ESERCITAZIONE WEEK 17 DAY4

EPICODE

Esercizio
Traccia

Provate a riprodurre l'errore di segmentazione modificando il programma come di seguito:

- Aumentando la dimensione del vettore a 30;

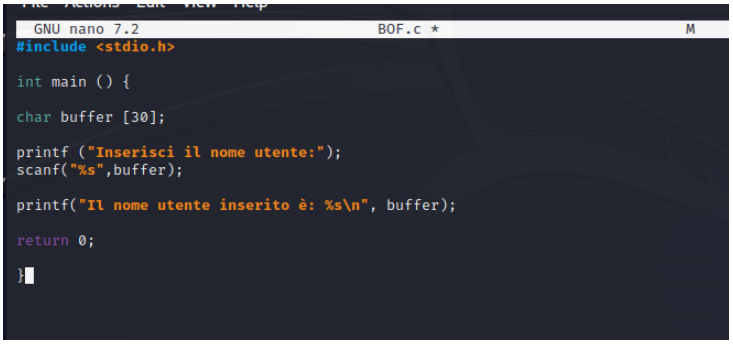
BUFFER OVERFLOW

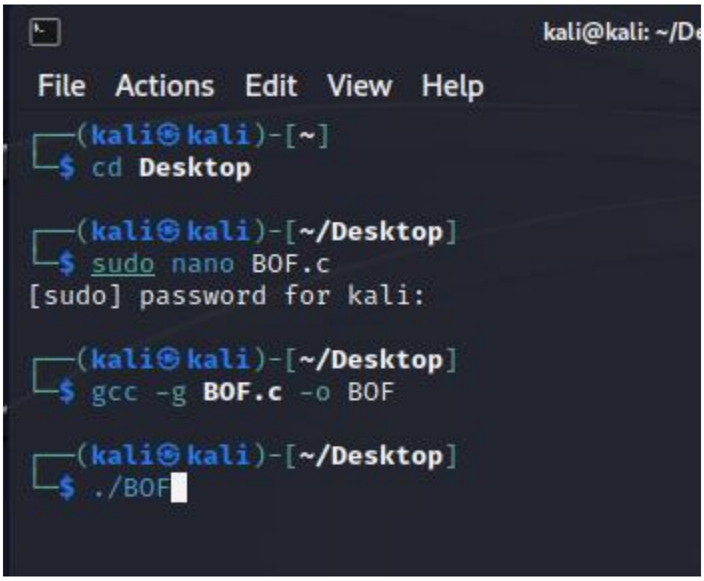
Si tratta di una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.

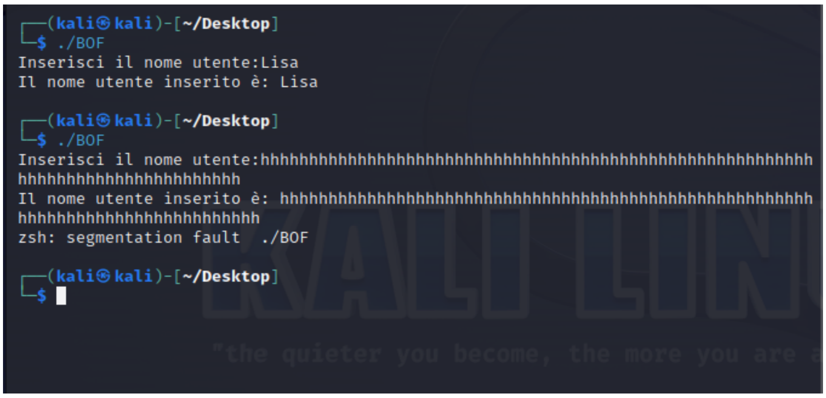
Simuliamo un caso di «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (come può essere ad esempio una posizione di memoria dedicata a funzioni del sistema operativo).

Si crea il seguente file eseguibile con il seguente codice:

Lo si compila e si esegue il caso di segementation fault, modificando la capienza del vettore buffer come da traccia: char buffer [30];




kali@kali: ~/De
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ sudo nano BOF.c
[sudo] password for kali:
(kali㉿kali)-[~/Desktop]
$ gcc -g BOF.c -o BOF
(kali㉿kali)-[~/Desktop]
$ ./BOF


(kali㉿kali)-[~/Desktop]
$ ./BOF
Inserisci il nome utente:Lisa
Il nome utente inserito è: Lisa
(kali㉿kali)-[~/Desktop]
$ ./BOF
Inserisci il nome utente:hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh
hhhhhhhhhhhhhhhhhhhhhhh
Il nome utente inserito è: hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh
hhhhhhhhhhhhhhhhhhhhhhhhh
zsh: segmentation fault ./BOF
(kali㉿kali)-[~/Desktop]
$