HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Anh Tú

XÂY DỰNG HỆ THỐNG GIÁM SÁT MẠNG DÀNH CHO BỆNH VIỆN ĐA KHOA CẤP TỈNH VỚI MÃ NGUỒN MỞ

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

THÀNH PHỐ HỒ CHÍ MINH – NĂM 2022

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. Đàm Quang Hồng Hải

(Ghi rõ học hàm, học vị)

Phản biện 1: ……

Phản biện 2: ……..

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng ..... năm.....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

MỞ ĐẦU

1. Lý do chọn đề tài

Công nghệ thông tin là phương tiện trợ giúp đắc lực và có hiệu quả cao trong công tác quản lý nền hành chính nói chung và quản lý ngành y tế nói riêng. Vì vậy, việc ứng dụng công nghệ thông tin trong công tác quản lý bệnh viện là một yêu cầu cấp bách nhằm góp phần nâng cao chất lượng, hiệu quả của công tác quản lý bệnh viện, thúc đẩy bệnh viện phát triển toàn diện, từng bước đáp ứng được yêu cầu về khám chữa bệnh và chăm sóc sức khỏe cho nhân dân.

Ứng dụng công nghệ thông tin trong ngành y tế gần như là điều bắt buộc để tiến tới xây dựng nền y tế thông minh. Số hóa và ứng dụng CNTT trong y tế giúp cắt giảm thủ tục hành chính cho công tác quản lý.

Những lợi ích mà CNTT mang lại là rất lớn cả về ý nghĩa kinh tế và xã hội, nhưng bên cạnh đó cũng tồn tại những thách thức đảm bảo về bảo mật và an toàn thông tin, nguy cơ bị mất ATTT như: Các tấn công vào dữ liệu hồ sơ điện tử của ngành chăm sóc sức khỏe và hệ thống cơ sở dữ liệu của ngành Y tế.

Trong lĩnh vực y tế cũng như với hầu hết các ngành nghề rủi ro bảo mật là rất lớn: Những cuộc tấn công lấy cắp hồ sơ y tế điện tử, dẫn đến lộ, lọt thông tin cá nhân nhạy cảm về sức khỏe và có nguy cơ đe dọa đến tính mạng con người.

Chính vì vậy, công tác bảo mật, an toàn thông tin trong ngành y tế nói chung, thông tin khám bệnh chữa bệnh của người bệnh nói riêng là vô cùng quan trọng.

Trước những yêu cầu đó, học viên chọn phần mềm Snort để thiết kế ứng dụng giám sát trực tuyến. Học viên chọn thực hiện đề tài **"Xây dựng hệ thống giám sát mạng dành cho Bệnh viện Đa khoa cấp tỉnh với mã nguồn mở."**

2. Tổng quan về vấn đề nghiên cứu

Trước xu hướng số hóa dịch vụ khám chữa bệnh, điển hình như triển khai y bạ điện tử, khám chữa bệnh từ xa, và số hóa dữ liệu y tế đặt ra yêu cầu cấp thiết cho các cơ sở y tế phải thiết lập cơ chế bảo vệ mạng nội bộ. Điều đó, đòi hỏi lãnh đạo cơ sở y tế phải nghiên cứu, thảo luận để sớm có chính sách về quản trị dữ liệu nói chung và dữ liệu sức khỏe nói riêng, có trách nhiệm ban hành quy chế nội bộ của đơn vị.

Nhằm thực hiện hoạt động khám chữa bệnh từ xa, quản lý đăng nhập hệ thống, sao lưu dữ liệu của hoạt động tư vấn khám bệnh, chữa bệnh từ xa, bảo mật thông tin, chống phần mềm độc hại, xử lý khẩn cấp khi xảy ra sự cố bảo mật, hệ thống thông tin mạng bị tấn công…Đây là nhóm dữ liệu có độ nhạy cảm cao, nếu không bảo mật, việc lộ thông tin sức khỏe có thể ảnh hưởng uy tín của cơ sở khám chữa bệnh, đến hạnh phúc của gia đình.

IDS ngày càng trở nên phổ biến và đóng vai trò quan trọng không thể thiếu trong bất ký chính sách bảo mật và an toàn thông tin của bất kỳ hệ thống thông tin nào.

Học viên xây dựng hệ thống phát hiện bất thường bằng cách sử dụng phần mềm phát hiện xâm nhập Snort. Đây là một hệ thống phát hiện và ngăn chặn đột nhập mạng mã mở được sử dụng rộng rãi.

3. Mục đích nghiên cứu

- Tìm hiểu về cách thức hoạt động và cách thức phát hiện xâm nhập của hệ thống IDS/IPS.

- Nghiên cứu và tìm hiểu cấu trúc tập luật, cách thức xử lý gói tin của Snort.

- Xây dựng, phát triển hệ thống phân tích, quản lý, giám sát hệ thống mạng dựa trên công cụ Snort, từ đó đưa ra các cảnh báo.

- Đồng thời, thu thập các thông tin về quá trình xâm nhập, tiến hành ghi và lưu trữ log, hỗ trợ cho việc phân tích và xem xét nguy cơ bị tấn công về sau.

4. Đối tượng và phạm vi nghiên cứu

- Đối tượng nghiên cứu: Phần mềm phát hiện xâm nhập Snort, các công cụ thu thập, phân tích log và cảnh báo.

+ Các chương trình phần mềm mở phát hiện xâm nhập

+ Các chương trình phần mềm mở phòng chống xâm nhập

+ Các chương trình phần mềm mở giám sát lưu lượng của hệ thống mạng

+ Các chương trình phần mềm mở giám sát thiết bị mạng và các dịch vụ mạng.

- Phạm vi nghiên cứu: Hệ thống mạng nội bộ tại cơ quan nơi học viên đang công tác.

5. Phương pháp nghiên cứu

- Nghiên cứu về lý thuyết phát hiện xâm nhập thông qua các tài liệu, các bài báo cáo.

- Nghiên cứu lý thuyết về Snort thông qua trang chủ của Snort, tài liệu hướng dẫn cho người sử dụng từ các nguồn khác.

- Phương pháp nghiên cứu có chọn lọc các tài liệu và kế thừa kết quả nghiên cứu của các đề tài nghiên cứu khoa học và các dự án khác có liên quan.

6. Dự kiến nội dung của luận văn

Chương 1: Cơ sở lý luận

Chương 2: Khảo sát hệ thống mạng hiện tại và phân tích nhu cầu bảo mật của Bệnh viện.

Chương 3: Nghiên cứu đề xuất xây dựng hệ thống giám sát Snort trực tuyến cho hệ thống mạng Bệnh viện.

