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 FIREWALL

Sinh viên thực hiện:

B22DCAT018 – Nguyễn Hoàng Anh

Giảng viên hướng dẫn: ThS. Ninh Thị Thu Trang

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC BẢNG

CHƯƠNG 1. TÌM HIỂU LÝ THUYẾT

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

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.

VMware Workstation cung cấp nhiều chế độ kết nối mạng khác nhau, giúp tạo ra một môi trường ảo hóa phù hợp với các yêu cầu thực tế. Dưới đây là chi tiết về từng chế độ mạng và ứng dụng của chúng trong hệ thống doanh nghiệp:

1.2.1.1 Bridged Network

Máy ảo kết nối trực tiếp với mạng vật lý của máy host, giống như một thiết bị độc lập trong mạng. Máy ảo sẽ nhận địa chỉ IP từ DHCP của mạng thật hoặc có thể được gán IP tĩnh. Có thể giao tiếp với các máy khác trong cùng mạng vật lý và truy cập internet.

1.2.1.2 NAT (Network Address Translation)

Máy ảo sử dụng một dải địa chỉ IP riêng, kết nối ra ngoài thông qua địa chỉ IP của máy host. VMware Workstation sẽ đóng vai trò là một router, thực hiện NAT để máy ảo có thể truy cập internet. Máy ảo không thể nhận kết nối trực tiếp từ bên ngoài trừ khi có cấu hình Port Forwarding.

1.2.1.3 Host-only Network

Máy ảo chỉ có thể giao tiếp với các máy ảo khác và máy host, không thể truy cập internet. Không liên quan đến mạng vật lý bên ngoài, giúp tạo một hệ thống mạng nội bộ độc lập.

1.2.1.4 Custom Network (VMnet1, VMnet8, vSwitch)

VMnet1 (Host-Only Network tùy chỉnh): Tương tự Host-Only nhưng có thể điều chỉnh các thông số mạng.

VMnet8 (NAT Network tùy chỉnh): Giống NAT nhưng có thể thay đổi địa chỉ IP, DHCP Server, Gateway.

vSwitch (Virtual Switch): Mạng ảo có thể định nghĩa nhiều kết nối và VLAN tùy chỉnh.

1.2.2 Tìm hiểu về pfsense

1.2.2.1 Pfsense là gì?

Pfsense là một tường lửa mã nguồn mở và bộ định tuyến (router) dựa trên hệ điều hành FreeBSD, được sử dụng rộng rãi trong các doanh nghiệp, tổ chức và hệ thống mạng cá nhân. pfSense có giao diện quản trị web trực quan, dễ sử dụng, cho phép quản lý mạng một cách linh hoạt mà không cần dòng lệnh phức tạp.

Pfsense có thể thay thế các thiết bị tường lửa đắt tiền như Cisco ASA, Fortinet, hoặc SonicWall trong nhiều môi trường khác nhau, từ doanh nghiệp nhỏ đến hệ thống mạng lớn.

1.2.2.2 Các tính năng của pfsense

Kiểm soát lưu lượng mạng (Firewall & NAT):

- Lọc gói tin (Packet Filtering): pfSense cho phép thiết lập các quy tắc kiểm soát lưu lượng dựa trên địa chỉ IP, giao thức, cổng, quốc gia (GeoIP), và ứng dụng.
- Network Address Translation (NAT): Hỗ trợ NAT 1:1, Port Forwarding, Outbound NAT giúp quản lý và điều hướng lưu lượng hiệu quả.

Hỗ trợ VPN (Virtual Private Network)

- OpenVPN & IPsec: Thiết lập kênh mã hóa bảo mật để kết nối từ xa.
- WireGuard: Hỗ trợ VPN nhanh, nhẹ, bảo mật cao.
- Site-to-Site VPN: Kết nối giữa các chi nhánh của doanh nghiệp.

Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)

- Snort & Suricata: Giám sát và phát hiện các cuộc tấn công mạng.
- Chặn tấn công DDoS, Brute Force, Malware, Botnet bằng cơ chế lọc gói tin thông minh.

Quản lý băng thông và chất lượng dịch vụ (QoS)

- Traffic Shaping: Hạn chế băng thông cho từng loại lưu lượng.
- Layer 7 Filtering: Phân tích và điều chỉnh lưu lượng theo ứng dụng (YouTube, Facebook, Torrent).

Hệ thống báo cáo & giám sát mạng

- pfSense Dashboard: Hiển thị trạng thái hệ thống, CPU, RAM, lưu lượng mạng.
- Packet Capture: Giám sát và phân tích lưu lượng theo thời gian thực.
- Syslog & RRD Graphs: Theo dõi nhật ký sự kiện, lưu lượng, và tấn công mạng.

Sd

1.2.2.3 Ưu điểm của pfSense so với các tường lửa truyền thống

Miễn phí, mã nguồn mở – Không tốn phí bản quyền như Cisco ASA, Fortinet.

Cấu hình linh hoạt – Hỗ trợ nhiều tính năng nâng cao mà không cần phần cứng đắt tiền.

Bảo mật mạnh mẽ – Cập nhật thường xuyên, hỗ trợ IPS, VPN, Firewall chuyên sâu.

Dễ sử dụng – Giao diện web thân thiện, không cần CLI phức tạp.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

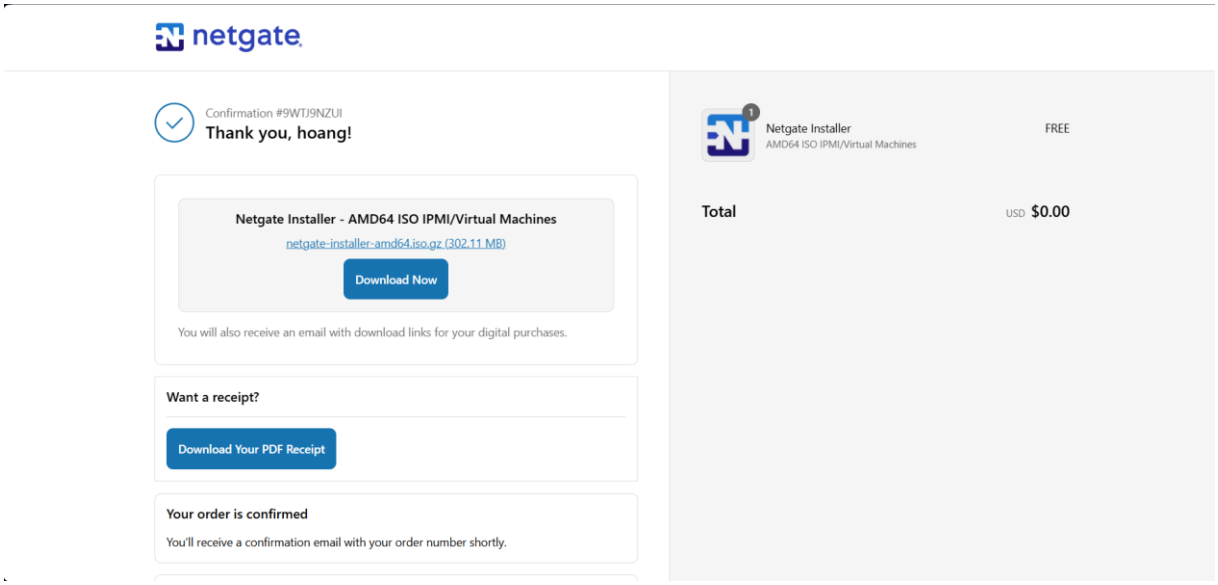
2.1 Chuẩn bị môi trường

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.

