

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM
KHOA ĐÀO TẠO CHẤT LƯỢNG CAO**



**BÁO CÁO MÔN ĐỒ ÁN CÔNG NGHỆ THÔNG TIN
ĐỀ TÀI: HỆ THỐNG SIEM**

Thực hiện:

Nguyễn Tuấn Trung - 20161388

Phan Chí Bảo - 20110441

GVHD: Th.S Huỳnh Nguyên Chính

Thành phố Hồ Chí Minh, Tháng 12 năm 2022

MỤC LỤC

CHƯƠNG 1. TỔNG QUAN VỀ TẤN CÔNG VÀ PHÁT HIỆN TẤN CÔNG MẠNG

1.1. TẤN CÔNG TRONG MẠNG MÁY TÍNH

1.1.1. Khái niệm về tấn công mạng.....	2
1.1.2. An toàn mạng	2
1.1.3. Lỗ hổng bảo mật	3
1.1.4. Các kiểu tấn công mạng phổ biến	3
1.1.5. Mô hình tấn công mạng	4
1.1.6. Một số dấu hiệu phát hiện hệ thống bị tấn công	6

1.2. HỆ THỐNG PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP IDS/IPS

1.2.1. Hệ thống phát hiện xâm nhập IDS	7
1.2.2. Network-based IDS	7
1.2.3. Host-based IDS	9
1.2.4. Hệ thống ngăn chặn xâm nhập IPS	11

1.3. HỆ THỐNG GIÁM SÁT AN NINH MẠNG

1.3.1. Giới thiệu hệ thống giám sát an ninh mạng	12
1.3.2. Mô hình giám sát an ninh mạng	12
1.3.3. Các công nghệ giám sát an ninh mạng	12

CHƯƠNG 2. PHÁT HIỆN TẤN CÔNG MẠNG VỚI CÔNG NGHỆ SIEM

2.1. GIỚI THIỆU VỀ CÔNG NGHỆ SIEM

2.1.1. Quản lý nhật ký sự kiện an ninh	15
2.1.2. Tuân thủ các quy định về CNTT	16
2.1.3. Tương quan liên kết các sự kiện an ninh	16
2.1.4. Cung cấp các hoạt động ứng phó	16
2.1.5. Đảm bảo an ninh thiết bị đầu cuối	16

2.2. THÀNH PHẦN VÀ HOẠT ĐỘNG CỦA SIEM

2.2.1. Thiết bị Nguồn	17
2.2.2. Thu thập Log	18
2.2.3. Chuẩn hóa và tổng hợp sự kiện an ninh	19
2.2.4. Tương quan sự kiện an ninh	19
2.2.5. Lưu trữ Log	20
2.2.6. Giám sát và cảnh báo	21

2.3. MỘT SỐ HỆ THỐNG TRIỂN KHAI SIEM	
2.3.1. MARS	22
2.3.2. IBM Qradar	22
2.3.3. Splunk	22
2.3.4. AlienVault OSSIM	23

CHƯƠNG 3. XÂY DỰNG CÔNG CỤ PHÁT HIỆN TẤN CÔNG MẠNG DỰA TRÊN CÔNG NGHỆ SIEM VỚI MÃ NGUỒN MỞ ALIENVAULT OSSIM

3.1. MỤC TIÊU XÂY DỰNG CÔNG CỤ.....	25
3.2. HỆ THỐNG VÀ MÔ HÌNH PHÁT HIỆN TẤN CÔNG MẠNG	
3.2.1. Hệ thống mã nguồn mở AlienVault OSSIM	25
3.2.2. Một số chức năng chính của AlienVault OSSIM	27
3.2.3. Mô hình tổng quan hệ thống phát hiện tấn công mạng dựa trên công nghệ Siem sử dụng công cụ AlienVault OSSIM	28
3.3. TRIỂN KHAI XÂY DỰNG	
3.3.1. Triển khai OSSIM vào hệ thống mạng	29
3.3.2. Một số công cụ được sử dụng trong OSSIM	30
3.3.3. Đánh giá rủi ro	31
3.3.4. Chuẩn hóa log	32
3.3.5. Xây dựng luật trong Ossim	34
3.4. THỬ NGHIỆM VÀ KẾT QUẢ	
3.4.1. Mô hình thử nghiệm thực tế	35
3.4.2. Tấn công thăm dò.....	37
3.4.3. Tấn công đăng nhập	40
3.4.4. Tấn công từ chối dịch vụ	43
3.4.5. Tấn công vào hệ quản trị cơ sở dữ liệu SQL	45
3.4.6. Đánh giá, kết quả	47
KẾT LUẬN	48
TÀI LIỆU THAM KHẢO	50

DANH MỤC TỪ VIẾT TẮT

Stt	Từ viết tắt	Nội dung
01	TCP	Transmission control protocol
02	Dos	Denial of Service (Từ chối dịch vụ)
03	Ddos	Distributed Denial of Service
04	Drdos	Distributed Reflection Denial of Service
05	IDS	Intrusion Detection Systems (Phát hiện xâm nhập)
06	NIDS	Network-based Intrusion Detection Systems
07	HIDS	Host-based Intrusion Detection Systems
08	CNTT	Công nghệ thông tin
09	SIEM	Security Information and Event Management
10	ARP	Address Resolution Protocol
11	CSDL	Cơ sở dữ liệu
12	OSSIM	Open Source Security Information Management
13	IIS	Internet Information Services

LỜI NÓI ĐẦU

Để giảm bớt khó khăn cho các cơ quan, tổ chức vừa và nhỏ trong việc giám sát và bảo vệ hệ thống mạng một cách hiệu quả. Nhóm em đã chọn đề tài ***“Tìm hiểu và xây dựng công cụ phát hiện tấn công mạng dựa trên công nghệ Siem”*** dưới sự hướng dẫn của **Th.S Huỳnh Nguyên Chính**

Đề án gồm 3 chương như sau:

Chương 1: Tổng quan về tấn công và phát hiện tấn công mạng. Khái quát về tình hình an ninh mạng, các kiểu tấn công mạng phổ biến, đi sâu tìm hiểu về hệ thống phát hiện tấn công, mô hình giám sát an ninh mạng đang được áp dụng.

Chương 2: Kỹ thuật phát hiện tấn công mạng với công nghệ Siem. Phân tích thành phần và cách thức hoạt động của Siem. Một số phần mềm ứng dụng công nghệ Siem.

Chương 3: Xây dựng công cụ phát hiện tấn công mạng dựa trên công nghệ Siem. Đưa ra mô hình hệ thống giám sát, phát hiện tấn công thực tế. Xây dựng công cụ phát hiện tấn công mạng dựa trên công nghệ Siem. Cuối cùng là phần đánh giá, kết luận và hướng phát triển của đề tài.

CHƯƠNG 1. TỔNG QUAN VỀ TẤN CÔNG VÀ PHÁT HIỆN TẤN CÔNG MẠNG

1.1. Tấn công trong mạng máy tính

1.1.1. Khái niệm về tấn công mạng

Tấn công mạng là hoạt động có chủ ý của kẻ phạm tội lợi dụng các lỗ hổng của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.

1.1.2. An toàn mạng

An toàn mạng là cách bảo vệ nhằm đảm bảo mọi tài nguyên mạng được sử dụng tương ứng với một chính sách hoạt động được ấn định và với chỉ những người có thẩm quyền tương ứng.

An toàn mạng thường bao gồm: Xác định chính xác các khả năng, nguy cơ xâm nhập mạng, các sự cố rủi ro đối với thiết bị, dữ liệu trên mạng để có các giải pháp phù hợp đảm bảo an toàn mạng.

- Có 4 kiểu vi phạm an toàn mạng

+ Sự phá hoại: Tài nguyên của hệ thống sẽ bị mất đi, không ở trạng thái sẵn sàng hoặc không thể sử dụng được (phần cứng, file dữ liệu, chương trình hoặc làm sai chức năng quản lý của hệ điều hành...)

+ Sự can thiệp: truy cập vào hệ thống sử dụng tài nguyên hệ thống hoặc sao chép chương trình, sao chép dữ liệu trái phép.

+ Sự sửa đổi: Thay đổi giá trị cơ sở dữ liệu, sửa đổi làm chương trình không hoạt động đúng với chức năng, thay đổi dữ liệu đang truyền qua phương tiện điện tử.

+ Sự giả mạo: Giả mạo những đối tượng hợp pháp trong hệ thống

- Các mục tiêu an toàn mạng

Đảm bảo an toàn mạng là nhằm mục đích đảm bảo cho tính đúng đắn, độ tin cậy cao nhất của thông tin được xử lý, đồng thời bảo vệ được các thông tin được lưu trữ trong các cơ sở dữ liệu và thông tin lưu chuyển trên mạng. Một hệ thống được xem

là an toàn chỉ có sự kết hợp của ba đặc tính: Tính bảo mật, tính toàn vẹn và tính sẵn sàng của tài nguyên mạng và các dịch vụ mạng. Vấn đề an toàn thông tin còn thể hiện qua mối quan hệ giữa người sử dụng với hệ thống mạng và tài nguyên mạng.

1.1.3. Lỗ hổng bảo mật

Lỗ hổng bảo mật là những lỗi phần mềm, lỗi trong đặc điểm kỹ thuật và thiết kế, nhưng đa số là lỗi trong lập trình. Các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ở các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows, UNIX; hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng [1].

Phân loại lỗ hổng bảo mật :

- Lỗ hổng loại C: Các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo Dos. Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống. Không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.
- Lỗ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình; Những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến mất hoặc lộ thông tin yêu cầu bảo mật.
- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài có thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

1.1.4. Các kiểu tấn công mạng phổ biến

- Tấn công thăm dò

Kiểu tấn công thăm dò là việc thu thập dữ liệu trái phép về tài nguyên, các lỗ hổng hoặc dịch vụ của hệ thống. Việc thăm dò được thăm dò theo các bước thăm dò thụ

động (thu thập các thông tin được công khai) và thăm dò chủ động(sử dụng các công cụ để tìm kiếm thông tin trên máy tính của nạn nhân) để chuẩn bị các giai đoạn tấn công tiếp theo.

- Nghe trộm (Eavesdropping)

Việc nghe trộm thông tin trên đường truyền có thể được thực hiện bằng việc cài keylog, phần mềm chặn bắt gói tin, phân tích giao thức hay thậm chí là các thiết bị phần cứng hỗ trợ việc “lắng nghe” các thông tin liên lạc trên mạng.

- Tấn công truy cập

Tấn công truy cập là kiểu tấn công giúp người xâm nhập lấy được quyền truy cập trái phép của một hệ thống bảo mật với mục đích thao túng dữ liệu, nâng cao đặc quyền hay đơn giản chỉ là truy cập vào hệ thống.

- Tấn công từ chối dịch vụ

Đây là cách tấn công làm cho hệ thống bị tấn công quá tải không thể cung cấp dịch vụ, làm gián đoạn hoạt động của hệ thống hoặc hệ thống phải nhưng hoạt động.

Mục đích là lợi dụng sự yếu kém của giao thức TCP (Transmission control protocol) để thực hiện tấn công từ chối dịch vụ Dos (Denial of Service), mới hơn là tấn công từ chối dịch vụ phân tán Ddos, mới nhất là tấn công từ chối dịch vụ theo phương pháp phản xạ Ddos.

- Giả mạo (Spoofing)

Trong một số trường hợp, một địa chỉ IP có thể bị giả mạo, kẻ tấn công cũng có thể sử dụng những chương trình đặc biệt để xây dựng các gói tin IP có vẻ như xuất phát từ những địa chỉ hợp lệ thuộc mạng nội bộ của một công ty. Sau khi đoạt được quyền truy cập vào mạng bằng IP hợp lệ, kẻ tấn công có thể thực hiện các ý đồ xấu như sửa đổi, định tuyến lại hay xóa dữ liệu hệ thống.

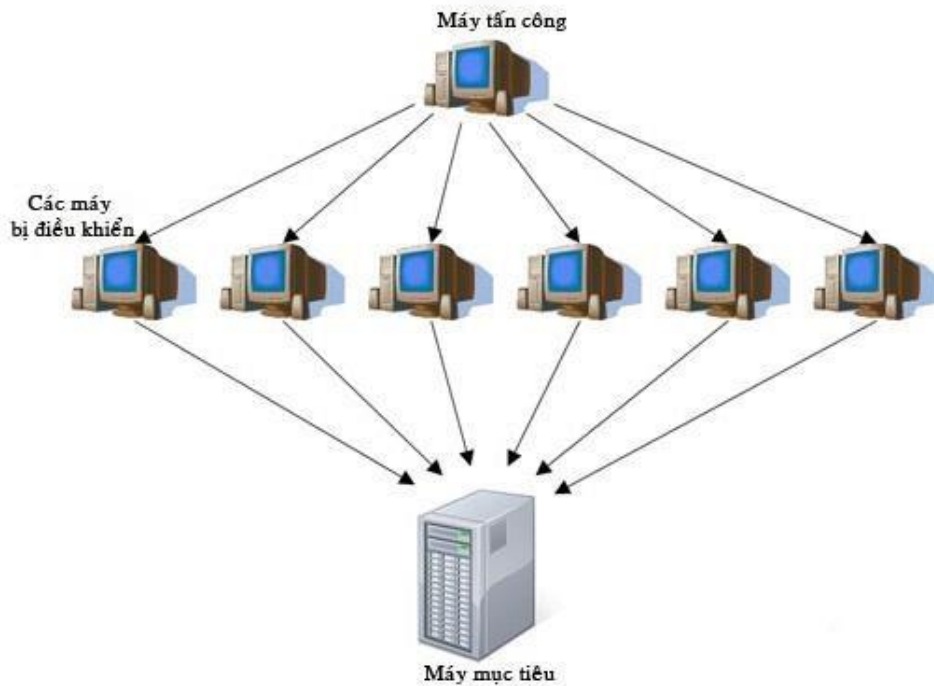
1.1.5. Mô hình tấn công mạng

- Mô hình tấn công truyền thống

Mô hình tấn công truyền thống là mô hình tấn công xuất phát từ một nguồn. từ một đến một hoặc từ một đến nhiều. Có nghĩa là cuộc tấn công xảy ra từ một nguồn gốc.

- Mô hình tấn công phân tán

Mô hình tấn công phân tán sử dụng quan hệ “nhiều đến một” và “nhiều đến nhiều”. Tấn công phân tán dựa trên các cuộc tấn công cổ điển thuộc nhóm từ chối dịch vụ, chính xác hơn là dựa trên các cuộc tấn công như Flood hay Storm (Những thuật ngữ trên có thể hiểu tương tự như “bão”, “Lũ lụt” hay “Thác tràn”)



Hình 1.1: Mô hình tấn công phân tán

- Các bước tấn công mạng



Hình 1.2: Các bước tấn công mạng

Các kiểu tấn công có nhiều hình thức khác nhau, nhưng thông thường đều thực hiện qua các bước như sau:

- + Xác định mục tiêu tấn công, nơi chuẩn bị tấn công.
- + Thu thập thông tin và tìm lỗ hổng
- + Lựa chọn mô hình tấn công và công cụ
- + Thực hiện tấn công
- + Xóa dấu vết: Người tấn công có thể xóa các tập tin log, xóa các cảnh báo từ hệ thống phát hiện xâm nhập. Nhưng ở các giai đoạn thu thập thông tin và dò tìm lỗ hổng trong bảo mật, người tấn công thường làm lưu lượng trong mạng thay đổi khác với lúc bình thường rất nhiều, đồng thời tài nguyên hệ thống bị ảnh hưởng đáng kể.

