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

LUẬN VĂN THẠC SĨ KỸ THUẬT
(*Theo định hướng ứng dụng*)

HÀ NỘI - 2022

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**

LUẬN VĂN THẠC SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. TRẦN QUANG ANH

HÀ NỘI - 2022

LỜI CẢM ƠN

Để thực hiện và hoàn thành đề tài luận văn thạc sĩ kỹ thuật này, tôi xin chân thành cảm ơn các Thầy, Cô Khoa Sau Đại học trường Học viện Bưu Chính Viễn Thông đã tận tình dạy dỗ, truyền đạt cho tôi nhiều kiến thức và kỹ năng quý báu.

Tôi xin gửi lời cảm ơn sâu sắc nhất đến giảng viên hướng dẫn trực tiếp của tôi – PGS.TS Trần Quang Anh. Cảm ơn thầy đã luôn lắng nghe những quan điểm cá nhân và đưa ra những nhận xét quý báu, góp ý và dẫn dắt tôi đi đúng hướng trong suốt thời gian thực hiện đề tài luận văn thạc sĩ kỹ thuật.

Tôi cũng xin chân thành cảm ơn sự giúp đỡ, quan tâm và động viên rất nhiều từ cơ quan, tổ chức và cá nhân trong quá trình thực hiện đề tài.

Luận văn cũng được hoàn thành dựa trên sự tham khảo, đúc kết kinh nghiệm từ các sách báo chuyên ngành, kết quả nghiên cứu liên quan. Tuy nhiên do kiến thức và thời gian có giới hạn nên đề tài khó tránh khỏi thiếu sót, kính mong quý thầy và các bạn đóng góp thêm để đề tài được hoàn chỉnh hơn!

Tôi xin chân thành cảm ơn !

Hà Nội, ngày tháng năm 2022

Học viên

Vương Thanh Hải

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi, kết quả đạt được trong luận văn là sản phẩm của riêng cá nhân, không sao chép lại của người khác. Trong toàn bộ nội dung của luận văn, những điều được trình bày hoặc là được tổng hợp từ nhiều nguồn tài liệu hoặc là của cá nhân. Tất cả các tài liệu tham khảo đều có xuất xứ rõ ràng và được trích dẫn hợp pháp. Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Hà Nội, ngày tháng năm 2022

Học viên

Vương Thanh Hải

MỤC LỤC

DANH MỤC VIẾT TẮT

Ký hiệu	Tên Tiếng Anh	Ý nghĩa Tiếng Việt
ADE	Adverse Drug Event	Công cụ phát hiện dị thường
CGI	Computer-Generated Imagery	Công nghệ mô phỏng hình ảnh bằng máy tính
CIS	Center for Internet Security	Trung Tâm An Ninh Internet
CPU	Central Processing Unit	Bộ xử lý trung tâm
DDOS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DNS	Domain Name Servers	Hệ thống phân giải tên miền
DOS	Denial of Service	Tấn công từ chối dịch vụ
FIM	Federated Identity Manager	Hệ thống quản lý nhận dạng
FTP	File Transfer Protocol	Giao thức truyền tải tập tin
GNU/GPL	GNU General Public License	Giấy phép phần mềm tự do
HIDS	Host Intrusion Detection System	Hệ thống phát hiện xâm nhập host
HTTP	Hypertext Transfer Protocol	Giao thức Truyền tải Siêu Văn Bản
ICMP	Internet Control Message Protocol	Giao thức Thông điệp Điều khiển Internet
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IP	Internet Protocol	Địa chỉ giao thức Internet
LAN	Local Area Network	Mạng cục bộ
NIC	Network Interface Card	Card giao tiếp mạng
NIDS	Network Intrusion Detection System	Hệ thống phát hiện xâm nhập mạng
PCI-DSS	Payment Card Industry Data Security Standard	Bộ tiêu chuẩn bảo mật dữ liệu thẻ thanh toán
RAM	Random Access Memory	Bộ nhớ truy xuất ngẫu nhiên
SEM	security event management	quản lý sự kiện bảo mật
SIEM	Security Information and Event Management	Quản lý thông tin và sự kiện bảo mật
SMB	Server Message Block	Hệ thống tệp Internet chung
SNMP	Simple Network Management Protocol	Giao thức giám sát mạng đơn giản
SSH	Secure Shell	Giao thức SSH
SSL	Secure Sockets Layer	Chứng chỉ socket bảo mật

TCP	Transmission Control Protocol	Giao thức TCP
UDP	User Datagram Protocol	Giao thức UCP
VPN	Virtual Private Network	Mạng riêng ảo
WMI	Windows Management Instrumentation	Thiết bị quản lý Windows
XSS	Cross-site scripting	Tấn công script độc hại
ML	Machine Learning	Phương pháp học máy

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG

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]. Cũng trong khoảng thời gian này, số lượng dạng tấn công không liên quan đến file (fileless attacks) – một dạng tấn công tinh vi và nguy hiểm mới được phát hiện trong thời gian gần đây tăng 256%.

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 văn tốt nghiệp của mình.

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

1.1. Tổng quan về xâm nhập

1.1.1. Khái quát về tấn công, xâm nhập

1.1.1.1. Mối đe dọa

Tất cả những hành động gây hư hại đến dữ liệu, tài nguyên của hệ thống mạng máy tính bao gồm: Phần mềm, các file, CSDL, phần cứng…..Đều có thể coi đó là những mối đe doạ (Threat). Các mối đe doạ hay gặp bao gồm:

- Phần mềm độc hại
- Lỗi phần mềm hoặc phần cứng
- Kẻ tấn công ở bên trong
- Mất trộm các thiết bị
- Kẻ tấn công ở bên ngoài
- Tai họa thiên nhiên
- Gián điệp công nghiệp
- Tấn công phá hoại

Trên thực tế, tất cả các mối đe dọa không là độc hại. Một số có thể chỉ là vô tình, hoặc ngẫu nhiên.

1.1.1.2. Điểm yếu(Weakness)

Trong một hệ thống mạng máy tính luôn tồn tại các điểm yếu (Weakness), các hacker có thể dựa vào các khiếm khuyết này để tấn công và xâm nhập vào hệ thống, nói chung các hệ thống luôn tồn tại các điểm yếu

1.1.1.3. Lỗ hổng (Vulnerability)

Trong bất kì một hệ thống nào đều tồn tại những lỗ hổng (Vulnerability),vì vậy hệ thống luôn luôn tiềm tàng các mối đe doạ gây tác hại cho hệ thống. Các nền tảng phần cứng và phần mềm sẽ luôn có các lỗ hổng(Vulnerability) bao gồm:

- Lỗi tràn bộ đệm (buffer overflows)
- Không kiểm tra đầu vào (unvalidated input)

- Điều khiển truy cập gặp các sự cố (access-control problems)

- Các điểm yếu trong trao quyền, xác thực (weaknesses in authentication, authorization)

- Hệ mật mã có các điểm yếu (weaknesses in cryptographic practices)

1.1.1.4. Quan hệ giữa các lỗ hổng và mối đe dọa

Các cuộc tấn công phá hoại thường bị hacker khai thác vào các mối đe doạ, các lỗ hổng đã biết, nếu hệ thống tồn tại những lỗ hổng thì khả năng rất cao là các mối đe doạ sẽ thành hiện thực.

Không thể khắc phục được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tấn công. Một cuộc tấn công (attack) vào các tài nguyên mạng và hệ thống máy tính được thực hiện bằng cách khai thác các lỗ hổng tồn tại trong hệ thống. Có thể kết luận như sau:

Tấn công = Lỗ hổng + Mối đe dọa

1.1.1.5. Phân loại tấn công, xâm nhập

Qua các ghi chép lại các cuộc tấn công xâm nhập có thể đưa ra 2 kiểu tấn công đó là: Tấn công thụ động và tấn công chủ động. Tấn công thụ động (Passive attacks) thông thường ít gây ra thay đổi trên hệ thống, chúng chỉ tồn tại ở dạng giám sát lưu lượng mạng hoặc lấy thông tin bằng hình thức nghe trộm. Ở chiều ngược lại tấn công chủ động (Active attacks) kẻ tấn công sẽ chiếm quyền truy cập trái phép vào hệ thống mạng máy tính, sau đó làm thay đổi file dữ liệu hoặc đánh cắp dữ liệu

Có 4 loại tấn công, xâm nhập chính như sau:

- Giả mạo (Fabrications): Thông tin sẽ bị kẻ tấn công làm giả mạo để đánh lừa người dùng.
- Chặn bắt (Interceptions): Thông tin sẽ bị nghe trộm trên đường chuyền, sau đó kẻ tấn công sẽ làm chuyển hướng thông tin nhằm mục đích sử dụng vào những việc trái phép, phạm pháp.
- Gây ngắt quãng (Interruptions): Gây ngắt kênh truyền thông dẫn đến việc không truyền được dữ liệu.
- Sửa đổi (Modifications): Thông tin sẽ bị sửa đổi trên đường truyền hoặc sửa đổi các file dữ liệu.

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……

Hacker khi đã lấy cắp được thông tin mật khẩu, kẻ tấn công sẽ dùng tài khoản đó để đăng nhập và thao tác bình thường mà không gặp trở ngại gì.

Có 3 kiểu tấn công vào mật khẩu điển hình:

- Tấn công dựa trên từ điển (Dictionary attack): Là một kỹ thuật vượt qua các cơ chế xác thực bằng cách thử các khóa mã, hay mật khẩu là các từ có nghĩa dễ nhớ, thông thường người dùng hay có xu hướng đặt mật khẩu là những từ đơn giản dễ nhớ. Hacker sẽ tận dụng và khai thác vào điểm yếu này của người dùng để nhanh chóng tìm ra mật khẩu chính xác.

- Tấn công vét cạn (Brute force attacks): Đó là hình thức thử mật khẩu đúng sai, hacker sẽ dùng một phần mềm đăng nhập rà soát qua hết các tài khoản . Việc dò mật khẩu càng trở nên phổ biến khi internet ngày càng chiếm vị thế quan trọng trong cuộc sống con người. Và tất nhiên số lượng tài khoản sẽ tăng lên nhanh chóng. Đồng nghĩa với nó là nhiều lỗ hổng, nhiều tài khoản sẽ bị dò mật khẩu hơn.

- Tấn công kết hợp(Combination attack): Là một phương pháp tấn công kết hợp 2 kiểu vét cạn và dựa vào tử điển. Phương pháp này thường sử dụng khi hacker đã nắm và biết được các thông tin về người dùng ví dụ: Tên, ngày sinh, địa chỉ, số điện thoại,… nhằm tiết kiệm thời gian.

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. Các dạng tấn công chèn mã độc:

- Có 2 dạng chính lỗi không kiểm tra đầu vào để tấn công : Tấn công chèn mã SQL (SQL Injection) và tấn công script kiểu XSS, CSRF.

+ Tấn công chèn mã SQL là kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng, làm sai lệch đí các câu truy vấn ban đầu bằng cách chèn thêm một đoạn SQL từ đó có thể khai thác dữ liệu từ database**.** Hacker chèn đoạn mã SQL injection để thực hiện các thao tác như một người quản trị web, trên cơ sở dữ liệu của ứng dụng.

+ Tấn công script kiểu XSS, CSRF là một trong những tấn công phổ biến và dễ bị tấn công nhất. Đối với những ứng dụng web thì tấn công kiểu XSS được coi là một trong những tấn công nguy hiểm nhất và có thể mang lại những hậu quả lớn và nghiêm trọng, XSS là một đoạn mã độc, hacker sẽ chèn mã độc thông qua các đoạn script để thực thi chúng ở phía Client, tấn công kiểu XSS sử dụng để mạo danh người dùng đánh cắp thông tin nhạy cảm của người dùng và dẫn dắt người dùng đến những trang web giả mạo. CSRF là một vectơ tấn công, có khả năng đánh lừa trình duyệt web, thực hiện các hoạt động không mong muốn trong ứng dụng người dùng đã đăng nhập.

- Hầu hết các chương trình hay hệ thống yêu cầu có dữ liệu đầu vào đều có thể tồn tại lỗ hổng, có nhiều kỹ thuật tấn công chèn mã độc khác như: PHP Injection, File Injection, …

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 :

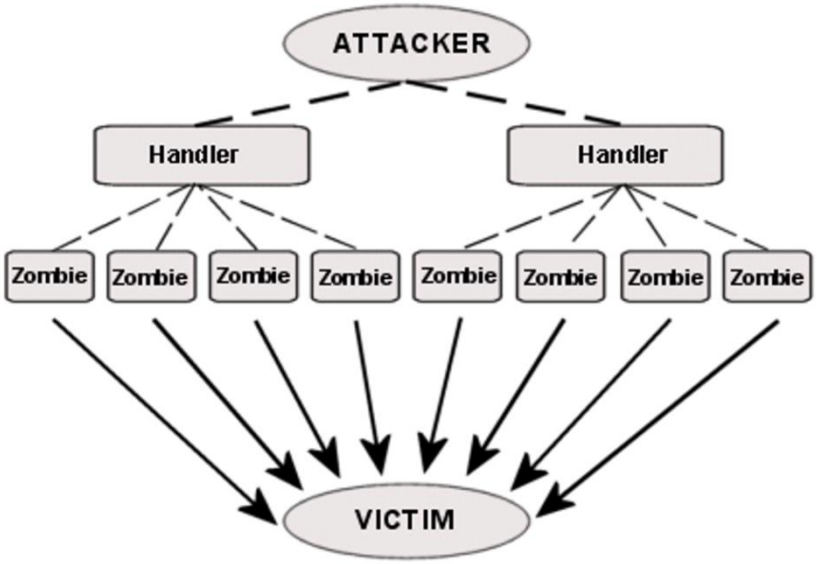
- Tấn công logic (Logic attacks): Các phần mềm ứng dụng thường sẽ có những sai sót đó là lỗ hổng để hacker dựa vào đó để tấn công làm giảm hiệu năng, hoặc đánh sập cả một hệ thống dẫn đến các dịch vụ ngừng hoạt động.

- Tấn công gây ngập lụt (Flooding attacks): Các phần mềm ứng dụng sẽ bị các hacker gửi một lượng lớn các yêu cầu(request) làm cho băng thông không đáp ứng được vì cạn kiệt đường truyền.

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.

DDoS khác DoS ở phạm vi tấn công, tấn công DDoS mạnh hơn DoS rất nhiều, điểm mạnh của hình thức này đó là nó được phân tán từ nhiều địa chỉ IP khác nhau chính vì vậy người bị tấn công sẽ rất khó phát hiện để ngăn chặn được. Hacker không chỉ sử dụng máy tính của họ để thực hiên cuộc tấn công vào một trang web hay một hệ thống mạng nào đó, mà còn lợi dụng hàng triệu máy tính khác để cài các chương trình tấn công tự động(automated agent). Minh họa một mô hình tấn công DDoS.



Hình 1.1. Mô hình tấn công DDoS

1.1.2.5. Tấn công giả mạo địa chỉ

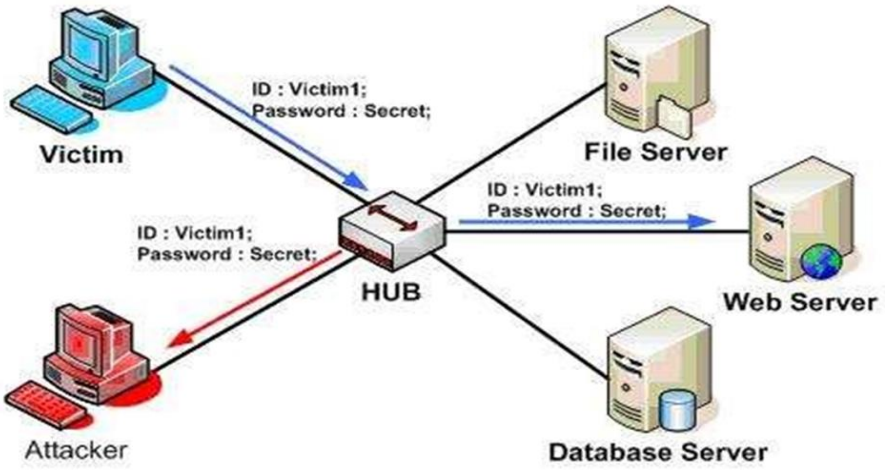
Là một loại tấn công mạng trong đó kẻ xâm nhập bắt chước một thiết bị hoặc người dùng hợp pháp khác để khởi động một cuộc tấn công vào mạng, hành động này của kẻ tấn công được gọi là IP Spoofing [4]. Để truy cập vào hệ thống mạng của bạn,

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. Hoặc cách khác là kẻ tấn công có thể sử dụng một địa chỉ IP bên ngoài nhưng đáng tin cậy trên hệ thống mạng của bạn. Các địa chỉ IP có thể được hệ thống tin tưởng là bởi vì các địa chỉ này có các đặc quyền đặc biệt trên các nguồn tài nguyên quan trọng trên hệ thống mạng, nếu hệ thống mạng không được cấu hình firewall hoặc router thì hacker sẽ dễ dàng thực hiện các cuộc tấn công xâm nhập vào mạng nội bộ.

