HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VƯƠNG THANH HẢI

NGHIÊN CỨU CÁC GIẢI PHÁP PHÁT HIỆN XÂM NHẬP VÀ ỨNG DỤNG CHO TRƯỜNG CAO ĐẲNG SƯ PHẠM HÀ TÂY

CHUYÊN NGÀNH : **KHOA HỌC MÁY TÍNH**

MÃ SỐ: **8.48.01.01**

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI - 2022

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TS. Trần Quang Anh

Phản biện 1: PGS.TS: Nguyễn Linh Giang

Phản biện 2: PGS.TS: Bùi Thu Lâm

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

Vào lúc: 16 giờ30 ngày 05 tháng 07 năm 2022

Có thể tìm hiểu luận văn tại:

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

MỞ ĐẦU

Cùng với sự phát triển của mạng Internet, mạng World Wide Web toàn cầu và các dịch vụ trên nền Internet, các dạng tấn công, xâm nhập vào các hệ thống mạng, máy chủ và thiết bị đầu cuối của người dùng cũng phát triển ở mức đáng lo ngại. Các dạng tội phạm trên không gian mạng trở nên rất phổ biến và luôn đứng đầu danh sách truy nã của Cục Điều tra liên bang Mỹ (FBI) trong những năm gần đây [1]. Về mặt địa lý, Việt Nam trong những năm gần đây luôn nằm trong top 10 nước là đích bị tấn công nhiều nhất [1]. Các dạng mã độc và tấn công, khai thác cũng tăng vọt trên các nền tảng di động và IoT. Hãng F-Secure ước tính số lượng tấn công, xâm nhập vào các thiết bị IoT tăng gấp 3 lần trong 6 tháng đầu năm 2019 [2].

Để phòng chống hiệu quả các dạng tấn công, xâm nhập vào các hệ thống mạng, máy chủ và thiết bị đầu cuối của người dùng, mô hình phòng vệ theo chiều sâu thường được áp dụng [3]. Trong đó, nhiều lớp bảo vệ được triển khai theo chiều sâu nhằm đảm bảo an toàn cho các tài sản thông tin quan trọng của cơ quan, tổ chức và người dùng. Các lớp bảo vệ như tường lửa, các hệ thống kiểm soát truy cập thường được xem là lớp bảo vệ đầu tiên trong hệ thống bảo vệ đa lớp. Tiếp theo, lớp bảo vệ thứ 2 gồm các hệ thống giám sát, phát hiện và ngăn chặn tấn công, xâm nhập được triển khai nhằm giám sát, phát hiện các dạng tấn công, xâm nhập nguy hiểm đã vượt qua lớp bảo vệ thứ nhất. Hiện nay, có nhiều giải pháp, hệ thống phát hiện tấn công, xâm nhập mã mở, miễn phí và thương mại đã được phát triển và triển khai ứng dụng. Mỗi giải pháp, hệ thống phát hiện tấn công, xâm nhập lại có các tính năng và khả năng giám sát, bảo vệ khác nhau. Việc nghiên cứu, khảo sát các hệ thống phát hiện tấn công, xâm nhập, nhằm lựa chọn hệ thống phát hiện xâm nhập phù hợp với nhu cầu cụ thể của mỗi cơ quan, tổ chức là việc làm cần thiết. Để thực hiện mục tiêu trên, học viên lựa chọn đề tài "Nghiên cứu các giải pháp phát hiện xâm nhập và ứng dụng cho Trường cao đẳng sư phạm Hà Tây" để thực hiện luận văntốt nghiệp của mình.

CHƯƠNG 1. TỔNG QUAN VỀ XÂM NHẬP VÀ PHÁT HIỆN XÂM NHẬP

1.1. Tổng quan về xâm nhập

Chương I trình bày về định nghĩa tấn công, xâm nhập hệ thống, khái quát các phương thức sử dụng, mục tiêu và tác hại của nó. Tiếp đó sẽ phân loại các dạng tấn công, xâm nhập và giới thiệu các phương thức tiêu biểu.

