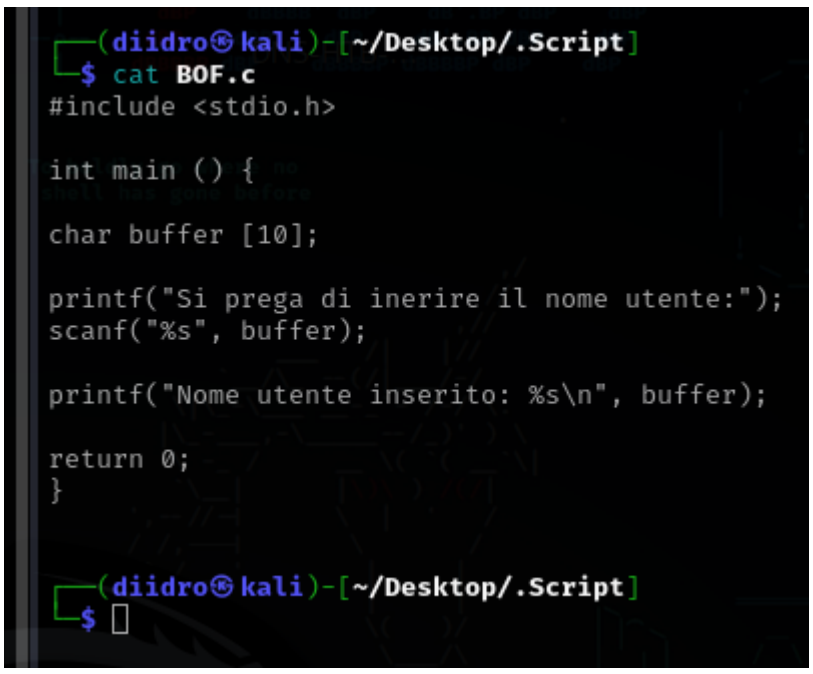
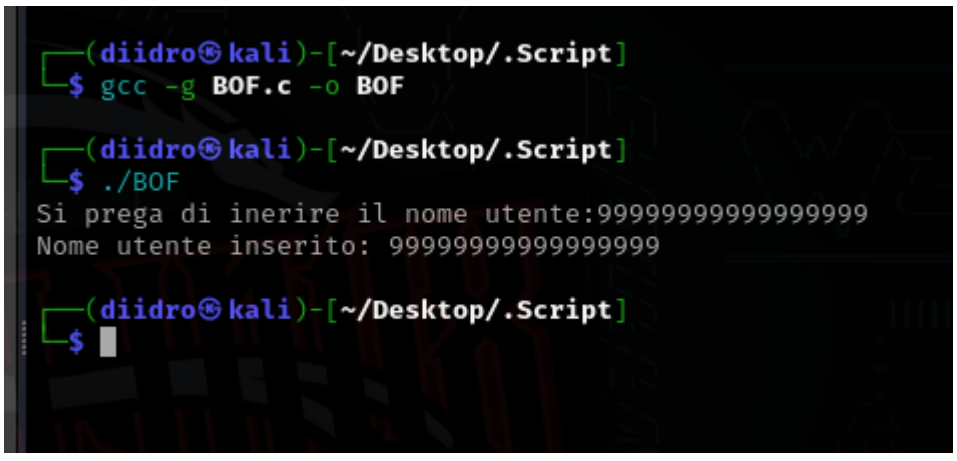
S7-L4

Il programma in C su cui ci baseremo è stato denominato BOF.c e contiene il seguente codice (char buffer 10):

