

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN 1



Môn học: Thực Tập Cơ Sở

Báo Cáo Bài Thực Hành 5

Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Đinh Trường Duy

Hà Nội, 2/2024

Mục lục

1. Mục đích	2
2. Nội dung thực hành	2
2.1. Cơ sở lý thuyết	2
2.1.1. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware	2
a. Switch ảo (Virtual Switch)	2
b. Card mạng ảo trên máy ảo	3
c. DHCP server ảo của Vmnet	3
d. LAN Segment	4
e. Các cơ chế hoạt động và các mô hình cơ bản khi cấu hình với switch ảo (VMnet)	5
2.1.2. Tìm hiểu về Pfsense	6
a. Giới thiệu	6
b. Các tính năng trong pfsense	6
c. Tổng kết	8
2.2. Nội dung thực hành	9
2.2.1. Chuẩn bị môi trường	9
2.2.2. Cấu hình topo mạng	9
2.2.3. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP	18
2.2.4. Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy Linux Victim trong mạng Internal	23
3. Kết luận	25
4. Tài liệu tham khảo	26

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.

2. Nội dung thực hành

2.1. Cơ sở lý thuyết

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

VMware Workstation là phần mềm ảo hóa trên máy tính, cung cấp khả năng chạy và mô phỏng nhiều hệ điều hành trên một máy tính vật lý. Wmware Workstation đi kèm - nhiều tính năng kết nối mạng giúp bạn tạo và quản lý mạng riêng, chia sẻ hoặc cách ly mạng bên trong Vmware.

Để có thể sử dụng phần mềm này hiệu quả, chúng ta cần phải hiểu về các kết nối mạng, cách thiết lập và cài đặt hệ thống mạng ảo trong phần mềm. Các thành phần hình thành nên mạng ảo trong VMware gồm switch ảo, card mạng ảo, DHCP server ảo và thiết bị NAT.

a. Switch ảo (Virtual Switch)

Cũng giống như switch vật lý, một Virtual Switch kết nối các thành phần mạng ảo lại với nhau. Những switch ảo hay còn gọi là mạng ảo, chúng có tên là VMnet0, VMnet1, VMnet2... một số switch ảo được gắn vào mạng một cách mặc định. Mặc định khi ta cài Wmware thì có sẵn 3 Switch ảo như sau:

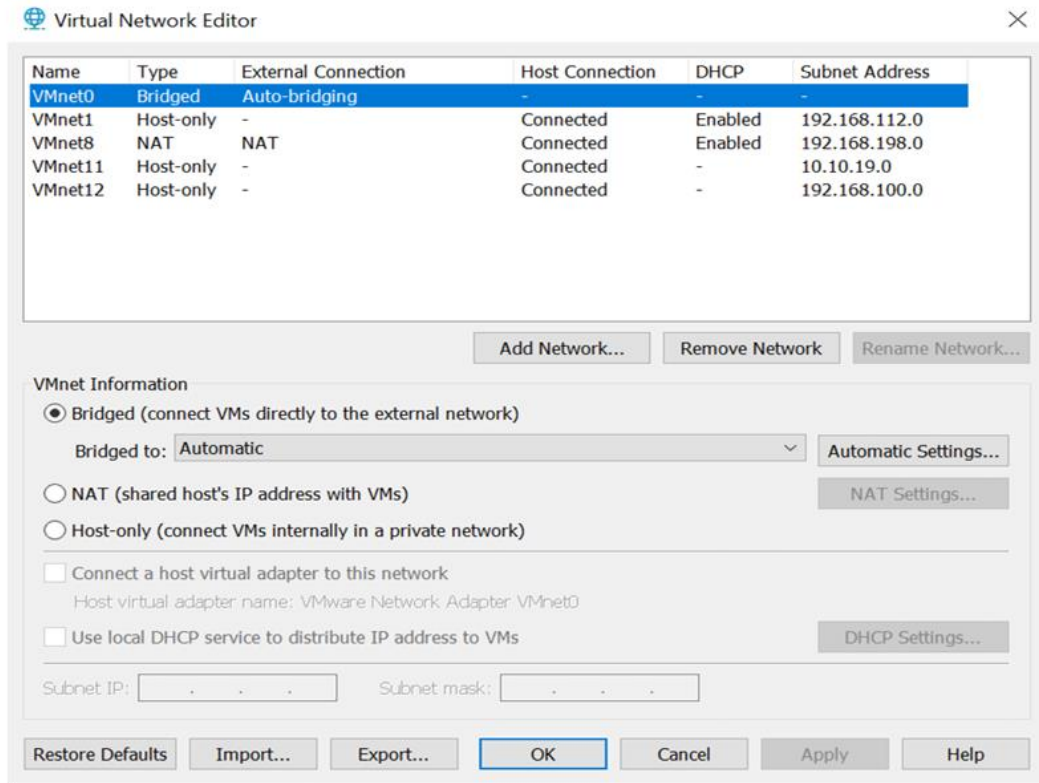
- VMnet0 chế độ Bridged (cầu nối),
- VMnet8 chế độ NAT
- VMnet1 chế độ Host-only.

Ta có thể thêm, bớt, chỉnh các option của VMnet bằng cách vào menu Edit -> Virtual Network Editor...

VMware Workstation (phiên bản 12) cho phép tạo 20 switch ảo trên Windows và 255 cái trên Linux. Trên mỗi Switch ảo trên Windows thì các kết nối của các máy tính ảo (host) vào mỗi Switch ảo là không giới hạn, còn trên Linux thì 32 máy ảo. Để thêm hoặc bớt VMnet ta có thể chọn Add Network... và Remove Network...

Khi ta tạo các VMnet, thì trên máy thật sẽ tạo ra những card mạng ảo tương ứng với VMnet đó, dùng để kết nối Virtual Switch với máy tính thật, giúp máy thật và máy ảo có thể liên lạc được với nhau. Riêng VMnet0 kết nối trực tiếp với card mạng vật lý

thông qua cơ chế bắt cầu (bridged) nên không tạo ra card VMnet. VMnet8 mặc định sẽ sử dụng cơ chế NAT. Các VMnet khác khi được thêm vào sẽ là Host-Only.



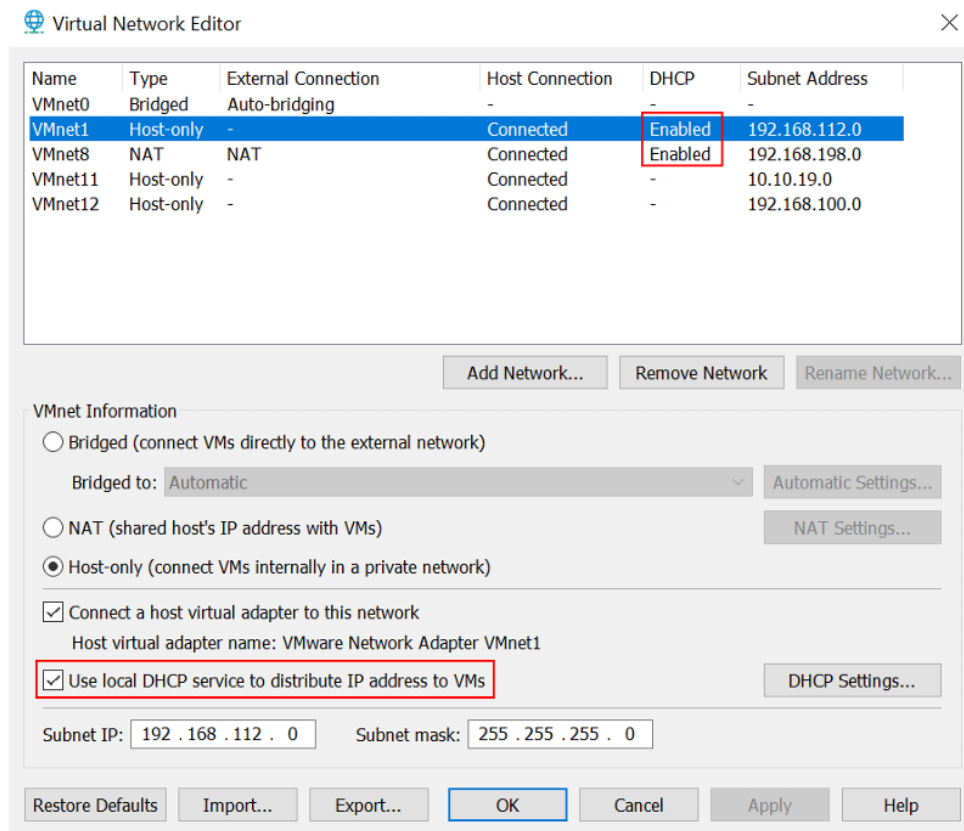
Trong một số trường hợp, có thể card mạng ảo kết nối máy thật với các VMnet chưa được bật lên. Để bật các card này, trên Virtual Network Editor, bạn chọn VMnet cần bật card kết nối từ máy thật vào VMnet, chọn check vào ô Connect a host virtual adapter to this network.

b. Card mạng ảo trên máy ảo

Khi bạn tạo một máy ảo mới, card mạng được tạo ra cho máy ảo, những card mạng này hiển thị trên hệ điều hành máy ảo với tên thiết bị như là AMD PCNET PCI hay Intel Pro/1000 MT Server Adapter. Từ VMware Workstation 6.0 trở về sau này máy ảo có thể hỗ trợ đến 10 card, các phiên bản trước bị giới hạn ở 3 card mạng. Thêm bớt card mạng bạn nhấn vào nút Add... hoặc Remove... trong Virtual Machine Setting

c. DHCP server ảo của Vmnet

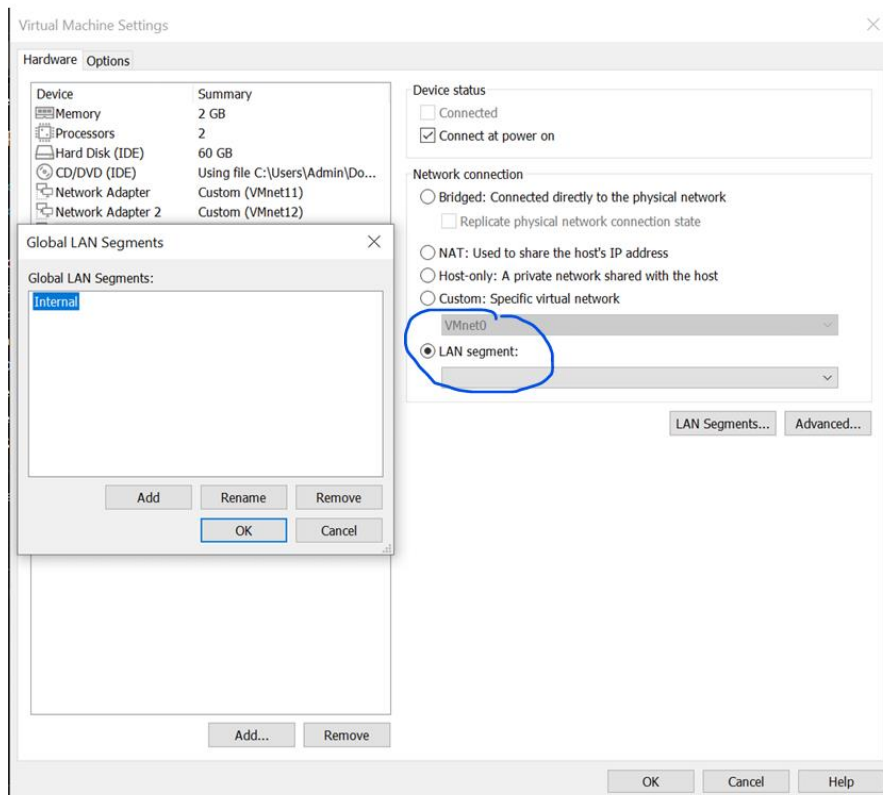
DHCP (Dynamic Host Configuration) server ảo đảm nhiệm việc cung cấp địa chỉ IP cho các máy ảo trong việc kết nối máy ảo vào các Switch ảo không có tính năng Bridged (VMnet0). DHCP server ảo cấp phát địa chỉ IP cho các máy ảo có kết nối với VMnet Host-only và NAT.



