TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT

VIỆN ĐÀO TẠO CÔNG NGHỆ THÔNG TIN-CHUYỂN ĐỔI SỐ

BÁO CÁO MÔN HỌC AN TOÀN BẢO MẬT THÔNG TIN

TÌM HIỂU VÀ THỬ NGHIỆM PHÒNG CHỐNG TẤN CÔNG DOS DỰA TRÊN ỨNG DỤNG IPFIRE

GVHD: Ths. Lê Từ Minh Trí

SVTH: Nhóm 5

1. **Nguyễn Hữu Nghĩa – 2124802050013**
2. **Lục Tấn Khoa – 21248020500**

Bình Dương 03/12/202

TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT

VIỆN ĐÀO TẠO CÔNG NGHỆ THÔNG TIN-CHUYỂN ĐỔI SỐ

BÁO CÁO MÔN HỌC AN TOÀN BẢO MẬT THÔNG TIN

TÌM HIỂU VÀ THỬ NGHIỆM PHÒNG CHỐNG TẤN CÔNG DOS DỰA TRÊN ỨNG DỤNG IPFIRE

GVHD: Ths. Lê Từ Minh Trí

SVTH: Nhóm 5

1. **Nguyễn Hữu Nghĩa – 2124802050013**
2. **Lục Tấn Khoa – 21248020500**

Bình Dương 03/12/2024

MỤC LỤC

DANH MỤC HÌNH

CHƯƠNG I. GIỚI THIỆU TỔNG QUAN

1.1. Giới thiệu đề tài

Trong bối cảnh phát triển mạnh mẽ của công nghệ thông tin, an ninh mạng ngày càng trở thành mối quan tâm hàng đầu đối với cá nhân, doanh nghiệp, và các tổ chức. Các cuộc tấn công mạng, đặc biệt là tấn công Từ chối Dịch vụ (Denial of Service - DoS), đang ngày càng gia tăng. Các cuộc tấn công DoS gây thiệt hại nghiêm trọng về kinh tế và làm gián đoạn hoạt động của các hệ thống thông tin quan trọng. Là sinh viên thuộc nhóm ngành công nghệ thông tin, nhóm em nhận thấy rằng việc hiểu rõ bản chất của các cuộc tấn công DoS và nghiên cứu các giải pháp phòng chống là vô cùng cần thiết, đặc biệt trong thời đại mà sự phụ thuộc vào mạng Internet là không thể thiếu. IPFire, một hệ điều hành tường lửa mã nguồn mở, là một công cụ tiềm năng để xây dựng các giải pháp phòng chống tấn công mạng nhờ tính linh hoạt, hiệu suất tốt và chi phí thấp. Tuy nhiên, việc nghiên cứu và thử nghiệm khả năng ứng dụng của IPFire trong phòng chống các cuộc tấn công DoS vẫn chưa được khai thác sâu rộng tại môi trường học thuật. Vì thế nhóm em quyết định chọn đề tài "Tìm hiểu và thử nghiệm phòng chống tấn công DoS dựa trên ứng dụng IPFire" nhằm nâng cáo kiến thức và kỹ năng. Ngoài ra, mong muốn có thể đóng góp một phần vào việc nâng cao nhận thức về an ninh mạng.

1.2. Mục tiêu đề tài

Đề tài tập trung vào việc:

- Tìm hiểu nguyên lý hoạt động của tấn công DoS.

- Thực hành mô phỏng tấn công DoS từ máy Client VM (Kali Linux) đến máy Server VM (Metasploitable2).

- Ứng dụng IPFire làm Firewall VM để phòng chống tấn công và đánh giá hiệu quả.

1.3. Các thành phần thử nghiệm

- Phần mềm VMWare phiên bản 17.5.2

- Client VM: Kali Linux – công cụ thực hiện tấn công.

- Firewall VM: IPFire – tường lửa bảo vệ mạng, ngăn chặn DoS.

- Server VM: Metasploitable2 – máy chủ mục tiêu tấn công.

CHƯƠNG II. TỔNG QUAN VỀ TẤN CÔNG DOS

2.1. Khái niệm về tấn công DoS

Tấn công DoS (Denial of Service) là một kiểu tấn công mạng với mục đích làm gián đoạn hoặc ngăn chặn người dùng hợp lệ truy cập vào tài nguyên hoặc dịch vụ của một hệ thống, máy chủ, hoặc mạng.

2.2. Mục tiêu của tấn công DoS

Làm quá tải hệ thống: Khiến hệ thống không thể xử lý yêu cầu từ người dùng hợp lệ.

Làm gián đoạn dịch vụ: Dịch vụ bị ngừng hoạt động, ảnh hưởng đến hoạt động kinh doanh hoặc trải nghiệm người dùng.

Tạo cơ hội để kẻ tấn công thực hiện các hoạt động độc hại khác (như tấn công xâm nhập).

2.3. Nguyên lý hoạt động

Tấn công DoS hoạt động bằng cách gửi một lượng lớn yêu cầu hoặc gói tin đến mục tiêu để:

Làm cạn kiệt tài nguyên máy chủ: Như CPU, RAM, hoặc dung lượng lưu trữ.

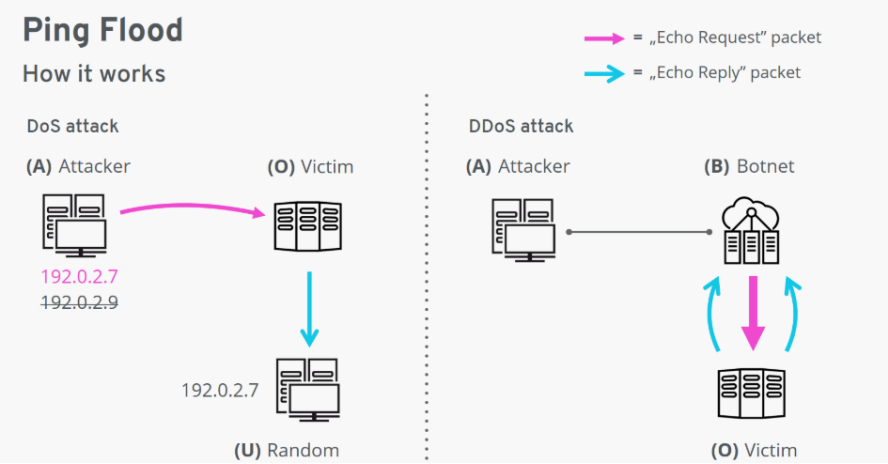
Gây nghẽn mạng: Làm quá tải băng thông, khiến dịch vụ không thể tiếp nhận lưu lượng hợp lệ.

Làm sập hệ thống: Lợi dụng lỗ hổng trong phần mềm hoặc giao thức để gây ra lỗi hệ thống.

2.4. Các loại hình tấn công DoS phổ biến

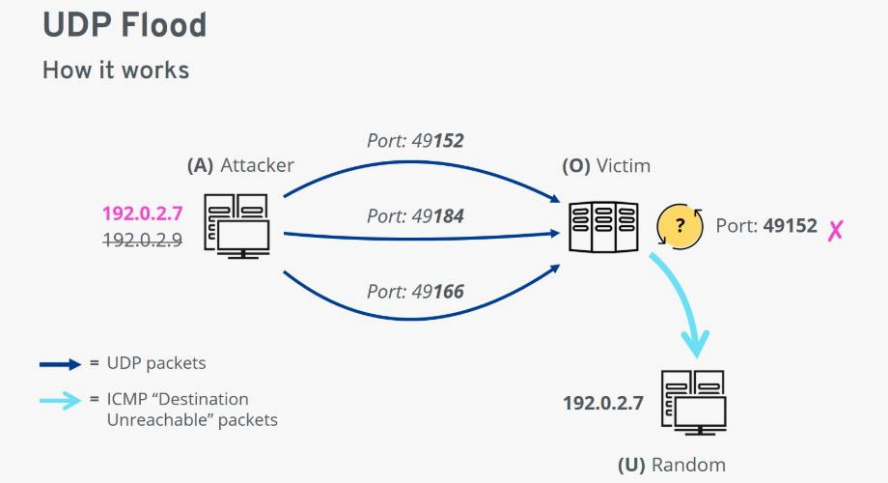
2.4.1. Tấn công dựa trên lưu lượng (Flooding Attack)

ICMP Flood (Ping Flood): Gửi một lượng lớn gói ICMP Echo Request (ping) đến mục tiêu, làm nghẽn băng thông hoặc CPU của máy chủ.



