HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 2.1
CÀI ĐẶT, CẤU HÌINH MẠNG DOANH NGHIỆP VỚI PFSENSE FIREWALL

Sinh viên thực hiện:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Các công ty thường bảo vệ hệ thống mạng bằng cách sử dụng tường lửa phần cứng hoặc phần mềm để kiểm soát lưu lượng mạng truy cập. Một số loại lưu lượng nhất định có thể bị chặn hoặc cho phép đi qua tường lửa. Việc hiểu cách thức hoạt động của tường lửa và mối quan hệ của nó với các mạng bên trong và bên ngoài sẽ rất quan trọng để có hiểu biết về bảo mật mạng.

Bài thực hành này giúp sinh viên có thể tự cài đặt, xây dựng một mạng doanh nghiệp với tường lửa để kiểm soát truy cập. Mạng mô phỏng môi trường mạng doanh nghiệp này có thể sử dụng trong các bài lab về ATTT sau này.

1.2 Tìm hiểu lý thuyết

1.2.1 Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware

VMwarecung cấp nhiều tùy chọn cấu hình mạng linh hoạt, giúp bạn mô phỏng các môi trường mạng thực tế.

1.2.1.1 Các chế độ mạng trong VMware

a) Mạng cầu nối (Bridged Network)

- Mô tả: Máy ảo kết nối trực tiếp với mạng vật lý thông qua card mạng của máy chủ (host). Máy ảo sẽ nhận địa chỉ IP từ router hoặc DHCP như các thiết bị thật.
- Ưu điểm:
    - Máy ảo hoạt động như một máy tính độc lập trong mạng LAN.
    - Truy cập được các thiết bị khác trên cùng mạng (ví dụ: máy in, máy chủ).
- Nhược điểm:
    - Máy ảo dễ bị tấn công nếu mạng không an toàn.
    - Yêu cầu mạng vật lý cho phép nhiều thiết bị kết nối.
- Ứng dụng:
    - Thiết lập và kiểm thử các dịch vụ mạng (Web server, FTP, SSH).
    - Kết nối máy ảo với các thiết bị vật lý trên cùng mạng LAN.

b) NAT (Network Address Translation)

- Mô tả: Máy ảo sử dụng IP riêng và chia sẻ kết nối Internet với máy chủ thông qua NAT.
- Ưu điểm:
    - Đơn giản, dễ cấu hình.
    - Máy ảo an toàn hơn vì không hiển thị trực tiếp trên mạng LAN.
- Nhược điểm:

- Không thể truy cập máy ảo từ bên ngoài mạng.
- Hạn chế trong việc triển khai các dịch vụ cần truy cập từ mạng ngoài.

- Ứng dụng:
  - Khi máy ảo chỉ cần kết nối Internet.
  - Kiểm thử các ứng dụng client như trình duyệt, phần mềm tải về.

c) Mạng nội bộ với máy chủ (Host-Only Network)

- Mô tả: Tạo một mạng riêng giữa máy chủ và máy ảo. Máy ảo không có quyền truy cập Internet hoặc mạng ngoài.
- Ưu điểm:
  - Cách ly hoàn toàn khỏi mạng bên ngoài.
  - Phù hợp để thiết lập môi trường kiểm thử an toàn.
- Nhược điểm:
  - Không truy cập được Internet hoặc các thiết bị bên ngoài.
- Ứng dụng:
  - Mô phỏng các hệ thống nội bộ, thử nghiệm dịch vụ mạng kín.
  - Tạo môi trường phát triển an toàn, không ảnh hưởng tới mạng bên ngoài.

d) Mạng tùy chỉnh (Custom)

- Mô tả: Người dùng có thể tạo và quản lý mạng ảo theo yêu cầu thông qua VMware Virtual Network Editor.
- Ưu điểm:
  - Linh hoạt, tùy chỉnh theo yêu cầu phức tạp.
  - Có thể tạo nhiều mạng ảo riêng biệt.
- Nhược điểm:
  - Cần kiến thức sâu hơn về mạng để cấu hình đúng.
- Ứng dụng:
  - Mô phỏng hệ thống mạng lớn, nhiều lớp (DMZ, VLAN).
  - Tạo môi trường kiểm thử cho các kịch bản phức tạp.

1.2.1.2 Các thành phần chính

a) VMware Virtual Network Adapters (Bộ điều hợp mạng ảo)

- Mỗi máy ảo có một hoặc nhiều card mạng ảo (Virtual Network Adapter), giống như card mạng vật lý trên máy thật.
- Loại card này có thể được gán vào các mạng khác nhau trong VMware.

- Có các kiểu card ảo như E1000, VMXNET3, PCnet32 (dành cho các hệ điều hành cũ).
- Người dùng có thể chọn Bridged, NAT, Host-Only hoặc mạng tùy chỉnh cho card mạng này.

b) VMware Network Switch (Bộ chuyển mạch ảo)

- Chức năng: Giống như một switch vật lý, giúp các máy ảo trong cùng một mạng có thể giao tiếp với nhau.
- Có 3 loại switch chính trong VMware Workstation:
  - VMnet0 (Bridged): Kết nối với mạng vật lý.
  - VMnet1 (Host-Only): Chỉ kết nối giữa máy ảo và máy chủ.
  - VMnet8 (NAT): Máy ảo dùng IP riêng, chia sẻ Internet với máy chủ.
- Người dùng có thể tạo thêm VMnet tùy chỉnh (VMnet2 - VMnet19) để mô phỏng các hệ thống mạng phức tạp.

c) VMware DHCP Server (Máy chủ DHCP ảo)

- Chức năng: Cấp phát địa chỉ IP tự động cho máy ảo nếu không có máy chủ DHCP bên ngoài.
- Hoạt động trên mạng Host-Only và NAT.
- Có thể bật/tắt trong VMware Virtual Network Editor.
- Ví dụ: Khi máy ảo sử dụng NAT, VMware DHCP sẽ cấp IP trong dải 192.168.xxx.xxx để máy ảo có thể truy cập Internet.

d) VMware NAT Service (Dịch vụ NAT)

- Chức năng: Dịch địa chỉ IP của máy ảo thành IP của máy chủ, giúp máy ảo truy cập Internet mà không cần IP công khai.
- Chỉ hoạt động khi chọn chế độ NAT (VMnet8).
- Có thể tùy chỉnh cổng (Port Forwarding) để máy ngoài truy cập máy ảo.
- Ví dụ: Nếu máy ảo chạy Web Server, có thể mở cổng 80 để máy bên ngoài truy cập qua NAT.

e) VMware Virtual Network Editor (Trình chỉnh sửa mạng ảo)

- Chức năng: Công cụ cho phép quản lý, tạo và tùy chỉnh các mạng ảo trong VMware.
- Tính năng chính:
  - Tạo và cấu hình mạng tùy chỉnh (VMnet).

- Cấu hình DHCP, NAT, dải IP.
- Thay đổi card mạng sử dụng cho chế độ Bridged.

1.2.2 Tìm hiểu về Pfsense

pfSense là một phân phối phần mềm mã nguồn mở dựa trên hệ điều hành FreeBSD, được thiết kế để hoạt động như một tường lửa và bộ định tuyến mạng mạnh mẽ. Được phát triển từ năm 2004, pfSense đã trở thành một giải pháp phổ biến cho cả cá nhân và doanh nghiệp nhờ tính linh hoạt và khả năng tùy chỉnh cao.

Các tính năng chính của pfSense:

- Tường lửa trạng thái (Stateful Firewall): pfSense sử dụng công cụ lọc gói PF từ OpenBSD, cho phép kiểm soát lưu lượng mạng dựa trên trạng thái kết nối, cung cấp khả năng bảo mật cao.
- Chuyển tiếp địa chỉ mạng (NAT): Hỗ trợ NAT để ánh xạ địa chỉ IP nội bộ sang địa chỉ IP công khai, giúp quản lý và bảo mật mạng nội bộ hiệu quả.
- Hỗ trợ VPN: pfSense tích hợp các giao thức VPN như IPsec, OpenVPN và L2TP, cho phép thiết lập kết nối an toàn giữa các mạng hoặc người dùng từ xa.
- Cân bằng tải và chuyển đổi dự phòng (High Availability): Sử dụng giao thức CARP, pfSense có thể cấu hình hai tường lửa trên hai máy giống hệt nhau để sao lưu và tự động thay thế trong trường hợp một trong hai bị lỗi, đảm bảo tính sẵn sàng cao cho hệ thống mạng.
- Cổng kiểm soát truy cập (Captive Portal): Cho phép quản lý truy cập mạng bằng cách yêu cầu người dùng xác thực trước khi sử dụng tài nguyên mạng, thường được sử dụng trong các môi trường như quán cà phê, khách sạn hoặc trường học.
- Hỗ trợ PPPoE Server: pfSense có thể hoạt động như một máy chủ PPPoE, cung cấp dịch vụ truy cập Internet cho các khách hàng thông qua giao thức PPPoE.
- Giám sát và báo cáo: Cung cấp các công cụ giám sát lưu lượng mạng, tạo biểu đồ RRD và cung cấp thông tin trạng thái theo thời gian thực, giúp quản trị viên theo dõi và phân tích hiệu suất mạng.

pfSense là một giải pháp tường lửa và bộ định tuyến mạnh mẽ, linh hoạt và đáng tin cậy, phù hợp cho cả môi trường gia đình và doanh nghiệp. Với khả năng tùy chỉnh cao và cộng đồng hỗ trợ nhiệt tình, pfSense giúp quản trị viên mạng xây dựng và quản lý hệ thống mạng an toàn và hiệu quả.

1.3 Kết chương

Ở chưởng này đã tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmvare và pfsense.

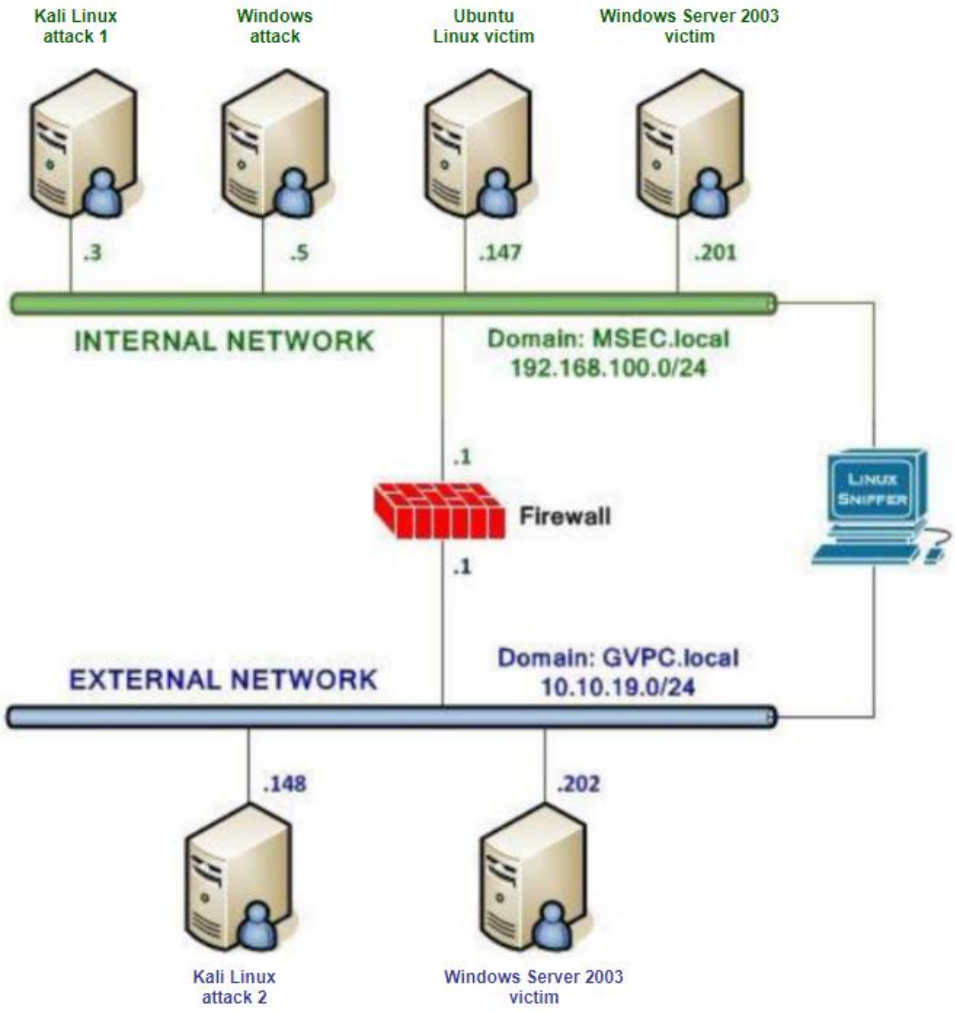
CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Trong mạng Internal:
    - Máy Kali Linux Attack
    - Máy Linux Victim
    - Máy Windows Server 2019
- Trong mạng External:
    - Máy Kali Linux Attack
    - Máy Windows Server 2019
- Máy pfsense Firewall

