BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC

THÀNH PHỐ HỒ CHÍ MINH

ĐỒ ÁN MÔN HỌC

BẢO MẬT NGƯỜI DÙNG CUỐI

Nguyễn Công Khang - 21DH110770

Phạm Đức Thiên Phúc - 21DH112813

Nguyễn Minh Đức – 21DH113591

GVGD: Th.S Đỗ Phi Hưng

LỜI NÓI ĐẦU

Hiện nay khoa học kỹ thuật ngày càng phát triển, an toàn thông tin là yếu tố quan trọng được đặt lên hàng đầu trong thời điểm hiện nay. Điển hình trong năm 2023, Việt Nam đã chịu ảnh hưởng nặng nề bởi 59837 vụ tấn công dữ liệu.

Môn học Bảo mật người dùng này đã giúp chúng em nắm vững kiến thức và kỹ năng cơ bản trong việc cảnh bảo và ngăn chặn các tấn công nhắm vào người dùng nhằm bảo vệ an toàn thông tin cho người dùng.

Chúng em rất cảm ơn thầy Th.S Đỗ Phi Hưng đã giúp em hoàn thành báo cáo này.

MỤC LỤC

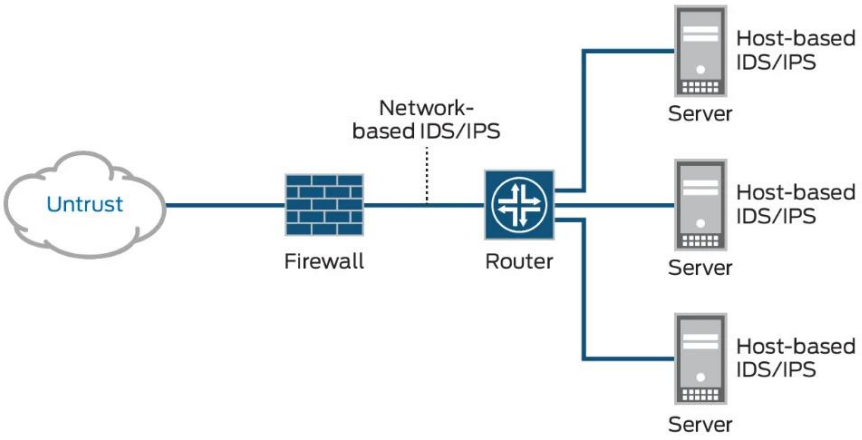
Danh mục hình ảnh

Chương 1: Cơ sở lý thuyết

I. IDS

1. Khái niệm

Hệ thống phát hiện xâm nhập – IDS là viết tắt của Intrusion Detection System. Đây là một phần mềm ứng dụng hoặc thiết bị 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.



Hình 1 Mô hình IDS

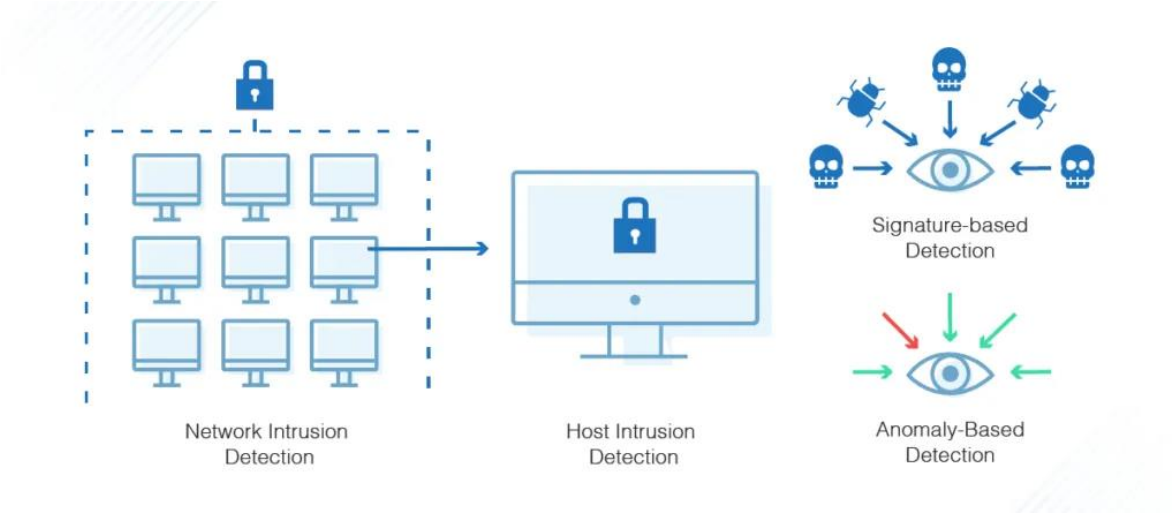
Hiện nay có hai loại hệ thống IDS chính:

- **NIDS (Network Intrusion Detection System)** – Hệ thống phát hiện xâm nhập mạng, hệ thống sẽ tập hợp các gói tin để phân tích sâu bên trong nhằm xác định các mối đe dọa tiềm tàng mà không làm thay đổi cấu trúc của gói tin.
- **HIDS (Host-based Intrusion Detection System)** – Hệ thống phát hiện xâm nhập dựa trên máy chủ, được cài đặt trực tiếp trên các máy tính cần theo dõi. HIDS giám sát lưu lượng đến và đi từ thiết bị để cảnh báo người dùng về những xâm nhập trái phép.

Các hệ thống IDS hiện đại được xây dựng để thu thập lưu lượng mạng từ mọi thiết bị thông qua cả NIDS và HIDS. Vì vậy có thể cải thiện đáng kể khả năng phát hiện xâm nhập trên hệ thống.

2. Phương thức hoạt động

Sau khi thu thập xong dữ liệu, IDS so khớp lưu lượng mạng với các mẫu lưu lượng có sẵn của những cuộc tấn công mạng khác (phương pháp này thường được gọi là tương quan mẫu – Pattern Correlation). Thông qua phương pháp này, hệ thống IDS có thể xác định xem những hoạt động bất thường có phải là dấu hiệu của sự tấn công hay không.



Hình 2 Phương thức hoạt động của IDS

Sau khi xác định xong hoạt động bất thường, hệ thống sẽ gửi thông báo đến các kỹ thuật viên hoặc quản trị viên được chỉ định trước. Khi đó quản trị viên có thể nhanh chóng thực hiện khắc phục sự cố, nhanh chóng ngăn chặn các tác nhân có hại để bảo vệ hệ thống.

Intrusion Detection System thường sử dụng hai phương pháp chính là phát hiện dựa trên chữ ký và phát hiện dựa trên sự bất thường.

- **Phát hiện dựa trên chữ ký (Signature-based intrusion detection):** Đây là phương pháp được thiết kế để tìm ra những nguy hiểm tiềm tàng bằng cách so sánh dung lượng mạng và nhật ký dữ liệu với những mẫu tấn công có sẵn trong hệ thống. Những mẫu này còn được gọi là chuỗi (sequence) và có thể bao gồm chuỗi byte, được gọi là chuỗi lệnh độc hại. Phát hiện dựa trên chữ ký cho phép các quản trị viên nhanh chóng phát hiện các cuộc tấn công vào mạng.
- **Phát hiện dựa trên sự bất thường (Anomaly-based intrusion detection)** được thiết kế để xác định các cuộc tấn công không xác định, chẳng hạn như phần mềm độc hại mới và thích ứng với chúng ngay lập tức bằng cách sử dụng máy học. Thông qua các kỹ thuật máy học cho phép Hệ thống phát hiện xâm nhập (IDS) tạo ra các đường cơ sở của mô hình tin cậy, sau đó so

sánh hành vi mới với các mô hình tin cậy đã được xác minh. Cảnh báo giả có thể xảy ra khi sử dụng IDS dựa trên sự bất thường, vì lưu lượng mạng hợp pháp chưa từng được biết đến trước đây cũng có thể bị xác định sai là hoạt động độc hại.

Hybrid Intrusion Detection System là một hệ thống lai giữa Network IDS và Host-based IDS. Nó kết hợp một hoặc nhiều các thành phần thích hợp của hai hệ thống lại với nhau. Các thông tin thu thập được trên máy trạm (Host agent data) kết hợp với thông tin thu thập được ở trên mạng để có được sự phân tích một cách chi tiết về hiện trạng hệ thống mạng.

