

BUFFER OVERFLOW



COS'E'?

Il buffer overflow è una vulnerabilità di sicurezza che si verifica quando un programma, durante l'esecuzione, scrive dati oltre i limiti di un buffer, sovraesponendosi a se stesso o ad altre aree di memoria adiacenti.

Un buffer è una zona di memoria temporanea utilizzata per conservare dati, e può essere utilizzato per vari scopi, come l'archiviazione di stringhe di caratteri.



BUFFER

Un buffer è una zona di memoria temporanea utilizzata per conservare dati, e può essere utilizzato per vari scopi, come l'archiviazione di stringhe di caratteri.



STACK

Gli oggetti o dati sono salvati all'interno delle STACK. Una macro-componente (definita allocazione) della RAM.

All'interno di essa avviene la LIFO, ossia l'aggiunta (PUSH) del dato, e poi rimozione dell'ultimo dato aggiunto (POP)



OBIETTIVO

Creare buffer overflow su un codice in C vulnerabile e creare errore di “segmentation fault”.

codice in C

```
GNU nano 6.3
#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;
}
```

ESECUZIONE CODICE

Eseguito il codice bisogna inserire il “nome utente” con massimo 10 valori

Ma se si supera avviene il cosiddetto “segmentation fault”.

Modificando buffer [10] in [30] si potranno inserire fino a 30 valori. E come nello screen affianco, superati quei 30 valori, darà sempre “segmentation fault”

```
File Actions Edit View Help
/usr/bin/ld: /tmp/ccg9yVS0.o: in function `main':
/home/kali/Desktop/BOF.c:7:(.text+0x18): undefined reference to `print'
/usr/bin/ld: /home/kali/Desktop/BOF.c:10:(.text+0x4e): undefined reference to `print'
collect2: error: ld returned 1 exit status

(kali㉿kali)-[~/Desktop]
$ nano BOF.c

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

(kali㉿kali)-[~/Desktop]
$ ./BOF
Inserire nome utente omar
Nome utente inserito: omar

(kali㉿kali)-[~/Desktop]
$ ./BOF
Inserire nome utente asdasdasdasdasdasdasdasdasdasdasdasdasdasdas
Nome utente inserito: asdasdasdasdasdasdasdasdasdasdasdasdasdasdas
zsh: segmentation fault ./BOF

(kali㉿kali)-[~/Desktop]
$ nano BOF.c

(kali㉿kali)-[~/Desktop]
$ ./BOF
Inserire nome utente sssssssssssssssssssss
Nome utente inserito: sssssssssssssssssssss
zsh: segmentation fault ./BOF

(kali㉿kali)-[~/Desktop]
$ nano BOF.c

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

(kali㉿kali)-[~/Desktop]
$ ./BOF
Inserire nome utente sssssssssssssssssssss
Nome utente inserito: sssssssssssssssssssss
zsh: segmentation fault ./BOF
```