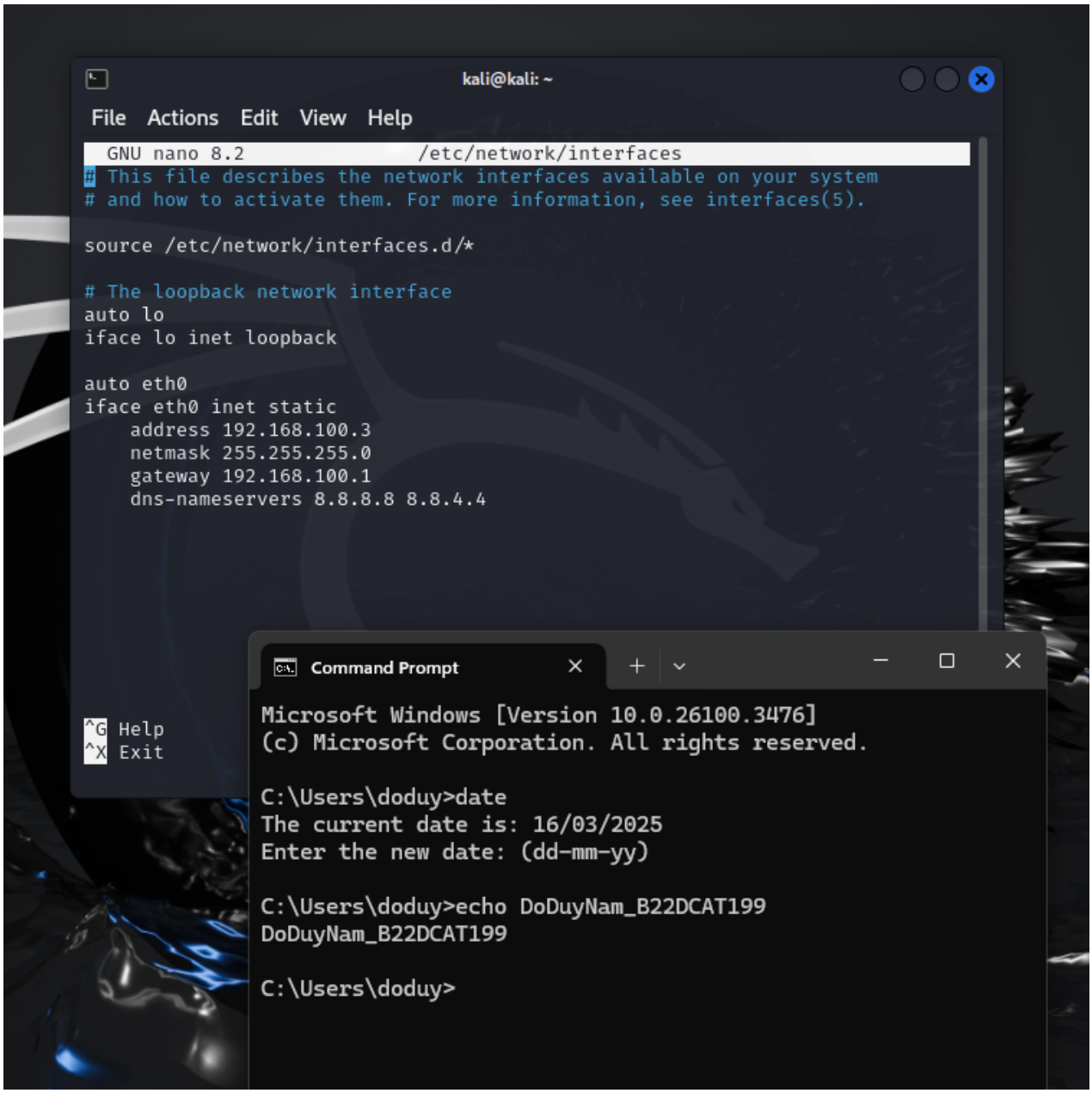
2.2 Các bước thực hiện

2.2.1 Cấu hình topo mạng

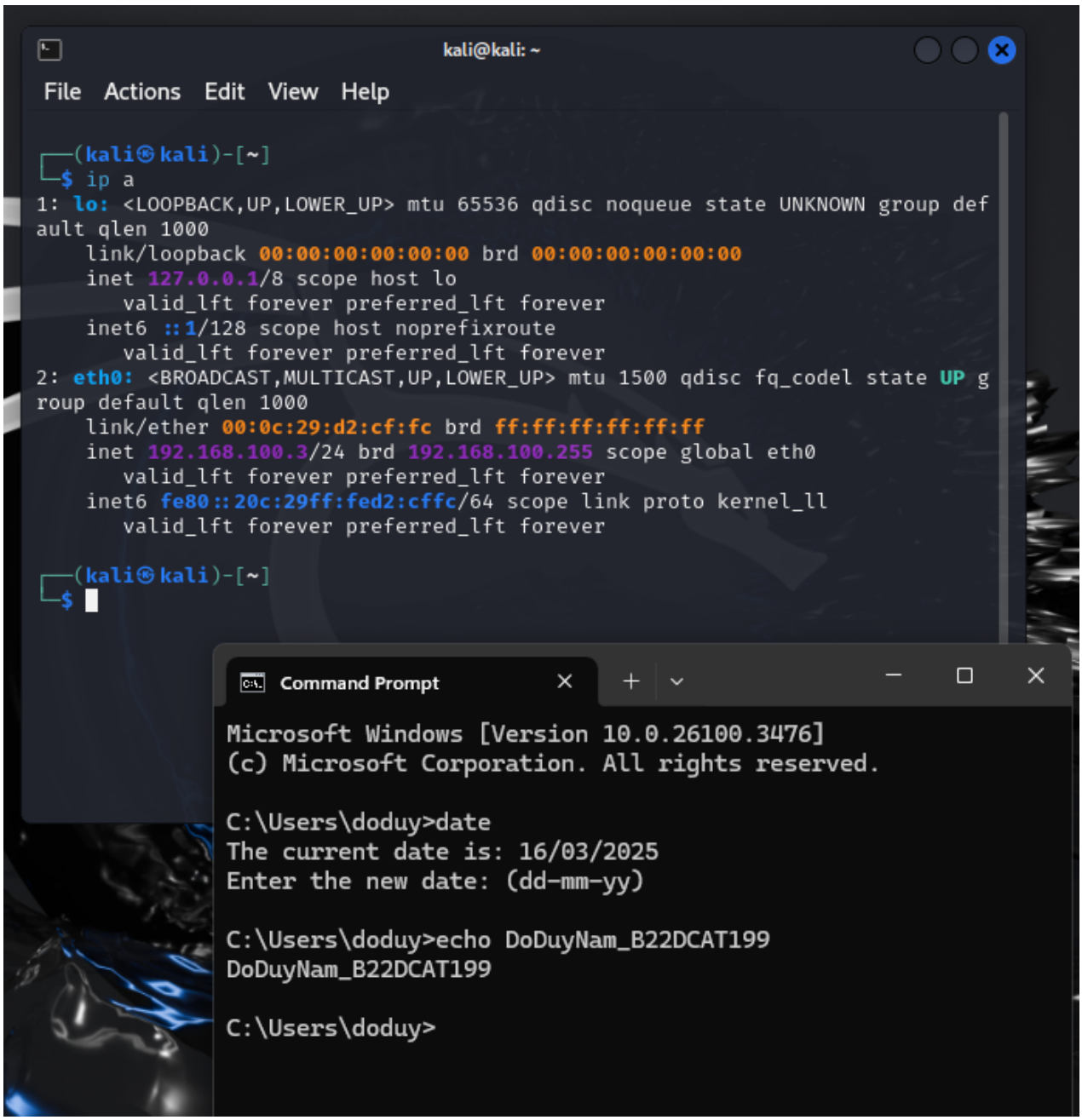


Hình 1 Cấu hình topo mạng yêu cầu

- Ở máy Kali Linux Attack trong mạng internal, sử dụng câu lệnh sudo nano /etc/network/interfaces để cấu hình lại địa chỉ IP thành 192.168.100.3

