

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



HỆ THỐNG PHÁT HIỆN VÀ PHÒNG CHỐNG XÂM NHẬP

LỚP: PROJ215879_22_1_16CLC

Môn: Đồ án Công nghệ thông tin

NHÓM: 1

GVHD: Huỳnh Nguyên Chính

Thành phố Hồ Chí Minh, Tháng 12 năm 2022

DANH SÁCH NHÓM

HỌC KÌ I, NĂM HỌC: 2022-2023

Tên đề tài: Hệ thống phát hiện và phòng chống xâm nhập

STT	Họ và tên	MSSV	Mức độ đóng góp
1	Võ Trần Bảo Nguyên	20110138	100%
2	Huỳnh Hồ Thọ Tỷ	20110597	100%

Nhận xét của giáo viên:

.....

.....

.....

.....

Ngàytháng.....năm.....

Giáo viên chấm điểm

Mục lục

1.	Đặc tả.....	5
1.1.	Mô tả project.....	5
1.2.	Cơ sở lý thuyết.....	5
1.2.1.	Khái niệm	5
1.2.2.	Phân loại	5
1.2.3.	Chức năng	7
1.2.4.	Các phương pháp nhận diện.....	8
1.2.5.	Cấu trúc/ Kiến trúc của hệ thống IDS/ IPS	9
1.3.	Công cụ, phần mềm sử dụng	12
1.3.1.	Snort	12
1.3.2.	Pfsense.....	13
2.	Phân công công việc.....	14
3.	Thiết kế.....	15
4.	Cài đặt và cấu hình.....	17
4.1.	Cài đặt Pfsense	17
4.2.	Cấu hình hệ thống (Snort)	24
5.	Kiểm thử hệ thống.....	30
5.1.	Thực hiện tình huống 1.....	30
5.2.	Thực hiện tình huống 2.....	32
6.	Kết luận	37
6.1.	Mục tiêu đạt được.....	37
6.2.	Đánh giá ưu và nhược điểm của sản phẩm.....	37
6.2.1.	Ưu điểm.....	37
6.2.2.	Nhược điểm.....	37
6.3.	Những hạn chế gặp phải của nhóm	38
6.4.	Định hướng phát triển.....	39
7.	TÀI LIỆU KHAM THẢO.....	40

Danh mục các hình

Hình 1.1 Sơ đồ các thành phần trong hệ thống	10
Hình 1.2 Kiến trúc của hệ thống IDS.....	11
Hình 1.3 Kiến trúc triển khai hệ thống.....	12
Hình 3.1 Sơ đồ các máy ảo sử dụng trong dự án	15
Hình 4.1 Màn hình tùy chọn tải file ISO cho máy pfSense	17
Hình 4.2 Thiết lập hệ thống mạng cho các máy ảo trên VMware	18
Hình 4.3 Màn hình cài đặt máy ảo trên Vmware	19
Hình 4.4 Màn hình tùy chọn file ISO.....	20
Hình 4.5 Giao diện cài đặt các thiết bị trên máy pfSense	21
Hình 4.6 Giao diện máy pfSense sau khi cài đặt với 2 card mạng	22
Hình 4.7 Màn hình đăng nhập trên GUI của pfSense	23
Hình 4.8 Giao diện Dashboard của pfSense	23
Hình 4.9 Cấu trúc rule của IDS/IPS	24
Hình 4.10 Giao diện Global Settings của Snort.....	25
Hình 4.11 Giao diện phần Oinkcode trên trang web của snort.....	26
Hình 4.12 Phần cuối của giao diện Global Settings.....	26
Hình 4.13 Giao diện phần Updates dùng để Update tải lên các bộ Rules	27
Hình 4.14 Giao diện thêm Interface ở phần Snort Interface.....	27
Hình 4.15 Giao diện của máy pfSense (Với 2 địa chỉ mạng mà ta đã cài đặt từ trước)	28
Hình 4.16 Giao diện Snort Interface sau khi thêm một interface mới.....	28
Hình 4.17 Giao diện thiết lập interface ở phần WAN Categories	29
Hình 4.18 Snort status của interface khi chưa được khởi động	29
Hình 5.1 Giao diện tạo custom rule cho Snort trên GUI	31
Hình 5.2 Màn hình terminal của máy Ubuntu thực hiện ping	31
Hình 5.3 Danh sách các thông báo phát hiện thành công các hoạt động sử dụng giao thức ICMP	32

Hình 5.4 Giao diện cài đặt Block ở phần WAN Setting	33
Hình 5.5 Màn hình ping trước khi từ máy pfSense đến máy Kali	33
Hình 5.6 Nơi chứa thư mục DdoS-Ripper dùng để thực hiện tấn công DoS.....	34
Hình 5.7 Màn hình Terminal khi đang trong quá trình thực hiện tấn công DoS	35
Hình 5.8 Danh sách một số Alert thu được sau khi cuộc tấn công bắt đầu	35
Hình 5.9 Giao diện hiển thị các IP đã bị chặn và các chi tiết các Alert liên quan	36
Hình 5.10 Ping thất bại sau khi đã tấn công và Snort đã thực hiện chặn địa chỉ IP	36

Danh mục các bảng

Bảng 2.1. Phân công công việc

Bảng 3.1 Bảng mô tả thông tin các máy ảo

Bảng 5.1 Bảng các tình huống kiểm thử

1. Đặc tả

1.1. Mô tả project

Mục tiêu của dự án này là tìm hiểu về các hệ thống phát hiện và phòng chống xâm nhập (IDS & IPS) thông qua các cơ sở lý thuyết của chúng, cách chúng được định nghĩa, cơ chế vận hành và cách thức hoạt động của chúng. Sau khi nắm sơ bộ về lý thuyết thì sẽ tiến hành cài đặt các phần mềm, công cụ để xây dựng hệ thống IDS & IPS trên môi trường giả lập là các máy ảo. Trong đó sẽ tiến hành kiểm thử các chức năng, thử nghiệm một số khả năng của IDS & IPS, giả lập các cuộc tấn công để kiểm tra khả năng chống chọi, chịu đựng của hệ thống, từ đó rút ra được các kinh nghiệm quý báu cho việc xây dựng, mở rộng và cách tổ chức một hệ thống IDS & IPS trên thực tế.

1.2. Cơ sở lý thuyết

1.2.1. Khái niệm

Intrusion Detection system (IDS) là một hệ thống giám sát hoạt động trên hệ thống mạng và phân tích để tìm ra các dấu hiệu vi phạm đến các quy định bảo mật máy tính, chính sách sử dụng và các tiêu chuẩn an toàn thông tin. Các dấu hiệu này xuất phát từ rất nhiều nguyên nhân khác nhau, như lây nhiễm malwares, hackers xâm nhập trái phép, người dung cuối truy nhập vào các tài nguyên không được phép truy cập,...

Intrusion Prevention system (IPS) là một hệ thống bao gồm cả chức năng phát hiện xâm nhập (Intrusion Detection – ID) và khả năng ngăn chặn các xâm nhập trái phép dựa trên sự kết hợp với các thành phần khác như Antivirus, Firewall hoặc sử dụng các tính năng ngăn chặn tích hợp. Do đó nó được coi là bản mở rộng của IDS.

1.2.2. Phân loại

Hệ thống IDS được chia làm 5 loại

- Network Intrusion Detection System (NIDS):

Được thiết lập tại một điểm dự kiến trong mạng để kiểm tra lưu lượng từ tất cả các thiết bị trên mạng. Nó thực hiện quan sát lưu lượng truyền trên toàn bộ mạng con và so sánh với lưu lượng truyền khi tập hợp các cuộc tấn công đã biết xảy ra. Khi một cuộc tấn công được xác định hoặc quan sát thấy hành vi bất thường, cảnh báo có thể được gửi đến quản trị viên.

- Host Intrusion Detection System (HIDS):

HIDS chạy trên các máy chủ hoặc thiết bị độc lập trên mạng. HIDS chỉ giám sát các gói đến và đi từ thiết bị và sẽ cảnh báo cho quản trị viên nếu phát hiện hoạt động đáng ngờ hoặc độc hại. Nó ghi nhận trạng thái của các tệp hệ thống hiện có và so sánh nó với trạng thái ghi nhận trước đó. Nếu các tệp hệ thống phân tích bị chỉnh sửa hoặc xóa, một cảnh báo sẽ được gửi đến quản trị viên để điều tra.

- Protocol-based Intrusion Detection System (PIDS):

Hệ thống phát hiện xâm nhập dựa trên giao thức (PIDS) bao gồm một hệ thống hoặc Agent luôn ở đầu phía trước của máy chủ, nó kiểm soát và diễn giải giao thức giữa người dùng (thiết bị) và máy chủ. PIDS bảo mật máy chủ web bằng cách thường xuyên theo dõi luồng giao thức HTTPS và chấp nhận giao thức HTTP liên quan. Vì HTTPS không được mã hóa nên trước khi nó vào tầng Presentation trong mô hình OSI, hệ thống này sẽ cần phải nằm trong này để sử dụng HTTPS.

- Application Protocol-based Intrusion Detection System (APIDS):

Hệ thống phát hiện xâm nhập dựa trên giao thức ứng dụng (APIDS) là một hệ thống hoặc Agent thường nằm trong một nhóm máy chủ. Nó xác định các xâm nhập bằng cách giám sát và diễn giải thông tin liên lạc trên các giao thức dành riêng cho ứng dụng.

- Hybrid Intrusion Detection System:

Hybrid Intrusion Detection System được tổ chức kết hợp của hai hoặc nhiều mô hình hệ thống phát hiện xâm nhập. Trong hệ thống này, Host agent hoặc dữ liệu hệ thống được kết hợp với thông tin mạng để phát triển một cái nhìn hoàn

chỉnh về hệ thống mạng. Hybrid Intrusion Detection System được cho là hiệu quả hơn khi so với các mô hình IDS đơn lẻ khác.

Hệ thống IPS được chia làm 4 loại

- Network-based intrusion prevention system (NIPS):

Giám sát toàn bộ mạng để tìm lưu lượng đáng ngờ bằng cách phân tích hoạt động của giao thức.

- Wireless intrusion prevention system (WIPS):

Giám sát toàn bộ mạng không dây để tìm lưu lượng đáng ngờ bằng cách phân tích hoạt động của giao thức mạng không dây

- Network behavior analysis (NBA):

Kiểm tra lưu lượng mạng để xác định các mối đe dọa tạo ra các luồng lưu lượng bất thường, chẳng hạn như các cuộc tấn công từ chối dịch vụ phân tán, các dạng phần mềm độc hại cụ thể và vi phạm chính sách.

- Host-based intrusion prevention system (HIPS):

Là một gói phần mềm có sẵn vận hành cho một máy chủ duy nhất, xác định hoạt động đáng ngờ bằng cách quét các sự kiện xảy ra trong máy chủ đó.

1.2.3. Chức năng

- Nhận diện các nguy cơ có thể xảy ra.
- Ghi nhận thông tin, log để phục vụ cho việc kiểm soát nguy cơ.
- Nhận diện các hoạt động thăm dò hệ thống.
- Nhận diện các yếu khuyết của chính sách bảo mật.
- Ngăn chặn vi phạm chính sách bảo mật.
- Lưu giữ thông tin liên quan đến các đối tượng quan sát.
- Cảnh báo những sự kiện quan trọng liên quan đến đối tượng quan sát.

- Ngăn chặn các tấn công (IPS).
- Xuất báo cáo cho người dùng tiện cho việc theo dõi.

1.2.4. Các phương pháp nhận diện

Các hệ thống IDS/IPS thường dùng nhiều phương pháp nhận diện khác nhau, riêng rẽ hoặc tích hợp nhằm mở rộng và tăng cường độ chính xác nhận diện. Gồm các phương pháp nhận diện chính sau:

- Nhận diện dựa vào dấu hiệu (Signature-base detection): sử dụng phương pháp so sánh các dấu hiệu của đối tượng quan sát với các dấu hiệu của các mối nguy hại đã biết. Phương pháp này có hiệu quả với các mối nguy hại đã biết nhưng hầu như không có hiệu quả hoặc hiệu quả rất ít đối với các mối nguy hại chưa biết, các mối nguy hại sử dụng kỹ thuật lẩn tránh và các biến thể của nó. Signature-based không thể theo vết và nhận diện trạng thái của các truyền thông phức tạp.