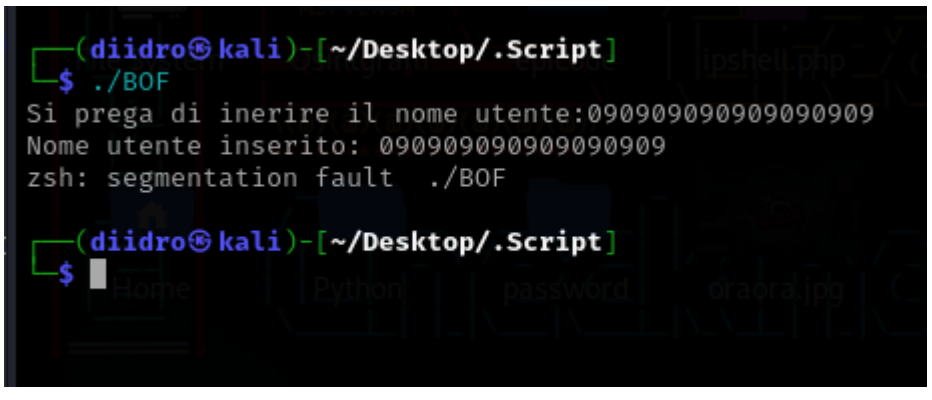


Utilizziamo il compilatore gcc specificando il file sorgente da compilare (BOF.c) ed il nome del file eseguibile risultante (BOF).

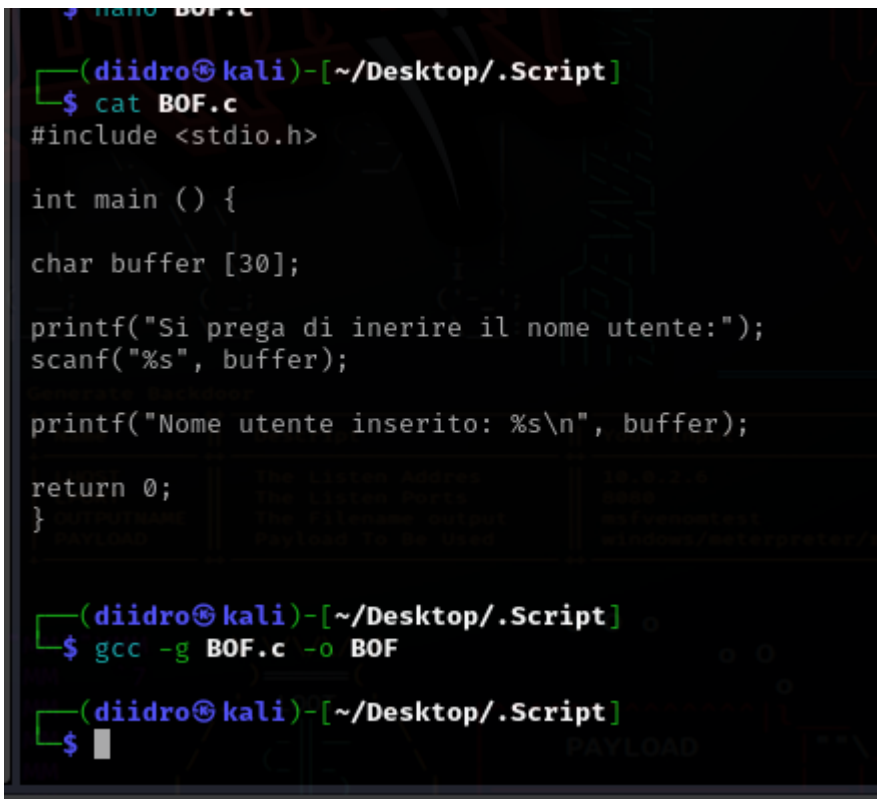
Fatto questo lanciamo BOF ed inseriamo dei caratteri (nel nostro caso ne abbiamo inseriti 17, il programma ha preso correttamente i dati inseriti).



Facendo varie prove abbiamo notato come, una volta inseriti 18 caratteri, il programma ci esponeva un errore di “segmentation fault” (errore che compare quando il programma tenta di accedere ad una memoria che non gli è permesso usare).



Modifichiamo il programma originale impostando un char buffer pari a 30 e vediamo cosa cambia.
Prima di lanciarlo bisogna riutilizzare il compilatore gcc come fatto in precedenza.



In questo caso abbiamo appreso come inserendo 39 caratteri, questi vengano presi correttamente dal programma; tuttavia, inseriti 41 caratteri, ricompare il segmentation fault.