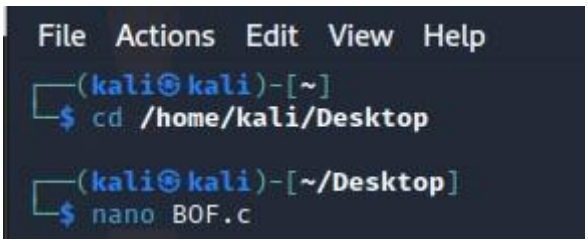
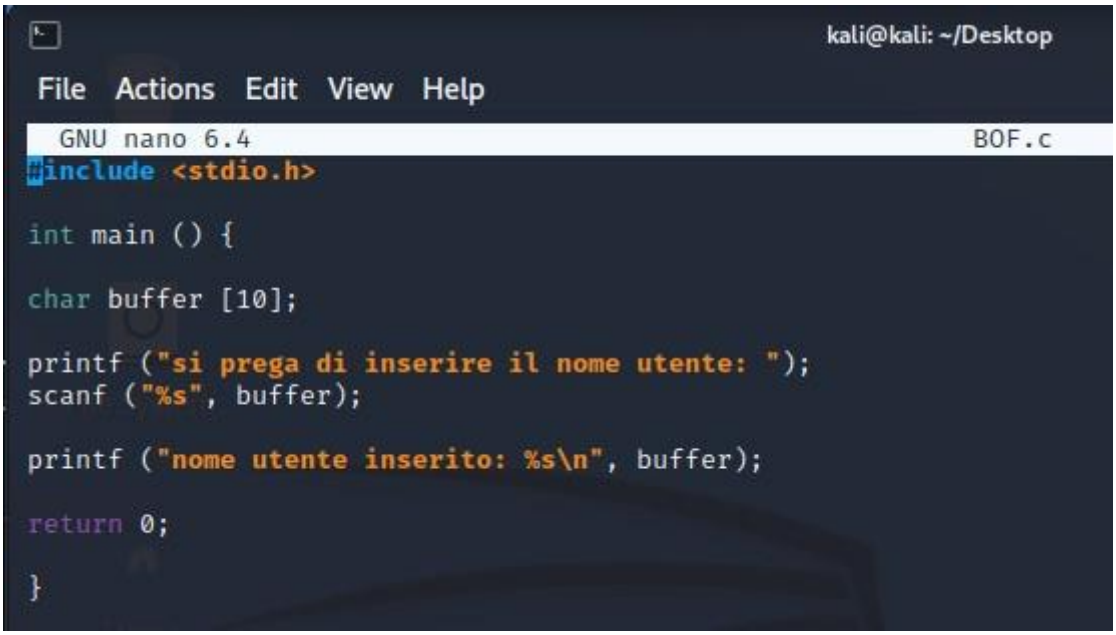
BUFFER OVERFLOW

Nell'esercizio di oggi andremo ad eseguire un attacco di buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.

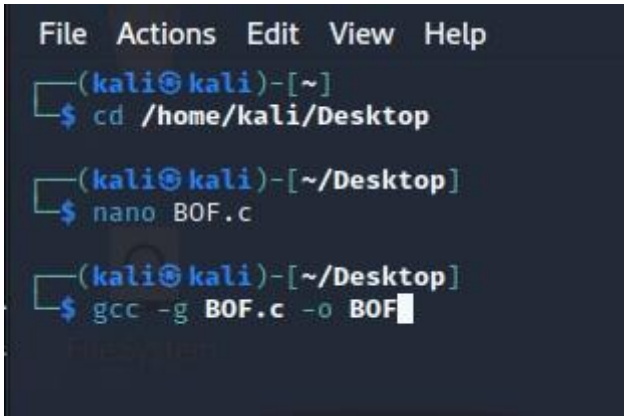
Andremo a scrivere un codice in linguaggio C volutamente vulnerabile ai BOF ed a scatenare una situazione di errore particolare chiamata "segmentation fault", ovvero un errore di memoria che si presenta quando un programma cerca innavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere.

Andremo quindi a spostarci nella directory "Desktop" per scrivere il nostro file.c .

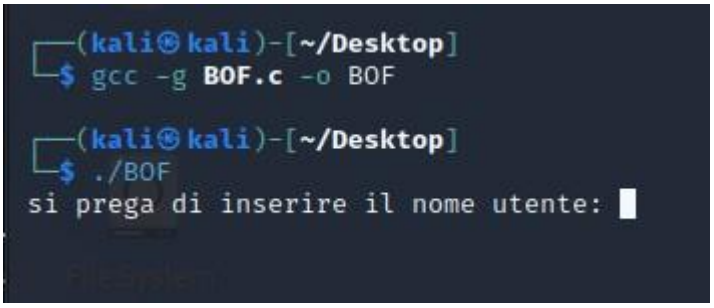




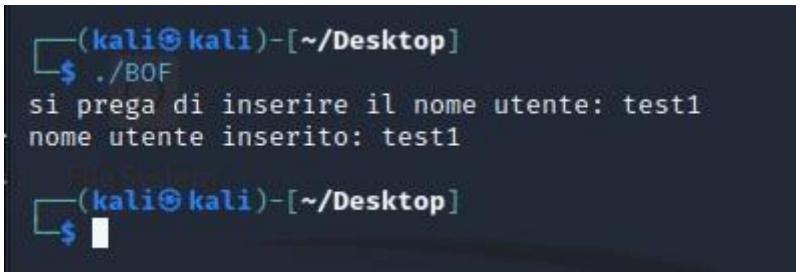
A questo punto andremo a compilare il file tramite il comando gcc -g BOF.c -o BOF.