Những dấu hiệu này rất có ích cho người quản trị mạng có thể phân tích và đánh giá tình hình hoạt động của hệ thống mạng. Hầu hết các cuộc tấn công đều tiến hành tuần tự như các bước đã nêu trên. Làm sao để biết hệ thống mạng đang bị tấn công, xâm nhập ngay từ hai bước đầu tiên là hết sức quan trọng.

1.1.6. Một số dấu hiệu phát hiện hệ thống bị tấn công

- Kiểm tra các dấu hiệu hệ thống có thể bị tấn công: Hệ thống thường bị treo hoặc thường xuyên xuất hiện những thông báo lỗi không rõ ràng.
- Kiểm tra tài khoản người dùng mới trên hệ thống: Một số tài khoản lạ, nhất là ID của tài khoản đó bằng 0.
- Kiểm tra sự xuất hiện các tập tin lạ.
- Kiểm tra thời gian thay đổi trên hệ thống, đặc biệt là các chương trình login.
- Kiểm tra hoạt động của các dịch vụ mà hệ thống cung cấp: Một trong các mục đích tấn công là làm cho tê liệt hệ thống, hình thức tấn công Dos. Sử dụng các tiện ích về mạng để phát hiện nguyên nhân trên hệ thống.
- Kiểm tra truy cập hệ thống bằng các tài khoản thông thường, đề phòng trường hợp các tài khoản này bị truy cập trái phép và thay đổi quyền truy cập mà người sử dụng hợp pháp không kiểm soát được.

- Kiểm tra các tệp tin có liên quan đến cấu hình mạng và dịch vụ. Nên loại bỏ các dịch vụ không cần thiết.

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống.

1.2. Hệ thống phát hiện và ngăn chặn xâm nhập IDS/IPS

1.2.1. Hệ thống phát hiện xâm nhập IDS

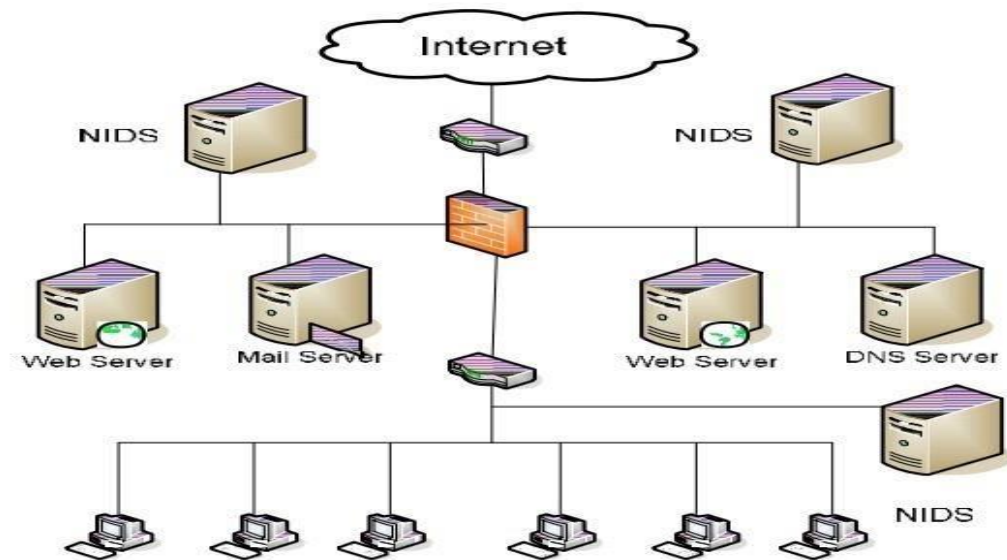
Intrusion Detection Systems (IDS) có thể là một thiết bị phần cứng hoặc phần mềm giúp giám sát máy tính, hệ thống mạng trước các hành động đe dọa đến hệ thống hoặc vi phạm chính sách an ninh và báo cáo lại cho người quản trị hệ thống. Một hệ thống phát hiện xâm nhập cài đặt trên hệ thống mạng giống như một hệ thống cảnh báo chống trộm trong một ngôi nhà.

IDS có thể được phân loại theo chức năng thành 2 loại là Network-based IDS và Host-based IDS. Mỗi loại có một cách tiếp cận riêng biệt để theo dõi và bảo vệ dữ liệu và mỗi loại cũng có những ưu nhược điểm riêng.

1.2.2. Network-based IDS

Hệ thống phát hiện xâm nhập dựa trên mạng hoạt động như một thiết bị độc lập trên mạng. Nó thường được đặt ở các segment mạng hoặc các điểm kết nối giữa các vùng mạng khác nhau. Nhờ đó nó có thể giám sát lưu lượng mạng từ nhiều host khác nhau trong vùng mạng đó.

Về cấu trúc thì NIDS thường bao gồm một tập hợp các cảm biến (sensors) được đặt ở các điểm khác nhau trong hệ thống mạng. Các cảm biến này sẽ thực hiện giám sát lưu lượng mạng, thực hiện phân tích cục bộ lưu lượng mạng đó và báo cáo về cho trung tâm quản lý (Center Management Console).



Hình 1.3: Mô hình triển khai hệ thống NIDS

Một số NIDS: Snort, Suricata, các NIDS của Cisco, Juniper...

Ưu điểm của NIDS:

- Quản lý được cả một network segment (gồm nhiều host). Chi phí thấp vì có thể giám sát cả một hệ thống mạng lớn với chỉ vài thiết bị (mạng được thiết kế tốt).
- Phát hiện và đối phó kịp thời: NIDS phát hiện các cuộc tấn công ngay khi xảy ra, vì thế việc cảnh báo và đối phó có thể thực hiện được nhanh hơn. VD: một hacker thực hiện tấn công DoS dựa trên TCP có thể bị NIDS phát hiện và ngăn chặn ngay bằng việc gửi yêu cầu TCP reset nhằm chấm dứt cuộc tấn công trước khi nó xâm nhập và phá vỡ máy bị hại.
- Có tính độc lập với OS (Operating System).
- Phát hiện được các cuộc tấn công mà HIDS bỏ qua: Khác với HIDS, NIDS kiểm tra header của tất cả các gói tin vì thế nó không bỏ sót các dấu hiệu xuất phát từ đây. Ví dụ nhiều cuộc tấn công DoS, TearDrop (phân nhỏ) chỉ được phát hiện khi xem header của các gói tin lưu chuyển trên mạng.

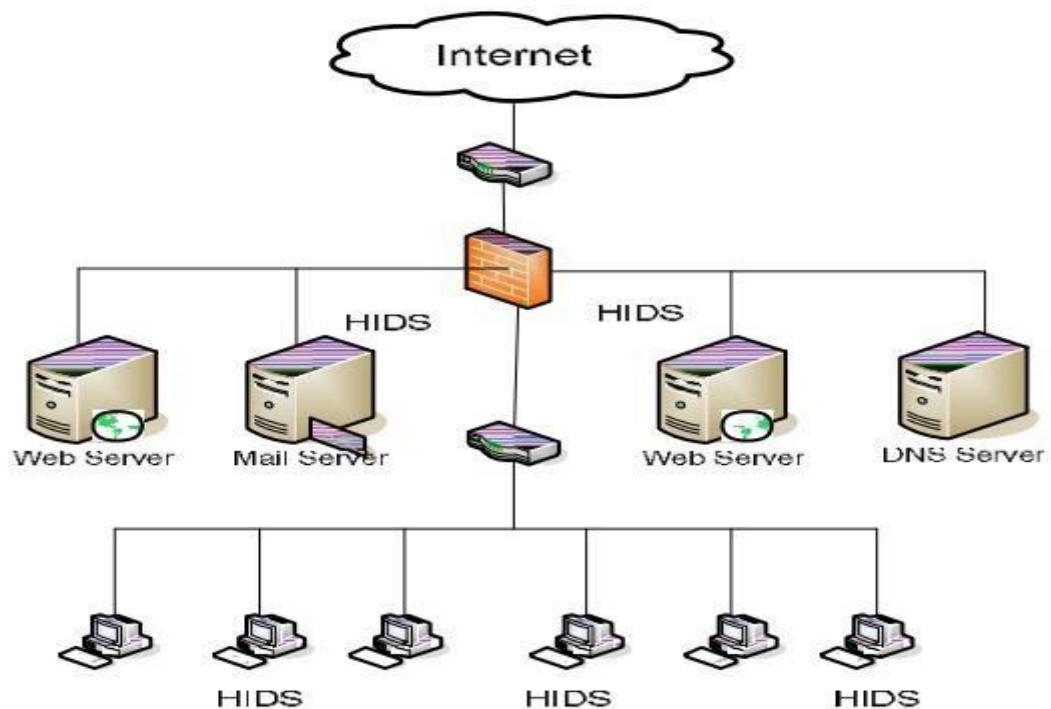
Nhược điểm của NIDS:

- NIDS có thể gặp khó khăn trong việc xử lý tất cả các gói tin trên một mạng có kích thước lớn và mật độ lưu thông cao. Điều này dẫn đến NIDS có thể sẽ không thể phát hiện ra một cuộc tấn công khi mạng đang ở trạng thái over-whelming (quá tải).
- Bị hạn chế bởi switch. Trên các mạng chuyển mạch hiện đại, các switch được sử dụng nhiều để chia mạng lớn thành các segment nhỏ để dễ quản lý. Vì NIDS chỉ kiểm tra trên segment mà nó kết nối trực tiếp nên nó không thể phát hiện tấn công trên một segment khác; dẫn đến việc tổ chức phải mua một số lượng lớn cảm biến nếu muốn bao phủ toàn hệ thống mạng của họ, làm tăng chi phí.
- NIDS không thể phân tích được các thông tin đã bị mã hóa (SSL, SSH...). - Một số hệ thống NIDS có thể gặp khó khăn với dạng tấn công phân mảnh gói dữ liệu (fragmenting packets).
- NIDS không thể phân biệt được một cuộc tấn công thành công hay thất bại. Nó chỉ có thể phân biệt được có một cuộc tấn công đã được khởi xướng. Điều này nghĩa là để biết được cuộc tấn công đó thành công hay thất bại người quản trị phải điều tra các máy chủ và xác định nó có bị xâm nhập hay không.

1.2.3. Host-based IDS

Hệ thống phát hiện xâm nhập dựa trên máy chủ hoạt động trên một máy trạm đơn. HIDS sẽ sử dụng các tài nguyên của máy chủ đó để theo dõi lưu lượng truy cập và phát hiện các cuộc tấn công nếu có. Bằng cách này HIDS có thể theo dõi được tất cả các hoạt động trên host đó như tập tin log và những lưu lượng mạng ra vào host đó. Ngoài ra nó còn theo dõi hệ điều hành, lịch sử sổ sách, các thông điệp báo lỗi của máy chủ.

HIDS cũng thường theo dõi những gì thay đổi trên hệ thống như các thuộc tính của hệ thống tập tin, các thuộc tính (kích thước, vị trí, quyền...) của tập tin, phát hiện tập tin mới được tạo ra hay xóa đi.



Hình 1.4: Mô hình hệ thống HIDS

Một số HIDS: Symantec ESM, OSSEC, Tripwire ...

Ưu điểm của HIDS:

- Giám sát được các hoạt động cụ thể của hệ thống: HIDS có thể giám sát các hoạt động mà NIDS không thể như: truy nhập file, thay đổi quyền, các hành động thực thi, truy nhập dịch vụ được phân quyền. Đồng thời nó cũng giám sát các hoạt động chỉ được thực hiện bởi người quản trị. Vì thế hệ thống HIDS có thể là một công cụ cực mạnh để phân tích các cuộc tấn công có thể xảy ra do nó thường cung cấp nhiều thông tin chi tiết và chính xác hơn một hệ NIDS.
- Có thể ngăn chặn các cuộc tấn công phân mảnh (Fragmentation Attacks). Bởi vậy nên HIDS thường được cài đặt trên các máy chủ xung yếu của tổ chức, các server trong vùng DMZ (do là mục tiêu tấn công chính).
- Không bị ảnh hưởng bởi các thiết bị chuyển mạch (switch).

Nhược điểm của HIDS:

- Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.
- HIDS không thể phát hiện việc quét mạng (network scan bằng nmap) do chỉ giám sát trên host mà nó được cài đặt.
- Có thể bị vô hiệu hóa bởi tấn công từ chối dịch vụ (DoS).
- Chiếm tài nguyên hệ thống: Do cài đặt trên máy cần bảo vệ nên nó sẽ sử dụng tài nguyên của hệ thống như RAM, CPU, Hard Disk dẫn đến có thể làm giảm hiệu suất của việc giám sát.
- HIDS sẽ không hoạt động khi hệ điều hành của host đó lỗi hoặc không hoạt động.

1.2.4. Hệ thống ngăn chặn xâm nhập IPS

Hệ thống ngăn ngừa xâm nhập nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe dọa tấn công bằng việc loại bỏ lưu lượng mạng bất hợp pháp, trong khi vẫn cho phép các hoạt động hợp pháp được tiếp tục.

IPS ngăn chặn các cuộc tấn công dưới những dạng sau:

- Ứng dụng không mong muốn và tấn công kiểu “Trojan horse” nhằm vào mạng và ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và danh sách kiểm soát truy nhập.
- Các tấn công từ chối dịch vụ như “lụt” các gói tin SYN và ICMP bởi việc dùng các thuật toán dựa trên cơ sở “ngưỡng”.
- Sự lạm dụng các ứng dụng và giao thức qua việc sử dụng những qui tắc giao thức ứng dụng và chữ kí.
- Những tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng giới hạn tài nguyên dựa trên cơ sở ngưỡng.

Các sản phẩm IPS không thể nhận biết được trạng thái tầng ứng dụng (chỉ có thể nhận biết được các dòng thông tin trên tầng mạng).

1.3. Hệ thống giám sát an ninh mạng

1.3.1. Giới thiệu hệ thống giám sát an ninh mạng

Hệ thống giám sát an ninh mạng được triển khai tại các hệ thống mạng có độ nhạy cảm cao hoặc có các thông tin cần bảo mật, hoặc cũng có thể đơn giản chỉ là để theo dõi các diễn biến của mạng [8].

1.3.2. Mô hình giám sát an ninh mạng

Về mô hình giám sát an ninh mạng được triển khai có hai dạng chính: Dạng phân tán và dạng hoạt động độc lập.

- Dạng phân tán: Là mô hình mà trong đó có hệ thống xử lý được đặt ở trung tâm và mọi hoạt động của hệ thống như: Các sự kiện, luồng dữ liệu,... sẽ được xử lý tại trung tâm sau đó được hiển thị lên giao diện Website. Đối với mô hình này thường đòi hỏi một sự đầu tư quy mô cả về thiết bị lẫn con người để vận hành hệ thống này.
- Dạng hoạt động độc lập: Đây là mô hình mà hệ thống được xây dựng riêng lẻ cho các đơn vị, và không liên quan tới nhau, có nghĩa là hệ thống hoạt động độc lập. Các nhật ký hệ thống và luồng dữ liệu được trực tiếp thu thập tại mạng con, sau đó đẩy về thiết bị giám sát an ninh mạng và tại đây luồng dữ liệu sẽ được xử lý. Mô hình này phù hợp cho các ngân hàng và đơn vị nhỏ và yêu cầu về đầu tư và lực lượng con người không cao [8].

