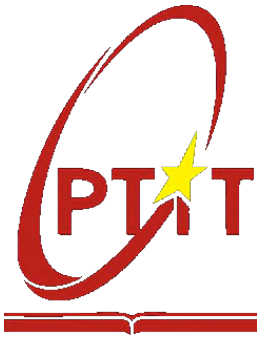
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



MÔN HỌC: THỰC TẬP CƠ SỞ

BÁO CÁO THỰC HÀNH BÀI SỐ 5

Cài đặt, cấu hình mạng doanh nghiệp với Pfsense Firewall

Giảng viên: Vũ Minh Mạnh

Sinh viên: Đỗ Quốc Tuân

Mã số sinh viên: B21DCAT201

Lớp: D21CQAT01-B

Hà Nội, tháng 3 năm 2024

MỤC LỤC

I.Cơ sở lý thuyết

1.1. Cấu hình mạng trong phần mềm mô phỏng Vmware/Virtual Box:

a, VM Workstation

- VMware Workstation cung cấp khả năng tạo mạng riêng, mạng biệt lập. VMware Workstation cũng cung cấp DHCP Server có thể dễ dàng sử dụng để phân phối Địa chỉ IP cho các máy ảo chạy trên nó. Bạn thậm chí có thể đặt giới hạn cho lưu lượng đến cũng như lưu lượng đi cho các máy ảo.
- Để truy cập Mạng trong VMware Workstation. Mở VMware Workstation => Chuyển đến menu edit. Bấm vào Virtual Network Editor.
- Có 3 mạng mặc định được tạo khi bạn cài đặt VMware Workstation. Đó là Vmnet0, VMnet1, VMnet8. Ba trong số chúng thuộc các loại khác nhau Bridged, Host-only và NAT.

+ Bridged Network: Máy ảo của bạn sẽ hoạt động như một máy ảo độc lập được kết nối với bộ chuyển mạch hoặc bộ định tuyến vật lý của bạn. Trong VM này sẽ trực tiếp lấy Địa chỉ IP từ Máy chủ DHCP có trong cơ sở hạ tầng của bạn. Nếu bạn sử dụng mạng cầu nối, máy ảo sẽ là thành viên đầy đủ trong mạng. Nó có quyền truy cập vào các máy khác trên mạng và có thể liên lạc với các máy khác trên mạng như thể nó là một máy tính vật lý trên mạng.

+ NAT network: Đây là mạng mặc định được sử dụng và chỉ định khi bạn tạo máy ảo. Trong trường hợp NAT, máy ảo của bạn không có địa chỉ IP riêng trên mạng bên ngoài. Thay vào đó, một mạng riêng biệt được thiết lập trên máy chủ. Máy ảo của bạn nhận được một địa chỉ trên mạng đó từ máy chủ DHCP Sever ảo của VMware. Thiết bị VMware NAT truyền dữ liệu mạng giữa một hoặc nhiều máy ảo và mạng bên ngoài. Nó xác định các gói dữ liệu đến dành cho từng máy ảo và gửi chúng đến đúng đích.

+ Host-only Network: được sử dụng khi bạn muốn tạo một mạng hoàn toàn biệt lập để máy ảo của bạn không thể nhìn thấy mạng hoặc Internet khác. Mạng chỉ dành cho máy chủ cung cấp kết nối mạng giữa máy ảo và máy chủ, sử dụng bộ điều hợp Ethernet ảo hiển thị với hệ điều hành máy chủ. Cách tiếp cận này có thể hữu ích nếu bạn cần thiết lập một mạng ảo bị cô lập.

b) VirtualBox

VirtualBox cung cấp một danh sách dài các chế độ mạng. Mỗi bộ điều hợp mạng ảo có thể được cấu hình riêng biệt để hoạt động ở một chế độ mạng khác nhau. Các chế độ mạng của VirtualBox:

- Not Attached: chế độ không kết nối mạng cho máy ảo.
- NAT Network: Chế độ này tương tự như chế độ NAT, sử dụng để cấu hình bộ định tuyến. Sử dụng NAT Network cho nhiều máy ảo, chúng có thể giao tiếp với nhau qua mạng. Các máy ảo có thể truy cập các máy chủ khác trong mạng vật lý và có thể truy cập các mạng bên ngoài bao gồm cả internet. Bất kỳ máy nào từ mạng bên ngoài cũng như từ mạng vật lý mà máy chủ được kết nối không thể truy cập vào các máy ảo được cấu hình để sử dụng chế độ này. Khi sử dụng chế độ này, không thể truy cập máy khách từ máy chủ khi sử dụng. Bộ định tuyến VirtualBox NAT tích hợp sẵn sử dụng

bộ điều khiển giao diện mạng vật lý của máy chủ VirtualBox làm giao diện mạng bên ngoài.
- Internal Network: (mạng nội bộ) VirtualBox được kết nối với một mạng ảo biệt lập. Các máy ảo được kết nối với mạng này có thể giao tiếp với nhau, nhưng chúng không thể giao tiếp với máy chủ VirtualBox hoặc với bất kỳ máy chủ nào khác trong mạng vật lý hoặc trong mạng bên ngoài. Máy ảo được kết nối với mạng nội bộ không thể được truy cập từ máy chủ lưu trữ hoặc bất kỳ thiết bị nào khác.
- Generic Driver: Chế độ mạng này cho phép chia sẻ giao diện mạng chung. Người dùng có thể chọn trình điều khiển thích hợp để được phân phối trong một gói mở rộng hoặc được bao gồm trong VirtualBox. Chế độ này gồm 2 chế độ phụ:
+ UDP Tunnel: Các máy ảo chạy trên các máy chủ khác nhau có thể giao tiếp minh bạch bằng cách sử dụng cơ sở hạ tầng mạng hiện có.
+ VDE Networking: Máy ảo có thể kết nối với công tắc phân tán ảo trên máy chủ Linux hoặc FreeBSD.

1.2. Phần mềm Pfsense

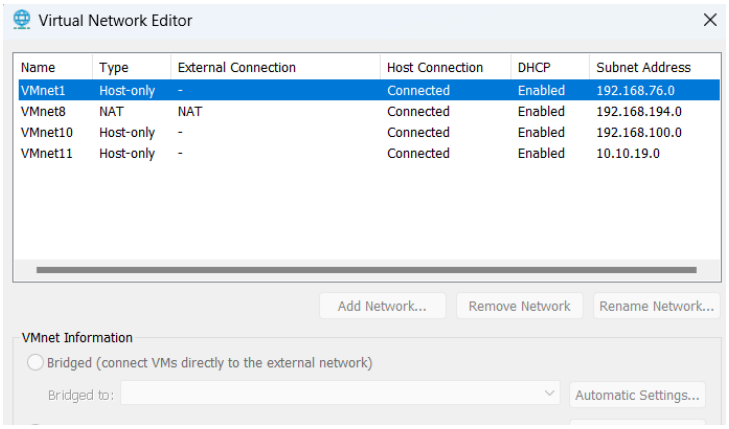
Pfsense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này cho phép mở rộng mạng của cơ quan, tổ chức, … mà không bị thỏa hiệp về sự bảo mật. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó. PfSense bao gồm nhiều tính năng giống nhưcác thiết bị tường lửa hoặc router thương mại, chẳng hạn như GUI trên nền Web tạo sự quản lý một cách dễ dàng. Pfsense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này cho phép mở rộng mạng của cơ quan, tổ chức, … mà không bị thỏa hiệp về sự bảo mật. 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. PfSense bao gồm nhiều tính năng giống nhưcác thiết bị tường lửa hoặc router thương mại, chẳng hạn như GUI trên nền Web tạo sự quản lý một cách dễ dàng.

