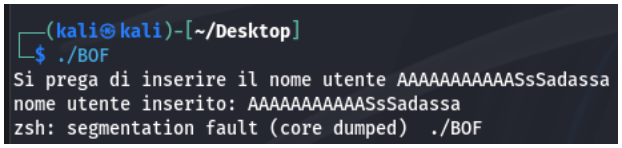
Esercitazione 3_ Modulo 2

Nella lezione dedicata agli attacchi di sistema, abbiamo parlato dei buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente. Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «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).

Scriviamo il codice per riempire il buffer di sistema il C salvandolo in sistema come BOF.c, successivamente ci posizioniamo nella catrtella che contiene il file scritto in c (BOF) e lo andiamo a lanciare con i comandi gcc -g BIF.c -o BOF in modo da poter eseguire il codice in Kali.

Lanciando il file come:
./BOF possiamo andare a riempire una stringa che una volta riepiti tutti i caratteri predefiniti possiamo vedere come il sistema esce dal buffer in quanto ha superato il numero massimo di caratteri consentiti dal linguaggio



Come possiamo vedere nell'immagine in alto nella stringa

- zsh: segmentation fault (core dumped) ./BOF il Sistema ci avvisa che il buffer è pieno ed esce dal processo