1.1.1. Khái quát về tấn công, xâm nhập

Khái niệm tấn công mạng (*hoặc "tấn công không gian mạng"*) trong tiếng Anh là Cyber attack (hoặc *Cyberattack*), được ghép bởi 2 từ: Cyber (thuộc không gian mạng internet) và *attack* (sự tấn công, phá hoại). Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử

1.1.2. Giới thiệu một số dạng tấn công, xâm nhập điển hình

1.1.2.1. Tấn công vào mật khẩu

Tấn công mật khẩu là hình thức hacker tìm cách hack mật khẩu và truy cập vào tài khoản của người dùng [3]. Thông tin của người dùng sẽ bị đánh cắp trên đường truyền từ máy chủ đến máy khách.Hoặc hacker cũng có thể đánh cắp mật khẩu thông qua các dạng tấn công XSS hoặc Social Engineering. Vì thế, tấn công mật khẩu còn có tên gọi khác là hack password. Mục đích chính của tấn công mật khẩu chính là truy cập tài khoản và lừa đảo. Một số tài khoản thường xuyên bị hack password, gmail. Nguy hiểm hơn là tấn công mật khẩu tài khoản ngân hàng, thẻ tín dụng……

1.1.2.2. Tấn công chèn mã độc

Tấn công chèn mã độc (Malicious Code Injection) Dữ liệu đầu vào bị các Hacker lợi dụng các kẽ hở trong phần mềm được các lập trình viên viết ra hoặc kẽ hở khi cấu hình hệ thống không kiểm tra và giám sát [3]. Mã độc có thể được hacker chèn vào trong quá trình người dùng thao tác các tệp dữ liệu nhập và thực thi chúng trên hệ thống của người dùng.

1.1.2.3. Tấn công từ chối dịch vụ

DoS (Denial of Service Attacks) hay còn gọi là tấn công từ chối dịch vụ, DoS hoạt động dưới dạng tấn công bằng cách "tuồn" ồ ạt traffic hoặc gửi thông tin có thể kích hoạt sự cố đến máy chủ, hệ thống hoặc mạng mục tiêu nhằm ngăn cản người dùng truy nhập các tài nguyên hệ thống [3]. Có 2 loại tấn công DoS chính là :

1.1.2.4. Tấn công từ chối dịch vụ phân tán

Tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service Attacks) mục tiêu của phương pháp tấn công này là nhắm đến các máy chủ (server), hacker sẽ sử dụng nhiều thiết bị, máy tính đã bị hack từ trước để đồng loạt gửi lượng lớn request và yêu cầu truy cập tới máy chủ làm cho máy chủ bị sập.

1.1.2.5. Tấn công giả mạo địa chỉ

Là một loại tấn công mạng trong đó kẻ xâm nhập bắt chước một thiết bị hoặc người dùng hợp pháp khác để khởi động một cuộc tấn công vào mạng, hành động này của kẻ tấn công được gọi là IP Spoofing [4]. Để truy cập vào hệ thống mạng của bạn, máy tính bên ngoài phải "giành" được một địa chỉ IP tin cậy trên hệ thống mạng. Vì vậy kẻ tấn công phải sử dụng một địa chỉ IP nằm trong phạm vi hệ thống mạng của bạn.

1.1.2.6. Tấn công nghe trộm

Thông tin sẽ bị đánh cắp bằng cách sử dụng các thiết bị phần cứng, phần mềm như: hub,router, card mạng….Khi thông tin được truyền qua internet các thiết bị sẽ bắt các gói tin, kẻ tấn công sẽ bí mật thu thập thông tin, theo dõi các gói tin trên đường truyền.

1.1.2.7. Tấn công kiểu người đứng giữa

Tấn công người đứng giữa (Man in the middle) là một thuật ngữ chung để chỉ những cuộc tấn công mà hacker sẽ đứng ở giữa người dùng và ứng dụng trong quá trình giao tiếp, nhằm nghe trộm hoặc mạo danh một trong các bên. Mục tiêu của tấn công Man in the Middle là đánh cắp thông tin cá nhân.

1.1.2.8. Tấn công kiểu kỹ thuật xã hội (Social Engineering)

Social Engineering được hiểu đơn giản là kỹ thuật tác động đến con người để đánh cắp thông tin hoặc nhằm đạt được một mục đích mong muốn. Kỹ thuật này dựa trên điểm yếu tâm lý và nhận thức sai lầm của người dùng về việc bảo mật thông tin. Theo đó, tin tặc chú trọng vào việc khai thác các thói quen tự nhiên của người dùng hơn là việc khai thác các lỗ hổng bảo mật của hệ thống.