- Nhận diện bất thường (Abnormaly-base detection): so sánh định nghĩa của những hoạt động bình thường và đối tượng quan sát nhằm xác định các độ lệch. Một hệ IDS/IPS sử dụng phương pháp Anormaly-base detection có các profiles đặc trưng cho các hành vi được coi là bình thường, được phát triển bằng cách giám sát các đặc điểm của hoạt động tiêu biểu trong một khoảng thời gian. Sau khi đã xây dựng được tập các profile này, hệ IDS/IPS sử dụng phương pháp thống kê để so sánh các đặc điểm của các hoạt động hiện tại với các ngưỡng định bởi profile tương ứng để phát hiện ra những bất thường. Profile sử dụng bởi phương pháp này có 2 loại là tĩnh (static) và động (dynamic). Static profile không thay đổi cho đến khi được tái tạo, chính vì vậy dần dần nó sẽ trở nên không chính xác, và cần phải được tái tạo định kỳ. Dynamic profile được tự động điều chỉnh mỗi khi có các sự kiện bổ sung được quan sát, nhưng chính điều này cũng làm cho nó trở nên dễ bị ảnh hưởng bởi các phép thử dung kỹ thuật giấu (evasion techniques). Ưu điểm chính của phương pháp này là nó rất có hiệu quả trong việc phát hiện ra các mối nguy hại chưa được biết đến.

- Phân tích trạng thái giao thức (Stateful protocol analysis): phân tích trạng thái giao thức là quá trình so sánh các profile định trước của hoạt động của mỗi giao thức được coi là bình thường với đối tượng quan sát từ đó xác định độ lệch. Khác với phương pháp Anomaly-base detection, phân tích trạng thái protocol dựa trên tập các profile tổng quát cung cấp bởi nhà sản xuất theo đó quy định 1 protocol nên làm và không nên làm gì. IDS/IPS có khả năng hiểu và theo dõi tình trạng của mạng và vận chuyển các giao thức ứng dụng có trạng thái. Nhược điểm của phương pháp này là chiếm nhiều tài nguyên do sự phức tạp trong việc phân tích và theo dõi nhiều phiên đồng thời. Một vấn đề nghiêm trọng là phương pháp phân tích trạng thái protocol không thể phát hiện các cuộc tấn công khi chúng không vi phạm các đặc tính của tập các hành vi chấp nhận của giao thức.

1.2.5. Cấu trúc/ Kiến trúc của hệ thống IDS/ IPS

- Cơ sở hạ tầng

Nhiệm vụ chính của hệ thống IDS/IPS là phòng thủ máy tính bằng cách phát hiện một cuộc tấn công và có thể đẩy lùi nó. Phát hiện vụ tấn công thù địch phụ thuộc vào số lượng và loại hành động thích hợp. Công tác phòng chống xâm nhập đòi hỏi một sự kết hợp tốt được lựa chọn của "mồi và bẫy" nhằm điều tra các mối đe dọa, nhiệm vụ chuyển hướng sự chú ý của kẻ xâm nhập từ các hệ thống cần bảo vệ sang các hệ thống giả lập là nhiệm vụ của 1 dạng IDS riêng biệt (Honeypot IDS), cả hai hệ thống thực và giả lập được liên tục giám sát và dữ liệu thu được được kiểm tra cẩn thận (đây là công việc chính của mỗi hệ IDS/IPS) để phát hiện các cuộc tấn công có thể (xâm nhập).

Một khi xâm nhập một đã được phát hiện, hệ thống IDS/IPS phát các cảnh báo đến người quản trị về sự kiện này. Bước tiếp theo được thực hiện, hoặc bởi các quản trị viên hoặc bởi chính hệ thống IDS/IPS , bằng cách áp dụng các biện pháp đôi phó (chấm dứt phiên làm việc, sao lưu hệ thống, định tuyến các kết nối đến Honeypot IDS hoặc sử dụng các cơ sở hạ tầng pháp lý,...), việc này tùy thuộc vào chính sách an ninh của mỗi tổ chức.

Hệ thống IDS/IPS là một thành phần của chính sách bảo mật. Trong số các nhiệm vụ IDS khác nhau, nhận dạng kẻ xâm nhập là một trong những nhiệm vụ cơ bản. Nó có thể hữu ích trong các nghiên cứu giám định sự cố và tiến hành cài đặt các bản vá thích hợp để cho phép phát hiện các cuộc tấn công trong tương lai nhằm vào mục tiêu cụ thể.



Hình 1.1 Sơ đồ các thành phần trong hệ thống

- Các thành phần cơ bản

- + Sensor/Agent: giám sát và phân tích các hoạt động. “Sensor” thường được dùng cho dạng Network-base IDS/IPS trong khi “Agent” thường được dùng cho dạng Host-base IDS/IPS.

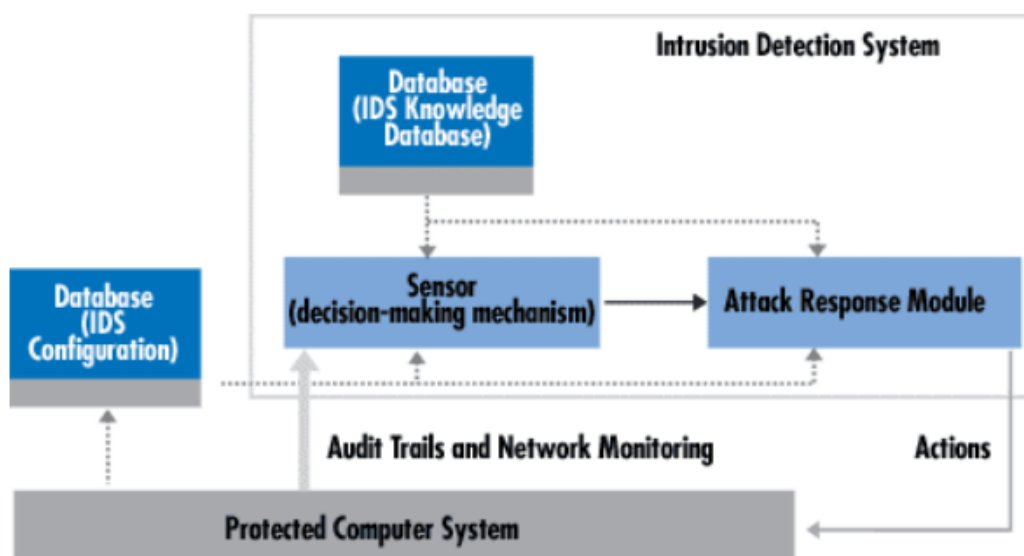
- + Management Server: là 1 thiết bị trung tâm dùng thu nhận các thông tin từ Sensor/Agent và quản lý chúng. 1 số Management Server có thể thực hiện việc phân tích các thông tin sự việc được cung cấp bởi Sensor/Agent và có thể nhận dạng được các sự kiện này dù các Sensor/Agent đơn lẻ không thể nhận diện.

- + Database server: dùng lưu trữ các thông tin từ Sensor/Agent hay Management Server

- + Console: là 1 chương trình cung cấp giao diện cho IDS/IPS users và Admins. Có thể cài đặt trên một máy tính bình thường dùng để phục vụ cho tác vụ quản trị, hoặc để giám sát, phân tích.

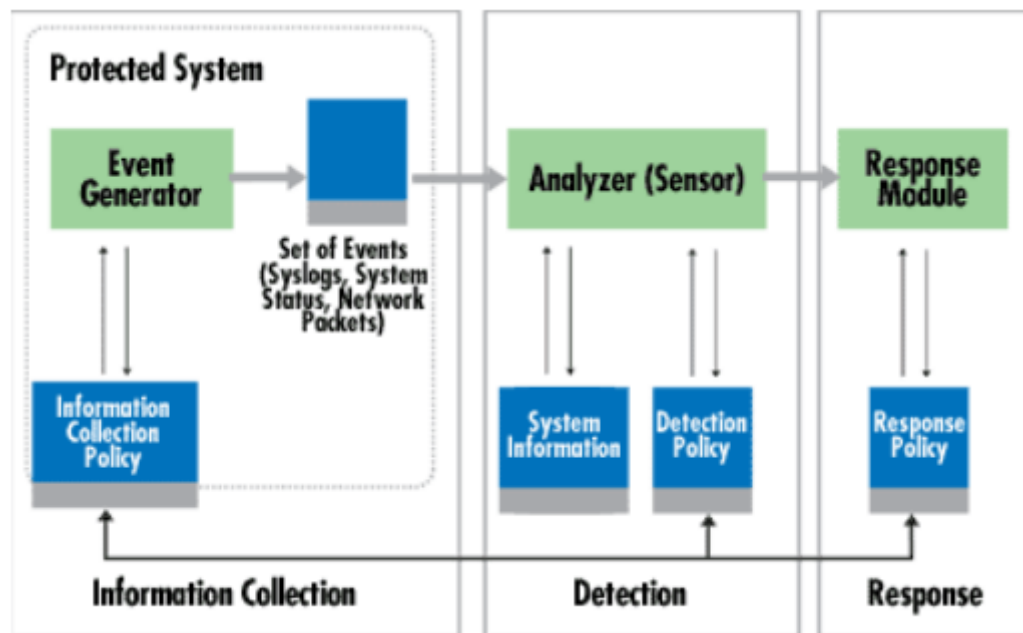
- Kiến trúc

Sensor là yếu tố cốt lõi trong một hệ thống IDS/IPS, nó có trách nhiệm phát hiện các xâm nhập nhờ chứa những cơ chế ra quyết định đối với sự xâm nhập. Sensor nhận dữ liệu từ ba nguồn thông tin chính: kiến thức cơ bản của IDS, nhật kí hệ thống và lộ trình đánh giá. Các thông tin này tạo cơ sở cho quá trình ra quyết định sau này. Sensor được tích hợp với các thành phần chịu trách nhiệm thu thập dữ liệu - một Trình tạo sự kiện (event generator). Các event generator (hệ điều hành, mạng, ứng dụng) tạo ra một chính sách nhất quán tập các sự kiện có thể là log hoặc audit của các sự kiện của hệ thống, hoặc các gói tin. Điều này kết hợp thiết lập cùng với các thông tin chính sách có thể được lưu trữ trong hệ thống bảo vệ hoặc bên ngoài. Trong những trường hợp nhất định, dữ liệu không được lưu trữ mà được chuyển trực tiếp đến các phân tích (thông thường áp dụng với các gói packet).



Hình 1.2 Kiến trúc của hệ thống IDS

Các hệ thống IDS/IPS có thể được triển khai theo 2 hướng là tập trung và phân tán. Một ví dụ cụ thể cho hướng triển khai tập trung là tích hợp IDS/IPS cùng với các thành phần an ninh khác như firewall. Triển khai phân tán (distributed IDS) bao gồm nhiều hệ IDS/IPS trong 1 hệ thống mạng lớn, được kết nối với nhau nhằm nâng cao khả năng nhận diện chính xác xâm nhập và đưa ra phản ứng thích hợp.



Hình 1.3 Kiến trúc triển khai hệ thống

1.3. Công cụ, phần mềm sử dụng

1.3.1. Snort

Snort là một hệ thống phát hiện xâm nhập mạng mã nguồn mở miễn phí và hệ thống ngăn chặn xâm nhập được tạo ra vào năm 1998 bởi Martin Roesch, người sáng lập và cựu CTO của Sourcefire. Snort hiện được phát triển bởi Cisco, công ty đã mua Sourcefire vào năm 2013. Snort có khả năng phân tích thời gian thực lưu lượng mạng, và ghi log gói tin trên nền mạng IP. Ban đầu được gọi công nghệ phát hiện và phòng chống xâm nhập hạng nhẹ, Snort đã dần phát triển và trở thành tiêu chuẩn trong việc phát hiện và phòng chống xâm nhập. Snort là một trong những công nghệ phát hiện và phòng chống xâm nhập được sử dụng rộng rãi nhất hiện nay.

