ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TRẦN VĂN THẨM

NGHIÊN CỨU KHẢ NĂNG AN TOÀN CỦA HỆ ĐIỀU HÀNH MẠNG

Chuyên ngành: Khoa học máy tính
Mã số: 60.48.01

LUẬN VĂN THẠC SỸ

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS HỒ VĂN CANH

Thái Nguyên, tháng 9 năm 2012

LỜI CAM ĐOAN

Tôi xin cam đoan bản Luận văn là công trình nghiên cứu khoa học độc lập của tôi. Luận văn này không sao chép toàn bộ các tài liệu, công trình nghiên cứu của người khác. Tất cả các đoạn trích dẫn nằm trong các tài liệu, công trình nghiên cứu của người khác đều được ghi rõ nguồn và chỉ rõ trong tài liệu tham khảo.

Tôi xin cam đoan những điều trên là đúng sự thật, nếu sai, tôi xin chịu hoàn toàn trách nhiệm.

TÁC GIẢ LUẬN VĂN

TRẦN VĂN THẨM

LỜI CẢM ƠN

Đầu tiên em xin gửi lời cảm ơn chân thành tới các thầy, cô trường Đại học Công Nghệ Thông Tin và Truyền Thông – Đại Học Thái Nguyên đã nhiệt tình giảng dạy và truyền đạt kiến thức cho em trong thời gian học tập tại trường.

Em xin gửi lời cảm ơn sâu sắc tới thầy Hồ Văn Canh, người đã định hướng, hướng dẫn và hỗ trợ em rất nhiều để hoàn thành luận văn này.

Em xin gửi lời cảm ơn tới các anh chị đồng nghiệp và cảm ơn bạn bè cùng khóa, cùng trường đã nhiệt tình hỗ trợ trong thời gian làm luận văn.

Mặc dù đã rất cố gắng hoàn thành luận văn này, xong luận văn sẽ khó tránh khỏi những thiếu xót. Em rất mong nhận được sự nhận xét, góp ý, tận tình chỉ bảo từ các thầy, cô.

Một lần nữa, em xin chân thành cảm ơn tất cả mọi người!

TÁC GIẢ LUẬN VĂN

TRẦN VĂN THẨM

BẢNG KÝ HIỆU VIẾT TẮT

Ký hiệu	Dạng đầy đủ
AVC	AccessVector Cache
DAC	Discretionary Access Control
HĐH	Hệ điều hành
LSM	Linux Security Module
MAC	Mandatory Access Control
MLS	Multi Level Security
NSA	National System Agent
PSL	Polgen Specification Language
RBAC	Role Based Access Control
RHEL	Red Hat Enterprise Linux
RMP	Role Mining Problem
SELinux	Security Enhanced Linux
TE	Type Enforcement

MỤC LỤC

DANH MỤC HÌNH

LỜI MỞ ĐẦU

Trong khung cảnh thế giới truyền thông dữ liệu, kết nối Internet không quá đắt, sự phát triển của các phần mềm, thì bảo mật trở thành một vấn đề rất quan trọng. Hiện nay vấn đề bảo mật trở thành một yêu cầu cơ bản bởi vì việc tính toán mạng là hoàn toàn chưa được bảo mật. Ví dụ, khi dữ liệu được truyền từ điểm A sang điểm B qua Internet trên đường đi nó có thể phải qua một số điểm khác trên tuyến đó, điều này cho phép người sử dụng khác có cơ hội để chặn bắt, thay đổi nó. Thậm trí những người dùng trên hệ thống cũng có thể biến đổi dữ liệu thành dạng khác mà chúng ta không mong muốn. Sự truy nhập không được ủy quyền tới hệ thống có thể được thực hiện bởi kẻ xâm nhập trái phép (intruder) hay là "cracker", những kẻ này sử dụng các kiến thức tiên tiến để giả dạng, đánh cắp những thông tin hoặc từ chối truy nhập tới nguồn tài nguyên.

Sự đa dạng của các hệ điều hành làm tăng nguy cơ từ tội phạm tin học. Hàng năm chúng ta phải chứng kiến nhiều lỗ hổng bảo mật bị khai thác trong các hệ điều hành thay thế, các chương trình và các trình duyệt web, cùng với đó là việc lợi dụng các lỗ hổng ứng dụng. Những cuộc tấn công vào các hệ thống cũ còn tồn tại mà không thể vá được (dù vẫn đang được sử dụng rộng rãi) như Linux, Sun Solaris, Windows sẽ tiếp tục xảy ra.

Một cuộc chạy đua vũ trang về phòng vệ không gian mạng đã bắt đầu với khái niệm an ninh ở mọi cấp độ trong một hệ thống thông tin, và mức độ của hệ điều hành không phải là ngoại lệ.

Luận văn này sẽ tiếp cận về một khía cạnh của vấn đề bảo mật, đó là trên hệ điều hành mã nguồn mở, đi sâu vào đơn giản hóa SELinux cho các máy chủ Internet sử dụng các hệ điều hành bảo mật với phương án làm giảm số lượng chính sách bảo mật cần phải viết cho một máy chủ Internet mà vẫn đảm bảo giữa được tính năng bảo mật nâng cao của SELinux so với hệ thống bảo mật Linux chuẩn. Ngoài ra luận văn đề cập đến việc sinh tự động các chính sách của SELinux bằng bộ công cụ Polgen và xây dựng một chương trình phân tích để người sử dụng hiểu rõ các chính sách đó mà không cần kiến thức chuyên sâu về SELinux. Nhờ đó phục vụ mục tiêu là giúp cho việc quản trị hệ thống SELinux được tốt hơn.