Các tính năng trong pfsense:
- Aliases: 1Aliases sẽ gom nhóm các IP, Port hoặc URL vào với nhau, 1 alias sẽ cho phép thay thế 1 host, 1 dải mạng, nhiều IP riêng biệt hay 1 nhóm port, URL.
- NAT: Pfsense có hỗ trợ nat static dưới dạng nat 1:1. IP private được nat sẽ luôn ra ngoài bằng IP public tương ứng.
- Firewall Rules: Là nơi lưu trữ tất cả các luật ra, vào trên pfsense. Mặc định PfSense cho phép mọi kết nối ra, vào.
- Traffic shaper: giúp quản trị mạng có thể tinh chỉnh, tối ưu hóa đường truyền trong pfsense.

II. Tiến hành thực hành

2.1. Cấu hình Topo mạng

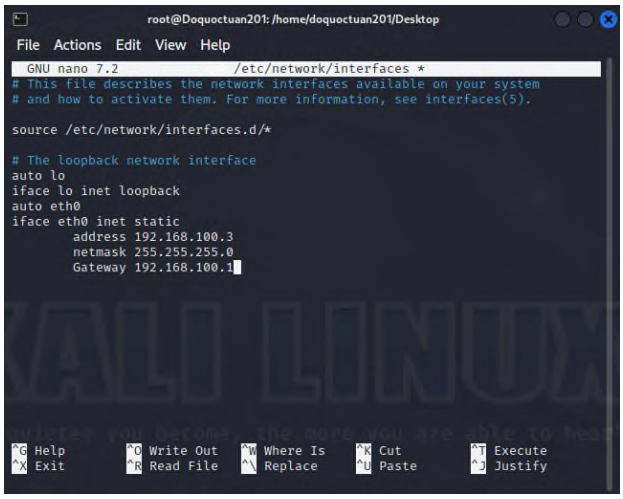
Tạo thêm 2 Subnet trên Vmware vmnet11 có địa chỉ 10.10.19.0/24 cho mạng External và vmnet10 có địa chỉ 192.168.100.0/24 cho mạng Internal



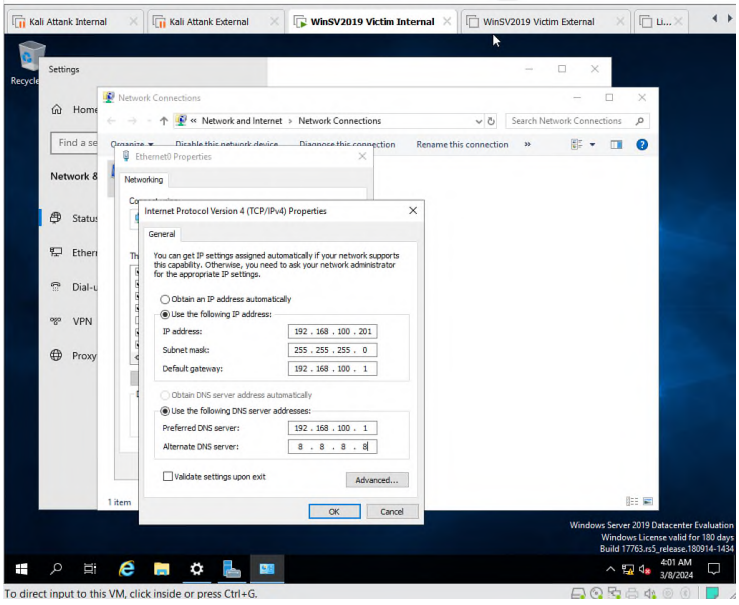
❖ Cấu hình địa chỉ IP cho các máy

- Mạng Internal

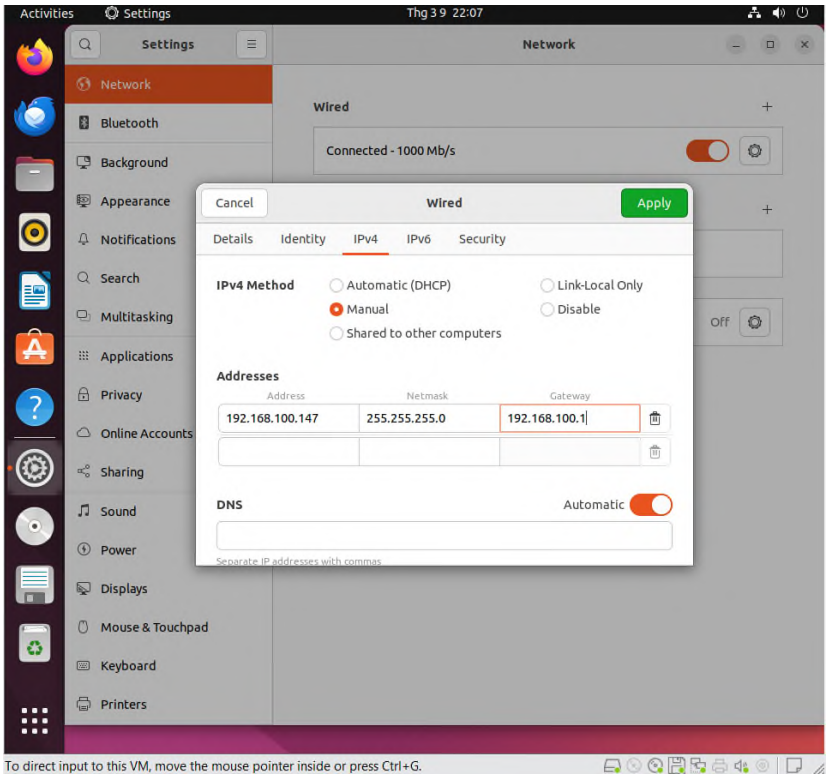
Cấu hình IP tĩnh cho máy Kali Attank Internal



