BÀI TẬP LỚN  
KHAI THÁC LỖ HỔNG PHẦN MỀM

# Mô tả bài tập

Sinh viên được cung cấp một bộ gồm 30 bài tập thực hành khai thác lỗ hổng phần mềm, bao gồm các lỗ hổng tràn bộ đệm, tràn số nguyên, chuỗi định dạng và bài tập về viết shellcode. Kèm theo bộ bài tập này là hướng dẫn thực hiện. Sinh viên có nhiệm vụ nghiên cứu tài liệu hướng dẫn để thực hiện lại các bài tập thực hành khai thác lỗ hổng phần mềm đã cho.

# Mức điểm tối đa

|  |  |
| --- | --- |
| Mức điểm tối đa | Tiêu chí |
| 5 | * Số lượng bài làm được: ≥ 3 * Có ít nhất một bài về format string * Có ít nhất một bài về buffer overflow |
| 6 | * Số lượng bài làm được: ≥ 5 * Có ít nhất một bài về format string * Có ít nhất một bài về buffer overflow |
| 7 | * Số lượng bài làm được: ≥ 7 * Có ít nhất một bài về format string * Có ít nhất một bài về buffer overflow * Có ít nhất một bài về integer overflow |
| 8 | * Số lượng bài làm được: ≥ 8 * Có ít nhất 2 bài về format string * Có ít nhất 2 bài về buffer overflow * Có ít nhất 2 bài về integer overflow |
| 9 | * Số lượng bài làm được: ≥ 9 * Có ít nhất 2 bài về format string * Có ít nhất 2 bài về buffer overflow * Có ít nhất 2 bài về integer overflow * Có ít nhất một bài về shellcode |
| 10 | * Số lượng bài làm được: ≥ 10 * Có ít nhất 2 bài về format string * Có ít nhất 2 bài về buffer overflow * Có ít nhất 2 bài về integer overflow * Có ít nhất 2 bài về shellcode |

# Yêu cầu đối với việc làm và trình bày kết quả

## Yêu cầu chung

Sinh viên làm các bài tập thực hành và trình bày kết quả dưới dạng tập tin Microsoft Office Word (hoặc định dạng khách tương thích).

Sinh viên phải tự mình làm bài tập thực hành. Không sao chép của người khác, không sao chép từ tài liệu hướng dẫn. Nếu phát hiện sự sao chép thì mọi sinh viên liên quan sẽ nhận 0 điểm (không phân biệt người sao chép hay người cho sao chép).

## Môi trường thực hành

Sinh viên được tùy ý chọn môi trường (hệ điều hành và các công cụ khác) để thực hiện bài tập lớn.

Đối với hệ điều hành cần đặt hostname là mã sinh viên, username là viết tắt các chữ cái đầu tiên trong họ và tên của sinh viên.

## Yêu cầu về trình bày

### Cấu trúc nội dung file báo cáo

1. Trang bìa

2. Mục lục

* Là đề mục cấp 1
* Đánh chỉ mục đến đề mục cấp 2

3. Giới thiệu môi trường thực hành

* Là đề mục cấp 1
* Giới thiệu về môi trường thực hành: hệ điều hành và các công cụ, các thiết lập đối với hệ điều hành và các công cụ trước khi thực hành

4. Kết quả thực hành

* Mỗi bài tập được trình bày trong phạm vi một đề mục cấp 1. Tiêu đề (tên) mỗi đề mục là tên của bài thực hành (sao chép chính xác tên bài thực hành trong tài liệu hướng dẫn thực hành)
* Các bài thực hành phải được sắp thứ tự như thứ tự trong tài liệu hướng dẫn thực hành.
* Nội dung trình bày cho mỗi bài thực hành cần có các phần sau:
  + Mô tả nhiệm vụ.
    - Là một đề mục cấp 2.
    - Mô tả những gì được cho và nhiệm vụ cần thực hiện.
    - Luận giải việc thực hiện bước thực hiện đầu tiên.
  + Các bước thực hiện.
    - Mỗi bước là một đề mục cấp 2
    - Mỗi bước cần được đánh số kèm theo mô tả ngắn ngọn việc cần làm ở bước đó. Ví dụ: “Bước 1. Dịch ngược chương trình”.
    - Nội dung mỗi bước cần được trình bày ngắn gọn, rõ ràng và NÊN thể hiện được 4 ý:
      1. Đã thực hiện thao tác nào;
      2. Kết quả thu được sau các thao tác;
      3. Phân tích kết quả để rút ra các thông tin/kết luận hữu ích;
      4. Luận giải việc thực hiện bước tiếp theo.

5. Tự chấm điểm

* Là đề mục cấp 1
* Sinh viên căn cứ vào quy định về mức điểm tối đa ở trên để đánh giá kết quả thực hành của mình. Nội dung gồm điểm tự đánh giá và diễn giải:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Điểm tự đánh giá: …….. (điểm)  Diễn giải điểm tự chấm:   |  |  | | --- | --- | | Tiêu chí | Diễn giải | |  |  | |  |  | |  |  | |  |  | |  |  | |

\*Cột “Tiêu chí”: liệt kê các tiêu chí (căn cứ vào “Mức điểm tối đa”) mà sinh viên đã đạt được, mỗi dòng một tiêu chí.

\* Cột “Diễn giải”: giải thích việc thấy sinh viên đáp ứng được tiêu chí tương ứng (tổng số bài tập đã giải, số thứ tự của các bài tập thỏa mãn tiêu chí)

### Quy cách trình bày báo cáo

* Phông chữ chính: Times New Roman, 14pt
* Trình bày mã nguồn:
  + Không thụt đầu dòng
  + Phông chữ họ Consolas hoặc Courier, Cỡ chữ tùy ý, từ 8 trở lên.
  + Khuyến cáo có màu để làm nổi bật (highlight) mã.
* Đánh số trang, ngoại trừ trang bìa
* Hình ảnh trong báo cáo phải sắc nét, không bị co. Nếu cần, phải cắt lấy phần thể hiện nội dung cần trình bày và loại bỏ những phần khác.

### Quy cách đặt tên tập tin kết quả

Tên tập tin báo cáo (chưa kể phần mở rộng) phải có dạng:

<Mã sinh viên>. <Họ và tên>

Trong đó họ và tên đầy đủ của sinh viên cần được viết đúng quy tắc chính tả tiếng Việt. Hai thành phần phân tách bởi 1 dấu chấm và 1 dấu cách.

## Nộp kết quả

Sinh viên nộp kết quả thông qua lớp trưởng.

Thời hạn: 23:59:59 Chủ Nhật, ngày 04/06/2023.

# Đánh giá kết quả

Giảng viên chủ yếu đánh giá kết quả qua văn bản báo cáo.

Giảng viên có thể yêu cầu sinh viên thực hiện lại bài thực hành bất kỳ. Nếu không thể thực hiện và có dấu hiệu cho thấy sinh viên không tự mình thực hiện bài thực hành trong báo cáo thì sẽ nhận 0 điểm cho toàn bộ báo cáo.