Tên: Nguyễn Trung Kiên

Lớp : 09\_ĐH\_CNPM2

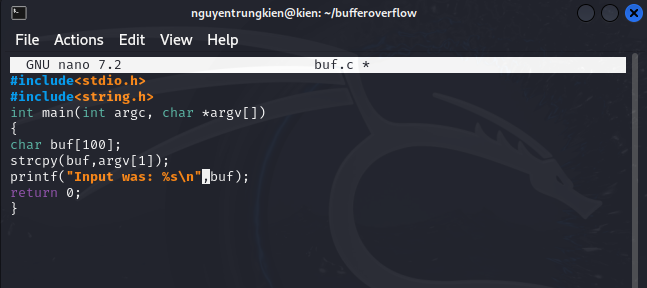
MSSV : 0950080057

KHAI THÁC VÀ NGĂN CHẶN LỖI BUFFER OVERFLOW

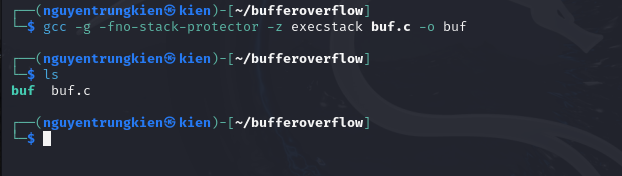
Câu 1: Khai thác lỗi Stack-based Buffer Overflow trên Linux 64 bit

1.1 Soạn thảo 1 chương trình buf.c

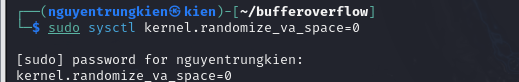




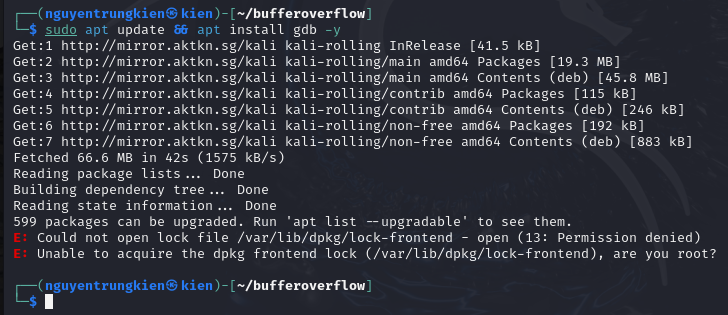
1.2 Biên dịch chương trình buf.c

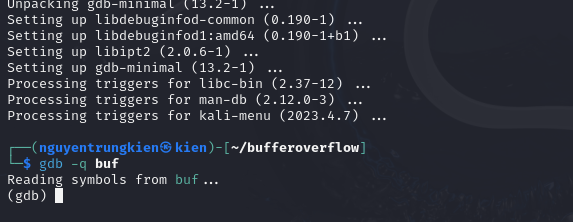


1.3 Tắt chức năng Address Space Layout Randomization (ASLR)

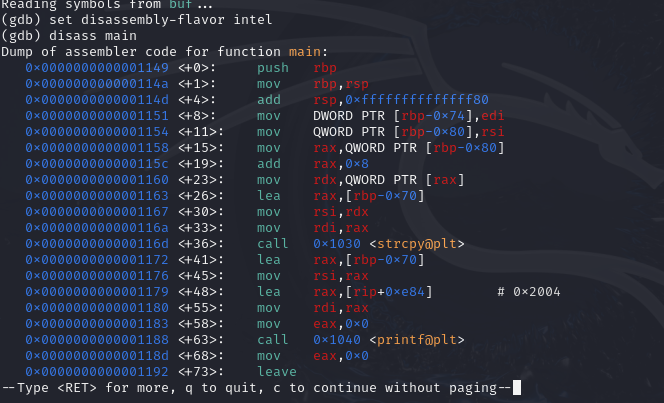


1.4 Cài đặt gdb và bắt đầu debug chương trình

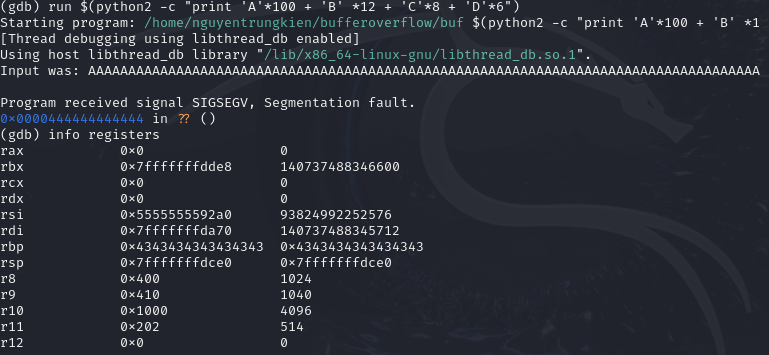


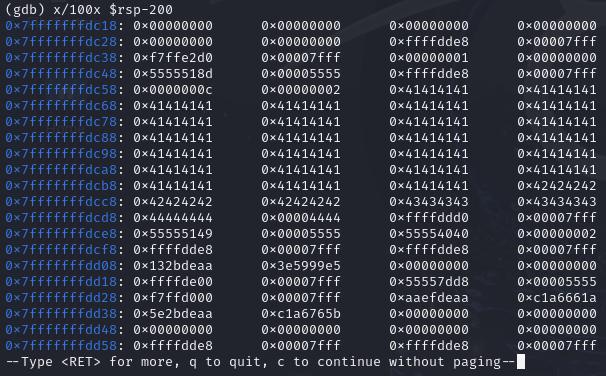


1.5Bên trong môi trường gdb, chọn cú pháp assembly theo kiến trúc Intel và chuyển hàm main thành ngôn ngữ assembly:



1.6 Xác định vị trí của return address (RIP)





1.7 Khai thác