1.1.2.9. Phần mềm độc hại

là tên gọi chung cho một số loại phần mềm, được thiết kế để truy cập trái phép vào các thiết bị máy,hoặc mạng và/hoặc cố ý làm hại người dùng các thiết bị này. Do đó, phần mềm được định nghĩa là phần mềm độc hại, tùy thuộc vào mục đích sử dụng của nó, một số sản phẩm phần mềm độc hại có thể thuộc một số loại cùng một lúc; những chương trình như vậy thường có đặc điểm của Trojans và sâu, và đôi khi cả virus

1.2. Tổng quan về phát hiện xâm nhập

1.2.1. Khái quát về phát hiện xâm nhập

Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) đây là một phần mềm chuyên dụng được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống. IDS thường là một phần của các hệ thống bảo mật hoặc phần mềm khác, đi kèm với nhiệm vụ bảo vệ hệ thống thông tin.

Mục đích chính của IDS là ngăn ngừa và phát hiện những hành động phá hoại tính bảo mật của hệ thống hoặc những hành vi như dò tìm, quét các cổng. Bằng việc kiểm tra giám sát sự đi lại của lưu lượng mạng qua những thiết bị IDS có thể xác định được những hành động xâm nhập.

1.2.1.1. Phát hiện xâm nhập mạng và phát hiện xâm nhập host

Hệ thống phát hiện tấn công, xâm nhập (Intrusion Detection System - IDS) là một phần mềm chuyên dụng được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống, hệ thống phát hiện tấn công, xâm nhập chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo. Kiến trúc thông thường của một hệ thống IDS bao gồm 3 thành phần chính: thành phần thu thập thông tin, thành phần phân tích thông tin, thành phần cảnh báo

1.2.1.2. Phân loại phát hiện tấn công, xâm nhập mạng

Có thể phân loại phát hiện tấn công, xâm nhập mạng theo 2 cách: Phân loại dựa trên kỹ thuật phát hiện và phân loại dựa trên nguồn dữ liệu, có thể chia các hệ thống phát hiện xâm nhập thành 2 loại: Hệ thống phát hiện xâm nhập cho host (Host-Based IDS, hoặc HIDS) và hệ thống phát hiện xâm nhập cho mạng (Network-Based IDS, hoặc NIDS).

a. HIDS(Host-based intrusion detection system)

- Lợi thế của HIDS:

+ Có khả năng xác định user liên quan tới một sự kiện.

+ HIDS có khả năng phát hiện các cuộc tấn công, xâm nhập diễn ra trên một máy, NIDS không có khả năng này.

+ Có thể phân tích các dữ liệu mã hoá.

- Hạn chế của HIDS:

+ Thông tin từ HIDS là không đáng tin cậy ngay khi có sự tấn công xâm nhập vào host này thành công.

+ Khi hệ điều hành bị phá hoại do tấn công, đồng thời HIDS cũng bị phá hoại. Trên các máy tính cục bộ cũng cần phải được thiết lập HIDS để giám sát.

+ HIDS không có chức năng phát hiện ra các cuộc dò quét mạng (Nmap, Netcat…).

+ HIDS cần có tài nguyên trên host để hoạt động.

b. NIDS (Network-Based intrusion detection system)

NIDS là hệ thống phát hiện xâm nhập phân tích lưu lượng mạng đi qua các hub, switch đã được cấu hình cổng theo dõi hoặc các nút mạng, NIDS có thể đứng trước hoặc sau firewall trong các hệ thống mạng để giám sát gói tin trao đổi giữa các thiết bị. NIDS theo dõi lưu lượng truy cập đi và đến của tất cả các thiết bị trong phân đoạn mạng giám sát..

Lợi thế của NIDS:

+ Quản lý được cả một network segment (gồm nhiều host).

+ Bảo trì và cài đặt đơn giản, không ảnh hưởng tới mạng.

+ Tránh DoS làm ảnh hưởng tới một host nào đó.