Snort có thể thực hiện phân tích giao thức và tìm kiếm nội dung, từ đó có thể phát hiện rất nhiều kiểu thăm dò và tấn công như buffer-overflow, stealth ports scanning, tấn công CGI, OS fingerprint, thăm dò SMB... Để có thể làm được điều này, Snort dùng 1 loại ngôn ngữ mô tả các quy tắc giao thông mạng mà nó sẽ thu thập hoặc bỏ qua, cũng như sử dụng cơ chế phát hiện xâm nhập theo kiến trúc modular plug-ins. Nó cũng có khả năng cảnh báo tức thời, kết hợp với các cơ chế cảnh báo syslog, tập tin người dùng chỉ định, Unix socket hoặc Winpopup message.

1.3.2. Pfsense

pfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, cho phép bạn mở rộng mạng của mình mà không bị vướng các vấn đề về sự bảo mật. Bắt đầu từ năm 2004, đây là một dự án bảo mật tập trung vào các hệ thống nhúng – pfSense đã có hơn 1 triệu lượt tải, được sử dụng để bảo vệ các mạng ở nhiều kích cỡ đa dạng, từ mạng gia đình đến mạng lớn của các công ty. Pfsense 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.

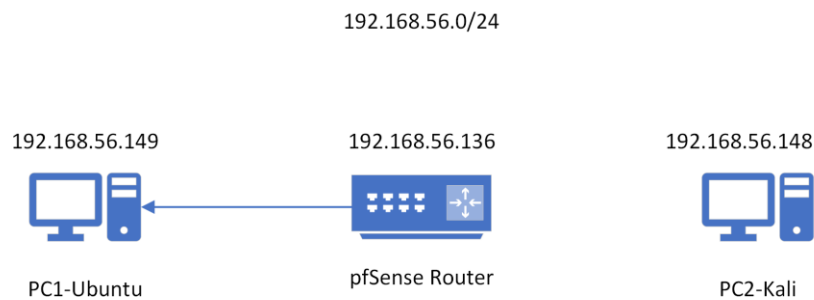
Pfsense bao gồm nhiều tính năng như trên các thiết bị tường lửa hoặc router thương mại, chẳng hạn như GUI trên nền Web tạo sự quản lý một cách dễ dàng. PfSense được dựa trên FreeBSD và giao thức Common Address Redundancy Protocol (CARP) của FreeBSD, cung cấp khả năng dự phòng bằng cách cho phép các quản trị viên nhóm hai hoặc nhiều tường lửa vào một nhóm tự động chuyển đổi dự phòng. Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải. Nhưng Pfsense như một tường lửa ngăn cách giữa mạng WAN và LAN nên máy cài đặt Pfsense cần ít nhất là 2 card mạng.

2. Phân công công việc

Bảng 2.1. Phân công công việc

TT	Tên Sinh viên	Công việc	Ước tính phần trăm đóng góp
1	Võ Trần Bảo Nguyên	<ul style="list-style-type: none">- Cấu hình hệ thống và viết báo cáo phần cấu hình hệ thống (chương 4)- Chạy thử nghiệm hệ thống và viết báo cáo chương 5 (Thử nghiệm hệ thống).- Viết báo cáo chương 3 (Thiết kế hệ thống).- Viết báo cáo chương 4 (Cài đặt hệ thống).	100%
2	Huỳnh Hồ Thọ Tỷ	<ul style="list-style-type: none">- Định dạng, dàn bố cục của báo cáo.- Tìm hiểu và viết báo cáo chương 1 (Đặc tả).- Cài đặt hệ thống và viết báo cáo phần cài đặt hệ thống (chương 4).- Viết kết luận.- Hiệu chỉnh báo cáo.	100%

3. Thiết kế



Hình 3.1 Sơ đồ các máy ảo sử dụng trong dự án

3.1 Bảng mô tả thông tin các máy ảo

Tên thiết bị	Hệ điều hành	Địa chỉ IP	Mô tả chi tiết
pfSense Router	FreeBSD	192.168.56.136	<ul style="list-style-type: none">- Một thiết bị định tuyến được cài đặt như một máy ảo chạy trên hệ điều hành FreeBSD.- Thiết bị cung cấp sẵn dịch vụ tường lửa và có khả năng tích hợp thêm dịch vụ IDS/IDS thông qua Snort- Ngoài ra khi cài đặt thiết bị còn được cài đặt thêm một hệ thống mạng riêng với bản thân là máy server với địa chỉ IP là 192.168.1.1
PC1	Ubuntu	192.168.56.149	<ul style="list-style-type: none">- Máy ảo được cài đặt và chạy trên hệ điều hành ubuntu- Thiết bị được kết nối với hệ thống mạng riêng của router để có thể truy cập vào GUI của

			pfSense Router thông qua địa chỉ: https://192.168.1.1
PC2	Kali	192.168.56.148	<ul style="list-style-type: none"> - Máy ảo được cài đặt và chạy trên hệ điều hành Kali - Thiết bị được cấp địa chỉ mạng cùng với 2 thiết bị trên để có thể thực hiện ping. - Thiết bị còn được cài đặt chương trình giả lập tấn công DDOS để thực hiện thử nghiệm hệ thống IDS/IPS

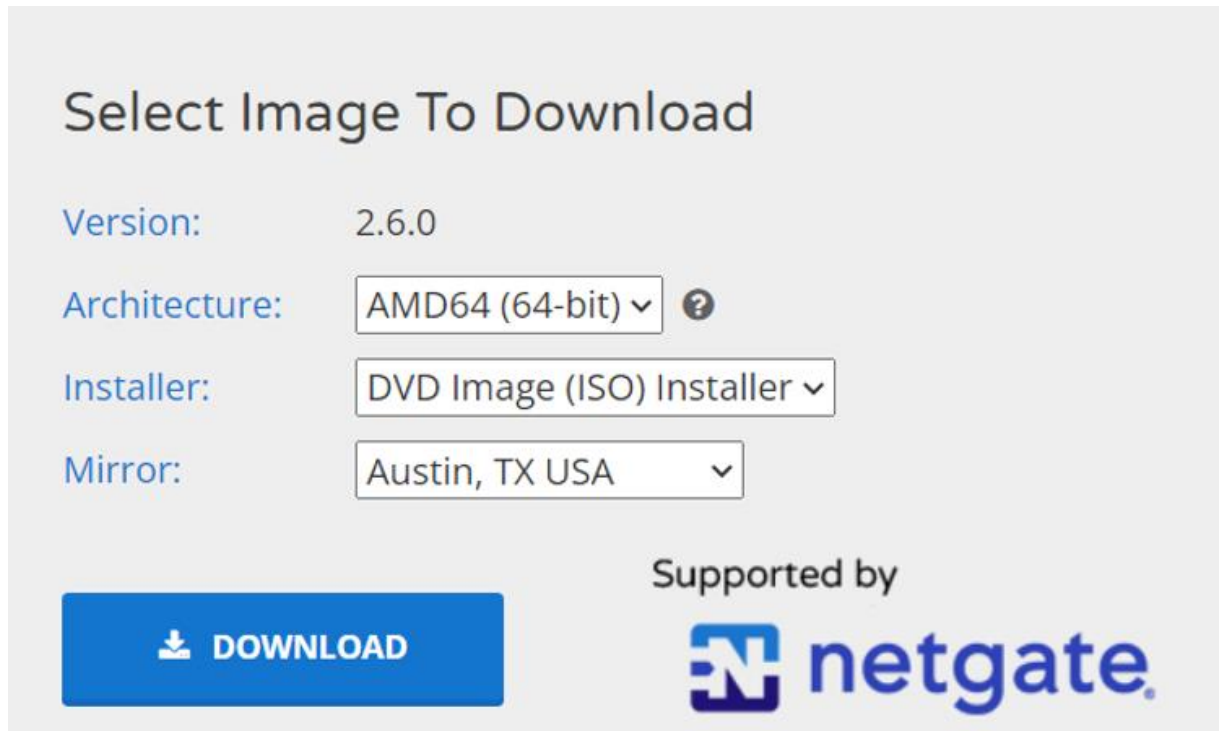
4. Cài đặt và cấu hình

4.1. Cài đặt Pfsense

- Tải file PfSense ISO image.

Link: <https://www.pfsense.org/download/>

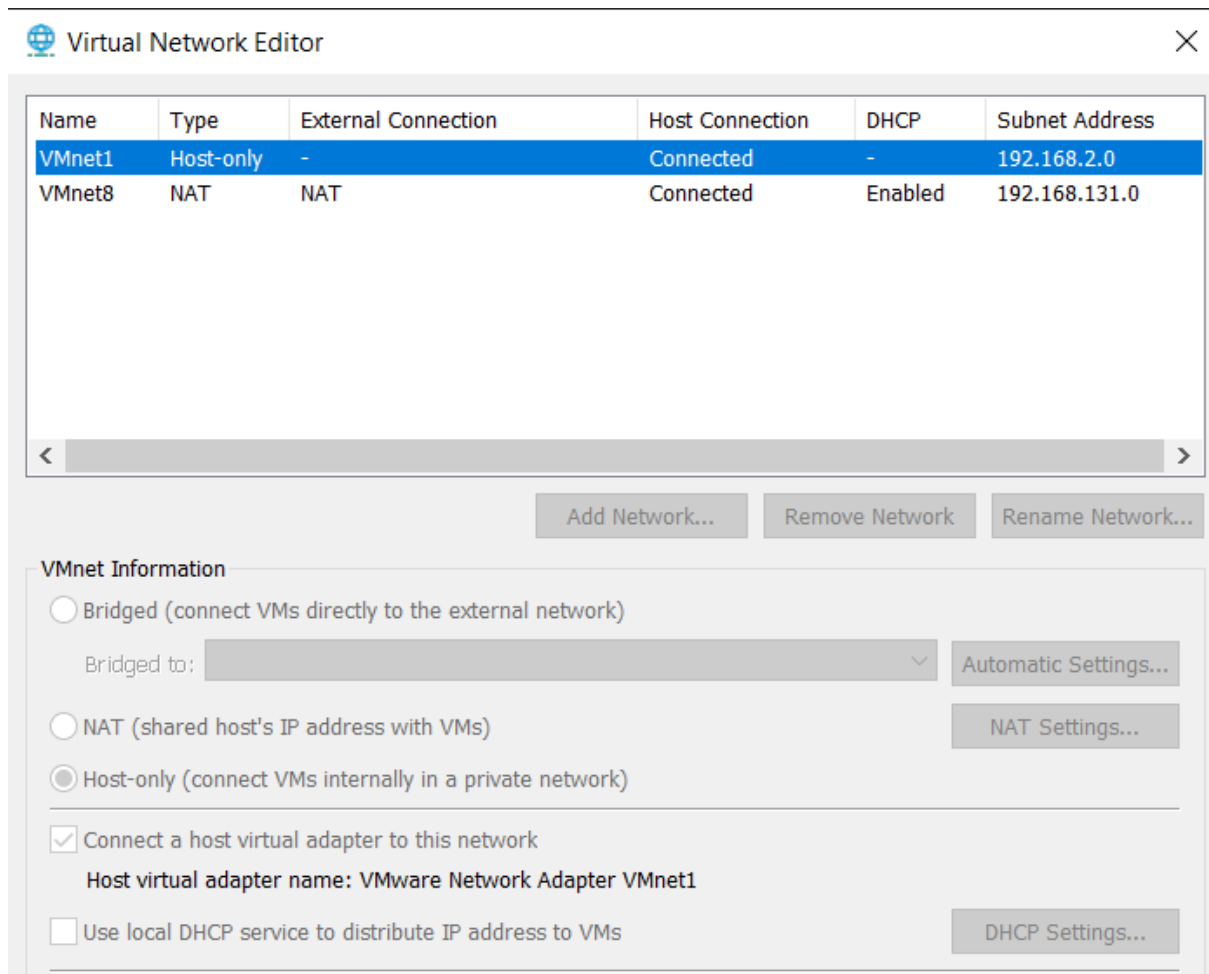
Chọn các thông số như hình



The screenshot shows the 'Select Image To Download' page on the PfSense website. It features four configuration options, each with a label and a value: 'Version' is set to '2.6.0'; 'Architecture' is set to 'AMD64 (64-bit)' with a dropdown arrow and a help icon; 'Installer' is set to 'DVD Image (ISO) Installer' with a dropdown arrow; and 'Mirror' is set to 'Austin, TX USA' with a dropdown arrow. Below these options is a large blue button with a download icon and the text 'DOWNLOAD'. To the right of the button, it says 'Supported by' followed by the Netgate logo and name.

