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

Nguyễn Đắc Thời

Chuyên ngành: HỆ THỐNG THÔNG TIN
Mã số: 8480104

TÓM TẮT LUẬN VĂN THẠC SĨ

TP HCM - NĂM 2022

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **TS.ĐÀM QUANG HỒNG HẢI**

(Ghi rõ học hàm, học vị)

Phản biện 1: ……

Phản biện 2: ……..

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

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

Có thể tìm hiểu luận văn tại:

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

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 04 phần như sau:

Chương 1: TỔNG QUAN VỀ AN TOÀN HỆ THỐNG MẠNG VÀ MẠNG VIETTEL TÂY NINH : nghiên cứu về IDS/IPS và các thành phần, phân loại, chức năng. Nghiên cứu về các loại IDS như Snort, Zeek, Suricata và các thành phần, kiến trúc, bộ luật ứng. Nghiên cứu về cách kết hợp các công cụ IDS, các công cụ phân tích, giao diện UI.

Chương 2: CÁC CÔNG NGHỆ AN TOÀN HỆ THỐNG MẠNG: về tình hình nghiên cứu IDS/IPS trên thế giới và trong nước. Các ứng dụng giảm sát hệ thống mạng đang được nghiên cứu và sử dụng trên thế giới.

Chương 3: XÂY DỰNG HỆ THỐNG PHÂN TÍCH QUẢN LÝ MẠNG TRÊN MÃ NGUỒN MỞ, TRIỂN KHAI VỚI CÁC CÔNG NGHỆ IDS KHÁC NHAU: mô phỏng hệ thống mạng Single- IDS, mô phỏng khả năng quản lý, giám sát mạng, so sánh, đánh giá ưu nhược điểm của từng loại IDS Snor, Suricata, Zeek.

Chương 4: XÂY DỰNG HỆ THỐNG QUẢN LÝ MẠNG ĐA LỚP VỚI NHIỀU CÔNG NGHỆ IDS, TRIỂN KHAI TẠI VIETTEL TÂY NINH: xây dựng Multi-IDS cho hệ thống quản lý mạng ứng dụng tại Viettel Tây Ninh.

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

1.1 Các công trình thế giới

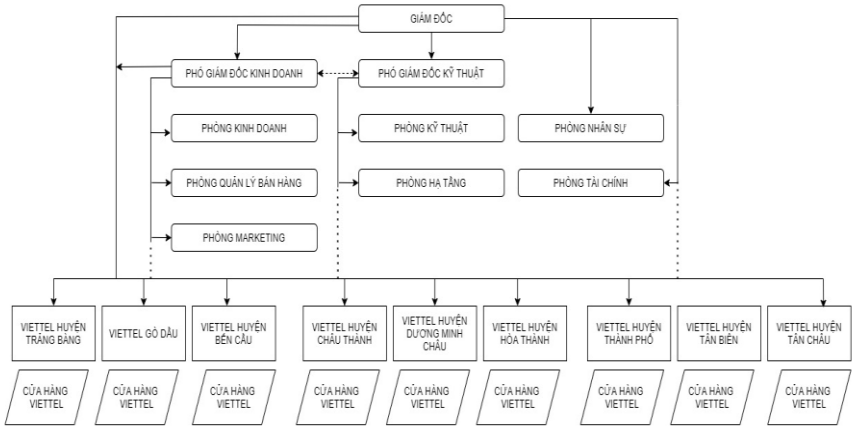
Trong tin học, xâm nhập có nghĩa là truy cập hoặc sử dụng trái phép hệ thống máy tính. Schell và Martin (2006, 180) định nghĩa hành động xâm nhập là "xâm nhập hệ thống máy tính bằng cách phá vỡ bảo mật hoặc khiến nó rơi vào trạng thái không an toàn". Để giám sát và cảnh báo các quản trị viên hệ thống 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.

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.

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.

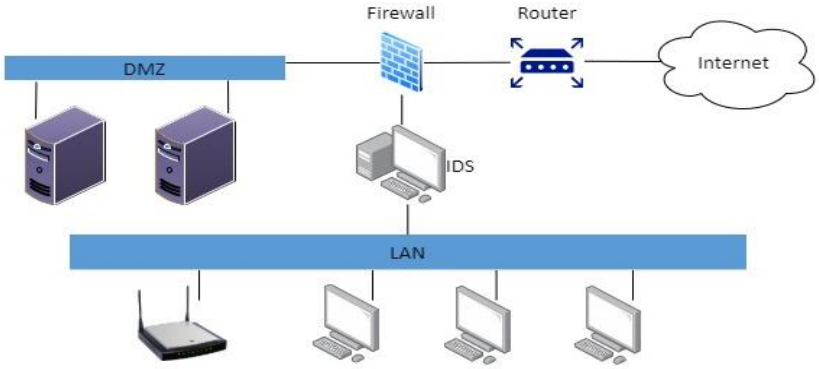
CHƯƠNG 2 - CÁC CÔNG NGHỆ AN TOÀN HỆ THỐNG MẠNG

2.1 Tổng quan hệ thống phát hiện xâm nhập IDS

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

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 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.