Nếu không muốn sử dụng DHCP server ảo của VMnet, bạn chỉ cần bỏ dấu check tại Use local DHCP service to distribute IP address to VMs. Nếu bạn muốn tùy chỉnh lại DHCP, bạn có thể chọn vào DHCP Setting, ở đây, bạn có thể chỉnh lại các tham số thời gian, tham số Scope IP (lưu ý: bạn chỉ có thể sửa lại vùng địa chỉ host chứ không được chỉnh lại vùng network).

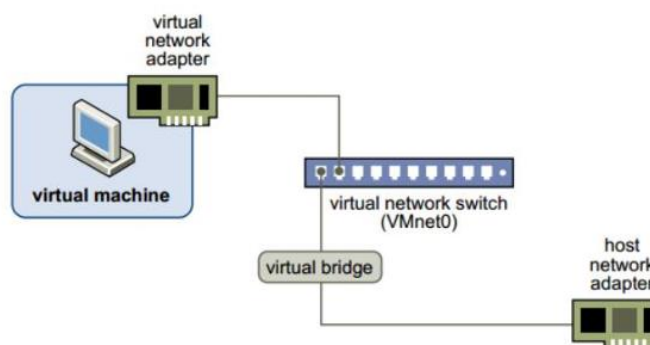
d. LAN Segment

Các card mạng của máy ảo có thể gắn kết với nhau thành từng LAN Segment. Không giống như VMnet, LAN Segment chỉ kết nối các máy ảo được gán trong một LAN Segment lại với nhau mà không có những tính năng như DHCP và LAN Segment không thể kết nối ra máy thật như các Virtual Switch VMnet.



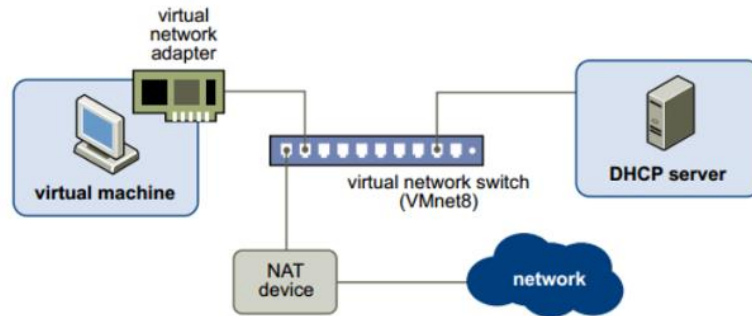
e. Các cơ chế hoạt động và các mô hình cơ bản khi cấu hình với switch ảo (VMnet)

- **Chế độ Bridge:** Ở chế độ này, card mạng trên máy ảo được gắn vào VMnet0, VMnet0 này liên kết trực tiếp với card mạng vật lý trên máy thật, máy ảo lúc này sẽ kết nối internet thông qua card mạng vật lý và có chung lớp mạng với card mạng vật lý.

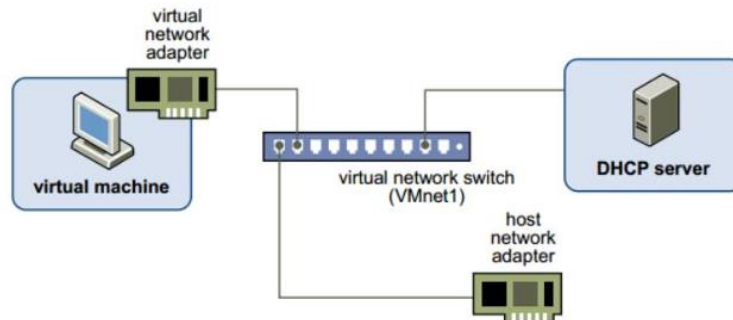


- **Chế độ NAT:** Ở chế độ này, card mạng của máy ảo kết nối với VMnet8, VNnet8 cho phép máy ảo đi ra mạng vật lý bên ngoài internet thông qua cơ chế NAT (NAT device). Lúc này lớp mạng bên trong máy ảo khác hoàn toàn với lớp mạng của card vật lý bên ngoài, hai mạng hoàn toàn tách biệt. IP của card mạng 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.



2.1.2. Tìm hiểu về Pfsense

a. Giới thiệu

Để bảo vệ hệ thống mạng thì ta có nhiều giải pháp như sử dụng router cisco, dùng firewall cứng, firewall mềm của microsoft như ISA ... Những thiết bị như trên rất tốn kinh phí vì vậy đối với các doanh nghiệp vừa và nhỏ thì giải pháp firewall mềm mã nguồn mở là một phương án hiệu quả. Pfsense là một ứng dụng có chức năng định tuyến vào tường lửa mạng và miễn phí dựa trên nền tảng FreeBSD có chức năng định tuyến và tường lửa rất mạnh. Pfsense được cấu hình qua giao diện GUI trên nền web nên có thể quản lý một cách dễ dàng. Nó hỗ trợ lọc theo địa chỉ nguồn, đích, cũng như port nguồn hay port đích đồng thời hỗ trợ định tuyến và có thể hoạt động trong chế độ bridge hay transparent. Nếu sử dụng pfsense là gateway, ta cũng có thể thấy rõ việc hỗ trợ NAT và port forward trên pfsense cũng như thực hiện cân bằng tải hay failover trên các đường mạng.

b. Các tính năng trong pfsense

❖ Aliases

Trong pfsense, firewall không thể có 1 rule gồm nhiều nhóm IP hoặc 1 nhóm port. Vì vậy, điều ta cần làm là gom nhóm các IP, Port hoặc URL vào thành 1 alias. Một alias sẽ cho phép thay thế 1 host, 1 dải mạng, nhiều IP riêng biệt hay 1 nhóm port, URL ... Alias giúp ta tiết kiệm được phần lớn thời gian nếu bạn sử dụng một cách chính xác như thay vì sử dụng hàng loạt rule để thiết lập cho nhiều địa chỉ, ta có thể sử dụng 1 rule duy nhất để gom nhóm lại.

❖ NAT

Pfsense có hỗ trợ nat static dưới dạng nat 1:1. Điều kiện để thực hiện được nat 1:1 là ta phải có IP public. Khi thực hiện nat 1:1 thì IP private được nat sẽ luôn ra ngoài bằng IP public tương ứng và các port cũng tương ứng trên IP public.

Pfsense hỗ trợ nat outbound mặc định với Automatic outbound NAT rule generation. Để cấu hình thủ công, ta chọn Manual Outbound NAT rule generation (AON - Advanced Outbound NAT) và xóa các rule mặc định của pfsense đi đồng thời cấu hình thêm các rule outbound.

Ngoài 3 kiểu Nat: port forward, 1:1 và outbound, pfsense còn hỗ trợ NAT Npt. Phương thức này thực hiện NAT đối với Ipv6.

❖ Firewall Rules

Là nơi lưu trữ tất cả các luật ra, vào trên pfsense. Mặc định PfSense cho phép mọi kết nối ra, vào (tại cổng LAN có sẵn rule any à any). Ta phải tạo các rule để quản lý mạng bên trong.

❖ Traffic shaper

Đây là tính năng giúp quản trị mạng có thể tinh chỉnh, tối ưu hóa đường truyền trong pfsense. Trong pfsense, 1 đường truyền băng thông sẽ chia ra các hàng khác nhau. Có 7 loại hàng trong pfsense:

- Hàng qACK: dành cho các gói ACK (gói xác nhận) trong giao thức TCP ở những ứng dụng chính cần được hỗ trợ như HTTP, SMTP ... luồng thông tin ACK tương đối nhỏ nhưng lại rất cần thiết để duy trì tốc độ lưu thông lớn.
- Hàng qVoIP: dành cho những loại lưu thông cần đảm bảo độ trễ nghiêm ngặt, thường dưới 10ms như VoIP, video conferences.
- Hàng qGames: dành cho những loại lưu thông cần đảm bảo độ trễ rất chặt chẽ, thường dưới 50ms như SSH, game online ...
- Hàng qOthersHigh: dành cho các loại ứng dụng quan trọng có tính tương tác rất cao, cần đáp ứng nhanh, cần độ trễ thấp như: NTP, DNS, SNMP ...
- Hàng qOthersDefault: dành cho các giao thức ứng dụng quan trọng có tính tương tác vừa, cần độ đáp ứng nhất định như HTTP, IMAP ...

- Hàng qOthersLow: dành cho các giao thức ứng dụng quan trọng nhưng có tính tương tác thấp như SMTP, POP3, FTP
- Hàng qP2P: dành cho các ứng dụng không tương tác, không cần đáp ứng nhanh như bittorrent

Mặc định trong pfsense, các hàng sẽ có độ ưu tiên từ thấp đến cao: qP2P < qOthersLow < qOthersDefault < qOthersHigh < qGames < qACK < qVoIP.

Ta có thể chỉnh lại độ ưu tiên priority cũng như dung lượng băng thông bandwidth mặc định mà các hàng chiếm để nâng cao băng thông cho các hàng tương ứng.

Pfsense cũng hỗ trợ giới hạn tốc độ download/upload của 1 IP hoặc 1 dải IP với ta thiết lập thông số tại phần limiter. Firewall pfsense hỗ trợ chặn những ứng dụng chạy trên layer 7 – application trong mô hình OSI như sip, ftp, http ... trong phần Layer 7.