Hình 4.1 Màn hình tùy chọn tải file ISO cho máy pfSense

- Cấu hình mạng cho máy ảo để chạy Pfsense
- Chọn Edit -> Virtual Network -> Virtual Network Editor -> Change settings.

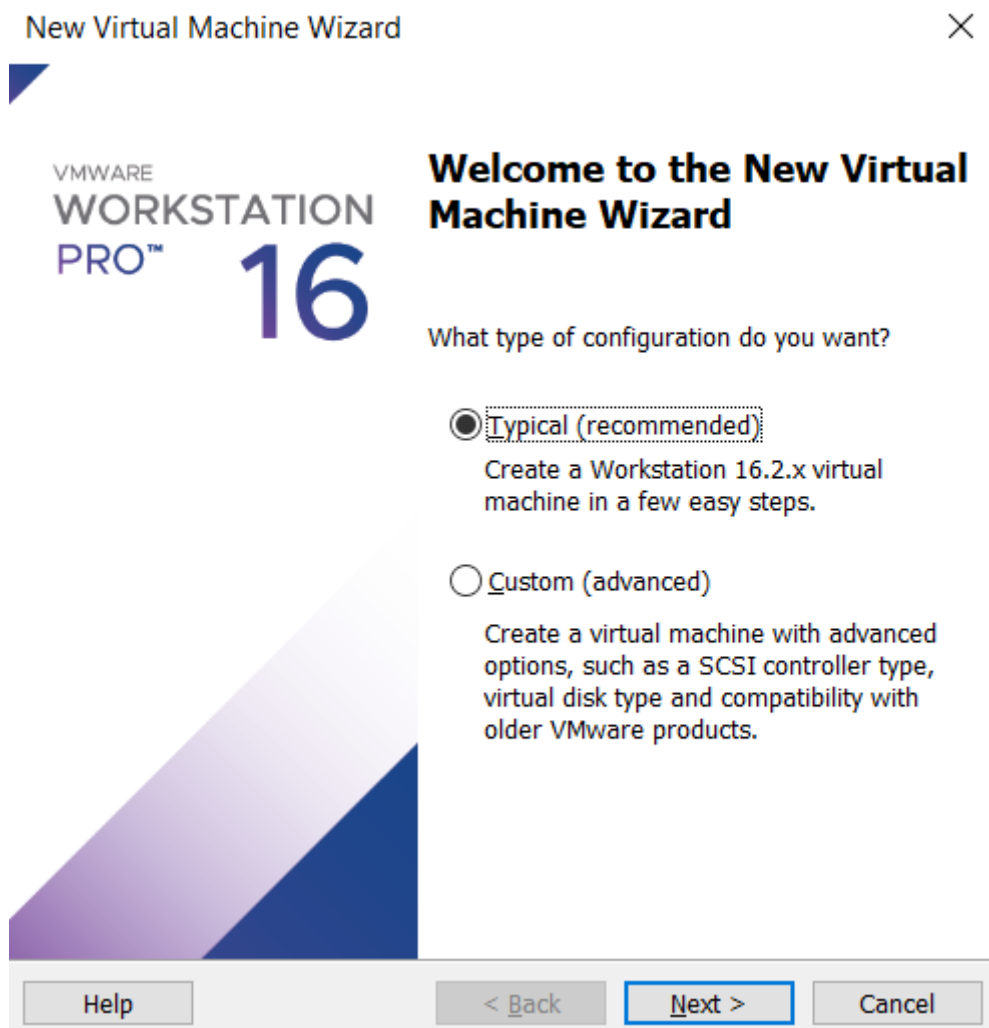


Hình 4.2 Thiết lập hệ thống mạng cho các máy ảo trên VMware

- Cấu hình VMnet1 cho mạng LAN làm adapter thứ hai -> chọn VMnet1 -> Host-only -> use Local DHCP service...

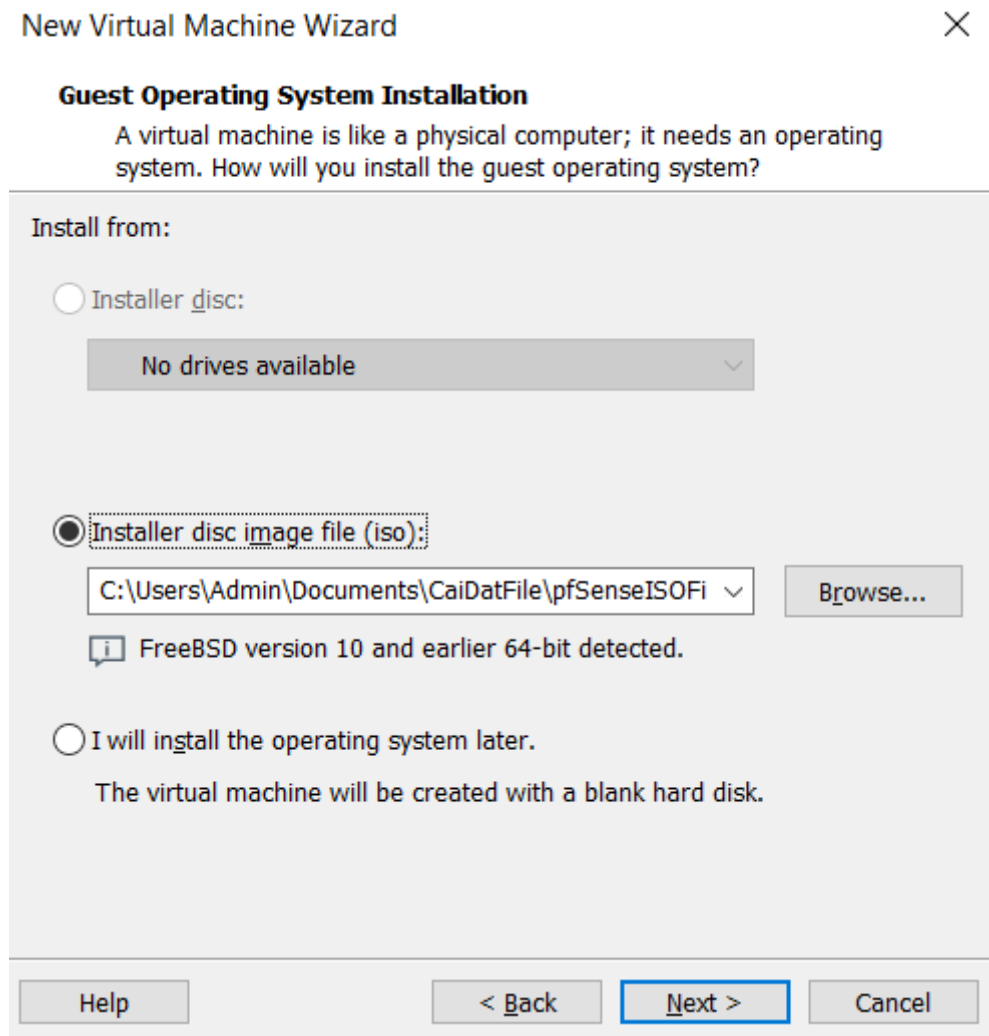
- Tạo máy ảo Pfsense

- Chọn File -> New Virtual Machine -> Typical



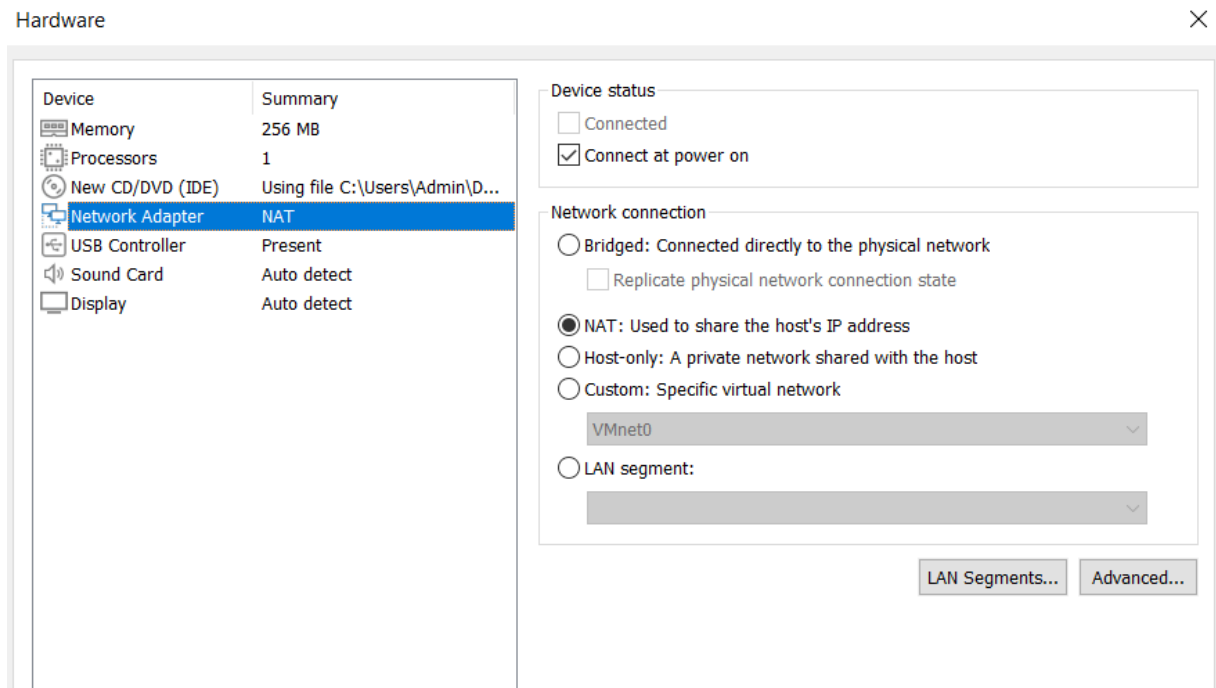
Hình 4.3 Màn hình cài đặt máy ảo trên VMware

- Chọn thư mục chứa file ISO của Pfsense



Hình 4.4 Màn hình tùy chọn file ISO

- Chọn Network Adapter, chọn mạng mà mặc định đang là NAT



Hình 4.5 Giao diện cài đặt các thiết bị trên máy pfSense










- Chọn Add -> Network Adapter -> Finish. Ở mạng thứ hai này, ta sẽ chọn Host-only
- Đóng giao diện Customize lại -> Chọn Power on this Virtual machine after creation -> Finish
- Sau đó máy sẽ chạy Pfsense, chọn đồng ý với các điều khoản -> Install -> Continue with default key map -> Auto (UFS) BIOS -> OK -> NO -> Reboot. Giữa các bước sẽ có thời gian đợi khác nhau, sau khi xong sẽ hiện lên giao diện Pfsense trên máy ảo.