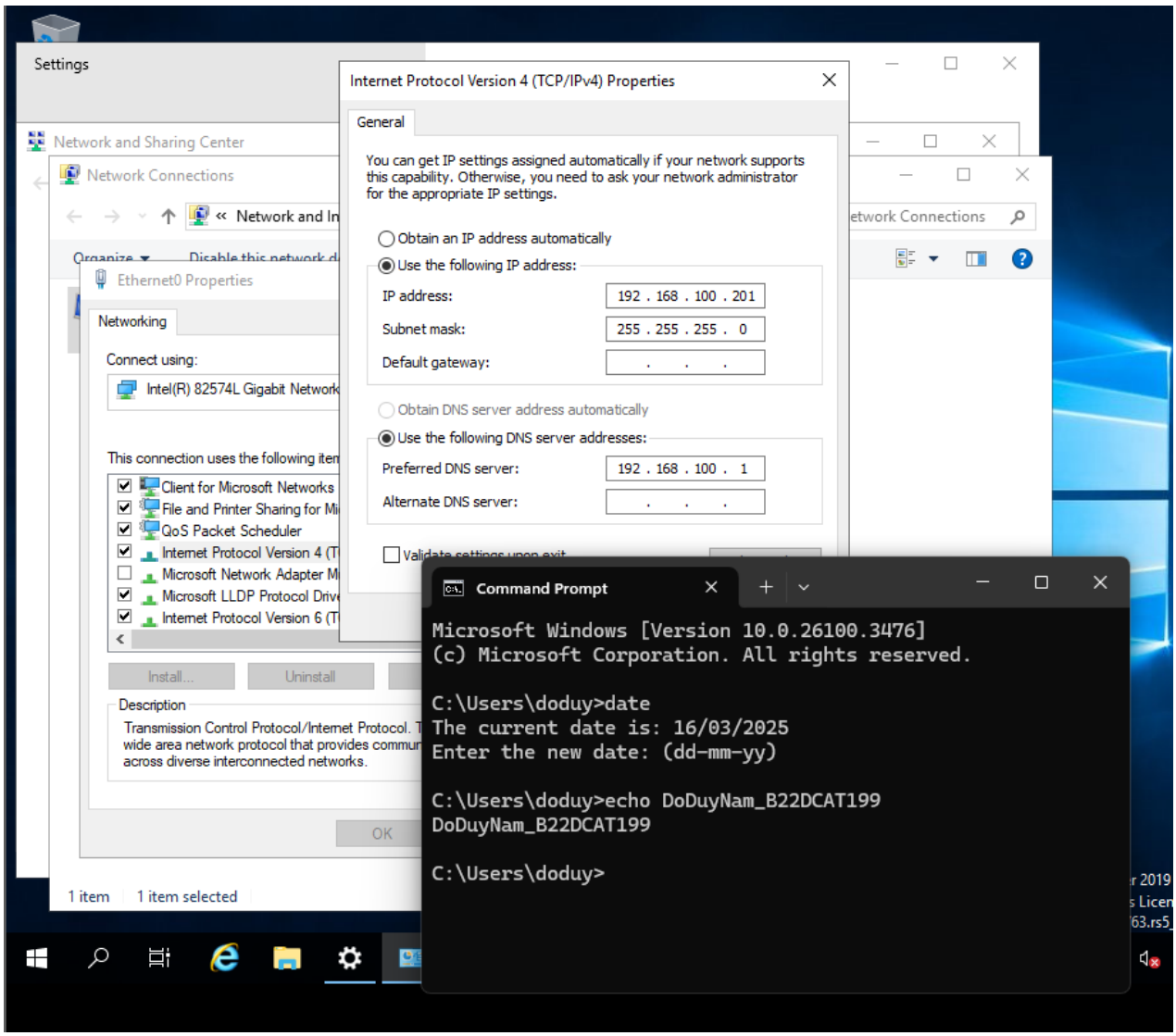


Hình 2 Cấu hình địa chỉ ip trên máy Kali Linux Attack trong mạng Internal

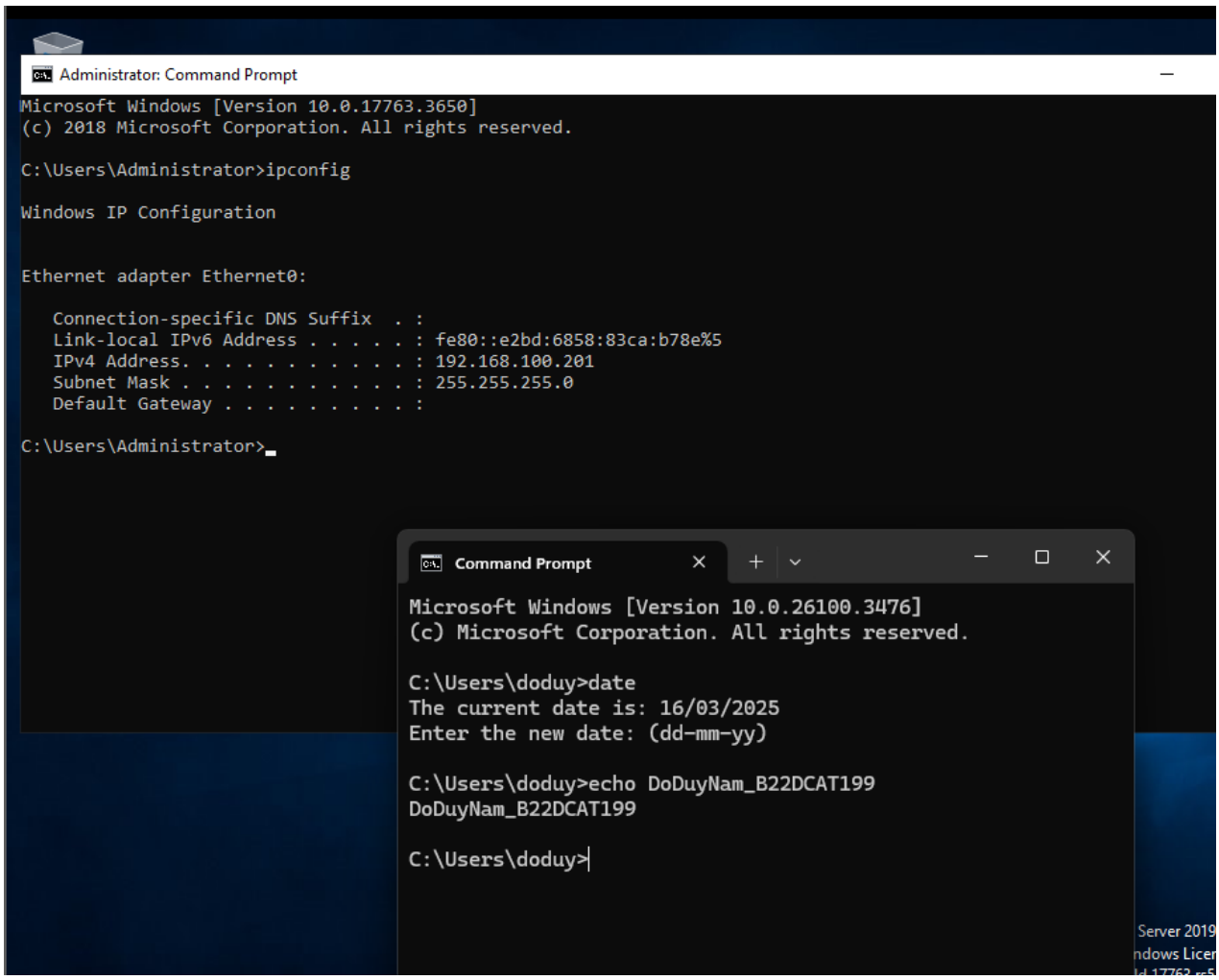


Hình 3 Cấu hình thành công địa chỉ IP cho máy Kali Linux Attack trong mạng Internal

- Ở máy Windows Server Victim trong mạng Internal cấu hình địa chỉ IP thành 192.16.100.201

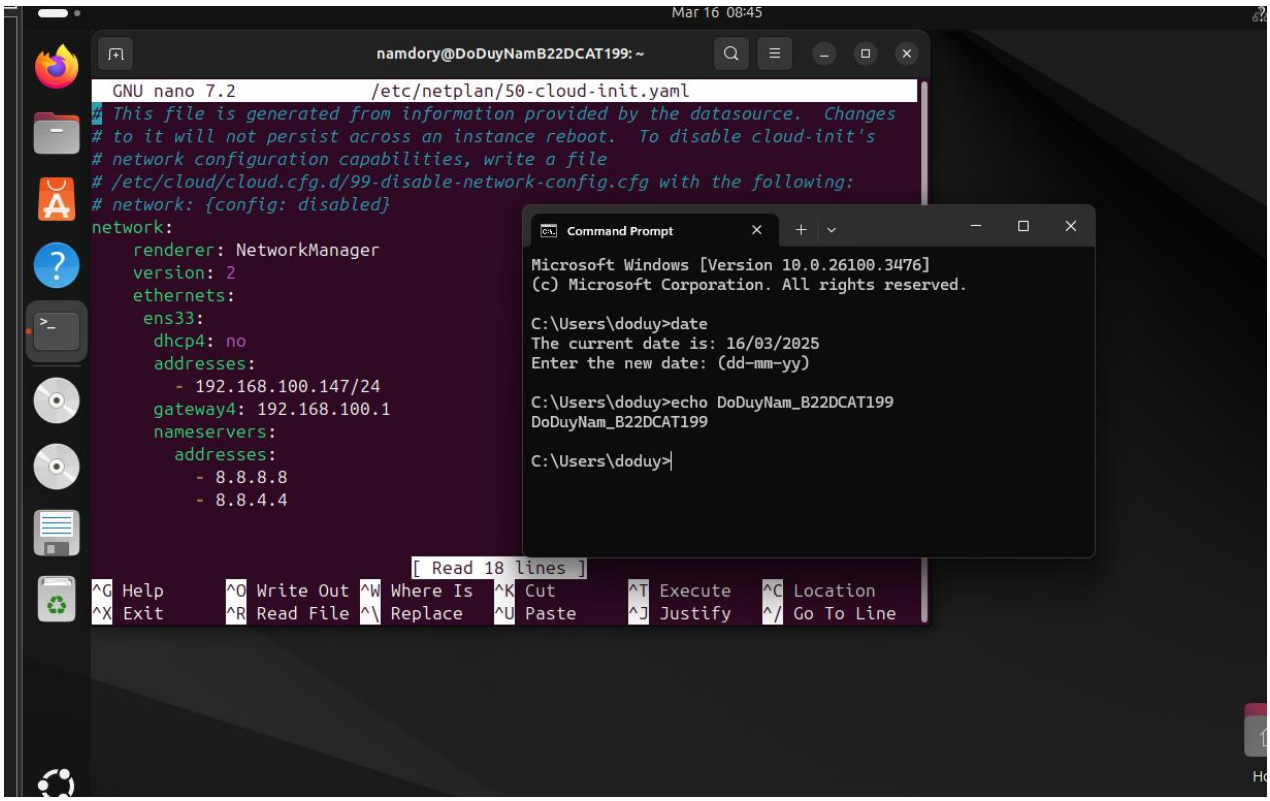


Hình 4 Cấu hình địa chỉ IP trên máy Windows Server Victim trong mạng Internal

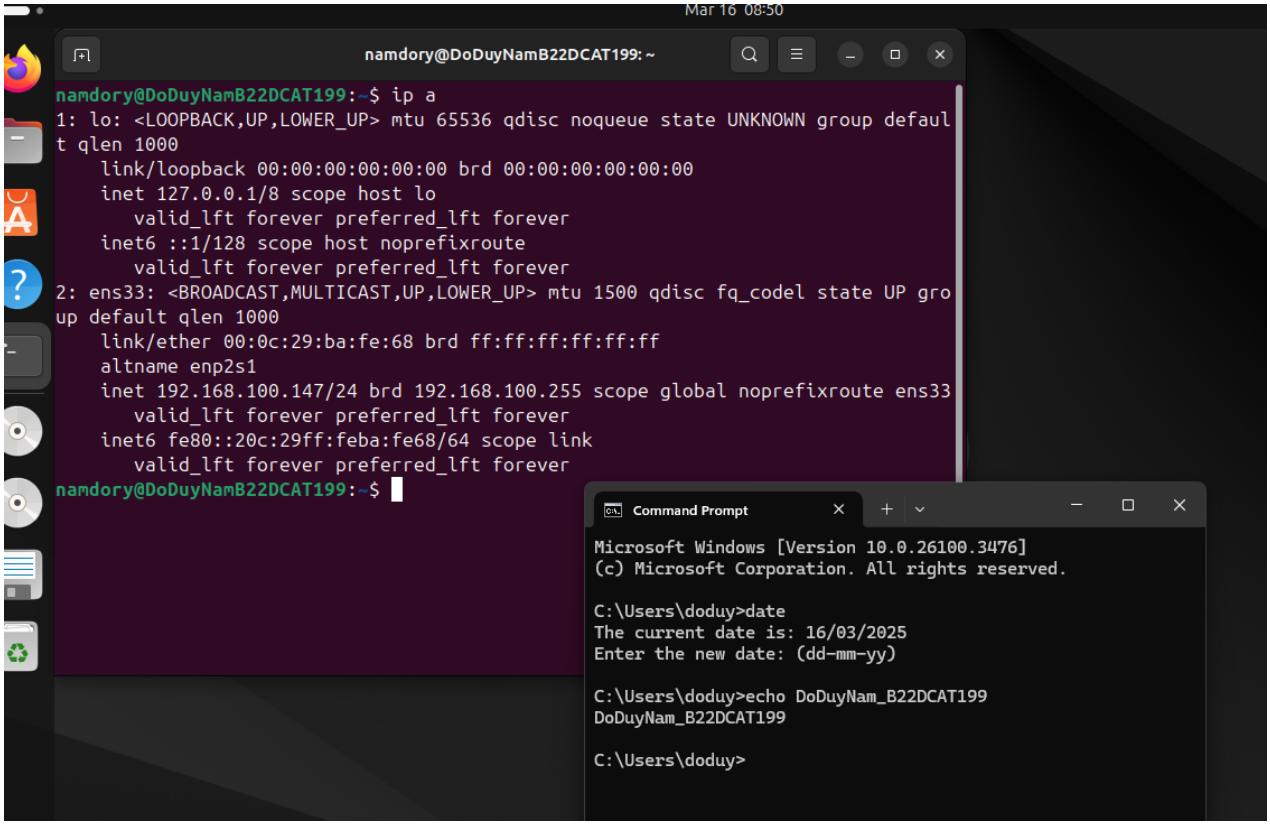


Hình 5 Cấu hình thành công địa chỉ IP trên máy Windows Server Victim trong mạng Internal