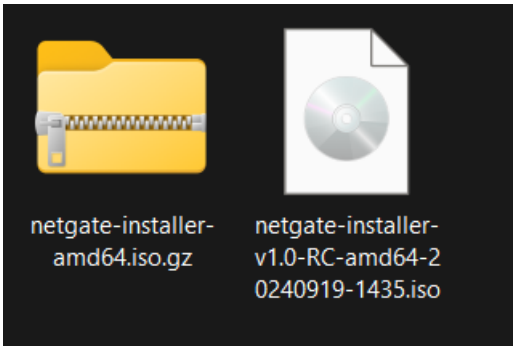
File cài đặt tường lửa Pfsense:

Tải file định dạng iso của pfsense



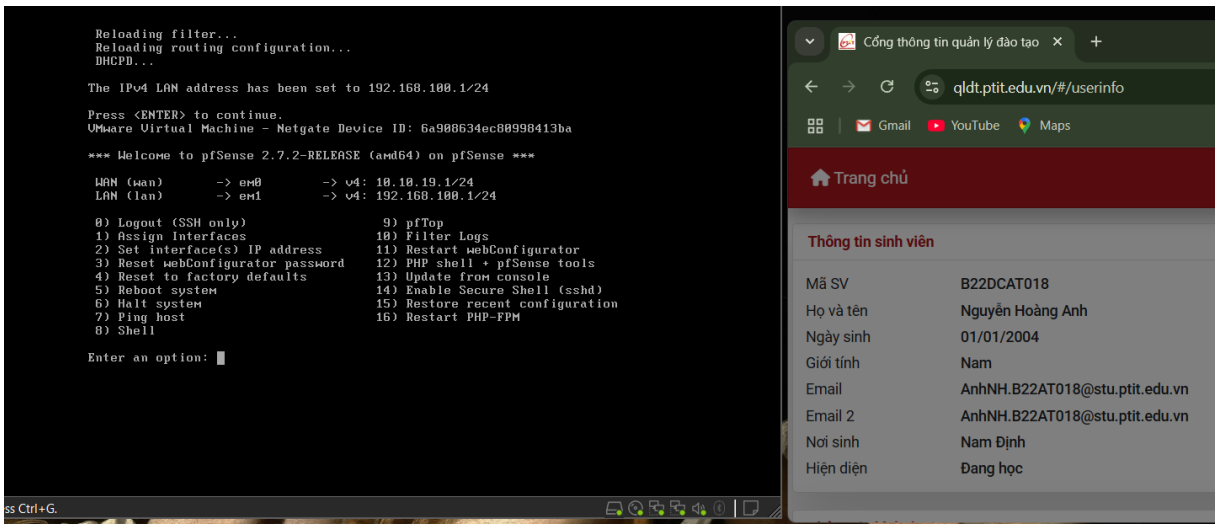
Hình 1 - file pfsense định dạng iso

Tải về và giải nén:



Hình 2 - file iso pfsense sau khi tải về dạng gz và sau khi giải nén

Cài đặt và cấu hình pfsense

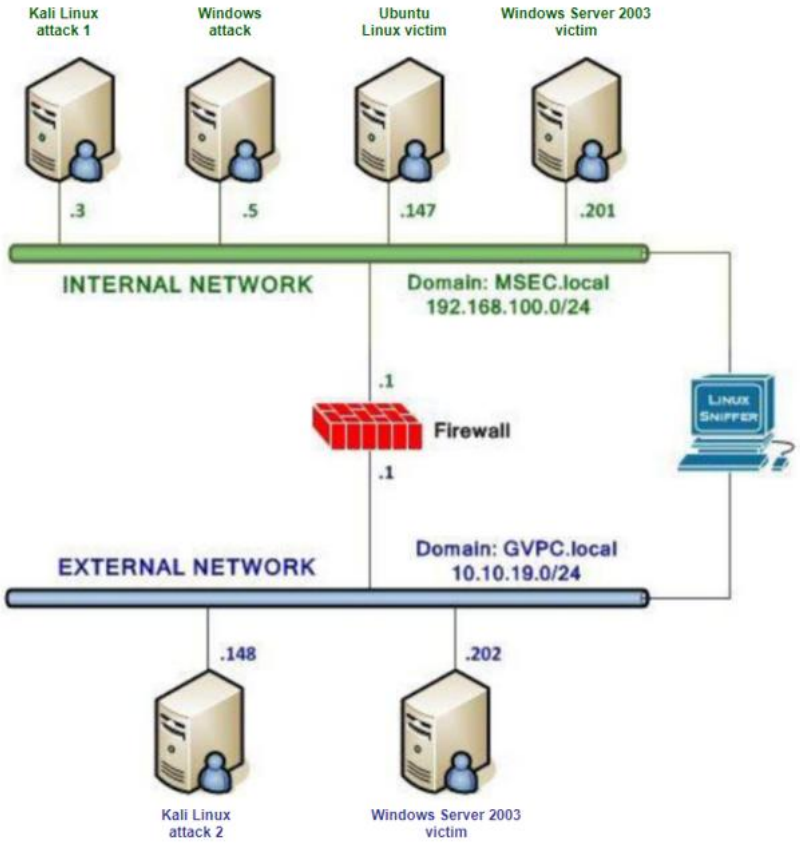


Hình 3 - cài đặt và cấu hình pfsense

2.2 Các bước thực hiện

2.2.1 Cấu hình topo mạng

Cấu hình topo mạng như hình dưới đây



Hình 4 - topo mạng theo yêu cầu đề bài

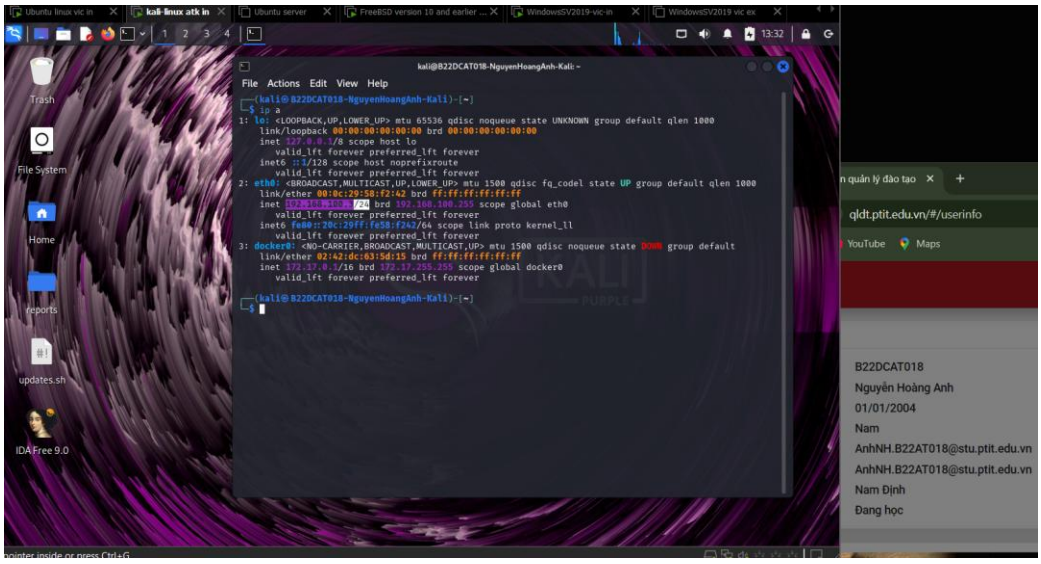
Thông tin yêu cầu về các thiết bị trong hệ thống:

Bảng 1 - thông tin các thiết bị trong hệ thống

Máy Kali Linux attack 1 trong mạng Internal	IP: 192.168.100.3 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng Internal	IP: 192.168.100.201 Mật khẩu root: password
Máy Linux Victim trong mạng Internal	IP: 192.168.100.147 Mật khẩu root: password
Máy pfSense Firewall	IP: 10.10.19.1, 192.168.100.1 Mật khẩu: admin/pfsense
Máy Linux Attack trong mạng External	IP: 10.10.19.148 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng External	IP: 10.10.19.202 Mật khẩu root: password

