Report Esercizio

W17-D5

Redatto da Andrea Sciattella

18/06/2024

TRACCIA

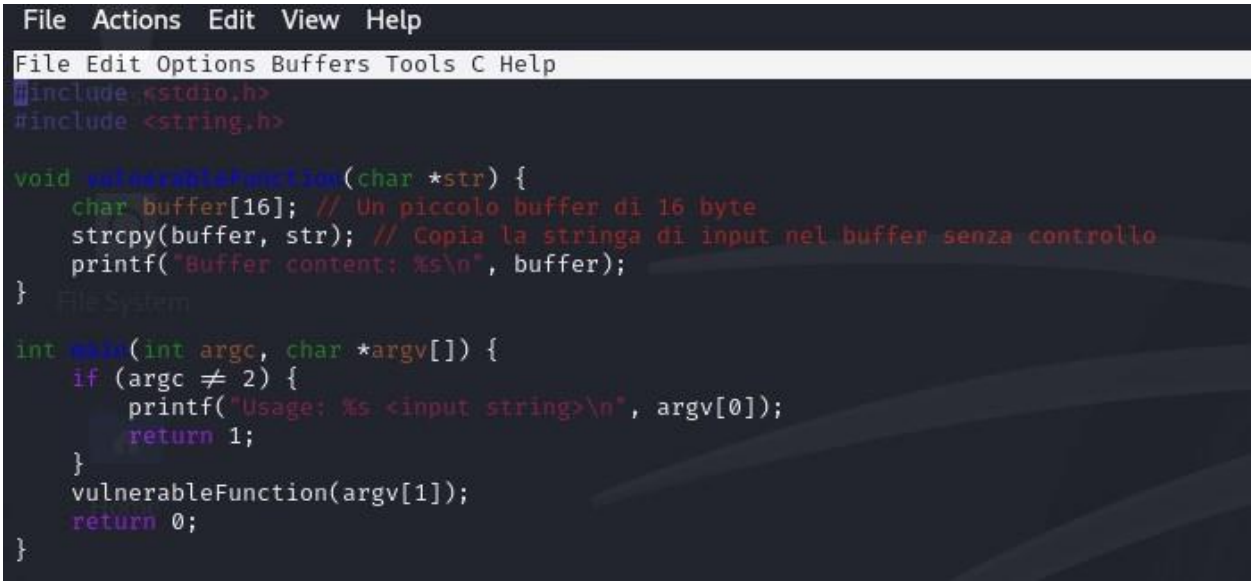
Nella lezione dedicata agli attacchi di sistema, abbiamo parlato dei buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente.

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).

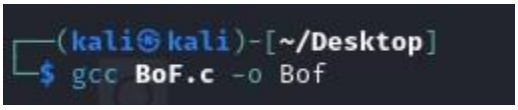
Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

SVOLGIMENTO ESERCIZIO

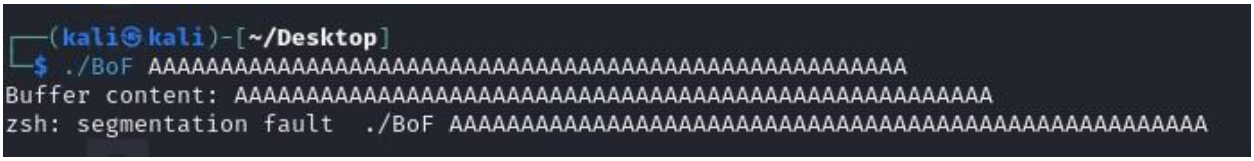
- Accediamo al desktop della macchina kali, e creaiamo il documento intitolato “BoF.c” con il comando touch



- Ora compiliamo il file con estensione C rinominandolo in “BoF”, tramite il compiler GCC



- Run the program e vediamo se il programma ha funzionato



- La frase “zsh: segmentation fault ./BoF AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA” conferma quindi il funzionamento del programma, quindi un Buffer Overflow.