❖ VPN

Một tính năng khác không thể thiếu đối với các gateway là VPN. Pfsense cũng hỗ trợ VPN qua 4 giao thức: IPSec, L2TP, PPTP và OpenVPN.

❖ Monitor băng thông

Pfsense có rất nhiều plugin hỗ trợ monitor băng thông. Sau đây là 1 số plugin thông dụng:

RRD Graphs

Đây là tool mặc định có sẵn khi cài pfsense. Với RRD graphs, ta có thể theo dõi được trạng thái của server: memory, process ... hay với băng thông của các đường truyền LAN, WAN ...

Một nhược điểm của RRD Graphs là không theo dõi được dung lượng từng IP.

Lightsquid

Lightsquid là package hỗ trợ xem report trên pfsense sau khi đã cài gói squid.

Với Lightsquid, ta có thể check dung lượng mỗi IP sử dụng theo ngày. Tổng dung lượng ngày hôm đó sử dụng hay các trang web đã vào ...

BandwidthD

1 plugin nữa có thể monitor dung lượng sử dụng của IP là BandwidthD. BandwidthD thống kê dữ liệu theo từng IP, dung lượng gửi, nhận, các giao thức sử dụng như FTP, HTTP ...

Ntop

1 plugin thường được sử dụng nữa là Ntop. Với Ntop, ta có thể theo dõi băng thông hiện tại IP nào sử dụng lớn nhất, dung lượng tải của cổng, kết nối tới internet ...

c. Tổng kết

Hoàn toàn miễn phí, giá cả là ưu thế vượt trội của tường lửa pfsense. Tuy nhiên, rõ ràng 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.

2.2. Nội dung thực hành

2.2.1. 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 – Phuong126)

2.2.2. Cấu hình topo mạng

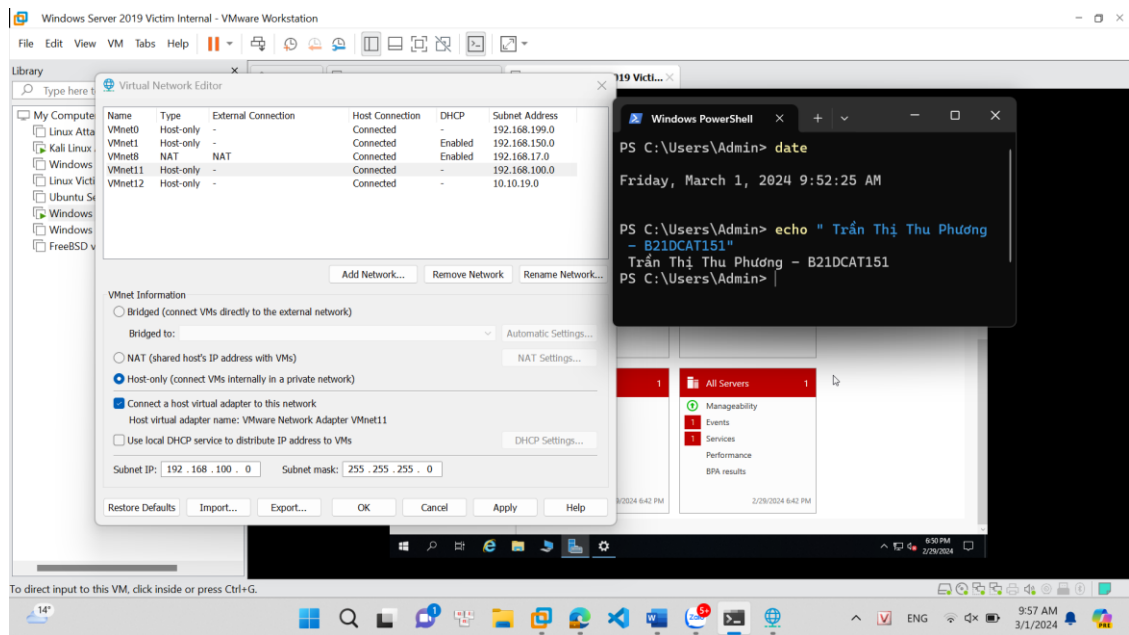
❖ Yêu cầu cài đặt và cấu hình hệ thống theo thông tin mô tả sau:

- 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

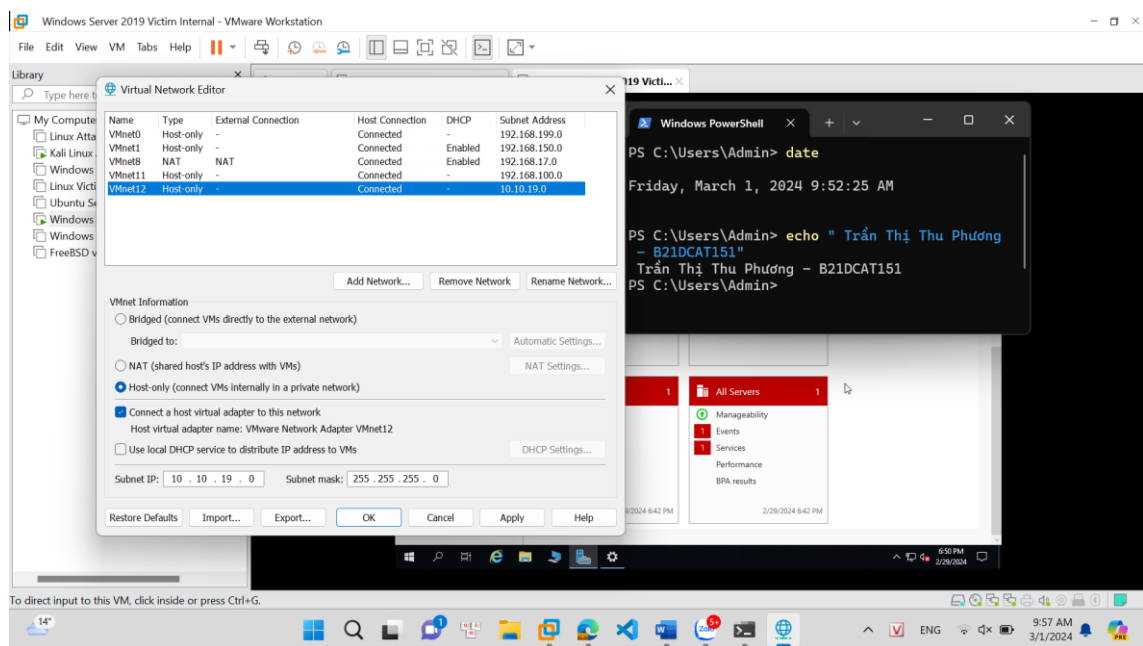
❖ Các bước thực hiện:

- Thêm card mạng ảo, VMnet11 và VMnet12 để tạo mạng cho các máy External và Internal.
 - + Vào VMware Workstation → Edit → Virtual Network Editor.

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall



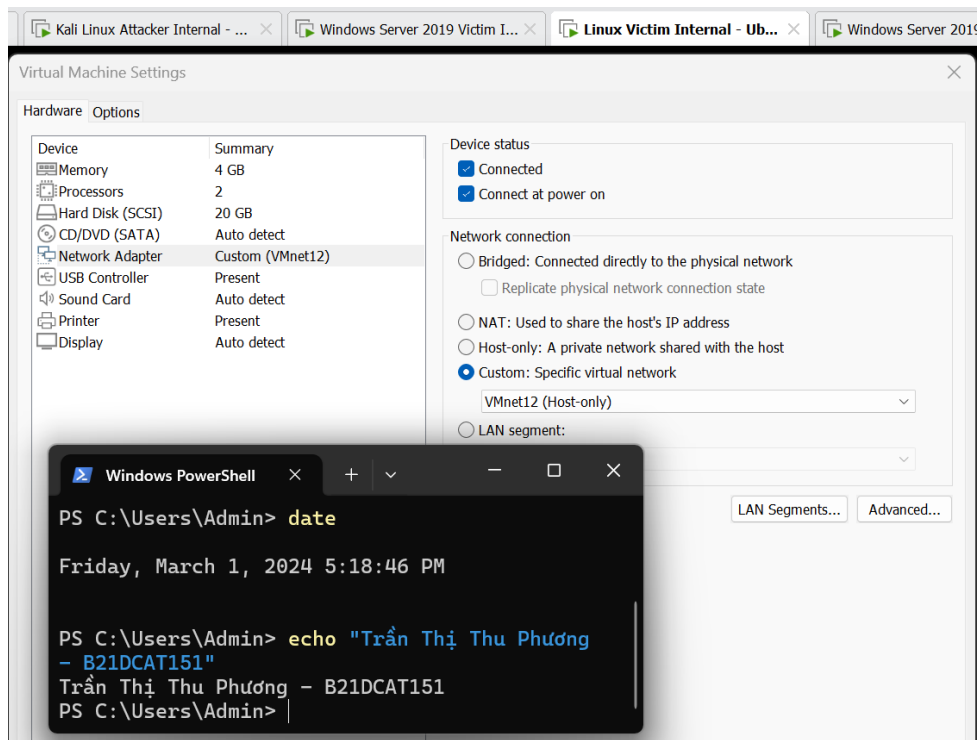
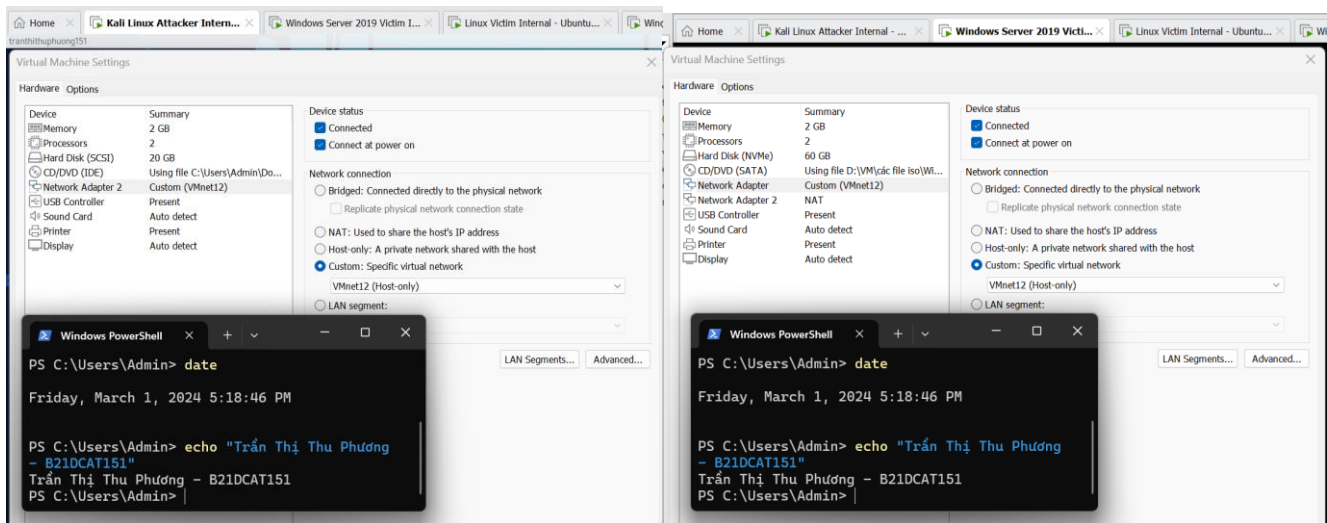
Mạng Vmware11