FreeBSD version 10 and earlier 64-bit

 Resume this virtual machine

 Edit virtual machine settings

▼ Devices

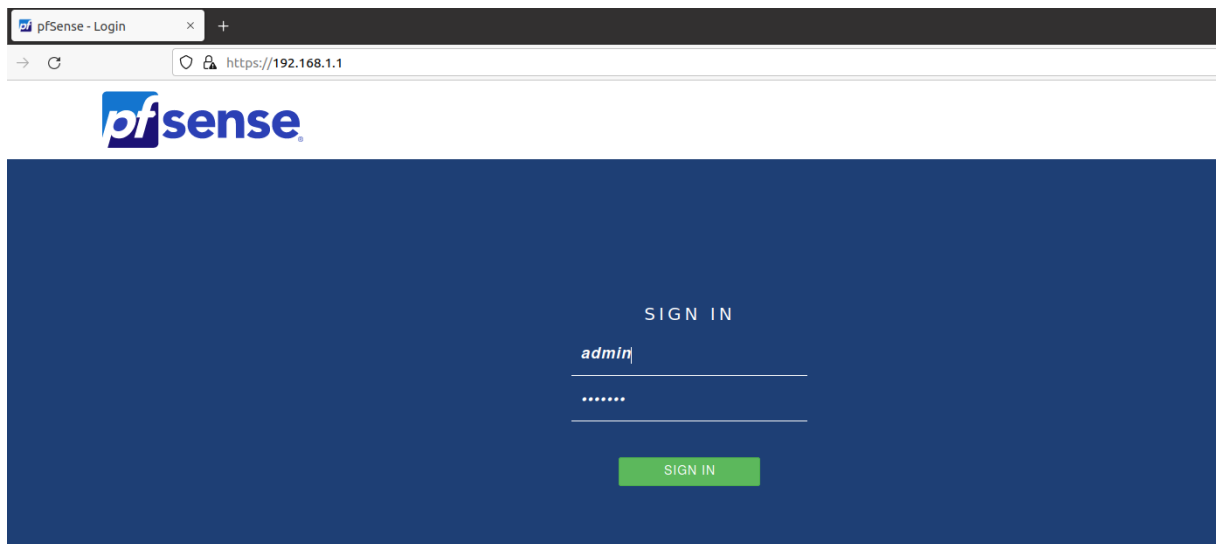
 Memory	2 GB
 Processors	1
 Hard Disk (SCSI)	20 GB
 CD/DVD (IDE)	Using file D:\pfS...
 Network Adapter	NAT
 Network Adapter 2	Host-only
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

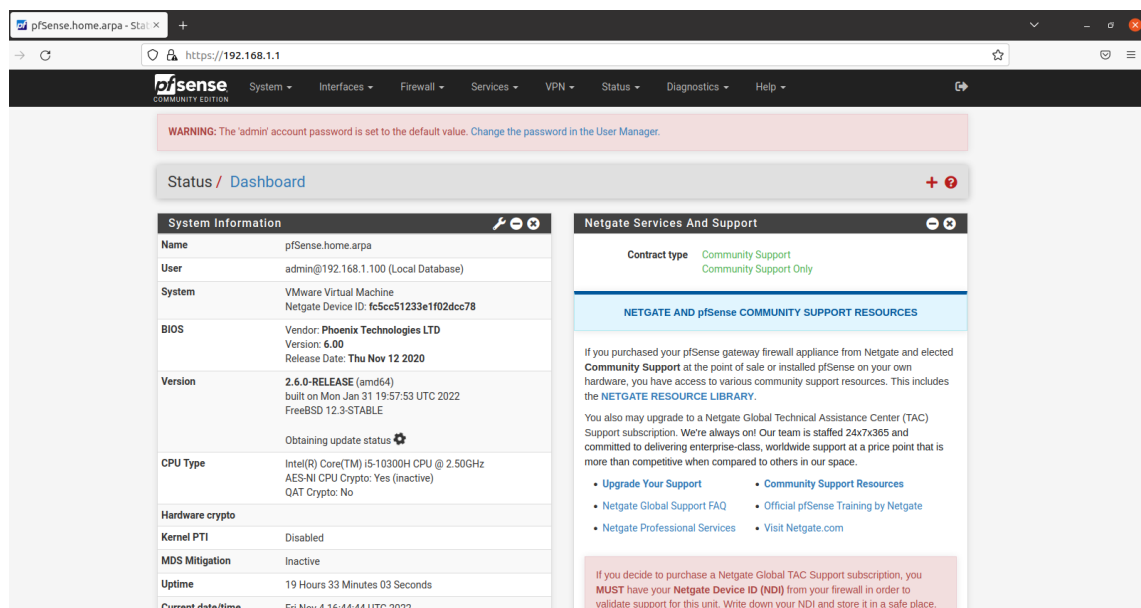
Hình 4.6 Giao diện máy pfSense sau khi cài đặt với 2 card mạng

- Sau khi cài đặt xong máy pfSense ta chỉ cần chạy máy ảo, sau đó chúng ta sử dụng máy Ubuntu đã chuẩn bị trước với một card mạng có kết nối host-only như trên để truy cập vào được dẫn <https://192.168.1.1/> đường dẫn này sẽ dẫn ta đến trang GUI của máy pfSense để ta có thể dễ dàng thiết lập các cài đặt cần thiết



Hình 4.7 Màn hình đăng nhập trên GUI của pfSense

- Tài khoản là admin và mật khẩu là pfsense
- Khi mới vào lần đầu sẽ có các bước Set up, chọn mặc định toàn bộ đến bước 6 thì có thể đổi mật khẩu vào Web GUI -> Chọn các lựa chọn mặc định đến khi xong sẽ hiện ra như sau



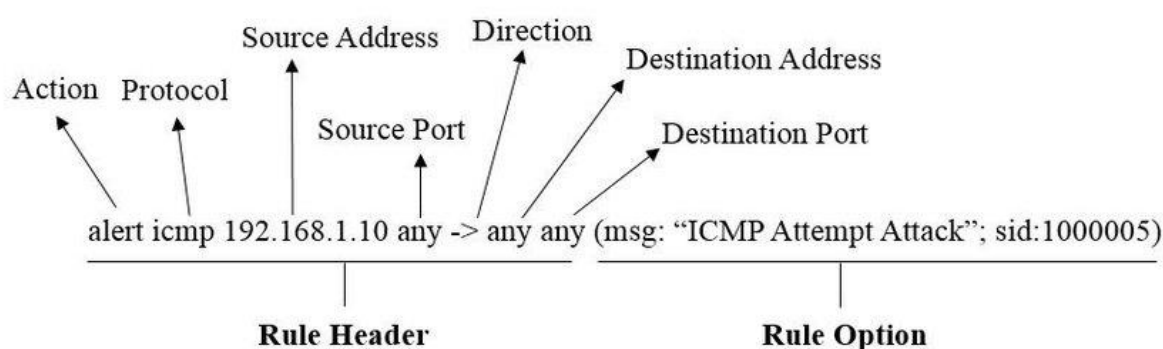
Hình 4.8 Giao diện Dashboard của pfSense

- Cài đặt VMWare tool, chọn System -> Packet manager -> Available Packages -> Gõ vmware tool -> Search -> Install

4.2.Cấu hình hệ thống (Snort)

- Tương tự như bước trên ta vẫn vào phần Available Package và gõ Snort sau đó install snort

- Sau khi đã có snort, ta sẽ bắt đầu cài đặt các rule cho snort. Rule trong IDS/IPS được thiết kế để xác định các tình huống xảy ra trên hệ thống mạng nào cần được phát hiện, ghi lại và chặn khi cần thiết, rule trong IDS/IPS được viết theo một quy luật chung đó là sự kết hợp giữa 2 phần header và options



Hình 4.9 Cấu trúc rule của IDS/IPS

- Phần header gồm:

+ Action: Hành động được thực thi khi mọi điều kiện phía sau nó thỏa mãn và đáp ứng được yêu cầu của Rule

+ Protocol: Xác định giao thức khi một gói tin được truyền trong môi trường mạng, các giao thức được sử dụng như TCP, UDP, ICMP,...

+ Address: Bao gồm Source Address và Destination Address (Địa chỉ nguồn và địa chỉ đích), các địa chỉ này thường là địa chỉ của một host, nhiều host hoặc là địa chỉ mạng

+ Port: Phần này được áp dụng khi phần protocol trên là TCP hoặc UDP để xác định cổng nguồn và cổng đích của mọi gói tin, trường hợp các giao thức khác thì phần này không có ý nghĩa

+ Direction: Xác định địa chỉ và cổng nào được sử dụng làm cổng đích hay cổng nguồn

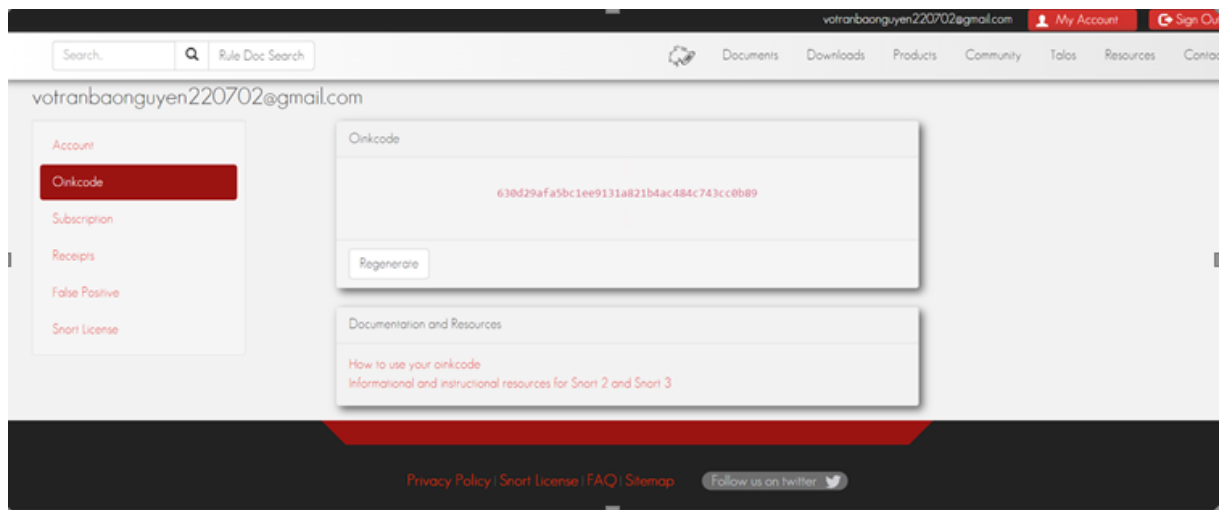
- Phần option là phần theo sau phần header, được đóng gói trong dấu ngoặc đơn, có thể có một hoặc nhiều option, mỗi option sẽ được phân cách nhau bằng dấu chấm phẩy. Khi có từ 2 option trở lên thì các option này sẽ hình thành phép logic AND, tức là Action của rule chỉ có thể thực hiện khi tất cả các option đều thỏa mãn. Thông thường các option sẽ có 2 phần là từ khóa và đối số, được phân cách với nhau bằng dấu hai chấm, ví dụ một option phổ biến: *msg: "Ping detected"*

- Thực tế Snort đã cung cấp cho ta rất nhiều bộ Rule được viết sẵn và ta chỉ cần cài đặt chúng như sau: Vào snort, chọn Global settings

Hình 4.10 Giao diện Global Settings của Snort

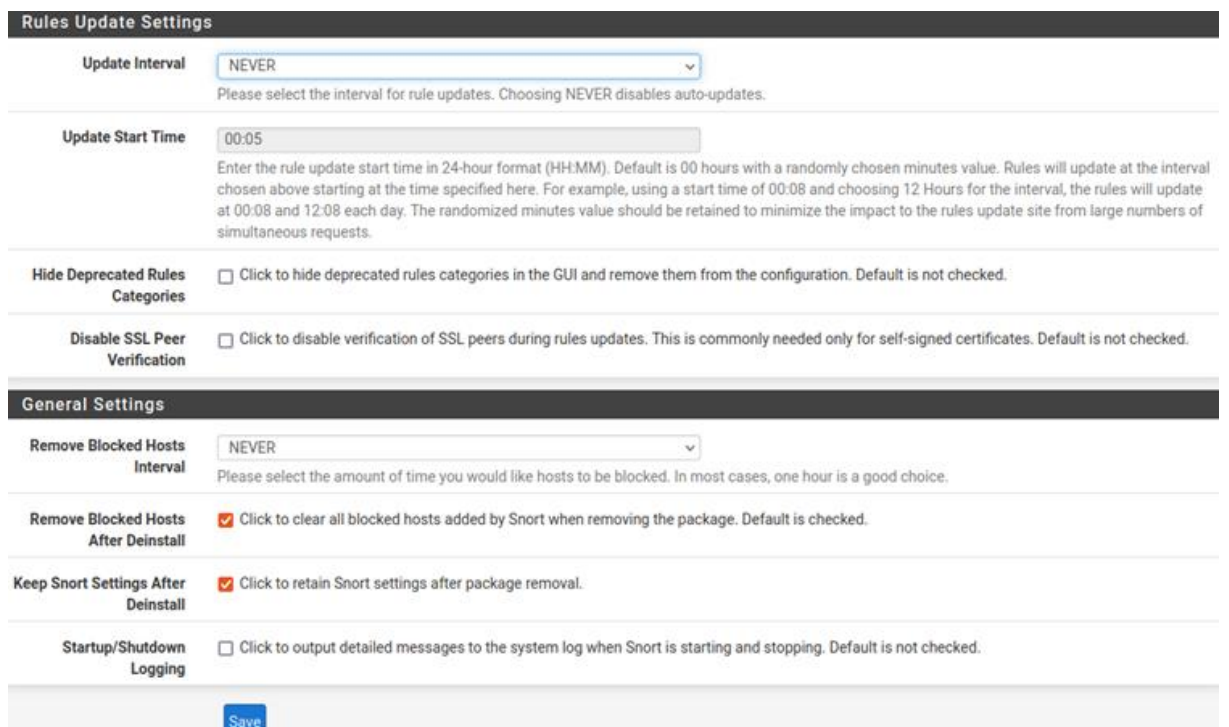
- Ở đây ta thấy có khá nhiều bộ Rules dành cho snort, trừ bộ Snort Subscriber Rules, các bộ Rules khác ta chỉ cần tích vào ô Click to enable

- Đối với bộ Snort Subscriber Rules, ta cần vào trang chủ của snort, tạo tài khoản, sau đó đăng nhập, vào phần My account, chọn phần Oinkcode sau đó sao chép dòng mã đó và dán vào phần Snort Oinkmaster Code trên GUI và tích vào Click to enable



Hình 4.11 Giao diện phần Oinkcode trên trang web của snort

- Ở phần Rules Update Settings Ta thay Update Interval thành NEVER, sau đó chọn save để lưu những thay đổi vừa rồi.



