

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI THỰC HÀNH

THỰC TẬP CƠ SỞ

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

Họ và tên: Nguyễn Huy Quang

Mã sinh viên: B20DCAT144

Giảng Viên: Nguyễn Hoa Cương

Hà Nội – 2023

I. Lý thuyết :

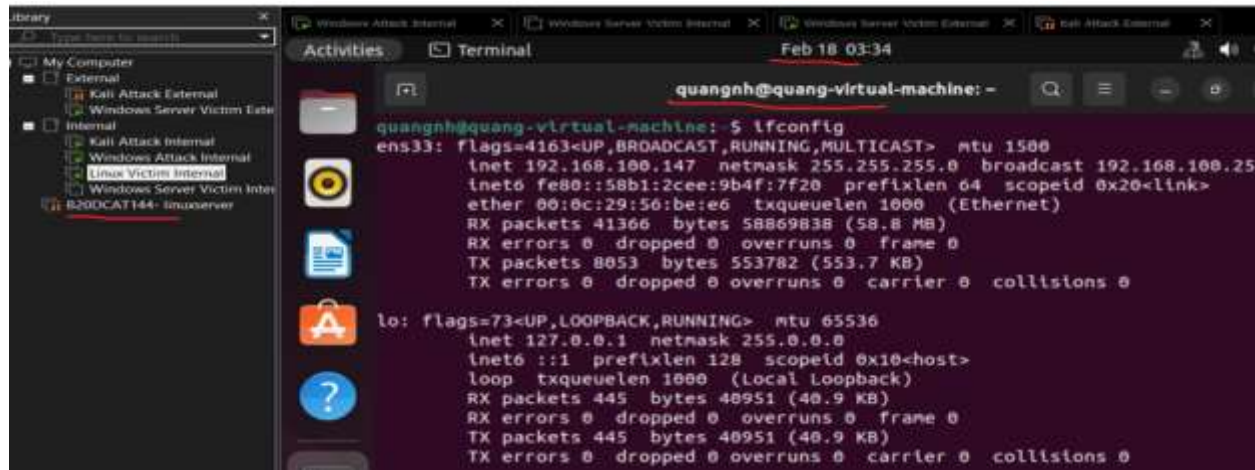
- Cấu hình mạng trong phần mềm mô phỏng Vmware
 - + VMware là một phần mềm ảo hóa dùng cho desktop mạnh và phổ biến, đi kèm nhiều tính năng cho phép tạo và quản lý mạng riêng tư.
 - + Các loại card mạng:
 - Bridge: card này sử dụng chính card mạng thật để kết nối ra ngoài Internet (card ethernet hoặc wireless). Do đó khi sử dụng card mạng này IP của máy ảo sẽ cùng với dải IP của máy thật.
 - Nat: sử dụng cách Nat địa chỉ IP của máy thật ra một địa chỉ khác cho máy ảo sử dụng. Card này cũng có thể kết nối ra bên ngoài Internet.
 - Host-only: hoàn toàn tách biệt với mạng thật. Card Hostonly chỉ có thể giao tiếp với máy ảo và các card Host-only trên các máy ảo khác.
- Pfsense
 - + Là phần mềm định tuyến/tường lửa mã nguồn mở miễn phí dành cho máy tính dựa trên hệ điều hành FreeBSD.
 - + Gồm tính năng gom nhóm các ports, host hoặc network khác nhau, tạo các rules để quản lý mạng bên trong Firewall.
 - + Có thể cấu hình sử dụng cho DHCP server, DNS server, WiFi access point và VPN server, cho phép cài đặt các gói mã nguồn mở của bên thứ ba như Snort,...

