Bộ môn An toàn Thông tin – Khoa Mạng máy tính và Truyền thông
Trường Đại học Công nghệ Thông tin – Đại học Quốc gia thành phố Hồ Chí Minh

6

Lab

Bài tập tổng hợp

Thực hành môn Lập trình An toàn &

Khai thác lỗ hổng phần mềm

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

BE SECURE
INSECLAB

A. TỔNG QUAN

A.1 Mục tiêu

Trong bài thực hành này, chúng ta sẽ ôn lại các kiến thức và thực hành các kỹ năng tấn công một số lỗ hổng đã học ở các lab trước để giải một số challenge CTF.

A.2 Hình thức thực hiện

- **Hình thức:** thực hiện các bài tập CTF Jeopardy theo nhóm.
- **Mô tả:** đây là các bài tập yêu cầu thực hiện khai thác, tấn công một số lỗ hổng tồn tại trong một số chương trình cho trước để tìm kiếm một thông tin bí mật – gọi là *flag.* Có thể tìm thấy và nộp được flag là minh chứng cho thấy sinh viên đã hoàn thành yêu cầu khai thác.

  Định dạng flag: W1{...}.
- Một số lưu ý trong quá trình làm bài:
  - Nghiêm cấm chia sẻ flag dưới mọi hình thức. Nếu bị phát hiện, các nhóm sẽ bị loại.
  - Việc tấn công vào các hệ thống không được thiết kế để tấn công ở các challenges bị cấm và sinh viên sẽ bị loại.
  - Nếu có thắc mắc về bất kỳ vấn đề gì, như nghi ngờ flag lỗi, thắc mắc về nội quy hoặc phát hiện lỗi hệ thống, vui lòng liên hệ GVHD.
  - Trường hợp phát hiện hệ thống có lỗi nằm ngoài phạm vi của các challenge, vui lòng thông báo ngay lập tức cho GVHD. **Tùy thuộc vào lỗ hổng phát hiện, sinh viên có thể có thêm điểm cộng từ phía GVHD.**

A.3 Môi trường thực hành

- Sinh viên thực hiện bài thực hành trên hệ thống vLab: https://vlab.uit.edu.vn. Mỗi nhóm sinh viên được cung cấp 2 máy ảo:
  - 01 máy ảo **vul** (Ubuntu 20 server) có lỗ hổng cần khai thác trong các challenge.
  - 01 máy ảo **vm** (Kali Linux) để làm môi trường cho attacker thực hiện khai thác.
- Công cụ có thể sử dụng:
  - pwndbg/gef
  - pwntools
  - IDA Pro

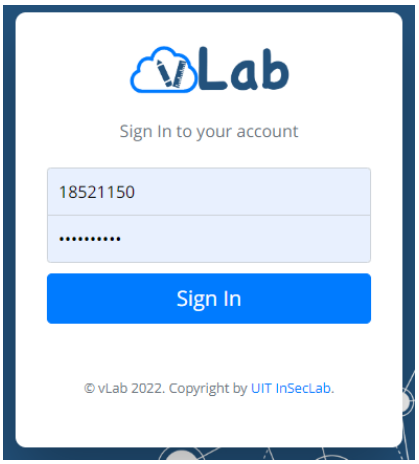
B. NỘI DUNG THỰC HÀNH

B.1 Hướng dẫn truy cập môi trường máy ảo

Các máy được cấp có địa chỉ tại: https://vlab.uit.edu.vn.