Hình 4.12 Phần cuối của giao diện Global Settings

- Tiếp theo, ta chọn phần Updates phía trên, ở phần Update Your Rule Set, chọn Update Rules và đợi cho tới khi Rules được Update thành công và phần Result hiện Success, lúc này ta đã thành công tải các bộ Rules về để sử dụng.

The screenshot shows the 'Updates' tab in the Snort configuration interface. It displays a table of installed rule sets and their MD5 signatures. Below the table, there is a section for 'Update Your Rule Set' showing the last update time and a successful result. There are buttons for 'Update Rules' and 'Force Update'.

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	fc82fafafadab30ae4f479ac8e69c2e65	Sunday, 27-Nov-22 06:24:21 UTC
Snort GPLv2 Community Rules	84fa18ed94d9583a3196efccd0418400	Sunday, 27-Nov-22 06:24:21 UTC
Emerging Threats Open Rules	8d85bb407dfa3a0b79e9f4b6c9fa434d	Sunday, 27-Nov-22 06:24:23 UTC
Snort OpenAppID Detectors	fb164dfe992d6022740a6b390d51765	Friday, 04-Nov-22 01:31:37 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Friday, 04-Nov-22 01:31:37 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Nov-28 2022 03:09 Result: **Success**

Update Rules: [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Hình 4.13 Giao diện phần Updates dùng để Update tải lên các bộ Rules

- Sau khi Update Rules xong, ta vào phần Snort Interfaces, nếu chưa có bất kì Interface nào, ta thực hiện tạo một interface mới bằng cách nhấn nút Add, sau đó giao diện tạo Interface sẽ hiện ra.

The screenshot shows the 'Snort Interfaces' tab in the Snort configuration interface. It displays a table of existing interfaces. Below the table, there is a section for 'Add Interface' with a form for creating a new interface. The form includes fields for 'Interface', 'Description', and 'Snap Length'.

Interface	Description	Snap Length
LAN (em1)	LAN	1518

Add Interface

General Settings

Enable: ☒ Enable interface

Interface: Choose the interface where this Snort instance will inspect traffic.

Description: Enter a meaningful description here for your reference.

Snap Length: Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Hình 4.14 Giao diện thêm Interface ở phần Snort Interface

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 4b112ed913d7ab0bb166
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.56.138/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

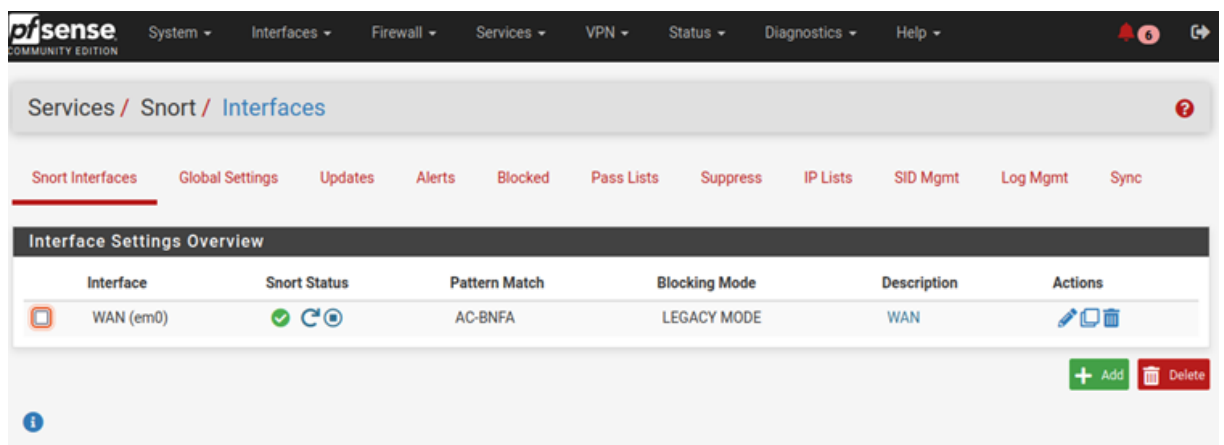
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Nov 28 02:17:39 ...
php-fpm[358]: /snort/snort_alerts.php: Successful login for user 'admin' from: 1
92.168.1.103 (Local Database)
```


Hình 4.15 Giao diện của máy pfSense (Với 2 địa chỉ mạng mà ta đã cài đặt từ trước)

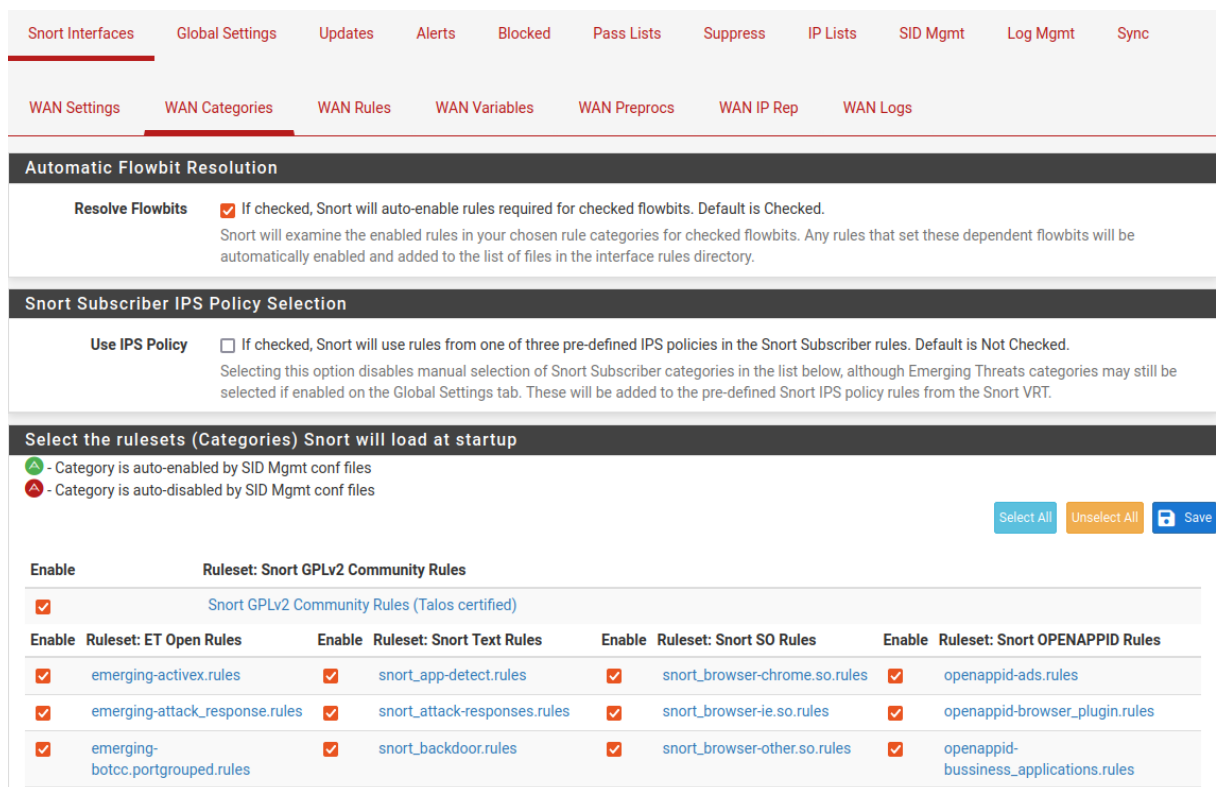
- Trong phần General Settings, phần interface ta chọn, loại mạng có cùng địa chỉ mạng với máy Kali mà ta chuẩn bị sử dụng, Ở đây ta chọn Wan(em0) với địa chỉ là 192.168.56.138. Sau đó ta kéo xuống cuối và chọn save.

- Sau khi hoàn thành xong ta sẽ có một interface như sau:



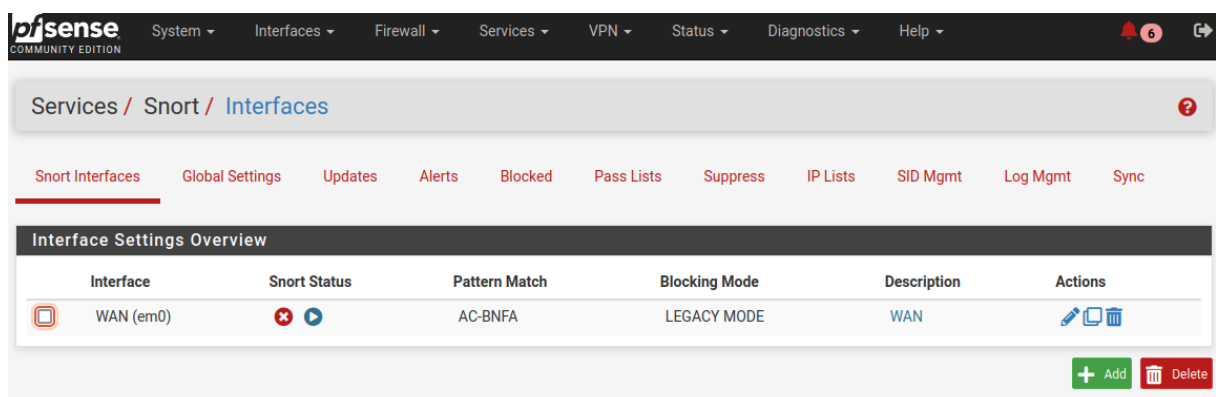
Hình 4.16 Giao diện Snort Interface sau khi thêm một interface mới

- Tiếp theo ta nhấn vào biểu tượng  và ta sẽ được đưa đến giao diện thiết lập cho interface, ở đây, ta chọn phần Wan Categories.



Hình 4.17 Giao diện thiết lập interface ở phần WAN Categories

- Ở phần Select the rulesets ta chọn Select All, sau đó Save, như vậy ta đã cập nhật các rule mà ta đã Update lúc đầu lên Interface. Sau đó ta chọn lại phần Snort Interfaces để quay về và bắt đầu chạy interface.



Hình 4.18 Snort status của interface khi chưa được khởi động

- Nhấn vào nút và đợi cho tới khi phần Snort Status chuyển sang là ta đã thành công chạy được snort trên hệ thống pfSense.

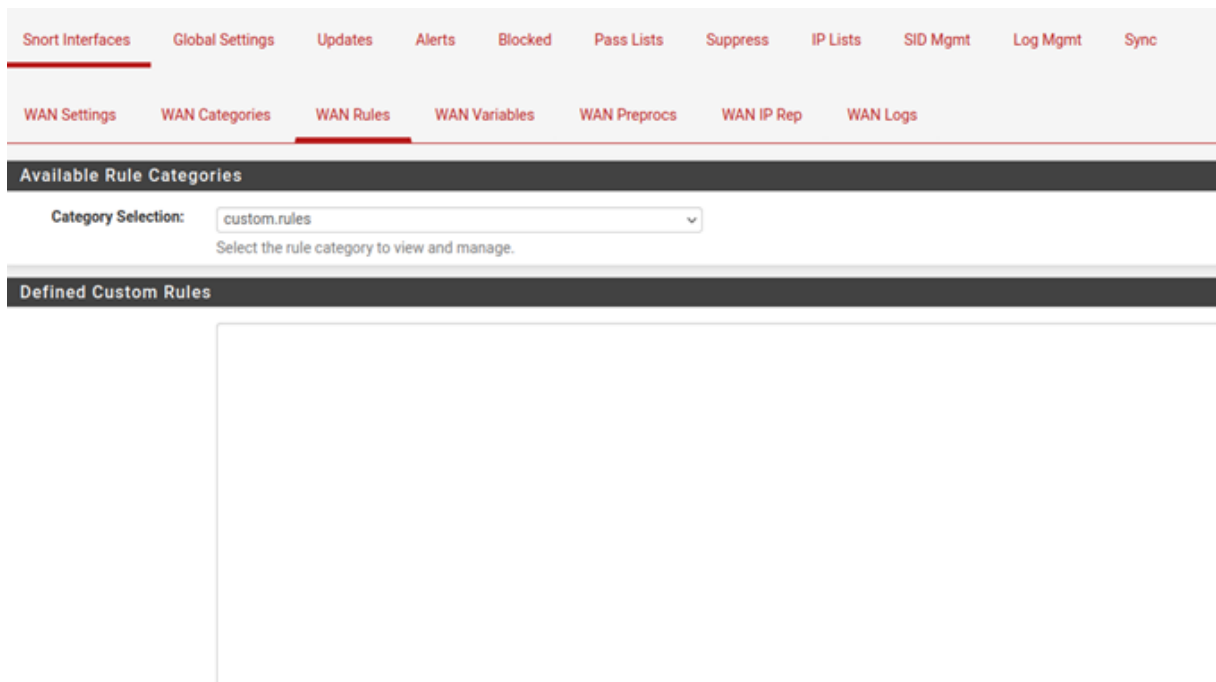
5. Kiểm thử hệ thống

5.1 Bảng các tình huống kiểm thử

STT	Tình huống	Mục đích
1	Cho máy Ubuntu ping tới máy Kali và sử dụng IDS/IPS (Snort) để tìm và phát hiện địa chỉ IP của 2 máy	Từ cấu trúc Rule cơ bản của IDS/IPS viết được một Rule có thể phát hiện hành động ping của các máy trên môi trường mạng
2	Thực hiện tấn công DoS từ máy Kali (Denial-of-Service) vào Router pfSense với địa chỉ IP server đã đặt là 192.168.1.1	Kiểm tra được Rules đã được tải ở phần đầu đã hoạt động đồng thời kiểm tra được khả năng ngăn chặn của snort (IPS)

5.1.Thực hiện tình huống 1

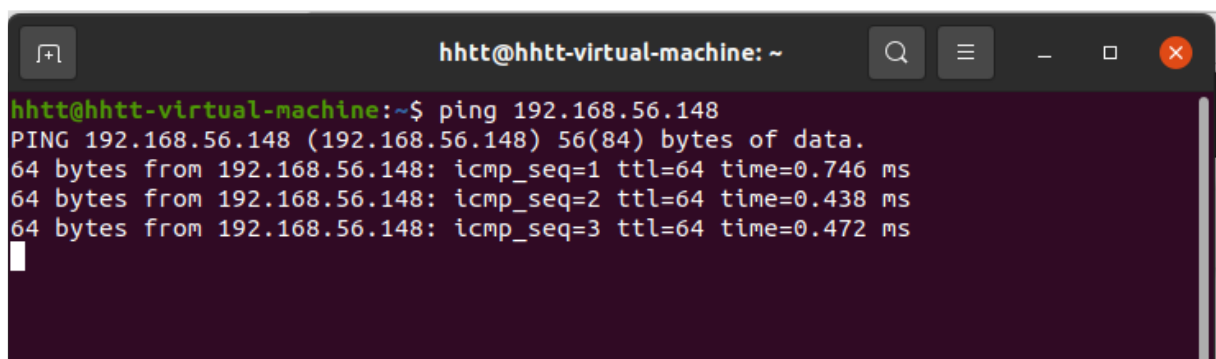
- Thiết lập snort rule bằng cách vào phần thiết lập cho interface và chọn mục WAN Rules, tại đây ở mục Available Rule Categories ta chọn mục Custom rule.



Hình 5.1 Giao diện tạo custom rule cho Snort trên GUI

- Tại phần Defined Custom Rules, ta sẽ thực hiện tạo Rule tại đây, nội dung rule như sau: `alert icmp any any -> any any (msg: "Ping detected"; sid: 1000001;)`. Ở đây **Action** được chọn là **alert**, phần **Protocol** được chọn là giao thức icmp (Internet Control Message Protocol), Address và port sẽ là any, còn lại phần **Option** sẽ chỉ có **msg** và **sid**

- Sau khi đã nhấn Save, ta sẽ thực hiện thử nghiệm bằng cách sử dụng lệnh ping từ máy **Ubuntu** với địa chỉ IP là **192.168.56.149** đến máy **Kali** với địa chỉ là **192.168.56.148**



Hình 5.2 Màn hình terminal của máy Ubuntu thực hiện ping

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

234 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-11-29 02:20:54		0	ICMP		192.168.56.2		192.168.56.138		1:1000001	Ping detected
2022-11-29 02:20:54		0	ICMP		192.168.56.138		192.168.56.2		1:1000001	Ping detected
2022-11-29 02:20:53		0	ICMP		192.168.56.148		192.168.56.149		1:1000001	Ping detected
2022-11-29 02:20:53		0	ICMP		192.168.56.149		192.168.56.148		1:1000001	Ping detected

Hình 5.3 Danh sách các thông báo phát hiện thành công các hoạt động sử dụng giao thức ICMP

- Ping thành công, và khi kiểm tra bảng Alert Log ta cũng sẽ thấy có hai dòng Alert có Source IP và Destination IP đúng với hai máy ta chọn, nhưng ngoài ra ta vẫn còn 2 dòng Alert khác ở đầu, vì ta đang thử nghiệm trên giao thức ICMP và ta cũng có một địa chỉ IP là **192.168.56.138** đây là địa chỉ của Router pfSense mà ta đang sử dụng, vì thế nên chúng ta cũng bắt được gói tin đó

5.2. Thực hiện tình huống 2

- Thực hiện bật chế độ Block trên Snort, chế độ này sẽ giúp ta thực hiện chức năng IPS của snort bằng cách xem xét các Alert xuất hiện và chặn địa chỉ nguồn hoặc địa chỉ đích (Hoặc cả hai) nằm trong Alert đó.

Alert Settings	
Send Alerts to System Log	<input type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures	<input type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable Unified2 Logging	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.
Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	<div>Legacy Mode</div> <p>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</p> <p>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</p>
Kill States	<input type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	<div>SRC</div> <p>Select which IP extracted from the packet you wish to block. Default is BOTH.</p>

Hình 5.4 Giao diện cài đặt Block ở phần WAN Setting

- Tại phần WAN Setting trong phần thiết lập cho interface, ta sẽ thấy phần Block Settings, ở đây ta tích vào ô Block Offender, và phía dưới ta để mục IPS Mode ở Legacy Mode và chỉnh mục Which IP to Block thành SRC để chỉ chặn mỗi IP của máy gây ra tấn công. Cuối cùng ta lưu lại cài đặt

- Tiếp theo ta thử nghiệm ping từ máy server tới máy Kali với địa chỉ IP 192.168.56.148 trước khi tấn công, ta thấy được quá trình ping đã thành công

