GIỚI THIỆU ĐỀ TÀI NHÓM 7

**XÂY DỰNG HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS-SNORT TRÊN LINUX**

An ninh thông tin nói chung và an ninh mạng nói riêng đang là vấn đề được quan tâm không chỉ ở Việt Nam mà trên toàn thế giới. Cùng với sự phát triển nhanh chóng của mạng Internet, việc đảm bảo an ninh cho các hệ thống thông tin càng trở nên cấp thiết hơn bao giờ hết.

Trong lĩnh vực an ninh mạng, phát hiện và phòng chống tấn công xâm nhập cho các mạng máy tính là một vấn đề cần thiết. Ngoài việc tăng cường chính sách bảo mật trong hệ thống, các tổ chức cần phải xác định rằng việc tăng các liên kết cũng làm tăng sự nguy hiểm với các dữ liệu quan trọng như việc sao chép dữ liệu, nghe trộm việc truyền nhằm lấy dữ liệu quan trọng.

Có rất nhiều giải pháp được đưa ra và để hạn chế những vấn đề nói trên tôi đã chọn đề tài “Xây dựng h*ệ thống phát hiện xâm nhập IDS – SNORT trên Linux*” để nghiên cứu.

Sơ lược về đề tài sẽ trình bày như sau:

* Tìm hiểu về bảo mật
* Nghiên cứu những phương pháp xâm nhập hệ thống– biện pháp ngăn ngừa
* Nghiên cứu về hệ thống phát hiện xâm nhập IDS
* Nghiên cứu công cụ IDS – Snort
* Xây dựng hệ thống Snort – IDS trên Linux

Theo đó, kết quả của đề tài chúng tôi muốn đạt được là phải:

* Biết được thông tin về bảo mật
* Biết cách tổng hợp và phân tích hệ thống phát hiện xâm nhập IDS.
* Nghiên cứu được các vấn đề liên quan đến chương trình snort.
* Sử dụng tốt hệ điều hành Linux
* Biết được phương pháp và triển khai cài đặt Snort trên Linux

Và bố cục đề tài gồm 5 chương:

* Chương I: Tổng quan về bảo mật
* Những nguy cơ đe dọa đối với bảo mật.
* Các phương pháp xâm nhập hệ thống – Biện pháp phát hiện và ngăn ngừa.
* Các giải pháp bảo mật an toàn cho hệ thống.
* Chương II: Hệ thống phát hiện xâm nhập IDS
* Tìm hiểu về kiến trúc và nguyên lý hoạt động của IDS.
* Phân loại IDS, phương thức phát hiện và cơ chế hoạt động IDS.
* Cách phát hiện kiểu tấn công thông dụng của IDS.
* Chương III: Triển khai ứng dụng dò tìm xâm nhập trên hệ thống Linux dựa trên Snort.
* Kiến trúc Snort.
* Bộ luật Snort.
* Chương IV: Demo
* Demo tấn công
* Demo phát hiện
* Chương V: Kết luận