1.3.3. Các công nghệ giám sát an ninh mạng

- Công nghệ NMS (Network Monitoring Solution) là công nghệ tập trung vào các giải pháp quản lý hiệu suất mạng, giám sát mạng, giám sát tình trạng gói tin, thời gian đáp ứng và số liệu hiệu suất của các thiết bị như router, switch, các máy chủ... NMS phân tích bằng thông tiêu thụ bởi người sử dụng và các ứng dụng thông qua NetFlow, Sflow, jFlow, FIX ... và đưa ra biểu đồ.

Thu thập, phân tích các bản ghi từ tường lửa.

Quản lý các địa chỉ IP sẽ cấp và đã được cấp. Theo dõi các cổng switch và các thiết bị kết nối với nó trong thời gian thực.

Quản trị qua giao diện web và Thiết lập các ngưỡng với nhiều cấp để đưa ra cảnh báo.



Hình 1.7: Giao diện web của một phần mềm NMS

NMS tối đa hóa độ sẵn sàng cho hệ thống bằng cách giám sát tất cả các thiết bị hoạt động trong hệ thống mạng, bao gồm máy chủ, máy trạm, thiết bị mạng và các ứng dụng. Khi có sự cố, NMS sẽ tự động cảnh báo để nhà quản trị có giải pháp kịp thời. Một số sản phẩm NMS của các nhà cung cấp hàng đầu thế giới còn có khả năng khuyến nghị, hướng dẫn các bước cho nhà quản trị khắc phục sự cố. Giải pháp do hệ thống đưa ra có thể không chính xác 100% vì chỉ là tập hợp kinh nghiệm của các chuyên gia hàng đầu thế giới trong cùng lĩnh vực, nhưng chúng cũng góp phần giảm thiểu thời gian tìm kiếm giải pháp, đặc biệt với các nhà quản trị chưa có nhiều kinh nghiệm.

- Công nghệ Siem

CHƯƠNG 2. PHÁT HIỆN TẤN CÔNG MẠNG VỚI CÔNG NGHỆ SIEM

2.1. Giới thiệu về công nghệ Siem

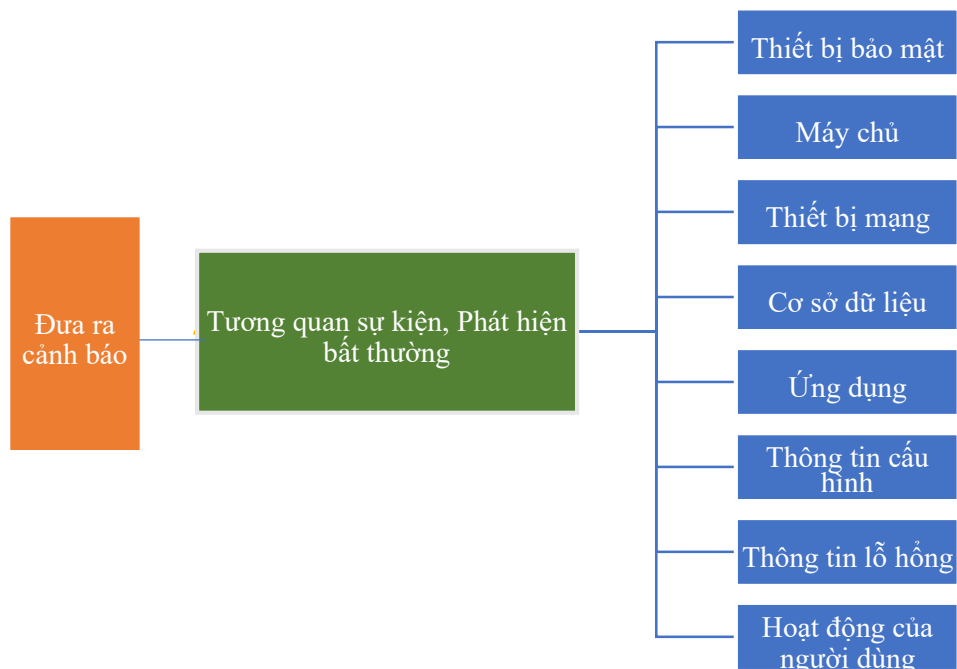
Một số giải pháp trước khi công nghệ Siem ra đời:

- Giải pháp quản lý an ninh thông tin - Security information management (SIM)

SIM là giải pháp công nghệ đầu tiên trong các giải pháp giám sát an ninh mạng. Ban đầu giải pháp SIM chỉ có khả năng lưu trữ các nhật ký sự kiện an ninh cho các hệ thống mạng (đây cũng là một trong các chức năng chính của giải pháp giám sát an ninh hiện nay). Hạn chế của giải pháp này là không có khả năng phân tích các sự kiện an ninh mà chỉ thực hiện việc lưu trữ chúng.

- Giải pháp quản lý các sự kiện an ninh - Security event management (SEM).
- Giải pháp quản lý đăng nhập - Log Management System (LMS): là một hệ thống thu thập và lưu trữ tập tin đăng nhập (từ hệ điều hành, ứng dụng, ...vv). Thông tin tập trung được thu thập từ nhiều nguồn. Người quản trị thay vì phải kiểm tra từng hệ thống riêng lẻ thì quản trị tập trung tại một điểm duy nhất.
- Tương quan sự kiện an ninh - Security Event Correlation (SEC): là giải pháp tương quan các sự kiện an ninh thu thập được theo các quy tắc đã cài đặt nhằm tăng hoặc giảm mức cảnh báo đối với một sự kiện an ninh.
- Giải pháp quản lý thông tin và sự kiện an ninh - Security information and event management (SIEM) là sự kết hợp của các giải pháp nêu trên. SIEM cung cấp việc tích hợp dữ liệu quản lý file log từ nhiều nguồn, bao gồm cả mạng, máy chủ, cơ sở dữ liệu, ứng dụng, cung cấp khả năng hợp nhất dữ liệu để tránh mất các sự kiện quan trọng. [9]

Giải pháp Quản lý và phân tích sự kiện an toàn thông tin là giải pháp toàn diện và hoàn chỉnh, cho phép các cơ quan, tổ chức thực hiện việc giám sát các sự kiện an toàn thông tin cho một hệ thống.



Hình 2.1: Hệ thống phát hiện tấn công mạng

SIEM cung cấp các dịch vụ sau:

- Quản lý nhật ký sự kiện an ninh (Log management).
- Tuân thủ các quy định về CNTT (IT regulatory compliance).
- Tương quan liên kết các sự kiện an ninh (Event correlation).
- Cung cấp các hoạt động ứng phó (Active response).
- Đảm bảo an ninh thiết bị đầu cuối (Endpoint security).

2.1.1. Quản lý nhật ký sự kiện an ninh

SIEM quản lý Log từ các thiết bị trong hệ thống. Bắt đầu với việc cấu hình các vị trí quan trọng trong hệ thống để gửi các sự kiện an ninh vào một cơ sở dữ liệu tập trung. SIEM sẽ chuẩn hóa các Log này về một định dạng duy nhất để phân tích, tương quan liên kết. Sau đó, SIEM lưu trữ các file Log, tổ chức, tìm kiếm và các dịch vụ khác để đáp ứng nhu cầu quản lý mà các tổ chức yêu cầu. Phần quản lý dữ liệu này cũng sử dụng để phân tích về thời gian thực, tình trạng khai thác dữ liệu và an ninh của toàn bộ hệ thống.

2.1.2. Tuân thủ các quy định về CNTT

Nhiều nhà cung cấp SIEM có các tập đóng gói sẵn các quy tắc được thiết kế đặc biệt để đáp ứng các yêu cầu về pháp luật và các quy định khác nhau mà các doanh nghiệp cần phải tuân thủ. Chúng được đóng gói và cung cấp bởi các nhà cung cấp miễn phí hoặc mất phí.

2.1.3. Tương quan liên kết các sự kiện an ninh

Sự tương quan liên kết giữa các sự kiện an ninh mang đem lại thông báo tốt hơn cho hệ thống. Cảnh báo của SIEM giúp chúng ta đưa ra cách ứng phó tùy thuộc vào các điều kiện.

2.1.4. Cung cấp các hoạt động ứng phó

Tất cả các thiết bị cung cấp đầu vào cho SIEM, các quy tắc và bộ lọc sẽ xác định và phân tích mối quan hệ giữa các thông tin đầu vào đó. Chúng ta có thể cấu hình các hành động và thực hiện các phản ứng ứng phó cho tất cả các sự kiện an ninh hoặc có thể cấu hình riêng biệt cho từng loại sự kiện khác nhau.

2.1.5. Đảm bảo an ninh thiết bị đầu cuối

Hầu hết các hệ thống SIEM có thể giám sát an ninh cho các thiết bị đầu cuối để thông báo sự an toàn của hệ thống. SIEM cung cấp việc quản lý cũng như đánh giá tài sản các thiết bị. Bên cạnh là việc dò quét lỗ hổng và cập nhật các bản vá. Nhiều hệ thống SIEM có thể theo dõi các thiết bị như PC, server, Firewall. Một số hệ thống SIEM thậm chí có thể quản lý an ninh cho thiết bị đầu cuối, có sự điều chỉnh và hoàn thiện hơn đối với thiết bị an ninh đó trên hệ thống. Như cấu hình Firewall, cập nhật và theo dõi Anti-Virus, chống spyware, chống spam email.

2.2. Thành phần và hoạt động của Siem

Thành phần cơ bản vẫn là thu thập thông tin, phân tích và lưu trữ. Các bản ghi Log được thu thập từ các thiết bị khác nhau và chúng có thể có những định dạng theo từng loại thiết bị. Chúng ta cần thu thập và chuẩn hóa dữ liệu, sau đó tiến hành phân tích từ các dữ liệu này và thực hiện tương quan sự kiện an ninh để đưa tới kết luận có một cuộc tấn công hay không. Việc đưa ra cảnh báo và các báo cáo sẽ được tạo

ra như một kết quả của việc phân tích. Các bản ghi Log được lưu trữ trực tiếp trên SIEM ít nhất vài giờ đồng hồ sau đó chuyển tới nơi lưu trữ lâu dài để phục vụ cho quá trình điều tra hoặc sử dụng sau này.

2.2.1. Thiết bị Nguồn

Hệ điều hành: Microsoft Windows và các biến thể của Linux và UNIX, AIX, Mac OS là những hệ điều hành thường hay được sử dụng. Hầu hết các hệ điều hành về cơ bản công nghệ khác nhau và thực hiện một nhiệm vụ nào đó nhưng một trong những điều mà tất cả đều có điểm chung là chúng tạo ra các bản ghi log. Các bản ghi log sẽ cho thấy hệ thống của bạn đã làm gì: Ai là người đăng nhập, làm những gì trên hệ thống... Các bản ghi log được tạo ra bởi một hệ điều hành về hệ thống và người sử dụng hoạt động sẽ rất hữu ích khi tiến hành ứng phó sự cố an ninh hoặc chẩn đoán vấn đề hay chỉ là việc cấu hình sai.

Thiết bị: Hầu hết các thiết bị là các hộp đen, các quản trị hệ thống không có quyền truy cập trực tiếp vào hệ thống để thực hiện một số việc quản lý cơ bản. Nhưng có thể quản lý các thiết bị thông qua một giao diện. Giao diện này có thể dựa trên web, dòng lệnh hoặc chạy qua một ứng dụng được tải về máy trạm của quản trị viên. Hệ điều hành các thiết bị mạng chạy có thể là một hệ điều hành thông thường, chẳng hạn như Microsoft Windows hoặc phiên bản của Linux, nhưng nó cũng có thể là một hệ điều hành riêng biệt. Ví dụ như một router hoặc switch. Nó phụ thuộc vào nhà cung cấp, chúng ta không bao giờ có thể truy cập trực tiếp vào hệ thống điều hành cơ bản của nó mà chỉ có thể truy cập vào thông qua dòng lệnh hoặc giao diện web được sử dụng để quản lý. Các thiết bị lưu trữ các bản ghi log của chúng trên hệ thống hoặc thường có thể được cấu hình để gửi các bản ghi ra thông qua syslog hoặc FTP.

Ứng dụng: Trong một hệ thống chúng ta có thể có hệ thống tên miền (DNS), dịch vụ cấp phát địa chỉ động (DHCP), máy chủ web, hệ thống thư điện tử và vô số các ứng dụng khác. Các bản ghi ứng dụng chứa thông tin chi tiết về tình trạng của ứng

dụng, ví dụ như thống kê, sai sót, hoặc thông tin tin nhắn. Một số ứng dụng sinh ra bản ghi log sẽ có ích.

Xác định bản ghi log cần thiết: Sau khi xác định các thiết bị nguồn trong hệ thống, chúng ta cần xem xét việc thu thập các bản ghi log từ các thiết bị nào là cần thiết và quan trọng cho SIEM. Một số điểm cần chú ý trong việc thu thập các bản ghi log như sau:

- Thiết bị nguồn nào được ưu tiên.
- Kích thước các bản ghi log sinh ra trong khoảng thời gian nhất định để xác định không gian lưu trữ.
- Tốc độ các thiết bị nguồn này sinh ra các bản ghi log để lựa chọn việc sử dụng đường truyền mạng khi thu thập các bản ghi.
- Cách thức liên kết
- Có cần các bản ghi log theo thời gian thực hay thiết lập quá trình thực hiện tại một thời điểm cụ thể trong ngày.

2.2.2. Thu thập Log

Khi các sự kiện an ninh được gửi đến máy chủ, mức độ ưu tiên sẽ được định dạng theo chuẩn từ 0 đến 5. Người quản trị có thể điều chỉnh các giá trị mặc định thông qua một bảng tiêu chuẩn và chính sách ưu tiên.

Chính sách thu thập thông tin: Có thể thiết lập một chính sách ưu tiên và thu thập ở các bộ cảm biến để lọc và củng cố các thông tin sự kiện an ninh trước khi gửi chúng đến máy chủ. Kỹ thuật này cho phép người quản trị dễ dàng điều tiết sự kiện an ninh và quản lý những thông tin, nếu không sẽ rất nhiều các sự kiện an ninh trong hệ thống mạng làm cho chúng ta lúng túng không biết bắt đầu từ đâu.

