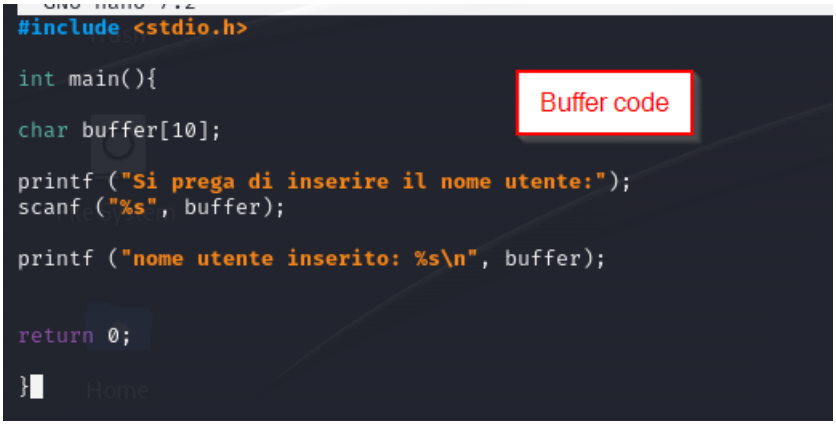
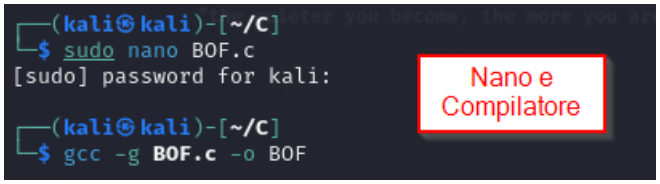
ESERCIZIO W17D4

L'esercizio ci porta a comprendere meglio come funziona una vulnerabilità del tipo buffer overflow. Procediamo col creare un file di testo per il nostro programma in C. Scriviamo e lanciamo sudo nano BOF.c.

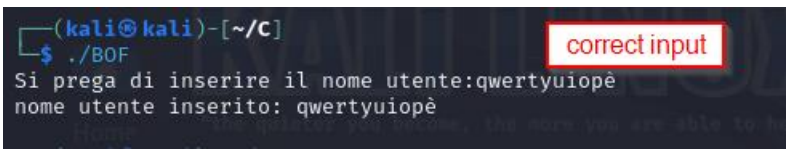
Dichiariamo un array che andremo a riempire con degli input di tipo stringa.



Una volta salvato il file, usciamo da quest'ultimo e passiamo alla fase di compilazione. Creiamo un file compilato chiamato BOF, da avviare per mezzo del comando ./BOF.



Il programma sembra rispondere bene. Abbiamo provato con un numero adeguato di input. Adesso, vediamo cosa succede se esageriamo.



Capiamo di essere andati troppo oltre quando sul terminale compare “segmentation fault”. Concludiamo l’esercitazione con l’ultima task. Cambiamo la grandezza del buffer dal programma, ricompiliamo, e diamoci alla pazza gioia con la tastiera, di nuovo.