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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

TP. HỒ CHÍ MINH - 2022

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

LUẬN VĂN THẠC SĨ KỸ THUẬT
(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC:
TS. Đàm Quang Hồng Hải

TP. HỒ CHÍ MINH – NĂM 2022

LỜI CAM ĐOAN

Tôi xin cam luận văn về đề tài **"Xây dựng hệ thống giám sát mạng dành cho bệnh viện đa khoa cấp tỉnh với mã nguồn mở"** là công trình nghiên cứu cá nhân của tôi trong thời gian qua. Tất cả số liệu dùng để sử dụng và áp dụng thử nghiệm trong luận văn và kết quả công trình nghiên cứu là do cá nhân học viên tự tìm tòi học tập, triển khai thử nghiệm một cách khách quan, đảm bảo tính trung thực, dựa trên nguồn gốc cơ sở dữ liệu rõ ràng và chưa được công khai trên bất kỳ hình thức nào.

Nếu phát hiện bất kỳ sự sao chép nào từ kết quả nghiên cứu khác hoặc sai sót về số liệu nghiên cứu, tôi xin hoàn toàn chịu trách nhiệm trước nhà trường và hội đồng.

TP.HCM, ngày 25 tháng 01 năm 2022

Học viên thực hiện luận văn

Nguyễn Anh Tú

LỜI CẢM ƠN

Lời đầu tiên tôi xin gửi lời cảm ơn chân thành và sâu sắc nhất đến thầy hướng dẫn - **TS. Đàm Quang Hồng Hải**. Trong suốt quá trình thực hiện luận văn, Thầy đã luôn trực tiếp, tận tình hướng dẫn, truyền tải và định hướng những kiến thức, kinh nghiệm quý báu cho tôi. Qua đây, tôi cũng xin gửi lời cảm ơn chân thành nhất đến với các thầy, cô trong trường Học viện Công nghệ Bưu chính Viễn thông đặc biệt là trong Khoa Đào tạo Sau đại học, cơ sở Thành phố Hồ Chí Minh đã luôn tạo điều kiện giúp đỡ và hướng dẫn tôi trong suốt quá trình học tập và nghiên cứu tại Học viện.

Để thuận tiện nghiên cứu và thử nghiệm đề tài, tôi cũng xin chân thành cảm ơn Ban lãnh đạo Bệnh viện Đa khoa tỉnh Tây Ninh đã tạo điều kiện cho tôi được học tập và nghiên cứu tại cơ quan. Đặc biệt tôi xin chân thành cám ơn các anh chị trong Tổ Công nghệ thông tin đã giúp đỡ nhiệt tình cũng như cung cấp các tài liệu nghiên cứu, giải đáp những thắc mắc trong quá trình nghiên cứu.

Và lời cám ơn cuối cùng, tôi xin dành cho gia đình, bạn bè, đồng nghiệp đã luôn động viên, ủng hộ và tạo mọi điều kiện để tôi có thể hoàn thành xuất sắc luận văn của mình.

Trong Luận văn chắc chắn sẽ không tránh khỏi những hạn chế và thiếu sót. Tôi rất mong nhận được các ý kiến đóng góp bổ ích của thầy cô, ban tư vấn và bạn đọc để đề tài ngày càng được hoàn thiện hơn và có thể ứng dụng vào cuộc sống.

Chân thành cảm ơn.

TP.HCM, ngày 25 tháng 01 năm 2022

Học viên thực hiện luận văn

Nguyễn Anh Tú

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
LAN	Local Area Network	Mạng máy tính cục bộ
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IPS	Intrusion Prevention Systems	Hệ thống ngăn ngừa xâm nhập
ICMP	Internet Control Message Protocol	Giao thức Thông điệp Điều khiển Internet
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
UDP	User Datagram Protocol	Giao thức truyền tải gói thông tin người dùng
DMZ	Demilitarized Zone	Vùng mạng trung lập giữa mạng nội bộ và mạng internet

DANH SÁCH HÌNH VẼ

MỞ ĐẦU

Bước sang thế kỉ XXI, với sự phát triển vượt bậc của cuộc cách mạng khoa học và công nghệ hiện đại và sự bùng nổ các công nghệ cao, trong đó công nghệ thông tin là yếu tố quan trọng có tác động sâu sắc đến toàn xã hội. 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.

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 lấy cắp hồ sơ y tế điện tử của ngành chăm sóc sức khỏe dẫn đến lộ 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 và thông tin khám bệnh chữa bệnh của người bệnh nói riêng là vô cùng quan trọng. Vì thế, cần nhiều hơn nữa những biện pháp giám sát, đảm bảo an toàn.

Lĩnh vực nghiên cứu mà luận văn tập trung vào là nội dung an toàn mạng máy tính để xây dựng một hệ thống phát hiện xâm nhập mạng máy tính, nhằm mục đích bảo vệ mạng máy tính khỏi sự tấn công, đột nhập của tin tặc và trợ giúp quản trị mạng thực hiện công việc bảo mật bằng các xây dựng quy trình đảm bảo an toàn cho hệ thống mạng máy tính.

Việc nghiên cứu và phát triển các sản phẩm về an ninh thông tin nói chung và an ninh mạng nói riêng là một nhu cầu bức thiết đối với hệ thống Bệnh viện Đa khoa cấp tỉnh. Khi mà các ứng dụng chạy trên đó ngày càng phát triển về cả quy mô và số lượng, thì những lỗ hổng về bảo mật ẩn chứa trong các hệ thống này cũng ngày càng nhiều. Bên cạnh đó, trình độ của các tin tặc trong nước trong thời gian qua đã có nhiều

bước tiến. Các nguyên lý, cách thức tấn công mà các tin tặc vận dụng đã có nhiều bổ sung và vận dụng linh hoạt.

Trước nhu cầu đó, học viên chọn thực hiện đề tải "***Xây dựng hệ thống giám sát mạng dành cho bệnh viện đa khoa cấp tỉnh với mã nguồn mở***".

Với mong muốn góp phần giải quyết những mặt hạn chế tồn tại về an ninh, an toàn trong hệ thống mạng Bệnh viện, đó là :

• Nghiên cứu, xây dựng quy trình đảm bảo an toàn cho hệ thống mạng máy tính dành cho Bệnh viện Đa khoa cấp tỉnh (mô hình triển khai dựa trên hệ thống mạng của Bệnh viện Đa khoa Tây Ninh).

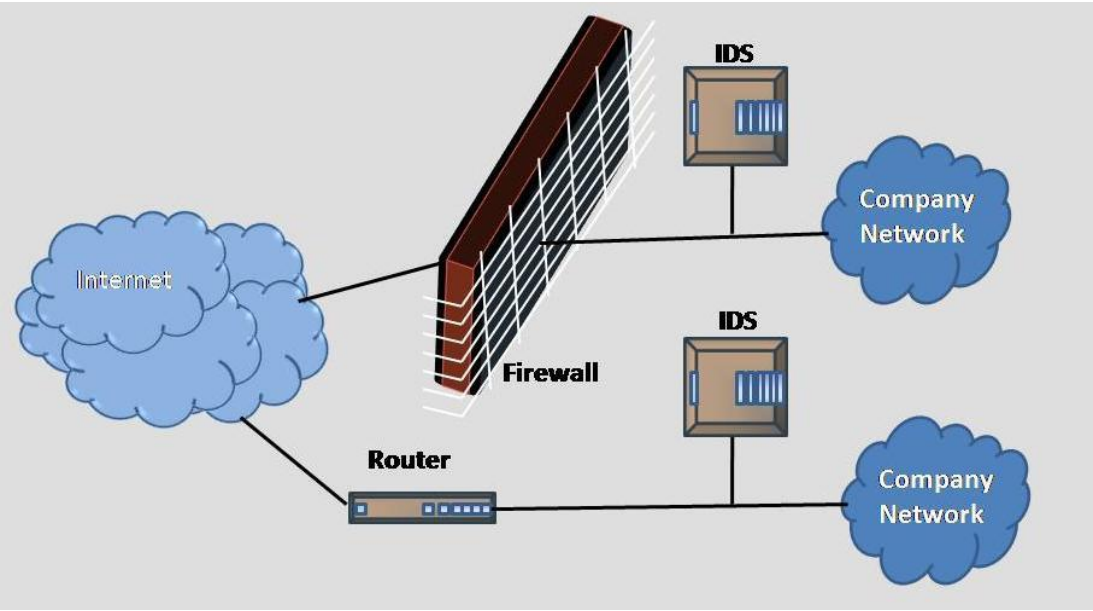
• Xây dựng, triển khai một hệ thống phần mềm phát hiện xâm nhập mạng dựa trên nền tảng phần mềm mã nguồn mở.

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, IPS

Ngày nay với sự phát triển của công nghệ thì Internet và các mạng nội bộ càng trở nên phổ biến. Cũng chính vì điều này đã tạo nên những thách thức về các vấn đề xâm nhập mạng trái phép buộc các nhà tổ chức phải bổ sung thêm những hệ thống kiểm soát các lỗ hổng về bảo mật công nghệ thông tin. Một trong các thuật ngữ được nhắc đến nhiều trong vấn đề này chính là hệ thống phát hiện xâm nhập – IDS.



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.

Phần mềm IDS cũng có thể phân biệt được đâu là những cuộc tấn công nội bộ (từ chính nhân viên trong tổ chức) hoặc từ bên ngoài (từ tin tặc). Trong một số trường hợp, IDS còn có thể phản ứng lại với các lưu lượng mạng độc hại bằng cách chặn IP nguồn truy cập mạng. Hiện nay có rất nhiều những phần mềm bị nhầm tưởng là IDS do đó người dùng cần phân biệt rõ để tránh những nhầm lẫn này.

Một số những thiết bị bảo mật dưới đây không phải là IDS như :

- Hệ thống ghi nhật ký mạng đây là các hệ thống giám sát lưu lượng trong mạng được sử dụng để phát hiện lỗ hổng đối với những cuộc tấn công từ chối dịch vụ (DoS) trên mạng đang bị tắc nghẽn.
- Các công cụ đánh giá lỗ hổng, các bộ quét bảo mật dùng để kiểm soát lỗi và lỗ hổng trong hệ điều hành, dịch vụ mạng.
- Các phần mềm diệt virus mặc dù có những tính năng giống hệ thống phát hiện xâm nhập nhưng xét về tổng thể thì chúng không phải là IDS.
- Tường lửa: Mặc dù có nhiều tường lửa hiện đại được tích hợp sẵn IDS, nhưng IDS không phải là tường lửa.

IDS phát hiện dựa trên các dấu hiệu đặc biệt về nguy cơ đã biết (giống như cách phần mềm diệt virus phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số chuẩn của hệ thống có thể chấp nhận được) để tìm ra các dấu hiệu bất thường.

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.

Một hệ thống IDS cần phải thỏa mãn những yêu cầu:

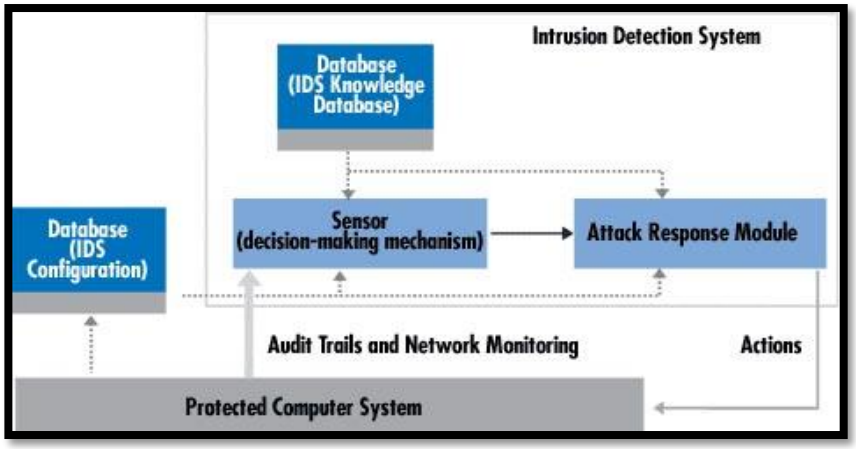
- Tính chính xác (Accuracy): IDS không được coi những hành động thông thường trong môi trường hệ thống là những hành động bất thường hay lạm dụng.
- Hiệu năng (Performance): Hiệu năng của IDS phải đủ để phát hiện xâm nhập trái phép trong thời gian thực.

- Tính trọn vẹn (Completeness): IDS không được bỏ qua một xâm nhập trái phép nào. Đây là một điều kiện khó thỏa mãn được.
- Chịu lỗi (Fault Tolerance): Bản thân IDS phải có khả năng chống lại tấn công.
- Khả năng mở rộng (Scalability): IDS phải có khả năng xử lý trong trạng thái xấu nhất là không bỏ sót thông tin nào. Yên cầu này liên quan tới hệ thống mà các sự kiện trong tương lai đến từ nhiều nguồn tài nguyên với số lượng host nhỏ. Với sự phát triển nhanh và mạnh của mạng máy tính, hệ thống có thể bị quá tải bởi sự tăng trưởng của số lượng sự kiện.

Một hệ thống chống xâm nhập (Intrusion Prevention System – IPS) được định nghĩa là một phần mềm hoặc một thiết bị chuyên dụng có khả năng ngăn chặn các nguy cơ gây mất an ninh.

Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.

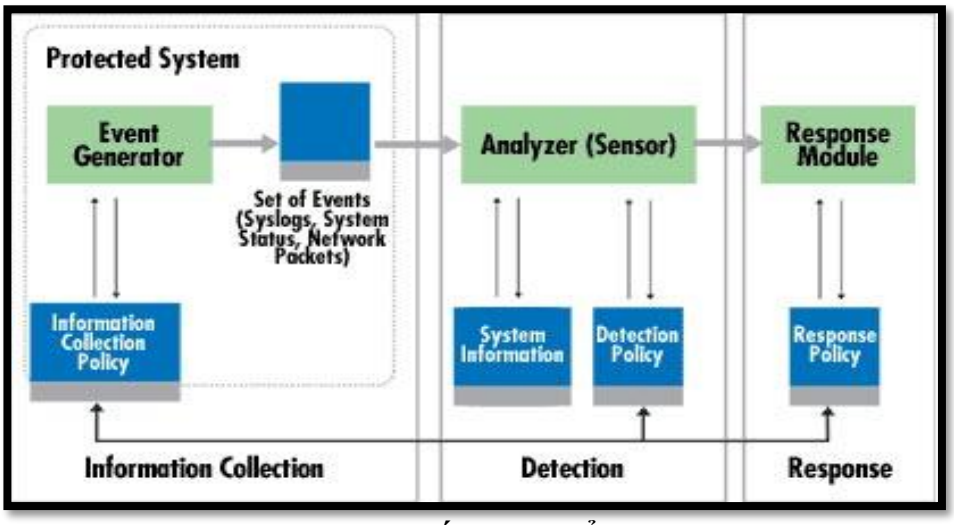
1.1.2 Kiến trúc của hệ thống phát hiện xâm nhập IDS



Hình 1.2: Một kiến trúc IDS mẫu

Kiến trúc của hệ thống phát hiện xâm nhập IDS bao gồm các thành phần chính:

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



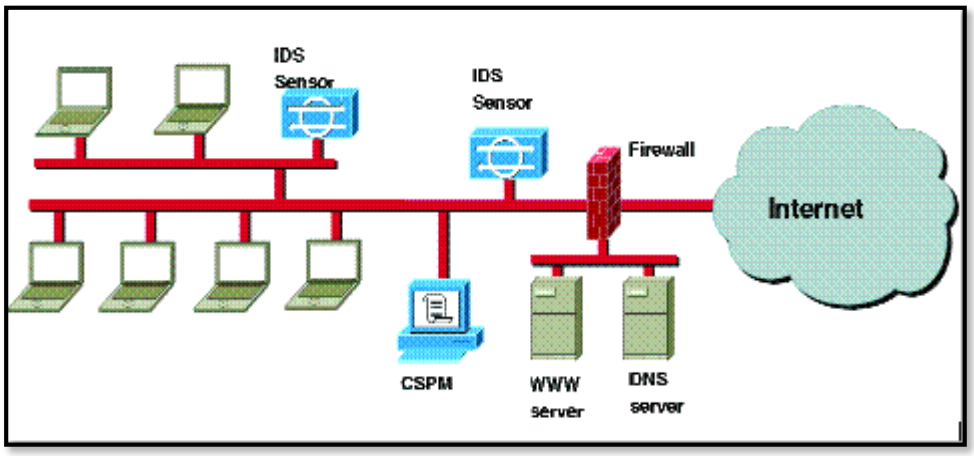
Hình 1.3: Hệ thống IDS điển hình

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.

Khi hệ thống mạng dùng các hub, chúng ta có thể đặt các bộ cảm biến trên bất kì port nào của hub vì mọi luồng traffic được gửi ra tất cả các port trên hub, và có thể phát hiện ra các luồng traffic bất thường.

Nhưng khi hệ thống cần sử dụng các switch, các switch chỉ gửi gói tin đến chính xác địa chỉ cần gửi trên từng port. Để giải quyết vấn đề này, một kỹ thuật thông dụng là sử dụng những con switch có port mở rộng (Expansion port). Port này được gọi là Switched Port Analyzer (SPAN) port.



Hình 1.4: Hệ thống phát hiện xâm nhập trái phép

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

được xem như lớp phòng vệ bổ sung, đảm bảo an toàn cho thông tin và hệ thống. Một số yêu cầu đối với IDS:

- Bảo vệ tính toàn vẹn (integrity) của dữ liệu, bảo đảm sự nhất quán của dữ liệu trong hệ thống. Các biện pháp đưa ra ngăn chặn được việc thay đổi bất hợp pháp hoặc phá hoại dữ liệu.
- Bảo vệ tính bí mật, giữ cho thông tin không bị lộ ra ngoài.
- Bảo vệ tính khả dụng, tức là đảm bảo cho hệ thống luôn sẵn sàng thực hiện yêu cầu truy nhập thông tin của người dùng hợp pháp.
- Bảo vệ tính riêng tư, tức là đảm bảo cho người sử dụng khai thác tài nguyên của hệ thống theo đúng chức năng, nhiệm vụ đã được phân cấp, ngăn chặn được sự truy cập thông tin bất hợp pháp.
- Cung cấp thông tin về sự xâm nhập, đưa ra những chính sách đối phó, khôi phục, sửa chữa...

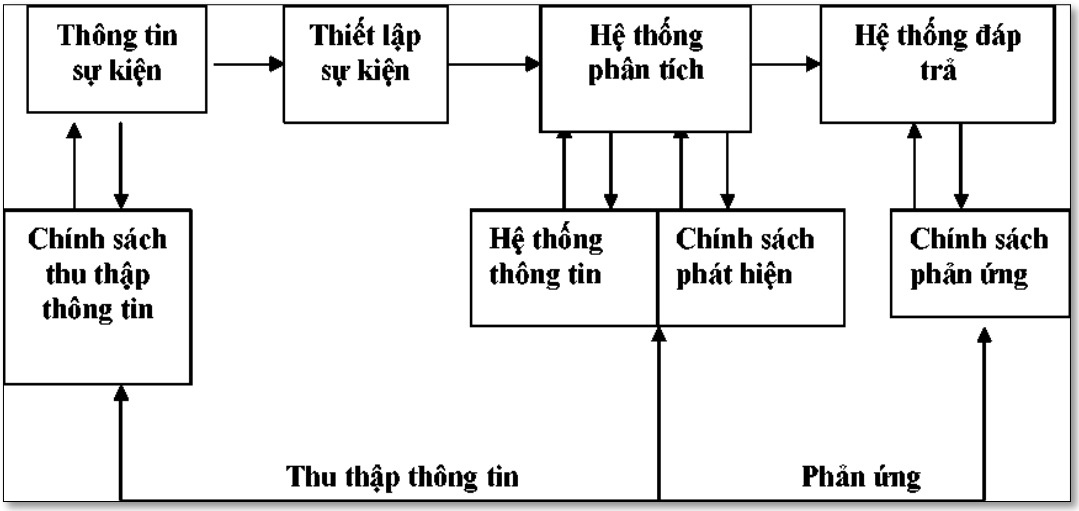
Chức năng quan trọng nhất của IDS là:

- Giám sát: Giám sát lưu lượng mạng các hoạt động bất thường và các hoạt động khả nghi.
- Cảnh báo: Khi đã biết được các hoạt động bất thường của một truy cập nào đó, IDS sẽ đưa ra cảnh báo về hệ thống cho người quản trị
- Bảo vệ: Dùng những thiết lập mặc định và những cấu hình từ nhà quản trị mà có những hành động chống lại kẻ xâm nhập

Chức năng mở rộng của IDS là:

- Phân biệt các cuộc tấn công từ trong hoặc từ bên ngoài: Nó có thể phân biệt được đâu là những truy cập hợp lệ (hoặc không hợp lệ) từ bên trong và đâu là cuộc tấn công từ bên ngoài.

- Phát hiện: Dựa vào so sánh lưu lượng mạng hiện tại với baseline, IDS có thể phát hiện ra những dấu hiệu bất thường và đưa ra các cảnh báo và bảo vệ ban đầu cho hệ thống.

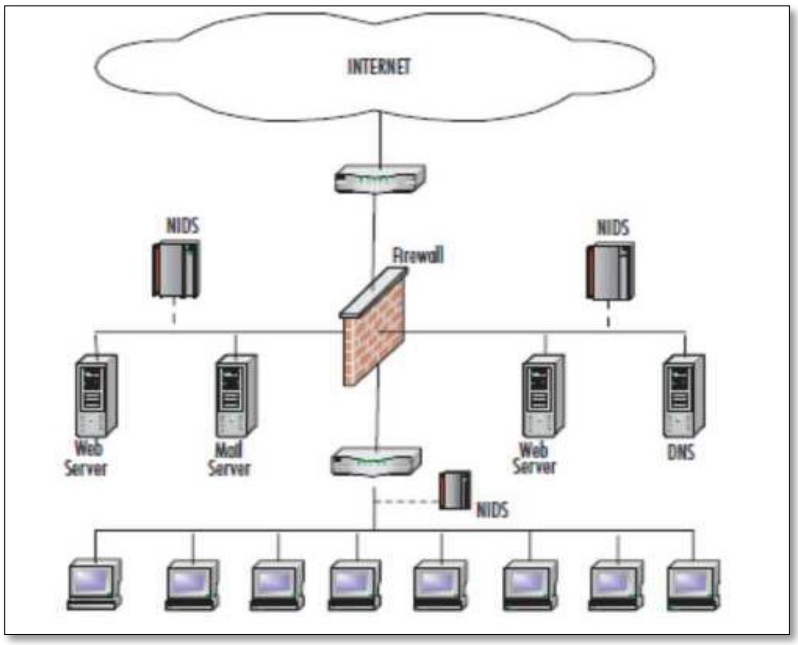


Hình 1.5: Mô hình chức năng IDS

1.1.4 Phân loại IDS/IPS

IDS sử dụng hai kĩ thuật để phát hiện xâm nhập đó là phát hiện hành vi và phát hiện dấu hiệu để xác nhận các cuộc tấn công. Từ đó có các loại IDS sau:

- 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. Một hệ thống NIDS nằm trực tiếp trên hệ thống mạng và nó phân tích các gói tin giao thông trên mạng để tìm kiếm những cuộc tấn công. NIDS nhận tất cả các gói tin trên các phân đoạn mạng được chỉ định (thậm chí gồm cả những gói tin đi đến chuyển mạch của mạng). Nó cẩn thận trong việc cấu trúc lại các luồng thông tin đó để tiện cho việc phân tích và so sánh chúng với các mẫu có sẵn trong cơ sở dữ liệu. Hầu hết các NIDS đều được cung cấp khả năng ghi lại các hành động diễn ra trên mạng và gửi những cảnh báo tới nhà quản trị với những hành động bất thường.

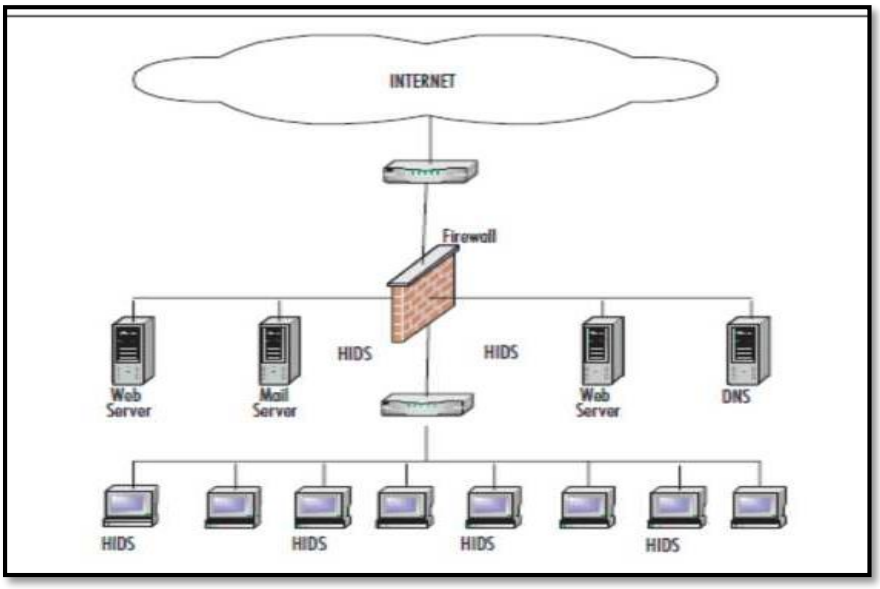


Hình 1.6: Các NIDS trong hệ thống mạng

- 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. HIDS chỉ giám sát các gói dữ liệu inbound và outbound từ thiết bị và cảnh báo người dùng hoặc quản trị viên về những hoạt động đáng ngờ được phát hiện.