Chương 4: Thực nghiệm và đánh giá

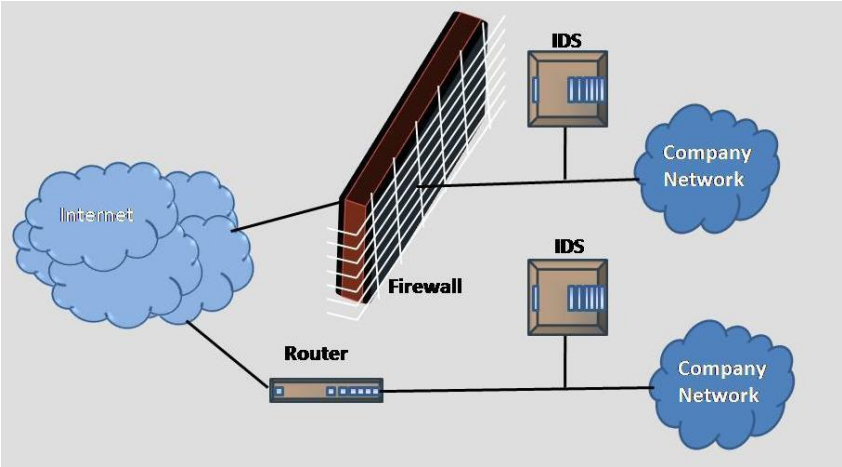
Chương 5: Kết luận và hướng phát triển

CHƯƠNG 1: CƠ SỞ LÝ LUẬN

Giới thiệu khái quát về IDS/IPS, công cụ để xây dựng hệ thống giám sát mạng Snort.

1.1 Giới thiệu về IDS

Hệ thống phát hiện xâm nhập được xây dựng để bảo vệ các tài nguyên của hệ thống mạng trước những Hacker không mong muốn.



Hình 1.1: Hệ thống phát hiện xâm nhập IDS

1.1.1 Khái niệm IDS

Hệ thống phát hiện xâm nhập - IDS (Intrusion Detection Systems) là phần mềm hoặc công cụ giúp bảo mật hệ thống và cảnh báo lỗi khi có các hành vi đáng ngờ xâm nhập vào hệ thống. Mục đích chính của IDS là ngăn ngừa và phát hiện những hành động phá hoại tính bảo mật của hệ thống hoặc những hành vi như dò tìm, quét các cổng.

IDS có hai chức năng chính là phát hiện các cuộc tấn công và cảnh báo các cuộc tấn công đó. Có hai phương pháp khác nhau trong việc phân tích các sự kiện để phát hiện các vụ tấn công: Phát hiện dựa trên các dấu hiệu và phát hiện sự bất thường.

1.1.2 Kiến trúc của hệ thống phát hiện xâm nhập IDS

- Thành phần thu thập gói tin (information collection).
- Thành phần phân tích gói tin (Detection).

- Thành phần phản hồi (Response) nếu gói tin đó được phát hiện là một cuộc tấn công.

1.1.2.1 Cảm biến (Sensor)

Bộ phận làm nhiệm vụ phát hiện các sự kiện có khả năng đe dọa an ninh của hệ thống mạng, Sensor có chức năng quét nội dung của các gói tin trên mạng, so sánh nội dung với các mẫu và phát hiện ra các dấu hiệu tấn công.

1.1.2.2 Agent

Thành phần giám sát và phân tích các hoạt động. "Sensor" thường được dùng cho dạng Network-base IDS/IPS trong khi "Agent" thường được dùng cho dạng Host-base IDS/IPS. Sensor/Agent là các bộ cảm biến được đặt trong hệ thống nhằm phát hiện những xâm nhập hoặc các dấu hiệu bất thường trên toàn mạng.

1.1.2.3 Trung tâm điều khiển (Console)

Thành phần phát hiện là bộ phận làm có nhiệm vụ giám sát các sự kiện, các cảnh báo được phát hiện và sinh ra từ Sensor và điều khiển hoạt động của các bộ Sensor.

1.1.2.4 Engine

Engine có nhiệm vụ ghi lại tất cả các báo cáo về các sự kiện được phát hiện bởi các Sensor trong một cơ sở dữ liệu và sử dụng hệ thống các luật để đưa ra các cảnh báo trên các sự kiện nhận được cho hệ thống hoặc cho người quản trị.

1.1.2.5 Thành phần cảnh báo (Alert Notification)

Thành phần cảnh báo có chức năng gửi những cảnh báo tới người quản trị.

Trong các hệ thống IDS hiện đại, lời cảnh báo có thể xuất hiện ở nhiều dạng như: cửa sổ pop - up, tiếng chuông, mail, …

1.1.3 Chức năng IDS/IPS: Hệ thống phát hiện xâm nhập cho phép các tổ chức bảo vệ hệ thống khỏi những đe dọa với việc gia tăng kết nối mạng và sự tin cậy của hệ thống thông tin. Các IDS là lớp phòng vệ bổ sung, đảm bảo an toàn cho hệ thống thông tin

Quan trọng nhất trong chức năng của IDS là: *Giám sát, Cảnh báo, Bảo vệ.*

1.1.4 Phân loại IDS/IPS

- NIDS (Network Intrusion Detection Systems): Phát hiện xâm nhập trên toàn hệ thống mạng, được đặt tại một điểm chiến lược hoặc những điểm giám sát lưu lượng traffic đến và đi từ các thiết bị trên mạng.

- HIDS (Host Intrusion Detection Systems): hệ thống phát hiện xâm nhập này chạy trên máy chủ riêng hoặc một thiết bị đặc biệt trên mạng.

- NNIDS (Network node Intrusion detection system): Kết hợp giữa HIDS và NIDS.

- HIDS và NIDS đều có những ưu và nhược điểm khác nhau

Hệ thống phát hiện xâm nhập NIDS và HIDS	
NIDS	**HIDS**
Phạm vi rộng (trên toàn hệ thống mạng)	Phạm vi hẹp (Chỉ trên một máy xác định)
Cài đặt phức tạp	Dễ cài đặt
Tốt cho việc phát hiện xâm nhập từ bên ngoài mạng	Tốt cho việc phát hiện xâm nhập từ bên trong mạng
Tốn kém	Ít tốn kém hơn
Phát hiện trên cơ sở những thứ được ghi lại trên toàn hệ thống mạng	Phát hiện dựa vào bản ghi nhật ký hệ thống trên chỉ máy đó
Kiểm tra phần đầu (header) của gói tin	Không kiểm tra phần (header) của gói tin
Trả lời gần như ngay lập tức	Chỉ trả lời sau khi một hành động trái phép cố gắng thực hiện
Không phụ thuộc hệ điều hành	Phụ thuộc hệ điều hành
Dò tìm tấn công bằng cách phân tích dữ liệu trong gói tin	Dò tìm các cuộc tấn công tại chỗ trước khi nó ra khỏi hệ thống mạng
Dò tìm các cố gắng tấn công	Kiểm tra sự thành công và thất bại của một cuộc tấn công

Hình 0.1: So sánh Hệ thống phát hiện xâm nhập NIDS và HIDS

1.1.5 Ưu và nhược điểm của IDS

- Ưu điểm:

- Thích hợp sử dụng để thu thập số liệu, bằng chứng phục vụ công tác điều tra và ứng cứu sự cố.
- Đem đến cái nhìn bao quát, toàn diện về toàn bộ hệ thống mạng.
- Là công cụ thích hợp phục vụ việc kiểm tra các sự cố trong hệ thống mạng.