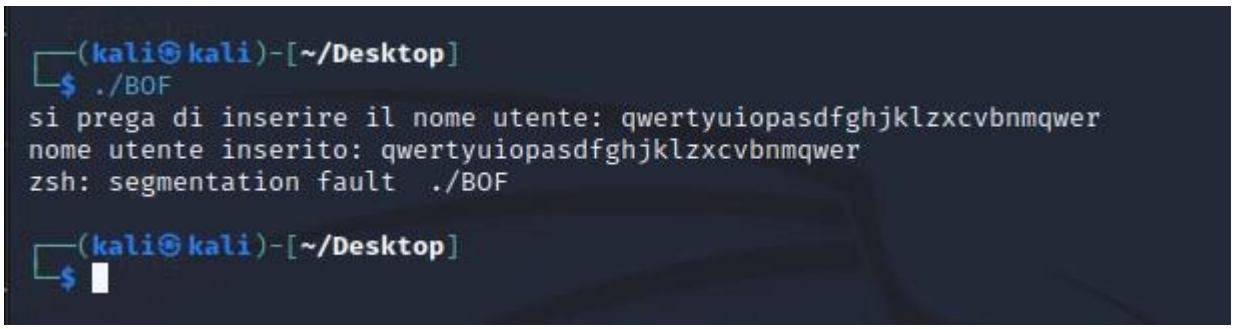
Andremo così ad eseguire il programma con il comando ./BOF



Il programma si avvierà chiedendoci di inserire il nome utente, come prima cosa inseriremo un nome utente di pochi caratteri.

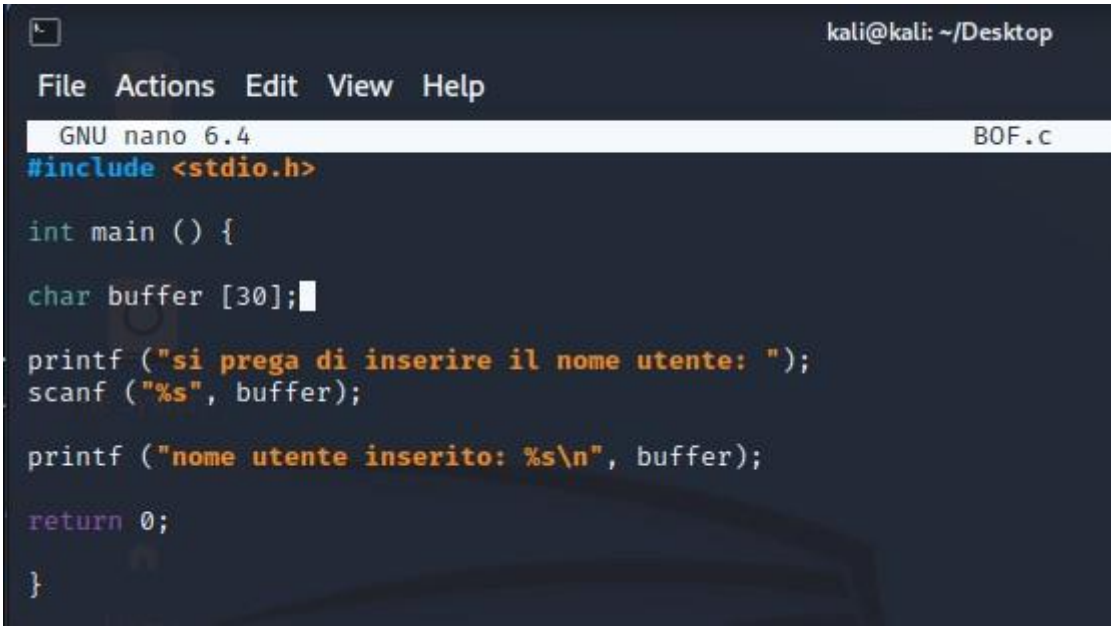


Come vediamo il programma non riporta nessun problema, in quanto il buffer accetta fino a 10 caratteri. Proveremo ora ad inserire 30 caratteri.



Il programma ritornerà un errore “segmentation fault”, ovvero errore di segmentazione. Esso avviene quando un programma tenta di scrivere contenuti su una porzione di memoria alla quale non ha accesso; questo è un esempio di buffer overflow.

Andremo ora a modificare la dimensione del vettore del buffer a 30.



Andremo ora ad inserire un nome utente più lungo verificando che non ci sia un errore di buffer.