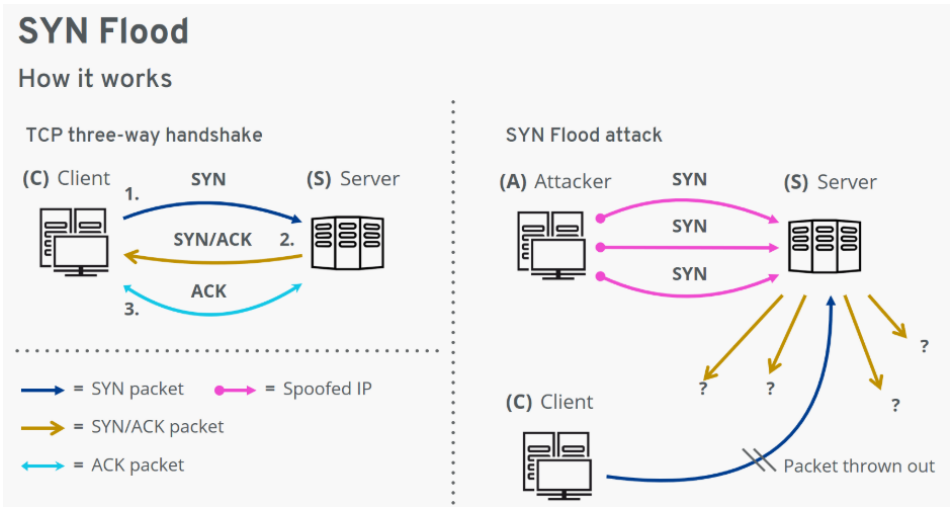
Hình 1: ICMP Flood

UDP Flood: Gửi hàng loạt gói UDP đến các cổng ngẫu nhiên trên máy chủ, khiến máy phải phản hồi và tiêu tốn tài nguyên.



Hình 2: UDP Flood

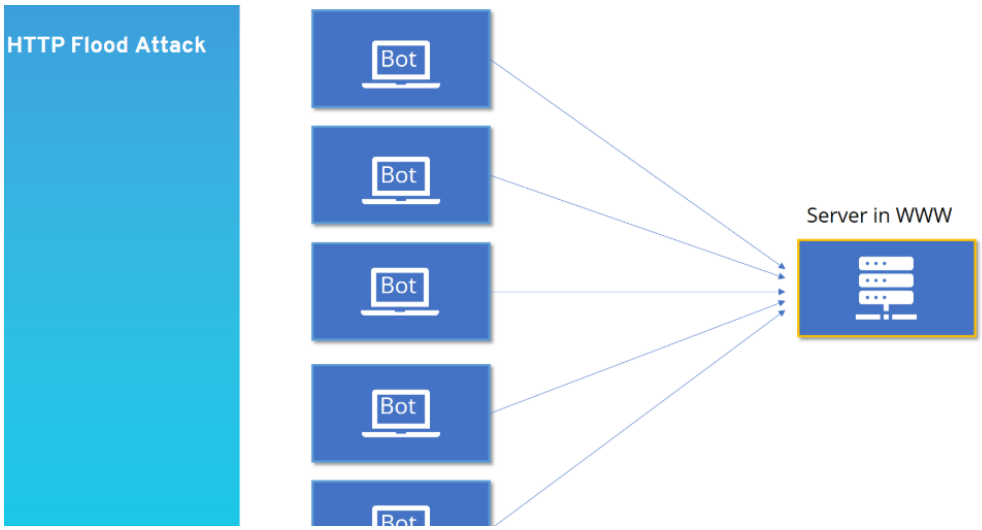
TCP SYN Flood: Gửi một lượng lớn yêu cầu TCP SYN để làm đầy bảng kết nối bán hoàn chỉnh (half-open connection), khiến máy chủ không thể thiết lập kết nối mới.



Hình 3: TCP SYN Flood

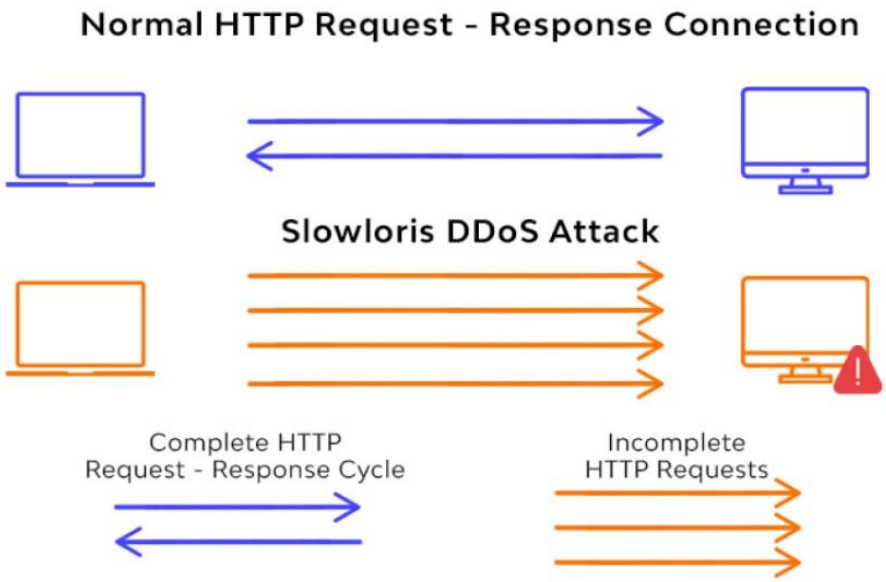
2.4.2. Tấn công ở lớp ứng dụng (Application Layer Attack)

HTTP Flood: Gửi các yêu cầu HTTP giả mạo hoặc dư thừa để làm quá tải máy chủ web.



Hình 4: HTTP Flood

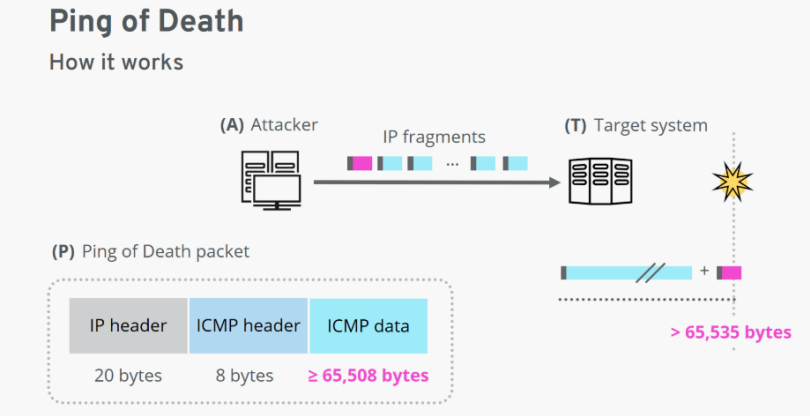
Slowloris: Gửi các yêu cầu HTTP không hoàn chỉnh để giữ kết nối mở lâu nhất có thể, làm cạn kiệt tài nguyên xử lý kết nối.



Hình 5: Slowloris DdoS Attack

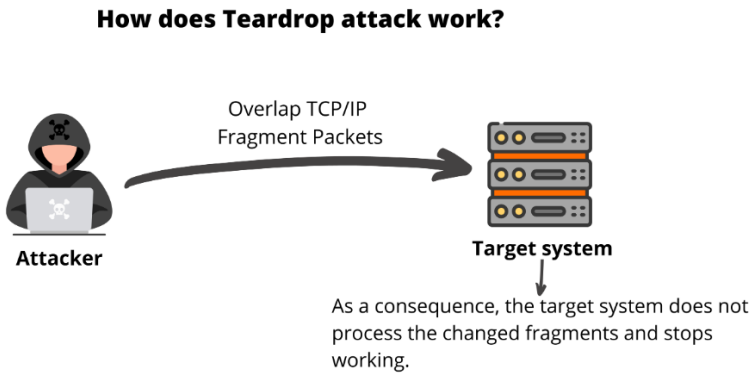
2.4.3. Tấn công khai thác lỗ hổng

Ping of Death: Gửi các gói ICMP quá lớn, vượt quá giới hạn cho phép của giao thức, làm sập hệ thống.



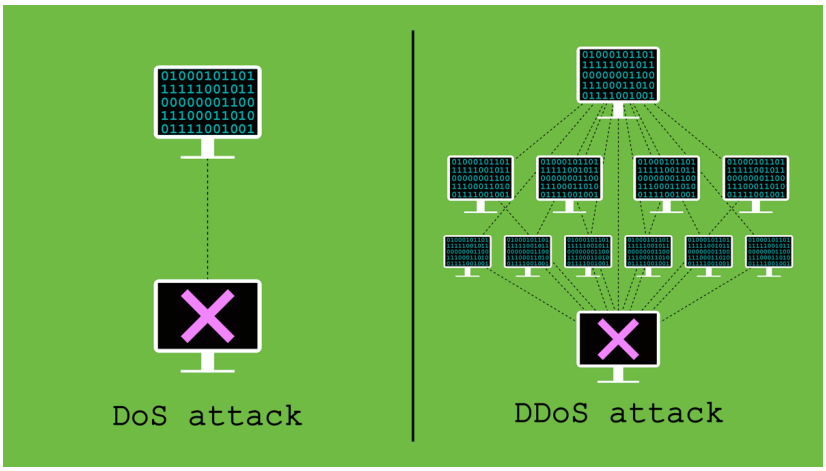
Hình 6: Ping of Death

Teardrop Attack: Gửi các gói tin IP bị phân mảnh không hợp lệ, khiến hệ thống không thể xử lý.



Hình 7: Teardrop Attack

2.5. Phân biệt Dos và DdoS



Hình 8: DoS và DDoS

DoS (Denial of Service): Tấn công từ một nguồn duy nhất.

DDoS (DIstributed Denial of Service): Tấn công từ nhiều nguồn, sử dụng nhiều nguồn tấn công đồng thời, thường là một mạng botnet với hàng ngàn thiết bị bị kiểm soát.

