

## BUFFER OVERFLOW – SEGMENTATION FAULT IN C

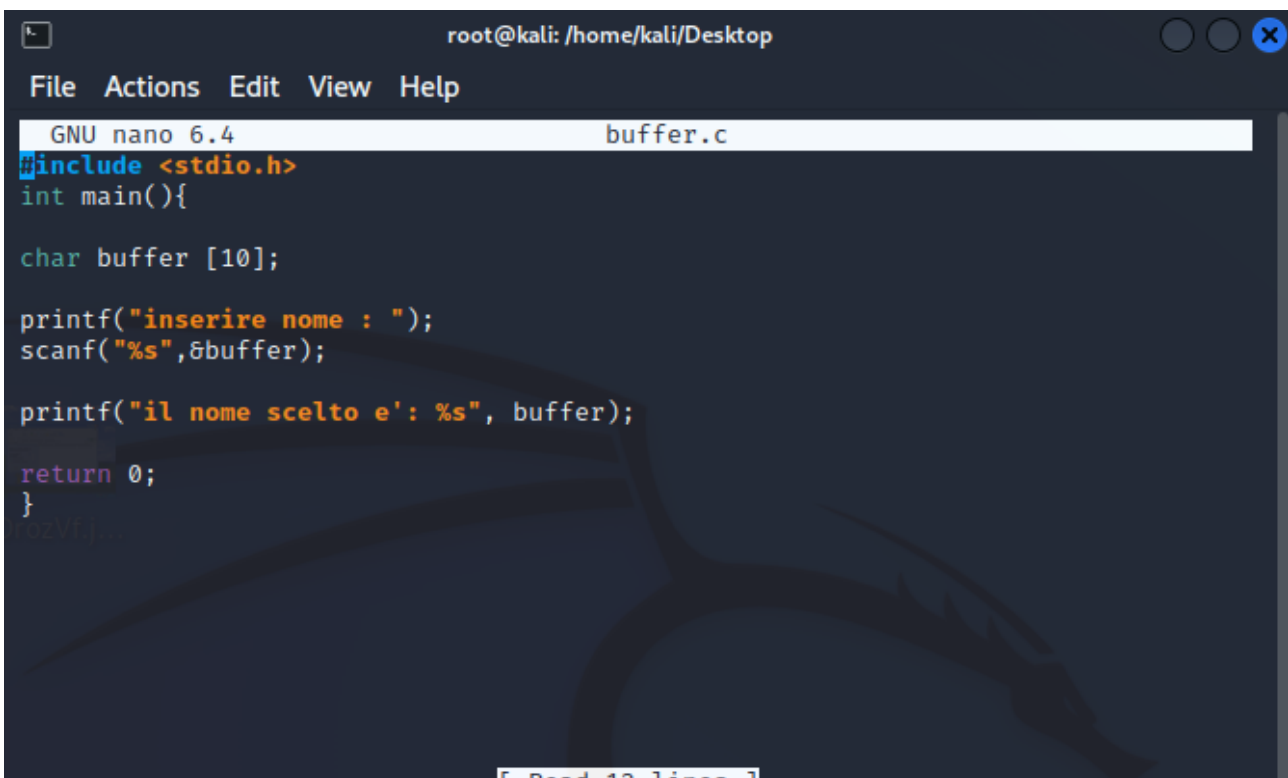
## TRACCIA:

Per la traccia di oggi ci veniva richiesto di scrivere un programma in C che acquisisca il nome utente, tramite input da tastiera. Lo scopo è quello di studiare il problema di segmentation fault che si palesa quando si inseriscono in input più caratteri rispetto a quelli predefiniti dall'array.

## RISOLUZIONE:

La risoluzione di questo problema è stata guidata dalla traccia stessa, così come la scrittura del codice.

In primo luogo abbiamo riprodotto l'esatto codice presente sulla slide, e come test abbiamo inserito una stringa che fosse maggiore della grandezza del nostro array (in questo caso 10).



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
GNU nano 6.4 buffer.c
#include <stdio.h>
int main(){
    char buffer [10];
    printf("inserire nome : ");
    scanf("%s",&buffer);
    printf("il nome scelto e': %s", buffer);
    return 0;
}
```

Potendo constatare difatti che il programma riporta un errore di segmentation fault.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop

(kali㉿kali)-[~/Desktop]
$ ./BOF
inserire nome : piudidieciaratteri
zsh: segmentation fault ./BOF

(kali㉿kali)-[~/Desktop]
$
```

Successivamente per la risoluzione, attenendoci alla traccia, abbiamo cambiato la grandezza dell'array da 10 a 30, risolvendo così di fatti l'errore di segmentation fault.

```
File Actions Edit View Help
GNU nano 6.4 buffer.c *
#include <stdio.h>
int main(){

char buffer [30];

printf("inserire nome : ");
scanf("%s",&buffer);

printf("il nome scelto e': %s", buffer);

return 0;
}
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop

(kali㉿kali)-[~/Desktop]
$ ./BOF
inserire nome : piudidieciaratteri
zsh: segmentation fault ./BOF

(kali㉿kali)-[~/Desktop]
$ ./BOF
inserire nome : piudidieciaratteri
il nome scelto e': piudidieciaratteri

(kali㉿kali)-[~/Desktop]
$
```