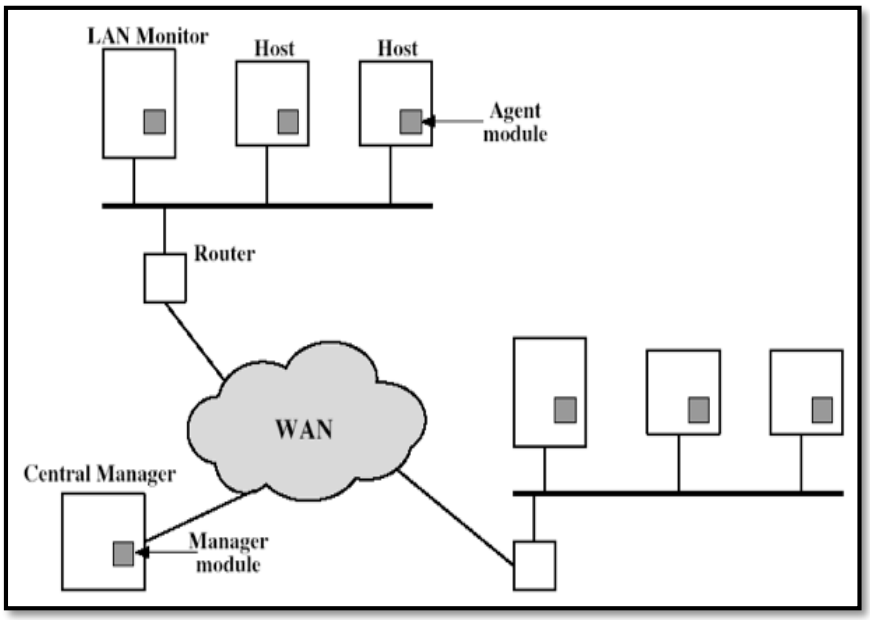
  HIDS thực chất là một ứng dụng chạy trên máy trạm, nó có chức năng quét toàn bộ hệ thống của máy đó bao gồm việc quét nhật ký hệ thống và các nhật ký sự kiện. Nó sẽ kiểm tra bất kỳ một hành động nào để xem nó có khớp nhật ký được ghi trong dữ liệu không.

  HIDS có thể được cài đặt trên nhiều dạng máy tính khác nhau cụ thể như các máy chủ, máy trạm, máy tính notebook. HIDS cho phép bạn thực hiện một cách linh hoạt trong các đoạn mạng mà NIDS không thể thực hiện được. Lưu lượng đã gửi tới host được phân tích và chuyển qua host nếu chúng không tiềm ẩn mã nguy hiểm. HIDS ưu việt hơn NIDS ở việc thay đổi các máy tính cục bộ. Trong khi đó NIDS tập trung vào cả mạng lớn có các host đó. HIDS cụ thể hơn đối với các nền ứng dụng và phục vụ mạnh mẽ cho thị trường Windows.



Hình 1.7: Các HIDS trong hệ thống mạng

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



Hình 1.8: Các NNIDS trong hệ thống mạng

Tuy nhiên 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 1.9: So sánh Hệ thống phát hiện xâm nhập NIDS và HIDS

1.1.5 Ưu và nhược điểm của IDS

- **<u>Ưu điểm:</u>**

- 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: Một Host A nằm trên mạng Internet tạo ra một gói tin mạng (ngoài firewall), gói tin được gửi đến Host B nằm trong mạng nội bộ (có hệ thống IDS).

Bước 2: Các cảm biến trong mạng đọc các gói tin trong khoảng thời gian trước khi nó được gửi ra khỏi mạng cục bộ (cảm biến này cần phải được đặt sao cho nó có thể đọc tất cả các gói tin).

Bước 3: Chương trình phát hiện nằm trong bộ cảm biến kiểm tra xem có gói tin nào có dấu hiệu vi phạm hay không. Khi có dấu hiệu vi phạm thì một cảnh báo sẽ được tạo ra và gửi đến giao diện điều khiển.

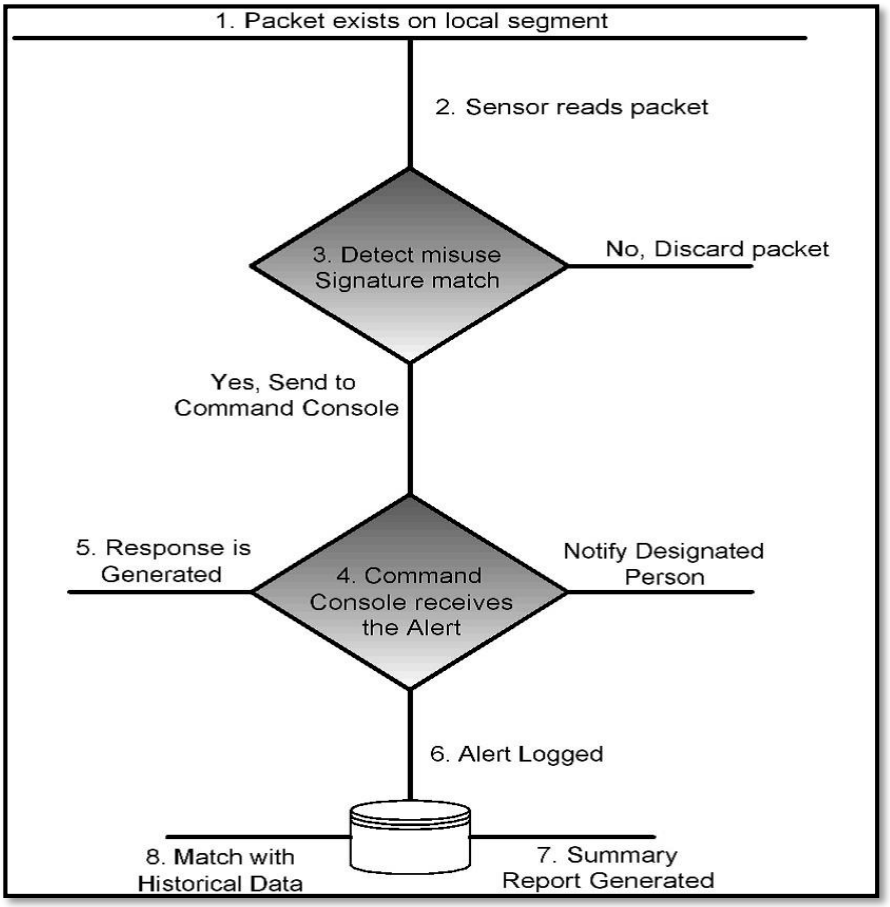
Bước 4: Khi giao diện điều khiển lệnh nhận được cảnh báo nó sẽ gửi thông báo cho một người hoặc một nhóm đã được chỉ định từ trước (thông qua email, cửa sổ popup, trang web v.v…).

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.



Hình 1.10: Quy trình hoạt động của IDS, IPS

1.2 Hệ thống Snort IDS

Một trong những phần mềm IDS phổ biến hiện nay là Snort. Đây là một sản phẩm NIDS mã nguồn mở với hệ thống signature database (được gọi là rule database) được cập nhật thường xuyên bởi nhiều thành viên trong cộng đồng Internet.

Snort đuợc thiết kế chính để thao tác bằng dòng lệnh (command line). Tuy nhiên nó có khả năng kết hợp với một phần mềm khác để tăng cường khả năng đa dạng của nó. Hiện nay Snort được sử dụng rộng rãi và là giải pháp mã nguồn mở tốt nhất.

1.2.1 Giới thiệu

Snort được phát triển từ năm 1998. Ban đầu nó chỉ được mong đợi với chức năng sniffer, tuy nhiên sau một thời gian phát triển nó trở thành một công cụ phát hiện xâm nhập mạnh mẽ và có thể thiết kế trên cả các máy trạm (HIDS) lẫn trên toàn hệ thống mạng (NIDS). Hiện nay Snort có thể chạy trên nhiều hệ thống nền như

Windows, Linux, OpenBSD, FreeBSD, NetBSD, Solaris, HP-UX, AIX, IRIX, MacOS.

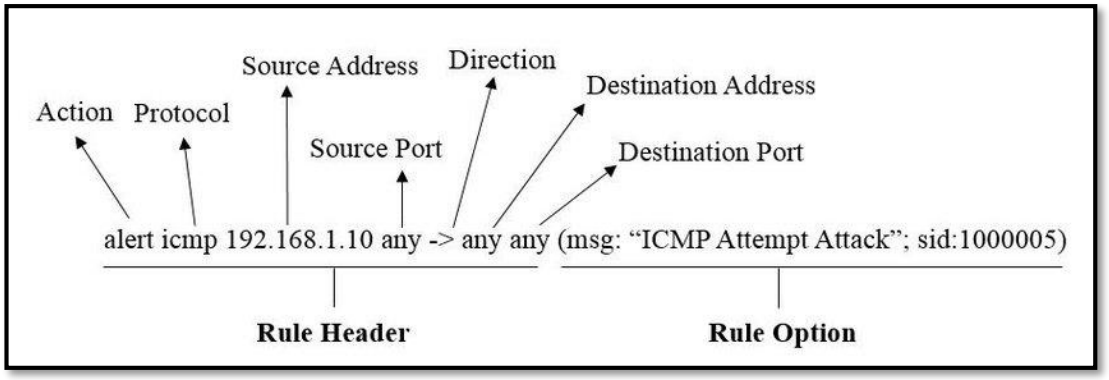
Tuy Snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời mà không phải sản phẩm thương mại nào cũng có thể có được. Với kiến trúc thiết kế theo kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình bằng việc cài đặt hay viết thêm mới các module.

Bên cạnh việc có thể hoạt động như một ứng dụng thu bắt gói tin thông thường, Snort còn có thể được cấu hình để chạy như một NIDS. Snort hỗ trợ khả năng hoạt động trên các giao thức sau: Ethernet, 802.11, Token Ring, FDDI, Cisco HDLC, SLIP, PPP, và PF của OpenBSD.

1.2.2 Luật trong Snort

Cũng giống như virus, hầu hết các hoạt động tấn công hay xâm nhập đều có các dấu hiệu riêng. Các thông tin về các dấu hiệu này sẽ được sử dụng để tạo nên các luật cho Snort. Thông thường, các bẫy (honey pots) được tạo ra để tìm hiểu xem các kẻ tấn công làm gì cũng như các thông tin về công cụ và công nghệ chúng sử dụng. Và ngược lại, cũng có các cơ sở dữ liệu về các lỗ hổng bảo mật mà những kẻ tấn công muốn khai thác. Các dạng tấn công đã biết này được dùng như các dấu hiệu để phát hiện tấn công xâm nhập. Các dấu hiệu đó có thể xuất hiện trong phần header của các gói tin hoặc nằm trong phần nội dung của chúng. 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.

Hãy xem xét một ví dụ đơn giản:



Hình 1.11: Luật trong Snort

Luật của Snort về logic đều gồm 2 phần: Phần Header và phần Option.

- Phần Header chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa các tiêu chuẩn để áp dụng luật với gói tin đó.
- Phần Option chứa một thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh luật với gói tin. Một luật có thể phát hiện được một hay nhiều hoạt động thăm dò hay tấn công. Các luật thông minh có khả năng áp dụng cho nhiều dấu hiệu xâm nhập.

Action	Protocol	Address	Port	Direction	Address	Port

Hình 1.12: Header luật của Snort

• Action: Phần qui định loại hành động nào được thực thi khi các dấu hiệu của gói tin được nhận dạng chính xác bằng luật đó. Thông thường, các hành động tạo ra một cảnh báo hoặc log thông điệp hoặc kích hoạt một luật khác.

• Protocol: Phần qui định việc áp dụng luật cho các packet chỉ thuộc một giao thức cụ thể nào đó. Ví dụ như *IP, TCP, UDP* ...

• Address: Phần địa chỉ nguồn và địa chỉ đích. Các địa chỉ có thể là một máy đơn, nhiều máy hoặc của một mạng nào đó. Trong hai phần địa chỉ trên

thì một sẽ là địa chỉ nguồn, một sẽ là địa chỉ đích và địa chỉ nào thuộc loại nào sẽ do phần Direction "➔" qui định.

• Port: Xác định các cổng nguồn và đích của một gói tin mà trên đó luật được áp dụng.

• Direction: Phần này sẽ chỉ ra đâu là địa chỉ nguồn, đâu là địa chỉ đích.

Ví dụ: *alert icmp any any -> any any (msg: "Ping with TTL=100";ttl: 100;)*

Phần đứng trước dấu mở ngoặc là phần Header của luật còn phần còn lại là phần Option. Chi tiết của phần Header như sau:

• Hành động của luật ở đây là ***"alert"***: một cảnh báo sẽ được tạo ra nếu như các điều kiện của gói tin là phù hợp với luật (gói tin luôn được log lại mỗi khi cảnh báo được tạo ra).

• Protocol của luật ở đây là ICMP tức là luật chỉ áp dụng cho các gói tin thuộc loại ICMP. Bởi vậy, nếu như một gói tin không thuộc loại ICMP thì phần còn lại của luật sẽ không cần đối chiếu.

• Địa chỉ nguồn ở đây là **"*any*"**: Tức là luật sẽ áp dụng cho tất cả các gói tin đến từ mọi nguồn còn cổng thì cũng là ***"any"*** vì đối với loại gói tin ICMP thì cổng không có ý nghĩa. Số hiệu cổng chỉ có ý nghĩa với các gói tin thuộc loại TCP hoặc UDP thôi.

• Còn phần Option trong dấu đóng ngoặc chỉ ra một cảnh báo chứa dòng "*Ping with TTL=100*" sẽ được tạo khi tìm thấy điều kiện *TTL=100*. TTL là Time to Live là một trường trong Header IP.

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. Một hành động được thực hiện khi và chỉ khi tất cả các điều kiện đều phù hợp. Có 5 hành động đã được định nghĩa nhưng chúng ta có thể tạo ra các hành động riêng tuỳ thuộc vào yêu cầu của mình. Đối

với các phiên bản trước của Snort thì khi nhiều luật là phù hợp với một gói tin nào đó thì chỉ một luật được áp dụng. Sau khi áp dụng luật đầu tiên thì các luật tiếp theo sẽ không áp dụng cho gói tin ấy nữa. Nhưng đối với các phiên bản sau của Snort thì tất cả các luật sẽ được áp dụng gói tin đó.

• Pass: Hành động này hướng dẫn Snort bỏ qua gói tin này. Hành động này đóng vai trò quan trọng trong việc tăng cường tốc độ hoạt động của Snort khi mà chúng ta không muốn áp dụng các kiểm tra trên các gói tin nhất định.

Ví dụ: Chúng ta sử dụng các bẫy (đặt trên một máy nào đó) để nhử các tin tặc tấn công vào thì chúng ta phải cho tất cả các gói tin đi đến được máy đó. Hoặc là dùng một máy quét để kiểm tra độ an toàn mạng của mình thì chúng ta phải bỏ qua tất cả các gói tin đến từ máy kiểm tra đó.

• Log: Hành động này dùng để log gói tin. Có thể log vào file hay vào cơ sở dữ liệu tuỳ thuộc vào nhu cầu của mình.

• Alert: Gửi một thông điệp cảnh báo khi dấu hiệu xâm nhập được phát hiện. Có nhiều cách để gửi thông điệp như gửi ra file hoặc ra một Console. Tất nhiên là sau khi gửi thông điệp cảnh báo thì gói tin sẽ được log lại.

• Activate: sử dụng để tạo ra một cảnh báo và kích hoạt một luật khác kiểm tra thêm các điều kiện của gói tin.

• Dynamic: chỉ ra đây là luật được gọi bởi các luật khác có hành động là Activate. Các hành động do người dùng định nghĩa: một hành động mới được định nghĩa theo cấu trúc sau:

```
ruletype action_name
{
action definition
}
```

Trong đó: Ruletype là từ khoá.

Hành động được định nghĩa chính xác trong dấu ngoặc nhọn: có thể là một hàm viết bằng ngôn ngữ C.

Ví dụ:

```
ruletype smb_db_alert
{
type alert
output alert_smb: workstation.list
output database: log, mysql, user=test password=test
dbname=snort host = localhost  }
```

Đây là hành động có tên là ***smb_db_alert*** dùng để gửi thông điệp cảnh báo dưới dạng cửa sổ pop-up SMB tới các máy có tên trong danh sách liệt kê trong file ***workstation.list*** và tới cơ sở dữ liệu MySQL tên là Snort.

b) Protocols

Là phần thứ hai của một luật có chức năng chỉ ra loại gói tin mà luật sẽ được áp dụng. Hiện tại Snort hiểu được các protocol sau:

- IP
- ICMP
- TCP
- UDP

Nếu là IP thì Snort sẽ kiểm tra Header của lớp liên kết để xác định loại gói tin. Nếu bất kì giao thức nào khác được sử dụng thì Snort sử dụng Header IP để xác định loại Protocol. Protocol chỉ đóng vai trò trong việc chỉ rõ tiêu chuẩn trong phần Header của luật. Phần Option của luật có thể có các điều kiện không liên quan gì đến Protocol.

c) Address

Có hai phần địa chỉ trong một luật của Snort. Các địa chỉ này được dùng để kiểm tra nguồn sinh ra và đích đến của gói tin. Địa chỉ có thể là địa chỉ của một IP đơn hoặc là địa chỉ của một mạng. Chúng ta có thể dùng từ any để áp dụng luật cho tất cả các địa chỉ. Địa chỉ được viết ngay theo sau một dấu gạch chéo và số bít trong Subnet mask.

Ví dụ: Địa chỉ *192.168.2.0/24* thể hiện mạng lớp C *192.168.2.0* với 24 bít của Subnet mask. Subnet mask 24 bit chính là *255.255.255.0*. Chúng ta biết rằng :

- *Nếu subnet mask là 24 bít thì đó là mạng lớp C*
- *Nếu subnet mask là 16 bít thì đó là mạng lớp B*
- *Nếu subnet mask là 8 bít thì đó là mạng lớp A*
- *Nếu subnet mask là 32 bít thì đó là địa chỉ IP đơn.*

Trong hai địa chỉ của một luật Snort thì có một địa chỉ là địa chỉ nguồn và địa chỉ còn lại là địa chỉ đích. Việc xác định đâu là địa chỉ nguồn, đâu là địa chỉ đích thì phụ thuộc vào phần Hướng (Direction).

Ví dụ: *alert tcp any any -> 192.168.1.10/32 80 (msg: "TTL=100"; ttl: 100;)*

Luật trên sẽ tạo ra một cảnh báo đối với tất cả các gói tin từ bất kì nguồn nào có TTL = 100 đi đến Web Server 192.168.1.10 tại cổng 80.

d) Ngăn chặn địa chỉ hay loại trừ địa chỉ

Snort cung cấp cho chúng ta kĩ thuật để loại trừ địa chỉ bằng cách sử dụng dấu phủ định (dấu !). Dấu phủ định này đứng trước địa chỉ sẽ chỉ cho Snort không kiểm tra các gói tin đến từ hay đi tới địa chỉ đó. Ví dụ, luật sau sẽ áp dụng cho tất cả các gói tin ngoại trừ các gói có nguồn xuất phát từ mạng lớp C *192.168.2.0*.

alert icmp ![192.168.2.0/24] any -> any any (msg: "Ping with TTL=100"; ttl: 100;).

e) Danh sách địa chỉ

Chúng ta có thể định rõ ra danh sách các địa chỉ trong một luật của Snort. Ví dụ nếu bạn muốn áp dụng luật cho tất cả các gói tin trừ các gói xuất phát từ hai mạng lớp C *192.168.2.0* và *192.168.8.0* thì luật được viết như sau:

alert icmp ![192.168.2.0/24, 192.168.8.0/24] any -> any any (msg: "Ping with TTL=100"; ttl: 100;)

Hai dấu **[]** chỉ cần dùng khi có dấu **!** đứng trước.

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. Ví dụ chúng ta có thể sử dụng số cổng nguồn là

23 để áp dụng luật cho tất cả các gói tin đến từ một Server Telnet. Từ **any** cũng được dùng để đại diện cho tất cả các cổng. Chú ý là số hiệu cổng chỉ có ý nghĩa trong các giao thức TCP và UDP thôi. Nếu Protocol của luật là IP hay ICMP thì số hiệu cổng không đóng vai trò gì cả.

Ví dụ : *alert tcp 192.168.2.0/24 23 -> any any (content: "confidential"; msg: "Detected confidential";)*

Số hiệu cổng chỉ hữu dụng khi chúng ta muốn áp dụng một luật chỉ cho một loại gói tin dữ liệu cụ thể nào đó. Ví dụ như là một luật để chống hack cho web thì chúng ta chỉ cần sử dụng cổng 80 để phát hiện tấn công.

g) Dãy cổng hay phạm vi cổng

Chúng 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 ":".

Ví dụ : *alert udp any 1024:2048 -> any any (msg: "UDP ports";)*

Chúng ta cũng có thể dùng cổng theo kiểu cận trên và cận dưới, tức là chỉ sử dụng cổng bắt đầu hoặc cổng kết thúc mà thôi. Ví dụ như là "1024:" hoặc là ":2048". Dấu phủ định cũng được áp dụng trong việc sử dụng cổng.

Ví dụ sau sẽ log tất cả các gói tin ngoại trừ các gói tin xuất phát từ cổng 53.

log udp any !53 -> any any log udp

Sau đây là một số cổng thông dụng hay là các cổng của các dịch vụ thông dụng nhất :

- 20 FPT DATA
- 21 FPT
- 22 SSH
- 23 Telnet
- 24 SMTP
- 53 DNS Server
- 80 HTTP

- 110 POP3
- 161 SNMP
- 443 HTTPS
- 3360 My SQL

h) Hướng - Direction

Chỉ ra đâu là nguồn đâu là đích, có thể là -> hay <- hoặc <>. Trường hợp <> là khi chúng 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 có nhiều Option thì các Option sẽ được phân cách với nhau bằng dấu chấm phẩy ”;”. 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.

Ví dụ: *msg: “Detected confidented”;*

Trong đó: *msg* là từ khoá; *“Detected confidented”* là tham số.

Sau đây là chi tiết một số các Option của luật Snort:

a) Từ khoá ack

Trong header TCP có chứa trường Acknowledgement Number với độ dài 32 bit. Trường này có ý nghĩa là chỉ ra số thứ tự tiếp theo gói tin TCP của bên gửi đang được chờ để nhận. Trường này chỉ có ý nghĩa khi mà cờ ACK được thiết lập.

Các công cụ như Nmap sử dụng đặc điểm này ping một máy. Ví dụ, nó có thể gửi một gói tin TCP tới cổng 80 với cờ ACK được bật và số thứ tự là 0. Bởi vậy, bên nhận sẽ thấy gói tin không hợp lệ và sẽ gửi trở lại gói tin RST. Khi mà Nmap nhận được gói tin RST thì tức là địa chỉ đích đang “sống”. Phương pháp này vẫn làm việc tốt đối với các máy không trả lời gói tin thuộc dạng ping ICMP ECHO REQUEST.

Vậy để kiểm tra loại ping TCP này thì chúng ta có thể dùng luật như sau:

alert tcp any any -> 192.168.1.0/24 any (flags: A; ack: 0; msg: "TCP ping detected")

b) Từ khoá classtype

Các luật có thể được phân loại và gán cho một số chỉ độ ưu tiên nào đó để nhóm và phân biệt chúng với nhau. Để hiểu rõ hơn về từ khoá này chúng ta đầu tiên phải hiểu được file *classification.config* (được bao gồm trong file *snort.conf* sử dụng từ khoá include). Mỗi dòng trong file *classification.config* có cú pháp như sau:

config classification: name, description, priority.

Trong đó:

- name: Tên dùng để phân loại, tên này sẽ được dùng với từ khoá classtype trong các luật Snort.
- description: Mô tả về loại lớp này
- priority: Số chỉ độ ưu tiên mặc định của lớp này. Độ ưu tiên này có thể được điều chỉnh trong từ khoá priority của phần option trong luật của Snort.

Ví dụ:

config classification: DoS , Denial of Service Attack, 2 và trong luật:

alert udp any any -> 192.168.1.0/24 6838 (msg:"DoS"; content: "server"; classtype: DoS;)

alert udp any any -> 192.168.1.0/24 6838 (msg:"DoS"; content: "server";

classtype: DoS; priority: 1;)

Trong câu lệnh thứ 2 thì chúng ta đã ghi đè lên giá trị priority mặc định của lớp đã định nghĩa.

c) Từ khoá content

Một đặc tính quan trọng của Snort là nó có khả năng tìm một mẫu dữ liệu bên trong một gói tin. Mẫu này có thể dưới dạng chuỗi ASCII hoặc là một chuỗi nhị phân dưới dạng các kí tự hệ 16. Giống như virus, các tấn công cũng có các dấu hiệu nhận dạng và từ khoá content này dùng để tìm các dấu hiệu đó bên trong gói tin.