Cấu hình máy Windows Server Internal. IP :192.168.100.201

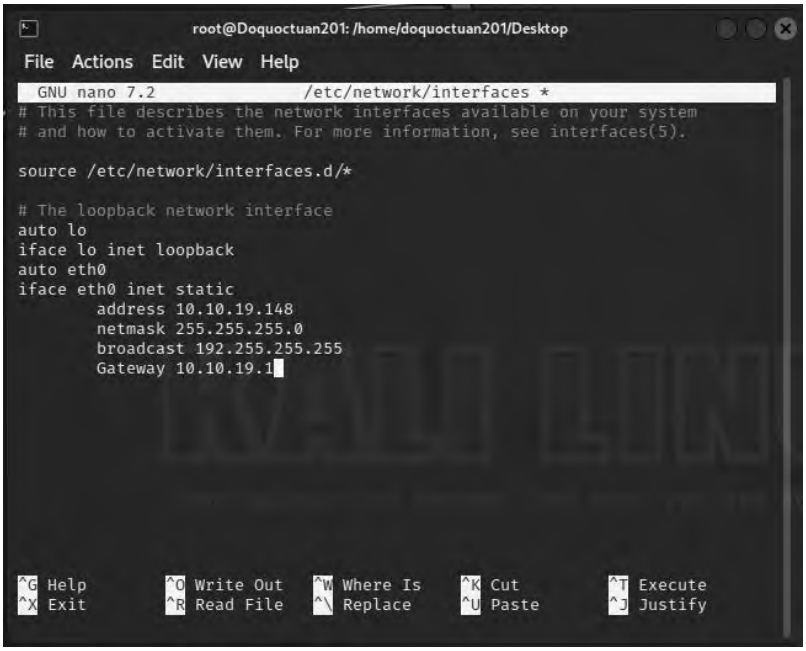


Cấu hình máy Ubuntu Internal. IP: 192.168.100.147

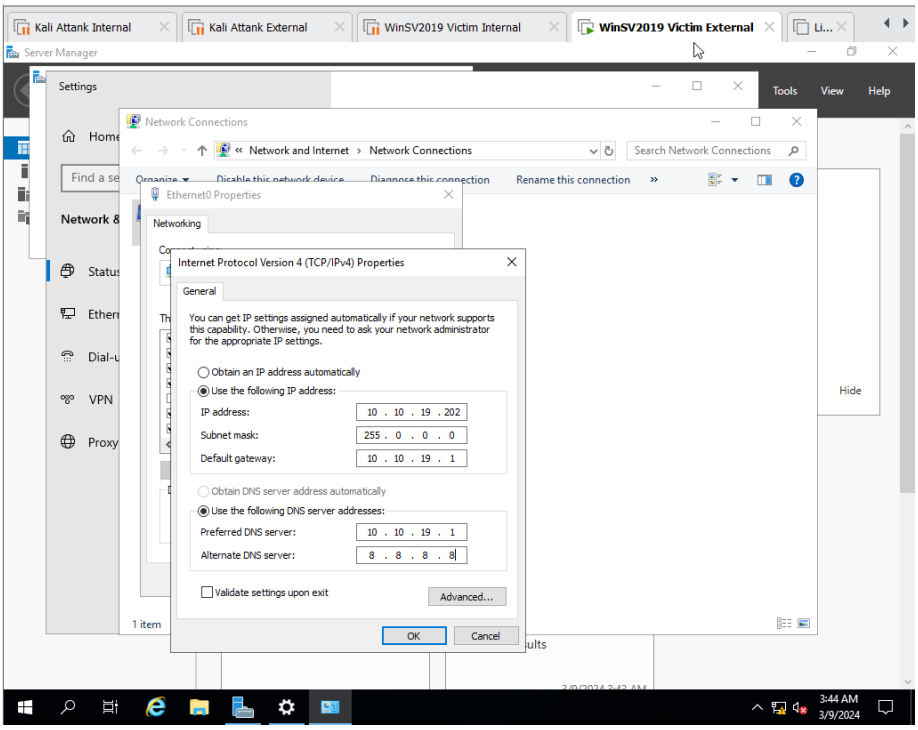


- Mạng External.

Cấu hình IP cho máy Kali Attank External



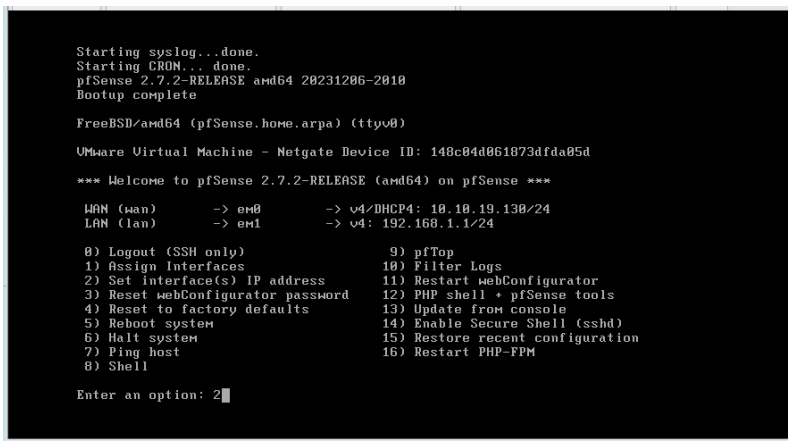
Cấu hình máy Window Server mạng External. IP: 10.10.19.202