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.

Một số phương pháp được sử dụng như : gói tin trên đường truyền, rà quét, spyware, keylogger,.... Mô hình tấn công nghe trộm được mô tả như Hình 1.2.

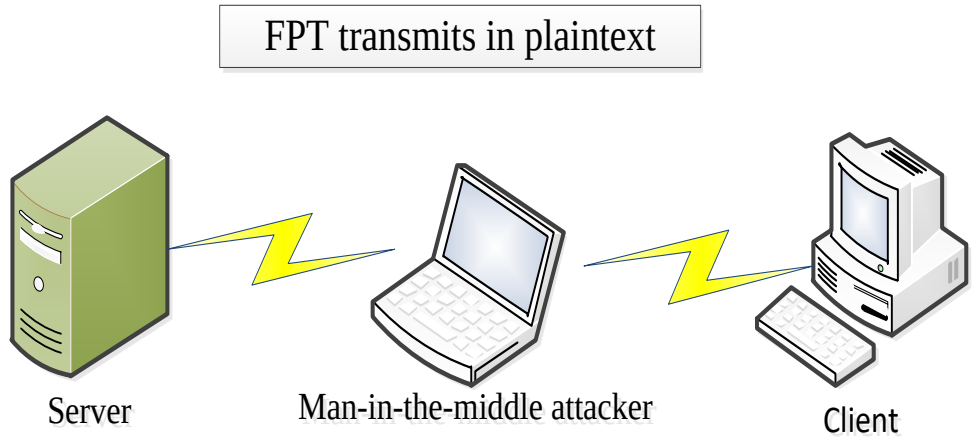


Hình 1.2. Mô hình của dạng tấn công nghe trộm

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. Chẳng hạn như thông tin đăng nhập hay số thẻ tín dụng. Các nạn nhân của tấn công Man in the middle thường là người dùng các ứng dụng tài chính, doanh nghiệp SaaS, trang web thương mại điện tử…Nói chung là những trang web yêu cầu có thông tin đăng nhập. Mục đích kiểu tấn công này được sử dụng để đánh cắp thông tin. Mô hình tấn công kiểu người đứng giữa trong Hình 1.3.



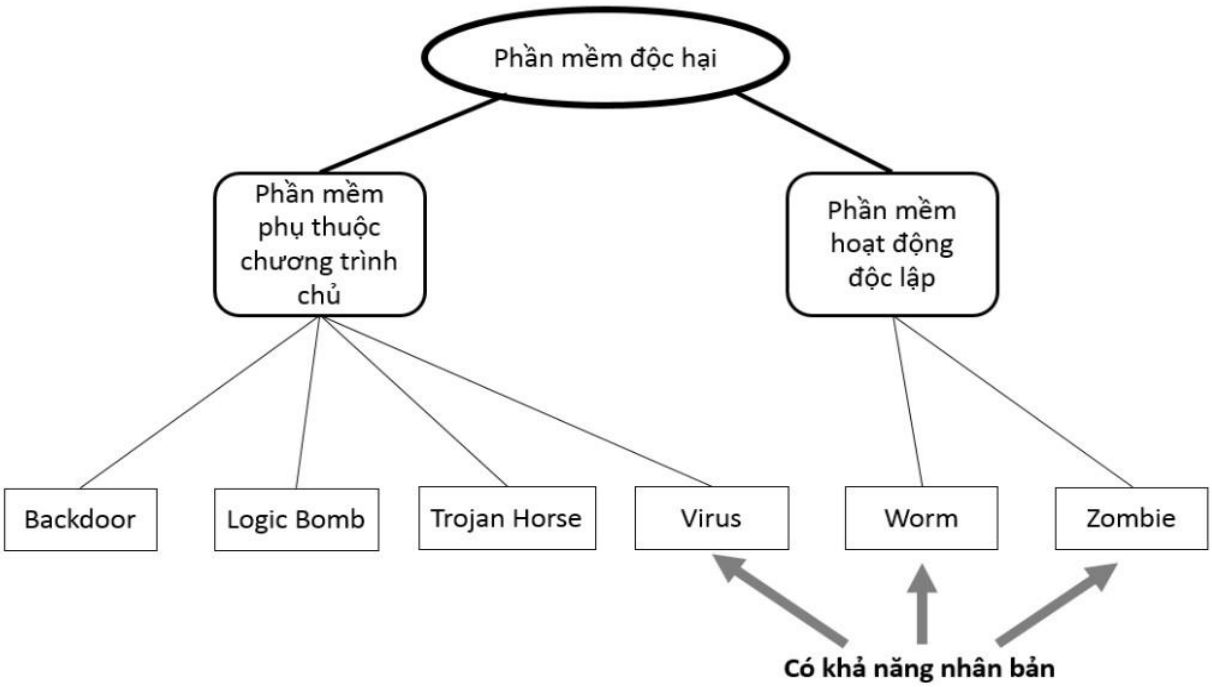
Hình 1.3. Mô hình tấn công kiểu người đứng giữa

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. Trong một cuộc tấn công Social Engineering , hacker sẽ đánh lừa nạn nhân bằng cách nói rằng họ đến từ một tổ chức đáng tin cậy. Trong một số trường hợp, hacker thậm chí sẽ đóng giả một người mà nạn nhân biết. Nếu hành vi đánh lừa có hiệu quả (nạn nhân tin rằng kẻ tấn công là người mà họ nói), hacker sẽ khuyến khích nạn nhân thực hiện thêm hành động. Điều này có thể cung cấp thông tin nhạy cảm như mật khẩu, ngày sinh, chi tiết tài khoản ngân hàng hoặc yêu cầu

chuyển tiền.Social Engineering không trực tiếp sử dụng các phương thức kỹ thuật (phá hủy hệ thống, tin tặc) nhưng có thể sẽ dùng các cách thức tinh vi để dẫn đến tấn công bằng kỹ thuật.

1.1.2.9. Phần mềm độc hại



Hình 1.4. Các dạng phần mềm độc hại

- Backdoor (Cửa hậu) là một loại phần mềm độc hại nhằm bỏ qua các quy trình xác thực thông thường để truy cập hệ thống. Do đó, cung cấp quyền truy cập từ xa đến các nguồn resources bên trong ứng dụng, chẳng hạn như database và server file, cho phép hacker khả năng thực thi lệnh trên hệ thống và cập nhật phần mềm độc hại. Backdoor được cài đặt bằng cách tận dụng thành phần dễ bị tấn công trong ứng dụng web, quản trị viên rất khó phát hiện ra backdoor.

- Logic bombs (Bom logic) Bom Logic là một đoạn mã độc hại thường được cố ý chèn vào phần mềm. Nó chỉ được kích hoạt trên mạng máy chủ khi đáp ứng một số điều kiện nhất định. Sau khi được kích hoạt, một quả bom logic sẽ thực thi một mã độc hại gây hại cho máy tính. Các điểm lập trình ứng dụng của bom logic cũng có thể bao gồm các biến khác sao cho quả bom được phóng sau một số mục cơ sở dữ liệu cụ thể. Tuy nhiên, các chuyên gia bảo mật máy tính tin rằng một số lỗ hổng hành

động nhất định cũng có thể phóng ra một quả bom logic và những loại bom logic này thực sự có thể gây ra tác hại lớn nhất. Một quả bom logic có thể được thực hiện bởi ai đó đang cố gắng phá hoại cơ sở dữ liệu khi họ khá chắc chắn rằng họ sẽ không có mặt để trải nghiệm các hiệu ứng, chẳng hạn như xóa toàn bộ cơ sở dữ liệu.

- Trojan horses (lấy tên theo tích "Con ngựa thành Troy") Trojan sẽ giả danh là phần mềm sạch, hợp pháp để ăn cắp dữ liệu người dùng. Điều khiến Trojan nguy hiểm là bởi khả năng lừa chính người dùng cài đặt chúng. Thủ đoạn thường thấy nhất là khi người dùng nhận được các thông báo cho biết máy tính bị tấn công. Chúng yêu cầu người dùng làm theo hướng dẫn để cài đặt chương trình dọn dẹp - thực chất là một Trojan. Chính bởi vậy, dù cài đặt phần mềm bảo mật cao cấp nhất, máy tính của bạn vẫn có thể bị nhiễm Trojan.

- Virus là một phần mềm được viết ra nhằm lấy cắp hoặc thay đổi thông tin các chương trình này. Chúng ta thường có xu hướng coi tất cả các phần mềm độc hại là virus, nhưng điều đó là không chính xác. Một virus sửa đổi các host files và khi bạn thực thi một file trong hệ thống của nạn nhân, bạn cũng sẽ thực thi virus. Ngày nay, với các loại phần mềm độc hại khác nhau lây nhiễm vào thế giới mạng, virus máy tính đã trở nên không quá phổ biến; chúng chiếm chưa đến 10% tổng số phần mềm độc hại. virus lây nhiễm các tệp khác, chúng là phần mềm độc hại duy nhất lây nhiễm các tệp khác và do đó, rất khó để dọn sạch chúng. Ngay cả các chương trình diệt virus tốt nhất cũng sống chung với điều này; hầu hết thời gian họ sẽ xóa hoặc cách ly tệp bị nhiễm và không thể thoát khỏi virus. Khi một chương trình đã nhiễm virus chạy thì virus tự động được kích hoạt.

- Sâu (Worms): worm còn gọi là sâu máy tính là các chương trình phần mềm khi tiếp xúc với máy tính (hoặc các thiết bị lưu thông tin khác) thì có khả năng lưu trú, tự nhân bản tức là tái tạo gấp nhiều lần những bản sao giống hệt nó mặc dù bạn không thực hiện bất kỳ thao tác gì. Các bản sao tự tìm cách lan truyền qua các máy tính khác trong cùng hệ thống mạng (thường là qua hệ thống thư điện tử) sử dụng cùng hệ điều hành mà người sử dụng không hề hay biết, ngoài tác hại thẳng lên máy bị nhiễm như: xóa và/hoặc thay đổi dữ liệu trong các máy tính đó, chiếm dung

lượng bộ nhớ làm cho máy hoạt động chậm hẳn lại hoặc bị "treo", nhiệm vụ chính của worm là phá các mạng (network) thông tin, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này. worm cũng là một loại virus có một số đặc tính riêng mà thôi. Sâu máy tính có thể xâm nhập vào hệ thống mail của bạn để tự gửi email đến tất cả các địa chỉ trong contact list của bạn.

- Zombie (còn được gọi là bots) là một phần mềm được thiết kế để giành quyền kiểm soát một máy tính có kết nối Internet. Mỗi máy này đều nằm dưới sự kiểm soát của một hệ thống ở trên, từ đó có thể điều khiển từ xa tới tất cả các máy bị nhiễm từ một điểm duy nhất. Bằng cách này, các tin tặc có thể thực hiện các cuộc tấn công quy mô lớn, bao gồm cả tấn công từ chối dịch vụ (DDos), lợi dụng sức mạnh của các "zombie" để tấn công áp đảo các trang web hoặc dịch vụ đến mức quá tải, gây ra tình trạng nghẽn mạng, treo máy…Các cuộc tấn công phổ biến khác của Botnet như đính kèm vào email spam, tăng độ lây nhiễm sang nhiều máy khác và cố gắng ăn cắp dữ liệu tài chính, trong khi các Botnet nhỏ hơn được sử dụng vào các mục tiêu đặc biệt nào đó. Botnet được thiết kế để ẩn mình sao cho người dùng hoàn toàn không biết máy của họ bị kiểm soát bởi tin tặc.

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.

Những cuộc tấn công, xâm nhập từ bên trong hoặc bên ngoài đều có thể bị hệ thống IDS nhận biết được thông qua hai thành phần quan trọng của IDS là sensor (bộ

cảm nhận) có chức năng chặn bắt và phân tích lưu lượng mạng, signature database là cơ sở dữ liệu chứa dấu hiệu của các cuộc tấn công đã được phát hiện và phân tích vì vậy để duy trì một hệ thống IDS phải cập nhật thường xuyên cơ sở dữ liệu.

Hệ thống IDS cần phải đáp ứng những yêu cầu sau:

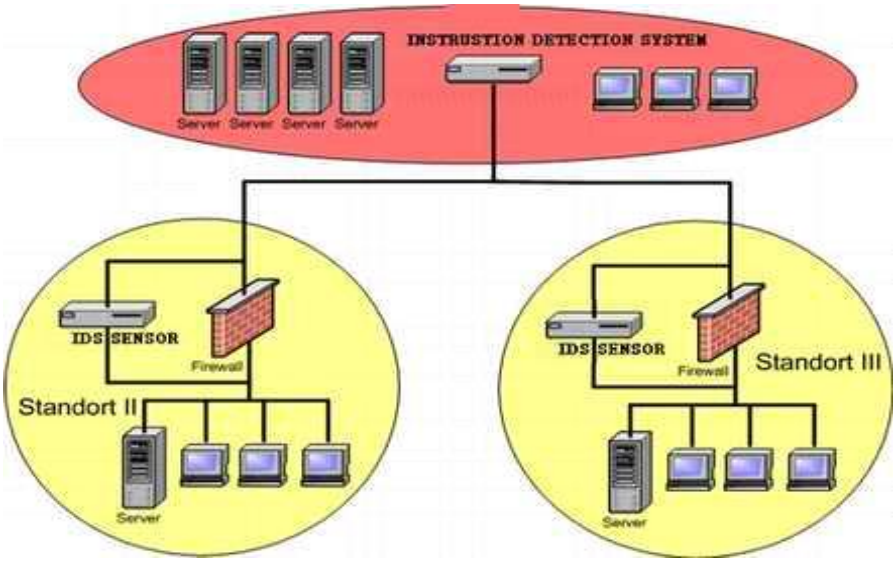
- Tính chính xác (Accuracy): không được coi những hành động thông thường trong môi trường hệ thống là những hành động bất thường hay lạm dụng hành động thông thường bị coi là bất thường được gọi là false positive.

- Hiệu năng (Performance):Phải đảm bảo hiệu năng của IDS có thể phát hiện xâm nhập trái phép trong thời gian thực (thời gian thực là hành động xâm nhập trái phép phải được phát hiện trước khi xảy ra hư hỏng nghiêm trọng tới hệ thống).

- Tính toàn vẹn (Completeness): IDS không được bỏ qua một xâm nhập trái phép nào (xâm nhập không bị phát hiện gọi là false negative). Đây là một điều kiện khó có thể thỏa mãn được vì hầu như không thể có tất cả thông tin về các tấn công từ quá khứ, hiên tại và tương lai.

- Chịu lỗi (Fault Tolerance): Nếu có cuộc tấn công, xâm nhập thì IDS phải có khả năng kháng cự lại.

- Khả năng mở rộng (Scalability): Trong một trạng thái xấu nhất IDS phải có khả năng xử lý và không bỏ sót thông tin, có liên quan đến hệ thống mà các sự kiện tương quan đến từ nhiều nguồn tài nguyên với số lượng host nhỏ. Với sự phát triển mạnh và nhanh của mạng máy tính, hệ thống có thể bị quá tải bởi sự tăng trưởng của số lượng sự kiện.



