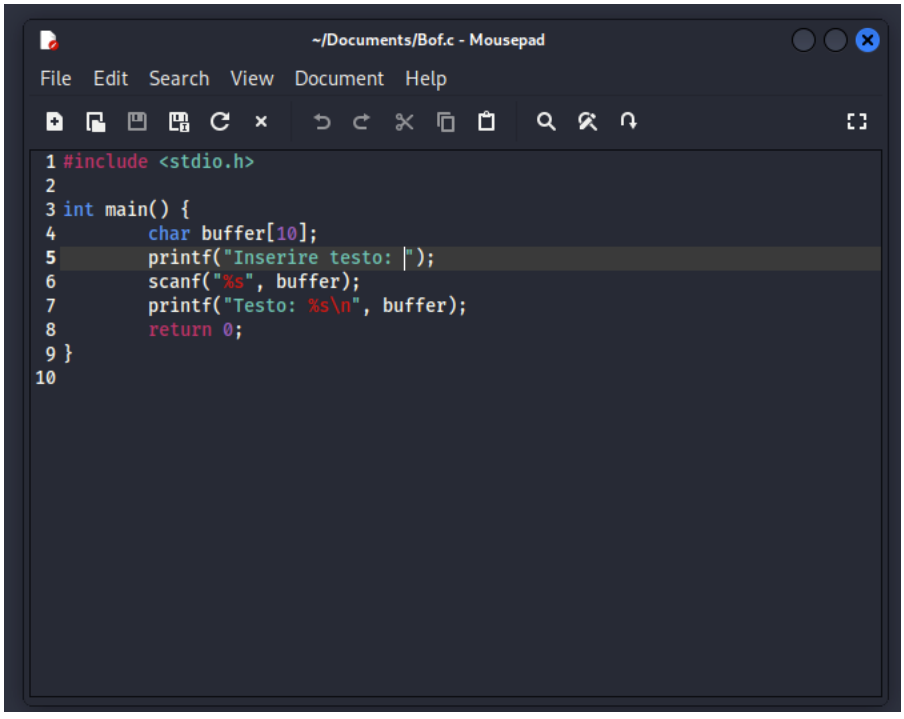
Traccia:

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.

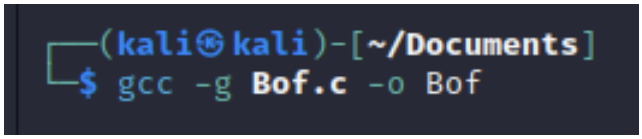
Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove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

Svolgimento:

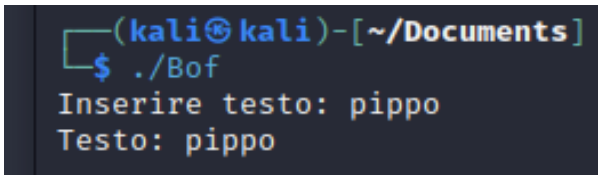
Creazione del file in Linguaggio C per andare a forzare un buffer overflow



Compilazione del file C per avere un eseguibile



Inserimento di un input più piccolo della dimensione del buffer



Inserimento di un input maggiore rispetto alla capacità del buffer con conseguente errore