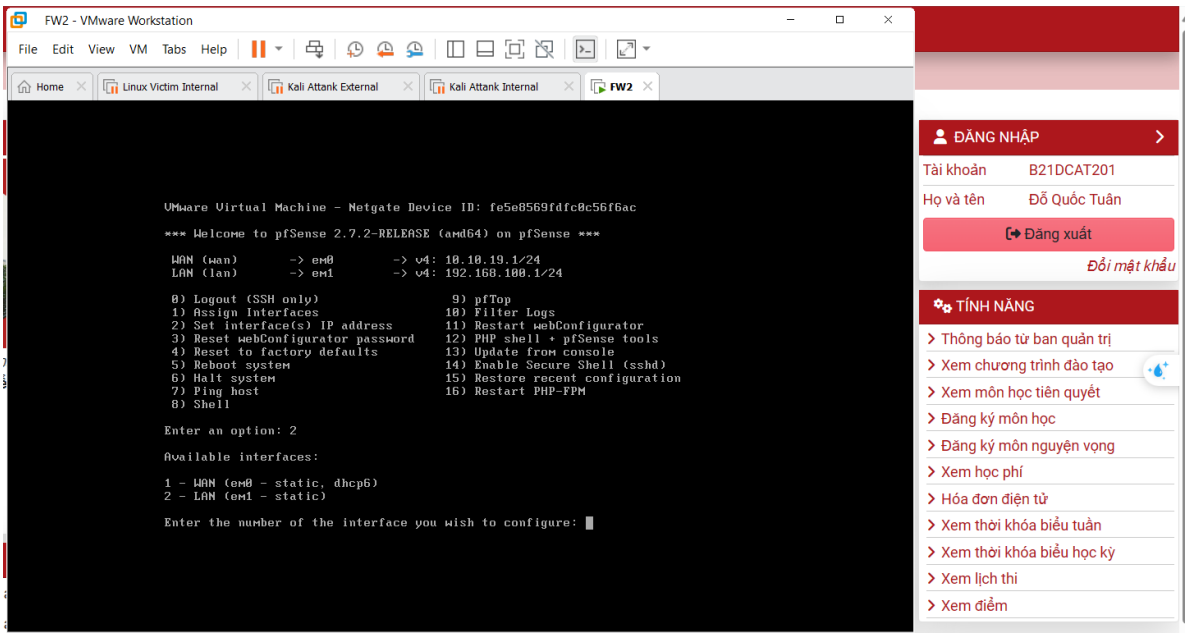
2.2. Cấu hình máy Pfsense

Chọn Install để cài đặt

Cài đặt thành công. Chọn lựa chọn 2 để cấu hình cho mạng WAN và LAN



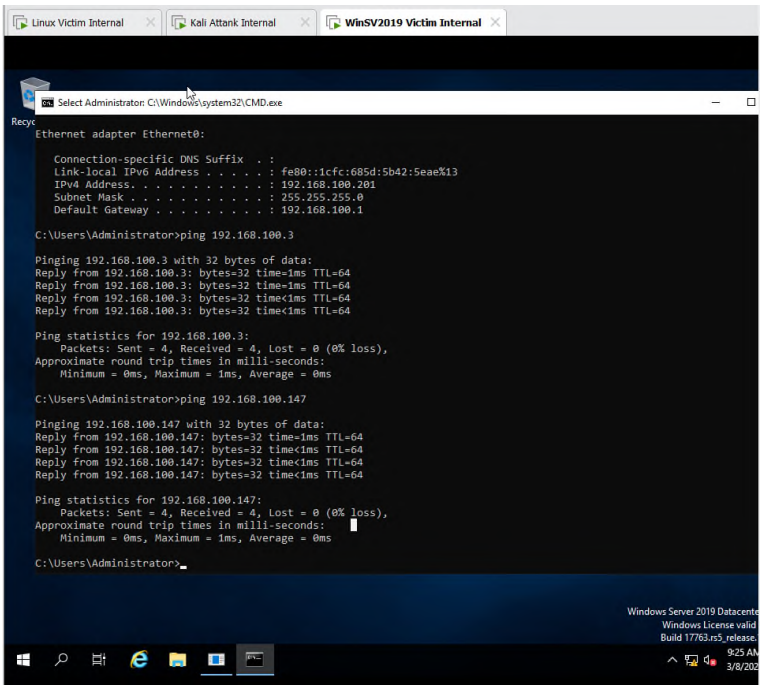
Sau khi cấu hình xong, ta được kết quả như sau:



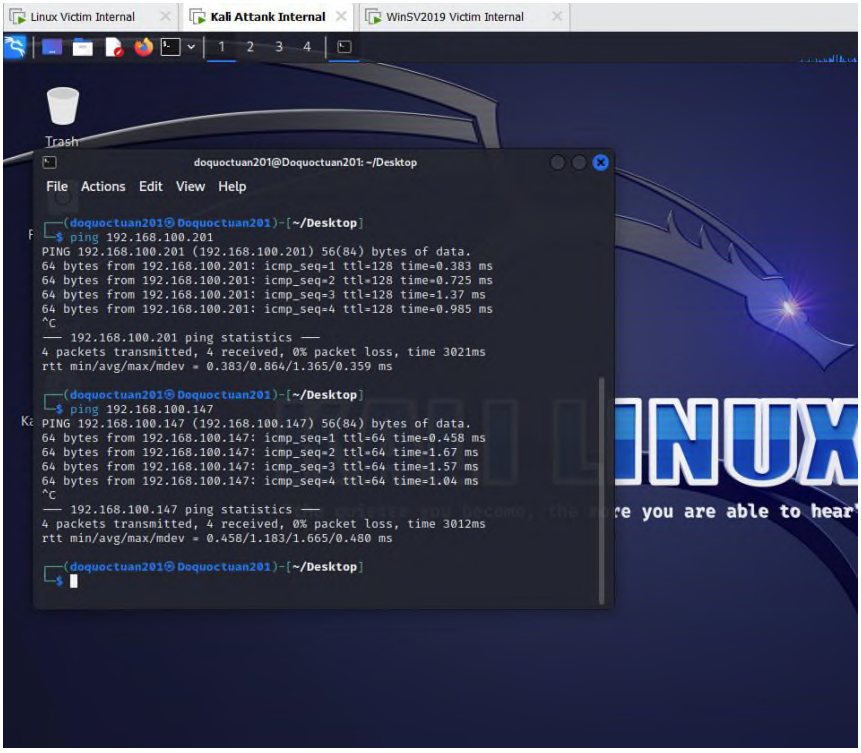
2.3. Kiểm tra kết nối giữa các máy

- ❖ Kiểm tra kết nối giữa các máy Internal

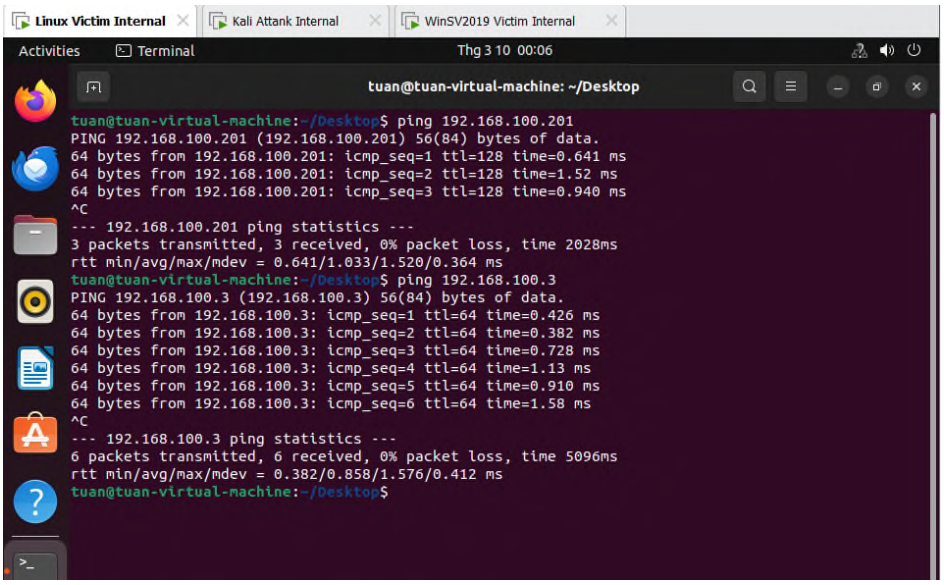
Ping từ máy Windows Server đến máy Kali và máy Ubuntu trong mạng Internal.



Ping từ máy Kali đến máy Windows server và máy Ubuntu trong mạng Internal.

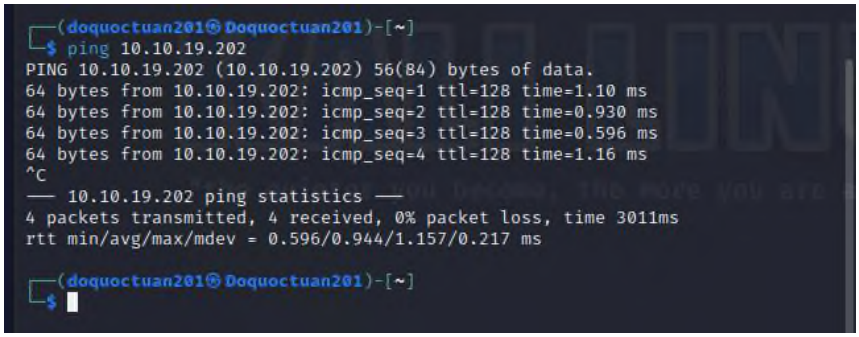


Ping từ máy Ubuntu đến máy Windows Server và Kali trong mạng Internal.