Ví dụ: *alert tcp 192.168.1.0/24 any -> ![192.168.1.0/24] any (content: "GET"; msg: "GET match";)*

Luật trên tìm mẫu "GET" trong phần dữ liệu của tất cả các gói tin TCP có nguồn đi từ mạng 192.168.1.0/24 và đi đến các địa chỉ không thuộc mạng đó. Từ "GET" này rất hay được dùng trong các tấn công HTTP. Một luật khác cũng thực hiện đúng nhiệm vụ giống như lệnh trên nhưng mẫu dữ liệu lại dưới dạng hệ 16 là: *alert tcp 192.168.1.0/24 any -> ![192.168.1.0/24] any (content: "|47 45 54|"; msg: "GET match";)*

Để ý rằng số 47 ở hệ 16 chính là bằng kí tự ASCII : G và tương tự 45 là E và 54 là T. Chúng ta có thể dùng cả hai dạng trên trong cùng một luật nhưng nhớ là phải để dạng thập lục phân giữa cặp kí tự ||. Tuy nhiên khi sử dụng từ khoá content chúng ta cần nhớ rằng:

Đối sánh nội dung sẽ phải xử lý tính toán rất lớn và chúng ta phải hết sức cân nhắc khi sử dụng nhiều luật có đối sánh nội dung. Chúng ta có thể sử dụng nhiều từ khoá content trong cùng một luật để tìm nhiều dấu hiệu trong cùng một gói tin. Đối sánh nội dung là công việc rất nhạy cảm. Có 3 từ khoá khác hay được dùng cùng với từ khoá content dùng để bổ sung thêm các điều kiện để tìm kiếm là :

- offset: Dùng để xác định vị trí bắt đầu tìm kiếm (chuỗi chứa trong từ khoá content) là offset tính từ đầu phần dữ liệu của gói tin.

  Ví dụ sau sẽ tìm chuỗi "HTTP" bắt đầu từ vị trí cách đầu đoạn dữ liệu của gói tin là 4 byte:

  alert tcp 192.168.1.0/24 any -> any any (content: "HTTP"; offset: 4; msg: "HTTP matched")

- dept: Dùng để xác định vị trí mà từ đó Snort sẽ dừng việc tìm kiếm từ khoá này cũng thường được dùng chung với từ khoá offset vừa nêu trên.

  Ví dụ:

  alert tcp 192.168.1.0/24 any -> any any (content: "HTTP"; offset: 4; dept: 40; msg: "HTTP matched").

Từ khoá này sẽ giúp cho việc tiêu tốn thời gian tìm kiếm khi mà đoạn dữ liệu trong gói tin là khá lớn.

- content-list: Được sử dụng cùng với một file. Tên file (được chỉ ra trong phần tham số của từ khoá này) là một file text chứa danh sách các chuỗi cần tìm trong phần dữ liệu của gói tin. Mỗi chuỗi nằm trên một dòng riêng biệt.

Ví dụ: File test có dạng như sau:

"test"

"Snort"

"NIDS"

và chúng ta có luật sau:

alert tcp 192.168.1.0/24 any -> any any (content-list: "test";msg: "This is my Test";).

Chúng ta cũng có thể dùng kí tự phủ định ! trước tên file để cảnh báo đối với các gói tin không tìm thấy một chuỗi nào trong file đó.

d) Từ khoá dsize

Dùng để đối sánh theo chiều dài của phần dữ liệu. Rất nhiều tấn công sử dụng lỗi tràn bộ đệm bằng cách gửi các gói tin có kích thước rất lớn. Sử dụng từ khoá này, chúng ta có thể so sánh độ lớn của phần dữ liệu của gói tin với một số nào đó.

alert ip any any -> 192.168.1.0/24 any (dsize: > 6000; msg: "Goi tin co kich thuoc lon";)

e) Từ khoá flags

Từ khoá này được dùng để phát hiện xem những bit cờ flag nào được bật (thiết lập) trong phần TCP header của gói tin. Mỗi cờ có thể được sử dụng như một tham số trong từ khoá flags. Sau đây là một số các cờ sử dụng trong từ khoá flags:

Flag	**Kí tự tham số dùng trong luật của Snort**
FIN (Finish Flag)	F
SYN - Sync Flag	S

RST - Reset Flag	R
PSH - Push Flag	P
ACK – Acknowledgment Flag	A
URG - Urgent Flag	U
Reserved Bit 1	1
Reserved Bit 2	2
No Flag set	0

Hình 1.13: Các cờ sử dụng với từ khoá Flags

Chúng ta có thể sử dụng các dấu +, * và ! để thực hiện các phép toán logic AND, OR và NOT trên các bit cờ muốn kiểm tra. Ví dụ luật sau đây sẽ phát hiện một hành động quét dùng gói tin TCP SYN-FIN:

alert tcp any any -> 192.168.1.0/24 any (flags: SF; msg: "SYNC-FIN packet detected";)

f) Từ khoá fragbits

Phần IP header của gói tin chứa 3 bit dùng để chống phân mảnh và tổng hợp các gói tin IP. Các bit đó là:

- Reserved Bit (RB) dùng để dành cho tương lai.
- Don't Fragment Bit (DF): nếu bit này được thiết lập thì tức là gói tin đó không bị phân mảnh.
- More Fragments Bit (MF): nếu được thiết lập thì tức là các phần khác (gói tin bị phân mảnh) của gói tin vẫn đang còn trên đường đi mà chưa tới đích. Nếu bit này không được thiết lập thì có nghĩa là đây là phần cuối cùng của gói tin (hoặc là gói duy nhất). Điều này xuất phát từ nguyên nhân: Nơi gửi đi phải chia gói tin IP thành nhiều đoạn nhỏ do phụ thuộc vào Đơn vị truyền dữ liệu lớn nhất cho phép (Maximum Transfer Units - MTU) trên đường truyền. Kích thước của gói tin không được phép vượt quá kích thước lớn nhất này. Do vậy, bit MF này giúp bên đích có thể tổng hợp lại các phần khác nhau thành một gói tin hoàn chỉnh.

Đôi khi các bit này bị các tin tặc sử dụng để tấn công và khai thác thông tin trên mạng của chúng ta. Ví dụ, bit DF có thể được dùng để tìm MTU lớn nhất và nhỏ nhất trên đường đi từ nguồn xuất phát đến đích đến. Sử dụng fragbits, chúng ta có thể kiểm tra xem các bit trên có được thiết lập hay không. Ví dụ luật sau sẽ phát hiện xem bit DF trong gói tin ICMP có được bật hay không:

alert icmp any any -> 192.168.1.0/24 any (fragbits: D; msg: "Dont Fragment bit set";)

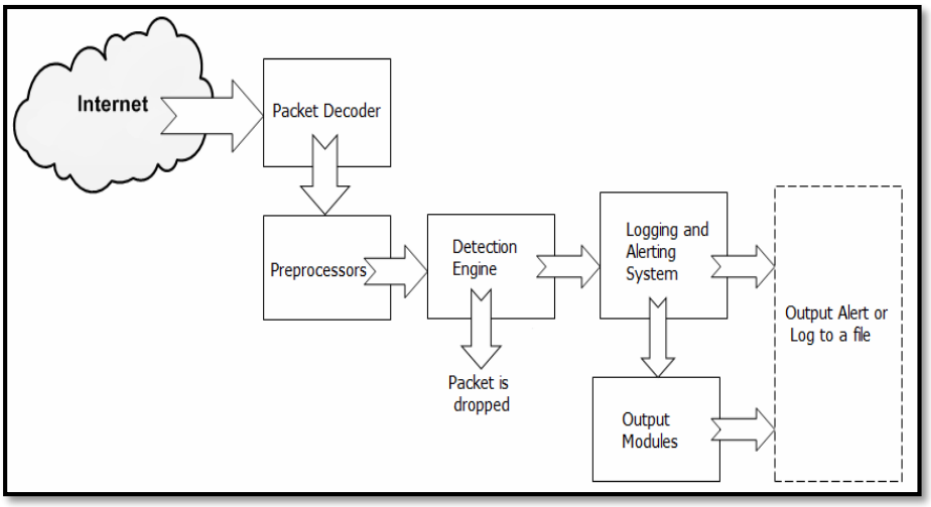
Trong luật này, D dùng cho bit DF, R cho bit dự trữ và M cho bit MF. Chúng ta cũng có thể dùng dấu phủ định ! trong luật này để kiểm tra khi bit không được bật: *alert icmp any any -> 192.168.1.0/24 any (fragbits: !D; msg: "Dont Fragment bit not set";)*

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:

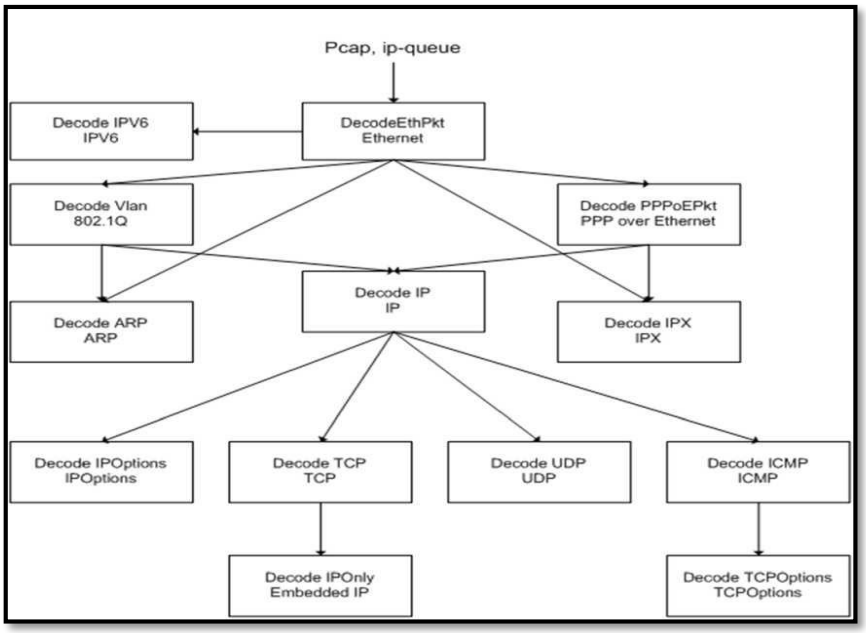
- Module giải mã gói tin (Packet Decoder)
- Module tiền xử lý (Preprocessors)
- Module phát hiện (Detection Engine)
- Module log và cảnh báo (Logging and Alerting System)
- Module kết xuất thông tin (Output Module)

Khi Snort hoạt động nó sẽ thực hiện việc lắng nghe và thu bắt tất cả các gói tin nào di chuyển qua. Các gói tin sau khi bị bắt được đưa vào Module Giải mã gói tin. Tiếp theo gói tin sẽ được đưa vào Module Tiền xử lý, rồi Module Phát hiện. Tại đây tùy theo việc có phát hiện được xâm nhập hay không mà gói tin có thể được bỏ qua để lưu thông tiếp hoặc được đưa vào Module Log và cảnh báo để xử lý. Khi các cảnh báo được xác định Module Kết xuất thông tin sẽ thực hiện việc đưa cảnh báo ra theo đúng định dạng mong muốn.



Hình 1.14: Kiến trúc của Snort

1.2.3.1 Module giải mã gói tin (Packet Decoder)



Hình 1.15: Giải mã gói tin Ethernet

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. Ba nhiệm vụ chính của các Module loại này là:

- Kết hợp lại các gói tin: Khi một lượng dữ liệu lớn được gửi đi, thông tin sẽ không đóng gói toàn bộ vào một gói tin mà phải thực hiện việc phân mảnh, chia gói tin ban đầu thành nhiều gói tin rồi mới gửi đi. Khi Snort nhận được các gói tin này nó phải thực hiện việc ghép nối lại để có được dữ liệu nguyên dạng ban đầu, từ đó mới thực hiện được các công việc xử lý tiếp. Như chúng ta đã biết khi một phiên làm việc của hệ thống diễn ra, sẽ có rất nhiều gói tin được trao đổi trong phiên đó. Một gói tin riêng lẻ sẽ không có trạng thái và nếu công việc phát hiện xâm nhập chỉ dựa hoàn toàn vào gói tin đó sẽ không đem lại hiệu quả cao. Module tiền xử lý stream giúp Snort có thể hiểu được các phiên làm việc khác nhau (nói cách khác đem lại tính có trạng thái cho các gói tin) từ đó giúp đạt được hiệu quả cao hơn trong việc phát hiện xâm nhập.
- Giải mã và chuẩn hóa giao thức (decode/normalize): Công việc phát hiện xâm nhập dựa trên dấu hiệu nhận dạng nhiều khi bị thất bại khi kiểm tra các giao thức có dữ liệu có thể được thể hiện dưới nhiều dạng khác nhau. Ví dụ: một web server có thể chấp nhận nhiều dạng URL như URL được viết dưới dạng mã hexa/Unicode, URL chấp nhận cả dấu \ hay / hoặc nhiều ký tự này liên tiếp cùng lúc. Chẳng hạn chúng ta có dấu hiệu nhận dạng “scripts/iisadmin”, kẻ tấn công có thể vượt qua được bằng cách tùy biến các yêu cầu gửi đến web server như sau:

  “scripts/./iisadmin”
  “scripts/examples/../iisadmin”
  “scripts\iisadmin” “scripts/.\iisadmin”

Hoặc thực hiện việc mã hóa các chuỗi này dưới dạng khác: Nếu Snort chỉ thực hiện đơn thuần việc so sánh dữ liệu với dấu hiệu nhận dạng sẽ xảy ra tình trạng bỏ sót các hành vi xâm nhập. Do vậy, một số Module tiền xử lý của Snort phải có nhiệm

vụ giải mã và chỉnh sửa, sắp xếp lại các thông tin đầu vào này để thông tin khi đưa đến Module phát hiện có thể phát hiện được mà không bỏ sót. Hiện nay Snort đã hỗ trợ việc giải mã và chuẩn hóa cho các giao thức: telnet, http, rpc, arp.

- Phát hiện các xâm nhập bất thường (nonrule/anormal): Các plugin tiền xử lý dạng này thường dùng để đối phó với các xâm nhập không thể hoặc rất khó phát hiện được bằng các luật thông thường hoặc các dấu hiệu bất thường trong giao thức. Các Module tiền xử lý dạng này có thể thực hiện việc phát hiện xâm nhập theo bất cứ cách nào mà chúng ta nghĩ ra từ đó tăng cường thêm tính năng cho Snort. Ví dụ, một plugin tiền xử lý có nhiệm vụ thống kê thông lượng mạng tại thời điểm bình thường để rồi khi có thông lượng mạng bất thường xảy ra nó có thể tính toán, phát hiện và đưa ra cảnh báo (phát hiện xâm nhập theo mô hình thống kê). Phiên bản hiện tại của Snort có đi kèm hai plugin giúp phát hiện các xâm nhập bất thường đó là portscan và bo (backoffice). Portcan dùng để đưa ra cảnh báo khi kẻ tấn công thực hiện việc quét các cổng của hệ thống để tìm lỗ hổng. Bo dùng để đưa ra cảnh báo khi hệ thống đã bị nhiễm trojan backoffice và kẻ tấn công từ xa kết nối tới backoffice thực hiện các lệnh từ xa.

1.2.3.3 Module phát hiện (Detection Engine)

. Trách nhiệm của nó là 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. Nếu gói tin là phù hợp với rule, hành động thích hợp được thực hiện.

Hiệu suất hoạt động của bộ phận này phụ thuộc các yếu tố như: Số lượng rule, cấu hình máy mà Snort đang chạy, tốc độ bus sử dụng cho máy Snort, lưu lượng mạng.

Detection Engine có thể phân chia gói tin và áp dụng rule cho các phần khác nhau của gói tin. Các phần đó có thể là:

- Phần IP header của gói tin.
- Phần header của tầng transport: Đây là phần tiêu đề bao gồm TCP, UDP hoặc các header của tầng transport khác. Nó cũng có thể làm việc với header của ICMP.

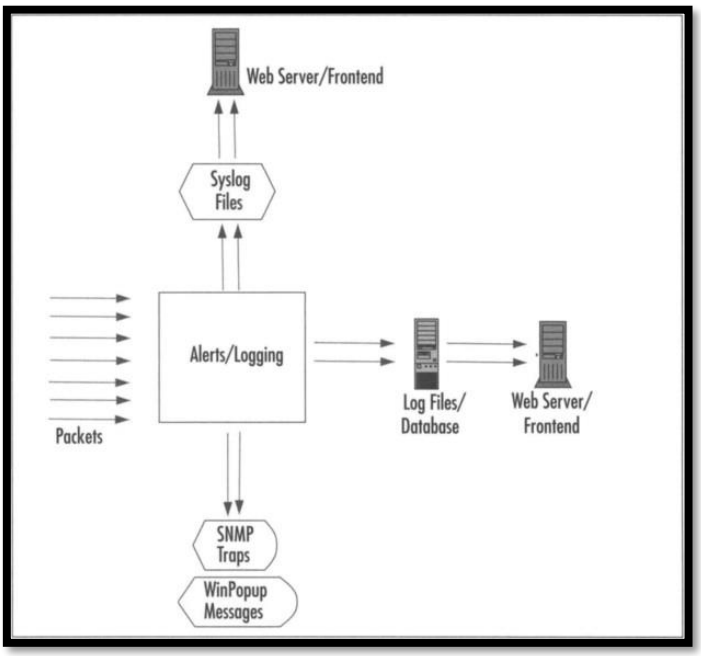
- Phần header của các lớp ứng dụng: Bao gồm header của lớp ứng dụng, nhưng không giới hạn, DNS header, FTP header, SNMP header, và SMTP header.
- Packet payload: Có nghĩa là có thể tạo ra rule được sử dụng bởi detection engine để tìm kiếm một chuỗi bên trong dữ liệu của gói tin.
- Một vấn đề nữa trong Module phát hiện đó là việc xử lý thế nào khi một gói tin bị phát hiện bởi nhiều luật. Do các luật trong Snort cũng được đánh thứ tự ưu tiên, nên một gói tin khi bị phát hiện bởi nhiều luật khác nhau, cảnh báo được đưa ra sẽ là cảnh báo ứng với luật có mức ưu tiên lớn nhất.

Bộ phận này hoạt động theo hai cách khác nhau theo hai phiên bản của Snort. ·
+ Phiên bản 1.x: Việc xử lý gói tin còn hạn chế trong trường hợp các dấu hiệu trong gói tin đó phù hợp với dấu hiệu trong nhiều rule. Khi đó nếu có rule nào được áp dụng trước thì các rule còn lại sẽ bị bỏ qua mặc dù các rule có độ ưu tiên khác nhau. Như vậy sẽ nảy sinh trường hợp các rule có độ ưu tiên cao hơn bị bỏ qua.
+ Phiên bản 2.x: Nhược điểm trên của phiên bản 1.x được khắc phục hoàn toàn nhờ vào cơ chế kiểm tra trên toàn bộ rule. Sau đó lấy ra rule có độ ưu tiên cao nhất để tạo thông báo.

Tốc độ của phiên bản 2.x nhanh hơn rất nhiều so với phiên bản 1.x nhờ phiên bản 2.x được biên dịch lại.

1.2.3.4 Modul 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.



Hình 1.16: Module Log và Cảnh báo

1.2.3.5 Modul 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. Tùy theo việc cấu hình hệ thống mà nó có thể thực hiện các công việc như:

- Ghi log file.
- Ghi syslog: Syslog và một chuẩn lưu trữ các file log được sử dụng rất nhiều trên các hệ thống Unix, Linux.
- Ghi cảnh báo vào cơ sở dữ liệu.
- Tạo file log dạng xml: Ghi log file dạng xml cho việc trao đổi và chia sẻ dữ liệu.
- Cấu hình lại Router, firewall.
- Gửi các cảnh báo được gói trong gói tin sử dụng giao thức.
- SNMP: Các gói tin dạng SNMP này sẽ được gửi tới một SNMP server từ đó giúp cho việc quản lý các cảnh báo và hệ thống IDS một cách tập trung và thuận tiện hơn.
- Gửi các thông điệp SMB (Server Message Block) tới các máy tính Windows.

1.2.4 Chế độ hoạt động của Snort

1.2.4.1 Snort Sniffer mode

Ở chế độ này, 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:

- Date and time
- Source IP address
- Source port number
- Destination IP address
- Destination port
- Transport layer protocol used in this packet
- Time to live or TTL value in this packet
- Type of service or TOS value
- Packet ID
- Length of IP header
- IP payload

1.2.4.2 Packet logger mode

Khi chạy ở chế độ này, Snort sẽ tập hợp tất cả các packet nó thấy được và đưa vào log theo cấu trúc phân tầng. Nói cách khác, 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. Snort đặt các packet vào trong file ASCII, với tên liên quan đến giao thức và cổng. Sự sắp xếp này dễ dàng nhận ra ai đang kết nối vào mạng của mình và giao thức, cổng nào đang sử dụng.

Đơn giản sử dụng ls-R để hiện danh sách các thư mục. Tuy nhiên sự phân cấp này sẽ tạo ra nhiều thư mục trong giờ cao điểm nên rất khó để xem hết tất cả thư mục và file này.

Nếu ai đó sử dụng full scan với 65536 TCP Port và 65535 UDP ports và sẽ tạo ra 131000 hoặc từng ấy file.

Log với dạng nhị phân (binary) tất cả những gì có thể đọc được bởi Snort, nó làm tăng tốc khả năng bắt gói tin của Snort. Hầu hết các hệ thống có thể capture và log ở tốc độ 100Mbps mà không có vấn đề gì. Để log packet ở chế độ nhị phân, sử dụng cờ -b:

#Snort -b -l /usr/local/log/Snort/temp.log

Khi đã capture, chúng ta có thể đọc lại file mới vừa tạo ra ngay với cỡ -r và phần hiển thị giống như ở mode sniffer:

#Snort -r /usr/local/log/Snort/temp.log

Trong phần này Snort không giới hạn để đọc các file binary trong chế độ sniffer. Chúng ta có thể chạy Snort ở chế độ NIDS với việc set các rule hoặc filters để tìm những traffic nghi ngờ.

1.2.4.3 NIDS mode

Snort thường được sử dụng như một NIDS. Nó nhẹ, nhanh chóng, hiệu quả và sử dụng các rule để áp dụng lên gói tin. 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. Thông tin về thông báo khi hoạt động ở chế độ này:

+ Fast mode: Date and time, Alert message, Source and destination IP address, Source and destination ports, Type of packet.

+ Full mode: Gồm các thông tin như chế độ fast mode và thêm một số thông tin sau: TTL value, TOS value, Length of Packet header, Length of packet, Type of packet, Code of packet, ID of packet, Sequence number.

1.2.4.4 Inline mode

Đây là 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
  + Tiếp nhận tất cả các trường hợp người bệnh từ ngoài vào hoặc từ các bệnh viện khác chuyển đến để cấp cứu, khám bệnh, chữa bệnh nội trú và ngoại trú.
  + Tổ chức khám sức khỏe và chứng nhận sức khỏe theo quy định của Nhà nước.

+ Có trách nhiệm giải quyết hầu hết các bệnh tật trong tỉnh và thành phố trực thuộc trung ương và các ngành.
+ Tổ chức khám giám định sức khỏe, khám giám định pháp y khi hội đồng giám định y khoa tỉnh, thành phố hoặc cơ quan bảo vệ pháp luật trưng cầu.
+ Chuyển người bệnh lên tuyến khi Bệnh viện không đủ khả năng giải quyết.

- Đào tạo cán bộ y tế
  + Bệnh viện là cơ sở thực hành đào tạo cán bộ y tế ở bậc đại học và trung học.
  + Tổ chức đào tạo liên tục cho các thành viên trong Bệnh viện và tuyến dưới để nâng cấp trình độ chuyên môn.

- Nghiên cứu khoa học về y học
  + Tổ chức nghiên cứu, hợp tác nghiên cứu các đề tài y học ở cấp Nhà nước, cấp Bộ hoặc cấp Cơ sở, chú trọng nghiên cứu về y học cổ truyền kết hợp với y học hiện đại và các phương pháp chữa bệnh không dùng thuốc
  + Nghiên cứu triển khai dịch tễ học cộng đồng trong công tác chăm sóc sức khỏe ban đầu lựa chọn ưu tiên thích hợp trong địa bàn tỉnh, thành phố và các ngành
  + Kết hợp với Bệnh viện tuyến trên và các Bệnh viện chuyên khoa đầu ngành để phát triển kỹ thuật của Bệnh viện.

- Chỉ đạo tuyến dưới về chuyên môn, kỹ thuật
  + Lập kế hoạch và chỉ đạo tuyến dưới (Bệnh viện hạng III) thực hiện việc phát triển kỹ thuật chuyên môn
  + Kết hợp với Bệnh viện tuyến dưới thực hiện các chương trình về chăm sóc sức khỏe ban đầu trong địa bàn tỉnh, thành phố và các ngành.

- Phòng bệnh

  Phối hợp với các cơ sở y tế dự phòng thường xuyên thực hiện nhiệm vụ phòng bệnh, phòng dịch.