Hình 1.5. Các vị trí đặt IDS trong mạng

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.

Hình 1.6. Kiến trúc thông thường của IDS

- Thành phần thu thập thông tin: Việc thu thập thông tin ở đây chính là việc lấy các thông tin liên quan đến tình trạng hoạt động của các thiết bị trong hệ thống mạng, lưu lượng mạng, gói tin truyền trong mạng. Tuy nhiên, trong những hệ thống mạng lớn thì các dịch vụ hay các thiết bị không đặt tại trên máy, một địa điểm mà nằm trên các máy chủ, các hệ thống con riêng biệt nhau. Các thành phần hệ thống cũng hoạt

động trên những nền tảng hoàn toàn khác nhau. Mô hình Log tập trung được đưa ra để giải quyết vấn đề này. Cụ thể, là tất cả Log sẽ được chuyển về một trung tâm để phân tích và xử lý. Các gói tin qua card mạng chúng đều được IDS phân tích, xử lý, sao lưu đến từng trường thông tin, sau đó xác định chúng thuộc kiểu gói tin nào, dịch vụ gì... sau khi phân tích xong các thông tin này được chuyển đến thành phần phân tích phát hiện tấn công.

- Thành phần phân tích thông tin: Chức năng này là quan trọng nhất và bộ cảm biến (sensor) đóng vai trò quyết định. Nhiệm vụ của bộ cảm biến là dùng để lọc thông tin và loại bỏ dữ liệu không tương thích, phát hiện những điều bất thường, những mối đe dọa của hệ thống. IDS tổng hợp và xử lý thông tin đưa về dạng chuẩn, sau đó hệ thống sẽ quyết định trạng thái hiện tại có phải là tấn công hay không, sau khi thông tin được tập hợp và đưa về dạng chuẩn sẽ sinh ra các cảnh báo.

- Thành phần cảnh báo: Là bước cuối cùng thực hiện việc tiếp nhận, đánh giá thông tin từ thành phần phân tích sau đó sẽ đưa ra các quyết định phản ứng, hình thức phản hồi đưa thông tin cảnh báo tới người quản trị và thực hiện những công tác nhằm chống lại những mối đe dọa, khắc phục các sự cố có thể sảy ra. Cảnh báo có thể thông qua email, SMS, hoặc thực thi các mã script nhằm hạn chế hậu quả của sự cố.

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

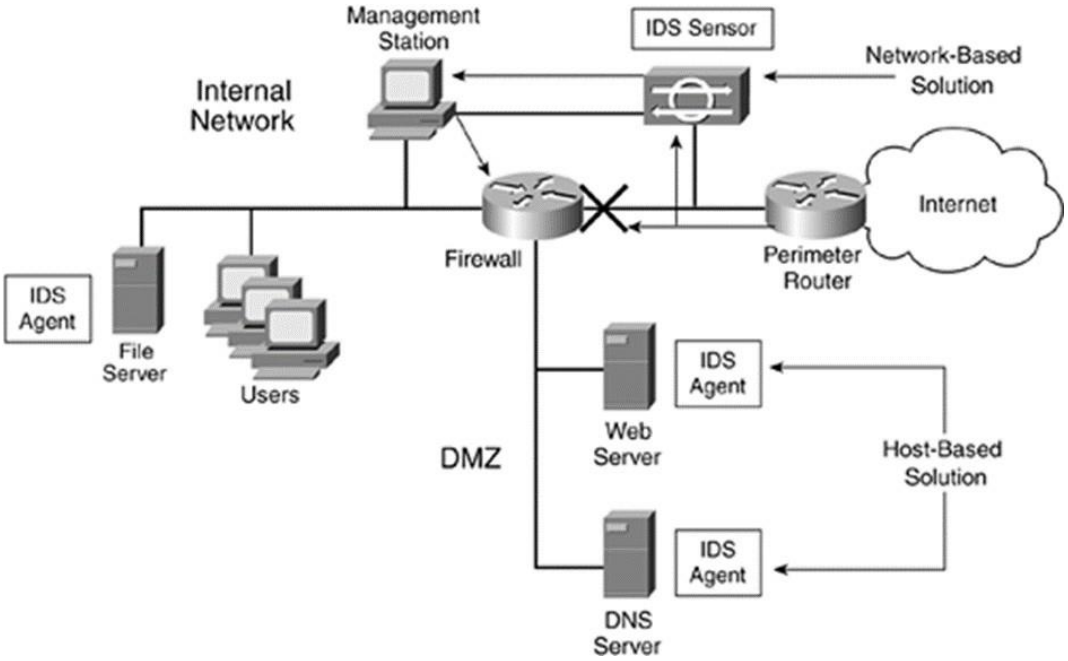
Có thể phân loại phát hiện tấn công, xâm nhập mạng theo 2 cách: Phân loại dựa trên kỹ thuật phát hiện và phân loại dựa trên nguồn dữ liệu. Dựa trên kỹ thuật phát hiện, có thể chia các kỹ thuật phát hiện thành 2 loại chính: Phát hiện dựa trên dấu hiệu hoặc chữ ký (Signature-Based) và phát hiện dựa trên bất thường (Anomaly-Based), 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)

HIDS được cài đặt cục bộ trên một máy tính (host) để giám sát hoạt động hoặc các hành vi xâm nhập trên máy tính. Hệ thống phát hiện xâm nhập dựa trên máy chủ HIDS hoạt động dựa trên thông tin được thu thập từ bên trong một hệ thống máy tính

riêng lẻ. Điểm thuận lợi này cho phép HIDS phân tích các hoạt động để xác định chính xác quá trình và người dùng nào tham gia vào một cuộc tấn công vào một hệ thống hoặc máy chủ cụ thể. HIDS không giám sát các hoạt động của cả một vùng mạng mà thường được đặt trên các server hay các máy client quan trọng trong vùng DMZ (Demilitarized Zone) HIDS có thể nhìn thấy kết quả của một cuộc tấn công có chủ đích, vì chúng có thể trực tiếp truy cập và giám sát các tệp dữ liệu và quy trình hệ điều hành mà cuộc tấn công nhắm mục tiêu.Nếu các thông tin thu thập được vượt quá ngưỡng cho phép thì hệ thống HIDS sẽ sinh ra cảnh báo.

Mô hình hệ thống các HIDS trong mạng minh họa trên Hình 1.7.



Hình 1.7. Mô hình hệ thống các HIDS trong mạng

HIDS giám sát các hoạt động trên host và có thể nhanh chóng phát hiện các tấn công local-to-root hoặc công local-to-local, HIDS có một khái niệm rõ ràng về thông tin nội bộ phù hợp, vì vậy các cuộc tấn công . Chính vì vậy công cụ phát hiện dị thường (ADE) có độ bao phủ và quản lý tốt hơn đối với các vấn đề bên trong vì khả năng phát hiện của chúng được dựa vào mẫu hành vi thông thường của người dùng.

- 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…).

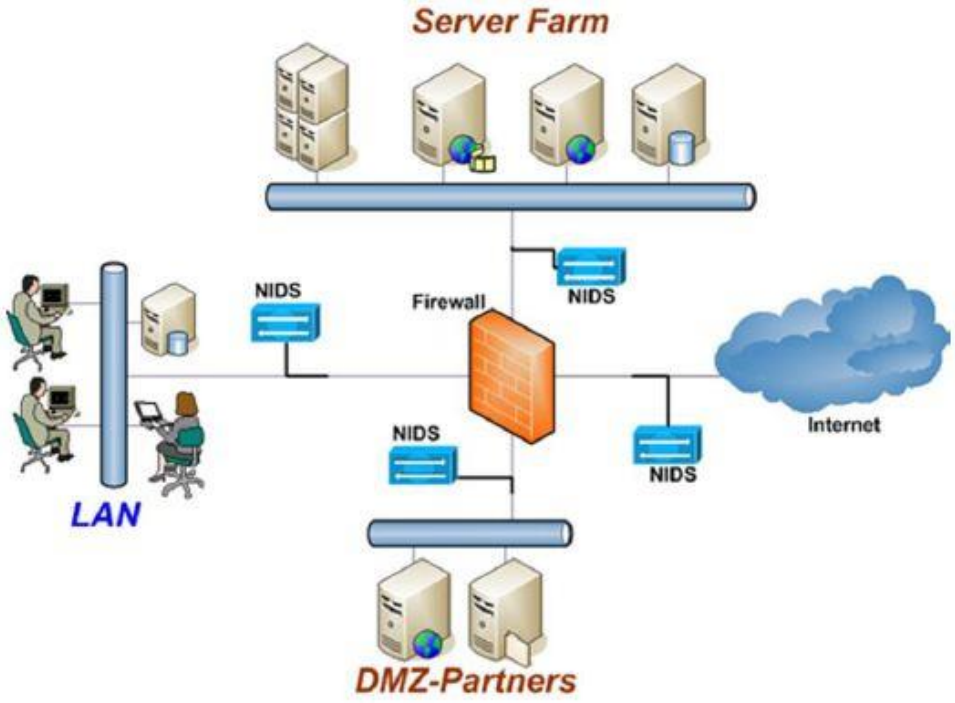
+ HIDS cần có tài nguyên trên host để hoạt động.

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. NIDS không thể phân tích các dữ liệu đã mã hóa, những luồng thông tin thu thập được từ việc giám sát hoạt động mạng như: Địa chỉ IP nguồn - đích, cổng nguồn – đích của các giao dịch TCP/UDP, các gói tin ICMP (Internet control message protocol) với thông điệp không tìm thấy trạm đích, các máy chủ và dịch vụ đang được sử dụng trong mạng. Đó là căn cứ để hệ thống phát hiện tấn công đột nhập có thể đưa ra các cảnh báo.

- NIDS ngoài luồng (out-stream): Các luồng dữ liệu không cho phép NIDS can thiệp một cách trực tiếp, chúng chỉ được sao chép và phân tích để phát hiện các dấu hiệu của các cuộc tấn công xâm nhập.

- NIDS trong luồng (in-stream): NIDS sẽ được đặt firewall để luồng dữ liệu đi qua đó, và có thêm chức năng chặn lưu thông.



Hình 1.8. Mô hình hệ thống các NIDS trong mạng

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)

Đây là các IDS hoạt động dựa trên chữ ký, giám sát các gói tin trên mạng tương tự như cách phần mềm diệt virus hoạt động [3]. Tuy nhiên Signature-Based có thể không phát hiện được những mối đe dọa mới, vì vậy cần có một cơ sở dữ liệu về các dấu hiệu xâm nhập hay còn gọi là (signature database), nó phải được cập nhật liên tục mỗi khi có một loại kỹ thuật tấn công xâm nhập mới. Tính chính xác của IDS phụ thuộc vào (signature database).

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. Quá trình xử lý dữ liệu đươc đem so sánh với các file dữ liệu mẫu có sẵn trong cơ sở dữ liệu đã có, nếu giống nhau thì sẽ đưa ra cảnh báo 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, nếu các hoạt động hiện tại không phù hợp với hoạt động thông thường của hệ thống IDS sẽ xác định là bất thường và gửi đi cảnh báo [3]. Ví dụ, trong điều kiện bình thường, lưu lượng trên một giao tiếp mạng của server là vào khoảng 25% băng thông cực đại của giao tiếp. Nếu tại một thời điểm nào đó, lưu lượng này đột ngột tăng lên đến 50% hoặc hơn nữa, thì có thể giả định rằng server đang bị tấn công DoS. Để hoạt động chính xác, các IDS loại này phải thực hiện một quá trình "học", tức là giám sát hoạt động của hệ thống trong điều kiện bình thường đề ghi nhận các thông số hoạt động, đây là cơ sở để phát hiện các bất thường về sau.

Trong thực tế, IDS là một kỹ thuật mới so với Firewall, tuy nhiên cho đến thời điểm hiện tại với sự phát triển mạnh mẽ của kỹ thuật tấn công thì IDS vẫn chưa thực sự chứng tỏ được tính hiệu quả của nó trong việc đảm bảo an toàn cho các hệ thống. Xu hướng hiện nay là chuyển dịch dần sang các hệ thống IPS có khả năng phát hiện và ngăn chặn một cách hiệu quả các cuộc tấn công mạng, đồng thời giảm thiểu thời gian chết và các chi phí ảnh hưởng đến hiệu quả hoạt động của mạng.

1.3. Kết luận chương 1

Như vậy, chương 1 đã trình bày tổng quan về tấn công, xâm nhập, các dạng tấn công xâm nhập thường gặp; đồng thời chương 1 cũng đã khái quát về phát hiện xâm nhập cũng như các kỹ thuật phát hiện xâm nhập qua đó ta có cái nhìn rõ hơn về tấn công, xâm nhập.

CHƯƠNG 2. CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP

2.1. Các hệ thống phát hiện xâm nhập mã mở

2.1.1. SNORT

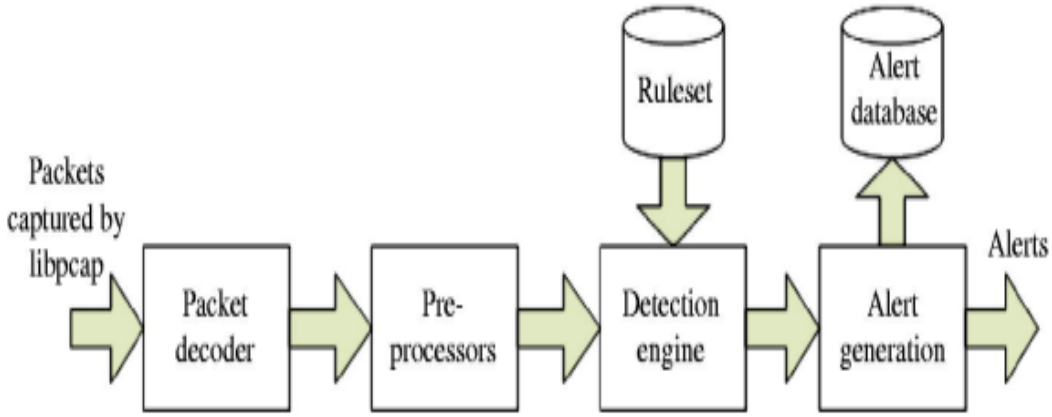
2.1.1.1. Giới thiệu về Snort

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 …

Snort có thể phát hiện và phản ứng với các cuộc tấn công bằng nhiều hình thức khác nhau chẳng hạn như gửi thông điệp cảnh báo, hay huỷ gói tin khi phát hiện có sự bất thường tất cả phụ thuộc vào cấu hình mà quản trị viên thiết lập, bên cạnh đó snort có thể cấu hình như một NIDS.

Cơ sở dữ liệu luật của Snort rất đa dạng lên tới hơn 2930 luật và được cập nhật thường xuyên đây là điều kiện tiên quyết để Snort hoạt động hiệu quả. Snort có thể cài đặt và hoạt động trên nhiều nền tảng như: Windows, MacOS, Linux, NetBSD,Solaris… Snort có kiến trúc theo kiểu module, nên tính năng của hệ thống có thể được quản trị viên cài đặt thêm cho hệ thống hoặc viết thêm các module mới

2.1.1.2. Thành phần và chức năng



Hình 2.1: Mô hình kiến trúc hệ thống Snort

Snort bao gồm 05 thành phần chính đó là:

a. Module giải mã gói tin (Packet Decoder)

Dữ liệu đi qua các cổng giao tiếp mạng sẽ được Module này là phân tích gói dữ liệu thô bắt được trên mạng và hồi phục thành gói dữ liệu hoàn chỉnh ở lớp application, làm đầu vào cho Module phát hiện.Module này có thể tạo ra cảnh báo cho riêng mình dựa vào các tiêu đề của giao thức, các gói tin bất thường không chính xác.

b. Module tiền xử lý (Preprocessors)

Xử lý các gói tin đã bắt được dựa trên một số plugin nhất định. Các plugin này kiểm tra hành vi hoặc sự bất thường của loại đã biết. Bộ tiền xử lý là một phần không thể thiếu của bất kỳ IDS nào để chuẩn bị các gói dữ liệu được kiểm tra bởi công cụ phát hiện dựa trên các quy tắc trong công cụ phát hiện vì những kẻ xâm nhập có thể sửa đổi các gói đó để thoát khỏi bất kỳ sự phát hiện nào.