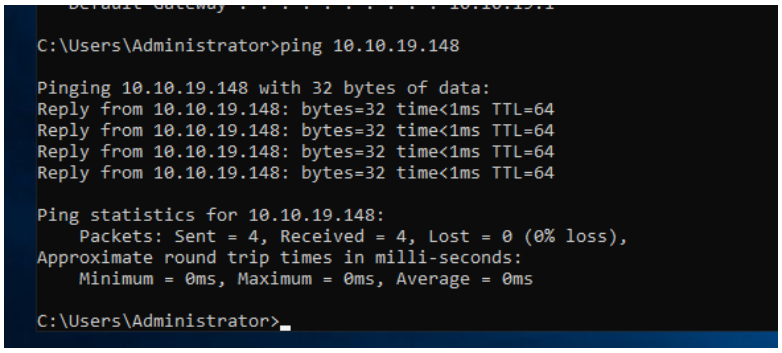


- ❖ Kiểm tra kết nối giữa các máy External.

Máy Kali External ping tới Windows Server External

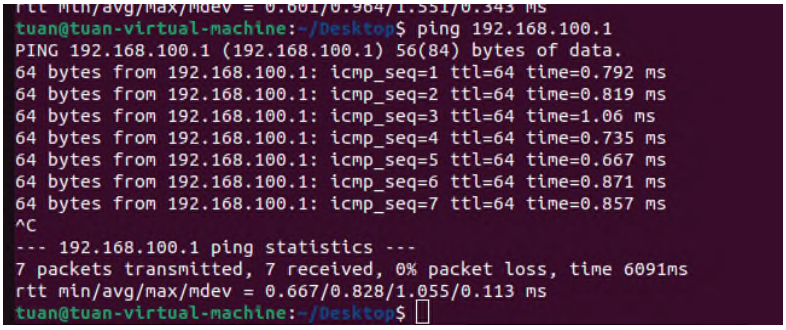


Máy Kali External ping tới Window Sever External

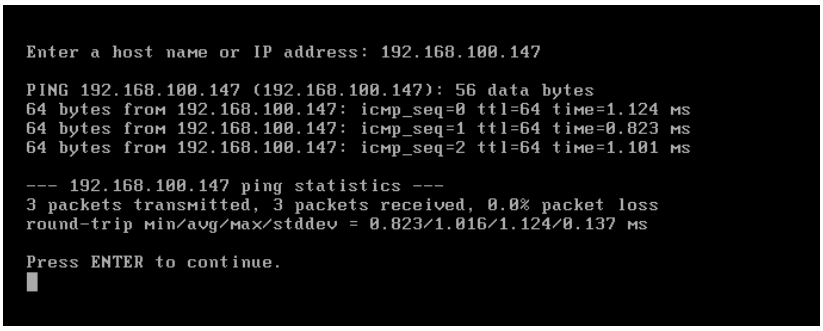


❖ Kiểm tra kết nối giữa các máy Internal, External và máy Pfsense.

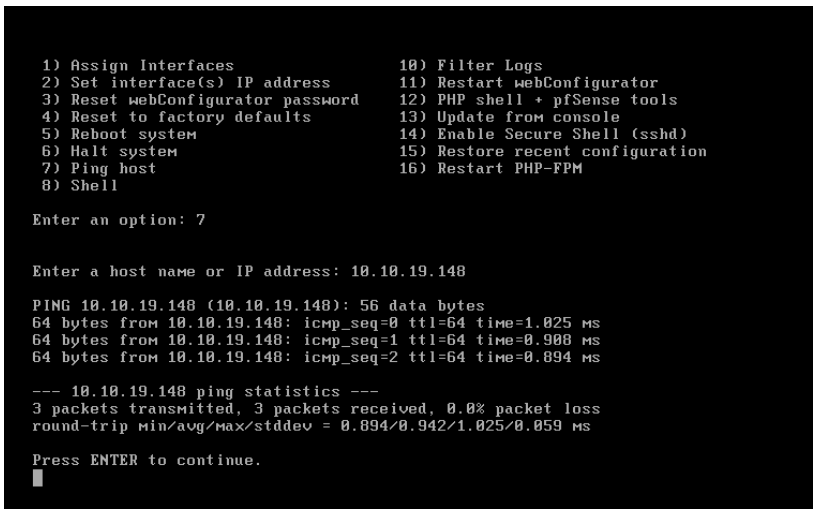
Máy Ubuntu Internal ping tới máy Pfsense