CHƯƠNG III. TỔNG QUAN VỀ IPFIRE

3.1. Giới thiệu về IPFire

IPFire là một hệ điều hành bảo mật mã nguồn mở được thiết kế dành riêng để bảo vệ mạng. Nó chủ yếu hoạt động như một firewall (tường lửa) và có thể được mở rộng để cung cấp các chức năng như VPN, lọc nội dung web, quản lý mạng, và phát hiện xâm nhập (IDS/IPS). IPFire được xây dựng trên nền tảng Linux và được tối ưu hóa để dễ dàng cấu hình, bảo trì và nâng cấp.

3.2. Các tính năng bảo mật của IPFire

3.2.1. Tường lửa (FireWall)

Hình 9: FireWall

- Lọc gói tin: Dựa trên giao thức, địa chỉ IP, cổng, và ứng dụng.
- Hỗ trợ NAT (Network Address Translation): Cấu hình mạng linh hoạt.
- Firewall Rules: Tùy chỉnh quy tắc tường lửa để quản lý lưu lượng truy cập.

3.2.2. Hệ thống phát hiện và ngăn chặn xâm nhập (Intrusion Prevention System-IPS)

- Phát hiện các mẫu lưu lượng đáng ngờ.
- Tự động chặn các cuộc tấn công xâm nhập.
- Cập nhật cơ sở dữ liệu mẫu tấn công thường xuyên.

3.2.3. Quản lý chất lượng dịch vụ (Quality of Service – Qos)

- Ưu tiên lưu lượng hợp lệ hoặc quan trọng.

- Giảm thiểu tác động từ các cuộc tấn công DoS.

3.2.4. Virtual Private Network (VPN)

Hỗ trợ kết nối VPN an toàn qua:

Hình 10: VPN

- IPSec: Dành cho các tổ chức yêu cầu bảo mật cao.

- OpenVPN: Dành cho kết nối từ xa với hiệu suất tốt.

3.2.5. Giám sát mạng (Monitoring and Logging)

- Quan sát lưu lượng: Hiển thị thông tin chi tiết về lưu lượng mạng theo thời gian thực.

- Ghi nhật ký: Ghi lại các sự kiện, kết nối, và lỗi để phân tích và kiểm tra bảo mật.

3.2.6. Proxy và lọc nội dung

- Proxy Server: Dùng để lưu trữ và quản lý các kết nối web.

- Content Filtering: Chặn truy cập các trang web không phù hợp hoặc nguy hiểm.

3.2.7. Bảo vệ chống tấn công DoS/DDoS

- Tự động phát hiện lưu lượng tấn công và chặn các gói tin bất thường.

- Quản lý kết nối để tránh hiện tượng quá tải tài nguyên mạng.

3.3. Kiến trúc mạng trong IPFire

RED (WAN): Là vùng kết nối trực tiếp với Internet, mọi lưu lượng từ vùng này được coi là không tin cậy và cần được giám sát chặt chẽ.

GREEN (LAN): Mạng nội bộ an toàn, nơi các thiết bị đáng tin cậy kết nối, thường là nơi đặt máy tính cá nhân hoặc máy chủ trong nội bộ tổ chức.

ORANGE (DMZ - Demilitarized Zone): Khu vực cách ly cho các máy chủ truy cập từ Internet giúp giảm thiểu rủi ro nếu máy chủ bị xâm nhập.

BLUE (Wireless): Khu vực dành riêng cho kết nối không dây (Wi-fi), yêu cầu xác thực trước khi truy cập mạng.

3.4. Ưu điểm và hạn chế của IPFire

3.4.1. Ưu điểm

IPFire hoàn toàn miễn phí, chỉ cần truy cập trang web chính thức và "Tải xuống". Tuy nhiên, phải chọn kiến trúc của thiết bị (X86_64 hoặc ARM) cho phù hợp với phiên bản cần tải xuống.

IPFire là một hệ điều hành tiêu thụ rất ít tài nguyên, thực tế có thể được sử dụng trên bất kỳ máy tính nào, mặc dù về mặt logic, hiệu suất thu được sẽ phụ thuộc vào phần cứng được sử dụng, rules trong tường lửa và thông số cài đặt của một hệ thống phát hiện và ngăn chặn xâm nhập. Tùy thuộc vào nhu cầu mà chúng ta sẽ cần phần cứng như thế nào.

3.4.2. Hạn chế

Giao diện người dùng hạn chế: Giao diện quản lý web (Web UI) của IPFire không thân thiện và trực quan như các giải pháp thương mại khác

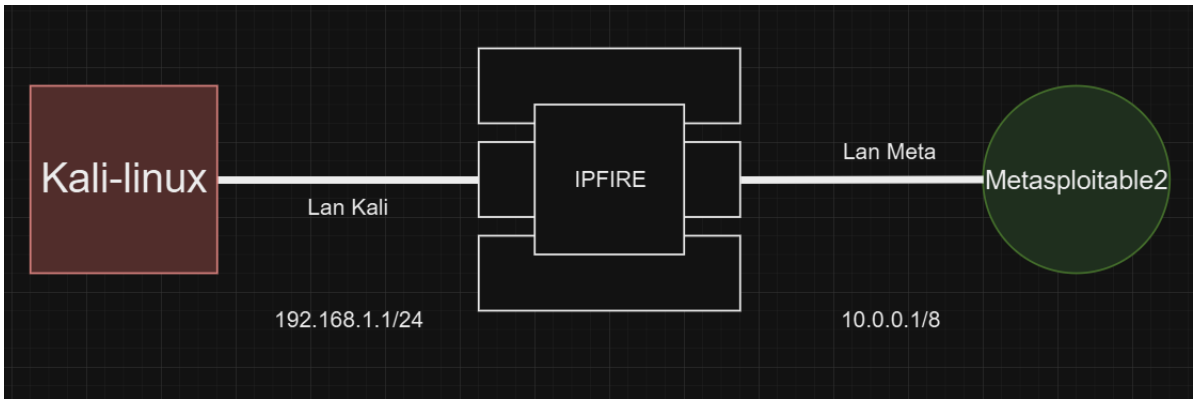
Hỗ trợ phần cứng bị hạn chế: Một số phần cứng mới hoặc cao cấp có thể không được hỗ trợ tốt. Điều này có thể làm giảm hiệu suất hoặc gây khó khăn khi triển khai trên các hệ thống đặc thù.

Công đồng nhỏ: So với các hệ thống firewall mã nguồn mở khác như pfSense hoặc OPNsense, IPFire có cộng đồng nhỏ hơn. Điều này có thể khiến việc tìm kiếm hỗ trợ hoặc tài liệu khó khăn hơn.

Khả năng mở rộng hạn chế: IPFire không được thiết kế để hoạt động trong các môi trường phức tạp, như các doanh nghiệp lớn cần hệ thống có khả năng mở rộng mạnh mẽ và khả năng chịu tải cao.

CHƯƠNG IV. THỰC HIỆN MÔ PHỎNG TẤN CÔNG DOS VÀ PHÒNG CHỐNG DỰA TRÊN ỨNG DỤNG IPFIRE

4.1. Sơ đồ cấu trúc mạng của đề tài



Hình 11: Sơ đồ mạng của đề tài

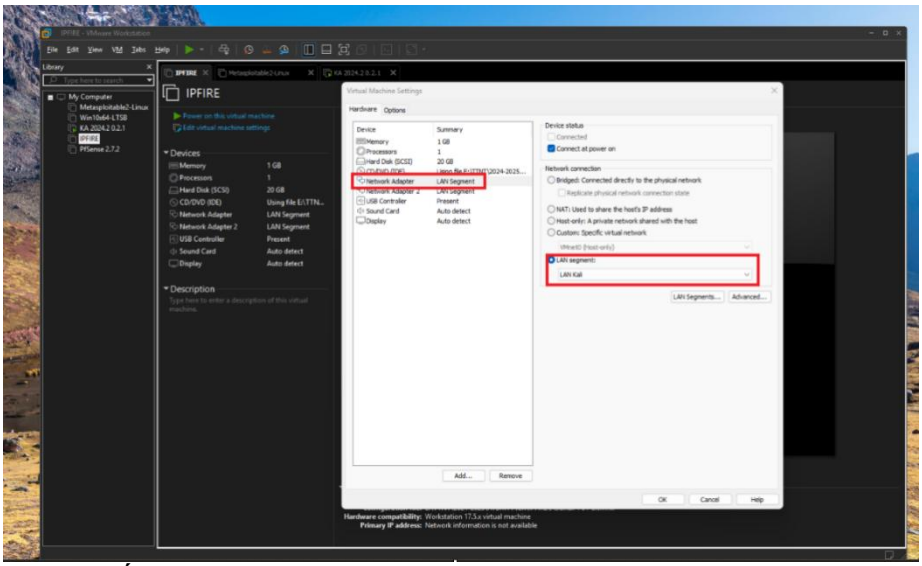
Ở đề tài này sẽ cần 2 mạng để triển khai, nhóm sẽ mô phỏng dây Lan Kali sẽ là mạng RED có ip là 192.168.1.1/24 có gateway là 192.168.1.1, dây Lan Meta sẽ là mạng GREEN có ip là 10.0.0.1/8 có gateway là 10.0.0.1