Mạng Vmware12

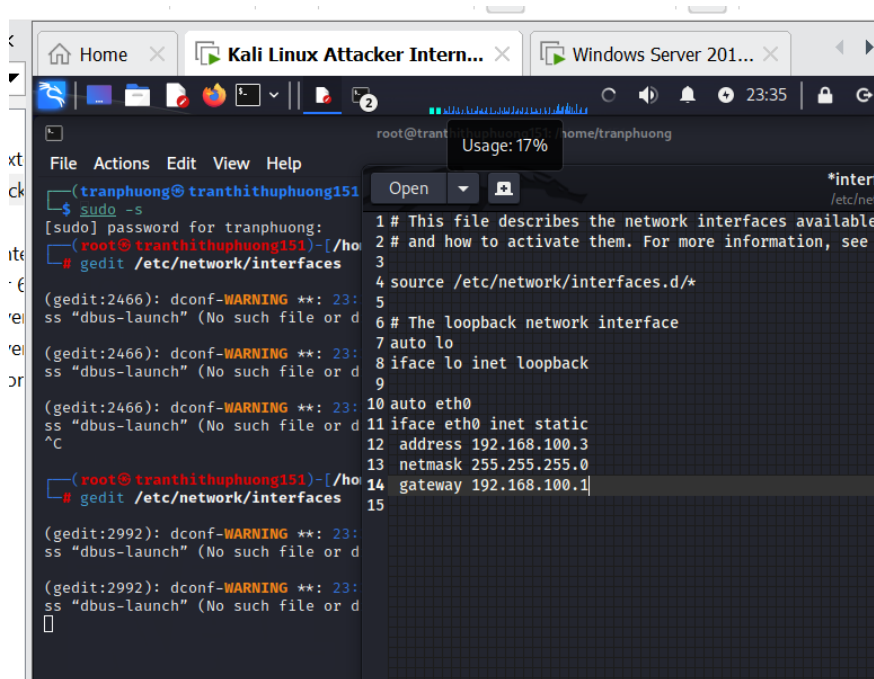
- Đối với các máy Internal: khi cài đặt với các máy Internal trong phần chọn card mạng ở Edit virtual machine settings, chọn mạng Internal đã tạo, **VMnet12**.

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall



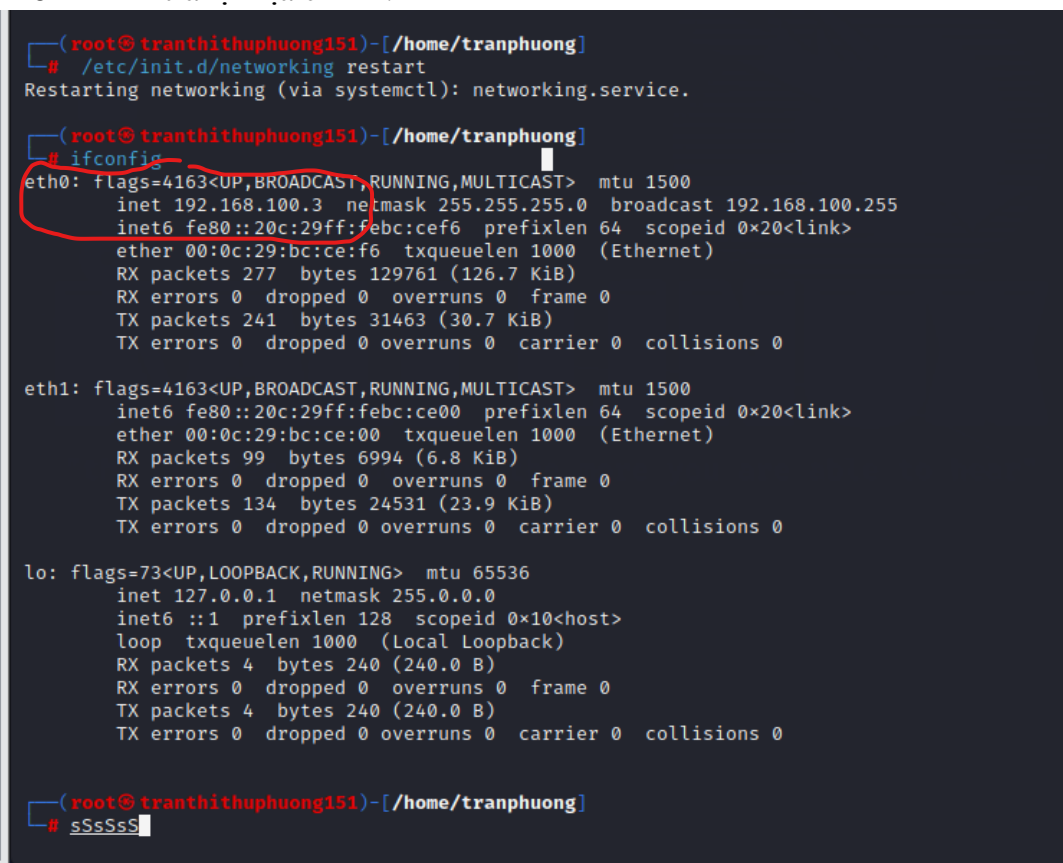
- + Cấu hình địa chỉ địa chỉ IP 192.168.100.3 cho máy Kali Linux Attack
 - o Chỉnh sửa file /etc/network/interfaces:
sudo gedit /etc/network/interfaces

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall



```
root@tranthithuphuong151:~# gedit /etc/network/interfaces
1 # This file describes the network interfaces available on your system
2 # and how to activate them. For more information, see the file
3 # /etc/network/interfaces.d/*
4 source /etc/network/interfaces.d/*
5
6 # The loopback network interface
7 auto lo
8 iface lo inet loopback
9
10 auto eth0
11 iface eth0 inet static
12 address 192.168.100.3
13 netmask 255.255.255.0
14 gateway 192.168.100.1
15
```

- Bật card mạng eth0 vừa được cấu hình: `/etc/init.d/networking restart`
- Kiểm tra lại địa chỉ IP:



```
(root@tranthithuphuong151)-[/home/tranphuong]
# /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.

(root@tranthithuphuong151)-[/home/tranphuong]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:febc:cef6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bc:ce:f6 txqueuelen 1000 (Ethernet)
    RX packets 277 bytes 129761 (126.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 241 bytes 31463 (30.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

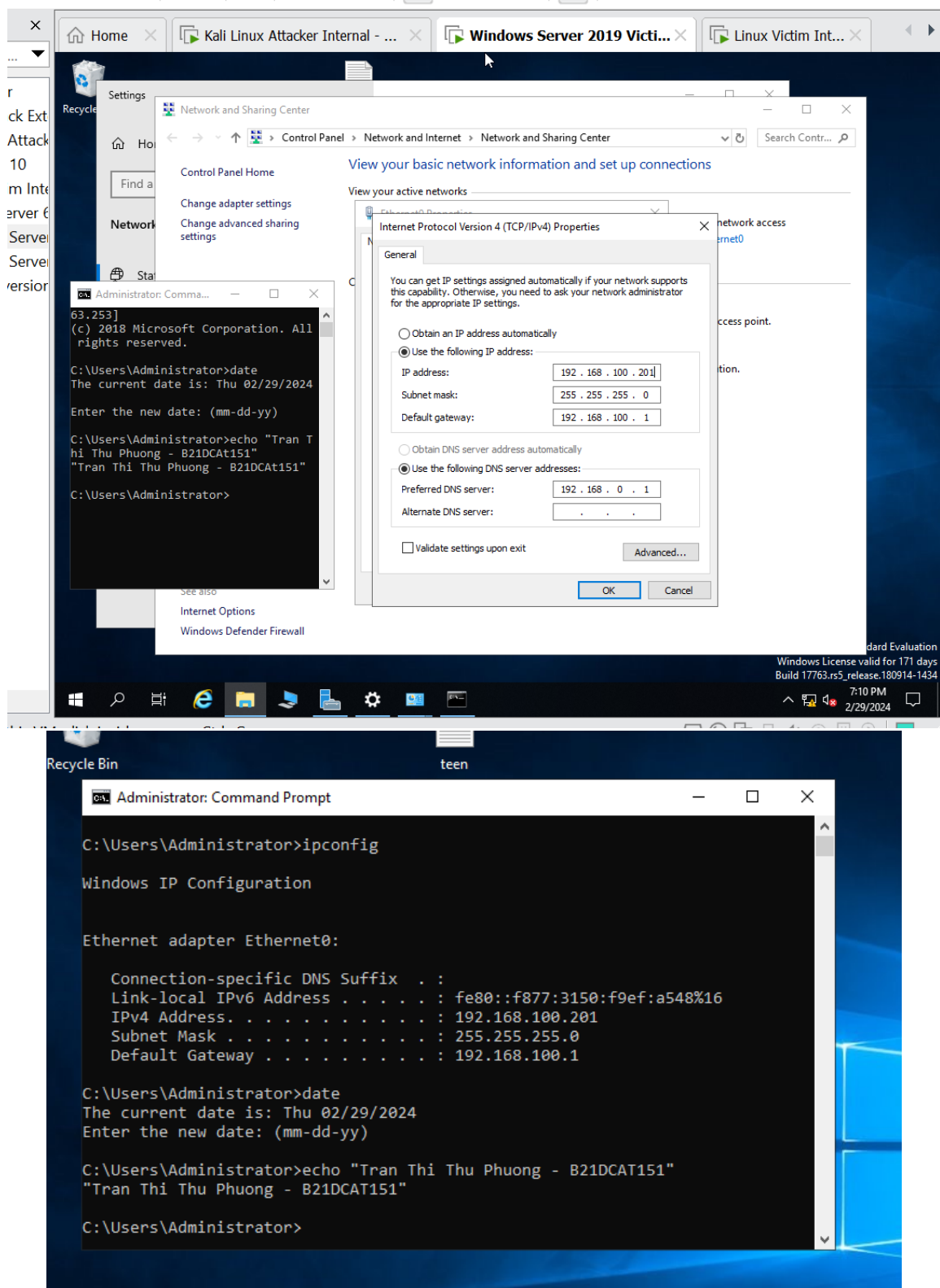
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::20c:29ff:febc:ce00 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bc:ce:00 txqueuelen 1000 (Ethernet)
    RX packets 99 bytes 6994 (6.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 134 bytes 24531 (23.9 KiB)
    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
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@tranthithuphuong151)-[/home/tranphuong]
# ssSsSs
```