- Hợp tác kinh tế y tế
    + Có kế hoạch sử dụng hiệu quả cao ngân sách Nhà nước cấp. Thực hiện nghiêm chỉnh các quy định của Nhà nước về thu, chi tài chính, từng bước thực hiện hạch toán chi phí khám bệnh, chữa bệnh.
    + Tạo thêm nguồn kinh phí từ các dịch vụ y tế: Viện phí, bảo hiểm y tế, đầu tư của nước ngoài và các tổ chức kinh tế khác

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. Kết hợp trung tâm tuyến huyện và cơ sở y tế tuyến xã, nâng cao khả năng phòng thủ của ngành y tế địa phương đối với các cuộc tấn công của tin tặc.

Nhận thấy sự cần thiết và khả năng áp dụng triển khai hệ thống giám sát mạng dành cho một Bệnh viện cấp tỉnh, học viên đã chọn Bệnh viện Đa khoa Tây Ninh – nơi học viên đang công tác, để triển khai đề xuất ứng dụng cảnh báo giám sát mạng dành cho bệnh viện đa khoa cấp tỉnh với mã nguồn mở.

2.2.1 Tóm tắt lịch sử

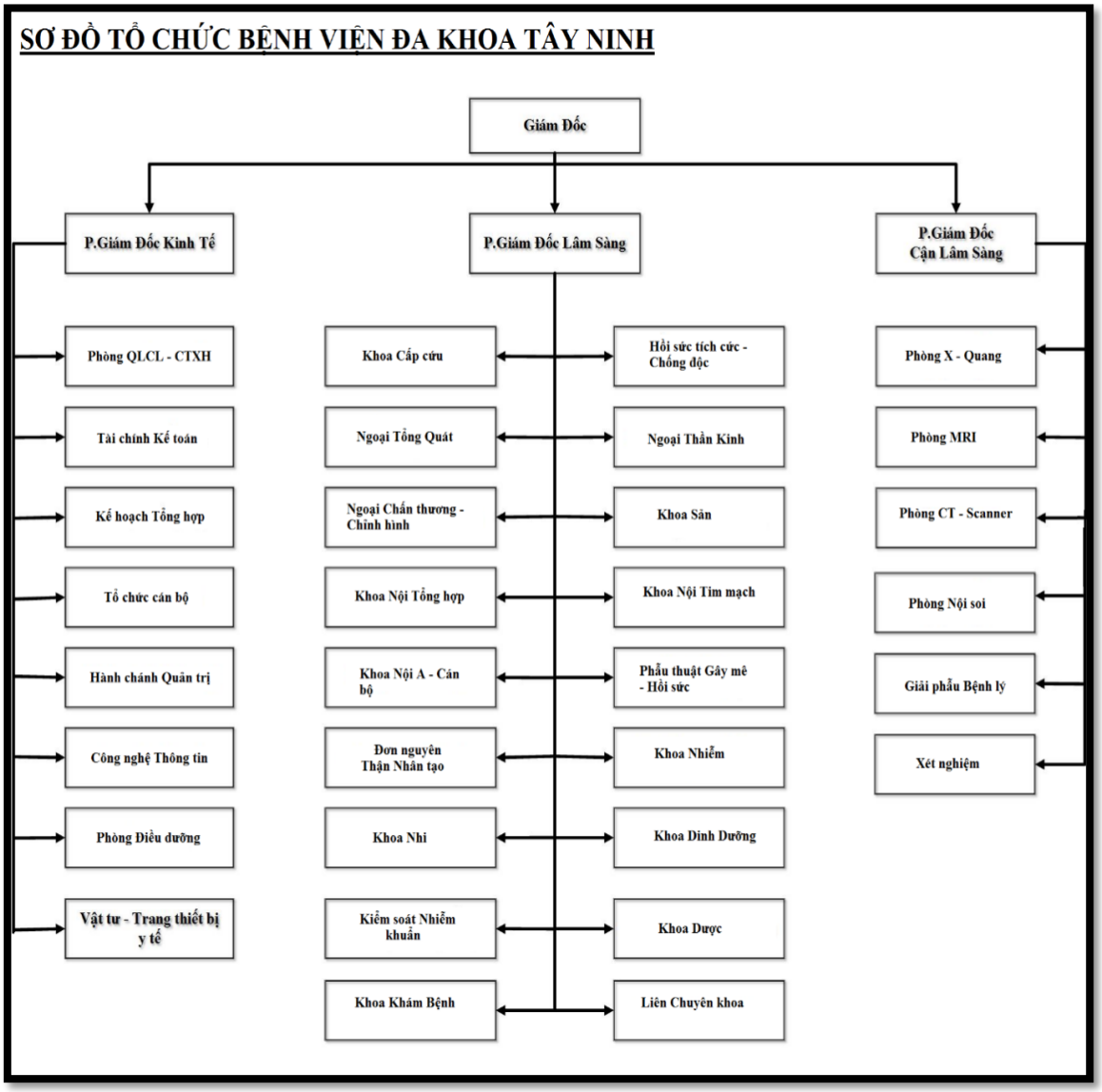
Bệnh viện Đa khoa Tây Ninh là bệnh viện cấp tỉnh hạng 2 của tỉnh Tây Ninh, được xây dựng năm 1999 với quy mô 700 giường. Trung bình một ngày Bệnh viện tiếp nhận khoảng hơn 1000 lượt đến khám và điều trị, đáp ứng nhu cầu khám chữa bệnh của nhân dân trong tỉnh và khu vực các tỉnh biên giới của nước Campuchia. Luôn tạo môi trường an toàn và thân thiện, với chất lượng chăm sóc cao và đội ngũ nhân viên nhiệt tình, năng động có trình độ chuyên môn và kỹ năng tương xứng với một bệnh viện đa khoa của khu vực miền Đông Nam Bộ.

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:

- Bao gồm: 32 phòng, khoa với đội ngũ gần 1000 nhân viên y tế.

- Ban Giám đốc gồm một Giám đốc, ba Phó giám đốc.
- Trưởng, Phó khoa, Bác sĩ và Nhân viên các Khoa.
- Trưởng, Phó phòng, Công nhân viên các phòng.



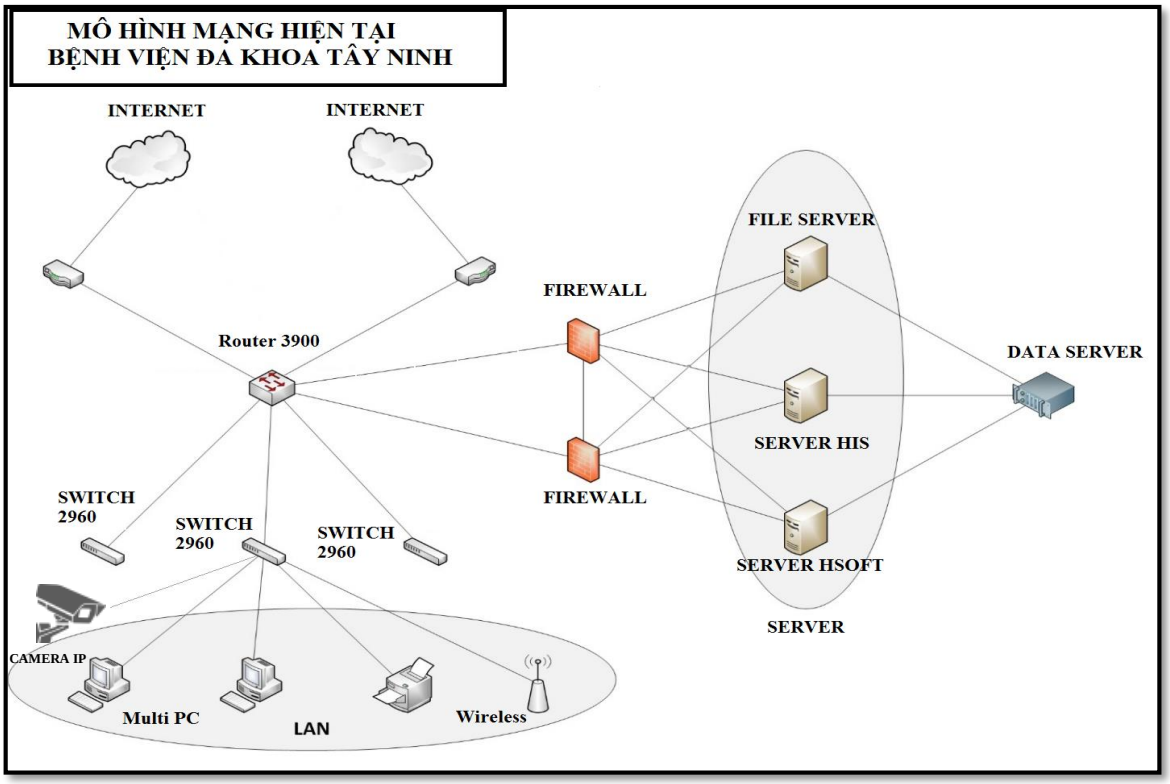
Hình 2.1: Sơ đồ tổ chức Bệnh viện Đa khoa Tây Ninh

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.
- Hệ thống mạng máy tính đã 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

Có 3 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.

Trong 32 phòng, khoa hiện tại của bệnh viện thì tất cả đều được kết nối hệ thống mạng máy tính dùng để xử lý, sử dụng dữ liệu, kết nối với hệ thống mạng trung tâm của bệnh viện.

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

- Có 11 Switch 2960, mỗi Switch 24 cổng làm nhiệm vụ chuyển mạch giữa các vùng VLAN với nhau.
- Thuê 2 đường cáp quang, thiết bị DrayTek 3900 làm Router (của nhà cung cấp dịch vụ) để cung cấp Internet cho toàn bệnh viện.
- Có đường mạng nội bộ sử dụng cáp quang tốc độ 1Gb nối giữa Router với các Switch. Đường mạng từ Switch đi đến máy Client sử dụng cáp thường 100Mb.
- Có hệ thống Data server dùng để lưu trữ dữ liệu của bệnh viện.
- Các máy in dùng riêng tại từng phòng, khoa trong bệnh viện.

2.3.3.4 Thực trạng về phần mềm

- Hệ thống hiện tại đang sử dụng phần mềm không bản quyền cho máy Server và máy Client.
- Máy Client dùng hệ điều hành Windows 7, Windows 10.
- Database Server dùng phần mềm Microsoft SQL Server 2008 để quản lý toàn bộ dữ liệu của bệnh viện.

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

Đặc điểm chung của một hệ thống mạng là có nhiều người sử dụng chung và phân tán về mặt địa lý nên việc bảo vệ tài nguyên (mất mát hoặc sử dụng không hợp lệ) phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.

Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đối tượng, đồng thời đảm bảo mạng hoạt động ổn định không bị tấn công bởi những kẻ phá hoại.

Nhưng trên thực tế, không có một mạng nào đảm bảo an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hóa bởi những kẻ có ý đồ xấu.

2.3.4.1 Các mối đe dọa tiềm năng đối với hệ thống

Trong thời gian qua, hệ thống mạng máy tính được các cấp quan tâm đầu tư. Tuy nhiên, vẫn chưa đảm bảo toàn vẹn và an toàn đúng mức, chỉ mới đáp ứng yêu cầu ở mức cơ bản.

Hệ thống mạng LAN (mạng nội bộ) được xây dựng cách dây hơn 20 năm, đã có nâng cấp sửa chữa nhưng 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.

Trước nhu cầu ứng phó với tình hình dịch bệnh COVID-19 phức tạp như hiện nay, theo phương châm phòng chống COVID-19 **"5K + vắc-xin + công nghệ"** do ***Thủ tướng Phạm Minh Chính*** đưa ra, nhiều công nghệ, ứng dụng công nghệ đã được Bệnh viện áp dụng cho bệnh nhân để phòng chống dịch như: *Khai báo y tế online, phần mềm hỗ trợ tiêm chủng quốc gia, ứng dụng sổ sức khỏe điện tử trên smartphone, cổng thông tin tiêm chủng COVID-19, thanh toán viện phí không dùng tiền mặt bằng mã QR Code. Bệnh viện đang tiếp nhận cách vận hành mới, các thách thức về bảo mật cũng vì thế xuất hiện và gia tăng.*

Hội nghị truyền hình trực tuyến đóng một vai trò vô cùng quan trọng đối với ngành y tế. Không những giúp tối ưu hóa quy trình, tiết kiệm chi phí, thời gian, công sức di chuyển cho cả bệnh nhân, bệnh viện và cả các cơ quan nhà nước. Nhất là trong khoảng thời gian này khi mà dịch bệnh diễn biến rất phức tạp, việc hạn chế di chuyển là điều hết sức cần thiết để đảm bảo an toàn sức khỏe. Do đó vấn đề an ninh thông tin cần được đặc biệt quan tâm.

Hệ thống phòng, chống vi rút trên máy chủ và máy tính cá nhân còn sử dụng phần mềm miễn phí nên hiệu quả sử dụng chỉ ở mức đơn giản, chưa thể phát hiện những loại mã độc mới, những vi rút ẩn danh dẫn đến hệ thống máy tính bị lây nhiễm vi rút nhiều.

Các Bác sĩ có nhu cầu sử dụng mạng Internet để tra cứu thông tin Bệnh nhân ngày càng cao như: Hệ thống lưu trữ và truyền tải hình ảnh (RIS-PACS), Telemedicine, Telehealth nếu không có phương án bảo mật hiệu quả thì có nguy cơ lây nhiễm vi rút rất lớn. Bên cạnh đó, và tạo cơ hội thuận lợi cho kẻ xấu tấn công lấy cắp thông tin ...

Việc truy cập của người sử dụng bên ngoài Internet vào hệ thống máy chủ web của bệnh viện ngày càng nhiều. Nếu không có hệ thống phòng chống hiệu quả sẽ có nguy cơ bị tấn công từ chối dịch vụ.

Nhân viên y tế và người dùng chưa được đào tạo để quản lý và khai thác mạng một cách hiệu quả, an ninh.

Chưa có một chính sách an ninh mạng thực sự nào được áp dụng. Điều này dẫn đến việc tổ chức, quản lý và sử dụng mạng không đúng theo ý muốn của quản trị mạng và dễ dàng gây nên các thiệt hại không lường trước.

Trên toàn mạng chỉ có một số cơ chế đảm bảo an ninh mạng như chứng thực người dùng. Điều này dẫn đến việc mạng không có khả năng phân cấp, điều khiển truy nhập, không có khả năng phản ứng lại các cuộc tấn công và khó có khả năng theo dõi toàn bộ hoạt động của mạng.

Đáp ứng được khả năng mở rộng quy mô hoạt động và ứng dụng công nghệ thông tin của Bệnh viện trong tương lai: Mở rộng về số lượng máy tính, số lượng máy chủ, các mạng LAN và các ứng dụng.

2.3.4.2 Nhu cầu bảo mật hệ thống mạng của bệnh viện

Đại dịch COVID-19 đã đẩy nhanh sự phát triển của khoa học công nghệ, rút ngắn thời gian công nghệ tới gần hơn với đời sống của con người, đặc biệt trong lĩnh vực y tế. Nhất là những công nghệ như chăm sóc sức khỏe từ xa, giám sát hay trí tuệ nhân tạo sẽ được ứng dụng trong Bệnh viện trong tương lai gần:

- Thay đổi cách cung cấp dịch vụ sức khỏe: Thẻ khám chữa bệnh điện tử sẽ giống như một bệnh án điện tử được lưu giữ tại hệ thống máy tính bệnh viện, bác sỹ điều trị có thể tra cứu thông tin liên quan người bệnh bất cứ lúc nào, bất cứ nơi đâu miễn là có đường truyền Internet.
- Bệnh viện tiến đến ứng dụng trí tuệ nhân tạo và nguồn dữ liệu Big Data vào phục vụ bệnh nhân, để bác sĩ tham khảo và đưa ra phác đồ điều trị nhiều bệnh nguy hiểm:
    + Ứng dụng trí tuệ nhân tạo (AI) trong chăm sóc sức khỏe, sử dụng các thuật toán và phần mềm, công nghệ cũng như nguồn dữ liệu lớn (Big Data) : Dựa vào nguồn dữ liệu thu thập được của người bệnh, các AI đồng bộ hóa trên kho dữ liệu, từ đó bác sĩ sẽ nhận được những gợi ý từ phương pháp chẩn đoán, điều trị, phác đồ hiện đại của các Bệnh viện lớn trên thế giới hoặc cập nhật để hỗ trợ chẩn đoán, điều trị ung thư, tim mạch, đái tháo đường…Trong một số ứng dụng khuyến nghị về dinh dưỡng cho bệnh nhân, phần mềm sẽ cho khuyến cáo, bác sĩ chẩn đoán sẽ rà soát khuyến cáo đó, nếu ổn thì có thể cung cấp cho bệnh nhân.
    + Ứng dụng trí tuệ nhân tạo trong nội soi tiêu hóa, chẩn đoán và dự báo dịch tễ bệnh lao phổi bằng X-quang sớm, hỗ trợ trong việc khám và chữa bệnh sẽ giúp tăng khả năng điều trị cho bệnh nhân.
    + Ứng dụng công nghệ AI vào phần mềm khám chữa bệnh HIS, phần mềm quản lý thông tin xét nghiệm giúp bệnh nhân giảm thời gian chờ đợi bác sĩ, có thể hẹn thêm bác sĩ mà không phải đối mặt nhiều người và nhiều vi khuẩn trong phòng chờ nhân viên y tế.
    + Công nghệ máy học AI còn được sử dụng để sàng lọc các dữ liệu khám bệnh, tìm kiếm ra sai lầm trong phương thức điều trị, tính không hiệu quả và những trường hợp không cần thiết đều sẽ được phát hiện nhanh chóng.
- Bệnh viện đẩy mạnh thăm khám trực tuyến: Cho phép đặt lịch khám từ xa, chủ động chọn thời gian khám, hỗ trợ nhắc lịch khám và tái khám, tư vấn sức khỏe 24/7, lưu trữ hồ sơ bệnh án điện tử và thanh toán tiện lợi từ xa dưới nhiều hình

thức…Nhằm giảm thiểu các lần tiếp xúc trực tiếp khám bệnh trực tiếp giữa bác sĩ và bệnh nhân. Bệnh nhân giao tiếp hoàn toàn với bác sĩ chỉ bằng một hoặc hai lần chạm vào thiết bị, giúp giảm chi phí và mở rộng quy mô khám chữa bệnh.

- Nghiên cứu ứng dụng kết nối vạn vật trong y tế (IoMT – Internet of Medical Things): Kết nối thiết bị điện tử chia sẻ và truyền tải dữ liệu lên hệ thống, kết nối hệ thống phần mềm thông tin bệnh viện (HIS), phần mềm thông tin xét nghiệm (LIS), phần mềm thông tin chẩn đoán hình ảnh (RIS), hệ thống lưu trữ và truyền tải hình ảnh (PACS), phần mềm bệnh án điện tử (ERM), định dạng người bệnh qua mã vạch, cảm biến. Hướng tới RFID PACS – Bệnh viện không in phim, qua đó tiết kiệm chi phí và hiệu quả trong kết nối, hội chẩn điện tử thời gian thực; Liên thông kết nối chuyển hồ sơ bệnh án điện tử giữa các bệnh viện tuyến huyện.
- Bộ Y tế đã có ban hành văn bản *Thông tư số 54/2017/TT-BYT* và *Thông tư số 46/2018/TT-BYT* hướng dẫn triển khai được hồ sơ bệnh án điện tử.
- Theo *Điều 20 Thông tư số 46/2018/TT-BYT* đã nêu rõ lộ trình thực hiện triển khai hồ sơ bệnh án điện tử tại các cơ sở khám bệnh, chữa bệnh như sau:
    + Giai đoạn từ năm 2024 – 2028: Tất cả các cơ sở khám bệnh, chữa bệnh trên toàn quốc phải triển khai hồ sơ bệnh án điện tử. Yêu cầu cấp thiết đặt ra là Bệnh viện phải trang bị hệ thống phát hiện xâm nhập (IDS), hệ thống ngăn chặn xâm nhập (IPS) để ngăn chặn tấn công có chủ đích và xâm nhập từ xa đảm bảo an toàn cho hệ thống máy chủ của bệnh viện.
- Nguy cơ tấn công mạng của tin tặc nhắm vào bệnh viện và các cơ sở y tế không chỉ nhằm mục đích lấy cắp tiền hoặc thông tin cá nhân như trước đây, mà còn khiến cho nhiều người tử vong. Thật vậy, theo kết quả một cuộc nghiên cứu và khảo sát vừa được công bố của Công ty An ninh mạng Censinet (Mỹ), gần 1/4 các bệnh viện và trung tâm chăm sóc sức khỏe đã bị tấn công mạng, chủ yếu bởi các loại mã độc tống tiền trong vòng 2 năm qua, khiến tỉ lệ bệnh nhân tử vong tăng cao và ảnh hưởng quá trình chăm sóc sức khỏe của người bệnh.
- Các chuyên gia bảo mật đã nhiều lần cảnh báo về việc các bệnh viện, trung tâm chăm sóc sức khỏe có thể trở thành mục tiêu tấn công của tin tặc và các loại mã

độc, nhưng cho đến nay những địa điểm này vẫn chưa có sự chuẩn bị thực sự đầy đủ. Nhiều thiết bị khám chữa bệnh đòi hỏi kết nối Internet để sử dụng và nếu bị mã độc tấn công, các thiết bị này không thể hoạt động và sẽ làm ảnh hưởng nghiêm trọng đến quá trình chữa trị cho bệnh nhân.

- Ngay cả khi các vụ tấn công mạng không nhằm vào hệ thống máy móc, thiết bị y tế của bệnh viện, mà nhằm mục tiêu lấy cắp dữ liệu của người bệnh, điều này cũng có thể ảnh hưởng đến kết quả chữa trị của bệnh nhân.

Nhận xét:

- Việc nghiên cứu và phát triển các sản phẩm về an ninh thông tin nói chung và an ninh mạng nói riêng, là một nhu cầu bức thiết đối với hệ thống mạng bệnh viện nhằm đảm bảo an ninh bảo mật hệ thống. Nhằm tăng cường khả năng bảo vệ nhiều lớp để tăng cường tính bảo mật các khu vực bên trong, nơi lưu giữ các nguồn tài nguyên mạng có giá trị nhất
- 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 giữa các khối nhà khi dữ liệu tập trung.
- Việc áp dụng cứng nhắc những ứng dụng công nghệ mới vào hệ thống mạng chưa thể đảm bảo việc nâng mức an toàn lên cao hơn. Bởi yếu tố con người mới là khía cạnh quan trọng nhất trong lĩnh vực bảo mật. Hiện nay, vẫn chưa có một nghiên cứu nào để cung cấp cho các quản trị mạng của Bệnh viện những hiểu biết cần thiết để thiết lập các quy tắc đảm bảo an ninh trong hệ thống.
- Khi mà các ứng dụng chạy hệ thống mạng ngày càng phát triển về cả quy mô và số lượng, thì những lỗ hổng về bảo mật ẩn chứa trong các hệ thống này cũng ngày càng nhiều. Bên cạnh đó, trình độ của các tin tặc trong nước trong thời gian qua đã có nhiều bước tiến. Các nguyên

lý, cách thức tấn công mà các tin tặc vận dụng đã có nhiều bổ sung và vận dụng linh hoạt.

- Thiết lập hệ thống bảo mật dữ liệu nội bộ cho Bệnh viện là rất cần thiết. Nhất là trước diễn biến của đại dịch COVID-19, nhu cầu lưu trữ thông tin người bệnh ngày càng lớn, nhu cầu tra cứu và sử dụng mạng máy tính trong Bệnh viện ngày càng cao: Kết nối hội nghị trực tuyến với các Bệnh viện Trung ương, khai báo y tế online, hội chẩn từ xa, Telemedicine, ...

2.3.5 Đề xuất chính sách bảo mật

Đối với Bệnh viện Đa khoa Tây Ninh, việc phải hoạt động suốt ngày đêm, trong tất cả các này thì việc đảm bảo cho hệ thống thông suốt, an ninh và bảo mật hệ thống là yêu cầu hết sức cấp bách, cực kì quan trọng. Đồng thời chú trọng tăng cường khả năng bảo vệ đa lớp, để bảo vệ tối ưu nhất cho dữ liệu bên trong. Đó là tất cả cơ sở dữ liệu của Bệnh viện, thông tin hồ sơ bệnh án của bệnh nhân hay các tài nguyên mạng có giá trị khác thậm chí còn liên quan đến vấn đề pháp lý.

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. Việc này có thể thực hiện được bằng phần mềm hay phần cứng, tuy nhiên việc thực hiện trên phần cứng (card mã hoá trên router hay thiết bị mã hoá cứng cắm ngoài trên đường truyền) có ưu điểm hơn là giảm độ trễ của các gói tin, sử dụng băng thông trên đường truyền hiệu quả hơn (nhất là trên WAN).

2.3.5.2 Bảo mật lớp truy cập

Bảo mật cho các đường truy nhập của người dùng quay số (dial-up): Thường áp dụng các hình thức xác thực người dùng, tạo các kênh VPN cho các kết nối dial-up,...

Firewall/IDS: Tại các khu vực cung cấp các máy chủ truy nhập cần bố trí các bức tường lửa (Firewall) kèm các bộ dò tìm tấn công (IDS) đảm bảo ngăn chặn các

truy nhập trái phép hay các dạng tấn công ngay từ cổng vào mạng, điều này là rất cần thiết bởi việc sử dụng các thiết bị hỗ trợ cho các kết nối truy nhập đồng thời lại có kết nối đi Internet.