2.2.1.1 Cấu hình các thiết bị trong topo

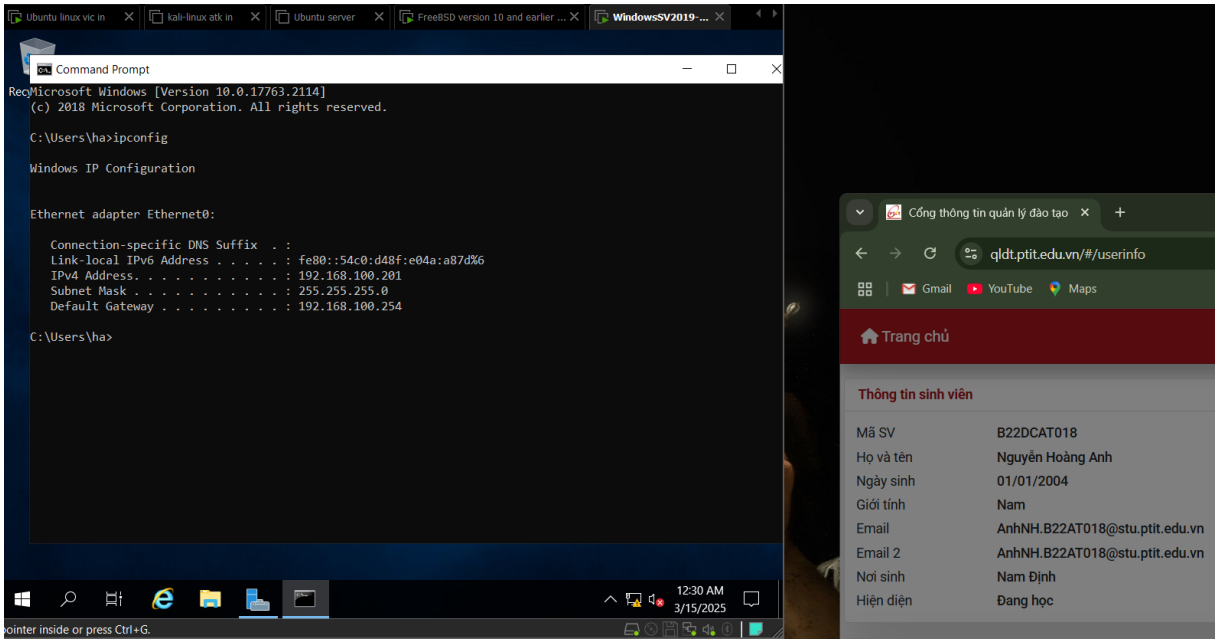
Máy kali linux attack 1 trong mạng internal: Ip: 192.168.100.3



Hình 5 - máy kali attack trong mạng internal

Máy windows server 2019 victim trong mạng internal:

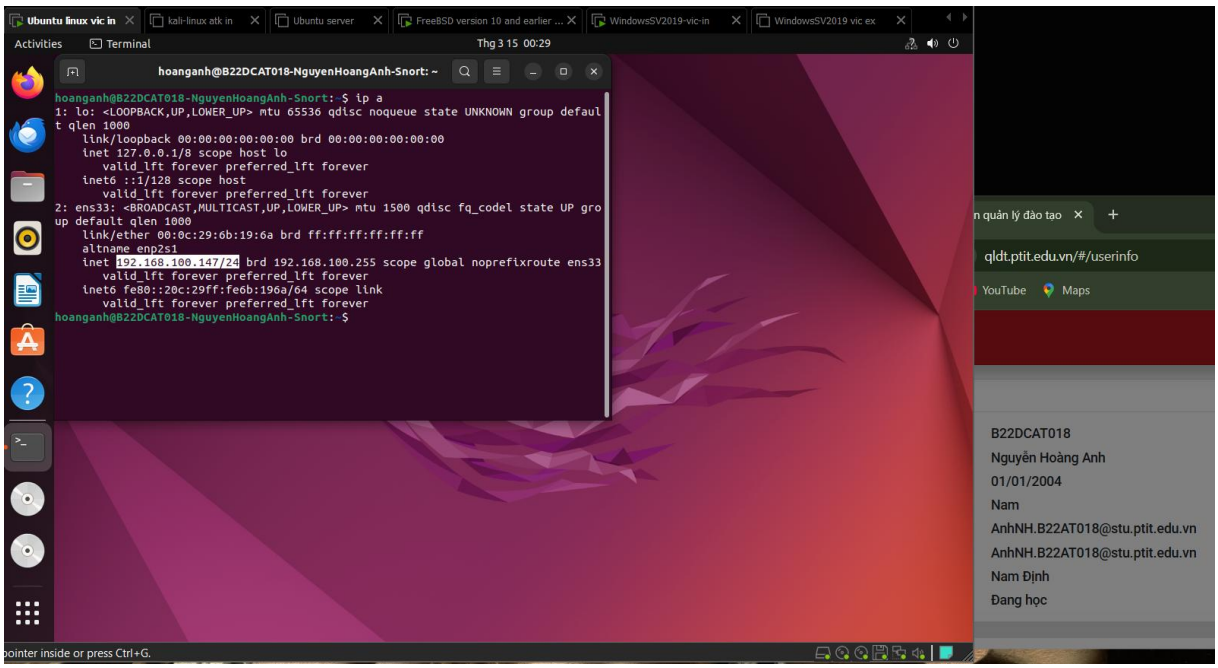
Ip: 192.168.100.201



Hình 6 - máy windows server 2019 victim trong mạng internal

Máy linux victim trong mạng internal:

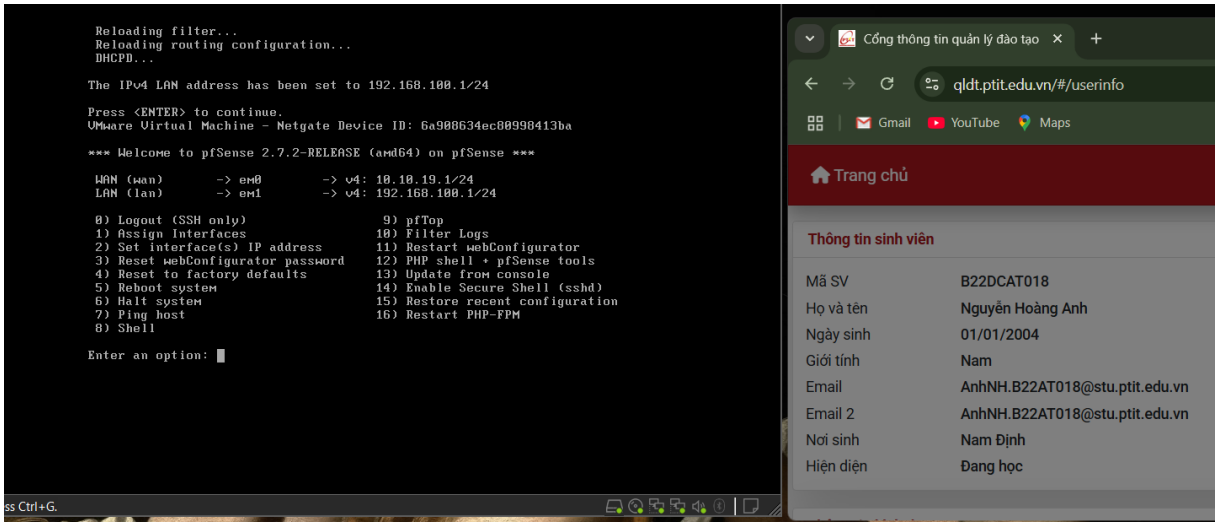
Ip: 192.168.100.147



Hình 7 - máy linux victim trong mạng internal

Máy pfsense:

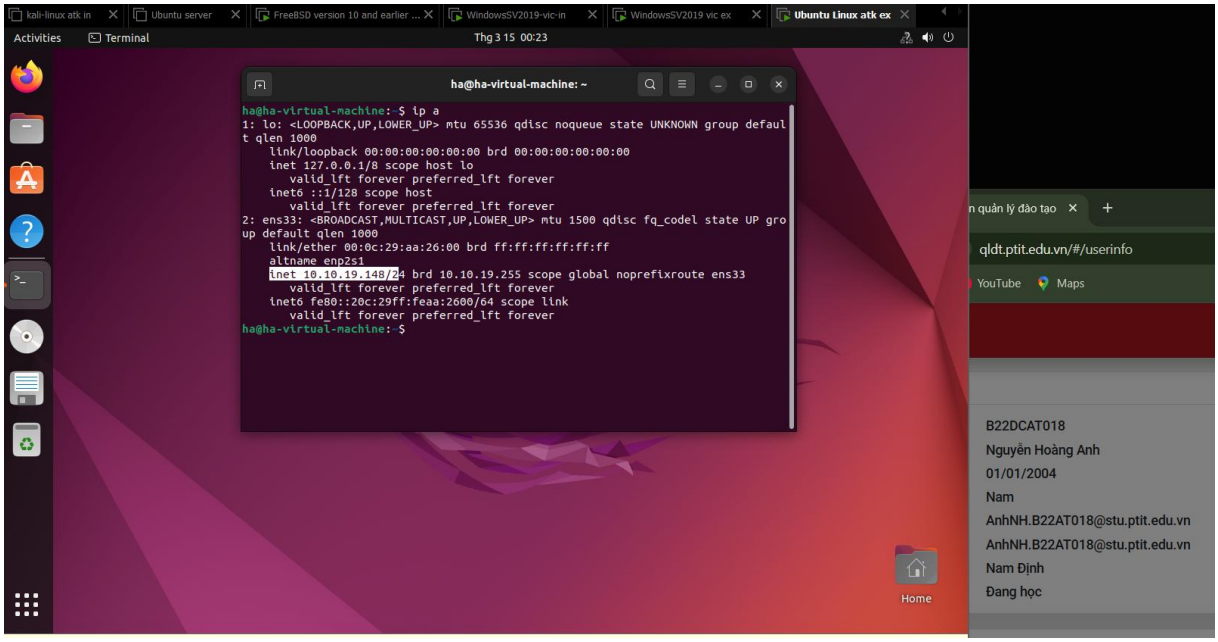
Ip: 10.10.19.1 và 192.168.100.1



Hình 8 - máy pfsense

Máy linux attack trong mạng external:

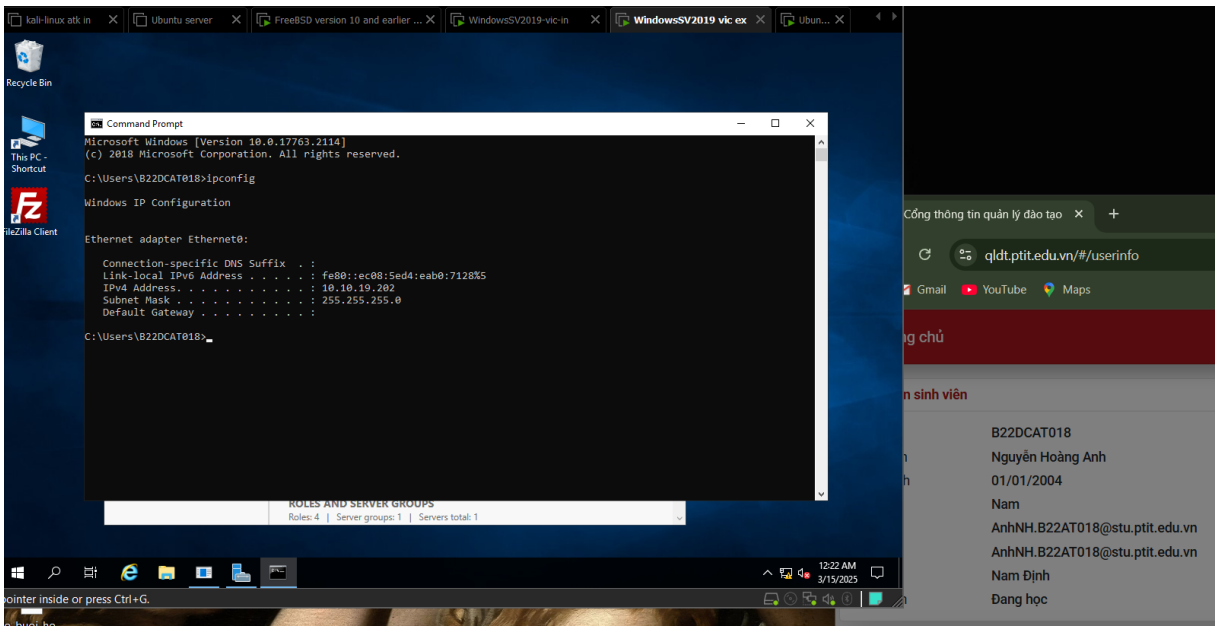
Ip: 10.10.19.148



Hình 9 - máy ubuntu linux attack trong mạng external

Máy windows server 2019 victim trong mạng external:

Ip: 10.10.19.202

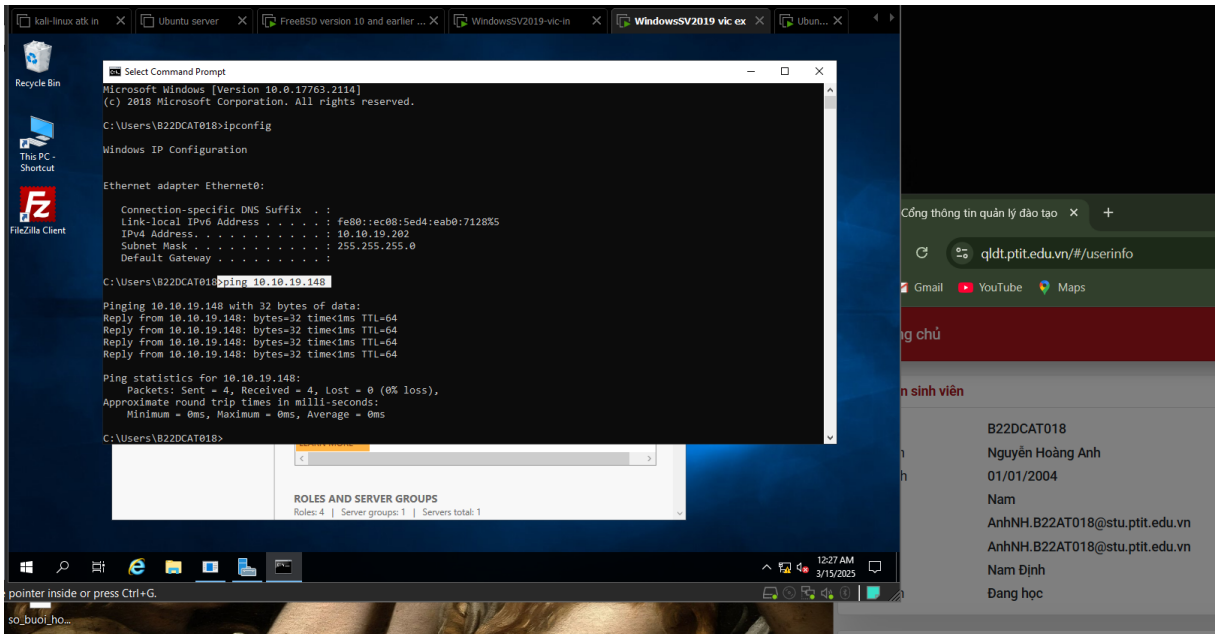


Hình 10 - máy windows server victim trong mạng external

2.2.1.2 Kiểm tra ping

- Trong mạng external:

Ping từ máy windows server external tới máy linux external:

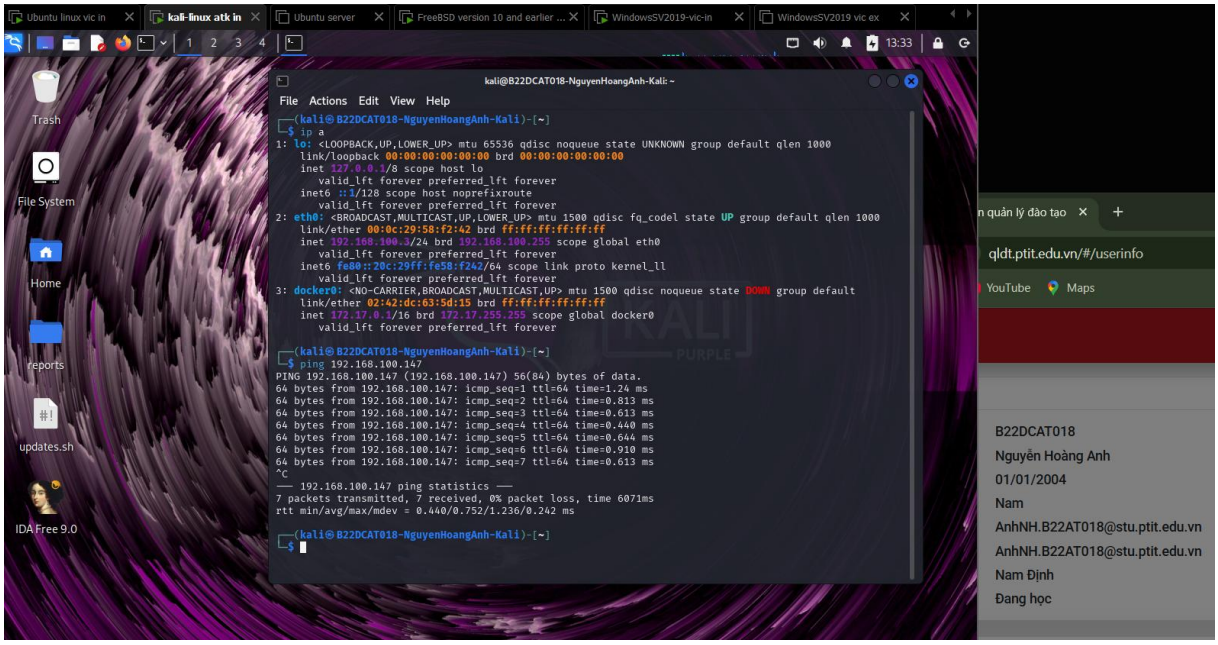


Hình 11 - ping từ windows server external tới linux external

➔ Ping thành công, chứng tỏ 2 máy ở mạng external đã thông nhau

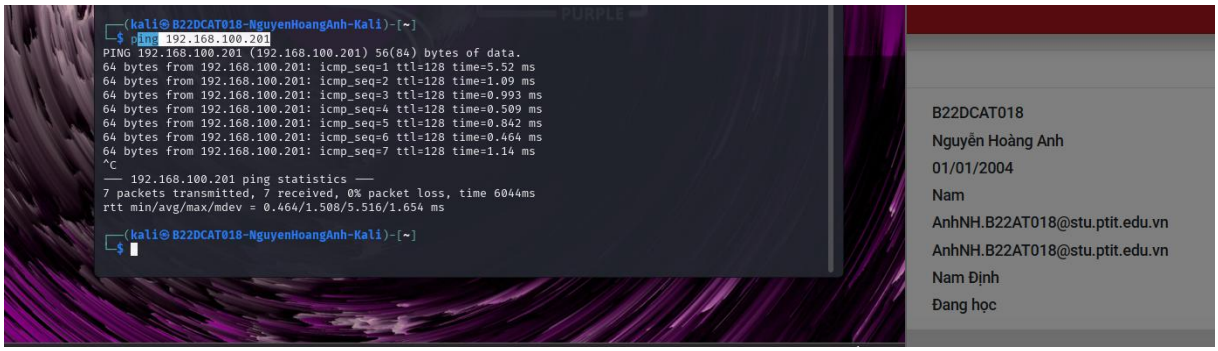
- Trong mạng internal:

Ping từ máy kali attack tới máy ubuntu linux victim:



Hình 12 - ping từ kali attack tới linux victim

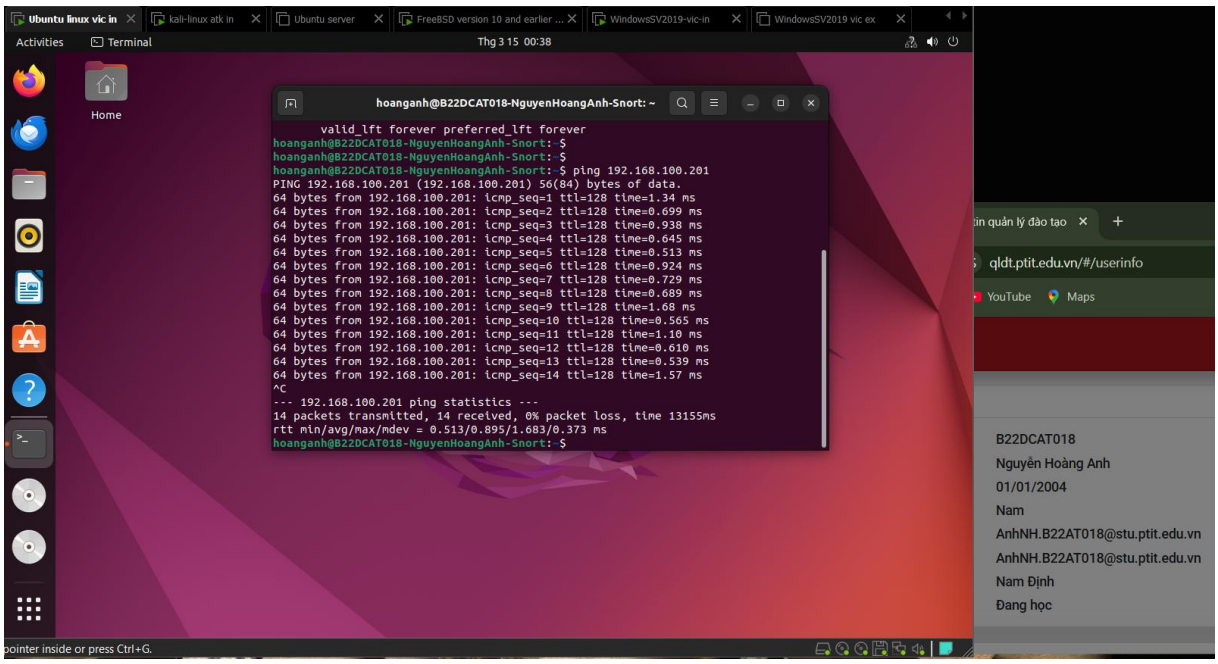
Ping từ máy kali attack tới máy windows server victim:



Hình 13 ping từ kali attack tới windows server victim

➔ Ping từ máy kali tới máy ubuntu và windows server trong mạng internal đều thành công

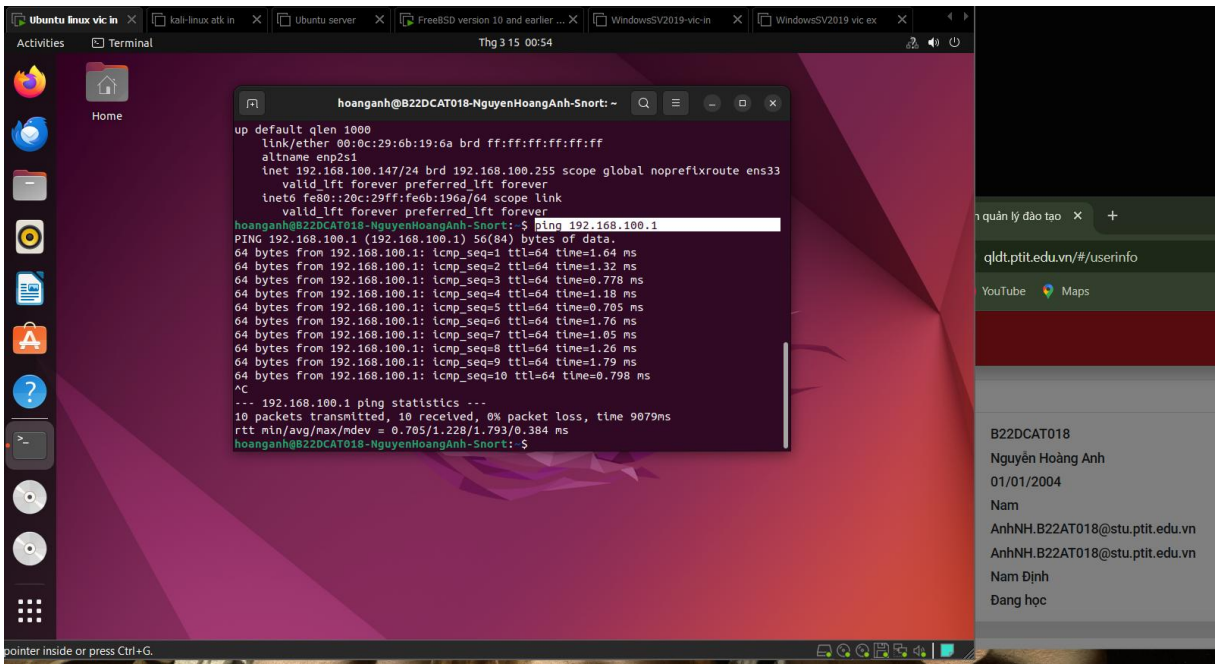
Ping từ máy linux tới máy windows server trong mạng internal:



Hình 14 - ping từ máy linux tới windows server

➔ Ping thành công từ máy linux tới máy windows server

Ping từ máy linux tới pfsense:



Hình 15 - ping từ linux tới pfsense

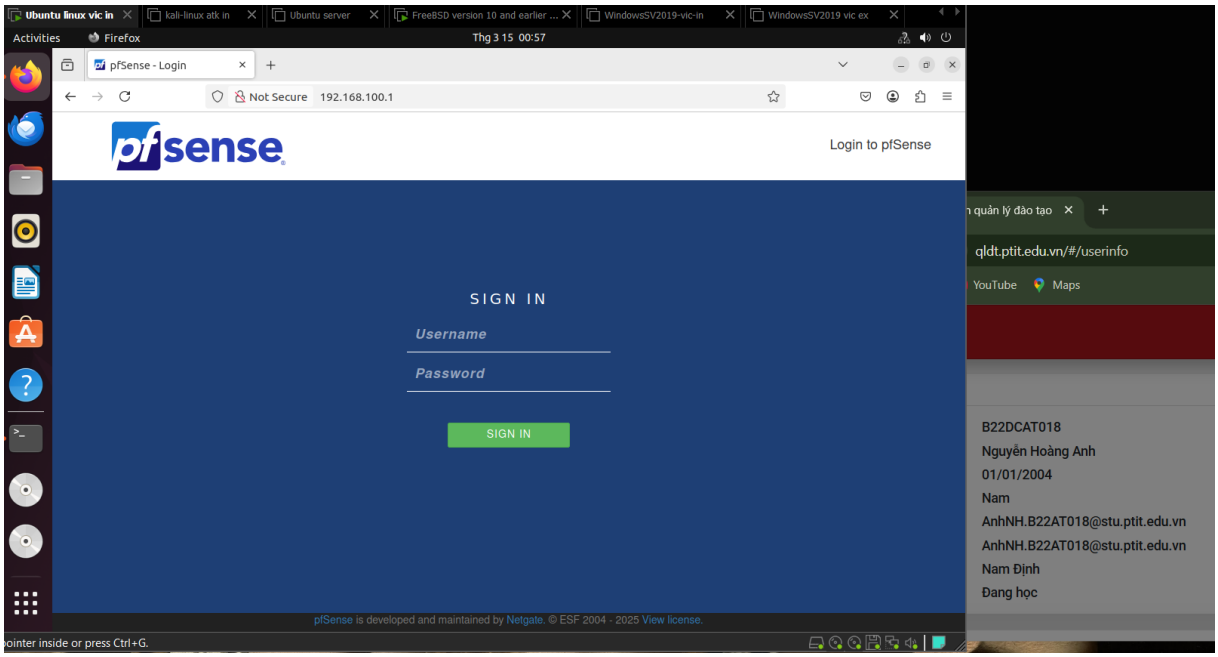
➔ Ping thành công từ máy linux tới máy pfsense

→ vậy tất cả các máy trong mạng internal đều đã thông nhau

2.2.2 Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

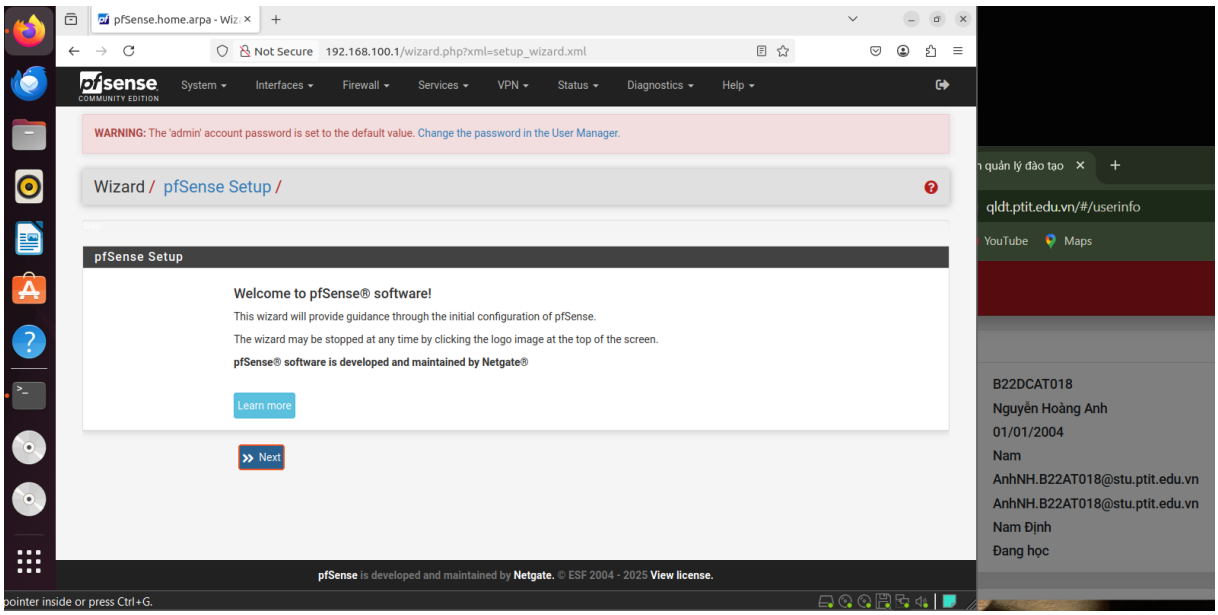
a) Cấu hình ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal. Các bước lần lượt như sau:

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



Hình 16 - giao diện web của pfsense

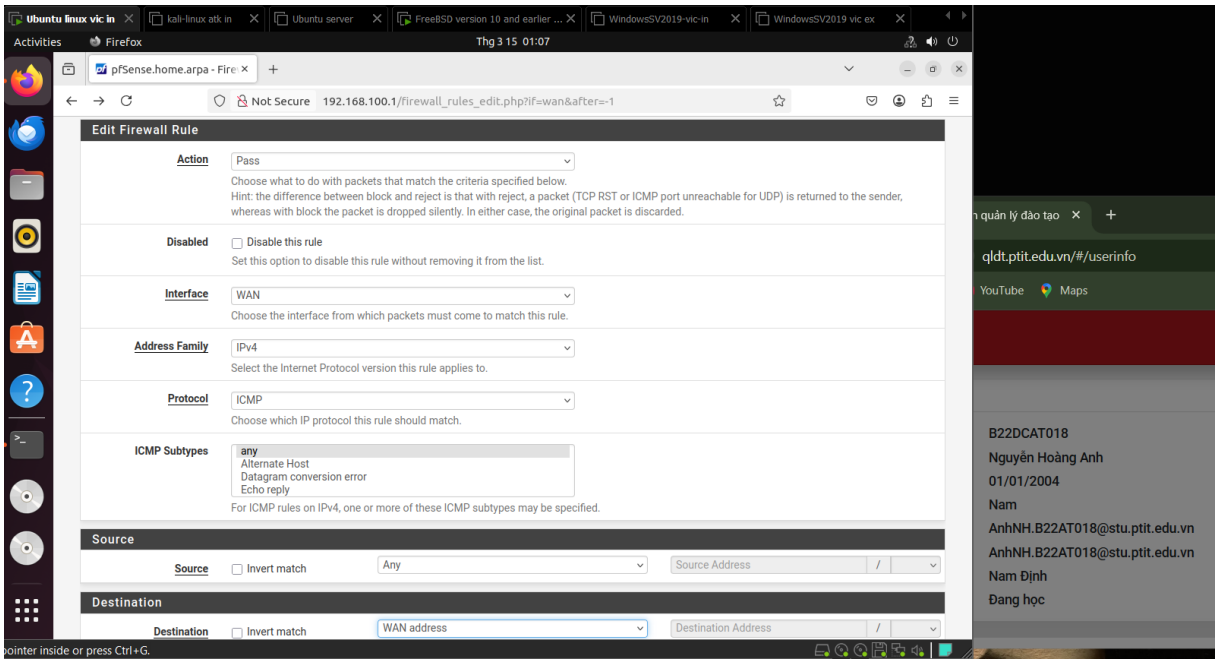
Đăng nhập và với tài khoản và mật khẩu lần lượt là: admin và pfsense



