Thực hành gỡ lỗi bộ nhớ với GDB

Viết một chương trình C có khả năng tái hiện ba lỗi bộ nhớ kinh điển: **Stack Overflow, Memory Leak, và Out of Memory**. Sau đó, sử dụng trình gỡ lỗi GDB để phân tích, tìm ra nguyên nhân gốc rễ của từng lỗi.

1. Yêu cầu chung

1.1. Viết một chương trình C duy nhất (**memory_lab.c**).
1.2. Chương trình nhận một tham số dòng lệnh để chọn lỗi cần tái hiện.

- **./memory_lab stack_overflow**: Gây ra lỗi Stack Overflow.
- **./memory_lab memory_leak**: Gây ra lỗi Memory Leak
- **./memory_lab out_of_memory**: Gây ra lỗi Out of Memory

2. Phân tích lỗi Stack Overflow **(Lưu ý là chưa làm phần này)**

2.1. Yêu cầu mã nguồn

- Viết một hàm sử dụng kỹ thuật đệ quy (recursion) để cố tình làm tràn bộ nhớ Stack.
- Hàm này nên in ra độ sâu hiện tại của lời gọi đệ quy để có thể quan sát được quá trình.

2.2. Yêu cầu phân tích bằng GDB
Chạy chương trình trong GDB với tham số stack. Khi chương trình gặp lỗi (Segmentation fault), hãy sử dụng GDB để trả lời các câu hỏi sau:

- Lệnh GDB nào cho phép bạn xem lại toàn bộ chuỗi các cuộc gọi hàm (call stack) đã dẫn đến lỗi?
- Quan sát kết quả của lệnh trên, hàm nào được gọi lặp đi lặp lại nhiều nhất? Điều này nói lên điều gì về bản chất của lỗi?
- Làm thế nào để xem thông tin về stack frame hiện tại (frame nơi xảy ra lỗi)?

3. Phân tích lỗi Memory Leak & Out of Memory

3.1. Yêu cầu mã nguồn

- Viết một hàm chứa một vòng lặp vô tận.
- Bên trong vòng lặp, liên tục cấp phát một khối bộ nhớ (ví dụ: 1KB) bằng malloc.
- Không được gọi free() để giải phóng bộ nhớ đó, tạo ra tình trạng Memory Leak.

- Chương trình phải kiểm tra nếu malloc trả về NULL. Khi điều này xảy ra (lỗi Out of Memory), hãy in ra một thông báo lỗi và thoát khỏi chương trình một cách an toàn.

3.2. Yêu cầu phân tích bằng GDB

Chạy chương trình trong GDB với tham số leak. Sử dụng các kỹ thuật của GDB để điều tra và trả lời các câu hỏi sau:

- Làm thế nào để bạn đặt một điểm dừng (breakpoint) trong GDB mà nó chỉ kích hoạt khi chương trình của bạn phát hiện ra lỗi Out of Memory (tức là khi malloc trả về NULL)?
- Khi chương trình dừng tại điểm đó, lệnh GDB nào giúp bạn xác định được hàm nào và tại dòng mã nào đã gây ra yêu cầu cấp phát bộ nhớ thất bại?
- Dựa trên việc phân tích mã nguồn tại vị trí lỗi, hãy chỉ ra chính xác dòng code hoặc logic nào đã gây ra tình trạng Memory Leak, dẫn đến việc cạn kiệt bộ nhớ.