II. Thực hành:

2.1 Cấu hình topo mạng

- a) Cài đặt và cấu hình hệ thống theo topo mạng

+ Kiểm tra lại IP- Trong mạng Internal + Cài đặt IP tĩnh cho máy Linux Victim

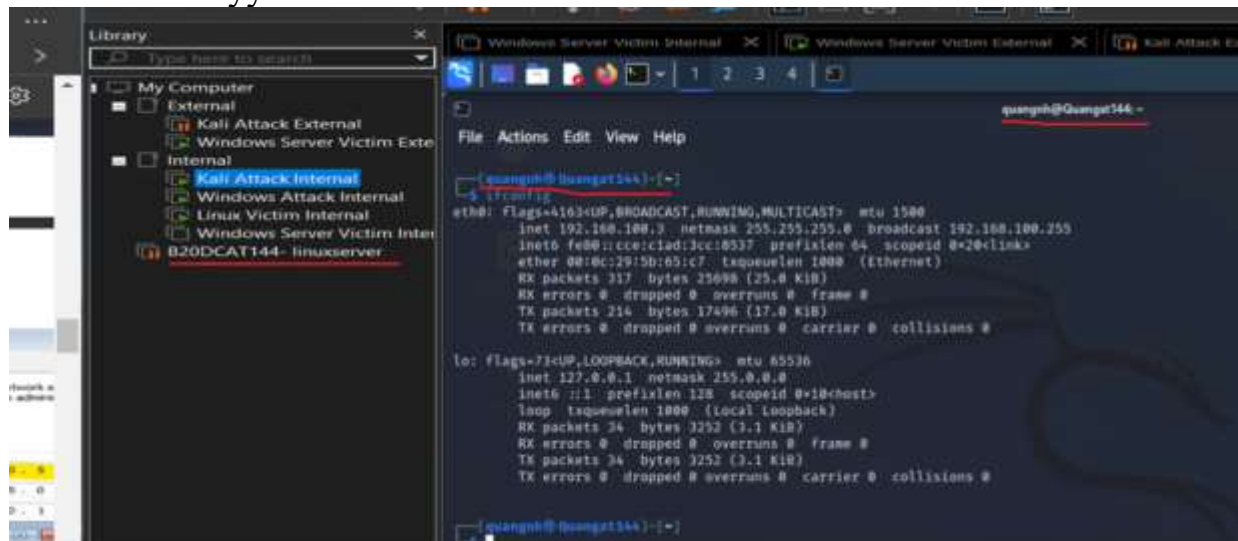


```
quangnh@quang-virtual-machine: ~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.147 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::58b1:2cee:9b4f:7f20 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:56:be:e6 txqueuelen 1000 (Ethernet)
    RX packets 41366 bytes 58869838 (58.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8053 bytes 553782 (553.7 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 445 bytes 40951 (40.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 445 bytes 40951 (40.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

+ Cài đặt IP tĩnh cho máy Kali Attack Internal

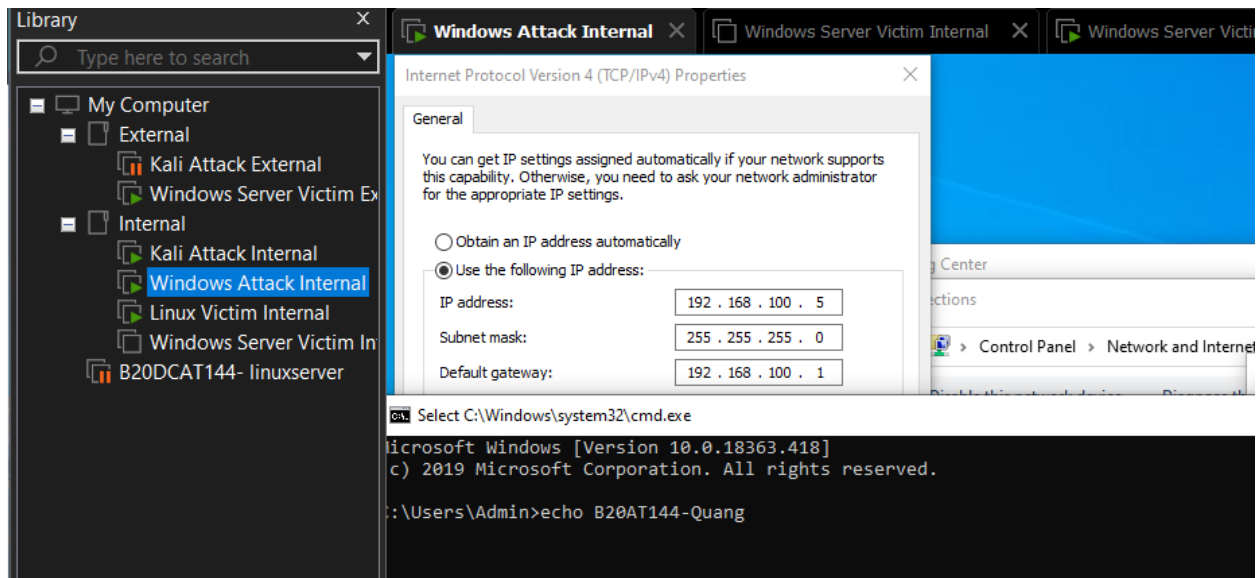
+ Kiểm tra địa chỉ IP+ Cài đặt IP tĩnh cho máy Windows Attack Internal+ Cài đặt IP tĩnh cho máy Windows Attack Internal



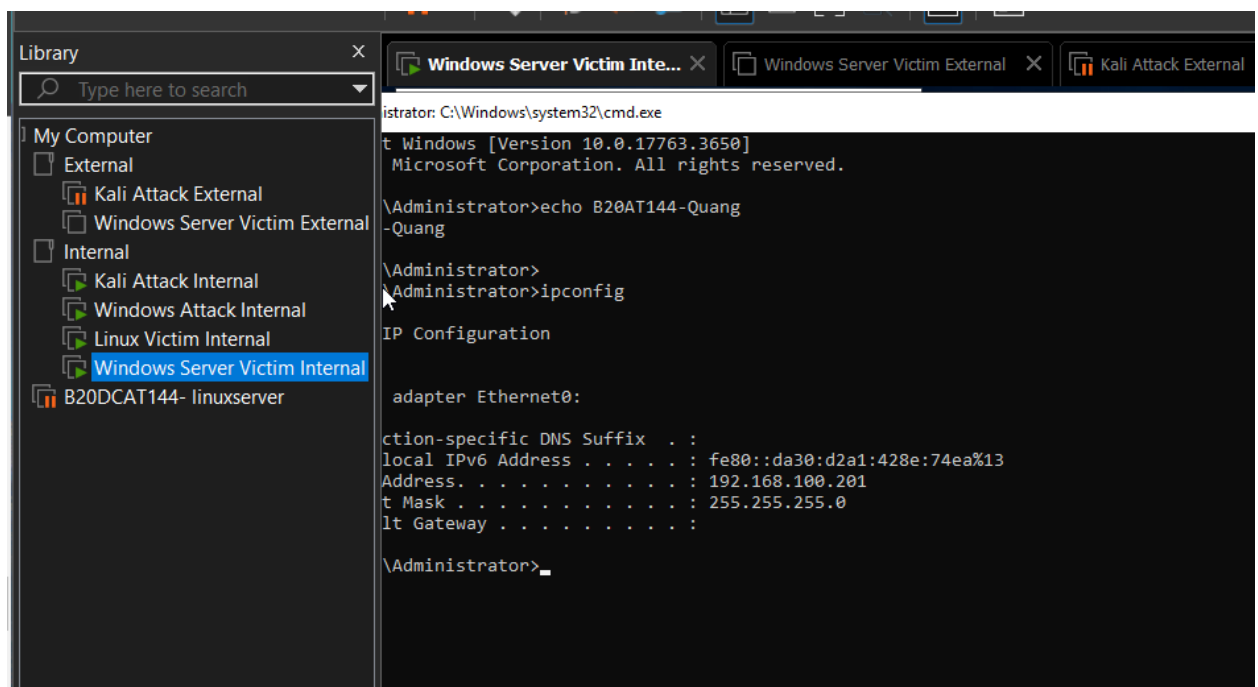
```
quangnh@Quang144: ~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::cde:cdad:3cc:8537 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:5b:a5:c7 txqueuelen 1000 (Ethernet)
    RX packets 317 bytes 23698 (23.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 216 bytes 17496 (17.0 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 34 bytes 3252 (3.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 3252 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

+ Cài đặt IP tĩnh cho máy Windows Attack Internal

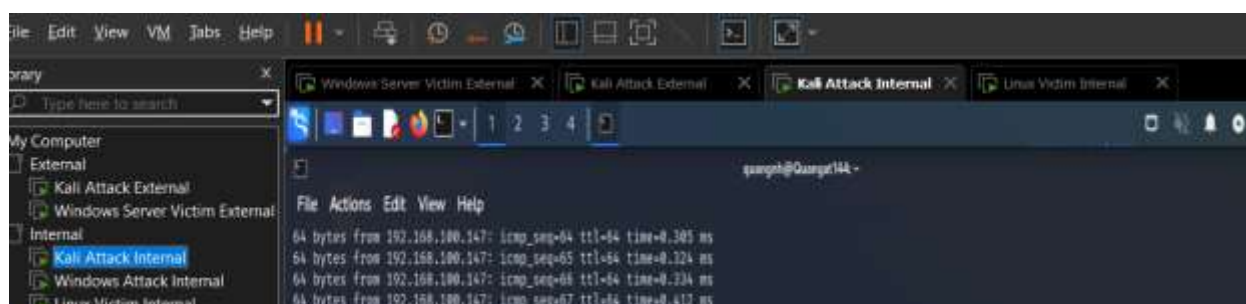
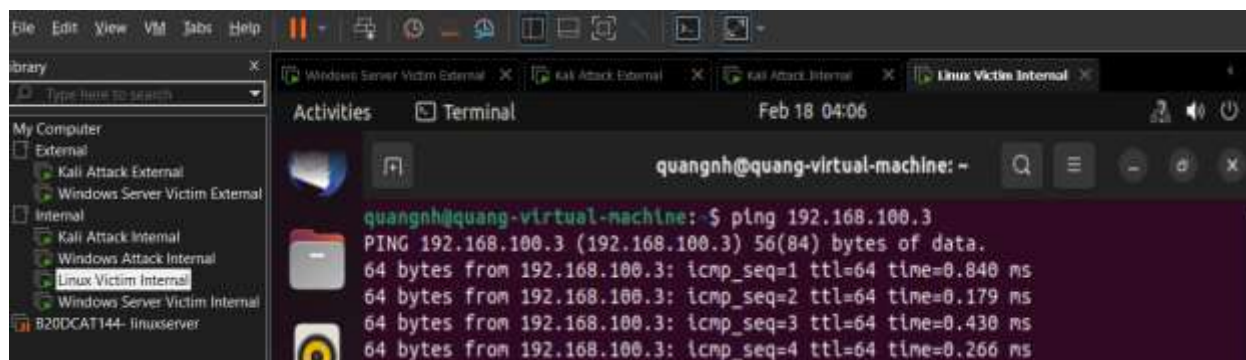