+ Có khả năng xác định được lỗi ở tầng Network (trong mô hình Open Systems Interconnection), độc lập với hệ điều hành.

Hạn chế của NIDS:

+ Khi không có có xâm nhập mà báo là có xâm nhập, dẫn đến trường hợp xảy ra báo động giả (false positive).

+ NIDS yêu cầu phải được cập nhật các chữ ký mới nhất để thực sự an toàn. Có độ trễ giữa thời điểm phát báo động và thời điểm bị tấn công.

+ Khi báo động được phát ra, hệ thống có thể đã bị hư hại.

+ Hạn chế về giới hạn băng thông.

+ Dữ liệu có thể bị tin tăc chia nhỏ ra để xâm nhập và tấn công vào hệ thống.

+ Không thông báo cho biết việc tấn công có thành công hay không.

1.2.2. Phát hiện xâm nhập dựa trên dấu hiệu và dựa trên bất thường

1.2.2.1 Phát hiện đột nhập dựa trên dấu hiệu (Signature-based)

Signature-based IDS là một cơ sở dữ liệu lưu trữ những kỹ thuật xâm nhập hay còn gọi là dấu hiệu, bao gồm tất cả các thông tin mô tả kiểu tấn công, dấu hiệu được lưu ở dạng cho phép so sánh trực tiếp với thông tin có trong chuỗi sự kiện, tuy nhiên Signature-based IDS cũng có những nhược điểm sau:

- Mô tả cuộc tấn công không chi tiết, khó hiểu.
- Cơ sở dữ liệu Signature-based IDS lớn chiếm nhiều dung lượng bộ nhớ

- Khó phát hiện được những kỹ thuật biến thể mới khi dấu hiệu càng cụ thể.

1.2.2.2. Phát hiện đột nhập dựa trên sự bất thường (Anomaly-based)

Đây là phương pháp phát hiện xâm nhập bằng cách so sánh(mang tính thống kê) các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (anomaly) có thể là dấu hiệu của xâm nhập

Kết luận chương I

CHƯƠNG 2. CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP

2.1. Các hệ thống phát hiện xâm nhập mã mở

Trong chương này sẽ cho chúng ta cái nhìn tổng quan về IDS bao gồm cả những điểm mạnh và điểm yếu của chúng. Chúng ta sẽ đề cập đến cả Network IDS và cả Host IDS. Sự khác nhau chủ yếu giữa NIDS và HIDS đó là dữ liệu mà nó tìm kiếm. Bên cạnh đó chương này cũng tìm hiểu một số hệ thống phát hiện xâm nhập tiêu biểu như: Snort, Suricata, OSSEC, SolarWinds Security Event Manager, IBM Qradar, Suricata.

2.1.1. SNORT

2.1.1.1. Giới thiệu về Snort

Snort là một hệ thống phát hiện xâm nhập mã nguồn mở (IDS) và hệ thống ngăn chặn xâm nhập (IPS) mạnh mẽ, cung cấp khả năng phân tích lưu lượng mạng theo thời gian thực và ghi nhật ký gói dữ liệu [5]. SNORT sử dụng ngôn ngữ dựa trên quy tắc kết hợp các phương pháp kiểm tra bất thường, giao thức và chữ ký để phát hiện hoạt động độc hại tiềm ẩn cũng như nhiều loại tấn công và thăm dò khác nhau, chẳng hạn như,stealth port scans,CGI attacks, SMB probes, OS fingerprinting buffer overflows attempts …

2.1.1.2. Thành phần và chức năng

Snort bao gồm 05 thành phần chính đó là:

a. *Module giải mã gói tin (Packet Decoder)*
b. *Module tiền xử lý (Preprocessors)*
c. *Module phát hiện (Detection Engine)*
d. *Module log và cảnh báo (Logging and Alerting System)*
e. *Module kết xuất thông tin (Output Module)*

2.1.1.3. Ưu điểm và nhược điểm của Snort

a. *Ưu điểm*

- Snort là phần mềm mã nguồn mở, hoạt động 24/7 theo thời gian thật.
- Snort có thể hoạt động đa nền tảng.
- Hệ cơ sở dữ liệu về các tập luật thường xuyên được cập nhật các hình thức xâm nhập mới.
- Có khả năng phát hiện một số lượng lớn các kiểu thăm dò, xâm nhập khácnhau như: buffer oveflow, CGI-Atack, Scan, ICMP, Virus...
- Snort có một số lượng người dùng và các nhà phát triển khá đông.
- Có rất nhiều các chương trình phụ trợ cung cấp các tính năng dễ sử dụng không phải là thuộc tính của Snort được thêm vào(add on).