3. Ưu, nhược điểm của IDS

Ưu điểm:

- IDS thích hợp sử dụng cho việc thu thập dữ liệu và bằng chứng của các cuộc tấn công mạng. Nhờ đó việc kiểm tra, điều tra và xử lý sự cố phát sinh dễ dàng, chính xác và kịp thời nhất.
- IDS giúp người dùng có cái toàn diện về hệ thống lưu lượng mạng. Bất cứ hoạt động khả nghi nào đều có thể được phát hiện nhanh chóng nhất.
- IDS giúp người dùng phòng ngừa, phản ứng kịp thời để có biện phát chống lại lại các hoạt động tấn công bất ngờ có thể diễn ra trên hệ thống mạng.
- Các số liệu, thông tin IDS ghi chép, lưu trữ có thể được sử dụng để nâng cao chất lượng hệ thống bảo mật. Chúng cũng là cơ sở để đánh giá rủi ro các cuộc tấn công mạng trong tương lai.

Nhược điểm:

- Người dùng cần điều chỉnh cấu hình IDS phù hợp nếu không sẽ xảy ra tình trạng báo động nhầm, báo động giả.
- Một số hệ thống IDS ngăn cản người dùng ở thiết bị khác truy cập vào hệ thống mạng.
- Khả năng phân tích lưu lượng traffic mã hóa khá thấp và chưa hiệu quả.
- Chi phí cài đặt hệ thống ISD khá cao và yêu cầu nhiều kỹ thuật phức tạp. Bạn cần cân nhắc nếu khả năng tài chính của doanh nghiệp hạn chế.

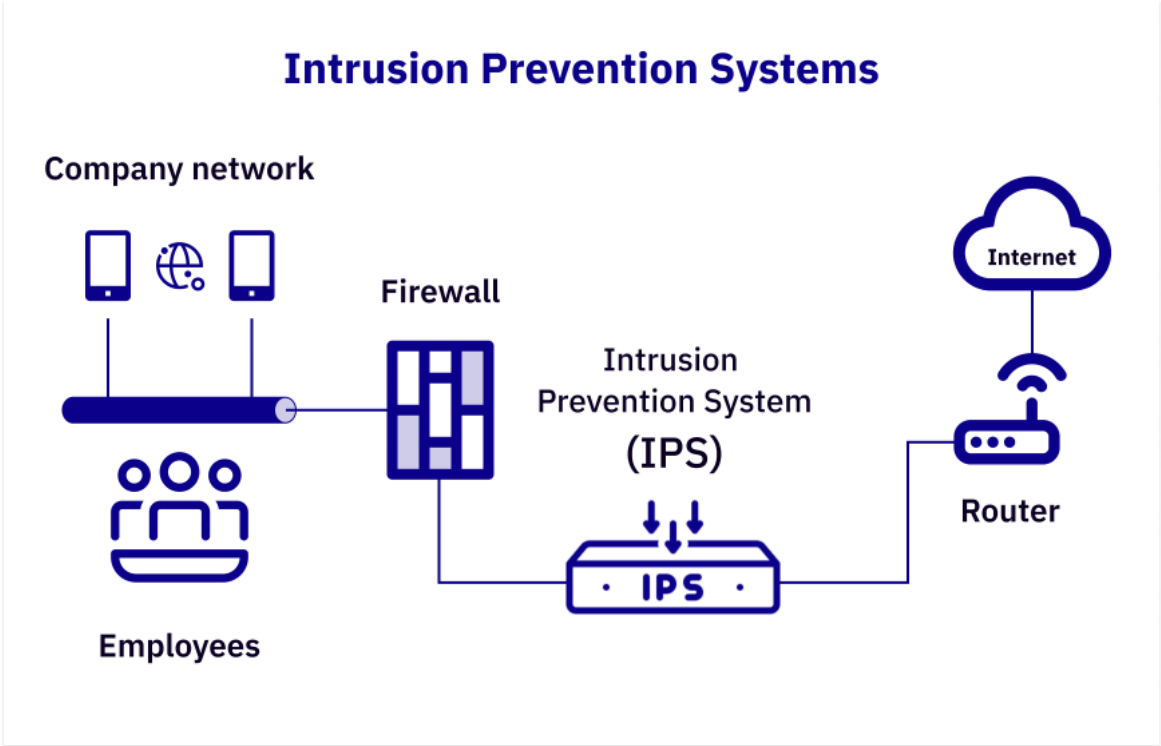
II. IPS

1. Khái niệm

IPS (viết tắt của Intrusion Prevention System) hiểu đơn giản là hệ thống được sử dụng để phát hiện và ngăn chặn các hoạt động xâm nhập. IPS thực hiện giám

sát hệ thống liên tục nhằm phát hiện các hoạt động bất thường, lưu lại các thông tin này, báo cáo cho quản trị hệ thống và thực hiện hoạt động ngăn chặn như đóng kết nối và đưa ra thiết lập tường lửa để ngăn các cuộc tấn công trong tương lai.

Các giải pháp IPS cũng có thể được dùng để phát hiện, ngăn chặn các vấn đề liên quan đến chính sách bảo mật của công ty, như ngăn chặn nhân viên và khách hàng trong mạng vi phạm các quy tắc bảo mật của công ty mà IPS được thiết lập.



Hình 3 Mô hình IPS

2. Phương thức hoạt động

IPS hoạt động bằng cách giám sát, quét tất cả lưu lượng mạng. IPS được thiết kế để có thể ngăn chặn nhiều mối đe dọa khác nhau, bao gồm:

- Khai thác lỗ hổng
- Mã độc
- Tấn công từ chối dịch vụ (DoS)
- Tấn công từ chối dịch vụ phân tán (DDoS)

IPS thực hiện kiểm tra tất cả gói tin truyền qua mạng theo thời gian thực. Nếu phát hiện thấy bất kỳ gói tin độc hại hoặc hoạt động đáng ngờ nào, IPS sẽ thực hiện một trong các hành động sau:

- Đóng kết nối và chặn địa chỉ IP nguồn vi phạm chính sách hoặc tài khoản người dùng truy cập không hợp pháp vào bất kỳ ứng dụng, máy chủ đích hoặc các tài nguyên mạng.
- Đưa ra cấu hình tường lửa để ngăn chặn các cuộc tấn công tương tự xảy ra trong tương lai.

IPS được cấu hình để nhằm bảo vệ hệ thống khỏi bị truy cập trái phép sử dụng một số cơ chế tiếp cận khác nhau:

- **Chữ ký:** cơ chế này dựa trên chữ ký đã được xác định của các mối đe dọa đã được phát hiện trước đó. Khi một cuộc tấn công được phát hiện khớp với một trong các chữ ký hoặc mẫu này, hệ thống sẽ thực hiện hành động cần thiết.
- **Sự bất thường:** hệ thống sẽ giám sát mọi hành vi bất thường trên hệ thống. Nếu phát hiện sự bất thường, hệ thống sẽ chặn quyền truy cập vào hệ thống mục tiêu ngay lập tức.
- **Chính sách:** cơ chế này yêu cầu quản trị hệ thống thiết lập cấu hình các chính sách bảo mật theo chính sách bảo mật của tổ chức đưa ra và cơ sở hạ tầng mạng trên thực tế. Khi một hoạt động xảy ra vi phạm chính sách bảo mật, cảnh báo sẽ được kích hoạt và gửi đến quản trị viên hệ thống.

3. Ưu, nhược điểm của IPS

Ưu điểm:

- **Ngăn chặn các cuộc tấn công trước khi gây hại:**

Một trong những ưu điểm quan trọng nhất của IPS là khả năng ngăn chặn các cuộc tấn công mạng trước khi chúng gây ra bất kỳ thiệt hại nào cho hệ thống. Điều này có nghĩa là IPS có khả năng phát hiện các biểu hiện của một cuộc tấn công mạng và can thiệp ngay lập tức để chặn đứng cuộc tấn công trước khi nó lan rộng và gây ra các vấn đề.

