

**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 HÌNH MẠNG DOANH NGHIỆP VỚI PFSENSE
FIRE**

Sinh viên thực hiện:

B22DCAT206

PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợt

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC HÌNH ẢNH	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH.....	4
1.1. 1. Cơ sở lý thuyết.....	4
a. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware.....	4
1.2.	8
1.3. <u>2.</u> Tìm hiểu về Pfsense	8
a. Giới thiệu	8
b. Các tính năng trong pfsense	9
1.4. Tổng kết	10
CHƯƠNG 2. NỘI DUNG THỰC HÀNH.....	11
1.5. 1. Chuẩn bị môi trường	11
1.6. 2. Các bước thực hiện	11
1.7. Kết luận.....	36
1.8. Tài liệu tham khảo	36

DANH MỤC HÌNH ẢNH

Hình 1: Thêm card mạng cho các máy ảo.....	12
Hình 2: Thêm card mạng cho các máy ảo.....	13
Hình 3: Thêm card mạng cho máy ảo	14
Hình 4: Cấu hình card mạng	15
Hình 5: Kiểm tra ip máy kali	16
Hình 6: Kiểm tra mạng máy server	17
Hình 7: Cấu hình mạng máy ubuntu	18
Hình 8: Ping máy internal cho nhau	19
Hình 9: Windows Server Victim à Kali Attack	20
Hình 10: Kali Attack và 2 máy còn lại	21
Hình 11: Thêm máy vào mạng ảo.....	22
Hình 12: Sudo ifconfig ens33 10.10.19.148 netmask 255.255.255.0.....	23
Hình 13: Cấu hình window external	24
Hình 14: Ping 2 máy External với nhau Windows Server và Linux Victim	25
Hình 15: Kali Linux Attack và Windows Server.....	26
Hình 16: Cài đặt card mạng cho máy ảo pfsense firewall	27
Hình 17: Khởi động máy pfsense và cài cấu hình	27
Hình 18: Ping thành công đến các máy	28
Hình 19: Cấu hình firewall	28
Hình 20: Cấu hình firewall	29
Hình 21: Cấu hình firewall	30
Hình 22: Ping từ kali attack đến các máy external	31
Hình 23: kiểm tra nmap	32
Hình 24: Cấu hình nat qua giao diện web.....	33
Hình 25: Cấu hình nat qua giao diện web.....	34
Hình 26: Chỉnh sửa file cấu hình	35
Hình 27: SSH ở máy Linux Victim Internal đã được bật	36

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1. Cơ sở lý thuyết

a. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng VMware

VMware Workstation là một phần mềm ảo hóa mạnh mẽ, cho phép người dùng chạy và mô phỏng nhiều hệ điều hành khác nhau trên một máy tính vật lý. Để tối ưu hóa việc sử dụng phần mềm này, việc hiểu rõ cách thức hoạt động của các kết nối mạng và cách thiết lập hệ thống mạng ảo là rất quan trọng. Mạng ảo trong VMware được xây dựng từ các thành phần chính như switch ảo, card mạng ảo, DHCP server ảo và thiết bị NAT.

- Switch ảo (Virtual Switch)

Tương tự như switch vật lý, switch ảo kết nối các thành phần mạng ảo với nhau, tạo thành các mạng ảo có tên như VMnet0, VMnet1, VMnet2, v.v. Khi cài đặt VMware Workstation, ba switch ảo mặc định được tạo sẵn với các chế độ như sau:

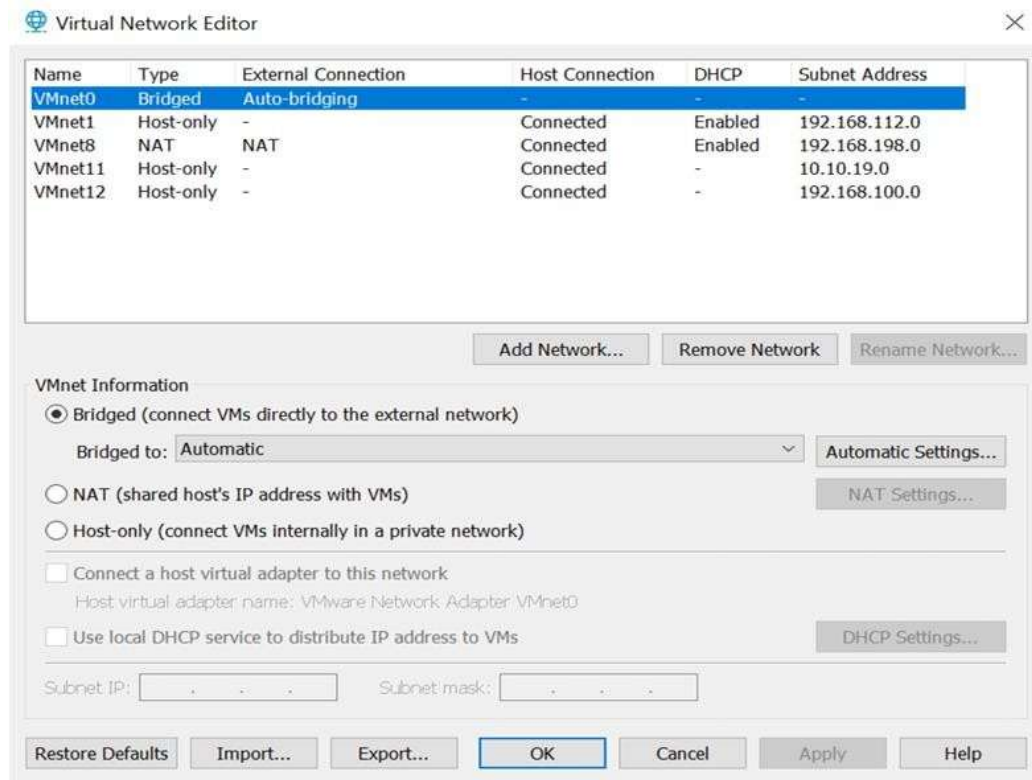
- VMnet0: Chế độ Bridged (cầu nối), liên kết trực tiếp với card mạng vật lý của máy tính.
- VMnet8: Chế độ NAT, cho phép máy ảo chia sẻ địa chỉ IP của máy thật để truy cập mạng bên ngoài.
- VMnet1: Chế độ Host-Only, chỉ cho phép giao tiếp giữa máy ảo và máy thật, cách ly khỏi mạng bên ngoài.

Người dùng có thể tùy chỉnh, thêm hoặc xóa các VMnet thông qua menu Edit -> Virtual Network Editor... trong VMware Workstation. Phiên bản 12 của phần mềm này hỗ trợ tạo tối đa 20 switch ảo trên hệ điều hành Windows và 255 switch ảo trên Linux. Trên Windows, số lượng máy ảo kết nối vào mỗi switch ảo là không giới hạn, trong khi trên Linux, con số này bị giới hạn ở 32 máy ảo. Để thêm hoặc xóa mạng ảo, bạn có thể sử dụng các tùy chọn Add Network... hoặc Remove Network....

- Card mạng ảo và kết nối

Khi tạo một VMnet, máy tính vật lý sẽ tự động tạo ra các card mạng ảo tương ứng để kết nối switch ảo với máy thật, giúp máy ảo và máy thật giao tiếp với nhau. Riêng VMnet0 không tạo card mạng ảo vì nó sử dụng cơ chế cầu nối (Bridged) để liên kết trực tiếp với card mạng vật lý. VMnet8 mặc định hoạt động ở chế độ NAT, trong khi các VMnet khác khi được thêm vào sẽ mặc định ở chế độ Host-Only.

Bằng cách hiểu và quản lý các thành phần này, bạn có thể thiết lập mạng ảo linh hoạt, phục vụ cho nhiều mục đích khác nhau như thử nghiệm, phát triển phần mềm hoặc mô phỏng môi trường mạng.



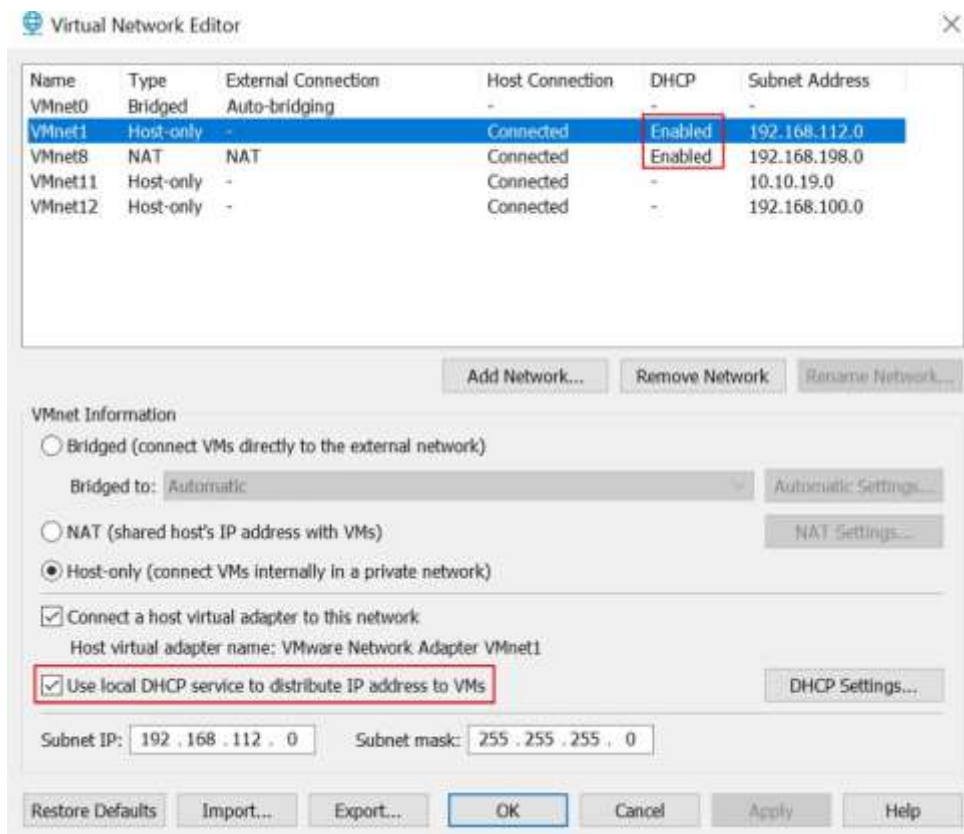
Trong một số trường hợp, card mạng ảo dùng để kết nối máy thật với các VMnet có thể chưa được kích hoạt. Để bật các card này, bạn vào Virtual Network Editor, chọn VMnet muốn kết nối, sau đó tích vào tùy chọn "Connect a host virtual adapter to this network" để thiết lập kết nối từ máy thật đến VMnet.

- Card mạng ảo trên máy ảo

Khi tạo một máy ảo mới, các card mạng ảo sẽ được tạo tự động cho máy ảo. Những card này xuất hiện trong hệ điều hành của máy ảo dưới dạng các thiết bị như AMD PCNET PCI hoặc Intel Pro/1000 MT Server Adapter. Kể từ VMware Workstation 6.0, máy ảo có thể hỗ trợ tối đa 10 card mạng, trong khi các phiên bản trước đó chỉ giới hạn ở 3 card. Để thêm hoặc xóa card mạng, bạn vào Virtual Machine Settings và nhấn nút "Add..." để thêm hoặc "Remove..." để xóa.

- DHCP server ảo của Vmnet

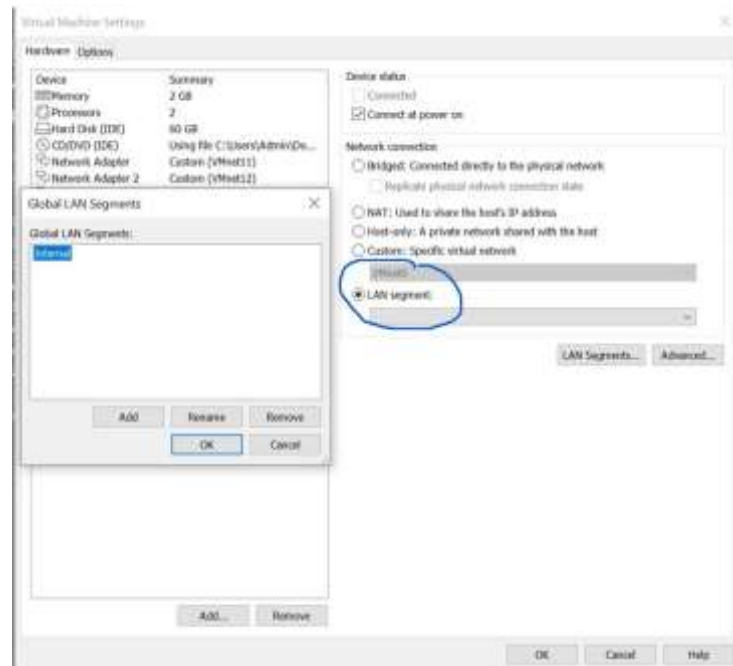
DHCP (Dynamic Host Configuration Protocol) server ảo chịu trách nhiệm cấp phát địa chỉ IP cho các máy ảo khi kết nối với các switch ảo không sử dụng chế độ Bridged (như VMnet0). Cụ thể, DHCP server ảo cung cấp địa chỉ IP cho các máy ảo sử dụng chế độ kết nối Host-only hoặc NAT.



