Hà Nội, 05/2016

HỌC VIỆN KỸ THẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN

ĐỀ TÀI:
TÌM HIỂU HỆ THỐNG GIÁM SÁT MÃ NGUỒN MỞ TẬP TRUNG OSSIM

HỌC VIỆN KỸ THẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

---ꕥ🕮ꕥ---

MÔN: AN TOÀN CƠ SỞ DỮ LIỆU

ĐỀ TÀI:
TÌM HIỂU HỆ THỐNG GIÁM SÁT MÃ NGUỒN MỞ TẬP TRUNG OSSIM

Cán bộ hướng dẫn: **Vũ Thị Vân.**

Nhóm sinh viên:

1. **Ngô Văn Thỉnh.**
2. **Phạm Công Lý.**
3. **Nguyễn Văn Hoàng.**
4. **Lê Văn Minh.**

Hà Nội, 05/2016

HỌC VIỆN KỸ THẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

---ꕥ🕮ꕥ---

MÔN: AN TOÀN CƠ SỞ DỮ LIỆU

ĐỀ TÀI:
TÌM HIỂU HỆ THỐNG GIÁM SÁT MÃ NGUỒN MỞ TẬP TRUNG OSSIM

Nhận xét: .....

.....

.....

.....

.....

.....

.....

.....

Điểm chuyên cần:.....

Điểm báo cáo: .....

Xác nhận của cán bộ hướng dẫn

MỤC LỤC

DANH MỤC HÌNH VẼ

LỜI NÓI ĐẦU

Ngày nay, thế giới đang ngày một phát triển, công nghệ thông tin đóng một vai trò quan trọng và không thể thiếu trong mọi lĩnh vực của đời sống. Số lượng máy tính gia tăng, đòi hỏi hệ thống mạng phải phát triển theo để đáp ứng nhu cầu kết nối toàn cầu. Hệ thống mạng ngày một phát triển đòi hỏi khả năng quản trị để có thể duy trì hoạt động của mạng một cách tốt nhất. Vì vậy người quản trị mạng cần một công cụ hỗ trợ khả năng quản trị.

Đối với một hệ thống mạng, để có thể duy trì mạng hoạt động tốt thì có rất nhiều thứ phải quản trị như là hiệu năng mạng, lưu lượng mạng, các ứng dụng chạy trên mạng, người sử dụng mạng, an ninh mạng. Security Information Event Management (SIEM) là một giải pháp hoàn chỉnh, đầy đủ cho phép các tổ chức thực hiện việc giám sát các sự kiện an toàn thông tin cho một hệ thống. Đây là công nghệ được các chuyên gia bảo mật rấtquan tâm trong thời gian gần đây. Nó sử dụng các phương pháp phân tích chuẩn hóa và mối tương quan giữa các sự kiện để đưa ra cảnh báo cho người quản trị.

Để đáp ứng thực hiện một giải pháp SIEM chúng em xin nghiên cứu đề tài "TÌM HIỂU HỆ THỐNG GIÁM SÁT MÃ NGUỒN MỞ TẬP TRUNG OSSIM". Đề tài tập trung tìm hiểu mô hình SIEM, nghiên cứu mô hình thiết bị hệ thống riêng biệt và tùy chọn trong mã nguồn mở OSSIM, từ đó tích hợp các công cụ an ninh mạng vào thiết bị. Từ đó đề xuất một mô hình giám sát an ninh mạng cho Học Viện Kỹ Thuật Mật Mã.

Do kiến thức còn hạn chế nên không tránh khỏi những thiếu sót, rất mong nhận được sự đóng góp của thầy cô và các bạn.

CHƯƠNG 1: TÌM HIỂU VỀ CÔNG NGHỆ PHÁT HIỆN XÂM NHẬP MẠNG IDS (Intrusion Detection System)

1.1. Khái niệm về phát hiện xâm nhập và ngăn chặn xâm nhập

Phát hiện xâm nhập là tiến trình theo dõi các sự kiện xảy ra trên một hệ thống máy tính hay hệ thống mạng, phân tích chúng để tìm ra các dấu hiệu xâm nhập bất hợp pháp. Xâm nhập bất hợp pháp được định nghĩa là sự cố gắng tìm mọi cách để xâm hại đến tính toàn vẹn, tính sẵn sàng, tính có thể tin cậy hay là sự cố gắng vượt qua các cơ chế bảo mật của hệ thống máy tính hay mạng đó.

Ngăn ngừa xâm nhập nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe doạ tấn công bằng việc loại bỏ những lưu lượng mạng có hại hay có ác ý trong khi vẫn cho phép các hoạt động hợp pháp tiếp tục. Mục đích ở đây là một hệ thống hoàn hảo – không có những báo động giả nào làm giảm năng suất người dùng cuối và không có những từ chối sai nào tạo ra rủi ro quá mức bên trong môi trường.

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

IDS và IPS có rất nhiều điểm chung, do đó hệ thống IDS và IPS có thể được gọi chung là IDP-Intrusion Detection and Prevention. Nội dung của chương sẽ được trình bày theo 2 phần chính: **Intrusion Detection** và **Intrusion Prevention.**

1.2. IDS (Intrusion Detection System- hệ thống phát hiện xâm nhập)

ID (Intrusion Detection) là giám sát các sự kiện đang xảy ra trong một hệ thống máy tính hoặc hệ thống mạng và phân tích để tìm ra các dấu hiệu của các sự cố có thể xảy ra vi phạm chính sách bảo mật máy tính, chính sách sử dụng chấp nhận các tiêu chuẩn an toàn thông tin. Các sự cố xuất phát từ rất nhiều nguyên nhân như: các phần mềm độc hại malware (Ví dụ: worms, spyware,…), các kẻ tấn công xâm nhập trái phép vào hệ thống từ Internet, người dùng cuối truy cập vào các tài nguyên không được phép truy cập,…

Hệ thống phát hiện xâm nhập trái phép là những ứng dụng phần mềm chuyên dụng để phát hiện xâm nhập vào hệ thống mạng cần bảo vệ. IDS được thiết kế không

phải với mục đích thay thế các phương pháp bảo mật truyền thống, mà để hoàn thiện nó.

1.2.1. Chức năng

Chức năng quan trọng nhất là: giám sát – cảnh báo – bảo vệ.

- Giám sát: lưu lượng mạng và các hoạt động khả nghi.
- Cảnh báo: báo cáo về tình trạng mạng cho hệ thống và nhà quản trị.
- Bảo vệ: Dùng những thiết lập mặc định và sự cấu hình từ nhà quản trị mà có những hành động thiết thực chống lại kẻ xâm nhập và phá hoại.

Chức năng mở rộng:

Phân biệt: tấn công bên trong và tấn công bên ngoài.

Phát hiện: những dấu hiệu bất thường dựa trên những gì đã biết hoặc nhờ vào sự so sánh thông lượng mạng hiện tại với baseline.

1.2.2. Phân loại

Có 2 loại IDS là Network Based IDS(NIDS) và Host Based IDS (HIDS):

a. ***Host Based IDS (HIDS)***

Bằng cách cài đặt một phần mềm trên tất cả các máy tính chủ, HIDS dựa trên máy chủ quan sát tất cả những hoạt động hệ thống, như các file log và những lưu lượng mạng thu thập được. Hệ thống dựa trên máy chủ cũng theo dõi OS, những cuộc gọi hệ thống, lịch sử sổ sách (audit log) và những thông điệp báo lỗi trên hệ thống máy chủ.

Lợi thế của HIDS:

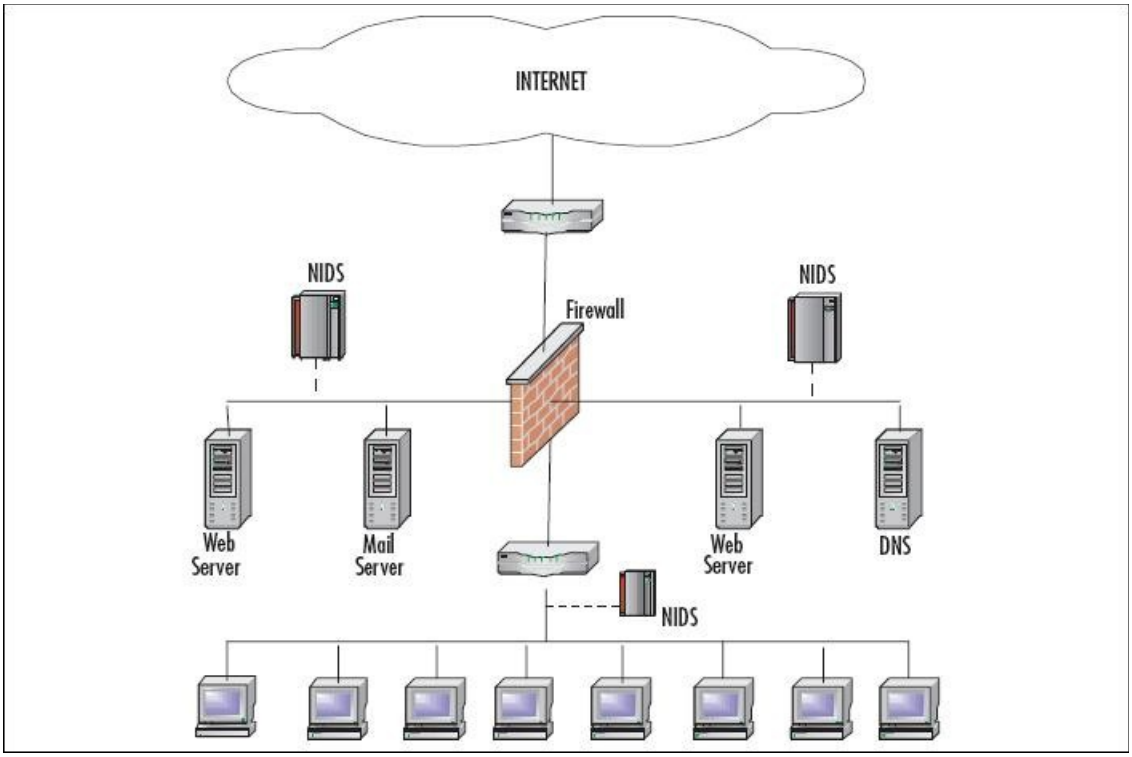
- Có khả năng xác đinh user liên quan tới một event.
- HIDS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy, NIDS không có khả năng này.
- Có thể phân tích các dữ liệu mã hoá.
- Cung cấp các thông tin về host trong lúc cuộc tấn công diễn ra trên host này.