Bước 1. Truy cập URL: https://vlab.uit.edu.vn

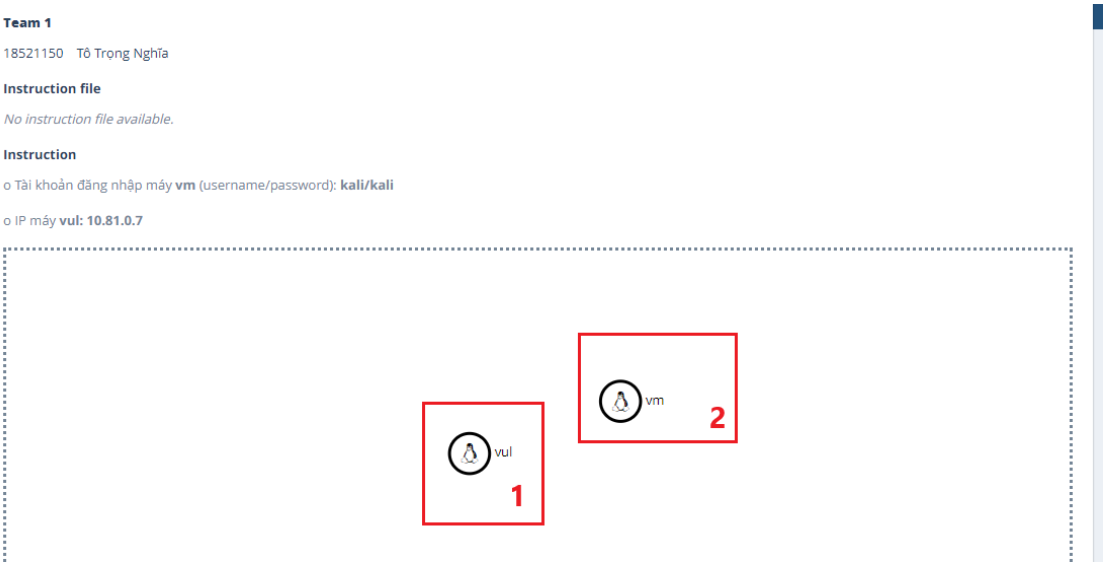
Bước 2. Chọn **Access to Vlab** và sử dụng tài khoản chứng thực để đăng nhập.



Bước 3. Truy cập bài thực hành với thông tin được GVTH cung cấp.

Bước 4. Xem thông tin mô hình mạng với 2 máy ảo.

Trong bài thực hành, vào tab **Information,** chúng ta có thể thấy giao diện như bên dưới. Sinh viên kiểm tra các thông tin được hiển thị trong tab này.



- Thông tin nhóm thực hành: Tên nhóm, danh sách các thành viên.
- Thông tin hướng dẫn để truy cập các máy ảo.
  - Thông tin đăng nhập máy **vm** (Kali Linux)
  - Địa chỉ IP của máy **vm** (máy có lỗ hổng)

Trong đó lưu ý, sinh viên chỉ có thể truy cập và tương tác với máy **vm** (Kali Linux), trong khi đó máy **vul** không hỗ trợ các truy cập qua SSH hay Console, sinh viên chỉ có thể khai thác máy này từ máy **vm** nằm cùng mạng.

Bước 5. Truy cập máy ảo vm

Nhấn chuột trái vào máy **vm**, sau đó chọn **Remote link(s) → SSH**. Đăng nhập vào máy với tài khoản được cung cấp và bắt đầu làm bài.

B.2 Challenges

B.2.1 Hướng dẫn chung

- Mỗi challenge có mức độ dễ/khó khác nhau và độc lập với nhau, sinh viên có thể tùy chọn thứ tự challenge muốn giải.
- Tên challenge có gợi ý về lỗ hổng/tấn công cần khai thác hoặc thực hiện.
- Mỗi challenge đều có 1 cờ dạng W1{...}.
- Ở tất cả các challenge, sinh viên giải bài như sau:
  - Mỗi challenge tương ứng với 1 port trên máy **vul**. Sử dụng lệnh nc như hướng dẫn sẽ kết nối đến challenge tương ứng.
  - File thực thi của mỗi challenge được cung cấp sẵn ở Lab 6 - Code reference – Password: difplqfRFU, sinh viên có thể phân tích file trên máy **vm** để tìm payload.
  - Gửi payload bằng cách viết file python như gợi ý bên dưới:

```
from pwntools import *
p = remote('10.81.0.7', 14004)          # change to correct IP and port
# prepare payload to send to vulnerable file
payload = 'xxxxxxx'
# send payload
p.sendline(payload)
p.interactive()
```

B.2.2 Danh sách các challenges

Có tất cả 4 challenge.