- **Tự động hóa:**

IPS thường tích hợp các cơ chế tự động hóa để tối ưu hóa việc phát hiện và phản ứng với các cuộc tấn công mạng. Sự tự động hóa này giúp giảm tải công

việc cho các quản trị viên mạng và đảm bảo rằng các biện pháp ngăn chặn được triển khai một cách nhanh chóng và hiệu quả.

- **Bảo vệ dựa trên chữ ký và hành vi:**

IPS có khả năng phân biệt giữa các cuộc tấn công dựa trên chữ ký và hành vi. Các cuộc tấn công dựa trên chữ ký thường sử dụng các mẫu tấn công đã biết, trong khi các cuộc tấn công dựa trên hành vi được xác định bằng cách theo dõi các hoạt động mạng bất thường.

Nhược điểm:

- **Lỗi phát hiện:**

Mặc dù IPS có khả năng phát hiện và ngăn chặn nhiều cuộc tấn công mạng, nó cũng có một số hạn chế. Một trong những vấn đề phổ biến là lỗi phát hiện, tức là IPS có thể báo cáo sai một hoạt động bình thường là một cuộc tấn công.

Cụ thể, nếu IPS không được cấu hình đúng hoặc không được cập nhật thường xuyên với các chữ ký mới, nó có thể tạo ra các cảnh báo giả. Điều này có thể dẫn đến việc thông báo về các cuộc tấn công không tồn tại, gây hoang mang và lãng phí thời gian và tài nguyên trong việc kiểm tra và xử lý các sự cố không đáng lo ngại.

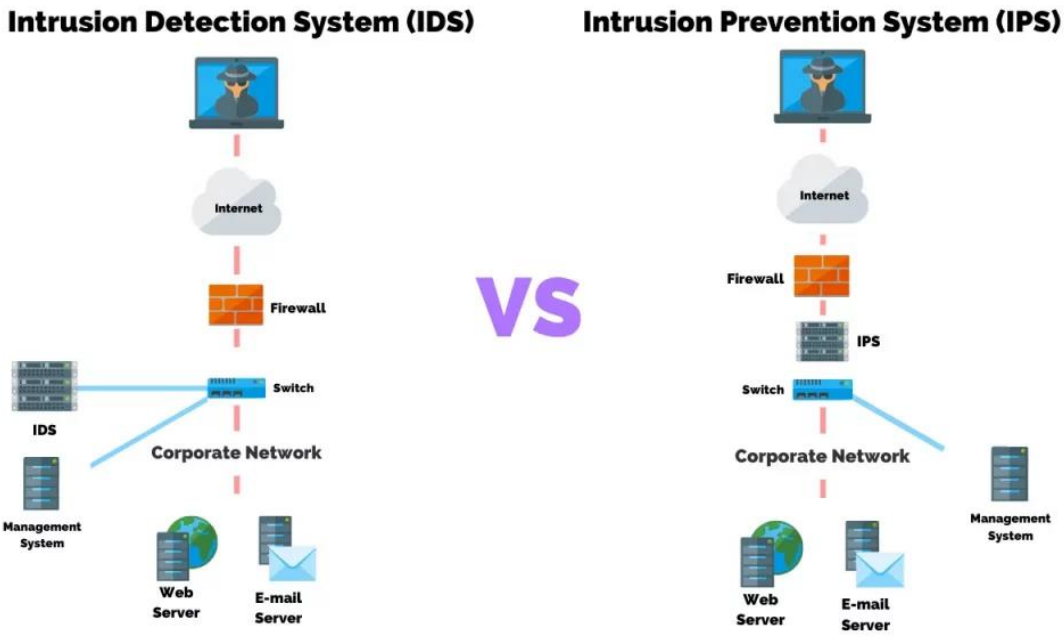
- **Chi phí:**

Việc triển khai và duy trì hệ thống IPS có thể tốn kém về tài chính và nguồn nhân lực. Cần đầu tư vào phần cứng và phần mềm IPS chất lượng cao, và cần có nhân viên chuyên nghiệp để cấu hình, quản lý và giám sát hệ thống này một cách hiệu quả.

III. Sự khác nhau giữa IDS và IPS

Trước tiên, IDS là một hệ thống phân tích lưu lượng mạng để tìm các thông tin khớp với những mẫu tấn công đã biết trước. Mặt khác, IPS có khả năng phân tích các packet và ngăn chặn việc gửi packet dựa trên những loại hình tấn công mà hệ thống phát hiện được. Từ đó có thể nhanh chóng ngăn chặn tấn công vào hệ thống.

Cả IDS lẫn IPS đều thuộc về cơ sở hạ tầng mạng, và đều so sánh các packet mạng với một CSDL cyberthreat có chứa những signature đã biết của tấn công mạng. Sau đó đánh dấu mọi packet khớp với các mẫu đã biết và cảnh báo cho admin hệ thống.



Hình 4 Khác nhau của IDS và IPS

Sự khác biệt chính giữa hai giải pháp là: IDS là một hệ thống giám sát, còn IPS là hệ thống kiểm soát.

IDS không thay đổi các packet mạng, còn IPS ngăn chặn việc gửi packet dựa trên nội dung của nó. Về nguyên lý hoạt động thì IPS tương tự như các tường lửa (tường lửa chặn lưu lượng bằng địa chỉ IP).

- **IDS:** Phân và giám sát lưu lượng mạng để tìm các dấu hiệu của tấn công mạng. Hệ thống này so sánh các hoạt động mạng hiện tại với CSDL có sẵn để xác định các hành vi đáng ngờ như: vi phạm chính sách, malware hay port scanner.
- **IPS:** Nằm trong cùng khu vực của firewall trên cơ sở hạ tầng (giữa môi trường bạn ngoài ra mạng ở trong). IPS chủ động chặn các lưu lượng dựa trên một cấu hình bảo mật cụ thể.

Hầu hết các nhà cung cấp dịch vụ IDS/IPS đều tích hợp những hệ thống IPS mới kèm theo firewall để thiết lập công nghệ UTM (Unified Threat Management) – có khả năng kết hợp chức năng của IDS và IPS thành một đơn vị duy nhất.

Nói chung, cả IDP và IPS đều đọc các packet mạng và so sánh nội dung với một CSDL có sẵn. Những điểm khác biệt chỉ nằm ở quá trình sau đó: IDS sẽ phát hiện và giám sát lưu lượng mà không tự thực hiện hành động cụ thể nào cả.

Còn IPS – một hệ thống kiểm soát – sẽ quyết định việc nhận hay bỏ packet mạng dựa trên những bộ quy tắc cho trước. Vì vậy, IDS cần có một người hay hệ thống khác giám sát kết quả và xác định các hành động cần thực hiện.

Tuy nhiên, cần lưu ý rằng IDS/IPS chỉ thực sự hiệu quả nếu có một bộ CSDL đủ tốt. Do đó hãy luôn cập nhật thêm dữ liệu và các bộ quy tắc mới cho CSDL của mình để bảo vệ hệ thống tốt nhất.

IV. Vì sao cần sử dụng IDS và IPS

Hiện nay, cyberattack đang ngày càng tăng mạnh cả về số lượng lẫn độ phức tạp. Việc triển khai các hệ thống IDS/IPS giúp giảm bớt thời gian, công sức và tài nguyên để bảo vệ hệ thống, đồng thời còn cung cấp dữ liệu để những quản trị viên có thể vạch ra những chiến lược cyber security hiệu quả.