Chương 1. VẤN ĐỀ AN NINH, AN TOÀN CỦA HỆ ĐIỀU HÀNH

Trong chương này đề cập đến những vấn đề bảo mật mà người quản trị hệ thống phải đối mặt. Nó bao trùm những triết lý bảo mật chung, đồng thời đưa ra một số ví dụ về cách thức bảo mật hệ thống nhằm chống những người xâm phạm hệ thống mà không được phép.

1.1. Vấn đề an toàn đối với công ty toàn cầu

Việc các trung tâm dữ liệu đứng độc lập cùng với các yêu cầu an toàn hoàn toàn tập trung đang giảm đi nhanh chóng trong các môi trường tính toán tập thể hiện đại đã được nói đến nhiều. Các môi trường phân tán hiệu năng cao và ưu thế hơn về giá cả, trong đó các hệ thống khách được tách khỏi các server trên mạng đang không ngừng tăng lên. Thêm vào đó, các mối liên kết giữa các tổ chức thương mại, cá nhân và chính phủ trên toàn thế giới đang mở rộng cộng đồng người dùng, họ có khả năng truy nhập tới những tài nguyên nội bộ của công ty.

Đồng thời, những người dùng ngày càng thông thạo và phức tạp hơn. Đáng tiếc, một số người đã dùng hiểu biết của họ với những mục đích không chính đáng. Mặc dù những hacker nổi tiếng luôn được đăng tải trên thông tin đại chúng, nhưng các nghiên cứu cho thấy phần lớn những hành động xâm phạm máy tính không bị phát hiện. Những xu hướng này đã làm nảy sinh những thay đổi về căn bản trong các yêu cầu an toàn đối với liên kết toàn cầu.

Không có gì ngạc nhiên khi mà an toàn nổi lên như là một vấn đề cốt lõi đối với các công ty mong muốn tận dụng những lợi ích trong việc thực thi các hệ thống phân tán toàn cầu, mà không làm nguy hiểm tới tính bí mật và toàn vẹn của thông tin nhạy cảm. Vì thế, những người quản trị hệ thống và mạng phải có khả năng lựa chọn những sản phẩm đáp ứng đầy đủ các tính năng nhằm vào những nhu cầu an toàn hay thay đổi của họ.

1.2. Chúng ta đang cố gắng bảo vệ những gì?

Trước khi chúng ta cố gắng thực hiện bảo vệ hệ thống, chúng ta phải xác định mức đe dọa nào cần bảo vệ, những rủi ro nào có thể nhận được, và sự nguy hiểm nào mà hệ thống phải chịu. Chúng ta nên phân tích hệ thống để biết những gì cần bảo vệ, tại sao bảo vệ nó, giá trị của nó, và người chịu trách nhiệm về dữ liệu của chúng ta.

- ***Sự rủi ro (risk)*** có thể do người truy nhập trái phép thành công khi cố gắng truy nhập máy tính của bạn. Họ có thể đọc hoặc ghi các tệp, hoặc thực thi các chương trình gây ra thiệt hại không? Họ có thể xóa dữ liệu không? Họ có thể cản trở bạn hoặc công ty bạn làm một số việc quan trọng không? Đừng quên: một người nào đó truy nhập vào tài khoản của bạn, hoặc hệ thống của bạn, có thể giả dạng là bạn...

Hơn nữa, có một tài khoản không an toàn trên hệ thống của bạn có thể gây nên toàn bộ mạng của bạn bị thỏa hiệp. Nếu bạn cho phép một người dùng đăng nhập sử dụng tệp hosts, hoặc sử dụng một dịch vụ không an toàn như là ftp, như vậy là bạn đã tạo cho người truy nhập trái phép bước chân vào cánh cửa hệ thống của bạn. Người truy nhập trái phép có một tài khoản người dùng trên hệ thống của bạn hoặc hệ thống của một người khác, nó có thể được sử dụng để truy nhập tới hệ thống khác hoặc tài khoản khác.

- ***Đe dọa (threat)*** là một điển hình của một ai đó với động cơ để đạt được sự truy nhập không được ủy quyền tới mạng hoặc máy tính của bạn. Bạn phải xác định ai mà bạn tin tưởng có quyền truy nhập tới hệ thống của bạn, và mối đe dọa nào có thể xảy ra. Có một vài dạng xâm nhập trái phép, bạn nên nhớ các đặc tính khác nhau của chúng khi bạn đang bảo vệ hệ thống của bạn.

- ***Tò mò (curious)*** - là một kiểu intruder thích tìm ra các kiểu hệ thống và dữ liệu mà bạn có.

- **Độc ác (malicious)** - kiểu intruder này xóa trang web của bạn hoặc bắt bạn phải mất nhiều thời gian, tiền bạc để khôi phục lại dữ liệu đã bị gây thiệt hại bởi anh ta.