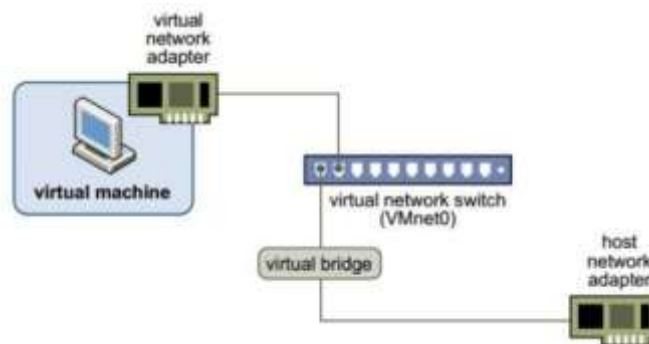
Nếu không muốn sử dụng DHCP server ảo của VMnet, bạn có thể bỏ chọn mục "Use local DHCP service to distribute IP address to VMs" trong Virtual Network Editor. Để tùy chỉnh DHCP, bạn vào phần "DHCP Settings", nơi có thể điều chỉnh các thông số như thời gian cấp phát hoặc phạm vi địa chỉ IP (Scope IP). Tuy nhiên, lưu ý rằng bạn chỉ có thể thay đổi vùng địa chỉ dành cho host, không thể sửa đổi vùng mạng (network).

- LAN Segment

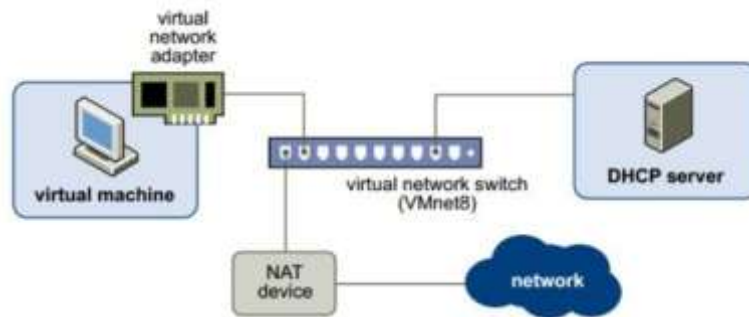
Các card mạng của máy ảo có thể được liên kết với nhau để tạo thành các LAN Segment riêng biệt. Khác với VMnet, LAN Segment chỉ kết nối các máy ảo được gán trong cùng một đoạn mạng mà không hỗ trợ các tính năng như DHCP. Hơn nữa, LAN Segment không thể kết nối ra máy thật như các switch ảo VMnet.



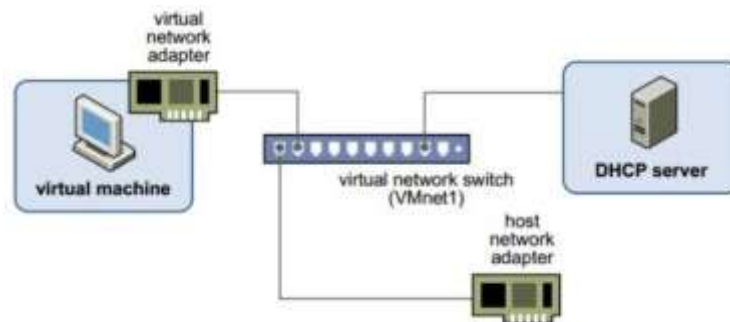
- Cơ chế hoạt động và mô hình cơ bản khi cấu hình switch ảo (VMnet)
- Chế độ Bridge: Trong chế độ này, card mạng của máy ảo được kết nối với VMnet0, và VMnet0 liên kết trực tiếp với card mạng vật lý của máy thật. Nhờ đó, máy ảo có thể truy cập internet thông qua card mạng vật lý và sử dụng cùng dải mạng với card mạng vật lý.



- Chế độ NAT: Ở chế độ này, card mạng của máy ảo kết nối với VMnet8, VNnet8 cho phép máy ảo đi ra mạng vật lý bên ngoài internet thông qua cơ chế NAT (NAT device). Lúc này lớp mạng bên trong máy ảo khác hoàn toàn với lớp mạng của card vật lý bên ngoài, hai mạng hoàn toàn tách biệt. IP của card mạng máy ảo sẽ được cấp bởi DHCP của VMnet8, trong trường hợp bạn muốn thiết lập IP tĩnh cho card mạng máy ảo bạn phải đảm bảo chung lớp mạng với VNnet8 thì máy ảo mới có thể đi internet.



- Cơ chế Host-only: Máy ảo được kết nối với VMnet có tính năng Host-only, trong trường hợp này là VMnet1. VMnet Host-only kết nối với một card mạng ảo tương ứng ngoài máy thật (như đã nói ở phần trên). Ở chế độ này, các máy ảo không có kết nối vào mạng vật lý bên ngoài hay internet thông qua máy thật, có nghĩa là mạng VMnet Host-only và mạng vật lý hoàn toàn tách biệt. IP của máy ảo được cấp bởi DHCP của VMnet tương ứng. Trong nhiều trường hợp đặc biệt cần cấu hình riêng, ta có thể tắt DHCP trên VMnet và cấu hình IP bằng tay cho máy ảo.



2. Tìm hiểu về PfSense

a. Giới thiệu

Để bảo vệ hệ thống mạng, có nhiều giải pháp như sử dụng router Cisco, tường lửa phần cứng, hoặc tường lửa phần mềm như Microsoft ISA. Tuy nhiên, các thiết bị này thường đòi hỏi chi phí cao, không phù hợp với các doanh nghiệp vừa và nhỏ. Trong trường hợp này, tường lửa mã nguồn mở như pfSense là một lựa chọn hiệu quả. pfSense là một phần mềm miễn phí, dựa trên FreeBSD, cung cấp khả năng định tuyến và tường lửa mạnh mẽ. Với giao diện quản lý GUI dựa trên web, pfSense dễ dàng cấu hình và vận hành. Nó hỗ trợ lọc gói tin dựa trên địa chỉ nguồn, đích, cổng nguồn hoặc cổng đích, đồng thời có khả năng định tuyến, hoạt động ở chế độ bridge hoặc transparent. Khi sử dụng pfSense làm gateway, người dùng có thể tận dụng các tính năng như NAT, chuyển tiếp cổng (port forwarding), cùng với khả năng cân bằng tải và chuyển đổi dự phòng (failover) cho các kết nối mạng.

b. Các tính năng trong pfsense

- Aliases

Trong pfSense, một quy tắc tường lửa không thể bao gồm nhiều nhóm địa chỉ IP hoặc cổng cùng lúc. Để giải quyết, bạn có thể sử dụng Aliases để gom các địa chỉ IP, cổng hoặc URL vào một nhóm duy nhất. Một alias có thể đại diện cho một host, một dải mạng, nhiều địa chỉ IP riêng lẻ, hoặc một tập hợp cổng, URL, v.v. Sử dụng alias giúp tiết kiệm thời gian đáng kể bằng cách thay thế nhiều quy tắc riêng lẻ bằng một quy tắc duy nhất, nếu được áp dụng đúng cách.

- NAT

- pfSense hỗ trợ NAT tĩnh 1:1, yêu cầu phải có địa chỉ IP công cộng (public IP). Với NAT 1:1, một địa chỉ IP riêng (private IP) sẽ luôn được ánh xạ ra một địa chỉ IP công cộng cố định, với các cổng tương ứng trên IP công cộng.
- pfSense cũng hỗ trợ NAT outbound mặc định thông qua chế độ "Automatic outbound NAT rule generation". Nếu muốn tùy chỉnh, bạn có thể chọn "Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)", xóa các quy tắc mặc định của pfSense và tạo các quy tắc outbound mới theo ý muốn.
- Ngoài các loại NAT như port forwarding, 1:1 và outbound, pfSense còn hỗ trợ NAT Npt dành cho IPv6, cho phép thực hiện NAT trên các địa chỉ IPv6.

- Firewall Rules

Các quy tắc tường lửa (Firewall Rules) trong pfSense lưu trữ tất cả các quy tắc kiểm soát lưu lượng vào và ra. Mặc định, pfSense cho phép mọi kết nối vào/ra tại cổng LAN (quy tắc "any to any"). Để quản lý mạng nội bộ, bạn cần tạo các quy tắc cụ thể để kiểm soát lưu lượng theo nhu cầu.

- Traffic shaper

Tính năng Traffic Shaper trong pfSense cho phép quản trị viên tối ưu hóa và điều chỉnh băng thông mạng. Băng thông được chia thành các hàng đợi (queues) khác nhau, với 7 loại hàng đợi được xác định theo mức độ ưu tiên:

- qACK: Dành cho các gói xác nhận (ACK) trong giao thức TCP, phục vụ các ứng dụng quan trọng như HTTP, SMTP. Lưu lượng ACK nhỏ nhưng cần thiết để duy trì tốc độ truyền dữ liệu lớn.
- qVoIP: Dành cho các ứng dụng yêu cầu độ trễ thấp nghiêm ngặt (dưới 10ms), như VoIP hoặc hội nghị video.
- qGames: Dành cho các ứng dụng cần độ trễ thấp (dưới 50ms), như SSH hoặc game trực tuyến.
- qOthersHigh: Dành cho các ứng dụng tương tác cao, yêu cầu phản hồi nhanh và độ trễ thấp, ví dụ: NTP, DNS, SNMP.
- qOthersDefault: Dành cho các ứng dụng có mức độ tương tác trung bình, như HTTP, IMAP.
- qOthersLow: Dành cho các ứng dụng quan trọng nhưng ít tương tác, như SMTP, POP3, FTP.
- qP2P: Dành cho các ứng dụng không yêu cầu phản hồi nhanh, như BitTorrent.

- Traffic Shaper và Độ ưu tiên hàng đợi
- Trong pfSense, các hàng đợi (queues) được mặc định sắp xếp theo thứ tự ưu tiên từ thấp đến cao: qP2P < qOthersLow < qOthersDefault < qOthersHigh < qGames < qACK < qVoIP.
- Người dùng có thể tùy chỉnh độ ưu tiên (priority) và phân bổ băng thông (bandwidth) mặc định cho từng hàng đợi để tối ưu hóa hiệu suất cho các loại lưu lượng cụ thể.
- Ngoài ra, pfSense cung cấp tính năng Limiter, cho phép giới hạn tốc độ tải xuống (download) và tải lên (upload) cho từng địa chỉ IP hoặc một dải IP. Tính năng Layer 7 của tường lửa pfSense còn hỗ trợ chặn các ứng dụng hoạt động ở tầng ứng dụng (Application Layer) trong mô hình OSI, chẳng hạn như SIP, FTP, HTTP, thông qua phân cấu hình Layer 7.
- VPN

pfSense tích hợp tính năng VPN, một yếu tố thiết yếu cho các gateway. Hệ thống hỗ trợ bốn giao thức VPN: IPSec, L2TP, PPTP, và OpenVPN, đáp ứng nhu cầu kết nối an toàn và linh hoạt.
- Giám sát băng thông

pfSense cung cấp nhiều plugin để theo dõi và quản lý băng thông, bao gồm:

- RRD Graphs: Công cụ mặc định có sẵn khi cài đặt pfSense, cho phép giám sát trạng thái server (như bộ nhớ, tiến trình) và băng thông của các giao diện mạng (LAN, WAN). Tuy nhiên, hạn chế của RRD Graphs là không thể theo dõi dung lượng sử dụng của từng IP.
- Lightsquid: Một gói bổ sung hoạt động cùng Squid, cung cấp báo cáo chi tiết về dung lượng sử dụng của từng IP theo ngày, tổng lưu lượng trong ngày, và danh sách các trang web đã truy cập.
- BandwidthD: Plugin này thống kê dữ liệu theo từng IP, bao gồm dung lượng gửi và nhận, cũng như các giao thức sử dụng như FTP, HTTP.
- Ntop: Một plugin phổ biến khác, cho phép theo dõi băng thông thời gian thực, xác định IP sử dụng băng thông lớn nhất, dung lượng tải của các cổng, và các kết nối đến internet.

c. Tổng kết

Hoàn toàn miễn phí, giá cả là ưu thế vượt trội của tường lửa pfsense. Tuy nhiên, rẻ không có nghĩa là kém chất lượng, tường lửa pfsense hoạt động rất ổn định với hiệu năng cao, tối ưu hóa mã nguồn và hệ điều hành. Vì vậy pfsense không cần phần cứng phải mạnh. Pfsense hoạt động như một thiết bị mạng tổng hợp với đầy đủ tính năng và sẵn sàng bất cứ lúc nào. Pfsense hỗ trợ rất nhiều plugin để thiết lập thêm các tính năng hữu ích mà người dùng thấy cần thiết. Như vậy, tường lửa pfSense là sự kết hợp hoàn hảo và mạnh mẽ, đem lại sự hợp lý cho các nhà tài chính, và sự tin tưởng cho các nhà quản trị.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

1. Chuẩn bị môi trường

Phần mềm VMWare Workstation.

Các file máy ảo VMware đã cài đặt trong các bài lab trước đó: máy trạm, máy chủ Windows và Linux.