+ Kiểm tra địa chỉ IP

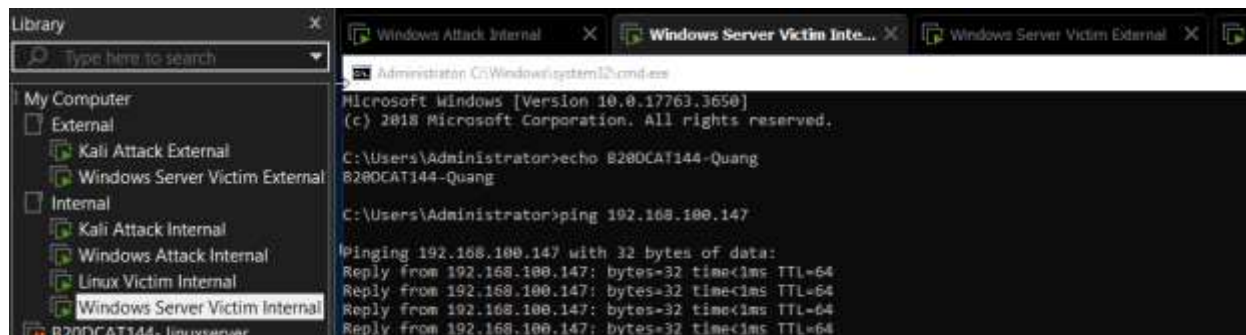
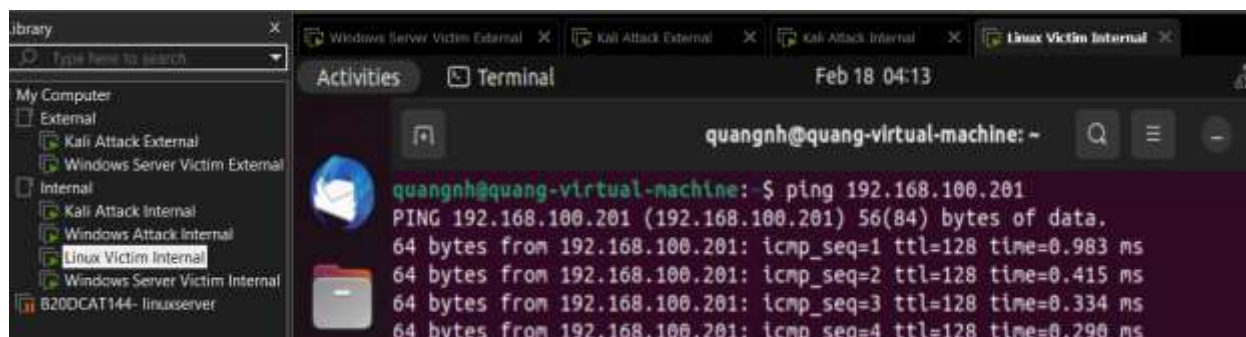


+ Kiểm tra các mạng trong Internal đã thông với nhau

- Linux Victim Internal với Kali Attack Internal



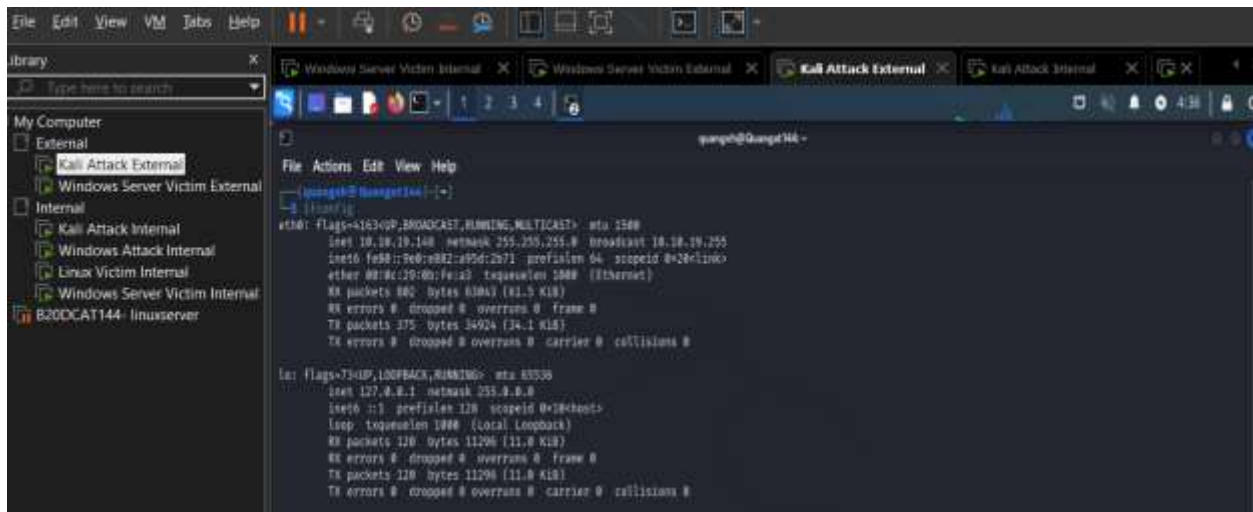
- Linux Victim Internal với Windows Server Victim Internal



