ESERCITAZIONE W17D4

EPICODE

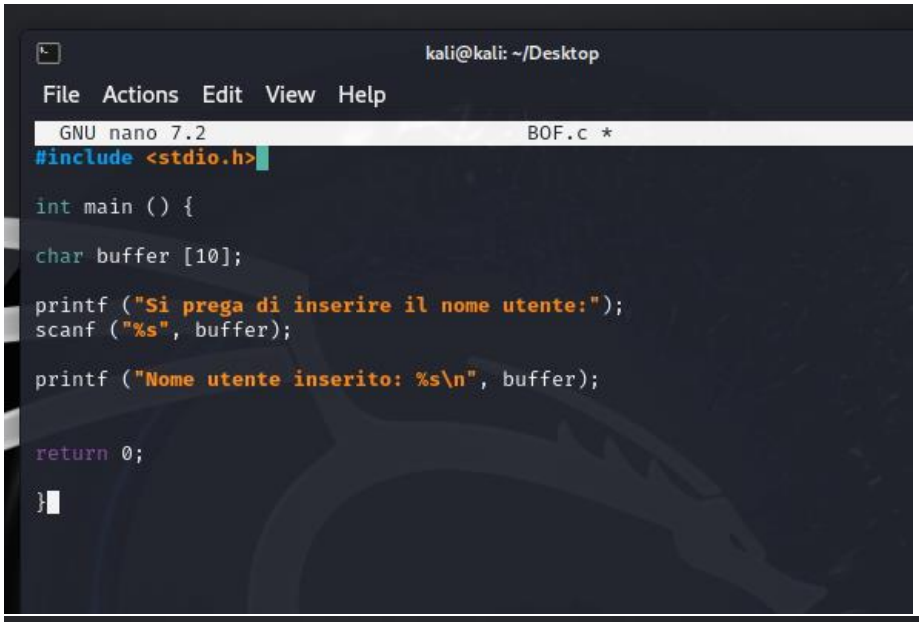
Esercizio
Traccia

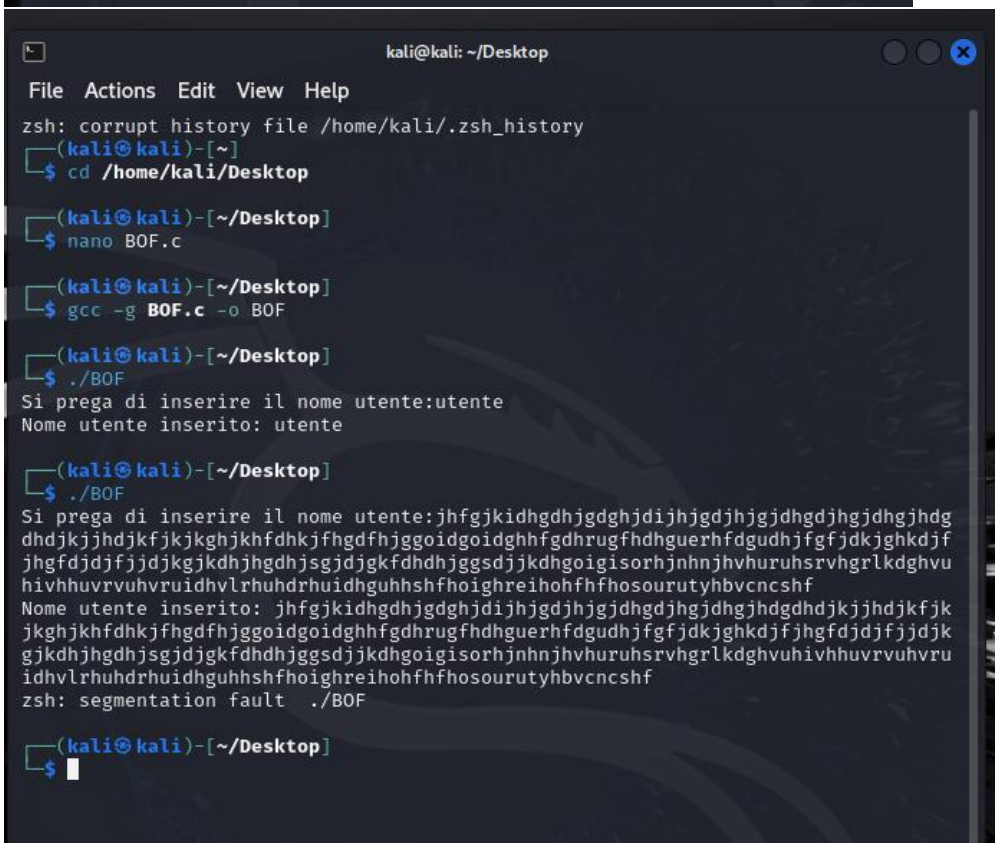
Traccia:

Nella lezione dedicata agli attacchi di sistema, abbiamo parlato dei buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.

