S7L4

LA TRACCIA CONSISTE NEL SCRIVERE 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).PER PRIMA COSA CREIAMO IL FILE SPOSTANDOCI SUL DESKTOP,CON IL COMANDO SUDO NANO ANDIAMO A CREARE IL CODICE CHIAMANDO IL FILE BOF.C

Riportiamo il codice con il buffer che accetta fino a 10 caratteri tutto questo in linguaggio C

```c
#include <stdio.h>

int main () {

char buffer [10];

printf("Si prega di inserire il nome utente:");
scanf("%s", buffer);

printf("Nome utente inserito: %s\n", buffer);

return 0;
```

Eseguiamo il file con i comandi indicati nelle immagini una volta eseguito il comando e proviamo A digitare più di 10 caratteri vediamo che succede

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gcc -g BOF.c -o BOF
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:aaaaaa
Nome utente inserito: aaaaaa

┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Nome utente inserito: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
zsh: segmentation fault  ./BOF
```

Come si può vedere dalla slide precedente viene riportato un errore di <<Segmentation fault>> adesso proviamo ad inserire un codice aumentadolo a 30 e modificandolo in modo che non si verifichi più

```c
#include <stdio.h>
#include <string.h>

int main() {
    char buffer[30];

    // Aumentando la dimensione del vettore a 30
    printf("Si prega di inserire il nome utente:");
    fgets(buffer, sizeof(buffer), stdin);

    // Fare la prova dell'errore modificando il codice in modo che l'errore non si verifichi
    // In alternativa, puoi anche controllare la lunghezza dell'input dell'utente prima di copiarlo nel buffer
    // Esempio di controllo:
    // if (strlen(buffer) >= 30) {
    //     printf("Errore: Lunghezza dell'input troppo lunga.\n");
    //     return 1;
    // }

    printf("Nome utente inserito: %s\n", buffer);

    return 0;
```

Ed ecco il codice eseguito senza la ripetizione dell'errore

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:fghjklqwertyuiopqwerasdfgbvcxz
Nome utente inserito: fghjklqwertyuiopqwerasdfgbvcxz
```