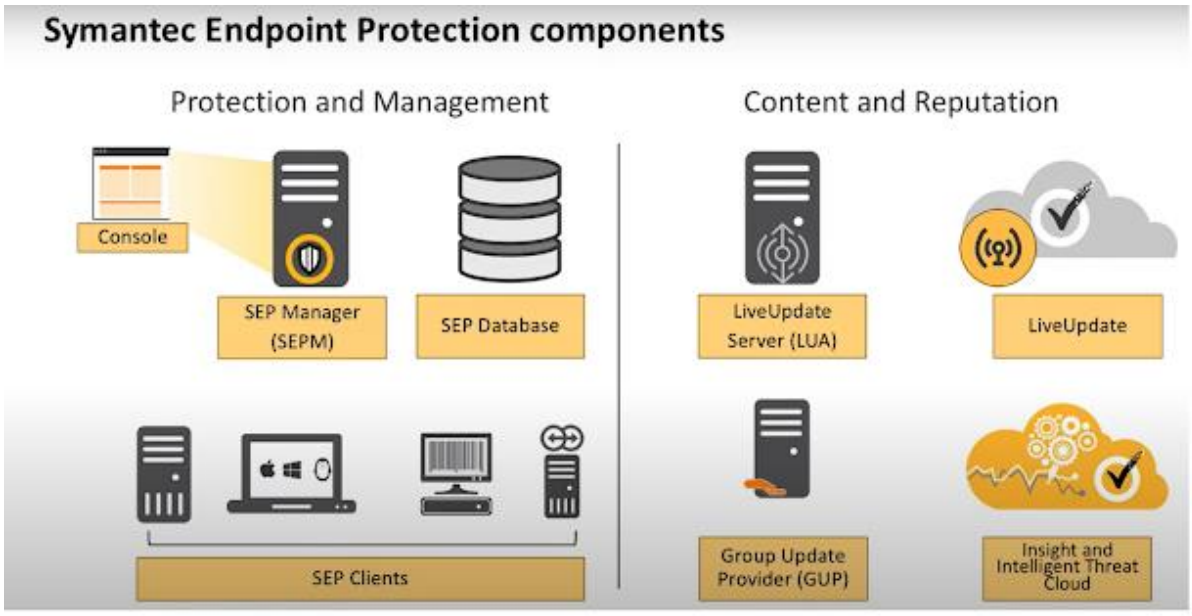
Cụ thể, ta có thể kể đến một số ưu điểm lớn nhất của IDS/IPS như sau:

- **Tự động hóa**: IDS/IPS đảm bảo hệ thống được bảo mật khỏi những mối nguy mà không cần quá nhiều tài nguyên của hệ thống.
- **Tuân thủ:** Việc triển khai IDS/IPS cho biết tổ chức của bạn đang tuân theo những quy tắc nghiêm ngặt về bảo mật của CIS.
- **Thực thi chính sách:** IDS/IPS có thể được cấu hình để thực thi những chính sách bảo mật ở cấp độ mạng.

V. System Endpoint

1. Khái niệm

Endpoint Protection là giải pháp bảo mật thiết bị đầu cuối khỏi các cuộc tấn công trên mạng, bảo vệ hệ thống máy tính khỏi các cuộc tấn công phức hợp hay các tấn công thế hệ mới, các dạng tấn công này được khai thác trên nhiều mức độ của hạ tầng mạng và để lại nhiều hậu quả nghiêm trọng cho cá nhân, doanh nghiệp và tổ chức.



Hình 5 Thành phần cơ bản của Endpoint Protection

2. Sự cần thiết

Dựa theo các báo cáo phân tích của các hãng Gartner, IDG hay Frost& Sullivan thì các thiết bị đầu cuối —Endpoint luôn là điểm yếu nhất về an ninh bảo mật, dễ bị tấn công cũng như bị tấn nhiều nhất trong hầu hết các doanh nghiệp. Do vậy việc cần phải có một giải pháp an ninh bảo mật để bảo vệ điểm yếu nhất bên trong hệ thống này.

Nếu xét về khía cạnh người dùng thì thiết bị đầu cuối sẽ bao gồm máy tính để bàn, máy tính xách tay/ultrabook và các thiết bị lưu trữ di động – đây cũng là những điểm cần được bảo vệ vì thường có rất nhiều điểm yếu cũng như là hay bị tấn công nhất.

Ngoài ra, trong một trung tâm dữ liệu thì từ máy chủ cho tới cơ sở dữ liệu, thiết bị lưu trữ đều được xem là thiết bị đầu cuối và cần được giám sát, bảo vệ. Đây đều là những thiết bị có chữa nhưng thông tin có giá trị liên quan đến hạ tầng mạng của doanh nghiệp nói riêng hay công việc kinh doanh của doanh nghiệp nói chung nên cần có các phương pháp để đảm bảo an toàn.

Việc ngày càng có nhiều thiết bị đầu cuối kết nối vào hệ thống, các doanh nghiệp/tổ chức bắt đầu phải tìm kiếm các phương pháp mới để bảo vệ tất cả các thiết bị này theo hướng phải bảo vệ mọi thông tin đồng thời phải có khả năng tối ưu một cách mềm dẻo, linh hoạt nhất.

3. Tính năng kỹ thuật

Giải pháp Endpoint Protection cung cấp một nền tảng bảo mật với nhiều thành phần hoạt động chặt chẽ với nhau không những giúp giảm thiểu sự phức tạp trong môi trường endpoint mà còn tăng được hiệu quả bảo mật cũng như đem đến một cái nhìn trực quan về các mối đe dọa đối với hệ thống diễn ra hàng ngày giúp người quản trị có thể dễ dàng và nhanh chóng đưa ra các phản ứng để chống lại những mối đe dọa này một cách chủ động.

- Được tích hợp nhiều mô đun bảo mật tạo nên lớp phòng thủ đa lớp mà vẫn giữ được sự đồng nhất.
- Có cơ chế phát hiện dựa trên đánh giá hành vi kết hợp với machine learning mang lại sự bảo vệ toàn diện hơn so với kỹ thuật phát hiện chỉ dựa trên signature.
- Bảo vệ người dùng khỏi mã độc bằng khả năng phát hiện và ngăn chặn các mối đe dọa dựa trên hành vi của chúng, từ đó ngăn chặn việc lây lan mã độc ra toàn hệ thống trong đó ransomeware là 1 ví dụ.
- Sử dụng trung tâm dữ liệu thông mình chứa thông tin về các mối đe dọa mà các mô đun có thể kết nối tới đây để lấy thông tin giúp gia tăng tốc độ phát hiện.
- Ngoài ra, giải pháp còn có thể tích hợp với giải pháp EDR để tăng khả năng khắc phục và thích nghi, giúp loại bỏ tận gốc các mối đe dọa ra khỏi hệ thống.

Do đó giải pháp Endpoint Protection đảm bảo những tiêu chí kỹ thuật sau:

3.1. Anti Malware

Endpoint Security: Kết hợp nhiều công nghệ để bảo vệ máy tính người dùng trong thời gian thực, phân tích và phát hiện các loại mã độc mới, mã độc nâng cao, từ đó ngăn chặn sớm trước khi chúng tác động đến người dùng hay cả hệ thống.

Dynamic Application Containment: Kiểm tra các hành vi một cách an toàn và ngăn chặn các mối đe dọa đến từ greyware, ransomware, patient-zero threat,…

Real Protect:

- Phát hiện và ngăn chặn các mối đe dọa nâng cao, zero-day bằng cách phấn tích hành vi tại thời gian thực kết hợp với công nghệ máy học (machine

learning) trích xuất các thông tin về hành vi trước và sau khi file thực thi và phân tích bộ nhớ để kết luận.
- Chống lại các loại mã độc có khả năng nhận biết sandbox bằng cách cho phép các hành vi "độc hại" được thực thi, sau đó phân tích chúng, kết hợp với Dymanic Application Containment để kiểm soát các hành vi độc hại này trước khi chúng kịp tác động lên máy tính.

Host IPS: Bảo vệ thiết bị khỏi các lỗ hổng bảo mật, unknown và zero-day threat.

Threat Intelligence: Liên tục cập nhật những mẫu, biến thể mã độc mới xuất hiện trên toàn cầu.

3.2. Web and Messaging Security

Kiểm soát Web bằng cách lọc URL và Safe Search:

- Cảnh báo người dùng về các website độc hại trước khi họ truy cập vào để giảm thiểu rủi ro cũng như tuân thủ quy chuẩn.
- Áp buộc các chính sách cho phép ủy quyền hay ngăn chặn việc truy cập web.

Anti-malware và anti-spam đối với email:

- Bảo vệ email server và ngăn chặn malware trước khi chúng tới được mail box người dùng.
- Phát hiện, làm sạch và ngăn chặn mã độc cho các hệ thống Microsoft Exchange và Lotus Domino.

3.3. Centralized Management

Kiểm soát chính sách, compliance, và report từ một giao diện theo dõi và quản trị duy nhất.

Đơn giản hóa trong việc quản lý nhiều môi trường OS khác nhau với các chính sách khác nhau.