Cơ chế thu thập các bản ghi log phụ thuộc vào từng thiết bị và có các phương thức thu thập như sau:

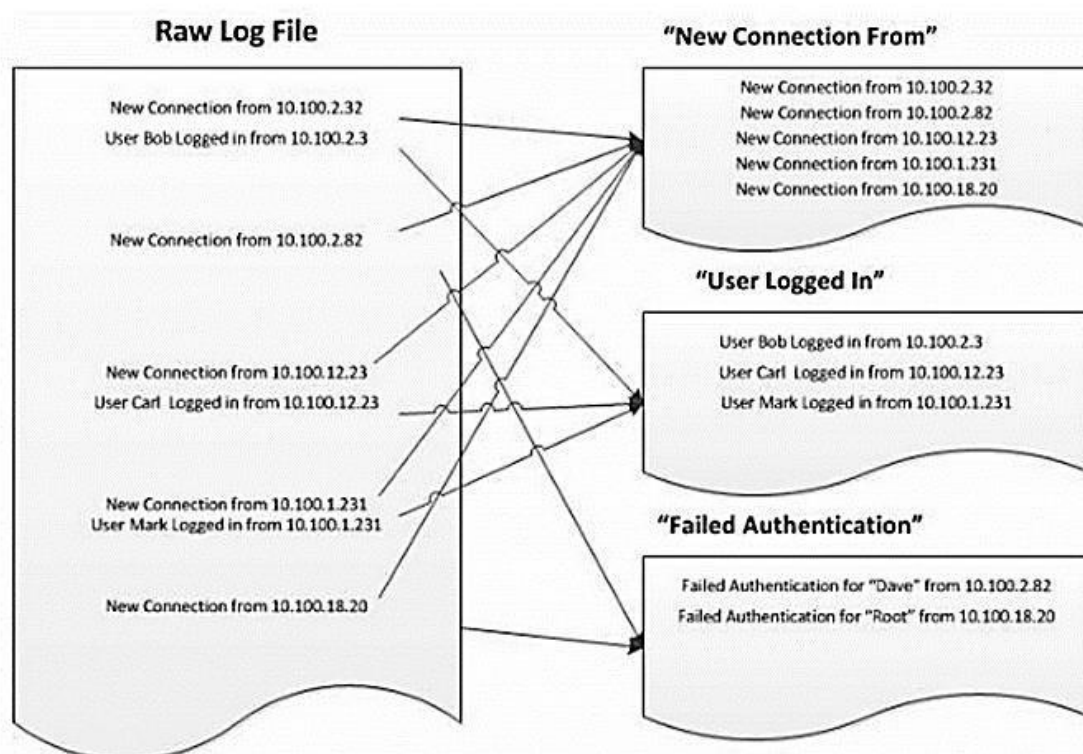
Push log

Pull log

Prebuilt Log collection

Trong trường hợp máy chủ Windows, để làm việc với các bản ghi không chuẩn thì sử dụng Windows Event Log và đưa Windows Event Log vào SIEM.

2.2.3. Chuẩn hóa và tổng hợp sự kiện an ninh



Hình 2.2: Mô tả chuẩn hóa sự kiện

Sau quá trình chuẩn hóa các bản ghi log thì quá trình tổng hợp sự kiện an ninh diễn ra. Mục đích của quá trình này là tổng hợp các sự kiện an ninh thuộc cùng một kiểu để thấy được sự tổng thể của hệ thống. Điều này có vẻ tương tự như với quá trình tương quan sự kiện an ninh nhưng thực sự không phải vậy. Tương quan sự kiện an ninh thì sẽ tổng hợp nhiều sự kiện an ninh khác nhau để đưa ra kết luận có hay không về một cuộc tấn công.

2.2.4. Tương quan sự kiện an ninh

Quá trình tương quan sự kiện an ninh là từ các bản ghi sự kiện an ninh khác nhau được liên kết lại với nhau nhằm đưa ra kết luận có hay không một tấn công vào hệ

thống. Quá trình đòi hỏi việc xử lý tập trung và chuyên sâu vì chúng phải hiểu được một tấn công diễn ra như thế nào.

Tương quan các sự kiện an ninh được thực hiện nhằm đơn giản hóa các thủ tục ứng phó sự cố cho hệ thống, bằng việc thể hiện một sự cố duy nhất được liên hệ từ nhiều sự kiện an ninh đến từ các thiết bị nguồn khác nhau. Chúng ta cần một cách để loại bỏ tất cả các thông tin sự kiện an ninh không liên quan trong các bản ghi log và chỉ cần theo dõi các thông tin sự kiện an ninh có thể chỉ ra một nguy hại qua nhiều sự kiện an ninh. Nó là sự kết hợp của các sự kiện khác nhau nhưng liên quan đến một sự cố duy nhất trong hệ thống. Thông thường có hai kiểu tương quan. Một là dựa trên các quy tắc kiến thức đã biết (Rule - based) và hai là dựa trên phương pháp thống kê (statistical-based).

Rule - based: Đây là phương pháp dựa trên hệ chuyên gia. Tương quan sự kiện dựa trên các quy tắc và kiến thức đã biết về các cuộc tấn công.

Statistical - based: Phương thức tương quan không sử dụng bất kỳ kiến thức của các hoạt động được cho là nguy hiểm đã biết trước đó.

2.2.5. Lưu trữ Log

Có ba cách mà có thể lưu trữ các bản ghi trong SIEM là: Dùng một cơ sở dữ liệu, file Text và dưới dạng file nhị phân.

- Lưu trữ dưới dạng cơ sở dữ liệu

. Cơ sở dữ liệu thường là một nền tảng cơ sở dữ liệu chuẩn như Oracle, MySQL, Microsoft SQL hoặc một trong các ứng dụng cơ sở dữ liệu lớn khác đang được sử dụng trong doanh nghiệp. Phương pháp này cho phép tương tác khá dễ dàng với dữ liệu vì các truy vấn cơ sở dữ liệu là một phần của ứng dụng cơ sở dữ liệu. Hiệu suất cũng khá tốt khi truy cập vào các bản ghi log trong cơ sở dữ liệu, phụ thuộc vào phần cứng cơ sở dữ liệu đang chạy, nhưng các ứng dụng cơ sở dữ liệu phải được tối ưu hóa để chạy với SIEM. Sử dụng cơ sở dữ liệu là một giải pháp tốt cho việc lưu trữ nhật ký.

- Lưu trữ dưới dạng file Text

Nếu các bản ghi log được lưu trữ trong một tập tin văn bản, thì sẽ không khó khăn khi một viết mã của riêng để mở các tập tin và lấy thông tin để cung cấp cho cho một ứng dụng khác. Một lợi ích khác là khi tập tin văn bản con người có thể đọc được và dễ dàng để nhà phân tích tìm kiếm và hiểu nó. Chúng ta có thể mở các tập tin và sử dụng lệnh grep hoặc một số công cụ tìm kiếm tập tin văn bản khác để tìm ra thông tin tìm kiếm mà không cần mở một giao diện điều khiển.

- Lưu trữ dưới dạng file nhị phân

2.2.6. Giám sát và cảnh báo

SIEM có một giao diện điều khiển dựa trên web hoặc ứng dụng tải về máy trạm. Cả hai giao diện sẽ cho phép tương tác với các dữ liệu được lưu trữ trong SIEM. Giao diện điều khiển được sử dụng để quản lý SIEM. Giao diện ứng dụng cho phép xử lý sự cố hoặc cung cấp cái nhìn tổng quan về môi trường của chúng ta.. Nó có thể xử lý tại một nơi duy nhất, phân tích tất cả các bản ghi log khác nhau dễ dàng bởi vì SIEM đã chuẩn hóa các thông tin dữ liệu đó.

SIEM cung cấp ba cách để thông báo tới các quản trị viên khi có một cuộc tấn công hay một hành vi bất thường đang xảy ra. Thứ nhất, SIEM có thể đưa ra một cảnh báo ngay khi chúng nhận ra rằng có điều gì bất thường. Thứ hai, SIEM sẽ gửi một thông báo vào một thời điểm được xác định trước của cuộc tấn công và thứ ba là các quản trị viên theo dõi giám sát SIEM theo thời gian thực thông qua một giao diện web. Các IDS thông thường đưa ra nhiều cảnh báo giả nhưng với SIEM tạo ra một tỷ lệ nhỏ các thông báo giả như vậy. Tuy nhiên tất cả những thông báo có thể là cần thiết để thực hiện một hành động hay đơn giản là bỏ qua nó còn tùy thuộc vào mức độ của sự kiện an ninh.

Báo cáo được lập lịch để đưa ra các báo cáo thường xuyên, được thể hiện theo chuẩn quốc tế và có thể thể hiện qua những biểu đồ trực quan, tổng thể về những số liệu.

2.3. Một số hệ thống triển khai Siem

2.3.1. MARS

Hệ thống theo dõi, giám sát và ứng phó (MARS - Monitoring Analysis and Response System) là một sản phẩm triển khai SIEM được sản xuất bởi Cisco. MARS là một sản phẩm thương mại rất được ưa chuộng trong việc triển khai SIEM.

Khi triển khai một cách chính xác thì MARS có thể:

- Xác định một cuộc tấn công nào được tiến hành.
- Hiện thị các thông tin chi tiết và mạng hay đường dẫn liên quan đến sự việc.
- Xác định các thiết bị có thể sử dụng để ngăn chặn các cuộc tấn công.
- Trong nhiều trường hợp nó có thể cung cấp các lệnh cụ thể áp dụng cho các thiết bị để ngăn chặn các cuộc tấn công.

2.3.2. IBM Qradar

Hệ thống QRadar đáp ứng yêu cầu tuân thủ để lưu trữ sự kiện an ninh, giám sát, báo cáo và bao gồm các chức năng sau đây để thực hiện yêu cầu an ninh bảo mật của tổ chức:

- Khả năng hiển thị theo thời gian thực
- Giảm cảnh báo giả vào ưu tiên các cảnh báo chính xác
- Quản lý các mối đe dọa một cách hiệu quả
- Cung cấp thông tin bảo mật trong môi trường điện toán đám mây
- Báo cáo các hoạt động và truy cập dữ liệu chi tiết
- Cung cấp giao diện theo dõi, quản trị đầy đủ

2.3.3. Splunk

Splunk là một phần mềm giám sát mạng dựa trên sức mạnh của việc phân tích Log.

Splunk thực hiện các công việc tìm kiếm, giám sát và phân tích dữ liệu logs lớn được sinh ra từ các ứng dụng, các hệ thống và các thiết bị hạ tầng mạng. Nó có thể thao tác tốt với nhiều loại định dạng dữ liệu khác nhau (Syslog, csv, apache-log,

access_combine ...). Splunk được xây dựng dựa trên nền tảng Lucene and MongoDB với một giao diện web rất trực quan [13].



Hình 2.4: Giao diện Web của Splunk

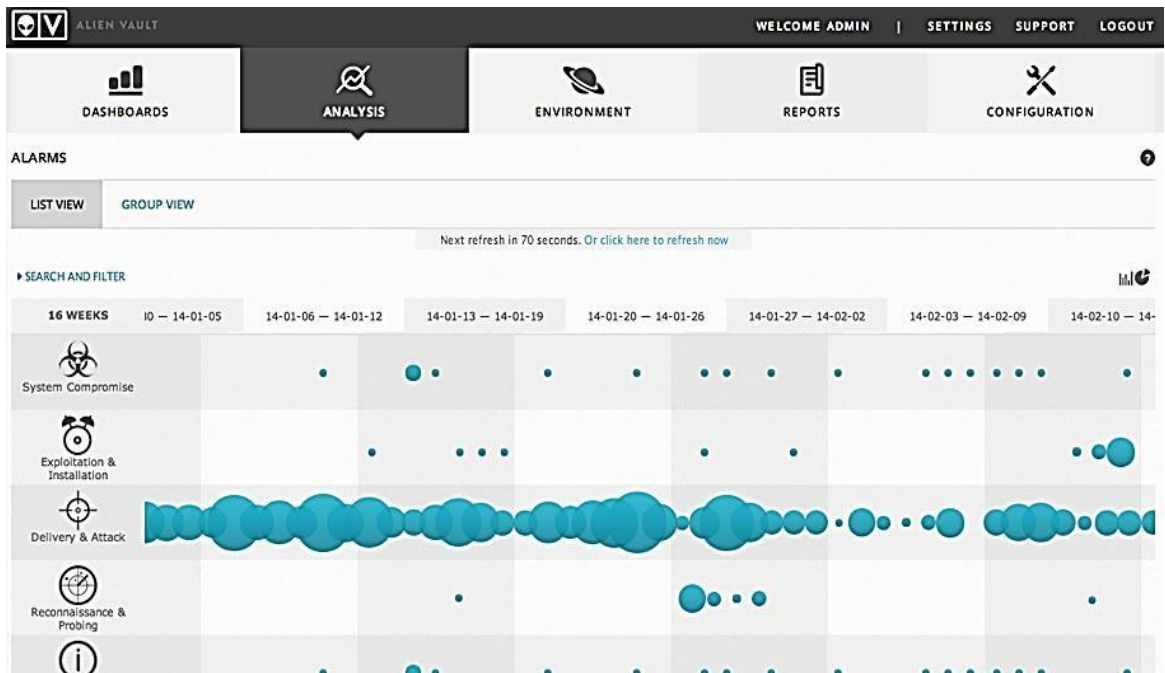
2.3.4. AlienVault OSSIM

OSSIM (Open Source Security Information Management) là một giải pháp SIEM và OSSIM là hệ thống giám sát an ninh mạng dựa trên nền tảng mã nguồn mở.

OSSIM thực hiện việc thu thập các sự kiện từ rất nhiều các thiết bị khác nhau như Firewall, IDS/IPS, các máy chủ, máy trạm,...trong hệ thống giám sát, từ các sự kiện có thể đưa ra các cảnh báo (alert) khác nhau.

Các sự kiện thu thập được từ nhiều nguồn khác nhau sau đó sẽ được OSSIM phân tích để tìm ra mối liên hệ giữa các sự kiện khác nhau và đưa ra được những thông tin tổng hợp nhất có liên quan đến an ninh trong hệ thống.

Những thông tin OSSIM sau khi đã được phân tích, tổng hợp sẽ được đưa vào báo cáo cụ thể, nó là kết quả đánh giá về mức độ an ninh trong hệ thống được giám sát [11].



Hình 2.5: Báo cáo của AlienVault OSSIM

CHƯƠNG 3. XÂY DỰNG CÔNG CỤ PHÁT HIỆN TẤN CÔNG MẠNG DỰA TRÊN CÔNG NGHỆ SIEM VỚI MÃ NGUỒN MỞ ALIENVAULT OSSIM

*** Đặc tả:**

SIEM thực hiện việc xử lý nhật ký và các sự kiện an ninh được gửi về từ các thiết bị các thiết bị mạng, các máy chủ (Server), các ứng dụng. SIEM giúp theo dõi sự kiện an ninh của hệ thống và thực hiện các hành động bảo vệ an toàn hệ thống. Nó gồm 2 thành phần chính thu thập nhật ký, thành phần phân tích nhật ký. SIEM là biện pháp tổng quan về giải pháp an toàn mạng hiện nay.

Thiết lập và hoàn thiện các luật sao cho hệ thống có thể phát hiện được hầu hết các kiểu tấn công mạng.

Bổ sung hoạt động ứng phó tự động cho các cảnh báo tấn công

3.1. Mục tiêu xây dựng công cụ

Nhận thấy khả năng triển khai hệ thống giám sát an ninh mạng của các cơ quan tổ chức nhỏ tại Việt Nam còn hạn chế cả về thiết bị lẫn nhân lực và hệ thống mã nguồn mở OSSIM là giải pháp dễ dàng triển khai và tiết kiệm chi phí nhất mà vẫn đảm bảo phòng chống và phát hiện tốt trước các cuộc tấn công. Tuy nhiên hệ thống cần phải xây dựng các công cụ, các luật phù hợp nhất với mạng cụ thể để hệ thống đưa ra các cảnh báo chính xác nhất và hạn chế tối đa cảnh báo giả.