- Ở máy Linux Victim Internal sử dụng câu lệnh sudo nano /etc/netplan để cấu hình địa chỉ IP thành 192.168.100.147

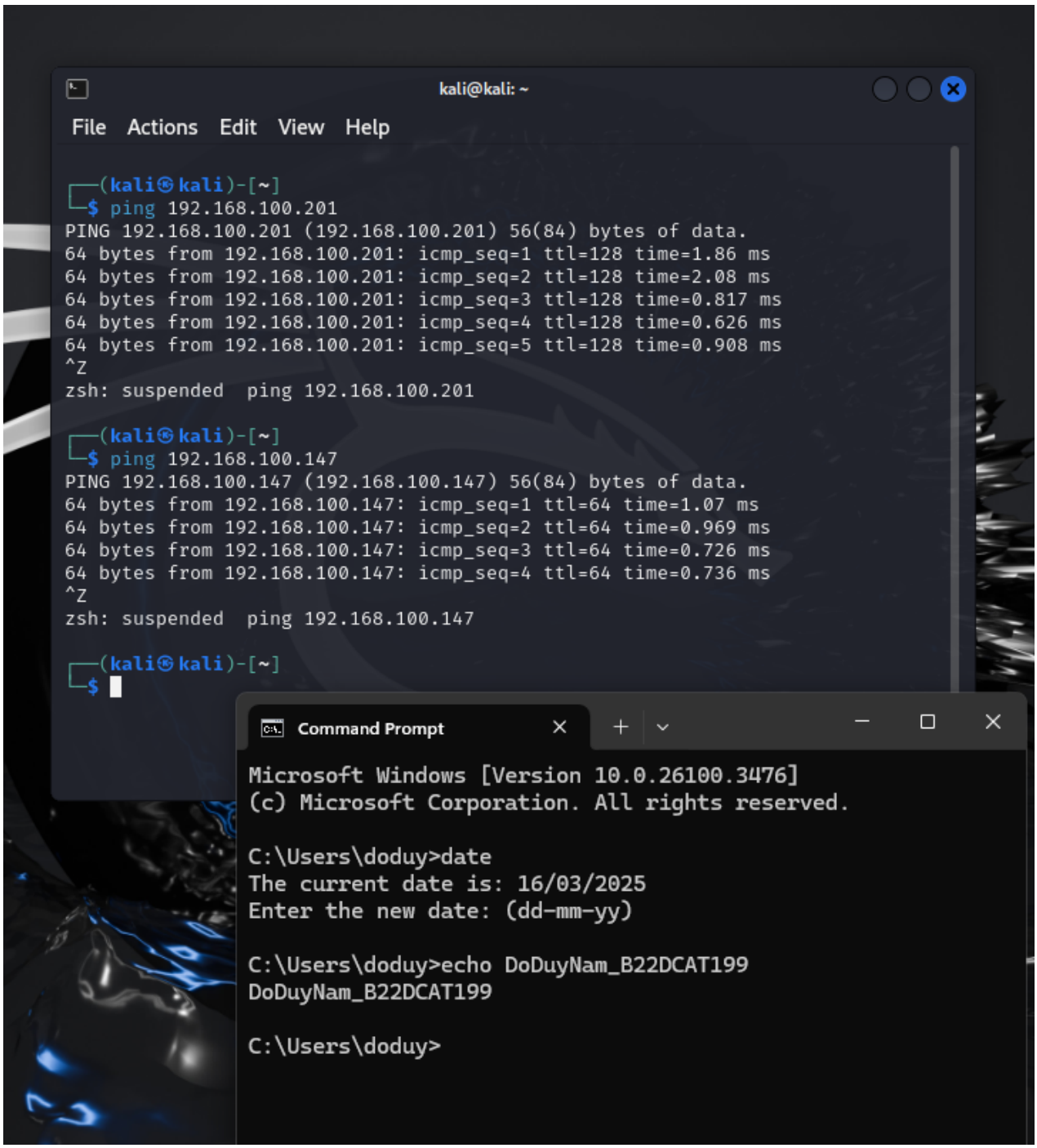


Hình 6 Cấu hình địa chỉ IP trên máy Linux Victim trong mạng Internal

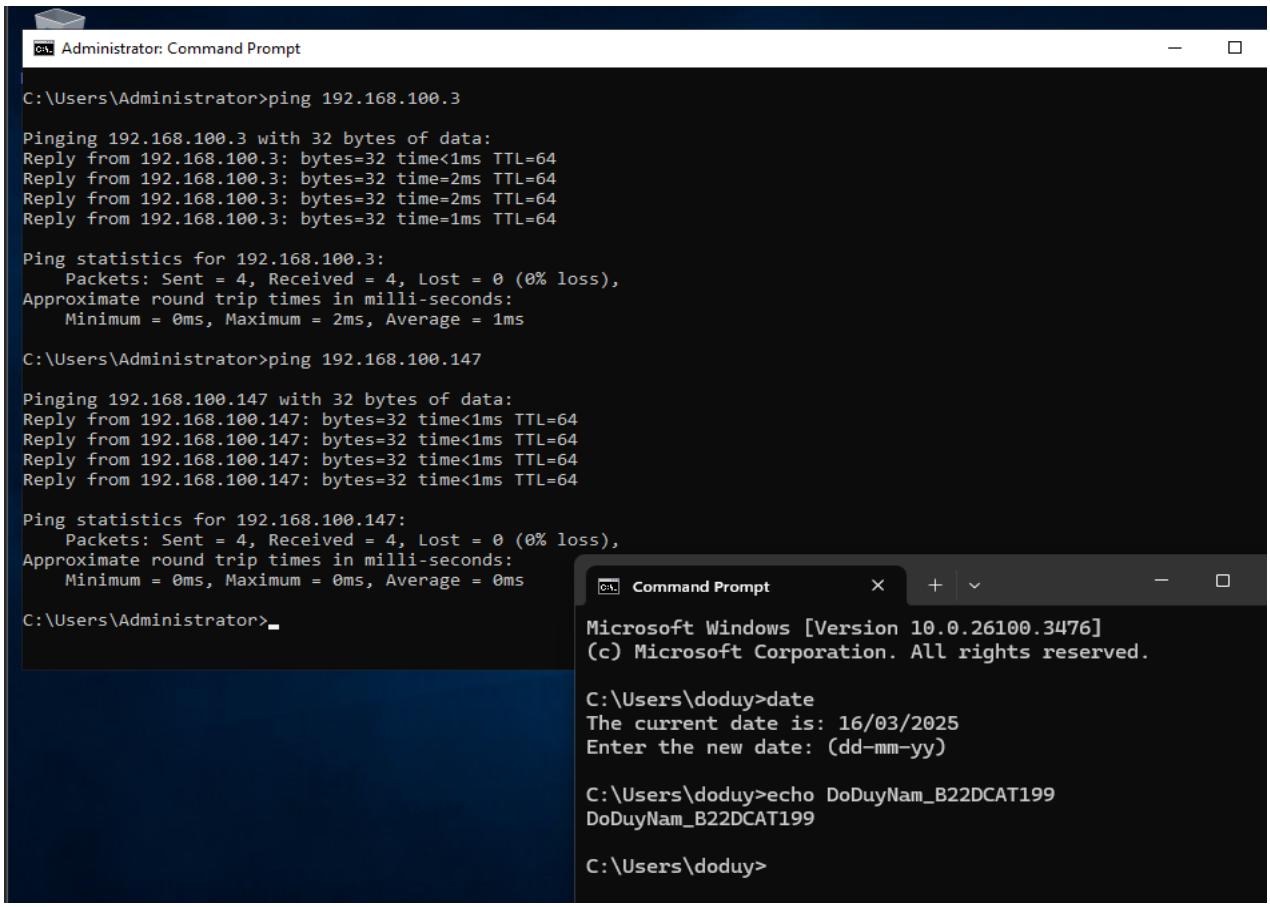


Hình 7 Cấu hình thành công địa chỉ IP trên máy Linux Victim trong mạng Internal

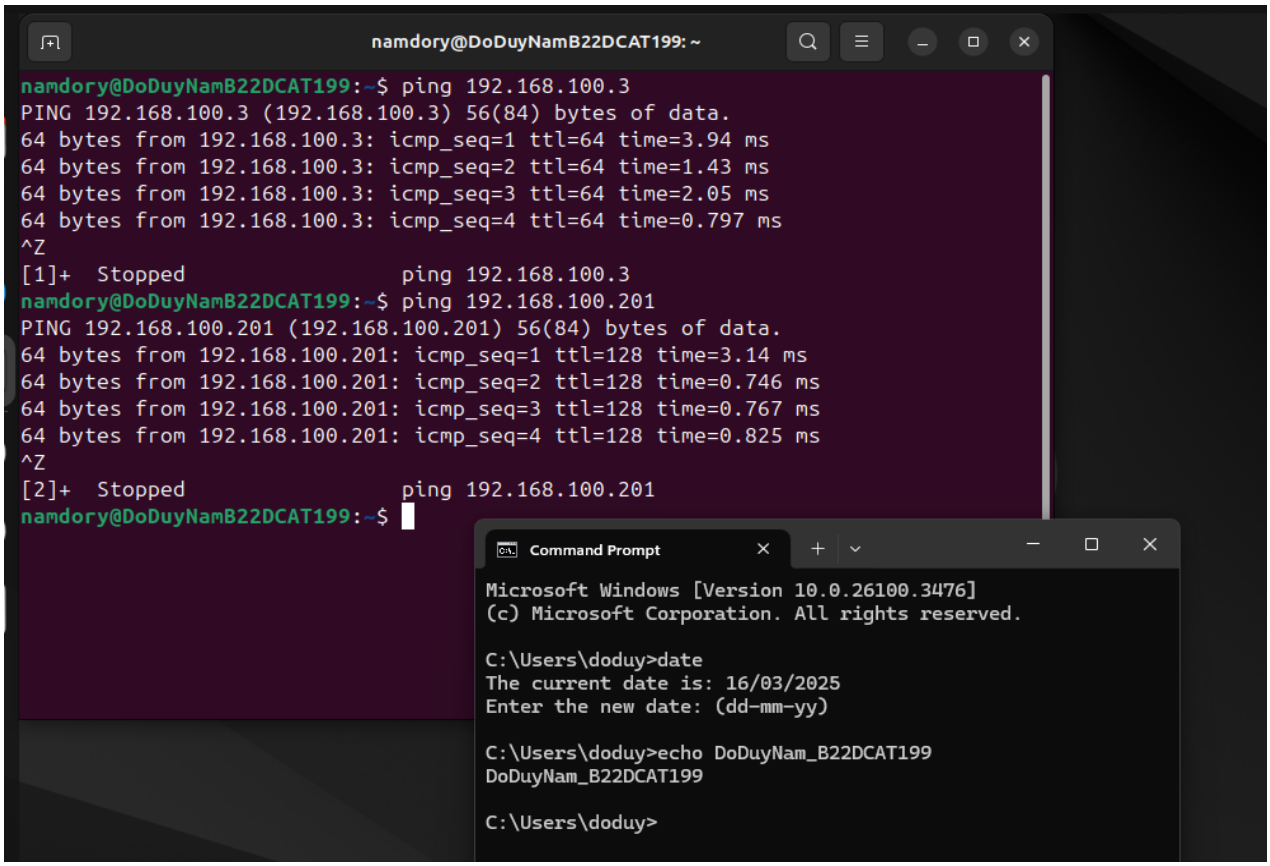
- Trên các máy trong mạng Internal sử dụng lệnh ping để kiểm tra