VI. PfSense

1. Khái niệm

PfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Bắt đầu vào năm 2004, khi m0n0wall mới bắt đầu chập chững– đây là một dự án bảo mật tập trung vào các hệ thống nhúng – pfSense đã có hơn 1 triệu download và được sử dụng để bảo vệ các mạng ở tất cả kích cỡ, từ các mạng gia đình đến các mạng lớn của của các công ty. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó.

2. Tính năng

- **Firewall và Router mạnh mẽ:** PfSense có khả năng quản lý các luồng dữ liệu ra/vào mạng một cách hiệu quả, bảo vệ hệ thống khỏi các mối đe dọa từ bên ngoài.
- **Quản lý VPN:** Hỗ trợ nhiều loại kết nối VPN như IPsec, OpenVPN, PPTP, và L2TP, giúp người dùng thiết lập các kết nối bảo mật giữa các mạng với nhau.
- **Hệ thống quản lý và giám sát mạnh mẽ:** PfSense cung cấp các công cụ giám sát và quản lý mạng chi tiết, giúp người quản trị dễ dàng theo dõi và kiểm soát mạng lưới.
- **Khả năng mở rộng:** Với hệ thống các gói mở rộng, người dùng có thể cài đặt thêm các tính năng và dịch vụ tùy theo nhu cầu cụ thể của họ.
- **Hỗ trợ đa dạng về phần cứng:** PfSense có thể chạy trên nhiều loại phần cứng khác nhau, từ các máy chủ chuyên dụng đến các thiết bị nhúng nhỏ gọn.
- **Giao diện web thân thiện:** Quản lý và cấu hình PfSense qua giao diện web trực quan, giúp người dùng dễ dàng thực hiện các thao tác cấu hình mà không cần phải sử dụng dòng lệnh.

3. Lý do sử dụng

3.1. Sức mạnh

Sức mạnh của tường lửa không chỉ phụ thuộc vào các quy tắc bạn đặt ra cho nó mà còn phụ thuộc vào mức độ chính xác của tường lửa, chẳng hạn như khả năng xác định các luồng dữ liệu đáp ứng tiêu chí bạn đặt ra về những gì được coi là nguy hiểm.

PfSense có nhiều tính năng và khả năng nâng cao giúp đảm bảo nó luôn tuân theo các quy tắc mặc định hoặc tùy chỉnh. Nó cũng lọc riêng lưu lượng truy cập, dù đến từ mạng thiết bị nội bộ hay Internet mở, cho phép bạn đặt các quy tắc và chính sách khác nhau cho từng loại.

Hình 6 Biểu tượng pfSense

3.2. Linh hoạt

Tường lửa pfSense cho phép bạn thêm và tích hợp các tính năng bổ sung dưới dạng code, nên nó đủ linh hoạt để hoạt động vừa như một tường lửa cơ bản vừa như một hệ thống bảo mật hoàn chỉnh.

3.3. Mã nguồn mở

Phần mềm nguồn mở không chỉ miễn phí, toàn bộ code của nó được mở để công chúng kiểm tra và sửa đổi mà không lo vi phạm bản quyền. Bất kỳ ai đủ điều kiện đều có thể đóng góp vào việc cải tiến phần mềm và nhờ những người khác kiểm tra chất lượng và tính xác thực của công việc.

Loại giám sát công khai này đảm bảo phần mềm là phiên bản tốt nhất có thể, mà quyền riêng tư của bạn không bị vi phạm khi sử dụng.

3.4. Thân thiện với người dùng

Tường lửa thường không thân thiện với người dùng mới. Chúng có rất nhiều cài đặt, tùy chọn và tính năng phức tạp cần tinh chỉnh.

Điều làm nên sự khác biệt của pfsense là giao diện của nó rất đơn giản, trực tiếp và dễ sử dụng. Nó cũng cung cấp tài liệu phong phú về các tính năng và tùy chọn với hướng dẫn từng bước, chưa kể đến rất nhiều diễn đàn online và hướng dẫn miễn phí chỉ dành riêng cho pfsense.

3.5. Khả năng chịu lỗi và quản lý tốc độ

Khả năng chịu lỗi (Fault Tolerance) là khi hệ thống của bạn tiếp tục hoạt động trong trường hợp một hoặc nhiều thành phần của nó bị lỗi. Trong trường hợp tường lửa, điều này nghĩa là luôn kết nối với internet bằng cách sử dụng tính năng multi-WAN của pfsense.

Với multi-WAN, bạn có nhiều kết nối internet chạy cùng một lúc, cho phép bạn chuyển sang kết nối tiếp theo trong trường hợp một kết nối bị lỗi. Nhiều kết nối cũng rất hữu ích nếu bạn đang muốn tăng tốc độ kết nối của mình bằng cách chia luồng dữ liệu qua nhiều kết nối thay vì một.

VII. Suricata

1. Khái niệm

Suricata là một công cụ mã nguồn mở dùng để phát hiện và ngăn chặn các cuộc tấn công mạng, do Open Information Security Foundation (OISF) phát triển. Nó được sử dụng rộng rãi trong lĩnh vực bảo mật mạng nhờ khả năng phân tích lưu lượng mạng chi tiết và phát hiện các mối đe dọa.

Hình 7 Biểu tượng Suricata

2. Tính năng

- **Phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS):** Suricata có khả năng phân tích lưu lượng mạng và phát hiện các hoạt động đáng ngờ dựa trên các quy tắc được định nghĩa trước, từ đó ngăn chặn các cuộc tấn công tiềm ẩn.
- **Phân tích gói tin và lưu lượng mạng:** Suricata có khả năng phân tích sâu các gói tin (Deep Packet Inspection - DPI) để phát hiện các mối đe dọa phức tạp và ẩn giấu.
- **Hỗ trợ đa luồng (Multithreading):** Suricata được thiết kế để tận dụng các kiến trúc đa nhân (multi-core), giúp nâng cao hiệu suất xử lý và khả năng mở rộng.
- **Tích hợp với nhiều hệ thống:** Suricata có thể được tích hợp với nhiều hệ thống quản lý bảo mật khác nhau như Splunk, ELK Stack, và các hệ thống SIEM khác để cung cấp cái nhìn tổng thể về an ninh mạng.
- **Chế độ offline và online:** Suricata có thể hoạt động cả trong chế độ giám sát trực tuyến (online) và phân tích dữ liệu đã ghi lại (offline), giúp linh hoạt trong việc giám sát và phân tích lưu lượng mạng.
- **Hỗ trợ nhiều giao thức:** Suricata có khả năng phân tích và giám sát nhiều giao thức mạng khác nhau, bao gồm HTTP, FTP, DNS, TLS, và nhiều giao thức khác.

