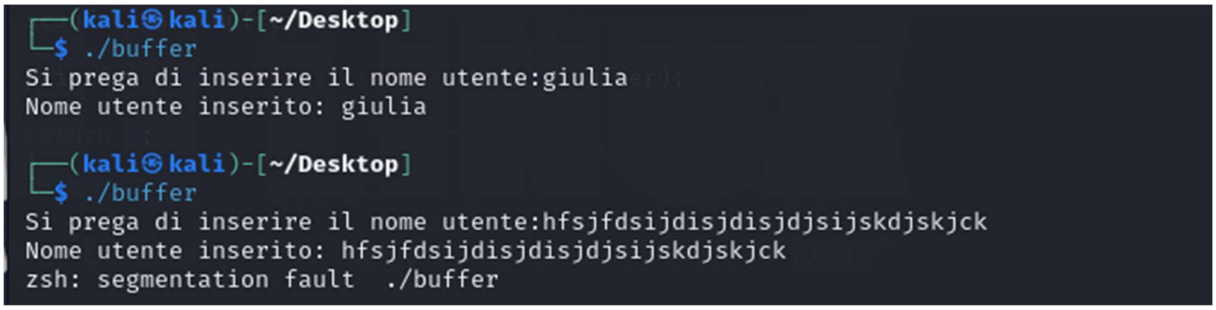
ESERCIZIO S7-L4

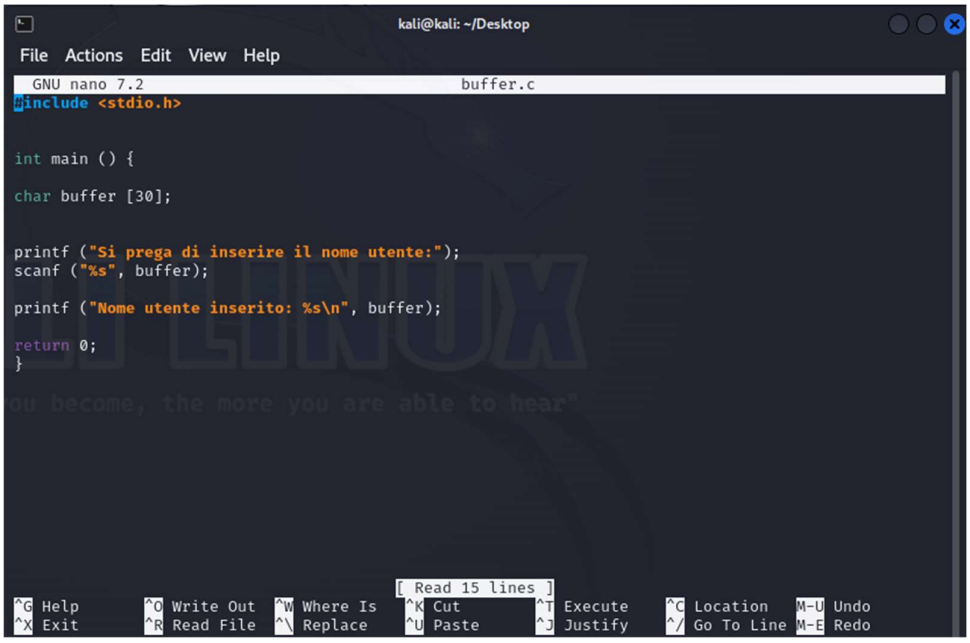
L'esercizio di oggi riguarda un programma in C vulnerabile al buffer overflow, cioè un errore di memoria che avviene quando un programma cerca di scrivere in parti di memoria dove non gli è permesso scrivere.

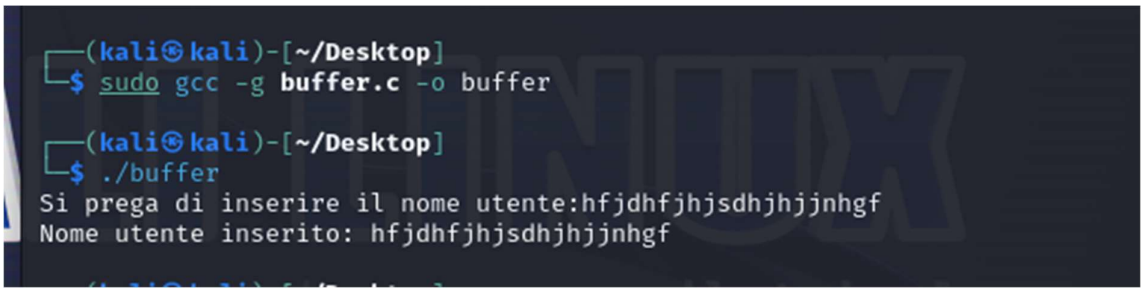
Il programma in questione ci chiede di inserire un nome utente, inserendo un nome di 6 caratteri esso non presenta nessun problema, perché il buffer accetta fino a 10 caratteri dichiarati nella variabile "char".

Inserendo più di 10 caratteri, il programma ci dà un errore del tipo «segmentation fault», ovvero errore di segmentazione, perché come menzionato prima, il programma tenta di scrivere su porzioni di memoria alla quale non ha accesso.



Aumentando il valore della variabile "char" a 30 caratteri, non dovrebbe dare errore se inseriamo fino a 30 caratteri circa.





Per rendere questo programma più sicuro, è consigliabile usare ad esempio “%29s” per evitare il buffer overflow. Inserendo ciò, il programma accetta in input solo i primi 29 caratteri scartando gli altri in modo tale che l’errore non si verifichi.