Hình 8 Máy Kali Linux trong mạng Internal ping thành công tới 2 máy còn lại

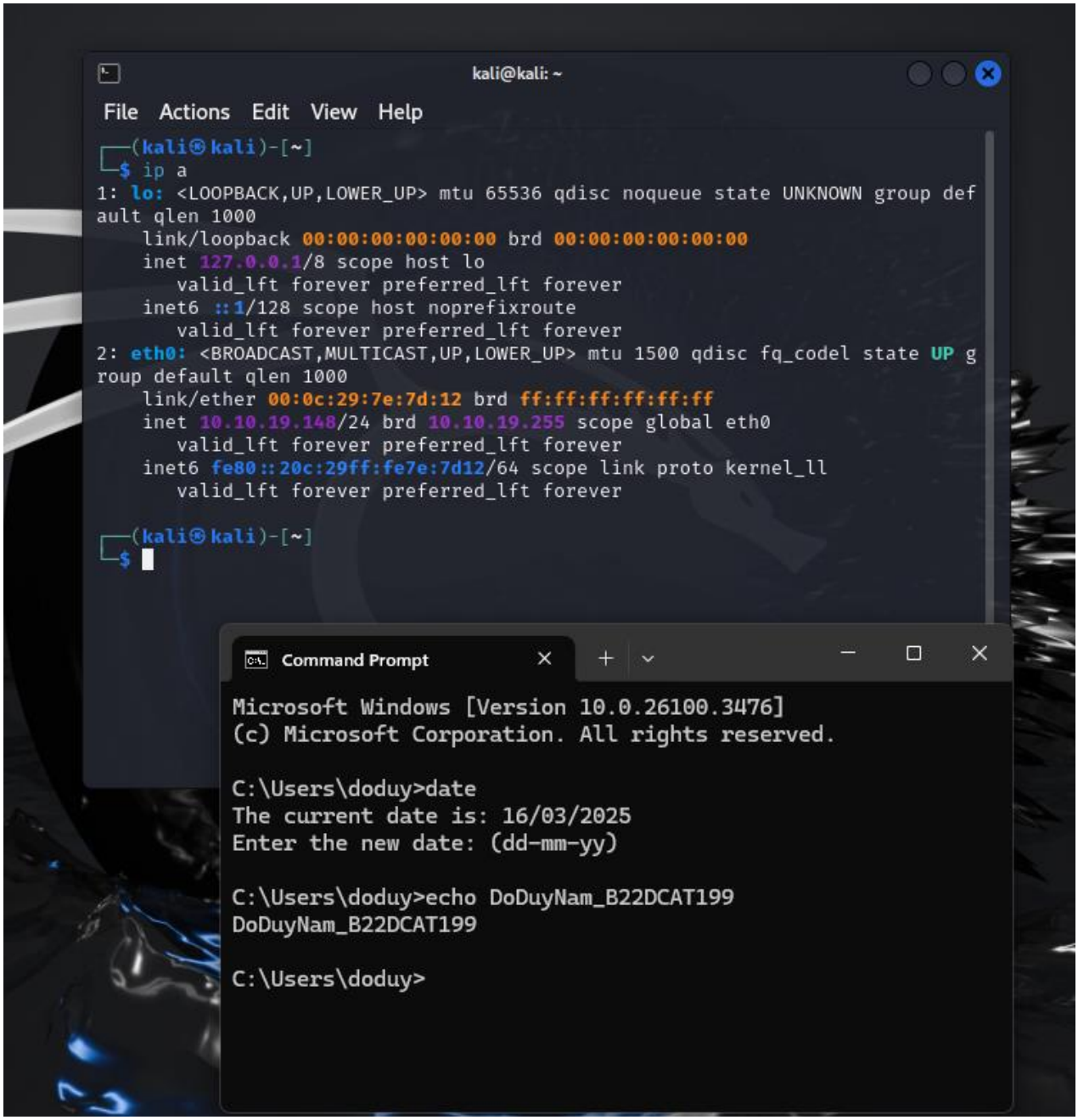


Hình 9 Máy Windows Server trong mạng Internal ping thành công tới 2 máy còn lại

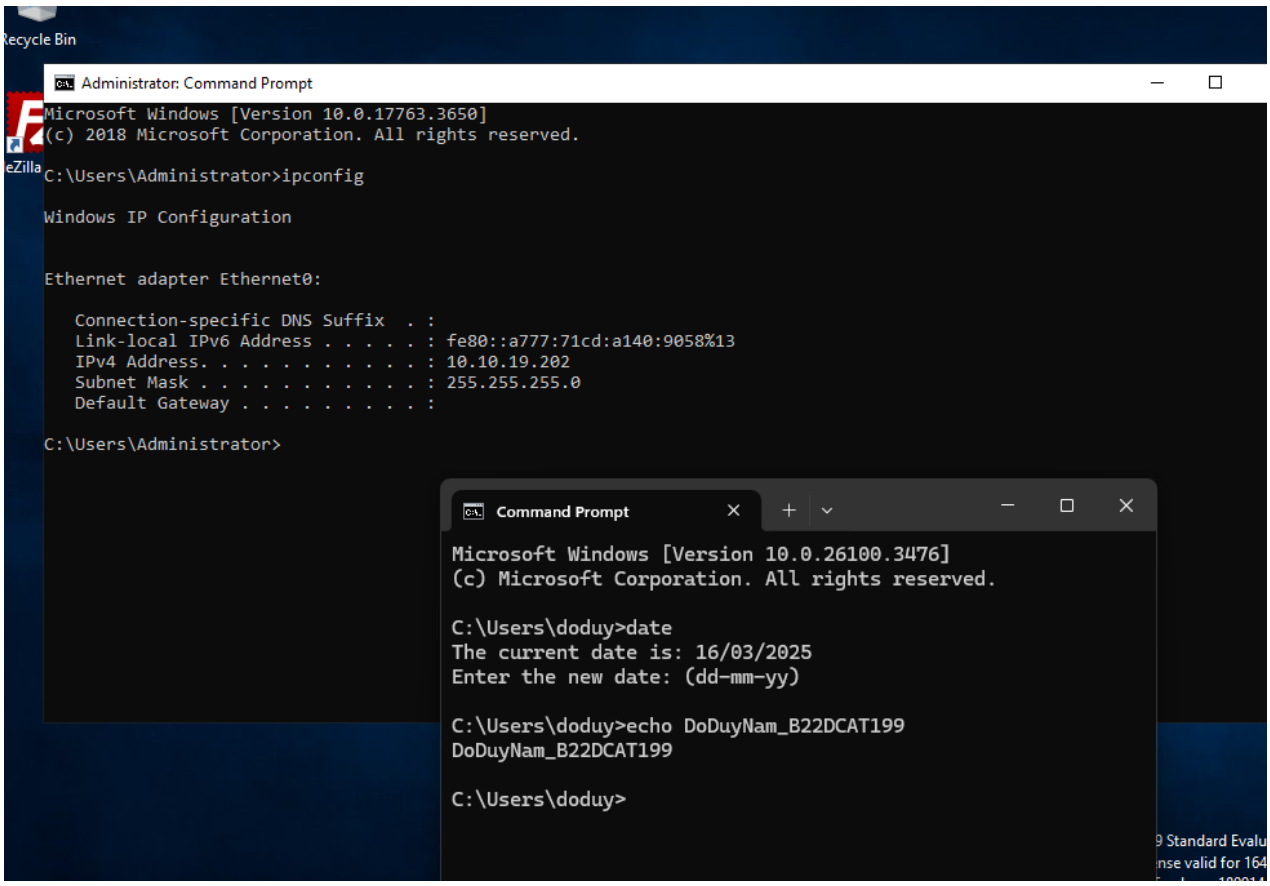


Hình 10 Máy Linux Victim trong mạng Internal ping thành công tới 2 máy còn lại

- Làm tương tự với các máy trong mạng External để cấu hình địa chỉ IP cho máy Linux Attack và máy Windows Server Victim với địa chỉ IP lần lượt là 10.10.19.148 và 10.10.19.202.