STT	Tên challege	Mức độ	Truy cập	Ghi chú
1	Stack Architect	Dễ	nc 10.81.0.7 **14004**	
2	Shellcode	Dễ	nc 10.81.0.7 **14003**	- Bắt buộc dùng open, read, write để đọc flag. - Không cần quan tâm đến seccomp. - Dùng syscall ngoài open, read, write sẽ bị khóa.
3	Autofmt	Trung bình	nc 10.81.0.7 **14001**	
4	Ropchain	Khó	nc 10.81.0.7 **14002**	

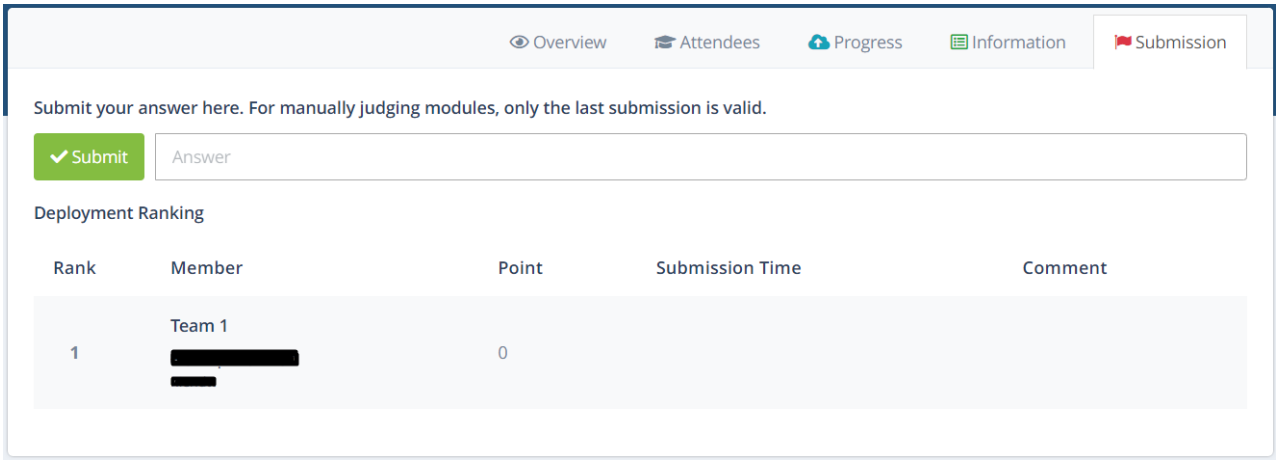
B.4 Hướng dẫn nộp bài

Để nộp bài, sinh viên cần thực hiện các công việc sau:

1. Submit flag tìm được trên vlab

Khi giải xong mỗi challenge, sinh viên cần nộp flag tìm được trên hệ thống vLab ở tab **Submission** của bài thực hành. Mỗi flag đúng sẽ nhận được thông báo chúc mừng và điểm của nhóm sẽ được cập nhật.

*Lưu ý: Các challenge được tính điểm độc lập với nhau, điểm của bài thực hành sẽ dựa trên **tổng điểm** của các challenge.*



2. Nộp write-up cách giải bài trên course

Sinh viên cần nộp báo cáo cách giải chi tiết đã thực hiện trong từng challenge. Nội dung báo cáo sẽ là cơ sở để GVTH đánh giá, kiểm chứng kết quả đã nộp trên vLab và tính điểm bài thực hành.

*Lưu ý: Sinh viên nộp flag trên vLab nhưng **không nộp báo cáo** thì xem như **sao chép bài**, sẽ bị 0 điểm.*

HẾT

Chúc các bạn hoàn thành tốt!