4.2. Cài đặt các máy ảo cần thiết

4.2.1. Máy ảo IPFire

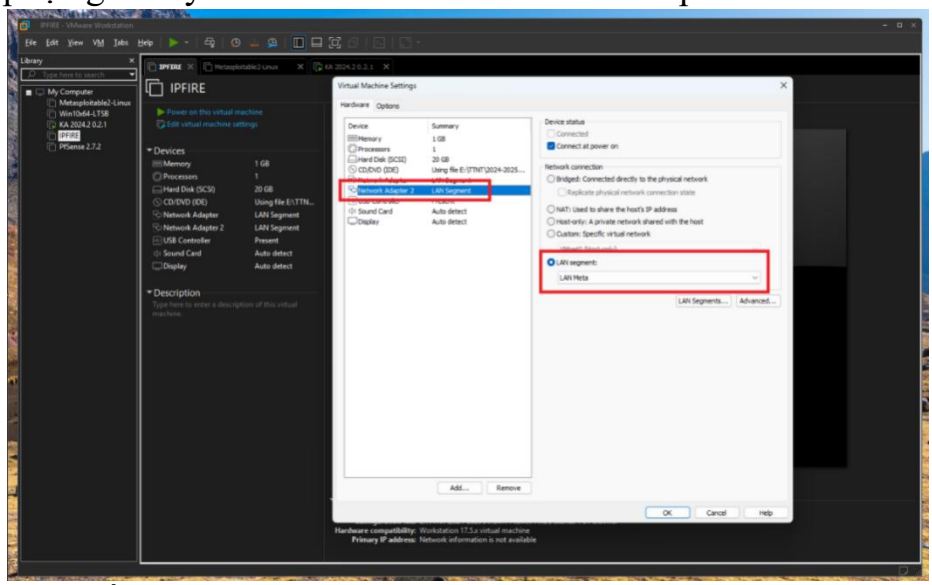
Download file iso IPFire về máy, sau đó khởi động phần mềm VMWare sau đó chọn tạo máy ảo mới, rồi làm theo các bước cần thiết để tạo máy ảo cài file iso IPFire.

Sau khi tạo máy ảo xong, tiến hành gắn dây “Lan Kali” vào “Network Adapter”.



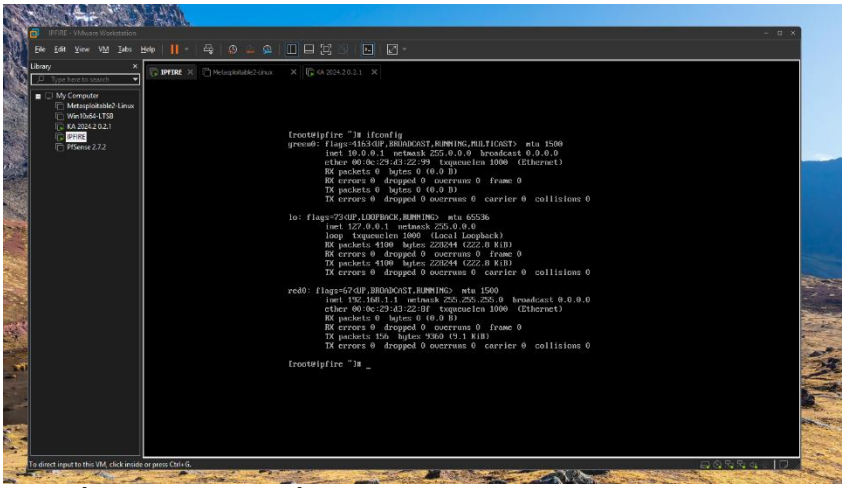
Hình 12: Gắn dây “Lan Kali” vào “Network Adapter” của máy ảo IPFire

Tiếp tục gắn dây “Lan Meta” vào “Network Adapter 2”.



Hình 13: Gắn dây “Lan Meta” vào “Network Adapter 2” của máy ảo IPFire

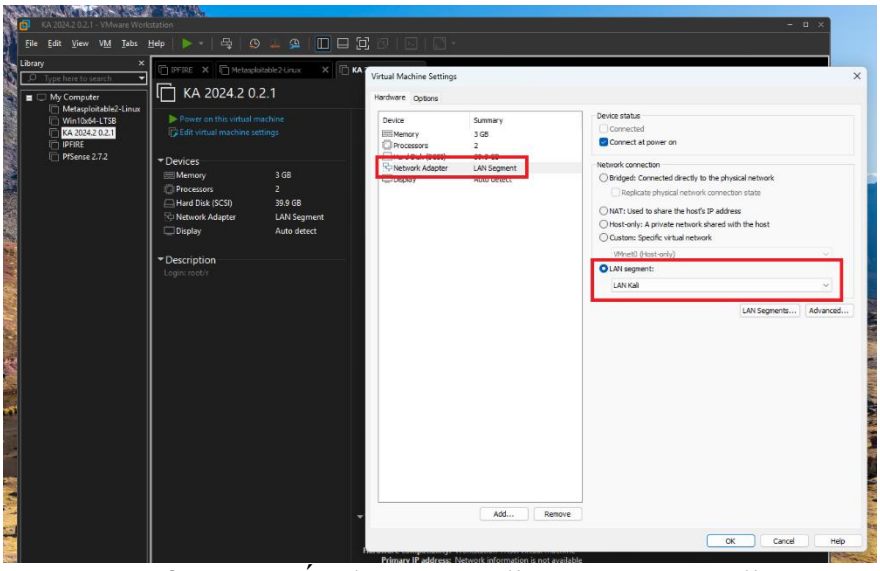
Sau khi gắn dây, khởi động máy và tiến hành cài đặt theo chỉ dẫn, tiếp đến cấu hình cho RED là dây “Lan Kali” có ip là 192.168.1.1/24, GREEN là dây “Lan Meta” có ip là 10.0.0.1/8.



Hình 14: Kết quả sau khi cấu hình ip cho RED và GREEN trên IPFire

4.2.2. Máy ảo Kali-linux

Sau khi tải về máy ảo kali được Thầy cung cấp, tiến hành mở máy ảo trong phần mềm VMWare sau đó gắn dây "Lan Kali" được tạo trên phần mềm VMWare.

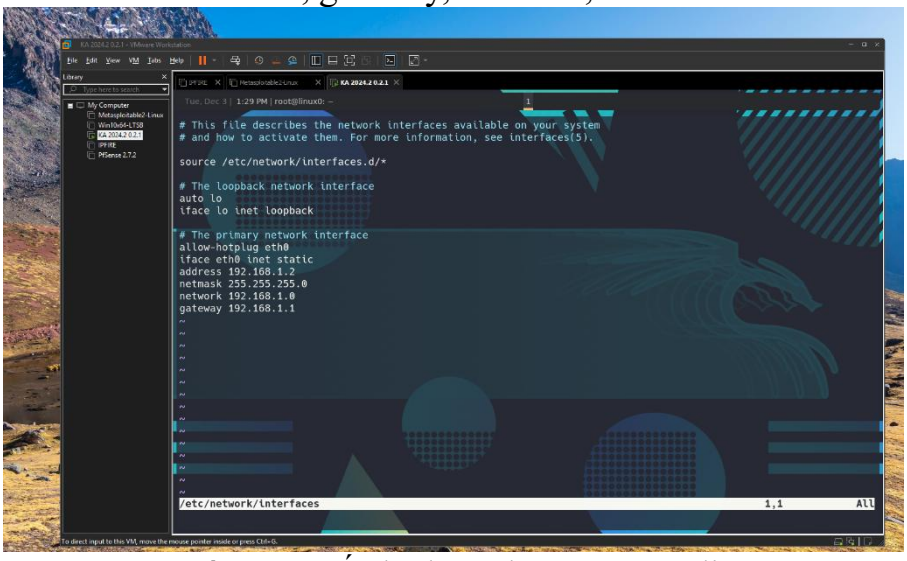


Hình 15: Gắn dây Lan Kali vào máy ảo Kali

Khởi động máy ảo Kali sau đó bật terminal để cấu hình ip.

Dùng câu lệnh "sudo vim /etc/network/interfaces" để vào file cấu hình ip.

Cấu hình ip cùng mạng với RED của IPFire như cấu hình ở trên với các thông tin cơ bản như: address, gateway, netmask, network.

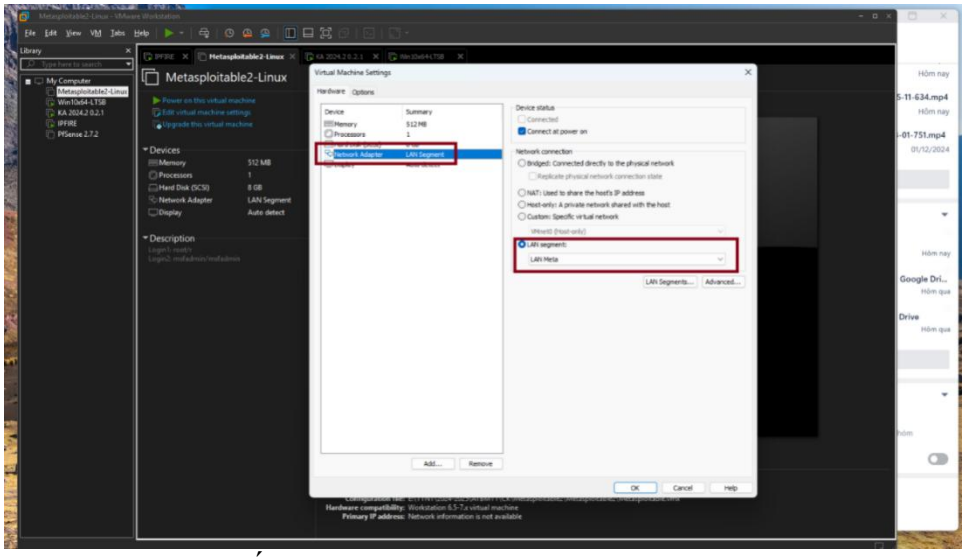


Hình 16: Cấu hình IP cho máy ảo Kali

Lúc này máy ảo Kali đã có thể ping được từ mạng REED tới ip gateway của mạng GREEN nhưng chưa thể ping vào các ip nội bộ bên trong mạng GREEN vì mặc định IPFire không cho phép điều đó.