File cài đặt tường lửa Pfsense

(Kali: tranphuong – phuong126, Windows Server 2019 victim : phamducnamb22dcat2062)

Cấu hình topo mạng

Yêu cầu cài đặt và cấu hình hệ thống theo thông tin mô tả sau:

Các máy Internal:

Máy Kali Linux Attack: IP: 192.168.100.3

Máy Windows Server 2019 Victim: IP: 192.168.100.201

Máy Linux Victim: IP: 192.168.100.147

Các máy External:

Máy Linux Attack: IP: 10.10.19.148

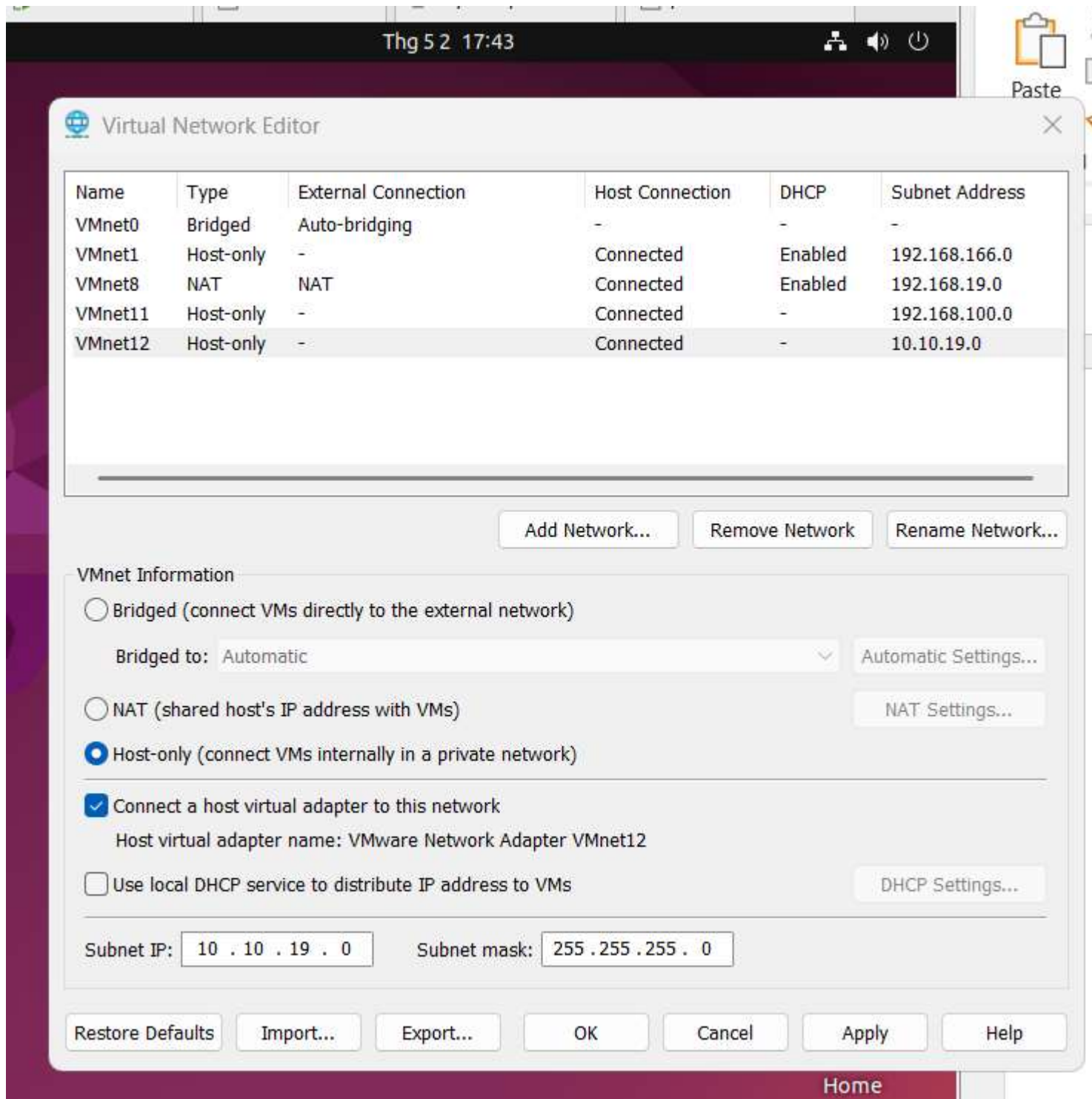
Máy Windows Server 2019 Victim: 10.10.19.202

Máy Pfsense firewall: IP: 10.10.19.1, 192.168.100.1

2. Các bước thực hiện:

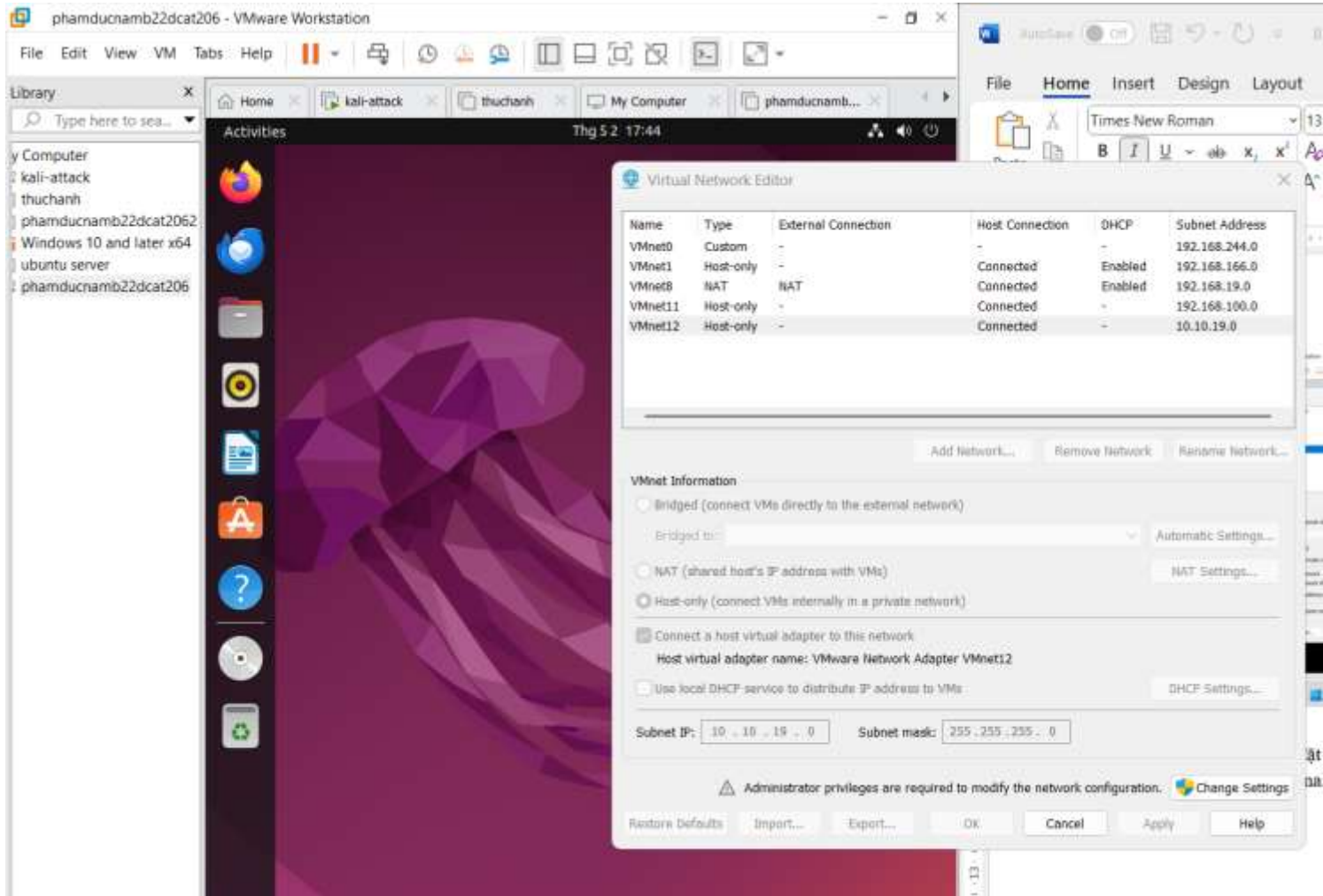
Thêm card mạng ảo, VMnet11 và VMnet12 để tạo mạng cho các máy External và Internal.

Vào VMware Workstation vào Edit vào Virtual Network Editor.



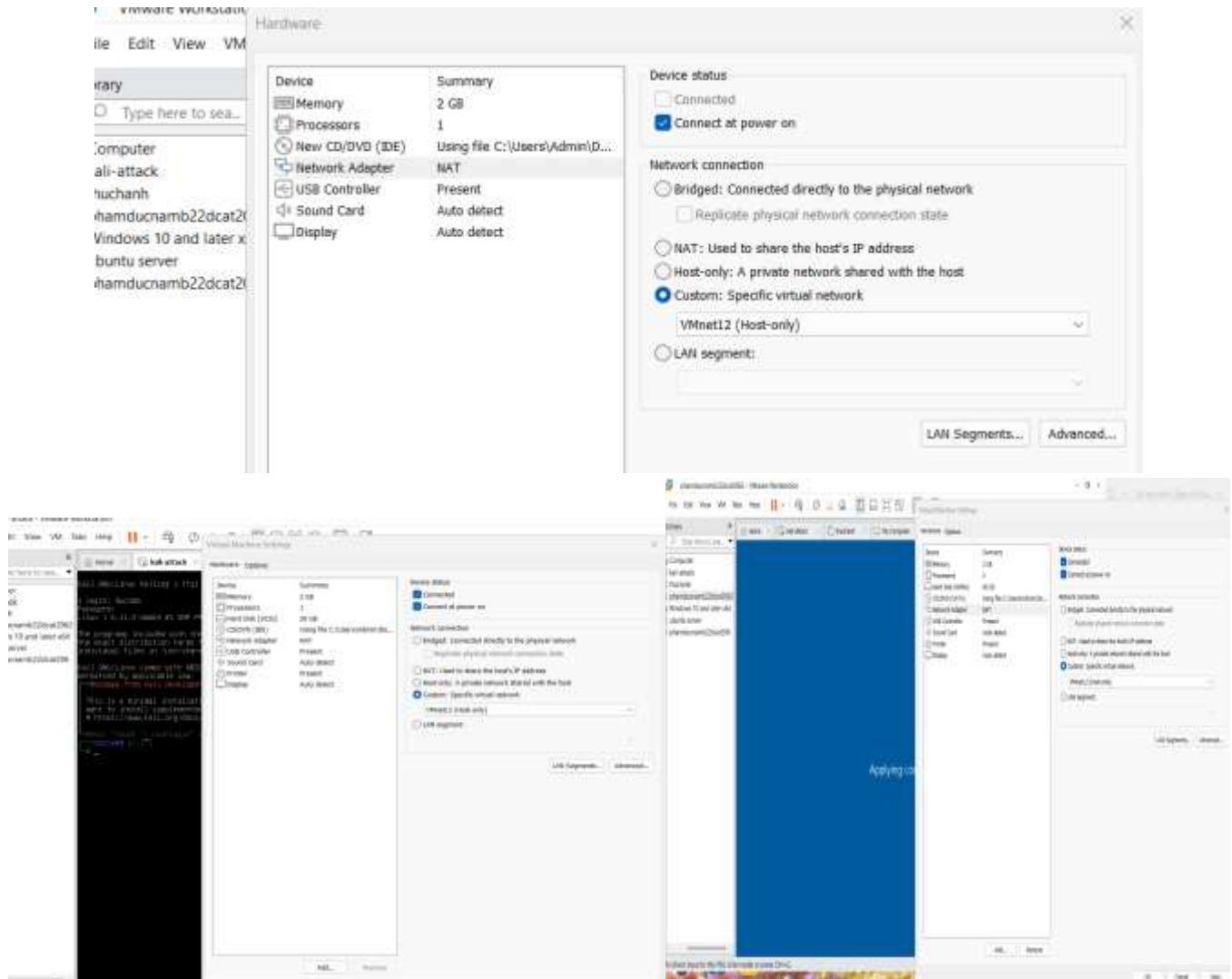
Hình 1 thêm card mạng cho các máy ảo

Mạng VMware11



Hình 2 thêm card mạng cho các máy ảo

Đối với các máy Internal: khi cài đặt với các máy Internal trong phần chọn card mạng ở Edit virtual machine settings, chọn mạng Internal đã tạo, VMnet12.

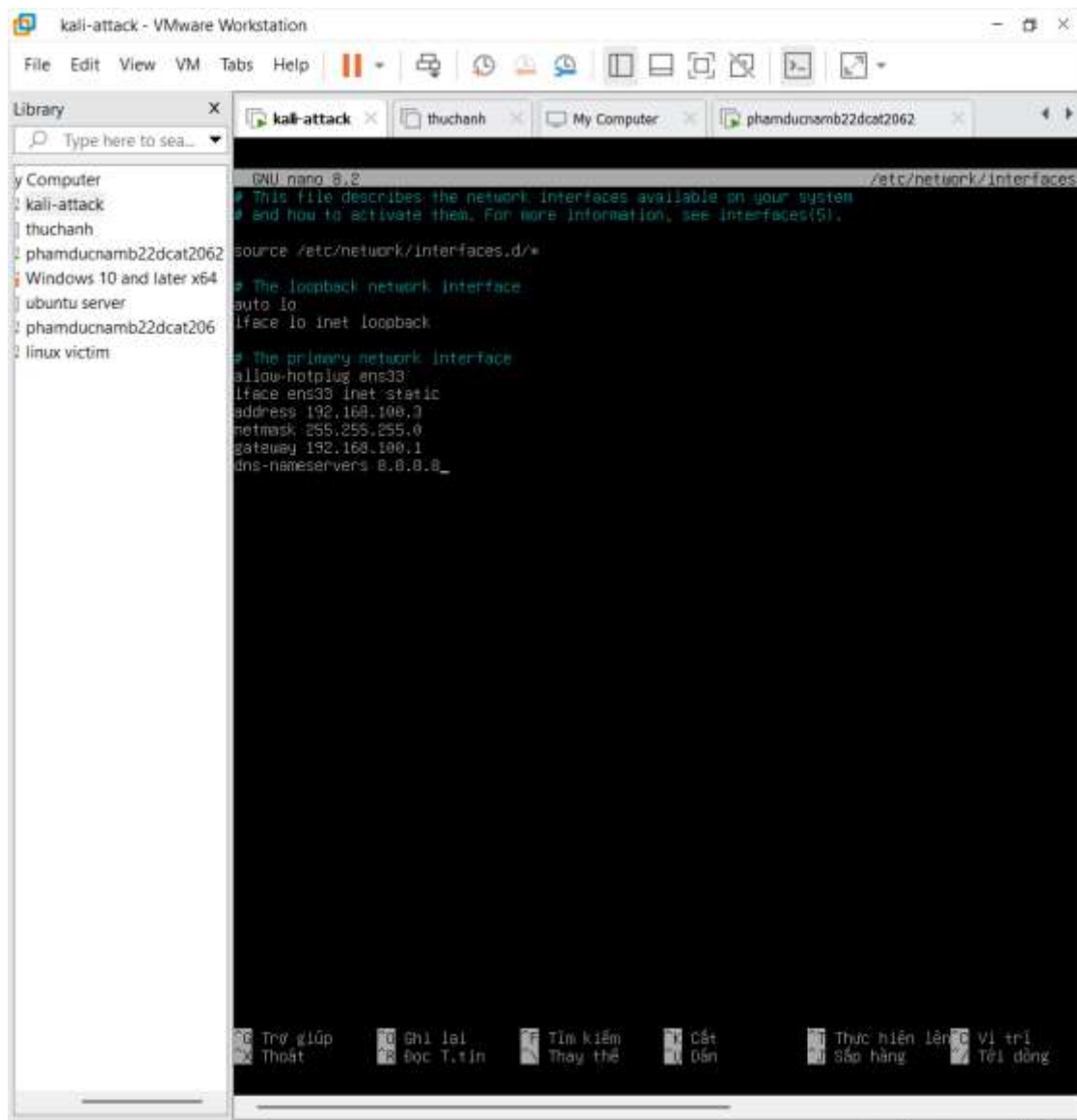


Hình 3 thêm card mạng cho máy ảo

Cấu hình địa chỉ địa chỉ IP 192.168.100.3 cho máy Kali Linux Attack

Chỉnh sửa file /etc/network/interfaces:

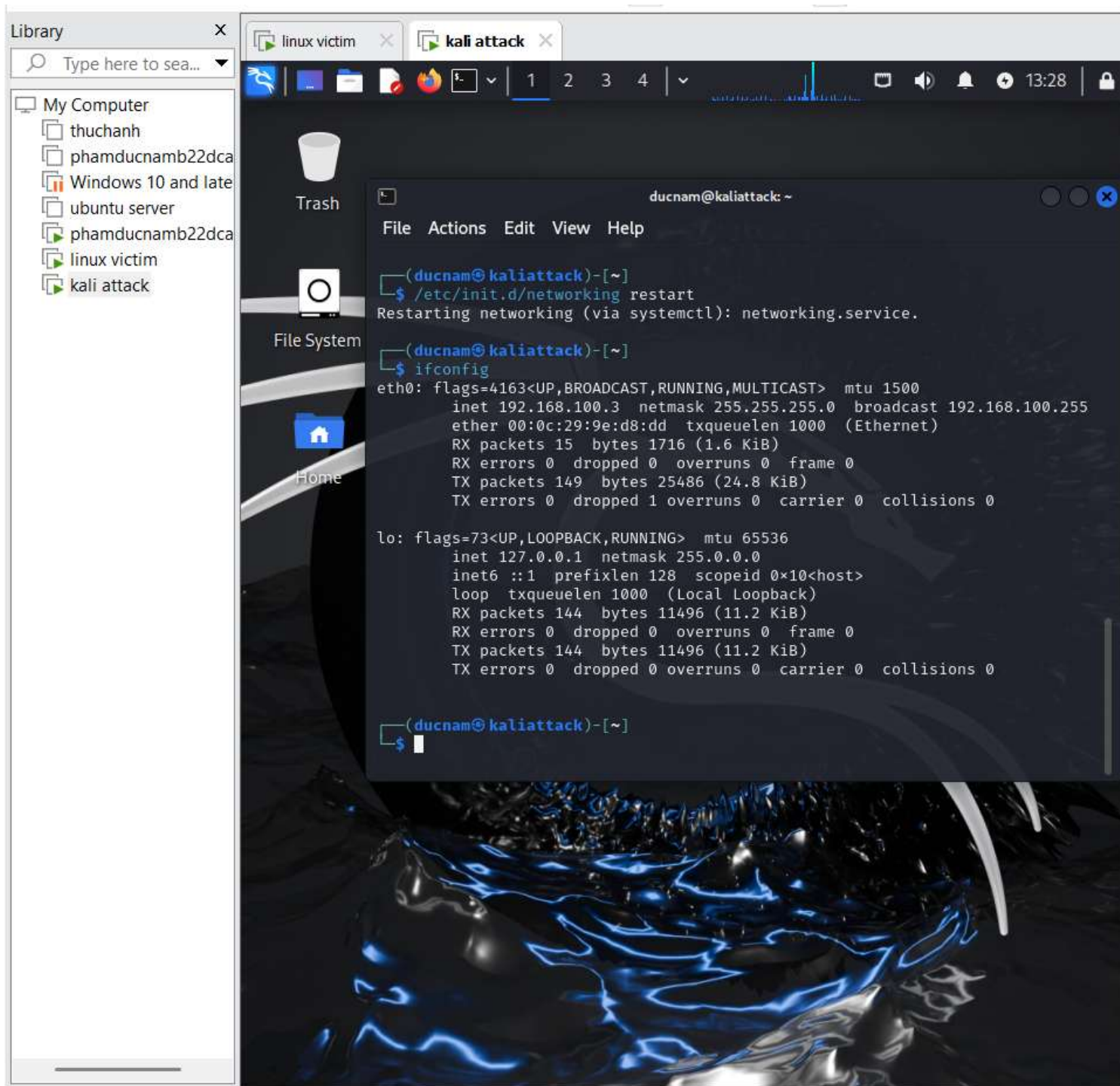
sudo nano /etc/network/interfaces



Hình 4 cấu hình card mạng

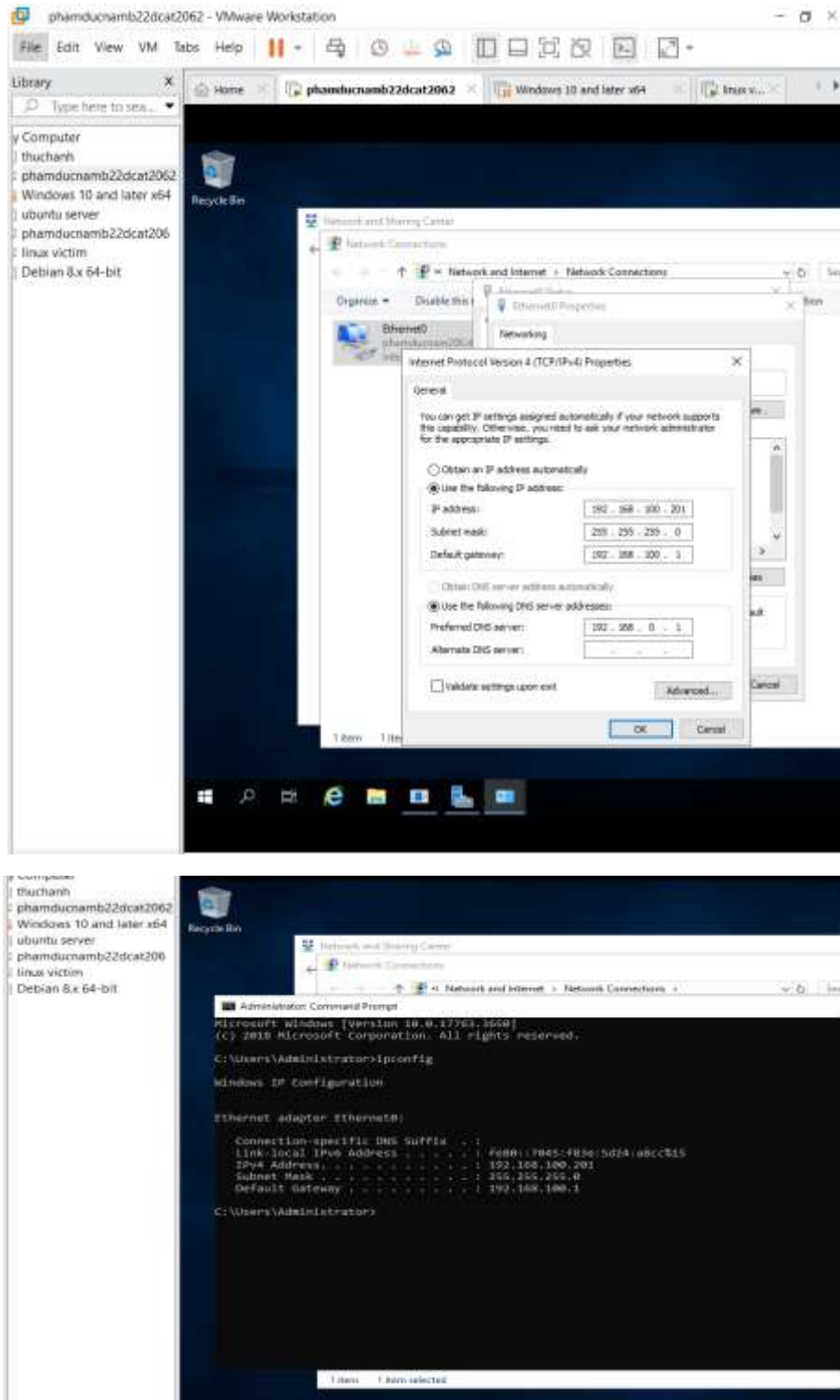
Bật card mạng eth0 vừa được cấu hình: */etc/init.d/networking restart*

Kiểm tra lại địa chỉ IP:



Hình 5 kiểm tra ip máy kali

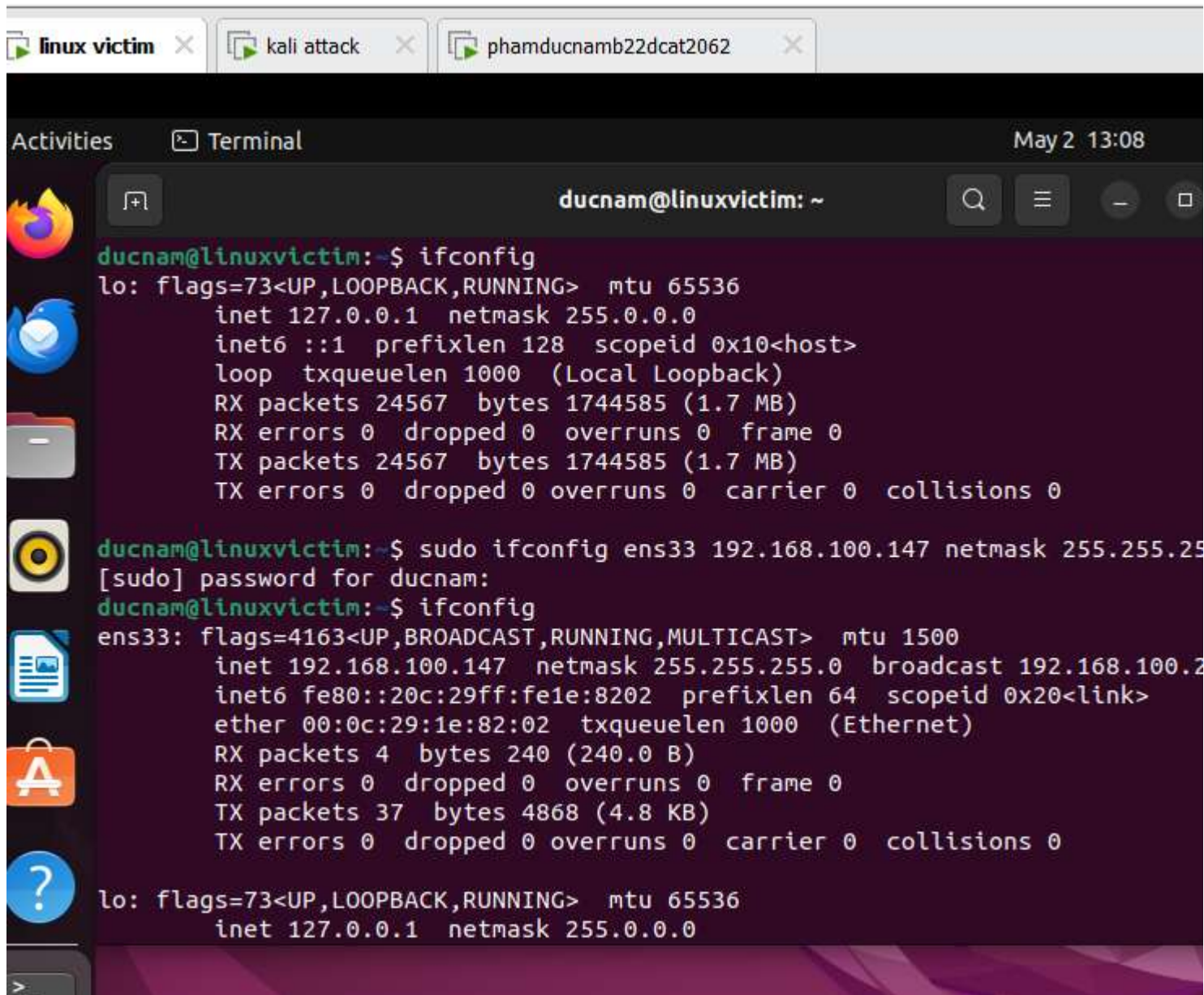
Cấu hình địa chỉ IP 192.168.100.201 cho máy Windows Server 2019:



Hình 6 kiểm tra mạng máy server

Cấu hình địa chỉ IP 192.168.100.147 cho máy Linux Victim:

Sudo ifconfig ens33 192.168.100.147 netmask 255.255.255.0



The screenshot shows a terminal window titled 'Terminal' with the user 'ducnam@linuxvictim'. The terminal displays the output of the 'ifconfig' command for the loopback interface 'lo' and the 'sudo ifconfig' command for the ethernet interface 'ens33'. The 'lo' interface is configured with IP 127.0.0.1 and netmask 255.0.0.0. The 'ens33' interface is configured with IP 192.168.100.147 and netmask 255.255.255.0. The terminal also shows the output of the 'ifconfig' command for the loopback interface 'lo' again.

