HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN ĐẮC THỜI

XÂY DỰNG CÁC HỆ THỐNG PHÂN TÍCH, QUẢN LÝ MẠNG TRÊN CƠ SỞ TÍCH HỢP NHIỀU MÃ NGUỒN MỞ

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

TP.HCM – NĂM 2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN ĐẮC THỜI

XÂY DỰNG CÁC HỆ THỐNG PHÂN TÍCH, QUẢN LÝ MẠNG TRÊN CƠ SỞ TÍCH HỢP NHIỀU MÃ NGUỒN MỞ

Chuyên ngành : HỆ THỐNG THÔNG TIN

Mã số: 8480104

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. ĐÀM QUANG HỒNG HẢI

TP.HCM – NĂM 2022

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi dưới sự hướng dẫn của Thầy **TS. Đàm Quang Hồng Hải.**

Kết quả đạt được đều là sản phẩm của cá nhân nghiên cứu, không sao chép lại của người khác. Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

TP.HCM, ngày 25 tháng 01 năm 2022

Học viên thực hiện luận văn

Nguyễn Đắc Thời

LỜI CẢM ƠN

Lời đầu tiên, tôi xin bày tỏ lòng biết ơn chân thành nhất đến Thầy **TS. Đàm Quang Hồng Hải**. Thầy đã trực tiếp hỗ trợ, định hướng xuyên suốt trong quá trình tôi thực hiện luận văn " **Xây dựng các hệ thống phân tích, quản lý mạng trên cơ sở tích hợp nhiều mã nguồn mở**".

Tôi cũng xin cảm ơn các Thầy Cô giảng viên của Học Viện Công Nghệ Bưu Chính Viễn Thông tại cơ sở Thành Phố Hồ Chí Minh đã tận tình giảng dạy, hướng dẫn tôi trong suốt quá trình học tập và nghiên cứu.

Cuối cùng, tôi xin chân thành cảm ơn những người thân, bạn bè, đồng nghiệp đã luôn động viên, sẻ chia, tạo điều kiện cho tôi hoàn thành tốt luận văn này.

Mặc dù tôi đã cố gắng thực hiện tốt các nội dung nghiên cứu, song cũng không tránh khỏi những thiếu sót nhất định. Tôi rất mong nhận được các ý kiến đóng góp của quý thầy cô để tôi hoàn thiện hơn luận văn của mình.

TP.HCM, ngày 25 tháng 01 năm 2022

Học viên thực hiện luận văn

Nguyễn Đắc Thời

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

LỜI MỞ ĐẦU

Hiện tại có rất nhiều công cụ IDS và các công cụ hỗ trợ phân tích log, trực quan hóa dữ liệu mã nguồn mở. Mỗi loại công cụ có những ưu điểm, nhược điểm khác nhau, và khi kết hợp lại sẽ có những hệ thống có tính phù hợp, hiệu quả khác nhau. Nghiên cứu của tác giả nhằm giúp quản trị viên có thể nhanh chóng lựa chọn được hệ thống tối ưu cho mô hình mạng hiện tại của doanh nghiệp.

Nhận thấy mô hình quản lý mạng hiện tại của Viettel Tây Ninh đang còn rất đơn sơ và nhiều thiếu sót cần cải thiện để đảm bảo an toàn thông tin, học viên thực hiện đề tải ***"Xây dựng các hệ thống phân tích, quản lý mạng trên cơ sở tích hợp nhiều mã nguồn mở"*** nhằm tiếp cận những kiến thức chuyên sâu, từ đó đưa ra những giải pháp phù hợp để giám sát hệ thống mạng LAN dựa trên hệ thống quản lý sử dụng các mã nguồn mở.

Nội dung luận văn được chia làm 05 phần như sau:

Chương 1: TỔNG QUAN VỀ AN TOÀN HỆ THỐNG MẠNG VÀ MẠNG VIETTEL TÂY NINH

Chương 2: CÁC CÔNG NGHỆ AN TOÀN HỆ THỐNG MẠNG:

Chương 3: XÂY DỰNG HỆ THỐNG PHÂN TÍCH QUẢN LÝ MẠNG TRÊN MÃ NGUỒN MỞ, TRIỂN KHAI VỚI CÁC CÔNG NGHỆ IDS KHÁC NHAU

Chương 4: CHƯƠNG 4 - XÂY DỰNG HỆ THỐNG PHÂN TÍCH QUẢN LÝ MẠNG ĐA LỚP VỚI NHIỀU CÔNG NGHỆ IDS MÃ NGUỒN MỞ ỨNG DỤNG TẠI VIETTEL TÂY NINH

Chương 5: CHƯƠNG 5 – KẾT LUẬN

CHƯƠNG 1-TỔNG QUAN VỀ AN TOÀN HỆ THỐNG MẠNG VÀ MẠNG VIETTEL TÂY NINH

1.1 Các công trình thế giới

Trong tin học, xâm nhập có nghĩa là truy cập hoặc sử dụng trái phép hệ thống máy tính. Schell và Martin (2006, 180) định nghĩa hành động xâm nhập là "xâm nhập hệ thống máy tính bằng cách phá vỡ bảo mật hoặc khiến nó rơi vào trạng thái không an toàn". Để giám sát và cảnh báo các quản trị viên hệ thống về việc sử dụng trái phép như vậy, cần có một công cụ. Rehman (2003, 5-6) mô tả IDS là hệ thống có các phương pháp và kỹ thuật để phát hiện hoạt động trái phép dựa trên các quy tắc và chữ ký. Các hệ thống phát hiện xâm nhập này cung cấp cho người quản trị hệ thống một công cụ khả thi có thể được sử dụng để tự động giám sát hệ thống và cung cấp cảnh báo cho người quản trị hệ thống. Sử dụng các hệ thống này, quản trị viên có thể phát hiện ra việc sử dụng trái phép hệ thống của họ và theo dõi việc sử dụng đáng ngờ.

Hệ thống phát hiện xâm nhập có lịch sử lâu đời hàng thập kỷ cùng với sự phát triển của hệ thống máy tính. Khan Pathan (2014, chương 2.) đã theo dõi sự khởi đầu của lịch sử IDS đến những năm 1980 khi nghiên cứu đầu tiên về các hệ thống như vậy được xuất bản. Sự phát triển của hệ thống chỉ như một đối tượng nghiên cứu học thuật tiếp tục cho đến đầu những năm 1990 khi các sản phẩm IDS thương mại đầu tiên được tung ra thị trường.

Hệ thống phát hiện xâm nhập có thể được phân loại bằng nhiều cách khác nhau dựa trên phương pháp phát hiện của chúng, tình hình trong kiến trúc hệ thống và các hành động sau phát hiện. Theo Khan Pathan (2014, chương 2) có các phương pháp phát hiện dựa trên chữ ký và điểm bất thường, hệ thống dựa trên máy chủ, dựa trên mạng hoặc kết hợp sử dụng vị trí cảm biến và hệ thống phát hiện xâm nhập và hệ thống ngăn chặn xâm nhập dựa trên các hành động sau phát hiện.

Phương pháp phát hiện chữ ký và điểm bất thường khác nhau trong cách hệ thống đánh giá lưu lượng truy cập. Các hệ thống dựa trên chữ ký phát hiện các cuộc

xâm nhập bằng cách lưu trữ các chữ ký của các cuộc tấn công và hành vi của các phương thức xâm nhập đã biết và so sánh các chữ ký này với các hành động, lệnh và lưu lượng mạng mà các phương thức xâm nhập đã biết này sử dụng. Khi một trận đấu được tìm thấy, sự kiện sẽ được báo cáo. Một ví dụ về phát hiện chữ ký sẽ là theo dõi lưu lượng mạng đến cổng dịch vụ hệ thống gửi các gói dữ liệu đang cố gắng khai thác một lỗi đã biết.

Trong phát hiện dựa trên sự bất thường, hệ thống đang theo dõi các hành động, lệnh và lưu lượng mạng và nhận thức được hành vi bình thường có thể chấp nhận được. Khi hành vi đủ khác với đường cơ sở bình thường, sự kiện sẽ được báo cáo. Một ví dụ về phát hiện bất thường sẽ là một máy chủ phụ trợ cố gắng thực hiện mộtSSH đi kết nốiđến máy chủ internet khi nó không được phép theo chính sách của công ty.

IDS dựa trên máy chủ (HIDS) được cài đặt trên mọi máy chủ yêu cầu phát hiện xâm nhập và chúng báo cáo tất cả các sự kiện diễn ra trên máy chủ mà chúng được cài đặt, ví dụ thay đổi tệp hoặc lệnh đáng ngờ. IDS dựa trên mạng (NIDS) giám sát lưu lượng mạng và báo cáo tất cả các sự kiện liên quan đến lưu lượng mạng mà chúng giám sát, ví dụ: các kết nối đáng ngờ hoặc gói dữ liệu có chứa các kiểu tấn công đã biết. Hybrid IDS là một hệ thống sử dụng kết hợp cả các phương pháp và kỹ thuật IDS dựa trên máy chủ và dựa trên mạng để phát hiện các hành vi xâm nhập.

Các phương pháp phát hiện sau chia IDS thành hai loại khác nhau. Sự phát triển hợp lý của một hệ thống phát hiện xâm nhập là một hệ thống ngăn chặn xâm nhập (IPS). NIST-800-94 (2-1) mô tả IPS là “phần mềm có tất cả các khả năng của một hệ thống phát hiện xâm nhập và cũng có thể cố gắng ngăn chặn các sự cố có thể xảy ra”. Bằng cách sử dụng các khả năng của IDS để phát hiện ra các xâm nhập có thể xảy ra, hệ thống IPS sẽ có hành động tích cực để ngăn chặn sự xâm nhập. Một ví dụ về sự kiện IPS sẽ là lưu lượng độc hại đến một cổng dịch vụ mạng; sau khi phát hiện, IPS sẽ cảnh báo việc quản lý sự kiện như vậy, nhưng cũng chặn lưu lượng mạng từ IP nguồn đến cổng dịch vụ mạng để ngăn chặn bất kỳ sự xâm nhập nào. Điều này cũng có nghĩa là IPS cần phải ở vị trí để thực hiện các hành động phòng ngừa này, ví dụ

như thực thể truyền qua mạng hoặc khi HIDS được cài đặt trên máy chủ là mục tiêu của sự xâm nhập.

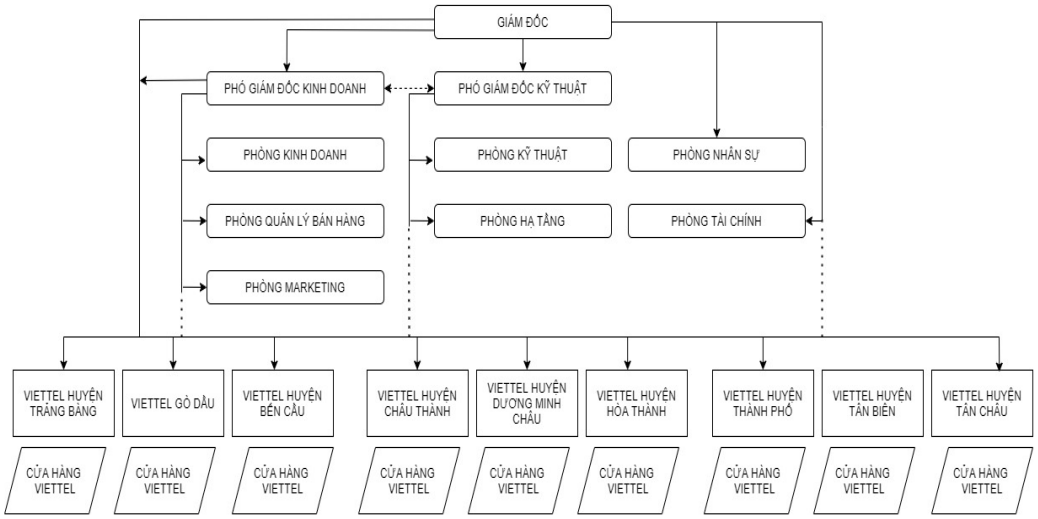
1.2 Các công trình trong nước

Trong nước, công nghệ IDS/IPS được áp dụng chủ yếu kế thừa từ các công trình nghiên cứu ngoài nước. Nhiều giải pháp xây dựng một hệ thống IPS trên thực tế đã được triển khai rất hiệu quả và được đánh giá cao. Hạn chế của những giải pháp này chỉ là triển khai hệ thống trên một phân đoạn mạng nhỏ, nên chưa đánh giá được hết hiệu suất của hệ thống và các vấn đề hệ thống IPS sẽ gặp phải khi triển khai thực tế.

Ngoài ra, nhiều giải pháp phát hiện và ngăn chặn xâm nhập mạng máy tính được triển khai tuy nhiên chỉ lựa chọn một trong các loại IDS hiện có như Snort, Suricata, Zeek. Chưa có sự đánh giá so sánh ưu điểm, nhược điểm của từng loại để phân tích và áp dụng một cách cụ thể vào từng loại hình doanh nghiệp.

1.3 Giới thiệu chung về Viettel Tây Ninh

Viettel Tây Ninh là một trong những đơn vị kinh doanh lớn nhất tỉnh Tây Ninh, với doanh thu hằng năm lên đến 1200 tỷ đồng, có lượng khách hàng lớn lên đến 800.000 khách hàng. Viettel Tây Ninh có trên dưới 500 cán bộ, nhân viên đang hoạt động ở nhiều kênh, lớp bán hàng từ mức tỉnh đến mức huyện.



Hình 1.1: Mô hình tổ chức tại Viettel Tây Ninh

1.4 Khảo sát hệ thống mạng tại Viettel Tây Ninh

Viettel Tây Ninh gồm có:

- Trụ sở chính tại Trung tâm Thành phố Tây Ninh:

+ 08 phòng ban chức năng riêng biệt: Phòng kinh doanh, Phòng kỹ thuật, Phòng nhân sự, Phòng CSKH, Phòng hạ tầng, Phòng tài chính, Phòng quản lý bán hàng, Phòng Marketing.

+ 01 Data center lưu trữ dữ liệu tập trung, các phần mềm ERP, kế toán, quản trị khách hàng, web server, FPT Server...

+ 01 Trung tâm bán lẻ chính thuộc trụ sở Viettel Tây Ninh(có sử dụng wifi)

- 09 Chi nhánh Viettel huyện tại trung tâm hành chính của từng huyện:

+ 01 Trung tâm bán hàng tại Viettel huyện (Gồm trưởng, phó huyện và 30 nhân sự bán hàng)

+ 01 Cửa hàng giao dịch với khách hàng (có sử dụng wifi để cung cấp trải nghiệm cho KH)

Tại trụ sở chính, hệ thống mạng LAN được kết nối và quản lý tập trung bằng Router chính. Hệ thống mạng LAN được quy hoạch mạng LAN nội bộ, chỉ có cán bộ nhân viên Viettel được phép sử dụng. Trụ sở chính là nơi đặt máy chủ dữ liệu, cho phép các chi nhánh kết nối đồng bộ dữ liệu.

Hệ thống mạng chi nhánh được trang bị server, hệ thống backup, lưu trữ và router cùng các phần mềm, ứng dụng, đường truyền WAN kết nối đến trụ sở chính.

a. Phân hệ quản trị mạng

Phân lớp mạng: Hệ thống mạng được thiết kế theo mô hình 3 lớp đảm bảo cho phát triển và bảo mật hệ thống.

Các lớp mạng được ngăn cách bởi Firewall nhằm ngăn chặn các xâm nhập bất hợp pháp từ bên trong cũng như bên ngoài cơ quan vào hệ thống trung tâm.

Máy chủ được phân theo chức năng phục vụ: Máy chủ Firewall, Máy chủ DNS, Web Server, Mail server, Application Server, Database Server, Backup Server. Hệ thống mạng được thiết kế đảm bảo cho phát triển và bảo mật hệ thống.

b. Phân hệ mạng DMZ

Máy chủ web Reverse proxy (Ngix Reverse Proxy) làm cổng giao tiếp chính với môi trường internet. Sử dụng hai máy chủ Web Apache đặt website, nhiệm vụ cân bằng tải cho trang. Các máy chủ web server kết nối vào cụm MySQL Cluster, nhiệm vụ cân bằng tải cho dịch vụ Database. Hai máy chủ web sẽ tự động đồng bộ dữ liệu của website theo thời gian thực.

c. Phân hệ máy chủ CSDL

Các máy chủ ứng dụng chứa các cơ sở dữ liệu chính (Data center), hết sức quan trọng do vậy khu vực này cần được đảm bảo an ninh bảo mật cao nhất.

Nhận xét

Hệ thống mạng của Viettel Tây Ninh 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 khi dữ liệu tập trung. Khi có tấn công xảy ra, quản trị viên không biết được tức thời để ngăn chặn, có thể dẫn đến việc đóng băng hệ thống, ngưng hoạt động toàn bộ hệ thống.

1.4.1 Các mối đe dọa tiềm năng đối với hệ thống

Hoạt động của Viettel Tây Ninh với số lượng cán bộ nhân viên lớn Hơn 500 nhân viên và hiện có hệ thống nhiều mạng LAN phân tán (Distributed Local networks) bao gồm mạng LAN của 09 chi nhánh huyện và Lan các phòng ban, trung tâm bán hàng. Khối lượng thông tin xử lý trong hoạt động khá lớn. Do đó trường cần xây dựng một hệ thống quản lý chung đảm bảo các yêu cầu về bảo mật. Hệ thống này phải đảm bảo các yêu cầu sau:

- Bảo đảm an toàn cho toàn bộ thông tin trên mạng, chống lại mọi sự truy nhập bất hợp pháp vào mạng. (Tấn công từ bên ngoài)
- Kiểm soát được mọi hành động truy nhập vào mạng của người sử dụng. Đảm bảo an ninh từ những người sử dụng bên trong. (tấn công từ bên trong).
- Đáp ứng được khả năng mở rộng của mạng trong tương lai: mở rộng về số lượng máy tính, số lượng máy chủ, các mạng LAN và các ứng dụng.

1.4.2 Phân tích chính sách bảo mật tại Viettel Tây Ninh

Để phân tích chính sách bảo mật, chúng ta phải phân tích được các vấn đề sau trong hệ thống thông tin của trường:

a. Xác định các tài nguyên cần được bảo vệ

Vấn đề quan trọng là phải xác định được các tài nguyên của mạng nội bộ có thể bị tác động bởi hệ thống bảo mật. Các tài nguyên cần được bảo vệ:

- Phần cứng: Các máy chủ của mạng, các máy tính, các thiết bị mạng (Routers, Access Servers).
- Phần mềm: Hệ điều hành của các máy chủ UNIX, Windows, các cơ sở dữ liệu và các phần mềm chuyên dụng.
- Dữ liệu: Đây là phần quan trọng cân được bảo vệ nhất. Dữ liệu này sẽ gồm có các dữ liệu liên quan đến dữ liệu khách hàng, các dữ liệu kinh doanh, dữ liệu kế toán.

b. Xác định các mối đe dọa hệ thống

Sau khi xác định tất cả các tài nguyên phải được bảo vệ,cần phải xác định mối đe dọa đối với các tài nguyên đó. Các mối đe doạ đó gồm có:

- Những truy nhập bất hợp pháp. Việc truy nhập vào các tài nguyên của mạng chỉ nên được thực hiện bởi những người đã xác định. Mối đe doạ chung mà mọi người quan tâm là việc truy nhập bất hợp pháp. Đặc thù của mối đe doạ này là sử dụng tên của người khác để truy nhập vào mạng và tài nguyên của nó.
- Sử dụng những chương trình dò tìm mật khẩu, Hút nạp dữ liệu (Spooling)
- Sử dụng lỗ hổng trong phần mềm: Không có phần mềm nào là không có lỗi. Một lỗi trong phần mềm là mối đe doạ chung của việc truy nhập bất hợp pháp.
- Mối đe doạ ảnh hưởng đến hoạt động bình thường của hệ thống (Denial of Service). Mạng thông tin nội bộ kết nối các tài nguyên có giá trị như máy tính, CSDL và cung cấp dịch vụ cho mọi thành viên của mạng. Tất cả người sử dụng của mạng đều tin rằng mọi hoạt động của mạng đều làm cho công việc

của họ trở nên có hiệu quả. Nếu mạng không làm việc thì sẽ có những mất mát trong hoạt động kinh doanh.

- Mối đe doạ từ bên trong. Người sử dụng bên trong mạng có nhiều cơ hội hơn để truy nhập vào các tài nguyên của hệ thống. Nếu người sử dụng trong mạng có ý muốn truy cập vào những tài nguyên của hệ thống thì họ sẽ gây nên một mối đe doạ cho mạng. Người sử dụng bên trong có thể được gán những quyền không cần thiết, có thể bị mất mật khẩu... và đó sẽ là mối đe doạ lớn đối với hệ thống an toàn mạng.

c. Xác định đối tượng có thể tấn công an toàn mạng đến Viettel Tây Ninh

Đối tượng tấn công đến Viettel Tây Ninh là nhóm đối tượng có khả năng CNTT cao, có kiến thức chuyên sâu và có mục đích tấn công rõ ràng:

- Đối tượng bên ngoài tấn công mục đích phá hoại hoặc khai thác thông tin.
- Đối tượng là nhân viên thuộc đơn vị A, muốn khai thác thông tin trái phép của đơn vị B thuộc Viettel Tây Ninh.
- Đối tượng là nhóm cấu kết giữa bên ngoài và nhân viên của Viettel Tây Ninh tấn công truy cập dữ liệu bất hợp pháp.

1.5 Kết luận chương

Những nghiên cứu vừa nêu trên đã đề cập đến triển khai các hệ thống phân tích, giám sát, quản lý mạng sử dụng các IDS. Trong luận văn này, tác giả tập trung nghiên cứu về các loại IDS, xây dựng các hệ thống Single – IDS, Multiple –IDS, thực nghiệm đánh giá hiệu quả, ưu điểm, nhược điểm của từng loại Single- IDS.

Tiếp theo, tác giả đưa ra sự kết hợp các loại Single - IDS khác nhau tạo nên hệ thống Mutiple – IDS tối ưu, có thể khắc phục được các nhược điểm của Single – IDS, bổ trợ lẫn nhau để đem lại tính hiệu quả cao nhất.

Từ đó, tác giả ứng dụng vào mô hình giám sát mạng hiện tại ở Viettel Tây Ninh, đề xuất xây dựng hệ thống Multiple- IDS phù hợp với đặc thù và có thể áp dụng được ngay tại Viettel Tây Ninh, đồng thời có tính dự trù cho tương lai khi doanh nghiệp có thể mở rộng hơn.

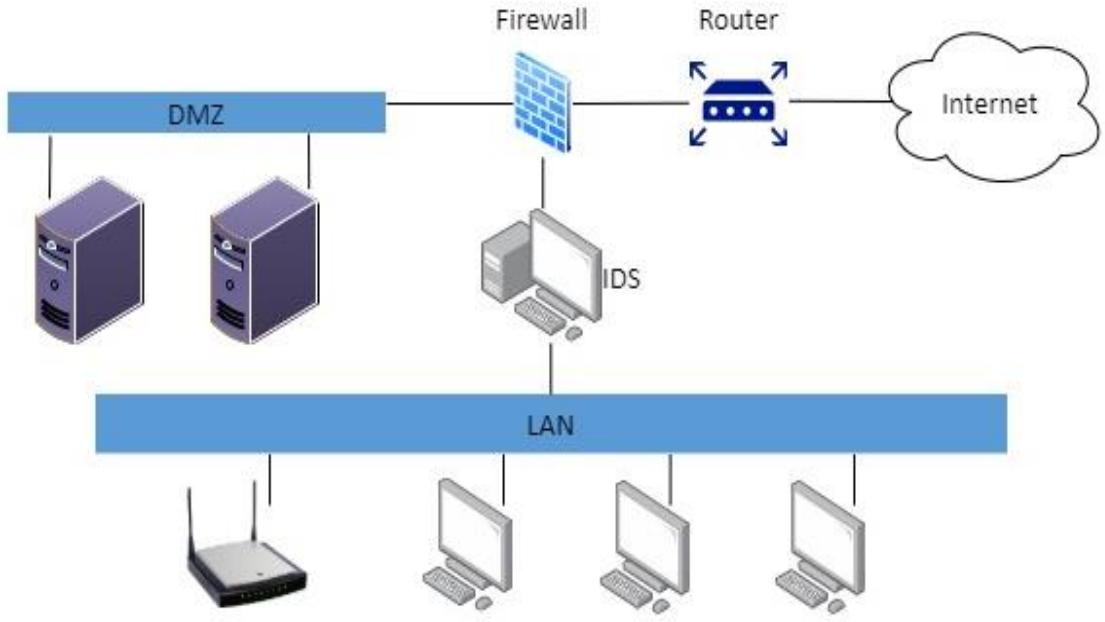
CHƯƠNG 2 - CÁC CÔNG NGHỆ AN TOÀN HỆ THỐNG MẠNG

2.1 Tổng quan hệ thống phát hiện xâm nhập IDS

2.1.1 Khái niệm IDS

IDS (Intrusion Detection System – hệ thống phát hiện xâm nhập) là thiết bị hoặc phần mềm ứng dụng giám sát, phân tích lưu lượng hệ thống hoặc lưu lượng mạng nhằm phát hiện các hành động bất thường, các hoạt động trái phép xâm nhập vào hệ thống.

IDS phát hiện dựa trên các dấu hiệu về nguy cơ đã biết (giống như cách thức hoạt động của antivirus) hoặc dựa trên việc so sánh lưu thông mạng hiện tại với thông số chuẩn của hệ thống để tìm ra các dấu hiệu bất thường. Từ đó đưa ra các cảnh báo đến quản trị viên.



Hình 2.1: Mô hình mạng NIDS

Chức năng cơ bản:

• Chức năng giám sát: các hành động bất thường, khả nghi.

• Chức năng cảnh báo: cảnh báo tới người quản trị khi có các hành động bất thường.

• Chức năng bảo vệ: bảo vệ chống lại kẻ xâm nhập, phá hoại bằng cách sử dụng những thiết lập mặc định và những cấu hình từ người quản trị.

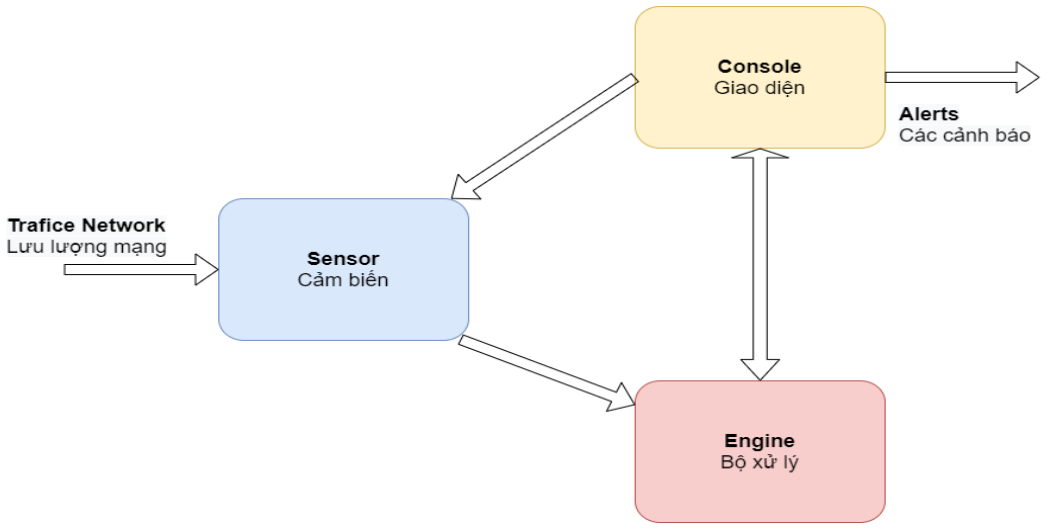
Chức năng mở rộng:

• Phân biệt được những tấn công tư bên ngoài và tấn công từ bên trong.