Thiết lập các luật để hệ thống có thể phát hiện ra các kiểu tấn công như: Tấn công đăng nhập, tấn công dò quét cổng, tấn công vào lỗ hổng ứng dụng Web, phát hiện ra máy trạm nằm trong mạng lưới botnet nhằm thực hiện tấn công DDOS, phát hiện ra tấn công từ nội bộ ...

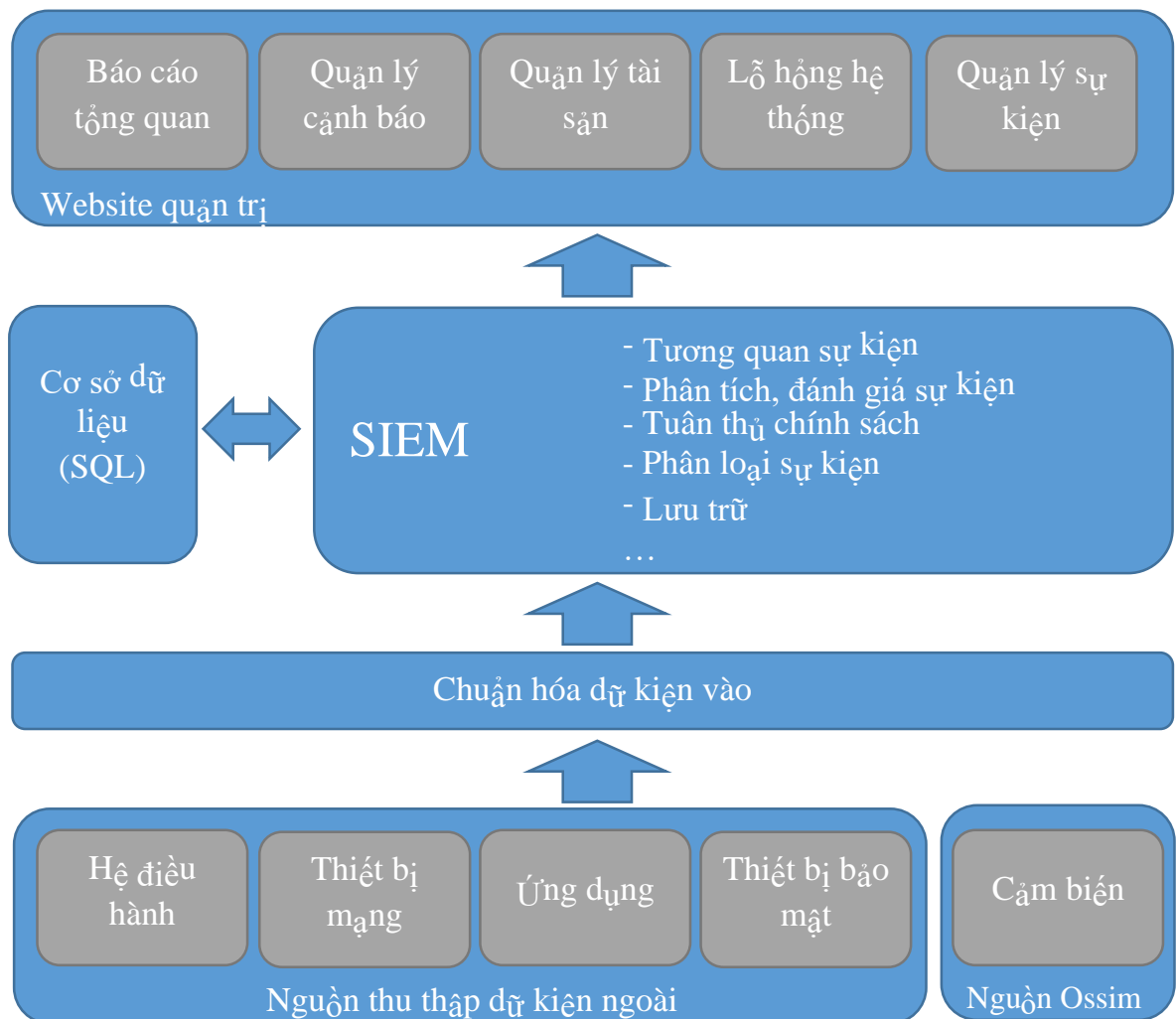
3.2. Hệ thống và mô hình phát hiện tấn công mạng

3.2.1. Hệ thống mã nguồn mở AlienVault OSSIM

AlienVault OSSIM (OSSIM) là một giải pháp giám sát an ninh mạng dựa trên nền tảng mã nguồn mở. OSSIM rất phù hợp với các hệ thống quy mô vừa và nhỏ, nó cho phép người dùng sử dụng có thể bổ xung, tùy biến chức năng sao cho phù

hợp nhất với hệ thống mạng đặc thù. OSSIM thể hiện rõ mục đích của công nghệ SIEM với các mục tiêu chính như sau:

- AlienVault OSSIM thực hiện việc thu thập các sự kiện từ rất nhiều các thiết bị khác nhau như Firewall, IDS/IPS, các máy chủ, máy trạm,...trong hệ thống giám sát, từ các sự kiện có thể đưa ra các cảnh báo (alert) khác nhau.
- Các sự kiện thu thập được từ nhiều nguồn khác nhau sau đó sẽ được OSSIM phân tích để tìm ra mối liên hệ giữa các sự kiện khác nhau và đưa ra được những thông tin tổng hợp nhất có liên quan đến an ninh trong hệ thống.

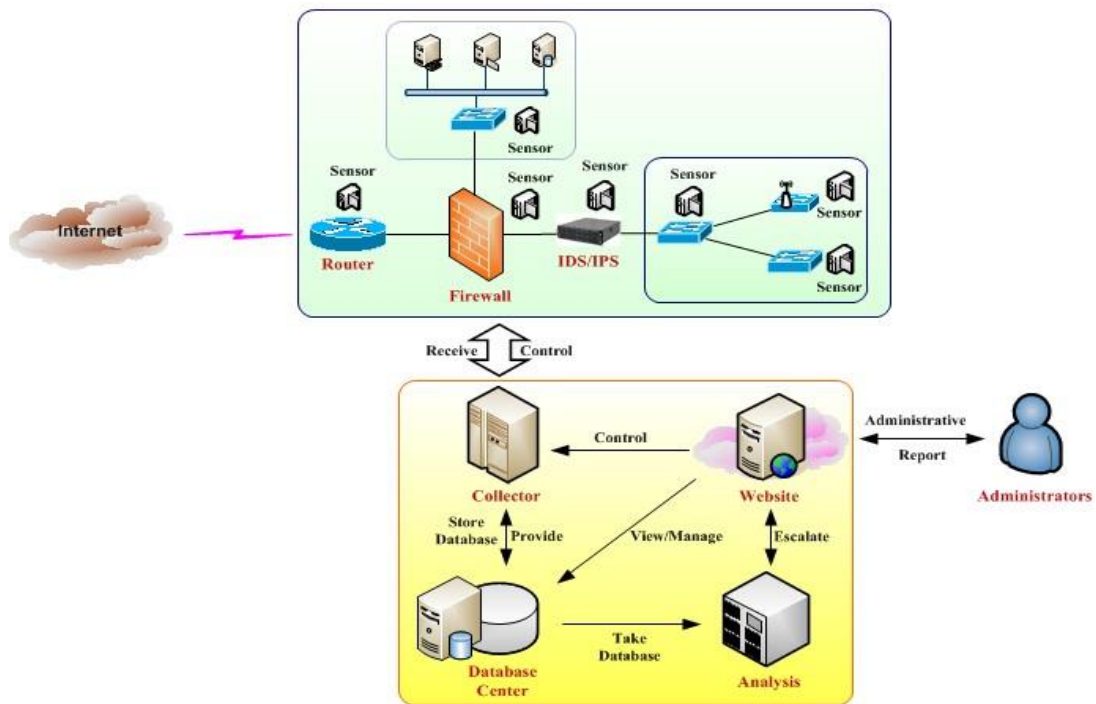


Hình 3.1: Mô hình hoạt động của OSSIM

- Những thông tin AlienVault OSSIM sau khi đã được phân tích, tổng hợp sẽ được đưa vào báo cáo cụ thể, nó là kết quả đánh giá về mức độ an ninh trong hệ thống được giám sát [11].

3.2.2. Một số chức năng chính của AlienVaultOSSIM

- Tìm kiếm tài nguyên (Asset Discovery):
 - + Sử dụng trực tiếp các công cụ quét trong mạng.
 - + Giám sát mạng.
 - + Kiểm kê tài nguyên.
 - + Phần mềm kiểm kê các Host.
- Đánh giá lỗ hổng (Vulnerability Assessment):
 - + Sử dụng các công cụ kiểm tra, phát hiện các lỗ hổng.
 - + Thực hiện giám sát các lỗ hổng.
- Phát hiện mối đe dọa (Threat Detection):
 - + Phát hiện mối đe dọa dựa trên Network IDS, Host IDS, Wireless IDS.
 - + Giám sát tính toàn vẹn của File.
- Giám sát hành vi (Behavioral Monitoring):
 - + Tập hợp thông tin nhật ký.
 - + Phân tích luồng lưu lượng mạng.
 - + Giám sát khả năng sẵn sàng của các dịch vụ.
 - + Thu thập và phân tích các gói tin.
- Bảo mật thông minh (Security Intelligence):
 - + Xác định mối quan hệ giữa các sự kiện thông qua SIEM.
 - + Phản ứng trước các sự cố.
 - + Báo cáo và các cảnh báo.



Hình 3.2: Mô hình tổng quan phát hiện tấn công mạng

3.2.3. Mô hình tổng quan hệ thống phát hiện tấn công mạng dựa trên công nghệ Siem sử dụng công cụ AlienVault OSSIM

- Máy trinh sát (Sensor):

Thành phần này đóng vai trò là các máy trinh sát nằm rải rác trên mạng để thu thập thông tin. Thành phần này bao gồm nhiều tiện ích, mỗi tiện ích là một phần mềm đơn lẻ, thực hiện một chức năng giám sát, thu thập, truy vấn thông tin từ môi trường mạng. Những thông tin thu được sẽ được gửi về cho thành phần Collector để phân tích.

- Máy thu thập (Collector):

Thành phần này làm nhiệm vụ thu nhận thông tin gửi về từ các máy trinh sát và tiến hành tổng hợp thông tin, gửi về cho CSDL để lưu trữ. Thành phần này cũng đóng vai trò điều phối công việc cho các máy trinh sát.

- Cơ sở dữ liệu (Database Center):

Thành phần này đóng vai trò lưu trữ các CSDL mà hệ thống giám sát an ninh mạng sử dụng. Tất cả dữ liệu sẽ được lưu theo định dạng có cấu trúc trong các CSDL trên máy chủ. Các thành phần khác sẽ phải giao tiếp với CSDL này để lưu trữ và truy vấn thông tin.

- Phân tích (Analysis):

Thành phần này sẽ tiến hành phân tích các thông tin thu thập được lưu trong CSDL để từ đó tìm ra các dấu hiệu bất thường. Sau khi phát hiện ra các hành vi bất thường, thành phần này sẽ làm nhiệm vụ gửi các thông tin cảnh báo cho người quản trị qua giao diện Website.

- Website:

Đây là thành phần trung tâm tương tác với người quản trị và mọi thành phần khác của hệ thống giám sát an ninh mạng. Thành phần này bao gồm một giao diện Web để quản trị có thể truy nhập, sử dụng các chức năng của hệ thống giám sát an ninh mạng: quản lý các máy trình sát, xem các thông tin thu thập được, yêu cầu một máy trình sát truy vấn thông tin và thiết lập cấu hình cho hệ thống, ...

Trong sơ đồ, những đường mũi tên biểu thị tương tác giữa các thành phần của hệ thống, những tương tác này có thể là truyền lệnh điều khiển hoặc dữ liệu.

3.3. Triển khai xây dựng

3.3.1. Triển khai OSSIM vào hệ thống mạng

Để triển khai OSSIM người quản trị cần nắm được đầy đủ thông tin về hệ thống mạng cần triển khai. Nắm được sơ đồ mạng, loại thiết bị, hệ điều hành, phần mềm đang được sử dụng. Đặc biệt là các máy chủ trọng yếu trong hệ thống.

- Yêu cầu phần cứng: Máy chủ

- + CPU: 3.2 GHz
- + Processor: 64 bit
- + RAM \geq 8 GB
- + Disk Space: \geq 40 GB
- + Total Cores \geq 4

- Phần mềm mã nguồn mở được cài đặt vào máy chủ: AlienVault OSSIM 5.2.5

3.3.2. Một số công cụ được sử dụng trong OSSIM

- Công cụ phát hiện xâm nhập dựa trên máy chủ (HIDS): OSSEC

OSSEC là một công cụ mã nguồn mở phát hiện xâm nhập trên host. Công cụ này cung cấp nền tảng phân tích log, kiểm tra tính toàn vẹn của tập tin, phát hiện rootkit, giám sát chính sách, thời gian thực và đưa ra cảnh báo.

- Công cụ phát hiện xâm nhập (NIDS): Suricata

Suricata là một công cụ IDS/IPS mã nguồn mở được tích hợp vào OSSIM nhằm phát hiện xâm nhập, theo dõi lưu lượng mạng. Suricata cũng hoạt động dựa trên luật được thay thế cho Snort ở phiên bản AlienVault OSSIM 5.2.

Công cụ này tính năng tương tự như Snort và hỗ trợ Snort (VRT) Rules tuy nhiên cách làm việc của chúng khác nhau. Snort sử dụng Single-threaded (đơn luồng) trong khi đó Suricata chạy Multi-threaded (đa luồng).

- Công cụ phát hiện xâm nhập không dây Wireless intrusion detection system (WIDS): Kismet

Kismet là công cụ phát hiện xâm nhập không dây, công cụ này làm việc chủ yếu với mạng Wi-fi (IEEE 802.11) nhưng có thể xử lý các loại mạng khác thông qua Plug-in.

- Công cụ giám sát các nút mạng (Monitoring of nodes of network): Nagios
- Nagios là công cụ giám sát mạng, các kết nối, theo dõi sự sẵn sàng, thời gian hoạt động và thời gian đáp ứng của tất cả các nút trên mạng.

- Công cụ phân tích bất thường trong mạng (Analysis of network anomalies): P0f, PADS, Arpwatch, etc.

ARP là một giao thức trong bộ giao thức TCP/IP, dùng để ánh xạ các địa chỉ IP thành địa chỉ vật lý (MAC) trong mạng cục bộ.

Arpwatch: là một công cụ giám sát hoạt động ethernet và lưu giữ một cơ sở dữ liệu của ethernet cùng với địa chỉ IP. Hoạt động của Arpwatch bao gồm hai bước chính. Trước hết, chương trình sẽ thu thập và lưu giữ những cặp ánh xạ địa chỉ vật lý – địa chỉ IP của các máy tính trong mạng. Ví dụ một máy tính trong mạng đang hoạt động với địa chỉ IP x.y.z.t có địa chỉ vật lý của giao diện mạng là aa:bb:cc:dd:ee:ff.

Sau bước này, chương trình sẽ giám sát các luồng dữ liệu lưu thông trên mạng, nếu chương trình phát hiện thấy một gói tin nào đó mang thông tin địa chỉ IP là x.y.z.t và địa chỉ vật lý khác aa:bb:cc:dd:ee:ff thì hệ thống sẽ phát ra cảnh báo. Vì trường hợp này có thể xảy ra khả năng một máy tính khác đang giả mạo địa chỉ IP x.y.z.t.