Ba nhiệm vụ chính của Module này là:

+ Kết hợp lại các gói tin

+ Giải mã và chuẩn hóa giao thức (decode/normalize)

+ Phát hiện các xâm nhập bất thường (nonrule /anormal)

c. Module phát hiện (Detection Engine)

Sau khi dữ liệu được xử lý bởi Module tiền xử lý, dữ liệu sau đó sẽ được chuyển cho Module phát hiện. Module phát hiện là thành phần quan trọng nhất của IDS dựa trên chữ ký trong Snort.

Nó khớp các gói dữ liệu với bộ quy tắc cho bất kỳ chữ ký xâm nhập nào có trong gói dữ liệu. Nếu các quy tắc khớp với các gói dữ liệu thì nó sẽ được chuyển đến bộ xử lý cảnh báo. Có thể mất nhiều thời gian khác nhau để phản hồi một số loại gói bất kể hệ thống máy tính mà nó đang chạy.

Detection Engine có khả năng tách các thành phần của gói tin ra và áp dụng các tập luật lên từng phần nào của gói tin đó. Các phần đó có thể là:

+ IP header

+ Header ở tầng giao vận: TCP, UDP

+ Header ở tầng ứng dụng: FTP header, DNS header, HTTP header,…

+ Phần tải của gói tin.

Các luật trong Snort cũng được đánh thứ tự ưu tiên, vì vậy khi một gói tin được phát hiện bởi nhiều tập luật khác nhau thì thông báo đưa ra sẽ là thông báo ứng với tập luật có mức ưu tiên lớn nhất.

d. Module log và cảnh báo (Logging and Alerting System)

Module này xử lý việc tạo ra các cảnh báo và ghi nhật ký. Tất cả các cảnh báo và nhật ký được lưu giữ trong các tệp văn bản thuần túy đơn giản hoặc tệp kiểu tcp-dump.

e. Module kết xuất thông tin (Output Module)

Module kết xuất thông tin giúp lưu các bản ghi được tạo bởi hệ thống ghi nhật ký và cảnh báo theo nhiều cách khác nhau như trong các tệp nhật ký văn bản thuần túy đơn giản, đăng nhập vào cơ sở dữ liệu như MySQL hoặc Oracle hoặc tạo XML tùy thuộc vào cấu hình được đặt thành tệp cấu hình Snort.

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 khác nhau như: buffer overflow, CGI-Attack, 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 xảy 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

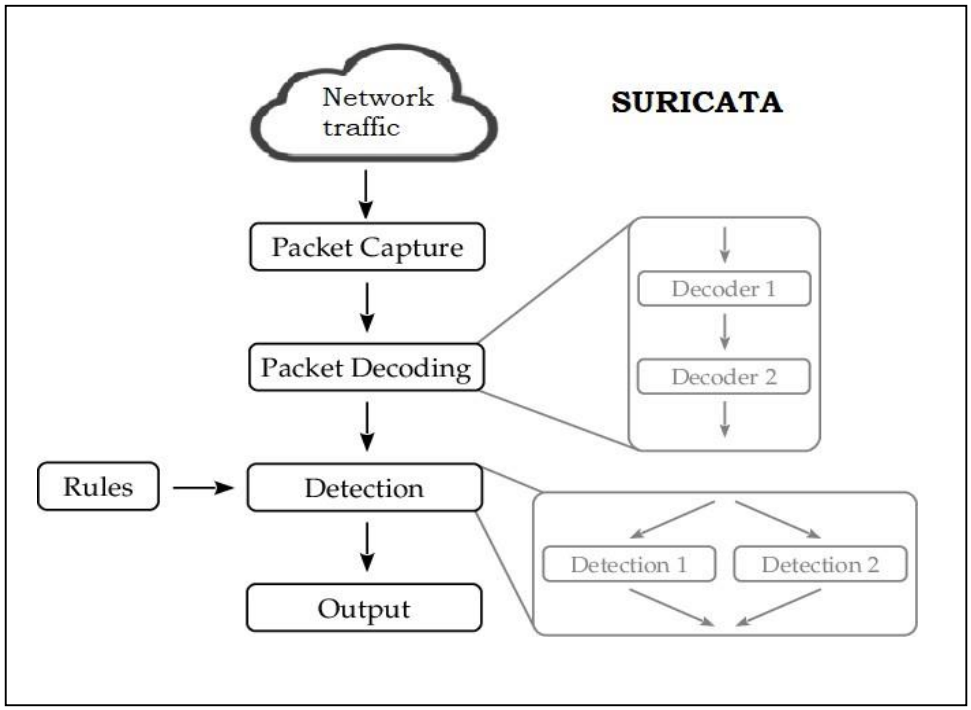
2.1.2.1. Giới thiệu Suricata.

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].

Suricata dựa trên một bộ quy tắc phát triển bên ngoài, để giám sát lưu lượng mạng và cung cấp cảnh báo cho người quản trị hệ thống khi xảy ra các sự kiện đáng ngờ. Được thiết kế để tương thích với các thành phần bảo mật mạng hiện có, cung cấp chức năng đầu ra hợp nhất và các tùy chọn thư viện có thể cắm để chấp nhận cuộc gọi từ các ứng dụng khác. Suricata là một công cụ đa luồng cung cấp tốc độ và hiệu quả cao hơn trong việc giám sát và phân tích lưu lượng mạng. Với khả năng xử lý

cao được hỗ trợ bởi chip CPU đa lõi suricata có thể tận dụng tối đa hiệu năng của phần cứng.

2.1.2.2. Thành phần chức năng của Suricata



Hình 2.2: Mô tả sơ đồ Suricata.

Kiến trúc của Suricata gồm 4 thành phần cơ bản:

a. Module giải mã gói tin (Packet Decoder)

Packet Decoder(module giải mã gói tin) là một thiết bị phần cứng hoặc phần mềm được đặt vào trong hệ thống mạng. Chức năng của nó tương tự như việc nghe lén trên điện thoại di động, nhưng thay vì hoạt động trên mạng điện thoại nó nghe lén trên mạng dữ liệu. Bởi vì trong mô hình mạng có nhiều giao thức cao cấp như TCP, UDP, ICMP... nên công việc của module giải mã gói tin là nó phải phân tích các giao thức đó thành thông tin mà con người có thể đọc và hiểu được.

Khi Suricata đã nhận các gói tin từ quá trình phân tích nó sẽ đi vào quá trình giải mã. Chính xác thì nơi mà gói tin đi vào bộ giải mã phụ thuộc vào lớp liên kết mà trước đó đọc được.

Bất kể là lớp liên kết nào đang được sử dụng, tất cả các bộ giải mã sẽ đều làm việc theo một kiểu chung. Đối với trường hợp các lớp cụ thể, con trỏ trong cấu trúc

của gói tin sẽ được thiết lập trỏ tới một phần khác của gói tin. Dựa vào các thông tin đã giải mã được, nó sẽ gọi các lớp cao hơn và giải mã cho đến khi không còn bộ giải mã nào nữa.

b. Module tiền xử lý (Preprocessors)

Module tiền xử lý là plug-in đóng vai trò quan trọng đối với hệ thống IDS/IPS, cho phép phân tích cú pháp dữ liệu theo những cách khác nhau. Nếu chạy Suricata mà không có bất cứ cấu hình nào về preprocessors trong tập tin cấu hình sẽ chỉ thấy từng gói dữ liệu riêng rẽ trên mạng. Điều này có thể làm IDS bỏ qua một số cuộc tấn công, vì nhiều loại hình tấn công hiện đại cố tình phân mảnh dữ liệu hoặc có tình đặt phần độc hại lên một gói tin và phần còn lại lên gói tin khác (kỹ thuật lẩn trốn).

Sau khi dữ liệu được module giải mã gói tin xử lý nó sẽ được đưa vào module tiền xử lý. Suricata cung cấp một loạt các module tiền xử lý ví dụ như: Frag3 (một module chống phân mảnh gói tin IP), sfPortscan (module được thiết kế chống lại các cuộc trinh sát, như scan port, xác định dịch vụ, scan OS), Stream5 (module tái gộp các gói tin ở tầng TCP).

Nhiệm vụ của module tiền xử lý là: kết hợp lại các gói tin, giải mã và chuẩn hóa giao thức và phát hiện các xâm nhập bất thường

c. Module phát hiện (Detection engine)

Module phát hiện là module quan trọng nhất của Suricata, các luồng dữ liệu sau khi được kiểm tra ở Preprocessors sẽ được xử lý bằng cách cách sử dụng các luật được định nghĩa trước để so sánh với dữ liệu thu thập được. Nếu dữ liệu trùng khớp với các tập luật sẽ tạo ra thông báo và kết xuất thông tin.

Bản thân suricata có nhiều các tập luật, có thể chia làm 2 loại:

- Phần Header: Luôn là thành phần đầu tiên trong rules và nó đòi hỏi các thành phần cần có trong rules. Nó đòi hỏi các thành phần sau: Log/alert, các loại giao thức Protocol
- Phần Options: Các gói tin sẽ được tạo ra để phù hợp với luật.

Bản thân suricata nó có rất nhiều các luật xử lý vì vậy bất cứ ai tìm hiểu về suricata cần phải nắm rõ về nó. Nếu đã hiểu được cấu trúc các luật trong suricata thì người dùng có thể dễ dàng tối ưu cấu hình cho hệ thống phát hiện xâm nhập của mình.

Các mức cảnh báo sẽ được đưa ra sẽ được ứng với tập luật có mức ưu tiên cao nhất do các luật được đánh thứ tự ưu tiên

d. Module log và cảnh báo (Alert generation)

Cuối cùng sau khi các luật đã phù hợp với dữ liệu, chúng sẽ được chuyển tới thành phần cảnh báo và ghi lại. Cơ chế log sẽ lưu trữ các gói tin đã kích hoạt, các luật còn cơ chế cảnh báo sẽ thông báo các phân tích bị thất bại.

Trong Suricata hỗ trợ các định dạng log như sau:

+ Eve.json

+ Fast.log

+ http.log

+ Stats.log

+ Unified2.alert

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: Suricata 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. Nó chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD, FreeBSD, MacOS, Solaris và Windows.

OSSEC là một dự án đang phát triển, với hơn 500.000 lượt tải xuống mỗi năm. Nó được sử dụng bởi tất cả mọi người, từ các doanh nghiệp lớn đến các doanh nghiệp nhỏ đến các cơ quan chính phủ làm hệ thống phát hiện xâm nhập máy chủ chính của họ - cả trên cơ sở và trên đám mây. Một trong những triển khai lớn nhất của OSSEC là Apple, ngoài ra Netflix và Facebook cũng đã sử dụng nó. Ngoài việc được triển khai để bảo vệ máy chủ, OSSEC, thường được sử dụng nghiêm ngặt như một công cụ phân tích nhật ký, giám sát và phân tích tường lửa, IDS, máy chủ web và nhật ký xác thực.

OSSEC cũng hoạt động dựa trên các luật của nó và người sử dụng có thể phân phối lại hoặc sửa đổi nó theo ý muốn hay mục đích của mình. Khách hàng có thể xác định cấu hình các sự cố muốn được cảnh báo. Tích hợp với smtp, sms và syslog cho phép khách hàng cập nhật các cảnh báo bằng cách gửi chúng đến các thiết bị hỗ trợ email. Các tùy chọn phản hồi tích cực để chặn một cuộc tấn công ngay lập tức cũng có sẵn. OSSEC chỉ có thể cài đặt trên Windows với tư cách là một agent.

2.1.3.2. Thành phần và chức năng

Phát hiện xâm nhập dựa trên nhật ký (Log based Intrusion Detection - LIDs)

Sử dụng dữ liệu nhật ký hệ thống, chủ động theo dõi và phân tích dữ liệu từ nhiều điểm dữ liệu nhật ký trong thời gian thực, cố gắng phát hiện một số điểm bất thường

Phát hiện phần mềm độc hại và Rootkit

Quy trình và phân tích cấp độ tệp để phát hiện các ứng dụng độc hại và rootkit

Phản hồi tích cực

Phản ứng với các cuộc tấn công và thay đổi trên hệ thống trong thời gian thực thông qua nhiều cơ chế bao gồm các chính sách tường lửa, tích hợp với các bên thứ 3 như CDN và các cổng hỗ trợ, cũng như các hành động tự phục hồi

Kiểm toán sự tuân thủ

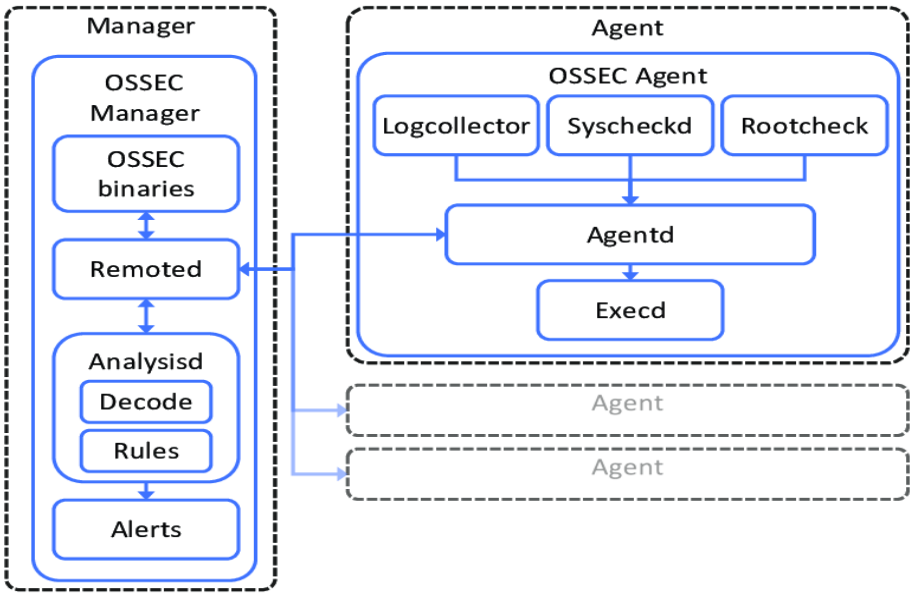
Kiểm tra mức độ ứng dụng và hệ thống để tuân thủ nhiều tiêu chuẩn chung như PCI-DSS và các tiêu chuẩn CIS

Hệ thống quản lý nhận dạng (File Integrity Monitoring - FIM):

Đối với cả tệp và cài đặt sổ đăng ký trong thời gian thực, không chỉ phát hiện các thay đổi đối với hệ thống, nó còn duy trì một bản sao pháp lý của dữ liệu khi nó thay đổi theo thời gian.

Kiểm kê hệ thống

Thu thập thông tin hệ thống, chẳng hạn như phần mềm đã cài đặt, phần cứng, việc sử dụng, dịch vụ mạng, bộ nghe và thông tin khác.



Hình 2.3: 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.

Server không chạy trên Windows OS.

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.

- Chiếm lượng memory và CPU nhỏ,không đáng kể
- 1 số thông tin được thu thập theo thời gian thực
- 1 số thông tin thì lại được thu thập định kỳ

Nhưng khi nói Agent thì là để chỉ máy Client được cài gói Ossec-agent.

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.

Khi cài đặt trong VMware ESX giúp nhận được thời điểm các VM guest được khởi tạo, xóa đi, khởi động,.. Ossec cũng giám sát việc login,logouts và các lỗi bên trong ESX server

Ngoài ra nó cũng cảnh báo nếu bất kỳ tùy chọn cấu hình không an toàn nào được bật.

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)

+ Kết hợp với smtp,sms,syslog sẽ cho phép người dùng nhận cảnh báo trên các thiết bị có hỗ trợ email

+ Ngoài ra tính năng Active-response có thể giúp block 1 cuộc tấn công ngay lập tức.

- 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 giám 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.

