BUFFER OVERFLOW

COS’E’?

Il buffer overflow è una vulnerabilità di sicurezza che si verifica quando un programma, durante l'esecuzione, scrive dati oltre i limiti di un buffer, sovraesponendosi a se stesso o ad altre aree di memoria adiacenti.

Un buffer è una zona di memoria temporanea utilizzata per conservare dati, e può essere utilizzato per vari scopi, come l'archiviazione di stringhe di caratteri.

BUFFER

Un buffer è una zona di memoria temporanea utilizzata per conservare dati, e può essere utilizzato per vari scopi, come l'archiviazione di stringhe di caratteri.

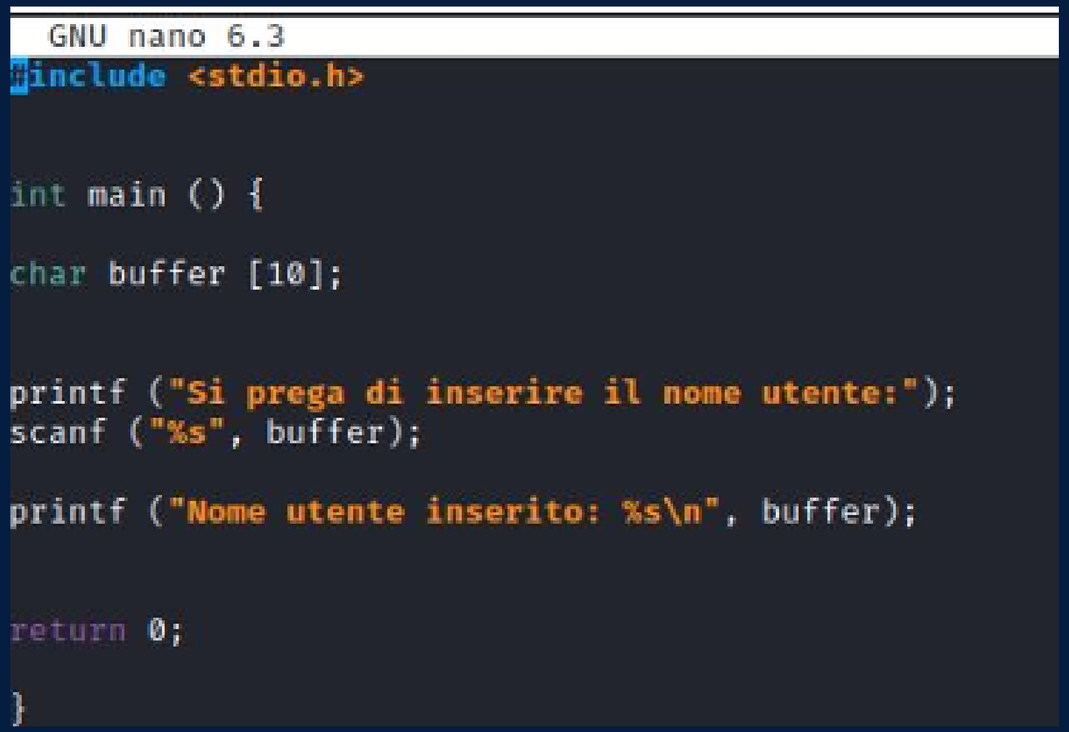
STACK

Gli oggetti o dati sono salvati all’interno delle STACK. Una macro-componente (definita allocazione) della RAM.
All’interno di essa avviene la LIFO, ossia l’aggiunta (PUSH) del dato, e poi rimozione dell’ultimo dato aggiunto (POP)

OBIETTIVO

Creare buffer overflow su un codice in C vulnerabile e creare errore di “segmentation fault”.

codice in C



ESECUZIONE CODICE

Eseguito il codice bisogna inserire il “nome utente” con massimo 10 valori

Ma se si supera avviene il cosiddetto “segmentation fault”.

Modificando buffer [10] in [30] si potranno inserire fino a 30 valori. E come nello screen affianco, superati quei 30 valori, darà sempre “segmentation fault