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, chúng tôi khuyến nghị sử dụng các ACL để điều khiển truy nhập trên toàn bộ các thiết bị này, đồng thời sử dụng các thiết bị dò tìm lỗ hổng (IDS) để dò tìm xác định các dấu hiệu tấn công vào các thiết bị mạng và các nguồn tài nguyên khác và có các biện pháp ngăn chặn kịp thời.

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 cũng như ăn cắp hay phá huỷ các thông tin có giá trị được chứa trong các máy chủ này. Việc bảo mật hệ thống máy chủ liên quan tới các công việc như:

- Bảo mật thông tin trên máy chủ: đảm bảo tính mã hoá, tính toàn vẹn và xác thực của thông tin
- Quản trị truy nhập vào máy chủ: áp dụng các công nghệ tiên tiến như smart card, Token…
- Chống truy nhập trái phép: sử dụng các bộ dò tìm IDS để phát hiện và báo động kịp thời khi có tấn công hay truy nhập trái phép vào hệ thống máy chủ.

2.3.5.5 Bảo mật mức hệ điều hành (HĐH)

Việc bảo mật cho HĐH máy chủ đảm bảo cho hệ thống làm việc ổn định việc hoạch định 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 là hết sức cần thiết để đảm bảo cho các hệ điều hành và các ứng dụng chạy trên nó được bảo vệ an ninh ngăn chặn các cuộc tấn công có thể xảy ra.

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), chúng tôi khuyến nghị thực hiện các kênh bảo mật từ người dùng đầu cuối tới các máy chủ ứng dụng để đảm bảo các tính bảo mật, toàn vẹn và xác thực của thông tin.

2.3.5.7 Bảo mật mức cơ sở dữ liệu (CSDL)

Có thể nói CSDL là 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, trong thiết kế thì đây là CSDL được đặt ở mức ưu tiên cao nhất.

Hệ thống mạng của bệnh viện với việc kết nối các site với độ tin cậy, an toàn cao, tôi đề xuất giải pháp với các tính năng sau:

- Có khả năng mở rộng và nâng cấp cao nhất mà chi phí đầu tư tiết kiệm nhất.
- Khả năng cài đặt, quản trị đơn giản. Giảm mức độ phức tạp, tốc độ và Routing của hệ thống mạng đến mức thấp nhất, dễ dàng cho các hệ thống thiết lập trong thời gian sau.
- Bao gồm hầu hết các tính năng bảo mật hiện có như Antivirus, IDS/IPS, VPN, WebBlock, Spam, Scanner…
- Quản trị tập trung toàn bộ hệ thống, cập nhật tư động và thường xuyên.
- Tốc độ xử lý cao trong các môi trường. Khả năng Loadbalancing cho nhiều kết nối đến các nhà cung cấp dịch vụ khác nhau**.**

2.3.5.8 Bảo mật cho mạng phân tán

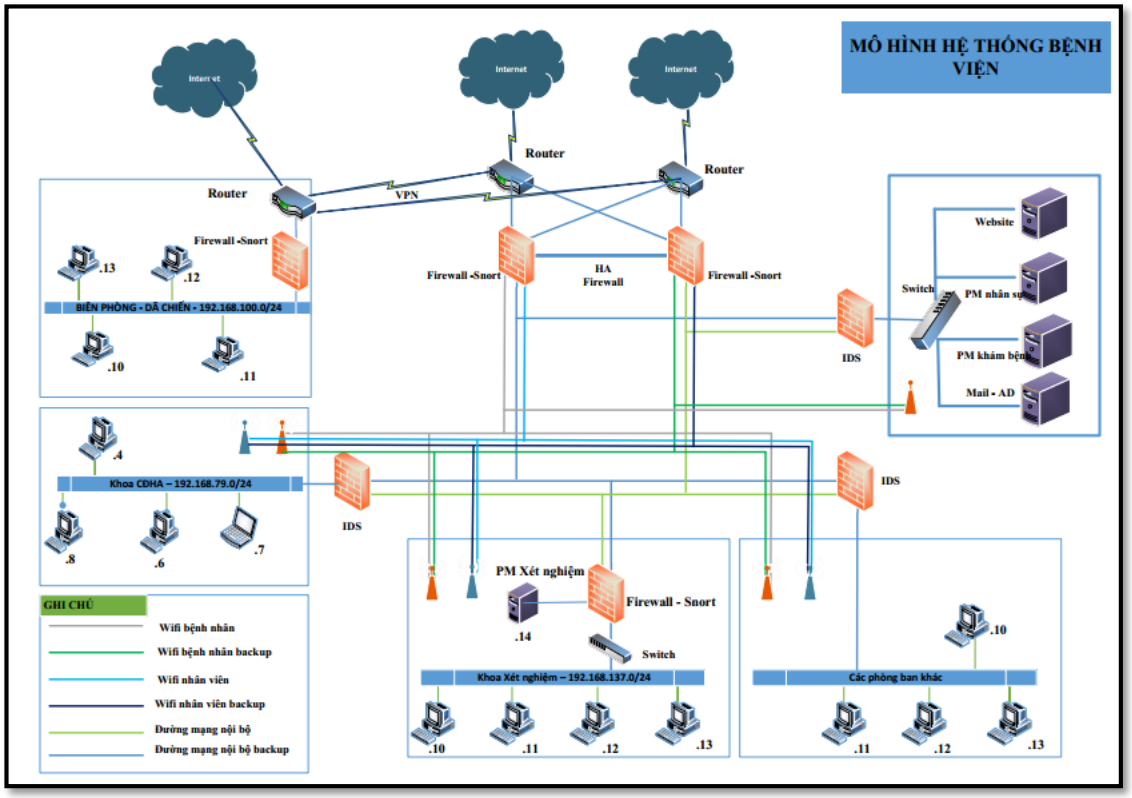
Do các mạng LAN kết nối với nhau qua môi trường internet, nên rất cần chính sách bảo mật ở mảng này, các dữ liệu thông tin trao đổi đi ra ngoài môi trường internet cần phải được mã hóa ở cấp độ cao.

Qua khảo sát, đa số các Khoa phòng gửi 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 BỆNH VIỆN

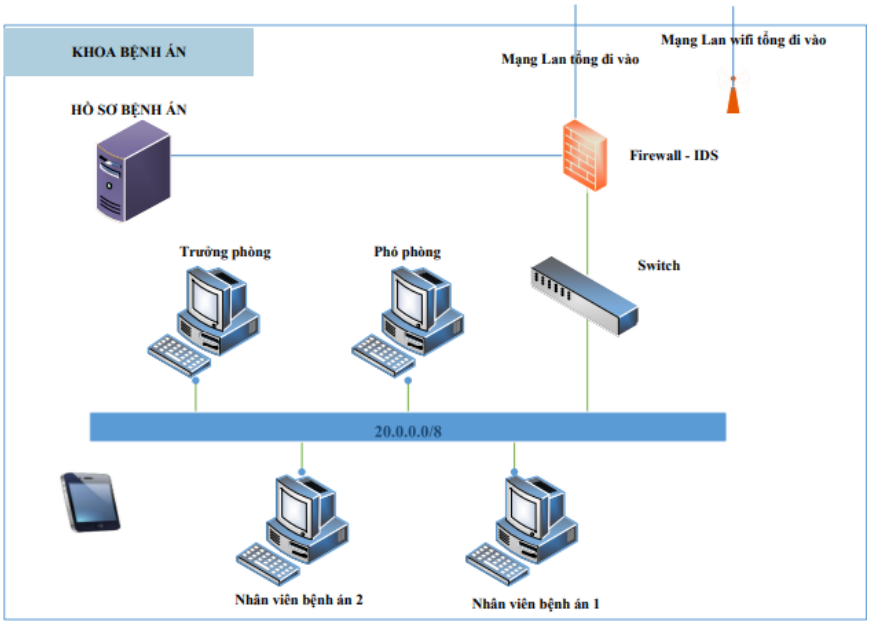
3.1 Giới thiệu chung

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. Cụ thể là đề xuất xây dựng ứng dụng và trung tâm lưu trữ log để có thể gửi mail cảnh báo dựa trên log của Snort được sử dụng với Pfsense, sẽ chuyển tiếp về Server phân loại và lưu trữ log của Splunk server. Từ đó đưa ra quyết định cảnh báo, nhắc nhở... trên hệ thống mạng LAN.



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

3.2 Mô hình nghiên cứu hệ thống mạng



Hình 3.2: Mô hình mạng khoa bệnh án bệnh viện đa khoa Tây Ninh

Mô tả mô hình

Mô hình nghiên cứu bao gồm các thành phần như sau:

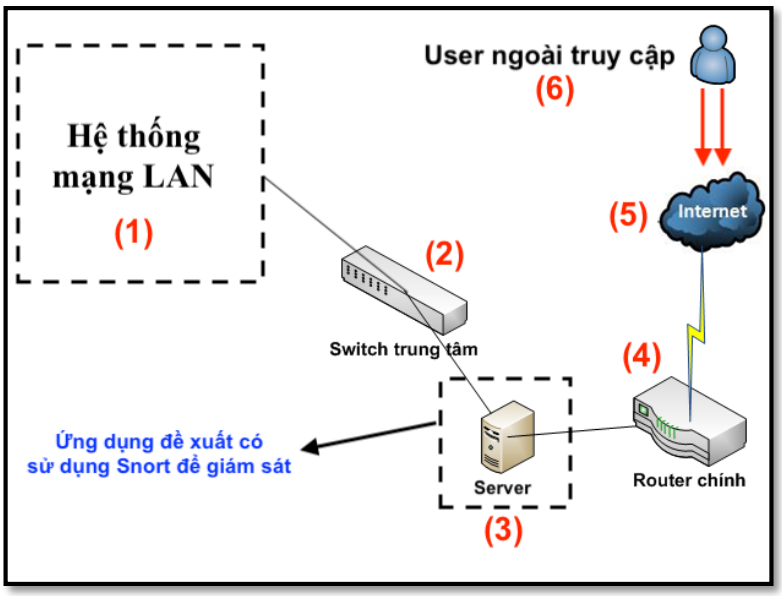
- *Router:* Đây là thiết bị cho phép hệ thống mạng nội bộ có thể kết nối với internet bằng cáp quang. Đảm nhiệm định tuyến, Nat, ….
- *Switch layout 3:* Đây là thiết bị kết nối toàn bộ hệ thống trong mạng Lan, đây là thiết bị kết nối trực tiếp với router chính. Đảm nhiệm chia VLan cho từng phòng ban.
- *Vùng DMZ:* Đây là vùng hệ thống chứa các máy chủ website, máy chủ quản lý tài khoản AD, máy chủ chứa phần mềm khám bệnh, nhân sự, …
- *Firewall -Snort:* Hệ thống giám sát mạng, phát hiện và phòng tránh xâm nhập trái phép của người dùng vào các hệ thống quan trọng của bệnh viện.
- *Các khoa xét nghiệm, khoa bệnh án, ... và đội biên phòng, bệnh viện dã chiến:* Hệ thống mạng dành cho các khoa, khu vực có chứa dữ liệu quan trọng, cần bảo mật mức cao.

- Ngoài ra hệ thống còn có 2 hệ thống Wifi dành cho bệnh nhân và nhân viên bệnh viện tách biệt với hệ thống quan trọng của bệnh viện.

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 cho môi trường mạng LAN



Hình 3.3: Mô hình hệ thống đề xuất tích hợp ứng dụng giám sát Snort

Mô tả mô hình

Người dùng từ môi trường ngoài internet đi vào hệ thống mạng nội bộ qua thiết bị router. Nếu với mô hình nghiên cứu ban đầu, router chính sẽ kết nối trực tiếp với hệ thống mạng nội bộ qua thiết bị switch trung tâm, với mô hình đề xuất giám sát hệ thống mạng, chúng ta sẽ đặt một Server Pfsense ngay giữa thiết bị router chính và switch trung tâm. Router chính sẽ không còn kết nối trực tiếp vào hệ thống mạng Lan mà phải kết nối trực tiếp vào Server Pfsense. Tại Server Pfsense này, chúng ta sẽ cài đặt phần mềm Snort để giám sát hệ thống, phát hiện và ngăn chặn tấn công thông qua internet.

Diễn giải mô hình

(1): Đây là hệ thống mạng LAN, bao gồm các nhánh máy chủ, nhánh máy tính các phòng ban, nhánh máy tính kết nối trang thiết bị y tế, ...

(2): Switch trung tâm là thiết bị kết nối hệ thống mạng LAN với router chính để kết nối ra ngoài internet, tuy nhiên với mô hình nghiên cứu tích hợp Pfsense và Snort, thì switch trung tâm sẽ kết nối với router chính thông qua server cài đặt Snort đã được đề xuất

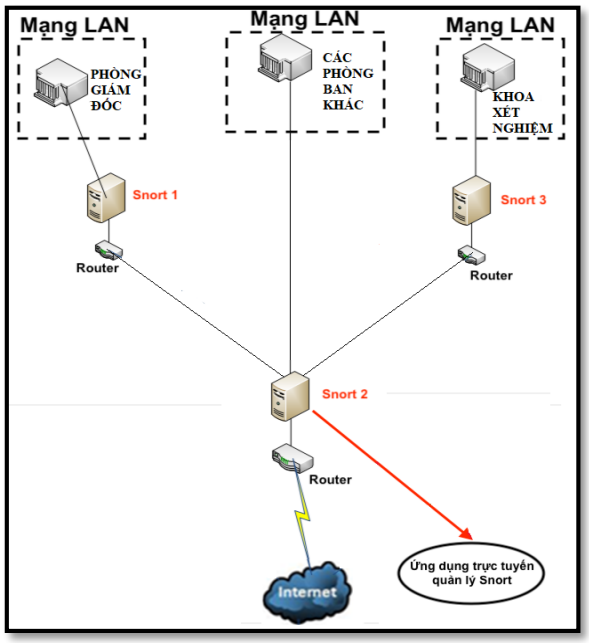
(3): Server cài đặt ứng dụng Snort để giám sát lưu lượng mạng vào ra hệ thống mạng LAN.

(4): Router chính là thiết bị của nhà mạng cung cấp

(5): Môi trượng mạng internet bên ngoài.

(6): User ngoài truy cập vào hệ thống mạng LAN để tra cứu thông tin cá nhân, sử dụng các dịch vụ của Bệnh viện.

b. Mô hình cho môi trường trực tuyến



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

Với mô hình chúng ta sẽ kế thừa từ mô hình hệ thống đề xuất tích hợp ứng dụng giám sát Snort cho mạng LAN. Với mô hình này, chúng ta có sẽ có 3 hệ thống mạng LAN tương ứng với mỗi mức độ quan trọng của phòng ban thuộc bệnh viện. Với mỗi hệ thống mạng LAN, ở mỗi router chính chúng ta sẽ thiết lập NAT để cho ứng dụng giám sát trực tuyến Snort có thể kết nối với nhau. Ở nhánh mạng LAN thứ 2 (Snort 2) chúng ta sẽ đặt ứng dụng trực tuyến trung tâm, đóng vai trò quản lý các Snort ở các nhánh mạng LAN khác.

3.3.2 Mục tiêu của ứng dụng đề xuất

Với mô hình đề xuất như trên, Snort sẽ đóng vai trò trung tâm để giám sát hệ thống mạng. Cùng với việc xây dựng thêm một ứng dụng trực tuyến để kết hợp với Snort, chúng ta sẽ có được những mục tiêu như sau:

- Giám sát toàn bộ các luồng dữ liệu trên hệ thống mạng LAN.
- Khi xảy ra hoặc bị sự cố tấn công từ client trong mạng LAN như: Virus lây lan trong mạng LAN, Trojan, Malware… 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 (với các mức độ khác nhau) tới người quản trị hệ thống và các client khác trong mạng LAN.

Việc sử dụng dữ liệu log của Snort, chúng ta sẽ 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

Ứng dụng đề xuất trong luận văn này là sự kết hợp và tái sử dụng kết quả của Pfsense và Snort để giám sát hệ thống mạng LAN, đưa ra quyết định cảnh báo khi phát hiện nguy cơ gây hại đến hệ thống. Ứng dụng đề xuất sẽ đọc và ghi lại các dữ liệu log thu được từ Snort bằng Pfsense từ các rules đã được cấu hình sẵn, rồi tiếp tục đẩy log về Splunk Server và từ đây người quản trị có thể tạo các câu lệnh để lọc và tạo ra các alert mong muốn để gửi về mail cảnh báo.

Dựa vào nghiên cứu các hệ thống IDS cũng như các ứng dụng tương tự đã công bố, luận văn này xin đề xuất ứng dụng gồm 2 nhóm module chính:

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

Trong module này, sẽ thực hiện nhiệm vụ tạo các rules của SNORT, và đưa vào cơ sở dữ liệu của ứng dụng. Những kết nối có các đặc điểm giống với các rules đã cấu hình thì sẽ được lưu lại log và hiện thị cảnh báo trên Pfsense. Log này đã được hiệu chỉnh và chỉ lưu lại những luồng dữ liệu đã được lọc, tức là phải có dấu hiệu cần lưu lại mới lưu vào Log. Mỗi file lưu theo cấu hình tùy chỉnh trong dịch vụ Snort chạy trên Pfsense theo dữ liệu các luồng truyền trên LAN.

(2) Module tổng hợp log và gửi cảnh báo

Ở Module này, là 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 email.

Bên cạnh đó, có thể tạo ra được các báo cáo, tổng hợp số lượng truy cập vào và ra internet, …

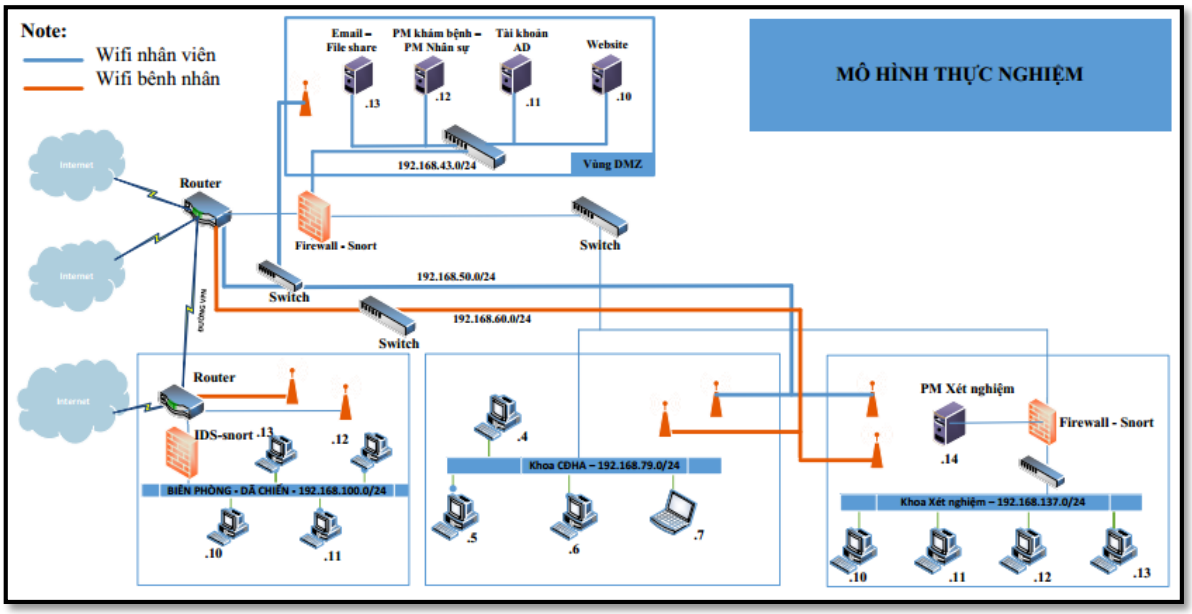
3.4 Kết luận Chương 3

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

Mô hình thực nghiệm



Hình 4.1: Mô hình thực nghiệm Bệnh viện Tây Ninh

4.1.1 Mục tiêu

Xây dựng hệ thống tường lửa IDS cho Bệnh viện Đa khoa Tây Ninh trong tương lai dựa trên sơ đồ mạng thực tế. Mục tiêu bảo vệ các phòng ban quan trọng và hệ thống cơ sở dữ liệu của Bệnh viện (dữ liệu khám chữa bệnh, dữ liệu tiền lương, dữ liệu xét nghiệm…)

Bên cạnh đó, xây dựng hệ thống Snort bảo vệ từng khoa riêng (khoa xét nghiệm). Mặt khác xây dựng hệ thống Snort quản lý Wifi cho nhân viên và bệnh nhân sử dụng. Bệnh nhân chỉ vào được Server Website để theo dõi tình hình khám chữa bệnh, chi phí, tình trạng các bệnh nhân và các dịch vụ của bệnh viện. Nhân viên sử dụng wifi được phép vào sử dụng để vào 1 hệ thống như webiste, hệ thống phần mềm khám bệnh và nhân sự (tùy theo phân quyền nhân viên vào hệ thống khác nhau).

Mục tiêu thử nghiệm hệ thống giám sát phát hiện tấn công IDS kết hợp nhiều IDS với nhau để đảm bảo phòng chống các cuộc tấn công từ nhiều phía như tấn công từ phòng ban với các phòng ban quan trọng, tấn công từ phòng không quan trong lên

hệ thống máy chủ, từ phòng quan trọng lên máy chủ, từ bệnh viện dã chiến – biên phòng vào hệ thống datacenter hoặc tấn công từ wifi người dùng của bệnh nhân và nhân viên vào các hệ thống quan trọng.

Mục tiêu xây dựng rule cảnh báo của các kịch bản nhằm phát hiện sự xâm nhập mạng bất thường trong hệ thống một cách chính xách nhất. Gửi thông tin về cuộc tấn công cho nhà quản trị mạng qua email một cách nhanh nhất. Từ đó, giúp cho nhà quản trị mạng có đủ thời gian để xây dựng cách phương án phòng thủ cho hệ thống. Bên cạnh đó, việc xây dựng các rule cho kịch bản tấn công cũng dựa vào sự phân bố lớp mạng của các khoa phòng trong hệ thống. Mục đích ghi nhận các cuộc tấn công nội bộ từ khoa phòng.

4.1.2 Thực hiện tấn công

4.1.2.1 Kịch bản tấn công 1

❖ **Mục đích**

Kẻ xâm nhập tổ chức tấn công 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. Tổ chức truy cập vượt quyền của các khoa phòng, tấn công vào máy chủ Khoa Xét nghiệm có chứa dữ liệu quan trọng để truy xuất các thông tin là kết quả Xét nghiệm HIV, SARS-CoV-2, các kết quả xét nghiệm quan trọng khác.

❖ **Mô tả**

Thực hiện tấn công từ chối dịch vụ DOS từ 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.

Để thực hiện đánh giá việc xây dựng Snort tại khoa Xét nghiệm hiệu quả trong bảo mật mạng, mục đích xây dựng các rule đưa ra biện pháp phòng chống tấn công từ các khoa khác xâm nhập trái phép vào máy chủ 192.168.137.12. Từ đó đưa ra các cảnh báo cho nhà quản trị mạng.

