

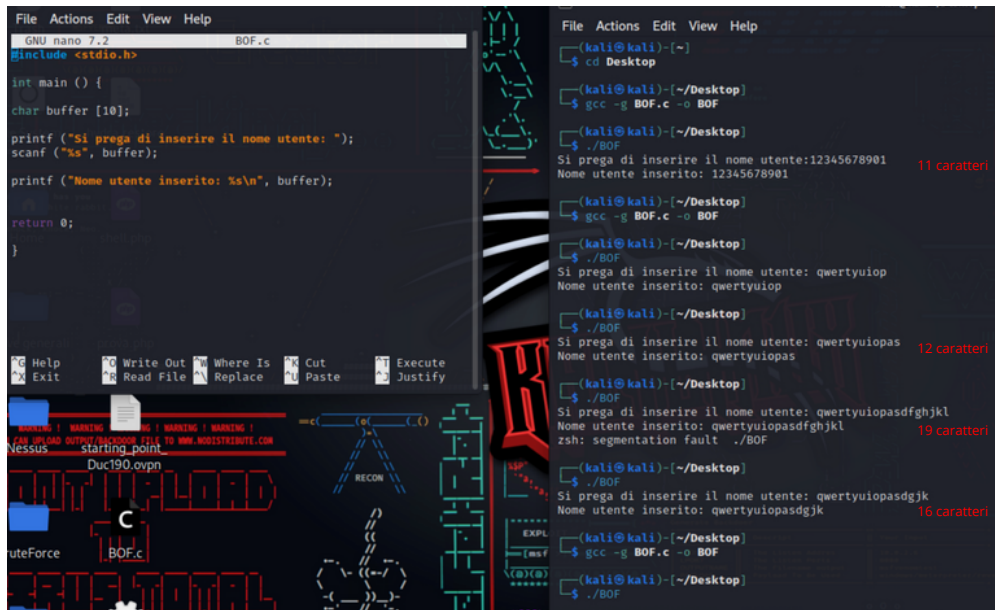
Esercizio S7L4

Traccia

Provate a riprodurre l'errore di segmentazione modificando il programma come di seguito:

- Aumentando la dimensione del vettore a 30;
- Fare la prova dell'errore
- modificare il codice in modo che l'errore non si verifichi (es aumentare il vettore a 30 o fare dei controlli)
- Verificare, modificando il codice, dove va a scrivere i caratteri in overflow

Dimensione del vettore = 10;



```
File Actions Edit View Help
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;
}

File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente:12345678901 11 caratteri
Nome utente inserito: 12345678901
(kali@kali)-[~/Desktop]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: qwertyuiop
Nome utente inserito: qwertyuiop
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: qwertyuiopas 12 caratteri
Nome utente inserito: qwertyuiopas
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: qwertyuiopasdfghjkl 19 caratteri
Nome utente inserito: qwertyuiopasdfghjkl
zsh: segmentation fault ./BOF
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: qwertyuiopasdgjk 16 caratteri
Nome utente inserito: qwertyuiopasdgjk
(kali@kali)-[~/Desktop]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Desktop]
$ ./BOF
```

Dimensione del vettore = 30;



```
File Actions Edit View Help
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;
}

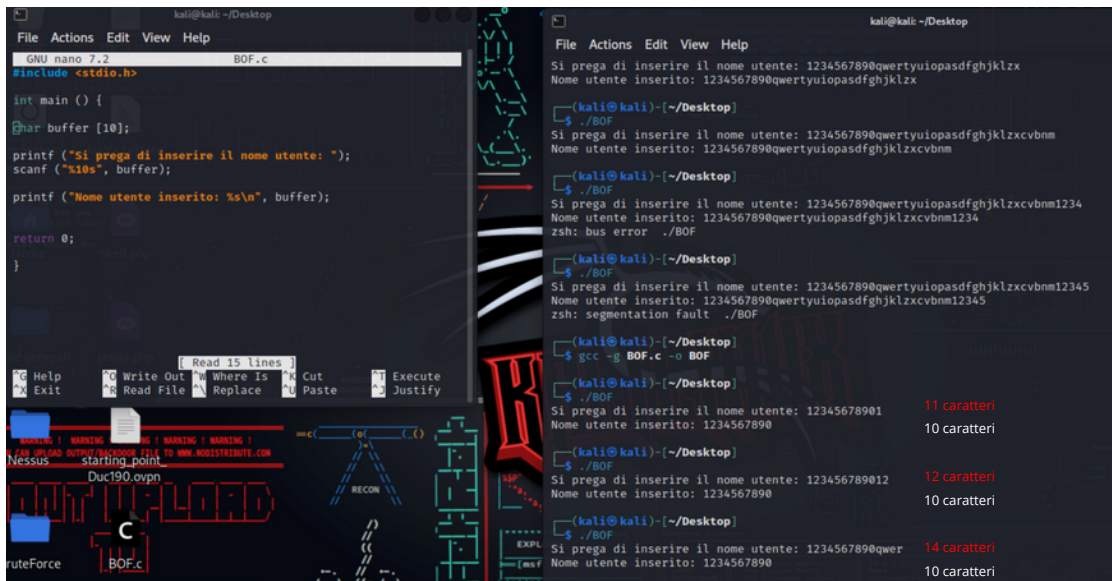
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ gcc -g BOF.c -o BOF
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiop 20 caratteri
Nome utente inserito: 1234567890qwertyuiop
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjkl 29 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjkl
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklz 30 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjklz
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzx 31 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjklzx
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcvbnm 36 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjklzxcvbnm
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcvbnm1234 40 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjklzxcvbnm1234
zsh: bus error ./BOF
(kali@kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcvbnm12345 41 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjklzxcvbnm12345
zsh: segmentation fault ./BOF
```

In entrambi i casi vi è il buffer overflow dato che il numero di caratteri supera il numero massimo scritto nel programma.

