**BUFFER OVERFLOW**

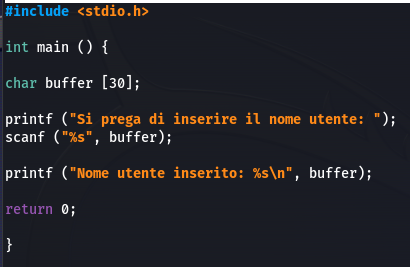
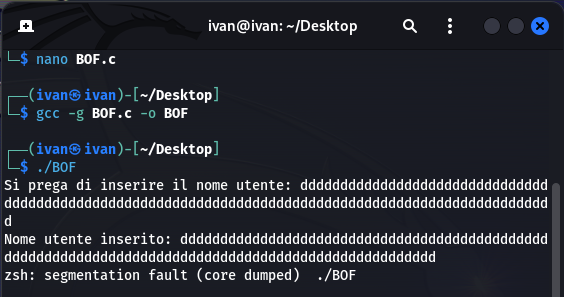
**TRACCIA**

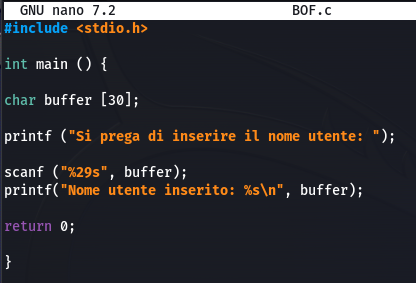
Provate a riprodurre l’errore di segmentazione modificando il programma come di seguito:   
1) Aumentando la dimensione del vettore a 30;   
2) Fare la prova dell’errore modificare il codice in modo che l’errore non si verifichi (es aumentare il vettore a 30 o fare dei controlli).

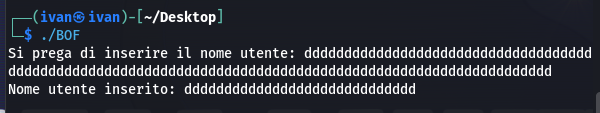
**LEGENDA**

Buffer Overflow: è una vulnerabilità che si verifica quando un programma, durante la scrittura di dati in un buffer di memoria, supera il limite del buffer, sovrascrivendo così dati nella memoria adiacente. Questa situazione può avere gravi conseguenze, in quanto un attaccante può sfruttare questa vulnerabilità per eseguire codice dannoso o manipolare il comportamento del programma in modi indesiderati.

**PROCEDURA**

Abbiamo scritto il seguente codice ed aumentato la dimensione del vettore a 30 caratteri massimi. Superandoli riscontriamo un problema di buffer overflow (come possiamo notare nella seconda immagine).

Siamo andati a risolvere il problema inserendo un limitatore di 30 caratteri “%29s”.

Così il programma ci stamperà sempre e solo i primi 30 caratteri senza l’errore di buffer overflow.