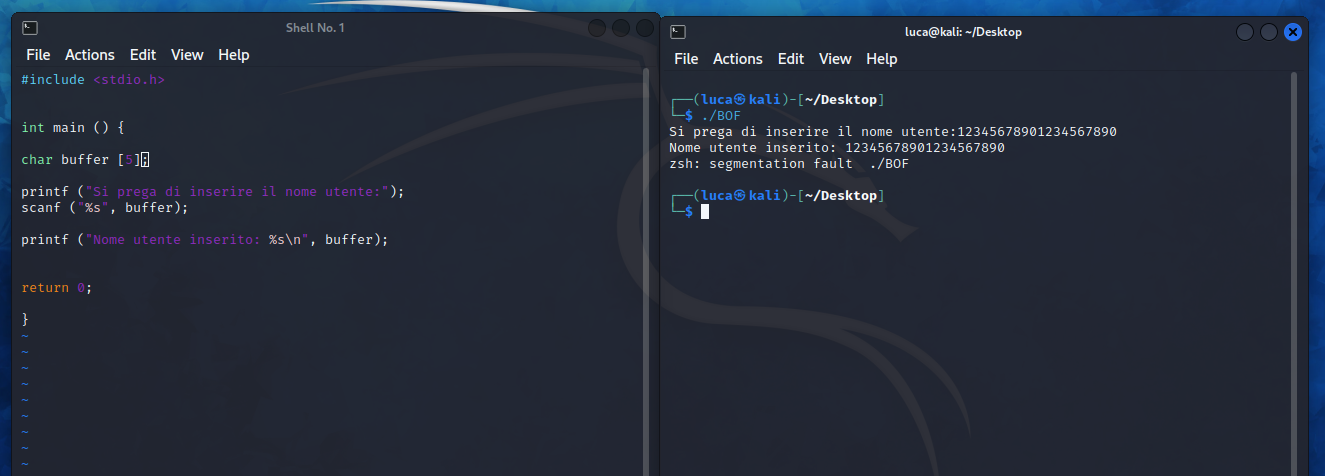
Buffer over flow

Il Buffer overflow è una vulnerabilità che può consentire a un attaccante di sovrascrivere l'area di memoria del buffer di un'applicazione causando il crash del programma stesso. Questo accade quando un programma non gestisce correttamente gli input di dati che può inserire un utente o non implementa sufficienti controlli di sicurezza per verificare che i dati immessi non superino le dimensioni del buffer.



Questo codice è soggetto a buffer overflow perché non è stato impostato alcun limite sulla dimensione del nome utente che può essere inserito. Quindi questo significa che, se l'utente inserisce un nome più lungo di 5 caratteri, il buffer verrà riempito e superato, sovrascrivendo altre aree di memoria rischiando di mandare in crash il programma stesso.

#include <stdio.h>

int main () {

char buffer [6];

printf ("Nome utente:");

fgets (buffer, 6, stdin);

printf ("Nome inserito: %s\n", buffer);

return 0;

}

Questo nuovo codice ha la funzione fgets () che legge una stringa dall'input fino a un carattere di terminazione specificato. Il carattere di terminazione predefinito è \n, quindi la funzione fgets () legge una stringa di 5 caratteri, più il carattere di terminazione.

In questo caso, il carattere di terminazione è specificato come 6. Ciò significa che la funzione fgets () leggerà una stringa di 5 caratteri, più il carattere di terminazione. Se l'utente inserisce più di 5 caratteri, i caratteri in eccesso verranno tagliati.

Ad esempio, se l'utente inserisce il nome "Mario Giordano", la funzione fgets () leggerà la stringa "Mario" e inserirà il carattere \0 alla fine della stringa. Di conseguenza tutto quello in eccesso che verrà scritto in input dall’utente verrà eliminato non rischiando che ci sia un sovraccarico di memoria buffer del programma.