Introduzione

Il buffer overflow è una vulnerabilità comune nei programmi che si verifica quando un programma tenta di scrivere più dati di quelli che il buffer può contenere. Questo tipo di vulnerabilità può portare a vari tipi di problemi, inclusi crash del programma e potenziali exploit di sicurezza. Questo report esamina due esercitazioni che illustrano il concetto di buffer overflow attraverso esempi pratici in linguaggio C.

Svolgimento

Il programma richiede all'utente di inserire un nome utente che viene memorizzato in un array di 10 caratteri. Se l'utente inserisce più di 10 caratteri, si verifica un errore di segmentazione (segmentation fault) a causa della sovrascrittura di aree di memoria non autorizzate:

1. **Creazione file BOF.c**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nano BOF.c
[sudo] password for kali:
```

```
File  Actions  Edit  View  Help
  GNU nano 8.0
#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;
}
```

1. **Compilazione del programma usando gcc:**

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

2. **Esecuzione del programma :**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:benedetto1
Nome utente inserito: benedetto1

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

3. un errore di segmentazione si verifica quando un programma tenta di scrivere su una porzione di memoria non consentita, tipicamente riservata ad altri processi o al sistema operativo.

Modifica del file BOF.c

In questo caso il programma richiede all'utente di inserire un nome utente che viene memorizzato in un array di 30 caratteri. Se l'utente inserisce più di 30 caratteri, si verifica un errore di segmentazione a causa della sovrascrittura di aree di memoria non autorizzate.

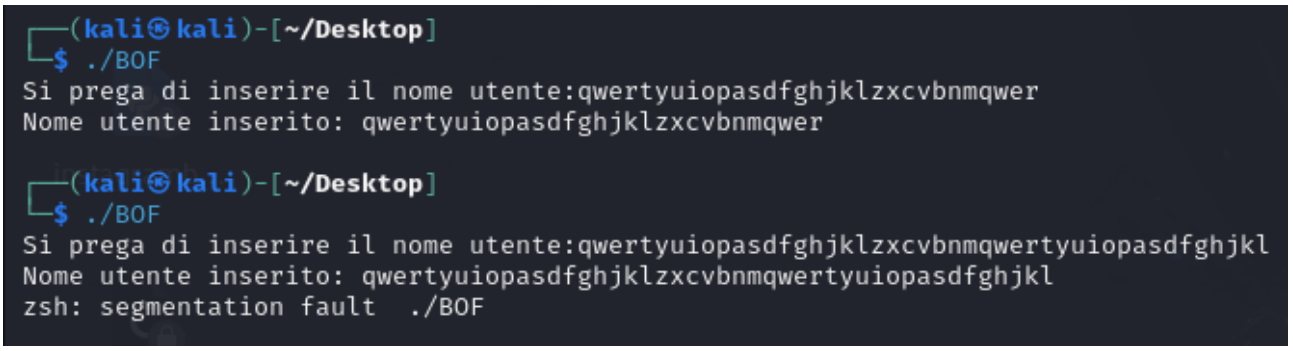
2. **Modifica del file in c:**

```
File  Actions  Edit  View  Help
  GNU nano 8.0
#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;
}
```

3. **Compilazione del file:**

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

4. **Esecuzione del programma:**



Modificando il file aggiungendo un array di 30, notiamo che adesso possiamo scrivere fino a 30 caratteri senza ricevere errori.
Naturalmente se superiamo questa soglia noteremo un segmentation fault , perché tentiamo di scrivere dove non ci è permesso.