• Phát hiện những dấu hiệu bất thường dựa vào sự so sánh lưu lượng mạng.

2.1.2 Các thành phần IDS

Một hệ thống IDS bao gồm 3 thành phần cơ bản là:



Hình 2.2: Các thành phần trong IDS

• Cảm biến (Sensor): có nhiệm vụ quét nội dung các gói tin trên mạng, so sánh nội dung với các mẫu và phát hiện các dấu hiệu hoặc sự kiện. Bộ phận chịu trách nhiệm phát hiện các sự kiện có nguy cơ đe dọa đến hệ thống mạng.

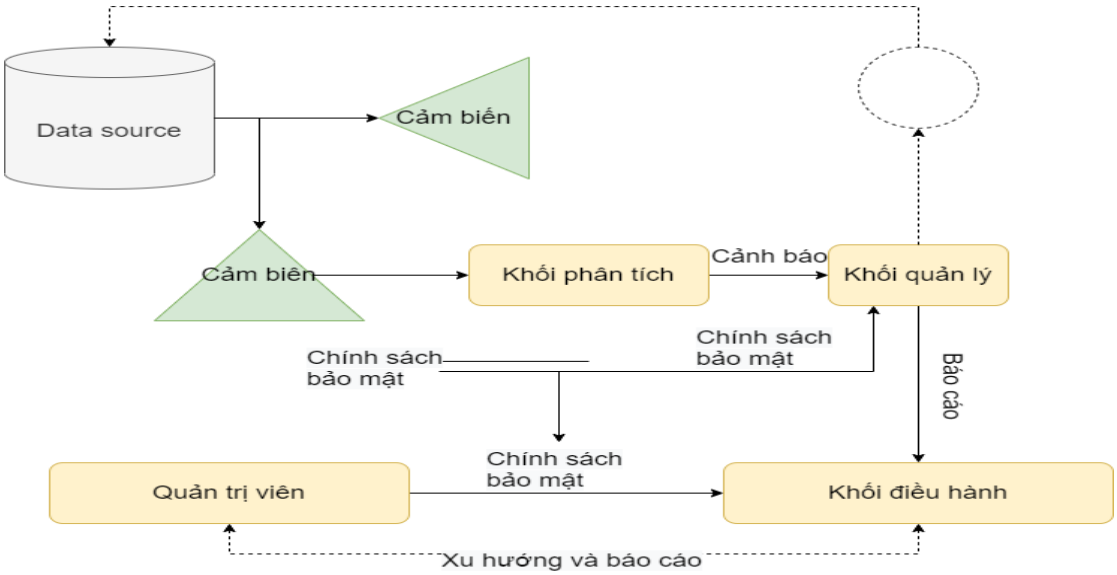
• Giao diện (Console): tương tác với quản trị viên, nhận cảm biến hoạt động của bộ điều khiển, Engine và đưa ra cảnh báo tấn công.

• Bộ xử lý (Engine):: chịu trách nhiệm ghi lại tất cả các báo cáo về các sự kiện do Cảm biến phát hiện trong cơ sở dữ liệu và sử dụng hệ thống quy tắc để đưa ra cảnh báo trên cảm biến. Các sự kiện sự kiện bảo mật được nhận cho hệ thống hoặc cho quản trị viên.

2.1.3 Cơ chế hoạt động IDS

Hệ thống IDS hoạt động theo cơ chế phát hiện và cảnh báo. Cảm biến là bộ phận được bố trí trên hệ thống tại các điểm cần điều khiển. Sensor bắt gói tin trên mạng, phân tích gói tin để tìm ra dấu hiệu tấn công, nếu gói tin có dấu hiệu bị tấn công, Sensor thiết lập tức là đánh dấu nó là sự kiện và gửi báo cáo lại cho Engine, Engine ghi lại tất cả các báo cáo của tất cả các Sensor , lưu các báo cáo trong cơ sở dữ liệu của nó và quyết định mức độ sẽ đi. cảnh báo cho sự kiện đã nhận. Console có nhiệm vụ giám sát, cảnh báo và điều khiển hoạt động của các Cảm biến.

Đối với hệ thống IDS truyền thống, các cảm biến hoạt động theo cơ chế "so sánh mẫu", các cảm biến bắt các gói tin trên mạng, đọc nội dung gói tin và so sánh các chuỗi trong nội dung gói tin với hệ thống mẫu tín hiệu xác định các cuộc tấn công hoặc mã độc để hệ thống, nếu trong nội dung gói có một chuỗi khớp với mẫu, Bộ cảm biến sẽ đánh dấu nó là một sự kiện hoặc có dấu hiệu của một cuộc tấn công và tạo ra một cảnh. báo chí. Các tín hiệu xác định các cuộc tấn công được tổng hợp và tập hợp lại thành một tập hợp được gọi là các chữ ký. Thông thường, các mẫu này được hình thành dựa trên kinh nghiệm ngăn chặn các cuộc tấn công, các trung tâm nghiên cứu được thành lập và các mẫu này được phát hành để cung cấp cho các hệ thống IDS trên khắp thế giới.



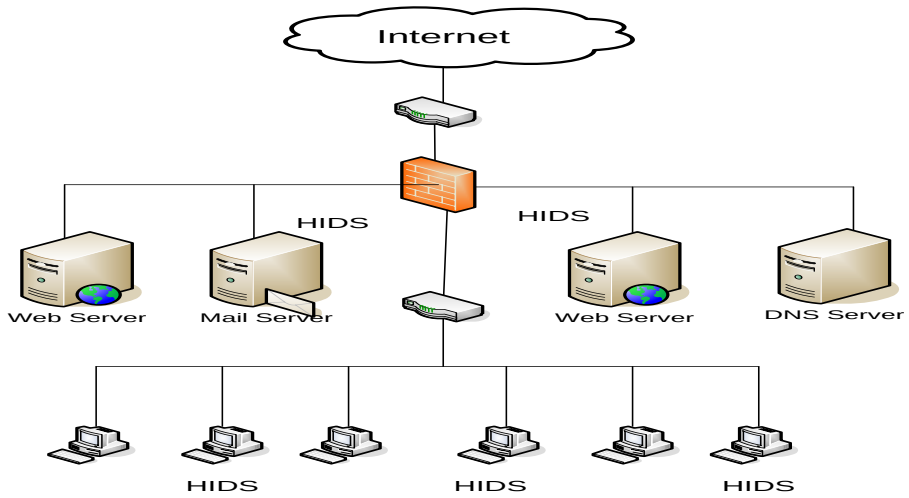
Hình 2.3: Hoạt động của IDS

2.1.4 Phân loại IDS

Về đối tượng giám sát, có hai loại IDS cơ bản nhất: IDS dựa trên máy chủ và IDS dựa trên mạng. Mỗi loại có một cách tiếp cận khác nhau để giám sát và phát hiện xâm nhập, đồng thời cũng có những ưu nhược điểm riêng. Nói tóm lại, IDS dựa trên máy chủ giám sát dữ liệu trên các máy tính riêng lẻ trong khi IDS dựa trên mạng giám sát lưu lượng của một mạng.

2.1.4.1 Host Base IDS (HIDS)

Hệ thống Host-based là loại IDS đầu tiên được nghiên cứu và triển khai. Bằng cách cài đặt phần mềm IDS trên các máy trạm (được gọi là Agent), HIDS có thể giám sát tất cả các hoạt động của hệ thống, các tệp nhật ký và lưu lượng mạng đi đến mỗi trạm.



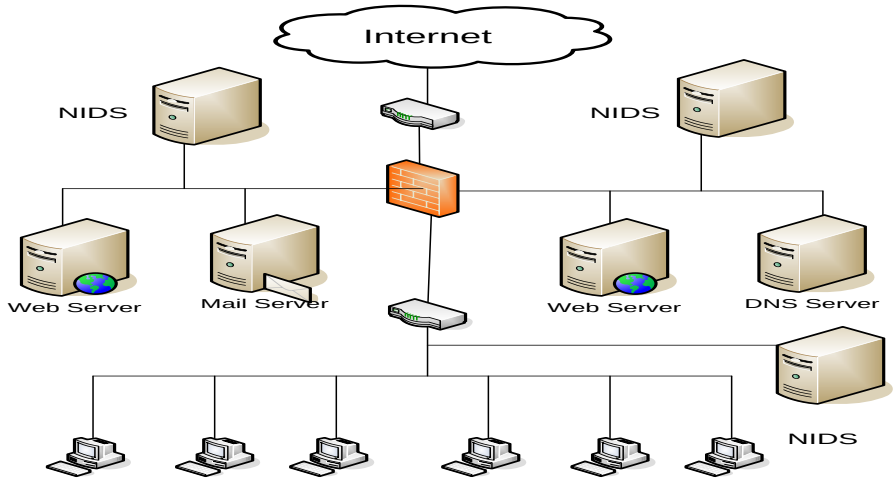
Hình 2.4: Mô hình mạng HIDS

2.1.4.2 Netwwork Base IDS (NIDS)

NIDS là giải pháp xác định truy cập trái phép bằng cách kiểm tra các luồng thông tin trên mạng và giám sát nhiều máy trạm, NIDS truy cập luồng thông tin trên mạng bằng cách kết nối với các Hub và Switch để bắt các gói tin. , phân tích nội dung gói tin và đưa ra cảnh báo.

Trong hệ thống NIDS, các cảm biến được đặt tại các điểm quan tâm trong mạng, thường ở phía trước DMZ hoặc ở rìa của mạng, các cảm biến thu nhận tất cả các gói

truyền đi trên mạng và phân tích nội dung của mạng. gói từng gói để phát hiện các chữ ký tấn công trong mạng.



Hình 2.5: Mô hình mạng NIDS

Bảng 2.1: So sánh HIDS và NIDS

So sánh HIDS và NIDS		
Nội dung	**HIDS**	**NIDS**
Quản trị	Phân tán trên từng máy trạm	Tập trung
Cài đặt	Dễ cài đặt	Khó cài đặt
Tính bao quát	Thấp, do mỗi máy trạm chỉ nhận được traffice của máy đó	Cao, do có cái nhìn toàn diện về traffic mạng
Phụ thuộc	Phụ thuộc hệ điều hành trên từng máy	Không phụ thuộc hệ điều hành máy trạm
Băng thông	Không ảnh hưởng	Có ảnh hưởng đến băng thông do thực hiện phân tích trên luồng mạng
Mã hóa	Có thể phân tích được dữ liệu đã mã hóa	Không phân tích được dữ liệu đã mã hóa
Báo động giả	Khó xảy ra	Có thể xảy ra

2.1.5 Các ứng dụng phổ biến hiện nay của IDS

Việc sử dụng IDS sẽ góp phần tăng cường quyền lực của người quản trị và cảnh báo kịp thời mọi diễn biến bất thường trên hệ thống mạng. Cụ thể, IDS có thể cảnh báo chúng ta về các hành động sau:

Tấn công từ chối dịch vụ: (DoS) có mục đích đóng băng hoặc khóa tài nguyên hệ thống mục tiêu. Cuối cùng thì mục tiêu không thể tiếp cận và phản hồi các gói tin đến. Các cuộc tấn công DoS vào các mục tiêu bao gồm ba loại: mạng, hệ thống và ứng dụng. NIDS có thể phát hiện các cuộc tấn công gói:

Quét và thăm dò (Scanning and Probe): Máy quét và thăm dò tự động sẽ tìm kiếm hệ thống trên mạng để xác định các điểm yếu. Việc dò tìm có thể được thực hiện bằng cách ping hệ thống cũng như kiểm tra các cổng TCP hoặc UDP để phát hiện các ứng dụng có lỗi đã biết. Phát hiện các hành động nguy hiểm trước khi chúng xảy ra. Host IDS cũng có hiệu quả chống lại kiểu tấn công này.

Tấn công bằng mật khẩu: Một IDS mạng có thể phát hiện và ngăn chặn các nỗ lực đoán mật khẩu, nhưng nó không hiệu quả trong việc phát hiện truy cập trái phép vào các tệp được mã hóa. Trong khi đó, Host IDS có hiệu quả trong việc phát hiện đoán mật khẩu cũng như truy cập trái phép.

Giành đặc quyền: Một khi kẻ tấn công đã xâm nhập vào hệ thống, chúng sẽ cố gắng chiếm quyền truy cập. Khi thành công, họ sẽ tìm cách phá hoại hệ thống hoặc đánh cắp thông tin quan trọng. Cả NIDS và HIDS đều có thể xác định các thay đổi đặc quyền.

Phá hoại mạng: Phá hoại bao gồm: thay đổi trang web, xóa tệp, phá hủy khối khởi động và chương trình hệ điều hành, định dạng ổ đĩa, sử dụng HIDS trong trường hợp này. hoàn toàn phù hợp. Với NIDS, có thể sử dụng các chữ ký tấn công được xác định trước để phát hiện chính xác các truy cập trái phép vào hệ điều hành.

Tấn công cơ sở hạ tầng bảo mật: Có nhiều kiểu tấn công can thiệp vào quyền kiểm soát cơ bản của cơ sở hạ tầng bảo mật, chẳng hạn như tạo tường lửa trái phép, sửa đổi tài khoản người dùng hoặc thay đổi cài đặt khác, quyền đối với tệp. Các cuộc tấn công

vào cơ sở hạ tầng cho phép kẻ xâm nhập có thêm quyền truy cập hoặc tạo ra nhiều con đường xâm nhập vào hệ thống.

2.2 Nghiên cứu các loại IDS phổ biến hiện nay

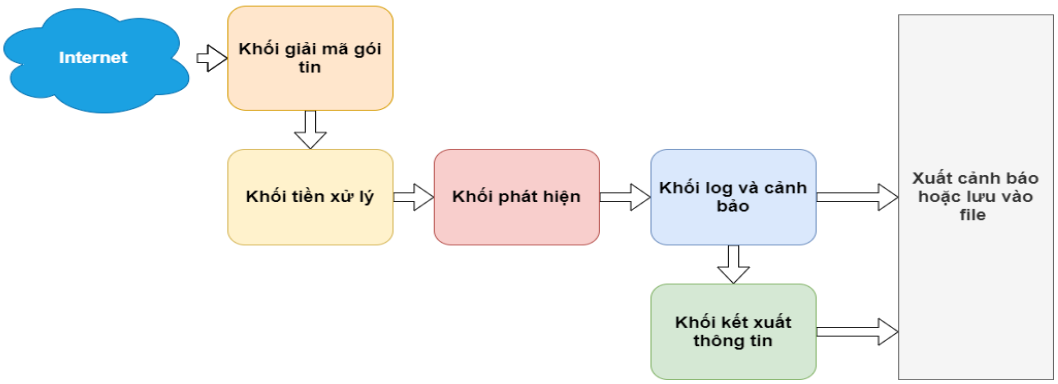
2.2.1 Snort

Snort là một NIDS do Martin Roesh phát triển theo mô hình mã nguồn mở. Mặc dù Snort là IDS miễn phí nhưng nó có rất nhiều tính năng tuyệt vời. Nó được xây dựng để phát hiện và ngăn chặn xâm nhập. Được thiết kế trên một mô-đun để kiểm tra các gói đến và đi bằng cách tạo ra các quy tắc để phát hiện các gói bất thường. Snort có thể chạy trên nhiều nền tảng như Linux, Windows, OpenBSD, NetBSD, FreeBSD, MacOS ,Solaris. Snort hỗ trợ các giao thức sau: Ethernet, Cisco HDLC, SLIP, 8021, HP-UX, AIX, IRIX, Token Ring, FDDI, PPP và PF của OpenBSD.

2.2.2 Kiến trúc Snort

Kiến trúc Snort gồm nhiều thành phần, với mỗi 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)



Hình 2.6: Kiến trúc của Snort

Khi Snort hoạt động, nó sẽ lắng nghe và nắm bắt tất cả các gói tin đi qua nó. Các gói đã bắt được sẽ được gửi đến Mô-đun giải mã gói. Sau đó, gói tin được đưa vào mô-đun Tiền xử lý và sau đó là mô-đun Phát hiện. Ở đây, tùy thuộc vào việc có phát hiện ra sự xâm nhập hay không, gói tin có thể được bỏ qua để tiếp tục lưu lượng hoặc được nhập vào mô-đun Nhật ký và Cảnh báo để xử lý. Sau khi các cảnh báo được xác định, mô-đun Đầu ra Thông tin sẽ thực hiện việc xuất các cảnh báo ở định dạng mong muốn. Sau đây, chúng ta sẽ đi tìm hiểu chi tiết hơn về cơ chế hoạt động và chức năng của từng thành phần.

2.2.3 Suricata

Suricata là một hệ thống phát hiện xâm nhập mã nguồn mở, được phát triển bởi Open Information Security Foundation (OISF).

Công cụ này không được phát triển để cạnh tranh hoặc thay thế những công cụ hiện có, nhưng nó sẽ mang lại những ý tưởng và công nghệ mới trong lĩnh vực an ninh mạng.

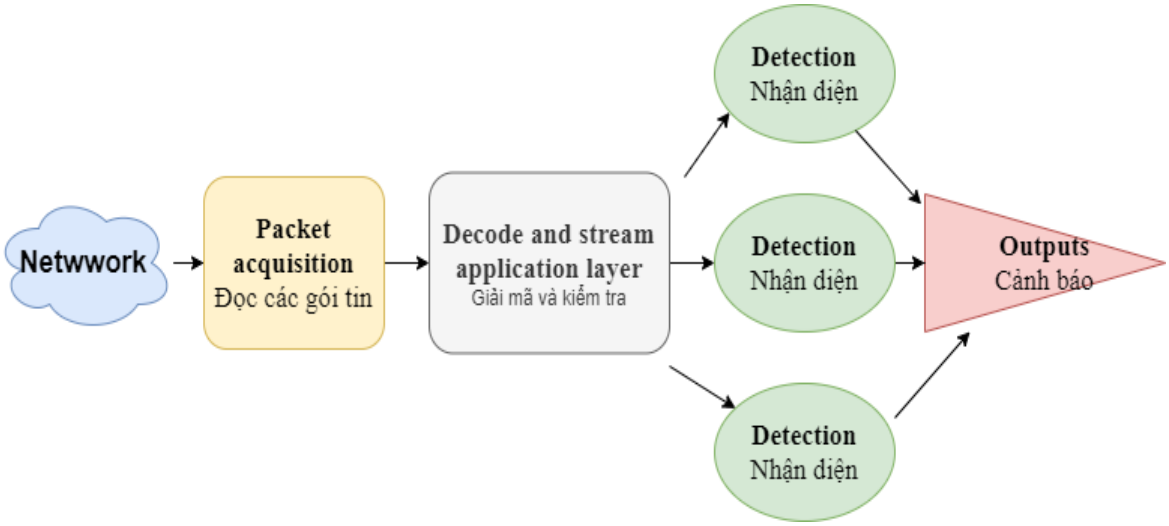
Suricata là công cụ phát hiện và ngăn chặn xâm nhập dựa trên quy tắc IDS / IPS (Hệ thống phát hiện xâm nhập / Hệ thống ngăn chặn xâm nhập) để giám sát lưu lượng mạng và đưa ra cảnh báo cho quản trị viên hệ thống khi xảy ra các sự kiện đáng ngờ. Ngoài ra, nó được thiết kế để tương thích với các thành phần an ninh mạng hiện có. Bản phát hành đầu tiên chạy trên nền tảng linux 2 với hỗ trợ nội tuyến và cấu hình giám sát lưu lượng thụ động có khả năng xử lý lưu lượng lên đến gigabit. Suricata là một công cụ IDS / IPS miễn phí trong khi vẫn cung cấp các tùy chọn có thể mở rộng cho các kiến trúc an ninh mạng phức tạp nhất.

Suricata tăng tốc độ và hiệu quả trong việc phân tích lưu lượng mạng nhờ hỗ trợ xử lý đa luồng. Ngoài việc tăng hiệu suất phần cứng (với phần cứng và card mạng hạn chế), công cụ này được xây dựng để tận dụng sức mạnh xử lý cao của các chip CPU đa lõi mới nhất.

2.2.4 Kiến trúc của Suricata

Suricata có 4 module luồng:

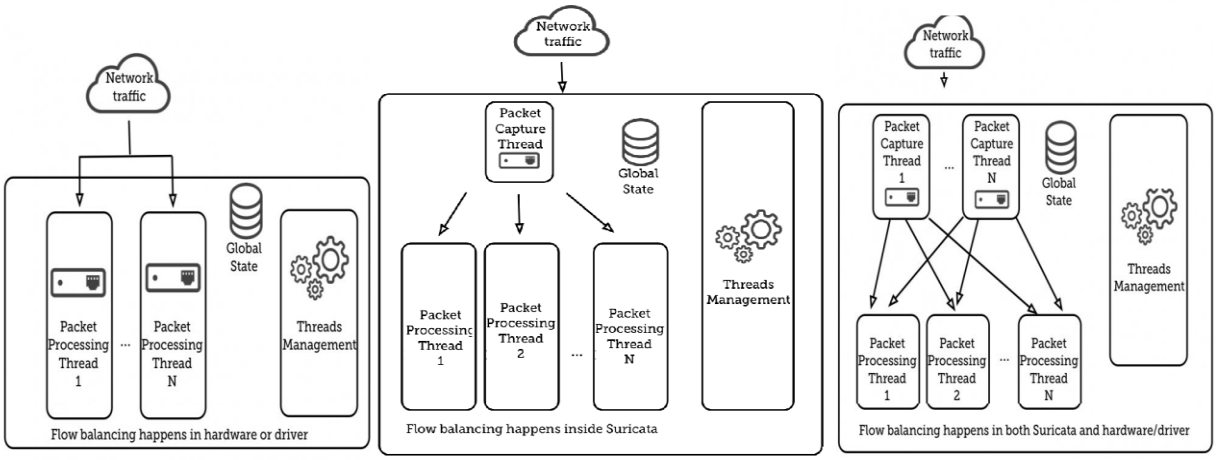
- **Packet acquisition**: chịu trách nhiệm đọc các gói tin từ mạng..
- **Decode and stream application layer**: giải mã các gói và kiểm tra ứng dụng.
- **Detection**: so sánh các chữ ký và có thể được chạy trong nhiều luồng.
- **Outputs**: trong mô-đun này, tất cả các báo động được xử lý.



Hình 2.7: Kiến trúc của Suricata

Các chế độ runmode của Suricata

- Worker**:** runmode hoạt động tốt nhất. Trong chế độ này, NIC / trình điều khiển đảm bảo các gói được cân bằng hợp lý qua các luồng xử lý của Suricata. Mỗi luồng xử lý gói sau đó chứa toàn bộ đường ống gói.
- Autofb (Single capture thread):
- Autofb (Multiple capture thread):
- Single: giống như Workers, tuy nhiên chỉ có một luồng xử lý gói duy nhất.



Hình 2.8: Các chế độ Runmode

2.2.5 Zeek

Zeek là một framework mã nguồn mở được sử dụng để phân tích và giám sát mạng. Nhiệm vụ chính là giám sát mạng dữ liệu mạng và cảnh báo, phát hiện tấn công. Zeek IDS thường được dùng để bảo vệ hạ tầng an ninh cho các trường đại học, trung tâm nghiên cứu, doanh nghiệp vừa và nhỏ…

Các tính năng của Zeek:

• Triển khai

Chạy trên các hệ thống kiểu UNIX (MacOS, FreeBSD, Linux…).

Phân tích thời gian thực hoặc ngoại tuyến.

Hỗ trợ cụm cluster, triển khai tốc độ cao, trên quy mô lớn.

Mã nguồn mở với giấy phéps BSD.

• Phân tích

Ghi log phục vụ cho việc phân tích.

Phân tích độc lập các giao thức tầng ứng dụng (DNS, FTP, HTTP, SSH, SSL, SMTP…)

Hỗ trợ IPv6 toàn diện.

Cảnh báo thời gian thực nếu xảy ra tấn công.

• Ngôn ngữ kịch bản

Ngôn ngữ hoàn chỉnh để phục vụ cho việc phân tích.

Mô hình lập trình dựa trên sự kiện.

Hỗ trợ mở rộng để theo dõi và quản lý trạng thái mạng theo thời gian.

• Giao diện

Bản ghi log có cấu trúc ASCII phù hợp.

Tích hợp để phân tích đầu vào thời gian thực.

Thư viện mở rộng C để trao đổi các sự kiện Zeek với các chương trình khác: Perl, Python, và Ruby…

Có khả năng gọi các tiến trình bên ngoài từ ngôn ngữ kịch bản.

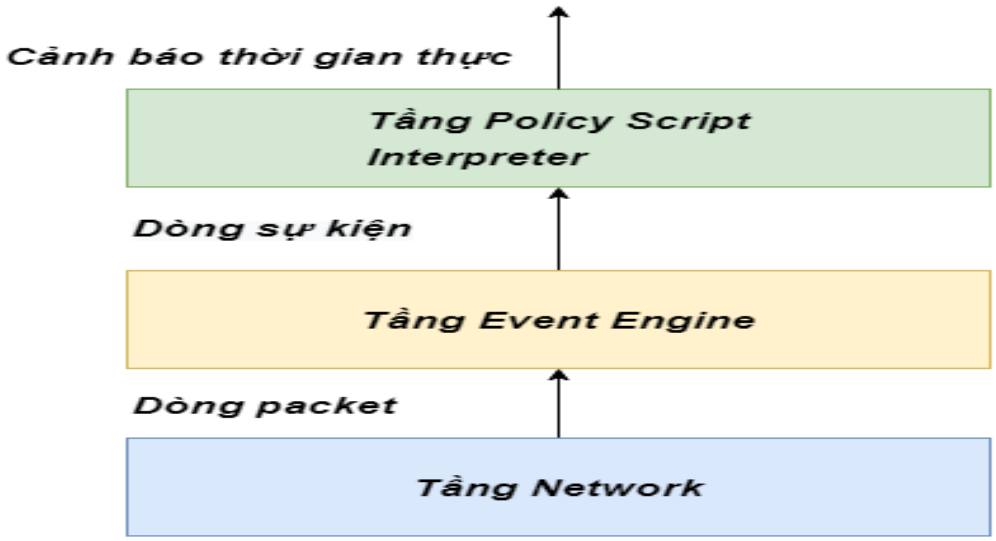
2.2.6 Kiến trúc của Zeek

Kiến trúc của Zeek IDS được chia thành các tầng. Về cơ bản, Zeek được chia thành các tầng sau:

• Tầng Network

• Tầng Event Engine

• Tầng Policy Script Interpreter



Hình 2.9: Kiến trúc của Zeek

Tầng Network

Là tầng thấp nhất trong các thành phần của Zeek, nơi tiếp nhận gói tin ra vào trong hệ thống mạng. Tầng này sử dụng libpcap, được sử dụng bởi công cụ phổ biến tcpdump, thư viện được sử dụng trên các hệ điều hành họ Unix.

Chức năng của libpcap:

• Cung cấp chức năng để bắt các gói tin, sử dụng để giám sát mạng cấp thấp.

• Nó giúp tách biệt Zeek các chi tiết của công nghệ network-link (Ethernet, FDDI, SLIP…), hỗ trợ port Zeek tới các biến thể Unix khác nhau (dễ dàng nâng cấp…)

• Nếu OS hỗ trợ các chức năng lọc gói tin mạnh mẽ ở kernel, như BPF thì libpcap sẽ giúp giảm thiểu lưu lượng vào trong kernel.

Các gói tin sau khi được lọc sẽ được chuyển lên tầng trên, Event Engine.