Công cụ phân tích Sense Analytics Engine nâng cao là trung tâm của giải pháp này, được thiết kế để ghi nhận lại các sự kiện, nhật ký thời gian thực, cũng như các luồng dữ liệu qua hệ thống mạng, từ đó phát hiện ra các lỗ hổng bảo mật và xâm nhập từ bên ngoài. Qradar SIEM là giải pháp bảo mật doanh nghiệp có khả năng mở rộng, hợp nhất từ nhiều nguồn dữ liệu, sự kiện từ hàng nghìn thiết bị của các hãng khác nhau nhờ hệ thống trung tâm cơ sở dữ liệu khổng lồ của IBM.

Qradar SIEM có thể cài đặt và triển khai đơn giản, dễ dàng với giao diện trực quan được chia thành các module riêng biệt, sẽ giúp bộ phận IT nhanh chóng xác định và khắc phục các cuộc tấn công mạng dựa trên mức độ ưu tiên, tính tuân thủ nhờ

hệ thống cảnh bảo các hoạt động bất thường, đảm bảo tối đa an toàn cho hệ thống từ bên trong lẫn bên ngoài.

Các dữ liệu được thu thập và phân tích bởi Qradar SIEM:

- Security events (Sự kiện bảo mật): Từ hệ thống Firewall, VPN, hệ thống phát hiện và ngăn chặn xâm nhập, cơ sở dữ liệu và hơn thế nữa.

- Network events (Sự kiện mạng): Từ các thiết bị endpoint như Switches, routers, servers, hosts…

- Network activity context (Bối cảnh hoạt động mạng): Kiến trúc 7 tầng từ hệ thống mạng và ứng dụng

- User or asset context (Bối cảnh người dùng và tài sản): Dữ liệu từ phạm vi thông tin định danh, thiết bị quản lý truy cập, công cụ quét lỗ hổng bảo mật

- Operating system information: Thông tin hệ điều hành, nhà cung cấp, phiên bản cụ thể trong tài nguyên mạng

- Application logs (Nhật ký ứng dụng): IBM QRadar có thể thu thập các sự kiện nhật ký và dữ liệu luồng mạng từ các ứng dụng dựa trên đám mây và nó có thể được triển khai như một dịch vụ cung cấp SaaS trên đám mây IBM, nơi việc triển khai và bảo trì được thuê ngoài.

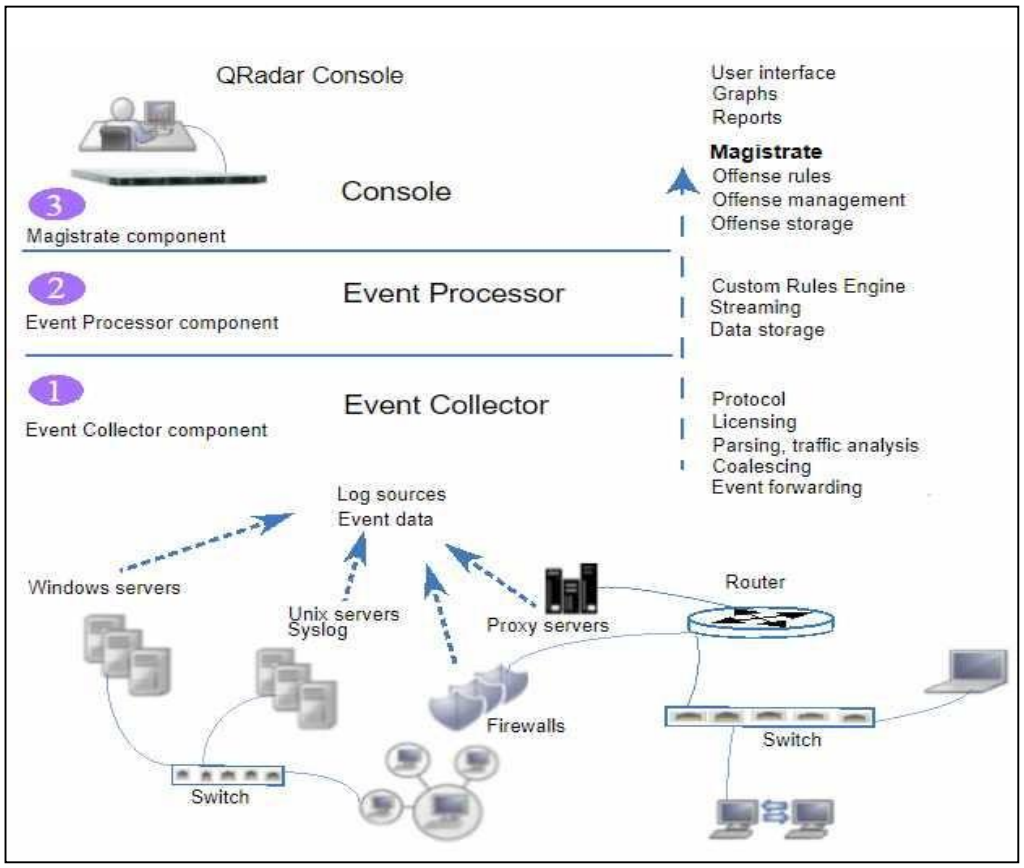
- Threat intelligence (Thông tin mối đe dọa): Theo tùy chọn, IBM QRadar SIEM có thể được mua một phần mở rộng giấy phép cho phép sử dụng IBM Security X-Force Threat Intelligence, tính năng này xác định các địa chỉ IP và URL có liên quan đến hoạt động độc hại. Đối với mỗi địa chỉ IP hoặc URL được xác định, nguồn cấp dữ liệu thông minh về mối đe dọa bao gồm điểm số và danh mục mối đe dọa, có thể giúp tổ chức phân tích và ưu tiên các mối đe dọa tốt hơn.

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 xử lý các dữ liệu đó. ECS gồm 3 thành phần chính:

- Event collector component
- Event processor component

- Magistrate



Hình 2.4: Minh hoạ sơ đồ IBM Qradar

a. Event Collector Component

Đối với Event

- Protocol: Nhận các dữ liệu đầu ra từ các giao thức mã nguồn Log mà các giao thức đó được Qradar hỗ trợ trong việc thu thập các sự kiện từ các thiết bị nguồn.
- Throttle: Giám sát số lượng sự kiện và lưu vào hệ thống để quản lý cấp phép đầu vào. Qradar sẽ cho phép lưu lượng các sự kiện đầu vào của mỗi thiết bị là bao nhiêu.
- Parsing: Lấy các sự kiện từ các thiết bị nguồn và phân tích.
- Log source traffic analysis & auto discovery: Áp dụng phân tích dữ liệu các sự kiện. Khi thu thập các trường sự kiện trên các thiết bị khác nhau, Qradar sẽ bóc tách các trường đó thành một chuẩn chung.

- Coalescing: Sự kiện được phân tích sau đó kết hợp lại dựa trên các loại sự kiện phổ biến. Khi 4 sự kiện được nhìn thấy với cùng một nguồn IP, IP đích, cổng đích và Tên truy nhập, các thông điệp tiếp theo cho đến 10 giây của cùng một khuôn mẫu được kết hợp lại với nhau. Điều này được thực hiện để giảm trùng lặp dữ liệu được lưu trữ.

- Event forwarding: Áp dụng quy tắc định tuyến cho hệ thống, chẳng hạn như gửi các tín hiệu đến các thiết bị ngoại vi, hệ thống SysLog bên ngoài, hệ thống JSON, hệ thống SIEM khác… Ở đây dữ liệu sẽ được chuyển đến Processor.

Đối với Flow

- Luồng trùng lặp: là quá trình loại bỏ các trùng lặp khi nhiều luồng QFlow giống nhau được thu thập cung cấp dữ liệu cho thiết bị xử lý luồng.

- Kết hợp bất đối xứng: Chịu trách nhiệm về kết hợp luồng bên trong và ngoài khi dữ liệu được cung cấp không đối xứng. Quá trình này có thể nhận ra các luồng từ mỗi bên và kết hợp chúng vào trong một bản ghi. Tuy nhiên, đôi khi không tồn tại dữ liệu ở hai bên.

- Throttle: Giám sát số sự kiện và lưu vào hệ thống để quản lý cấp phép đầu vào.

- Chuyển tiếp: Áp dụng quy tắc định tuyến cho hệ thống, chẳng hạn như gửi các tín hiệu đến các thiết bị ngoại vi, hệ thống SysLog bên ngoài, hệ thống JSON, hệ thống SIEM khác…

b. Event Processor Component

- Custom Rules Engine: Chịu trách nhiệm xử lý các sự kiện nhận được từ Qradar và so sánh chúng với các luật, duy trì theo dõi các hệ thống có liên quan đến sự kiện theo thời gian. Tạo ra các thông báo cho người dùng và các vi phạm.

- Host profile: Chịu trách nhiệm giải quyết các thông tin tài sản từ luồng dữ liệu thụ động. Luồng cung cấp thông tin về hoạt động mạng và cho phép Qradar xây dựng một cơ sở dữ liệu về tài sản.

- Streaming: Chịu trách nhiệm cho việc gửi dữ liệu sự kiện thời gian thực đến Console khi người dùng đang xem các sự kiện từ tab Log Activity với thời gian thực.

- Storage: Theo thời gian cơ sở dữ liệu các sự kiện và luồng được lưu trữ theo từng phút. Dữ liệu được lưu trữ nơi sự kiện được xử lý. Những sự kiện đi vào thiết bị, chúng được xử lý bởi ECS và được lưu trữ cục bộ trên thiết bị trong giai đoạn lưu trữ của ECS. Khi thu thập Log từ các Collector, các Log được cho là an toàn và không an toàn (có sự tấn công) sẽ được lưu trữ tại Ariel máy chủ Processor. Riêng Log không an toàn (có sự tấn công) sẽ được lưu trữ tại Ariel của Console.

c. Magistrate

Magistrate Processing Core (MPC) Chịu trách nhiệm tương quan giữa các hành vi vi phạm với các sự kiện được gửi từ nhiều Event Processor. Chỉ có Console mới có thành phần Magistrate

- Offenses rules: Giám sát và tác động đến các sự kiện vi phạm, chẳng hạn như tạo ra các thông báo email khi có các sự kiện vi phạm các quy tắc được để ra.
- Offense management: Cập nhật, quản lý các hành vi vi phạm. Tiếp cận các hành vi vi phạm để đưa cho người sử dụng các thông tin về vi phạm qua Tab Offenses.
- Offense storage: Ghi dữ liệu hành vi vi phạm đến một cơ sở dữ liệu. Cơ sở dữ liệu trên Console thường lưu dữ các sự kiện vi phạm.

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.
- IBM QRadar có khả năng lưu trữ nhiều người thuê trong một lần triển khai. Miền được tạo cho mỗi người thuê liên kết các nguồn dữ liệu với chúng và cách ly môi trường của người thuê với nhau.
- IBM cung cấp tài liệu đặc biệt cho từng khía cạnh của sản phẩm, đây là một lợi thế lớn để hiểu giải pháp, triển khai và quản trị nó.

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

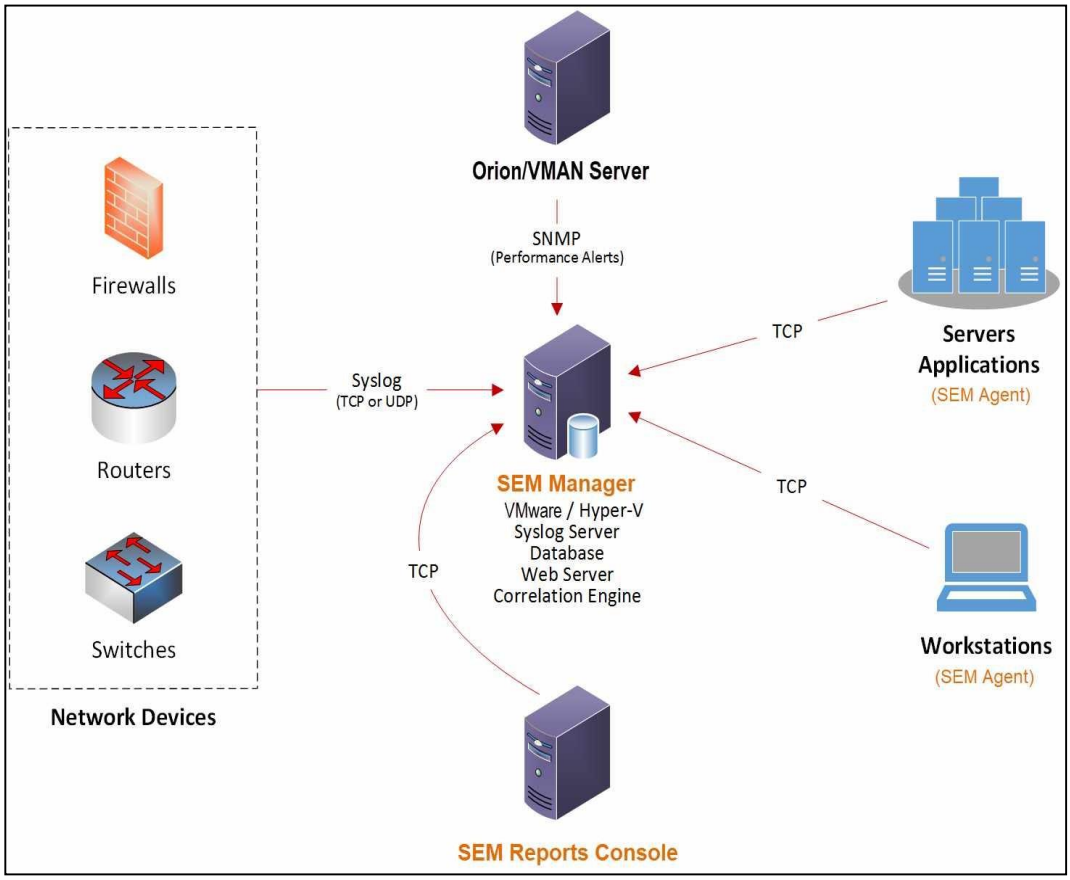
SSEM là một phần mềm giải pháp phát hiện xâm nhập máy tính cạnh tranh về chi phí phục vụ cho việc tuân thủ bảo mật và quản lý nhật ký [9]. SSEM sử dụng cách tiếp cận chủ động giúp người dùng xác định được các mối đe dọa trong thời gian thực. SSEM tự động thu thập và đăng nhập dữ liệu từ các thiết bị mạng, hệ thống và các ứng dụng trên toàn cơ sở hạ tầng CNTT. Sau đó nó sẽ bình thường hóa dữ liệu này sang một định dạng phù hợp và thực hiện nhiều sự kiện tương quan, cùng với khả năng riêng biệt để thiết lập ngưỡng hoạt động độc lập cho mỗi sự kiện hoặc cho mỗi nhóm các sự kiện. Đây là thiết bị bảo mật thông minh mà người dùng có thể tin tưởng sử dụng và giảm thiểu những sự cố không mong muốn.

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.

- Ops Center: Cung cấp các đồ họa biểu diễn dữ liệu nhật ký và sự kiện. Nó bao gồm một số Widgets giúp dễ xác định các khu vực có vấn đề và hiển thị các điểm nóng trong hệ thống mạng. Có thể chọn các widget từ thư viện tiện ích hoặc thêm các tiện ích tùy chỉnh phản ánh các sự kiện.
- Monitor: Hiển thị các sự kiện trong thời gian thực khi chúng xảy ra trong mạng. Có thể xem chi tiết của một sự kiện cụ thể hoặc tập trung vào các loại sự kiện cụ thể. Chế độ xem này cũng bao gồm một số tiện ích để giúp bạn xác định xu hướng hoặc sự bất thường xảy ra trong mạng của bạn.

- Explore: Cung cấp các công cụ để điều tra các sự kiện và dữ liệu chi tiết. Chọn nDepth để tìm kiếm hoặc xem dữ liệu sự kiện hoặc thông điệp tường trình. Chọn Utilities để xem các tiện ích bổ sung.
- Build: Tạo các thành phần người dùng xử lý dữ liệu trên SSEM Manager. Chọn Group để xây dựng và quản lý nhóm. Chọn Rules để xây dựng và quản lý các quy tắc chính sách. Chọn Users để thêm và quản lý người dùng bảng điều khiển.
- Manager: Quản lý các thuộc tính cho các thiết bị và node. Chọn Thiết bị để thêm và quản lý thiết bị. Chọn Nút để quản lý các trạm (agent) và để xem các thiết bị syslog
- Analyze: Cung cấp tổng quan về tính năng Báo cáo trích xuất và trình bày dữ liệu từ cơ sở dữ liệu. Tính năng này tính năng này hiện tại chưa sử dụng được.