Máy Pfsense ping tới máy Ubuntu Internal



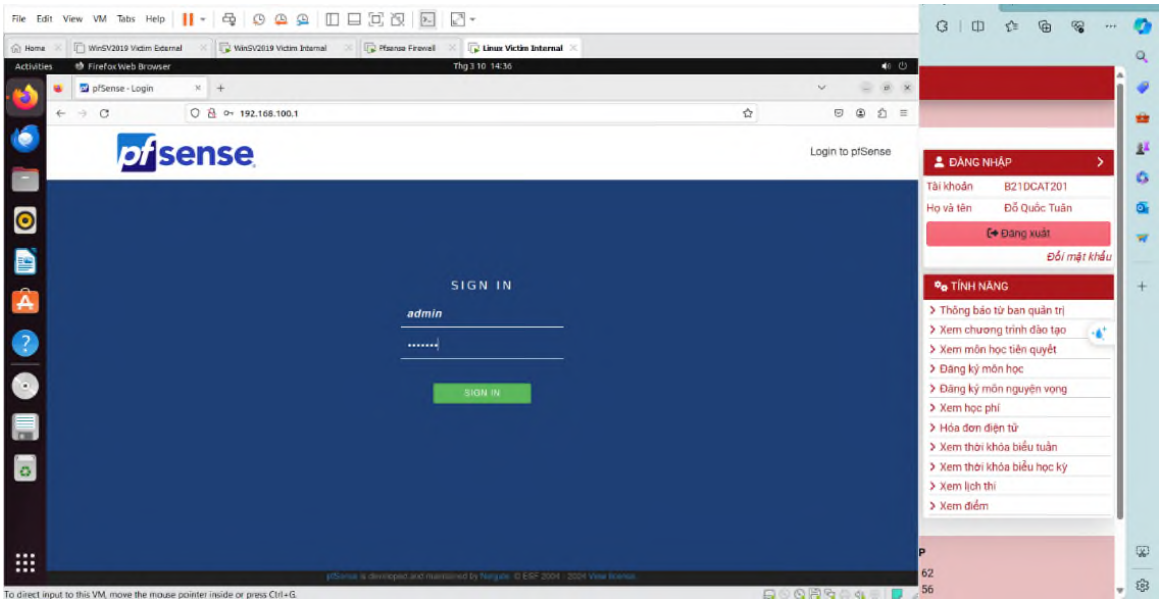
Máy Pfsense ping tới máy Kali External



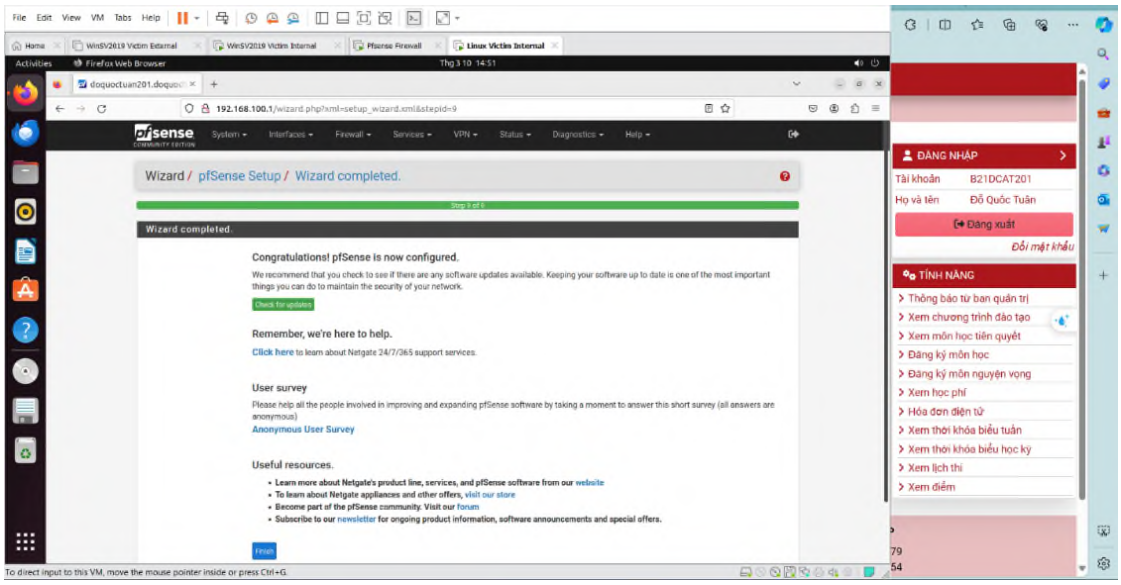
2.4. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

- Trên máy Linux victim ở mạng trong, vào trình duyệt gõ http://192.168.100.1 để cấu hình pfsense qua giao diện web.

-> Đăng nhập với username: admin & passwork: pfsense

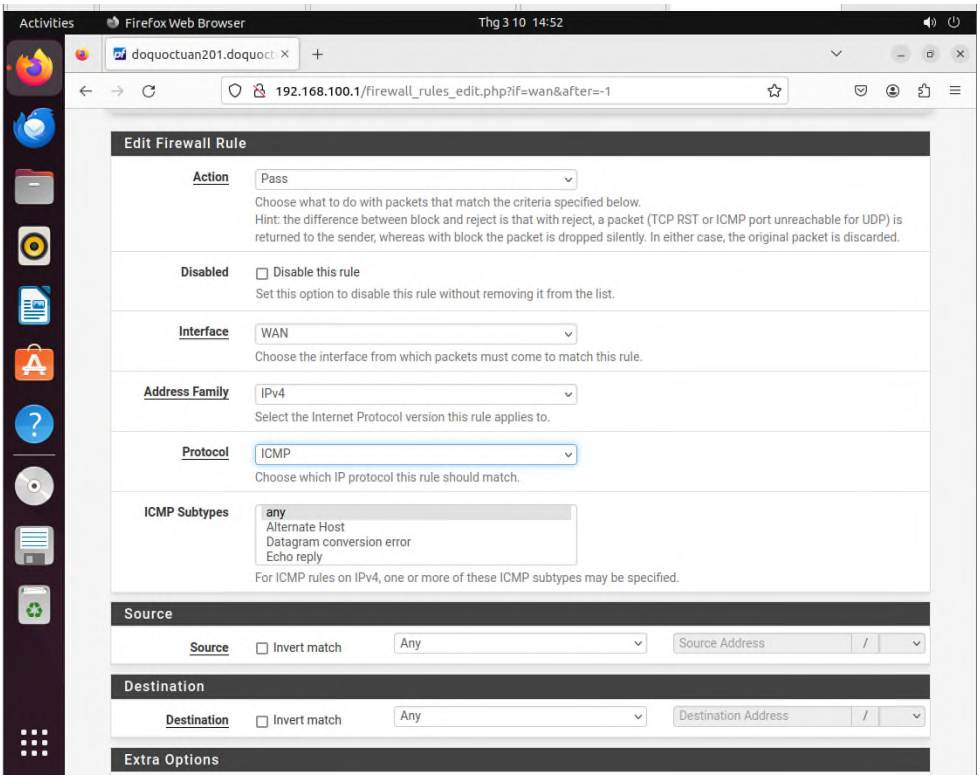


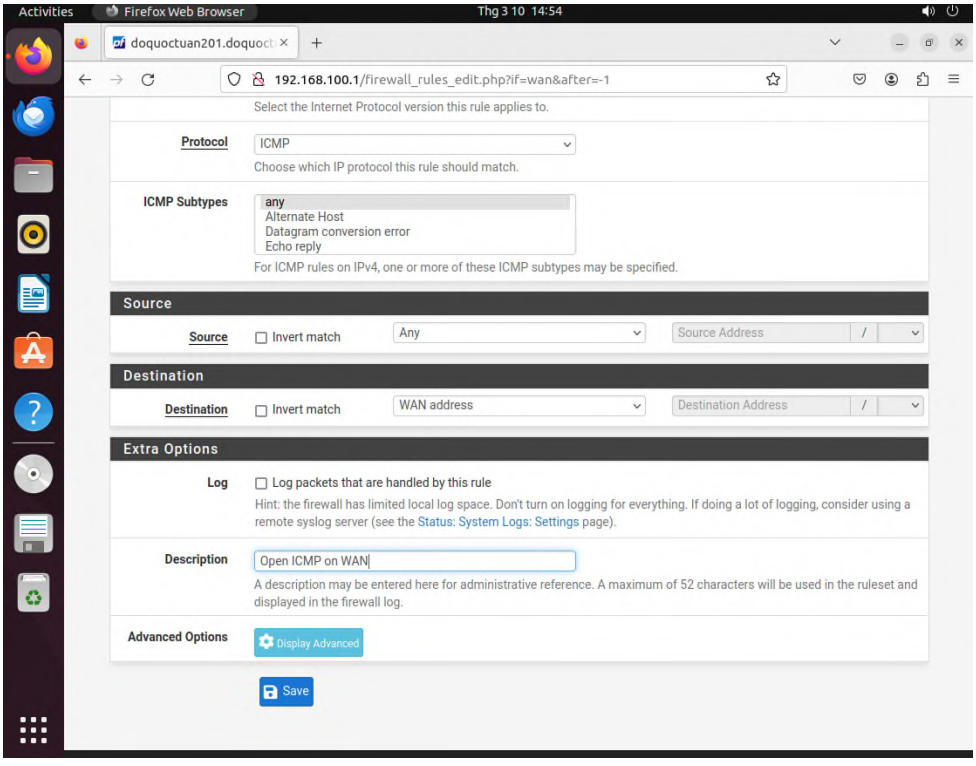
Cấu hình thành công pfsense qua giao diện web