Tầng Event Engine

Tầng Event Engine nhận các gói tin đã được lọc, thực hiện kiểm tra tính toàn vẹn để đảm bảo rằng gói tin có cấu trúc phù hợp, bao gồm kiểm tra checksum của IP header. Nếu kiểm tra thất bại, Zeek sẽ tạo ra một cảnh báo tương ứng và loại bỏ gói tin. Zeek cũng tiến hành lắp ráp các mảnh gói tin lại với nhau thành các gói dữ liệu hoàn chỉnh trước khi tiến hành kiểm tra.

Sau khi kiểm tra thành công, nó tìm kiếm trạng thái kết nối liên kết với 2 địa chỉ IP và 2 port TCP hoặc UDP. Sau đó, nó gửi gói tin tới trình xử lý cho kết nối tương ứng. Zeek duy trì file tcpdump liên kết với lưu lượng mạng. Trình xử lý kết nối sẽ quyết định việc lưu lại toàn bộ gói tin, hoặc là header, hoặc không lưu gì cả.

Tùy thuộc vào gói tin TCP hay UDP để trình xử lý thực việc với payload của từng gói tin.

• TCP: Với mỗi gói tin TCP, trình xử lý kết nối (một hàm ảo C++) kiểm tra toàn bộ TCP header và xác thực TCP checksum qua header và payload. Nếu thành công, nó kiểm tra TCP header chứa cờ SYN/FIN/RST hay không, và sẽ điều chỉnh trạng thái kết nối tương ứng. Cuối cùng, nó gọi trình xử lý để thực hiện với payload.

• UDP: Tương tự như TCP nhưng đơn giản hơn, do nó không có trạng thái kết nối.

Tầng Policy Script Interpreter

Sau khi tầng Event Engine thực hiện xong việc xử lý một gói tin, nó kiểm tra liệu tiến trình trên có tạo ra bất kì sự kiện nào hay không (dựa vào hàng đợi FIFO). Nó sẽ xử lý lần lượt từng sự kiện cho đến khi hàng đợi trống.

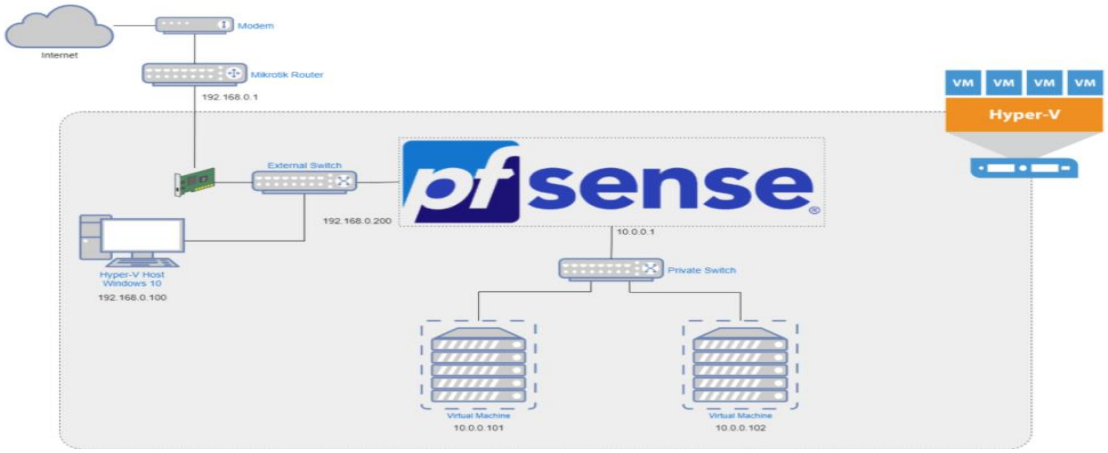
Policy Script Interpreter thực thi những đoạn script được viết bằng ngôn ngữ kịch bản Zeek. Với mỗi sự kiện được truyền vào bộ thông dịch, trước hết Zeek tìm ra trình xử lý sự kiện tương ứng với sự kiện đó (hay còn gọi là các event handler), lấy những thông tin trong sự kiện tạo ra và truyền vào các tham số tương ứng trong event handler và thông dịch ra code tương ứng. Những đoạn code này có thể thực thi các đoạn mã Zeek khác, bao gồm tạo ra một sự kiện mới, ghi log, tạo thông báo, ghi dữ liệu vào đĩa, hoặc chỉnh sửa trạng thái.

2.3 Các phần mềm mở tích hợp với các phần mềm IDS

2.3.1 Pfsense

Để bảo vệ cho hệ thống mạng bên trong thì chúng ta có giải pháp sử dụng thiết bị tường lửa cứng như PIX Firewall của Cisco…, hoặc dùng tưởng lửa mềm của Microsoft như ISA … Tuy nhiên những thành phần kể trên tương đối tốn kém. Vì vậy đối với người dùng không muốn tốn tiền nhưng lại muốn có một tường lửa bảo vệ hệ thống mạng bên trong (mạng nội bộ) khi mà chúng ta giao tiếp với hệ thống mạng bên ngoài (Internet) thì pfSense là một giải pháp tiết kiệm và hiệu quả tương đối tốt nhất đối với người dùng.

PfSense là một ứng dụng có chức năng định tuyến, tường lửa và miễn phí, ứng dụng này sẽ cho phép chúng ta mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Bắt đầu vào năm 2004, khi firewall mới bắt đầu chập chững – đây là một dự án bảo mật tập trung vào các hệ thống nhúng – pfSense đã có hơn 1 triệu lượt download và được sử dụng để bảo vệ các mạng có tất cả kích cỡ, từ mạng gia đình đến các mạng lớn của các công ty/doanh nghiệp. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi lần phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó.

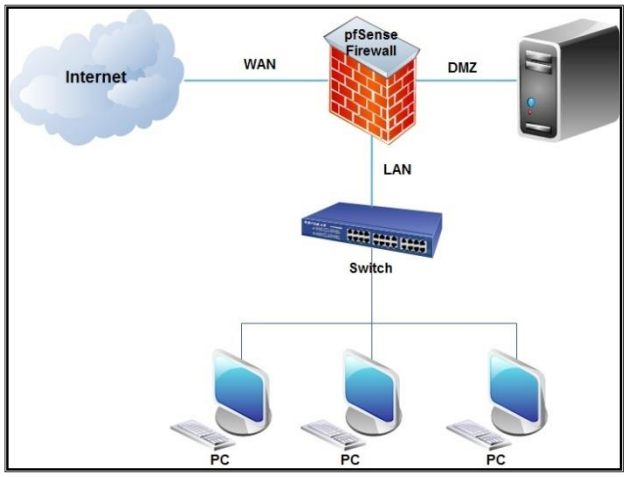


Hình 2.10: Vị trí của pfsense trong mạng doanh nghiệp

PfSense bao gồm nhiều tính năng mà chúng ta vẫn thấy trên các thiết bị tường lửa hoặc router thương mại, chẳng hạn như giao diện người dùng (GUI) trên nền Web tạo sự quản lý một cách dễ dàng. Trong khi đó phần mềm miễn phí này còn có nhiều tính năng ấn tượng đối với firewall/router miễn phí, tuy nhiên cũng có một số hạn chế.

PfSense hỗ trợ lọc bởi địa chỉ nguồn và địa chỉ đích, cổng nguồn hoặc cổng đích hay địa chỉ IP. Nó cũng hỗ trợ chính sách định tuyến và cơ chế hoạt động trong chế độ brigde hoặc transparent, cho phép chún ta chỉ cần đặt pfSense ở giữa các thiết bị mạng mà không cần đòi hỏi việc cấu hình bổ sung. PfSense cung cấp cơ chế NAT và tính năng chuyển tiếp cổng, tuy nhiên ứng dụng này vẫn còn một số hạn chế với Point-to-Point Tunneling Protocol (PPTP), Generic Routing Encapsulation (GRE) và Session Initiation Protocol (SIP) khi sử dụng NAT.

PfSense được dựa trên FreeBSD và giao thức Common Address Redundancy Protocol (CARP) của FreeBSD, cung cấp khả năng dự phòng bằng cách cho phép các quản trị viên nhóm hai hoặc nhiều tường lửa vào một nhóm tự động chuyển đổi dự phòng. Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải. Tuy nhiên có một hạn chế với nó ở chỗ chỉ có thể thực hiện cân bằng lưu lượng phân phối giữa hai kết nối WAN và không thể chỉ định được lưu lượng cho qua một kết nối.



Hình 2.11: Mô hình triển khai pfSense cho doanh nghiệp nhỏ

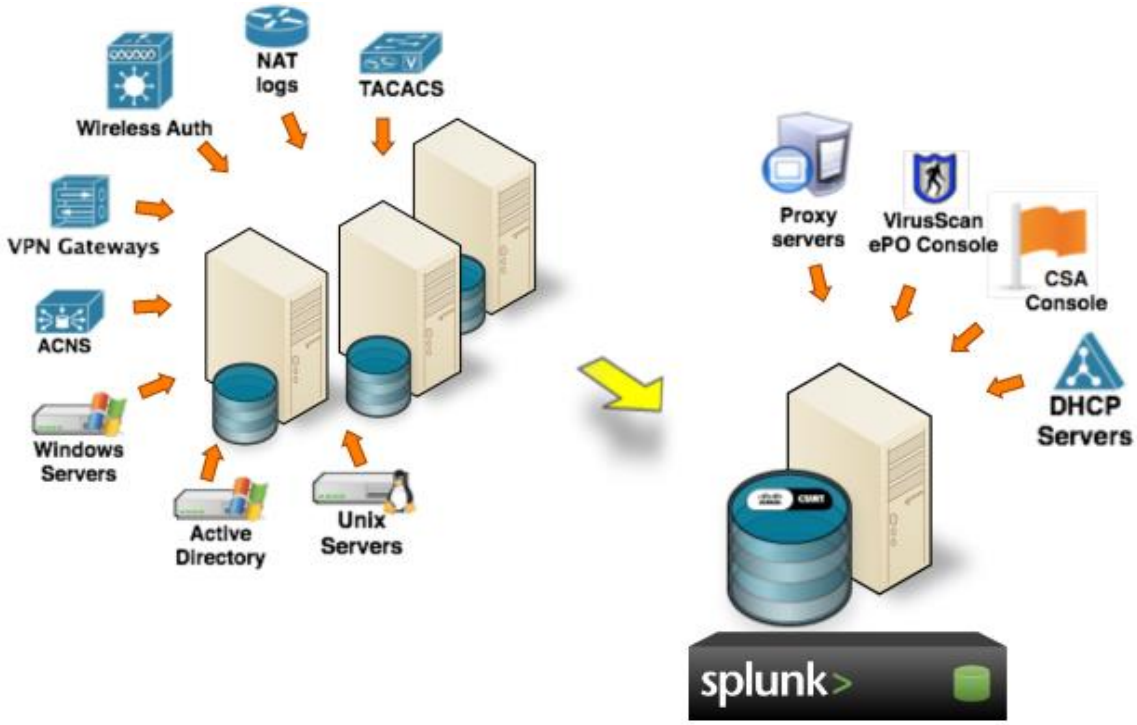
2.3.2 Splunk

Splunk là phần mềm cho phép CNTT có thể tìm kiếm và duyệt logs và các dữ liệu IT trong thời gian thực. Người dùng có thể ngay lập tức phát hiện ra sự cố ở bất cứ ứng dụng nào, hoặc ở các máy chủ và thiết bị; cảnh báo các nguy cơ tiềm ẩn và báo cáo các hoạt động của các dịch vụ và thành phần khác nhau trong mạng. Và đây cũng là giải pháp troubleshoot cho hệ thống.

Splunk là một công cụ dữ liệu rất linh hoạt và khả năng mở rộng cho các dữ liệu máy tính được tạo ra bởi cơ sở hạ tầng CNTT của CNTT. Nó thu thập ,lập chỉ mục và khai thác những dữ liệu được tạo ra từ bất cứ nguồn nào , định dạng hoặc vị trí bao gồm cả đóng gói và các ứng dụng tùy chỉnh , máy chủ ứng dụng , máy chủ web , cơ sở dữ liệu , mạng , máy ảo, hypervisors, hệ điều hành và nhiều hơn nữa mà không cần phải phân tích cú pháp tùy chỉnh , bộ điều hợp hoặc một cơ sở dữ liệu trên các phụ trợ .

Splunk được sử dụng để cung cấp một cái nhìn rõ ràng, chi tiết về toàn bộ hệ thống công nghệ thông tin. Nó liên kết các dữ liệu riêng biệt của các thiết bị, ứng dụng riêng biệt lại với nhau một cách tự động, giúp quá trình tìm kiếm điều tra trở nên nhanh chóng, đơn giản đi rất nhiều.

Chủ động giám sát các dữ liệu để phát hiện các bất thường theo thời gian thực. Cho phép người dùng ngay lập tức đi sâu chi tiết vào vấn đề gặp phải để có hướng giải quyết một cách chính xác và nhanh chóng nhất.



Hình 2.12: Splunk

2.4 Một số phần mềm, công cụ tấn công mạng

2.4.1 WireShark

WireSharklà một công cụ phân tích giao thức. Công cụ này cho phép kiểm tra các sự kiện trong mạng bằng cách thực hiện chặn bắt các gói tin và phân tích trực tiếp. Nó cho phép phân tích các gói tin ở mức độ rất chi tiết. Wireshark có thể hoạt động trên nhiều phiên bản hệ điều hành khác nhau như: Windows, Linux, OS X, Solaries, FreeBSD... Việc sử dụng WireShark yêu cầu phải có những hiểu biết và kiến thức chuyên môn về mạng và giao thức mạng khá tốt. Đây là một công cụ giành cho các chuyên gia phân tích mạng.

2.4.2 Nmap

Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành.

Mặc dù Nmap đã không ngừng được phát triển, cải tiến qua nhiều năm và cực kỳ linh hoạt, nhưng nền tảng của nó vẫn là một công cụ quét cổng, thu thập thông tin bằng cách gửi các gói dữ liệu thô đến các cổng hệ thống. Sau đó nó lắng nghe và phân tích các phản hồi và xác định xem các cổng đó được mở, đóng hoặc lọc theo một cách nào đó, ví dụ như tường lửa. Các thuật ngữ khác được sử dụng để chỉ hoạt động quét cổng (port scanning) bao gồm dò tìm cổng (discovery) hoặc liệt kê cổng (enumeration).

2.4.3 Hydra

Hydra là một trình bẻ khóa đăng nhập song song hỗ trợ nhiều giao thức để tấn công. Nó rất nhanh và linh hoạt, và dễ dàng thêm các mô-đun mới. Công cụ này giúp các nhà nghiên cứu và nhà tư vấn bảo mật có thể chỉ ra việc truy cập trái phép vào hệ thống từ xa dễ dàng như thế nào.

Nó hỗ trợ: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP (S) -FORM-GET, HTTP (S) -FORM-POST, HTTP (S) -GET, HTTP (S) -HEAD, HTTP- Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB (NT) , SMTP, SMTP Enum, SNMP v1 + v2 + v3, SOCKS5, SSH (v1 và v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC và XMPP.

2.5 Kết luận chương

Trong chương này, tác giải đã nghiên cứu tìm hiểu khái quát hệ thống IDS: khái niệm, chức năng, các loại , các công cụ tấn công mạng.

Tìm hiểu và cách thức hoạt động của các loại IDS phổ biến như: Snort, Suricata, Zeek, các loại kiến trúc của IDS. Từ đó tác giả có thể ứng dụng và xây dựng các hệ thống cho các chương tiếp theo và kiểm nghiệm các kịch bản tấn công bằng các công cụ đã nghiên cứu.

CHƯƠNG 3 - XÂY DỰNG HỆ THỐNG PHÂN TÍCH QUẢN LÝ MẠNG TÍCH HỢP MÃ NGUỒN MỞ TRIỂN KHAI VỚI CÁC CÔNG NGHỆ IDS KHÁC NHAU

3.1 Mục tiêu

- Xây dựng hệ thống phân tích quản lý mạng ứng dụng cho mạng doanh nghiệp vừa và nhỏ bằng cách tích hợp nhiều mã nguồn mở với một trong các loại IDS đã tìm hiểu (Snort, Suricata, Zeek).
- Đánh giá cũng như so sánh tính hiệu quả của 3 hệ thống giám sát mã nguồn mở. Mục tiêu xây dựng áp dụng cho các loại doanh nghiệp có quy mô khác nhau.
- Xây dựng được hệ thống phân tích quản lý mạng áp dụng được cho doanh nghiệp có quy mô vừa và nhỏ có quy mô hệ thống mạng đơn giản từ 1-2 vùng mạng.

3.2 Phương pháp

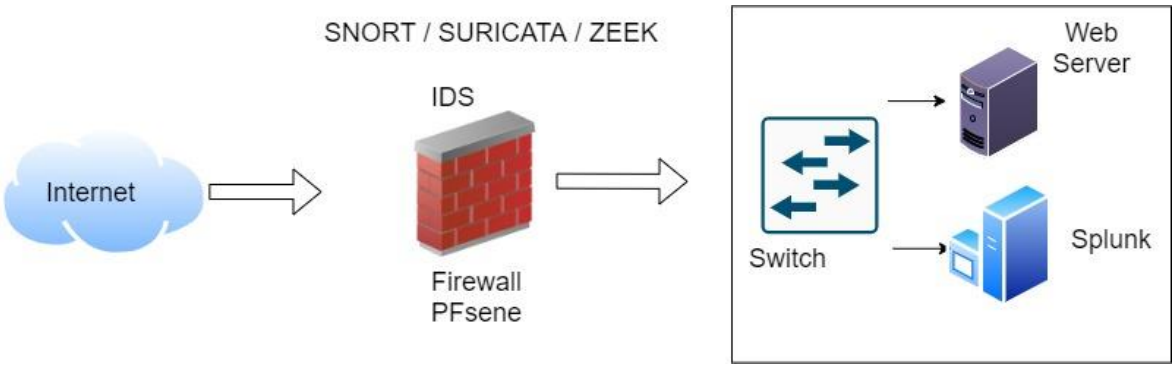
- Xây dựng từng hệ thống giám sát mạng mã nguồn mở trên hệ thống IDS: Snort, Suricata và Zeek, tích hợp các mã nguồn mở phân tích như: Splunk, pfSense...
- Các giải pháp kết hợp được tham khảo trên cộng đồng mã nguồn mở sao cho sự kết hợp mang lại hiểu quả nhất, trực quan nhất
- Sử dụng một bộ loại công cụ bổ trợ (pFsenne, Splunk..) để có thể so sánh hiệu quả của các loại IDS.

3.3 Mô hình triển khai

- Triển khai 3 hệ thống phân tích giám sát mạng mã nguồn mở là snort, suricata và zeek được phân vùng những vùng mạng quan trọng như hệ thống datacenter, hay các hệ thống máy chủ ở các chi nhánh huyện.
- Ba hệ thống được thiết kế trên cùng bộ phần cứng như nhau để cùng đánh giá đúng nhất.
- Môi trường thử nghiệm được tạo với các máy chủ ảo chạy trên phần mềm ảo hóa VMWare. Phần mềm VMWare cho phép chạy tất cả các máy chủ đang thử nghiệm trên cùng một máy và giảm bớt sự phức tạp của việc thiết lập thử nghiệm. VMWare

là một dự án mã nguồn mở và miễn phí để sử dụng cho mục đích cá nhân và giáo dục sử dụng.

- Môi trường thử nghiệm có ba máy chủ đích, nhiều máy con khác nhau, tất cả đều nằm trong cùng một hệ thống.
- Các thử nghiệm được chạy một lần và kết quả được ghi lại từ tất cả các máy IDS, do đó làm cho các thử nghiệm và kết quả có thể so sánh được mà không có khả năng xảy ra lỗi thử nghiệm giữa các giải pháp do môi trường trong tình huống thử nghiệm.



Hình 3.1: Mô hình mạng đưa vào thử nghiệm singgle- IDS

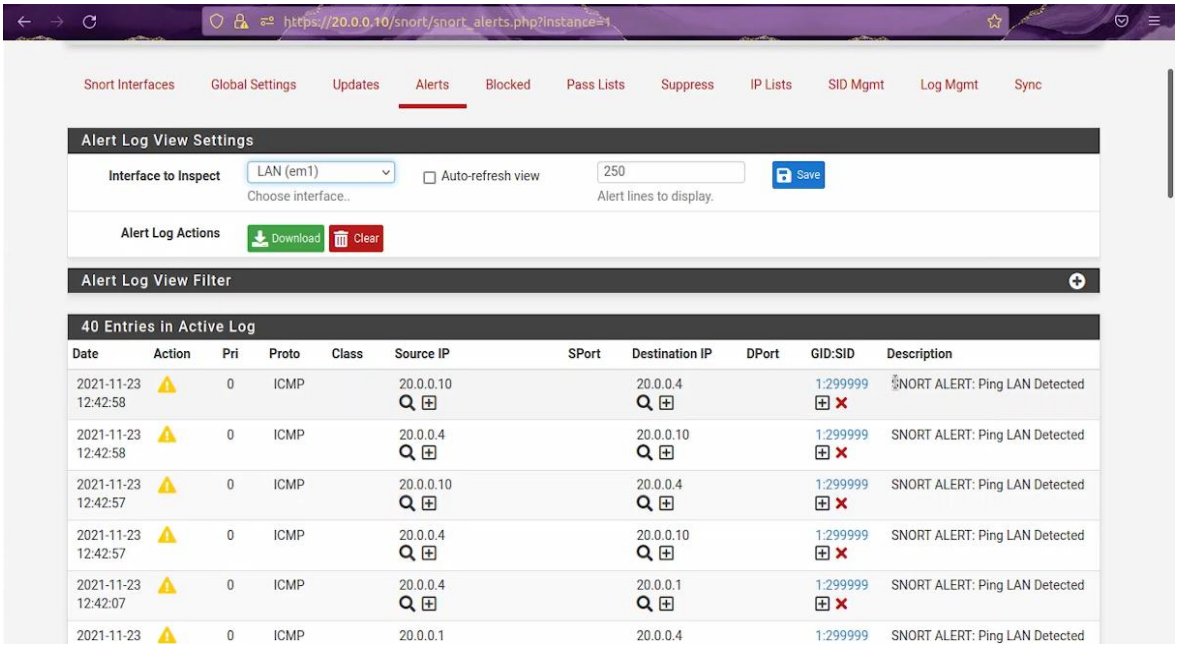
3.4 Thực nghiệm hệ thống IDS

3.4.1 Thực nghiệm hệ thống với Snort IDS

Để hệ thống phát hiện được tấn công từ các vùng mạng lên hệ thống Datacenter thì chúng ta sẽ cài Snort trên Pfsence để giám sát và lưu thông tin điều khiển,đưa ra cảnh báo…. Dưới đây là 4 kịch bản thực nghiệm với Snort - IDS.

Thực nghiệm tấn công Ping/Scan port

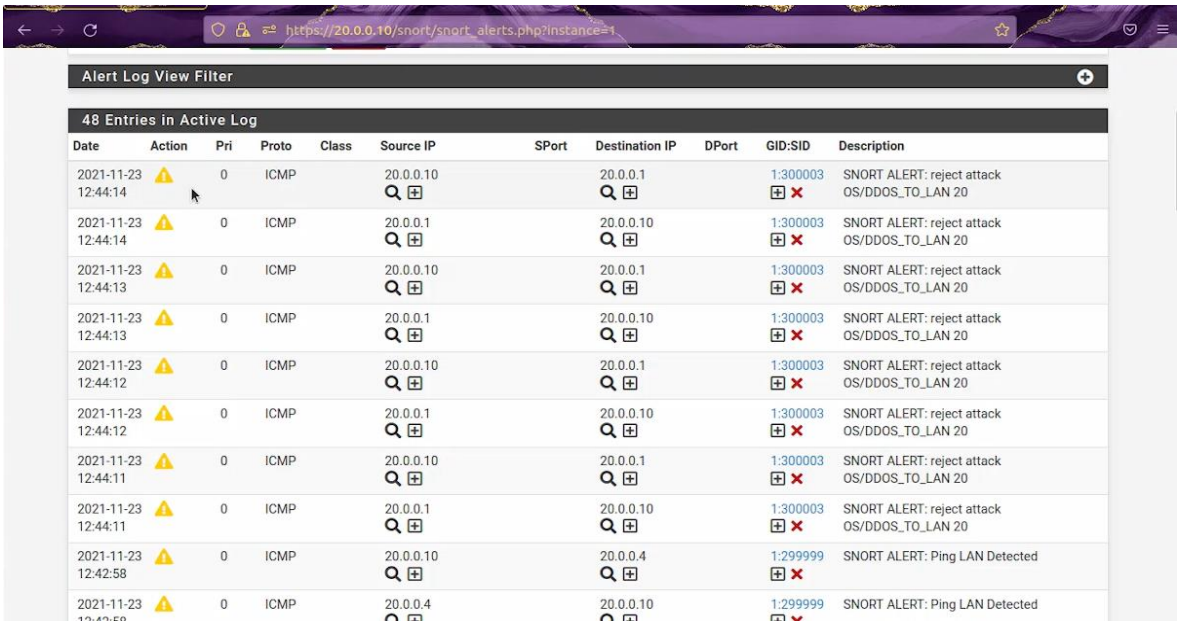
Thực hiện tấn công Scan port /Ping từ máy có địa chỉ 20.0.0.1/8 tấn công vào hệ thống máy chủ có IP là 20.0.0.4/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



Hình 3.2: Tấn công bằng Ping/Scan port

Thực nghiệm tấn công DOS

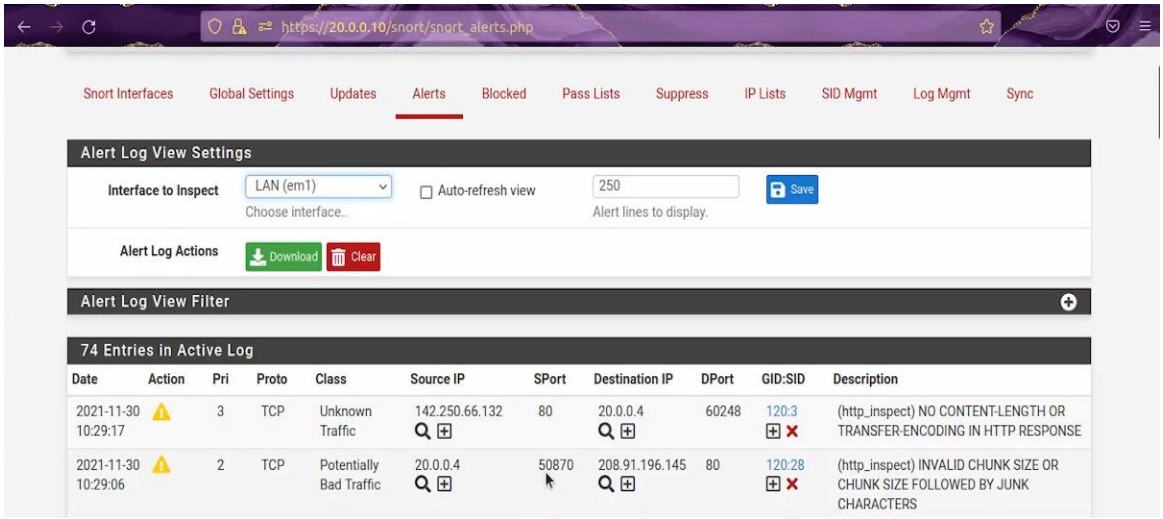
Thực hiện tấn công DOS từ máy có địa chỉ 20.0.0.1/8, 20.0.0.2/8, 20.0.0.3/8… tấn công vào hệ thống máy chủ có IP là 20.0.0.1/8, 20.0.0.2/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