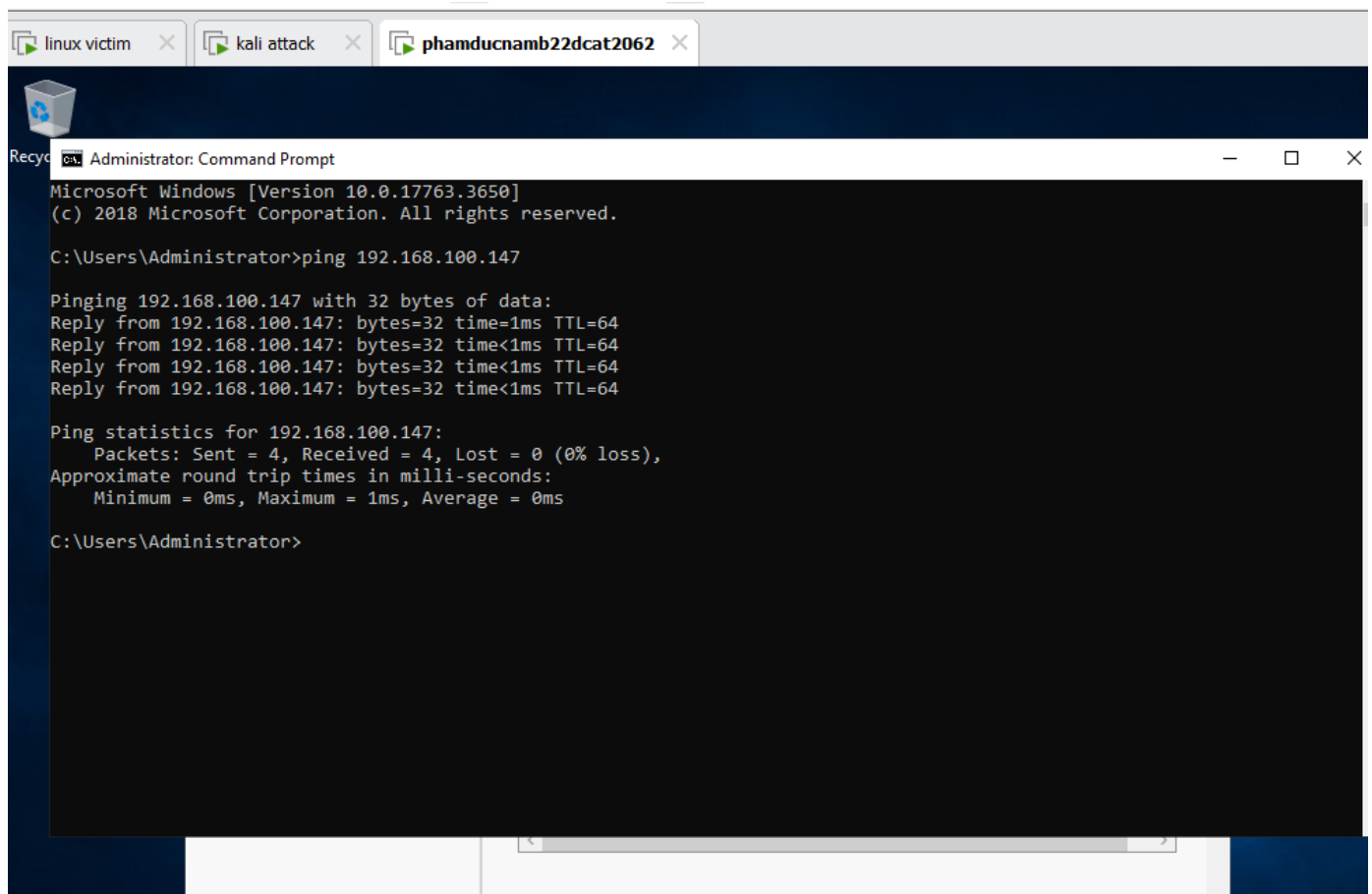
```
ducnam@linuxvictim:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 24567  bytes 1744585 (1.7 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 24567  bytes 1744585 (1.7 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ducnam@linuxvictim:~$ sudo ifconfig ens33 192.168.100.147 netmask 255.255.255.0
[sudo] password for ducnam:
ducnam@linuxvictim:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.100.147  netmask 255.255.255.0  broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe1e:8202  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:1e:82:02  txqueuelen 1000  (Ethernet)
    RX packets 4  bytes 240 (240.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 37  bytes 4868 (4.8 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
```

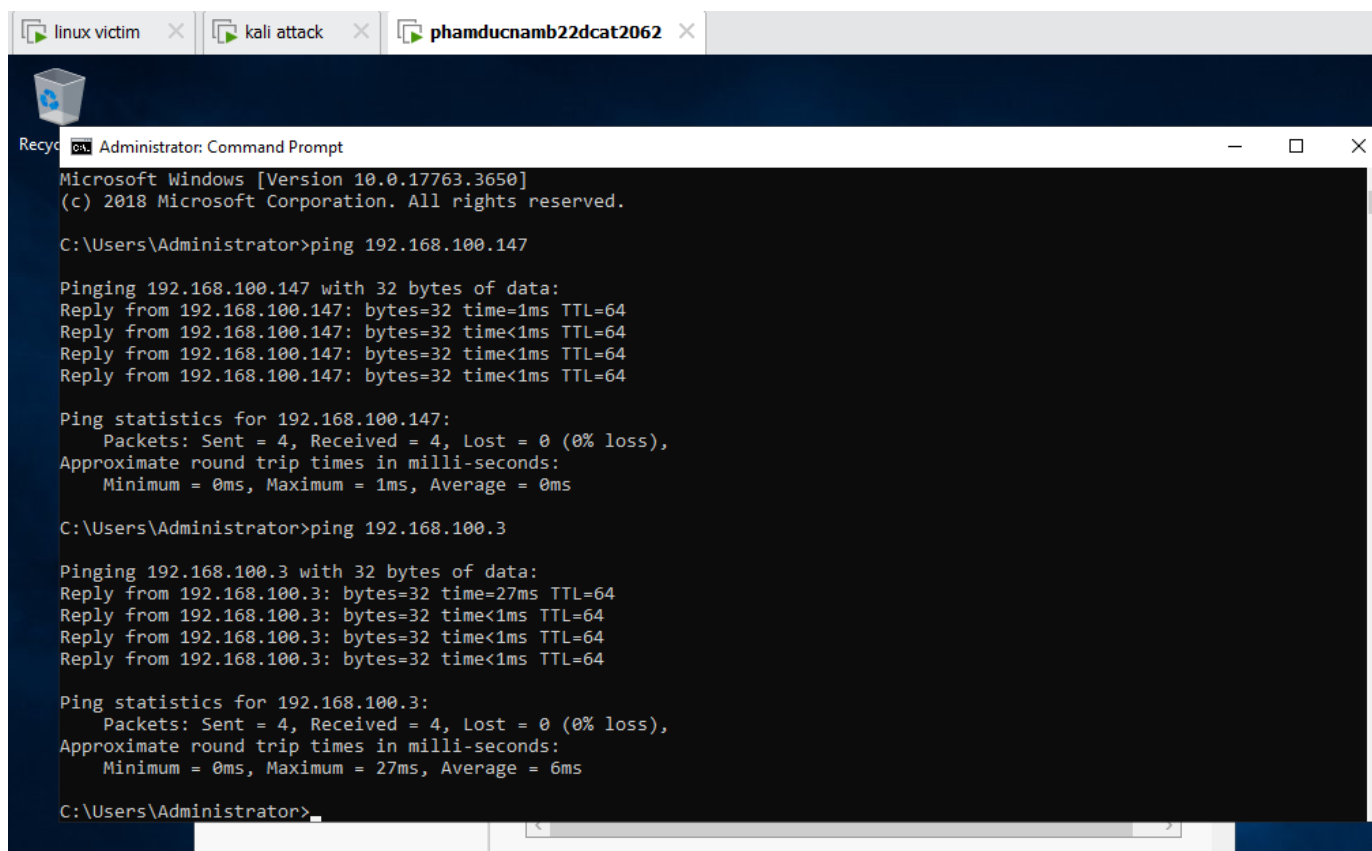
Hình 7 cấu hình mạng máy ubuntu

Ping thử các máy Internal với nhau



Hình 8 ping máy internal cho nhau

Windows Server và Linux Victim



The screenshot shows a Windows Server desktop environment with three browser tabs at the top: 'linux victim', 'kali attack', and 'phamducnamb22dcat2062'. The main window is an 'Administrator: Command Prompt' with a black background and white text. It displays the output of two ping commands. The first command is 'ping 192.168.100.147', which shows four successful replies with a time of 1ms and TTL of 64. The second command is 'ping 192.168.100.3', which shows four successful replies with a time of 27ms and TTL of 64. The window title bar includes a 'Recycle Bin' icon and standard minimize, maximize, and close buttons.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.100.147

Pinging 192.168.100.147 with 32 bytes of data:
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

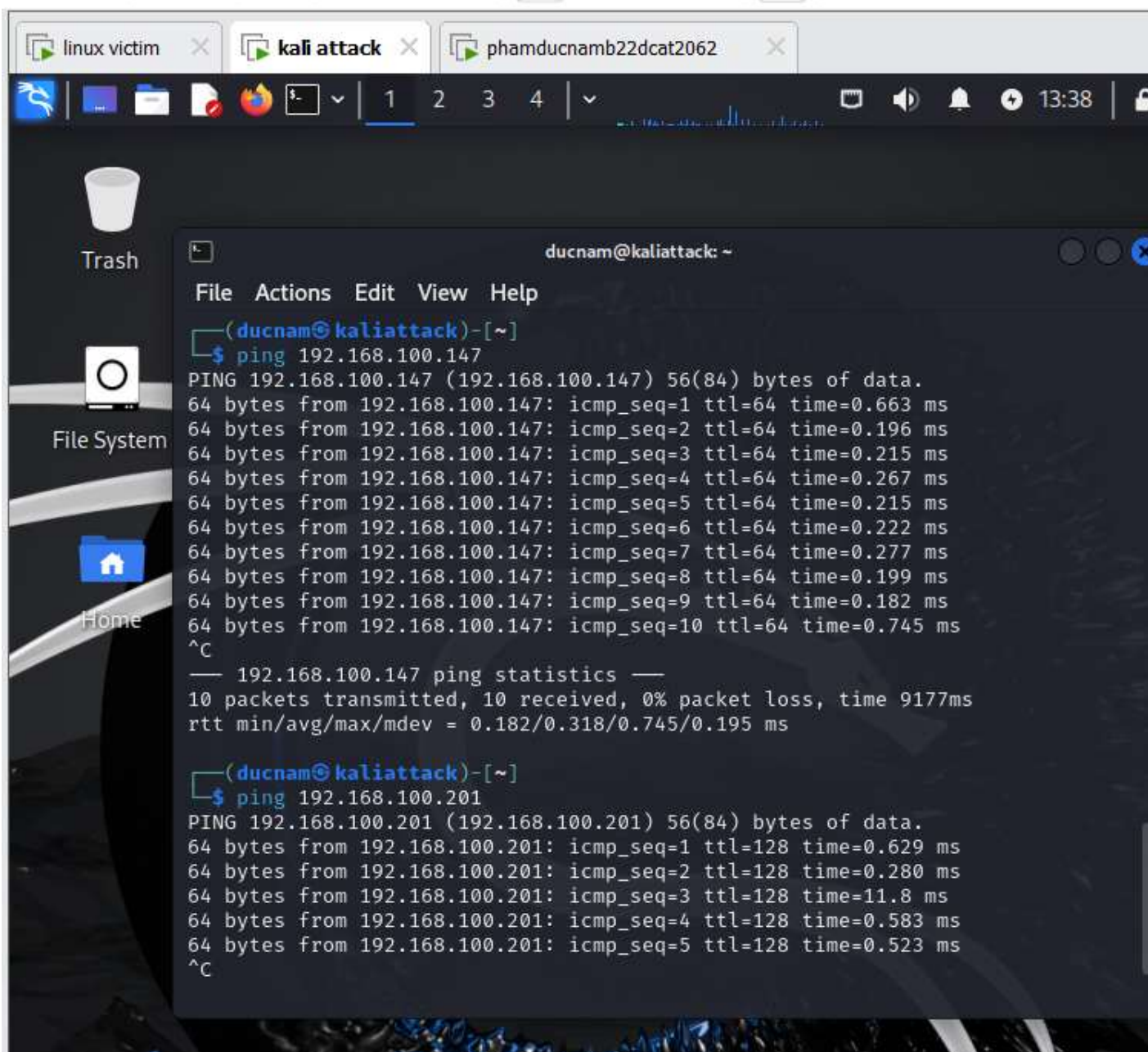
C:\Users\Administrator>ping 192.168.100.3

Pinging 192.168.100.3 with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time=27ms TTL=64
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 27ms, Average = 6ms