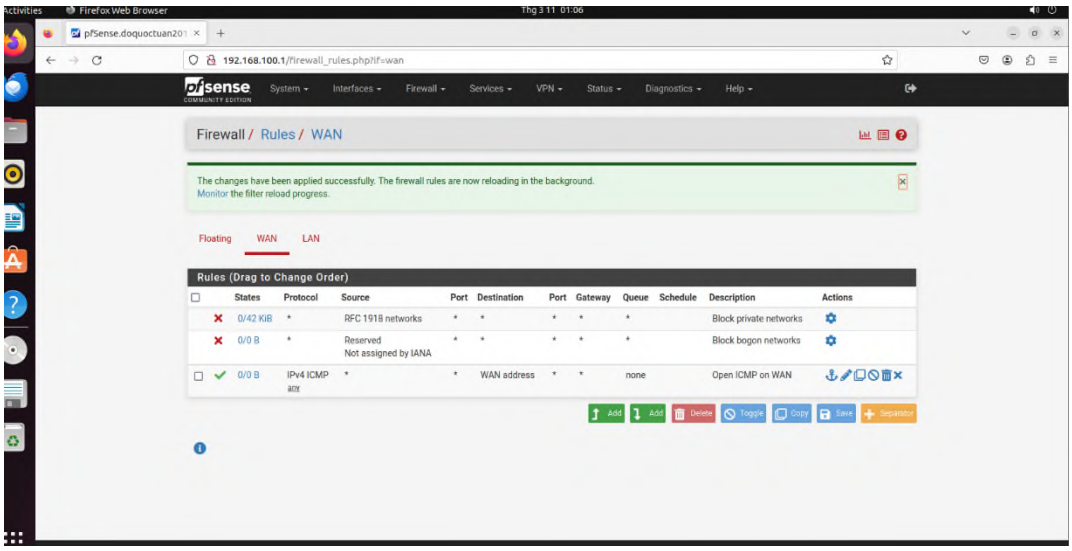
Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1.

Tại FireWall trên thanh công cụ, chọn Rules.Sau đó nhấn Add để thêm luật. Chỉnh sửa các mục như các ảnh bên dưới.

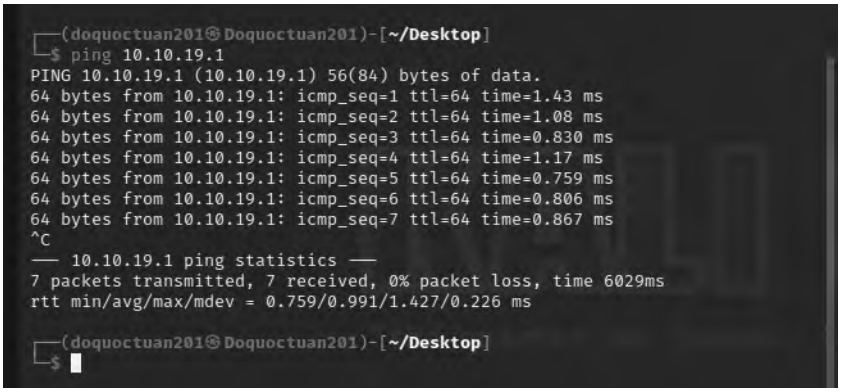




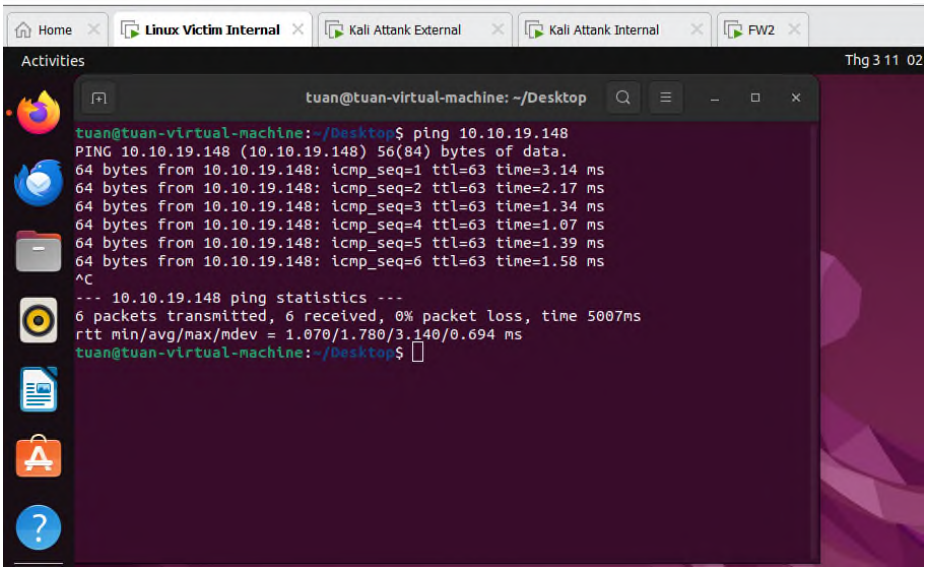
Chọn Apply Changes để lưu thay đổi.



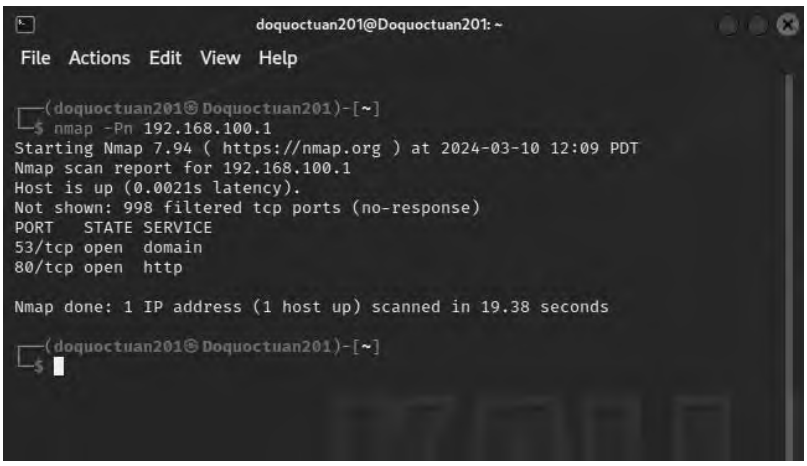
Kiểm tra bằng các ping tới 10.10.19.1 từ máy Kali attank ở mạng External



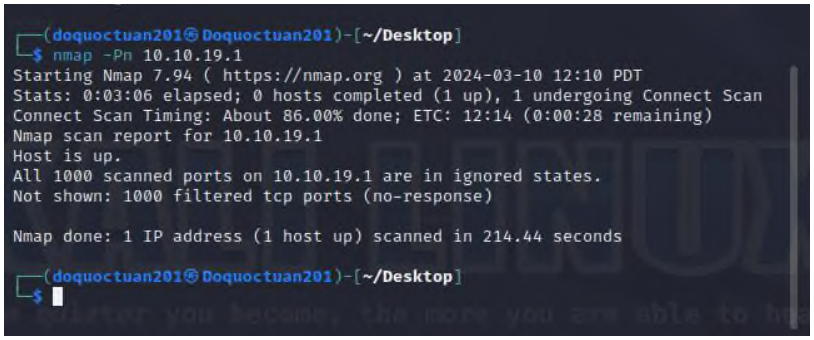
Máy Ubuntu Internal có thể ping từ mạng Internal ra máy Kali External ở mạng ngoài