Hạn chế của HIDS:

- Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.
- Khi OS bị "hạ" do tấn công, đồng thời HIDS cũng bị "hạ".
- HIDS phải được thiết lập trên từng host cần giám sát.

- HIDS không có khả năng phát hiện các cuộc dò quét mạng (Nmap, Netcat…).
- HIDS cần tài nguyên trên host để hoạt động.
- HIDS có thể không hiệu quả khi bị DOS.
- Đa số chạy trên hệ điều hành Window. Tuy nhiên cũng đã có 1 số chạy được trên UNIX và những hệ điều hành khác.

b. ***Network Base IDS (NIDS)***



Hình 1. ***NIDS***

Hệ thống NIDS dựa trên mạng sử dụng bộ dò và bộ cảm biến cài đặt trên toàn mạng. Những bộ dò này theo dõi trên mạng nhằm tìm kiếm những lưu lượng trùng với những mô tả sơ lược được định nghĩa hay là những dấu hiệu. Những bộ cảm biến thu nhận và phân tích lưu lượng trong thời gian thực. Khi ghi nhận được một mẫu lưu lượng hay dấu hiệu, bộ cảm biến gửi tín hiệu cảnh báo đến trạm quản trị và có thể được cấu hình nhằm tìm ra biện pháp ngăn chặn những xâm nhập xa hơn. NIDS là tập nhiều sensor được đặt ở toàn mạng để theo dõi những gói tin trong mạng so sánh với với mẫu đã được định nghĩa để phát hiện đó là tấn công hay không.

Lợi thế của Network-Based IDS:

- Quản lý được cả một network segment (gồm nhiều host).
- "Trong suốt" với người sử dụng lẫn kẻ tấn công.

- Cài đặt và bảo trì đơn giản, không ảnh hưởng tới mạng.
- Tránh DOS ảnh hưởng tới một host nào đó.
- Có khả năng xác định lỗi ở tầng Network (trong mô hình OSI).
- Độc lập với OS.

Hạn chế của Network-Based IDS:

- Có thể xảy ra trường hợp báo động giả (false positive), tức không có intrusion mà NIDS báo là có intrusion.
- Không thể phân tích các traffic đã được encrypt (vd: SSL, SSH, IPSec…).
- NIDS đòi hỏi phải được cập nhật các signature mới nhất để thực sự an toàn.
- Có độ trễ giữa thời điểm bị attack với thời điểm phát báo động. Khi báo động được phát ra, hệ thống có thể đã bị tổn hại.
- Không cho biết việc attack có thành công hay không.Một trong những hạn chế là giới hạn băng thông. Những bộ dò mạng phải nhận tất cả các lưu lượng mạng, sắp xếp lại những lưu lượng đó cũng như phân tích chúng.

1.2.3. Kiến trúc và nguyên lý hoạt động

IDS/IPS bao gồm các thành phần chính:

- Thành phân thu thập gói tin.
- Thành phần phát hiện gói tin.
- Thành phần xử lý gói tin.

a. Thành phần thu thập gói tin:

Thành phần này có nhiệm vụ lấy tất cả các gói tin đi đến mạng. Thông thường các gói tin có địa chỉ đích không phải là của một card mạng thì sẽ bị card mạng đó hủy bỏ nhưng card mạng của IDS được đặt ở chế độ thu nhận tất cả. Tất cả các gói tin qua chúng đều được sao chụp, xử lý, phân tích đến từng trường thông tin. Bộ thu thập gói tin sẽ đọc thông tin từng trường trong gói tin, xác định chúng thuốc kiểu gói tin nào, dịch vụ gì…Các thông tin này được chuyển đến thành phần phát hiện.

b. Thành phần phát hiện gói tin:

Bộ cảm biến đóng vai trò quyết định trong thành phần này. Bộ cảm biến được tích hợp với thành phần sưu tập dữ liệu – một bộ tạo sự kiện. Cách sưu tập này được xác định bởi chính sách tạo sự kiện để định nghĩa chế độ lọc thông tin sự kiện. Bộ

tạo sự kiện (hệ điều hành, mạng, ứng dụng) cung cấp một số chính sách thích hợp cho các sự kiện, có thể là một bản ghi các sự kiện của hệ thống hoặc các gói mạng. Số chính sách này cùng với thông tin chính sách có thể được lưu trong hệ thống được bảo vệ hoặc bên ngoài. Trong trường hợp nào đó, ví dụ khi luồng dữ liệu sự kiện được truyền tải trực tiếp đến bộ phân tích mà không có sự lưu dữ liệu nào được thực hiện.

1.3. IPS

IPS có hai chức năng chính là phát hiện các cuộc tấn công và chống lại các cuộc tấn công đó. Phần lớn hệ thống IPS được đặt ở vành đai mạng, đủ khả năng bảo vệ tất cả các thiết bị trong mạng.

1.3.1. Kiến trúc chung của các hệ thống IPS

- Module phân tích luồng dữ liệu.
- Modul phát hiện tấn công.
- Modul phản ứng.

Khi có dấu hiệu của sự tấn công hoặc thâm nhập, modul phát hiện tấn công sẽ gửi tín hiệu báo hiệu có sự tấn công hoặc thâm nhập đến modul phản ứng. Lúc đó modul phản ứng sẽ kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị. Tại modul này, nếu chỉ đưa ra các cảnh báo tới các người quản trị và dừng lại ở đó thì hệ thống này được gọi là hệ thống phòng thủ bị động. Modul phản ứng này tùy theo hệ thống mà có các chức năng và phương pháp ngăn chặn khác nhau. Dưới đây là một số kỹ thuật ngăn chặn.

- Kết thúc tiến trình: Cơ chế của kỹ thuật này là hệ thống IPS gửi các gói tin nhằm phá huỷ tiến trình bị nghi ngờ. Tuy nhiên phương pháp này có một số nhược điểm. Thời gian gửi gói tin can thiệp chậm hơn so với thời điểm tin tặc bắt đầu tấn công, dẫn đến tình trạng tấn công xong rồi mới bắt đầu can thiệp.
- Huỷ bỏ tấn công: Kỹ thuật này dùng tường lửa để hủy bỏ gói tin hoặc chặn đường một gói tin đơn, một phiên làm việc hoặc một luồng thông tin tấn công. Kiểu phản ứng này là an toàn nhất nhưng lại có nhược điểm là dễ nhầm với các gói tin hợp lệ.
- Thay đổi các chính sách của tường lửa: Kỹ thuật này cho phép người quản trị cấu hình lại chính sách bảo mật khi cuộc tấn công xảy ra. Sự

cấu hình lại là tạm thời thay đổi các chính sách điều khiển truy nhập bởi người dùng đặc biệt trong khi cảnh báo tới người quản trị.

- Cảnh báo thời gian thực: Gửi các cảnh báo thời gian thực đến người quản trị để họ nắm được chi tiết các cuộc tấn công, các đặc điểm và thông tin về chúng.
- Ghi lại vào tệp tin: Các dữ liệu của các gói tin sẽ được lưu trữ trong hệ thống các tệp tin log. Mục đích để các người quản trị có thể theo dõi các luồng thông tin và là nguồn thông tin giúp cho modul phát hiện tấn công hoạt động.

1.3.2. Các kiểu hệ thống IPS

Có hai kiểu kiến trúc IPS chính là IPS ngoài luồng và IPS trong luồng.

a. IPS ngoài luồng: Hệ thống IPS ngoài luồng không can thiệp trực tiếp vào luồng dữ liệu. Luồng dữ liệu vào hệ thống mạng sẽ cùng đi qua tường lửa và IPS. IPS có thể kiểm soát luồng dữ liệu vào, phân tích và phát hiện các dấu hiệu của sự xâm nhập, tấn công.

b. IPS trong luồng: Vị trí IPS nằm trước bức tường lửa, luồng dữ liệu phải đi qua IPS trước khi tới bức tường lửa.

