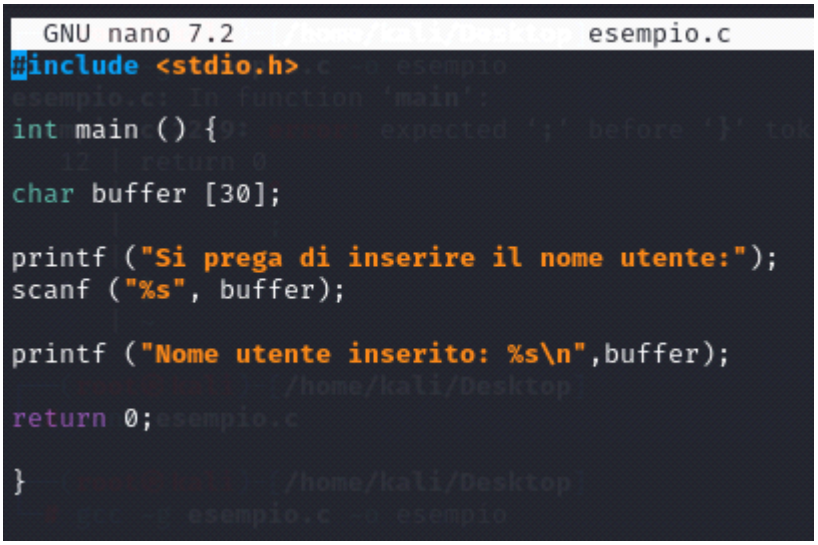
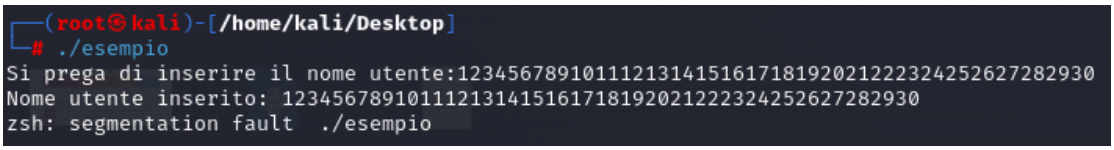
Report Vulnerabilità Buffer Overflow

Per questo attacco abbiamo sfruttato una vulnerabilità nel codice ovvero il limite del buffer, che ci permetteva di occupare spazio di memoria non dedicato a noi.



Come vediamo il limite dell'array è 30, quindi avremo un determinato spazio di memoria massimo per inserire il nome utente, se proviamo a inserire un nome utente con più di 30 caratteri il sistema andrà in buffer overflow, come vediamo dall'errore che viene riportato:



In questo modo, l'attaccante potrebbe sovrascrivere posizioni di memoria adiacenti che contengono informazioni critiche, come puntatori a funzioni o indirizzi di ritorno.

Ciò può portare a due tipi principali di attacchi: accesso non autorizzato ed esecuzione di codice.