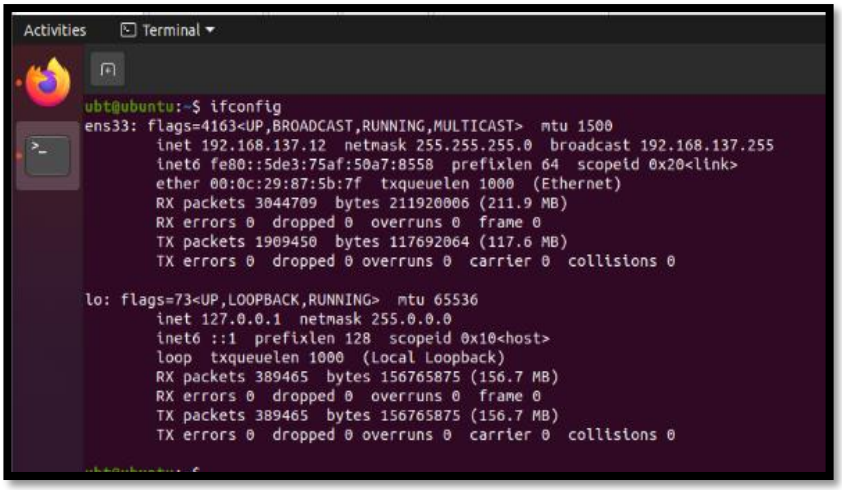
IP 5 máy tính ở vùng bên ngoài:

- Máy thứ nhất Kali 192.168.79.14 ở vùng bên ngoài
- Máy thứ hai ParrotOS 192.168.79.15 ở vùng bên ngoài
- Máy thứ ba Ubuntu 192.168.79.16 ở vùng bên ngoài
- Máy thứ tư Ubuntu 192.168.79.17 ở vùng bên ngoài
- Máy thứ năm Ubuntu 192.168.79.18 ở vùng bên ngoài

IP 5 máy tính ở vùng bên trong:

- Máy thứ 1 Kali 192.168.137.15 ở vùng bên trong
- Máy thư 2 ParrotOS 192.168.137.19 ở vùng bên trong
- Máy thứ 3 Ubuntu 192.168.137.20 ở vùng bên trong
- Máy thứ 4 Ubuntu 192.168.137.21 ở vùng bên trong
- Máy thứ 5 Ubuntu 192.168.137.22 ở vùng bên trong

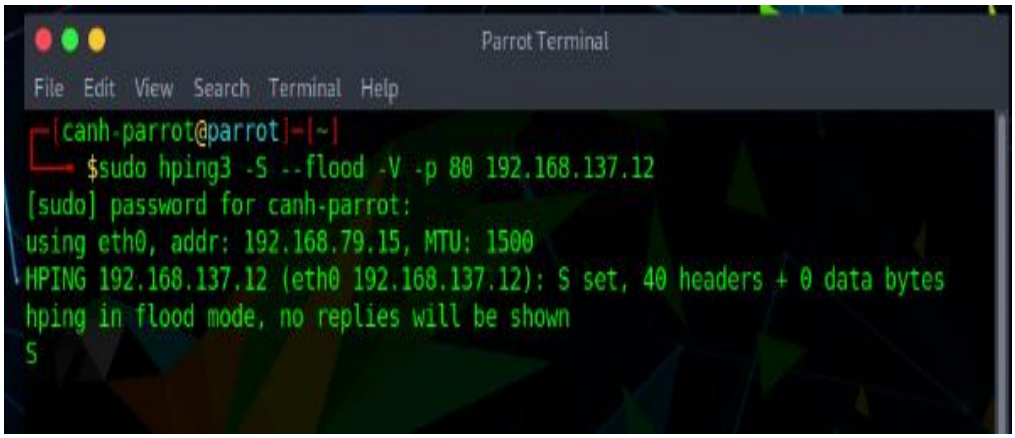
❖ **Thực hiện tấn công:** Tấn công cùng lúc 10 máy vào mục tiêu máy chủ Khoa xét nghiệm có địa chỉ IP 192.168.137.12



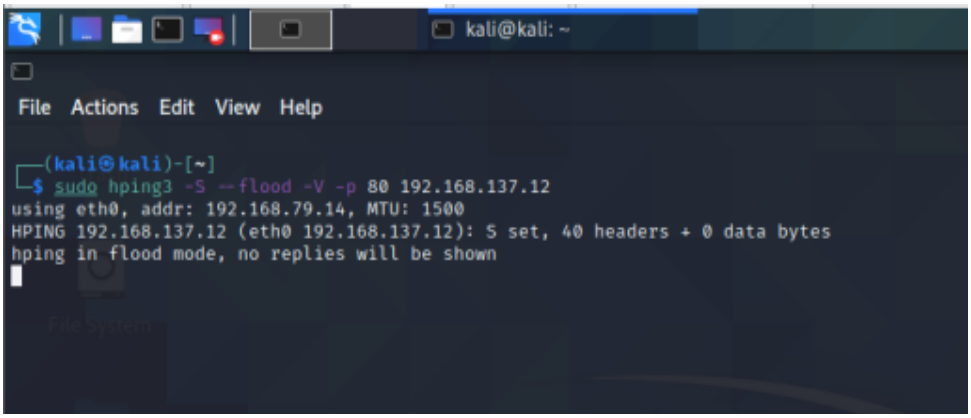
Hình 4.2: Địa chỉ máy mục tiêu Kịch bản 1

Sử dụng câu lệnh DoS qua Port 80, tấn công cùng lúc 10 máy, mục đích phá hoại làm nghẽn đường mạng của máy chủ khoa Xét nghiệm:

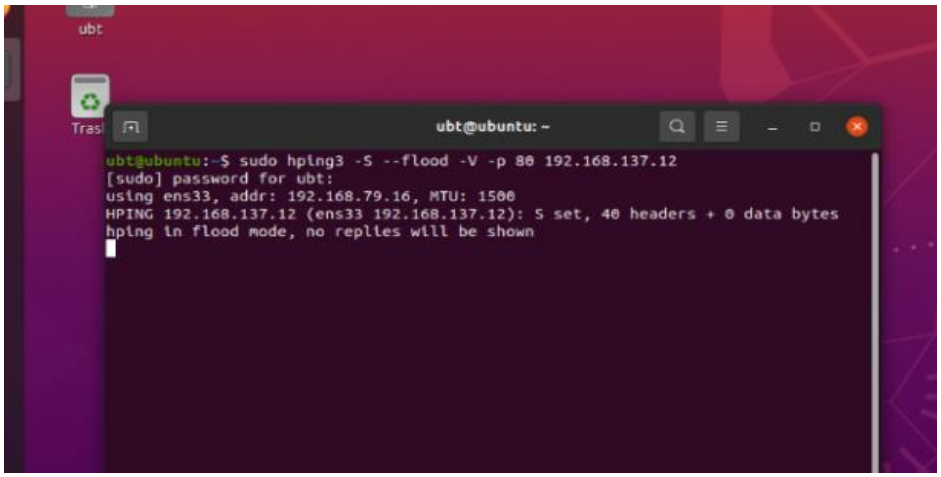
sudo hping3 -S --flood -V -p 80 192.168.137.12



Hình 4.3: Tấn công trên máy Parrot

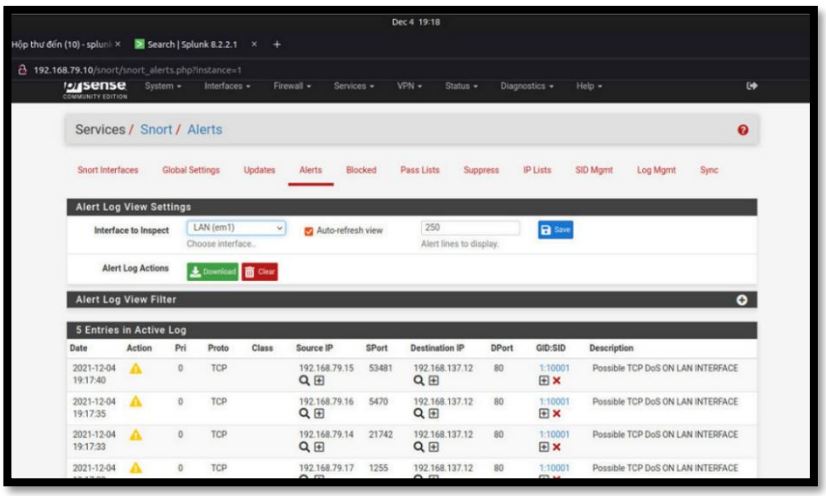


Hình 4.4: Tấn công trên máy kali



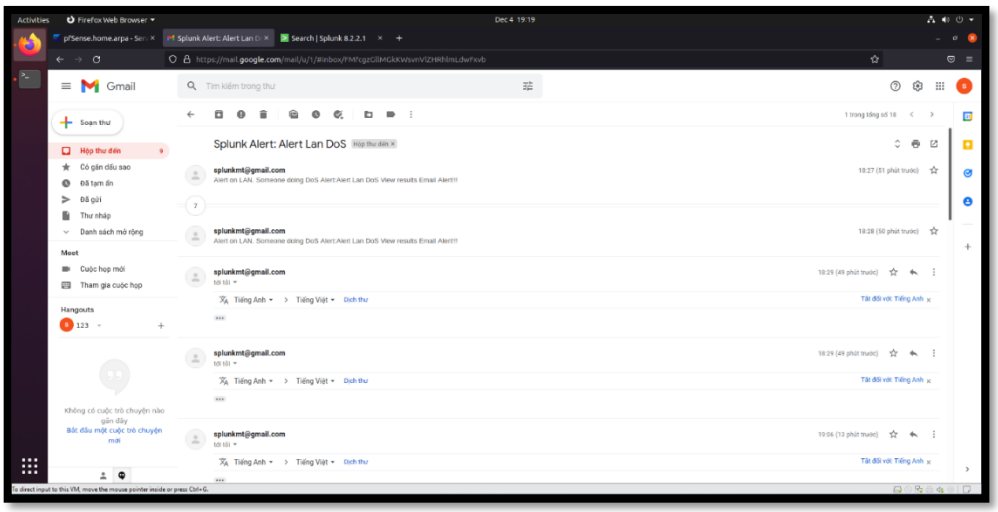
Hình 4.5: Tấn công trên máy Ubuntu

❖ **Kết quả thu được**



Hình 4.6: Màn hình cảnh báo trong kịch bản 1

Lúc này Snort server sẽ gửi log sang cho Mail server cho nhà quản trị mạng để theo dõi.



Hình 4.7: Mail cảnh báo về DoS trong kịch bản 1

Kết quả là Snort ghi nhận được log của 10 máy tấn công và ngay lập tức gửi về Server ghi log tập trung. Tại đây, với những cấu hình alerts đã được cấu hình sẵn thì người quản trị sẽ nhận được mail cảnh báo một cách sớm nhất và từ đó có thể đưa ra các giải pháp để hạn chế và phòng chống cuộc tấn công này.

4.1.2.2 Kịch bản tấn công 2

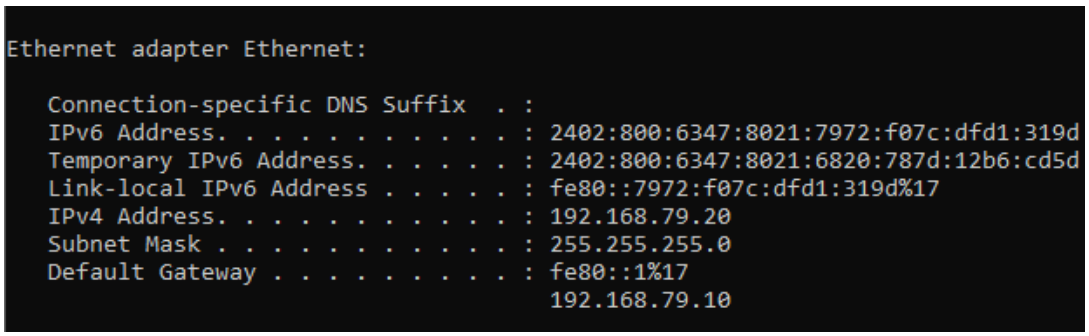
❖ **Mục đích**

Thực hiện tấn công từ máy tính vùng ngoài có dãy địa chỉ (192.168.79.0/24) thuộc các khoa phòng không quan trọng khác, tấn công trái phép máy tính ở vùng mạng Active Directory có dãy địa chỉ 192.168.137.0/24 của khoa Xét nghiệm nhằm mục đích lấy cắp thông tin, truy cập tài liệu cá nhân.

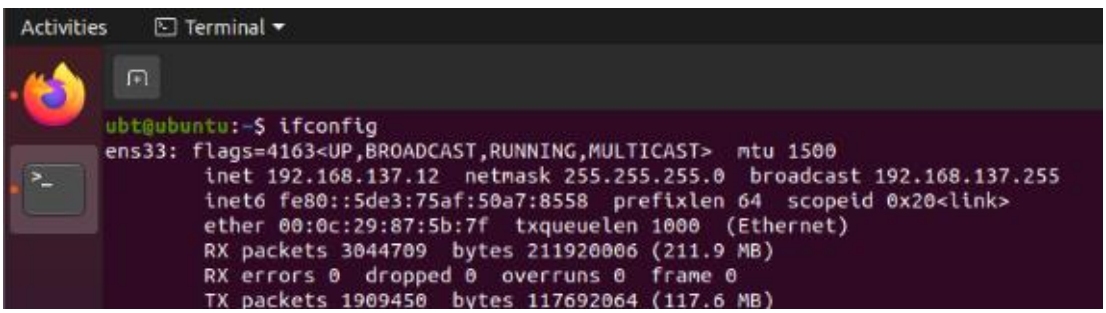
Mục đích xây dựng kịch bản nhằm kiểm tra các rule đã chặn được nhân viên các khoa phòng truy cập vượt quyền trái phép giữa các phòng ban. Qua đó giúp nhà quản trị mạng xây dựng được có các rule hiệu quả trong bảo đảm an toàn thông tin trong hệ thống.

❖ **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.

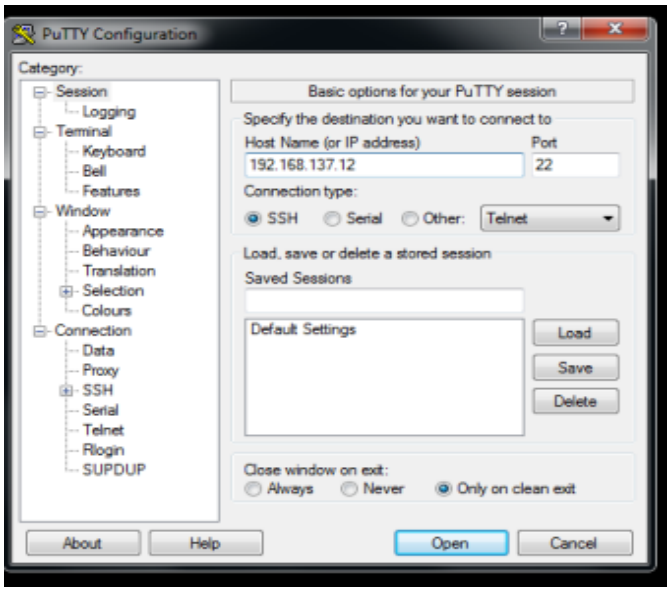


Hình 4.8: Địa chỉ máy tấn công trong kịch bản 2

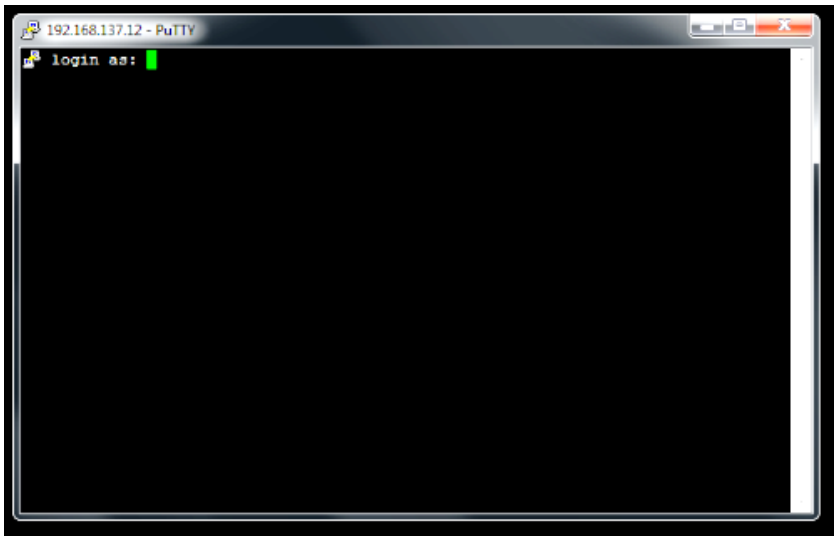


Hình 4.9: Địa chỉ máy mục tiêu trong kịch bản 2

❖ **Thực hiện tấn công:** Sử dụng phần mềm Putty trên hệ điều hành Window 7 để xâm nhập tiến hành remote lên máy tính Linux:



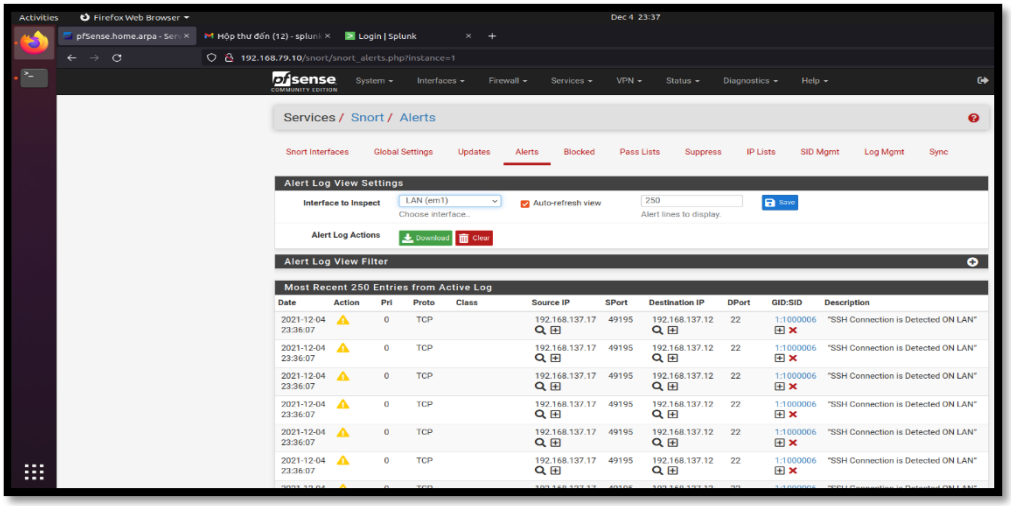
Hình 4.10: Nhập thông tin máy mục tiêu



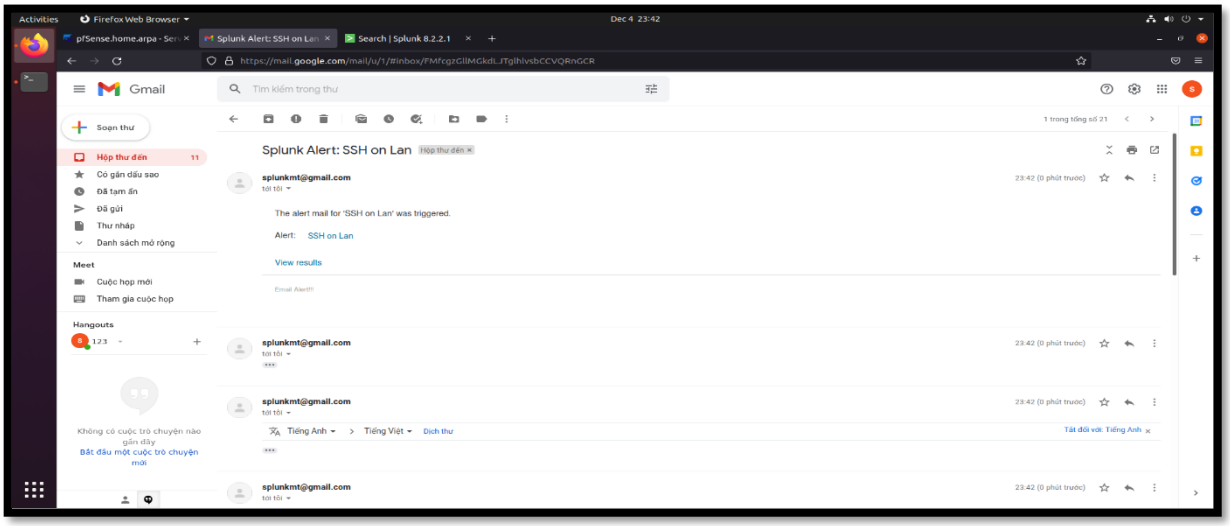
Hình 4.11: Tiến hành SSH vào máy Ubuntu mục tiêu.

❖ **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 mail về cho nhà quản trị mạng.



Hình 4.12: Màn hình cảnh báo trong kịch bản 2



Hình 4.13: Nội dung cảnh báo về mail trong kịch bản 2

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. Nhằm mục đích thực hiện các kết nối không cần thiết ra bên ngoài, mục đích làm lộ thông tin tài khoản, hệ thống.

❖ **Mô tả**

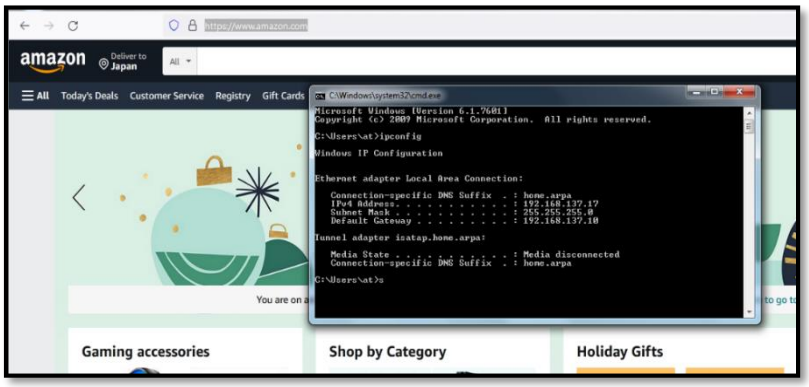
Sử dụng 1 tài khoản vùng mạng Active Directory truy cập vào các Website không cần thiết cho công việc như: Facebook, Youtube,… không được nhà quản trị mạng cho phép và sau đó hệ thống sẽ gửi log về báo hiệu cho Server Snort.

❖ **Thực hiện tấn công**

Tài khoản người dùng này được đặt tên là "***at***". Khi sử dụng các trình duyệt Web, hệ thống yêu cầu người dùng đăng nhập tài khoản Active Directory để sử dụng trình duyệt.

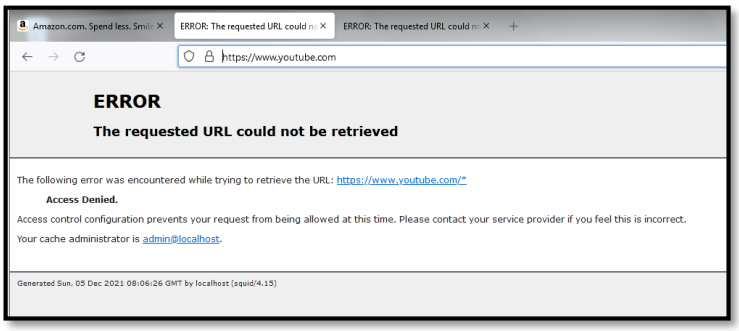
Hình 4.14: Đăng nhập để sử dụng proxy kịch bản 3

Với tài khoản **"*at*",** được phân quyền cho phép truy cập vào trang web : https://www.amazon.com/



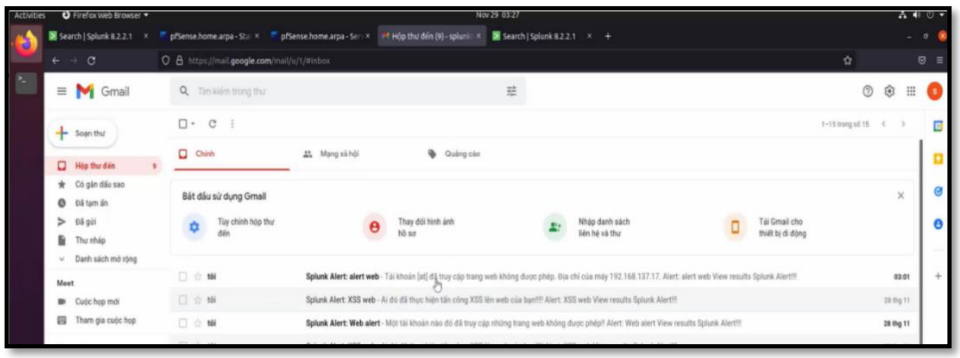
Hình 4.15: Đăng nhập và sử dụng thành công

Sau đó, tài khoản ***"at"*** tiến hành truy cập vào các trang web như: https://www.youtube.com/ và https://www.facebook.com/ không được phân quyền, sẽ bị hệ thống tường lửa Pfsense ngăn chặn thì trả về cùng 1 kết quả từ chối.



Hình 4.16: Truy cập vào trang web bị chặn

Và sau đó WebServer sẽ nhận được log cảnh báo do phần mềm Splunk gửi về và báo qua mail cho nhà quản trị mạng.



Hình 4.17: Nội dung cảnh báo về mail trong kịch bản 3

4.1.2.4 Kịch bản tấn công 4

❖ **Mục đích**

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. Mục đích kiểm tra khả năng bảo vệ của hệ thống Snort đối với được các cuộc tấn công bằng nhiều máy cùng lúc và đưa ra cảnh báo mail cho nhà quản trị mạng.

Thực hiện tấn công DOS nhằm mục đích phá hoại hệ thống thông tin Bệnh viện, tấn công hệ thống máy chủ WebServer.

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

❖ **Mô tả**

Phòng ban ở vùng DMZ có chứa máy chủ Web Server có địa chỉ IP 192.168.43.138.

Hình 4.18: Địa chỉ máy mục tiêu trong kịch bản 4

Hình 4.19: Giao diện Website nội bộ của bệnh viện

IP của 5 máy thực hiện tấn công như sau:

- Máy thứ 1 Kali: 192.168.43.136
- Máy thứ 2 Parrot: 192.168.43.137
- Máy thứ 3 Ubuntu: 192.168.43.138
- Máy thứ 4 Ubuntu 192.168.43.139
- Máy thứ 5 Ubuntu 192.168.43.140

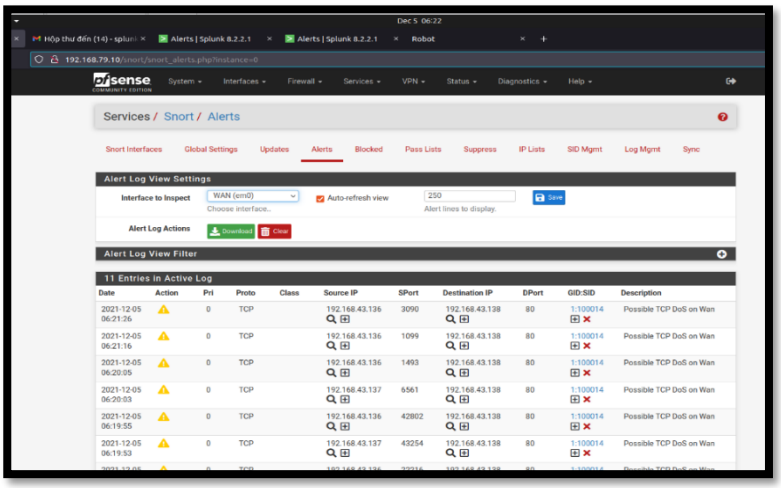
❖ **Thực hiện tấn công:**

Tất cả 5 máy này sẽ thực hiện DoS vào máy vùng DMZ cùng lúc.