```

Enter a host name or IP address: 192.168.56.148

PING 192.168.56.148 (192.168.56.148): 56 data bytes
64 bytes from 192.168.56.148: icmp_seq=0 ttl=64 time=1.029 ms
64 bytes from 192.168.56.148: icmp_seq=1 ttl=64 time=0.717 ms
64 bytes from 192.168.56.148: icmp_seq=2 ttl=64 time=0.702 ms

--- 192.168.56.148 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.702/0.816/1.029/0.151 ms

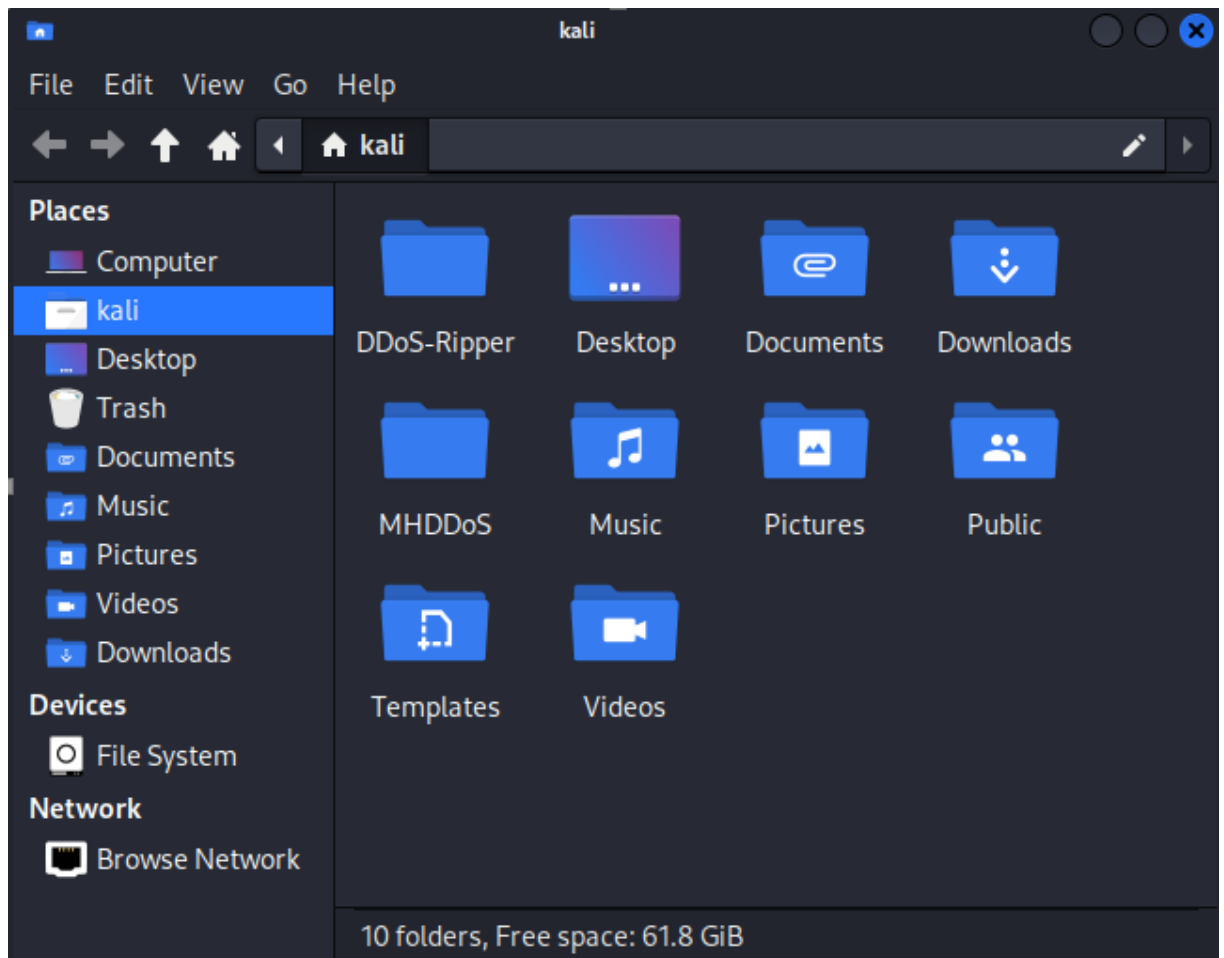
Press ENTER to continue.

```

Hình 5.5 Màn hình ping trước khi từ máy pfSense đến máy Kali

- Thực hiện cài đặt tool **DDoS-Ripper** đây là một tool được viết bằng ngôn ngữ Python giúp thực hiện tấn công DoS lên một server có địa chỉ nhất định, khi chạy tool sẽ xác nhận địa chỉ server và port ta muốn tấn công, sau đó tool sẽ

thực hiện gửi một loạt các yêu cầu lên server đó tại port đã chỉ định. Tool không thực sự ngăn chặn việc sử dụng tài nguyên nhưng đủ để snort phát hiện được và thông báo lỗi cũng như chặn địa chỉ IP của máy chạy tool đấy trên server.



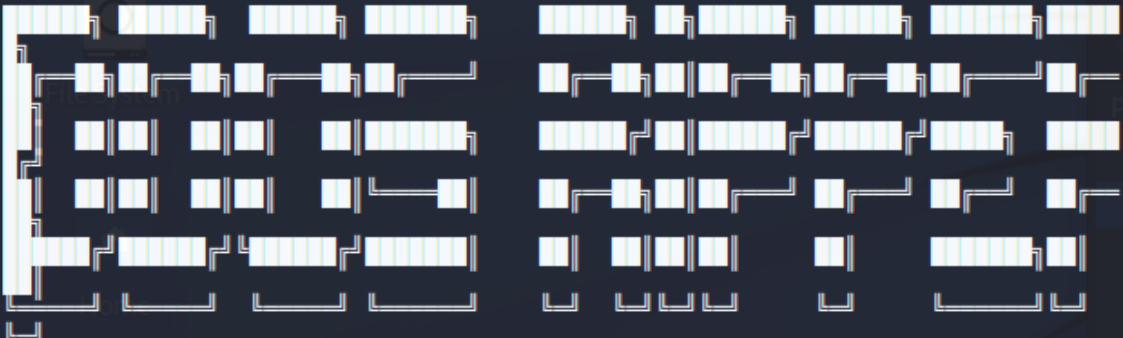
Hình 5.6 Nơi chứa thư mục DdoS-Ripper dùng để thực hiện tấn công DoS

- Sử dụng link github: <https://github.com/palahsu/DDoS-Ripper.git> và Clone folder về máy Kali, sau đó ta mở terminal từ thư mục DDoS-Ripper ở đây để thực hiện tấn công ta sẽ chạy dòng lệnh sau: `python3 DRipper.py -s 192.168.1.1` ở đây 192.168.1.1 là địa chỉ Server (Router pfSense)

