BUFFER OVERFLOW



Michelangelo Borromeo

Os Kali Linux

INDICE

- 1) Creazione codice **Python**
- 2) Segmentation Fault



Creazione codice Python



Creazione codice Python



(coding)

Iniziamo con la creazione del file .py Ci rechiamo sul desktop con il comando

cd Desktop



ed inviamo un

pwd

```
___(kali⊕kali)-[~/Desktop]
_$ pwd
/home/kali/Desktop
```

per verificare che la locazione sia quella richiesta.

A questo punto possiamo creare il file richiesto BOF.c

Con il comando

nano BOF.c

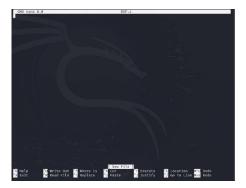
```
(kali@ kali)-[~/Desktop]
s nano BOF.c
```

E ci aprirà un file in C

Creazione codice **Python**



(coding)



A questo punto possiamo andare a trascrivere il codice che ci permetterà di poter effettuare la segmentation fail.

```
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;
}
```

Ora ctl+x e salviamo.

Andiamo a compilare il programma con il comando

gcc -g BOF -o BOF

```
___(kali⊛ kali)-[~]

$ gcc -g BOF.c -o BOF
```

Segmentation Fault



Segmentation Fault



(Exploit)

Possiamo eseguire il programma con il comando

./BOF

```
[ (kali⊛ kali)-[~]
$ ./BOF
```

invio

```
___(kali⊕ kali)-[~]
$ ./BOF
Si prega di inserire il nome utente:
```

E partirà il programma.

Ora possiamo procedere a riprodurre la segmentation fault inserendo + di 10 caratteri

```
(kali⊗kali)-[~]
$ ./BOF

Si prega di inserire il nome utente:ciaoatuttiquestoèuntest
Nome utente inserito: ciaoatuttiquestoèuntest
zsh: segmentation fault ./BOF
```

Una volta inerito il nome utente con + di 10 caratteri, apparirà l'errore di segmentation fault. Un errore di segmentazione ha luogo quando un programma tenta di accedere ad una posizione di memoria alla quale non gli è permesso accedere, oppure quando tenta di accedervi in una maniera che non gli è concessa

Test con dimensione del vettore a 30 caratteri:

```
(kali⊗ kali)-[~]
$ ./BOF
Si prega di inserire il nome utente:ifiuejwaoifhyqiouwyehufiqhewrpiuogqhjeroipuqoaghierjhivgo0qajeroi
vgjqer0èiojugvq0erojugv0pqejor'bvgoqe'bpoqjrkgivbopqjarg0voipjqrgvbio0jpuqw3rgvb0pju+r0w3hj9ub+00 R
3GIOVJ3WRIOPGVPJJMPOEWrdjkgvwjrvgiajerèjbe
Nome utente inserito: ifiuejwaoifhyqiouwyehufiqhewrpiuogqhjeroipuqoaghierjhivgo0qajeroivgjqer0èiojugv
q0erojugv0pqejor'bvgoqe'bpoqjrkgivbopqjarg0voipjqrgvbio0jpuqw3rgvb0pju+r0w3hj9ub+00
zsh: segmentation fault ./BOF
```





Michelangelo Borromeo