2.2.3 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.

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

2.3.1 Pfsnene

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.

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 .

2.4 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.

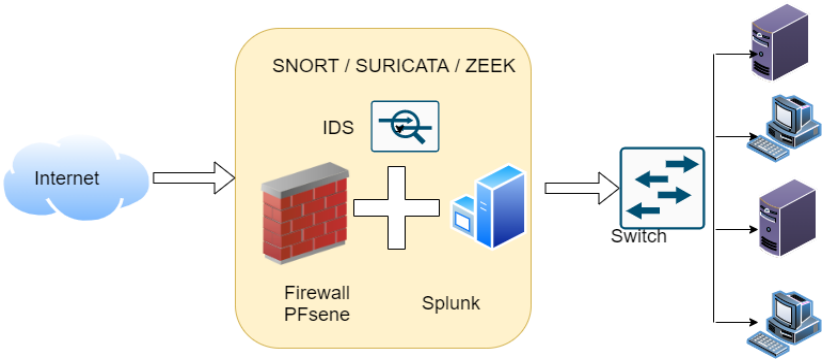
3.2 Phương pháp

- 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

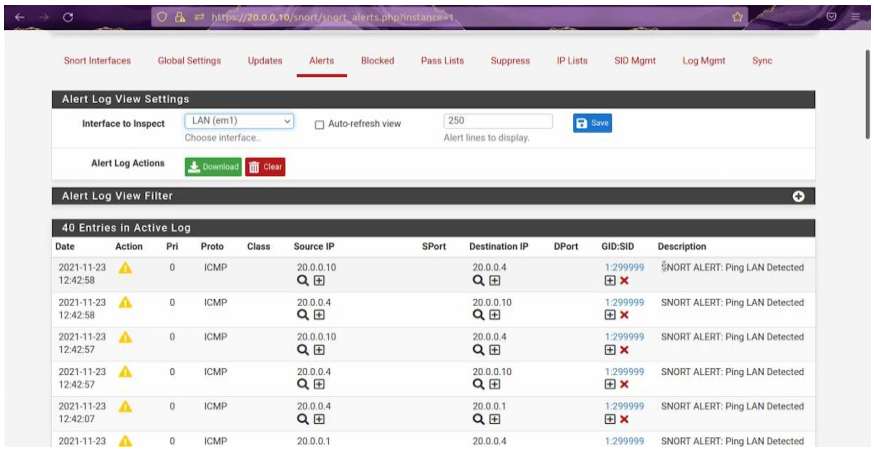
3.4 Thực nghiệm hệ thống IDS

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:

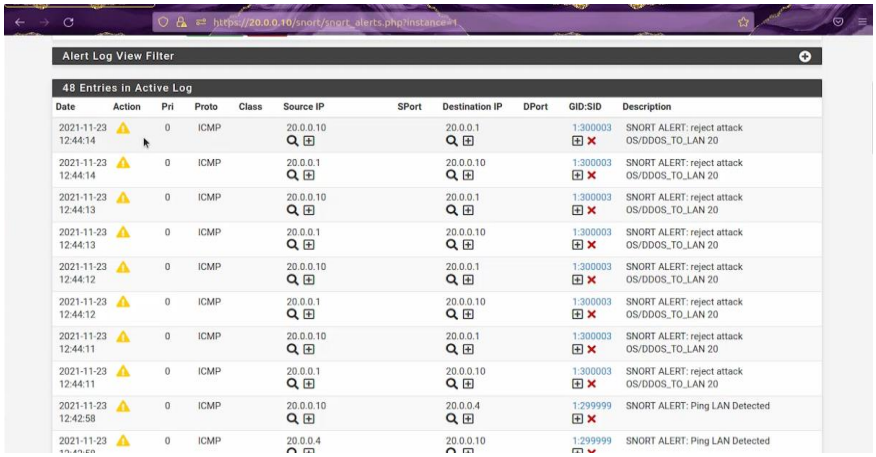
Thực hiện tấn công Scan port /Ping từ máy có địa chỉ 20.0.0.00/8 tấn công vào hệ thống máy chủ có IP là 20.0.0/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



Hình 3.2: Tấn công bằng Ping/Scan port

Thực nghiệm tấn công DOS.