PADs: là công cụ phát hiện thụ động tài sản. Công cụ này theo dõi lưu lượng mạng, các bản ghi log và dịch vụ. Dữ liệu này được theo dõi bởi OSSIM khi có sự bất thường trong dịch vụ mạng.

P0f: Công cụ P0f được sử dụng thu thập thông tin về hệ điều hành. Công cụ này theo dõi lưu lượng truy cập mạng và xác định hệ điều hành. Thông tin này rất hữu ích trong quá trình suy luận tương quan.

- Công cụ Quét lỗ hổng trong hệ thống (Vulnerability scanner): OpenVAS

Đây là một công cụ mã nguồn mở quét lỗ hổng phổ biến. Được sử dụng để quản lý và quét các lỗ hổng trong hệ thống mạng.

3.3.3. Đánh giá rủi ro

Đánh giá rủi ro là việc làm quan trọng nhằm xác định cái gì là quan trọng cái gì là không. Việc đánh giá rủi ro được coi như là một trợ lý của quá trình ra quyết định. OSSIM tính toán rủi ro cho từng sự kiện an ninh. Việc tính toán này dựa trên ba thông số sau:

- Giá trị tài sản (Mất bao nhiêu giá trị nếu bị xâm nhập)
- Nguy cơ nào sẽ xảy ra.
- Xác suất xảy ra nó là bao nhiêu.

Bản ghi log được cung cấp từ các nguồn dữ liệu khác nhau đến máy chủ OSSIM. Các bản ghi log chuẩn hóa và hiển thị trong giao diện quản lý web như các sự kiện an ninh. Tickets được tự mở hoặc tự động tạo ra trong OSSIM. Để xử lý sự cố, OSSIM sẽ được xem xét báo động, tạo ra một ticket về sự cố có liên quan và gán nó cho thành phần thích hợp. Báo động xảy ra khi giá trị rủi ro của sự kiện an ninh bằng hoặc lớn hơn một giá trị nào đó. Rủi ro được tính toán theo công thức sau:

$$[\text{ASSET VALUE}(0-5) * \text{PRIORITY}(0-5) * \text{RELIABILITY}(0-10)] / 25 = \text{RISK}$$

OF THE EVENT(0-10)

Trong đó:

ASSET VALUE: Giá trị của tài sản.

PRIORITY: Độ ưu tiên cho từng sự kiện an ninh.

RELIABILITY: Độ tin cậy của sự kiện an ninh.

RISK OF THE EVENT: Mức độ rủi ro của sự kiện an ninh.

Các tài sản trong OSSIM có giá trị tài sản từ 0-5. Số càng cao là tài sản có giá trị cao. Tài sản là một thiết bị, một máy chủ hoặc có thể là một nhóm máy chủ, các nhóm máy chủ, mạng và nhóm mạng. Căn cứ vào độ rủi ro của sự kiện để nhận thấy xác suất của một cuộc tấn công.

3.3.4. Chuẩn hóa log

Trong OSSIM, Plugin được tạo ra nhằm chuẩn hóa các log đầu vào khác nhau thành một dạng bản ghi chuẩn duy nhất hoặc trích xuất dữ liệu cần trong bản log đầu vào và chuyển nó thành một sự kiện. Mặc định OSSIM đã có những plugin cho những nguồn dữ liệu thường gặp. Tuy nhiên thực tế ngày càng phát sinh nhiều nguồn dữ liệu mới hay đặc thù thiết bị của từng hệ thống mạng. Trong trường hợp này cần tạo ra những plugin mới để OSSIM có thể làm việc được.

Plugin trong OSSIM bao gồm hai tập tin:

<plugin_name>.cfg Tập tin này nằm trong thư mục /etc/ossim/agent/plugins.

Tập tin này quy định cụ thể thông số, quy tắc dữ liệu của file log cần chuẩn hóa. Cơ bản tập tin này bao gồm: Vị trí của nguồn dữ liệu nhận được, biểu thức và các quy tắc cần thiết để phân tích nguồn dữ liệu.

<plugin_name>.sql tập tin này nằm trong:

/usr/share/doc/ossim-mysql/contrib/plugins

Tập tin này mô tả mọi sự kiện được dùng để đánh giá, tương quan hay lưu trữ như:

ID Plugin

ID của loại sự kiện

Tên gán cho sự kiện

Mức độ ưu tiên và giá trị độ tin cậy

- Tập tin <plugin_name>.cfg được biên tập cụ thể như sau:

+ Phần Header: Tất cả các Plugin đều có một phần tiêu đề như sau

```
# AlienVault plugin
```

```
# Author: AlienVault Team
```

```
# Plugin {{ Tên Plugin }} id:{{ plugin_id }} version: -
```

```
# Last modification: {{ LAST_MODIFICATION_DATE }}
```

```
#
```

```
# Plugin Selection Info:
```

```
# {{ vendor }}:{{ model }}:{{ version }}:{{ per_asset }}
```

```
#
```

```
#END-HEADER
```

```
#
```

+ Phần cấu hình chi tiết: Ví dụ cấu hình cho file log từ phần mềm diệt virus

Mcafee

```
[DEFAULT] // phần thiết lập mặc định cho các sự kiện
```

```
plugin_id=1571 [config] type=detector //kiểu của
```

```
plugin enable=yes source=log
```

```
location=/var/log/mcafee.log // vị trí file log
```

```
create_file=false process= start=no stop=no startup=
```

```
shutdown=
```

```
[translation] //bảng dịch
```

```
BLOCKED=1
```

```
[mcafee-blocked] //quy tắc cho sự kiện event_type=event //kiểu của sự kiện (event, aler...)
```

```
regexp="(P<date>\d+\d+\d+\t\TIME...)\t(.*)\t(.*)\t(.*)\t(.*)"
```

```
//Biểu thức mô tả dữ liệu
```

```
plugin_sid=1 Dữ liệu chuẩn
```

```
filename=${$3}
```

```
date={normalize_date($date)}
```

```
hóa
```

```
được để gửi đến Server
```

OSSIM

```
userdata1={$4}
```

```
src_ip={$5}
```

- Tập tin <plugin_name>.sql được biên tập cụ thể như sau:

```
-- McAfee Antivirus
```

```
-- Plugin id: 1571
```

```
DELETE FROM plugin WHERE id = "1571";
```

```
DELETE FROM plugin_sid where plugin_id = "1571";
```

```
INSERT IGNORE INTO plugin (id, type, name, description) VALUES  
(1571, 1, 'mcafee', 'McAfee Antivirus');
```

```
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id,  
name, priority, reliability) VALUES (1571, 1, NULL, NULL, 'McAfee  
Antivirus: BLOCKED', 1, 3);
```

- Để đưa plugin này vào hoạt động ta phải sao chép hai tệp này đến đúng địa chỉ nêu trên và tiến hành cập nhật cơ sở dữ liệu bằng lệnh:

```
cat exchangews.sql | ossim-db ossim-  
server restart
```



3.3.5. Xây dựng luật trong Ossim

“Luật” Trong OSSIM ta có thể hiểu đơn giản nó giống như các quy tắc hay luật lệ. Nó sẽ có phần mô tả một trạng thái hay hành động gì sẽ xảy ra khi trạng thái đầu vào đúng. OSSIM cho phép người sử dụng có thể viết các luật của riêng mình sao cho phù hợp nhất với hệ thống mạng. Thay vì phải phụ thuộc vào nhà cung cấp, một cơ quan bên ngoài, hoặc phải cập nhật khi có một cuộc tấn công mới hay một phương pháp khai thác lỗ hổng mới được phát hiện. Người quản trị có thể viết riêng một luật dành cho hệ thống của mình dựa vào các sự kiện bất thường hoặc khi nhìn thấy các lưu lượng, sự kiện mạng bất thường trên giao diện quản lý sự kiện theo thời gian thực.

SECURITY EVENTS (SIEM) ?

SIEM REAL-TIME

PAUSE Done: [8 new rows]

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	OTX	SOURCE IP	DEST IP
2016-07-18 17:33:16	AlienVault NIDS: "ET SCAN NMAP -sS window 1024"	0	AlienVault NIDS	alienvault	N/A	 14.189.242.65:49733	Host-192-168-1-102:3389
2016-07-18 17:32:59	AlienVault NIDS: "ET SCAN NMAP -sS window 1024"	0	AlienVault NIDS	Sensor1	N/A	 14.189.242.65:49733	May-chu-Web-22:80
2016-07-18 17:32:34	AlienVault HIDS: Login session closed [USERNAME].	0	AlienVault HIDS-syslog	alienvault	N/A	alienvault	alienvault
2016-07-18 17:32:34	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	alienvault	N/A	alienvault	alienvault
2016-07-18 17:32:32	sudo: Session closed	0	sudo	alienvault	N/A	0.0.0.0	alienvault
2016-07-18 17:32:32	SSHD: Received disconnect	0	ssh	alienvault	N/A	alienvault	alienvault:22
2016-07-18 17:32:28	AlienVault HIDS: Successful login during non-business hours.	0	AlienVault HIDS-login_time	alienvault	N/A	alienvault	alienvault

Hình 3.3: Quản lý sự kiện theo thời gian thực

Ưu điểm của việc tự viết các luật là có thể tùy biến và cập nhật một cách cực kỳ nhanh chóng khi hệ thống mạng có sự bất thường. Trong OSSIM luật được biên tập trong file user.xml

Cấu trúc một luật để đưa ra cảnh báo khi phát hiện bất thường trong hệ thống như sau:

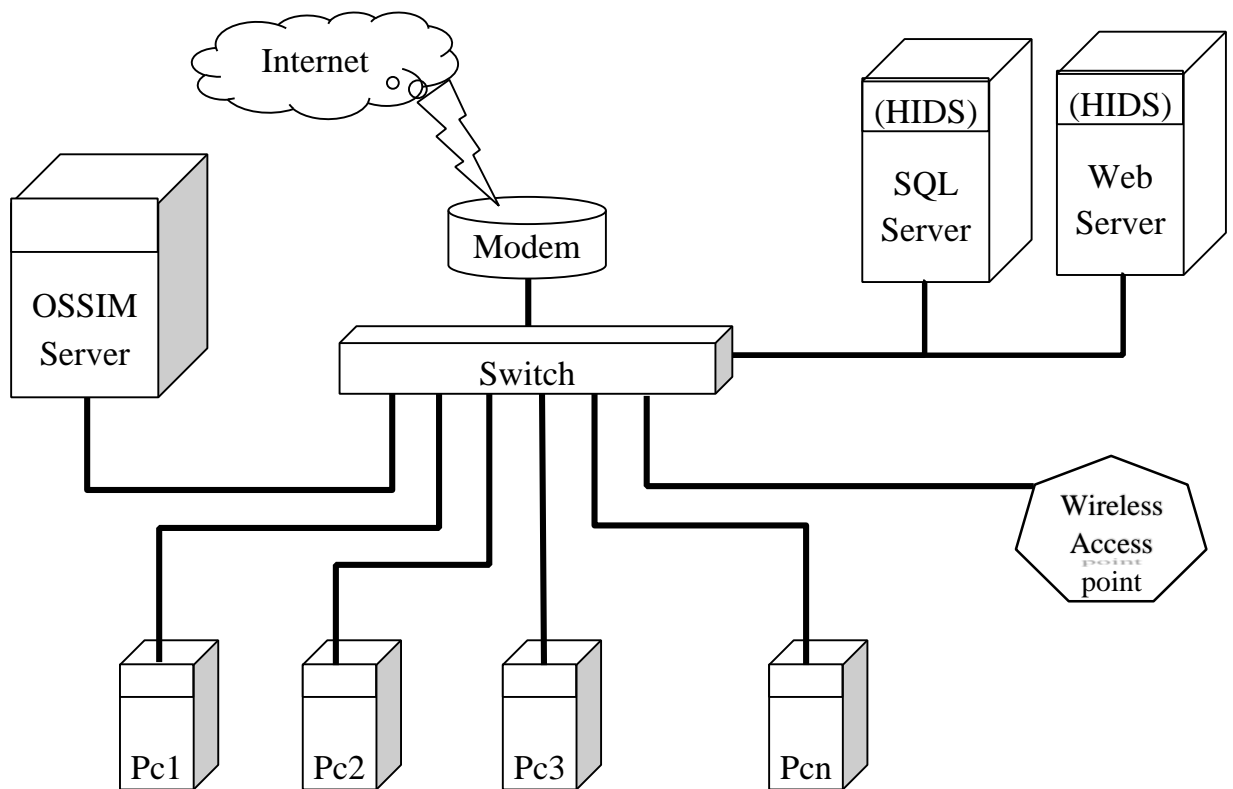
```
<directive id="ID" name="Tên của chỉ thị" priority="độ ưu tiên 1-5">
  <rule type="loại quy tắc" name="tên quy tắc" reliability="Độ tin cậy"
    occurrence="số lần xảy ra" from="địa chỉ nguồn" to="địa chỉ đích"
    port_from="cổng nguồn" port_to="cổng đích" plugin_id="id của nguồn dữ
    liệu" plugin_sid="id của sự kiện" protocol="Giao thức" sensor="địa chỉ của
    cảm biến">
    </rule>
  </directive>
```

Các luật này có thể được xếp thành nhiều lớp nhằm đánh giá chính xác hơn về sự kiện và tăng độ tin cậy của sự kiện.

3.4. Thử nghiệm và kết quả

3.4.1. Mô hình thử nghiệm thực tế

Đưa hệ thống phát hiện tấn công mạng OSSIM vào thử nghiệm với mô hình:



Hình 3.4: Sơ Đồ bố trí

*** Mô tả: Hệ thống trên bao gồm**

- Cài đặt và cấu hình:

- + Modem (Dùng kết nối internet)
- + Switch (Thiết bị chuyển mạch kết nối các thiết bị trong mạng)
- + Wireless Access point (Thiết bị thu phát sóng wifi)

- Máy chủ Web

- + Địa chỉ IP: 192.168.1.22
- + Hệ điều hành: Windows Server 2008
- + Cài đặt IIS làm

webserver + HIDS:

OSSEC Agent

- Máy chủ SQL Server

- + Địa chỉ IP: 192.168.1.102

- + Hệ điều hành: Windows Server 2012
 - + Hệ quản trị cơ sở dữ liệu: Microsoft SQL Server 2008 R2
 - + HIDS: OSSEC Agent
 - Máy chủ Phát hiện tấn công mạng OSSIM
 - + Địa chỉ IP: 192.168.1.212
 - Các máy trạm từ pc1, pc2 đến pcn
- Hệ điều hành của các máy trạm rất đa dạng từ Windows xp, Windows 7, Windows 8, windows 10 ...

Các máy trạm này có địa chỉ IP nằm trong vùng 192.168.1.0/24

*** Các trường hợp kiểm thử hệ thống:**

- Tấn công thăm dò (Sử dụng phần mềm Nmap).
- Tấn công đăng nhập vào dịch vụ Remote desktop.
- Phát hiện máy trạm nội bộ nằm trong mạng lưới botnet bị điều khiển để thực hiện tấn công DDOS. - Tấn công SQL Injection.