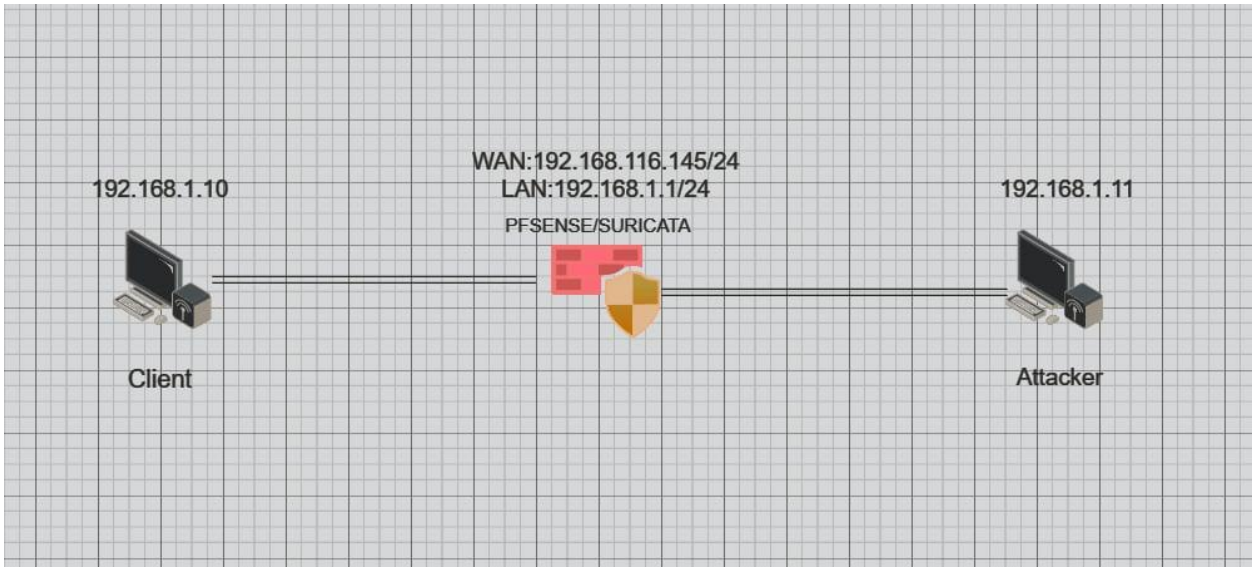
Chương 2: Thực hành

I. Thiết kế hệ thống

Giả định bảo mật cho người dùng cuối

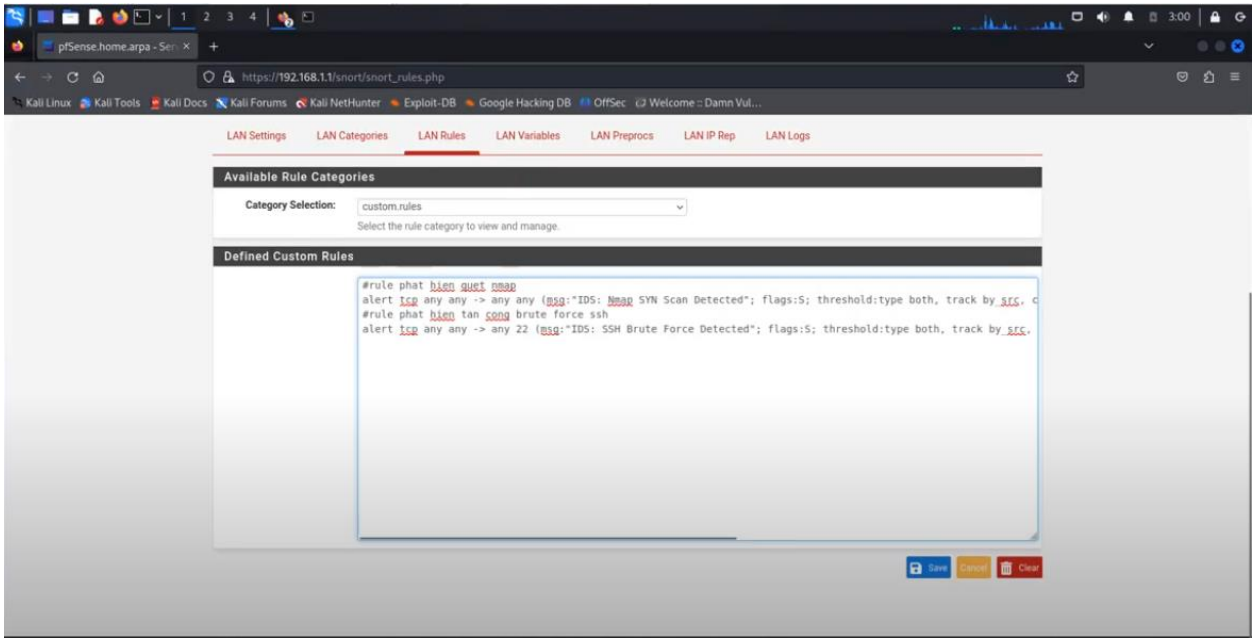
Hệ thống bao gồm:

- 1 máy Kali Linux chạy làm máy Client:
  - IP: 192.168.1.10
  - Cài đặt rule IDS/IPS/Endpoint System
- 1 máy cài pfSense
  - LAN: 192.168.1.1/24
  - WAN: 192.168.116.145/24
  - Cài đặt tích hợp Suricata lên pfSense
- 1 máy Kali Linux chạy làm máy Attack
  - IP: 192.168.1.11
  - Tiến hành tấn công vào máy Client để test tính bảo mật của hệ thống

