Step 0: Cài đặt Ubuntu và các file stack.c, exploit.c/exploit.py

A screenshot of a computer

Description automatically generated

Step 1: Vô hiệu hóa địa chỉ ngẫu nhiên

A screenshot of a computer

Description automatically generated

* Địa chỉ ngẫu nhiên (Adress randomization) là một cơ chế của hệ điều hành để chống các cuộc tấn công. Vì thế cần phải tắt nó đi để thực hiện bài lab.

Step 2: Kiếm địa chỉ của mã độc:

* Tạo file thực thi stack\_dbg từ file stack.c.
* Các lệnh -z execstack 🡪 cấp quyền thực thi vào vùng nhớ stack, -fno-stack-protector 🡪 tắt bảo vệ stack, -m32 để tạo file 32bit khi sử dụng trên máy 64 bit

A screenshot of a computer

Description automatically generated

* Tạo thành công file thực thi stack\_debug

A screen shot of a computer program

Description automatically generated

* Tạo file badfile

A screenshot of a computer

Description automatically generated

* Tạo thành công file badfile

A screen shot of a computer

Description automatically generated

* Debug file stack\_dbg

A screenshot of a computer

Description automatically generated

* Đặt break point bof

A screenshot of a computer

Description automatically generated

* Lấy địa chỉ epb:

A screenshot of a computer program

Description automatically generated

* Lấy địa chỉ của biến buffer:

A screenshot of a computer program

Description automatically generated

* Tính toán hiệu số giữa địa chỉ buffer và ebp

A screenshot of a computer program

Description automatically generated

Step 3: chỉnh sửa file exploit.c

* Điền giá trị cần thiết vào file exploit.c

A screen shot of a computer

Description automatically generated

Step 4: Thực thi

* Thay đổi shell mặc định

A computer screen shot of a program

Description automatically generated

* Tạo file thực thi stack

A screenshot of a computer

Description automatically generated

* Chown về root

A screenshot of a computer

Description automatically generated

* Bật bit đặc biệt:

A screenshot of a computer

Description automatically generated