- Với một cơ sở hạ tầng an ninh hiện có, không cần phải thay thế Snort

b. Nhược điểm

- Snort vẫn có thể đưa ra những báo động giả về các mối nguy hại có thể sảy ra cho hệ thống,trường hợp này gọi là (False Positive).
- Các dữ liệu khi đã được mã hoá thì Snort không phân tích được như SSH,SSL…
- Dữ liệu về các kiểu tấn công xâm nhập luôn phải được cập nhật thường xuyên để đảm bảo hiệu quả của NIDS.
- Khi hệ thống bị tấn công xâm nhập thì không biết được cuộc tấn công đó có thành công hay không.
- Một trong những hạn chế là giới hạn băng thông.

2.1.2. SURICATA

2.1.2.1. Giới thiệu Suricata.

Suricata là một công cụ mạng IDS hiệu suất cao (Hệ thống phát hiện xâm nhập), IPS và bảo mật mạng, được phát triển bởi OISF, đây là một ứng dụng mã nguồn mở đa nền tảng và Là tài sản của một nền tảng phi lợi nhuận của cộng đồng Open Information Security Foundation (OISF) [6].

2.1.2.2. Thành phần chức năng của Suricata

Kiến trúc của Suricata gồm 4 thành phần cơ bản:

a. Module giải mã gói tin (Packet Decoder)

b. Module tiền xử lý (Preprocessors)

c. Module phát hiện (Detection engine)

d. Module log và cảnh báo (Alert generation)

2.1.2.3. Ưu điểm và nhược điểm của Suricata

a. Ưu điểm

- Dễ dàng cấu hình: người quản trị đều có thể biết và cấu hình hệ thống theo mong muốn của mình.
- Suricata là phần mềm mã nguồn mở: Sricata được phát hành dưới giấy phép phần mềm tự do GNU/GPL (GNU General Public License) điều này có nghĩa là bất cứ ai cũng có thể sử dụng Suricata một cách miễn phí dù đó là doanh nghiệp hay người dùng cá nhân. Suricata có một cộng đồng người sử dụng lớn.
- Chạy trên nhiều hệ điều hành khác nhau: Chạy trên các hệ điều hành nguồn mở như Linux, CentOS. Debian, Fedora, FreeBSD, Window, Mac OS X…
- Hệ cơ sở dữ liệu các tập luật thường xuyên được bổ sung và cập nhật các hình thức xâm nhập mới.

b. Nhược điểm.

- Đối với việc xử lý gói tin có dung lượng lớn nhiều Gb sẽ làm giảm hiệu xuất hoạt động của CPU đây là vấn đề hạn chế của Suricata

2.1.3. OSSEC

2.1.3.1. Giới thiệu về OSSEC

OSSEC là một Hệ thống phát hiện xâm nhập dựa trên máy chủ (HIDS), đa nền tảng miễn phí, mã nguồn mở có nhiều cơ chế bảo mật khác nhau [7]. OSSEC có một công cụ phân tích và tương quan mạnh mẽ tích hợp và giám sát và phân tích log, giám sát tính toàn vẹn của file, giám sát đăng ký Windows thực thi chính sách tập trung, phát hiện rootkit, cảnh báo thời gian thực và phản hồi tích cực.

.

2.1.3.2. Thành phần và chức năng

Các thành phần của OSSEC

a. Manager (Server)

Lưu trữ cơ sở dữ liệu của việc kiểm tra tính toàn vẹn file Kiểm tra các log, event.