➢ Nhược điểm:

- Cần được cấu hình hợp lý, nếu không sẽ gây ra tình trạng báo động nhầm
- Khả năng phân tích traffic mã hóa tương đối thấp.
- Chi phí phát triển và vận hành hệ thống tương đối cao

1.1.6 Quy trình hoạt động của IDS

Bước 1: Hệ thống sẽ thực hiện theo dõi, giám sát toàn bộ hoạt động của lưu lượng mạng, các hoạt động bất thường.

Bước 2: Hệ thống IDS sẽ cảnh báo nếu phát hiện có ai xâm nhập cho người quản trị.

Bước 3: Thực hiện bảo vệ hệ thống.

Bước 4: Khi giao diện điều khiển lệnh nhận được cảnh báo nó sẽ gửi thông báo cho một người hoặc một nhóm đã được chỉ định từ trước (thông qua email, cửa sổ popup, trang web v.v…).

Bước 5: Phản hồi được khởi tạo theo quy định ứng với dấu hiệu xâm nhập này.

Bước 6: Các cảnh báo được lưu lại để tham khảo trong tương lai (trên địa chỉ cục bộ hoặc trên cơ sở dữ liệu).

Bước 7: Một báo cáo tóm tắt về chi tiết của sự cố được tạo ra.

Bước 8: Cảnh báo được so sánh với các dữ liệu khác để xác định xem đây có phải là cuộc tấn công hay không.

1.2 Hệ thống Snort IDS

Snort là một sản phẩm NIDS mã nguồn mở với hệ thống signature database (được gọi là rule database), được thiết kế chính để thao tác bằng dòng lệnh.

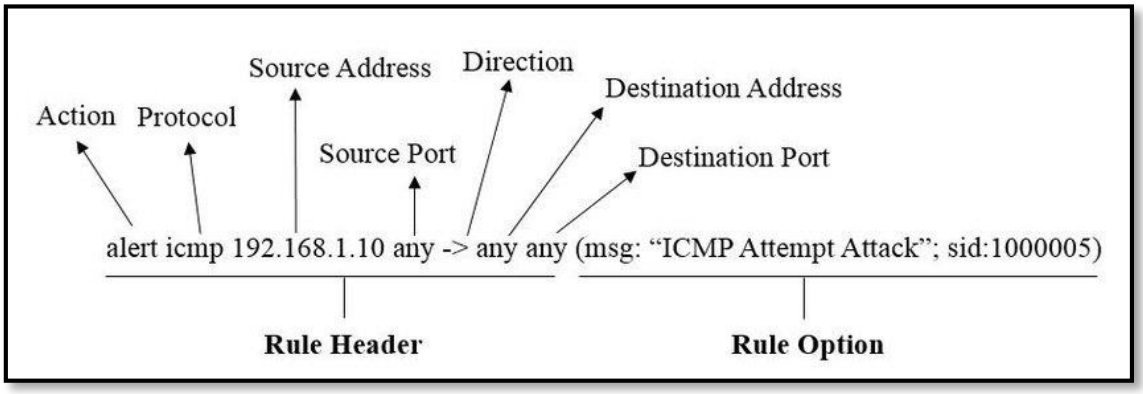
1.2.1 Giới thiệu

Snort được phát triển từ năm 1998. Ban đầu nó chỉ được mong đợi với chức năng sniffer. Hiện nay Snort có thể chạy trên nhiều hệ thống nền như Windows, Linux, OpenBSD, FreeBSD, NetBSD, Solaris, HP-UX, AIX, IRIX, MacOS. Với kiến trúc thiết kế theo kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình bằng việc cài đặt hay viết thêm mới các module.

1.2.2 Luật trong Snort

Hệ thống phát hiện của Snort hoạt động dựa trên các luật (rules) và các luật này lại được dựa trên các dấu hiệu nhận dạng tấn công. Các luật có thể được áp dụng cho tất cả các phần khác nhau của một gói tin dữ liệu .Một luật có thể được sử dụng để tạo nên một thông điệp cảnh báo, log một thông điệp hay có thể bỏ qua một gói tin.

Luật trong Snort được chia làm 2 phần: Header và Option.



Hình 1.11: Luật trong Snort

1.2.2.1 Các thành phần Header của luật

a) *Hành động của luật (Rule Action):* Là phần đầu tiên của luật, chỉ ra hành động nào được thực hiện khi mà các điều kiện của luật được thoã mãn.

b) *Protocols:* Là phần thứ hai của một luật có chức năng chỉ ra loại gói tin mà luật sẽ được áp dụng.

c) *Address:* Địa chỉ có thể là địa chỉ của một IP đơn hoặc là địa chỉ của một mạng. Các địa chỉ này được dùng để kiểm tra nguồn sinh ra và đích đến của gói tin.

d) *Ngăn chặn địa chỉ hay loại trừ địa chỉ:* Snort cung cấp cho ta kĩ thuật để loại trừ địa chỉ bằng cách sử dụng dấu phủ định (dấu !).

e) *Danh sách địa chỉ:* Chúng ta có thể định rõ ra danh sách các địa chỉ trong một luật của Snort.

f) *Cổng (Port Number):* Số hiệu cổng dùng để áp dụng luật cho các gói tin đến từ hoặc đi đến một cổng hay một phạm vi cổng cụ thể nào đó.

g) *Dãy cổng hay phạm vi cổng:* Ta có thể áp dụng luật cho dãy các cổng thay vì chỉ cho một cổng nào đó. Cổng bắt đầu và cổng kết thúc phân cách nhau bởi dấu hai chấm ":".

h) *Hướng — Direction:* Chỉ ra đâu là nguồn đâu là đích, có thể là ➔ hay ➔ hoặc <>. Trường hợp <> là khi ta muốn kiểm tra cả Client và Server.

1.2.2.2 Các thành phần Option của luật

Phần Rule Option nằm ngay sau phần Rule Header và được bao bọc trong dấu ngoặc đơn.

Nếu nhiều Option được sử dụng thì các Option này phải đồng thời được thoã mãn tức là theo logic các Option này liên kết với nhau bằng AND.

Mọi option được định nghĩa bằng các từ khoá. Một số các option còn chứa các tham số. Nói chung một option gồm 2 phần: Một từ khoá và một tham số, hai phần này phân cách nhau bằng dấu hai chấm.

1.2.3 Kiến trúc và cơ chế hoạt động của Snort

Kiến trúc của Snort bao gồm nhiều thành phần, với mỗi thành phần có một chức năng riêng. Các phần chính đó là:

1.2.3.1 Module giải mã gói tin (Packet Decoder): Snort sử dụng thư viện pcap để bắt mọi gói tin trên mạng lưu thông qua hệ thống. Một gói tin sau khi được giải mã sẽ được đưa tiếp vào Module tiền xử lý.

1.2.3.2 Module tiền xử lý (Preprocessors): Module tiền xử lý là một Module rất quan trọng đối với bất kỳ một hệ thống IDS nào để có thể chuẩn bị gói dữ liệu đưa và cho Module Phát hiện phân tích.

1.2.3.3 Module phát hiện (Detection Engine): phát hiện bất kì dấu hiệu tấn công nào tồn tại trong gói tin bằng cách sử dụng các rule để đối chiếu với thông tin trong gói tin.