Hình 3.3: Tấn công bằng DoS vào LAN

Thực nghiệm phát hiện virut khi sử dụng giao thức HTTP

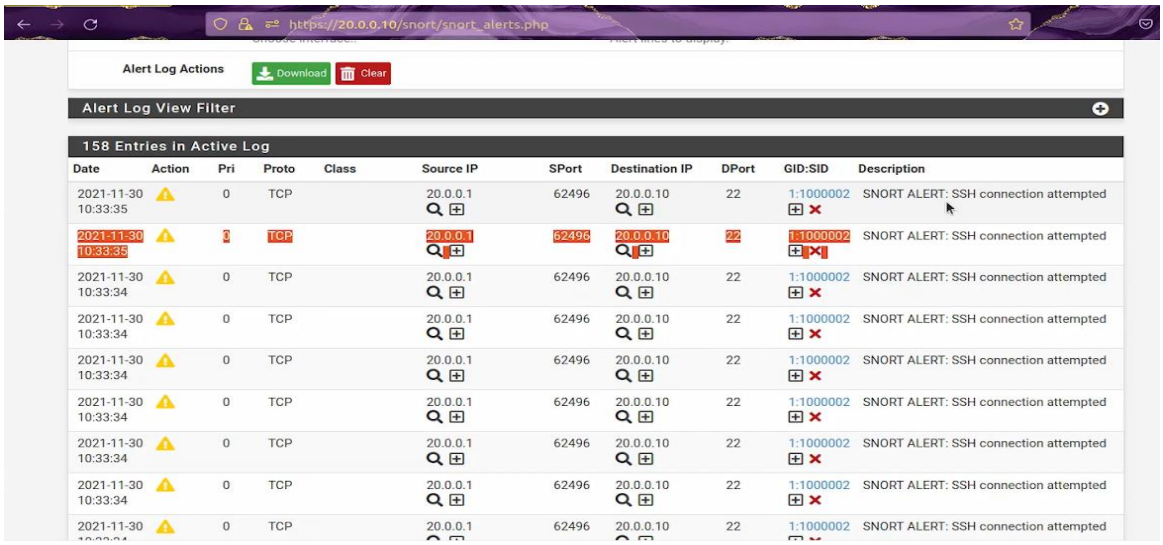
Thực hiện tấn công virut dựa trên giao thức HTTP từ máy có địa chỉ 20.0.0.1/8, 14250636/16… tấn công vào hệ thống máy chủ có IP là 20.0.0.2/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



Hình 3.4: Phát hiện virus trong khi sử dụng giao thức HTTP

Thực nghiệm tấn công SSH

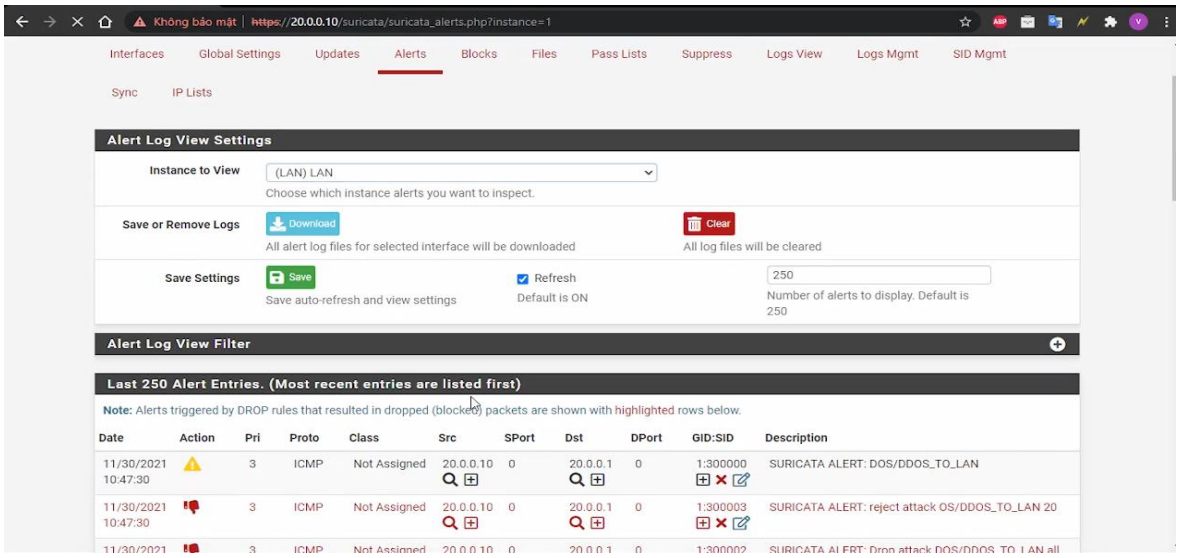
Thực hiện tấn công SSH từ máy có địa chỉ 20.0.0.1/8… tấn công vào hệ thống máy chủ có IP là 20.0.0.2/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



Hình 3.5: Phát hiện SSH connect

3.4.2 Thực nghiệm đánh giá trên Suricata

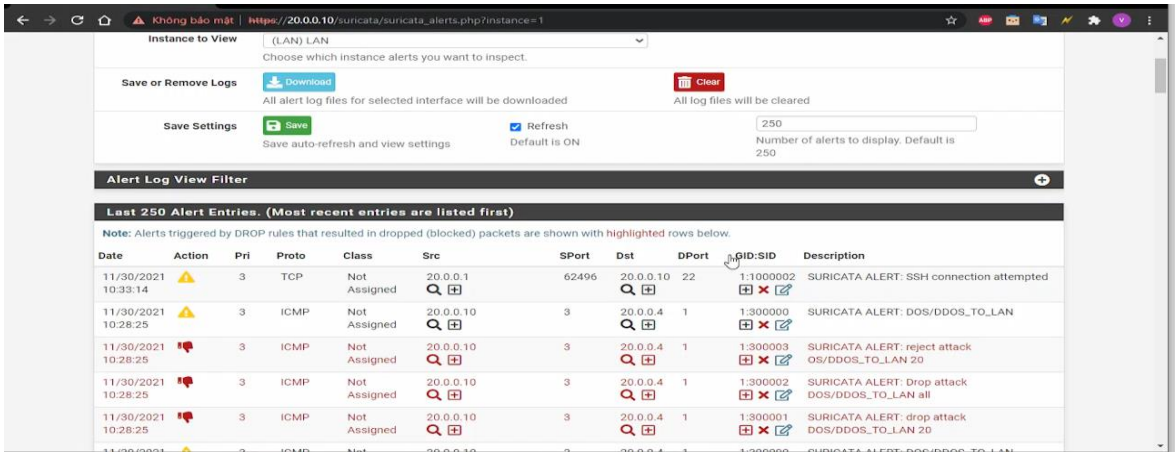
Để hệ thống phát hiện được tấn công từ các vùng mạng lên hệ thống Datacenter thì chúng ta sẽ cài Suricata trên Pfsence để giám sát và lưu thông tin điều khiển, đưa ra cảnh báo…. Dưới đây là 4 mô hình thực nghiệm với IDS – Suricata.



Hình 3.6: Thực hiện mở Spunk để giám sát Suricata

Thực nghiệm tấn công DOS

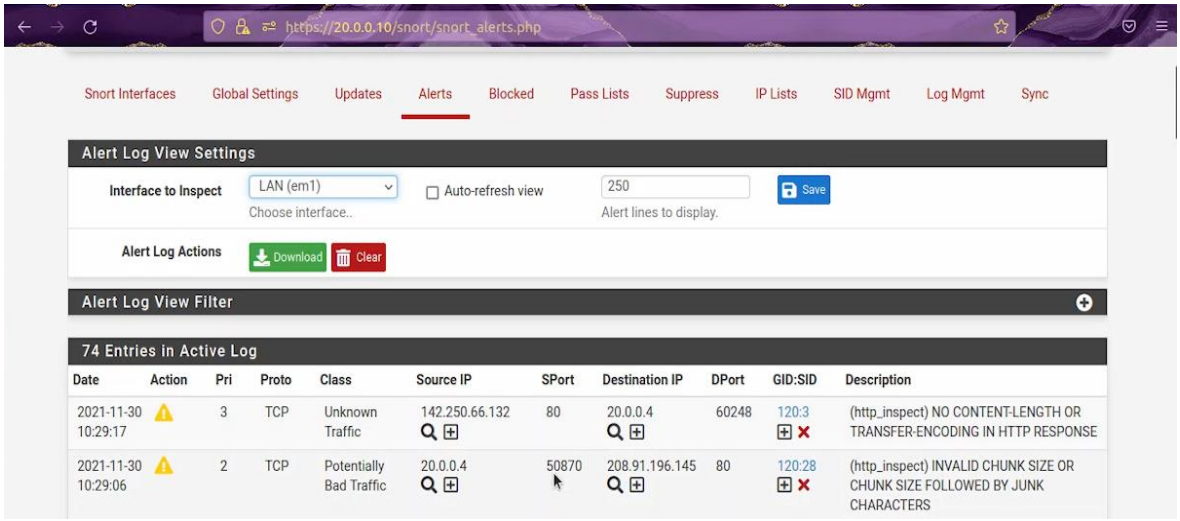
Thực hiện tấn công DOS từ máy có địa chỉ 20.0.0.1/8, 20.0.0.2/8… tấn công vào hệ thống máy chủ có IP là 20.0.0.1/8, 20.0.2/8. Sau khi tấn hệ thống Datacenter thì Suricata đã phát hiện và cảnh báo:



Hình 3.7: Phát hiện và ngăn chặn DoS lên LAN

Thực nghiệm phát hiện virut khi sử dụng giao thức HTTP

Thực hiện tấn công virut dựa trên giao thức HTTP từ máy có địa chỉ 20.0.0.1/8, 142.250.66.132 tấn công vào hệ thống máy chủ có IP là 20.0.0.2/8. Sau khi tấn hệ thống Datacenter thì Suricata đã phát hiện và cảnh báo.



Hình 3.8: Hiển thị trên virus lên hệ thống Suricata

3.4.3 Thực nghiệm đánh giá trên zeek

Để hệ thống phát hiện được tấn công từ các vùng mạng lên hệ thống Datacenter thì chúng ta sẽ cài Zeek trên Elastic stack để giám sát và lưu thông tin điều khiển,đưa ra cảnh báo…. Dưới đây là các mô hình thực nghiệm với IDS –Zeek.

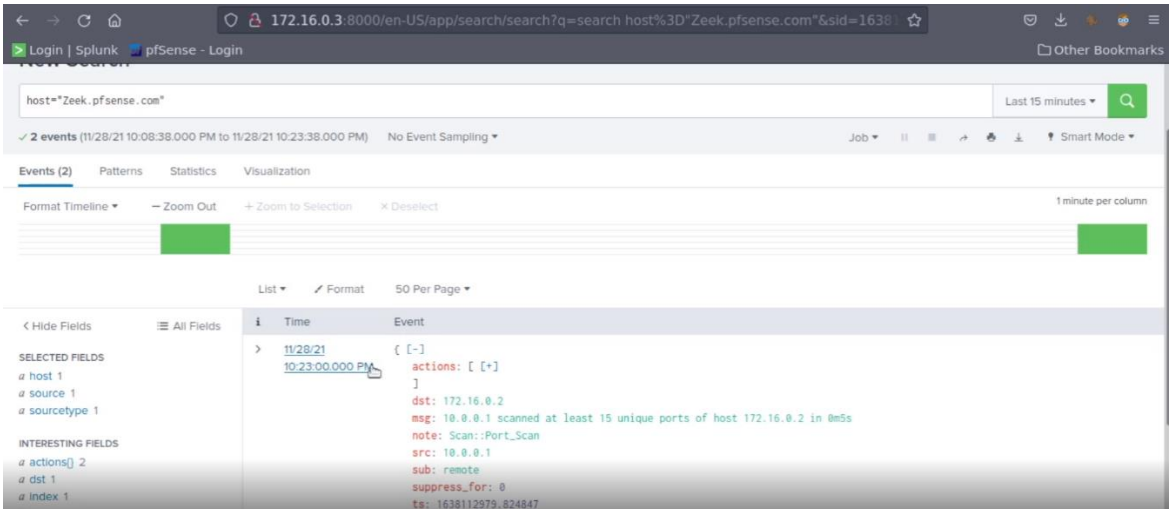
Thực nghiệm tấn công Ping/Scan port

Thực hiện tấn công Scan port /Ping từ máy có địa chỉ 172.16.0/8 tấn công vào hệ thống máy chủ. Sau khi tấn hệ thống Datacenter thì Zeek đã phát hiện và cảnh:

```
root@Inspiron-5459:/# nmap 172.16.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-08 00:36 +07
Nmap scan report for 172.16.0.2
Host is up (0.0043s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
9090/tcp open   zeus-admin
```

Hình 3.9: Thực nghiệm tấn công port scan đến mạng nội bộ mà zeek giám sát

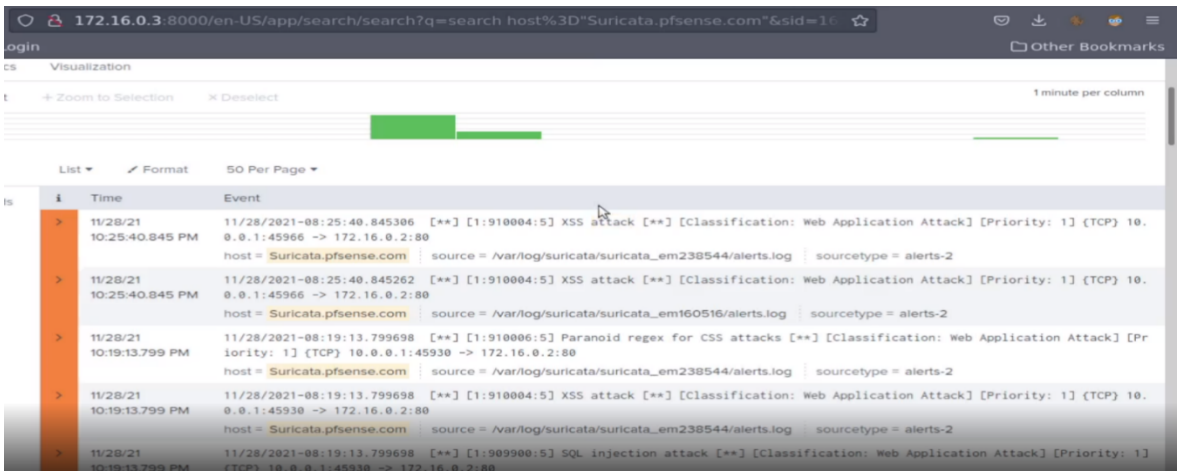
Hình 3.10: Các cảnh báo lưu tại file /usr/local/logs/current/notice.log



Hình 3.11: Phát hiện port scan trên vùng mạng

Thực nghiệm tấn công XSS

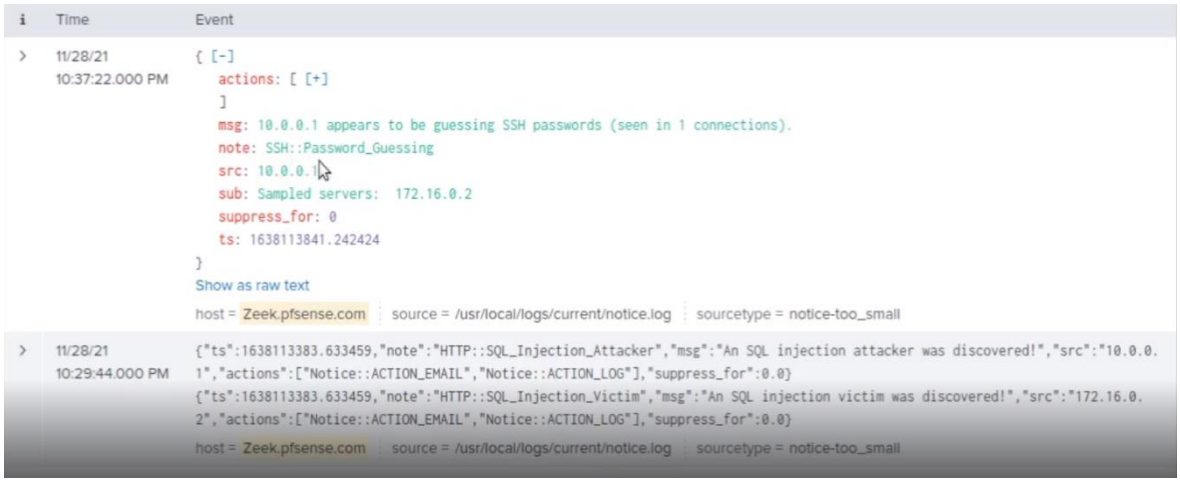
Thực hiện tấn công Scan port /Ping từ máy có địa chỉ 172.16.0/8 tấn công vào hệ thống máy chủ. Sau khi tấn hệ thống Datacenter thì Zeek đã phát hiện và cảnh:



Hình 3.12: Phát hiện XSS attack trên máy chủ We

Thực nghiệm tấn công SQL Injection

Thực hiện tấn công Scan port /Ping từ máy có địa chỉ 1726.0/8 tấn công vào hệ thống máy chủ. Sau khi tấn hệ thống Datacenter thì Zeek đã phát hiện và cảnh:



Hình 3.13: Phát hiện brute-force password trên máy chủ Web

3.5 Đánh giá thực nghiệm

Qua kết quả thực nhiệm của 3 hệ thống IDS (Snort, Suricata và zeek) chúng ta thụ được một số tiêu chí đánh giá như: tính đúng sai, nhận biết tấn công, thời gian xử lý và tiêu hao tài nguyên trên hệ thống IDS như sau:

a. Nhận biết được tấn công

- Suricata không nhận biết được ping hay là dos.
- Snort nhận biết được khi nào có ping, khi nào có dos.
- Snort nhận biết được website có chứa virus hoặc chứa nội dung không phải virus.
- Zeek nhận biết được có kết nối ssh từ xa thất bại trong trường hợp nhập sai tài khoản và mật khẩu. Snort và Suricata chỉ nhận biết được so kết nối SSH còn nhập đúng hay sai tài khoản/mật khẩu không phân biệt được.

b. Mức độ chính xác

Bảng 3.1: Mức độ chính xác

Loại hình tấn công/Hệ thống IDS	Suricata	Snort	Zeek

Thực hiện SSH	OK	OK	OK
Khai thác thông tin hệ thống			OK
DOS/DDOS	OK	OK	
Virus		OK	

c. Độ trễ

- Snort tốn nhiều thời gian để hiện thông báo (đối với ssh)
- Suricata tốn ít thời gian hơn (đối với ssh)
- Đối với DOS/DDOS Thì Suricata và Snort có thời gian phát hiện và chặn tấn công như nhau
- Zeek có mức độ xử lý chậm do phải xử lý một lượng lớn gói tin qua nó.

d. Tiêu hao tài nguyên:

So sánh trên số liệu trước khi tấn công và số liệu sau khi tấn công.

Bảng 3.2: Tiêu hao tài nguyên

Hệ thống IDS/Tiêu chuẩn so sánh	Suricata	Snort	ZEEK
CPU (1)	20-50	20-50	20-50
CPU (2)	30-60-70-100	20-50-60	30-60-70
RAM (1)	70	70	70
RAM (2)	70	70	70
Băng thông (1)	1k-3kB/s	1k-3kB/s	100-120kbps
Băng thông (2)	100-700kB/s	50-100kB/s	100-120kbps

3.6 Kết luận chương

Qua quá trình thực nghiệm, các hệ thống IDS đều có những ưu nhược điểm khác nhau, chi tiết như sau:

- Snort IDS có khả năng nhận biết nhanh các tấn công cơ bản SSH, DDOS, Virus, có độ trễ xử lý thấp cảnh báo thấp, có mức tiêu hao tài nguyên và lưu lượng mạng thấp. Tuy nhiên không có khả năng nhận biết các tấn công khai thác thông tin ở

lớp ứng dụng. Snort dễ sử dụng, có cộng đồng hỗ trợ lớn, có thể giúp quản trị viên áp dụng được ngay tại doanh nghiệp có quy mô vừa và nhỏ. Hệ thống quản lý, và cảnh báo bằng mail dễ cấu hình và sử dụng. Ở Tây Ninh Snort phù hợp với một số loại hình doanh nghiệp phù hợp: Trung tâm dạy học Anh Ngữ Việt Mỹ, các doanh nghiệp kinh doanh vận tải như nhà xe Đồng Phước,....

- Suricata IDS, tương tự như Snort, nó có đầy đủ các khả năng phát hiện tấn công, bảo vệ. Mặc khác, Suricata có hỗ trợ xử lý đa luồng, giúp xử lý hiệu quả đối với các hệ thống lớn hơn, xử lý nhanh hơn Snort. Tuy nhiên, qua thực nghiệm, Suricata vẫn có nhiều nhược điểm như chưa phân biệt được Ping hay Ddos, chưa hỗ trợ phát hiện và chặn khi client truy cập các địa chỉ web không tin cậy. Suricata phù hợp được xây dựng với các doanh nghiệp lớn, có hệ thống mạng phức tạp và hỗ trợ đa nhân, đa luồng, nhưng vẫn cần hỗ trợ các thành phần tường lửa, antivirus bên trong để có thể ngăn chặn được các xâm nhập. Suricata phù hợp với các doanh nghiệp quy mô tương đối như: Công ty TNHH Gain Lucky, SaiLun, Việt Nam Mộc Bài...

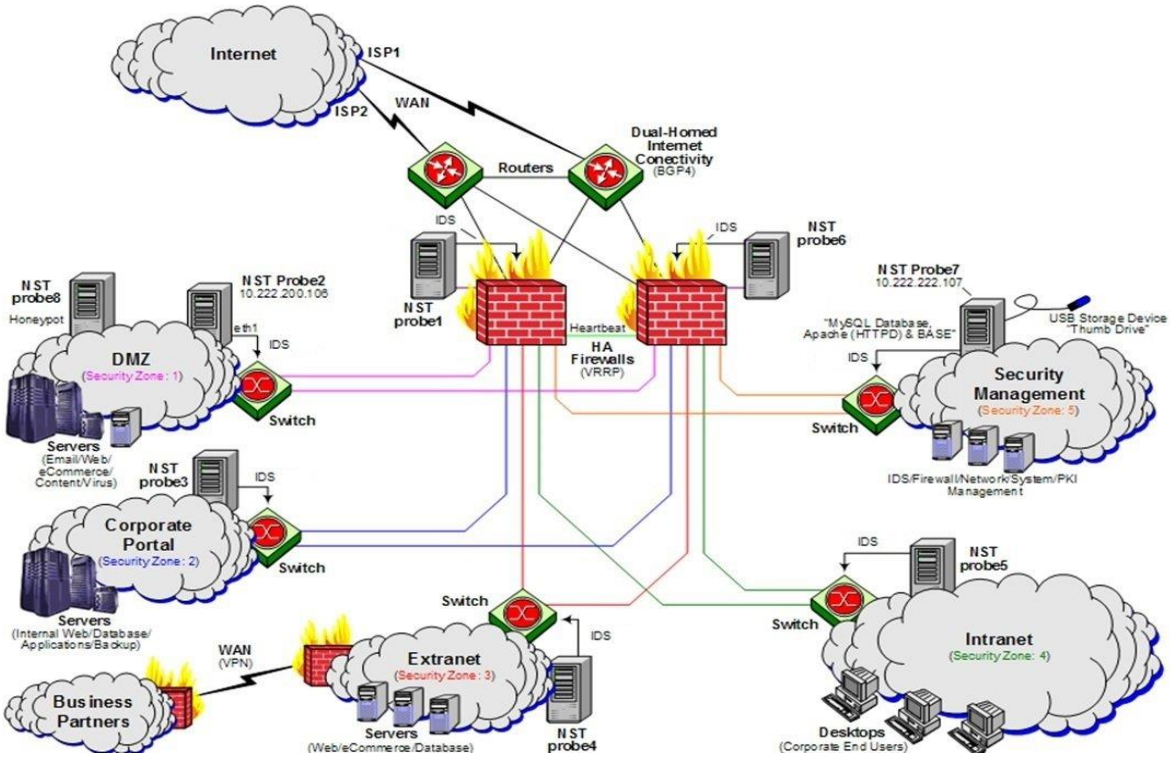
- Zeek IDS: hệ thống IDS có giao diện sử dụng là câu lệnh phức tạp, các quy tắc rule phức tạp, nếu sự dụng các rule đơn giản thì rất tiêu tốn thời gian để xử lý. Tuy nhiên ZEEK có thể giám sát chi tiết hệ thống mạng, có phát hiện tất cả những bất lượng của lưu lượng mạng. Khác với Snort và Suricata, Zeek hoạt động mạnh và hiệu quả ở tầng ứng dụng. Do đó Zeek có thể ứng dụng trong các hệ thống cần mức bảo mật cao hơn trong doanh nghiệp như Datacenter, vùng DMZ có bảo mật cao như Hệ thống FTP server, Camera server. Ứng dụng tại Tây Ninh cho các doanh nghiệp như: Các công ty tài chính, ngân hàng, Viettel,...Bên cạnh đó, rule của zeek có thể phát triển để phân tích mã đọc bằng cách tích hợp các script, vì vậy zeek có khả năng tùy biến và mở rộng cao hơn.

Tác giả nhận định mỗi loại IDS có những ưu điểm, nhược điểm khác nhau, tuy mỗi mô hình doanh nghiệp, quản trị viên có thể tham khảo và lựa chọn hệ thống phù hợp. Tuy nhiên đối với các mô hình doanh nghiệp lớn, có nhiều vùng mạng cần phải đánh giá và có những kết hợp để có thể xây được hệ thống bảo vệ toàn diện.

CHƯƠNG 4 - XÂY DỰNG HỆ THỐNG PHÂN TÍCH QUẢN LÝ MẠNG ĐA LỚP VỚI NHIỀU CÔNG NGHỆ IDS MÃ NGUỒN MỞ ỨNG DỤNG TẠI VIETTEL TÂY NINH

4.1 Đặc tả hệ thống mạng doanh nghiệp cỡ lớn

Đối với hệ thống mạng cỡ lớn có nhiều phân vùng mạng phức tạp, việc xây dựng hệ thống Singgle IDS chưa bảo vệ toàn diện cho doanh nghiệp như các đánh giá, phân tích ở chương 3. Đặc biệt đối với các doanh nghiệp có quy mô lớn, nhiều nguy cơ bị tấn công, như từ bên trong, từ bên ngoài.



Hình 4.1: Mô hình mạng doanh nghiệp lớn

Phân vùng mạng là một trong những phương pháp quản lý an toàn thông tin. Việc phân vùng có thể áp dụng phân tách vật lý hay luận lý.

- Phân tách vật lý là phân tách theo vị trí, khu vực vật lý nhất định.

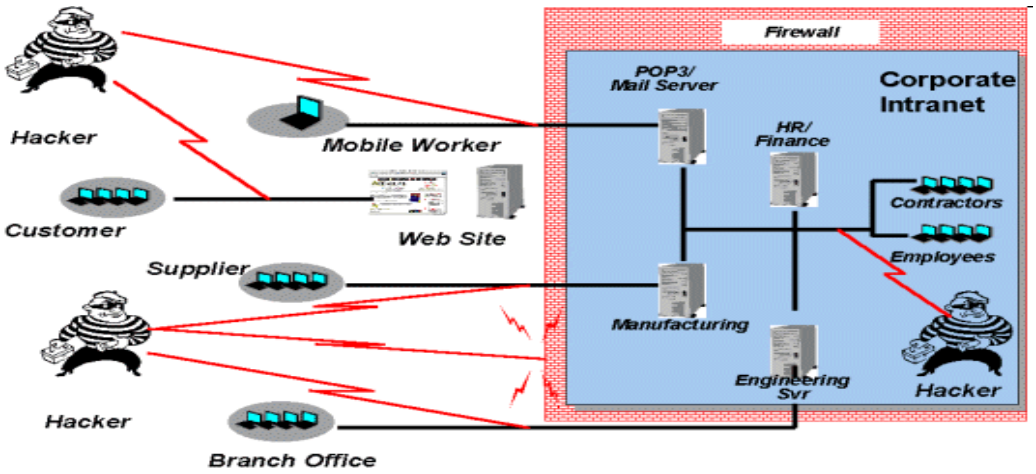
- Phân tách luận lý là phân chia thành các phân đoạn mạng như VLAN, mỗi VLAN được đặt một địa chỉ mạng khác nhau, từ đó, các chính sách truy cập cho mỗi VLAN cũng khác nhau.