Quản lý, lưu tất cả các rule, decoder (bộ giải mã), cấu hình chính. Điều này giúp dễ dàng quản lý, dù cho có lượng lớn Agent.

b. Agent

Bản chất thì là 1 phần mềm được cài đặt trên máy client giúp thu thập các thông tin và gửi cho Server để phân tích, thống kê..

c. Agentless

Là các hệ thống không cài được gói agent trên các Agentless này có thể thực hiện việc kiểm tra tính toàn vẹn giúp monitor firewall, router hay thậm chí cả hệ thống Unix

d. Ảo hóa/ Vmware

Cho phép cài đặt agent trên các guest OS (Máy ảo).Ngoài ra cũng được cài đặt trong VMware ESX nhưng có thể dẫn đến sự cố không hỗ trợ.

e. Firewalls, switches and routers

Chính là các Agentless, Ossec có thể nhận và phân tích nhật ký hệ thống từ nhiều firewall, switch, router. Nó support tất cả Cisco routers, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint và nhiều thiết bị khác

2.1.3.3. Ưu nhược điểm của Ossec

a. Ưu điểm

- Đa nền tảng (Linux, Mac OS , Window,Solaris)
- Real-time Alert (Cảnh báo thời gian thực)
- Có thể tích hợp với các hệ thống hiện đại (SIM/SEM)
- Server dễ dàng quản lý tập trung các chính sách trên nhiều OS.
- Giám sát trên agent, agentless (Client không cài đặt được gói agent) như router, firewall

b. Nhược điểm

- Nâng cấp Ossec đòi hỏi người quản trị phải có chuyên môn tốt vì quá trình này phức tạp, khó khăn, các quy tăc cũ sẽ bị xoá hoặc ghi đè sau khi hệ thống được nâng cấp.

2.2. Các hệ thống phát hiện xâm nhập thương mại

2.2.1. IBM Qradar

2.2.1.1. IBM Qradar là gì?

IBM Qradar là một hệ thống tích hợp các chức năng thu thập, xử lý, tổng hợp và lưu trữ dữ liệu mạng trong thời gian thực [8]. Qradar hoạt động như một trung tâm giảm sát, bảo mật cho doanh nghiệp, tổ chức với giao diện trực quan, được tích hợp với hàng trăm sản phẩm của IBM cũng như các hãng công nghệ khác.

2.2.1.2. Thành phần và chức năng.

Trong giải pháp giám sát an ninh mạng của Qradar, Event Correlation Service là dịch vụ cốt lõi chịu trách nhiệm cho việc thu thập các sự kiện và luồng dữ liệu rồi sử lý các dữ liệu đó. ECS gồm 3 thành phần chính:

- Event collector component
- Event processor component
- Magistrate

2.2.1.3. Ưu nhược điểm của IBM Qradar

a. Ưu điểm

Giải pháp của IBM hỗ trợ các tùy chọn triển khai Tính khả dụng cao (Hight Availability-HA) cho cả thiết bị vật lý và thiết bị ảo với phương pháp tiếp cận máy chủ chính và phụ được kết hợp thành một cụm, trong đó máy chủ phụ ở trạng thái chờ và trong trường hợp máy chủ chính bị lỗi sẽ đảm nhận chức năng triển khai.

b. Nhược điểm

- Đối với người sử dụng, QRadar có kiến trúc hơi phức tạp khiến việc quản lý tất cả các bộ phận trong cấu trúc tương đối khó khăn.
- Các yêu cầu cấu hình máy đáp ứng đối với hệ thống là khá cao.

2.2.2. SolarWinds Security Event Manager (SSEM)

2.2.2.1. Giới thiệu về SSEM

SSEM là một phần mềm giải pháp phát hiện xâm nhập máy tính cạnh tranh về chi phí phục vụ cho việc tuân thủ bảo mật và quản lý nhật ký [9]. SSEM sử dụng cách tiếp cận chủ động giúp người dùng xác định được các mối đe dọa trong thời gian thực. SSEM tự động thu thập và đăng nhập dữ liệu từ các thiết bị mạng, hệ thống và các ứng dụng trên toàn cơ sở hạ tầng CNTT.