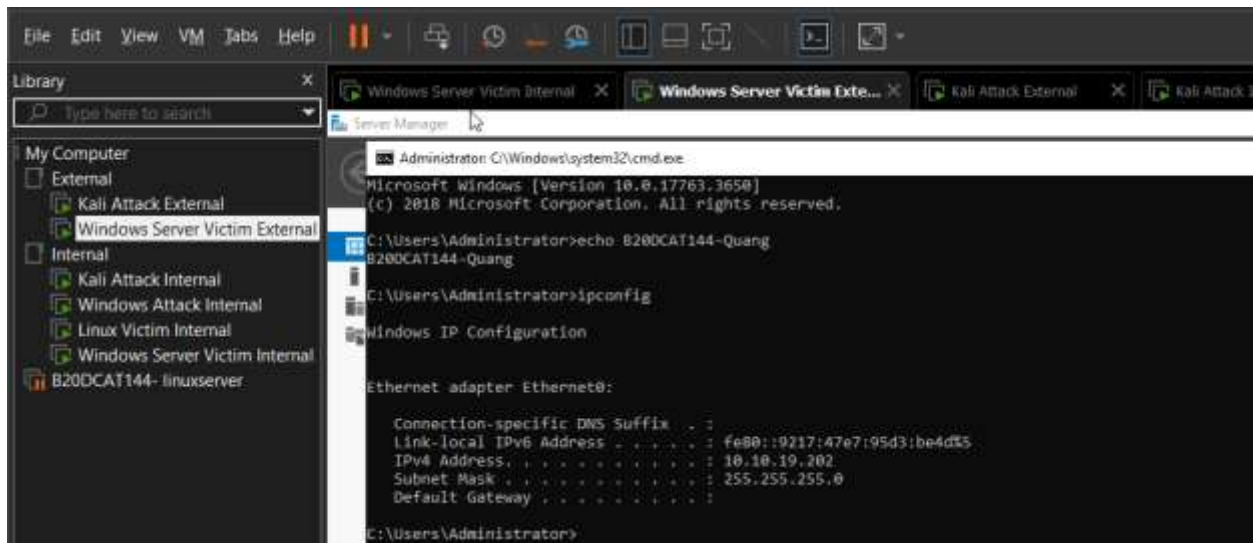
- Trong mạng External

+ Cài đặt IP tĩnh cho máy Kali Attack External tương tự như trong phần Internal

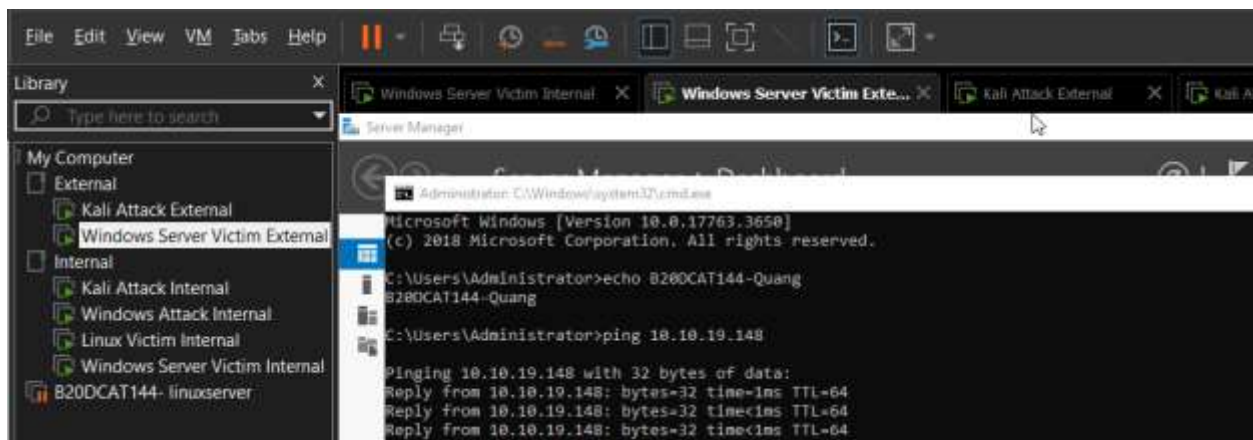
+ Kiểm tra địa chỉ IP

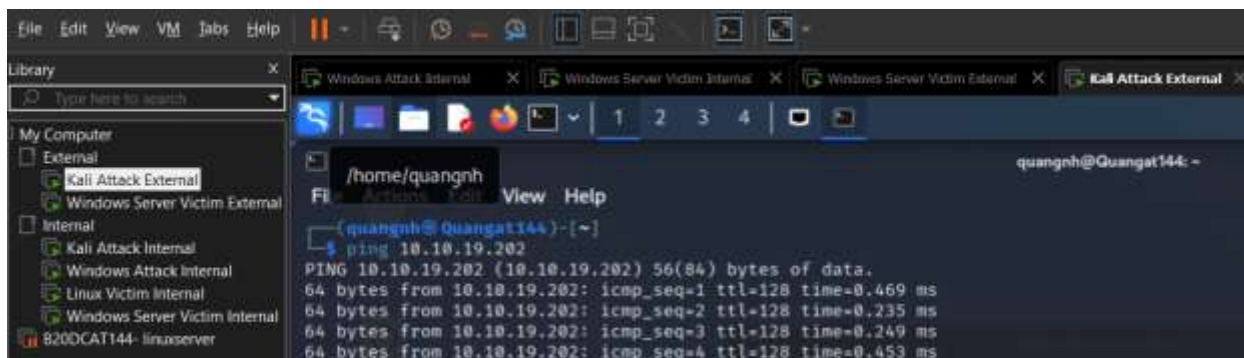


+ Cài đặt IP tĩnh cho máy Windows Server Victim External tương tự như trong phần Internal



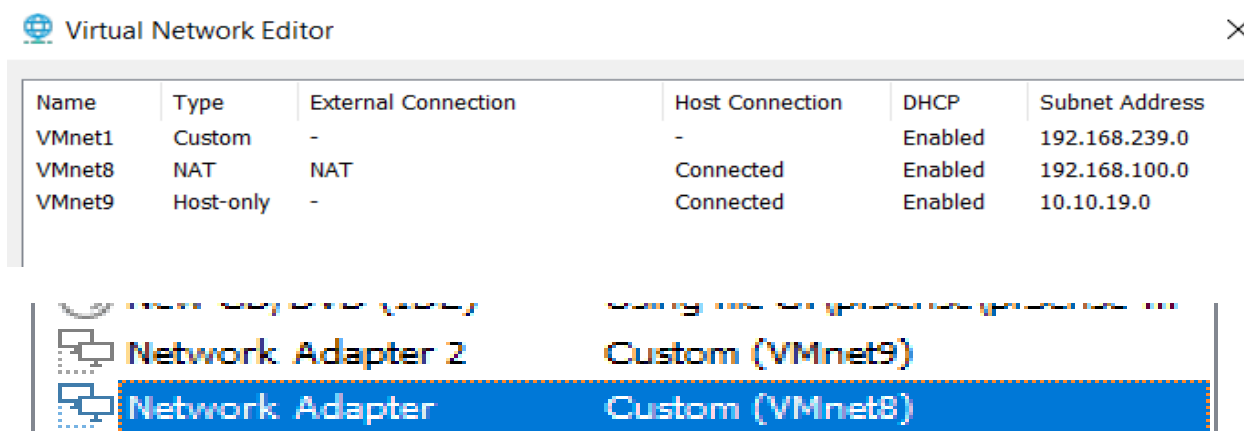
+ Kiểm tra các mạng trong External đã thông với nhau



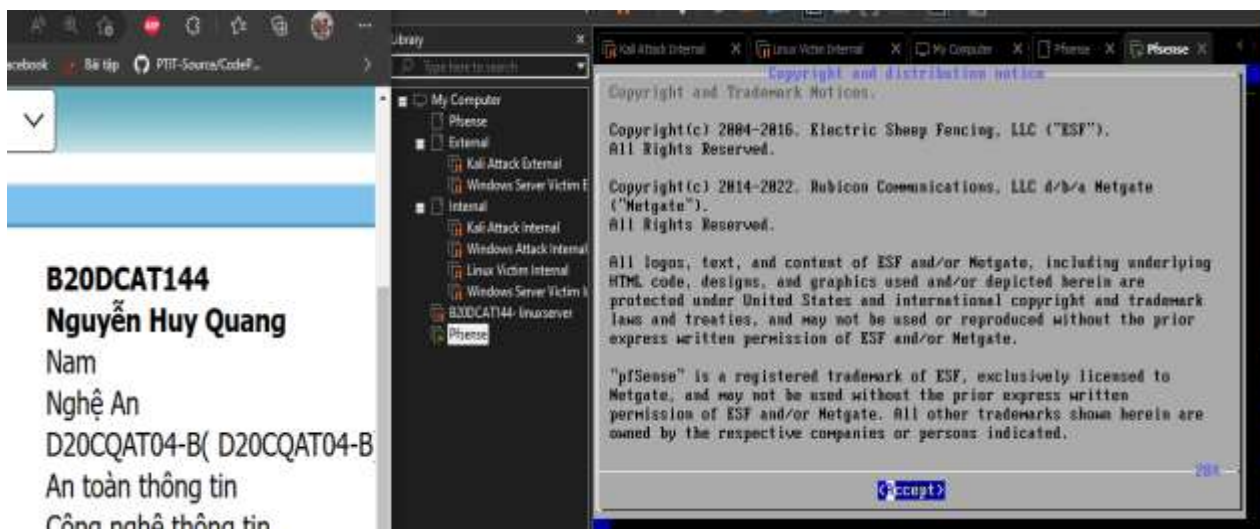


- Cài đặt Pfsense.