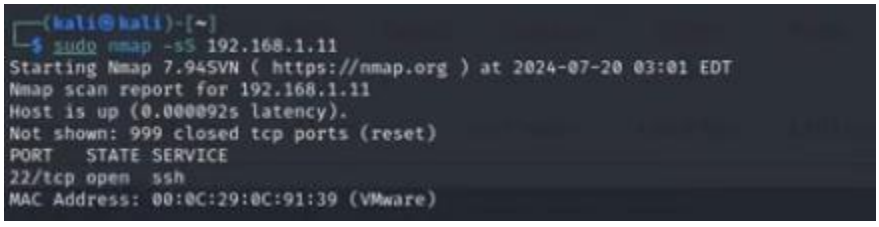


Hình 8 Sơ đồ hệ thống

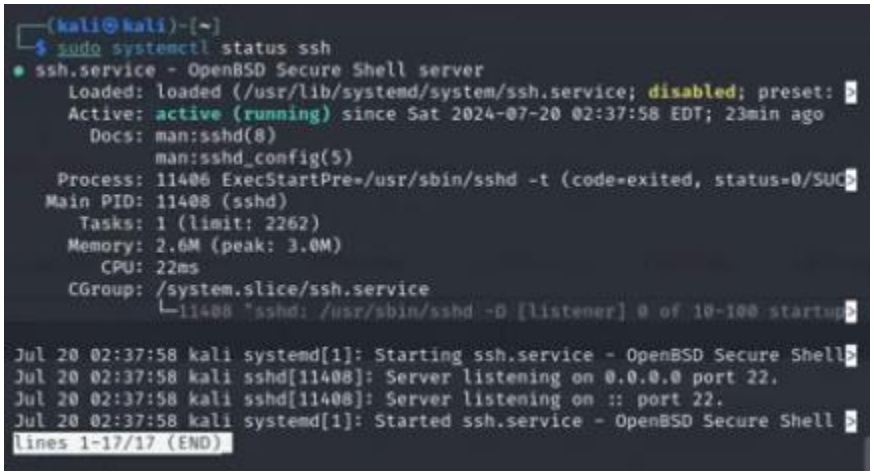
II. IDS



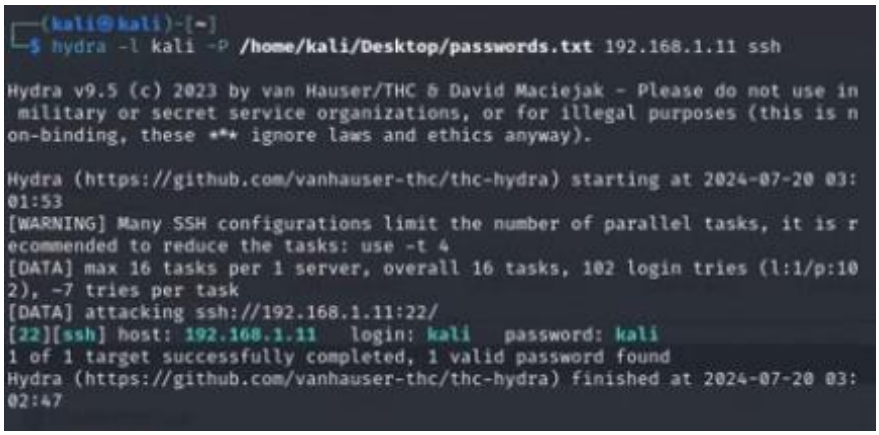
Hình 9 Rule IDS



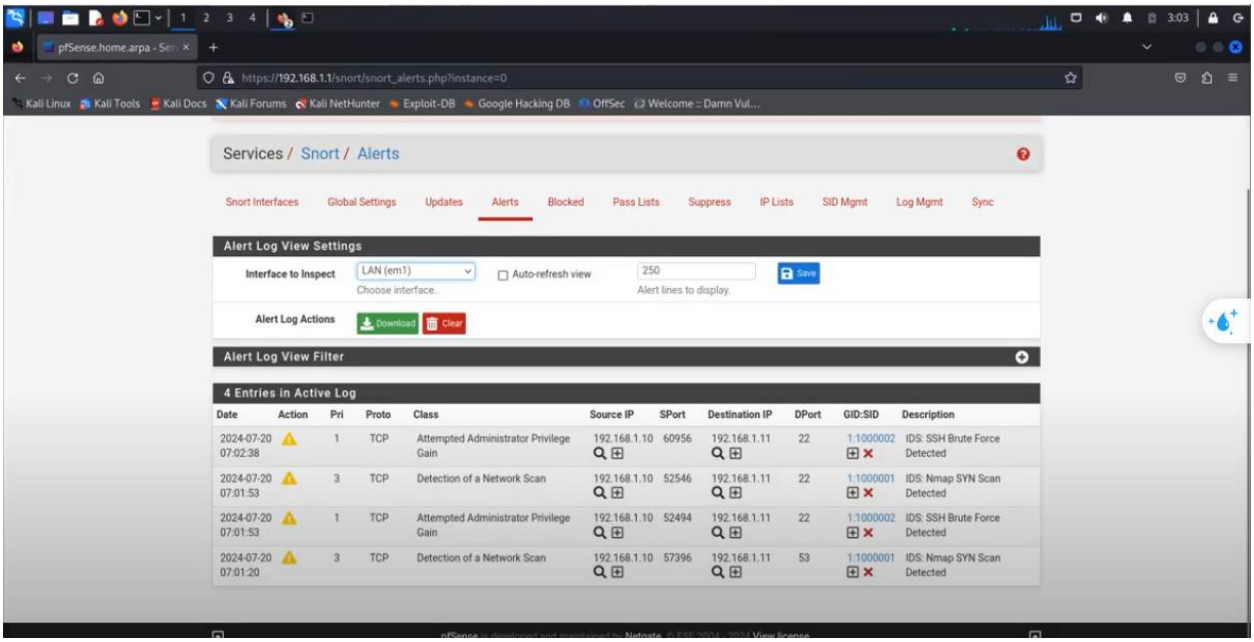
Hình 10 Quét SYN kiểm tra cổng mở



Hình 11 Kiểm tra trạng thái SSH

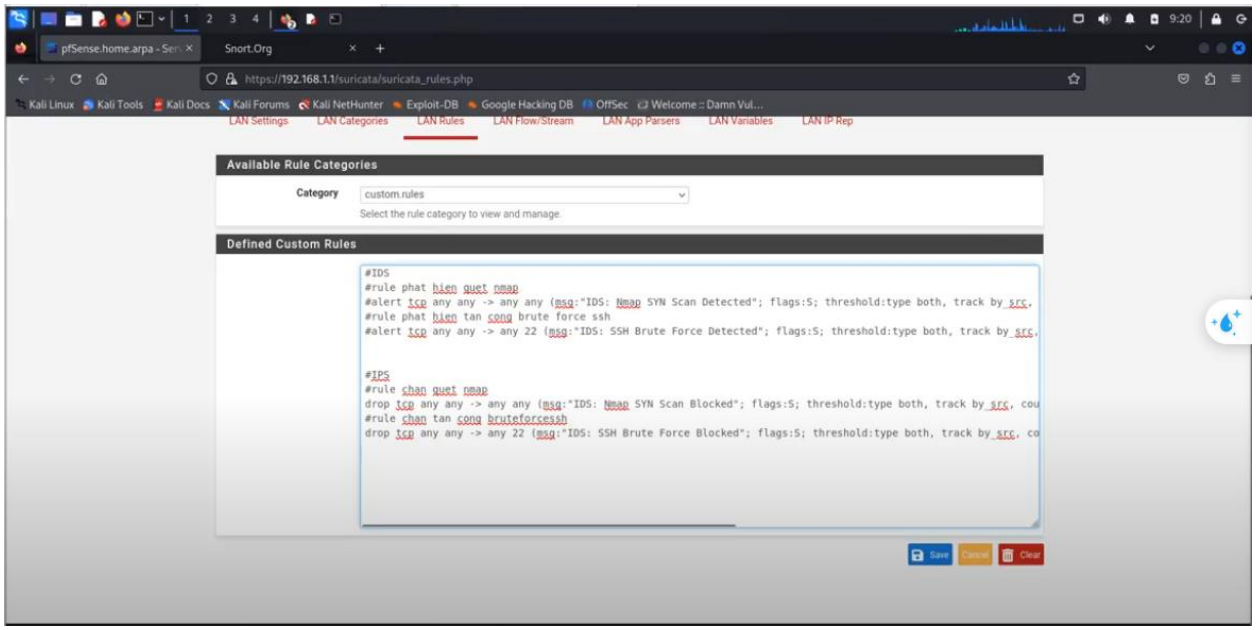


Hình 12 Brute Force vào hệ thống

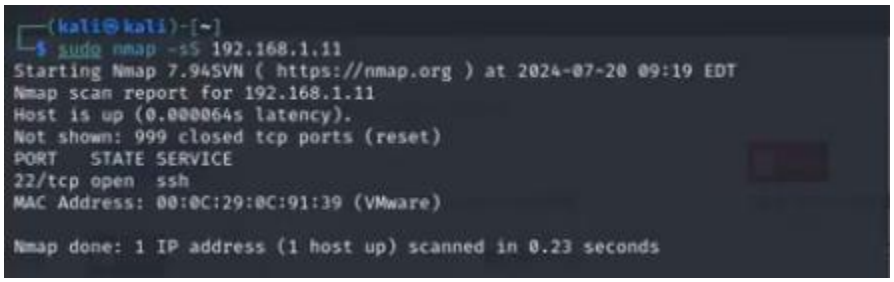


Hình 13 Hệ thống đưa ra cảnh báo

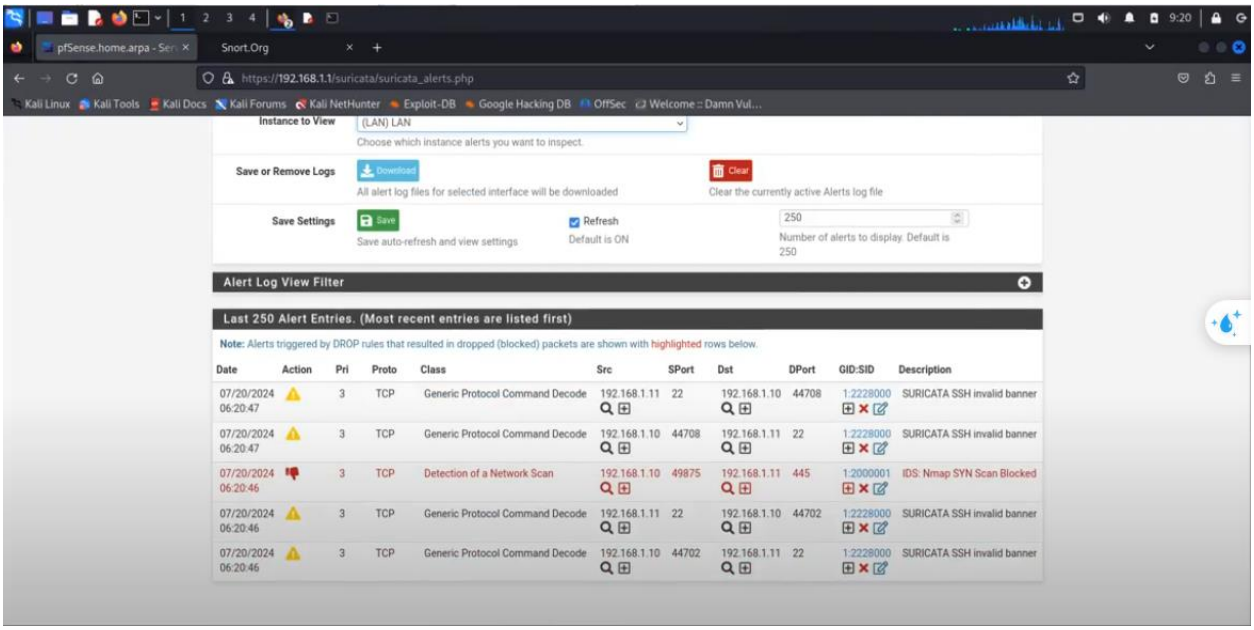