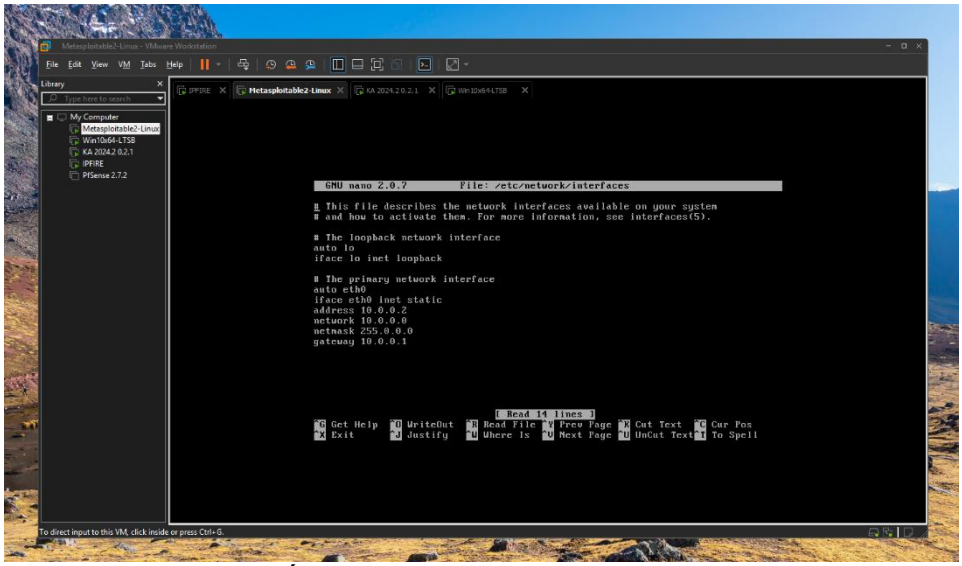
4.2.3. Máy ảo Metasploitable2

Sau khi tải về file máy ảo Metasploitable2 được Thầy cung cấp, tiến hành mở máy ảo trên VMWare, sau đó gắn dây "Lan Meta" vào "Network Adapter".



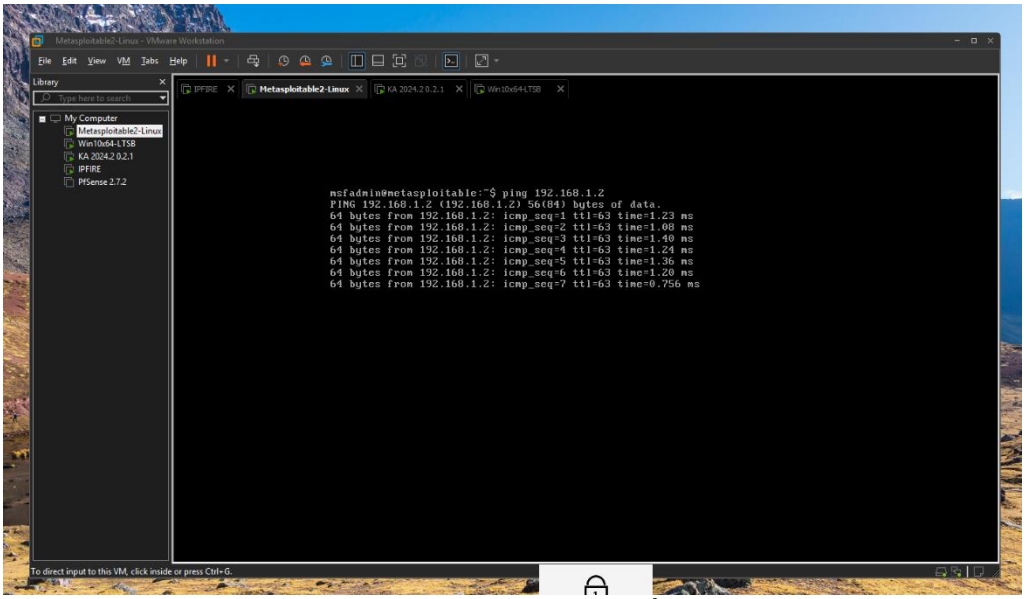
Hình 17: Gắn dây "Lan Meta" vào máy Metasploitable2

Tiếp tục khởi động máy ảo Metasploitable2 lên và tiến hành dùng câu lệnh "sudo nano /etc/network/interfaces" để cấu hình ip cùng mạng với GREEN của máy IPFire đã cấu hình bên trên với các thông tin cơ bản như address, netmask, gateway, network.



Hình 18: Cấu hình ip máy ảo Metasploitable2

Lúc này, máy ảo Metasploitable2 đã có thể ping nội bộ trong mạng GREEN và ping được đến mạng RED của IPFire cụ thể là ping được đến máy ảo Kali với ip là 192.168.1.2

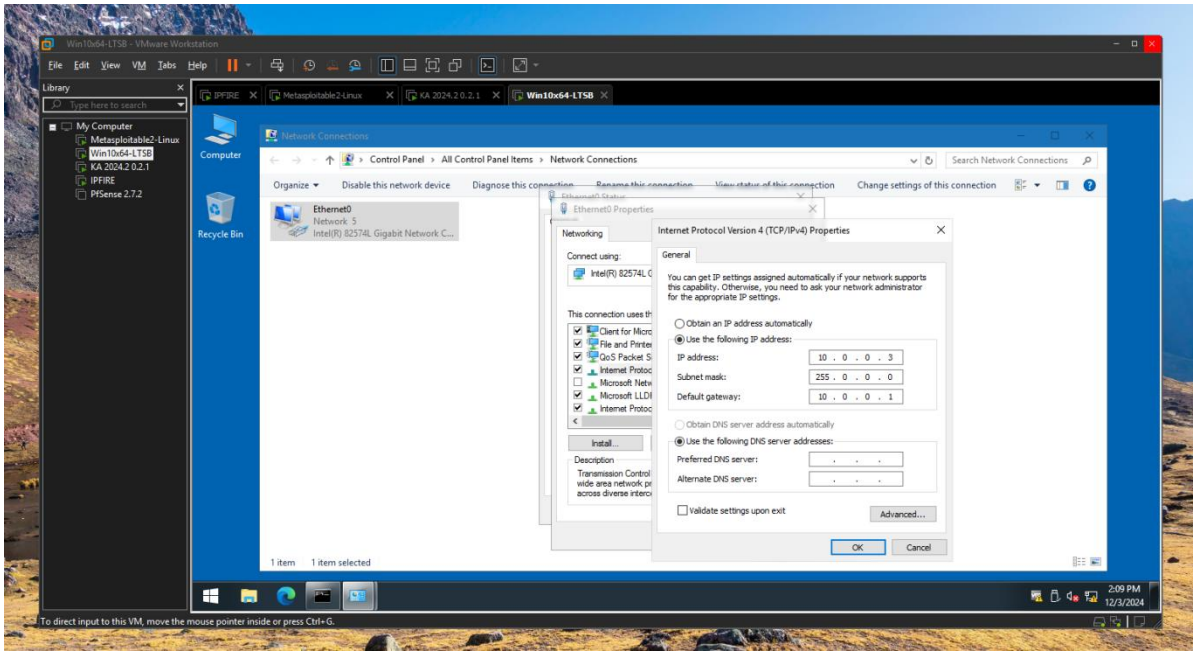


Hình 19: Ping từ máy Metasploitable đến máy Kali.