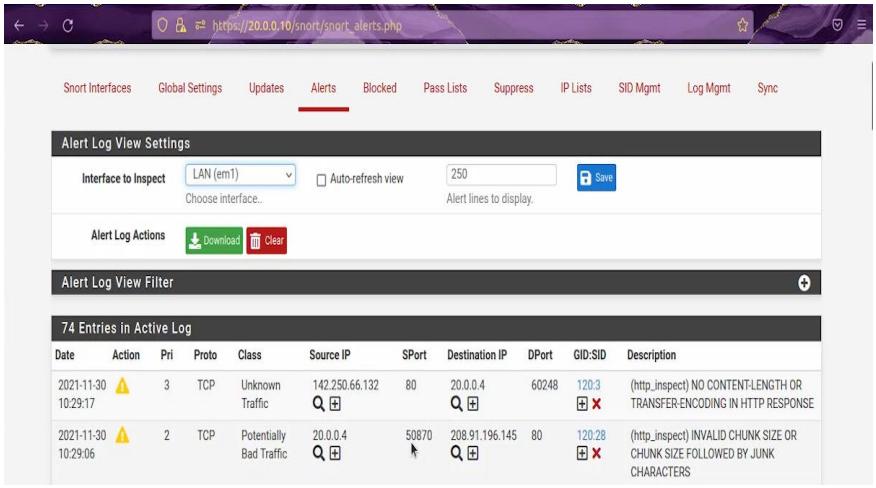
Thực hiện tấn công DOS từ máy có địa chỉ 20.0.00/8, 20.0.0/8, 20.0.0/8… tấn công vào hệ thống máy chủ có IP là 20.0.0/8, 20.0.0/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



Hình 3.3: Tấn công bằng DoS vào LAN

Thực nghiệm phát hiện virut khi sử dụng giao thức HTTP.

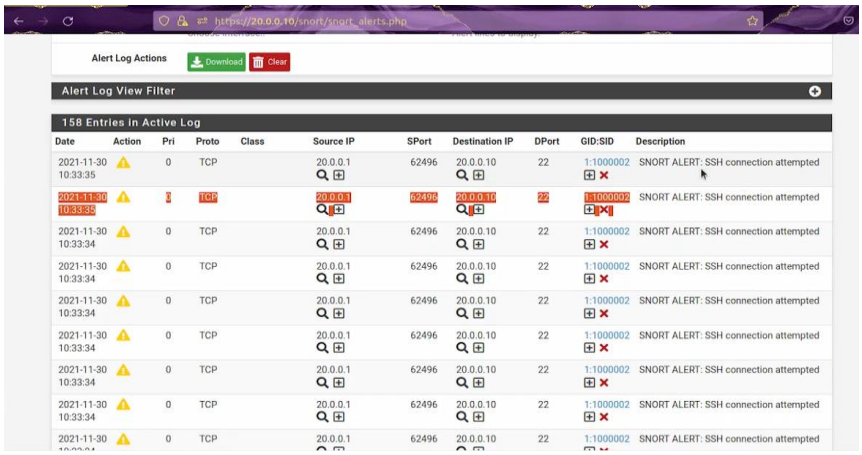
Thực hiện tấn công virut dựa trên giao thức HTTP từ máy có địa chỉ 20.0.0/8, 14250636/16… tấn công vào hệ thống máy chủ có IP là 20.0.0/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:



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 20.0.0/8… tấn công vào hệ thống máy chủ có IP là 20.0.00/8. Sau khi tấn hệ thống Datacenter thì Snort đã phát hiện và cảnh báo:

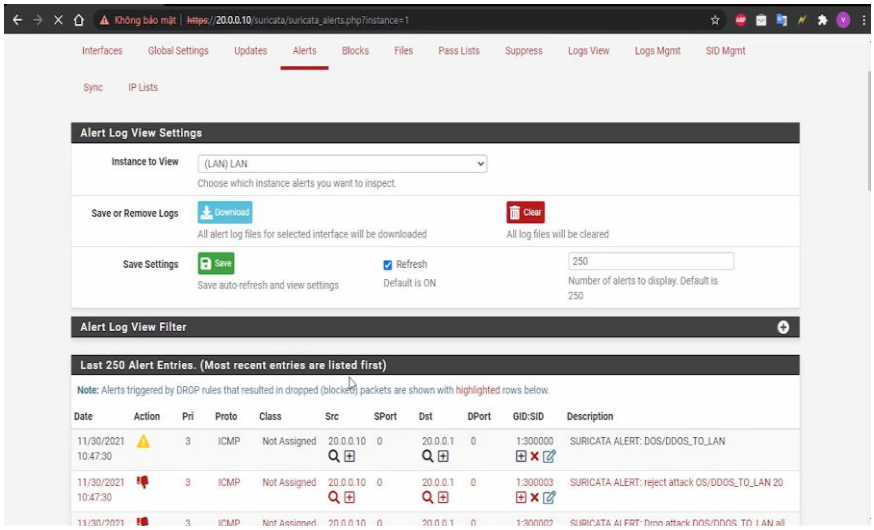


Hình 3.5: Phát hiện SSH connect

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….