III. IPS



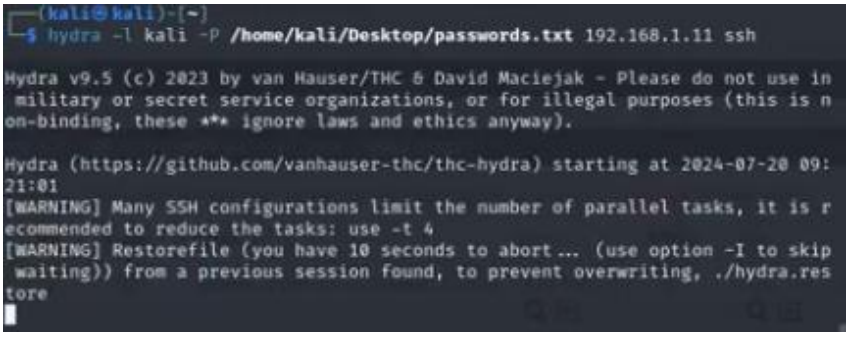
Hình 14 Rule IPS



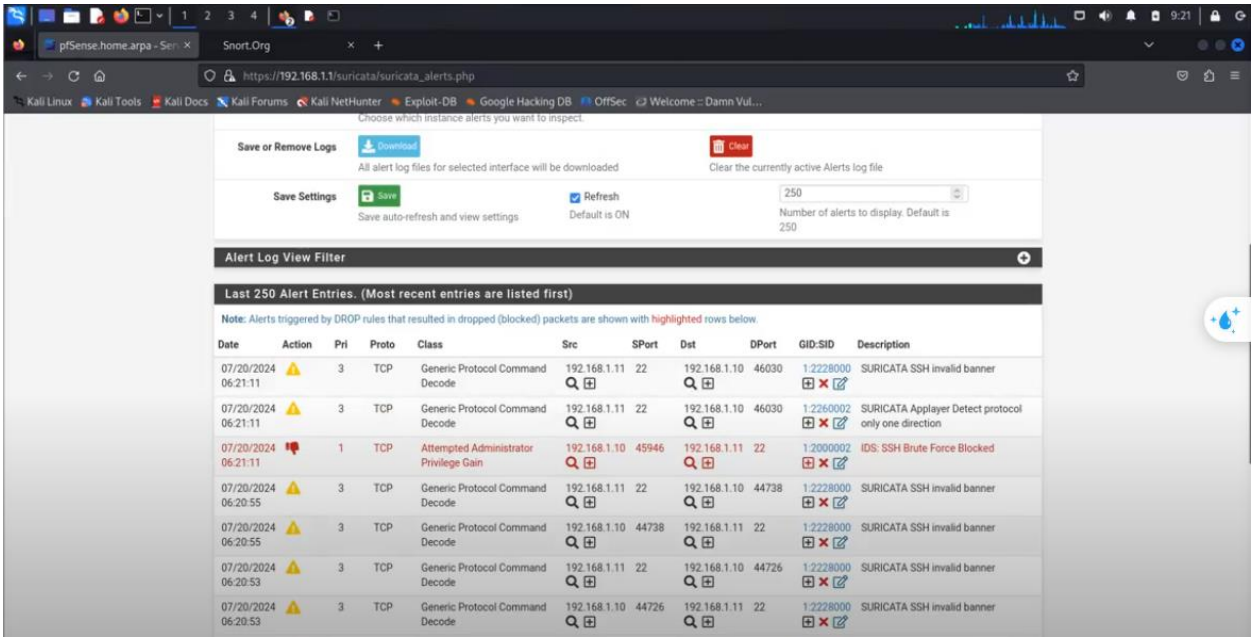
Hình 15 Quét SYN kiểm tra cổng mở



Hình 16 Hệ thống đã cảnh báo và chặn

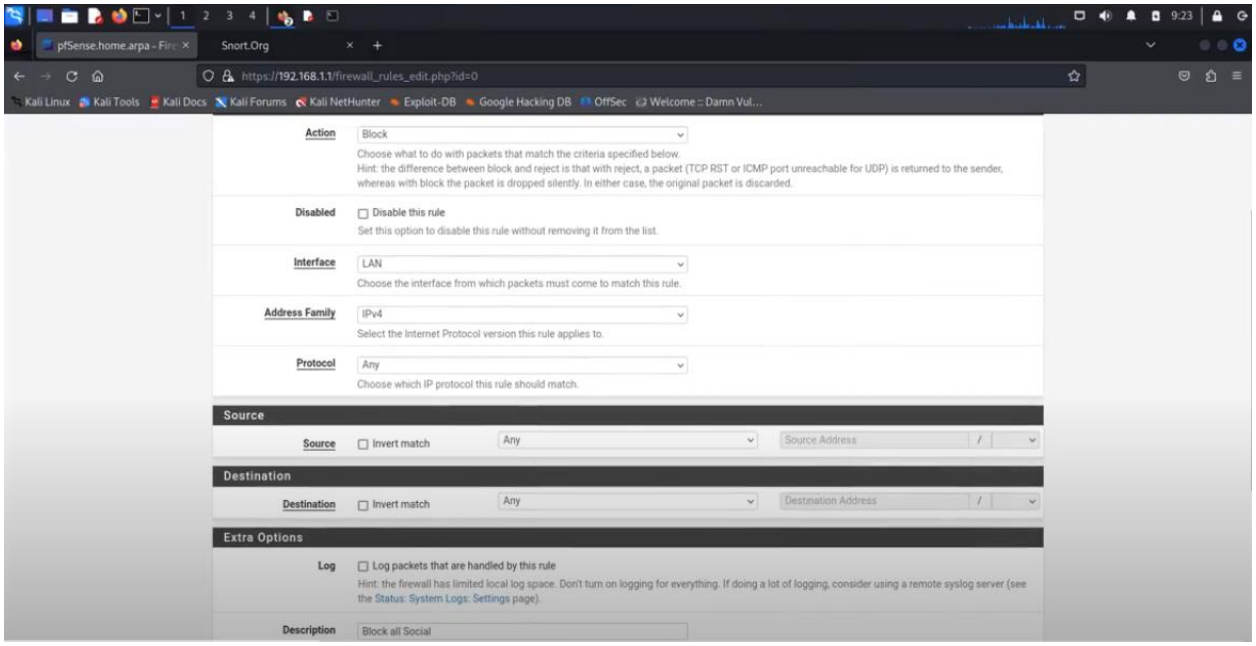


Hình 17 Brute Force vào hệ thống

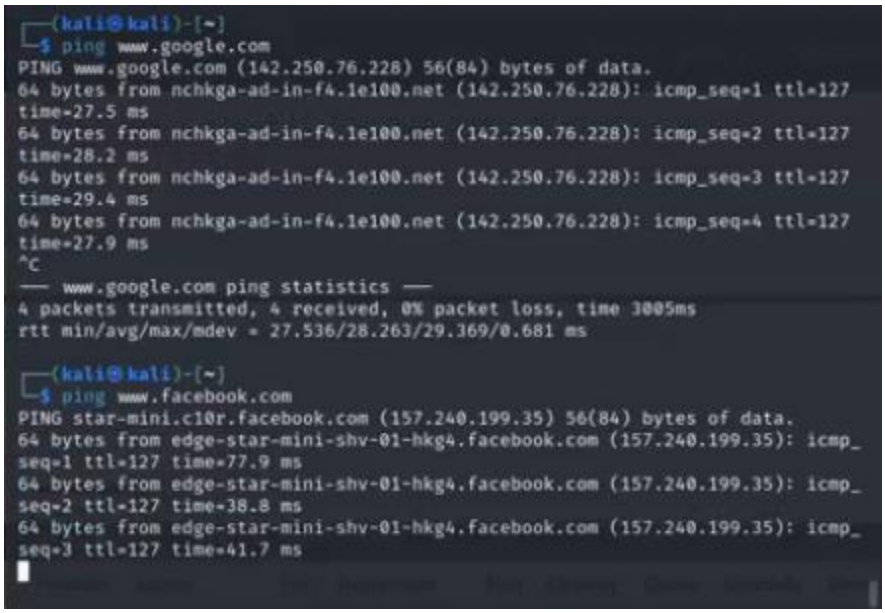


Hình 18 Hệ thống đưa ra cảnh báo và chặn

IV. Endpoint System



Hình 19 Rule endpoint system chặn truy cập mạng



Hình 20 Trước khi chặn

Hình 21 Sau khi chặn