```

(kali㉿kali)-[~/DDoS-Ripper]
$ python3 DRipper.py -s 192.168.1.1

```



```

mmmer

192.168.1.1 port: 80 turbo: 135
Please wait...
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→
Mon Nov 28 22:07:37 2022 ←packet sent! rippering→

```

©EngineRipper
reference by Ha

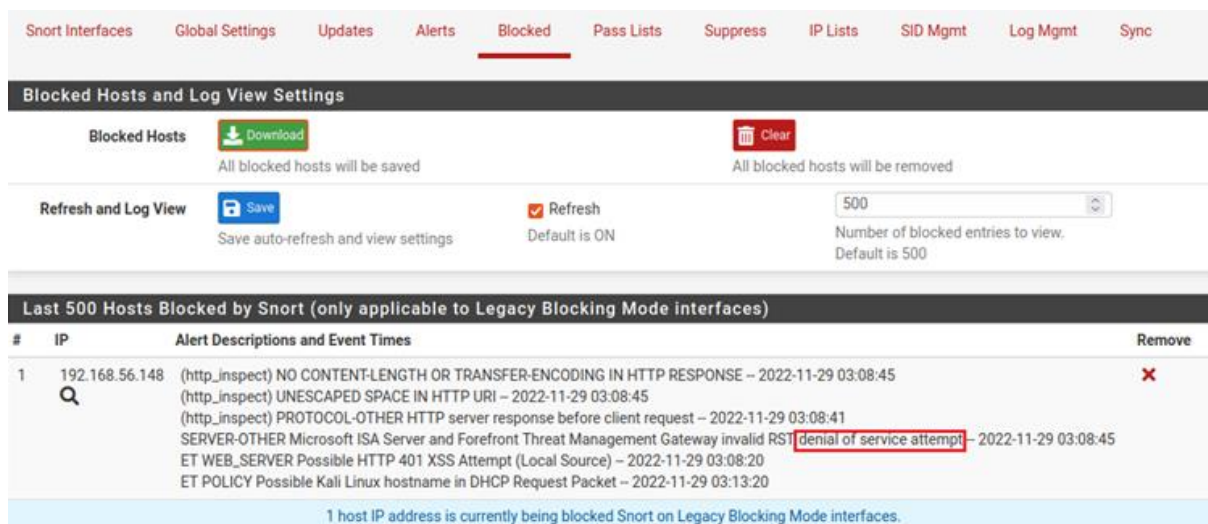
Hình 5.7 Màn hình Terminal khi đang trong quá trình thực hiện tấn công DoS

- Thực hiện kiểm tra Alert Log ta thấy được các log hiển thị *Unknown Traffic* là lúc server đang nhận các packet được gửi, và có một log hiển thị *Attempted Denial of Service* tức là Snort đã phát hiện được đây là tấn công DoS.

2022-11-29 03:08:45	3	TCP	Unknown Traffic	192.168.56.148 58012	192.168.1.1 80	119.33	(http_inspect) UNESCAPED SPACE IN HTTP URI
2022-11-29 03:08:45	3	TCP	Unknown Traffic	192.168.1.1 80	192.168.56.148 58012	120.3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2022-11-29 03:08:45	3	TCP	Unknown Traffic	192.168.56.148 58000	192.168.1.1 80	119.33	(http_inspect) UNESCAPED SPACE IN HTTP URI
2022-11-29 03:08:45	2	TCP	Attempted Denial of Service	192.168.56.148 58000	192.168.1.1 80	3:15474	SERVER-OTHER Microsoft ISA Server and Forefront Threat Management Gateway invalid RST denial of service attempt

Hình 5.8 Danh sách một số Alert thu được sau khi cuộc tấn công bắt đầu

- Kiểm tra phần Block ta cũng sẽ thấy được Snort đã chặn địa chỉ IP 192.168.56.148 của máy Kali với một loạt các Alert Description đã xuất hiện bên bảng Alert và trong đó có một Alert liên quan tới DoS



Hình 5.9 Giao diện hiển thị các IP đã bị chặn và các chi tiết các Alert liên quan

- Thực hiện ping lại từ máy pfSense một lần nữa ta thấy được là ta sẽ không thể ping tới máy Kali với địa chỉ IP 192.168.56.148 được nữa và sẽ hiện ra là *Permission denied*.

```

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: 7

Enter a host name or IP address: 192.168.56.148

ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
PING 192.168.56.148 (192.168.56.148): 56 data bytes

--- 192.168.56.148 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss

Press ENTER to continue.

```

Hình 5.10 Ping thất bại sau khi đã tấn công và Snort đã thực hiện chặn địa chỉ IP

6. Kết luận

6.1. Mục tiêu đạt được

- Thông qua quá trình thực hiện đề tài này, nhóm đã có một cái nhìn tổng quan về *Hệ thống phát hiện và phòng chống xâm nhập*, hay còn gọi là *IDS & IPS*. Nắm bắt được các định nghĩa, cách phân loại, các thuật toán đã và đang sử dụng, các mô hình kiến trúc và cơ sở hạ tầng của *IDS & IPS* một cách rõ ràng, thấu đáo.

- Vận dụng được những kiến thức đã đạt được về *Hệ thống phát hiện và phòng chống xâm nhập* để bắt tay vào việc mô phỏng chúng thông qua các công cụ, phần mềm, giả lập thích hợp, thực hiện các bài Lab liên quan tới chủ đề này. Từ đó rút ra được nhiều kinh nghiệm quý báu cho việc tạo dựng một hệ thống *IDS & IPS*.

- Trong quá trình làm đề tài, ngoài những kiến thức về chuyên ngành mà nhóm đã đạt được như đã nói trên thì còn học được thêm những kỹ năng mềm cần thiết như khả năng làm việc nhóm, cách để chia sẻ ý kiến của bản thân cũng như tiếp thu kiến thức từ những người đồng hành, cách phân chia công việc phù hợp, kỹ năng chọn lọc thông tin, cách tổ chức quy trình cho việc thực hiện một đồ án.

6.2. Đánh giá ưu và nhược điểm của sản phẩm

6.2.1. Ưu điểm

- Hệ thống sở hữu các tính năng hữu ích cho việc phát hiện và phòng chống xâm nhập, có một cấu trúc rõ ràng, mang hình dáng chuẩn chỉ của một *IDS & IPS*.

- Hệ thống có thể phát hiện, ngăn chặn những tấn công thông thường, phổ biến và vẫn có thể tiếp tục được cấu hình sâu hơn với những tấn công phức tạp bằng khả năng tùy chỉnh Rules cực kỳ mạnh mẽ.

6.2.2. Nhược điểm

- Quy mô và độ phức tạp của hệ thống là chưa đủ lớn cho một hệ thống phòng thủ mạng.

- Phần mềm, công cụ mà nhóm triển khai chỉ mang tính thử nghiệm, giả lập và không thể áp dụng vào thực tế khi mà những cuộc tấn công vào hệ thống cực kỳ mãnh liệt và khó đoán.

6.3.Những hạn chế gặp phải của nhóm

Trong quá trình thực hiện đề tài, nhóm đã gặp những khó khăn tiêu biểu như

- *Vấn đề về tài liệu:* tài liệu về những đề tài chuyên ngành cơ bản là rất khó để tìm kiếm. Chính xác hơn là với sự phát triển của Internet thì khả năng truy cập tới các tài liệu đã mở rộng hơn rất nhiều so với lúc trước, tuy nhiên mặt trái của nó là sẽ có rất nhiều những tài liệu có thông tin không chính xác hoặc chưa được kiểm chứng. Hơn hết, Công nghệ nói chung và Mạng/ An ninh mạng nói riêng luôn luôn được cập nhật, cải tiến mỗi ngày với tốc độ rất cao, thế nên cho dù tìm được tài liệu chuẩn chỉ thì vẫn có thể không dùng được do đã quá lỗi thời với thực tế, việc áp dụng chúng là vô tác dụng. Vì vậy một kỹ năng chọn lọc thông tin là cực kỳ cần thiết.

- *Vấn đề về khả năng và kinh nghiệm thực tiễn:* Đây chính là lần đầu nhóm bắt tay vào thực hiện một đề tài về chuyên đề Mạng và An ninh mạng vì thế kinh nghiệm về việc xây dựng một hệ thống như là IDS & IPS gần như là con số không. Nhóm phải bắt đầu tìm hiểu từ nền tảng, những thứ cơ bản nhất rồi nâng cấp lên từ từ để có thể thực hiện đề tài.

- *Những lỗi phát sinh của công cụ, phần mềm dùng để thực hành:* Mặc dù đã chọn lọc kỹ càng, thực hiện đầy đủ các quy trình thì những phần mềm vẫn phát sinh những lỗi không mong muốn, bug và glitch tràn lan trên các công cụ. Đa phần những lỗi phát sinh là do sự mâu thuẫn giữa tài liệu và phần mềm trên thực tế, chủ yếu là chúng khác phiên bản hoặc tác giả phiên bản mới đã ngưng không viết tài liệu nữa.

6.4.Định hướng phát triển

Thông qua đề tài, nhóm đã tương đối nắm bắt được về IDS & IPS trên môi trường giả lập, vì thế định hướng của nhóm sẽ là triển khai chúng trên thực tế, nâng cấp quy mô lẫn độ phức tạp của hệ thống, biến chúng thành một thứ có thể vận dụng được vào cuộc sống, vào công việc hàng ngày chứ không đơn thuần chỉ là các thí nghiệm và lý thuyết giản đơn.

7. TÀI LIỆU KHAM THẢO

- “Intrusion Detection Systems” by “Przemyslaw Kazienko Piotr Dorosz”.

<https://techgenix.com/intrusion-detection-systems-ids-part-i-network-intrusions-attack-symptoms-ids-tasks-and-ids-architecture/>

- Install Snort on Linux-Ubuntu.

<https://linuxopsys.com/topics/install-snort-on-ubuntu>

- Sử dụng Pfsense.

https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html?fbclid=IwAR2ce_rBQ08_XQZwrsaCD8fQAgCywIG6VHkqbFTzW3yoJ5x_NuRsC4nn1FM#launching-snort-configuration-gui

- Và nhiều nguồn đa dạng khác trên Internet.