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

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với PfSense firewall



Kiểm tra lại

- + 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

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

```
tranh
tranthithuphuongb21dcat151@slave-1: ~
File Edit View Search Terminal Help
tranthithuphuongb21dcat151@slave-1:~$ sudo ifconfig ens33 192.168.100.147
netmask 255.255.255.0
tranthithuphuongb21dcat151@slave-1:~$ 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
    ether 00:0c:29:67:7c:cb txqueuelen 1000 (Ethernet)
    RX packets 16 bytes 1376 (1.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 128 bytes 18061 (18.0 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
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2084 bytes 149013 (149.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2084 bytes 149013 (149.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tranthithuphuongb21dcat151@slave-1:~$
```

+ Ping thử các máy Internal với nhau

```
terminal - ... x Windows Server 2019 Victi... x
Recycle Bin teen
Administrator: Command Prompt
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 = 1ms, Maximum = 1ms, Average = 1ms

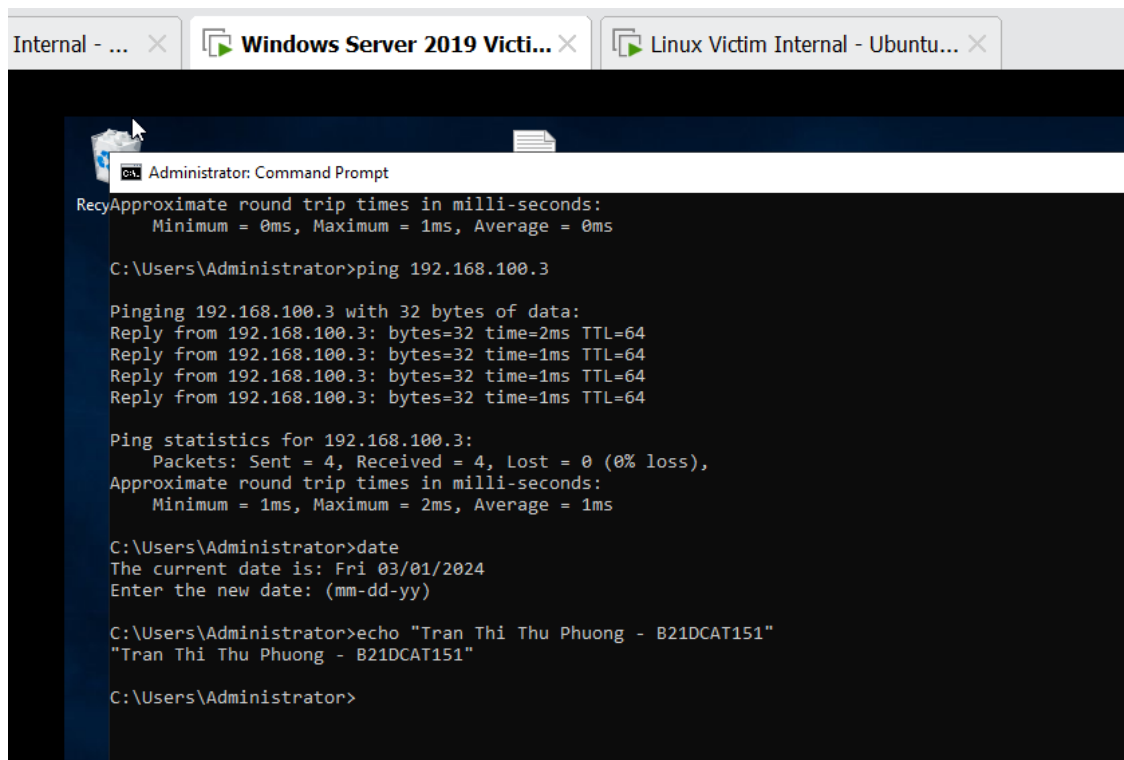
C:\Users\Administrator>date
The current date is: Thu 02/29/2024
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo "Tran Thi Thu Phuong - B21DCAT151"
"Tran Thi Thu Phuong - B21DCAT151"

C:\Users\Administrator>
```

Windows Server → Linux Victim

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall



The screenshot shows a Windows Server 2019 desktop environment. A Command Prompt window is open, displaying the following commands and their outputs:

```
Administrator: Command Prompt
ReceApproximate 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=2ms 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

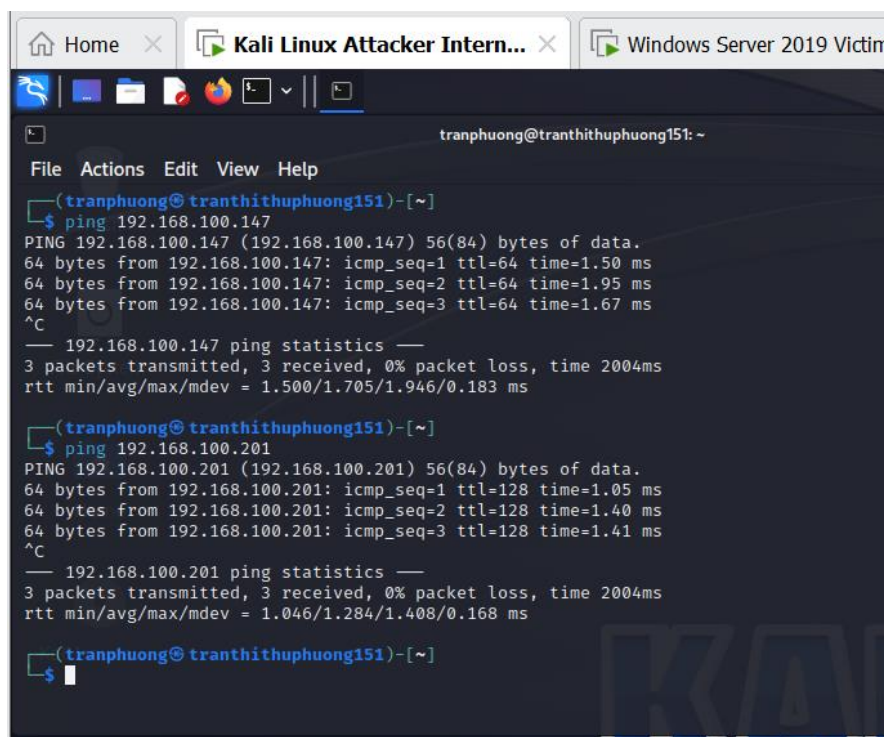
Ping statistics for 192.168.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Administrator>date
The current date is: Fri 03/01/2024
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo "Tran Thi Thu Phuong - B21DCAT151"
"Tran Thi Thu Phuong - B21DCAT151"

C:\Users\Administrator>
```

Windows Server Victim → Kali Attack



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the following commands and their outputs:

```
Home x Kali Linux Attacker Intern... x Windows Server 2019 Victim
tranphuong@tranthithuphuong151: ~
File Actions Edit View Help

(tranphuong@tranthithuphuong151)-[~]
$ ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data.
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=1.50 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=1.95 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=1.67 ms
^C
--- 192.168.100.147 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.500/1.705/1.946/0.183 ms

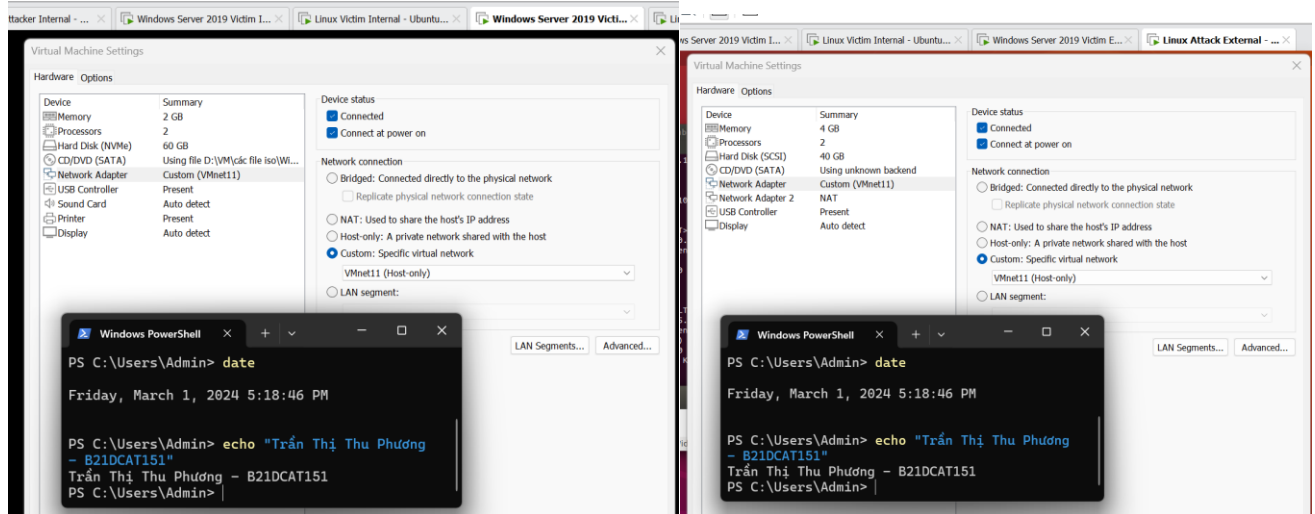
(tranphuong@tranthithuphuong151)-[~]
$ ping 192.168.100.201
PING 192.168.100.201 (192.168.100.201) 56(84) bytes of data.
64 bytes from 192.168.100.201: icmp_seq=1 ttl=128 time=1.05 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=1.40 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=128 time=1.41 ms
^C
--- 192.168.100.201 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.046/1.284/1.408/0.168 ms

(tranphuong@tranthithuphuong151)-[~]
$
```

Kali Attack → 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.