CHƯƠNG 2: TÌM HIỂU VỀ HỆ THỐNG QUẢN LÝ SỰ KIỆN VÀ GIÁM SÁT AN NINH MẠNG (SIEM)

2.1. Tổng quan về hệ thống SIEM

Sercurity information event management (SIEM) là một giải pháp hoàn chỉnh cho phép các tổ chức thực hiện việc giám sát các sự kiện an toàn thông tin cho một hệ thống. SIEM là sự kết hợp một số tính năng của quản lí thông tin an ninh (SEM) và quản lí sự kiện an ninh (SIM). Trong đó hệ thống mã nguồn mở SIEM có thể được tách làm hai chức năng:

Sercurity event management (SEM): Thu thập các event log data do các thành phần (thiết bị, ứng dụng) trong hệ thống tạo ra. Sau đó tập trung hóa việc lưu trữ và xử lý, phân tích các sự kiện rồi lập báo cáo, đưa ra thông báo, cảnh báo liên quan đến an ninh của hệ thống.

Sercurity information management (SIM): Thông tin được lưu trữ từ SIM, được sử dụng để báo cáo dữ liệu đăng nhập cho bất kì thời gian nhất định.

SIM và SEM thường bị nhầm lẫn với nhau nhưng thực ra giữa chúng tồn tại những điểm giống và khác nhau cơ bản sau:

SEM giám sát hệ thống và phân tích các event gần như trong thời gian thực để giúp phát hiện các mối đe dọa an ninh, các dấu hiện bất thường nhanh nhất có thể nhưng cũng chính vì thế mà lượng dữ liệu sự kiện đổ về nó rất nhiều và nó không cung cấp khả năng lưu trữ lâu dài cho các dữ liệu log.

Ngược lại, SIM tuy không có khả năng thu thập và xử lý các sự kiện trong thơi gian thực nhưng lại mạnh về quản lý log và có thể lưu trữ một lượng lớn dữ liệu log trong một thời gian dài.

Security Information and Event Management (SIEM) là sự kết hợp của SEM và SIM lại với nhau nhằm khắc phục những hạn chế của chúng.

- Thu thập log: Thu thập dữ liệu từ nhiều nguồn, bao gồm cả mạng, bảo mật, máy chủ, cơ sở dữ liệu, ứng dụng…cung cấp khả năng hợp nhất dữ liệu được giám sát tránh để mất các sự kiện quan trọng.

- Tương quan giữa các sự kiện: Tìm kiếm các thuộc tính chung và liên kết các sự kiện với nhau.
- Nhóm các sự kiện giống nhau.
- Phân tích và luồng thông tin.

Ba yếu tố chính triển khai cho SIEM:

- Tầm nhìn trước mối đe dọa thời gian thực.
- Vận hành hiệu quả.
- Tính tuân thủ và các yêu cầu riêng cho hệ thống quản lý log.

2.2. Hoạt động của hệ thống SIEM

2.2.1. Thu thập thông tin

Mục đích của việc thu thập thông tin là để nắm bắt các thông tin từ các thiết bị an ninh khác nhau và cung cấp nó cho các máy chủ để chuẩn hoá và phân tích tiếp.

Chính sách thu thập thông tin có thể thiết lạp 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 điều tiết sự kiện an ninh và quản lý những thông tin, nếu không sẽ có rất nhiều sự kiện an ninh trong hệ thống mạng làm cho chúng ta lúng túng không biết bắt đầu từ đâu.

SIEM thu thập các bản ghi Log từ rất nhiều các thiết bị khác nhau, việc truyền các bản ghi log từ các thiết bị nguồn tới SIEM cần được giữ bí mật, xác thực và tin cậy bằng việc sử dụng syslog hoặc các giao thức SNMP, OPSEC, SFTP, IDXP.

Có 2 cách để SIEM thu thập bản ghi Log từ các thiết bị nguồn đó là: sử dụng phương thức push log hoặc sử dụng phương thức pull log.

2.2.2. Chuẩn hoá và tổng hợp sự kiện an ninh

Sau khi thu thập thông tin các bản ghi log sec được SIEM chuẩn hoá để đưa về cùng một định dạng. Nếu các thiết bị không hỗ trợ các giao thức này chúng ta phải sử dụng các Agent. Đó là một điều cần thực hiện lấy các bản ghi

log có định dạng mà SIEM có thể hiểu được. Việc cài đặt các Agent có thể kéo dài quá trình triển khai SIEM nhưng chúng ta sẽ có những bản ghi log theo dạng chuẩn mong muốn.

Sau quá trình chuẩn hoá các bản ghi log thì quá trình tổng hợp sự kiện an ninh sẽ diễn ra. Mục đích của quá trình này là tổng hợp các sự kiện an ninh thuộc cùng kiểu để thấy được sự tổng thể của hệ thống. Điều này gần giống với quá trình phân tích tương quan sự kiện.

2.2.3. Phân tích tương quan sự kiện an ninh

Quá trình phân tích tương quan sự kiện này 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. Qúa trình này đòi hỏi việc sử lý tập trung và chuyên sâu vì chúng phải hiểu được một tấn công diễn ra như thế nào. Mà thông thường sẽ sử dụng các thông tin dữ liệu trong cơ sở dữ liệu có sẵn liên kết với các thông tin về bối cảnh trong môi trường mạng của hệ thống. Các thông tin này có thể như các thư mục người dùng, các thiết bị và các vị trí của chúng. Điều tuyệt vời là SIEM có thể cập nhật từ các sự kiện an ninh mới mà dữ liệu gửi về.

2.2.4. Cảnh báo và báo cáo

SIEM cung cấp 3 cách để thông báo tới quản trị viên về một cuộc tấn công hay một hành vi bất thường đang sảy 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. Thứ 3 là các quản trị viên theo dõi giám sát SIEM theo thời gian thực thông qua giao diện web. Các IDS thông thường đưa ra các thông báo giả nhưng với SIEM nó 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 tuỳ thuộc vào mức độ của sự kiện an ninh.

2.2.5. Lưu trữ

Khi phân tích thì các dữ liệu được lưu trữ trực tuyến và khi không còn cần thiết thì chúng sẽ được chuyển tới nơi khác lưu trữ dài hạn. Dữ liệu được lưu trữ

dưới dạng đã chuẩn hoá nhằm đẩy nhanh tốc độ tìm kiếm sử dụng sau này. Thông thường chúng được lưu trữ dưới dạng nén và có thể được mã hoá. SIEM cung cấp khả năng lưu trữ đến hàng trăm triệu sự kiện khác nhau.

2.3. OSSIM

Hiện tại vấn đề thu thập và quản lý các sự kiện từ tất cả các thiết bị CNTT như: FW, IPS/IDS, Servers, Switch, App, Router,.. đang là vấn đề quan trọng với doanh nghiệp, nếu không có việc thu thập và quản lý log tập trung và lâu dài sẽ làm ảnh hưởng đến quá trình phân tich và tìm ra những sự cố trong qua trình vận hành, các thông tin bị rò rỉ môt cách tràn lan trong doanh nghiệp, gây ra những thiệt hại vê kinh tế cho doanh nghiệp, vì vây giải pháp SIEM của AlientVault đã ra đời và đáp ứng được các yêu cầu đang tồn đong trong cách quản lý thu thập tất các sự kiện, các truy cập trái phép vào hệ thống CNTT, giúp người quản trị dễ dàng phát hiện các vấn đề sau:

- Hệ thống giám sát an ninh tập trung của AlientVault sẽ thu thập log và giám sát, báo cáo về các hoạt động xảy ra trên các hệ thống Firewall, server, Antivirus system, IPS system, các truy cập từ xa, các thiết bị VPN, thiết bị định tuyến….
- Ngoài việc thu thập thông tin về nguy cơ và sự cố an toàn mạng, hệ thống này còn giúp các doanh nghiệp chủ động và dễ dàng nhận dạng, sử lý nhanh các nguy cơ này.
- AlientVault đáp ứng nhu cầu về việc trang bị một hệ thống giám sát an ninh tập trung chủ động, dễ dàng cài đặt và sử dụng, tiết kiệm thời gian và nhân lực cho quá trình quản trị.
- Lưu trữ thông tin dài hạn để làm chứng cứ, phục vụ điều tra theo các tiêu chuẩn về bảo mật công nghệ thông tin.

Open Source Security Information Managerment (OSSIM): là một mã nguồn mở quản lý thông tin và sự kiện an ninh bao gồm tập hợp các công cụ được thiết kế để trợ giúp các nhân viên quản trị phát hiện và phòng chống xâm nhập.

