

4. Consolidamento conoscenze

- Buffer overflow

Con nano andiamo a scrivere un piccolo codice in c dove possiamo inserire una stringa con nome utente.

```
GNU nano 7.2 BOF.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;
}
```

```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania]
$ nano BOF.c
(kali@kali)-[~/Scrivania]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente:mariano
Nome utente inserito: mariano
(kali@kali)-[~/Scrivania]
$
```

Se inseriamo una stringa inferiore ai 10 caratteri il programma ce lo riporta nel secondo print.

Se invece inseriamo una stringa superiore a 10 caratteri, ci restituisce un errore di segmentazione.

```
└─$ ./Buffer
Si prega di inserire il nome utente:jfdnkndcosnoscncndicnnc
Nome utente inserito: jfdnkndcosnoscncndicnnc
zsh: segmentation fault ./Buffer
```

Possiamo andare a modificare il file del programma andando ad estendere i caratteri che possiamo inserire per evitare tale errore

```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2 BOF.c *
#include <stdio.h>
...
int main () {
    char buffer [30];

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

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

    return 0;
}
```