Phát hiện lỗi và 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 file trình chiếu (PowerPoint hoặc tương tự); mỗi bài tập được trình bày riêng trong một file trình chiếu.

Sinh viên phải tự mình làm bài tập thực hành. Sinh viên có thể hỏi bất kỳ ai, có thể tham khảo bài làm của bất kỳ ai... nhưng phải HIỂU và phải TỰ MÌNH làm bài tập; các hình ảnh được sử dụng trong báo cáo kết quả phải là hình ảnh do chính mình thực hiện.

Nếu phát hiện sự sao chép, dù chỉ 01 slide thì mọi sinh viên liên quan sẽ nhận 0 điểm (không phân biệt người sao chép hay người cho sao chép).

## Yêu cầu về minh chứng

Trên máy (Linux) được sử dụng để làm các bài tập thực hành, sinh viên phải đặt username trùng với họ và tên của mình (sử dụng các chữ cái thường, viết liền, không dấu, đầy đủ họ và tên).

## Yêu cầu về trình bày

### Cấu trúc nội dung file báo cáo

Nội dung mỗi file trình chiếu phải bao gồm:

* Mô tả bài tập tương ứng
* Các bước thực hiện bài tập, mỗi bước được mô tả bằng lời, và hình ảnh minh họa

### Quy cách trình bày báo cáo

* Các slide phải được đánh số
* Văn bản trên slide phải có cỡ chữ tối thiểu là 28pt.
* Khi đưa hình ảnh vào slide, cần phải cắt lấy phần thể hiện nội dung cần trình bày và loại bỏ những phần khác; kéo giãn hình ảnh tới kích thước lớn nhất có thể mà vẫn giữ nguyên tỉ lệ giữa chiều cao và chiều ngang của ảnh.

### Quy cách đặt tên file kết quả

Tên file trình chiếu (chưa kể phần mở rộng) phải có dạng:

<Tên sinh viên>. <TT bài tập>. <Tên bài tập>

Trong đó

* <Tên sinh viên> là họ và tên đầy đủ của sinh viên, viết đúng chính tả (viết Hoa) bằng tiếng Việt có dấu
* <TT bài tập> là số thứ tự của bài tập trong danh sách các bài tập, viết đủ 02 chữ số
* <Tên bài tập> là tên của bài tập trong danh sách bài tập

Lưu ý: 3 thành phần trên đây được phân tách nhau bởi một dấu chấm và một dấu khoảng trắng (dấu cách). Dấu khoảng trắng phải đặt sau dấu chấm; còn trước dấu chấm không được phép có dấu khoảng trắng.

Ví dụ, nếu sinh viên Trần Văn Bình làm bài tập “Level07” thì tên file kết quả tương ứng sẽ là:

Trần Văn Bình. 08. Level07

Và nếu sinh viên này làm được bài “Bufferoverflow-overwrite-command” thì tên file kết quả tương ứng sẽ là:

Trần Văn Bình. 14. Bufferoverflow-overwrite-command

## Nộp kết quả

### Hình thức nộp

Sau khi làm xong các bài tập hoặc đến hạn phải nộp bài tập, sinh viên cần thực hiện các việc sau:

* Soạn bảng tự chấm điểm bài tập thực hành (có mẫu kèm theo)
* Tạo thư mục với tên:

LHPM<TT Lớp>. <TT Sinh viên>. <Họ và tên>

Trong đó:

* + <TT Lớp> là số thứ tự của lớp học phần, ghi đủ 02 chữ số.
  + <TT Sinh viên> là số thứ tự của sinh viên trong danh sách điểm danh, viết đủ 02 chữ số;
  + <Họ và tên> là họ và tên đầy đủ của sinh viên, viết đúng chính tả (viết Hoa theo đúng quy tắc viết tên riêng) bằng tiếng Việt có dấu.

Lưu ý rằng 3 thành phần này phân tách nhau bởi một dấu chấm và một dấu khoảng trắng.

* Sao chép bảng tự chấm điểm và tất cả các file trình chiếu (file báo cáo kết quả) vào thư mục vừa tạo
* Nén toàn bộ thư mục nói trên (“LHPM<TT Lớp>. <TT Sinh viên>. <Họ và tên>”) thành một file nén và gửi cho giảng viên qua email. Tiêu đề email như tên thư mục.

### Thời hạn nộp

Hạn chót để nộp bài: **23:59:59 thứ 7 ngày 10/10/2020** (theo giờ Hà Nội). Sau thời hạn đó (dù chỉ 1 phút), giảng viên sẽ không nhận bài.

# Đánh giá kết quả

### Nguyên tắc chung

Giảng viên đánh giá kết quả làm bài tập thực hành của sinh viên theo hai hình thức: nghe sinh viên trình bày trên lớp và chấm ở nhà theo nội dung báo cáo được gửi qua email.

Trước thời hạn nộp nêu trên, nếu sinh viên đã làm bài tập (có thể chưa đầy đủ tất cả bài tập cần thiết) và xung phong trình bày trước lớp thì sẽ được cộng điểm.

### Sinh viên trình bày kết quả trên lớp

Ở các buổi học sau thời hạn nộp kết quả làm bài tập thực hành, sinh viên phải luôn sẵn sàng cho việc trình bày kết quả trước lớp. Trình bày kết quả trước hết là trình bày theo slide đã chuẩn bị; và có thể bao gồm việc thực hiện lại (demo) quá trình làm bài tập thực hành.

Trên lớp, giảng viên sẽ chỉ định sinh viên bất kỳ trình bày một bài tập bất kỳ trong số những bài tập mà sinh viên đã báo cáo kết quả. Sinh viên sử dụng file trình chiếu đã chuẩn bị để trình bày bài thực hành được chỉ định. Mỗi bài tập được trình bày không quá 10 phút.

Trong một số trường hợp (khi thấy cần thiết), giảng viên sẽ yêu cầu sinh viên thực hiện lại trên lớp bài thực hành đã được chỉ định.

### Một số trường hợp đặc biệt

* Nếu sinh viên không thể làm lại được bài tập được chỉ định thì sẽ bị coi là gian lận và phải nhận 0 điểm.
* Sinh viên được chỉ định trình bày nhưng vắng mặt sẽ nhận 0 điểm.