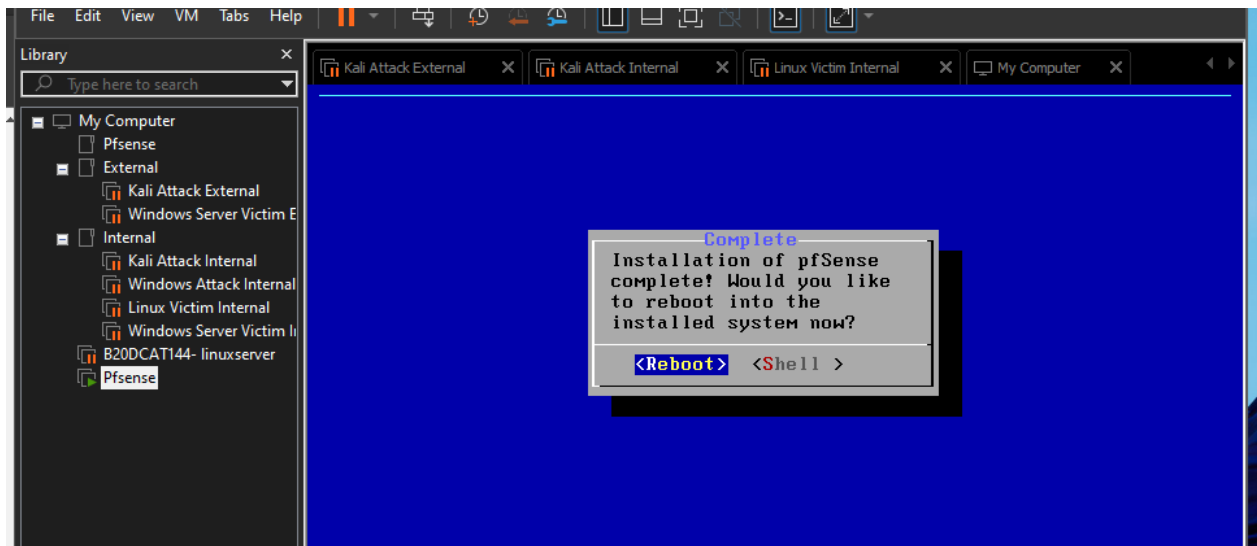
+ Trong Vmware, tạo thêm một Network Adapter



+ Màn hình cài đặt Pfsense



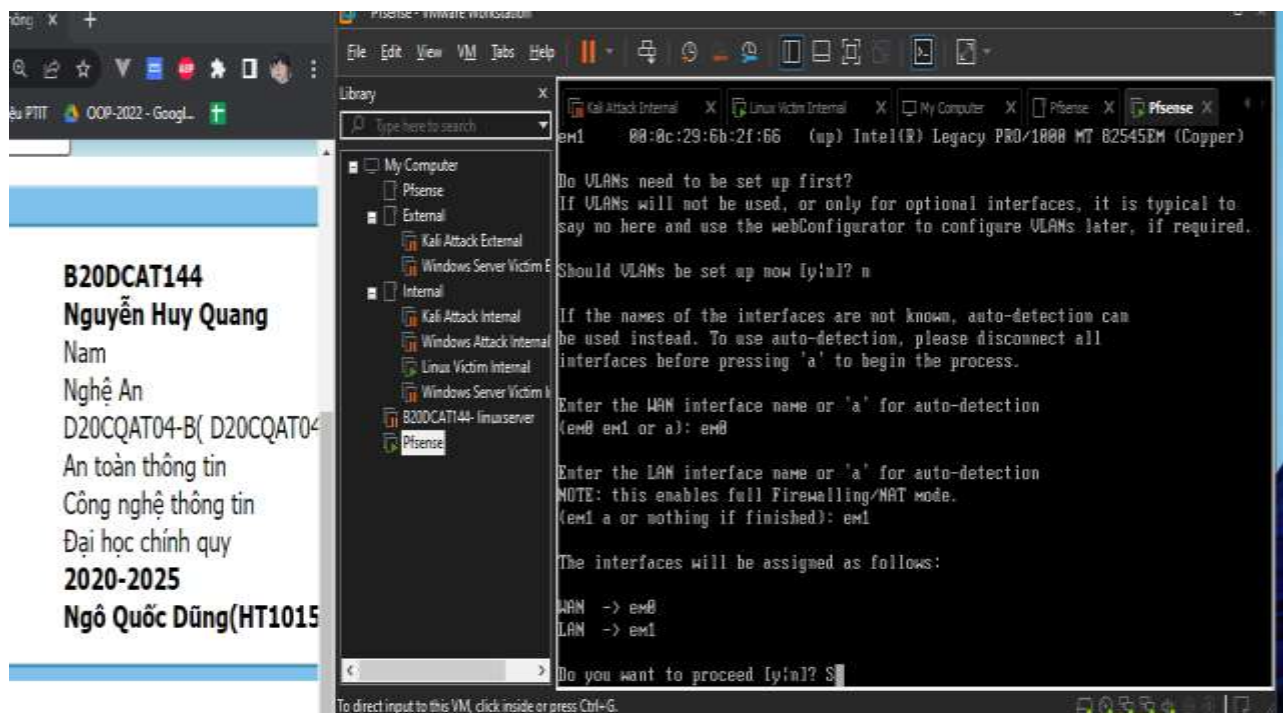
+ Sau khi cài đặt xong, khởi động lại Pfsense



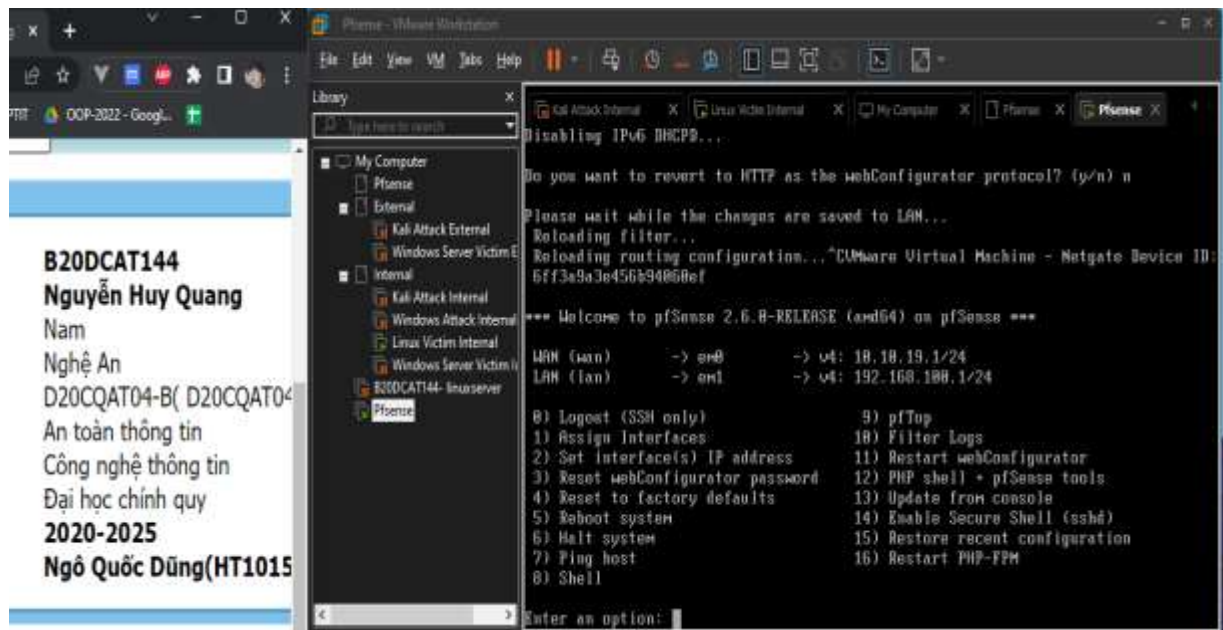
2.2 Cài đặt cấu hình pfSense firewall cho lưu lượng ICMP.