4.2.4. Máy ảo win10x64-LTSB

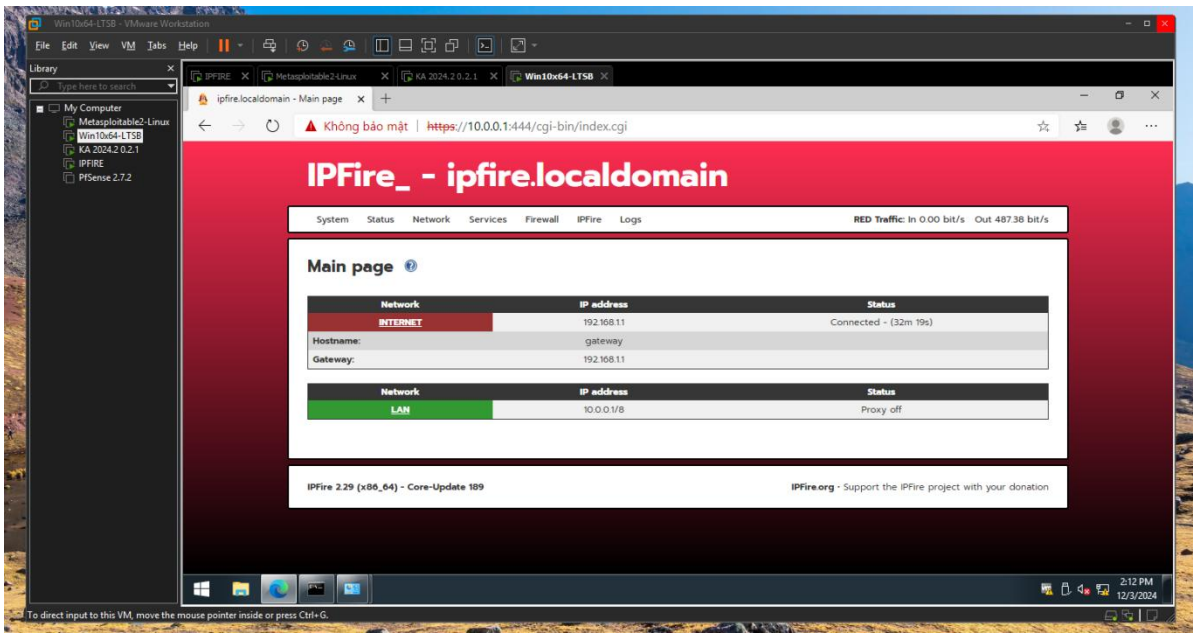
Để có thể tinh chỉnh FireWall Rules của IPFire trên giao diện website nên nhóm có cài thêm 1 máy ảo windows để sử dụng trình duyệt web.

Thầy có cung cấp máy ảo win10x64-LSTB, nên sau khi tải về, nhóm chỉ cần mở máy ảo trên phần mềm VMWare sau đó tiến hành gắn dây “Lan Meta” cho máy ảo win10x64-LSTB vì để truy cập website của IPFire thì phải truy cập thông qua địa chỉ ip của mạng GREEN là 10.0.0.1 đã cấu hình ở trên. Sau đó cấu hình ip tĩnh để máy win cùng mạng với mạng GREEN của IPFire.



Hình 20: Cấu hình ip tĩnh cho máy win10x64-LTSB

Lúc này dùng trình duyệt web có sẵn trên máy, truy cập https://10.0.0.1:444 để vào được giao diện của IPFire và đăng nhập với <tk><mk>:<admin><admin



Hình 21: Giao diện website của IPFire

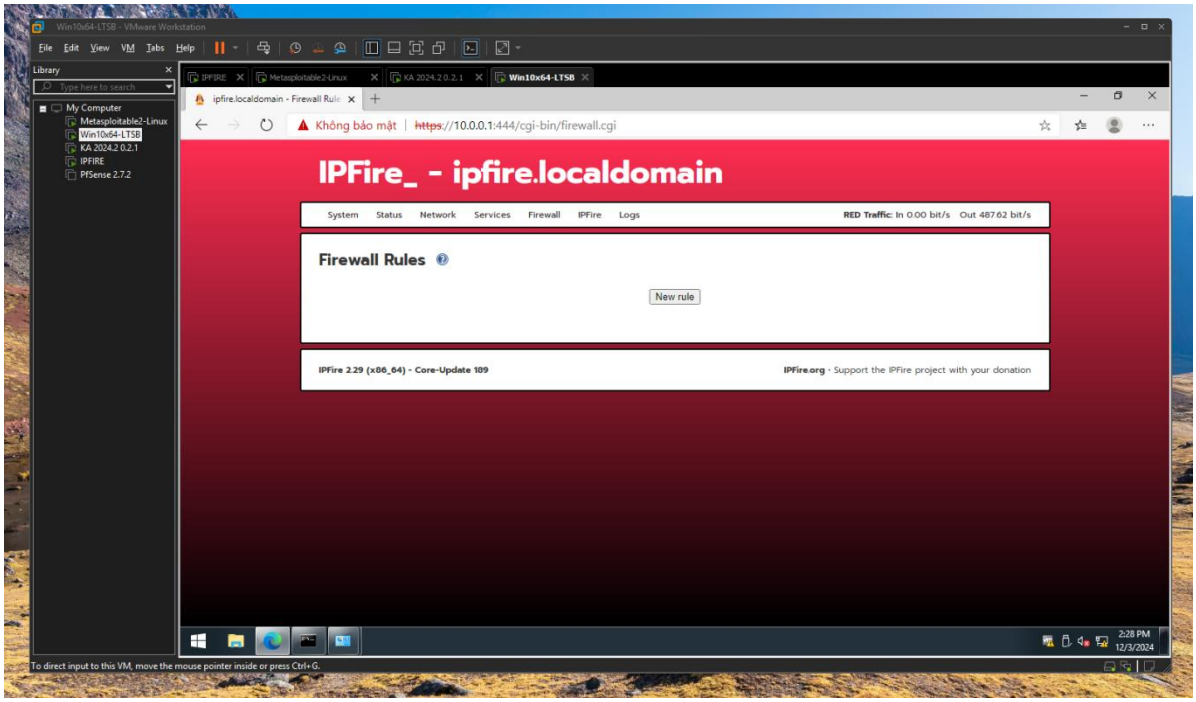
4.3. Thiết lập FireWall Rules của IPFire

Mặc định lúc này IPFire không cho phép mạng RED có thể ping được vào mạng GREEN vì mạng RED đại diện cho internet bên ngoài, những ip không tin cậy. Để có thể dùng máy ảo Kali (thuộc mạng RED) tấn công Dos vào máy ảo Metasploitable2 (thuộc mạng GREEN) thì cần thiết lập FireWall Rules cho

phép ping từ mạng RED vào mạng GREEN. Có thể là cho một ip bất kỳ hoặc tất cả ip trong mạng RED ping vào một ip bất kỳ hoặc tất cả ip trong mạng GREEN

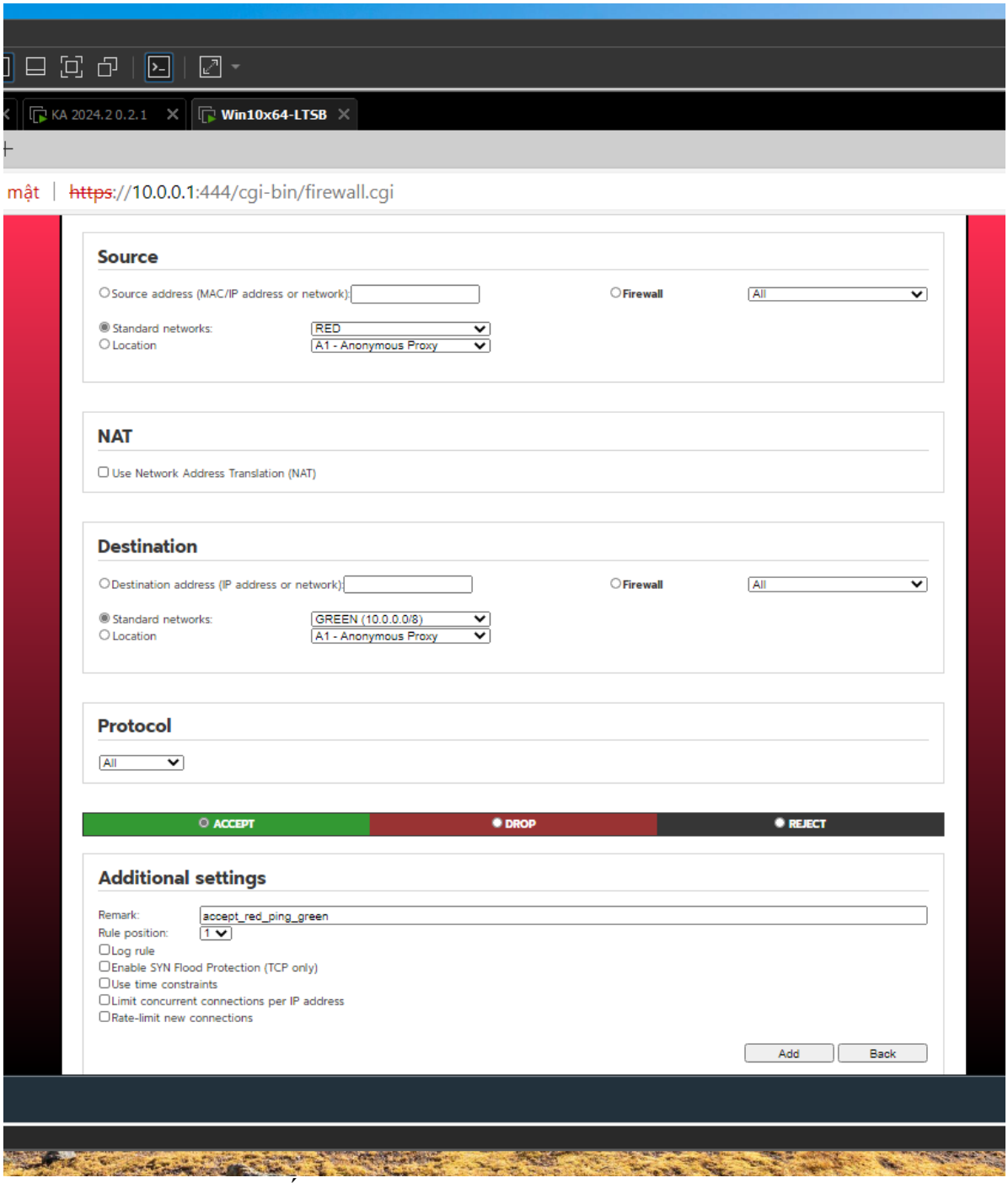
Trong đề tài này, vì mỗi mạng RED hoặc GREEN chỉ có một vài ip nên nhóm sẽ thiết lập một FireWall Rules cho phép tất cả các ip trong mạng RED ping vào được tất cả các ip trong mạng GREEN.