OSSIM thu thập các thông tin từ các sensor như snort, ARPwatch, Ntop, …..và đọc các thông tin cảnh báo từ các loại thông tin hiện nay như CheckPoint, RealSecure, server Unix…….phân tích đánh giá mức độ an ninh và rủi ro của các sự kiện an toàn thông tin.

AlientVault OpenSource SIEM là một hệ thống an ninh toàn diện bao gồm từ mức độ phát hiện lên đến một mức độ điều hành tạo ra các số liệu và báo cáo. AlientVault được cung cấp như một sản phẩm bảo mật cho phép bạn tích hợp vào một giao diện điều khiển tất cả các thiết bị và các công cụ bảo mật có sẵn trên mạng của bạn, cũng như cài đặt các công cụ bảo mật có uy tín nguồn mở như snort, OpenVas, Ntop, OSSEC……

2.3.1. Các chức năng quan trọng của OSSIM

2.3.1.1. Bảo vệ thông tin và tài nguyên quan trọng

Thực hiện theo dõi theo thời gian thực các tài nguyên quan trọng trong hệ thống như: File server, các hệ thống kiểm soát và các cơ sở dữ liệu giúp nhận ra những trạng thái bất ổn ngay cả khi các hệ thống đang hoạt động bình thường. OSSIM phân tích từng mảnh nhỏ các thông tin mà nó thu thập để nhận ra những điểm yếu trong hệ thống từ đó đưa ra những hành động cảnh bảo sớm cho người quản trị.

2.3.1.2. Cải thiện khả năng điều tra và khắc phục sự cố

Áp lực trong việc thu thập và lưu trữ dữ liệu có liên quan đến kiểm toán từ nhiều nguồn khác nhau. Việc quản lý nhật ký không hiệu quả, việc tìm kiếm thông tin từ hàng Terabytes dữ liệu là gần như không thể. Trong khi các sự kiện này thực sự cần thiết trong để hỗ trợ cho việc kiểm toán và điều tra. AlientVault có thể giúp hệ thống lưu trữ và quản lý một lượng lớn dữ liệu nhật ký đồng thời cho phép nhanh chóng xử lý, phân tích điều tra hoặc tự động báo cáo theo cấu hình của người quản trị hệ thống.

2.3.1.3. Theo dõi hành động bất thường của người dùng

AlientVault cung cấp khả năng quan sát toàn diện hệ thống, cho biết ai đang kết nối và làm gì trên hệ thống mạng. AlientVault liên kết các thông tin người dùng như: tên, vai trò cùng với thông tin chính xác về các ứng dụng và vị trí trong mạng để cung cấp khả năng xác minh các kết nối giữa người dùng thực tế (không chỉ dựa vào IP Address) với những hành động có mức độ rủi ro cao.

2.3.1.4. Cung cấp sự tuân thủ với chi phí thấp

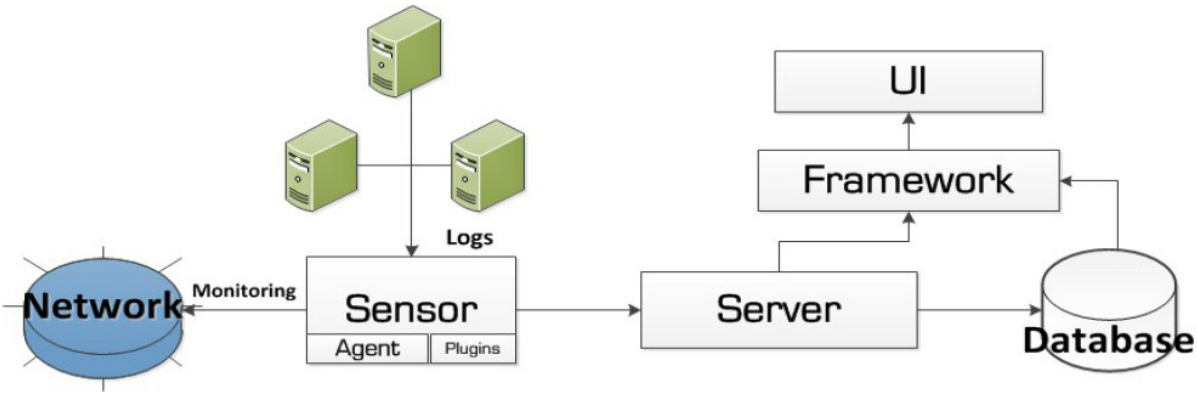
Để vượt qua được các bước trong quá trình kiểm toán, hệ thống mạng của một tổ chức phải đủ khả năng tự động chống đỡ trước các tấn công và bảo vệ các thông tin bí mật. AlientVault xây dựng sẵn và cung cấp các gói cho phép đáp ứng các tuân thủ này theo các yêu cầu cụ thể. Kết quả là các báo cáo tuân thủ sẽ được tự động thực hiện và kiểm soát tuân thủ được giám sát liên tục, hiệu quả mang lại nhanh chóng trong khi chi phí thấp.

2.3.2. Kiến trúc hệ thống OSSIM

Công việc cốt lõi của OSSIM là có trách nhiệm thu thập sự kiện, quản lý và tương quan, cũng như đánh giá rủi ro và cảnh báo, các công cụ mày được viết bằng C. Các công cụ khác được cung cấp bởi OSSIM bao gồm agent sử dụng để thu thập thông tin hệ thống mạng, một giao diện dựa trên nền web PHP, và Python deamon, framework, chịu trách nhiệm quản lý và giám sát các bộ phận khác của OSSIM. Để lưu trữ dữ liệu, OSSIM dựa trên cơ sở dữ liệu SQL.

Để đơn giản quá trình quản lý thông tin trên mạng bao gồm các host hay firewall hay IDS, SERVER….., OSSIM là tập hợp các thành phần riêng lẻ được tích hợp lại, cho phép chúng ta điều khiển qua dao diện web.

Một hệ thống OSSIM điển hình được triển khai bao gồm bốn nhân tố: Sensor, Server, Database, Framework. Tất cả các thành phần của OSSIM là các module độc lập và có thể cấu hình theo nhu cầu của người quản trị. Tất cả các thành phần này có thể đặt ở các phần cứng khác nhau. Tách riêng từng thành phần hoặc đặt chúng chung trên cùng một thiết bị.



Hình 2. Kiến trúc hệ thống OSSIM

Trong đó:

- Sensor: các thiết bị được triển t\khai trong mạng để giám sát các hoạt động mạng. Chúng thường là:
  - Các detector và monitor, thu thập dữ liệu một cách thụ động qua các bản mẫu và được lưu trong các Agent của OSSIM.
  - Gồm các Agent OSSIM : có vai trò nhận dữ liệu từ các host trong mạng như router hoặc firewall, giao tiếp và gửi dữ liệu các sự kiện tới server quản lý trung tâm và được cấu hình trong file Output.py trong ossim-agent.
  - Một cấu hình senser OSSIM điển hình gồm các chức năng như: IDS (Snort), quét lỗ hổng (Nessus), phát hiện sự bất thường (Spade, p0f, pads,……), giám sát mạng (Ntop), thu thập thông tin từ router, firewall, IDS. Các công cụ này được tích hợp vào cấu hình của sensor.
- Server
  - Công việc chính là chuẩn hoá, thu thập, ưu tiên hoá, đánh giá rủi ro và thiết lập mối tương quan các bộ máy bên trong. Các công việc duy trì hoạt động như sao lưu, lập lịch sao lưu, tạo các thư mục online hoặc tiến hành quét toàn bộ hệ thống.
  - Việc thu thập thông tin, chuẩn hoá và đánh giá rủi ro cho hệ thống, phân loại các loại tập tin, các dấu hiệu bất thường cho hệ thống sẽ được gửi lên Framework để phân loại hành động

và mức độ cảnh báo cho hệ thống và đưa đến database để lưu trữ các sự kiện, các thông tin cho hệ thống qua port 3306.

- Framework: quản lý các thành phần OSSIM và kết nối chúng lại với nhau. Cung cấp giao diện web, quản lý cấu hình thành phần OSSIM và truyền thông.
- Cơ sở dữ liệu: cơ sở dữ liệu lưu trữ các sự kiện, các thông tin hữu ích cho việc quản lý của hệ thống. Nó là cơ sở dữ liệu SQL.

2.3.3. Các công cụ được tích hợp trong OSSIM

2.3.3.1. Snort IDS

- Là một công cụ mã nguồn mở có khả năng phát hiệm xâm nhập , những dấu hiệu bất thường , phân tích lưu lượng và gói tin đăng nhập trên các mạng IP . Nó có thể thực hiện phân tích các giao thức , các nội dung tìm kiếm và có thể phát hiện hàng loạt các cuộc tấn công và thăm dò như tấn công tràn bộ đệm, quét cổng tàng hình , tần công CGI , thăm dò SMB …
- Snort bao gồm nhiều thành phần , với mỗi thành phần thực hiện một chức năng riêng:
  - Module giải mã gói tin.
  - Module tiền xử lý.
  - Module phát hiện.
  - Module log và cảnh báo.
  - Module kết xuất thông tin.
- Nessus: Là công cụ quét lỗ hổng bảo mật dùng để kiểm tra tính an toàn cho một hệ thống, tính bảo mật của một trang web từ xa, máy tính cục bộ hay những thiết bị bảo vệ thông tin…
- Các thành phần chính:
  - Nessus Engine: nhận, thực thi và trả lời lại các yêu cầu quét của người dùng. Việc quét các lỗ hổng được thực hiện theo các chỉ dẫn của các plugin (một tập các câu lệnh script của ngôn ngữ kịch bản NASL).
  - Nessus Plugin: hệ thống file của ngôn ngữ kịch bản NASL, gồm các file định nghĩa .inc và file kịch bản .nasl.
  - Nessus Sever(Nessusd): thực hiện nhân các yêu cầu quét của người dùng sau đó phân tích, tổng hợp , trả lại lại kết quả cho Nessus Client.

