Bài: 1.8 Giới thiệu về Ethical Hacking - Định lượng điểm yếu

Xem bài học trên website để ủng hộ Kteam: 1.8 Giới thiệu về Ethical Hacking - Định lượng điểm yếu

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Định lượng điểm yếu

Đây là quá trình **kiểm tra, nhận dạng, phân tích khả năng của thiết bị** bao gồm quá trình thực thi bảo mật trên hệ thống để chống lại những mối đe dọa. Qua việc định lượng điểm yếu, ta có thể xác định chỗ nào còn thiếu sót, những mối đe dọa tới hệ thống, phạm vi của điểm yếu, ước tính tính cần thiết và hiệu quả của các biện pháp bảo mật bổ sung.

Các loại định lượng điểm yếu

Sau đây là các loại định lượng điểm yếu

1. Định lượng chủ động (Active assessment)
2. Định lượng bị động (Passive assessment)
3. Định lượng Host-based (Host-based assessment)
4. Định lượng nội bộ (Internal assessment)
5. Định lượng bên ngoài (external assessment)
6. Định lượng mạng
7. Định lượng mạng wifi
8. Định lượng ứng dụng

Phương pháp định lượng điểm yếu mạng

Định lượng mạng là **sự kiểm tra khả năng xảy ra cuộc tấn công và khả năng điểm yếu có thể tồn tại trong hệ thống** mạng. Dưới đây là những bước của định lượng yếu điểm:

1. Thu thập (Acquisition)
2. Nhận dạng (Identification)
3. Phân tích (analyzing)
4. Ước lượng (evaluation)
5. Làm báo cáo (Generate reports)

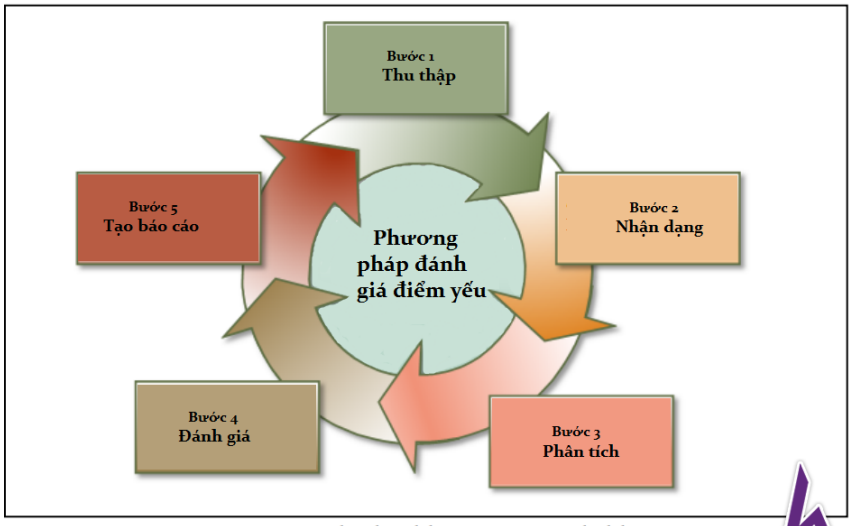

Figure 1-13 Network Vulnerability Assessment Methodology

Thu nhập: chuẩn bị và bước đầu đánh giá điểm yếu, luật lệ và quy trình liên quan đến định lượng điểm yếu

Nhận dạng: trong bước này, cần tương tác với khác hàng, nhân viên, quản lý hoặc những người khác liên quan tới thiết kế cấu trúc mạng để tập hợp thông tin công nghệ.

Phân tích: đánh giá những thông tin đã thu thập được dưới dạng tài liệu sưu tầm hoặc sự tương tác một đối một. Công đoạn phân tích cơ bản thường là:Đánh giá thông tin

- Phân tích những kết quả xác định điểm yếu trước đó
- Định lượng nguy cơ
- Phân tích nguy cơ và điểm yếu
- Ước lượng tính hiệu quả của luật bảo mật hiện hành.

Ước lượng:

Công đoạn này bao gồm:

- Xem xét những điểm yếu đã được phát hiện
- Nhận dạng lỗ hổng, khoảng trống trong bảo mật hiện hành
- Xác định kiểm soát bảo mật cần thiết để giải quyết vấn đề và điểm yếu
- Nhận dạng những gì cần nâng cấp, điều chỉnh.

Tạo báo cáo:

Là công đoạn **cung cấp tài liệu từ những bản báo cáo nháp cho việc xem xét về sau**. Báo cáo này hỗ trợ ta nhận dạng điểm yếu trong công đoạn thu thập. Những báo cáo được thu thập cũng quan trọng trong việc kiểm tra và thử nghiệm. Mỗi khi cần điều chỉnh trong cơ chế bảo mật, những báo cáo này giúp ta thiết kế hệ thống bảo mật. Cơ sở dữ liệu trung tâm thường nắm giữ các báo cáo này.

Báo cáo bao gồm :

- Nhiệm vụ của mỗi cá nhân trong tổ
- Phương pháp và công cụ đã dùng
- Những gì đã khám phá
- Lời khuyên
- Những thông tin thu thập từ nhiều công đoạn khác nhau
- Sơ đồ tư duy

Mindmap