BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của mã độc**

**Lab 3: Simple worm**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.N21.ANTT.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Thiên An | 20520378 | 20520378@gm.uit.edu.vn |
| 2 | Nguyễn Quang Huy | 20520546 | 20520546@gm.uit.edu.vn |
| 3 | Bùi Đức Hoàng | 20520514 | 20520514@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu 1 | 100% |
| 2 | Yêu cầu 2 | 100% |
| 3 | Yêu cầu 3 | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Yêu cầu 1:

***example1.c :***

Text

Description automatically generated

Để hiểu được chương trình đã làm gì để gọi hàm function(), ta biên dịch chương trình bằng gcc sử dụng option -S để cho output là code assembly:

Text

Description automatically generated

Hàm function() sau khi được biên dịch:

Text

Description automatically generated with medium confidence

Thao tác này đưa 3 đối số vào stack và gọi hàm. Lệnh ‘call’ sẽ đưa con trỏ chỉ vị trí thực thi (instruction pointer – IP) vào trong stack. Chúng ta sẽ gọi IP đã lưu trữ là địa chỉ trả về (RET). Điều đầu tiên được thực hiện trong hàm là tiến trình prolog:

Text

Description automatically generated

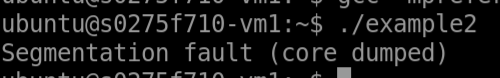
Đầu tiên đoạn mã đẩy ebp vào trong stack. Sau đó, sao chép giá trị hiện tại của Stack Pointer(SP) vào ebp, làm cho ebp trở thành Frame Pointer(FP) mới. Chúng ta sẽ gọi con trỏ FP được lưu trữ là SFP. Sau đó nó cấp phát không gian cho các biến local bằng cách trừ kích thước của chúng từ SP.

***example2.c :***

Text

Description automatically generated

Chương trình chứa hàm gây ra lỗi buffer overflow. Hàm sao chép một chuỗi mà không kiểm tra giới hạn bằng cách sử dụng hàm strcpy() thay vì strncpy(). Nếu chạy chương trình này sẽ gặp lỗi “Segmentation fault (core dumped)”.



Chương trình bị lỗi trên là do hàm strcpy() đang sao chép nội dung của \*str(larger\_string[] vào buffer[] cho đến khi xuất hiện ký tự null trên chuỗi. buffer[] nhỏ hơn rất nhiều so với \*str, buffer[] dài 16byte và chúng ta đang cố gắng nhập vào 256byte. Điều này có nghĩa tất cả 240 byte sau buffer trên stack đang bị ghi đè. Điều này bao gồm SFP, RET và thậm chí \*str! Chúng ta đã lấp đầy large\_string với ký tự ‘A’. Giá trị hex là 0x41. Vậy địa chỉ trả về hiện tại là 0x41414141. Đây là ngoài không gian địa chỉ của tiến trình. Đó là lý do tại sao khi hàm trả về cố gắng đọc lệnh tiếp theo từ địa chỉ đó, ta sẽ nhận được “segmentation fault”. Vì vậy buffer overflow cho phép chúng ta thay đổi địa chỉ trả về của một hàm. Theo cách này chúng ta có thể thay đổi luồng thực thi của chương trình.

***example3.c :***

Chúng ta sẽ thay đổi đoạn code ví dụ trước để có thể ghi đè lên địa chỉ trả về và chứng minh chúng ta có thể thực thi mã tùy ý. Ngay trước buffer[] trên stack là SFP, và trước đó là return address. Đó là 4 byte cuối trước buffer1[]. buffer1[] có độ dài 8 byte. Vậy địa chỉ trả về cách 12 byte từ đầu đến buffer1[]. Chúng ta sẽ thay đổi giá trị trả về sao cho sau lời gọi hàm sẽ nhảy đến câu lệnh gán ‘x=1;’. Để làm được điều đó chúng ta cần thêm 8byte vào địa chỉ trả về.

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)