Creazione di un programma in linguaggio C per una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente, il «**Buffer OverFlow**» (BOF)

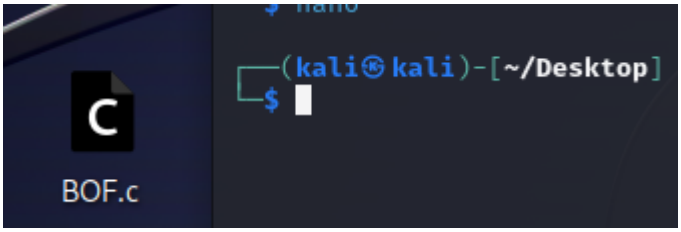
Il BOF è un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (es. una posizione di memoria dedicata a funzioni del sistema operativo)

Esercizio

Scritto il codice in linguaggio C usando il comando «**nano**»

```
  GNU nano 7.2
#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;

}
```

Salvato con il nome «**BOF.c**»



Compilazione del programma con il comando «**gcc -g BOF.c –o BOF**»

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

Eseguito con «**./BOF**» utilizzando il nome Costantino di 10 caratteri

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

Inserendo un nome utente di 30 caratteri viene visualizzato il messaggio «**segmentation fault**» (errore di segmentazione)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:abcdefghijklmnopqrstuvwxyz1234
Nome utente inserito: abcdefghijklmnopqrstuvwxyz1234
zsh: segmentation fault  ./BOF
```

Extra

Modificato il programma aumentando il valore dei caratteri da 10 a 30

```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;

}
```

Dopo averlo compliato ed eseguito, è stato inserito un nume utente di 40 caratteri.

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

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

┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente: hippopotomonstrosesquipedaliofobia123456
Nome utente inserito: hippopotomonstrosesquipedaliofobia123456
zsh: bus error  ./BOF
```

Viene visualizzato il messaggio «**bus error**».

Possibile Soluzione

```c
#include <stdio.h>


int main () {

char buffer [10];

printf ("Si prega di inserire il nome utente [Max 10 caratteri]: ");
scanf ("%s", buffer);

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

return 0;

}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente [Max 10 caratteri]: 1234567890
Nome utente inserito: 1234567890
```