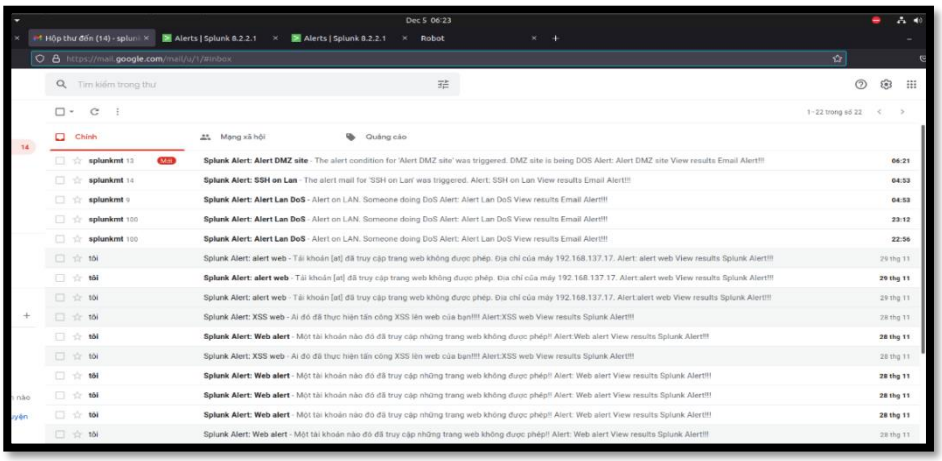
Câu lệnh tấn công sử dụng: ***sudo hping3 -S --flood -V -p 80 192.168.43.138***

Hình 4.20: Tấn công DOS từ máy Kali kịch bản 4

❖ Kết quả thu được



Hình 4.21: Màn hình cảnh báo trong kịch bản 4



Hình 4.22: Nội dung cảnh báo về mail trong kịch bản 4

4.1.2.5 Kịch bản tấn công 5

❖ **Mục đích**

Thực hiện tấn công cùng lúc bằng 5 máy từ mạng WAN vào hệ thống máy chủ WebServer vùng DMZ.

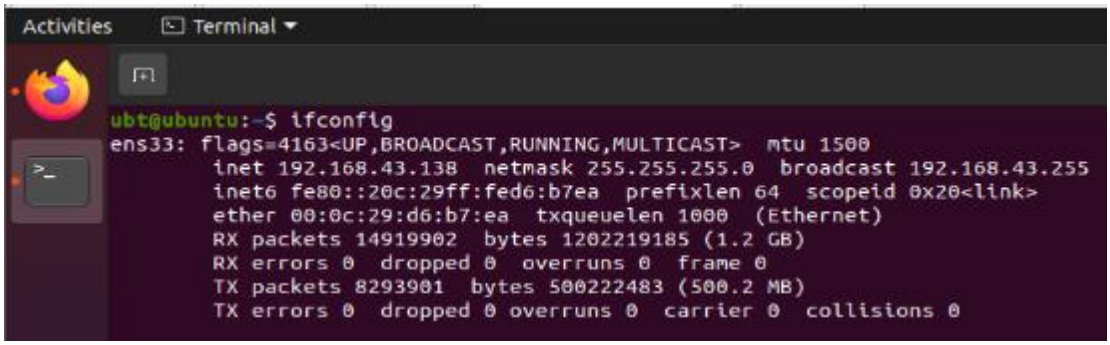
Thực hiện tấn công nhiều máy từ bệnh viện dã chiến – biên phòng vào hệ thống máy chủ Webserver vùng DMZ.

Lợi dụng tấn công thông qua lỗ hỏng XSS vào hệ thống máy chủ để xác định các rule xây dựng trên hệ thống IDS-Snort chặn được các tấn công, từ đó đưa ra cảnh báo mail cho nhà quản trị mạng.

Mục đích tấn công cùng lúc bằng nhiều máy nhằm phá hoại Cổng thông tin điện tử của Bệnh viện.

❖ **Mô tả**

Phòng ban ở vùng DMZ có chứa web server có địa chỉ: 192.168.43.138



Hình 4.23: Địa chỉ máy mục tiêu trong kịch bản 5

Những máy tấn công thuộc 2 vùng mạng khác nhau đó là từ bên ngoài và từ bên trong:

IP 5 máy từ vùng mạng bên ngoài

- Máy thứ 1 Parrot: 192.168.43.137
- Máy thứ 2 Ubuntu: 192.168.43.140
- Máy thứ 3 Ubuntu: 192.168.43.139
- Máy thứ 4 Ubuntu: 192.168.43.138
- Máy thứ 5 Ubuntu: IP 192.168.43.138

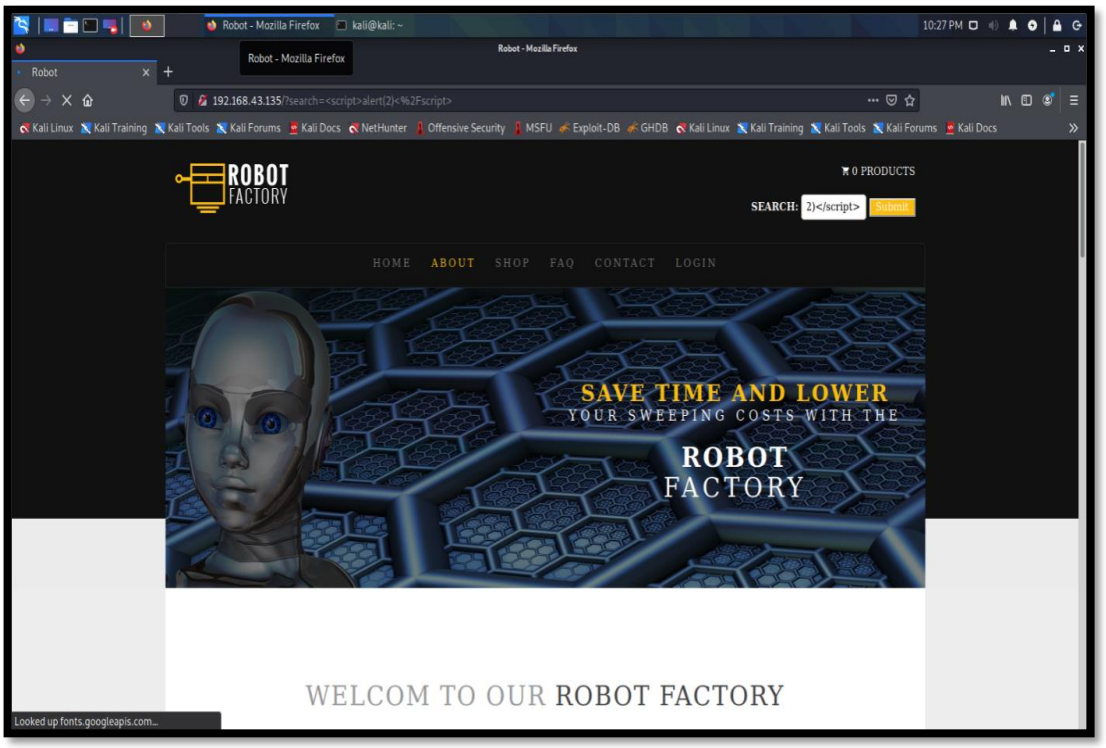
❖ **Thực hiện tấn công**

Thực hiện tấn công bằng 5 máy tính ở các vùng mạng khác nhau, tấn công cùng lúc lên WebServer bằng lỗ hổng Web.

Mục đích kiểm tra khả năng bảo vệ của hệ thống cảnh báo Snort đối với được các cuộc tấn công bằng nhiều máy cùng lúc và đưa ra cảnh báo mail cho nhà quản trị mạng.

Câu lệnh XSS cơ bản được sử dụng:

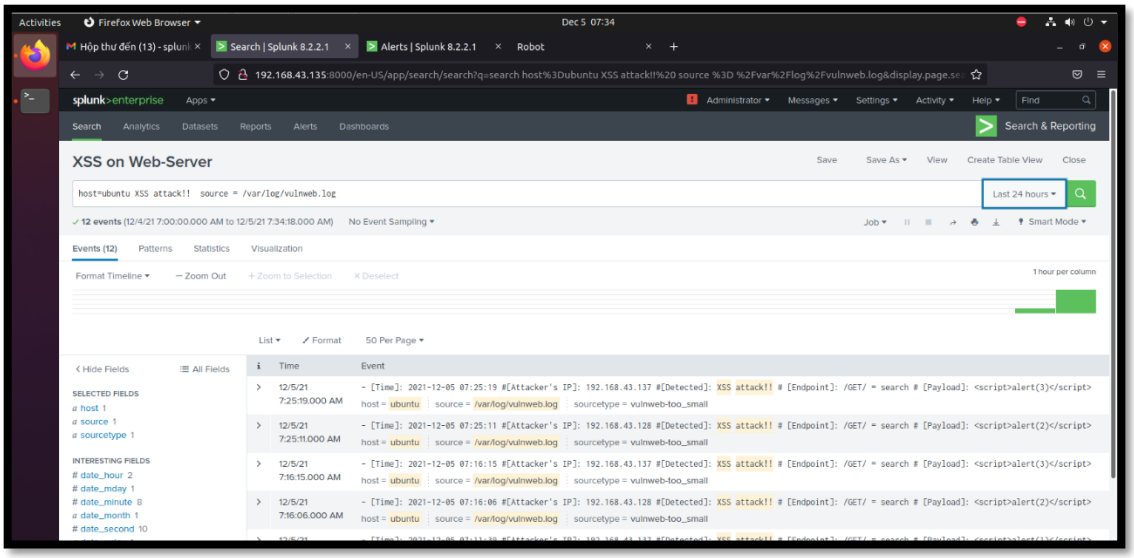
<script>alert(1)</script>



Hình 4.24: Thực hiện tấn công XSS trong kịch bản 5

➢ **Kết quả thu được**

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



Hình 4.25: Màn hình cảnh báo trên server Splunk kịch bản 5

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.

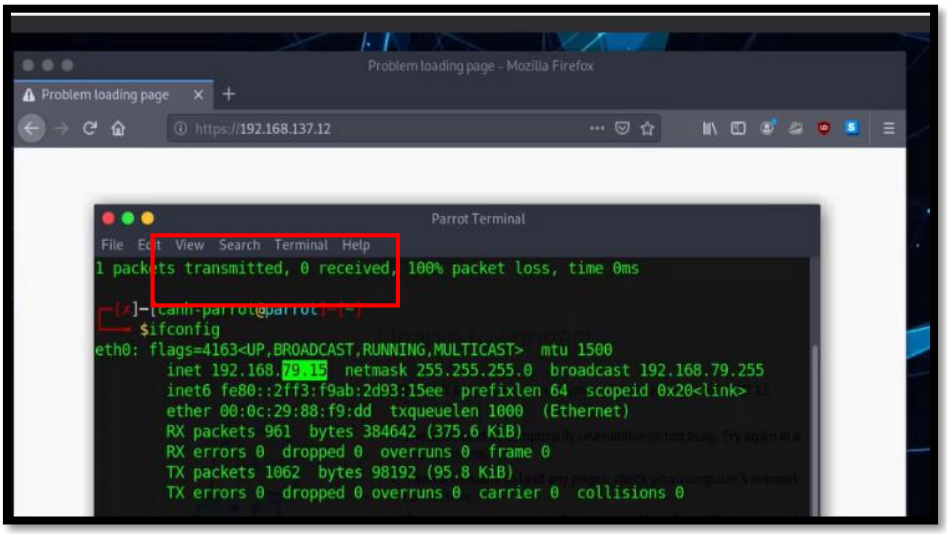
Mục đích kiểm tra được độ bảo mật Snort với hệ thống vùng DMZ, quản lý các Wifi cho bệnh nhân và nhân viên của bệnh viện. Cung cấp cho nhà quản trị mạng phương án phòng chống tấn công WLAN.

Thực hiện tấn công để IDS-Snort phát hiện và cảnh báo bảo vệ hệ thống từ WLAN

❖ **Mô tả**

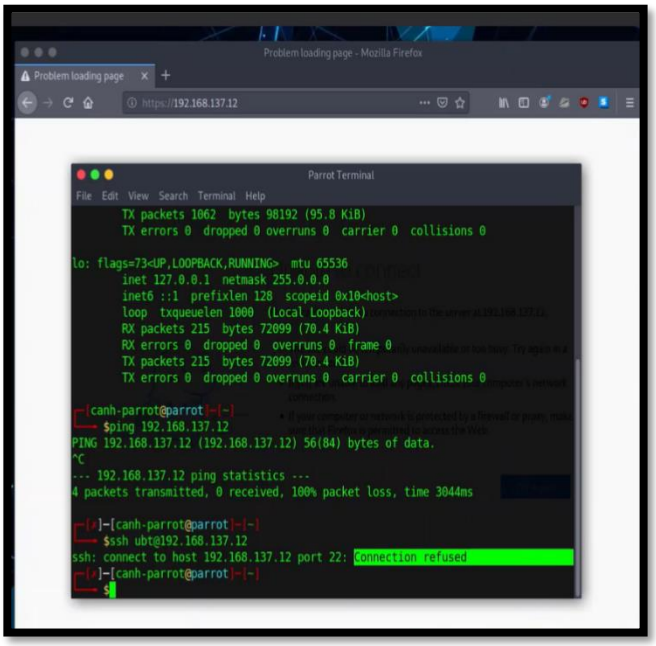
Thực hiện tấn công bằng 2 máy từ vùng mạng ngoài: Máy nhân viên được phép vào máy chủ web, máy chủ phần mềm, còn máy bệnh nhân thì chỉ được phép vào máy chủ Website nhưng không được vào máy chủ phần mềm.

Máy bệnh nhân có IP 192.168.79.15 được coi như là máy bệnh nhân sẽ chỉ được phép truy cập vào máy chủ web. Còn máy nhân viên có IP: 192.168.79.14 thì được cho phép vào các hệ thống máy chủ.



Hình 4.26: Máy bệnh nhân có IP bị chặn trong kịch bản 6

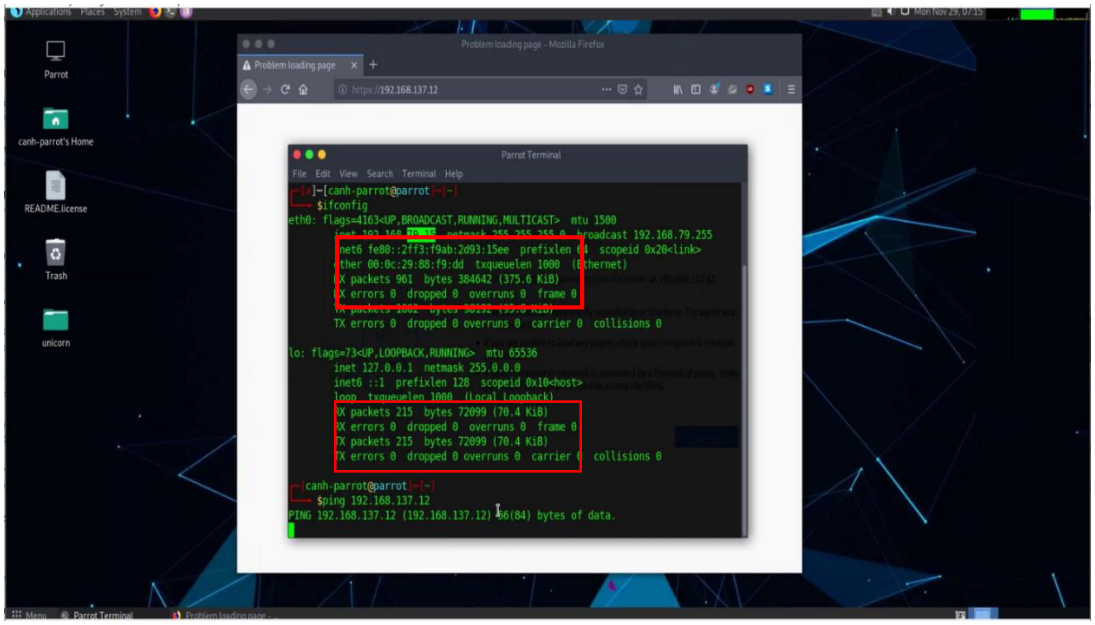
❖ **Thực hiện tấn công**



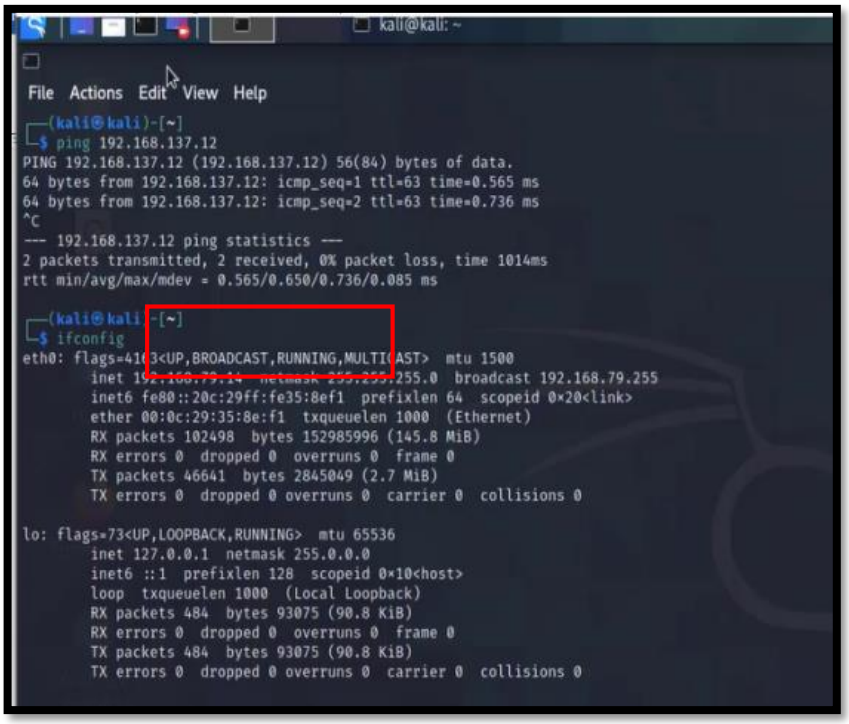
Hình 4.27: Thực hiện SSH trên máy mục tiêu trong kịch bản 6

❖ **Kết quả**

Và khi bệnh nhân cố gắng sử dụng tấn công SSH lên server thì không thể nào thực hiện được:



Hình 4.28: Máy bệnh nhân kết quả truy cập web từ máy bị chặn



Hình 4.29: Kết quả trên 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 dã chiến 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

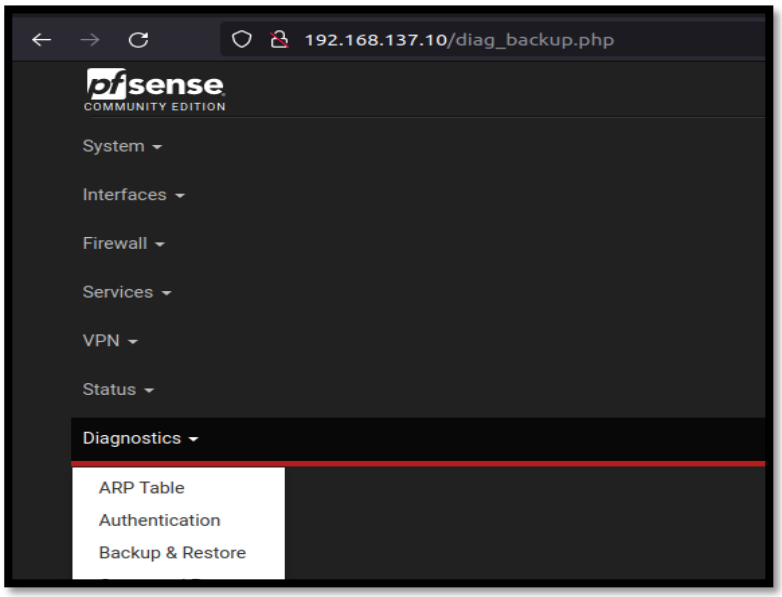
Ở đây vì là bệnh viện dã chiến không lớn như bệnh viện chính nên chúng ta sẽ chỉ sử dụng 1 hệ thống mạng LAN để kết nối

❖ **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.

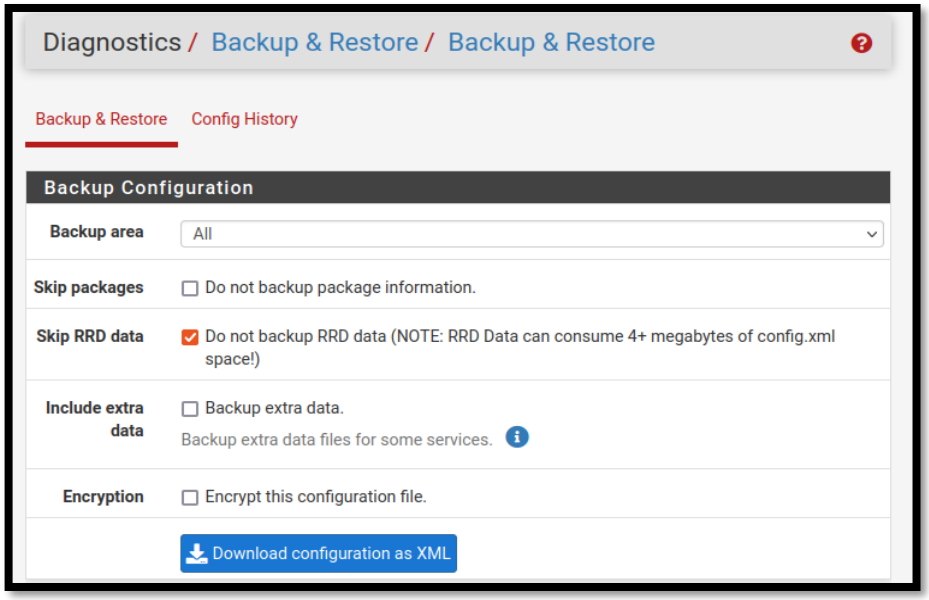
Xây dựng một hệ thống mạng hoàn toàn mới với dãy địa chỉ mạng LAN 192.168.140.0/24.

