Buffer Overflow

Indice

1. Traccia

Abbiamo già parlato del buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.

Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (come può essere ad esempio una posizione di memoria dedicata a funzioni del sistema operativo).

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

- **Aumentando la dimensione del vettore a 30;**

2. Creazione di un nuovo documento su kali Linux

Procediamo con la creazione di un nuovo documento con estensione **.c** sul desktop.
Da terminale eseguiamo il comando ***cd /home/Kali/Desktop***, e eseguiamo il comando ***nano BOF.c*** per la creazione del nuovo file.

Fatto ciò scriviamo il programma in ***C***, che sarà il seguente.

```
#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. Esecuzione del programma

A questo punto dopo aver salvato il file, lo compiliamo eseguendo il comando ***gcc –g BOF.c –o BOF*** e passiamo all'esecuzione dello stesso con il comando ***./BOF***

Il programma si avvia e ci chiede di inserire un nome utente.
Come abbiamo visto nel codice il buffer accetta dino a 10 caratteri (***char buffer [30];***), quindi possiamo inserire un nome utente di massimo 30 caratteri.

Come possiamo vedere nell'immagine qui di sotto inserendo un nome utente con meno di 30 caratteri il programma viene eseguito correttamente

Nel caso in cui inseriamo un nome utente con più di 30 caratteri ci dovrebbe dare un errore, ***"segmentation fault"***.
L'errore di segmentazione avviene quando un programma tenta di scrivere contenuti su una porzione di memoria alla quale non ha accesso. Questo è un esempio di ***BOF (Buffer Overflow)***.

Ma notiamo che nell'immagine qui di sotto anche inserendo un nome utente con più di 30 caratteri non ci restituisce nessun errore, questo è dovuto dall'architettura del software della macchina Kali.