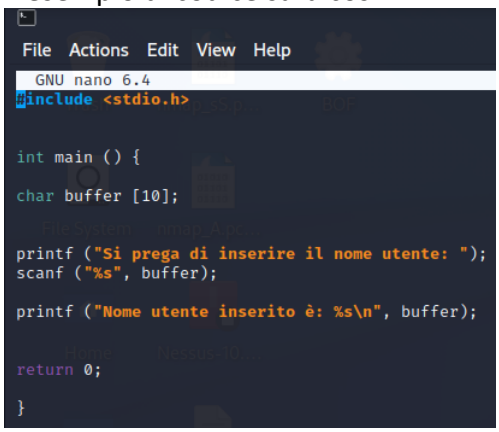
FRANCESCO PERSICHETTI

Esempio di esercizio in C vulnerabile al BOF (buffer overflow)

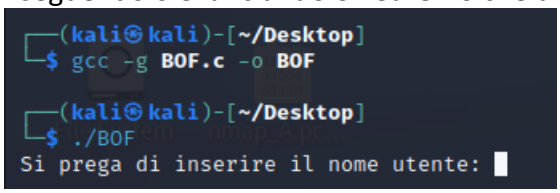
Scrivo il mio codice in C dove imposto che l'utente può inserire una stringa di massimo 10 caratteri, con il comando "sudo nano BOF.c"

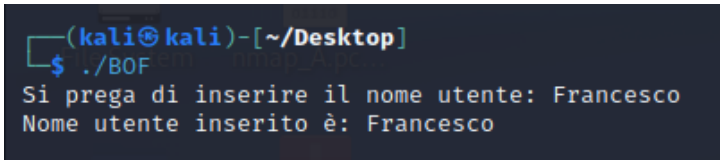


L'esempio di codice sarà così

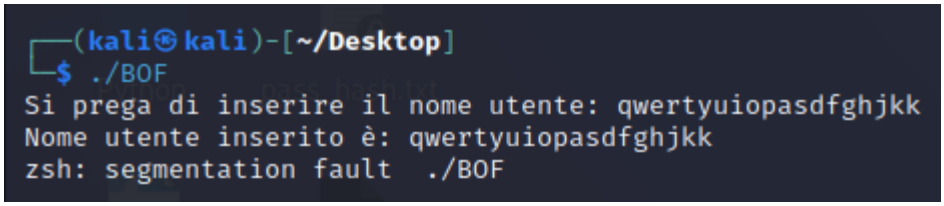


Eseguendolo e lanciandolo vedremo che una stringa entro i 10 caratteri verranno accettati





Nel caso scrivessi una stringa più lunga mi restituirà l'errore "segmentation fault" ossia errore di segmentazione che avviene quando il programma tenta di sovrascrivere dati in una porzione di memoria a cui non ha accesso



Si può risolvere aumentando le dimensioni del buffer