Ở giao diện web của IPFire, chọn "FireWall -> FireWall Rules" để vào giao diện quản lý FireWall Rules.



Hình 22: Giao diện quản lý FireWall Rules

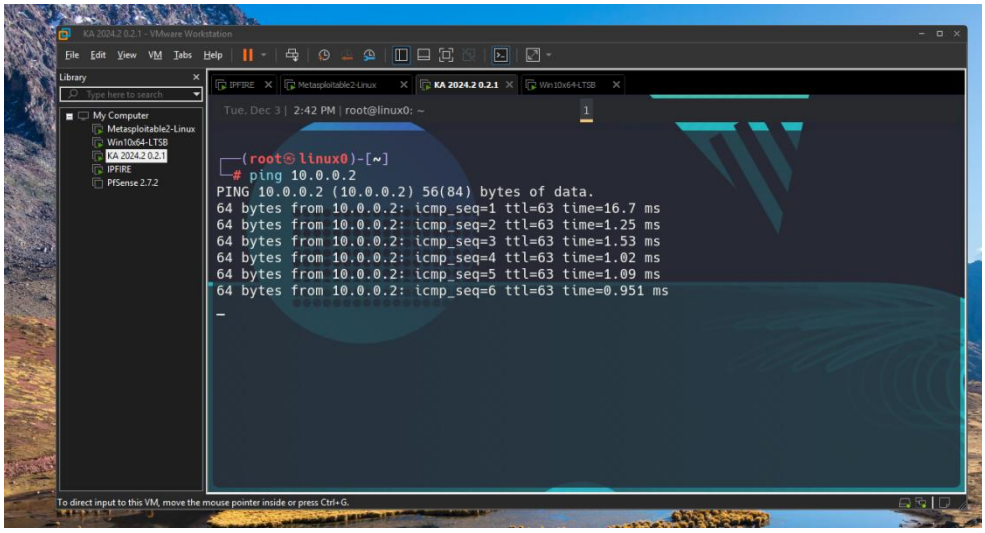
Sau đó chọn "new rule" để vào giao diện thiết lập FireWall Rules. Ở đây, trong phần "Source" nếu muốn chỉ cụ thể ip nào thì gõ vào phần "Source address", nhóm thiết lập cho phép cả mạng RED nên chọn vào "Standard network" là RED. Tiếp đến phần "Destination" nếu muốn chỉ cụ thể ip nào là đích thì có thể gõ vào phần "Destination address", nhóm thiết lập cho cả mạng GREEN là ip đích nên chọn vào "Standard network" là GREEN. Phần "Protocol" là giao thức, thì nhóm để mặc định là "All". Tiếp đến phần có 3 màu xanh, đỏ, đen, nhóm thiết lập rule này là cho phép nên chọn vào "ACCEPT". Tiếp đến phần "Remark" là để đặt tên cho rule để tiện quản lý. Mục "Rule position" là thiết lập vị trí của rule. Nếu có nhiều rule thì sẽ sắp sếp theo thứ tự tăng dần từ 1, ưu tiên rule ở trên. Nhóm chỉ thiết lập 1 rule nên để luôn mặc định là 1. Sau khi hoàn tất thiết lập rule thì chọn "Add".



Hình 23: Thiết lập FireWall Rules trên giao diện web của IPFire

Sau khi chọn "Add" sẽ quay lại giao diện quản lý rules, sau đó nhấn chọn "Apply changes" để IPFire bắt đầu áp dụng các thay đổi trên.

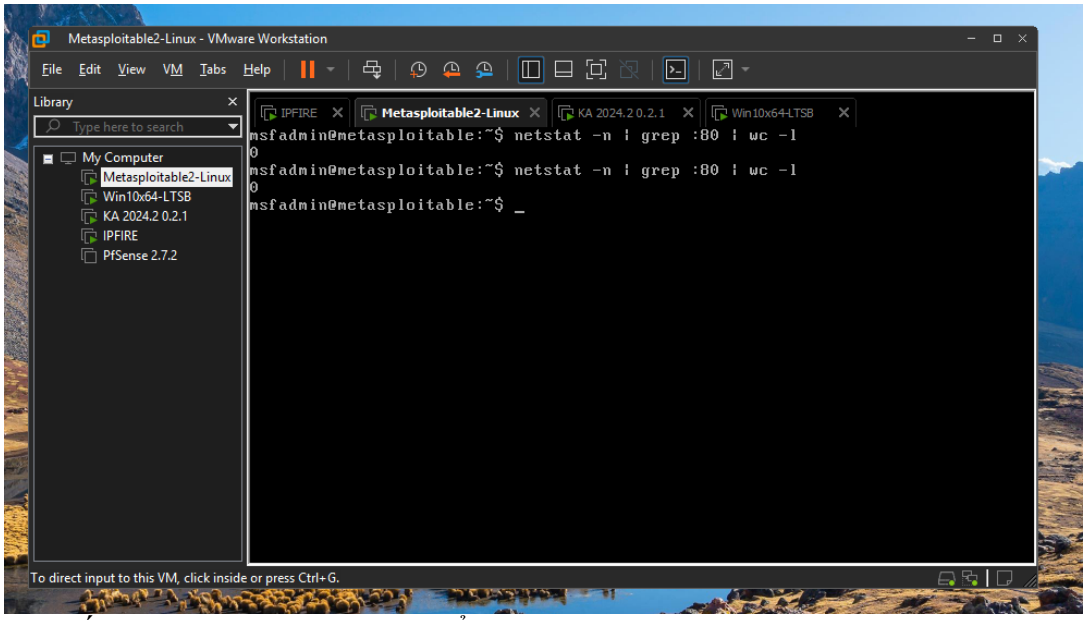
Sau khi thiết lập FireWall Rules cho phép mạng RED ping vào mạng GREEN thì máy ảo Kali đã có thể ping được đến máy ảo Metasploitable2 với ip là 10.0.0.2.



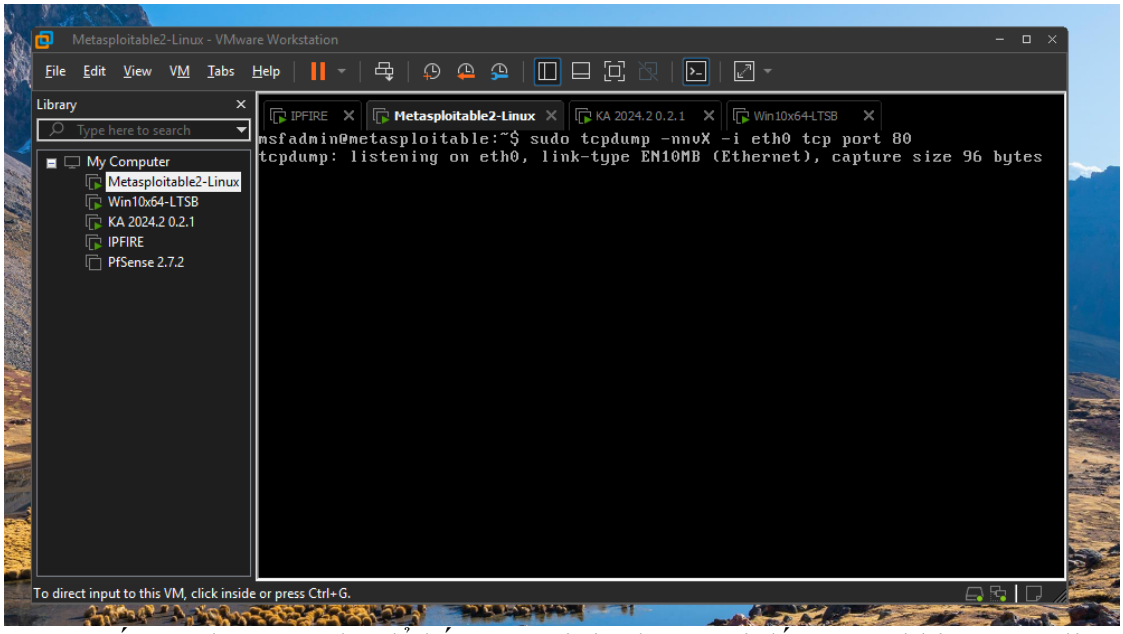
Hình 24: Thực hiện ping từ máy ảo Kali sang máy ảo Metasploitable2 sau khi đã thiết lập FireWall Rules

4.4. Tấn công Dos từ máy Kali sang máy Metasploitable2

Để nhận biết được máy ảo Metasploitable2 bị Dos vào thì có thể sử dụng câu lệnh "netstat -n | grep :80 | wc -l" để xem có bao nhiêu connection đến cổng 80 trước và sau khi chạy lệnh Dos bên máy Kali. Hoặc có thể dùng câu lệnh "sudo tcpdump -nnvX -i eth0 tcp port 80" để bắt các gói tin đến eth0.