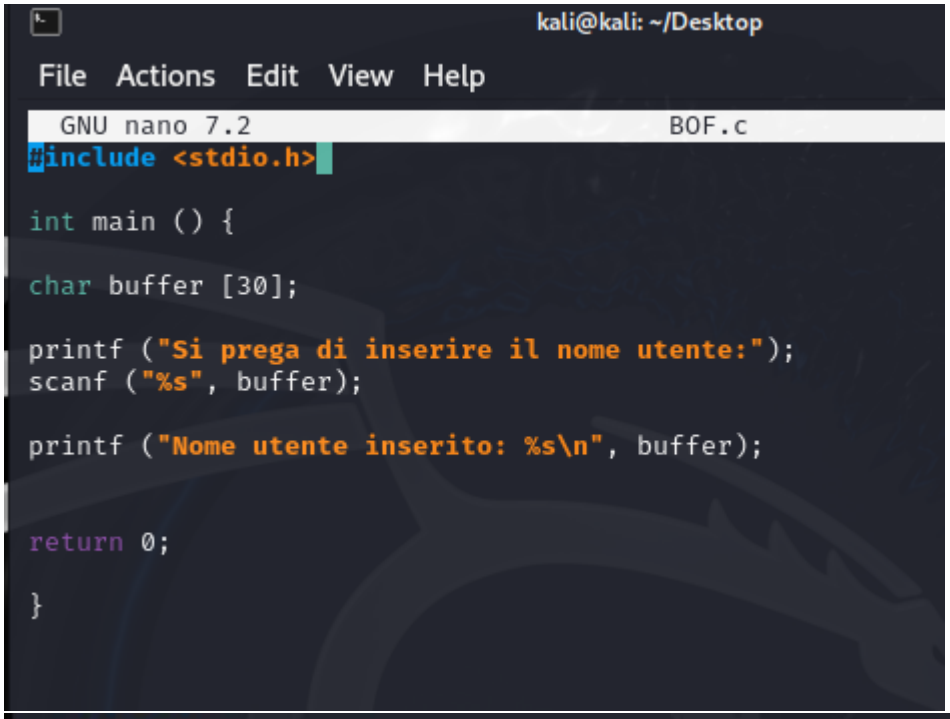
Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (come può essere ad esempio una posizione di memoria dedicata a funzioni del sistema operativo).

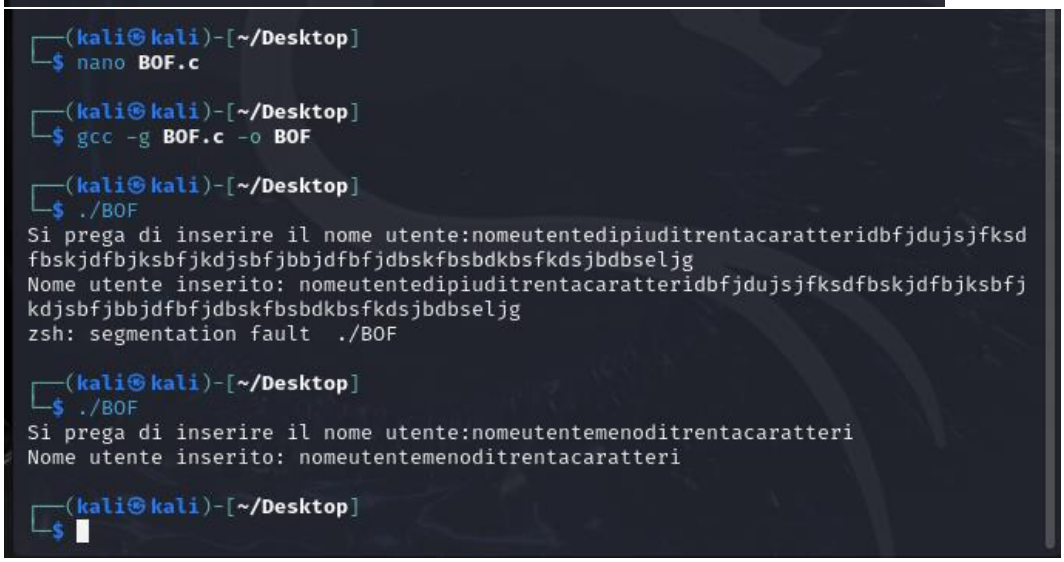
Creazione e test del codice della traccia





Modifica e test del codice aumentando le dimensioni del vettore a 30





Conclusioni

Con la modifica, abbiamo risolto i problemi relativi all'inserimento di un numero di caratteri inferiore a 30. Tuttavia, quando inseriamo un numero di caratteri superiore a 30, riscontriamo un errore di segmentazione. Questo indica che stiamo tentando di scrivere una parte dell'input su una porzione di memoria non accessibile.