- Nessus client: hiện thị kết quả quét lại cho người dùng thông qua trình duyệt web.
- Nessus Knowledge Base: "Cơ sở dữ liệu đã biết" của Nessus cho phép các Plugin sau tận dụng dữ liệu kết quả của Plugin trước đó. Điều này giúp Nessus dễ dàng mở rộng và tăng tốc độ thực thi.

2.3.3.2. Ntop: Giám sát mạng

- Là công cụ được dùng để giám sát và đo lường lưu lượng mạng. Ntop cung cấp các biểu đồ và các số liệu thống kê từ phân tích các lưu lượng mạng được giám sát. Ntop đồng thời cũng chứa rất nhiều thông tin và các loại dữ liệu chạy trong mạng , tạo một hồ sơ cho phép theo dõi từng người dùng trong mạng.
- Công việc chính của Ntop:
  - Đo lưu lượng
  - Giám sát lưu lượng.
  - Lập kế hoạch và tối ưu hóa mạng.
  - Phát hiện các vi phạm an ninh mạng.

2.3.3.3. Nagios: Giám sát hiệu năng

- Là công cụ giám sát các ứng dụng , dịch vụ điều hành hệ thống , giao thức mạng, hệ thống số liệu và các thành phần cơ sở hạ tầng.
- Nagios có các chức năng sau:
  - Giam sát trạng thái hoạt động của các dịch vụ mạng (SMTP,HTTP, ICMP, FPT , SSH, DNS, web proxy, name server, TCP port, UDP port, cơ sở dữ liệu, my SQL….).
  - Giam sát các tài nguyên các máy phục vụ và các thiết bị đầu cuối : Tình trạng sử dụng CPU, tình trạng sử dụng ổ đĩa cứng, tình trạng sử dụng bộ nhớ trong và swap, số tiến trình đang chạy, các tệp log hệ thống…
  - Giam sát các thông số an toàn các thiết bị phần cứng trên host như: nhiệt độ CPU , tốc độ quạt, pin, giờ hệ thống…
  - Giám sát các thiết bị mạng có IP như swich, router và máy in , Nagios có thể theo dõi tình trạng hoạt động của từng trạng thái bật tắt của từng cổng, lưu lượng băng thông qua mỗi cổng.

- Cảnh báo cho người quản trị bằng nhiều hình thức như email, tin nhắn bằng âm thanh nếu có thiết bị, dịch vụ gặp trục trặc.
- Tổng hợp lưu trữ và báo cáo định kỳ về tình trạng hoạt động của mạng.

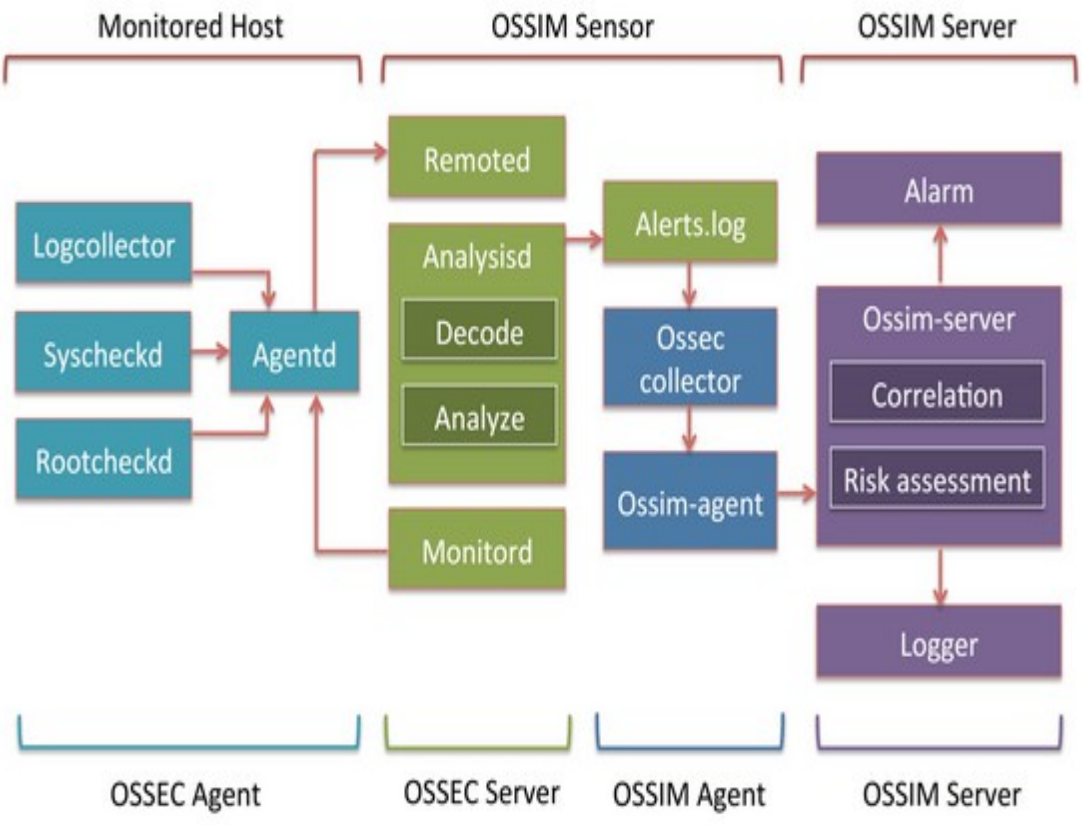
2.3.3.4. Ngoài ra còn có

- Oiris , Snare: host IDS.
- Spade, HW Aberant Behaviuor: phát hiện bất thường.
- Arpwatch, P0f,Pads, Fprobe: giám sát thụ động.
- Nmap: quét mạng.
- Acid/Base: phân tích pháp lý.
- OSVDB: cơ sở dữ liệu lỗ hổng.

2.3.4. OCCEC

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.

2.3.4.1. Kiến trúc của OSSEC



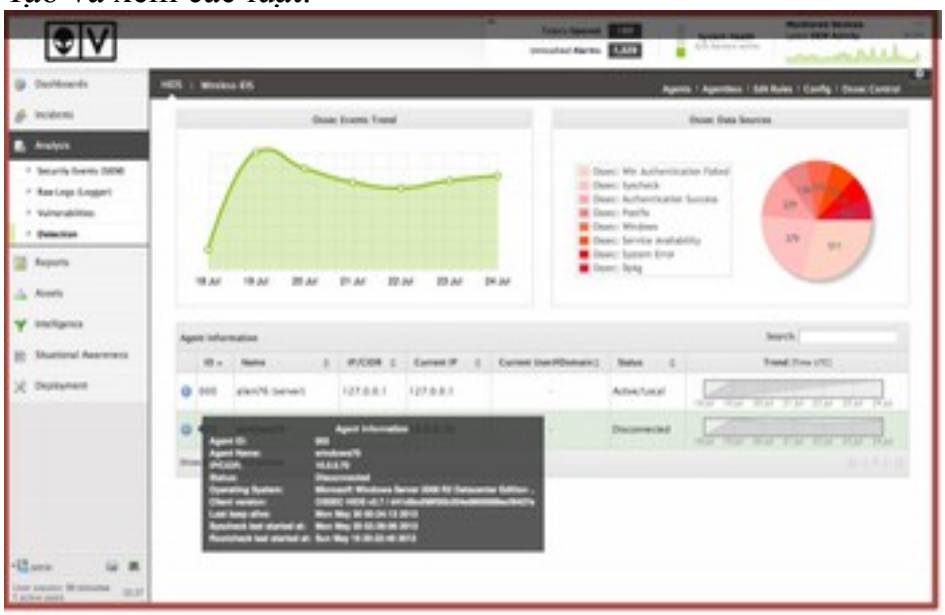
Hình 2. Kiến trúc tích hợp OCCEC

Trong đó:

- OSSEC Agent:
  - Logcollectord : đọc các bản ghi.
  - Syscheckd : kiểm tra tính toàn vẹn file.
  - Rootcheckd: Phát hiện các malware/rootkit.
  - Agentd: chuyển tiếp dữ liệu đến máy chủ.
- OSSEC Server:
  - Remoted: Nhận dữ liệu từ các bộ cảm biến (Agent).
  - Analysisd: Sử lý dữ liệu.
  - Monitord: Giám sát các bộ cảm biến (Agent).