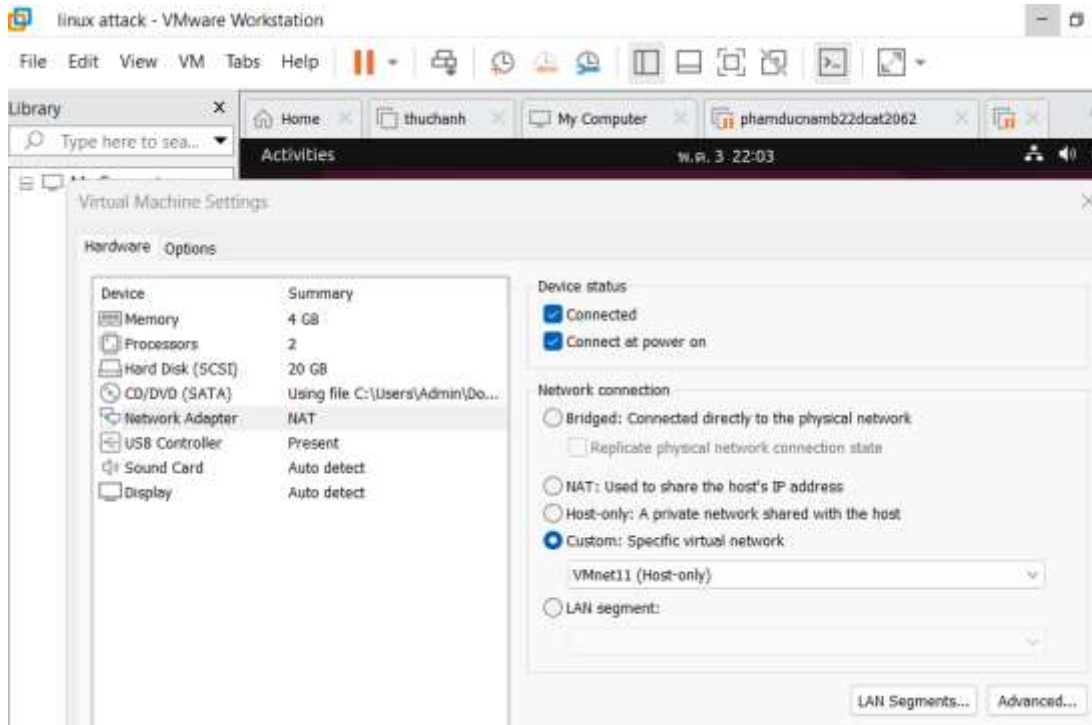
C:\Users\Administrator>
```

Hình 9 Windows Server Victim à Kali Attack



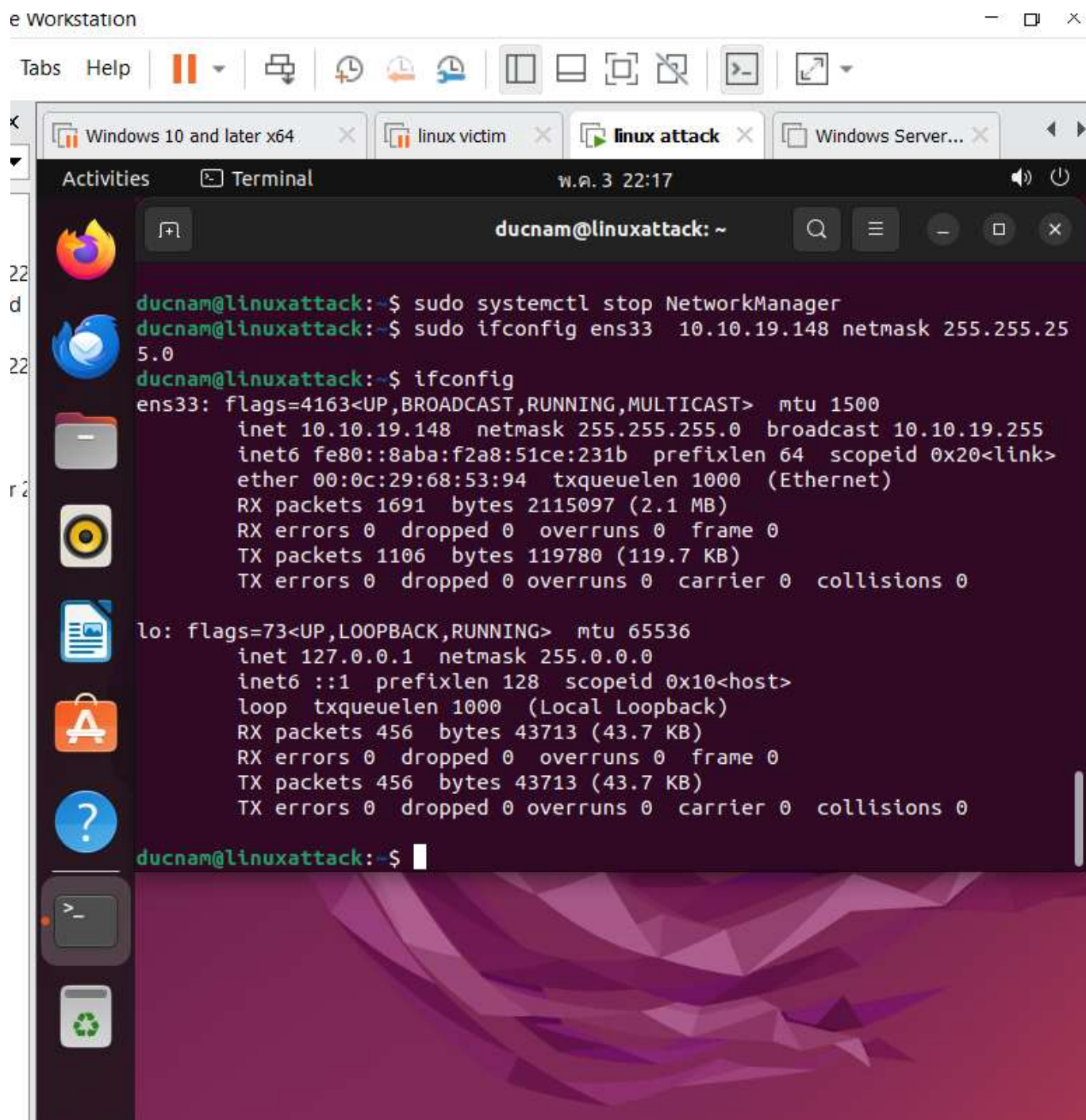
Hình 10 Kali Attack và 2 máy còn lại

Đối với các máy External: khi cài đặt với các máy External trong phần chọn card mạng ở Edit virtual machine settings, chọn mạng External đã tạo, VMnet11.



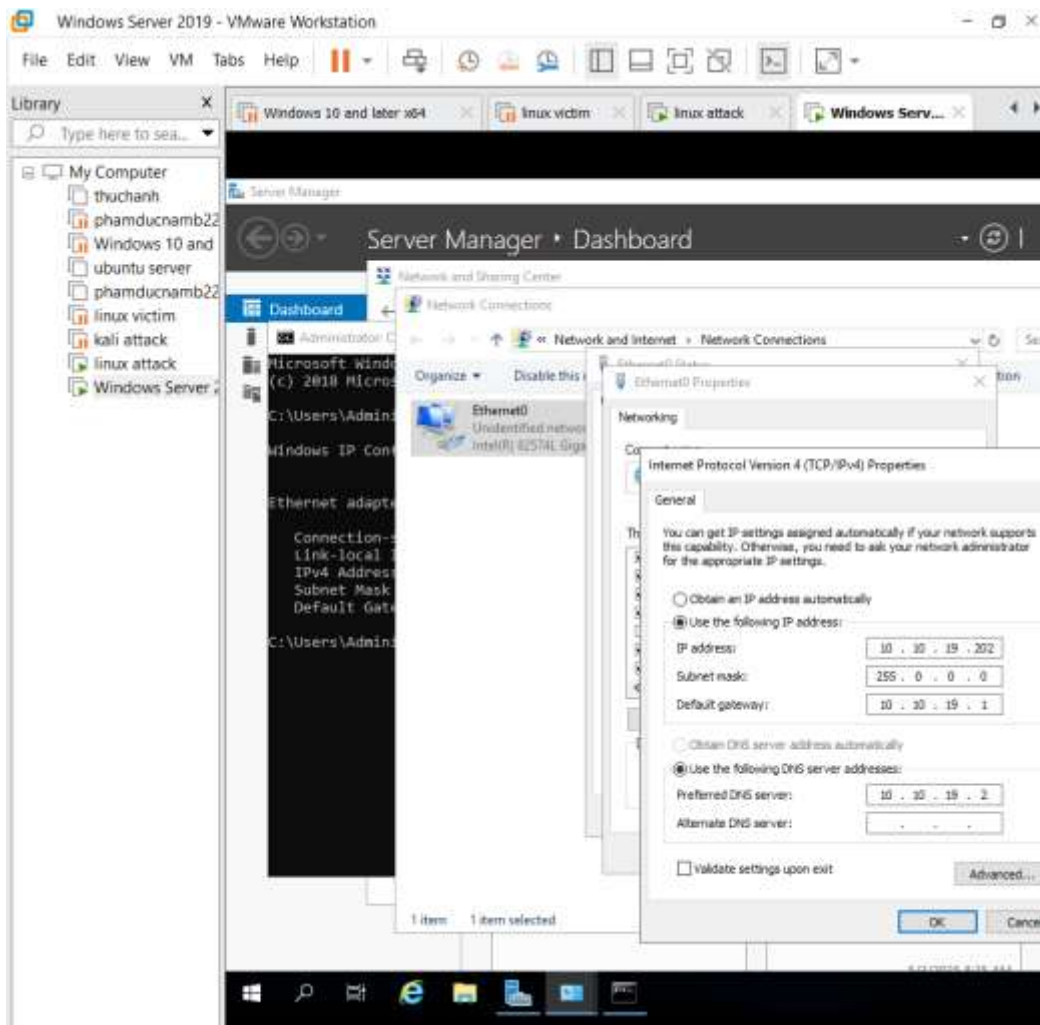
Hình 11 thêm máy vào mạng ảo

Cấu hình IP 10.10.19.148 cho máy Linux Attack:

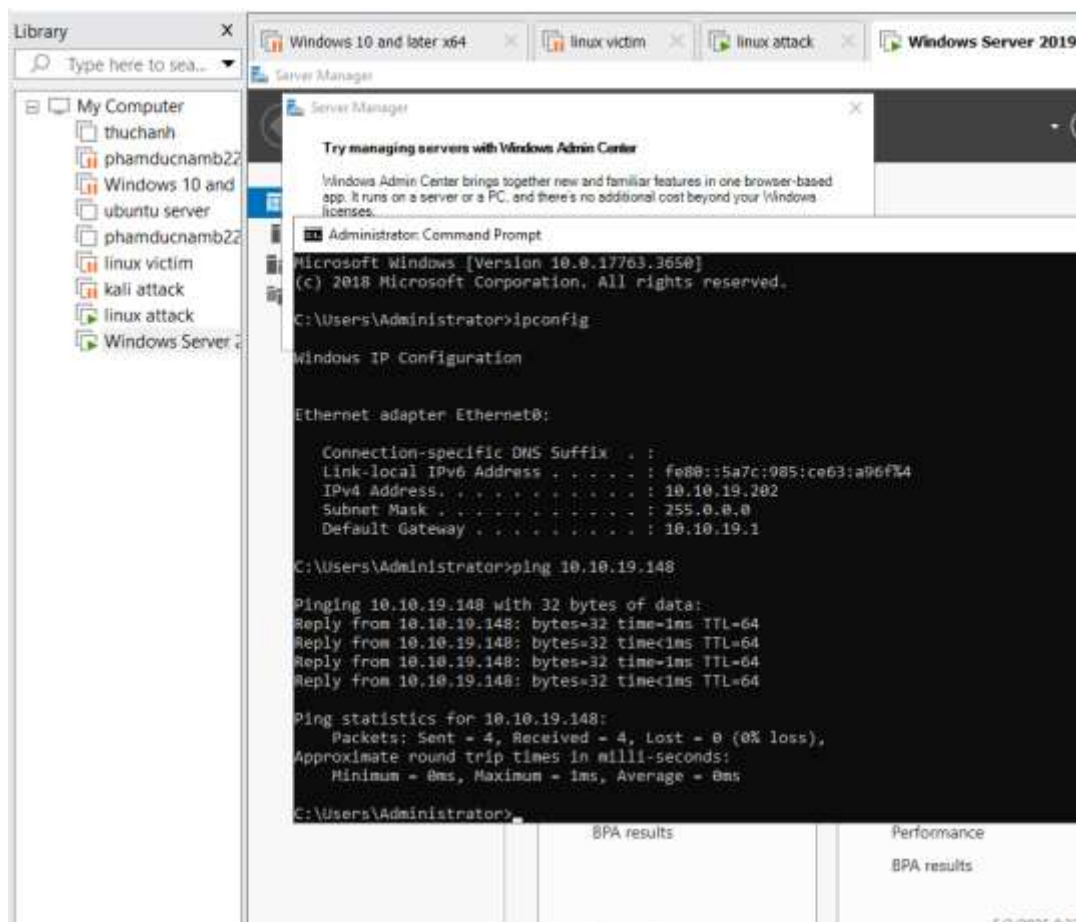


Hình 12 `sudo ifconfig ens33 10.10.19.148 netmask 255.255.255.0`

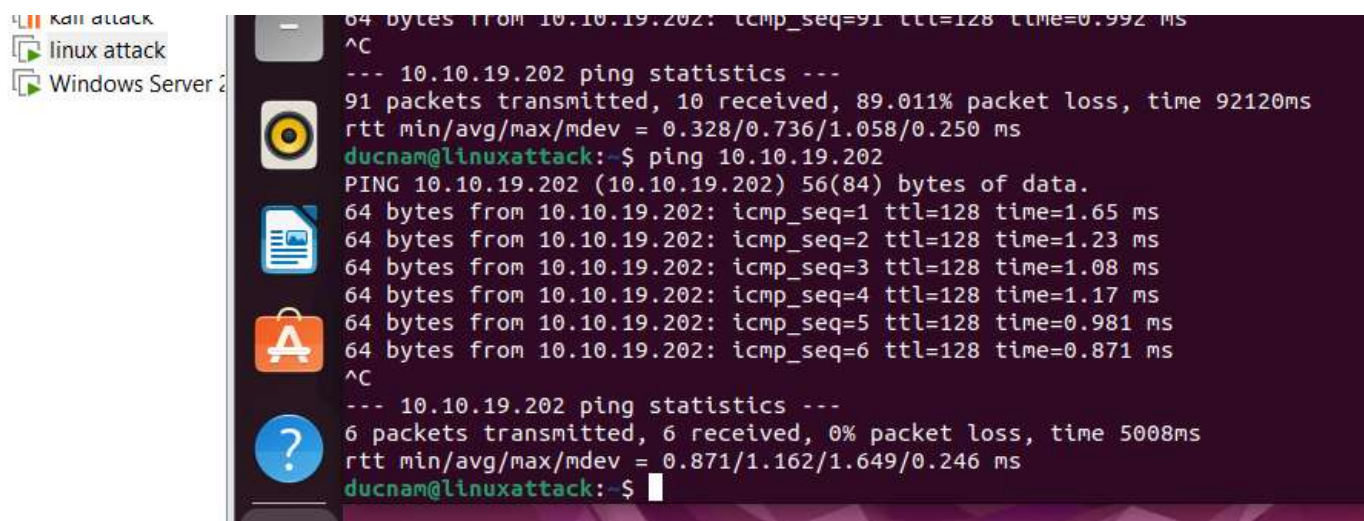
Cấu hình IP 10.10.19.202 cho máy Windows Server 2019:



Hình 13 cấu hình window external



Hình 14 Ping 2 máy External với nhau Windows Server và Linux Victim



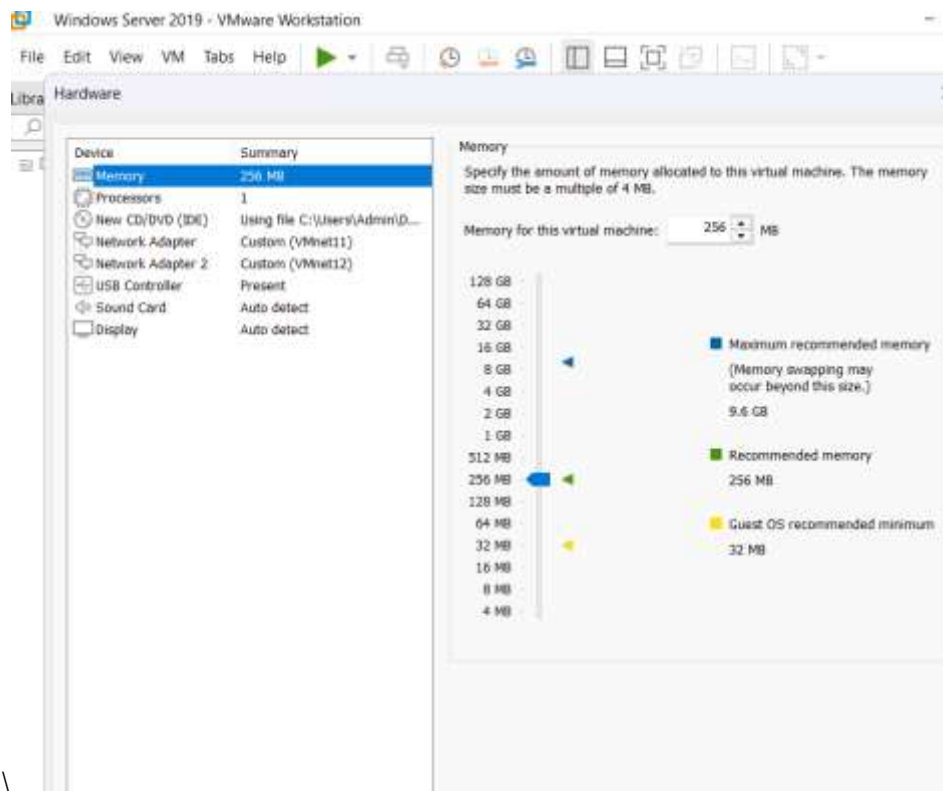
```
64 bytes from 10.10.19.202: icmp_seq=91 ttl=128 time=0.992 ms
^C
--- 10.10.19.202 ping statistics ---
91 packets transmitted, 10 received, 89.011% packet loss, time 92120ms
rtt min/avg/max/mdev = 0.328/0.736/1.058/0.250 ms
ducnam@linuxattack:~$ ping 10.10.19.202
PING 10.10.19.202 (10.10.19.202) 56(84) bytes of data:
64 bytes from 10.10.19.202: icmp_seq=1 ttl=128 time=1.65 ms
64 bytes from 10.10.19.202: icmp_seq=2 ttl=128 time=1.23 ms
64 bytes from 10.10.19.202: icmp_seq=3 ttl=128 time=1.08 ms
64 bytes from 10.10.19.202: icmp_seq=4 ttl=128 time=1.17 ms
64 bytes from 10.10.19.202: icmp_seq=5 ttl=128 time=0.981 ms
64 bytes from 10.10.19.202: icmp_seq=6 ttl=128 time=0.871 ms
^C
