Đặt vấn đề: trong thực tế chúng ta chỉ có file thực thi của chương trình. Vì vậy muốn tìm kiếm và khai thác lỗ hổng ta cần

1) dịch ngược file thực thi về dạng code (sử dụng công cụ IDA Pro, gdb)

2) phân tích code đã dịch ngược để tìm kiếm lỗ hổng

3) viết mã khai thác lỗ hổng

Các bài thực hành của môn này cũng được thiết kế theo kịch bản như vậy

Trong tệp “Bộ bài tập thực hành.rar” là các file thực thi, ngoài ra còn có một số file mã nguồn để đối chiếu trong quá trình thực hiện.

Việc dịch ngược và phân tích code được thực hiện trên máy Window, sử dụng công cụ IDA Pro 6.6

Việc khai thác được thực hiện trên máy ảo Ubuntu (mật khẩu 123456a@)