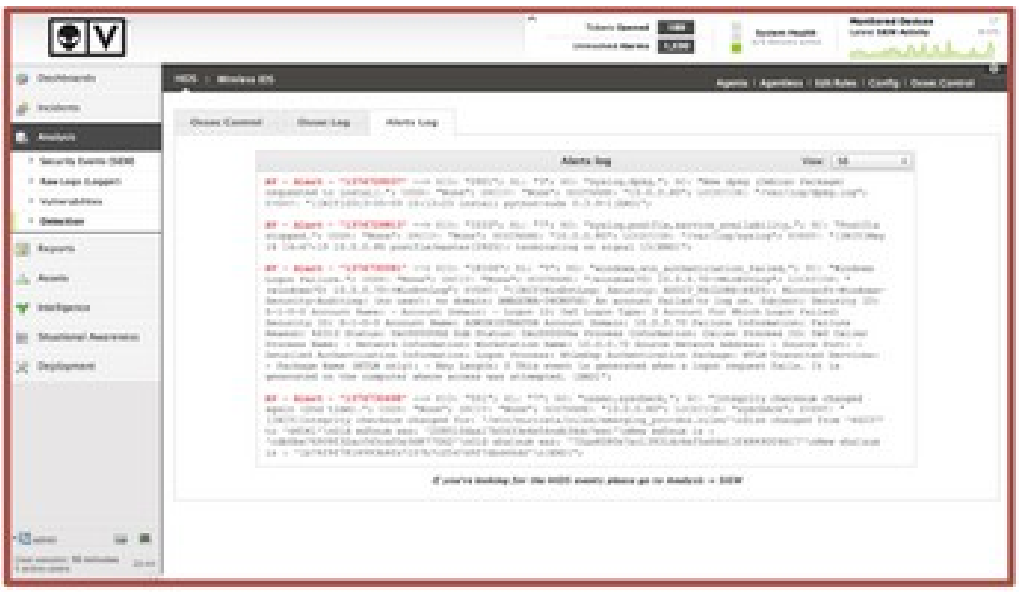
2.3.4.2. Giao diện đồ hoạ của OSSEC

- Trạng thái giám sát.
- Xem các sự kiện.
- Quản lý điều khiển các bộ cảm biến (Agent).
- Quản lý cấu hình.
- Tạo và xem các luật.



Hình 2. Giao diện đồ họa của OSSEC

- Xem các bản ghi (log).
- Quản lý điều khiển các server.
- Quản lý các triển khai.
- Tạo các báo cáo PDF/HTML



Hình 2. Xem các bản ghi (log)

CHƯƠNG 3: KHẢO SÁT, PHÂN TÍCH VÀ ĐỀ XUẤT THIẾT KẾ GIẢI PHÁP OSSIM CHO HỌC VIỆN

3.1. Khảo sát học viện

3.1.1. Mục tiêu

Mục tiêu: Thiết kế xây dựng hệ thống mạng máy tính an toàn dựa trên quy trình đã học.

Yêu cầu: Xây dựng mạng máy tính cho Học viện Kỹ thuật mật mã theo quy trình đã học. Việc xây dựng phải thể hiện được tất cả các bước trong quy trình. Thông tin về Học viện như sau:

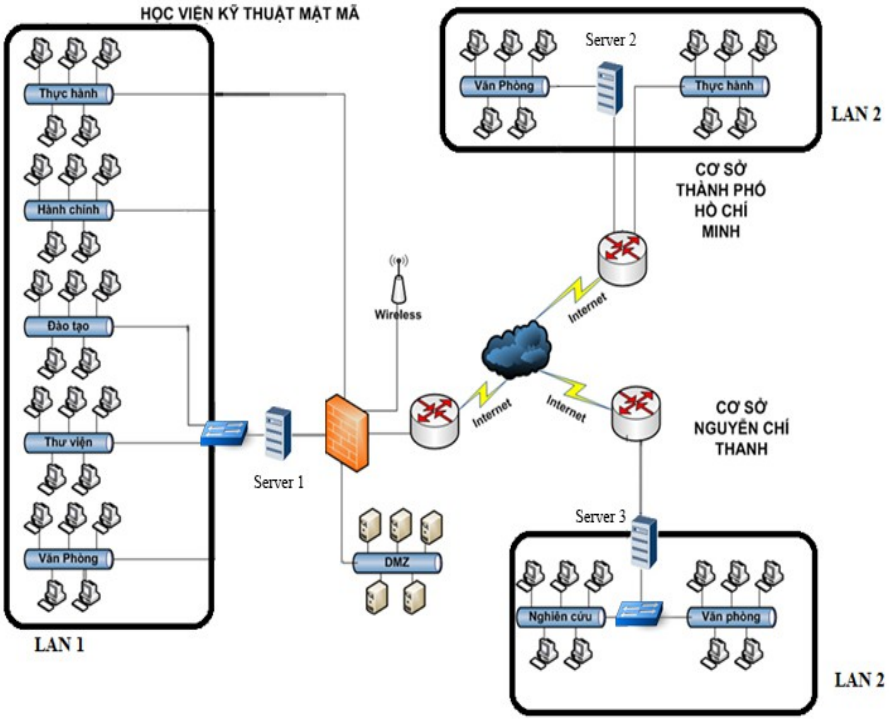
Học viện gồm: 2 cơ sở: Học viện tại đường Chiến Thắng - Hà Nội (cơ sở 1), Trung tâm nghiên cứu tại Nguyễn Chí Thanh – Hà Nội (cơ sở 2), và cơ sở học viện phía Nam tại TP Hồ Chí Minh (cơ sở 3)

Cơ sở 1: Gồm có các phòng ban tại học viện: hành chính, đào tạo, thư viện, các khoa, có các phòng thực hành cho sinh viên, khu vực DMZ (hiện chưa triển khai dịch vụ gì).

Cơ sở 2: gồm các phòng nghiên cứu, mạng văn phòng.

Cơ sở 3: gồm các phòng thực hành, mạng văn phòng của cơ sở.

Các cơ sở của Học viện chưa kết nối với nhau thành một mạng.



Hình 3. Mô hình khảo sát mạng máy tính tại Học viện.

3.2. Phân tích học viện

3.2.1. Xác định các tài sản trên mạng

Tài sản trên mạng bao gồm:

- Các thiết bị phần cứng như switch, router, dây cáp, các máy chủ máy trạm, hạ tầng mạng nói chung.
- Các phần mềm, các tệp tin, các dữ liệu của Học viện được lưu trữ trên các máy chủ.

3.2.2. Các loại rủi ro

Các rủi ro có thể ảnh hưởng tới hệ thống mạng:

- Các tấn công vào khu vực DMZ khi mà các vùng đó chạy dịch vụ: web, mail, DNS.
- Các tấn công tới người dùng (Social engineering) trong mạng.
- Tấn công vào mạng LAN của Học viện.
- Tấn công nghe trộm trên đường truyền.
- Tấn công vào từ chối dịch vụ vào hệ thống mạng văn phòng của các phòng, ban.
- Tấn công bằng mã độc vào hệ thống mạng thông qua người dung hoặc các phương tiện khác.

- Mạng chưa có hệ thống dự phòng, hệ thống cân bằng tải, vv.. do vậy tính sẵn sàng của hệ thống còn nhiều điểm hạn chế.
- Xâm nhập vật lý tới các thiết bị cụ thể của hệ thống.
- Thiên tai, lũ lụt vv…

3.2.3. Xác định các yêu cầu của học viện

Tính sẵn sàng:

- Hệ thống mạng văn phòng của Học viện yêu cầu sẵn sàng trong suốt giờ hành chính từ 7h-19h hàng ngày. (Nối các phòng ban ở các cơ sở với site trung tâm).
- Hệ thống DMZ cung cấp các dịch vụ cho sinh viên cần tính sẵn sàng liên tục để sinh viên có thể truy câp, download, upload các tài liệu, phục vụ cho việc học tập.
- Các đường nối từ switch lớp Access lên switch lớp Distribute và Core đều có đường dự phòng.
- Đối với đường Internet có thêm đường dự phòng.

Tính bí mật:

- Tiến hành phân loại các loại tệp tin, thư mục bằng việc gắn nhãn cho chúng, từ đó phân quyền truy cập và mã hóa các file dữ liệu tùy theo nhãn của chúng.
- Trong các phần mềm nếu như sử dụng mã hóa thì phải phải sử dụng mã hóa AES chế độ CBC, dùng Diffie-hellman cho tra đổi khóa, RSA cho việc ký số.

Tính toàn vẹn:

- Tiến hành việc ký số (và mã) tới các công văn, các file dữ liệu nhạy cảm để đảm bảo tính toàn vẹn của chúng khi được lấy gửi đi trên đường truyền.
- Sử dụng thuật toán SHA-1trong các chương trình cần đảm bảo tính toàn vẹn của dữ liệu.