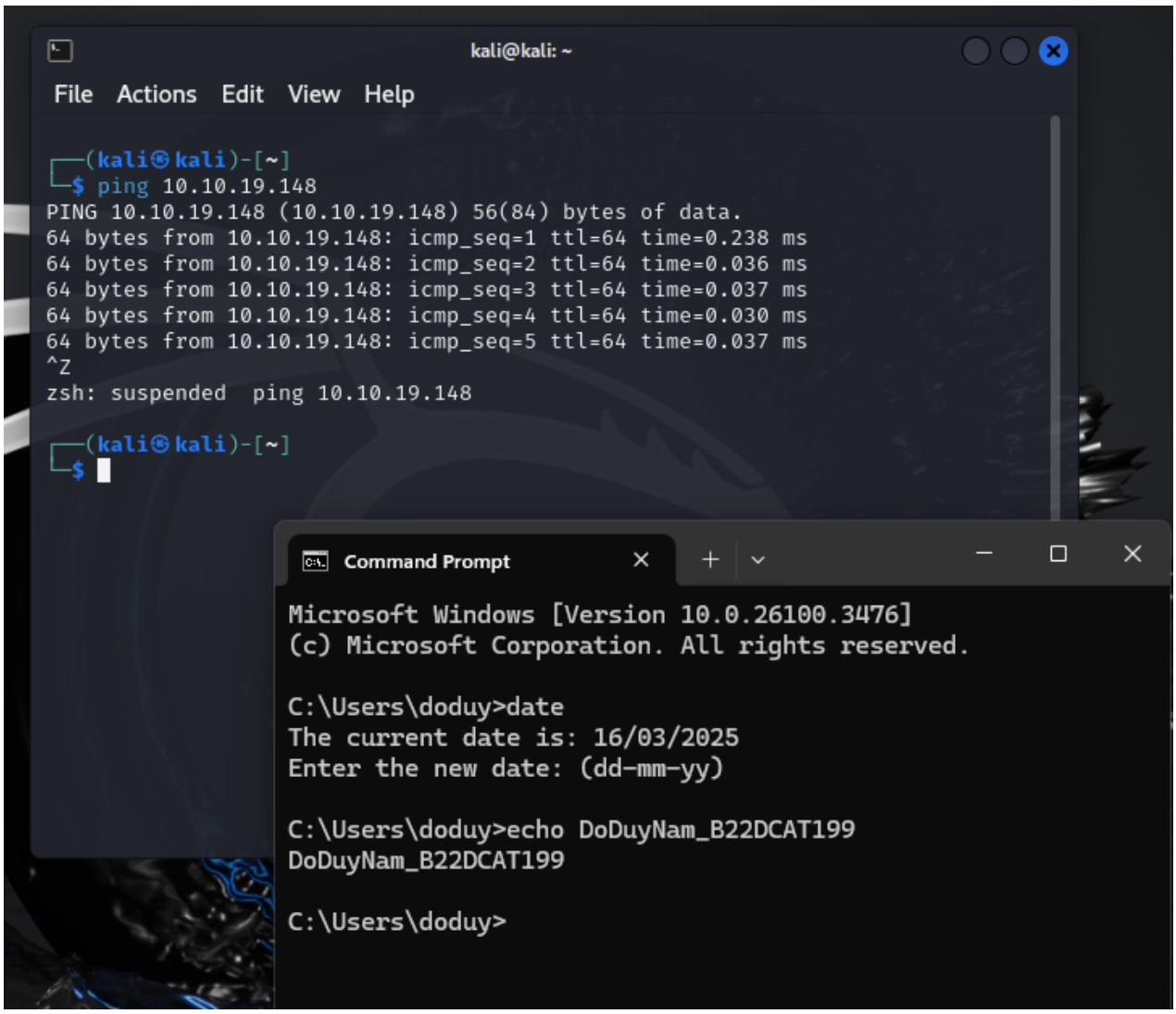


Hình 11 Cấu hình thành công địa chỉ IP trên máy Linux Attack trong mạng External

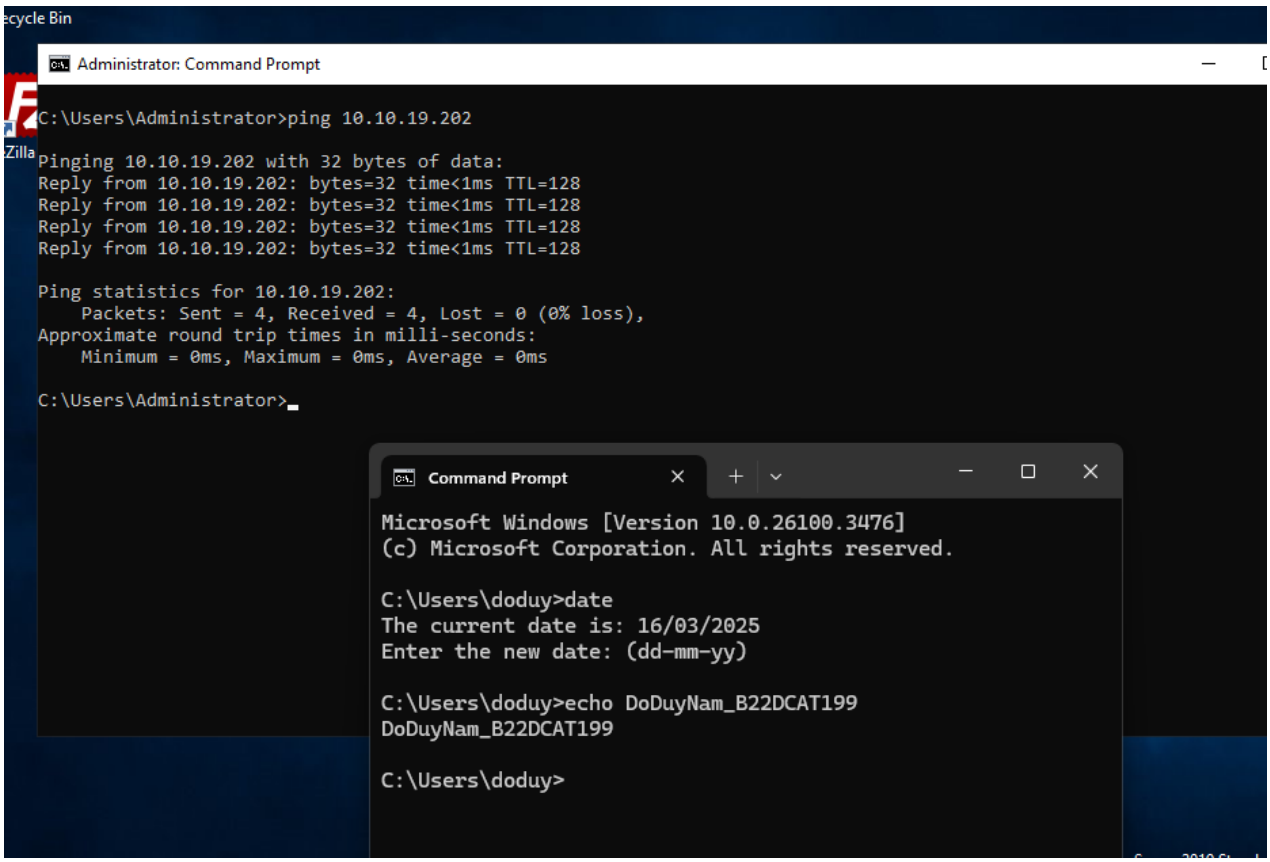


Hình 12 Cấu hình thành công địa chỉ IP trên máy Windows Server Victim trong mạng External

- Trên các máy External sử dụng lệnh ping để kiểm tra

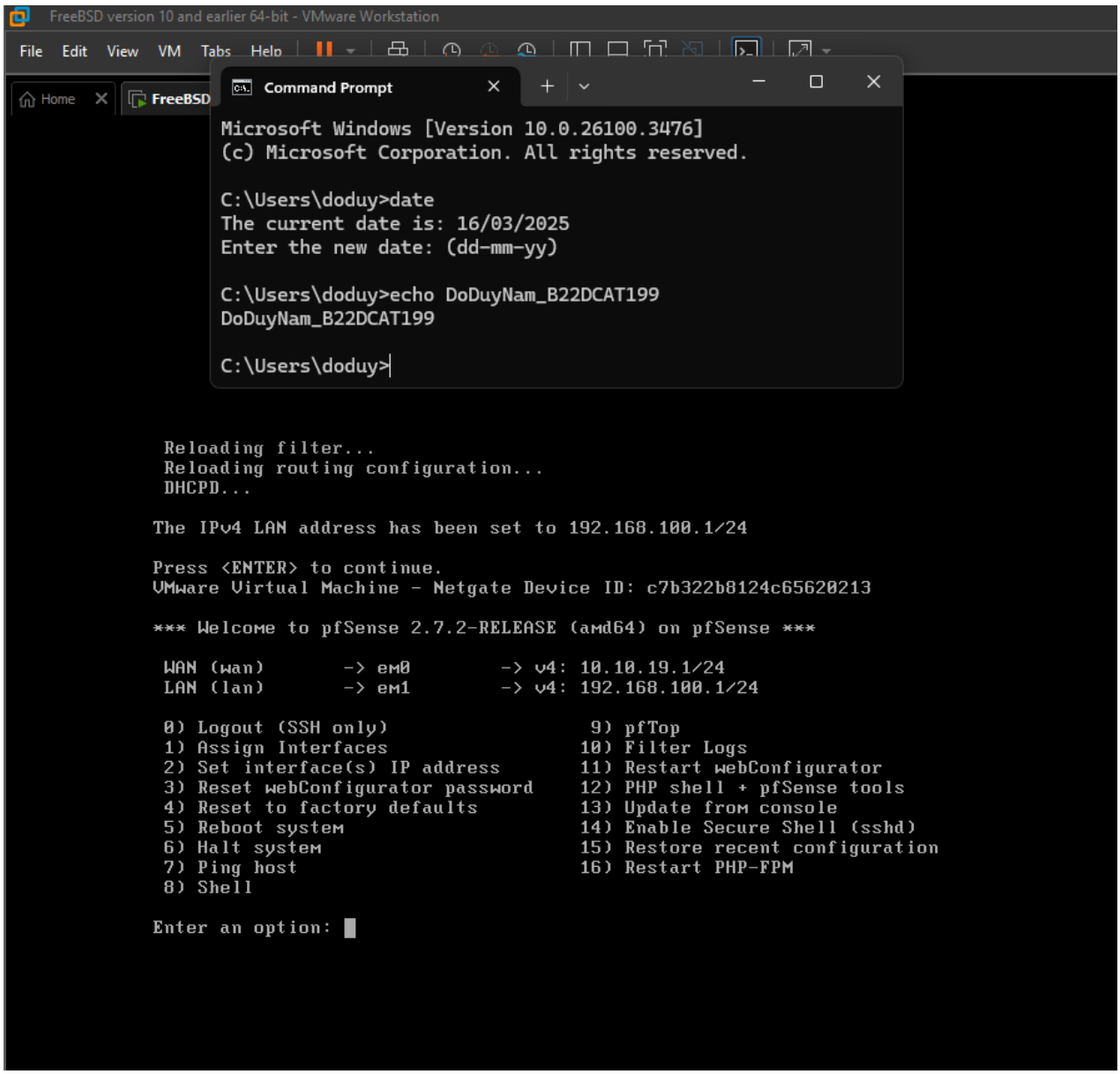


Hình 13 Máy Linux Attack ping thành công tới máy Windows Server Victim trong mạng External



Hình 14 Máy Windows Server Victim ping thành công tới máy Linux Attack trong mạng External

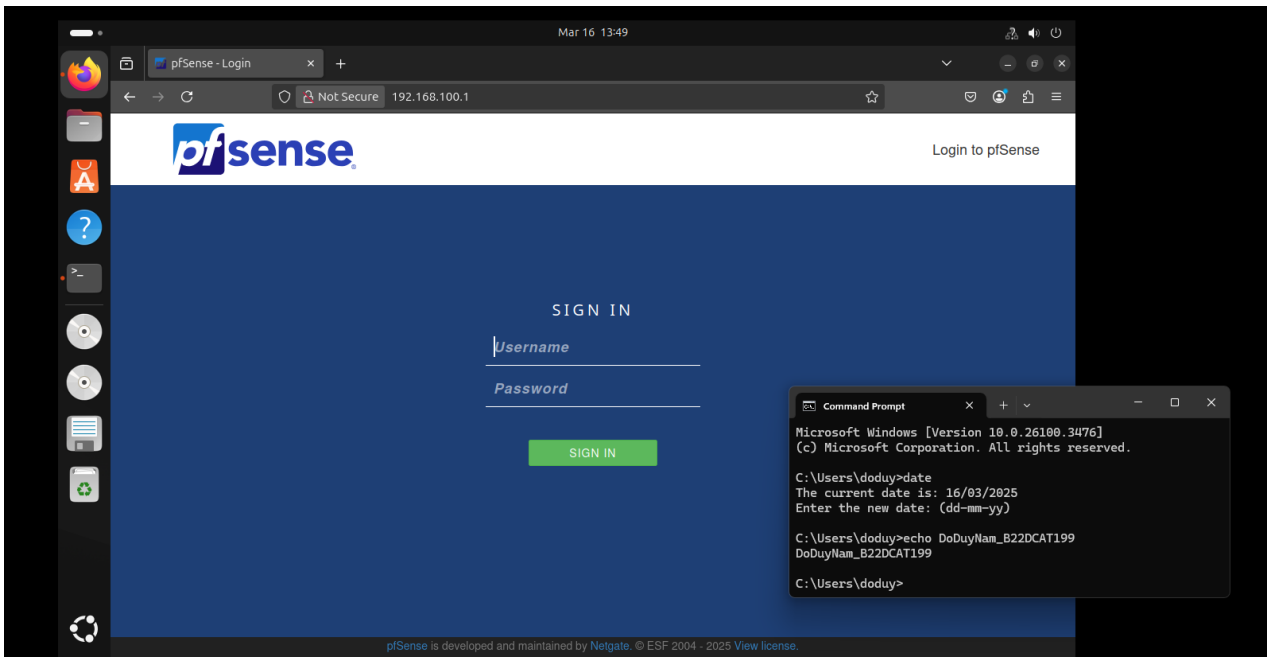
- Ở máy pfsense cấu hình địa chỉ IP là 10.10.19.1 cho mạng WAN và 192.168.100.1 cho mạng LAN