--- 10.10.19.202 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 0.871/1.162/1.649/0.246 ms
ducnam@linuxattack:~$
```

Hình 15 Kali Linux Attack và Windows Server

Chú ý: Khi ping từ các máy khác đến máy Windows Server nếu không ping thành công thì cần tắt tường lửa trên Windows

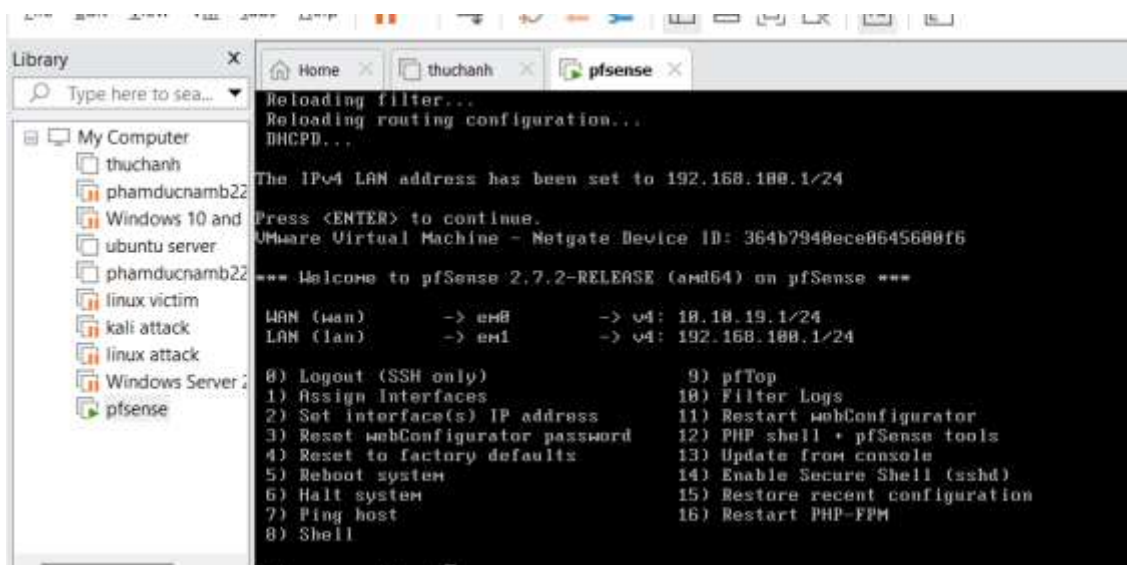
Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

Cài đặt card mạng Vmware11 và Vmware12 cho máy ảo pfsense firewall



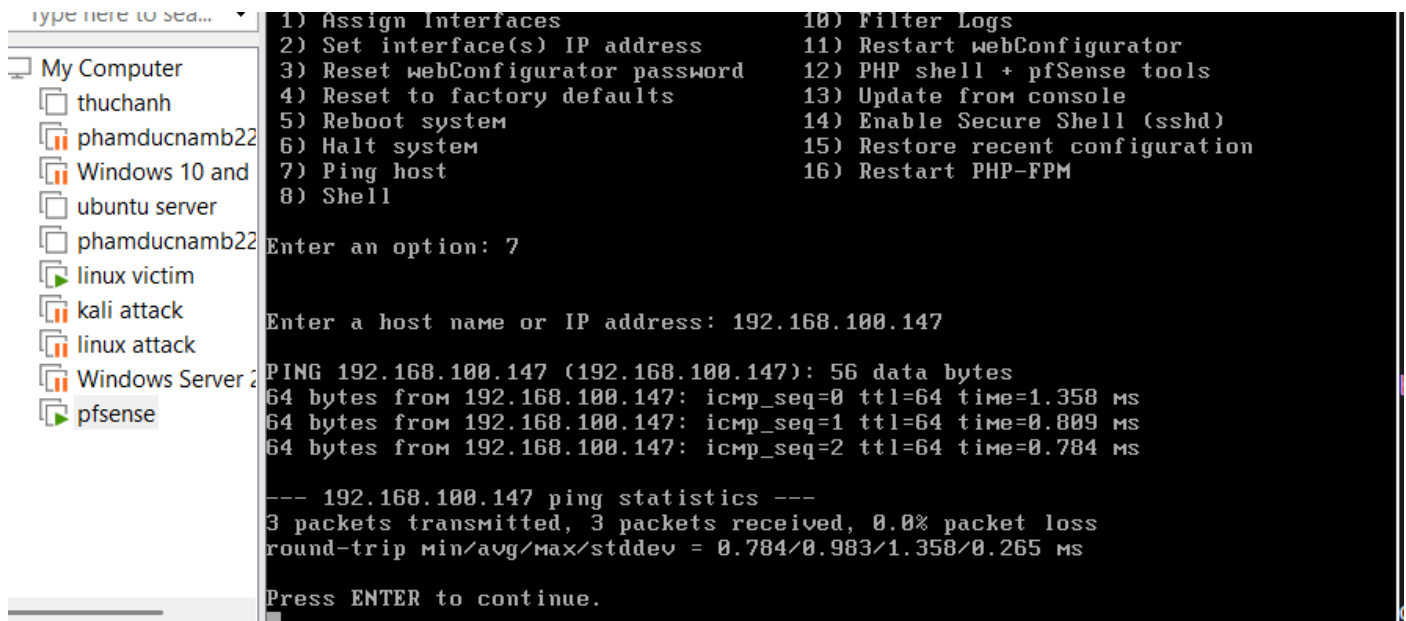
Hình 16 cài đặt card mạng cho máy ảo pfsense firewall

Khởi động máy ảo, cài đặt cấu hình WAN interfaces và LAN interfaces. Chú ý, cả mạng WAN và mạng LAN đều không cần cài đặt IPv6 và DHCP. Ta được kết quả:



Hình 17 khởi động máy pfsense và cài cấu hình

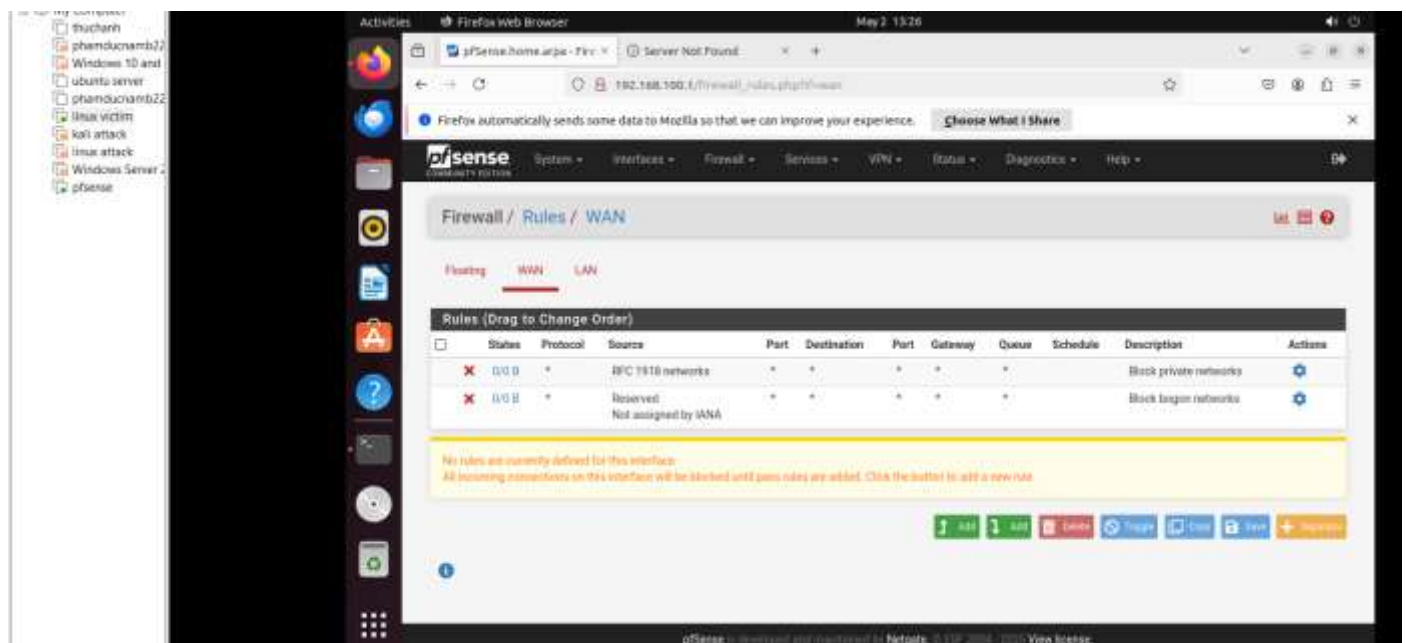
Ping thành công pfsense đến host ở LAN. Đến bước này máy ở External vẫn chưa ping được đến 10.10.19.1. Cần cấu hình firewall rule cho phép ICMP.



Hình 18 ping thành công đến các máy

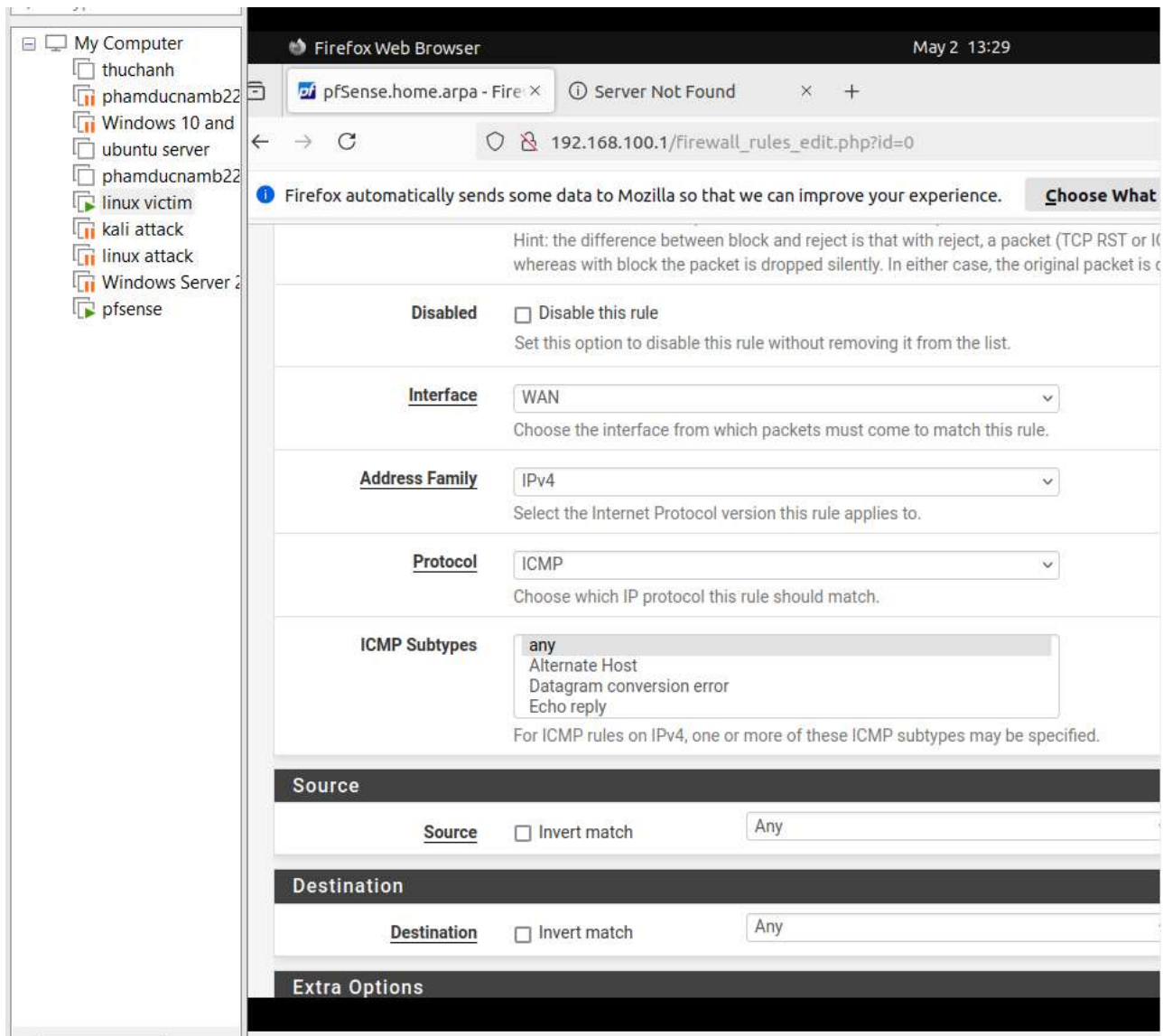
Cấu hình Firewall trên Pfsense:

Trên máy Linux victim ở mạng Internal, vào <http://192.168.100.1> để cấu hình pfsense qua giao diện web. Cần để những Rules ban đầu như hình bên dưới.



Hình 19 cấu hình firewall

Chọn Add để đặt tường lửa cho phép lưu lượng ICMP đi qua và Save và Apply change.



Hình 20 cấu hình firewall

Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>		0/0 B	IPv4 ICMP any	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Hình 21 cấu hình firewall

Bây giờ đã có thể ping từ Kali Linux Attack trong mạng External đến PfSense.