1.2.3.4 Module Log và Cảnh báo (Logging and Alerting System): Khi bộ phận Detection engine phát hiện ra các dấu hiệu tấn công thì nó sẽ thông báo cho bộ phận Logging and Alerting System. Các ghi nhận, thông báo có thể được lưu dưới dạng văn bản hoặc một số định dạng khác. Mặc định thì chúng được lưu tại thư mục ./var/log/snort.

1.2.3.5 Module kết xuất thông tin (Output Module): Module này có thể thực hiện các thao tác khác nhau tùy theo việc bạn muốn lưu kết quả xuất ra như thế nào.

1.2.4 Chế độ hoạt động của Snort

1.2.4.1 Snort Sniffer mode: Snort hoạt động như một chương trình thu thập và phân tích gói tin thông thường. Không cần sử dụng file cấu hình, các thông tin Snort sẽ thu được khi hoạt động ở chế độ này.

1.2.4.2 Packet logger mode: Snort sẽ tập hợp tất cả các packet nó thấy được và đưa vào log theo cấu trúc phân tầng. Một thư mục mới sẽ được tạo ra ứng với mỗi địa chỉ nó bắt được, và dữ liệu sẽ phụ thuộc vào địa chỉ mà nó lưu trong thư mục đó.

1.2.4.3 NIDS mode: Snort thường được sử dụng như một NIDS. Khi phát hiện có dấu hiệu tấn công ở trong gói tin thì nó sẽ ghi lại và tạo thông báo. Khi dùng ở chế độ này phải khai báo file cấu hình cho Snort hoạt động

1.2.4.4 Inline mode: Phiên bản chỉnh sửa từ Snort cho phép phân tích các gói tin từ Firewall Iptables sử dụng các tập lệnh mới như: Pass, drop, reject.

CHƯƠNG 2: KHẢO SÁT HỆ THỐNG MẠNG HIỆN TẠI VÀ PHÂN TÍCH NHU CẦU BẢO MẬT CỦA BỆNH VIỆN

2.1 Khái niệm Bệnh viện Đa khoa cấp tỉnh

Bệnh viện đa khoa cấp tỉnh là cơ sở khám bệnh, chữa bệnh của tỉnh thành phố trực thuộc Trung ương hoặc khu vực các huyện trong tỉnh và các Ngành. Có đội ngũ cán bộ chuyên khoa cơ bản có trình độ chuyên môn sâu có trang bị thích hợp đủ khả năng hỗ trợ cho Bệnh viện cấp huyện.

2.1.1 Đặc điểm của Bệnh viện Đa khoa cấp tỉnh

Cơ sở khám bệnh, chữa bệnh bảo hiểm y tế ban đầu tuyến tỉnh và tương đương:

- Bệnh viện đa khoa tỉnh, thành phố trực thuộc trung ương
- Bệnh viện đa khoa hạng I, hạng II thuộc các Bộ, Ngành, hoặc trực thuộc đơn vị thuộc các Bộ, Ngành
- Bệnh viện chuyên khoa, Viện chuyên khoa, Trung tâm chuyên khoa, Trung tâm y tế dự phòng tỉnh, thành phố trực thuộc trung ương có Phòng khám đa khoa
- Bệnh viện Nhi, Bệnh viện Sản – Nhi tỉnh, thành phố trực thuộc trung ương
- Bệnh viện đa khoa tư nhân tương đương hạng I, tương đương hạng II
- Bệnh viện y học cổ truyền tỉnh, thành phố trực thuộc trung ương, Bộ, Ngành
- Bệnh viện y học cổ truyền tư nhân tương đương hạng I, tương đương hạng II
- Phòng khám thuộc Ban bảo vệ chăm sóc sức khỏe cán bộ tỉnh, thành phố trực thuộc trung ương
- Bệnh viện hạng II thuộc Bộ Quốc phòng, Bệnh viện quân – dân y hạng II, các cơ sở khám bệnh, chữa bệnh khác theo quy định của Bộ trưởng Bộ Quốc phòng.

2.1.2 Chức năng – nhiệm vụ

- Cấp cứu – Khám bệnh - Chữa bệnh
- Đào tạo cán bộ y tế
- Nghiên cứu khoa học về y học
- Chỉ đạo tuyến dưới về chuyên môn, kỹ thuật
- Phòng bệnh
- Hợp tác kinh tế y tế

2.2 Giới thiệu chung về Bệnh viện Đa khoa Tây Ninh : Luận văn đề xuất mô hình giám sát phát hiện xâm nhập mạng trái phép dựa trên quy mô của một Bệnh viện cấp

tỉnh. Nhằm đảm bảo rằng trong tương lai có thể đem mô hình áp dụng cho các Bệnh viện đa khoa cấp tỉnh và các tuyến tương đương khác.

2.2.1 Tóm tắt lịch sử: Bệnh viện Đa khoa Tây Ninh là bệnh viện hạng 2 của tỉnh Tây Ninh, được xây dựng năm 1999 với quy mô 700 giường. Trung bình một ngày Bệnh viện tiếp nhận khoảng hơn 1000 lượt đến khám và điều trị.

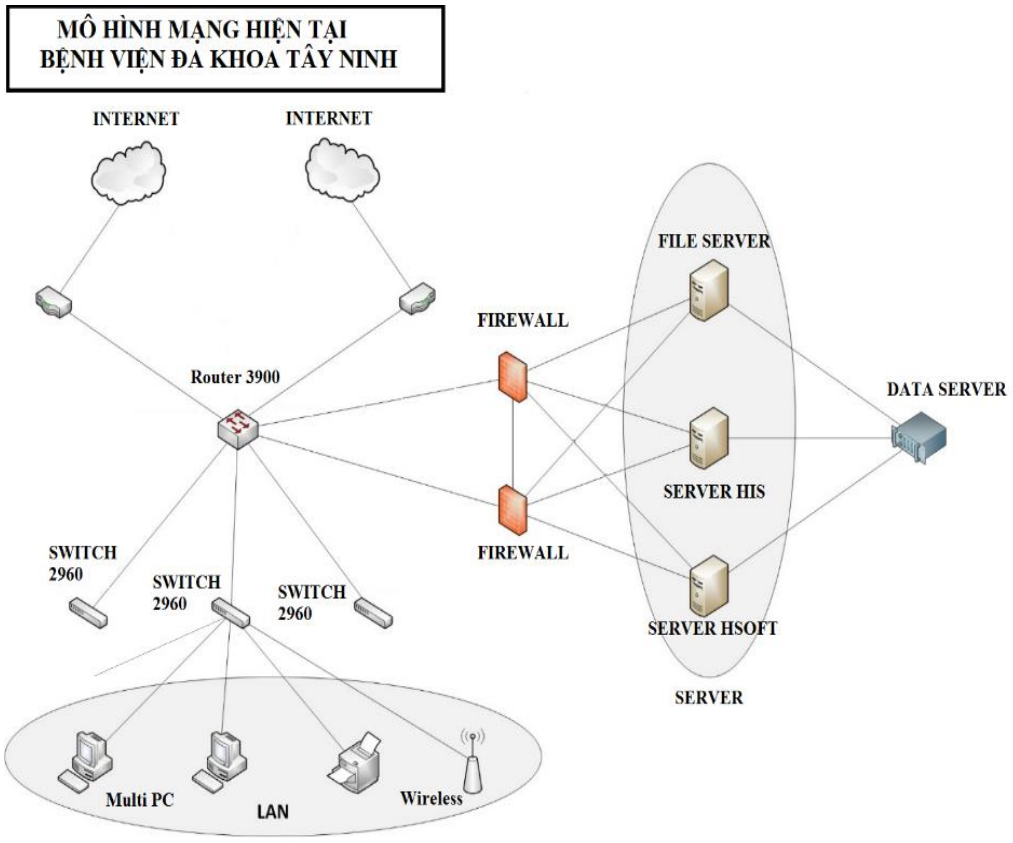
2.2.2 Sơ lược cơ cấu tổ chức của bệnh viện:

Cơ cấu tổ chức nhân sự của Bệnh viện Đa khoa Tây Ninh bao gồm nhiều 32 khoa lâm sàng và phòng chức năng với đội ngũ gần 1000 nhân viên y tế.

2.3 Tổng quan hệ thống mạng

2.3.1 Lịch sử hình thành: Hệ thống mạng máy tính của Bệnh viện Đa khoa Tây Ninh được xây dựng từ năm 2000, được nâng cấp một lần vào năm 2011.

2.3.2 Sơ đồ hệ thống mạng hiện tại



Hình 2.2: Sơ đồ mạng hiện tại của Bệnh viện Đa khoa Tây Ninh

2.3.3 Thực trạng hệ thống mạng

2.3.3.1 Hệ thống máy Server hiện tại

Hệ thống máy Server dùng hệ điều hành Unix, trong đó 1 máy làm chức năng quản lý tập trung các dữ liệu người dùng, 1 máy cài đặt các chương trình quản lý tập trung các ứng dụng của bệnh viện HIS, 1 máy làm chứng năng File Server để quản lý, lưu trữ, bảo đảm an toàn cho dữ liệu trên Data server.

2.3.3.2 Hệ thống máy Client

Hệ thống mạng có khoảng gần 200 máy Client được bố trí trong các phòng, khoa tùy theo nhu cầu sử dụng. Các máy Client được cài đặt hệ điều hành Windows 7, Windows 10 trên đó cài đặt ứng dụng văn phòng, phần mềm khám chữa bệnh VNPT-HIS, chương trình chuyên biệt phục vụ công việc của từng phòng, khoa.

2.3.3.3 Thực trạng các thiết bị phần cứng và cáp mạng

- Hệ thống gồm 2 đường internet mạng LAN, WAN.
- Có các Switch làm nhiệm vụ chuyển mạch giữa các vùng VLAN, đường mạng nội bộ sử dụng cáp quang tốc độ 1Gb nối giữa Router với các Switch.
- Hệ thống Data server dùng để lưu trữ dữ liệu.

2.3.3.4 Thực trạng về phần mềm: Windows Server 2008, Windows 10, Windows 7, VNPT-HIS, HTKK, MISA, ...

2.3.3.5 Thực trạng hệ thống bảo mật: Có triển khai 2 Firewall kết nối song song để bảo vệ cho vùng máy Server.

2.3.4 Phân tích tiềm năng và nhu cầu bảo mật đối với hệ thống mạng của Bệnh viện

2.3.4.1 Các mối đe dọa tiềm năng đối với hệ thống

a) Nguy cơ của hệ thống

- Hệ thống mạng máy tính chưa đảm bảo toàn vẹn và an toàn đúng mức, chỉ mới đáp ứng yêu cầu ở mức cơ bản.

- Hệ thống mạng LAN không có sự đồng bộ, máy tính phân bố rời rạc không tập trung. Thế hệ thiết bị mạng đã cũ, lỗi thời không còn bắt kịp tình trạng phát triển tin tặc hiện nay tiềm ẩn nhiều nguy cơ bị tấn công mạng.

- Bệnh viện đang tiếp nhận cách vận hành mới áp dúng nhiều thiết bị và công nghệ vào hệ thống mạng để ứng phó với tình hình chống dịch của ngành Y tế, các thách thức về bảo mật cũng vì thế xuất hiện và gia tăng.

- Chưa có một chính sách an ninh mạng thực sự nào được áp dụng.

b) Nhu cầu bảo mật hệ thống mạng của bệnh viện: Trong tương lai gần, Bệnh viện áp dụng nhiều công nghệ như chăm sóc sức khỏe từ xa, giám sát hay trí tuệ nhân tạo.

- Bệnh viện tiến đến ứng dụng trí tuệ nhân tạo và nguồn dữ liệu Big Data vào phục vụ bệnh nhân. Nghiên cứu ứng dụng kết nối vạn vật trong y tế (IoMT – Internet of Medical Things), liên thông kết nối chuyển hồ sơ bệnh án điện tử giữa các bệnh viện tuyến huyện, triển khai được hồ sơ bệnh án điện tử.

- Nguy cơ tấn công mạng của tin tặc nhắm vào bệnh viện và các cơ sở y tế ngày càng cao.

- Hệ thống mạng của Bệnh viện hiện nay đã kết nối với nhau tuy nhiên khả năng về bảo mật chưa được cao nhất, kết nối chưa thực sự bảo đảm về an ninh.

2.3.5 Đề xuất chính sách bảo mật

2.3.5.1 Bảo vệ mức mạng: Bảo đảm an toàn đường truyền nhằm bảo mật các thông tin truyền tải trên hệ thống mạng, dựa vào các phương thức mã hoá thông tin trên đường truyền, các công cụ xác định tính nguyên vẹn và chính xác của thông tin.

2.3.5.2 Bảo mật lớp truy cập: Thường áp dụng các hình thức xác thực người dùng, tạo các kênh VPN cho các kết nối. IDS đảm bảo ngăn chặn các truy nhập trái phép hay các dạng tấn công ngay từ cổng vào mạng.

2.3.5.3 Bảo mật mức thiết bị: Các thiết bị mạng như Router và switch, firewall…là các điểm nút của mạng hết sức quan trọng và cần được bảo vệ.

2.3.5.4 Bảo mật mức máy chủ: Hệ thống máy chủ thực hiện các công việc dịch vụ khác nhau trong mạng, có thể nói đây là nguồn tài nguyên chính hết sức quan trọng và là mục tiêu của nhiều cuộc tấn công từ bên trong cũng như bên ngoài.

2.3.5.5 Bảo mật mức Hệ Điều Hành (HĐH) : Xây dựng các chính sách cài đặt, cập nhật, backup dữ liệu hay sử dụng các phần mềm bổ sung (Patch) bịt lỗ hổng trên các HĐH.

2.3.5.6 Bảo mật ở mức ứng dụng: Đảm bảo việc truy nhập vào các dịch vụ và phần mềm Web, mail, CSDL.

2.3.5.7 Bảo mật mức CSDL: Lõi của toàn bộ hệ thống bảo mật thông tin, toàn bộ thông tin quan trọng mang tính chất sống còn được tập trung trên các CSDL.

