

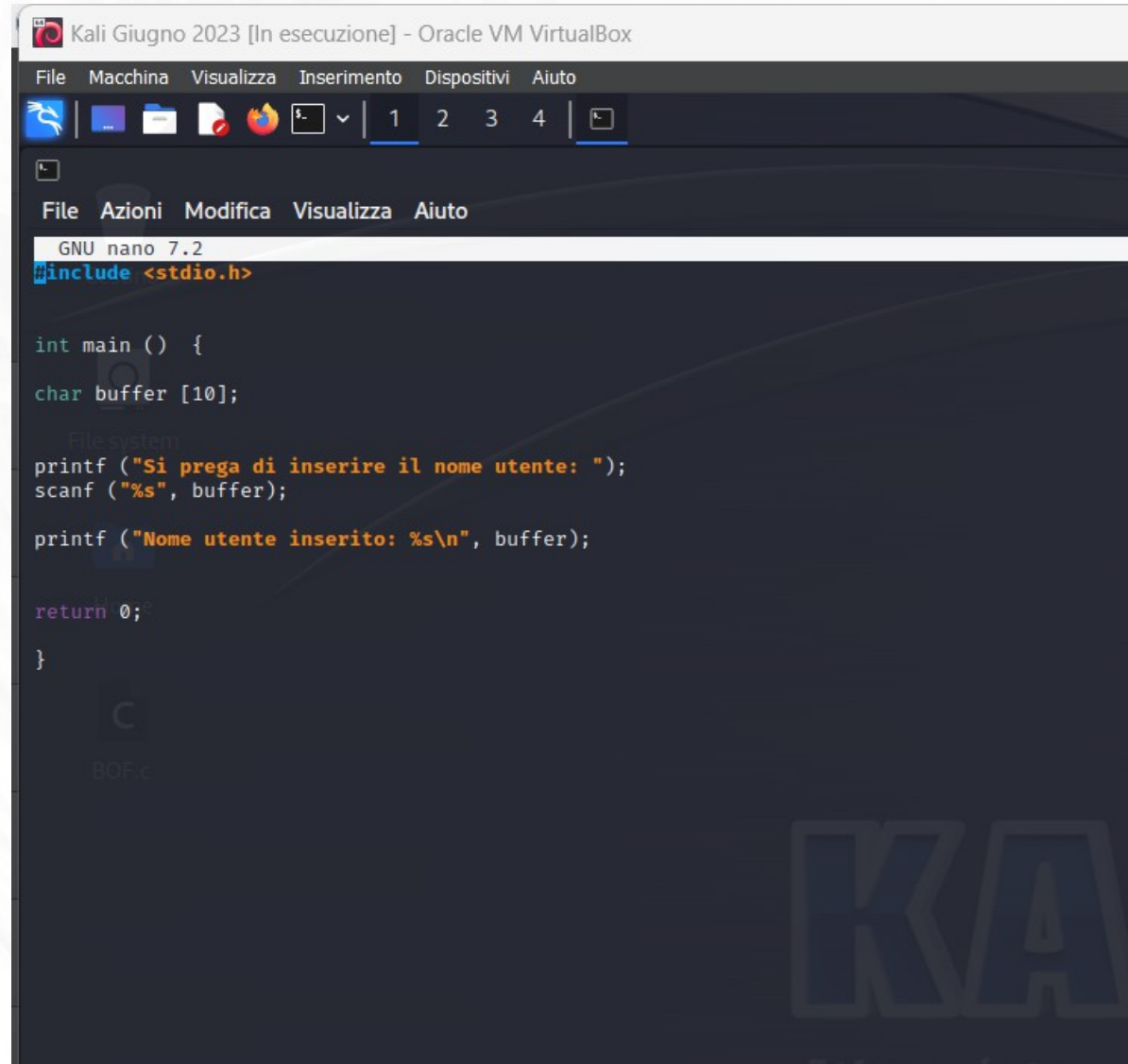
ESERCIZIO M5 D2

BUFFER OVERFLOW

~/Scrivania/BOF.c

1 - Creazione del file BOF.c situato nel desktop

```
(marco@kali)-[~]  
$ cd Scrivania  
  
(marco@kali)-[~/Scrivania]  
$ nano BOF.c
```



Kali Giugno 2023 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

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;  
}
```

2 – Compilazione e avvio programma con test di inserimento con 5 lettere (prova)

```
(marco@kali)-[~/Scrivania]
$ nano BOF.c

(marco@kali)-[~/Scrivania]
$ gcc -g BOF.c -o BOF

(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: prova
Nome utente inserito: prova

(marco@kali)-[~/Scrivania]
$
```

3 – Test di inserimento con 15 e 30 lettere per testare il bufferoverflow. Con 30 si evince un errore di “segmentation fault”

```
(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: provaprova
Nome utente inserito: provaprova

(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: provaprova
Nome utente inserito: provaprova
zsh: segmentation fault ./BOF

(marco@kali)-[~/Scrivania]
$
```

4 – Modifica del programma aumentando la dimensione del vettore “buffer” a 30 e conseguente prova di efficacia, una volta compilato ed avviato il programma, con inserimento di una parola di 30 lettere

```
GNU nano 7.2
#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;
}
```

```
(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: provaprovaprovaprovaprovaprova
Nome utente inserito: provaprovaprovaprovaprovaprova
zsh: segmentation fault ./BOF

(marco@kali)-[~/Scrivania]
$ nano BOF.c

(marco@kali)-[~/Scrivania]
$ gcc -g BOF.c -o BOF

(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: provaprovaprovaprovaprovaprova
Nome utente inserito: provaprovaprovaprovaprovaprova

(marco@kali)-[~/Scrivania]
$
```

5 – Test di inserimento con 60 lettere per testare di nuovo il bufferoverflow ed ovviamente si evince di nuovo un errore di “segmentation fault”

```
(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: provaprovaprovaprovaprovaprova
Nome utente inserito: provaprovaprovaprovaprovaprova

(marco@kali)-[~/Scrivania]
$ ./BOF
Si prega di inserire il nome utente: provaprovaprovaprovaprovaprova
Nome utente inserito: provaprovaprovaprovaprovaprova
zsh: segmentation fault ./BOF

(marco@kali)-[~/Scrivania]
$
```