Cấu hình tường lửa cho phép 1 cổng và chuyển hướng lưu lượng

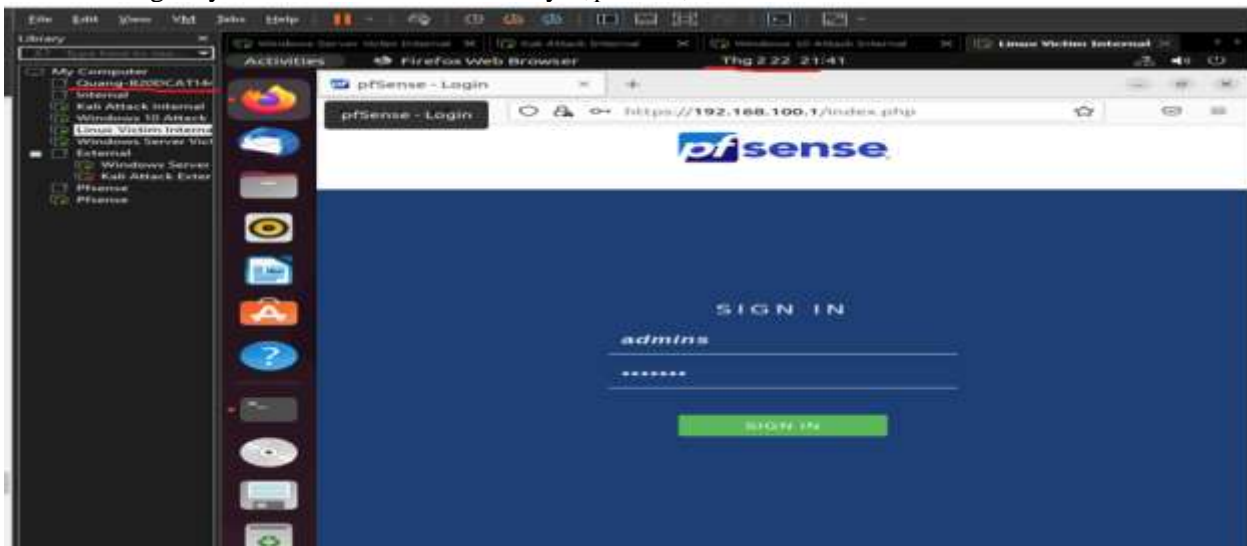
- Gán em0 cho LAN và em1 cho Wan



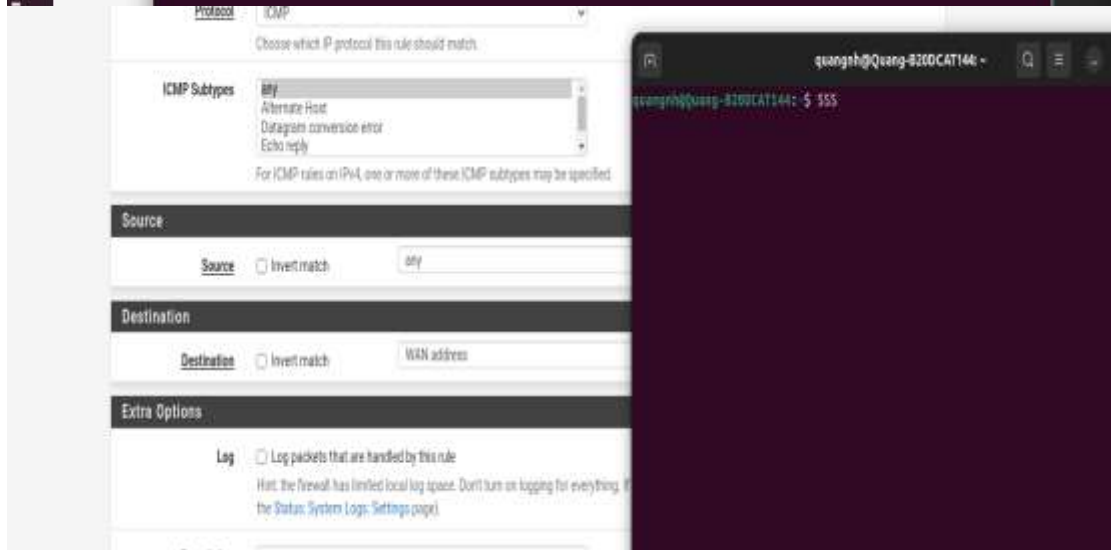
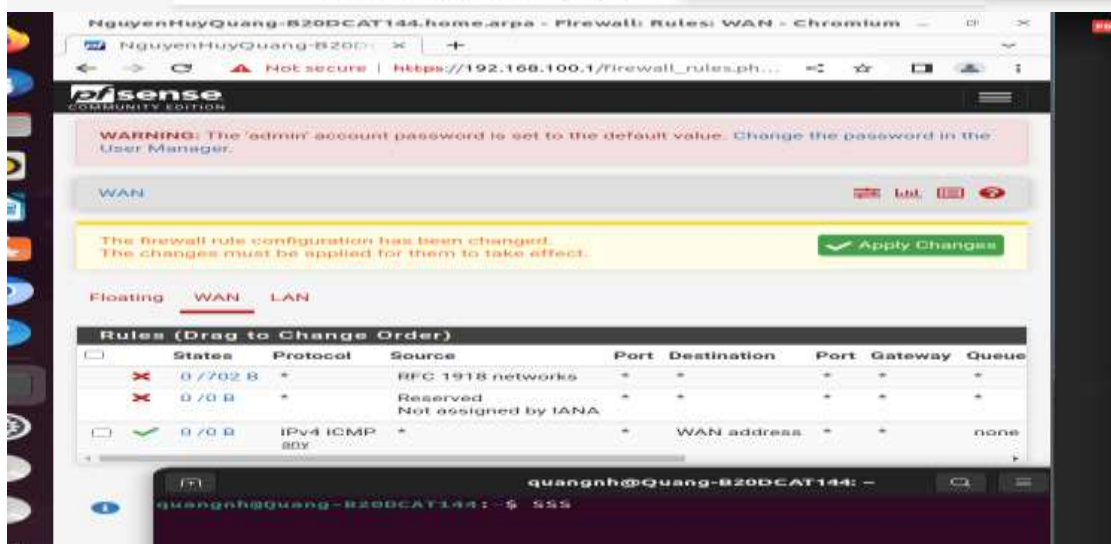
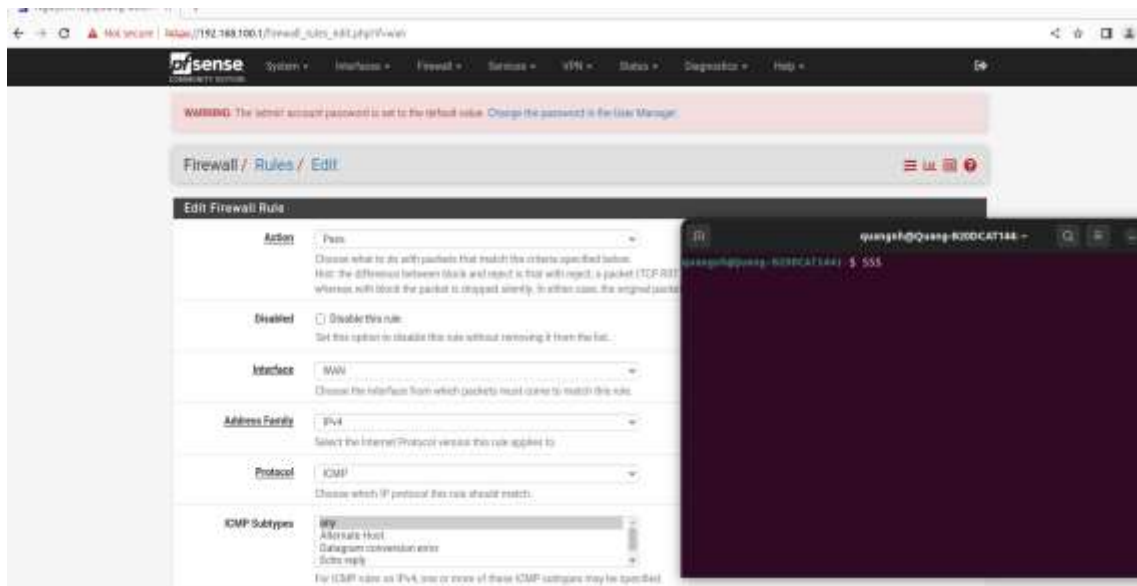
- Sau khi đặt địa chỉ IP ta sẽ được hình bên dưới

