**Họ tên: Trịnh Xuân Chinh – TH24.09**

**BÀI TẬP VÀ THỰC HÀNH HỌC PHẦN BẢO MẬT: (*BUỔI 2*)**

**Câu hỏi:**

1. Hãy nêu các kỹ thuật xâm phạm.

Các phương pháp tấn công cơ bản bao gồm

* Tìm mục tiêu và thu thập thông tin
* Truy cập ban đầu
* Leo thang quyền
* Lần vết khôi phục

Mục tiêu chính là giành được mật khẩu và sau đó dùng quyền truy cập của người sở hữu

1. Hãy nêu cách suy đoán mật khẩu, đưa ra các giải pháp bảo vệ mật khẩu.

Đoán mật khẩu là một trong các hướng tấn công chung nhất. Kẻ tấn công đã biết tên người sử dụng đăng nhập (từ trang email/web) và tìm cách đoán mật khẩu.

* + Mặc định, mật khẩu ngắn, tìm kiếm các từ chung
  + Thông tin của người dùng (thay đổi tên, ngày sinh, số điện thoại, các mối quan tâm và từ chung)
  + Tìm kiếm tổng thể mọi khả năng của mật khẩu

Kẻ xâm nhập kiểm tra đăng nhập với tệp mật khẩu đánh cắp được. Sự thành công của việc đoán mật khẩu phụ thuộc vào mật khẩu được chọn bởi người dùng. Tổng quan chỉ ra rằng nhiều người sử dụng chọn mật khẩu không cẩn thận.

Các giải pháp bảo vệ mật khẩu:

* + - độ dài tối thiểu > 6
    - đòi hỏi trộn chữ hoa và chữ thường, số và dấu chấm
    - không chọn từ trong từ điển
    - Tạo mật khẩu – máy tính tự sinh

1. Hãy nêu ra các nguyên nhân gây ra lỗ hổng cho máy tính. Cách khắc phục lỗ hổng đó.

- Lỗi bảo vệ hệ thống bằng mật khẩu

Lỗi này là lỗ hổng đầu tiên cho phép người truy cập bỏ qua hoặc giả mạo quy trình xác thực trước khi tiến vào bên trong hệ thống (đăng nhập vào hệ thống).

* Mật khẩu truy cập yếu
* Lỗi đặt mật khẩu thông dụng (123456, admin, iloveyou,...).
* Lỗi đặt mật khẩu quá ngắn: kẻ tấn công có thể dùng các công cụ quét mật khẩu và dễ dàng tìm ra mật khẩu để truy cập vào hệ thống.
* Xác thực chỉ một lớp (chỉ cần mật khẩu để đăng nhập).
* Cấp quyền truy cập không hợp lý.
* Thời gian kết thúc phiên không được cấu hình hoặc quá lâu.

Cách khắc phục là đặt mật khẩu từ 6 kí tự trở lên, bao gồm ít nhất 1 kí tự in hoa, kí tự thường, kí tự đặc biệt, chữ số. Không đặt mật khẩu trùng với các tài khoản khác

1. Hãy nêu ra tầm quan trọng của bức tường lửa. Cách bảo mật của bức tường lửa.

**Tường lửa (Firewall)** là một bức rào chắn giữa mạng nội bộ (local network) với một mạng khác (chẳng hạn như Internet), điều khiển lưu lượng ra vào giữa hai mạng này. Nếu như không có tường lửa thì lưu lượng ra vào mạng nội bộ sẽ không chịu bất kỳ sự điều tiết nào, còn một khi tường lửa được xây dựng thì lưu lượng ra vào sẽ do các thiết lập trên tường lửa quy định.

**Cách bảo mật của tường lửa:** một tường lửa có thể lọc lưu lượng từ các nguồn truy cập nguy hiểm như hacker, một số loại virus tấn công để chúng không thể phá hoại hay làm tê liệt hệ thống của bạn. Ngoài ra vì các nguồn truy cập ra vào giữa mạng nội bộ và mạng khác đều phải thông qua tường lửa nên tường lửa còn có tác dụng theo dõi, phân tích các luồng lưu lượng truy cập và quyết định sẽ làm gì với những luồng lưu lượng đáng ngờ như khoá lại một số nguồn dữ liệu không cho phép truy cập hoặc theo dõi một giao dịch đáng ngờ nào đó.

Do đó, việc thiết lập tường lửa là hết sức quan trọng, đặc biệt là đối với những máy tính thường xuyên kết nối internet.

5. Nêu ra các phương pháp tấn công web. Kể tên những phần mềm thường dùng để bảo vệ web.

**Bài tập:**

Hoàn thiện các bài tập ở chương 2 (Buổi 2)