Các phân vùng mạng thông thường trong một tổ chức/doanh nghiệp:

- Mạng nội bộ Intranet
- Mạng ngoài Extranet
- Mạng Demilitarized Zone (DMZ)
- Mạng riêng ảo Virtual private networks – VPN
- Mạng không dây trong tổ chức/doanh nghiệp

Khi áp dụng việc vùng mạng, phạm vi của truy cập của mỗi vùng mạng cần được xác đinh rõ. Truy cập giữa các vùng có thể được cho phép nhưng cần được kiểm soát chặt chẽ thông qua các gateway (firewall, router có chức năng filtering). Các tiêu chí cho việc phân tách mạng thành các vùng, và việc truy cập giữa các vùng cần dựa trên đánh giá bảo mật của mỗi vùng.

Dữ liệu của tổ chức/doanh nghiệp được truy xuất bởi các nhân viên bên trong mạng cục bộ, còn có thể được truy xuất bởi các chi nhánh, đại lý, nhân viên từ nhà riêng hoặc đang đi công tác xa, khách hàng, nhà cung cấp... dẫn đến các Hacker có thể tấn công vào các kết nối này.



Hình 4.2: Các nguy cơ tấn công vào mạng doanh nghiệp

Việc thiết kế bảo vệ hệ thống mạng nhiều tầng cần tuân thủ theo một số nguyên tắc:

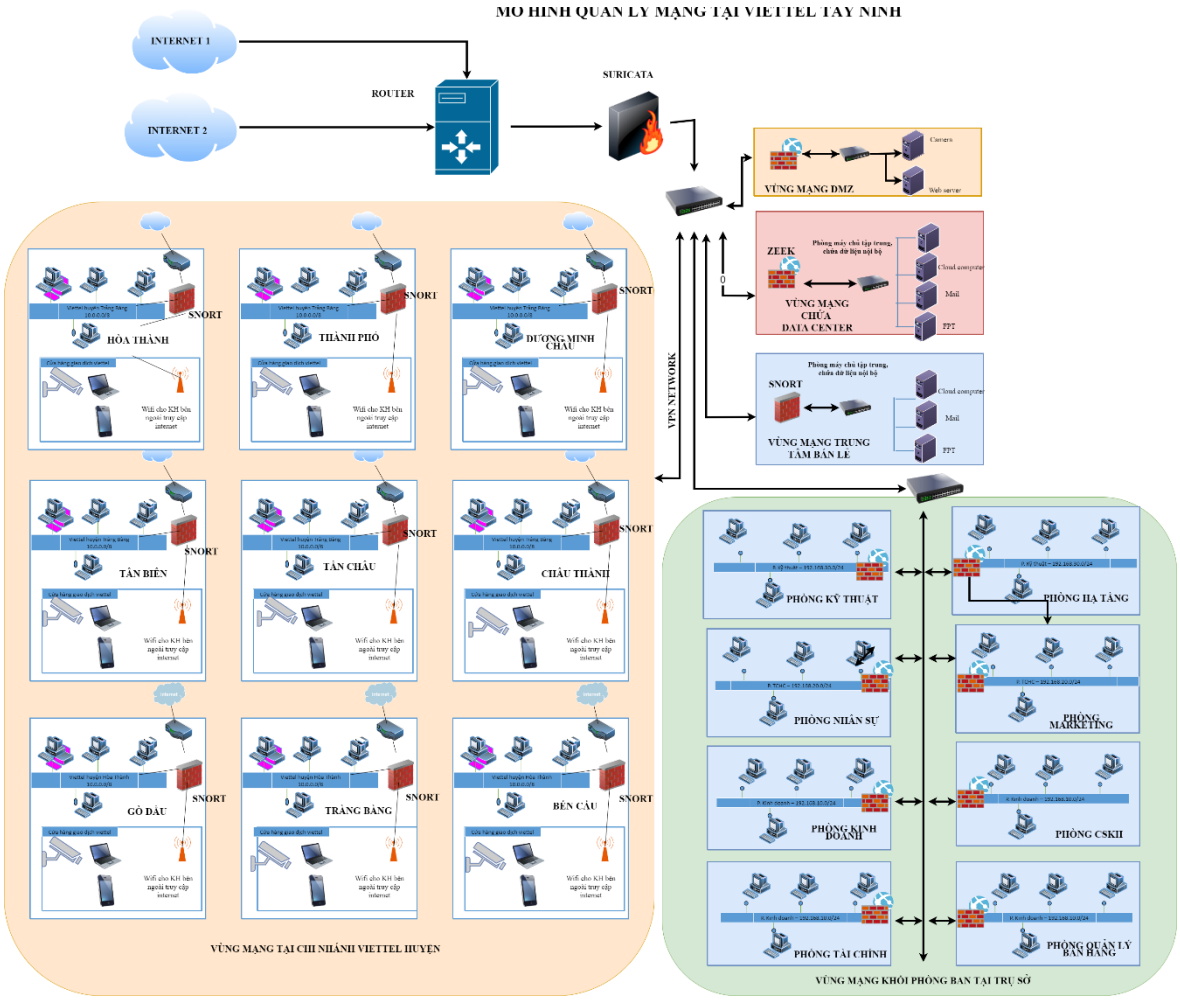
Bảo vệ có chiều sâu

Hệ thống phải được bảo vệ theo chiều sâu, phân thành nhiều tầng và tách thành nhiều lớp riêng biệt. Mỗi tầng và lớp sẽ được thực hiện các chính sách bảo mật sao cho phù hợp với yêu cầu truy cập của tầng/lớp đó, càng đi vào sâu thì yêu cầu mức độ bảo mật càng cao. Việc truy cập giữa các tầng/lớp mạng có thể được cho phép nhưng cần được kiểm soát chặt chẽ thông qua các gateway, firewall và bổ sung giám sát bằng IDS. Trong trường hợp một tầng/lớp bị xâm nhập thì xâm nhập trái phép đó không thể gây ảnh hưởng sang các tầng/lớp khác

Kết hợp nhiều công nghệ

Cần sử dụng đồng thời nhiều công nghệ và giải pháp bảo mật kết hợp nhằm tăng cường sức mạnh hệ thống phòng vệ. Khi thực hiện một công việc cụ thể cần có sự kết hợp của nhiều công cụ khác nhau. Bởi vì mỗi công cụ đều tồn tại kẽ hở, nếu chỉ sử dụng cùng một công cụ cho loại công việc đó trên toàn hệ thống thì kẻ tấn công có thể lợi dụng kẽ hở để thực hiện tấn công, dễ dàng xuyên qua toàn bộ hệ thống bảo vệ xuống tới tầng cuối cùng. Điều này làm cho việc phân tầng, phân lớp hệ thống mạng trở nên vô nghĩa

4.2 Mô hình thực nghiệm hệ thống kết hợp nhiều IDS- ứng dụng tại Viettel Tây Ninh



Hình 4.3: Hệ thống mạng Viettel Tây Ninh và các chi nhánh

Yêu cầu bảo vệ

Việc đảm bảo an ninh bảo mật hệ thống là hết sức quan trọng. Với hệ thống mạng có nhiều chi nhánh và đặc thù kinh doanh ngành viễn thông của Viettel Tây Ninh, cần phải có sự giám sát liên tục các hành động bất thường và phản ứng ngay lập tức để ngăn chặn các nguy cơ có thể xảy ra. Tuy nhiên nguồn nhân lực không thể bảo đảm giám sát 24/7. Vì vậy cần phải xây dựng một hệ thống giám sát tự động, chủ động theo dõi luồng dữ liệu luân chuyển trong hệ thống và đưa ra cảnh báo ngay lập tức. Hệ thống phải bảo vệ được nhiều lớp, qua mỗi lớp có yêu cầu về bảo mật riêng như đối với Datacenter của doanh nghiệp cần có sự bảo vệ chuyên sâu đối với các đối

tượng có khả năng công nghệ thông tin cao, mục đích tấn công rõ ràng, có khả năng cấu kết với nhân viên bên trong vùng mạng xâm nhập.

4.3 Xây dựng hệ thống Mutiple-IDS ứng dụng tại Viettel Tây Ninh

Mỗi IDS chỉ có ưu nhược điểm nhất định. Đặc biệt, công nghệ IDS Zeek hoạt động ở tầng ứng dụng để chống lại các tấn công chuyên sâu như HTTP Attack. Suricata hỗ trợ

Vì vậy cách hiệu quả nhất là kết hợp nhiều IDS hoạt động cùng lúc để hệ thống có thể phát hiện đa dạng các loại tấn công, bảo vệ toàn diện cho toàn bộ hệ thống.

Vùng mạng trụ sở chính là vùng mạng lớn nhất Viettel Tây Ninh. Đây là nơi làm việc của 8 phòng ban bao gồm nhiều nhân viên. Đồng thời đây là nơi đặt DataCenter chứa toàn bộ dữ liệu của hệ thống, cùng lúc đồng bộ dữ liệu từ 9 chi nhánh trên toàn tỉnh Tây Ninh. Bên cạnh đó vùng mạng này còn là nơi xây dựng ứng dụng web để đáp ứng dịch vụ cho khách hàng truy cập từ bên ngoài Internet. Với một lượng lớn dữ liệu kết nối cùng lúc như vậy, vùng mạng này cần một IDS hoạt động với hiệu suất cao để luồng dữ liệu được luân chuyển liên tục, vừa đảm bảo vùng mạng được bảo vệ, vừa đảm bảo độ trễ của kết nối là nhỏ nhất. Từ các kết quả phân tích các IDS độc lập, Suricata là IDS phù hợp nhất để cài đặt tại điểm chiến lược của trụ sở chính nhờ khả năng xử lý đa luồng của hệ thống IDS này.

Nằm sâu bên trong vùng mạng nội bộ là DataCenter của toàn hệ thống. Đây là nơi chứa máy chủ dữ liệu, máy chủ ứng dụng web, cung cấp dịch vụ FTP cho toàn bộ nhân viên. Vùng mạng này cũng được bảo vệ bởi Suricata, các kết nối không được cấp phép hoàn toàn có thể bị chặn lại. Tuy nhiên cần lưu ý rằng đây là nơi cần được cho phép luồng dữ liệu vào ra, và Suricata không thể nhận biết được toàn bộ luồng dữ liệu hợp lệ đó có đang tồn tại điều gì bất thường hay không. Hệ thống mạng Viettel Tây Ninh cung cấp dịch vụ FTP để chia sẻ dữ liệu cho nhân viên của từng phòng ban riêng biệt. Suricata sẽ không thể phân biệt được nhân viên phòng ban này có đang cố gắng đăng nhập vào tài khoản FTP của nhân viên phòng ban khác để lấy dữ liệu hay không. Thay vào đó, chúng ta có thể sử dụng Zeek IDS để theo dõi các kết nối và phát hiện các cố gắng kết nối thất bại để đưa ra cảnh báo về loại hình tấn công này.

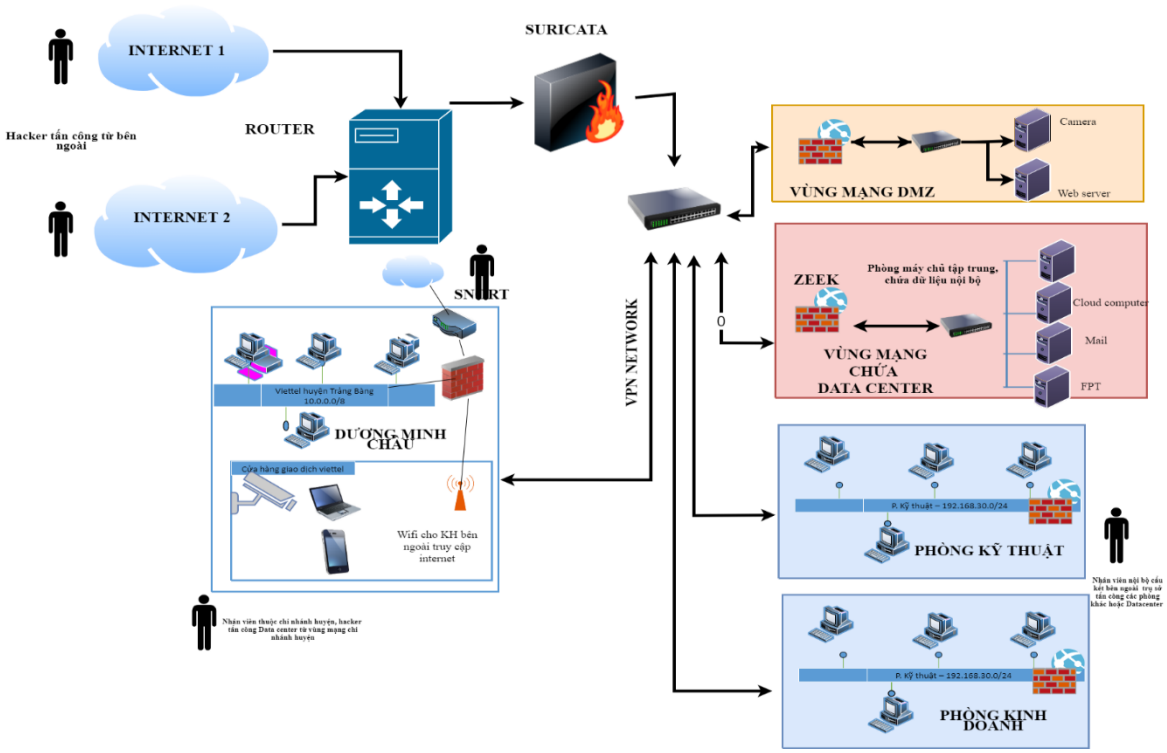
Vì vậy vùng DataCenter nằm trong trụ sở chính cần có sự kết hợp bảo vệ của cả Suricata và Zeek.

Các vùng mạng chi nhánh cũng được cung cấp các máy chủ để hỗ trợ việc xử lý dữ liệu tại chi nhánh một cách nhanh nhất. Do đó tại đây cũng cần một IDS bảo vệ các máy chủ chi nhánh trước sự tấn công của các gián điệp tại mạng nội bộ chi nhánh.

Bên cạnh đó, với việc nhiều chi nhánh cùng kết nối về trụ sở chính, việc ngăn chặn các kết nối tấn công xuất phát ngay tại chi nhánh cũng góp phần giảm tải khối lượng công việc mà IDS trụ sở cần để xử lý. Giả sử nếu có nhiều chi nhánh cùng bị nhiễm mã độc và thực hiện tấn công DDOS đến trụ sở thì toàn bộ kết nối DDOS này đều không gây ảnh hưởng đến tốc độ và khả năng đáp ứng dịch vụ của trụ sở và các chi nhánh khác. Để lựa chọn IDS sử dụng tại các chi nhánh có cấu trúc mạng đơn giản và khả năng ngăn chặn DOS tốt thì IDS tại các chi nhánh này sẽ là Snort.

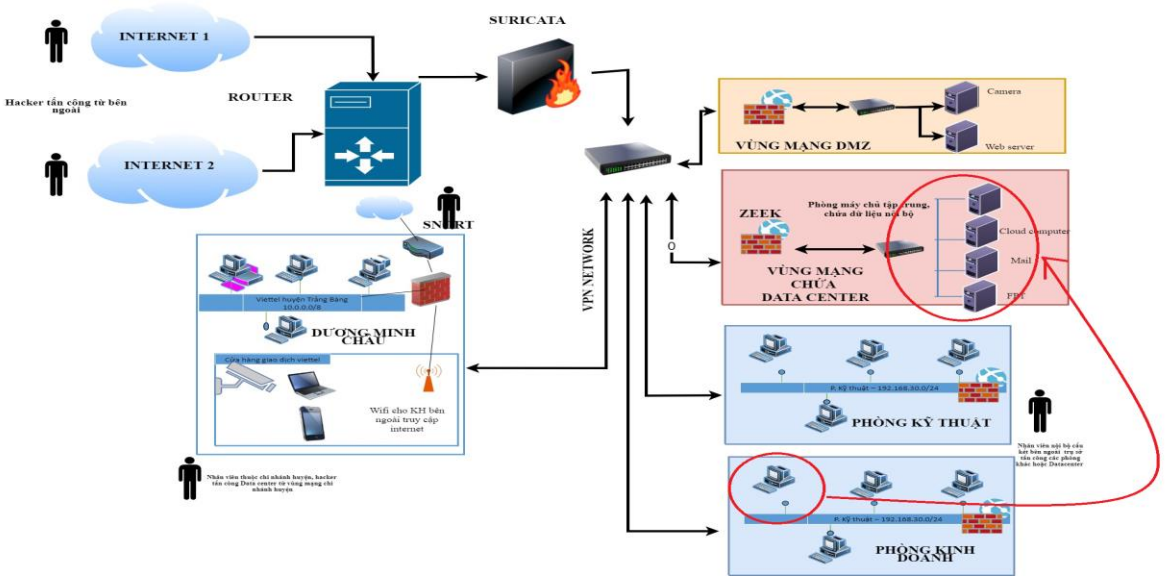
4.4 Xây dựng các kịch bản kiểm thử nghiệm tấn công

Các kịch bản được xây dựng nhằm kiểm tra khả năng phát hiện và phòng chống tấn công của 3 hệ thống IDS tích hợp bằng cách triển khai tấn công kết hợp nhiều kịch bản: Từ ngoài Internet tấn công vào bên trong, bên trong ra ngoài, kết hợp cả hai. Thông qua các kịch bản ta sẽ làm rõ được khả năng bảo vệ các vùng DMZ, DataCenter… các IDS phát hiện, phòng chống được nhiều cuộc tấn công vào và gửi cảnh báo tới quản trị viên hệ thống



Hình 4.4: Các yêu cầu bảo vệ của mạng ở Viettel Tây Ninh

4.4.1 Kịch bản 1: Tấn công từ phòng ban nội bộ của trụ sở chính lên DataCenter



Hình 4.4.1: Kịch bản 1- Tấn công nội bộ bên trong trụ sở

4.4.1.1 Mục đích

Người tấn công: nhân viên A muốn tấn công Datacenter để phá hoại hoặc đánh cắp dữ liệu, kịch bản thực hiện tấn công nhằm kiểm tra khả năng tồn tại của DataCenter trước nhiều cuộc tấn công và khả năng phát hiện tấn công của IDS phòng ban nội bộ + trụ sở chính.

4.4.1.2 Mô tả

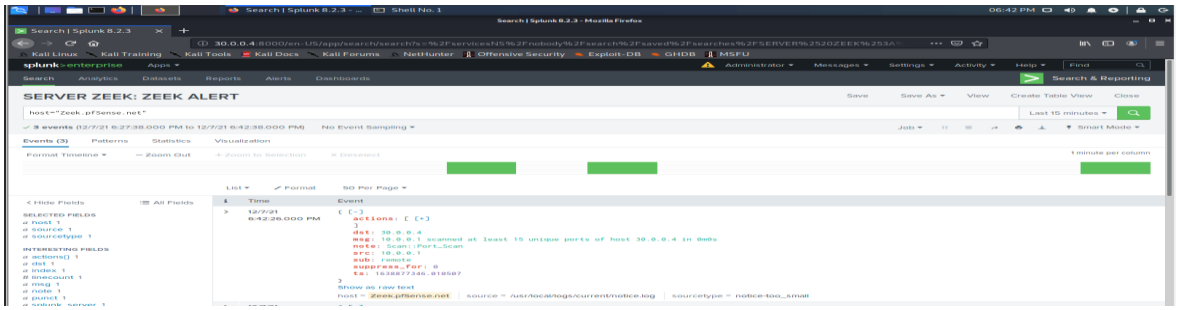
Sử dụng các máy nội bộ thuộc vùng mạng trụ sở 10.0.0.0/8 (10.0.0.1/8; 10.0.0.2/8; 10.0.0.3/8) tấn công tới mục tiêu là máy chủ nằm trong vùng DataCenter (30.0.0.4/8)

Các máy thực hiện đồng thời các hình thức tấn công:

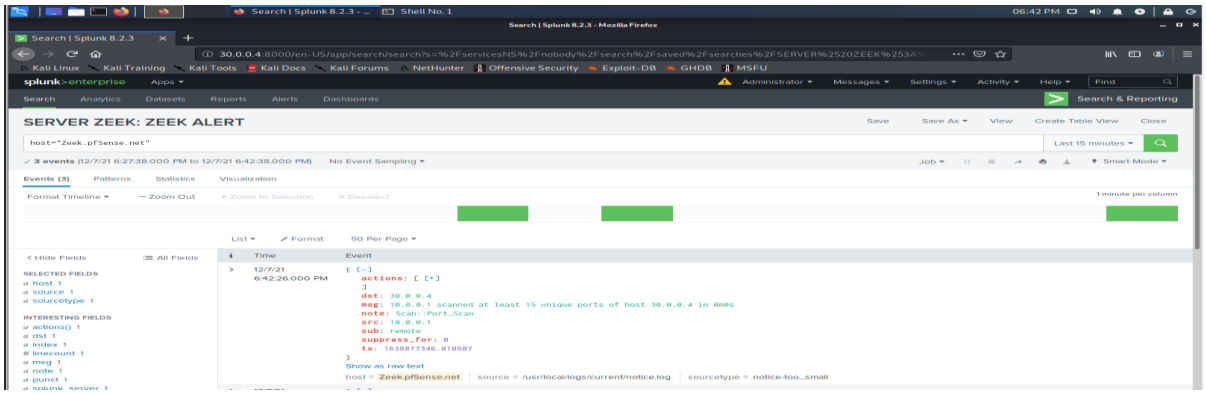
Máy 10.0.0.1/8: Thực hiện tấn công port scan và brute-force dò tìm mật khẩu đăng nhập SSH

Quá trình tấn công

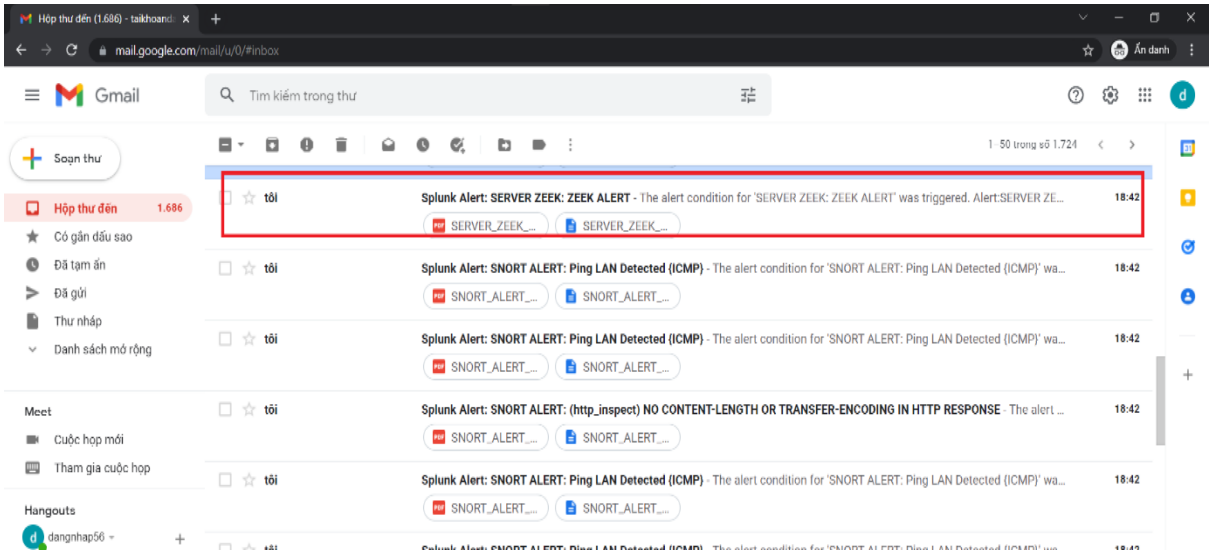
- Tấn công được phát hiện và gửi mail tại zeek server



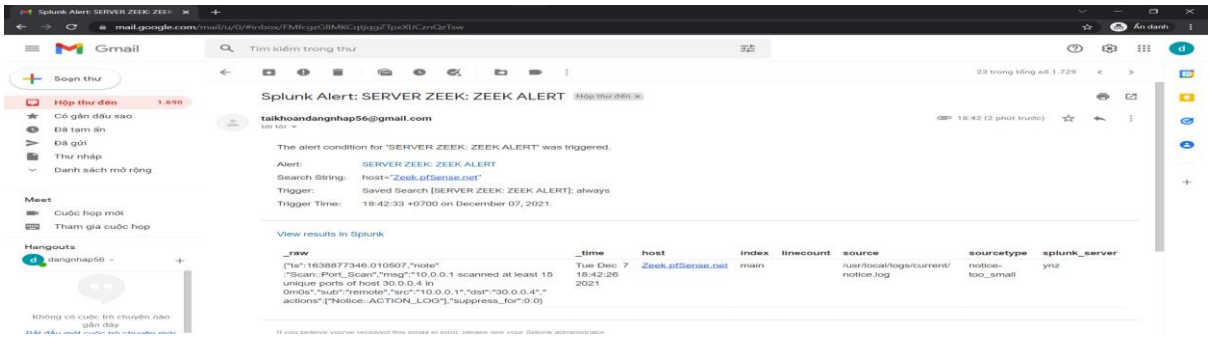
Hình 4.6: Tấn công được phát hiện và gửi mail tại zeek server



Hình 4.6: Log splunk

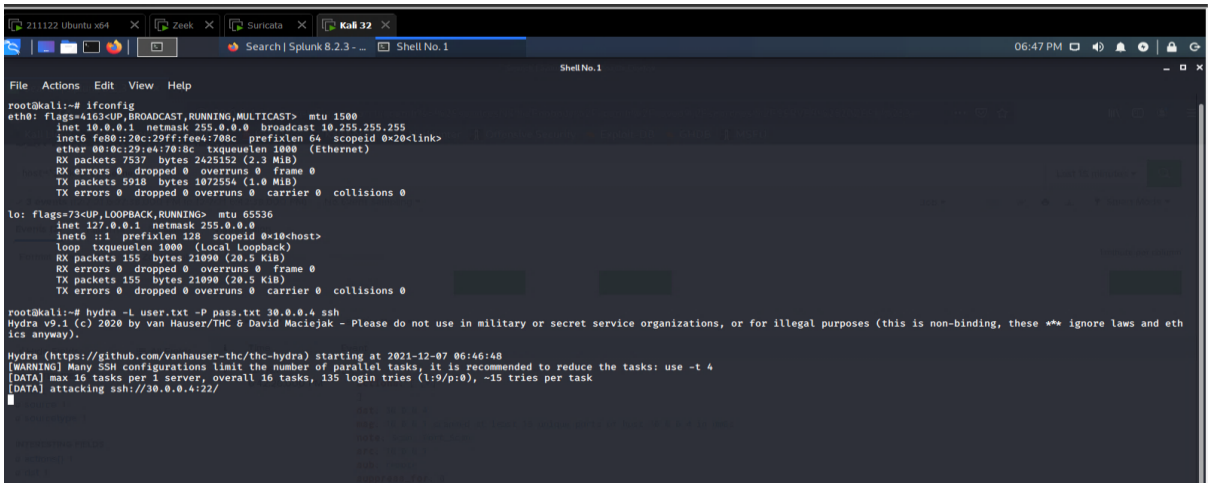


Hình 4.7: Mail cảnh báo



Hình 4.8: Mail cảnh báo (2)

