Buffer Overflow

Pablo Andres Balbuena Rios

Esercizio 4 Settimana 7

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

- Aumentando la dimensione del vettore a 30.

Il Codice

Il codice chiede all'utente di inserire un nome utente e memorizza l'input in un array di caratteri chiamato "buffer". Successivamente, stampa il nome utente inserito. Tuttavia, il codice è vulnerabile a buffer overflow in quanto non specifica la lunghezza massima dell'input, il che potrebbe portare a problemi di sicurezza.

```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;

}
```

```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;

}
```

Buffer Overflow

Il buffer overflow si verifica quando un input più lungo del previsto sovrascrive la memoria adiacente al buffer. Quando il massimo della stringa è 10 e l'utente inserisce un nome più lungo di 30 caratteri, può causare un overflow e sovrascrivere la memoria, potenzialmente causando problemi di sicurezza come il controllo del flusso del programma.

char buffer [10]

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
 prega di inserire il nome utente: qwertyuiopqwertyuiopqwertyuiopasdfghjkl
me utente inserito qwertyuiopqwertyuiopqwertyuiopasdfghjkl
h: segmentation fault  ./BOF
```

char buffer [30]

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