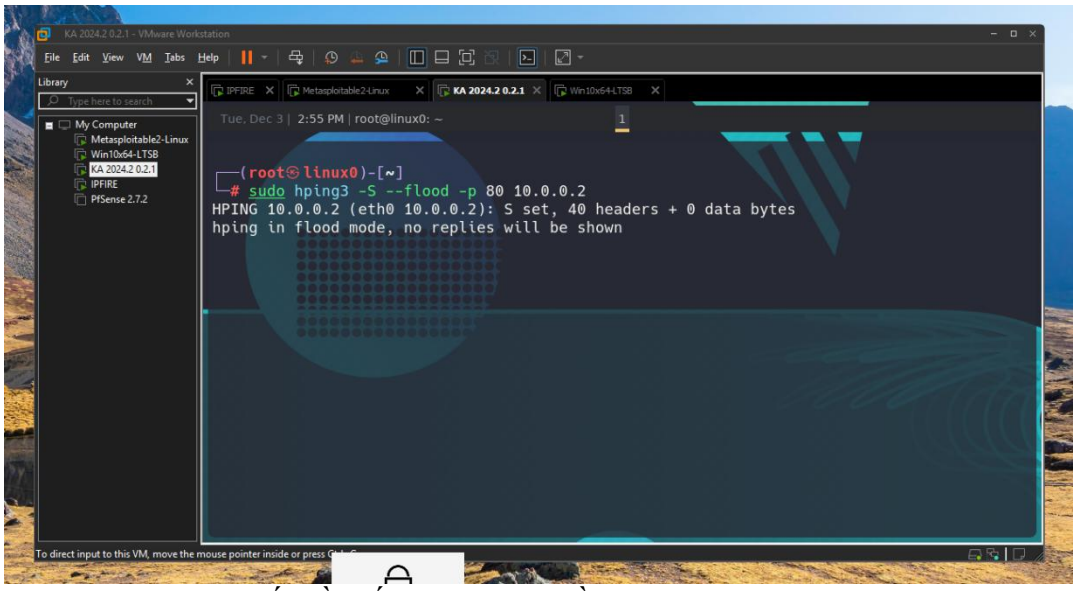


Hình 25: số lượng các connection ở cổng 80 của máy Metasploitable2 trước khi máy Kali chạy lên tấn công



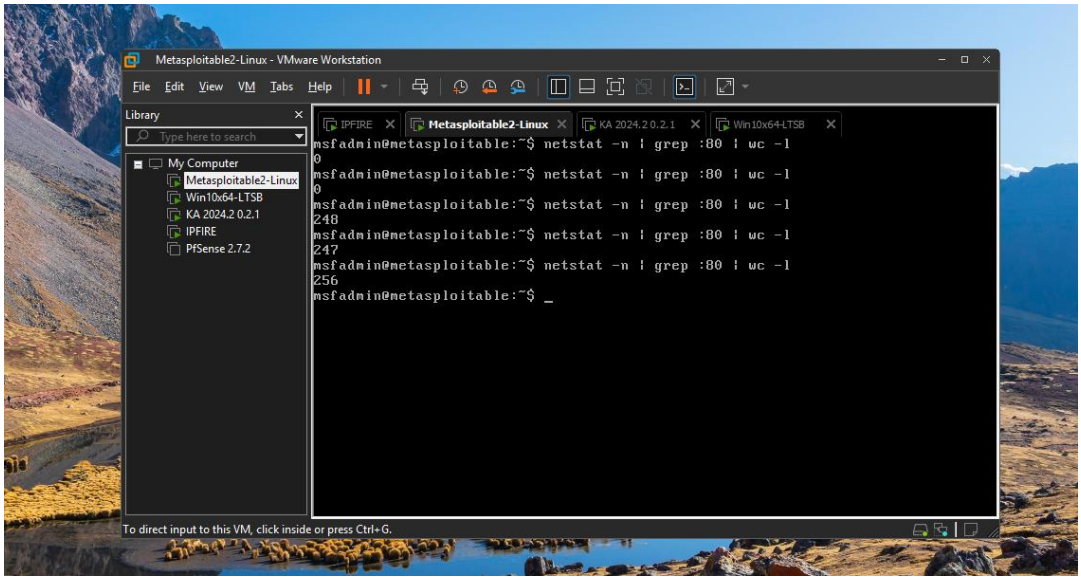
Hình 26: Lắng nghe trên eth0 để bắt các gói tin được gửi đến trước khi máy Kali chạy lệnh tấn công

Vào terminal trên máy ảo Kali, sử dụng câu lệnh "sudo hping3 -S --flood -p 80 10.0.0.2" để thực hiện tấn công DoS vào máy ảo Metasploitable2.

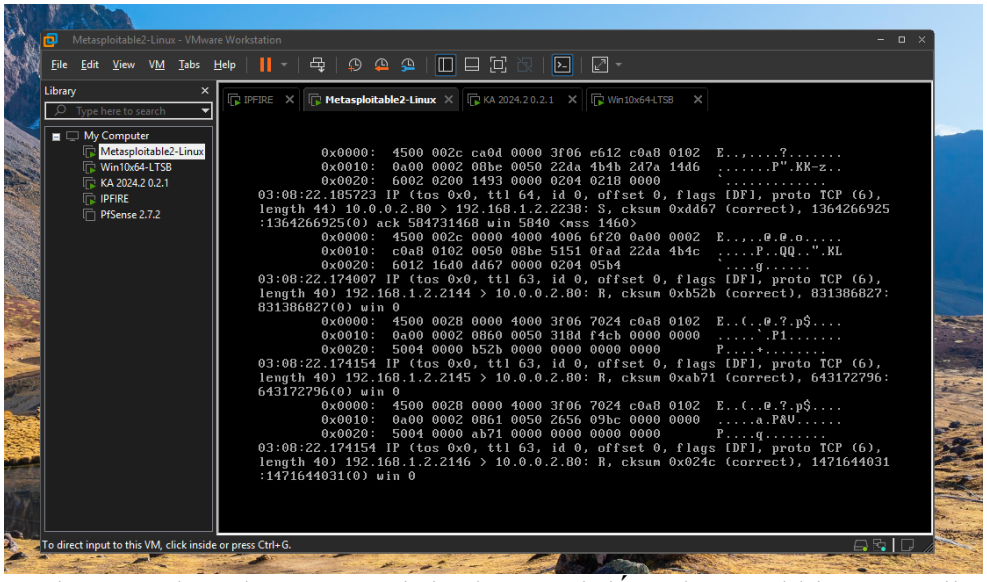


Hình 27: Bắt đầu tấn công DoS bằng hping3 trên máy Kali

Sau đó vào lại máy Metasploitable2 để kiểm tra lại các connection ở cổng 80 sau chạy lệnh tấn công DoS.



Hình 28: Số lượng connections ở cổng 80 của máy Metasploitable2 sau máy Kali chạy lệnh tấn công.



Hình 29: Liên tục nhận được các gói tin được gửi đến eth0 sau khi máy Kali chạy lệnh tấn công

Có thể thấy rằng số lượng connections đã tăng lên đáng kể và các gói tin được gửi đến liên tục. Điều này cho thấy là máy Metasploitable2 đang bị tấn công.

Vì thế, để phòng chống các cuộc tấn công đến từ các ip không đáng tin cậy, cần phải có FireWall Rules để ngăng chặn. Bây giờ chỉ cần vào giao diện quản lý rules của IPFire, bỏ tick phần “Activate” sau đó chọn “Apply changes” thì IPFire sẽ bắt đầu ngăn chặn, không cho phép các ip từ mạng RED (các ip ngoài internet, nguy hiểm, không đáng tin cậy) ping vào được nội bộ mạng GREEN nữa. Từ đó ngăn chặn được các cuộc tấn công DoS giúp bảo vệ, các ip bên trong mạng GREEn an toàn.

CHƯƠNG V. KẾT LUẬN

5.1. Kết quả đạt được

Hiểu và áp dụng được cấu trúc mạng của IPFire, cách thức hoạt động của FireWall để ngăn chặn cuộc tấn công từ các ip nguy hiểm, không an toàn đến các ip nội bộ bên trong vùng an toàn.

Mô phỏng được cuộc tấn công DoS từ máy ảo Kali đến máy ảo Metasploitable2 và ngăn chặn nó thông qua FireWall Rules của IPFire.

5.2. Hạn chế

Chưa thiết lập được cơ chế tự backup dữ liệu trên máy Metasploitable2

CHƯƠNG VI. TÀI LIỆU THAM KHẢO

1. Kiến trúc TCP/IP và mạng Intranet: Chương 5: Đảm bảo an minh mạng nội bộ Intranet.
   Link: https://users.soict.hust.edu.vn/hoangph/textbook/ch05-1.html
   Ngày truy cập: 02/12/2024.
2. Triển khai FireWall IPFire: Cài đặt IPFire.
   Link: https://tinyactive.com/trien-khai-firewall-ipfire-cai-dat-ipfire/
   Ngày truy cập: 02/12/2024.