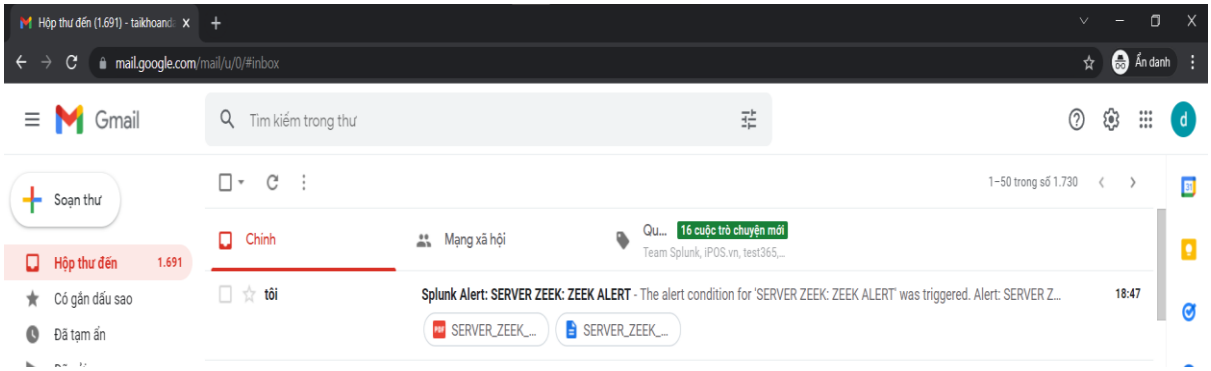
Quá trình tấn công



Hình 4.9: Tấn công brute-force dò tìm mật khẩu các tài khoản SSH

Zeek log và cảnh báo

➢ Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

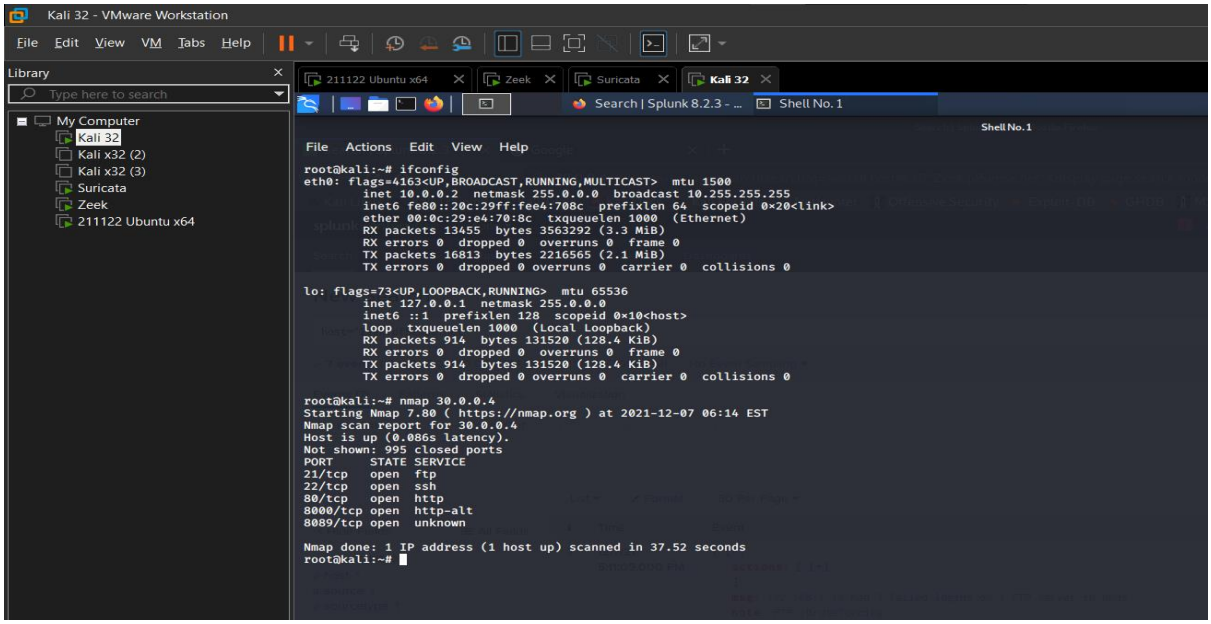


Hình 4.10: Cảnh báo mail

Máy 10.0.0.2/8: Thực hiện tấn công port scan và brute-force dò tìm mật khẩu các tài khoản FTP

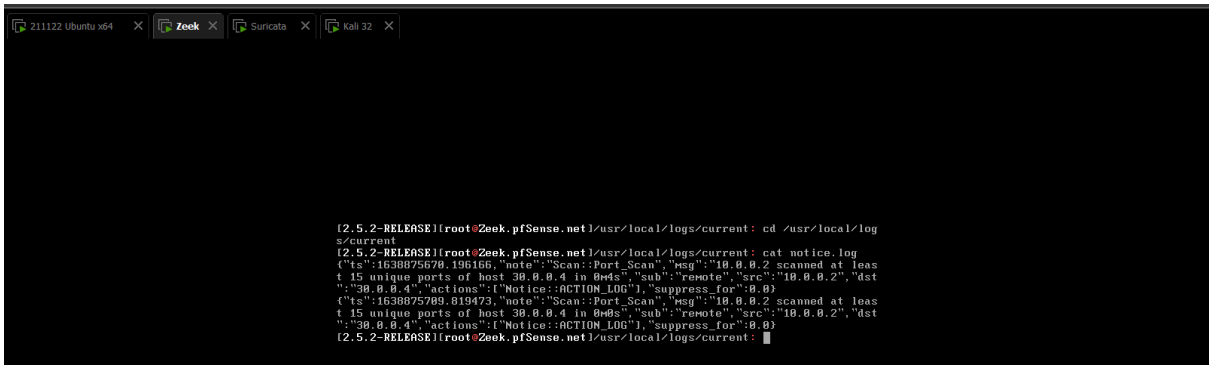
➢ Ip máy tấn công: 10.0.0.2/8

Tấn công port scan vào zeek datacenter



Hình 4.11: Ip máy tấn công: 10.0.0.2/8

➢ Tấn công được phát hiện và gửi mail cảnh bảo tại zeek server

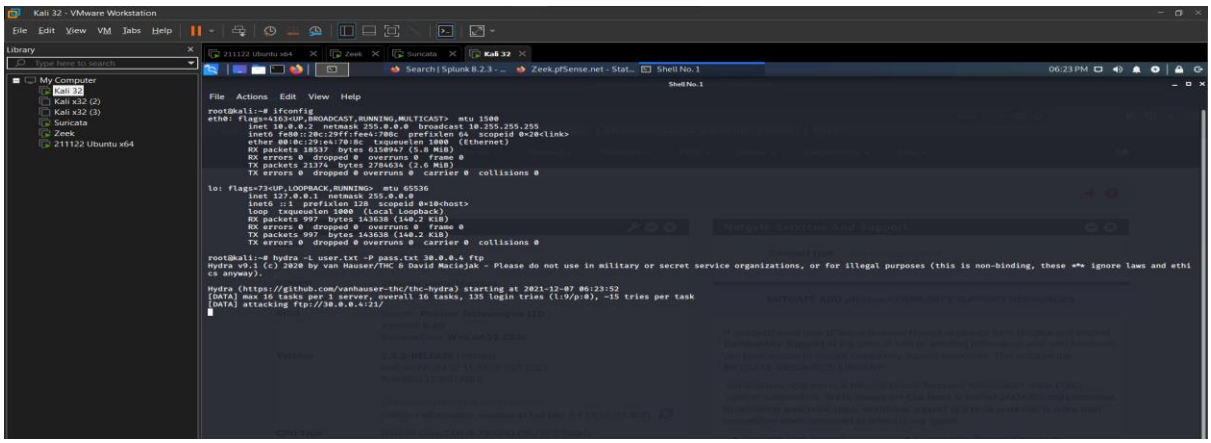


Hình 4.12: Tấn công được phát hiện và gửi log tại zeek server

- Mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

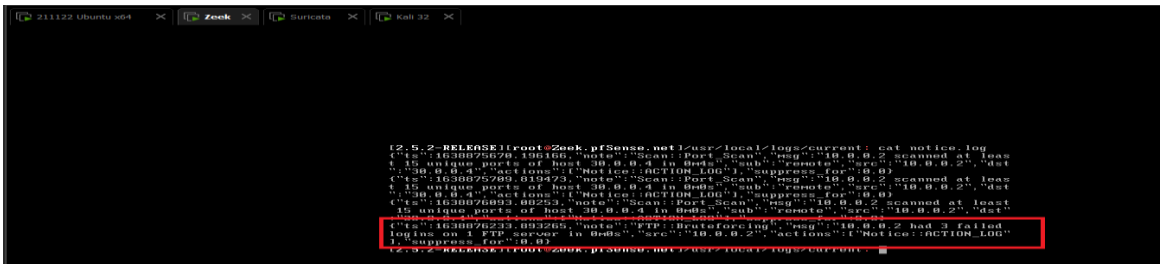
Tấn công brute-force dò tìm mật khẩu các tài khoản FTP

- Quá trình tấn công



Hình 4.13: Quá trình tấn công

- Log và cảnh báo mail



Hình 4.14: Log IDS

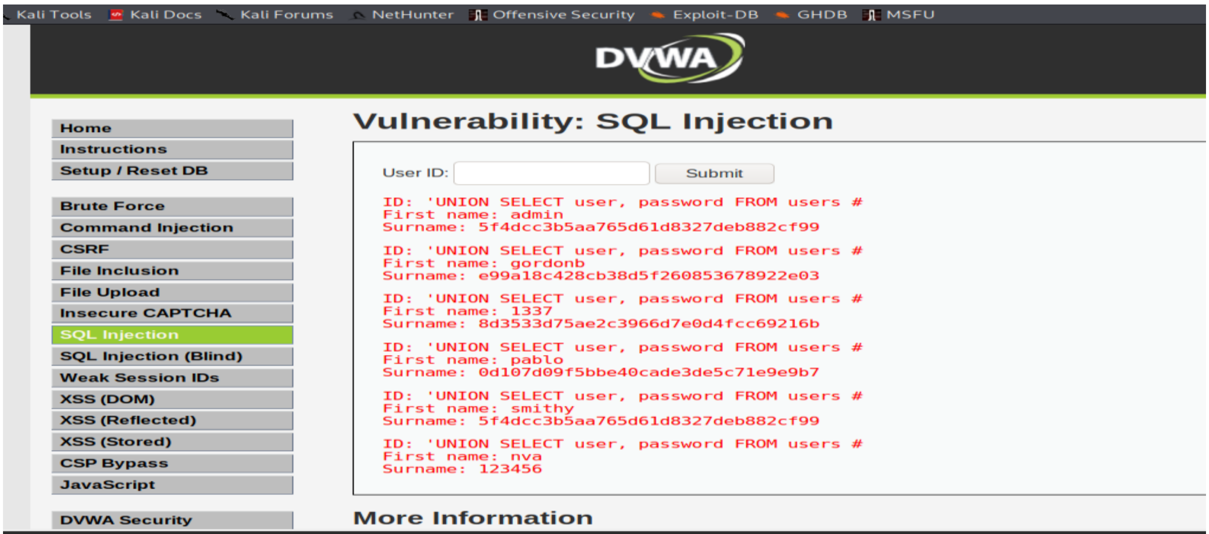
- Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

Máy 10.0.0.3/8: Thực hiện tấn công SQL injection vào ứng dụng web

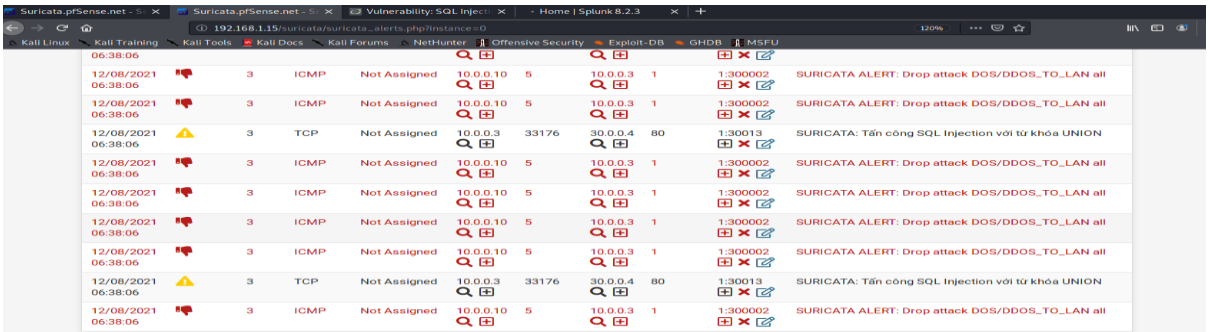
- Các hình thức tấn công trên nhằm mục đích kiểm tra khả năng phát hiện gián điệp từ mạng nội bộ
- ip máy tấn công

Tấn công SQL Injection

- Web Server DVWA



Hình 4.15: Quá trình tấn công Web Server DVWA



Hình 4.16: Log IDS

- Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SURICATA: Tấn công SQL Injection với từ khóa UNION…"

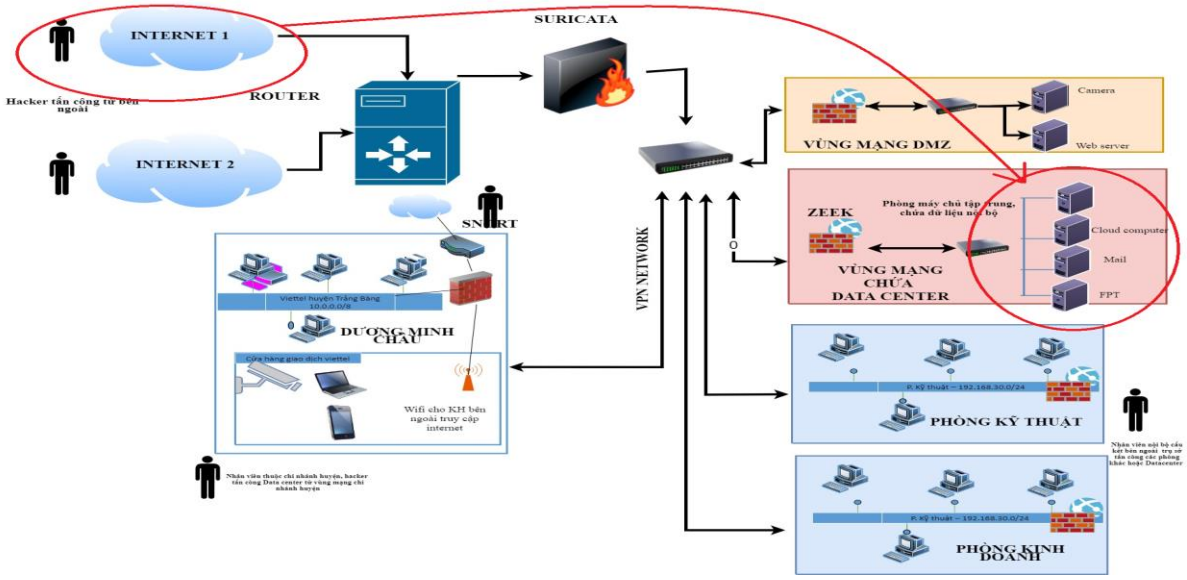
Đánh giá

Cuối cùng, sử dụng toàn bộ 3 máy trên tấn công DOS vào server 30.0.0.4/8 nhằm kiểm tra khả năng bảo vệ của IDS trước loại hình tấn công từ chối dịch vụ, đảm bảo khả năng đáp ứng dịch vụ ngay cả khi bị tấn công từ bên trong.

4.4.1.3 Đánh giá kịch bản

Qua kịch bản 1, ta thấy được 2 IDS Suricata và Zeek đã hoạt động hiệu quả, chặn được tấn công từ phòng ban trụ sở + chi nhánh và Datacenter vẫn tồn tại tốt trước nhiều cuộc tấn công

4.4.2 Kịch bản 2: Tấn công từ Internet vào Datacenter



Hình 4.4.2: Kịch bản 2- Tấn công từ bên ngoài internet

4.4.2.1 Mục đích

- Người tấn công: người bên ngoài muốn phá hoại hoặc lấy dữ liệu từ Datacenter

- Kịch bản thực hiện tấn công nhằm kiểm tra khả năng tồn tại của DataCenter trước nhiều cuộc tấn công và khả năng phát hiện tấn công của IDS của trụ sở chính (trụ sở chính có chức năng chặn tấn công từ Internet **vào)**

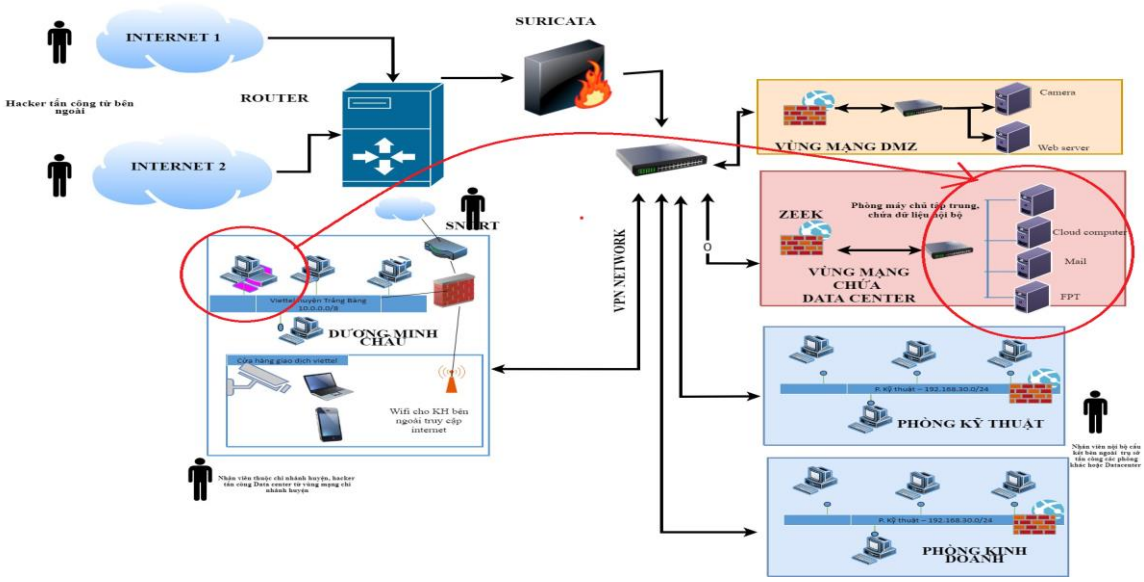
4.4.2.2 Mô tả

- Giả định máy chủ nằm trong vùng DataCenter (30.0.0.0/8) cung cấp dịch vụ Web và dịch vụ chia sẻ file FTP cho các nhân viên làm việc từ xa. Máy chủ này được NAT ra IP public (192.168.1.16) để khách hàng có thể truy cập từ ngoài InternetTạo rule firewall không cho nat ra ngoài, nên các máy ngoài Internet không ping được **tới** gateway firewall (192.168.1.11) -> Hạn chế nguy cơ từ bên ngoài 6 máy từ Internet đồng loạt tấn công vào DataCenter (30.0.0.4/8):
    - Máy Internet 1: Tấn công port scan, FTP brute-force
    - Máy Internet 2: Tấn công SSH brute-force, XSS
    - Máy Internet 3: Tấn công FTP brute-foce, SQL injection
- Các cuộc tấn công này nhằm kiểm tra khả năng phát hiện của IDS đối với các cuộc tấn công khai thác thông tin từ bên ngoài InternetSau khi hoàn thành tấn công các hình thức trên, sử dụng toàn bộ 6 máy từ Internet tấn công DOS tạo thành cuộc tấn công từ chối dịch vụ phân tán (DDOS), nhằm kiểm tra khả năng sống sót của máy chủ dịch vụ trước hình thức tấn công DDOS từ bên ngoài

4.4.2.3 Đánh giá kịch bản

Qua kịch bản 2, ta thấy được khả năng tồn tại tốt của DataCenter trước nhiều cuộc tấn công và khả năng phát hiện tấn công của IDS của trụ sở chính (trụ sở chính có chức năng chặn tấn công từ Internet vào)

4.4.3 Kịch bản 3: Tấn công từ vùng nội bộ chi nhánh huyện lên DataCenter



Hình 4.4.3: Kịch bản 3- Tấn công chi nhánh huyện lên Datacenter

4.4.3.1 Mục đích

- Nhân viên thuộc chi nhánh huyện tấn công Data center
- Kịch bản thực hiện tấn công nhằm kiểm tra khả năng tồn tại của DataCenter trước nhiều cuộc tấn công và khả năng phát hiện tấn công của IDS vùng nội bộ chi nhánh (lớp mạng 22.0.0.1/8 và 20.0.0.2/8)Qua đó kiểm tra độ mạnh của hệ thống IDS Snort và IDS Zeek, IDS Suricata

4.4.3.2 Mô tả

- Sử dụng các máy nội bộ 22.0.0.0/8 (22.0.0.1/8; 22.0.0.2/8; 22.0.0.2/8) thuộc vùng mạng chi nhánh (có IP WAN là 19268) tấn công tới mục tiêu là máy chủ nằm trong vùng DataCenter (30.0.0.4/8) của vùng mạng trụ sở (có IP WAN là 19268)
- Máy chủ (30.0.0.4/8) được NAT từ IP private (30.0.0.4/8) ra IP WAN (192.168.1.11) để các máy từ chi nhánh có thể truy cập và trao đổi dữ liệu với trụ sở.
- Các máy chi nhánh thực hiện đồng thời các hình thức tấn công:

Máy 22.0.0.1/8: Thực hiện tấn công brute-force dò tìm mật khẩu đăng nhập SSH

Log IDS

- Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

Máy 22.0.0.2/8: Thực hiện tấn công port scan và brute-force dò tìm mật khẩu các tài khoản FTP

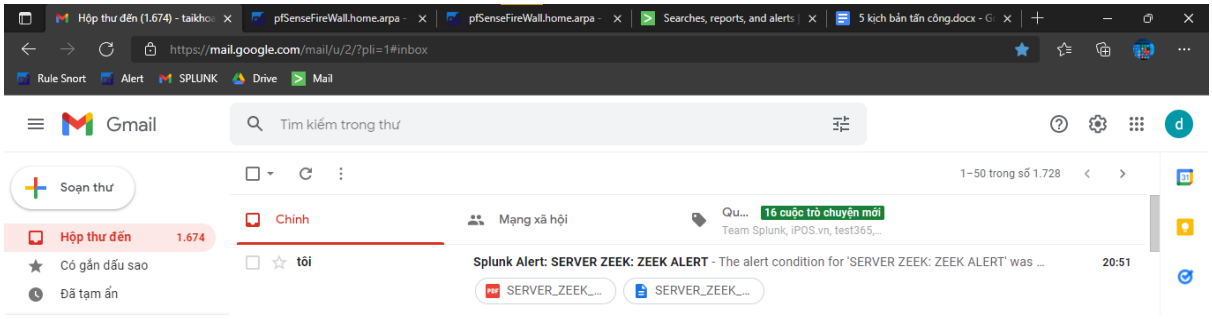
Quá trình tấn công

Hình 4.18: Quá trình tấn công

- Log IDS

Hình 4.19: Log IDS

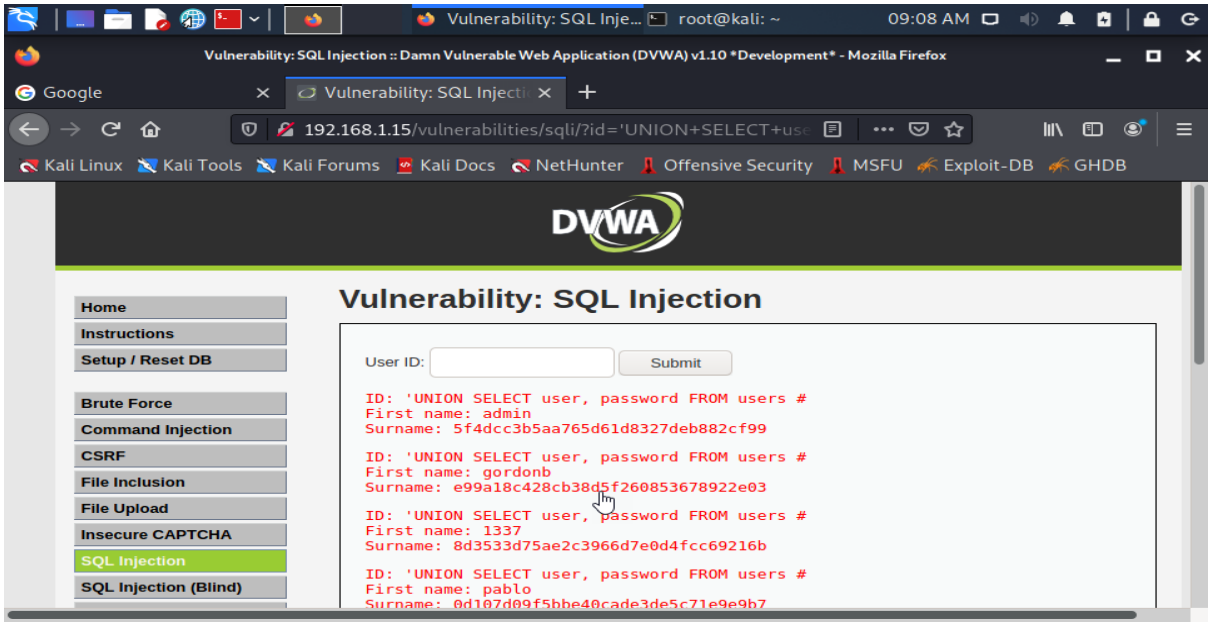
- Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"



Hình 4.20: Cảnh báo mail về cho quản trị viên hệ thống

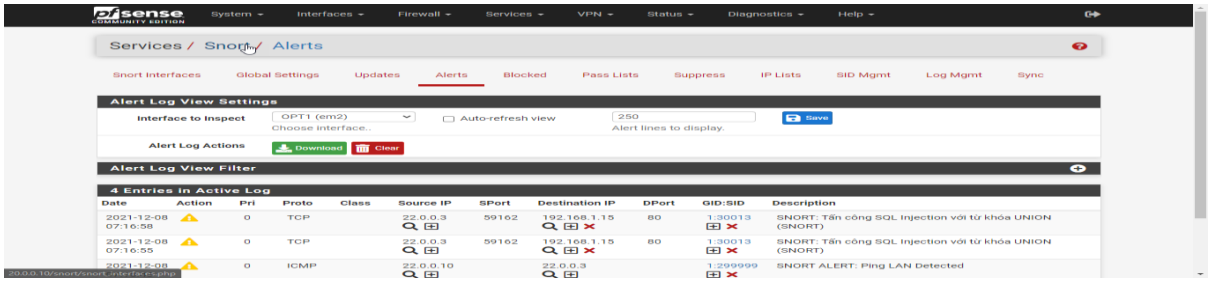
Máy 22.0.0.3/8: Thực hiện tấn công, SQL injection vào ứng dụng web

Quá trình tấn công



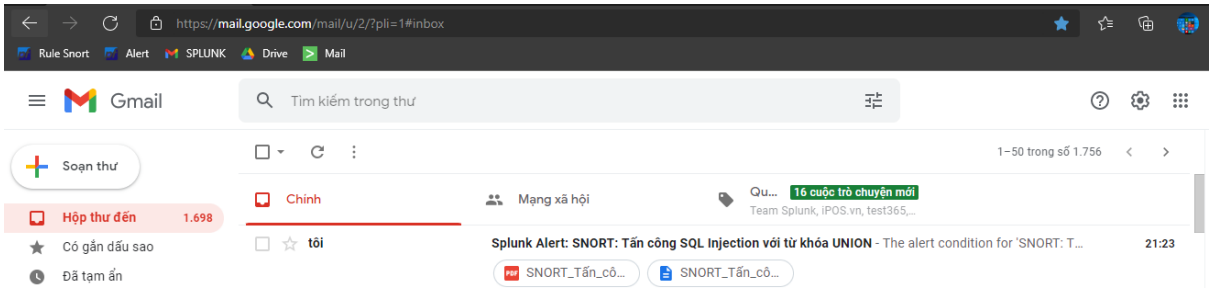
Hình 4.21: Quá trình tấn công SQL Injection vào DVWA

- Log IDS



Hình 4.22: Log được IDS ghi lại

- Cảnh báo mail



Hình 4.23: Cảnh báo mail

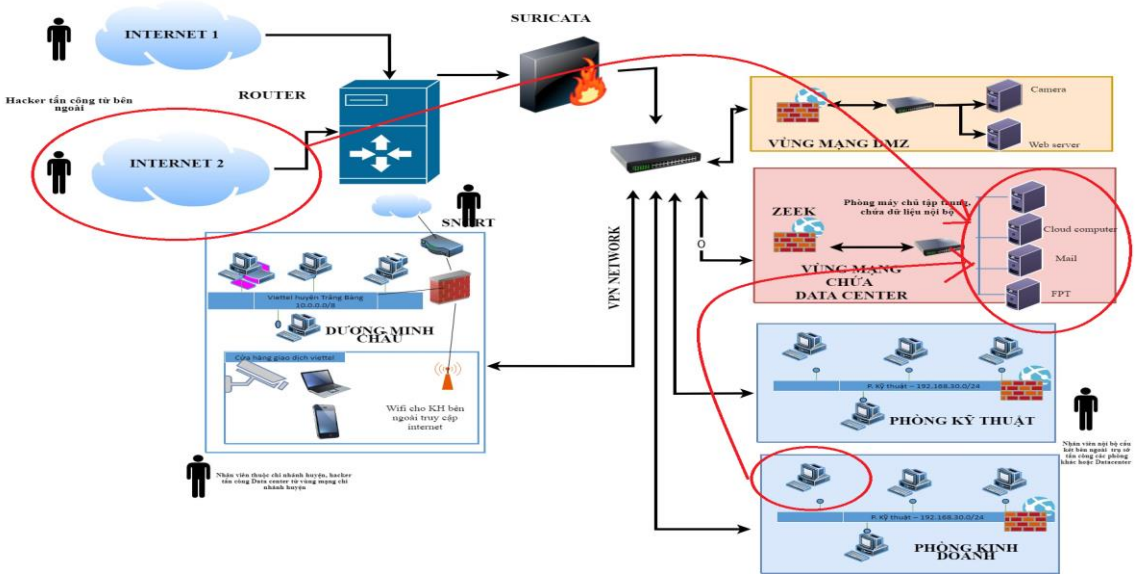
Đánh giá

- Sau khi hoàn thành các hình thức tấn công trên, cả 3 máy đồng loạt thực hiện DOS về server trụ sở.
- Các cuộc tấn công này nhằm kiểm tra khả năng ngăn chặn các hình thức tấn công gián điệp ngay tại IDS của chi nhánh trước khi luồng dữ liệu tấn công được chuyển về trụ sở.