Chúng ta sẽ thử nghiệm và theo dõi cảnh báo qua giao diện Web của hệ thống phát hiện tấn công OSSIM.

3.4.2. Tấn công thăm dò

Trong thử nghiệm này tôi sử dụng phần mềm quét cổng Nmap từ một máy trạm trên Internet tới địa chỉ của web server.

- Luật được viết như sau để đưa ra cảnh báo với kiểu tấn công này:

```
<directive id="50011" name="Phat hien tan cong quet cong" priority="3">
  <rule type="detector" name="xuat hien hanh dong quet cong" reliability="1"
occurrence="1" from="!HOME_NET" to="HOME_NET" port_from="ANY"
port_to="ANY" plugin_id="1001" plugin_sid="2000536,2000537,2000538,
2000540,2000543,2000544,2000545,2000546,2000575,2001219,2001553,200
1569,
```

2001579,2001580,2001581,2001582,2001583,2001609,2001610,2001611,2001689,

2001904,2001906,2001972,2009582">

<rules>

<rule type="detector" name="Lap lai hanh dong quet cong" reliability="6" occurrence="2" from="1:SRC_IP" to="HOME_NET" time_out="1000"

port_from="ANY" port_to="ANY" plugin_id="1001"

plugin_sid="2000536,2000537,2000538,

2000540,2000543,2000544,2000545,2000546,2000575,2001219,2001553,2001569,

2001579,2001580,2001581,2001582,2001583,2001609,2001610,2001611,2001689,

2001904,2001906,2001972,2009582">

</rules>

</rule>

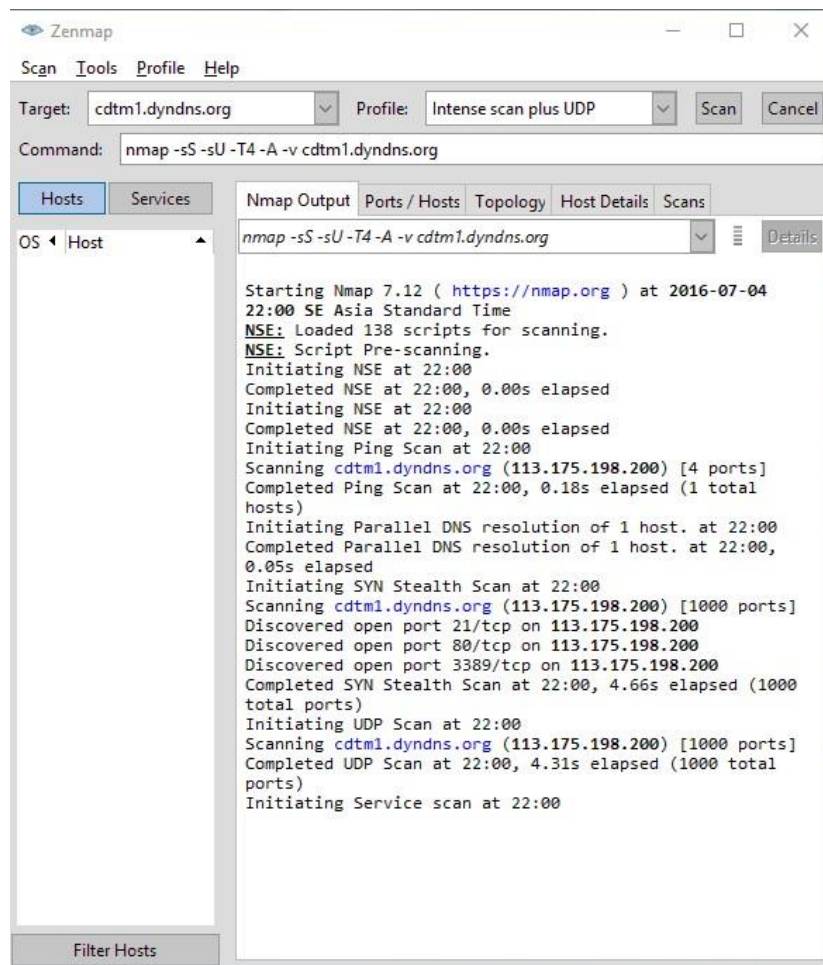
</directive>

- Với ý nghĩa như sau:

Tạo ra một chỉ thị có id là 40001 với tên của chỉ thị là “Phat hien tan cong quet cong” và độ ưu tiên là 3.

Trong chỉ thị này bao gồm 2 luật với mức độ tin cậy tăng dần. Luật thứ nhất có độ tin cậy là 1 nếu số lần xuất hiện của sự kiện là 1, địa chỉ nguồn là từ !HOME_NET (địa chỉ bất kỳ nằm ngoài vùng địa chỉ mạng nội bộ) đến địa chỉ đích là địa chỉ thuộc mạng nội bộ, các cổng dịch vụ là bất kỳ. Dữ liệu sự kiện được lấy từ nguồn có ID là 1001 (Dữ liệu NIDS) với các sự kiện có ID là 2000536, 2000537, 2000538, 2000540, 2000543, 2000544, 2000545, 2000546 ...

Luật thứ hai được đặt tên là “Lap lai hanh dong quet cong”. Xuất hiện kiểu sự kiện được liệt kê trong Plugin_SID hai lần trong 1000 giây từ ip nguồn như luật thứ nhất đến ip trong mạng nội bộ. Các cổng vẫn là bất kỳ. Thì tăng độ tin cậy lên 6



Hình 3.5: Phần mềm Nmap

- Cảnh báo trên giao diện web:

SHOW

20

 ENTRIES

ACTIONS

	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION	
<input checked="" type="checkbox"/>	2016-07-18 17:33:37	open	Suspicious Behaviour	Port Scan	2	N/A	14.189.242.65:18134	Host-192-168-1-102.ms-term-serv	
<input type="checkbox"/>	2016-07-18 17:25:40	open	Bruteforce Authentication	Ket noi, dang nhap thu	3	N/A	Host-192-168-1-102.ms-term-serv	42.61.39.187:49161	
<input type="checkbox"/>	2016-07-17 19:24:57	open	Bruteforce Authentication	Microsoft Remote Desktop	1	N/A	104.155.228.102:52717	Host-192-168-1-102.ms-term-serv	
<input type="checkbox"/>	2016-07-17 15:17:21	open	Suspicious Behaviour	Port Scan	2	N/A	14.189.242.65:11209	Host-192-168-1-102.ms-term-serv	
<input type="checkbox"/>	2016-07-17 15:07:01	open	Bruteforce Authentication	Microsoft Remote Desktop	1	N/A	14.189.242.65:50090	Host-192-168-1-102.ms-term-serv	
<input type="checkbox"/>	2016-07-17 15:06:11	open	Bruteforce Authentication	Microsoft Remote Desktop	1	N/A	14.189.242.65:50080	Host-192-168-1-102.ms-term-serv	
<input type="checkbox"/>	2016-07-17 11:39:26	open	Bruteforce Authentication	Ket noi, dang nhap thu	3	N/A	Host-192-168-1-102.ms-term-serv	104.155.228.102:50100	
<input type="checkbox"/>	2016-07-17 11:39:10	open	Bruteforce Authentication	Microsoft Remote Desktop	1	N/A	104.155.228.102:64081	Host-192-168-1-102.ms-term-serv	
<input type="checkbox"/>	2016-07-16 21:10:37	open	Bruteforce Authentication	Microsoft Remote Desktop	1		218.255.234.146:63862	Host-192-168-1-102.ms-term-serv	

Hình 3.6: Cảnh báo tấn công quét cổng

ALARMS

LIST VIEW GROUP VIEW

Alarms > Phát hiện tấn công quét cổng

Suspicious Behaviour — Port Scan

Status	Risk	Attack Pattern	Created	Duration	# Events	OTX Indicators
Open	2	external to external one-to-many	23 hours ago	38 secs	3	0

Source (1)
14.189.242.65
Location: Vietnam
Asset Groups: Unknown
Networks: Unknown
OTX IP Reputation: No

Destination (2)
192.168.1.102
Host-192-168-1-102 (192.168.1.102)
Location: Unknown
Asset Groups: Unknown
Networks: Local_192_168_1_0_24
OTX IP Reputation: No

Hình 3.7: Chi tiết cảnh báo tấn công quét cổng

EVENTS							
#	ALARM	RISK	DATE	SOURCE	DESTINATION	OTX	CORRELATION LEVEL
1	Phát hiện tấn công quét cổng	2	2016-07-18 17:33:37	14.189.242.65:18134	Host-192-168-1-102:ms-term-serv	N/A	2
Alarm Summary [Total events matched with high rule level: 0 - Total Events: 2 - Unique Dst IPAddr: 2 - Unique Types: 2 - Unique Dst Ports: 2]							
1	AlienVault NIDS: "ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection"	0	2016-07-18 17:33:37	14.189.242.65:18134	Host-192-168-1-102:ms-term-serv	N/A	2
2	AlienVault NIDS: "ET SCAN NMAP -sS window 1024"	0	2016-07-18 17:32:59	14.189.242.65:49733	May-chu-Web-22:http	N/A	2
3	AlienVault NIDS: "ET SCAN NMAP -sS window 1024"	0	2016-07-18 17:33:16	14.189.242.65:49733	Host-192-168-1-102:ms-term-serv	N/A	1

Hình 3.8: Các sự kiện tương quan cho cảnh báo quét cổng

Trong thử nghiệm này khi quét cổng bằng Nmap hệ thống thu thập được các sự kiện quét cổng từ IP: 113.175.198.200 đến các cổng dịch vụ ftp, http, mg-term-serv... của máy trong hệ thống mạng. Tương quan các sự kiện này OSSIM đã đưa ra cảnh báo hệ thống đang có hành động quét cổng bất thường.

3.4.3. Tấn công đăng nhập

Tấn công đăng nhập (Bruteforce attack) là dạng tấn công hoạt động bằng cách thử tất cả các chuỗi mật khẩu có thể để tìm ra mật khẩu. Hiện nay dạng tấn công này đang rất phổ biến do cơ chế đăng nhập vào các dịch vụ của hệ điều hành windows khá dễ dàng. Bruteforce attack rất đơn giản, dễ hiểu nhưng khó để phòng chống triệt để. Kiểu tấn công này sẽ luôn tìm được mật khẩu đúng vấn đề chỉ là thời gian.

Thử nghiệm bằng cách sử dụng phương pháp dò mật khẩu đăng nhập vào dịch vụ Remote của windows server 2008 trên máy chủ SQL Server (IP: 192.168.1.22) từ một máy tính bên ngoài hệ thống mạng.

Thiết lập luật cho kiểu tấn công này như sau:

```
<directive id="50012" name="Bruteforce attack,tan cong dang nhap Microsoft
Remote Desktop toi DST_IP" priority="4">
  <rule type="detector" name="Phat hien dang nhap that bai" reliability="1"
occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
plugin_id="1001" plugin_sid="2012709,2012710,2012712,2012711">
    <rules>
      <rule type="detector" name="Lap lai dang nhap that bai" reliability="2"
occurrence="50" from="1:SRC_IP" to="1:DST_IP" port_from="ANY"
time_out="300" port_to="ANY" plugin_id="1001"
plugin_sid="2012709,2012710,2012712,2012711">
        <rules>
          <rule type="detector" name="Lap lai dang nhap that bai" reliability="6"
occurrence="500" from="1:SRC_IP" to="1:DST_IP" port_from="ANY"
time_out="4800" port_to="ANY" plugin_id="1001"
plugin_sid="2012709,2012710,2012712,2012711">
            </rule>
          </rules>
        </rule>
      </rules>
    </rules>
  </rule>
</directive>
```

Thực hiện đăng nhập thử nhiều lần bằng dịch vụ Remote Desktop với tên và mật khẩu sai vào máy chủ web server. Server này có IP nội bộ là 192.168.1.22 và địa chỉ được mở cổng dịch vụ Remote desktop trong modem để sử dụng trên Internet là:

cdtm1.dyndns.org:3388. Tấn công thử nghiệm từ một máy tính ngoài hệ thống mạng



Hình 3.9: Kết nối tới máy chủ Web bằng dịch vụ Remote desktop

Sau khi thử sai nhiều lần mật khẩu hệ thống sẽ đưa ra cảnh báo như

sau:

SHOW20ENTRIES

DATE

STATUS

INTENT & STRATEGY

METHOD

RISK

OTX

SOURCE

DESTINATION

2016-07-18
22:26:40

open

Bruteforce Authentication

Microsoft Remote Desktop

1

N/A

14.189.242.65:56066

May-chu-Web-22.ms-term-serv

DELIVERY & ATTACK: BRUTEFORCE AUTHENTICATION

ATTACK PATTERN: EXTERNAL TO INTERNAL ONE-TO-ONE

OPEN & CLOSED ALARMS

TOTAL EVENTS

11

2016-07-18 22:26:40

DURATION

25

SECS

ELAPSED TIME

4

MINS

VIEW DETAILS

CLOSE

DELETE

APPLY LABEL

2016-07-18
21:19:45

open

Bruteforce Authentication

Ket noi, dang nhap thu

3

N/A

Host-192-168-1-102.ms-term-serv

42.61.39.187:50939

2016-07-18
17:33:37

open

Suspicious Behaviour

Port Scan

2

N/A

14.189.242.65:18134

Host-192-168-1-102.ms-term-serv

Hình 3.10: Cảnh báo tấn công đăng nhập

EVENTS							
#	ALARM	RISK	DATE	SOURCE	DESTINATION	OTX	CORRELATION LEVEL
1	Tan cong vao dich vu Remote Desktop	1	2016-07-18 22:26:40	14.189.242.65:56066	May-chu-Web-22.ms-term-serv	N/A	2
Alarm Summary [Total events matched with high rule level: 0 - Total Events: 10 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]							
1	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:22	14.189.242.65:56066	May-chu-Web-22.ms-term-serv	N/A	2
2	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:22	14.189.242.65:56066	May-chu-Web-22.ms-term-serv	N/A	2
3	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:22	14.189.242.65:56066	May-chu-Web-22.ms-term-serv	N/A	2
4	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:19	14.189.242.65:56065	May-chu-Web-22.ms-term-serv	N/A	2
5	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:19	14.189.242.65:56065	May-chu-Web-22.ms-term-serv	N/A	2
6	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:19	14.189.242.65:56065	May-chu-Web-22.ms-term-serv	N/A	2
7	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:19	14.189.242.65:56065	May-chu-Web-22.ms-term-serv	N/A	2
8	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:19	14.189.242.65:56065	May-chu-Web-22.ms-term-serv	N/A	2
9	AlienVault NIDS: "ET POLICY MS Remote Desktop Administrator Login Request"	0	2016-07-18 22:26:19	14.189.242.65:56065	May-chu-Web-22.ms-term-serv	N/A	2

Hình 3.11: Các sự kiện tương quan cho cảnh báo đăng nhập

Trong thử nghiệm này OSSIM dựa vào các sự kiện có ID là 2012709 được thu thập từ NIDS để đưa ra cảnh báo.

3.4.4. Tấn công từ chối dịch vụ

Trong thử nghiệm này, giả sử một máy tính trong mạng nội bộ bị nhiễm mã độc và đang thuộc một mạng lưới botnet. Luật được xây dựng nhằm phát hiện ra máy tính bị nhiễm mã độc này khi nó bị điều khiển tấn công Dos đến một mục tiêu nào đó.