Il Buffer Overflow è un tipo di exploit che va a sfruttare una vulnerabilità già presente nel codice. E' una vulnerabilità che avviene quando i dati che vengono inseriti sono oltre il limite della memoria buffer e questo per mette a chi ne fa uso di prendere controllo del dispositivo attaccato. La colpa è del programmatore che non ha risanato la vulnerabilità o della persona che non ha fatto l'aggiornamento che permetteva di risolvere il problema.

Come soluzione si può aggiungere il limitatore di caratteri ammessi nell'argomento cioè all'interno della funzione scanf.

Dimensione vettore = 10



```
GNU nano 7.2 BOF.c
#include <stdio.h>

int main () {
    char buffer [10];

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

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

    return 0;
}
```

```
kali@kali: ~/Desktop
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzx
Nome utente inserito: 1234567890qwertyuiopasdfghjklzx

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcvbnm
Nome utente inserito: 1234567890qwertyuiopasdfghjklzxcvbnm

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcvbnm1234
Nome utente inserito: 1234567890qwertyuiopasdfghjklzxcvbnm1234
zsh: segmentation fault ./BOF

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcvbnm12345
Nome utente inserito: 1234567890qwertyuiopasdfghjklzxcvbnm12345
zsh: segmentation fault ./BOF

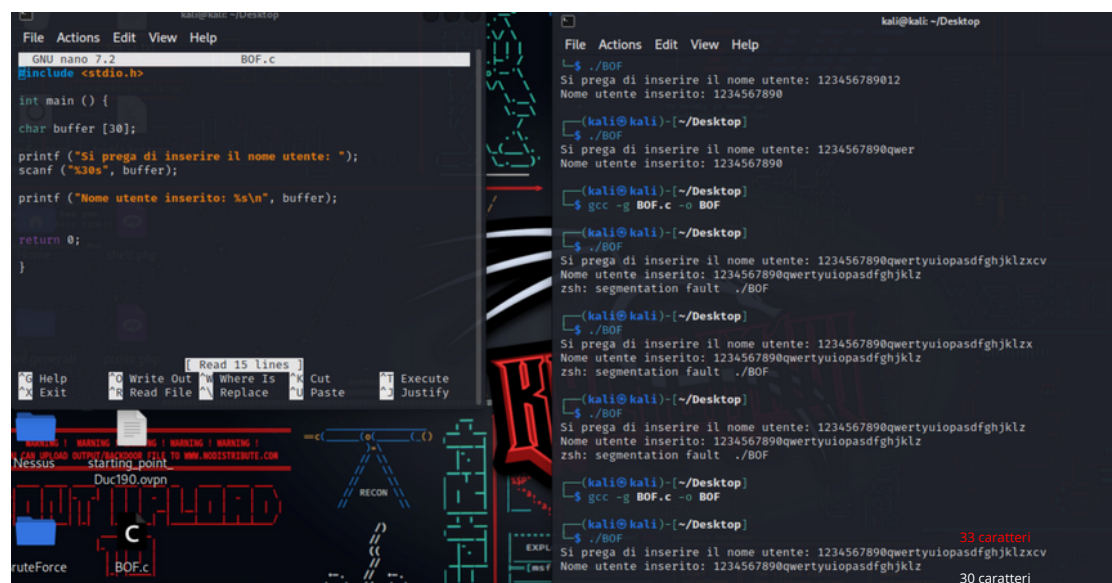
(kali@kali)~[/Desktop]
$ gcc -g BOF.c -o BOF

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 12345678901 11 caratteri
Nome utente inserito: 1234567890 10 caratteri

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 123456789012 12 caratteri
Nome utente inserito: 1234567890 10 caratteri

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwer 14 caratteri
Nome utente inserito: 1234567890 10 caratteri
```

Dimensione vettore = 30



```
GNU nano 7.2 BOF.c
#include <stdio.h>

int main () {
    char buffer [30];

    printf ("Si prega di inserire il nome utente: ");
    scanf ("%30s", buffer);

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

    return 0;
}
```

```
kali@kali: ~/Desktop
$ ./BOF
Si prega di inserire il nome utente: 123456789012
Nome utente inserito: 1234567890

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwer
Nome utente inserito: 1234567890

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

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcv
Nome utente inserito: 1234567890qwertyuiopasdfghjklz
zsh: segmentation fault ./BOF

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzx
Nome utente inserito: 1234567890qwertyuiopasdfghjklz
zsh: segmentation fault ./BOF

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklz
Nome utente inserito: 1234567890qwertyuiopasdfghjklz
zsh: segmentation fault ./BOF

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

(kali@kali)~[/Desktop]
$ ./BOF
Si prega di inserire il nome utente: 1234567890qwertyuiopasdfghjklzxcv 33 caratteri
Nome utente inserito: 1234567890qwertyuiopasdfghjklz 30 caratteri
```