Quét các cổng mở ở mạng Internal



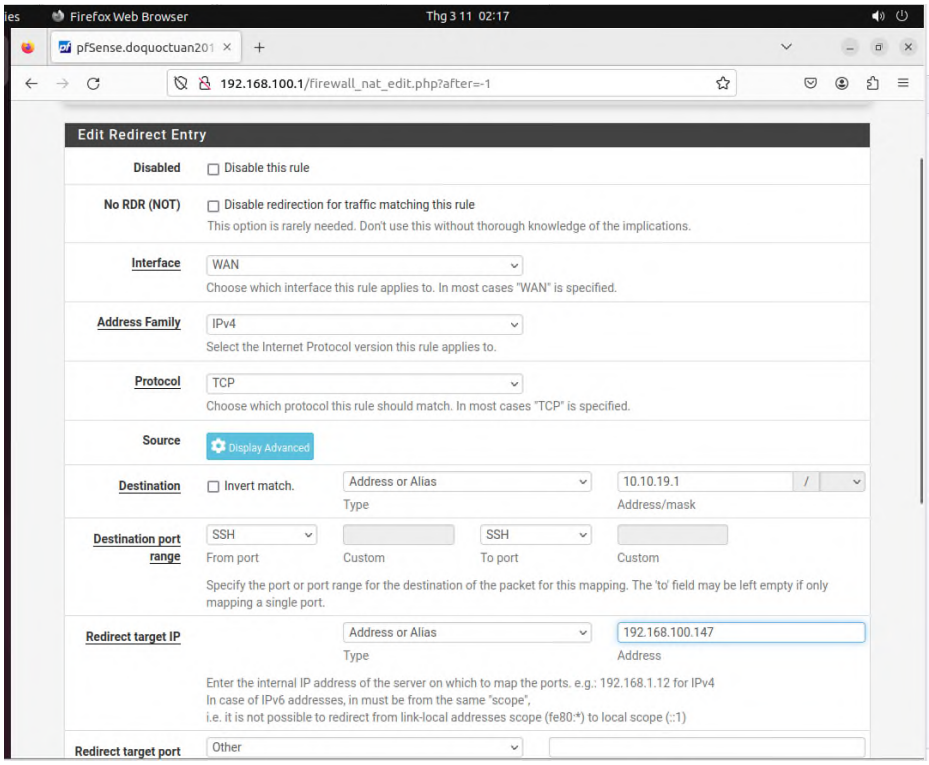
Quét các cổng mở ở mạng External

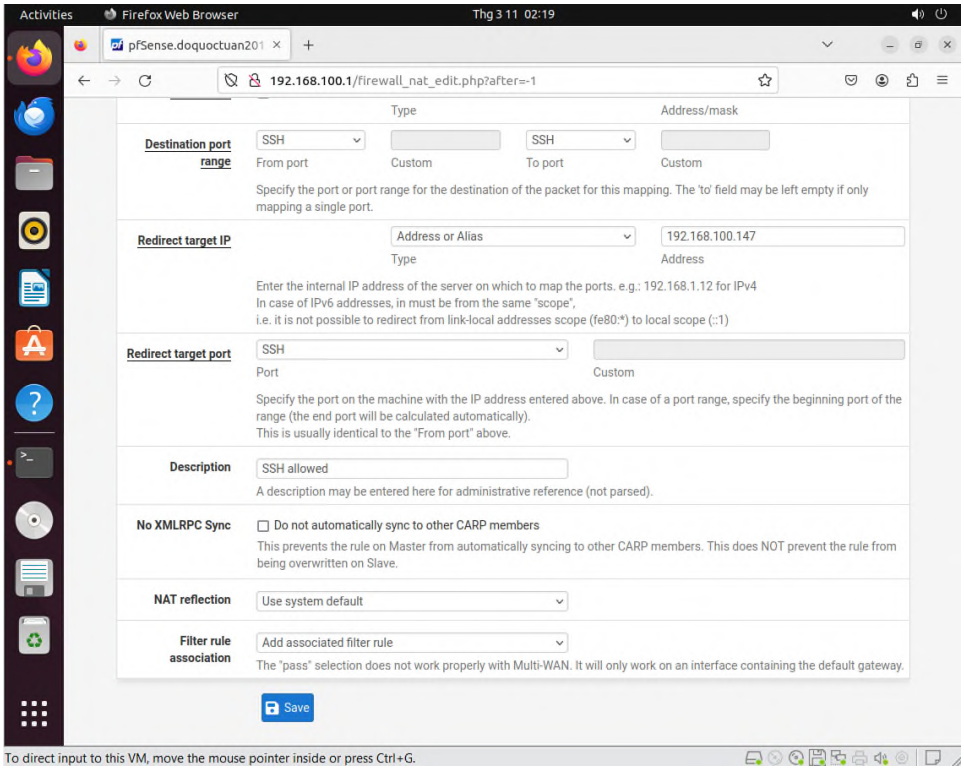


- Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng của pfSense?
+ Trong giao diện mạng Internal, theo mặc định có 2 cổng TCP được mở: Cổng 80(HTTP), Cổng 53(domain)
+ Trong giao diện mạng External không có cổng TCP nào được mở

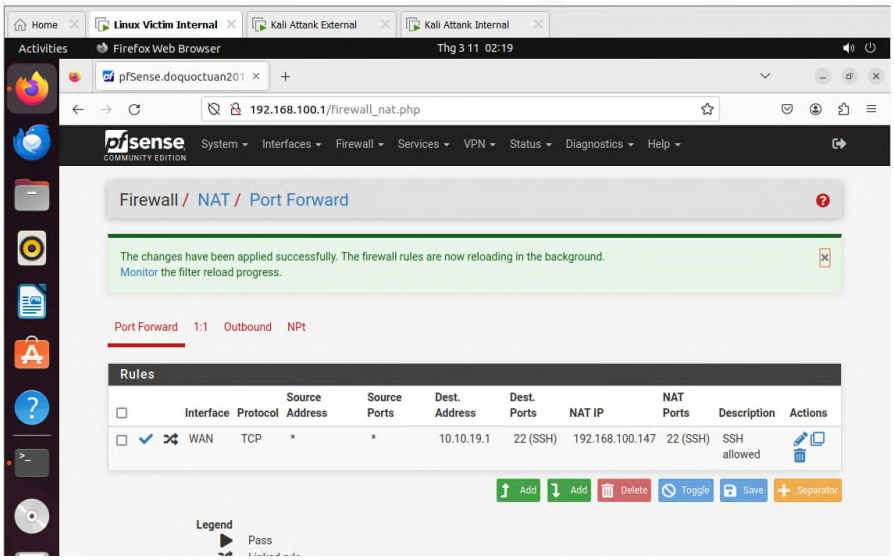
2.5. Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

- Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy Ubuntu Linux victim mạng Internal) được truy cập từ bên ngoài thông qua port forwarding. Nghĩa là khi các máy khách từ mạng 10.10.19.0/24 kết nối với địa chỉ IP của tường lửa pfSense của 10.10.19.1, chúng sẽ được chuyển hướng đến máy Linux victim trong mạng Internal.





Nhấn Apply Change để lưu thay đổi.



Kiểm tra bằng cách truy cập ssh tới 10.10.19.1 từ máy Kali External.

III. Kết luận

- Xây dựng topo mạng và cài đặt, cấu hình địa chỉ IP thành công, các máy trong mạng ping được nhau
- Cài đặt, cấu hình thành công ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal.
- Cài đặt thành công cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal.