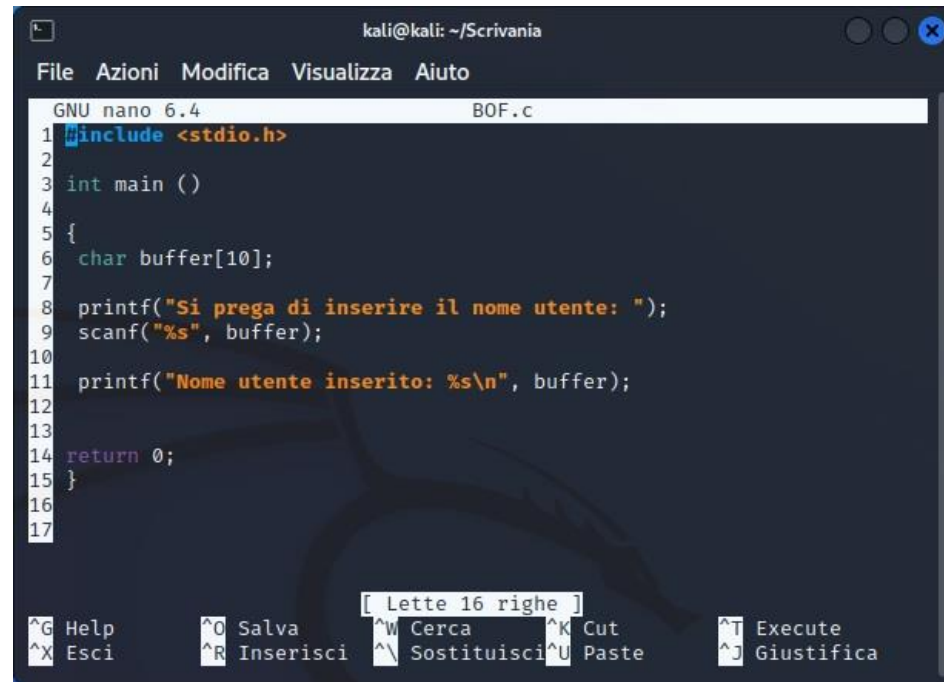


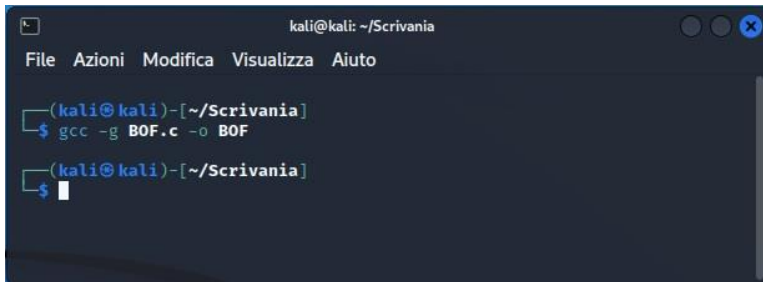
Buffer overflow

Vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente

Nella seguente dimostrazione si analizza la particolare situazione di errore chiamata: *segmentation fault*



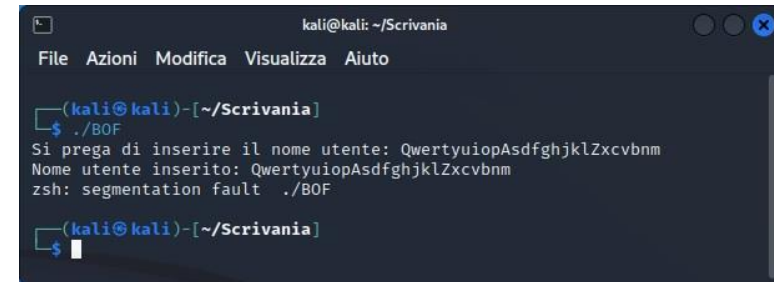
```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
GNU nano 6.4 BOF.c
1 #include <stdio.h>
2
3 int main ()
4 {
5
6     char buffer[10];
7
8     printf("Si prega di inserire il nome utente: ");
9     scanf("%s", buffer);
10
11     printf("Nome utente inserito: %s\n", buffer);
12
13
14     return 0;
15 }
16
17
[Lette 16 righe]
^G Help      ^O Salva     ^W Cerca     ^K Cut        ^T Execute
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste      ^J Giustifica
```



```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Scrivania]
$
```



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

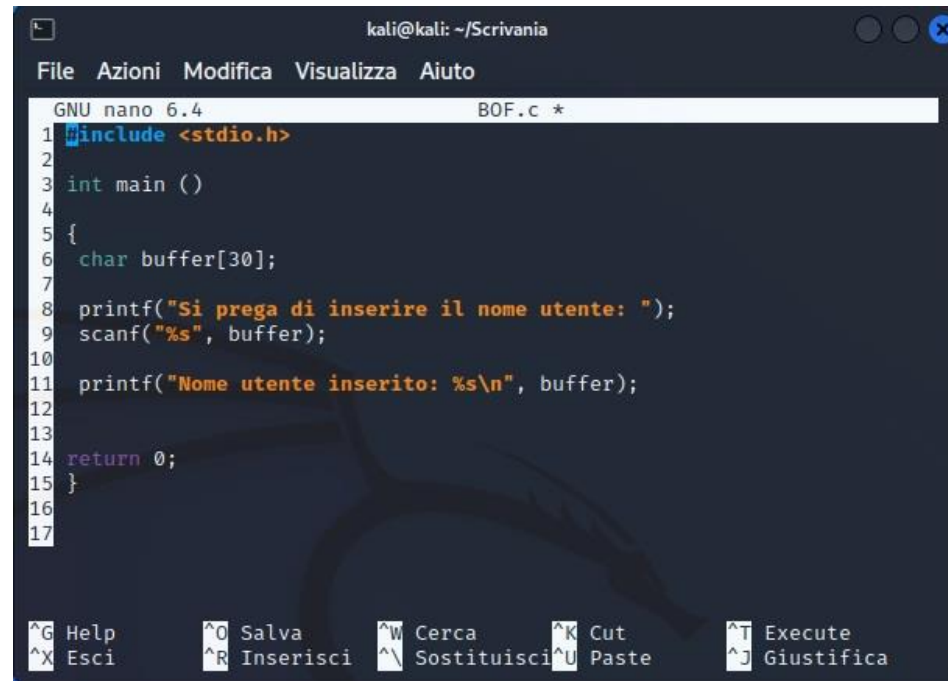


```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: QwertyuiopAsdfghjklZxcvbnm
Nome utente inserito: QwertyuiopAsdfghjklZxcvbnm
zsh: segmentation fault ./BOF
(kali@kali)-[~/Scrivania]
$
```

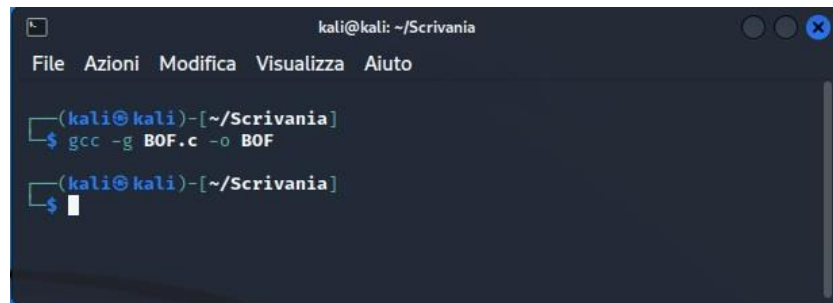
Buffer overflow

Dalla VM Kali, digitando nel terminale il comando: `nano BOF.c`, si apre l'editor di testo nano per scrivere, all'interno del file BOF.c, il codice, come riportato nell'immagine in alto, volutamente vulnerabile ai Buffer OverFlow, e salvandolo, con la combinazione dei tasti: CTRL + X e, successivamente premendo il tasto y.

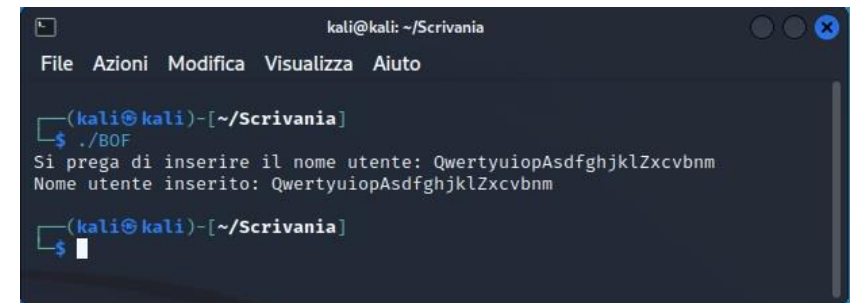
Il file creato si compila con il comando: `gcc -g BOF.c -o BOF`, come mostrato nell'immagine in basso a sinistra e, si esegue, come mostrato nell'immagine in basso al centro, con il comando `./BOF`, senza riportare nessun problema, visto che, il buffer, accetta fino a dieci caratteri, a differenza di come si vede nell'immagine in basso a destra, dove è stato inserito un numero maggiore di caratteri consentiti.



```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
GNU nano 6.4 BOF.c *
1 #include <stdio.h>
2
3 int main ()
4 {
5     char buffer[30];
6     printf("Si prega di inserire il nome utente: ");
7     scanf("%s", buffer);
8     printf("Nome utente inserito: %s\n", buffer);
9
10
11
12
13
14 return 0;
15 }
16
17
^G Help      ^O Salva     ^W Cerca    ^K Cut       ^T Execute
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste     ^J Giustifica
```



```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Scrivania]
$
```



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

Buffer overflow

Dalla VM Kali, digitando nel terminale il comando: `nano BOF.c`, si apre l'editor di testo nano per modificare il file BOF.c con il codice, come riportato nell'immagine in alto, non più vulnerabile ai Buffer OverFlow visto nella precedente slide, e salvandolo, con la combinazione dei tasti: CTRL + X e, successivamente premendo il tasto y.

Il file creato si compila con il comando: `gcc -g BOF.c -o BOF`, come mostrato nell'immagine in basso a sinistra e, si esegue, come mostrato nell'immagine in basso a destra, con il comando `./BOF`, senza riportare nessun problema, visto che, il buffer, in questa modifica, accetta fino a trenta caratteri.