Hình 17 - giao diện sau khi đăng nhập thành công

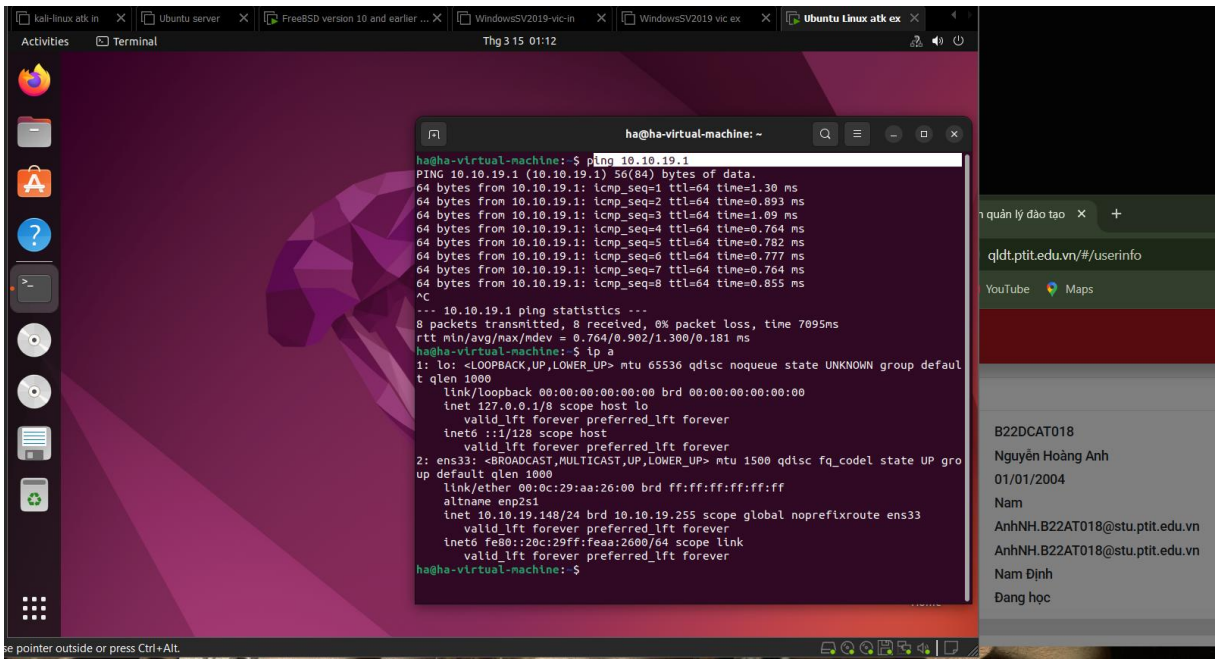
- Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1

Cấu hình rule firewall để external có thể ping tới giao diện 10.10.19.1



Hình 18 - cấu hình rule firewall

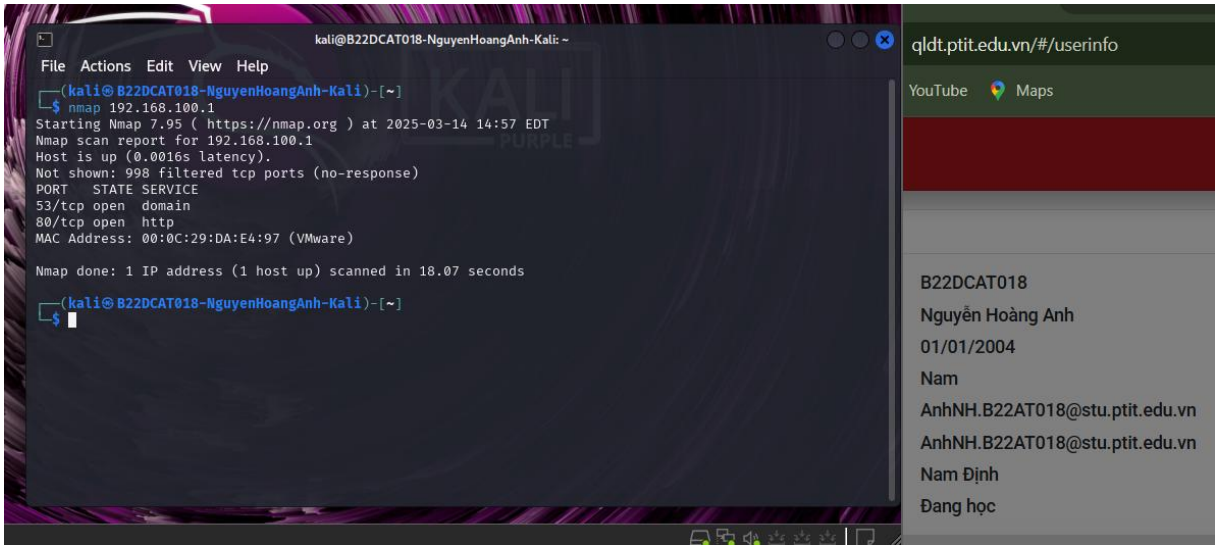
- Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Linux attack ở mạng ngoài.



Hình 19 - ping từ máy linux attack ở mạng external tới 10.10.19.1

b) Trả lời câu hỏi:

– Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng trong của pfSense?

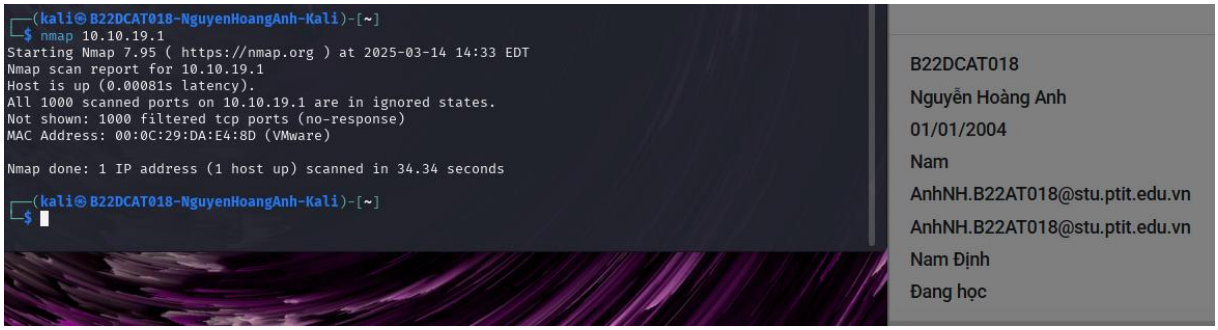


Hình 20 - quét cổng 192.168.100.1

Sử dụng nmap để quét cổng: nmap 192.168.100.1

➔ 2 cổng đang mở

– Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng ngoài của pfSense?