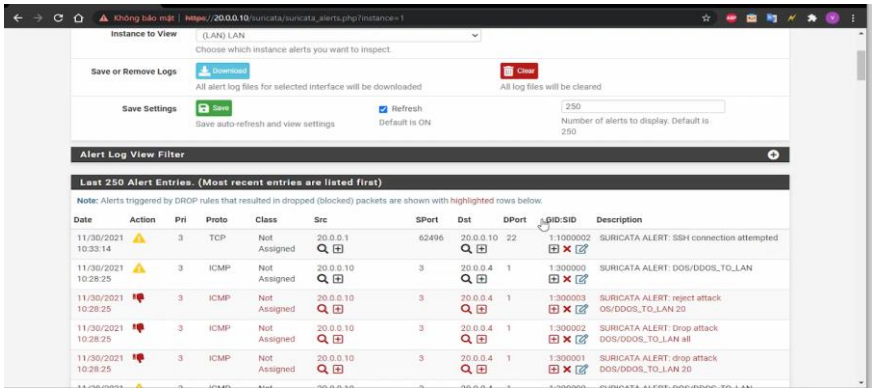
Dưới đây là 4 mô hình thực nghiệm với IDS – Suricata.



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 20.0.00/8, 20.0.0/8… tấn công vào hệ thống máy chủ có IP là 20.0.00/8, 20.0.0/8. 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

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.

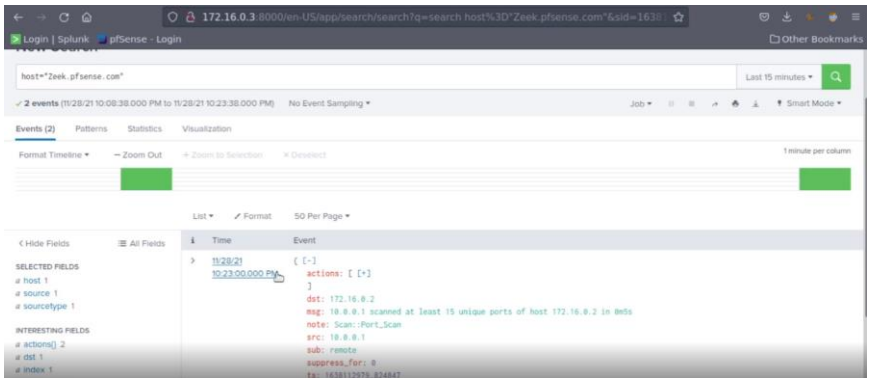
Thực nghiệm tấn công Ping/Scan port:

Thực hiện tấn công Scan port /Ping từ máy có địa chỉ 1726.0/8 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 3.8: Thực nghiệm tấn công port scan đến mạng nội bộ mà zeek giám sát

Hình 3.9: Các cảnh báo lưu tại file /usr/local/logs/current/notice.log



Hình 3.10: Phát hiện port scan trên vùng mạng

3.5 Kết luận

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...

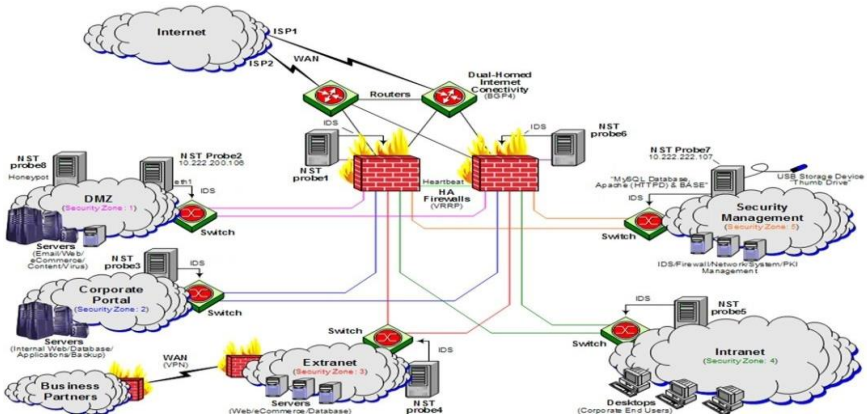
Zeek IDS: hệ thống IDS có giao diện sử dụng là câu lệnh phức tạp, các quy tắc rule phức tạp, nếu sự dụng các rule đơn giản thì rất tiêu tốn thời gian để xử lý. Tuy nhiên ZEEK có thể giám sát chi tiết hệ thống mạng, có phát hiện tất cả những bất lượng của lưu lượng mạng. Khác với Snort và Suricata, Zeek 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,...

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.