Hình 15 Cấu hình địa chỉ IP thành công trên máy pfsense

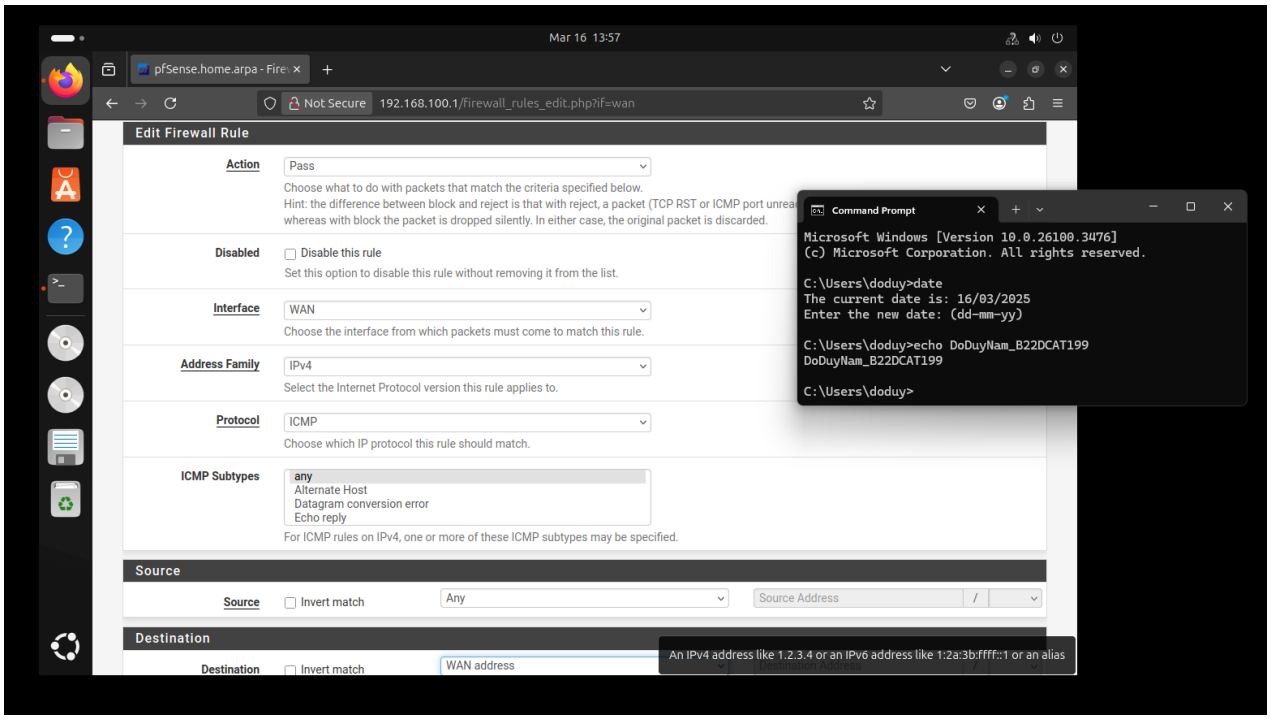
2.2.2 Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

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



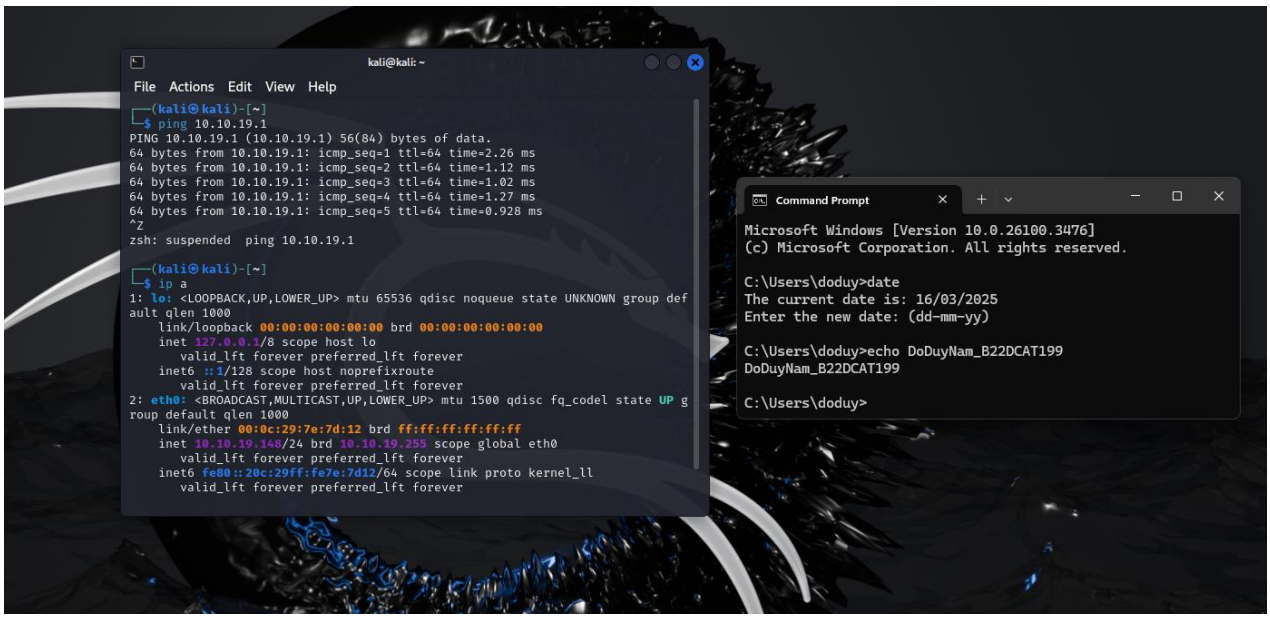
Hình 16 Truy cập vào pfsense qua giao diện Web

- Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1 như hình dưới đây



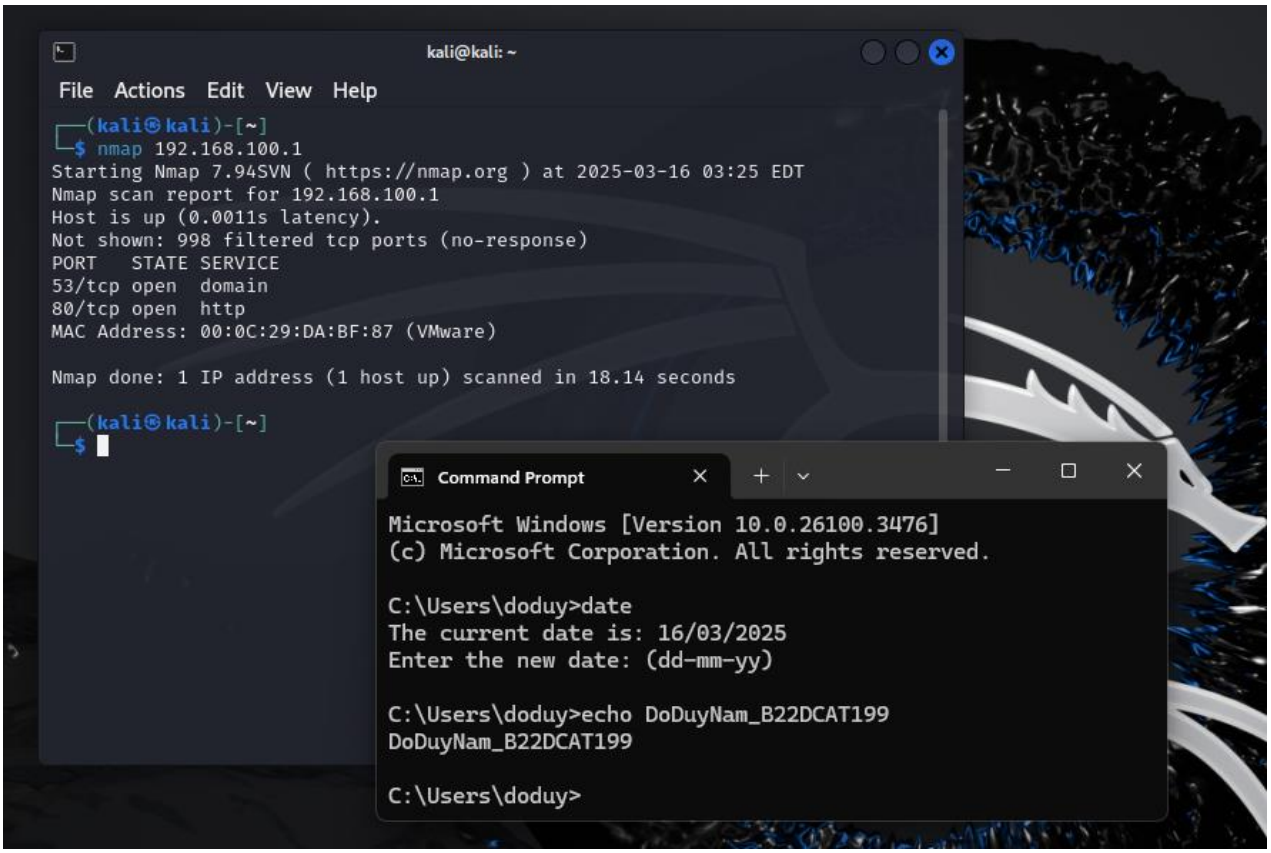
Hình 17 Cấu hình luật firewall

- Ở máy Kali attack trong mạng External ping tới 10.10.19.1 để kiểm tra



Hình 18 Máy Kali attack ở mạng External ping thành công tới địa chỉ 10.10.19.1

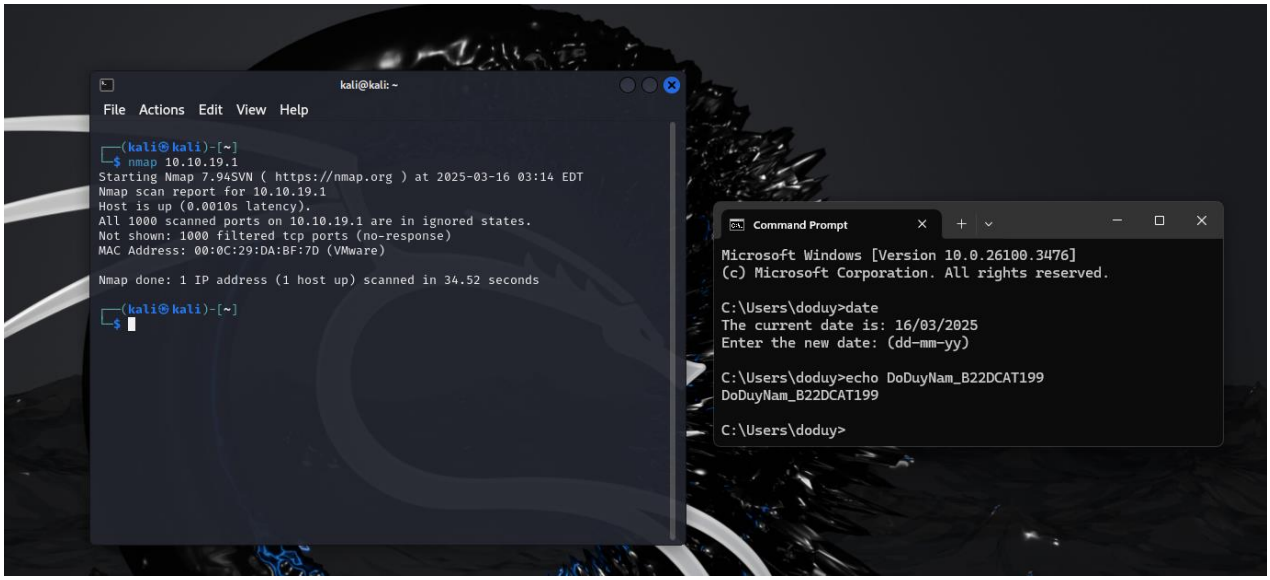
- Trả lời câu hỏi:
    - Theo mặc định, có 2 cổng TCP mở trên giao diện mạng Internal của pfsense. Sử dụng nmap 192.168.100.1 để kiểm tra.