```
kali@kali: ~  
File Actions Edit View Help  
aunt qlen 1000  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
    valid_lft forever preferred_lft forever  
inet6 ::1/128 scope host noprefixroute  
    valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
roup default qlen 1000  
link/ether 00:0c:29:b0:99:cc brd ff:ff:ff:ff:ff:ff  
inet 10.10.19.148/24 brd 10.10.19.255 scope global eth0  
    valid_lft forever preferred_lft forever  
inet6 fe80::20c:29ff:feb0:99cc/64 scope link proto kernel_ll  
    valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$ ping 10.10.19.1  
PING 10.10.19.1 (10.10.19.1) 56(84) bytes of data.  
64 bytes from 10.10.19.1: icmp_seq=1 ttl=64 time=0.604 ms  
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.764 ms  
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.521 ms  
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=1.22 ms  
64 bytes from 10.10.19.1: icmp_seq=5 ttl=64 time=0.311 ms  
64 bytes from 10.10.19.1: icmp_seq=6 ttl=64 time=0.336 ms  
^C  
— 10.10.19.1 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5098ms  
rtt min/avg/max/mdev = 0.311/0.625/1.217/0.306 ms  
  
Command Prompt  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\Admin>B22DCAT206-PHAMDUCNAM  
'B22DCAT206-PHAMDUCNAM' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\Admin>_
```

Hình 22 ping từ kali attack đến các máy external

Trả lời các câu hỏi:

Theo mặc định, có 2 cổng TCP mở trên giao diện mạng Internal của Pfsense. Xem và kiểm tra: nmap 192.168.100.1

```
└─$ nmap 192.168.100.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-01 08:50 B
Nmap scan report for 192.168.100.1
Host is up (0.0042s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http

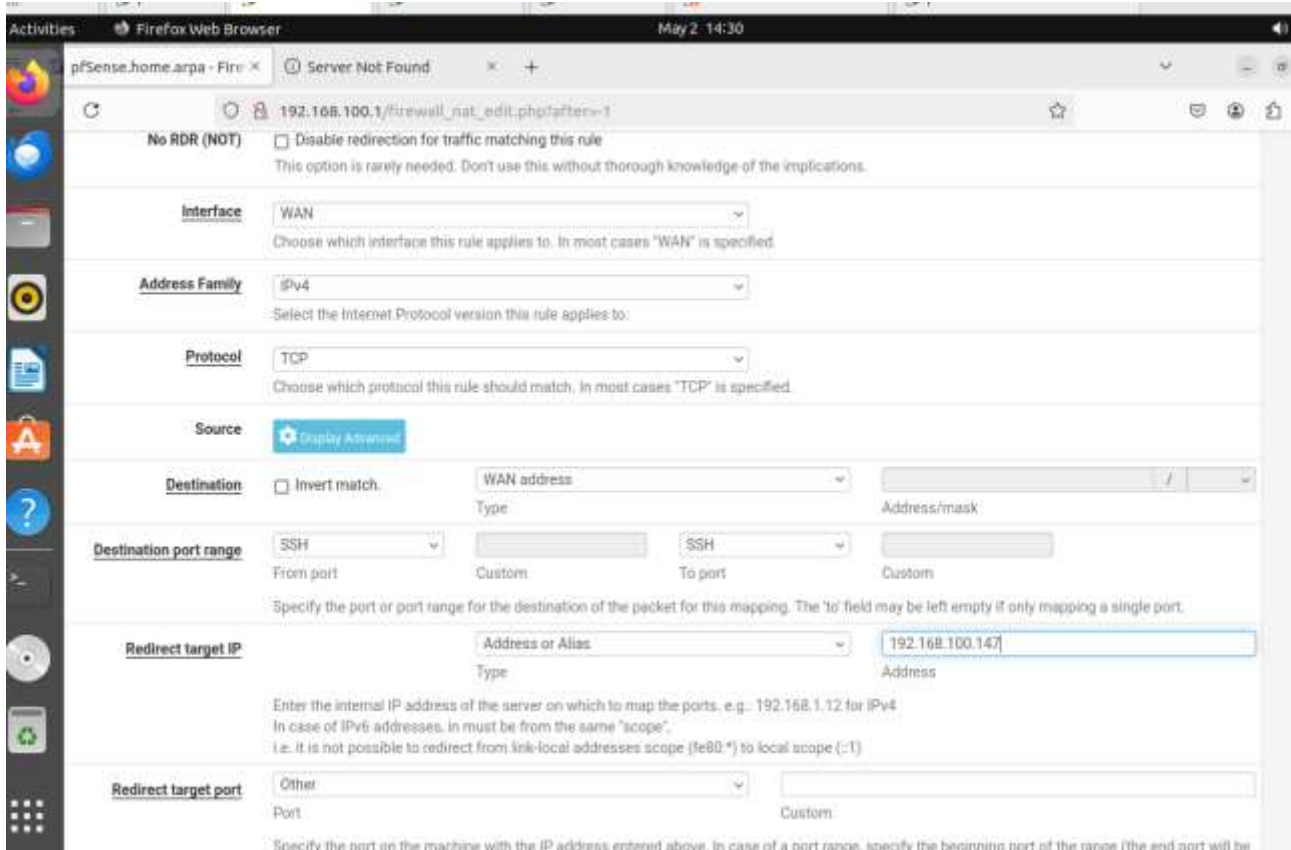
Nmap done: 1 IP address (1 host up) scanned in 17.64 seconds
```

Hình 23 kiểm tra nmap

Theo mặc định, không có cổng TCP nào mở trên giao diện mạng External của Pfsense. Xem và kiểm tra: nmap 10.10.19.1

Cài đặt cấu hình pfSense firewall cho phép chuyển hướng lưu lượng tới các máy Linux Victim trong mạng Internal

Vào <http://192.168.100.1> ở máy internal để cấu hình nat qua giao diện web



Hình 24 cấu hình nat qua giao diện web

Redirect target IP

Type: Address:

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope".
i.e. It is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

Other

Port: Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description

A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync

☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

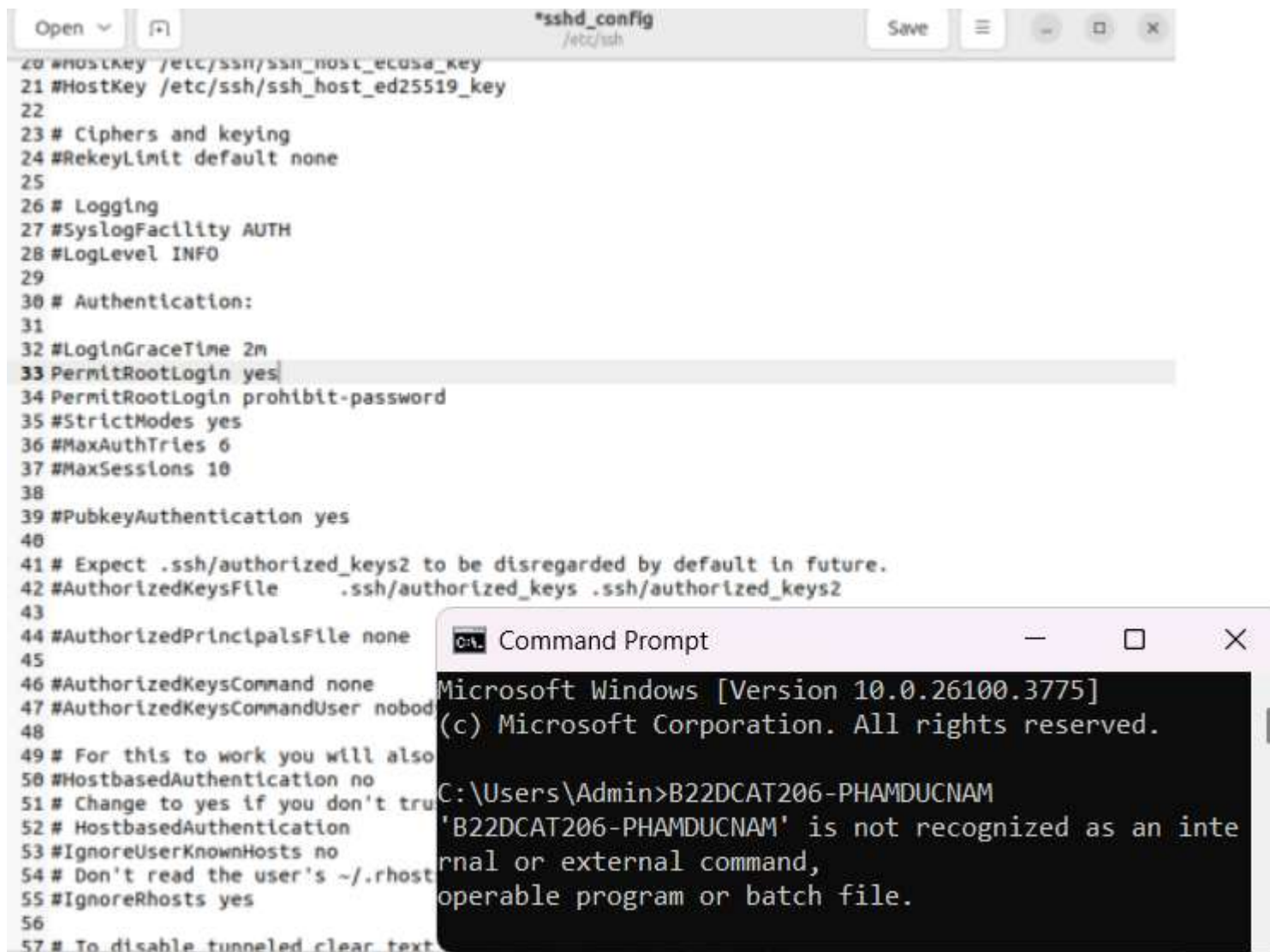
NAT reflection

Filter rule association

The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Hình 25 cấu hình nat qua giao diện web

Ở máy Victim mạng Internal, cấu hình cho phép dịch vụ ssh.



Hình 26 chỉnh sửa file cấu hình

```
c) Microsoft Corporation. All rights reserved.

:\Users\Admin>B22DCAT206-PHAMDUCNAM

commit changes to dconf:
file or directory)
hline:~$ sudo systemctl s

atus ssh
ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
  Active: active (running) since Sun 2025-03-23 23:21:49 +07; 17min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 853 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 942 (sshd)
    Tasks: 1 (limit: 2211)
   Memory: 376.0K
      CPU: 82ms
   CGroup: /system.slice/ssh.service
           └─942 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Hình 27 SSH ở máy Linux Victim Internal đã được bật

Kết luận

Lý thuyết về cấu hình mạng trong phần mềm mô phỏng VMware

Lý thuyết về Pfsense firewall

Cách cấu hình topo mạng

Cách cài đặt, cấu hình pfsense firewall, cách cài đặt firewall rules, chuyển hướng lưu lượng trong pfsense firewall thành công

Tài liệu tham khảo

[1]. VMware Workstation Networking Overview:

<https://masteringvmware.com/vmware-workstation-networkingoverview/>

[2]. Giới thiệu về Pfsense:

<https://viblo.asia/p/network-gioi-thieu-vepfsense> N0bDM6LXv2X4

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