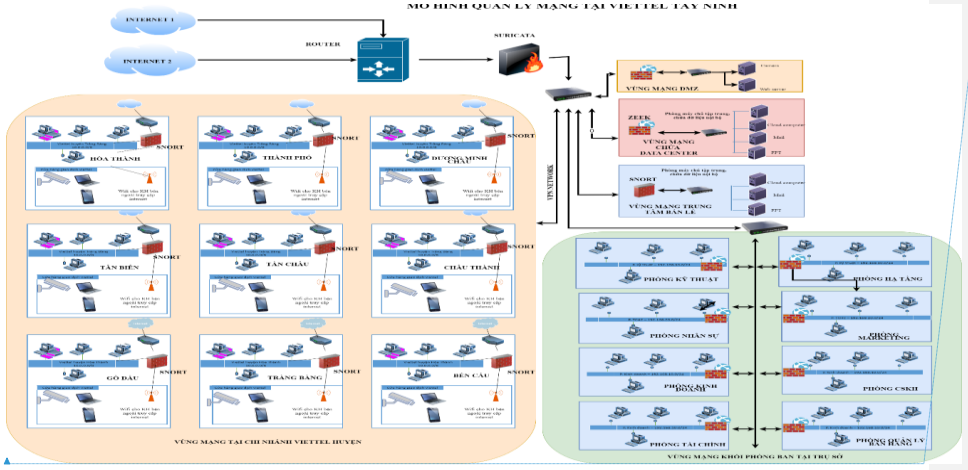
CHƯƠNG 4 - XÂY DỰNG HỆ THỐNG PHÂN TÍCH QUẢN LÝ MẠNG ĐA LỚP VỚI NHIỀU CÔNG NGHỆ IDS - ỨNG DỤNG TẠI VIETTEL TÂY NINH

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.



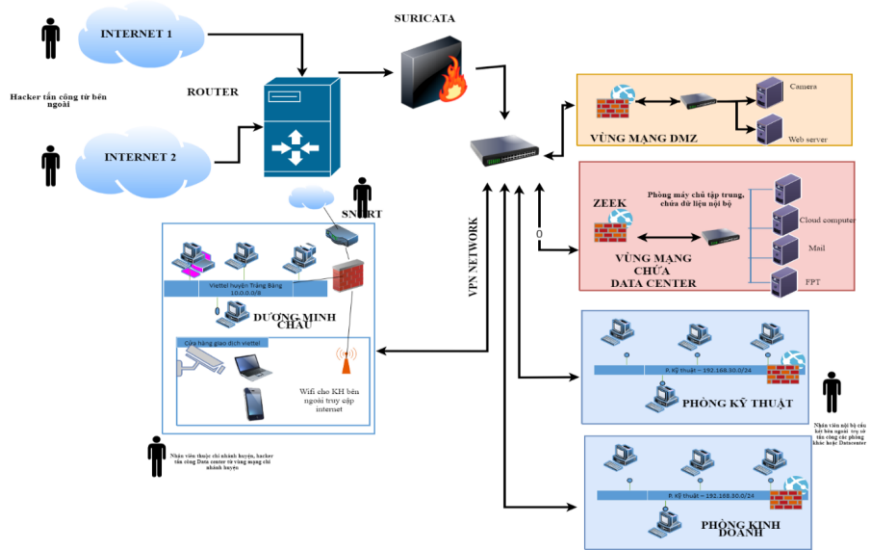
Hình 4.1: Mô hình mạng doanh nghiệp lớn



Hình 4.2: Mô hình mạng Viettel Tây Ninh

Formatted: Not Highlight

4.2 Xây dựng các kịch bản kiểm thử nghiệm tấn công



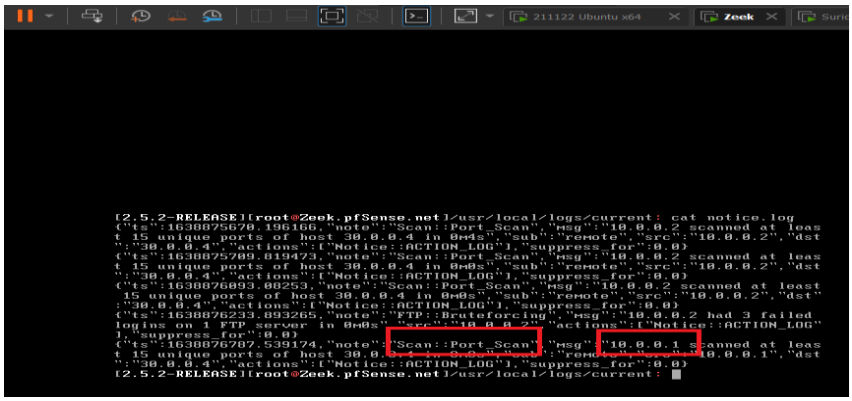
Hình 4.3: Các yêu cầu bảo vệ của mạng ở Viettel Tây Ninh

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

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.

