

SỞ GIÁO DỤC VÀ ĐÀO TẠO
THÀNH PHỐ HỒ CHÍ MINH
TÊN ĐƠN VỊ: TRƯỜNG
CAO ĐẲNG LÝ TỰ TRỌNG
TP. HỒ CHÍ MINH

BẢN MÔ TẢ NỘI DUNG CƠ BẢN CỦA SÁNG KIẾN

Tên Sáng kiến:

KHAI THÁC MÃ LỖI TRONG WINDOWS ĐỂ CHIẾM QUYỀN HỆ THỐNG

Tác giả:

Chức vụ:

Đơn vị công tác:

1. Thực trạng

Theo đánh giá từ các Nhà chuyên môn về lĩnh vực an ninh hệ thống thì các lỗ hổng bảo mật là những điểm yếu luôn tồn tại trên hệ thống hoặc ẩn chứa trong một dịch vụ hệ thống nào đó cung cấp, qua đó tin tặc có thể khai thác một số mã lỗi, từ đó xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Có nhiều nguyên nhân gây ra lỗ hổng bảo mật: Cấp quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể còn tồn tại ngay chính tại hệ điều hành như trong Windows, UNIX, hệ điều hành các thiết bị router, modem hoặc trong các ứng dụng thường xuyên sử dụng như word processing, các hệ Databases.

Do lỗi bản thân hệ thống, do người quản trị yếu, không am hiểu sâu các dịch vụ trong hệ thống, do người sử dụng có ý thức bảo mật kém. Nhìn chung, điểm yếu ở yếu tố con người cũng được xem là lỗ hổng bảo mật.

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng đến chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng đến toàn bộ hệ thống... các lỗ hổng bảo mật sẽ là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ trong hệ thống Windows.

Thiết nghĩ, đây là một trong những chuyên đề cần bổ sung và cập nhật vào khung chương trình giảng dạy cho học sinh – sinh viên chuyên ngành an ninh mạng tại khoa Công nghệ Thông tin, nhằm trang bị thêm cho các em những vấn đề chuyên sâu và mang tính ứng dụng cao.

Qua bài sáng kiến kinh nghiệm này, tôi muốn trình bày chi tiết về kỹ thuật khai thác lỗi bảo mật để học sinh - sinh viên tiếp cận một cách trực quan nhằm tạo hứng khởi trong học tập và chia sẻ thêm kinh nghiệm với đồng nghiệp cùng quan tâm và đóng góp ý kiến.

2. Nội dung sáng kiến

Sáng kiến bao gồm các đề mục với các đặc điểm sau:

- Nội dung là các công việc thiết thực và cần thiết trong thực tế.
- Có bài giải mẫu để HS-SV tham khảo
- Có video hướng dẫn thao tác mẫu.
- Các yêu cầu của mỗi đề mục đều bám sát các nội dung sau:

I- Cơ sở lý thuyết

1. Trình bày về kỹ thuật khai thác tấn công chủ động – thụ động

1.1 Tấn công chủ động

1.2 Tấn công thụ động

2. Mạo danh truy cập trái phép

3. Tấn công Man-in-the-Middle – Giả mạo ARP Cache

3.1 Man in the Middle

3.2 Giả mạo ARP cache

II- Thực nghiệm

III-Đánh giá và kiến nghị

3. Hiệu quả mang lại:

Sáng kiến kinh nghiệm (SKKN) được thử nghiệm từ năm học 2019-2020 đối với các lớp 19C2-QTM1 theo hình thức kết hợp lý thuyết với thực nghiệm tại lớp.

Sau khi áp dụng SKKN, sinh viên cảm thấy hào hứng và có hứng thú với môn học, các em hiểu và nắm bắt môn học có tính chiều sâu hơn. Đặc biệt, những gì đạt được do chính các em trải nghiệm tại lớp đã tiếp thêm sự yêu thích của môn học kỹ liên quan về bảo mật hệ thống.

Sáng kiến kinh nghiệm cũng nhằm bổ sung thêm vào kho kiến thức làm nguồn tư liệu cho các sinh viên, đặc biệt giúp cho các giảng có nguồn tài liệu tham khảo .

Các giảng viên có thể dùng SKKN như bài bài tập lớn hay đề tài của môn học để giao cho HS-SV.

❖ Kết quả áp dụng SKKN trên một số lớp 2019-2020:

STT	Lớp	Tỷ lệ xếp giỏi	Tỷ lệ xếp loại khá	Tỷ lệ xếp TB	Tỷ lệ xếp loại TB yếu	Tỷ lệ xếp loại kém
1	19C2-QTM1	3.5%	17.5%	73.5%		

Đánh giá phạm vi ảnh hưởng của Sáng kiến:

- ☒ Chỉ có hiệu quả trong phạm vi Đơn vị áp dụng.
- ☐ Đã được chuyển giao, nhân rộng việc áp dụng ra phạm vi sở, ngành theo chứng cứ đính kèm.
- ☐ Đã phục vụ rộng rãi người dân trên địa bàn Thành phố, hoặc đã được chuyển giao, nhân rộng việc áp dụng trên địa bàn Thành phố theo chứng cứ đính kèm.
- ☐ Đã phục vụ rộng rãi người dân tại Việt Nam, hoặc đã được chuyển giao, nhân rộng việc áp dụng tại nhiều tỉnh, thành theo chứng cứ đính kèm.

Bộ phận/Đơn vị áp dụng *Thành phố Hồ Chí Minh, ngày 20 tháng 01 năm 2021*

Người viết sáng kiến