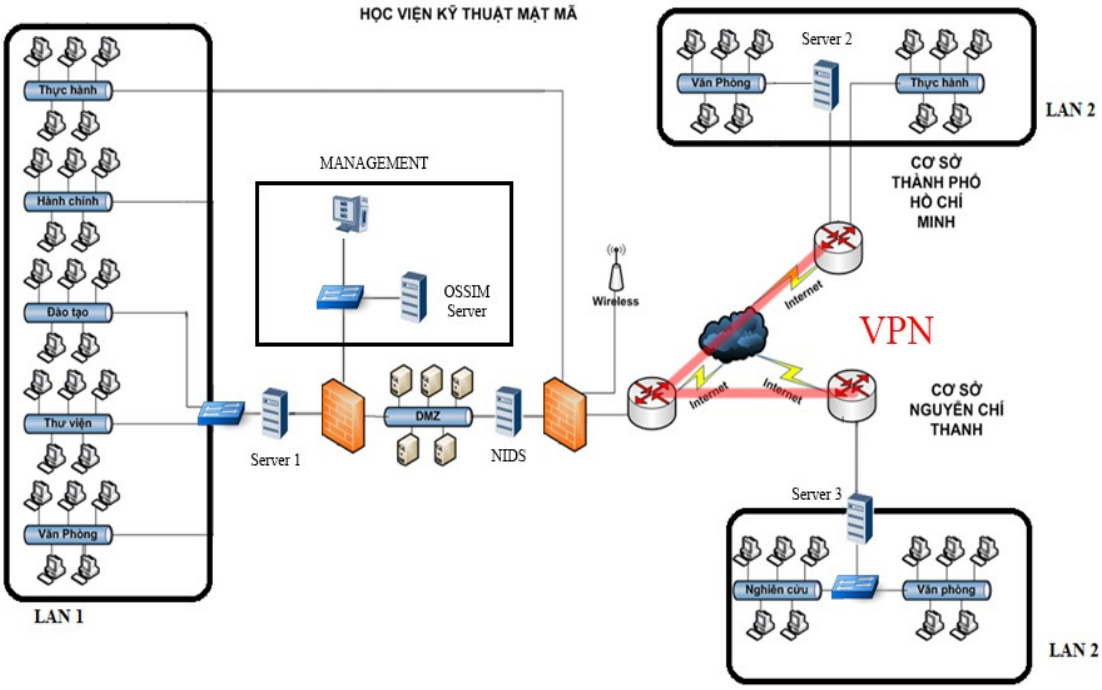
Chính sách an toàn và các thành phần cần thiết khác:

- Sử dụng firewall: Thực thi các chính sách an toàn chung của toàn hệ thống.

- Sử dụng hệ thống phòng chống phát hiện xâm nhập để phát hiện các lưu thông bất thường trên mạng, từ đó cảnh báo tới người quản trị và có những biện pháp ngăn chặn nhưng lưu thông bất thường này.
- Chia VLAN theo các phòng, để tiện lợi trong việc phân quyền, trao đổi dữ liệu, tránh truy cập thông tin trái phép giữa các phòng ban.
- Ban hành các chính sách truy cập, chính sách quy định trách nhiệm, tới các nhân viên, sinh viên, quản trị trong hệ thống học viện.
- Xây dựng chính sách đảm bảo an toàn cho các thành phần sau:
    - Máy chủ dịch vụ: Web, mail, ftp.
    - Máy chủ nội bộ.
    - Máy tính cá nhân trong mạng nội bộ.
    - Chính sách chung về chia sẻ và truy cập dữ liệu cho nhân viên các phòng ban học viện.
- Xây dựng hệ thống giám sát an ninh mạng để giám sát toàn bộ hoạt động của hệ thống mạng Học viện.

3.3. Đề xuất thiết kế giải pháp OSSIM cho học viện.

Sau quá trình đã khảo sát và phân tích học viện như trên chúng em xin đề xuất thiết kế giải pháp OSSIM: xây dựng một hệ thống giám sát an ninh mạng để giám sát toàn bộ hoạt động của hệ thống mạng học viện như sau:



Hình 3. Sơ đồ Học viện đề xuất.

➢ **Cấu hình thiết bị:**

- **Tường lửa (Firewall):**
  - Firewall đề xuất thêm: (thiết bị ASA5520-BUN-K9 của Cisco) có nhiệm vụ quản lý lưu lượng và các truy cập mạng giữa các khu vực LAN, Mabagement và DMZ. Ngoài ra ASA5520-BUN-K9 còn có chức năng cân bằng tải nâng cao khả năng điều khiển lưu lượng. Cisco ASA 5520 tích hợp cả IDS/IPS nên được sử dụng để cài đặt IDS/IPS luôn cho khu vực DMZ nhằm phát hiện những dấu hiệu tấn công vào khu vực này.
- **Mạng riêng ảo (VPN):**
  - Thực hiện theo mô hình kết nối VPN LAN to LAN.
  - Học viện có 3 cơ sở. Tại cơ sở chính ở 141 Chiến Thắng, Thanh Trì, Hà Nội sử dụng Vigor3300V và cơ sở 2 và 3 sử dụng Vigor2900V.
  - Giúp các nhân viên các văn phòng làm việc ở các cơ sở 2 và 3 có thể truy cập dữ liệu tại văn phòng cơ sở chính thông qua mã hóa của kênh VPN, nhằm tránh rò rĩ những thông tin quan trọng.
- **OSSEC:**
  - Sử dụng cài đặt các OSSEC cho các máy chủ trong vùng DMZ và tất cả các máy trong vùng LAN.
  - Việc sử dụng OSSEC nó tương tự như là một HIDS để phát hiện các cuộc xâm nhập,tấn công.
- **NIDS:**
  - OS: CentOS 7.
  - CPU: E8400 3.0GHz – 2 Cores.
  - RAM: 2GB.
  - DISK: 500GB.

  Thiết bị phát hiện xâm nhập dựa vào lưu lượng mạng.
- **OSSIM Server:**
  - OS: Debian Linux.
  - CPU: E5620 2.4GHz – 4 Cores / 8 threads.
  - RAM: 24GB.

- STORAGE: 3TB.
- Thiết bị chính dùng để quản lý thông tin và sự kiện an ninh.

➢ **Phân tích hệ thống đã xây dựng:**

Việc xây dựng mô hình trên giúp giám sát, đảm bảo an ninh cho hệ thống mạng của Học viện bởi các cuộc tấn công ngoài và trong mạng Học viện.

- **Các cuộc tấn công từ Internet:**

Mạng Internet vừa là một trợ thủ đắc lực và cũng là một hiểm họa to lớn cho mọi người truy cập vào internet.

Các loại tấn công này thường nhằm vào người dùng hoặc các lỗ hổng trong hệ thống nhằm mục đích:

- Lấy cắp thông tin người dùng (có thể là bất kì ai trong hệ thống).
- Lấy cắp dữ liệu ở vùng DMZ (mail ,web , DNS).
- Truy nhập vượt tường lửa để tới vùng DMZ.
- Làm gián đoạn hệ thống, hệ thống chậm đi.

Tấn công từ chối dịch vụ DDoS- Botnet

Hiện nay, hàng loạt phần mềm độc hại (malware) rất nguy hiểm như Zeus, SpyEye, Filon, Clod Bugat, Kraken, Grum, Bobax, Pushdo, Rustock, Bagle, Mega- D... đã được thiết kế để tạo ra các loại mạng botnet với các chức năng khác nhau: Botnet để tấn công DDoS, lấy cắp thông tin về người dùng trong hệ thống và gửi thư rác spam. Hacker tạo ra ngày càng nhiều malware với các môđun phức tạp, chứa các lệnh khác nhau để trao đổi, xây dựng ra các mạng Botnet riêng với nhu cầu, mục đích khác nhau.

Ví dụ như, Grum là mạng Botnet để phát tán thư rác, hoạt động theo chế độ ẩn của rootkit, lây nhiễm vào khóa registry AutoRun, để luôn luôn được kích hoạt và phát tán hàng chục tỷ thư rác mỗi ngày. Zeus và SpyEye được thiết kế để lập mạng Botnet lấy cắp thông tin về người dùng trong hệ thống và gửi về một Domain trung gian, sau đó được chuyển tiếp đến một Domain chứa cơ sở dữ liệu cung cấp cho hacker. Phổ biến nhất là các mạng Botnet được sử dụng để tấn công từ chối dịch vụ, tấn công DDoS qui mô lớn.

Khi xảy ra các cuộc tấn công từ chối dịch vụ vào hệ thống của học viện việc làm cho lưu lượng mạng tăng đột biến sẽ được các thiết bị phát hiện xâm nhập NIDS phát hiện.

Tấn công lỗ hổng bảo mật web

+ Loại thứ nhất: là các tấn công như SQL injection được sử dụng ngày càng nhiều. Đặc biệt, các website sử dụng chung server hoặc chung hệ thống máy chủ của nhà cung cấp dịch vụ ISP dễ bị trở thành cầu nối tấn công sang các đích khác.

➔ Khi xảy ra các cuộc tấn công như thế này thì việc lấy log sẽ được gửi từ các thiết bị Router, tường lửa, NIDS,OSSEC được cài trong các máy chủ web…

+ Thứ hai : là tấn công vào mạng nội bộ LAN thông qua VPN.