Hình 19 Có 2 cổng TCP mở trên giao diện mạng Internal

- Theo mặc định, không có cổng TCP nào mở trên giao diện mạng External của pfsense.

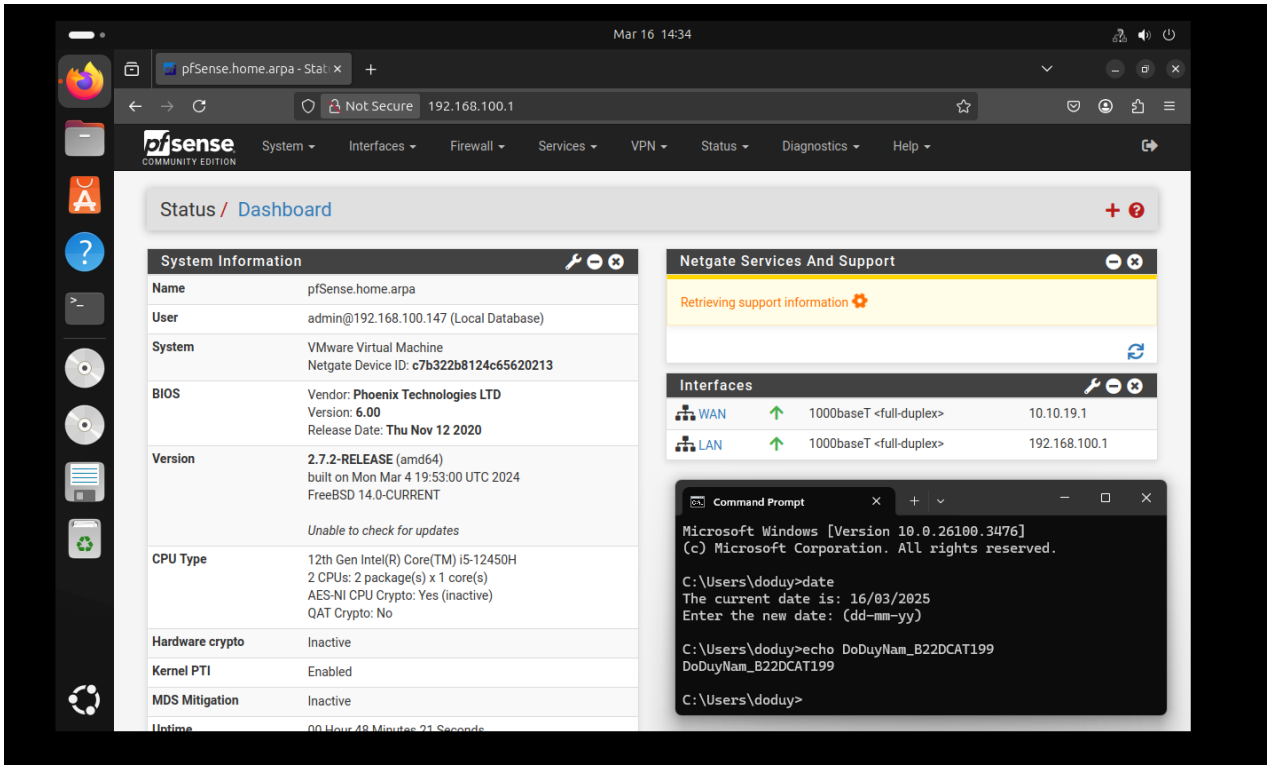
Sử dụng nmap 10.10.19.1 để kiểm tra.



Hình 20 Không có cổng TCP nào mở trên giao diện mạng External

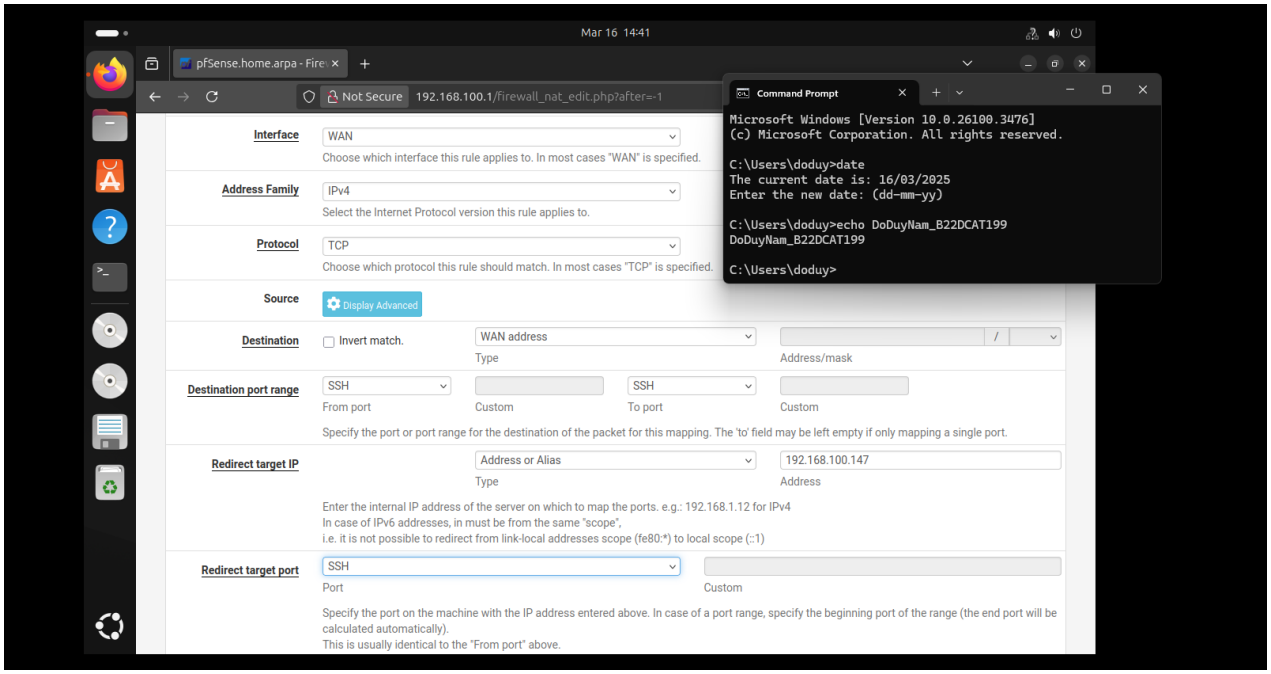
2.2.3 Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

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



Hình 21 Truy cập vào pfsense qua giao diện Web

- Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy 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.

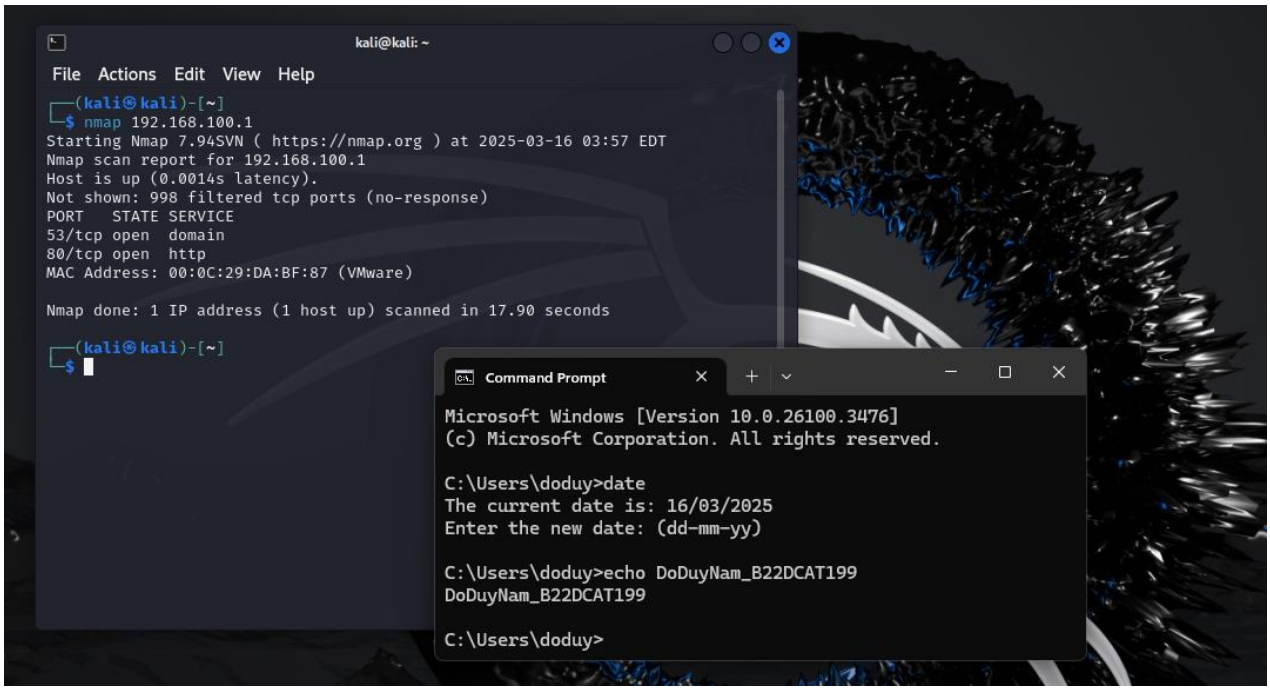


Hình 22 Cấu hình cổng SSH

- Ở trên máy Linux attack trong mạng External SSH tới 10.10.19.1 và sử dụng câu lệnh ifconfig để kiểm tra địa chỉ IP có phải là 192.168.100.147 hay không.

Hình 23 SSH tới 10.10.19.1 thành công và đúng là địa chỉ IP 192.168.100.147

- Trên máy Kali LInux trong mạng Internal sử dụng câu lệnh nmap 192.168.100.1 để kiểm tra các cổng được phép truy cập trên mạng Internal



Hình 24 Các cổng được phép truy cập trên mạng Internal

2.3 Kết luận

Ở chương này đã hướng dẫn cài đặt và cấu hình hệ thống theo topo mạng và thông tin như đề bài yêu cầu. Bên cạnh đó cũng hướng dẫn cài đặt cấu hình pfsense firewall cho lưu lượng ICMP và cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

KẾT LUẬN

- Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware
- Tìm hiểu về pfsense
- Cài đặt và cấu hình thành công hệ thống theo topo mạng đề bài yêu cầu
- Cài đặt cấu hình thành công pfsense firewall cho lưu lượng ICMP
- Cài đặt cấu hình thành công pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

TÀI LIỆU THAM KHẢO

[1] Vmware Workstation Networking Overview: https://masteringvmware.com/vmware-workstation-networking-overview/

[2] Network in VMware Workstation: https://github.com/ducnc/vmware-workstation-network

[3] Lab 7 pfsense firewall của CSSIA CompTIA Security+®

[4] Advanced Penetration Testing for Highly-Secured Environments Second Edition

[5] Giới thiệu về Pfsense: https://viblo.asia/p/network-gioi-thieu-ve-pfsense-N0bDM6LXv2X4