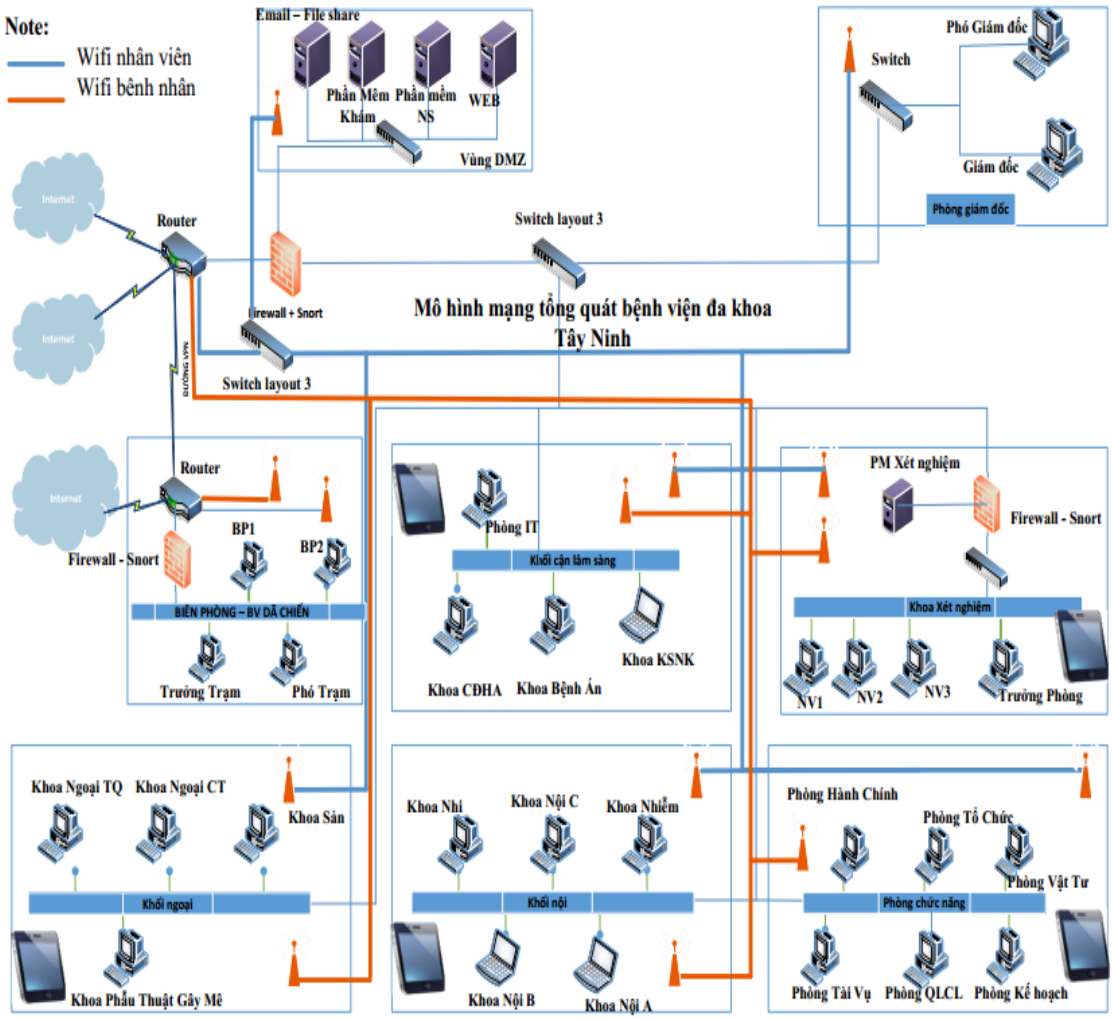
2.3.5.8 Bảo mật cho mạng phân tán: Dữ liệu, thông tin đều qua các dạng mail, nên cần tập trung sử dụng mail server của bệnh viện, tránh sử dụng các dịch vụ mail của bên thứ ba để gửi các thông tin quan trọng.

CHƯƠNG 3: NGHIÊN CỨU ĐỀ XUẤT XÂY DỰNG HỆ THỐNG GIÁM SÁT SNORT TRỰC TUYẾN CHO HỆ THỐNG MẠNG BỆNH VIỆN TÂY NINH

3.1 Giới thiệu chung

Trong chương này trình bày về mô hình ứng dụng đề xuất kết hợp với SNORT và PFSENSE giám sát trực tuyến hệ thống mạng LAN nói chung, mạng LAN của bệnh viện Tây Ninh nói riêng.