➔Để tấn công vào được mạng nội bộ LAN thì việc thu thập log sẽ được lấy từ các thiết bị router,máy chủ nội bộ(cơ sở 2 và 3), router,tường lửa,NIDS,máy chủ nội bộ.

+ Thứ ba: là hình thức tấn công vào cơ sở dữ liệu của hệ thốngvới mục đích lấy cắp dữ liệu, phá hoại, thay đổi nội dung. Hacker xâm nhập vào cơ sở dữ liệu của hệ thống, từng bước thay đổi quyền điều khiển và tiến tới chiếm toàn quyền điều khiển cơ sở dữ liệu. Trong nhiều vụ, hacker lấy được quyền truy cập cao nhất của webserver, mailserver, backup và đã kiểm soát hoàn toàn hệ thống mạng một cách bí mật, để cùng lúc tấn công, phá hoại cơ sở dữ liệu của cả hệ thống và hệ thống backup.

➔Khi xảy ra các cuộc tấn công như thế này thì việc lấy log sẽ được gửi từ các thiết bị Router, tường lửa, NIDS,OSSEC được cài trong các máy chủ DB…

Tấn công trên tầng ứng dụng

Đây là cách tấn công lợi dụng các lỗ hổng phần mềm ứng dụng trên các máy chủ như Email, PostScript, FTP... để lấy quyền truy nhập vào hệ thống như quyền quản trị, quyền điều khiển hệ thống và từ đó kiểm soát hệ thống để tiến hành hoạt động phá hoại.

Cách tấn công điển hình trên tầng ứng dụng là dùng phần mềm Trojan. Các đoạn chương trình này được cấy ghép hoặc thay thế những đoạn chương trình khác nằm trong một ứng dụng dùng chung, cung cấp tính năng phổ biến phục vụ người dùng, nhưng có thêm chức năng chỉ có hacker biết (theo dõi quá trình đăng nhập hệ thống mạng, lấy trộm thông tin tài khoản, password hoặc thông tin nhạy cảm khác). Hacker cũng có thể thay đổi một số tính năng của ứng dụng, như cấu hình hệ thống thư điện tử luôn gửi một bản copy đến địa chỉ hacker, cho phéphacker có thể đọc được toàn bộ thông tin trao đổi của doanh nghiệp với các đối tác qua thư điện tử...

Hacker còn lấy cắp thông tin bằng cách sử dụng Trojan xây dựng một giao diện giống hệt giao diện đăng nhập bình thường của website, lừa người dùng tin rằng đó là giao diện đăng nhập hợp lệ. Sau đó, trojan giữ lại thông tin đăng nhập và gửi thông báo lỗi, yêu cầu người dùng đăng nhập lại và khởi động giao diện đăng nhập của ứng dụng. Người dùng tin rằng đã nhập sai mật khẩu và sẽ nhập lại để truy nhập vào hệ thống một cách bình thường mà không hề biết thông tin đã bị lấy.

➔Khi xảy ra các cuộc tấn công như thế này thì việc lấy log sẽ được gửi từ các thiết bị Router, tường lửa, NIDS,OSSEC được cài trong các máy chủ Mail,FTP…

Tấn công vào tường lửa

Hiện nay trên thị trường có 3 loại tường lửa : ủy nhiệm ứng dụng (application proxies), cổng lọc gói tin (packet filtering getways), tường lửa điều khiển trạng thái.

Mục đích của tấn công tường lửa là lấy được địa chỉ ip của tường lửa rồi giả mạo địa chỉ IP của tường lửa tấn công vào vùng DMZ.

Nhận dạng tường lửa: Hầu hết thì các tường lửa thường có 1 số dạng đặc trưng, chỉ cần thực hiện một số thao tác như quét cổng và firewalking và lấy banner (thông tin giới thiệu-tiêu đề) là hacker có thể xác định được loại tường lửa, phiên bản và quy luật của chúng.

Các cuộc tấn công từ bên trong học viện

Trong hầu hết trường hợp, nhân viên là người hiểu rõ hệ thống mạng mà họ đang sử dụng hơn bất cứ người ngoài cuộc. Ít nhất, họ có quyền truy cập hợp pháp cho các tài khoản người dùng và mỗi người có quyền hạn truy cập khác nhau. Nhân viên cố ý đe dọa an ninh bao gồm:

+ Nhân viên sử dụng các kỹ thuật hack để nâng cấp hợp pháp quyền truy cập của họ lên root hay quản trị viên truy cập, cho phép họ tiết lộ bí mật thương mại, ăn cắp tiền và dĩ nhiên là có thể cho mục đích cá nhân hoặc chính trị v.v

+ Nhân viên tận dụng lợi thế của truy cập hợp pháp để tiết lộ bí mật thương mại, ăn cắp tiền, và tương tự cho mục đích cá nhân hoặc chính trị.

+ Người nhà của nhân viên trong lúc đến văn phòng đã truy cập vào máy tính công ty gây ảnh hưởng đến an ninh hệ thống.

+ Những người đột nhập vào phòng máy an ninh để nắm quyền truy cập những mainframe và những hệ thống lớn khác.

+ Cựu nhân viên, đặc biệt là những người không tự nguyện rời khỏi tổ chức có ý định trả thù. Do đã am hiểu hệ thống từ trước, họ có thể tấn công hệ thống dễ dàng gây tổn thất cho công ty.

Ngoài những hiểm họa do cố ý, nhân viên cũng có thể gây ra rất nhiều thiệt hại vô ý, chẳng hạn như:

+ Trở thành nạn nhân của kỹ thuật tấn công xã hội, vô tình giúp một hacker giành quyền truy cập mạng trái phép.

+Vô tình tiết lộ thông tin bí mật.

+ Gây hư hại ở mức vật lý của thiết bị, dẫn đến mất dữ liệu.

+ Sử dụng không đúng chức năng của hệ thống, vô tình xóa hoặc sửa đổi dữ liệu.

Hầu hết các mối đe dọa nhân viên vô ý gây nên thiệt hại, về mặt lý thuyết có thể được xử lý thông qua giáo dục nhân viên. Ví dụ, có thể khuyên các nhân viên không nên viết mật khẩu trên các ghi chú và dán trên màn hình à sẽ giúp ngăn ngừa xâm nhập mật khẩu. Tuy nhiên, khi bạn đang đối phó với con người, ngay cả những giáo dục tốt nhất vẫn không thể đảm bảo nó sẽ bị lãng quên trong một khoảng thời gian nào đó.

➔Các bản log sẽ được thu thập từ các OSSEC được cài đặt trong máy tinh của nhân viên trong LAN, switch, máy chủ nội bộ…

KẾT LUẬN

Chúng ta có thể thấy rằng không thể có một biện pháp bảo mật hoàn hảo và toàn vẹn nào có thể giải quyết hết tất cả các vấn đề về bảo mật của một mạng máy tính. Để có một sự an toàn cao nhất cho mạng máy tình cần phải sử dụng một hệ thống bảo mật bao gồm nhiều biện pháp bảo mật và phải biết kết hợp chúng một cách hợp lý và hiệu quả nhất. Đề tài đã tìm hiểu IDS/IPS và đã đi sâu tìm hểu về SIEM và OSSIM trình bày được các khái niệm , đăc điểm, cấu trúc, chức năng và các giải pháp để sử dụng chúng một cách hiệu quả nhất.

Qua đó chúng ta biết được OSSIM là một hệ thống mã nguồn mở phục vụ đắc lực cho hệ thống an ninh mạng, việc xây dựng một thiết bị tích hợp mã nguồn mở OSSIM có tính ứng dụng rất cao trong bối cảnh các hệ thống mạng đang ngày một phát triển. Cùng với đó là sự tích hợp hoàn hảo của các phần mềm mã nguồn mở đó vào hệ thống OSSIM, nhằm cung cấp khả năng giao tiếp thân thiện và hiệu quả hơn với người quản trị mạng. Tất cả những ưu điểm đó đã đưa hệ thống OSSIM trở thành một giải pháp tương đối hoàn thiện cho các hệ thống mạng doanh nghiệp hiện nay.

Và đặc biệt qua đề tài này chúng ta đã thiết kế xây dựng được hệ thống giám sát an ninh mạng để giám sát toàn bộ hoạt động của hệ thống mạng Học viện dựa trên phần mềm mã nguồn mở OSSIM.

TÀI LIỆU THAM KHẢO

[1] Nguyen Xuan Hoai, McKay, R.I., and Abbass, H.A. 2003, Tree Adjoining Grammars, Language Bias, and Genetic Programming. In *Proceedings of European Conference on Genetic Programming, Lecture Notes in Computer Science (LNCS) 2610*, 335-344, Springer-Verlag.

[2] Poli, R., Langdon, W., and McPhee, N. 2008. *A Field Guide to Genetic Programming*, Lulu Enterprise.

[3]AlienVault_Unified_System_Description_1.0.

Nguồn:*http://alienvault.com/docs/AlienVault_Unified_System_Description_1.0.pdf*