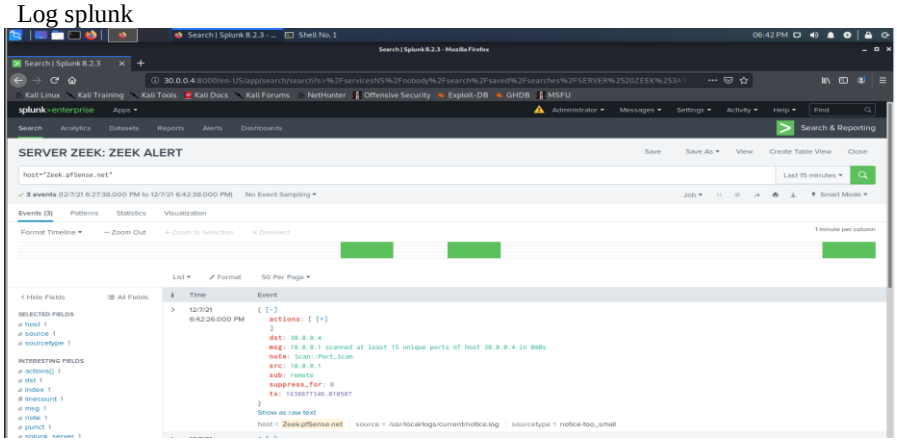
Đánh giá

Qua kịch bản 1, ta thấy được 2 IDS Snort 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.Tấn công được phát hiện và gửi mail tại Zeek server



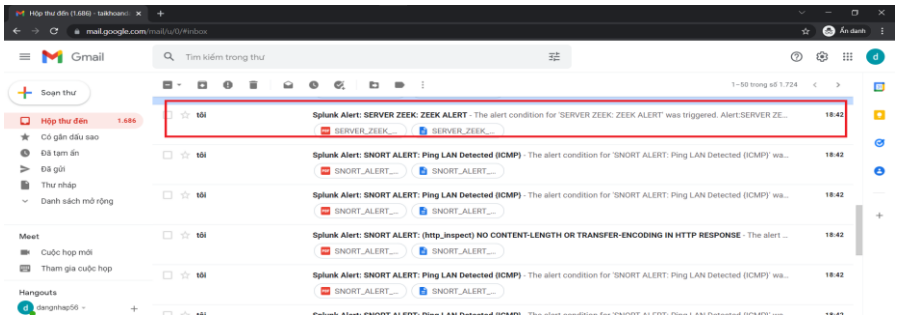
Hình 4.4: Tấn công được phát hiện và gửi mail tại zeek server

Log splunk

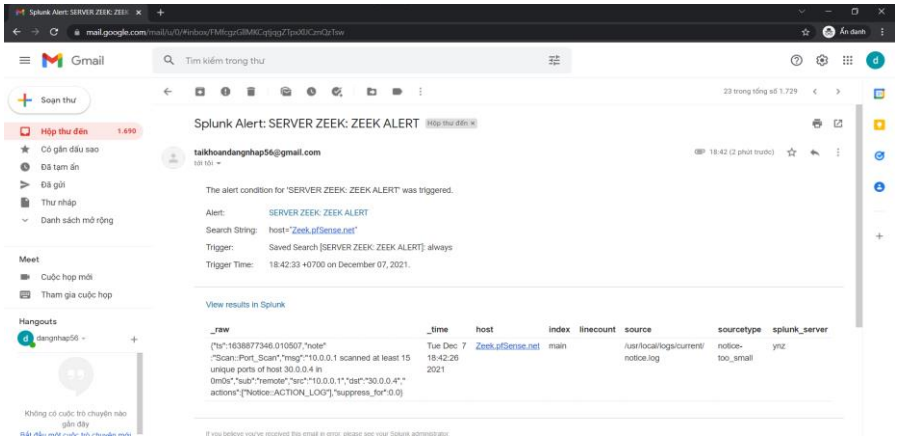


Hình 4.5: Log splunk

- Mail



Hình 4.6: Mail cảnh báo



Hình 4.7: Mail cảnh báo (2)

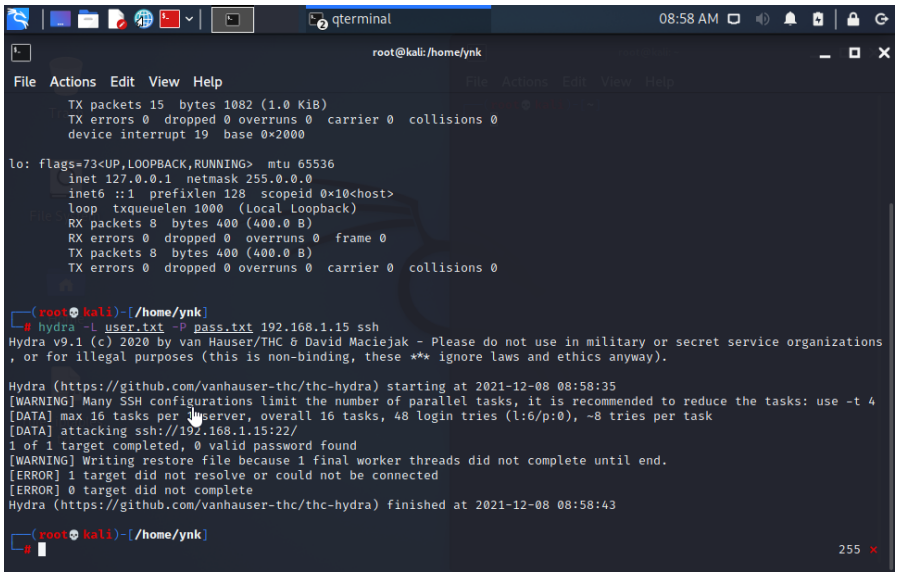
4.2.2 Kịch bản 2: Tấn công từ Internet vào Datacenter