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

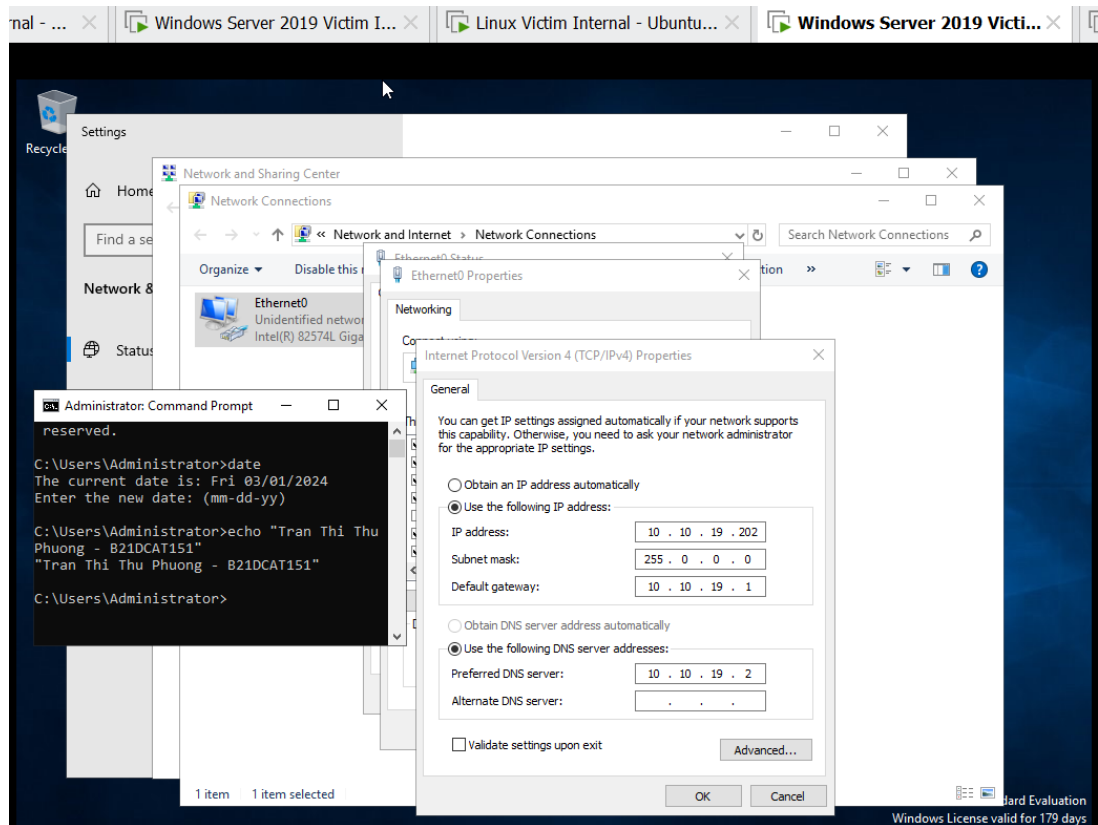


- + Cấu hình IP 10.10.19.148 cho máy Linux Attack:
sudo ifconfig eth1 10.10.19.148 netmask 255.255.255.0

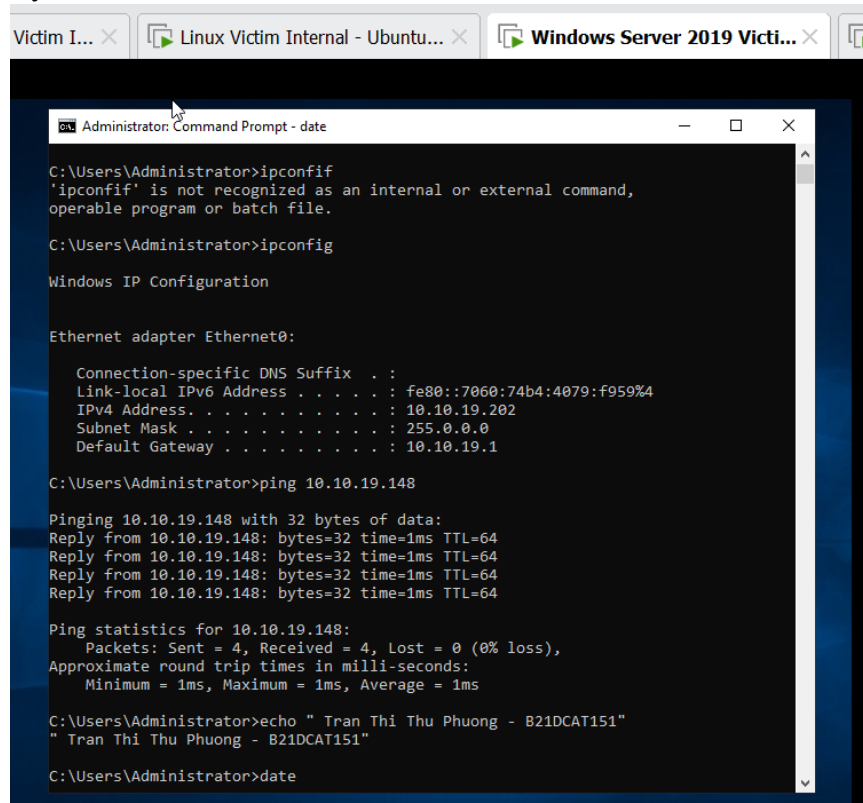
```
tranphuong@tranthithuphuong151: ~  
(tranphuong@tranthithuphuong151)-[~]  
$ sudo ifup eth1  
(tranphuong@tranthithuphuong151)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.17.166 netmask 255.255.255.0 broadcast 192.168.17.255  
    inet6 fe80::20c:29ff:fe38:c8dc prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:38:c8:dc txqueuelen 1000 (Ethernet)  
    RX packets 2666 bytes 3643172 (3.4 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 496 bytes 41216 (40.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.10.19.148 netmask 255.255.255.0 broadcast 10.10.19.255  
    ether 00:0c:29:38:c8:e6 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    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
```

- + Cấu hình IP 10.10.19.202 cho máy Windows Server 2019:

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall



+ Ping 2 máy External với nhau



Windows Server → Linux Victim

```
tranphuong@tranthithuphuong151: ~  
TX packets 32  bytes 1920 (1.8 KiB)  
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
(tranphuong@tranthithuphuong151)-[~]  
$ 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=1.73 ms  
64 bytes from 10.10.19.202: icmp_seq=2 ttl=128 time=1.35 ms  
64 bytes from 10.10.19.202: icmp_seq=3 ttl=128 time=1.21 ms  
64 bytes from 10.10.19.202: icmp_seq=4 ttl=128 time=1.03 ms  
64 bytes from 10.10.19.202: icmp_seq=5 ttl=128 time=1.22 ms  
64 bytes from 10.10.19.202: icmp_seq=6 ttl=128 time=1.24 ms  
64 bytes from 10.10.19.202: icmp_seq=7 ttl=128 time=1.35 ms  
64 bytes from 10.10.19.202: icmp_seq=8 ttl=128 time=1.32 ms  
^Z  
zsh: suspended  ping 10.10.19.202
```

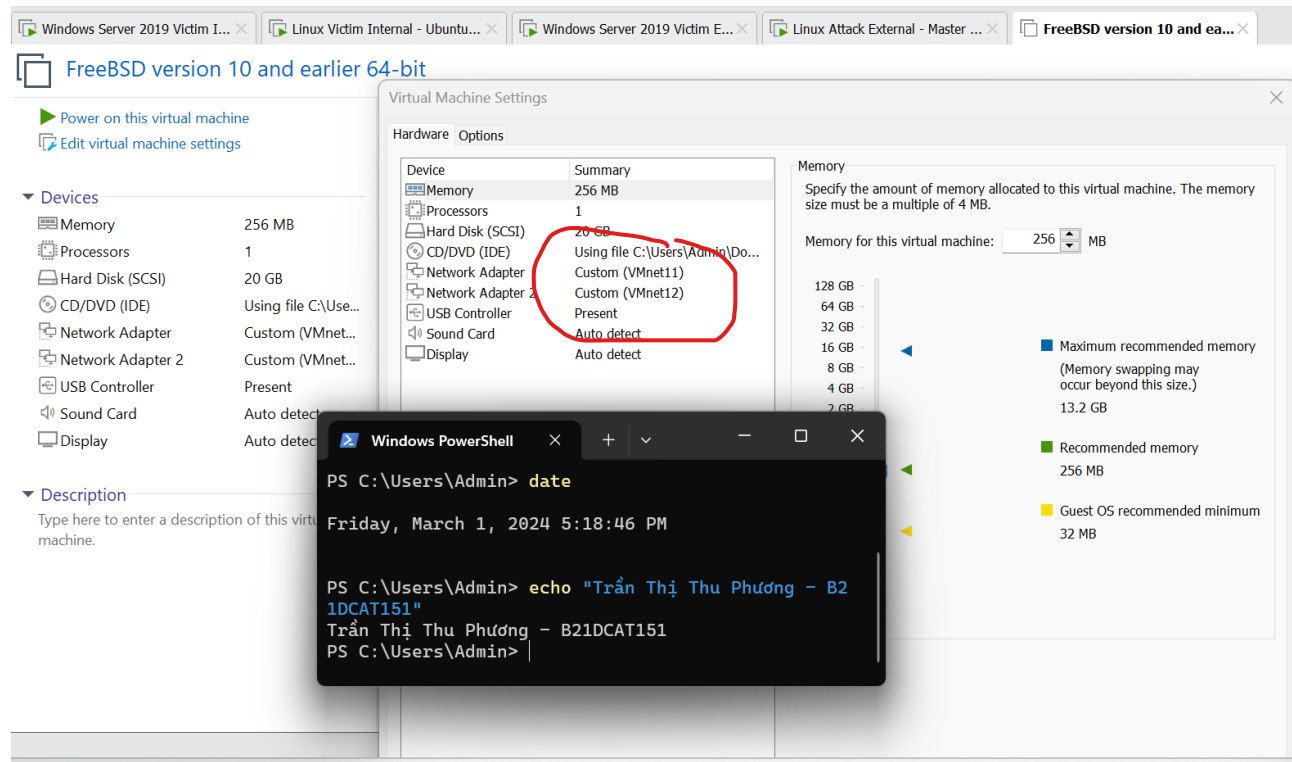
Kali Linux Attack → Windows Server

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

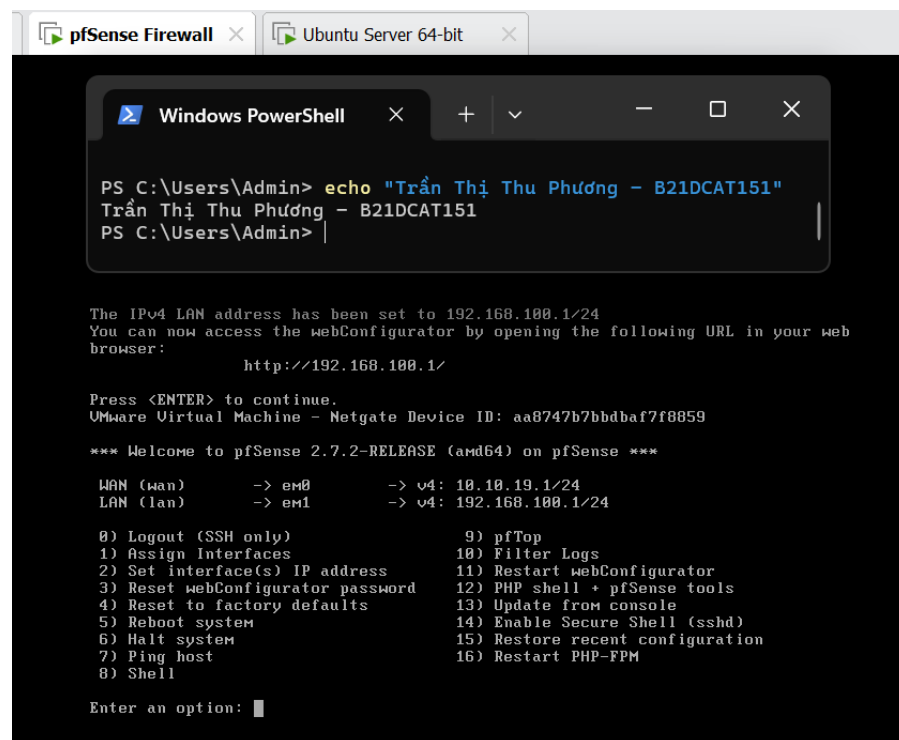
2.2.3. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