Hình 2.5: Minh họa sơ đồ SolarWinds Security Event Manager.

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]. McAfee Network Security Platform kết hợp khả năng phát hiện và ngăn chặn xâm nhập theo thời gian thực để tạo ra hệ thống an ninh mạng toàn diện và hiệu quả.

2.2.3.2. Thành phần và chức năng

- Bảo vệ phần mềm độc hại nâng cao: Nhiều biện pháp bảo vệ phần mềm độc hại không có chữ ký với nhận dạng nâng cao, tương quan dữ liệu và phân tích. MNSP thực hiện kiểm tra sâu hơn lưu lượng truy cập để phát hiện các chương trình và tải xuống tệp độc hại. Nó sử dụng các tùy chọn quét phần mềm độc hại khác nhau để bảo vệ phần mềm độc hại nâng cao. Điều này bao gồm một trình giả lập PDF được nhúng để phát hiện các mối đe dọa tập lệnh java zero-day trong các bản tải xuống PDF. Nó cũng chạy công cụ chống phần mềm độc hại cổng vào thiết bị NTBA. Ngoài ra, MNSP trích xuất các tệp độc hại tiềm ẩn có thể được gửi lên đám mây McAfee để phân tích. Các tệp đã gửi sau đó được thực thi trong một môi trường ảo.

- Bảo vệ các ứng dụng web: MNSP cung cấp các tính năng khác nhau để bảo vệ các máy chủ ứng dụng web của người sử dụng. Ví dụ, nó sử dụng một công cụ heuristic để phát hiện việc đưa vào SQL. Nền tảng an ninh mạng có thể kiểm tra phản hồi HTTP để đảm bảo máy chủ của họ không bị xâm phạm. Bộ cảm biến nền tảng bảo mật mạng giải mã và phân tích lưu lượng SSL dựa trên khóa cá nhân của máy chủ. Tùy thuộc vào kết quả của cuộc kiểm tra, giao thông được phép đi vào khách hàng hoặc bị chặn.

- Nhận dạng ứng dụng: MNSP có thể xác định các ứng dụng đi qua mạng và hành động trên chúng như được định cấu hình. Vì vậy, người sử dụng có thể cho phép hoặc chặn các ứng dụng hoặc tính năng ứng dụng cụ thể trên mạng của mình. Ví dụ: họ có thể chặn các kết nối đến Facebook từ mạng của mình trong khi vẫn cho phép tất cả các lưu lượng HTTP khác.

- Xác định người dùng và nhóm người dùng: MNSP tích hợp với McAfee Logon Collector để xác định người dùng Windows AD trên mạng của người sử dụng và cả nhóm người dùng mà họ thuộc về. Điều này có nghĩa là bây giờ họ có thể kiểm soát dựa trên người dùng thay vì địa chỉ IP của họ, điều này không phải lúc nào cũng đáng tin cậy. Ví dụ: địa chỉ IP động có thể khác nhau dựa trên việc người dùng kết nối từ văn phòng hay bên ngoài văn phòng.

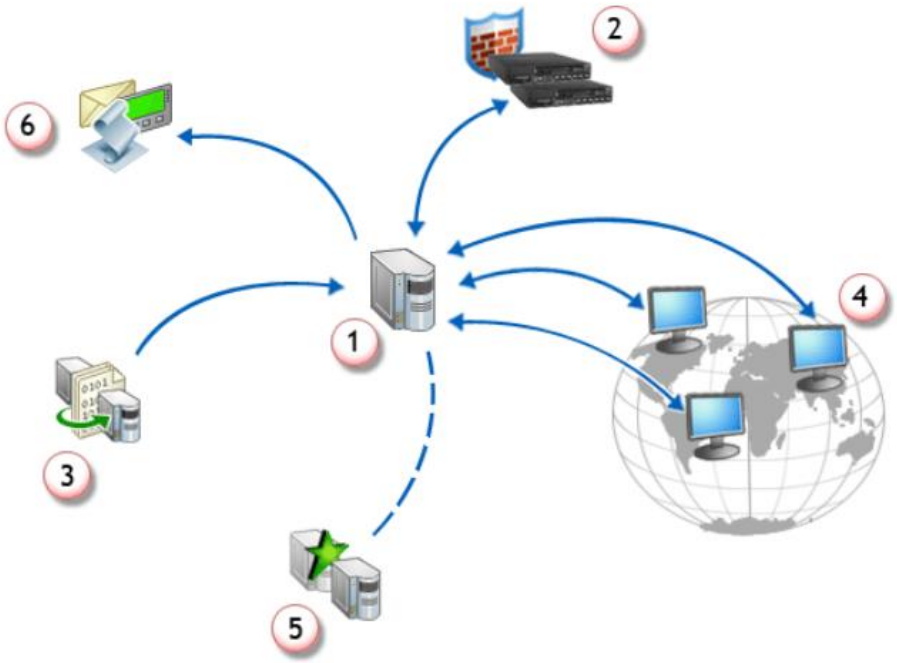
- Xác định loại máy chủ: MNSP lập cấu hình các thiết bị để giải quyết các rủi ro do BYOD. Nó tích hợp với McAfee ePO và NTBA để xác định loại thiết bị và hệ

điều hành cho từng máy chủ trên mạng của người sử dụng. Nếu một máy chủ cụ thể được nhắm mục tiêu cho một cuộc tấn công, họ cũng có thể đánh giá xem cuộc tấn công đó có liên quan hay không dựa trên loại thiết bị và hệ điều hành.

- Bảo vệ máy ảo: Các phiên bản ảo của Cảm biến cho phép người sử dụng giám sát lưu lượng ngang hàng giữa các máy ảo ngay cả trong cùng một máy chủ ảo. Cảm biến nền tảng bảo mật mạng ảo được gọi là Cảm biến IPS ảo hoặc Cảm biến ảo. Có thể triển khai Cảm biến IPS ảo như một thiết bị ảo trong nền tảng ảo hóa như máy chủ VMware ESXi. Sau đó, có thể cấu hình Cảm biến IPS ảo để bảo vệ mạng ảo bên trong nền tảng ảo hóa hoặc thậm chí bên ngoài. Dựa trên thiết kế mạng và các yêu cầu bảo mật, có thể định cấu hình Cảm biến IPS ảo để được nội tuyến giữa các máy ảo hoặc định cấu hình nó ở chế độ IDS. Cũng có thể sử dụng Cảm biến IPS ảo để kiểm tra lưu lượng giữa các máy chủ vật lý.

- Phân tích lưu lượng mạng của người sử dụng: Cảm biến IPS tích hợp với thiết bị NTBA để chủ động cung cấp khả năng hiển thị về bất kỳ hành vi bất thường nào trên mạng của bạn. Họ giám sát một cách thụ động mạng của bạn để giúp xác định các mối đe dọa từ APT và thậm chí khắc phục sự cố mạng. NTBA thu thập một lượng lớn dữ liệu, được chuyển đổi thành thông tin có ý nghĩa và phù hợp, và được trình bày ở định dạng đồ họa dễ hiểu.

- Tích hợp với các sản phẩm McAfee khác: Một 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.



Hình 2.6 : Minh họa sơ đồ McAfee Network Security Platform.

- Tùy chọn triển khai linh hoạt MNSP cung cấp các thiết bị có dung lượng thông lượng khác nhau để đáp ứng các phân đoạn mạng tốc độ cao hơn hiện nay. Chúng được thiết kế để bảo vệ toàn diện mà không ảnh hưởng đến hiệu suất. Thông lượng của các thiết bị này nằm trong khoảng từ 100 Mbps cho phép bảo vệ trong phạm vi từ 100 Mbps đến 40 Gbps.

- VIPS - Áp dụng các chính sách ở cấp giao diện và giao diện phụ: Tính năng VIPS cho phép bạn định cấu hình nhiều chính sách cho nhiều môi trường và hướng lưu lượng duy nhất, tất cả đều được giám sát bằng một Cảm biến duy nhất. Mục tiêu của ảo hóa là quét chi tiết. Ảo hóa cho phép bạn áp dụng nhiều chính sách cho lưu lượng truy cập qua một giao diện duy nhất. Bằng cách này, một chính sách quét duy nhất có thể được áp dụng cho một máy chủ hoặc một nhóm máy chủ, khi lưu lượng truy cập của chúng sẽ không đi qua một cổng Cảm biến duy nhất.

- Tính sẵn sàng cao: Cảm biến hỗ trợ triển khai tính sẵn sàng cao, sử dụng chuyển đổi dự phòng Cảm biến trạng thái giữa hai Cảm biến ở chế độ chờ nóng. Các cảm biến được kết nối với nhau, sao chép lưu lượng giữa chúng và duy trì đồng bộ hóa.

Nếu một Cảm biến bị lỗi, Cảm biến dự phòng sẽ tự động tiếp quản và tiếp tục theo dõi lưu lượng mà không bị mất trạng thái phiên hoặc suy giảm cấp độ bảo vệ.

- Quản lý IPS có thể mở rộng: Một kiến trúc dựa trên web có thể mở rộng cho phép khách hàng quản lý hiệu quả việc triển khai IPS của họ trong khi giảm chi phí hoạt động. Cơ chế cập nhật phần mềm và chữ ký theo thời gian thực của MNSP có thể định cấu hình tự động hóa quá trình duy trì hệ thống hoàn chỉnh mà không cần hoặc không có sự can thiệp của con người, do đó giảm chi phí vận hành liên tục.

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 theo bảng dưới đây:

Tiêu chí	**Snort**	**Suricata**	**Ossec**	**IBM Qradar**	**SSEM**	**MNSP**
Luồng xử lý	Đơn luồng	Đa luồng	Đa luồng	Đa luồng	Đa luồng	Đa luồng

Sử dụng tài nguyên hệ thống	Trung bình	Nhiều	Nhiều	Nhiều	Nhiều	Nhiều
Tỷ lệ bỏ qua gói tin khi lưu lượng ít	Cao	Thấp	Thấp	Thấp	Thấp	Thấp
Kỹ thuật phát hiện xâm nhập	Signature-based IDS	Signature-based IDS	Signature-based IDS, Anomaly-based	Signature-based IDS	Signature-based IDS	Signature-based IDS
Tập luật	Sử dụng các luật từ VRT, Emerging Threat, cũng như là các tập luật được viết bởi cộng đồng	Sử dụng các luật từ VRT, Emerging Threat. Ngoài ra còn hỗ trợ các luật được viết bằng Lua script.	OSSEC làm việc dựa trên các luật được định nghĩa sẵn trong các file. Các file được đặt trong thư mục /var/ossec/rules/.	Công cụ quy tắc tùy chỉnh (CRE)	Công cụ quy tắc tùy chỉnh (CRE)	Công cụ quy tắc tùy chỉnh (CRE)
Kết quả đầu ra	Có thể ghi kết quả đầu ra	Cho phép ghi kết quả	Phân tích các log nhận được từ các agent hay agentless	Chuyển tiếp dữ liệu	Báo cáo có thể được tạo với các	Kết quả đầu ra là các thông

	dưới dạng Syslog, tcpdump, csv hoặc unified2.	đầu ra dưới dạng Eve json và syslog. Ngoài ra còn hỗ trợ dùng Lua script để lấy kết quả đầu ra	(gọi chung là client) và xuất ra các cảnh báo. Các cảnh báo này có thể xuất ra cho các các công cụ xử lý log như Logstash, Elastic Search để hiển thị cho người quản trị bằng Kibana, lưu trữ trong cơ sở dữ liệu	tới các mục tiêu ngoại vi, hệ thống Syslog bên ngoài, hệ thống JSON và các SIEM khác.	cấp dữ liệu và đồ họa khác nhau, bao gồm báo cáo chính, báo cáo chi tiết và báo cáo cao nhất. Cũng có thể tạo lịch trình tạo và gửi báo cáo theo yêu cầu. Dễ dàng xuất báo cáo sang nhiều định dạng khác nhau như TXT, PDF, CSV, DOC, XLS, HTML.	báo cảnh báo dạng email, tin nhắn, tập lệnh
Hệ điều hành hỗ trợ	Linux, FreeBSD, OpenBSD,	Linux, FreeBSD, MacOS,	Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris và	Linux, Windows	Window, VMware	Windows, Linux, macOS.

	MacOS, Windows	Windows	Microsoft Windows.			

Bảng 1: So sánh các hệ thống phát hiện xâm nhập

2.4. Kết luận chương 2

Chương II đã trình bày về kiến trúc, hoạt động cũng như tính năng của các hệ thống phát hiện xâm nhập mạng Snort, Suricata, Ossec. Bên cạnh đó chương này còn trình bày về các hệ thống phát hiện xâm nhập tích hợp IBM Qradar, SolaWinds Secủity Manager, McAfree cho phép tìm kiếm, phát hiện xâm nhập cả hệ thống mạng và máy chủ, đồng thời hiển thị các logs thu thập được cho người dùng phân tích. Từ đó đưa ra bảng so sánh các hệ thống này.

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

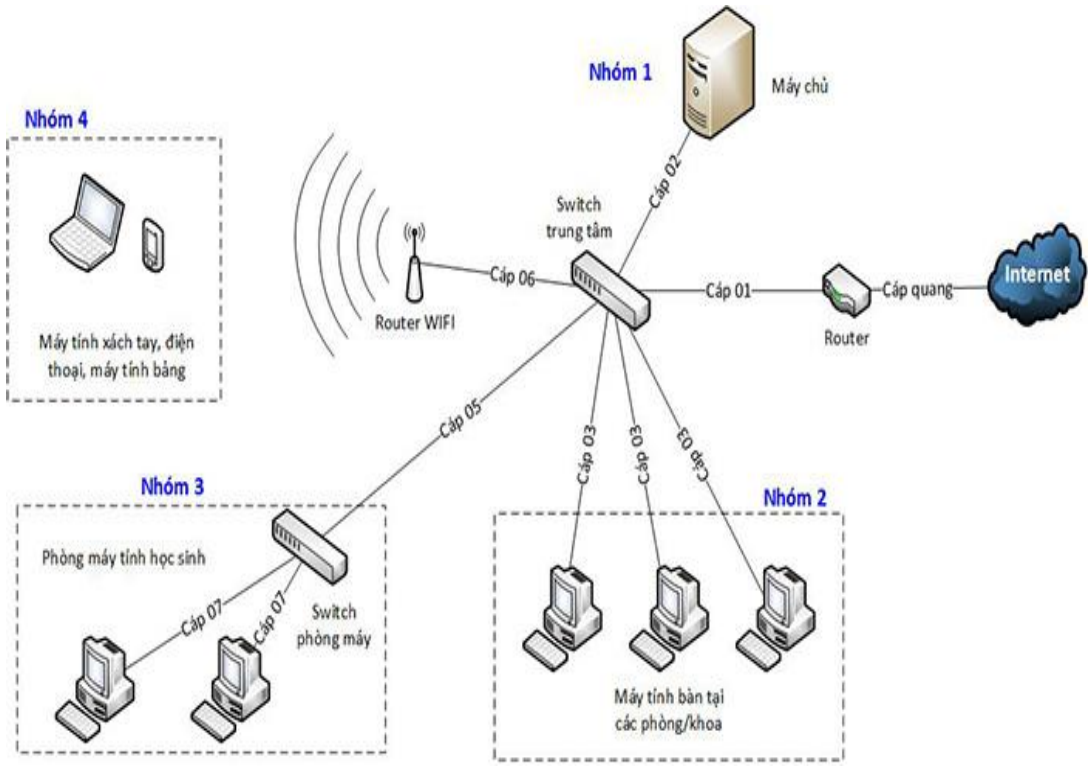
3.1.1 Khảo sát hệ thống mạng Trường cao đẳng sư phạm Hà Tây

Hình 3.1: Phối cảnh tổng thể trường 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.