- 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)

Đánh giá

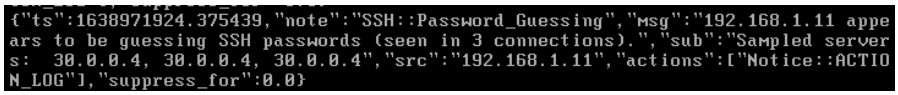
Qua kịch bản 2, ta thấy được khả năng tồn tại tốt của DataCenter trước nhiều cuộc tấn công và khả năng phát hiện tấn công của IDS của trụ sở chính (trụ sở chính có chức năng chặn tấn công từ Internet vào)

➢ Quá trình tấn công



Hình 4.8: Quá trình tấn công

➢ Log IDS



Hình 4.9: 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…"

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

- 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 22.0.0.0/8 và 20.0.0.0/8)Qua đó kiểm tra độ mạnh của hệ thống IDS Snort và IDS Zeek, IDS Suricata

Đánh giá

Sau khi hoàn thành các hình thức tấn công trên, cả 3 máy đồng loạt thực hiện DOS về server trụ sở.

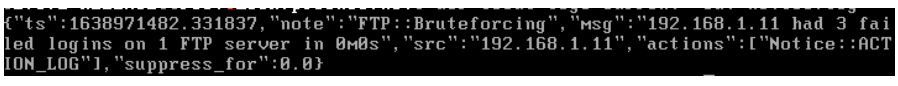
Các cuộc tấn công này nhằm kiểm tra khả năng ngăn chặn các hình thức tấn công gián điệp ngay tại IDS của chi nhánh trước khi luồng dữ liệu tấn công được chuyển về trụ sở.

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.

➢ Quá trình tấn công

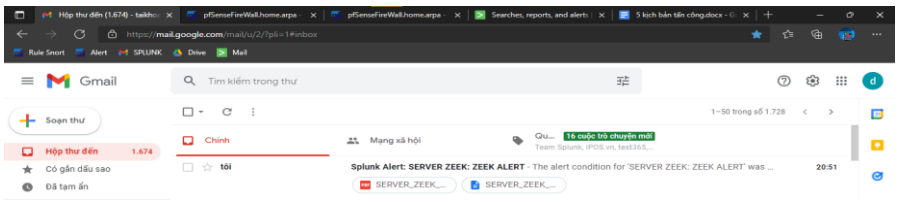
Hình 4.10: Quá trình tấn công

Log IDS



Hình 4.11: 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 4.12: Cảnh báo mail về cho quản trị viên hệ thống

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

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)

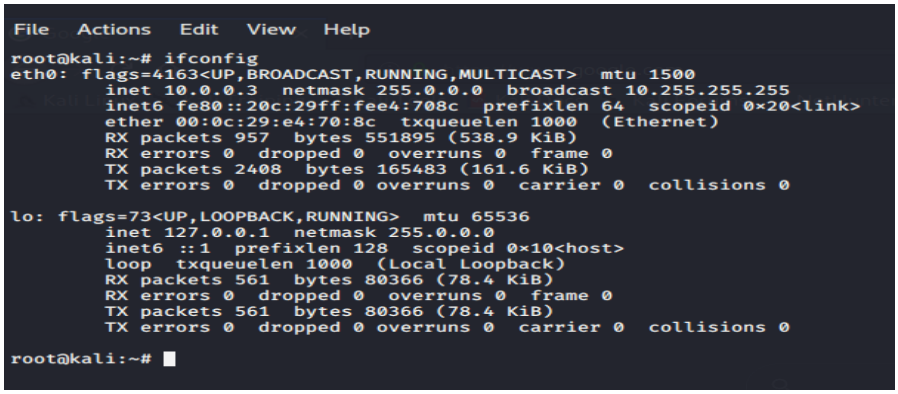
Các cuộc tấn công này nhằm kiểm tra khả năng bảo vệ của IDS trụ sở trước các cuộc tấn công đồng thời từ trong và cả ngoài mạng doanh nghiệp.