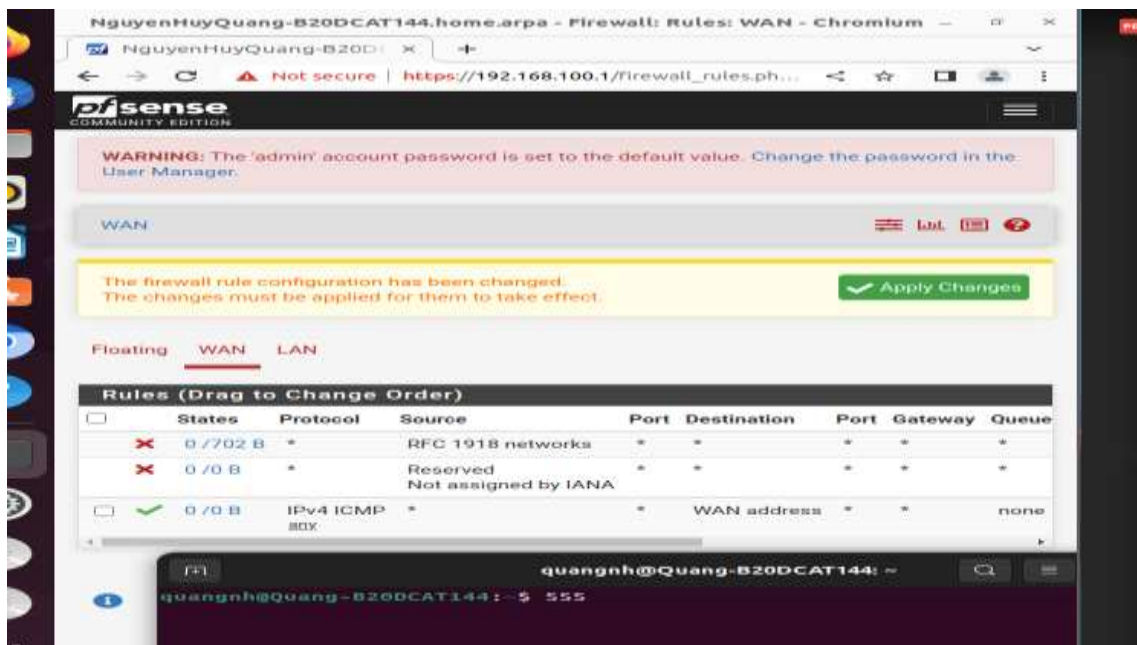


- Dùng máy Ubuntu Victim Internal truy cập vào địa chỉ 192.16



- Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1
- Cài đặt phương thức ICMP





- Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali Attack External

```
File Actions Edit View Help
(quangnh@Quang-B20DCAT144)-[~]
$ 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=0.281 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.356 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.353 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=0.332 ms
64 bytes from 10.10.19.1: icmp_seq=5 ttl=64 time=0.404 ms
64 bytes from 10.10.19.1: icmp_seq=6 ttl=64 time=0.329 ms
64 bytes from 10.10.19.1: icmp_seq=7 ttl=64 time=0.364 ms
64 bytes from 10.10.19.1: icmp_seq=8 ttl=64 time=0.430 ms
64 bytes from 10.10.19.1: icmp_seq=9 ttl=64 time=0.318 ms
^C
--- 10.10.19.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8197ms
rtt min/avg/max/mdev = 0.281/0.351/0.430/0.042 ms
(quangnh@Quang-B20DCAT144)-[~]
$ 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=0.219 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.251 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.273 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=0.268 ms
^C
--- 10.10.19.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.219/0.252/0.273/0.021 ms
(quangnh@Quang-B20DCAT144)-[~]
$
```

- Trả lời câu hỏi
 - Theo mặc định, có 4 cổng TCP mở trên giao diện mạng Internal của pfSense: Cổng 80 (HTTP), cổng 53(DOMAIN), cổng 22 (ssh) và cổng 443(HTTPS)

```
(quangnh@Quang-B20DCAT144-Kali)-[~]
$ nmap -Pn 192.168.100.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 06:13 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00049s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 17.94 seconds
(quangnh@Quang-B20DCAT144-Kali)-[~]
$ date
Sat Apr  8 06:13:37 AM EDT 2023
(quangnh@Quang-B20DCAT144-Kali)-[~]
$
```

- Theo mặc định, không có cổng TCP mở trên giao diện mạng External của pfSense:

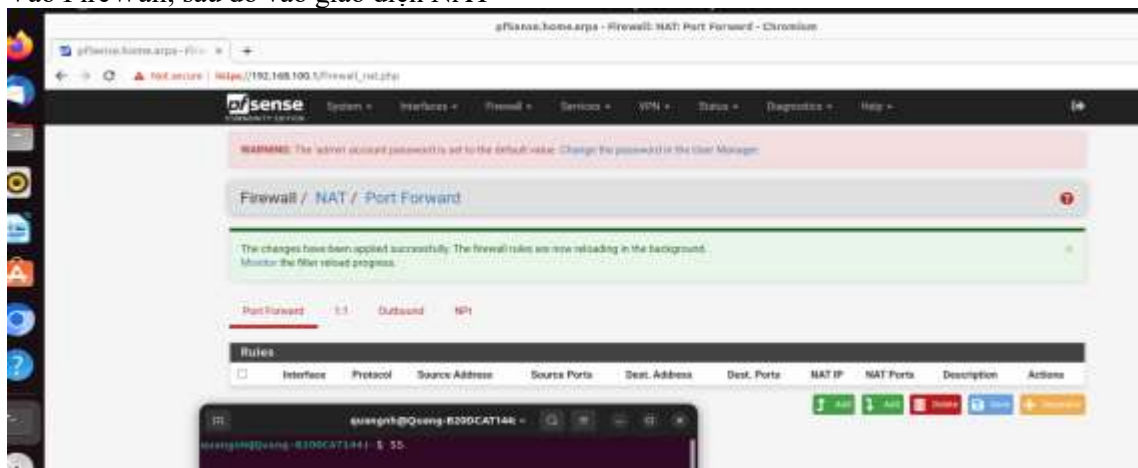
```
quangnh@Quang-B20DCAT144: $ nmap -Pn 10.10.19.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 17:06 +07
Nmap scan report for 10.10.19.1
Host is up.
All 1000 scanned ports on 10.10.19.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 215.23 seconds
quangnh@Quang-B20DCAT144: $ date
Thứ bảy, 08 Tháng 4 năm 2023 17:11:16 +07
quangnh@Quang-B20DCAT144: $
```