Qua khảo sát hệ thống mạng, máy tính tại trường Cao đẳng sư phạm Hà Tây được xây dựng dựa trên kiến trúc module hóa (chia làm nhiều vùng). Gồm có các phòng ban tại trường: 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)

3.1.1.1. Sơ đồ mạng



Hình 3.2:Mô hình mạng máy tính trường Sư phạm Hà Tây

Cụ thể hệ thống mạng được chia làm các vùng sau:

- Nhóm 1:Hệ thống máy chủ
- Nhóm 2:Máy tính tại các phòng ban, khoa
- Nhóm 3:Hệ thống máy tính phòng thực hành
- Nhóm 4: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, 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 trường

- 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 dùng 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

3.1.2 Giải pháp và mô hình triển khai

3.1.2.1 Giải pháp

Sử dụng tường lửa Suricata để phát hiện xâm nhập và ngăn chặn những lưu lượng, sự kiện bất ngờ xảy ra trong các máy tính của các phòng ban để sớm có thể có những biện pháp xử lí kịp thời tránh mất an toàn thông tin.

- Hệ thống mạng trong trường được chia làm 2 khu vực
  - Khu vực mạng ngoài: có kết nối Internet
  - Khu vực mạng trong: không có kết nối Internet
- Chức năng của hệ thống
  - Truy cập Internet an toàn: Cho phép người dùng đang làm việc ở mạng trong, không có kết nối Internet, truy cập Internet và bảo vệ an ninh dữ liệu, chống thất thoát dữ liệu, thông tin và ngăn chặn phơi nhiễm mã độc.
- Bảng các thành phần của hệ thống

Thành phần	**Tính chất**	**Ghi chú**
Phòng thực hành	Nơi thực hành của các bạn sinh viên	192.168.10.X
Phòng hành chính	Nơi quản lí hồ sơ, giấy tờ, lưu trữ dữ liệu của sinh viên	192.168.20.X
Phòng đào tạo	Nơi tham mưu và giúp hiệu trưởng định hướng, phát triển công tác đào tạo của trường. Quản lí thông tin đào tạo của trường	192.168.30.X

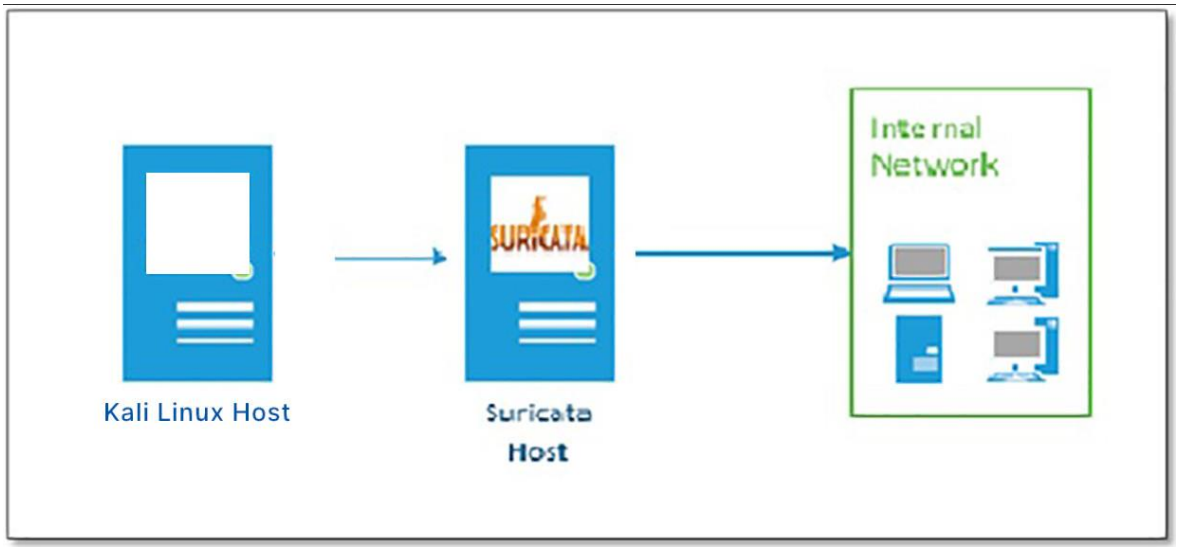
Thư viện	Nơi sinh viên có thể tìm hiểu, tra cứu các tài liệu liên quan đến việc học tập	192.168.40.X
Văn phòng	Là nơi của các giáo viên làm việc , trao đổi và họp trong quá trình công tác	192.168.50.X
Khu vực DMZ	Là nơi lưu trữ tài liệu, các phầm mềm hỗ trợ học tập cho sinh viên	10.1.1.X

Bảng 2: Các thành phần của hệ thống mạng

3.1.2.2 Mô hình triển khai

Hệ thống thử nghiệm được triển khai cài đặt gồm 2 máy như sau:

- Máy Kali Linux sử dụng các công cụ để thực hiện các kịch bản tấn công mạng đến máy mục tiêu là máy Ubuntu chạy Suricata.
- Máy Ubuntu cài đặt và cấu hình hệ thống phát hiện xâm nhập Suricata để đưa ra cảnh báo.



Hình 3.3: Mô hình triển khai suricata

3.2. Cài đặt và cấu hình hệ thống phát hiện xâm nhập Suricata

3.2.1. Yêu cầu phần cứng và phần mềm

Hệ thống thử nghiệm được triển khai trên máy ảo chạy hệ điều hành Ubuntu Linux với các yêu cầu phần cứng và phần mềm sau:

- Hệ thống chạy CPU Intel Core i5, 4GB RAM, 100GB HDD
- Ubuntu phiên bản 16.04
- Bộ phần mềm phát hiện xâm nhập Suricata phiên bản 6.0.5.

- Ứng dụng web chứa lỗi cho thử nghiệm (DVWA).
- Kali Linux phiên bản 2021 (sử dụng làm máy tấn công).

3.2.2. Cài đặt

Hệ thống được cài đặt theo các bước sau:

Bước 1: Cài đặt Suricata

- Cập nhật hệ thống với kho chứa phần mềm Suricata

  $ sudo add-apt-repository ppa:oisf/suricata-stable
- Cài đặt phần mềm Suricata

  sudo apt-get install suricata
- Thiết lập cho phép chạy tự động và khởi chạy Suricata: sudo systemctl enable suricata.service

Bước 2: Cấu hình lần đầu cho Suricata

- Chỉnh sửa file cấu hình Suricata

  $ sudo pico /etc/suricata/suricata.yaml

Chỉnh sửa interface mà Suricata giám sát là ‘eth0’ hoặc giao diện mạng trên máy cài đặt:

```
# Linux high speed capture support
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
. . .
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
```

EXTERNAL_NET: "!$HOME_NET"

Bước 3: Bổ sung các luật phát hiện vào file /etc/suricata/rules/users.rules

- Chỉnh sửa file cấu hình Suricata /etc/suricata/suricata.yaml cho phép sử dụng luật từ file users.rules

```
##
## Configure Suricata to load Suricata-Update managed rules.
##
default-rule-path: /etc/suricata/rules
rule-files:
  - users.rules
```

- Tạo mới các luật trong file users.rules với nội dung như sau:

```
# Luat phat hien tan cong ra quet cong
alert tcp any any -> $HOME_NET any (msg:"Phat hien tan cong ra quet cong dich vu"; fragbits:D; flags:S; threshold: type both, track by_src, count 100, seconds 5; sid:10000001;)
# Luat phat hien tan cong SYN Flood
alert tcp any any -> $HOME_NET any (msg:"Phat hien tan cong TCP SYN Flood"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:10000002;)
# Luat phat hien tan cong SQLi - OR
alert tcp any any -> any 80 (msg:"Phat hien tan cong SQLi - OR"; content:"or"; nocase; sid:10000009;)
# Luat phat hien tan cong SQLi - UNION
alert tcp any any -> any 80 (msg:"Phat hien tan cong SQLi - UNION"; content:"union"; nocase; sid:10000010;)
# Phat hien tan cong duyet duong dan
alert tcp any any -> any 80 (msg:"Phat hien tan cong duyet duong dan"; content:"../"; nocase; sid:10000012;)
# Phat hien tan con Brute force SSH
```

alert tcp any any -> $HOME_NET 22 (msg:"Phat hien tan cong SSH brute force"; flow:to_server,established; content:"SSH-"; depth:4; detection_filter:track by_src, count 3, seconds 30; metadata:service ssh; classtype:misc-activity;sid:10000007;)

Phat hien goi tin ping

alert icmp any any -> $HOME_NET any (msg:"Phat hien goi tin Ping"; sid:10000008; classtype:icmp-event;)

Bước 4: Kiểm tra cấu hình Suricata

$ sudo suricata -T -c /etc/suricata/suricata.yaml -v

Bước 5: Khởi động và kiểm tra trạng thái hoạt động của Suricata

$ sudo systemctl start suricata.service

$ sudo systemctl status suricata.service

Bước 6: Xem kết quả chạy thử trong Suricata log

$ sudo tail -f /var/log/suricata/suricata.log (log hoạt động)

$ sudo tail -f /var/log/suricata/fast.log (log chứa các cảnh báo)

3.3. Thử nghiệm và đánh giá

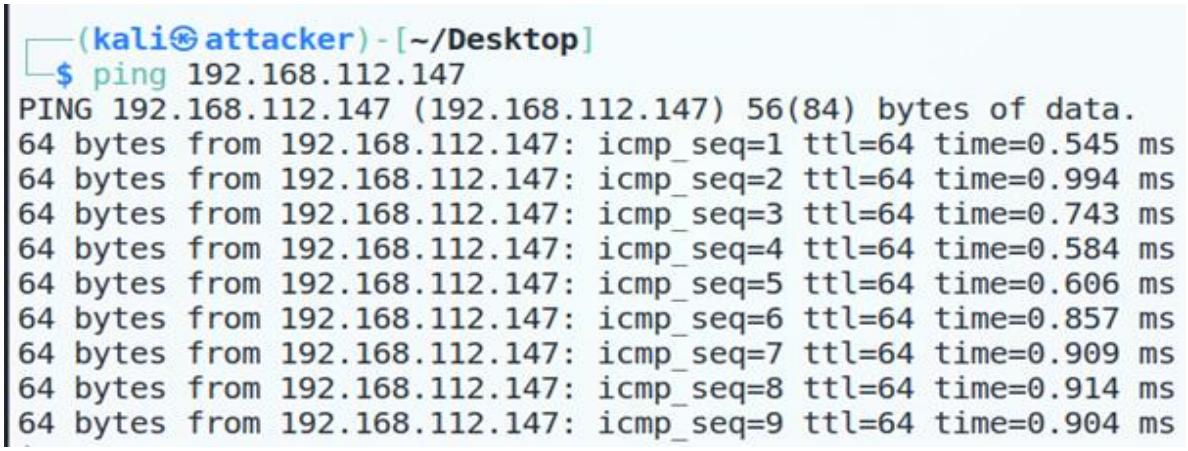
3.3.1. Các thử nghiệm phát hiện và kết quả

3.3.1.1. Phát hiện các gói tin Ping

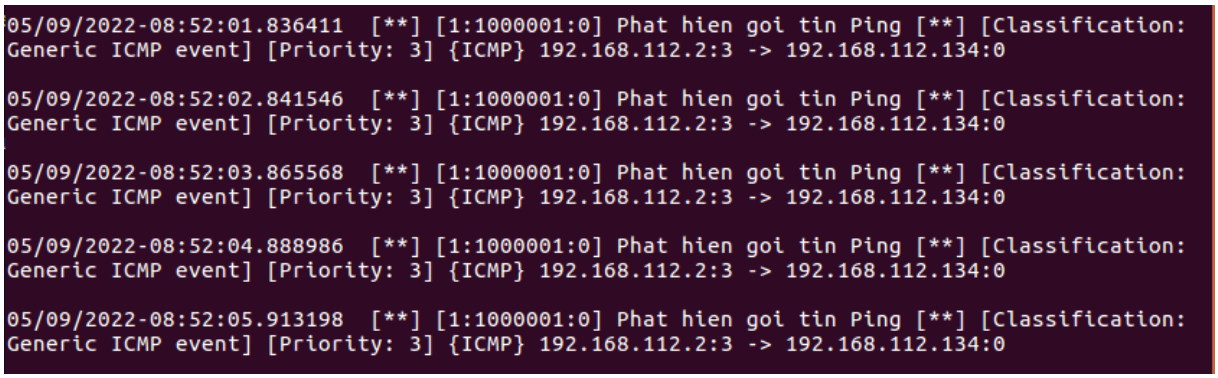
- Kịch bản: Trên máy tấn công (Kali Linux) sử dụng lệnh ping để ping máy chạy Suricata. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.
- Luật phát hiện sử dụng:

alert icmp any any -> $HOME_NET any (msg:"Phat hien goi tin Ping"; sid:10000008; classtype:icmp-event;)

- Kết quả cho như trên các hình 3.4 và 3.5



Hình 3.4: Ping từ máy tấn công đến máy Suricata



Hình 3.5: Suricata cảnh báo phát hiện gói tin Ping

3.3.1.2. Phát hiện tấn công rà quét cổng dịch vụ

- Kịch bản: Trên máy tấn công sử dụng lệnh nmap để quét các cổng dịch vụ chạy trên máy chạy Suricata. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.
- Luật phát hiện sử dụng:

alert tcp any any -> $HOME_NET any (msg:"Phat hien tan cong ra quet cong dich vu"; fragbits:D; flags:S; threshold: type both, track by_src, count 100, seconds 5; sid:10000001;)

- Kết quả cho như trên các hình 3.6 và 3.7.

```
┌──(kali㉿attacker)-[~/Desktop]
└─$ nmap -sV 192.168.112.147
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-09 14:17 +07
Nmap scan report for 192.168.112.147
Host is up (0.0031s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

Hình 3.6 : Sử dụng nmap để quét cổng dịch vụ trên máy Suricata

```
05/09/2022-14:16:13.999037  [**] [1:10000001:0] Phat hien tan cong ra quet cong dich vu [**]
 [Classification: (null)] [Priority: 3] {TCP} 192.168.112.134:41618 -> 192.168.112.147:1112

05/09/2022-14:16:28.658790  [**] [1:10000001:0] Phat hien tan cong ra quet cong dich vu [**]
 [Classification: (null)] [Priority: 3] {TCP} 192.168.112.134:58292 -> 192.168.112.147:1141

05/09/2022-14:17:38.743893  [**] [1:10000001:0] Phat hien tan cong ra quet cong dich vu [**]
 [Classification: (null)] [Priority: 3] {TCP} 192.168.112.134:53524 -> 192.168.112.147:8701
```

Hình 3.7: Suricata cảnh báo phát hiện tấn công rà quét cổng dịch vụ

3.3.1.3. Phát hiện tấn công SSH brute force

- Kịch bản: Trên máy tấn công sử dụng công cụ Hydra để tấn công brute force tìm mật khẩu của dịch vụ SSH trên máy chạy Suricata. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.
- Luật phát hiện sử dụng:

alert tcp any any -> $HOME_NET 22 (msg:"Phat hien tan cong SSH brute force"; flow:to_server, established; content:"SSH-"; depth:4; detection_filter: track by_src, count 3, seconds 30; metadata:service ssh; classtype:misc-activity; sid:10000007;)

- Kết quả cho như trên các hình 3.8 và 3.9.