4.4.3.3 Đánh giá kịch bản

Qua kịch bản 3, ta thấy được khả năng tồn tại tốt của DataCenter trước nhiều cuộc tấn công và khả năng phát hiện tấn công của IDS của vùng nội bộ chi nhánh. Và 3 cả hệ thống IDS đều phát hiện được tấn công vào Data Center từ vùng chi nhánh huyện.

4.4.4 *Kịch bản 4: Tấn công kết hợp giữa Internet và các phòng ban cùng tấn công DataCenter tại trụ sở*



Hình 4.4.4: Kịch bản 4 tấn công kết hợp trong ngoài

4.4.4.1 Mục đích

- Người bên ngoài cấu kết nhân viên tấn công Datacenter
- Kịch bản thực hiện tấn công nhằm kiểm tra khả năng tồn tại của tại trụ sở và phát hiện được gián điệp cấu kết với nhân viên bên trong nội bộ -> Kiểm tra khả năng phát hiện cảnh báo giả của hệ thống IDS Suricata + Zeek (là khả năng phân biệt được lúc nào có tấn công thật, lúc nào tấn công giả và lúc nào là gián điệp)
- Các cuộc tấn công này nhằm kiểm tra khả năng bảo vệ của IDS trụ sở trước các cuộc tấn công đồng thời từ trong và cả ngoài mạng doanh nghiệp.

4.4.4.2 Mô tả

- 1 máy từ mạng nội bộ trụ sở (10.0.0.0/8), 1 máy từ nội bộ chi nhánh (22.0.0.0/8), 1 máy từ Internet tấn công vào server (30.0.0.0/8)Các máy của mỗi vùng mạng thực hiện đồng thời các cuộc tấn công:
- Máy nội bộ trụ sở (10.0.0.0/8): Port scan, FTP brute-force

- Port Scan

Quá trình tấn công

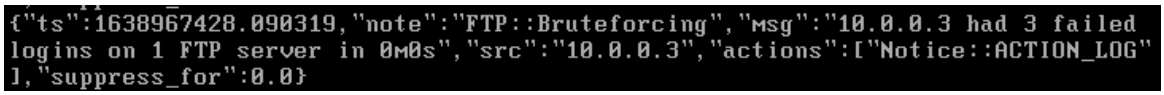
Log của IDS

Hình 4.24: Log của IDS

Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER: ZEEK ALERT…"

Brute-force vào FTP

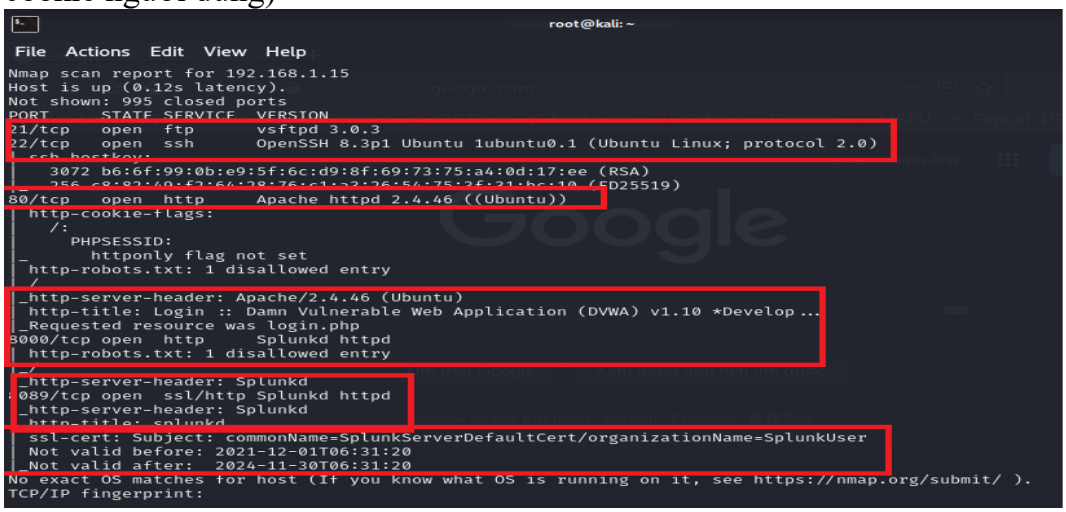
Log của IDS



Hình 4.25: Log của IDS

- Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

Tấn công vào nội bộ chi nhánh (22.0.0.1/8): Port scan, SSH brute-force, XSS (lấy cookie người dùng)



Hình 4.26: Kết quả tấn công Port Scan

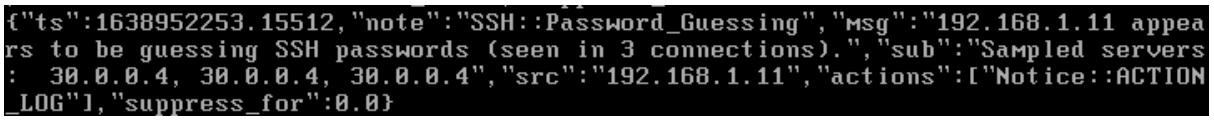
- Log được IDS ghi lại

Hình 4.27: Log được IDS ghi lại

Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

SSH brute-force

- Quá trình tấn công
- Log ghi lại



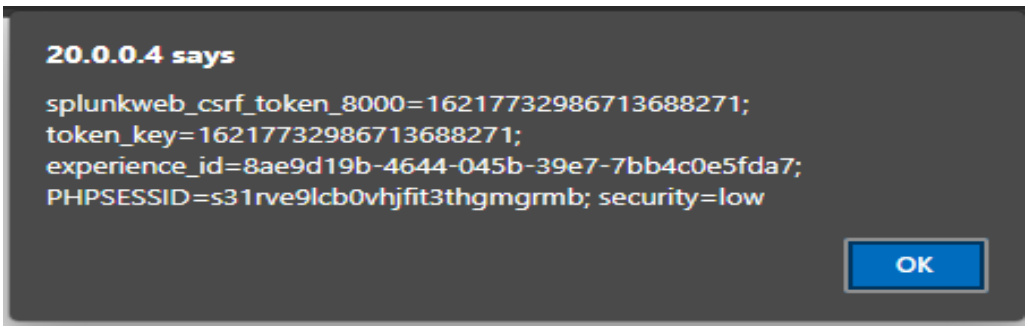
Hình 4.28: Log ghi lại

- Mail cảnh báo: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SERVER ZEEK ALERT…"

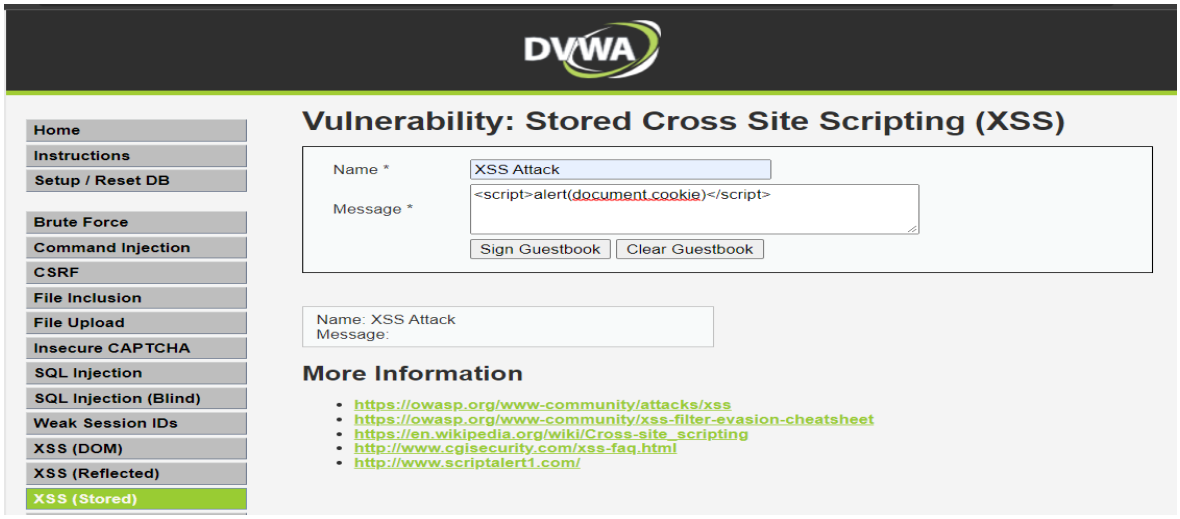
- **XSS**

  Quá trình tấn công

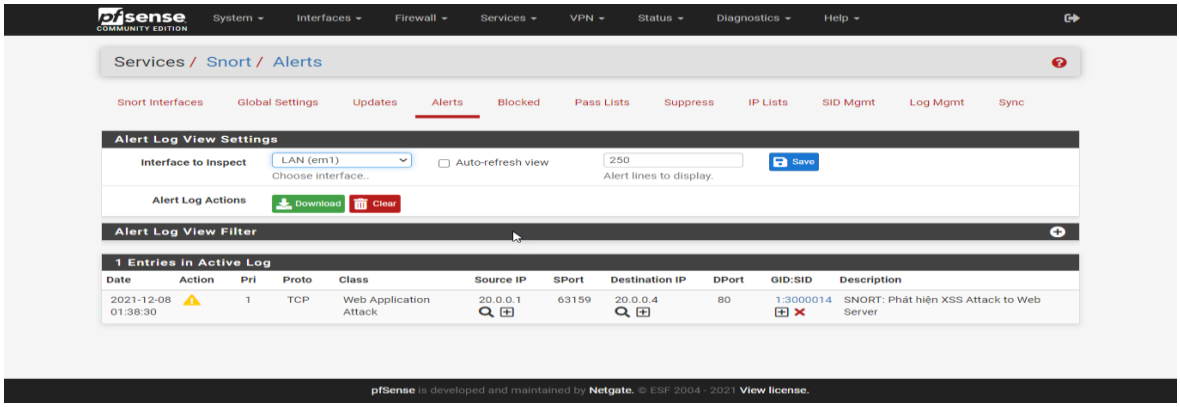
  - Log ghi lại



Hình 4.29: Tấn công XSS lấy Cookie người dùng



Hình 4.30: Log ghi lại



Hình 4.31: Quá trình tấn công vào DVWA

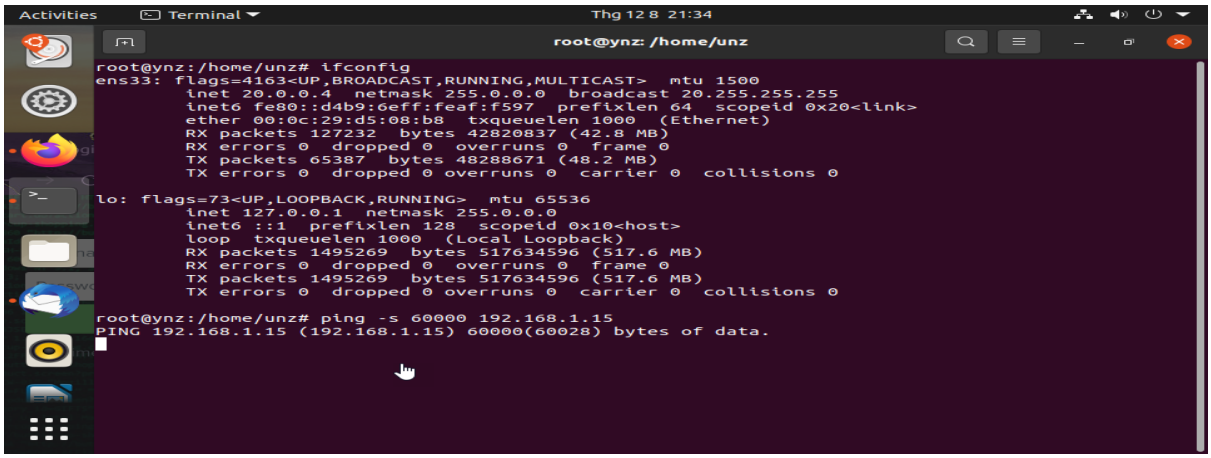
Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SNORT: Phát hiện XSS Attack to Web Server", và các thông số của cuộc tấn công như ip máy tấn công, thời gian, hình thức, loại hình tấn công…

- Internet: Port-Scan, FTP brute-force
- DOS vào server tran, FTP brute-force
- Sau khi hoàn thành các hình thức tấn công trên, sử dụng 1 máy từ mạng nội bộ trụ sở 10.0.0.1/8, 1 máy từ mạng nội bộ chi nhánh 22.0.0.1/8, 1 máy từ vùng DMZ 20.0.0.1/8 đồng loạt tấn công DOS vào server trụ sở (30.0.0.4/8).

- **Ip các máy tấn công**
- Máy 1: 10.0.0.1/8
- Máy 2: 22.0.0.1/8
- Máy 3: 20.0.0.1/8

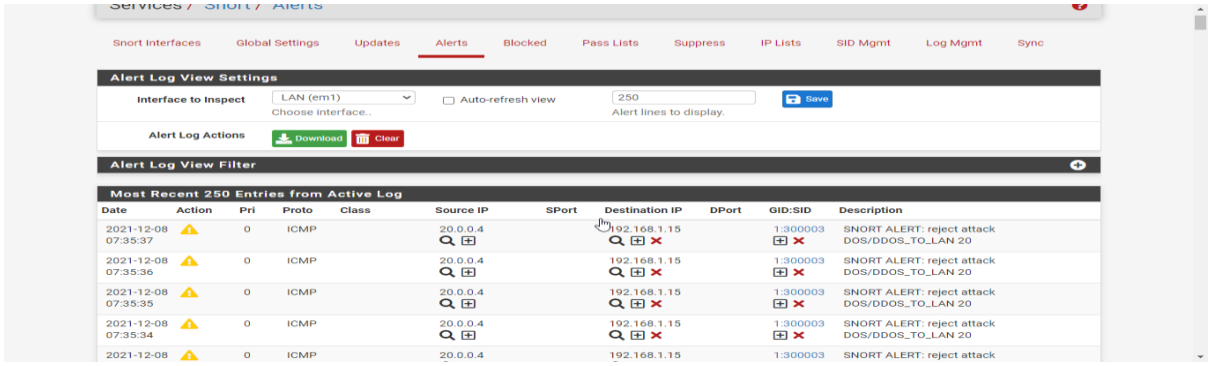
Quá trình tấn công

- Máy 1: 10.0.0.1/8
- Máy 2: 22.0.0.1/8
- Máy 3: 20.0.0.1/8

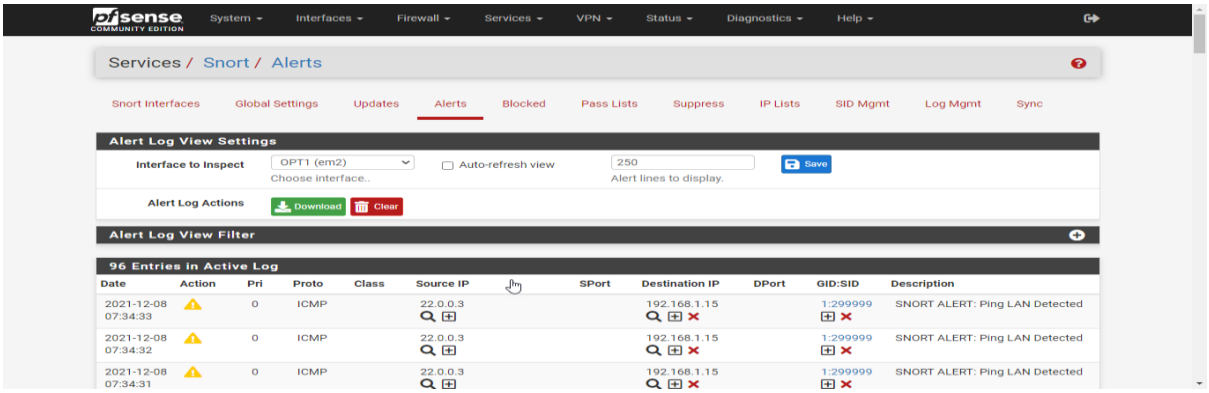


Hình 4.32: Quá trình tấn công (máy 3)

Log ghi lại đầy đủ các ip tấn công



Hình 4.33: Log ghi lại bởi IDS



Hình 4.34: Log ghi lại bởi IDS (2)

- Mail cảnh báo: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công "Splunk Alert: SNORT ALERT: reject attack DOS/DDOS_TO_LAN 20 …"

Các cuộc tấn công này nhằm kiểm tra khả năng bảo vệ của IDS trụ sở trước các cuộc tấn công đồng thời từ trong và cả ngoài mạng doanh nghiệp.

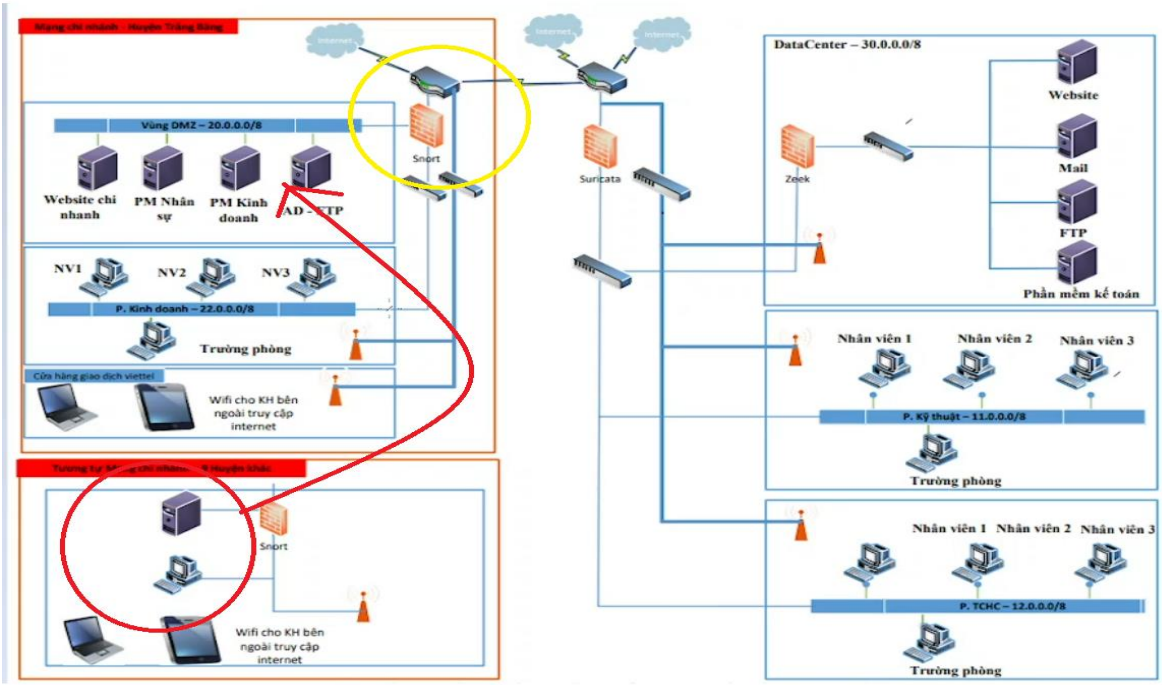
- Đánh giá kịch bảnNgười bên ngoài cấu kết nhân viên tấn công Datacenter
- Kịch bản thực hiện tấn công nhằm kiểm tra khả năng tồn tại của tại trụ sở và phát hiện được gián điệp cấu kết với nhân viên bên trong nội bộ -> Kiểm tra khả năng phát hiện cảnh báo giả của hệ thống IDS Suricata + Zeek (là khả năng phân biệt được lúc nào có tấn công thật, lúc nào tấn công giả và lúc nào là gián điệp)
- Các cuộc tấn công này nhằm kiểm tra khả năng bảo vệ của IDS trụ sở trước các cuộc tấn công đồng thời từ trong và cả ngoài mạng doanh nghiệp.

4.4.4.3 Đánh giá kịch bản

- Kịch bản thực hiện tấn công nhằm kiểm tra khả năng tồn tại của tại trụ sở và phát hiện được gián điệp cấu kết với nhân viên bên trong nội bộ -> Kiểm tra khả năng phát hiện cảnh báo giả của hệ thống IDS Suricata + Zeek (là khả năng phân biệt được lúc nào có tấn công thật, lúc nào tấn công giả và lúc nào là gián điệp). Kết quả thu được cho thấy IDS tại trụ sở phát hiện được gián điệp cấu kết với nhân viên bên trong nội bộ.

- Các cuộc tấn công này nhằm kiểm tra khả năng bảo vệ của IDS trụ sở trước các cuộc tấn công đồng thời từ trong và cả ngoài mạng doanh nghiệp.