Đánh giá

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

- ip máy tấn công



Hình 4.13: Ip máy tấn công

Log của IDS

Hình 4.14: 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…"

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

Nội bộ chi nhánh tấn công vào máy chủ chi nhánh huyện

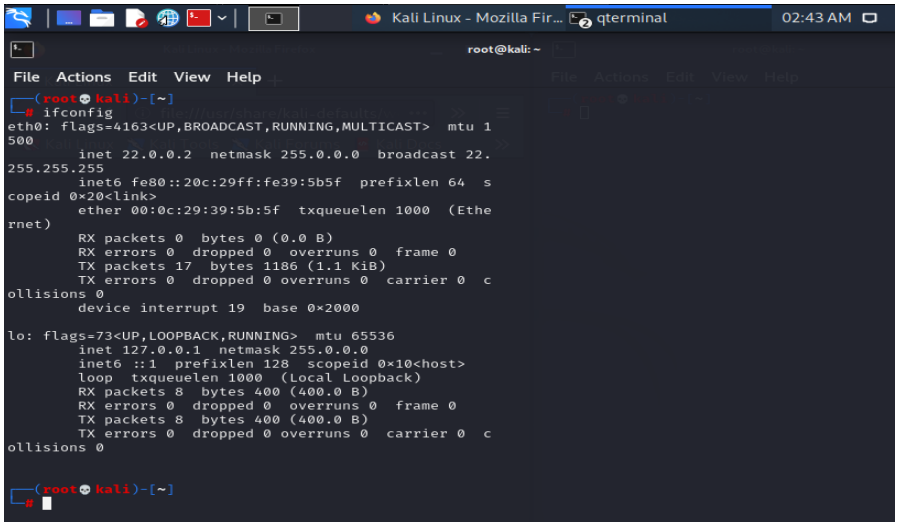
Sử dụng các máy nội bộ 22.0.0.0/8 (22.0.0/8; 22.0.0/8) thuộc vùng mạng nội bộ chi nhánh tấn công vào máy chủ ở vùng DMZ chi nhánh (20.0.0/8)

Máy 22.0.0/8: 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

Đánh giá

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.

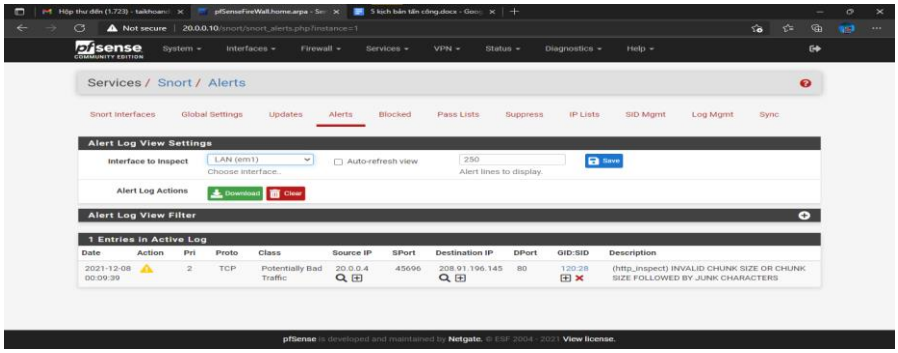


Hình 4.15: Ip máy tấn công

- 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/)

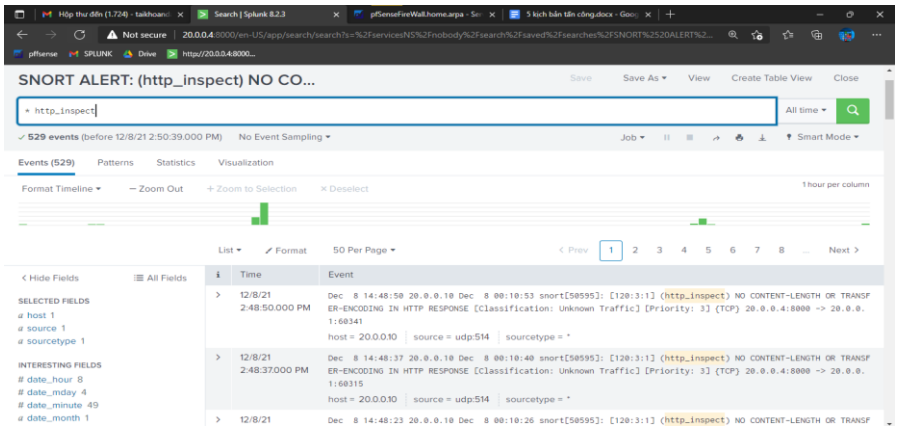
Hình 4.16: Quá trình tấn công

- Log Snort



Hình 4.17: Log ghi lại bởi IDS

- Log Splunk



Hình 4.18: 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…

4.3 Kết luận

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 phần 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 VÀ ĐÁNH GIÁ

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 dựng mô hình đang thực hiện trên môi trường giả lập do quy mô phần cứng chưa kịp thời xây dựng. 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.