```
┌──(kali㉿attacker)-[~/Desktop]
└─$ hydra -l ubuntu -P /tmp/pass-list.txt 192.168.112.147 ssh                255 ×
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
 or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-09 09:11:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
d to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 54 login tries (l:1/p:0), ~54 trie
s per task
[DATA] attacking ssh://192.168.112.147:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-09 09:11:25
```

Hình 3.8: Sử dụng Hydra để tấn công SSH brute force trên máy Suricata

```
05/09/2022-09:11:17.320458  [**] [1:10000007:0] Phat hien tan cong SSH brute force [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 192.168.112.134:52000 -> 192.168.112.147:22

05/09/2022-09:11:17.321185  [**] [1:10000007:0] Phat hien tan cong SSH brute force [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 192.168.112.134:52004 -> 192.168.112.147:22

05/09/2022-09:11:17.321968  [**] [1:10000007:0] Phat hien tan cong SSH brute force [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 192.168.112.134:52014 -> 192.168.112.147:22

05/09/2022-09:11:17.322344  [**] [1:10000007:0] Phat hien tan cong SSH brute force [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 192.168.112.134:52010 -> 192.168.112.147:22

05/09/2022-09:11:17.324087  [**] [1:10000007:0] Phat hien tan cong SSH brute force [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 192.168.112.134:52018 -> 192.168.112.147:22

05/09/2022-09:11:17.324381  [**] [1:10000007:0] Phat hien tan cong SSH brute force [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 192.168.112.134:52020 -> 192.168.112.147:22
```

Hình 3.9: Suricata cảnh báo phát hiện tấn công SSH brute force

3.3.1.4. Phát hiện tấn công DoS TCP SYN Flood

- Kịch bản: Trên máy tấn công sử dụng công cụ hping3 để tấn công TCP SYN Flood máy chạy Suricata. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.
- Luật phát hiện sử dụng:

alert tcp any any -> $HOME_NET any (msg:"Phat hien tan cong TCP SYN Flood"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:10000002;)

- Kết quả cho như trên các hình 3.10 và 3.11.

```
┌──(kali㉿attacker)-[~/Desktop]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.112.147
[sudo] password for kali:
HPING 192.168.112.147 (eth0 192.168.112.147): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Hình 3.10: Sử dụng hping3 để tấn công TCP SYN Flood máy Suricata

```
05/09/2022-08:32:16.359158  [**] [1:10000002:0] Phat hien tan cong TCP SYN Flood [**] [Class
ification: Misc activity] [Priority: 3] {TCP} 96.229.140.42:13628 -> 192.168.112.147:80

05/09/2022-08:32:21.401257  [**] [1:10000002:0] Phat hien tan cong TCP SYN Flood [**] [Class
ification: Misc activity] [Priority: 3] {TCP} 156.185.217.40:31402 -> 192.168.112.147:80

05/09/2022-08:32:26.326769  [**] [1:10000002:0] Phat hien tan cong TCP SYN Flood [**] [Class
ification: Misc activity] [Priority: 3] {TCP} 246.218.115.5:52492 -> 192.168.112.147:80

05/09/2022-08:32:31.396366  [**] [1:10000002:0] Phat hien tan cong TCP SYN Flood [**] [Class
ification: Misc activity] [Priority: 3] {TCP} 251.226.17.37:56807 -> 192.168.112.147:80

05/09/2022-08:32:36.351298  [**] [1:10000002:0] Phat hien tan cong TCP SYN Flood [**] [Class
ification: Misc activity] [Priority: 3] {TCP} 26.5.14.219:942 -> 192.168.112.147:80
```

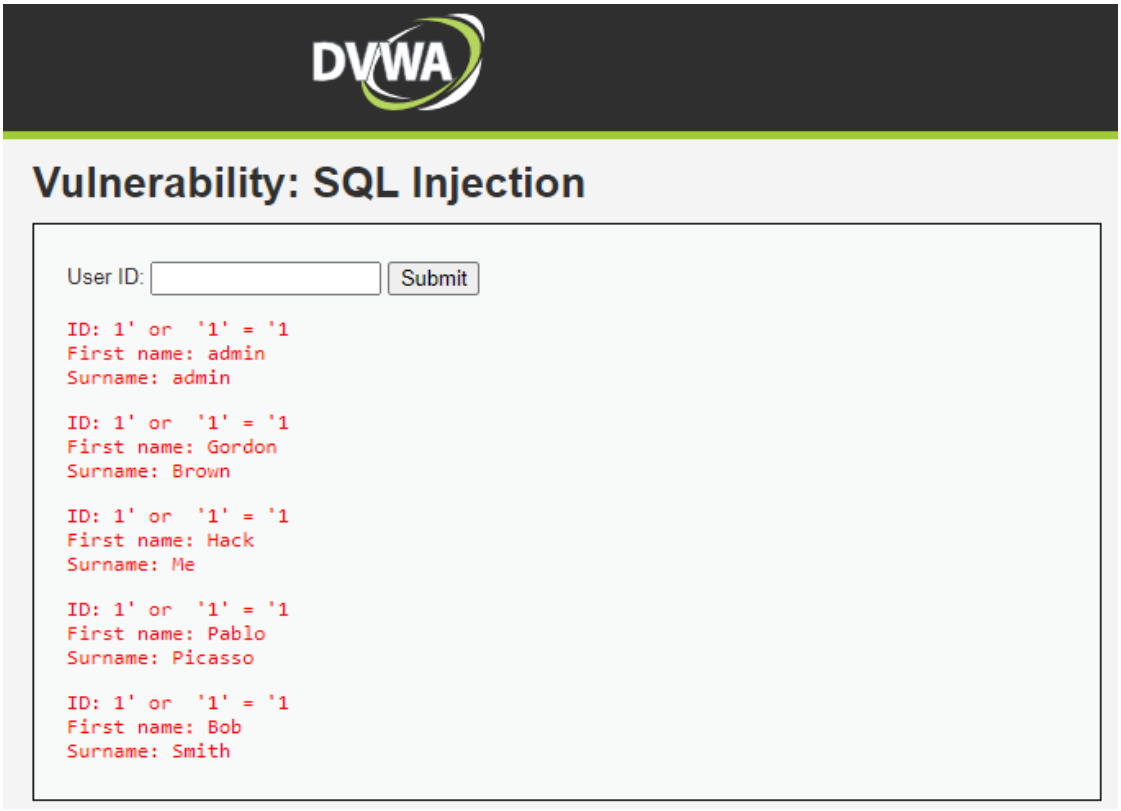
Hình 3.11: Suricata cảnh báo phát hiện tấn công TCP SYN Flood

3.3.1.5. Phát hiện tấn công SQLi - OR

- Kịch bản: Trên máy tấn công sử dụng trình duyệt để truy cập ứng dụng web DVWA chạy trên máy chạy Suricata. Nhập chuỗi " 1' or '1' = '1 " vào ô User ID. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.
- Luật phát hiện sử dụng:

alert tcp any any -> any 80 (msg:"Phat hien tan cong SQLi - OR"; content:"or"; nocase; sid:10000009;)

- Kết quả cho như trên các hình 3.12 và 3.13.



Hình 3.12: Tấn công SQLi - OR vào ứng dụng web DVWA trên máy Suricata

```
05/09/2022-13:38:15.998963  [**] [1:10000009:0] Phat hien tan cong SQLi - OR [**] [Classific
ation: (null)] [Priority: 3] {TCP} 192.168.112.1:57362 -> 192.168.112.147:80

05/09/2022-13:39:03.895503  [**] [1:10000009:0] Phat hien tan cong SQLi - OR [**] [Classific
ation: (null)] [Priority: 3] {TCP} 192.168.112.1:57363 -> 192.168.112.147:80

05/09/2022-13:43:04.670138  [**] [1:10000009:0] Phat hien tan cong SQLi - OR [**] [Classific
ation: (null)] [Priority: 3] {TCP} 192.168.112.1:57385 -> 192.168.112.147:80

05/09/2022-13:43:50.948078  [**] [1:10000009:0] Phat hien tan cong SQLi - OR [**] [Classific
ation: (null)] [Priority: 3] {TCP} 192.168.112.1:57389 -> 192.168.112.147:80
```

Hình 3.13 :Suricata cảnh báo phát hiện tấn công SQLi - OR

3.3.1.6. Phát hiện tấn công SQLi - UNION

- Kịch bản: Trên máy tấn công sử dụng trình duyệt để truy cập ứng dụng web DVWA chạy trên máy chạy Suricata. Nhập chuỗi " -1 union select user, password from users -- " vào ô User ID. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.
- Luật phát hiện sử dụng:

alert tcp any any -> any 80 (msg:"Phat hien tan cong SQLi - UNION"; content:"union"; nocase; sid:10000010;)

- Kết quả cho như trên các hình 3.14 và 3.15.

Hình 3.14: Tấn công SQLi - UNION vào ứng dụng web DVWA trên máy Suricata

```
05/09/2022-09:42:05.360846  [**] [1:10000010:0] Phat hien tan cong SQLi - UNION [**] [Classi
fication: (null)] [Priority: 3] {TCP} 192.168.112.1:56314 -> 192.168.112.147:80

05/09/2022-09:42:23.792985  [**] [1:10000010:0] Phat hien tan cong SQLi - UNION [**] [Classi
fication: (null)] [Priority: 3] {TCP} 192.168.112.1:56315 -> 192.168.112.147:80

05/09/2022-13:23:38.902800  [**] [1:10000010:0] Phat hien tan cong SQLi - UNION [**] [Classi
fication: (null)] [Priority: 3] {TCP} 192.168.112.1:57259 -> 192.168.112.147:80

05/09/2022-13:23:57.171395  [**] [1:10000010:0] Phat hien tan cong SQLi - UNION [**] [Classi
fication: (null)] [Priority: 3] {TCP} 192.168.112.1:57265 -> 192.168.112.147:80
```

Hình 3.15: Suricata cảnh báo phát hiện tấn công SQLi - UNION

3.3.1.7. Phát hiện tấn công duyệt đường dẫn

- Kịch bản: Trên máy tấn công sử dụng trình duyệt để truy cập ứng dụng web DVWA chạy trên máy chạy Suricata. Truy cập URL

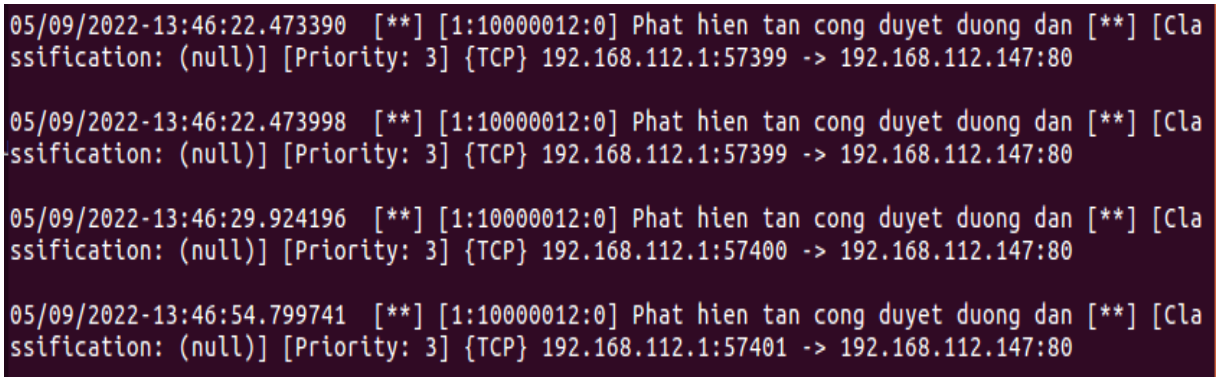
http://192.168.11.147/DVWA/vulnerabilities/fi/?page=../../../../../../../../etc/password để truy cập file chứa danh sách người dùng hệ thống. Trên máy Suricata xem log phát hiện trong file /var/log/suricata/fast.log.

- Luật phát hiện sử dụng:

alert tcp any any -> any 80 (msg:"Phat hien tan cong duyet duong dan"; content:"../"; nocase; sid:10000012;)

- Kết quả cho như trên các hình 3.16 và 3.17.

Hình 3.16: Tấn công duyệt đường dẫn vào ứng dụng DVWA trên máy Suricata



Hình 3.17: Suricata cảnh báo phát hiện tấn công duyệt đường dẫn

3.3.2. Nhận xét

Sau khi phát hiện các tình huống xâm nhập hệ thống, suricata sẽ tổng hợp logs và chuyển qua một bộ phân tích chung sau đó xuất ra các cảnh báo.

Hệ thống phát hiện xâm nhập sử dụng Suricata đã phát hiện chính xác 7 kịch bản tấn công hệ thống. Cụ thể:

- Phát hiện được các gói tin ping và rà quét cổng là các dạng tấn công thám thính.
- Phát hiện được tấn công DoS TCP SYN Flood.
- Phát hiện được tấn công dò tìm tài khoản - mật khẩu - brute force.
- Phát hiện được một số dạng tấn công web, như SQLi và duyệt đường dẫn.

3.4. Kết luận chương 3

Chương 3 đã mô tả việc triển khai thử nghiệm hệ thống phát hiện xâm nhập Suricata cho trường CĐSP Hà Tây, bao gồm giới thiệu hiện trạng hệ thống mạng và vấn đề bảo mật của hệ thống mạng của trường, mô hình triển khai thử nghiệm, vấn đề cài đặt, cấu hình Suricata và thử nghiệm phát hiện một số dạng tấn công sử dụng Suricata. Các kết quả ban đầu cho thấy, hệ thống phát hiện xâm nhập sử dụng Suricata đã phát hiện chính xác 7 kịch bản tấn công hệ thống.

KẾT LUẬN

Các kết quả đạt được:

Luận văn này tập trung nghiên cứu về thu thập, xử lý, phân tích log truy cập, phục vụ phát hiện các hành vi bất thường và nguy cơ mất an toàn thông tin trong hệ thống mạng của trường Cao Đẳng Sư Phạm Hà Tây. Các nội dung đã thực hiện trong luận văn bao gồm:

- Trình tổng quan về tấn công, xâm nhập mạng, các dạng tấn công xâm nhập thường gặp; đồng thời cũng đã khái quát về phát hiện xâm nhập cũng như các kỹ thuật phát hiện xâm nhập qua đó ta có cái nhìn rõ hơn về tấn công, xâm nhập.

- Mô tả một số nền tảng về công cụ xử lý và phân tích log truy nhập, từ đó rút ra so sánh, đánh giá để tìm ra mô hình triển khai phù hợp.

- Trình bày kiến trúc, hoạt động tính năng của các hệ thống xâm nhập mạng phổ biến hiện nay là Snort, Suricata. Từ đó, đưa ra so sánh về ưu, nhược điểm của các hệ thống này.

- Cài đặt hệ thống phát hiện tấn công, xâm nhập mạng với nền tảng mã nguồn mở như Suricata. Thử nghiệm các kịch bản tấn công cụ thể và đưa ra kết quả cảnh báo khi bị tấn công.

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.

- Xây dựng và bổ sung thêm các tập luật giám sát, phát hiện bất thường và các nguy cơ ATTT, đảm bảo khả năng phát hiện kịp thời các nguy cơ mất an ninh an toàn; đồng thời có thể tích hợp thêm hệ thống ngăn chặn và tấn công mạng, tích hợp tính năng cảnh báo qua email, telegram…

DANH MỤC TÀI LIỆU THAM KHẢO

[1] NortonLifeLock Inc., 10 cyber security facts and statistics for 2018, https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html, truy cập tháng 5.2022

[2] CSO, Top cybersecurity facts, figures and statistics for 2020, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html, truy cập tháng 5.2022

[3] Hoàng Xuân Dậu, Giáo trình cơ sở an toàn thông tin, Học viện công nghệ BCVT, Nhà xuất bản Thông tin và Truyền thông, 2020.

[4] https://resources.cystack.net/, truy nhập tháng 5.2022.

[5] Snort, https://www.snort.org, truy cập tháng 5.2022

[6] Suricata, https://suricata-ids.org/, truy cập tháng 5.2022

[7] OSSEC, https://www.ossec.net, truy cập tháng 5.2022

[8] IBM QRadar SIEM, https://www.ibm.com/vn-en/products/qradar-siem, truy cập tháng 5.2022

[9] SolarWinds Security Event Manager, https://www.solarwinds.com, truy cập tháng 5.2022

[10] McAfee Network Security Platform,https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html, truy cập tháng 5.2022

[11] https://www.fortinet.com/it/resources/cyberglossary/, truy nhập tháng 5.2022

[12] https://www.guru99.com/elk-stack-tutorial.html, truy nhập tháng 5.2022.