4.4.5 Kịch bản 5: Nội bộ chi nhánh tấn công vào DMZ chi nhánh huyện



Hình 4.4.5: Kịch bản 5- Tấn công nội bộ tại CN huyện

4.4.5.1 Mục đích

- Các cuộc tấn công này nhằm kiểm tra khả năng bảo vệ của IDS Snort vùng DMZ chi nhánh huyện trước các cuộc tấn công đồng thời từ bên trong và khả năng phát hiện cảnh báo giả của IDS Snort

4.4.5.2 Mô tả

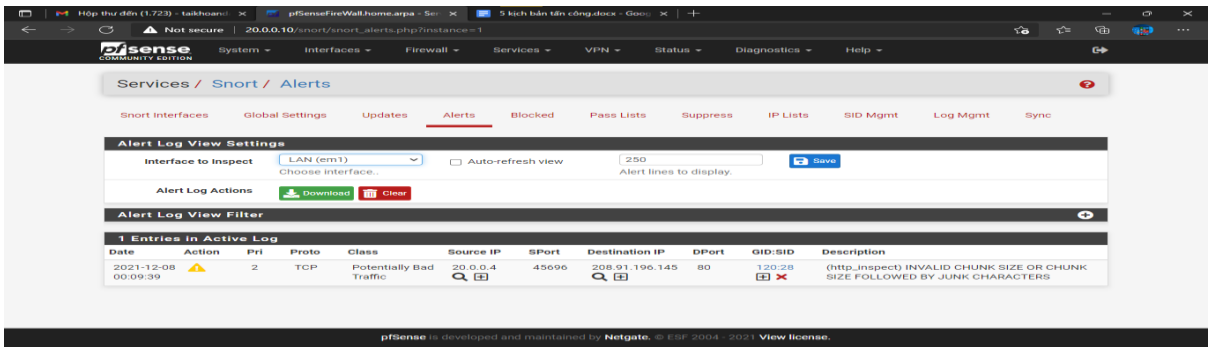
- Nội bộ chi nhánh tấn công vào máy chủ chi nhánh huyện
- Sử dụng các máy nội bộ 22.0.0.0/8 (22.0.0.1/8; 22.0.0.2/8) thuộc vùng mạng nội bộ chi nhánh tấn công vào máy chủ ở vùng DMZ chi nhánh (20.0.0.4/8)
- Máy 22.0.0.1/8: Thực hiện tấn công XSS, SQL injection vào ứng dụng web

Máy 22.0.0.2/8: Thực hiện tấn công bằng mã độc vào ứng dụng Web

Quá trình tấn công (gián điệp truy cập các website chứa mã độc nhằm phá hoại hệ thống) (Nguồn các website: https://archive.siasat.com/news/top-100-dangerous-websites-revealed-29507/)

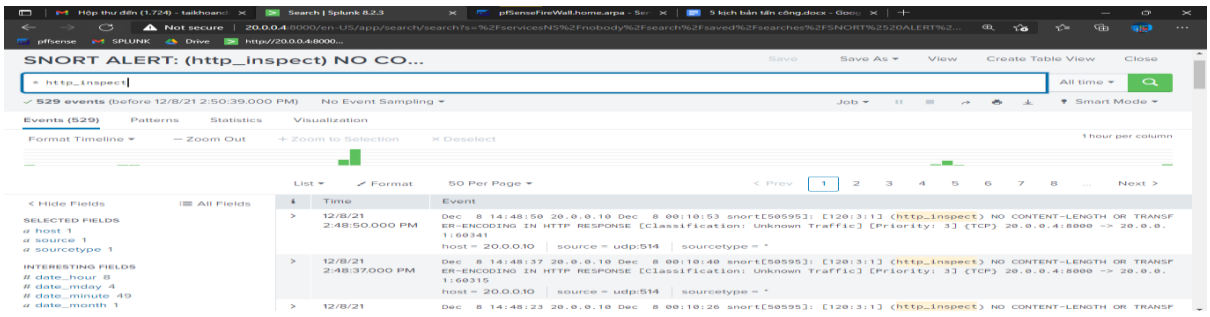
Hình 4.35: Quá trình tấn công

- Log Snort



Hình 4.36: Log ghi lại bởi IDS

- Log Splunk



Hình 4.37: Log ghi lại bởi Log Server Splunk

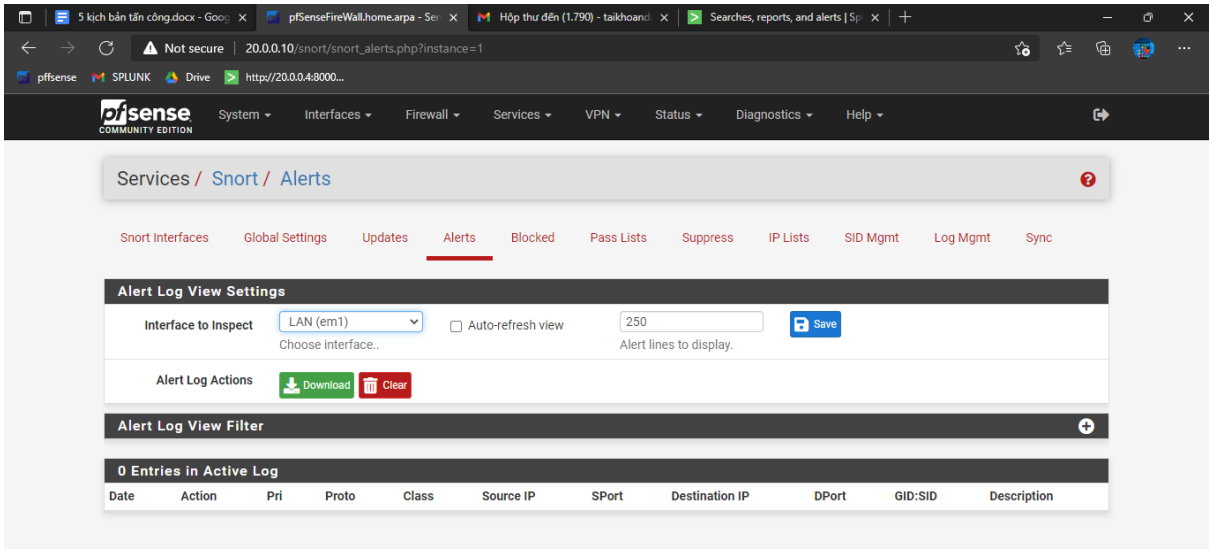
- Cảnh báo mail: Sau khi tấn công, splunk tạo alert và gửi mail tới mail của quản trị viên hệ thống quay lập tức, nội dung mail thông báo đúng loại tấn công

"Splunk Alert: SNORT ALERT: (http_inspect): NO CONTENT-LENGTH OR TRANSFER-ENCODING IN H…", và các thông số của cuộc tấn công như ip máy tấn công, thời gian, hình thức, loại hình tấn công…

22.0.0.1/8: Thực hiện tấn công port scan và brute-force dò tìm mật khẩu đăng nhập SSHPort scan

Hình 4.38: Quá trình tấn công

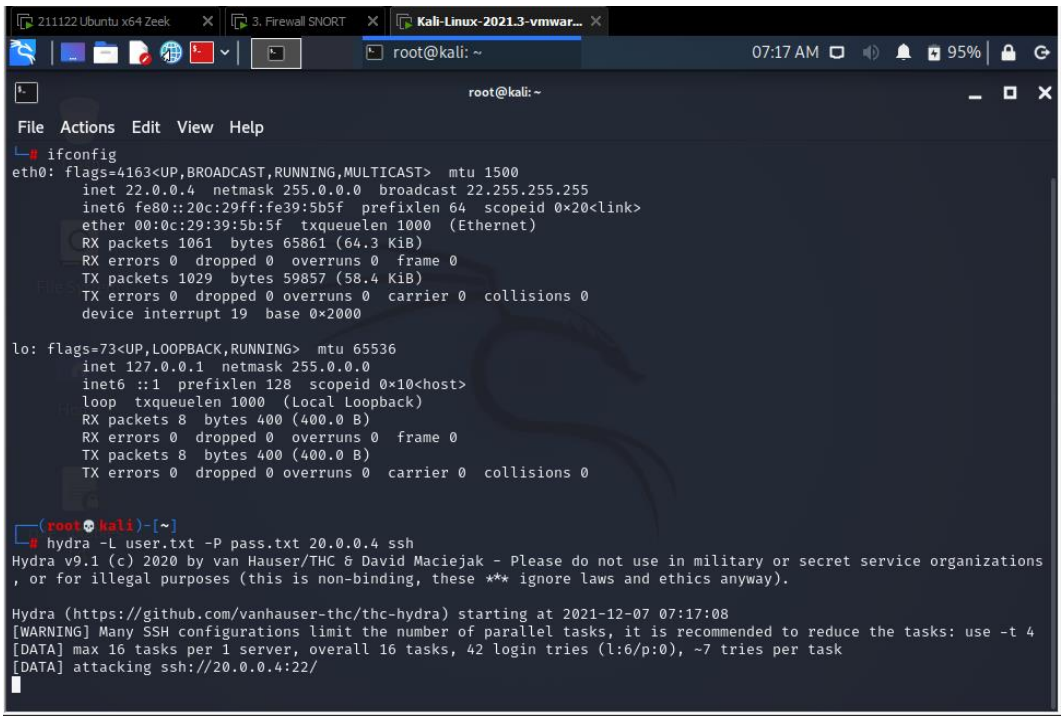
- Log SNORT ghi lại



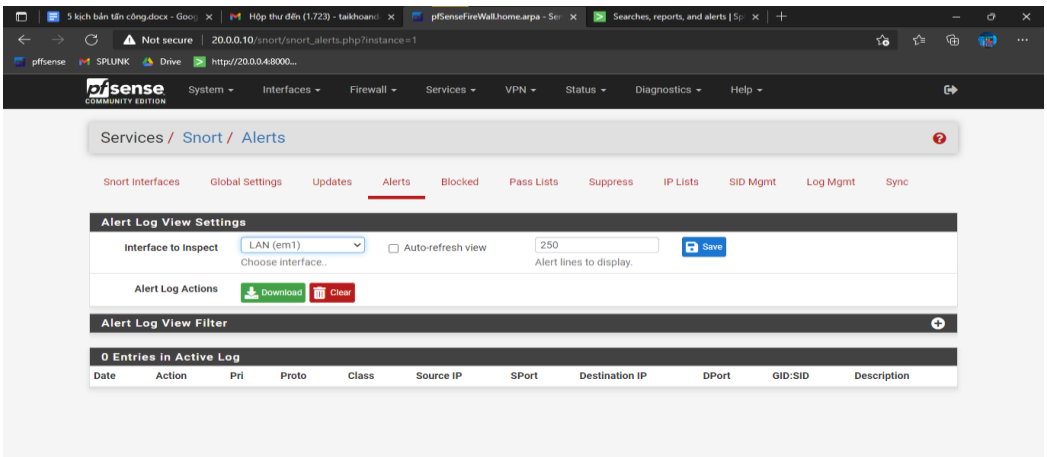
Hình 4.39: Log được IDS ghi lại

- Cảnh báo mail: SNORT không phát hiện được tấn công port_scan nên không ghi log và gửi cảnh báo mail tới quản trị viên hệ thống.

- Máy 22.0.0.1/8:



Hình 4.40: Quá trình tấn công Brute Force dò tìm mật khẩu đăng nhập SSH



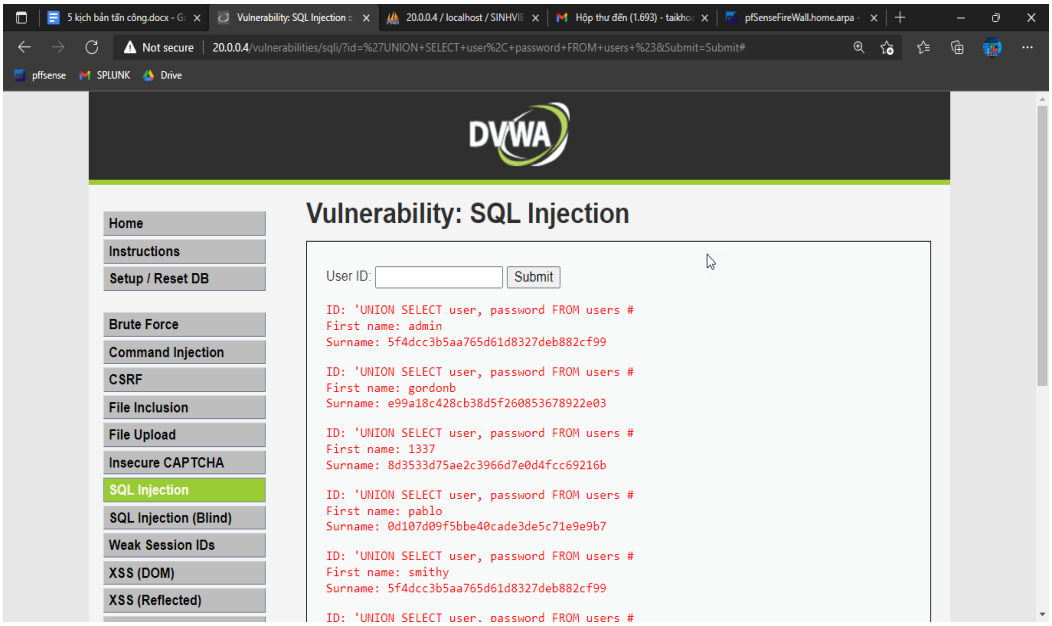
Hình 4.41: Log Snort

- Cảnh báo mail: SNORT không phát hiện được tấn công brute-force dò tìm mật khẩu đăng nhập SSH nên không ghi log và gửi cảnh báo mail tới quản trị viên hệ thống.

Máy 22.0.0.2/8: Thực hiện tấn công XSS, SQL injection vào ứng dụng web

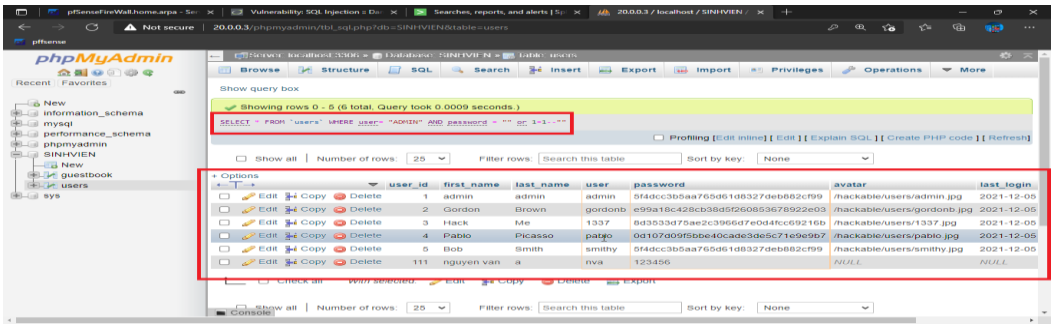
- Ip máy tấn công:

- Tấn công vào Web Server DVWA
- Tấn công Sql Injection bằng từ khóa OR
- Tấn công Sql Injection bằng từ khóa UNION

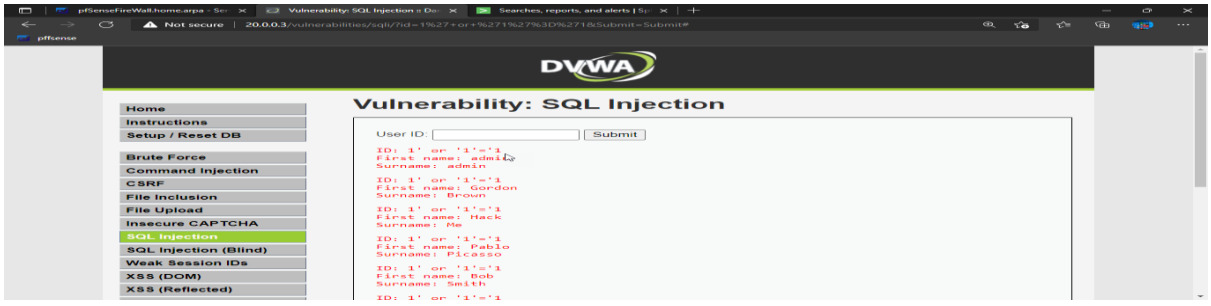


Hình 4.42: Tấn công SQL Injection bằng từ khóa UNION

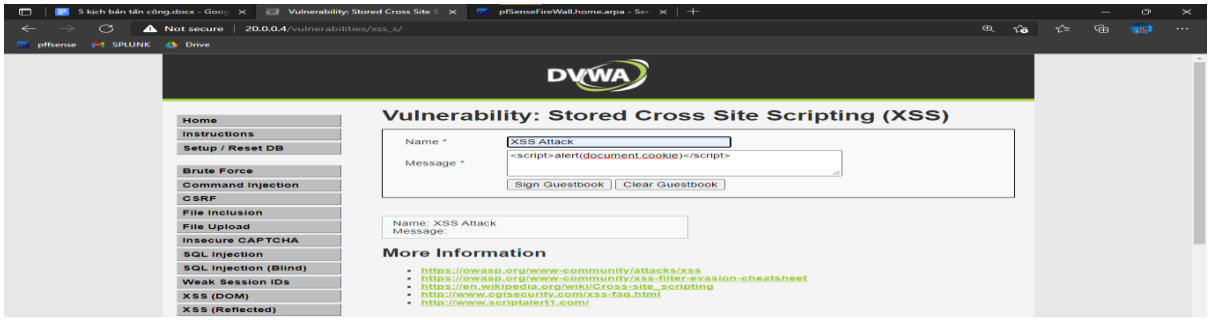
➢ Tấn công phpmyadmin



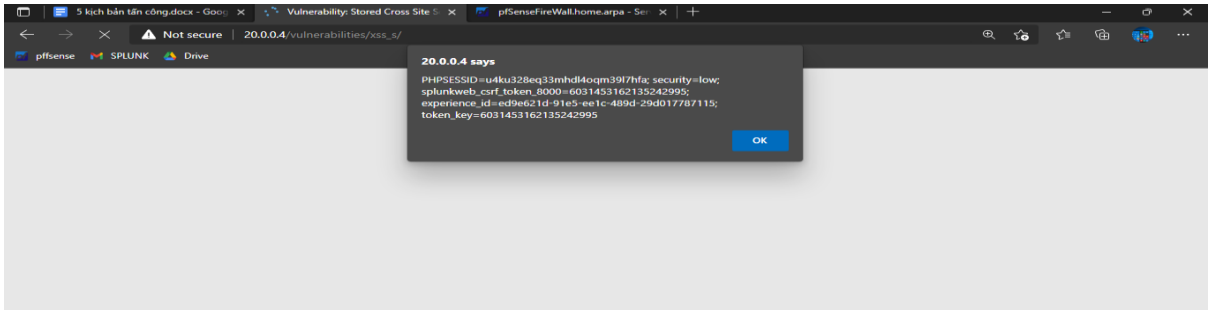
Hình 4.43: Tấn công vào phpmyadmin bằng từ khóa OR



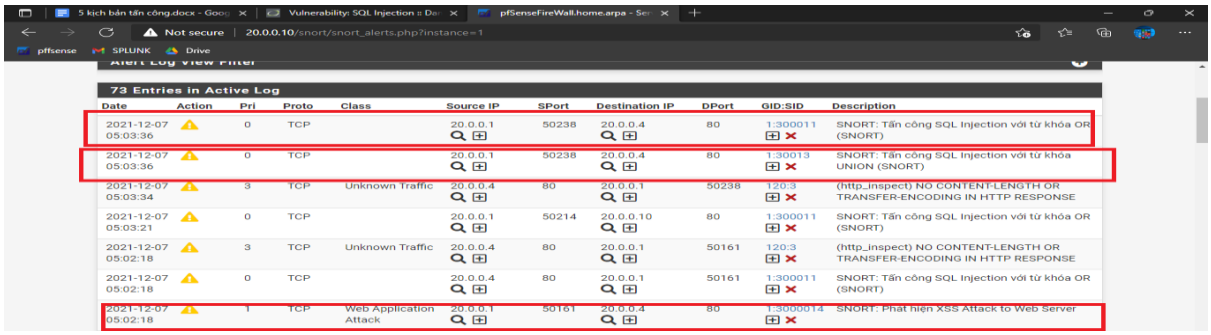
Hình 4.44: Tấn công phpmyadmin bằng từ khóa O



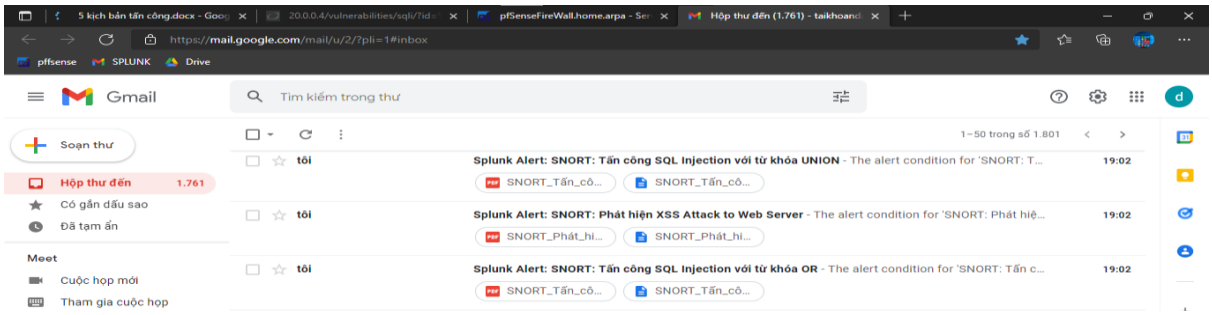
Hình 4.45: Tấn công XSS lấy cookie người dùng



Hình 4.46: Tấn công XSS lấy cookie người dùng (2)



Hình 4.47: Snort Alert: 2 rule phát hiện ở 2 Web Server và rule phát hiện XSS



Hình 4.48: Mail cảnh báo

Email gửi về admin: SNORT phát hiện được các cuộc tấn công trên, và ghi log, gửi log về splunk, sau đó splunk tiến hành gửi mail cảnh báo tới quản trị viên hệ thống (mail mô tả đầy đủ thông tin về các cuộc tấn công như thời gian, ip máy tấn công, hình thức, loại hình tấn công…)

Các cuộc tấn công này nhằm mục đích kiểm tra khả năng phát hiện tấn công gián điệp trong mạng nội bộ của chi nhánh, bảo vệ sự an toàn cho máy chủ chi nhánh.

Sau khi hoàn thành các hình thức tấn công trên, sử dụng cả 3 máy tấn công DOS vào server DMZ của chi nhánh (20.0.0.4/8) nhằm kiểm tra khả năng bảo vệ của IDS trước các cuộc tấn công DOS từ nội bộ.

Bên cạnh đó còn thực hiện thử nghiệm gián điệp tiến hành tải virus vào máy nội bộ (22.0.0.1/8) với ý định phát tán virus vào mạng nội bộ chi nhánh nhằm phá hoại mạng.

Thử nghiệm này nhằm mục đích kiểm tra khả năng ngăn chặn virus của Snort IDS.

4.4.5.3 Đánh giá kịch bản

Kết quả kịch bản 5 cho thấy được khả năng bảo vệ vùng DMZ chi nhánh huyện của IDS Snort là rất tốt, IDS Snort phát hiện được nhiều cuộc tấn công vào vùng DMZ, ngăn chặn và gửi cảnh báo tới quản trị viên hệ thống.

4.5 Kết luận chương

Thông qua những kịch bản trên, cho thấy hệ thống bảo vệ được cả mạng trong và ngoài doanh nghiệp, vùng mạng nội bộ (các chi nhánh ở huyện) và dùng Datacenter…3 hệ thống IDS bổ sung và tương tác với nhau tạo ra tập luật (Rule) hoàn chỉnh, chặn được DOS, SSH Brute Force, FTP Brute Force, Port Scan…nếu tách riêng 3 hệ thống thì mỗi hệ thống với mỗi điểm yếu riêng sẽ ảnh hưởng tới mạng doanh nghiệp. Khi tích hợp 3 IDS vào một hệ thống, ta được hệ thống tích hợp 3 IDS (Snort, Suricata, Zeek) bảo vệ mạng doanh nghiệp cả trong lẫn ngoài, chống lại nhiều cuộc tấn công, và phát hiện gián điệp….

Qua xây dựng và thực nghiệm, tác giả nhận định hệ thống kết hợp nhiều IDS mang lại hiệu quả toàn diện, bảo vệ tất cả các vùng mạng, với mức bảo vệ chuyên sâu đối

với mô hình mạng doanh nghiệp cỡ lớn. Tuy nhiên, doanh nghiệp phải có đủ nguồn lực về nhân sự, cần người quản trị có kiến thức sâu về các loại IDS, có đủ tài chính cho lĩnh vực công nghệ thông tin. Đặc biệt đối với đơn vị hiện tại của tác giả là Viettel Tây Ninh, góp xây dựng và ứng dụng thực tế trong thời gian tới đảm bảo yêu cầu về bảo mật của đơn vị và mở rộng quy mô trong thời gian tới.

CHƯƠNG 5- KẾT LUẬN

5.1 Về mặt lý thuyết

Luận văn này đã nghiên cứu ba giải pháp IDS mã nguồn mở khác nhau, Snort, Suricata và Zeek, để so sánh với nhau như thế nào về mặt cung cấp bảo mật cho môi trường mạng doanh nghiệp vừa và nhỏ. Snort, Suricata và Zeek là các công cụ IDS mã nguồn mở được thiết lập phù hợp để sử dụng chung. Các sản phẩm mã nguồn mở khác hoặc dựa trên máy chủ hoặc bị giới hạn bằng cách nào đó. Cùng với sự kết hợp với những công cụ có liên quan để tạo nên một hệ thống hoàn thiện hơn.

Ngoài ta, luận văn thực hiện nghiên cứu được các nguy cơ tấn công từ nhiều vùng mạng và dạng tấn công khác nhau và đề xuất được các mô hình mạng cho doanh nghiệp cỡ vừa và nhỏ với Single IDS và Multiple IDS. Từ đó giúp quản trị viên có khả năng ứng dụng nhanh vào mô hình doanh nghiệp của mình.

5.2 Về mặt thực tiễn

Tác giả xây dựng hệ thống quản lý mạng sử dụng Single IDS và Multiple IDS nhằm ứng dụng để tư vấn và triển khai cho nhiều loại doanh nghiệp khác nhau như:

Ba hệ thống phân tích quản lý mạng sử dụng Single IDS kết hợp với các công cụ mã mở khác, để ứng dụng tư vấn cho các doanh nghiệp đối tác của Viettel Tây Ninh trên địa bàn.

Hệ thống Multiple IDS sử dụng 3 công nghệ IDS khác nhau kết hợp để bảo vệ toàn diện cho doanh nghiệp cỡ lớn.

Xây dựng và đề xuất hệ thống quản lý mạng phù hợp với mô hình mạng tại Viettel Tây Ninh, đáp ứng đủ các yêu cầu về bảo mật nhiều lớp, đồng thời dự đoán nhiều nguy cơ bị xâm nhập từ nhiều vùng mạng với nhiều kịch bản tấn công được dự đoán trước.

5.3 Về hạn chế

Việc xây dưng mô hình đang thực hiện trên môi trường giả lập. Do đó việc đánh giá hệ thống có thể chưa hoàn toàn chính xác so với thực tế, mặc dù tác giả xây dựng

nhiều kịch bản nhất có thể xảy ra với số quy mô số lượng 4 máy thật mô phỏng các vùng mạng.

Về quy mô, khi triển khai cho các doanh nghiệp cỡ lớn sẽ gặp các hạn chế về khả năng xử lý dữ liệu lớn, chưa đủ đáp ứng yêu cầu về cân bằn tải (Load Balancing), bộ luật (Rule) của các hệ thống IDS chưa được tích hợp AI (trí tuệ nhân tạo) để Rule có thể tự học và chặn được các hình thức tấn công mới và biến đổi liên tục.

Trong tình hình dịch bệnh, mô hình chưa thực hiện được tất cả tấn công đa dang mà chỉ đang dừng lại ở những cuộc tấn công cơ bản và thường gặp như DoS, điều khiển SSH, Brute-Force, XSS, SQL injection trên Web Server.

5.4 Hướng phát triển

Triển khai hệ thống đa dạng và mềm dẻo. Có thể đan xen hệ thống này vào lồng ghép trong hệ thống kia. Hệ thống dự định sẽ mở rộng thêm nhiều dịch vụ công nghệ thông tin vào như quản lý hệ thống AD, quản lý thêm nhiều server quan trọng và phức tạp hơn.

Hướng tiếp theo của đề tài, áp dụng công nghệ máy học, học sâu, trí tuệ nhân tạo vào hệ thống, đặc biệt là tích hợp máy học vào bộ Rule của các hệ thống IDS nhằm giúp hệ thống có thể tự học qua bộ dữ liệu có sẵn để đủ khả năng phát hiện các hình thức tấn công mới, tinh vi hơn. Hệ thống còn giúp quản trị viên không phụ thuộc các luật có sẵn, không cần update các bộ luật liên tục mà vẫn đảm bảo hệ thống có thể tự phân tích, đánh giá, ngăn chặn, giúp giảm tải cho quản trị viên và chi phí quản trị cho doanh nghiệp.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Blokdyk, G. (November 21, 2020). *Intrusion Prevention Systems A Complete Guide - 2021 Edition.* 5STARCooks.

[2] Blokdyk, G. (September 19, 2019). *Pfsense A Complete Guide - 2020 Edition* . 5STARCooks.

[3] Chapman, C. (November 21, 2020). *Intrusion Prevention Systems A Complete Guide - 2021 Edition* . 5STARCooks.

[4] ERIC, A. (August 24, 2020). *Gestion et Exploitation d'une Solution IPS et IDS: Détection-Prévention d'intrusion, Méthodes de Détection d'Attaque, Comparaison entre IPS et IDS, Implementation de l'IDP-Juniper.* Kindle .

[5] Mehta, D. (Feb 26, 2021). *Splunk Certified Study Guide: Prepare for the User, Power User, and Enterprise Admin Certifications 1st ed. Edition.* Apress.

[6] Miedaner, T. (December 22, 2018). *Open Source Tarpit – Labrea Tarpit Appliance. (Reality Check Series Book 8) Kindle Edition.* Kindle .

[7] Miedaner, T. (February 4, 2017). *Security Incident Detection and Response (Reality Check Series Book 5)* . Kindle .

[8] Miedaner, T. (July 26, 2018). *Open Source IDS and Logging - Generation 2 Suricata And Central Syslog Appliance (Reality Check Series Book 7) Kindle Edition.* Kindle .

[9] Miedaner, T. (June 16, 2020). *Full Disk Encryption – Still Here (Reality Check Series Book 9) Kindle Edition.* Kindle .

[10] Rosanitsch, S. (Sep 18, 2018). *pfSense 2.4 Starter Guide: Get started with securing your Home Network using Open Source Technology* .

[11] Sadiqui, A. (February 19, 2020). *Computer Network Security 1st Edition* . Wiley-ISTE.

[12] Surber, L. R. (January 31, 2017). *Virtualization Complete: Business Basic Edition (Proxmox-freeNAS-Zentyal-pfSense).* Linux Solutions(LRS-TEK).

[13] Zientara, D. (December 17, 2018). *pfSense 2.x Cookbook: Manage and maintain your network using pfSense, 2nd Edition 2nd Edition, Kindle Edition.* Packt Publishing.

[14] Zientara, D. (May 9, 2018). *Mastering pfSense,: Manage, secure, and monitor your on-premise and cloud network with pfSense 2.4, 2nd Edition.* Packt Publishing.

[15] Zientara, D. (May 9, 2018). *Mastering pfSense,: Manage, secure, and monitor your on-premise and cloud network with pfSense 2.4, 2nd Edition 2nd Edition.* Packt Publishing.