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



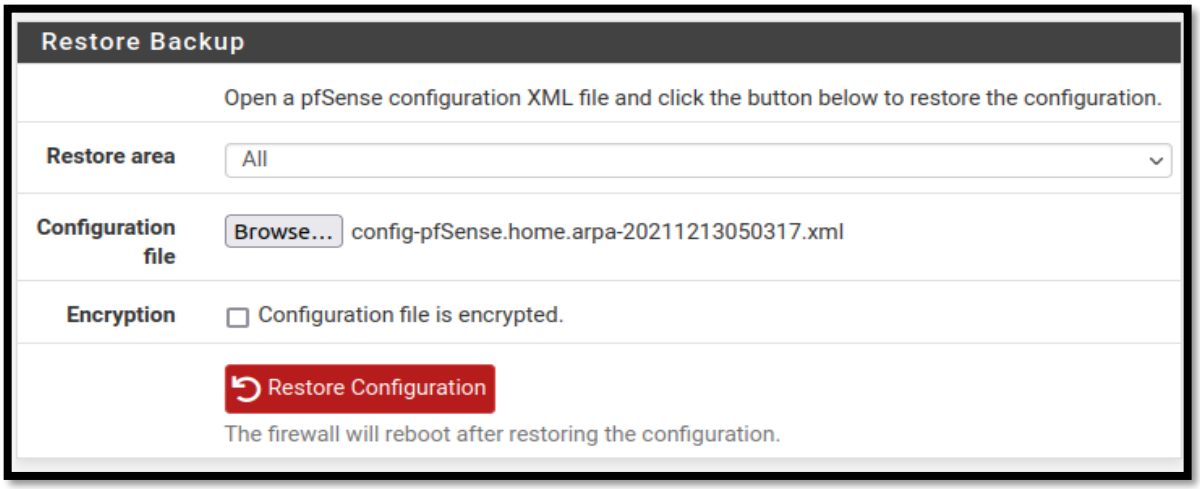
Hình 4.30: Backup và Restore của pfsense

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



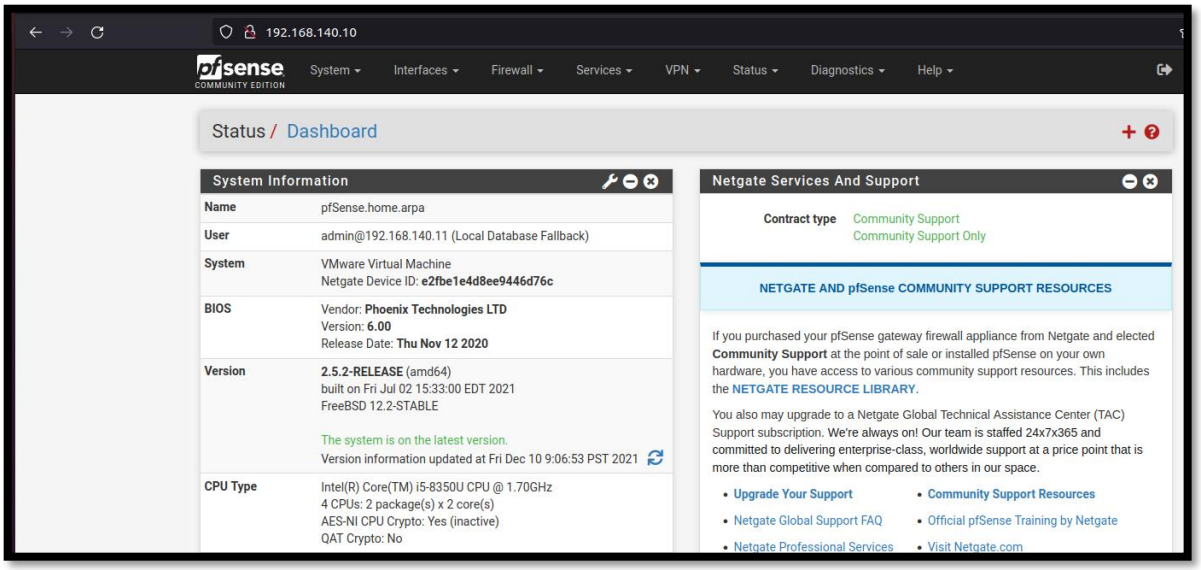
Hình 4.31: Xuất ra file Backup Configuration

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



Hình 4.32: Nhập file Backup vào hệ thống mới

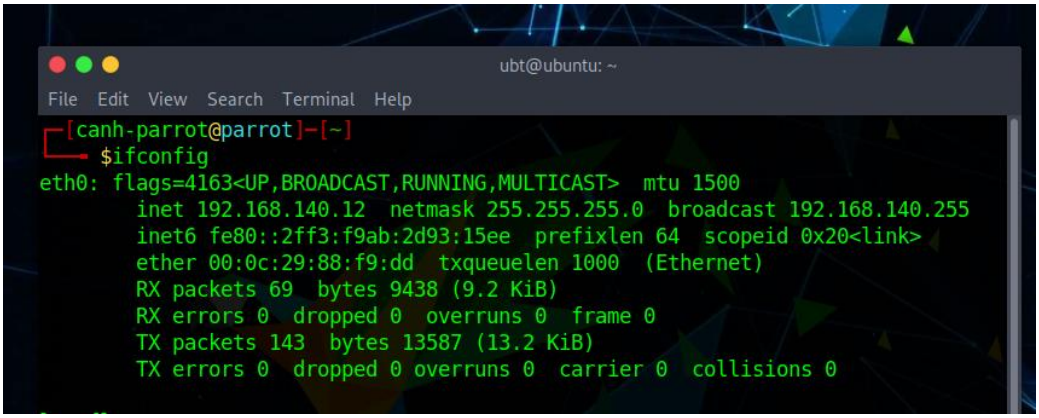
Tùy chỉnh lại hệ thống mạng cho hệ thống. Sau đó đăng nhập màn hình quản lý của người quản trị. Đăng nhập xong sẽ có giao diện như sau:



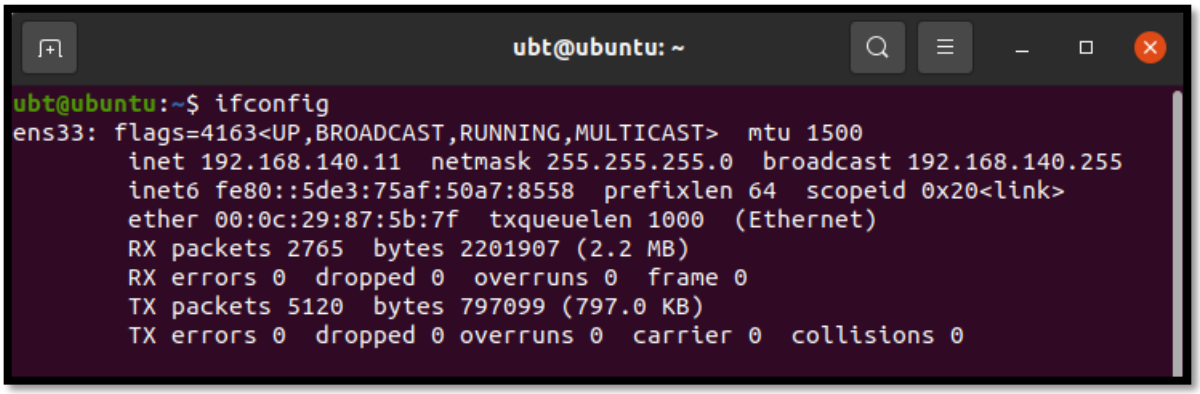
Hình 4.33: Giao diện Snort của máy mới

Vậy là công đoạn thiết lập máy chủ hoàn tất. Hệ thống công nghệ thông tin có thể đáp ứng được nhu cầu mở rộng mạng lưới cơ sở y tế cũng như hệ thống khám chữa bệnh của Bệnh viện. Đáp ứng tức thời trong trường hợp phục vụ tình hình chống dịch bệnh COVID-19 cấp bách của ngành Y tế địa phương, của tỉnh.

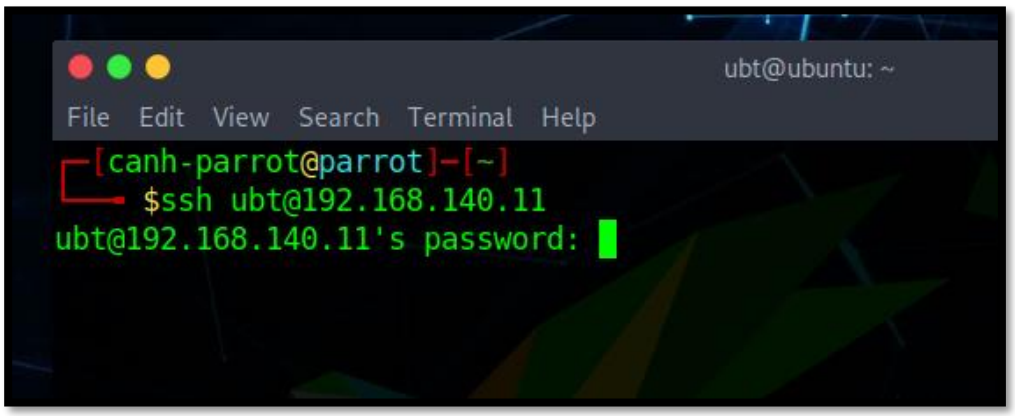
Thử nghiệm thực hiện tấn công và ngăn chặn để kiểm tra hệ thống.



Hình 4.34: Địa chỉ IP máy tấn công trong kịch bản 7

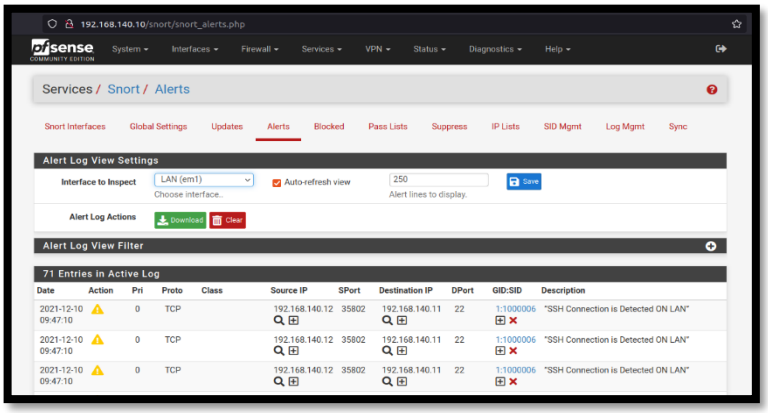


Hình 4.35: Địa chỉ IP máy bị tấn công trong kịch bản 7



Hình 4.36: Thực hiện tấn công SSH

❖ **Kết quả thu được**



Hình 4.37: Thông tin log lại tấn công của máy snort mới

4.1.3 Đánh giá

4.1.3.1 Đánh giá tính hiệu quả

- Với mô hình và các cấu hình đã đề xuất, mạng bênh viện sẽ được chia thành nhiều phân lớp có thể dễ dàng trong việc quản lý và xử lý các mối đe dọa đến hệ thống một cách sớm nhất và không gây ảnh hưởng cho các lớp mạng quan trọng.
- Các snort sẽ bổ trợ cho nhau trong việc giám sát và quản lý các kết nối ra vào hệ thống một cách chặt chẽ và có thể backup cho nhau nếu cần.
- Mỗi snort quản lý một vùng nhất định nên khi cần xử lý hoặc tương tác với vùng nào chúng ta chỉ cần truy cập vào snort đang đảm nhiệm chức năng đó. Giúp cho người quản trị dễ dàng đưa ra các chính sách phụ hợp với từng vùng.
- Các rules đề xuất sẽ giảm tối thiểu khả năng hệ thống bị đưa vào trạng thái downtime và cũng như bảo vệ hệ thống tránh khỏi các nguy cơ tấn công vào các máy quan trọng. Tránh việc tin tặc sẽ kiểm soát các vùng Server và đánh cắp thông tin.
- Trên địa bàn tỉnh và trong các cơ sở y tế, chưa có hệ thống giám sát an ninh mạng nào được áp dụng nên mô hình đề xuất là điểm mới. Phòng thủ trước các cuộc tấn công của tin tặc không bao giờ là thừa. Khi bị tấn công, hệ thống có sự chuẩn bị ứng phó sẽ tốt hơn các hệ thống khác không được trang bị chức năng giám sát mạng.
- Với các kịch bản đã xây dựng cho mô hình đề xuất, qua đó phát hiện được những điểm yếu của hệ thống mạng, nhằm chuẩn bị tốt nhất cho các trường hợp tấn công có thể xảy ra trong tương lai của Bệnh viện.

4.1.3.2 Đánh giá nguy cơ rủi ro

- Hệ thống IDS đã xây dựng còn chưa không nhận biết tấn công chèn mã độc vào file chính thống đi vào hệ thống dẫn đến rủi ro lớn là rất dễ mất dữ liệu hay mã hóa để tống tiền. Trong khi các hình thức tấn công mã độc tống tiền rất phổ biến hiện nay.

- Ngoài ra, nếu bị vô hiệu hóa hệ thống IDS khả năng hệ thống dễ tấn công ăn cắp dữ liệu, mã hóa hay phá hoại rất cao. Nên khi xây dựng hệ thống IDS, các nhà quản trị mạng luôn phải kết hợp với các thiết bị Backup, tường lửa để bảo mật và sẵn sàng hoạt động một cách tốt nhất.
- Hệ thống có nguy cơ bị lỗi thời so với trình độ và cách thức tấn công của tin tặc. Nên nhà quản trị mạng cần cập nhật hệ thống lên các bản mới nhất, rà soát bản vá giảm thiểu nguy cơ cho hệ thống.

Qua kết quả thực nghiệm giám sát hệ thống IDS Snort áp dụng trong Bệnh viện Đa khoa tỉnh Tây Ninh cho thấy khi kết hợp nhiều IDS-Snort thì kết quả bảo vệ hệ thống tốt hơn nhiều so với 1 IDS bảo vệ đường mạng tổng (đường internet vào), cụ thể:

- Thực nghiệm tấn công vào khoa xét nghiệm: Khi chúng ta xác định khoa xét là khoa quan trọng khi đây là nơi cho biết kết quả của bệnh nhân chính xác nhất qua xét nghiệm, để tránh bị lộ bí mật một số bệnh tình nhạy cảm của bệnh nhân ra ngoài nên chúng ta cần đặt 1 IDS-Snort để bảo vệ khoa xét nghiệm. Thử nghiệm các cuộc tấn công từ phòng ban khác tấn công Dos, tấn công SSH đều bằng chặn và phát hiện tại IDS, và cảnh báo cho quản trị mạng biết qua mail. Ngoài ra, cũng thử nghiệm cuộc tấn công từ bên ngoài vào khoa xét nghiệm bằng mạng Wan hoặc Wifi của người dùng thì đều được phát hiện chặn bởi 2 IDS trong hệ thống.
- Thực nghiệm tấn công từ các khóa không quan trong vào hệ thống máy chủ: nắm bắt được các mối nguy hiểm từ thực tế vào hệ thống máy chủ nên khi đây cũng nơi chứa hầu hết các dữ liệu quan trọng như thông tin bệnh nhân, hồ sơ nhân viên, và tài khoản người dùng, … nên đặt 1 IDS trước hệ thống datacenter để bảo vệ hệ thống. Qua các thử nghiệm tấn công từ các bên ngoài, từ bên trong hệ thống đều phát hiện và chặn tấn công hầu hết tất cả các cuộc tấn công như DOS, SSH, Scan port, brute force và cảnh báo qua mail người quản trị.
- Thực nghiệm tấn công từ các bệnh viện dã chiến vào hệ thống bệnh viện đa khoa tỉnh Tây Ninh: các cuộc tấn công đều phải đi qua 2 IDS-Snort (1 IDS-

Snort ở bệnh viện dã chiến, 1 IDS vào mạng bệnh viện) cho thấy những tấn công đã bị chặn tại IDS-Snort của bệnh viện dã chiến, ngoài ra 1 số cuộc tấn công đã vượt qua IDS-Snort của bệnh viện dã chiến thì cũng bị chặn tại IDS-Snort đi vào hệ thống mạng của bệnh viện đa khoa tỉnh Tây Ninh.

Tóm lại, qua hệ thống giám sát, phát hiện tấn công kết hợp nhiều IDS-Snort bảo vệ từng khu vực tốt hơn nhiều với hệ thống 1 IDS-Snort bảo vệ hệ thống mạng bệnh viện. Nó phòng chống được các cuộc tấn công mà 1 IDS khống thể giám sát được như tấn công nội bộ hoặc một số cuộc tấn công có thể vượt qua IDS-Snort thứ nhất.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1. Kết luận

5.1.1 Về mặt lý thuyết

Trong khuôn khổ xây dựng và thông qua triển khai, nghiên cứu về hệ thống mã nguồn mở đối với hệ thống bệnh viện tỉnh. Về mặt lý thuyết đồ án đã nêu ra được các vấn đề cơ bản nhất của một hệ thống phát hiện xâm nhập và hệ thống ngăn chặn xâm nhập bằng IDS snort và các tool khác. Bên cạnh đó, đưa ra các nhận thức về những yêu cầu cần thiết để thiết lập và duy trì một hệ thống mạng an toàn. Các nội dung nghiên cứu mà đề tài đã đặt ra và giải quyết được như sau:

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

- Tìm hiểu cơ bản về hệ thống giám sát an ninh mạng, các thành phần và chức năng chính của hệ thống giam sát an ninh mạng.

- Nghiên cứu, tìm hiểu và khai thác hệ thống phát hiện xâm nhập mạng IDS và ngăn chặn xâm nhập mạng IPS.

- 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.

- Kết hợp xây dựng được giao diện quản trị ứng dụng SNORT trực quan với người sử dụng thông qua cộng cụ Pfsence.

- 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.

- Xây dựng hệ thống cảnh báo qua mail sử dụng splunk.

5.1.2 Về mặt thực tiễn

Snort sẽ giám sát và phân tích các hoạt động trong mạng theo các phân đoạn mạng khác nhau. Với hệ thống mạng bệnh viện khá phức tạp khi cần nhiều vùng truy cập và các cấp bậc khác nhau về việc bảo về an toàn mạng. Điểm khác biệt trong đồ án này đến từ việc sử dụng nhiều snort IDS trong một hệ thống mạng. SNORT sẽ được đặt ở 3 phân vùng: Phân vùng nội bộ - Mạng LAN của bệnh viện, Phân vùng DMZ – vùng mạng WAN bên ngoài và Phân vùng Remote – Mạng truy cập từ xa của các bệnh viện dã chiến. Đối với mỗi một phân vùng mạng SNORT cũng sẽ có những rules và mục đích quản lý và tùy chỉnh để thực hiện giám sát mạng khác nhau. SNORT vùng DMZ sẽ được đặt với mục đích sử dụng cho việc giám sát các cuộc tấn công từ bên ngoài, bên trong, có nhiệm vụ bảo vệ vùng ngoại vi của hệ thống mạng và hoạt động như một IDS mở rộng. SNORT vùng Remote sẽ có nhiệm vụ quản lý và giám sát lưu lượng truy cập giữa mạng nội bộ và các quyền truy cập từ xa được cấp cho các nhân viên ở bệnh viện dã chiến. Cuối cùng là SNORT vùng LAN để giám sát luồng mạng cục bộ được gán cho các nhóm khác nhau. Và bởi vì SNORT là ứng dụng single theard nên việc sử dụng nhiều IDS cũng sẽ giúp tăng tốc độ xử lý dẫn đến việc xác định và phân tích các hoạt động đáng ngờ một cách nhanh chóng và chính xác hơn. Khi một SNORT gặp vấn đề về các cuộc tấn công từ các tác nhân gây hại, các SNORT còn lại có thể bổ trợ và vẫn đảm bảo được tính khả dụng và chức năng giám sát của hệ thống mạng, đảm báo hệ thống vẫn có thể hoạt động một cách bình thường mà không gây ra sự cố đình trệ. Bên cạnh đó là khả năng bảo vệ đối với các vùng mạng tối quan trọng trong hệ thống mạng được giám sát và quản lý bằng các quy định cũng như luật lệ một cách chặt chẽ hơn và khả năng bảo mật cũng được nâng lên một bậc.

- 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.

- Xây dựng được các chính xác rule bảo vệ hệ thống mạng bệnh viện từ các mối nguy hại bên trong và bên ngoài hệ thống.

5.2 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 như bệnh viện các tuyến huyện.

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

+ Nghiên cứu tích hợp hệ thống Snort với các IDS khác cũng như các tool khác để hỗ trợ phát hiện các cuộc tấn công và bất thường hơn, giả lập nhiều dạng tấn công hệ thống.

+ Xây dựng các hệ thống cảnh báo kết hợp Snort với AI để đưa ra những kết quả chính xác hơn, tốt hơn và nhanh hơn.

TÀI LIỆU THAM KHẢO

[1]. A. Abdelsalam, S. Salsano, F. Clad, P. Camarillo and C. Filsfils (2018), "SR-Snort: IPv6 Segment Routing Aware IDS/IPS" IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 1.2.

[2]. A. Khurat and W. Sawangphol (2019), "An Ontology for SNORT Rule" 2019 16th International Joint Conference on Computer Science and Software Engineering (JCSSE), pp. 49-55.

[3]. B. Habib, F. Khurshid, A. H. Dar and Z. Shah (2019), "DDoS Mitigation in Eucalyptus Cloud Platform Using Snort and Packet Filtering — IP-Tables" 2019 4th International Conference on Information Systems and Computer Networks (ISCON), pp. 546-550.

[4]. B. M. Khammas, S. Hasan, R. A. Ahmed, J. S. Bassi and I. Ismail (2018), "Accuracy Improved Malware Detection Method using Snort Sub-signatures and Machine Learning Techniques" 2018 10th Computer Science and Electronic Engineering (CEEC), pp. 107-112.

[5]. B. Siregar, R. F. Dwiputra Purba, Seniman and F. Fahmi (2018), "Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm" 2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), pp. 55-59.

[6]. B. -Y. Zhang, C. -Z. Wei, X. -H. Yang and B. -B. Song (2018), "Design and implementation of a network based intrusion detection systems" 2018 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), pp. 451.454.

[7]. C. Li, J. Yang, G. Li and K. Wang (2019), "A Lightweight Estimation Algorithm To Auto Configure Snort Fast Pattern Matcher" IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium), pp. 175-182.

[8]. D. Fadhilah and M. I. Marzuki (2020), "Performance Analysis of IDS Snort and IDS Suricata with Many-Core Processor in Virtual Machines Against Dos/DDoS Attacks" 2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP), pp. 157-162.

[9]. G. Zhang and E. Li (2020), "Research on IDS Snort Based on Classic Clustering Algorithm" International Conference on Urban Engineering and Management Science (ICUEMS), pp. 673.676.

[10]. H. Hendrawan, P. Sukarno and M. A. Nugroho (2019), "Quality of Service (QoS) Comparison Analysis of Snort IDS and Bro IDS Application in Software Define Network (SDN) Architecture" 2019 7th International Conference on Information and Communication Technology (ICoICT), pp. 1.7.

[11]. H. M. Elshafie, T. M. Mahmoud and A. A. Ali (2019), "Improving the Performance of the Snort Intrusion Detection Using Clonal Selection" 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), pp. 104.110.

[12]. İlayda Gündoüdu; Ali Aydın Selçuk; Süleyman özarslan (2021), “Effectiveness Analysis of Public Rule Sets Used in Snort Intrusion Detection System” 2021 29th Signal Processing and Communications Applications Conference (SIU), pp. 1.4.

[13]. J. E. C. de la Cruz, C. A. R. Goyzueta and C. D. Cahuana (2020), "Intrusion Detection and Prevention System for Production Supervision in Small Businesses Based on Raspberry Pi and Snort" IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing (INTERCON), pp. 1.4.

[14]. S. A. Changazi, I. Shafi, K. Saleh, M. H. Islam, S. M. Hussainn and A. Ali (2019), "Performance Enhancement of Snort IDS through Kernel Modification" 2019 8th International Conference on Information and Communication Technologies (ICICT), pp. 155-161.

[15]. S. k. Kang, D. Lindskog and H. Samuel (2019), "An Implementation of Hierarchical Intrusion Detection Systems Using Snort and Federated Databases" 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) pp. 1521.1525.

[16]. R. M. A. Ujjan, Z. Pervez and K. Dahal (2019), "Snort Based Collaborative Intrusion Detection System Using Blockchain in SDN" 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), pp. 1.8.

[17]. M. F. Kabir and S. Hartmann (2018), "Cyber security challenges: An efficient intrusion detection system design," 2018 International Young Engineers Forum (YEF-ECE), pp. 19-24.

[18]. M. Qayyum, W. Hamid and M. A. Shah (2018), "Performance Analysis of Snort using Network Function Virtualization" 2018 24th International Conference on Automation and Computing (ICAC), pp. 1.6.

[19]. X. Sun, D. Zhang, M. Liu, Z. He, H. Li and J. Li (2018), "Detecting and Resolving Inconsistencies in Snort" 2018 IEEE 17th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), pp. 552.560.

[20]. Z. Hassan, Shahzeb, R. Odarchenko, S. Gnatyuk, A. Zaman and M. Shah (2018), "Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems" 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), pp. 283.288.

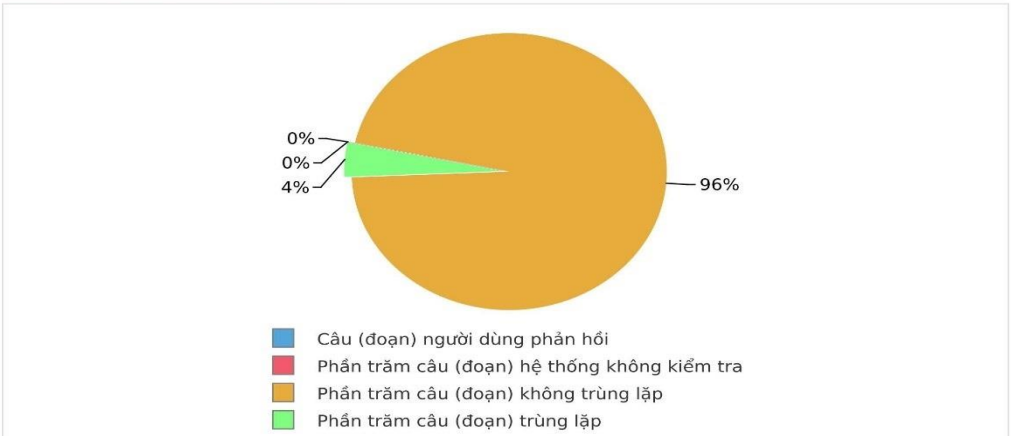
Hệ thống hỗ trợ nâng cao chất lượng tài liệu

KẾT QUẢ KIỂM TRA TRÙNG LẶP TÀI LIỆU

THÔNG TIN TÀI LIỆU

Tác giả	Nguyễn Anh Tú
Tên tài liệu	Xây dựng hệ thống giám sát mạng dành cho Bệnh viện Đa khoa cấp tỉnh với mã nguồn mở
Thời gian kiểm tra	25-01-2022, 15:06:31
Thời gian tạo báo cáo	25-01-2022, 15:08:52

KẾT QUẢ KIỂM TRA TRÙNG LẶP



Điểm	4
Nguồn trùng lặp tiêu biểu	[text.123doc.org, 123doc.org, thuvienphapluat.vn]

HỌC VIÊN **NGƯỜI HƯỚNG DẪN KHOA HỌC**

NGUYỄN ANH TÚ **TS. ĐÀM QUANG HỒNG HẢI**

BẢN CAM ĐOAN

Tôi cam đoan đã thực hiện việc kiểm tra mức độ tương đồng nội dung luận văn/luận án qua phần mềm DoIT một cách trung thực và đạt kết quả mức độ tương đồng **4%** toàn bộ nội dung luận văn/luận án. Bản luận văn/luận án kiểm tra qua phần mềm là bản cứng luận văn/luận án đã nộp bảo vệ trước hội đồng. Nếu sai tôi xin chịu các hình thức kỷ luật theo quy định hiện hành của Học viện.

TP.HCM, ngày 25 tháng 01 năm 2022

HỌC VIÊN CAO HỌC

NGUYỄN ANH TÚ