

S7-L4

Il programma in C su cui ci baseremo è stato denominato BOF.c e contiene il seguente codice (char buffer 10):

```
(diidro@kali)-[~/Desktop/.Script]
$ cat BOF.c
#include <stdio.h>

int main () {
    char buffer [10];

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

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

    return 0;
}

(diidro@kali)-[~/Desktop/.Script]
$
```

Utilizziamo il compilatore gcc specificando il file sorgente da compilare (BOF.c) ed il nome del file eseguibile risultante (BOF).

Fatto questo lanciamo BOF ed inseriamo dei caratteri (nel nostro caso ne abbiamo inseriti 17, il programma ha preso correttamente i dati inseriti).

```
(diidro@kali)-[~/Desktop/.Script]
$ gcc -g BOF.c -o BOF

(diidro@kali)-[~/Desktop/.Script]
$ ./BOF
Si prega di inerire il nome utente:99999999999999999
Nome utente inserito: 99999999999999999

(diidro@kali)-[~/Desktop/.Script]
$
```

Facendo varie prove abbiamo notato come, una volta inseriti 18 caratteri, il programma ci esponeva un errore di "segmentation fault" (errore che compare quando il programma tenta di accedere ad una memoria che non gli è permesso usare).

```
(diidro@kali)-[~/Desktop/.Script]
$ ./BOF
Si prega di inerire il nome utente:090909090909090909
Nome utente inserito: 090909090909090909
zsh: segmentation fault ./BOF

(diidro@kali)-[~/Desktop/.Script]
$
```

Modifichiamo il programma originale impostando un char buffer pari a 30 e vediamo cosa cambia.
Prima di lanciarlo bisogna riutilizzare il compilatore gcc come fatto in precedenza.

```
(diidro@kali)-[~/Desktop/.Script]
$ cat BOF.c
#include <stdio.h>

int main () {

char buffer [30];

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

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

return 0;
}

(diidro@kali)-[~/Desktop/.Script]
$ gcc -g BOF.c -o BOF

(diidro@kali)-[~/Desktop/.Script]
$
```

In questo caso abbiamo appreso come inserendo 39 caratteri, questi vengono presi correttamente dal programma; tuttavia, inseriti 41 caratteri, ricompare il segmentation fault.

```
(diidro@kali)-[~/Desktop/.Script]
$ ./BOF
Si prega di inerire il nome utente:0000000000999999999988888888887777777777
Nome utente inserito: 0000000000999999999988888888887777777777
knock, knock, Neo.

(diidro@kali)-[~/Desktop/.Script]
$
```

```
(diidro@kali)-[~/Desktop/.Script]
$ ./BOF
Si prega di inerire il nome utente:0000000000999999999988888888887777777777
Nome utente inserito: 0000000000999999999988888888887777777777
zsh: segmentation fault ./BOF
```