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

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với PfSense firewall

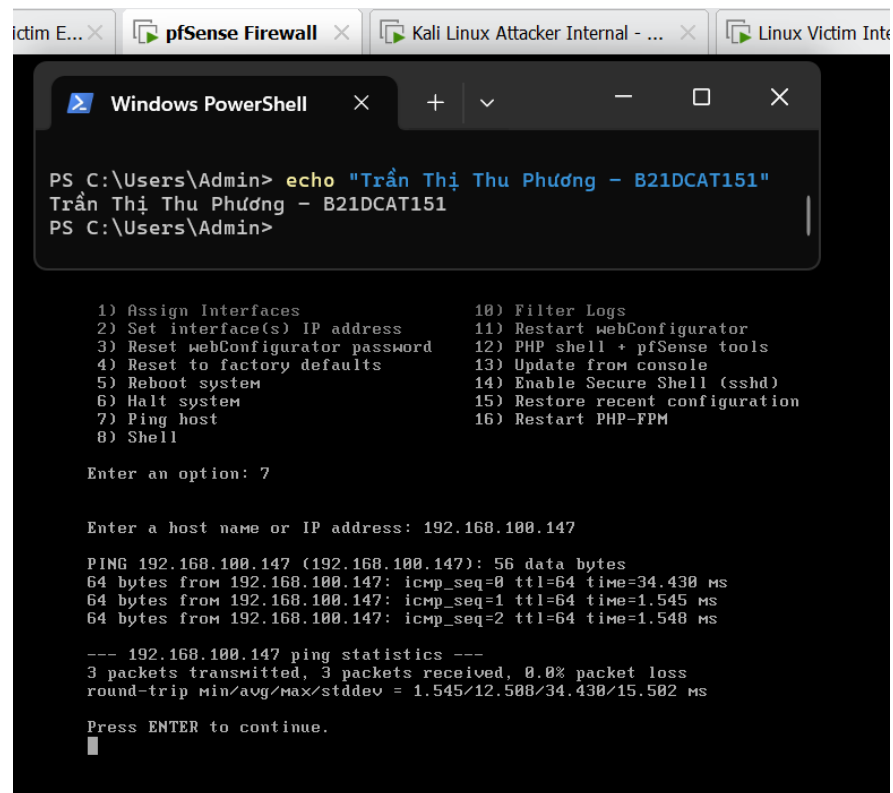


- Khởi động máy ảo, cài đặt cấu hình WAN interfaces và LAN interfaces. Chú ý, cả mạng WAN và mạng LAN đều không cần cài đặt IPv6 và DHCP. Ta được kết quả:



Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

- 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.



```
PS C:\Users\Admin> echo "Trần Thị Thu Phương - B21DCAT151"
Trần Thị Thu Phương - B21DCAT151
PS C:\Users\Admin>

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

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

Enter an option: 7

Enter a host name or IP address: 192.168.100.147

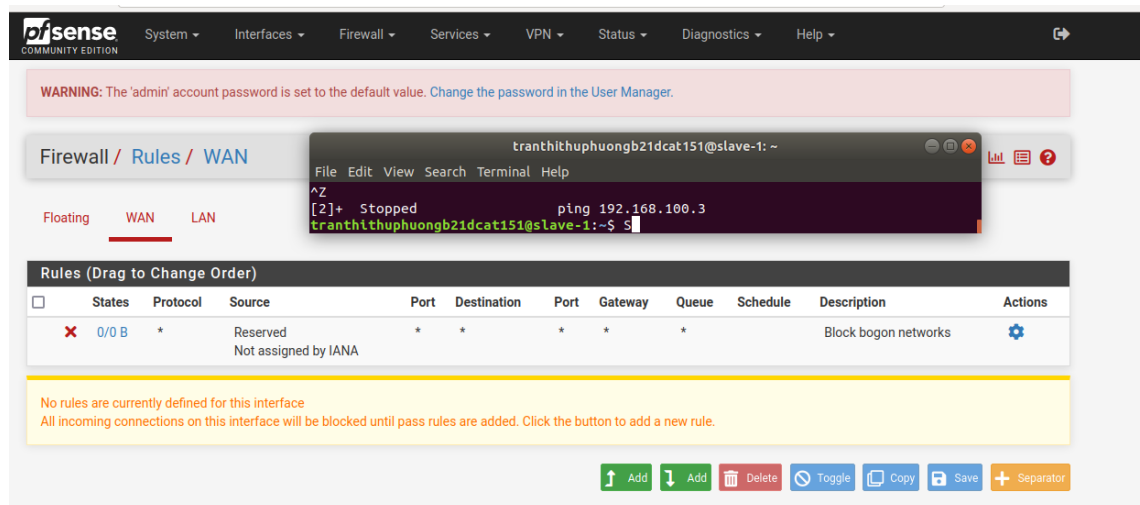
PING 192.168.100.147 (192.168.100.147): 56 data bytes
64 bytes from 192.168.100.147: icmp_seq=0 ttl=64 time=34.430 ms
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=1.545 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=1.548 ms

--- 192.168.100.147 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.545/12.508/34.430/15.502 ms

Press ENTER to continue.
```

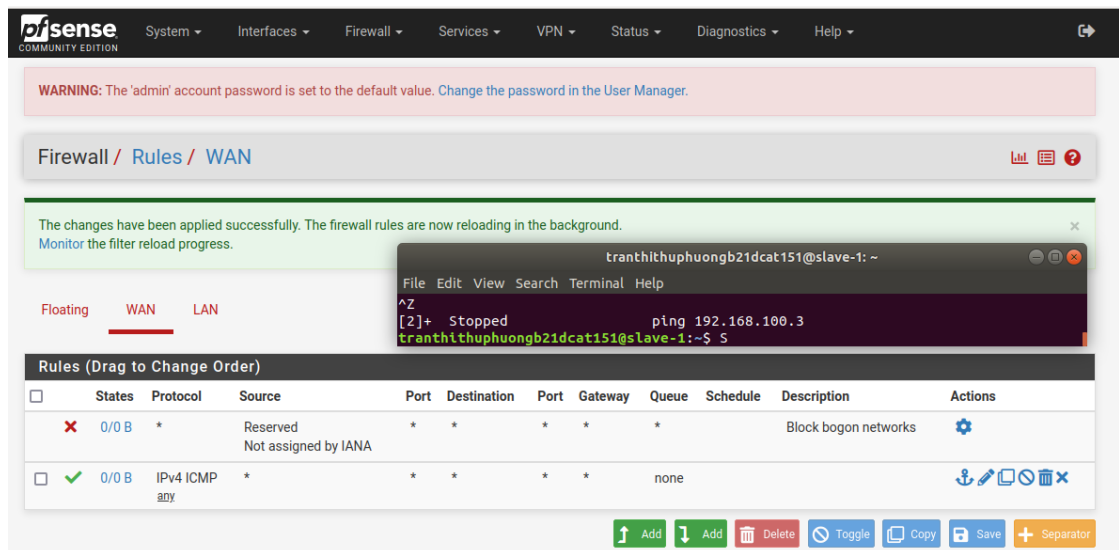
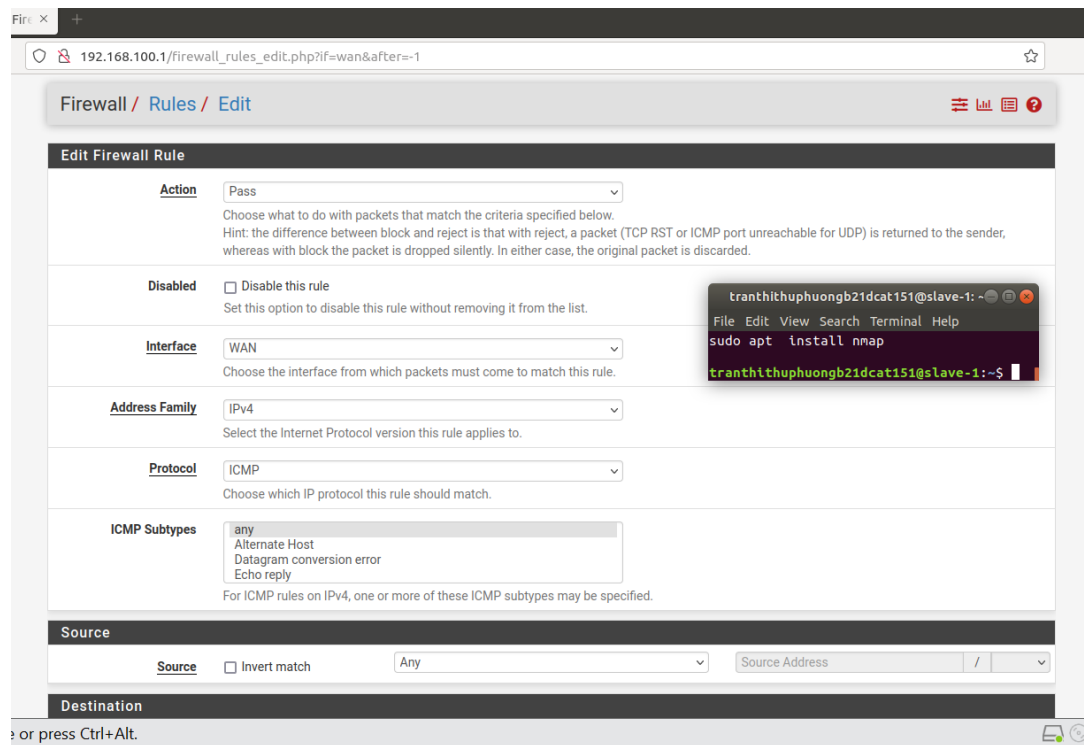
- Cấu hình Firewall trên Pfsense:

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.