3.2 Mô hình nghiên cứu hệ thống mạng

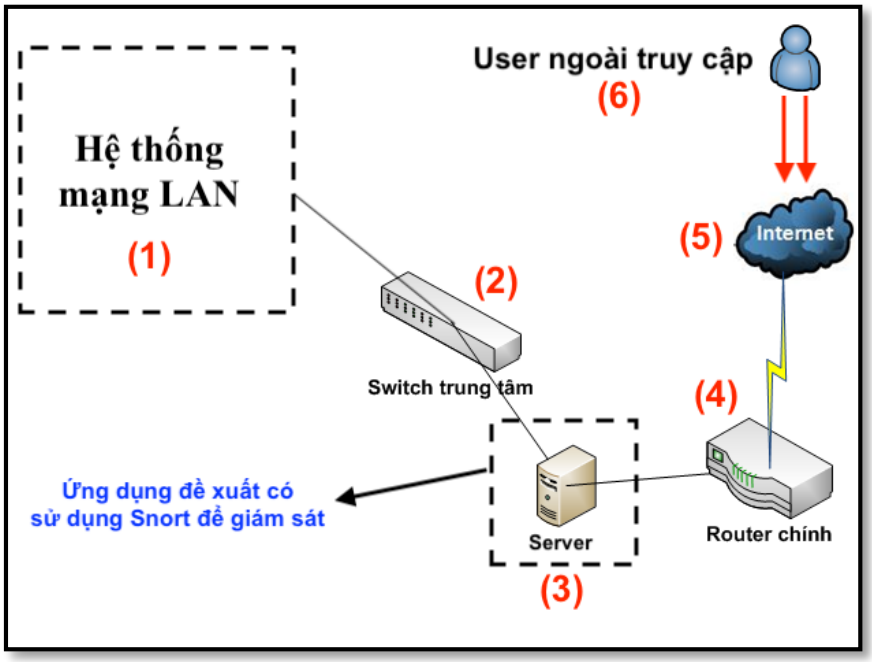


Hình 3.1: Mô hình mạng tổng quát bệnh viện đa khoa Tây Ninh

3.3 Đề xuất hệ thống giám sát SNORT trực tuyến

3.3.1 Mô hình - Cấu trúc hệ thống đề xuất

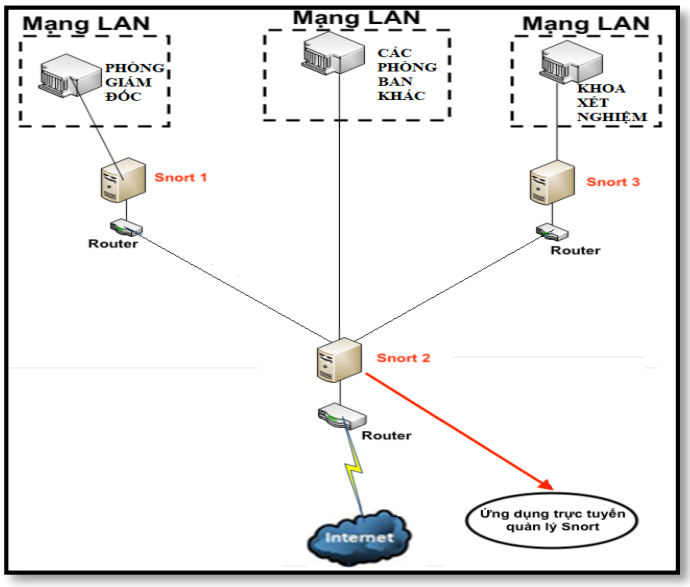
a) Mô hình Snort cho mạng LAN



Hình 3.3: Mô hình đề xuất tích hợp ứng dụng giám sát Snort cho mạng LAN

Với mô hình này, Snort sẽ giám sát được toàn bộ hệ thống mạng LAN và kiểm soát được lưu lượng, giám sát các hoạt động trong hệ thống.

b) Mô hình cho môi trường trực tuyến



Hình 3.4: Mô hình đề xuất tích hợp ứng dụng giám sát Snort cho trực tuyến

3.3.2 Mục tiêu của ứng dụng đề xuất

- Giám sát toàn bộ các luồng dữ liệu trên hệ thống mạng LAN.
- Snort sẽ phân tích ghi log, trên cơ sở đọc dữ liệu log, ứng dụng đề xuất sẽ phân tích, định danh các vấn đề, từ đó ra quyết định gửi cảnh báo hay nhắc nhở
- Tiến hành phân tích log trên cơ sở sử dụng Splunk Server. Đây là điểm mới của luận văn này cũng như điểm mới ứng dụng đề xuất.

3.3.3 Các module chính của hệ thống

(1) Module tạo rules và lưu dữ liệu LOG từ SNORT của PFSENSE

- Snort trên Pfsense
- Một vài rules của SNORT

(2) Module tổng hợp log và gửi cảnh báo

- Module sử dụng các log được chuyển tới từ các server PFSENSE. Từ đó, tạo các câu lệnh và các chuỗi string phù hợp với các mong muốn gửi cảnh báo về mail.
- Bên cạnh đó, có thể tạo ra được các báo cáo, tổng hợp số lượng truy cập vào và ra internet, …

3.4 Kết luận Chương

Với việc đề xuất ứng dụng cảnh báo dựa trên giám sát SNORT, luận văn sẽ hướng tới xây dựng một ứng dụng có tính trực tuyến cao để cảnh báo và giám sát.

Bên cạnh đó với việc áp dụng lưu trữ server log tập trung Splunk các file log của Snort để phân tích thống kê theo yêu cầu cho người quản trị hệ thống sẽ phần nào giúp cho người quản trị có công cụ hỗ trợ đắc lực, cũng như mở ra hướng phát triển sâu hơn về khoa học dữ liệu trong an toàn thông tin.

CHƯƠNG 4: THỰC NGHIỆM VÀ ĐÁNH GIÁ

4.1 Thực nghiệm hệ thống IDS – Snort

4.1.1 Mục tiêu

- Xây dựng hệ thống tường lửa IDS cho Bệnh viện đa khoa Tây Ninh trong tương lai

- Xây dựng hệ thống Snort bảo vệ từng khoa riêng

- Xây dựng hệ thống Snort quản lý Wifi cho nhân viên và bệnh nhân sử dụng

4.1.2 Thực hiện tấn công

4.1.2.1 Kịch bản tấn công 1

- ***Mục đích***

  Tổ chức tấn công từ chối dịch vụ DOS từ các phía, từ các máy nội bộ khoa Xét nghiệm và các máy thuộc phòng không quan trọng khác (khoa Chẩn đoán hình ảnh) thực hiện tấn công cùng lúc bằng 10 máy cả vùng mạng trong và vùng mạng ngoài.

- ***Mô tả***

  5 máy ở vùng mạng trong (lớp mạng : 192.168.137.0/24) của khoa Xét nghiệm và 5 máy từ vùng mạng ngoài (192.168.79.0/24) của khoa CĐHA, tấn công cùng lúc 10 máy vào máy chủ Khoa xét nghiệm có địa chỉ IP 192.168.137.12

- ***Kết quả thu được***

  Snort ghi nhận được log của 10 máy tấn công và ngay lập tức gửi về Server ghi log tập trung, gửi log sang cho Mail server cho nhà quản trị mạng để theo dõi.

4.1.2.2 Kịch bản tấn công 2

- ***Mục đích:*** Tấn công từ máy tính vùng ngoài có dãy địa chỉ thuộc các khoa phòng không quan trọng khác, tấn công trái phép máy tính ở vùng

mạng Active Directory của khoa Xét nghiệm nhằm mục đích lấy cắp thông tin, truy cập tài liệu cá nhân.

❖ ***Mô tả***

Sử dụng 1 máy hệ điều hành Window 7 ở vùng mạng có địa chỉ IP 192.168.79.20 thuộc khoa Ngoại Tổng Quát để tấn công SSH vào máy tính khác ở vùng mạng Active Directory có địa chỉ IP 192.168.137.12.

❖ ***Kết quả thu được***

Trên giao diện Pfsense, hệ thống giám sát Server Snort đã ghi nhận được chi tiết các cảnh báo của cuộc tấn công, và tiến hành gửi email về cho nhà quản trị mạng.

4.1.2.3 Kịch bản tấn công 3

❖ **Mục đích**

Thực hiện truy cập vượt quyền từ các tài khoản thuộc vùng mạng Active Directory, truy cập trái phép vào các Website không được nhà quản trị mạng cho phép.

❖ **Mô tả**

Sử dụng 1 tài khoản vùng mạng Active Directory truy cập vào các Website : Facebook, Youtube,… không được nhà quản trị mạng cho phép và sau đó hệ thống sẽ gửi log về báo hiệu cho Server Snort.

❖ **Kết quả thu được**

- Hệ thống tường lửa Pfsense ngăn chặn và trả về cùng 1 kết quả từ chối truy cập website.
- WebServer sẽ nhận được log cảnh báo do phần mềm Splunk gửi về và báo qua mail cho nhà quản trị mạng.

4.1.2.4 Kịch bản tấn công 4

❖ **Mục đích**

Thực hiện tấn công DOS từ vùng mạng ngoài nhằm mục đích phá hoại hệ hệ thống máy chủ WebServer.

❖ **Mô tả**

Thực hiện tấn công DOS bằng 5 máy cùng lúc từ vùng mạng ngoài 192.168.43.0/24 của các khoa phòng trong Bệnh viện lên hệ thống máy chủ có địa chỉ IP : 192.168.43.38 Webs ở vùng DMZ.

❖ **Kết quả thu được**

Cảnh báo về DoS vùng DMZ trong SNORT, mail cảnh báo về DoS vùng DMZ.