2.2.2.2. Thành phần và chức năng.

SSEM cung cấp quản lý qua giao diện WEB trực quan dễ dàng sử dụng cho người dùng các thành phần chính của SSEM gồm: Ops Center, Monitor, Explore, Bulid, Manager, Analyze**.**

2.2.2.3. Ưu nhược điểm của SSEM

a. Ưu điểm của SSEM

- Tự động hóa và nhúng thông minh cung cấp một trung tâm hoạt động bảo mật giám sát 24/7
- Phát hiện sự kiện nhanh hơn và cảnh báo về cảnh báo mối đe dọa dựa trên IP
- Phát hiện thông minh và đáng tin cậy hơn về hoạt động đáng ngờ và độc hại bao gồm phần mềm độc hại, người trong cuộc và các mối đe dọa nâng cao
- Giúp loại bỏ các quy trình báo cáo thủ công tốn nhiều thời gian
- Rút ngắn thời gian trả lời thông qua khả năng phản hồi mạnh mẽ
- Tự động chặn lạm dụng thông qua phản hồi tích cực đối với các vi phạm chính sách mạng, hệ thống và truy cập
- Tích hợp công cụ bảo mật mở rộng bằng cách cung cấp khả năng chuyển tiếp nhật ký hoặc ghi dữ liệu sang các công cụ khác
- Giám sát và chặn sử dụng USB dựa trên các quy tắc chính sách hành vi
- Quá trình đăng nhập dễ dàng với người dùng với tích hợp đăng nhập một lần
- Cung cấp khả năng quản lý dễ dàng với nhiều tùy biến.

b. Nhược điểm của SSEM

- Là sản phẩm có phí
- Được đóng gói sẵn nên giảm khả năng tùy biến.
- Chỉ chạy được trên môi trường Window và VMware.

2.2.3. McAfee Network Security Platform

2.2.3.1. Giới thiệu về MNSP

McAfee Network Security Platform (MNSP) [trước đây là McAfee IntruShield] là sự kết hợp của các thiết bị mạng và phần mềm giúp phát hiện và ngăn chặn chính xác các hành vi xâm nhập, từ chối dịch vụ (DoS) và các cuộc tấn công từ chối dịch vụ (DDoS) phân tán và sử dụng sai mục đích mạng [10].

2.2.3.2. Thành phần và chức năng

McAfee Network Security Platform (MNSP) có nhiều chức năng và thành phần như bảo vệ phần mềm độc hại nâng cao, bảo vệ các ứng dụng web, nhận dạng ứng dụng, xác định người dùng và nhóm người dùng, xác định loại máy chủ, bảo vệ máy ảo, phân tích lưu lượng mạng của người sử dụng,m ột trong những lợi thế lớn nhất mà MNSP mang lại là khả năng tích hợp với các sản phẩm McAfee khác để tăng hiệu quả.

2.2.3.3. Ưu điểm và nhược điểm

a. Ưu điểm

- Nhanh chóng phát hiện và ngăn chặn các mối đe doạ để bảo vệ các ứng dụng và dữ liệu
- Giải pháp hiệu xuất cao, có thể mở rộng cho các môi trường năng động
- Quản lý tập trung cho khả năng hiển thị và kiểm soát
- Phát hiện nâng cao, bao gồm phân tích phần mềm độc hại không có chữ ký
- Giải mã SSL đến và đi để kiểm tra lưu lượng mạng
- Tính khả dụng cao và bảo vệ phục hồi sau thảm hoạ
- Các thiết bị ảo có sẵn

b. Nhược điểm

- Sử dụng tốn nhiều tài nguyên.
- Giao diện không thân thiện với người dùng

2.3. So sánh các hệ thống phát hiện xâm nhập

Qua những phân tích, những đánh giá về khái niệm, kiến trúc cũng như cơ chế hoạt động của các hệ thống phát hiện xâm nhập ở trên ta có thể so sánh các hệ thống này và đưa ra được những ưu điểm và nhược điểm của các hệ thống phát hiện xâm nhập.

2.4. Kết luận chương II

.