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

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall



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


```
(tranphuong@tranthithuphuong151)-[~]
$ 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=1.34 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=1.47 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=1.36 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=1.29 ms
64 bytes from 10.10.19.1: icmp_seq=5 ttl=64 time=1.38 ms
64 bytes from 10.10.19.1: icmp_seq=6 ttl=64 time=1.79 ms
64 bytes from 10.10.19.1: icmp_seq=7 ttl=64 time=1.45 ms
^C
--- 10.10.19.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 1.294/1.441/1.794/0.154 ms

(tranphuong@tranthithuphuong151)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.166 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::20c:29ff:fe38:c8dc prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:38:c8:dc txqueuelen 1000 (Ethernet)
    RX packets 2695 bytes 3646340 (3.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 513 bytes 42725 (41.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.148 netmask 255.255.255.0 broadcast 10.10.19.255
    ether 00:0c:29:38:c8:e6 txqueuelen 1000 (Ethernet)
    RX packets 535 bytes 45774 (44.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 407 bytes 36390 (35.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

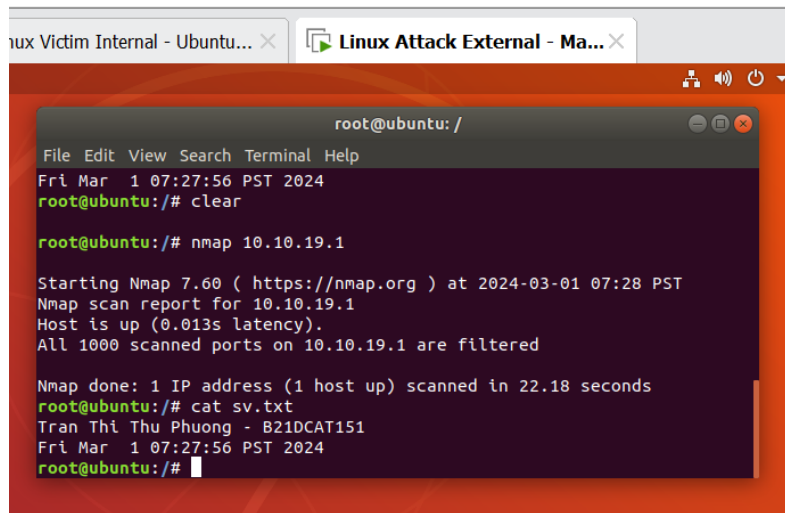
- Trả lời các câu hỏi:
 - + Theo mặc định, có 2 cổng TCP mở trên giao diện mạng Internal của Pfsense. Xem và kiểm tra: `nmap 192.168.100.1`

```
(tranphuong@tranthithuphuong151)-[~]
$ nmap 192.168.100.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-01 08:50 EST
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

(tranphuong@tranthithuphuong151)-[~]
$ ping 10.10.19.1
```

- + 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`



```
root@ubuntu: /
File Edit View Search Terminal Help
Fri Mar 1 07:27:56 PST 2024
root@ubuntu: /# clear

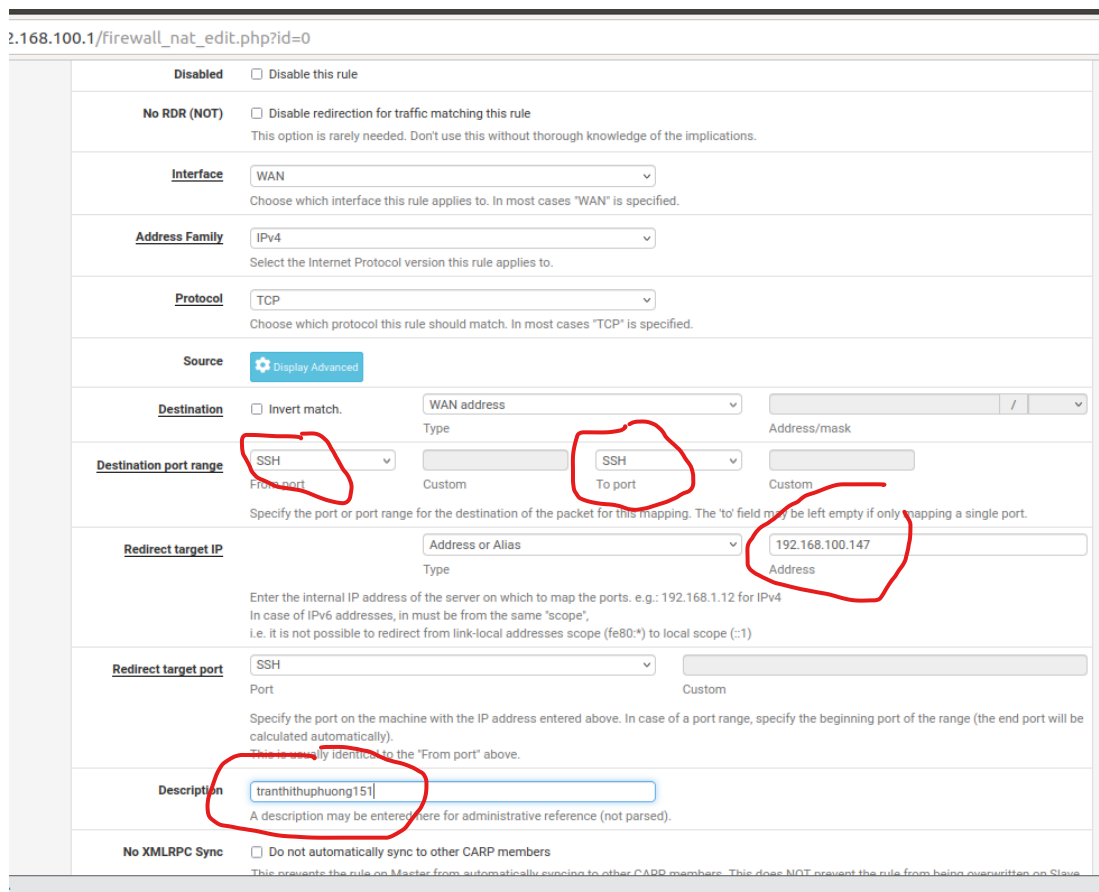
root@ubuntu: /# nmap 10.10.19.1

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-01 07:28 PST
Nmap scan report for 10.10.19.1
Host is up (0.013s latency).
All 1000 scanned ports on 10.10.19.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 22.18 seconds
root@ubuntu: /# cat sv.txt
Tran Thi Thu Phuong - B21DCAT151
Fri Mar 1 07:27:56 PST 2024
root@ubuntu: /#
```

2.2.4. 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



2.168.100.1/firewall_nat_edit.php?id=0

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match. WAN address Type Address/mask

Destination port range SSH From port SSH To port
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Address or Alias Type 192.168.100.147 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 SSH Port
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 tranthithuphuong151
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.

Bài 5 – Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

192.168.100.1/firewall_nat_edit.php?id=0

80%

Destination ☐ Invert match. WAN address /

Type Address/mask

Destination port range SSH From port Custom To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Address or Alias 192.168.100.147

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 SSH 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 tranthithuphuong151

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 or Masquerade from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Create new associated filter rule

Rule Information

Created	3/2/24 01:08:02 by admin@192.168.100.147 (Local Database)
Updated	3/2/24 03:29:31 by admin@192.168.100.147 (Local Database)

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

```
File Edit View Search Terminal Help
tranthithuphuongb21dcat151@slave-1:~$ sudo gedit /etc/ssh/sshd_config
[sudo] password for tranthithuphuong:
** (gedit:5574): WARNING **: 17:17:00: attribute metadata::gedit-position
tranthithuphuongb21dcat151@slave-1:~$
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
# HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
# RekeyLimit default none

# Logging
# SyslogFacility AUTH
# LogLevel INFO

# Authentication:
# LoginGraceTime 120
PermitRootLogin yes
PermitRootLogin prohibit-password
# StrictModes yes
# MaxAuthTries 6
# MaxSessions 10
# RSAAuthentication yes
# PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in
```

Chỉnh sửa file cấu hình: `sudo gedit /etc/ssh/sshd_config`

```
tranthithuphuongb21dcat151@slave-1:~$ sudo -s
root@slave-1:~# systemctl enable ssh.service
Synchronizing state of ssh.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@slave-1:~# service ssh status.
 * Usage: /etc/init.d/ssh {start|stop|reload|force-reload|restart|try-rest
art|status}
root@slave-1:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset
   Active: active (running) since Fri 2024-03-01 11:41:48 PST; 16min ago
   Main PID: 1211 (sshd)
     Tasks: 1 (limit: 4620)
    CGroup: /system.slice/ssh.service
            └─1211 /usr/sbin/sshd -D

Mar 01 11:41:48 slave-1 systemd[1]: Starting OpenBSD Secure Shell server..
Mar 01 11:41:48 slave-1 sshd[1211]: Server listening on 0.0.0.0 port 22.
Mar 01 11:41:48 slave-1 sshd[1211]: Server listening on :: port 22.
Mar 01 11:41:48 slave-1 systemd[1]: Started OpenBSD Secure Shell server.
Mar 01 11:46:40 slave-1 systemd[1]: Reloading OpenBSD Secure Shell server.
Mar 01 11:46:40 slave-1 sshd[1211]: Received SIGHUP; restarting.
Mar 01 11:46:40 slave-1 systemd[1]: Reloaded OpenBSD Secure Shell server.
Mar 01 11:46:40 slave-1 sshd[1211]: Server listening on 0.0.0.0 port 22.
Mar 01 11:46:40 slave-1 sshd[1211]: Server listening on :: port 22.
lines 1-17/17 (END)
```

SSH ở máy Linux Victim Internal đã được bật

- Máy Kali Linux Attacker External đã có thể SSH đến máy Linux Victim Internal

```
(tranhithuphuongb21dcat151)-[~]
$ ssh root@10.10.19.1
root@10.10.19.1's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

5 Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

152 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sun Mar  3 10:40:18 2024 from 10.10.19.148
root@slave-1:~# 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
    ether 00:0c:29:67:7c:cb txqueuelen 1000 (Ethernet)
    RX packets 1054 bytes 236715 (236.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7327 bytes 1194736 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 102.168.17.171 netmask 255.255.255.0 broadcast 102.168.17.255
```

SSH thành công từ máy Kali Linux Attack External đến máy Linux Victim Internal

3. 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

4. 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+®