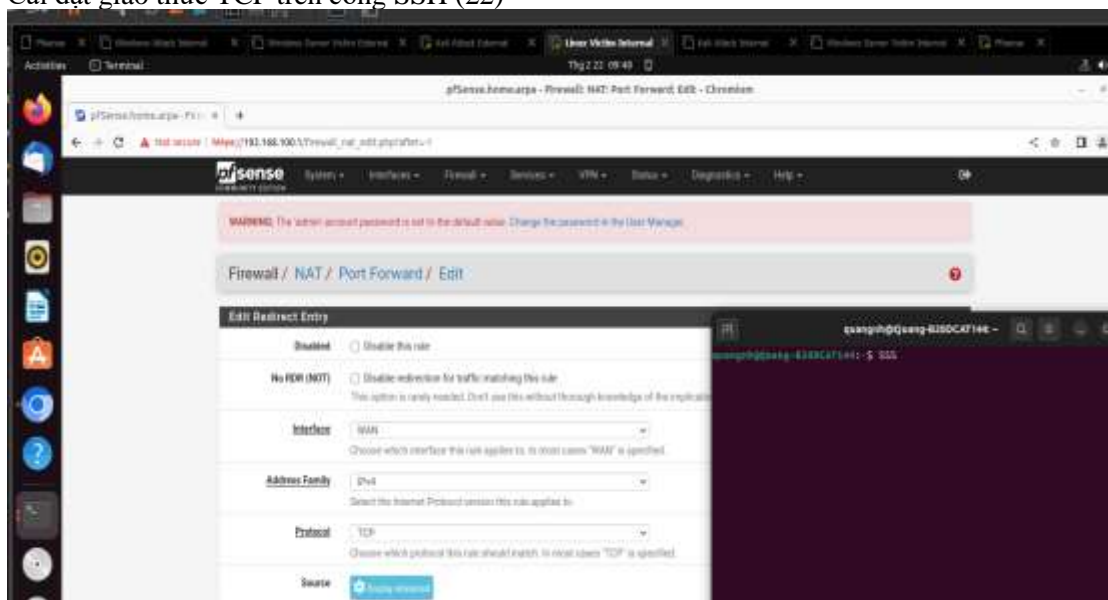
2.3 Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal.

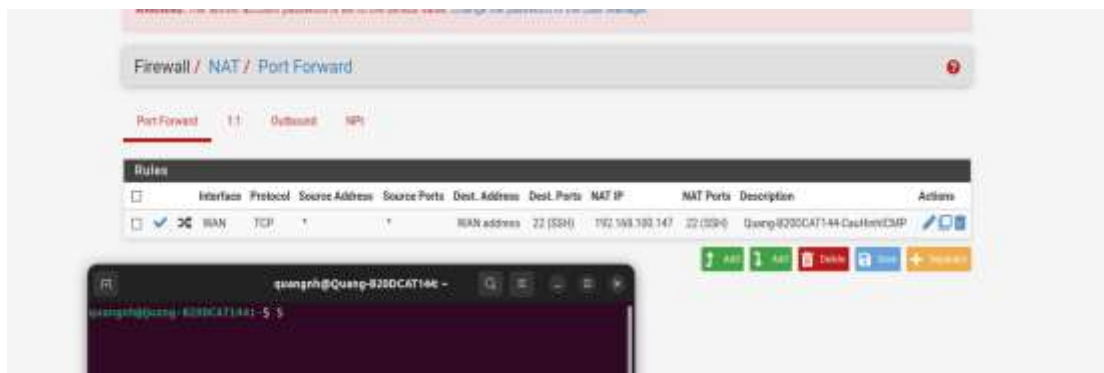
Cấu hình trường lựa cho phép 1 cổng và chuyển hướng lưu lượng

- Trên máy Ubuntu Victim Internal, vào 192.168.100.1 để cấu hình NAT trên pfsense qua giao diện web
- Vào FireWall, sau đó vào giao diện NAT



- Cài đặt giao thức TCP trên cổng SSH (22)





- ```

File Actions Edit View Help
[quangnh@Quang-B20DCAT144:~]$ sudo su
[sudo] password for quangnh:
The authenticity of host '10.10.19.1 (10.10.19.1)' can't be established.
ED25519 key fingerprint is SHA256:OVwUcgcGJeeD/tznVHhIscwB2Qpzb4vJMSr/4sRmuE4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.19.1' (ED25519) to the list of known hosts.
quangnh@10.10.19.1's password:
Permission denied, please try again.
quangnh@10.10.19.1's password:
Permission denied, please try again.
quangnh@10.10.19.1's password:
quangnh@10.10.19.1: Permission denied (publickey,password).

[quangnh@Quang-B20DCAT144:~]$ sudo su
[sudo] password for quangnh:
[sudo] unable to resolve host Quang-B20DCAT144: Temporary failure in name resolution
quangnh@10.10.19.1's password:

[quangnh@Quang-B20DCAT144:~]$ su 10.10.19.1
The authenticity of host '10.10.19.1 (10.10.19.1)' can't be established.
ED25519 key fingerprint is SHA256:OVwUcgcGJeeD/tznVHhIscwB2Qpzb4vJMSr/4sRmuE4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.19.1' (ED25519) to the list of known hosts.
quangnh@10.10.19.1's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.10.0-22-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

quangnh@Quang-B20DCAT144:~$

```



- Kiểm tra IP máy

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
quangnh@Quang-B20DCAT144:~$ 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::7b65:7d82:4ed2:36 prefixlen 64 scopeid 0x20<link>
 ether 00:0c:29:aa:c9:c5 txqueuelen 1000 (Ethernet)
 RX packets 17464 bytes 3330174 (3.3 MB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 15704 bytes 1237339 (1.2 MB)
 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 19461 bytes 1411562 (1.4 MB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 19461 bytes 1411562 (1.4 MB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

quangnh@Quang-B20DCAT144:~$
```

```
quangnh@Quang-B20DCAT144:~$ nmap 192.168.100.1
Starting Nmap 7.80 (https://nmap.org) at 2023-02-22 20:11 +07
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.00074s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
quangnh@Quang-B20DCAT144:~$
::1 ff02::2 ip6-localnet Quang-B20DCAT144
fe00::0 ip6-allnodes ip6-loopback
ff00::0 ip6-allrouters ip6-mcastprefix
ff02::1 ip6-localhost localhost
```