**BÀI LAB 2:**

**REVERSE ENGINEERING BASIC**

# Giới thiệu

Bài lab này sẽ giúp các bạn sinh viên làm quen với ngôn ngữ assembly intel x86 và các kĩ thuật RE đơn giản.

**Yêu cầu bài lab:**

Đây là môt bài lab được biên soạn lại từ bộ Lab Assignment cùa trường CMU – USA, bài lab này tương đối khó và cần nhiều nỗ lực của các bạn sinh viên để làm. Các kiến thức cần để giải bài lab này gồm có:

* Toàn bộ kiến thức về ngôn ngữ assembly x86 trong chương 3 sách Computer System: A Programmer’s Perspective.
* Cách thức sử dụng một chương trình assembler bất kì : GDB, OllyGDB, Immunity, IDA … Khuyến nghị sử dụng IDA.
* Kiến thức về remote debugger trên desktop khi sử dụng IDA.

Trong nội dung bài lab, giáo viên thực hành sẽ hướng dẫn sơ lược về cách thức cài đặt, làm quen với trình assembler IDA cũng như cách remote debugger trên desktop. Tuy nhiên các bạn sinh viên cần phải nghiên cứu nhiều hơn mới có thể hoàn tất được bài lab.

Sinh viên làm bài lab theo hướng dẫn và ghi đáp án vào file có dạng **MSSV\_csappLab2.txt** hoăc .docx.

# Nội dung bài lab

## Bomb defusing Game

Trong bài lab này, CMU đã xây dựng một trò chơi từ bộ kiến thức trong chương 3 sách CSAPP. Một chương trình đã được lập trình sẵn và có hoạt động như một quả bomb máy tính. Quả bomb này gồm 6 pha, mỗi pha yêu cầu một input riêng để ngắt pha. Nếu input sai, bomb sẽ nổ và trò chơi kết thúc.

Để phù hợp với năng lực của trường UIT, người biên soạn đã tối cấu trúc lại các pha như sau:

Bộ pha cơ bản : Pha 1 , 2 , 3

Bộ pha trung bình – khó : Pha 4 và 5

Bộ pha rất khó : Pha 6

Độ khó của mỗi pha được đánh giá bằng dấu (\*) như sau:

Pha 1: \*

Pha 2: \*\*

Pha 3: \*\*\*

Pha 4: \*\*\*\*\*

Pha 5: \*\*\*\*

Pha 6: \*\*\*\*\*\*

Trong bài lab này sinh viên sẽ giải mỗi pha của Bomb khi thực thi file thực thi “bomb” và ghi lại đáp án vào file dạng text.

## Cách thức chạy file và giải Pha

Đính kèm theo bài lab này là một file thực thi ELF trên hệ điều hành linux có tên “bomb”.

Dùng lệnh file trên linux để xem thông tin ELF của file.

Dùng lệnh chmod cho file chạy toàn quyền r, w, x

Dùng lệnh strings để đọc sơ lược nội dung trong file.

**Hướng dẫn tải chương trình IDA và Remote Desktop Debuging:**

Các bạn tải chương trình IDA Pro 6.6 trong link sau:

<https://www.dropbox.com/s/klhyb93a1wmk26y/IDAPro6.6full.7z?dl=0>

Giải nén và copy thư mục IDAPro6.6full vào C:\Program Files\

Double click vô thư mục IDAPro, vào thư mục dbgsrv copy file **linux\_server** và **linux\_serverx64** vào thư mục chứa file bomb trên máy linux

Trong máy Linux, cd vào thư mục chứa 3 file đó, chạy lệnh:

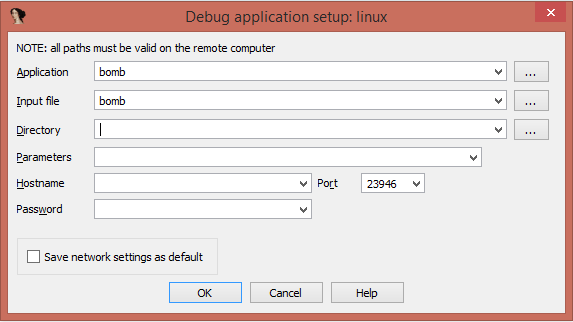
*chmod 777 \**

*./linux\_server*

Copy file bomb lên máy windows chạy IDA. Trên máy windows, chạy chương trình IDA bản 32bit. Trong của sổ *IDA: Quick Start* hiện ra chọn New, chọn file bomb.

Trên thanh menu, chọn Debugger/Select Debugger, chọn Remote Linux Debugger.

Bấm start process ( dấu mũi tên màu xanh lá), một của sổ hiện ra hỏi thông tin của Linux debugger. Ta nhập như hình



Mục Hostname nhập IP của máy linux. Mục Password là password đăng nhập của máy linux. Sau đó bấm OK. Lúc này chương trình sẽ tự liên kết với file linux\_server trên máy linux để debug.

Tới đây các bạn sinh viên phải tự tìm hiểu thêm về IDA và ngôn ngữ assembly để hoàn tất vài lab. Điểm của bài lab sẽ được tính như sau:

Pha 1: 2 điểm

Pha 2: 2 điểm

Pha 3: 3 điểm

Pha 4: 1 điểm

Pha 5: 1 điểm

Pha 6: 1 điểm

**Các thông tin liên quan:**

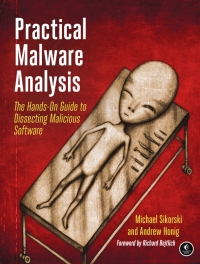
Hướng dẫn Remote Desktop Debugger của anh Đặng Minh Trí lớp ANTN2012:

<https://www.youtube.com/watch?v=Lh2TXlyrSIM>

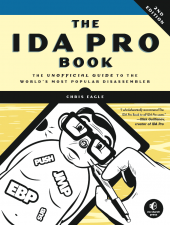
Hướng dẫn sử dụng IDA:

Các bạn có thể tìm đọc 2 quyển sách sau:

Mức cơ bản: Chương nói về IDA trong sách **Practical Malware Analysis**



Mức nâng cao: Quyển **IDA Pro Book**



Kiến thức về Assembly, các bạn có thể tìm đọc quyển **Practical Reverse Engineering**