4.1.2.5 Kịch bản tấn công 5

❖ **Mục đích**

Lợi dụng tấn công thông qua lỗ hỏng XSS vào hệ thống máy chủ mục đích tấn công cùng lúc bằng nhiều máy nhằm phá hoại Cổng thông tin điện tử của Bệnh viện.

❖ **Mô tả**

- Thực hiện tấn công cùng lúc bằng 5 máy từ mạng WAN vào hệ thống máy chủ WebServer vùng DMZ.
- Thực hiện tấn công lên WebServer bằng lỗ hổng Web. Câu lệnh xss cơ bản được sử sụng:

<script>alert(1)</script>

❖ **Kết quả thu được**

Phần mềm Splunk server tiến hành ghi log và gửi mail cho nha quản trị mạng. Nội dung là các log của tất cả những máy cố gắng tấn công vào Web-Server.

4.1.2.6 Kịch bản tấn công 6

- **Mục đích**

  Giả lập mạng WLAN để tấn công hệ thống bằng các máy tượng trưng tượng trưng cho 2 vùng WLAN là wifi nhân viên và wifi bệnh nhân.

- **Mô tả**

  Thực hiện tấn công bằng 2 máy từ vùng mạng ngoài : Máy nhân viên có IP: 192.168.79.14 được phép vào máy chủ web, máy chủ phần mềm, còn máy bệnh nhân IP 192.168.79.15 thì chỉ được phép vào máy chủ Website nhưng không được vào máy chủ phần mềm.

- **Kết quả thu được**

  Bệnh nhân cố gắng sử dụng tấn công SSH lên server thì không thể nào thực hiện được, còn máy nhân viên được phép truy cập.

4.1.2.7 Kịch bản tấn công 7

- **Mục đích**

  Nhằm mục đích xây dựng một mô hình bệnh viện thật nhanh chóng, cho trường hợp ứng phó với tình hình dịch bệnh COVID phức tạp như hiện nay. Hoặc bệnh viện có nhu cầu mở rộng cơ sở y tế ra địa bàn khác trong tỉnh trong tương lai.

  Sao chép cũng như di dời hệ thống quản lý sang vùng khác.

  Ở đây vì là bệnh viện dã chiến không lớn như bệnh viện chính nên chúng ta sẽ chỉ sử dụng 1 hệ thống mạng LAN để kết nối.

- **Mô tả**

  Trước tiên, chúng ta cần phải backup hệ thống IDS của bệnh viện đa khoa. Sử dụng chức năng Backup & Restore của pfsense.

  Xây dựng một hệ thống mạng hoàn toàn mới với dãy địa chỉ mạng LAN 192.168.140.0/24.

  Xây dựng các rule trên IDS-Snort để phát hiện tấn công vào hệ thống Server.

  Tiến hành sử dụng chức năng Backup Configuration để di dời hệ thống IDS sang bệnh viện dã chiến.

  Sau đó, lấy file XML đã xuất ra rồi import vào pfsense mới.

Tùy chỉnh lại hệ thống mạng cho hệ thống. Sau đó đăng nhập màn hình quản lý của người quản trị.

- **Kết quả thu được**

Thông tin tấn công, xâm nhập mạng của Bệnh viện Dã chiến khi được triển khai hệ thống IDS mới ghi nhận đã ghi nhận log.

Cảnh báo cho nhà quản trị mạng để có phương án bảo mật hệ thống.

4.1.3 Đánh giá

Việc ứng dụng khai phá dữ liệu cũng như khoa học dữ liệu vào trong bảo vệ LAN và phòng ngừa tấn công LAN, là một trong những xu thế hiện nay. Việc kết hợp các thuật toán thông minh với các công cụ giám sát mạng và ứng dụng quản lý trực tuyến được xây dựng cũng là một trong những hướng phát triển tốt và giúp bảo vệ người dùng LAN tốt hơn. Thực nghiệm trong luận văn này chỉ thể hiện được một phần nào đó trong việc quản trị hệ thống mạng và xử lý LOG của SNORT và Splunk Server. Kết quả thu được trùng khớp và có khả quan trong việc kết hợp SNORT và các server xử lý log tập trung.

Việc mô phỏng thực nghiệm đã phần nào cho thấy một cách thức tiếp cận mới trong việc phòng chống và giám sát an ninh trên mạng nói chung và mạng LAN nói riêng.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1 Kết quả đạt được

5.1.1 Về mặt lý thuyết

- Đạt được các mục tiêu kiến thức về hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.

- Tìm hiểu được kiến trúc và cách thức hoạt động của Snort. Phân tích các tập tin log, các cảnh báo, dựa vào đó có luật phù hợp để phát hiện và ngăn chặn xâm nhập.

- Tìm hiểu và khảo sát mạng LAN tại cơ quan công tác, đưa ra nhận định về an toàn, bảo mật thông tin và cách phòng chống những nguy cơ tấn công trong mạng LAN.

- Phân tích được một số trường hợp tấn công, phân tích được một số tập luật của các dạng tấn công phổ biến.

5.1.2 Về mặt thực tiễn

- Luận văn đã đưa ra được giải pháp và các chính sách bảo mật, an ninh mạng trong mạng LAN tại cơ quan.

- Nghiên cứu và xây dựng ứng dụng giám sát Snort trực tuyến và tích hợp vào trong hệ thống mạng LAN thực tế.

- Đề xuất mô hình nghiên cứu mạng LAN tích hợp ứng dụng quản lý Snort trực tuyến để giám sát hệ thống.

5.2.2 Hạn chế

- Luận văn được thực hiện trong thời điểm dịch bệnh, do đó việc xây dựng mô hình phải thực hiện trên môi trường ảo hóa hoàn toàn. Dẫn đến, việc đánh giá hệ thống có thể không hoàn toàn chính xác so với thực tế.

Môi trường ảo hóa chỉ gồm 15 máy tính để triển khai hệ thống IDS, thực hiện các tấn công cơ bản và thường gặp như DoS, điều khiển SSH, Brute-Force, XSS, SQL injection trên Web Server.

5.3 Hướng phát triển tiếp theo của đề tài

- Tích hợp Snort vào các hệ thống mạng LAN phức tạp tại các cơ sở khác.

- Xây dựng ứng dụng hoàn chỉnh để quản lý Snort cho toàn bộ các hệ thống chi nhánh mạng LAN.

- Nghiên cứu các phương pháp & thuật toán phat hiện bất thường khác để tăng khả năng phòng thủ của hệ thống,cải tiến tốc độ tính toán của các thuật toán phân tích dữ liệu.

- Hiệu quả kinh tế - xã hội:

+ Chi phí thấp cho hệ thống tốt, có đầy đủ chức năng của một hệ thống phát hiện xâm nhập

+ Kết hợp với các hệ thống nguồn mở khác như iptables, hệ thống giám sát Nagios cho ứng dụng Web có thể xây dựng một hệ thống tốt có khả năng ngăn chặn các cuộc tấn công, phân tích, theo dõi và nâng cao hiệu xuất của dịch vụ với chi phí rất thấp.