Luật được thiết lập cho kiểu tấn công này như sau:

```
<directive id="50013" name="Tan con tu choi dich vu tu SRC_IP"
priority="3"> <rule type="detector" name="phat hien Dos" reliability="1"
occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
plugin_id="1001" plugin_sid="2013097">
<rules>
<rule type="detector" name="Phat hien dos" reliability="3"
occurrence="60" from="1:SRC_IP" to="1:DST_IP" port_from="ANY"
time_out="30" port_to="1:DST_PORT" plugin_id="1001"
plugin_sid="2013097">
</rules>
```



```

<rule type="detector" name="tan cong dos" reliability="6"
occurrence="100" from="1:SRC_IP" to="1:DST_IP" port_from="ANY"
time_out="60" port_to="1:DST_PORT" plugin_id="1001"
plugin_sid="2013097">

</rule>

</rules>

</rule>

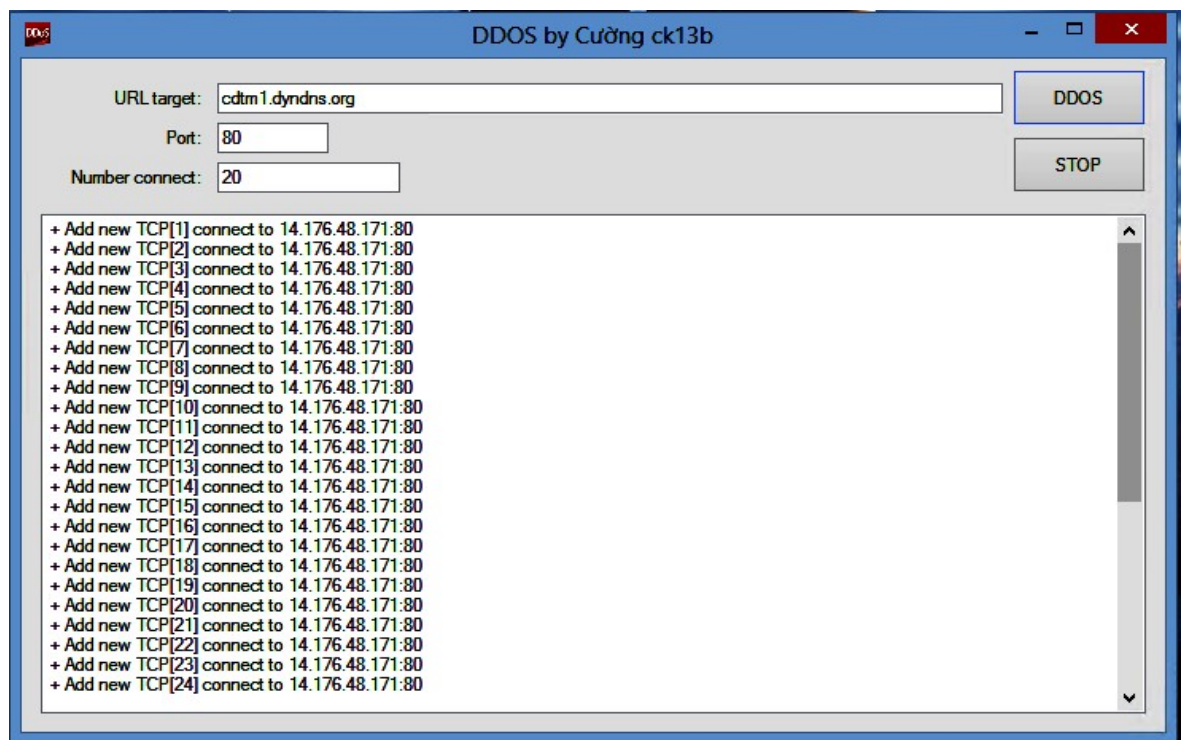
</rules>

</rule>

</directive>

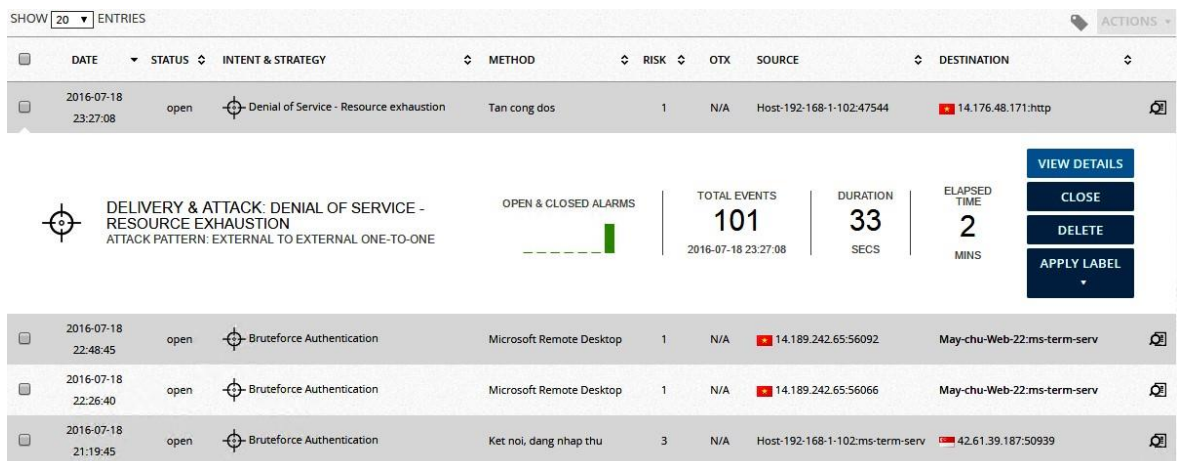
```

Trên máy trạm bất kỳ trong mạng nội bộ sử dụng một công cụ tấn công từ chối dịch vụ vào địa chỉ cdtm1.dyndns.org



Hình 3.12: Công cụ tấn công từ chối dịch vụ

Ngay sau khi công cụ tấn công gửi đi đạt ngưỡng lớn hơn 100 kết nối trong thời gian 60 giây. OSSIM sẽ đưa ra cảnh báo như sau:



Hình 3.13: Cảnh báo có tấn công dos từ ip nội bộ

Từ cảnh báo trên người quản trị biết được máy nào đang bị nhiễm mã độc trong hệ thống.

3.4.5. Tấn công vào hệ quản trị cơ sở dữ liệu SQL

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,... trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

- Luật được thiết lập cho kiểu tấn công này như sau:

```
<directive id="50014" name="Tan cong SQL injection vao dia chi DST_IP"
priority="3">
```

```
<rule type="detector" name="Phat hien SQL injection" reliability="6"
occurrence="1" from="!HOME_NET" to="HOME_NET" port_from="ANY"
port_to="ANY" plugin_id="1001"
plugin_sid="2006443,2006444,2006445,2006446,2006447,2008175,2008176,2
0084
```

```

67,2010037,2010084,2010085,2010086,2010284,2010285,2010963,2010964,2
01096
5,2010966,2010967,2011035,2011039,2011042,2011424,2013068,2014352"
protocol="TCP">
  <rules>
    <rule type="detector" name="Phat hien SQL injection" reliability="8"
occurrence="2" from="1:DST_IP" to="1:SRC_IP" port_from="ANY"
port_to="ANY" plugin_id="1001"
plugin_sid="2006443,2006444,2006445,2006446,2006447,2008175,2008176,2
0084
67,2010037,2010084,2010085,2010086,2010284,2010285,2010963,2010964,2
01096
5,2010966,2010967,2011035,2011039,2011042,2011424,2013068,2014352"
protocol="TCP" time_out="360">
  </rule>
</rules>
</rule>
</directive>

```

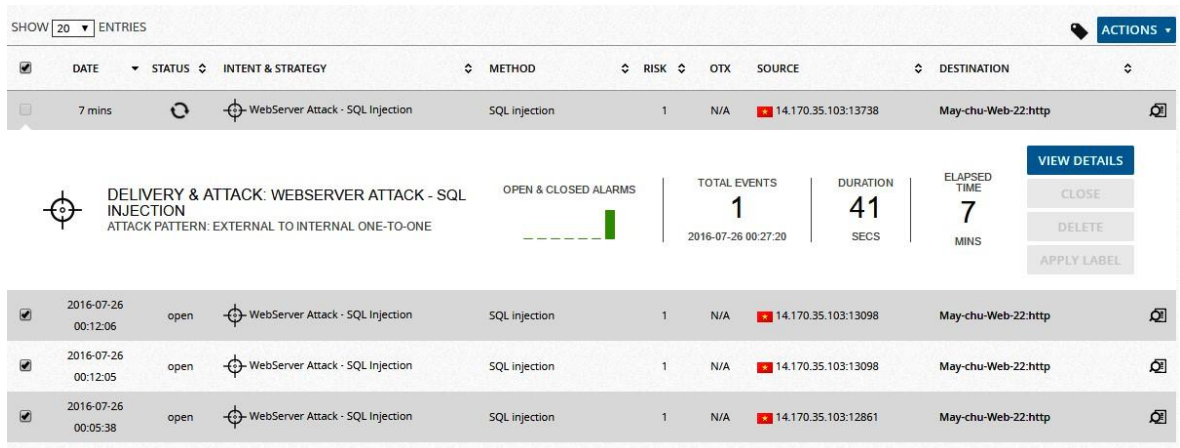
- Thực hiện tấn công thử nghiệm SQL injection vào máy chủ web. Thực hiện câu truy vấn sau để liệt kê cột id và pass trong bảng user:

UNION SELECT id,pass FROM user



Hình 3.14: Tấn công SQL injection

Hệ thống OSSIM đã đưa ra cảnh báo dựa vào sự kiện có id là 2006445 (Sự kiện có câu truy vấn SELECT FROM bất thường) và 2006446 (Sự kiện có câu truy vấn UNION SELECT bất thường)



Hình 3.15: Cảnh báo cho tấn công SQL injection

3.4.6. Đánh giá, kết quả

Như vậy sau khi tiến hành 4 thử nghiệm các chức năng của hệ thống phát hiện tấn công mạng OSSIM cùng các công cụ hỗ trợ được cài đặt như Ossec, Suricata, Kismet, Nagios ... Ta thấy các chức năng của hệ thống hoạt động ổn định. Các luật đã thiết đặt hoạt động chính xác, các tấn công thử nghiệm được thực hiện nhiều lần đều được phát hiện và đưa ra cảnh báo kịp thời.

Độ trễ đưa ra cảnh báo của hệ thống đối với các tấn công thử nghiệm trung bình là 25 giây. Độ trễ này còn cao nguyên nhân do tốc độ phản ứng máy chủ cài đặt OSSIM còn thấp.

Ngoài sự hoạt động ổn định của các chức năng chính, hệ thống còn đảm bảo được các yếu tố:

- Hoạt động giám sát hiệu quả mà không ảnh hưởng tới hiệu suất hoạt động của hệ thống mạng
- Trong suốt với người sử dụng.
- Thích ứng nhanh khi có thay đổi từ phía người quản trị: Thêm luật, thay đổi cấu hình, chỉnh sửa luật, ...

Hệ thống này hoàn toàn có thể triển khai vào thực tế.

*** Danh mục thiết bị và dự trù kinh phí:**

TT	Tên thiết bị	Số lượng	Đơn giá	Thành tiền
1	Modern	1	200.000	200.000
2	Switch	1	250.000	250.000
3	PC	4	10.000.000	40.000.000
4	Wireless Access point	1	4.000.000	4.000.000
5	Server	3	20.000.000	60.000.000

*** Phân công công việc**

Mã số SV	Tên SV	Mô tả khái quát mảng công việc SV thực hiện trong đồ án.	Ước tính phần trăm đóng góp
20161388	Nguyễn Tuấn Trung	Tìm hiểu về tổng quan về tấn công mạng, phát hiện tấn công mạng với SIEM và phát hiện tấn công, thiết kế hệ thống SIEM bằng cisco packet tracer	50%
20110441	Phan Chí Bảo	Tìm hiểu về phát hiện tấn công mạng với SIEM, xây dựng công cụ phát hiện tấn công mạng dựa trên công nghệ SIEM với mã nguồn mở Alienvault OSSIM, tham gia thiết kế cisco packet tracer	50%

KẾT LUẬN

An toàn thông tin ở Việt Nam đang trở thành một vấn đề nóng bỏng nhất qua hàng loạt các vụ việc các hệ thống lớn bị tấn công. **OSSIM** là công cụ phát hiện tấn công hiệu quả mà chi phí triển khai thấp, chỉ cần một máy chủ với cấu hình vừa phải với hệ thống mạng nhỏ. Sau đó thiết lập cấu hình, xây dựng các luật cho phù hợp với hệ thống mạng đó.

Tuy nhiên, để xây dựng được một hệ thống giám sát an ninh mạng hoàn thiện không phải là công việc dễ dàng. Nó đòi hỏi phải có sự hiểu biết sâu rộng về các phần mềm, các kiến thức về hệ thống, về lập trình, .. cùng các kiến thức về an toàn thông tin.

Bên cạnh những kết quả thu được nhóm em tự thấy đồ án còn nhiều hạn chế như: Kiến thức còn hạn chế nên phần trình bày những vấn đề đã tìm hiểu được còn sơ sài. Số lượng các luật xây dựng để phát hiện các kiểu tấn công còn ít.

Hướng phát triển của đồ án

- Thiết lập và hoàn thiện các luật sao cho hệ thống có thể phát hiện được hầu hết các kiểu tấn công mạng.
- Bổ sung hoạt động ứng phó tự động cho các cảnh báo tấn công

TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] Phạm Thế Quế, *Công nghệ mạng máy tính*, Nhà xuất bản Bưu điện, Hà Nội.
- [2] Trần Đức Sự, Phạm Minh Thuấn, *Giáo trình Phòng chống và điều tra tội phạm máy tính*, Học viện mật mã.
- [3] Vũ Bảo Thạch, “*Giáo trình Thực hành An toàn Mạng*”, Học viện mật mã, Hà Nội.
- [4] Nguyễn Đại Thọ, *An ninh mạng*, Đại học quốc gia Hà Nội.

Tiếng Anh

- [5] Steve Manzuik, Ken Pfeil, Andre, *Network Security Assessment*. Syngress.

- [6] ITU (1999), “*Internet protocol data communication service – IP packet transfer and availability performance parameters*”, ITU-T Recommendation Y.1540, Feb.
- [7] Roberta Bragg, Mark Rhodes – Ousley, Keith Strassberg , *Network Security*, McGraw-Hill Education.
- [8] Richard Bejtlich, *The Practice of Network Security Monitoring*, 2013

Trang web

- [9] <http://antoanthongtin.vn/Detail.aspx?CatID=afad3c1b-8ab0-41b3-9364fe76366f1531&NewsID=738aa8aa-5a16-44a7-aec1-b2f7bc49a831>
- [10] <http://securitydaily.net/tong-quan-ve-he-thong-giam-sat-an-ninh-mang/>
- [11] <https://www.alienvault.com/documentation/>
- [12] <https://voer.edu.vn/m/mot-so-giai-phap-nham-dam-bao-an-toan-an-ninh-mang-va-bao-mat-du-lieu/7fd336a8>
- [13] <http://docs.splunk.com/Documentation/ES/4.2.0/User/Overview>
- [14] <http://www-03.ibm.com/software/products/en/qradar-siem>