CHƯƠNG 3. THỬ NGHIỆM TRIỂN KHAI GIẢI PHÁP PHÁT HIỆN XÂM NHẬP SURICATA CHO HỆ THỐNG MẠNG TRƯỜNG CAO ĐẲNG SƯ PHẠM HÀ TÂY

3.1. Khảo sát và triển khai mô hình

3.1.1 Khảo sát hệ thống mạng Trường cao đẳng sư phạm Hà Tây

Trường Cao đẳng sư phạm Hà Tây được xây dựng trên diện tích 14 ha bao gồm 81 phòng học và giảng đường đạt tiêu chuẩn, 10 phòng thực hành, thí nghiệm; ngoài ra còn có nhà tập Đa năng; Trung tâm thư viện hiện đại với diện tích trên 4000m2 đã đưa vào sử dụng; sân bãi, nhà thi đấu, bể bơi đang được xây dựng và nhiều trang thiết bị khác đáp ứng đủ nhu cầu dạy học.

3.1.1.1. Sơ đồ mạng

Cụ thể hệ thống mạng được chia làm các vùng sau:Hệ thống máy chủ,Máy tính tại các phòng ban, khoa,Hệ thống máy tính phòn thực hành,Máy tính xách tay, điện thoại, máy tính bảng

3.1.1.2. Những tồn tại của hệ thống mạng tại trường.

Hiện nay, trường chưa được cài hệ thống tường lửa để bảo vệ toàn thể máy tình các phòng ban, các khu vực mạng tránh khỏi các hiểm họa, nguy cơ về an toàn thông tin.

3.1.2 Mô hình triển khai

Các công cụ cần thiết để triển khai mô hình:

- VMware Workstation
- Hệ điều hành Centos 7
- Hệ điều hành Ubuntu
- Hệ điều hành Kali Linux
- ServerSuricata 6.0.3

3.1. Cài đặt và cấu hình Suricata

3.2.1. Cài đặt Suricata

Trước khi cài đặt phần mềm chúng ta tiến hành cài đặt các thành phần cần thiết cho Suricata, thực hiện theo thứ tự sau đây trên máy Centos 7, khi service suricata khởi chạy có thể sử dụng lệnh sau để kiểm tra:

#curl http://testmyids.com

3.2.2. Câu hình, tạo tập luật cho Suricata

Ta sẽ tiến hành cấu hình cho các tham biến trong tập rules của Suricata. Đầu tiên, ta sẽ phải thiết lập lại các biến cho các khu vực (địa chỉ IP) khác nhau và các biến cho các cổng. Mục đích của việc thiết lập biến này giúp cho việc thay đổi dễ dàng khi cần thiết.

3.2. Một số kịch bản thử nghiệm, kết quả và đánh giá

Một số phương thức tấn công phổ biến như : Tấn công rà quét cổng, tấn công DoS, tấn công duyệt đường dẫn, tấn công Nmap Scan, tấn công SSH Scan…..

3.3.1. Tấn công quét cổng

3.3.2. Tấn công DoS/DdoS

3.3.3. Tấn công duyệt đường dẫn

3.3.4. Tấn công Nmap Scan

3.3.5. Tấn công SSH Scan

3.4. Kết luận chương III

Chương 3 đã đưa ra mô hình thử nghiệm giải pháp phát hiện xâm nhập dựa trên giám sát lưu lương mạng, đồng thời cũng trình bày chi tiết các cài đặt, thiết lập hệ thống phát hiện xâm nhập và tấn công mạng dựa trên nền tảng mã nguồn mở Suricata. Dựa trên các kết quả cho thấy hệ thống hoạt động ổn định, có khả năng giám sát và phát hiện các bất thường và nguy cơ an ninh an toàn thông tin; đồng thời hệ thống cũng hỗ trợ các tính năng quản trị và hiển thị dữ liệu đa dạng, tiện dụng cho người dùng cuối.

KẾT LUẬN

Các kết quả đạt được:

Hệ thống cảnh báo phát hiện xâm nhập khi triển khai tại trường Cao Đẳng Sư Phạm Hà Tây với ngưỡng phù hợp thì mô hình mạng đã hoạt động tốt.

Luận văn có thể được phát triển theo các hướng sau:

Triển khai thử nghiệm mô hình phát hiện tấn công, xâm nhập mạng dựa trên Suricata kết hợp Elastic Stack cho phát hiện bất thường và các nguy cơ ATTT trên hệ thống mạng thực. Hoàn thiện tối ưu hóa hệ thống để có thể phân tích xử lý logs nhanh chóng và tăng hiệu năng của hệ thống.