Hình 21 - quét cổng 10.10.19.1

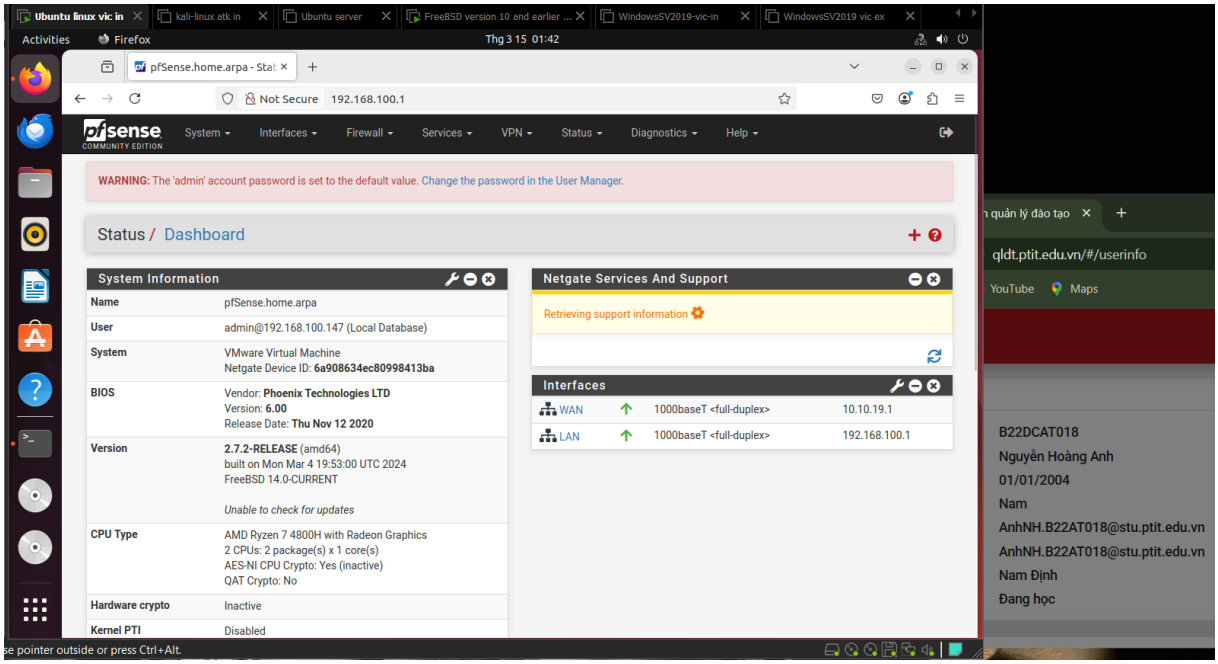
Sử dụng nmap để quét cổng: *nmap 10.10.19.1*

➔ 1 cổng đang mở

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

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

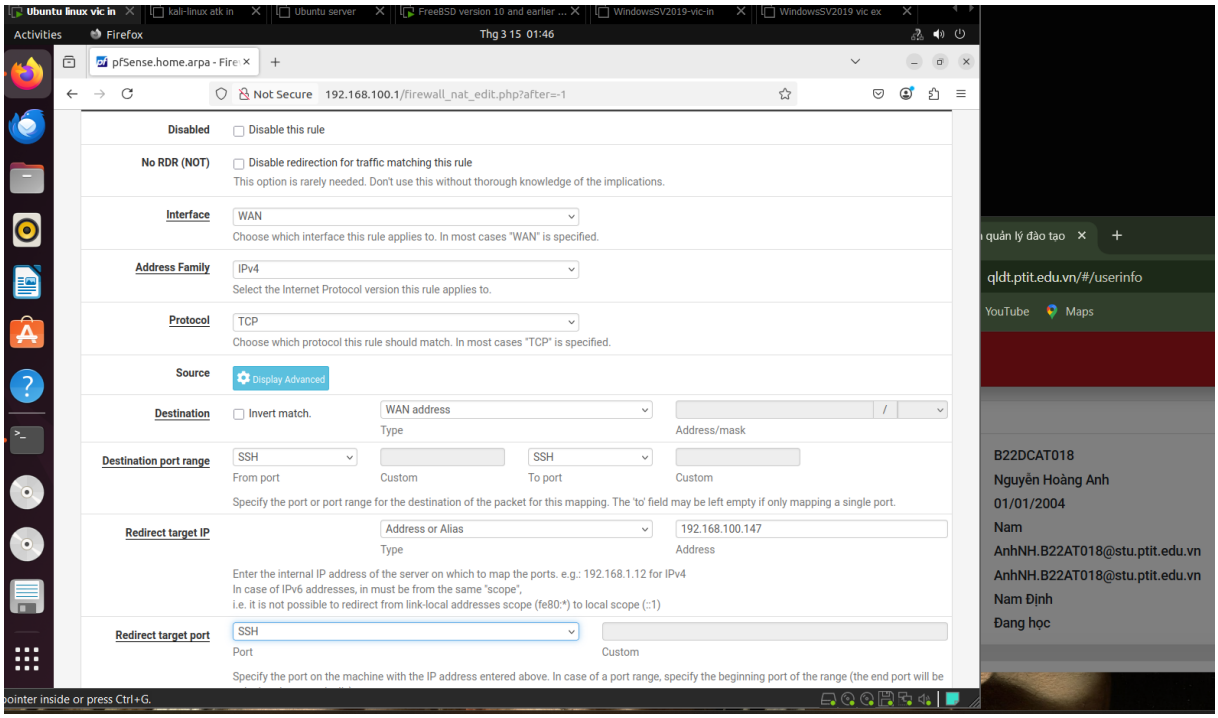
- Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình NAT trên pfsense qua giao diện web.



Hình 22 - giao diện 192.168.100.1

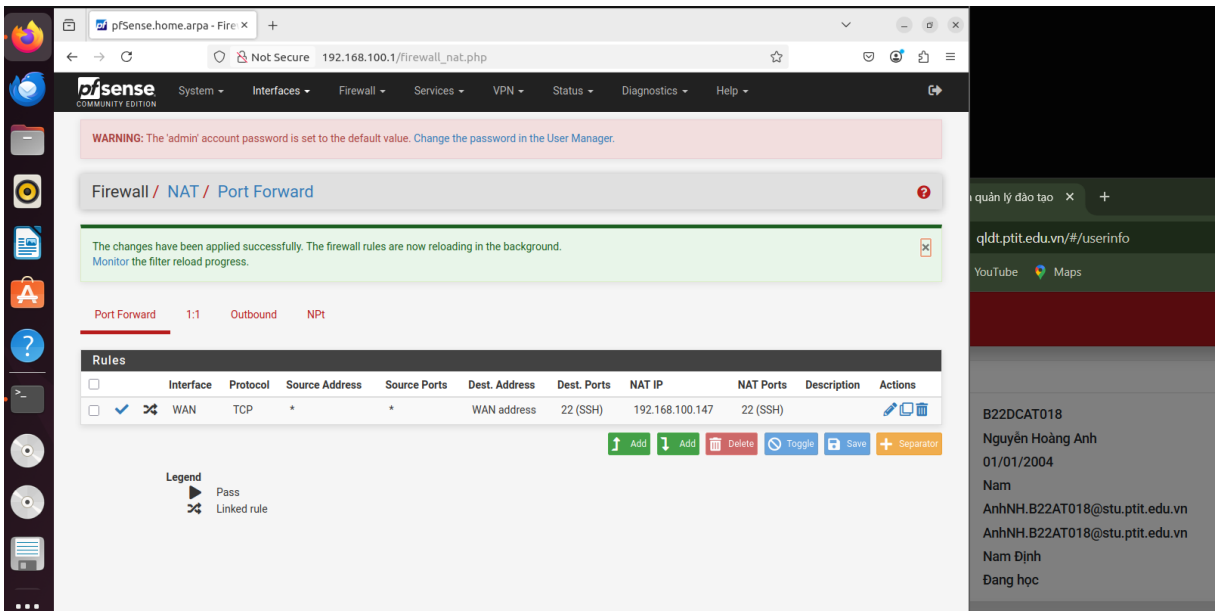
- Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy Linux victim mạng Internal) được truy cập từ bên ngoài thông qua port forwarding. Nghĩa là khi các máy khách từ mạng 10.10.19.0/24 kết nối với địa chỉ IP của tường lửa pfSense của 10.10.19.1, chúng sẽ được chuyển hướng đến máy Linux victim trong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

Cấu hình rule mới để cho phép cổng ssh trên ip 192.168.100.147 được truy cập từ bên ngoài



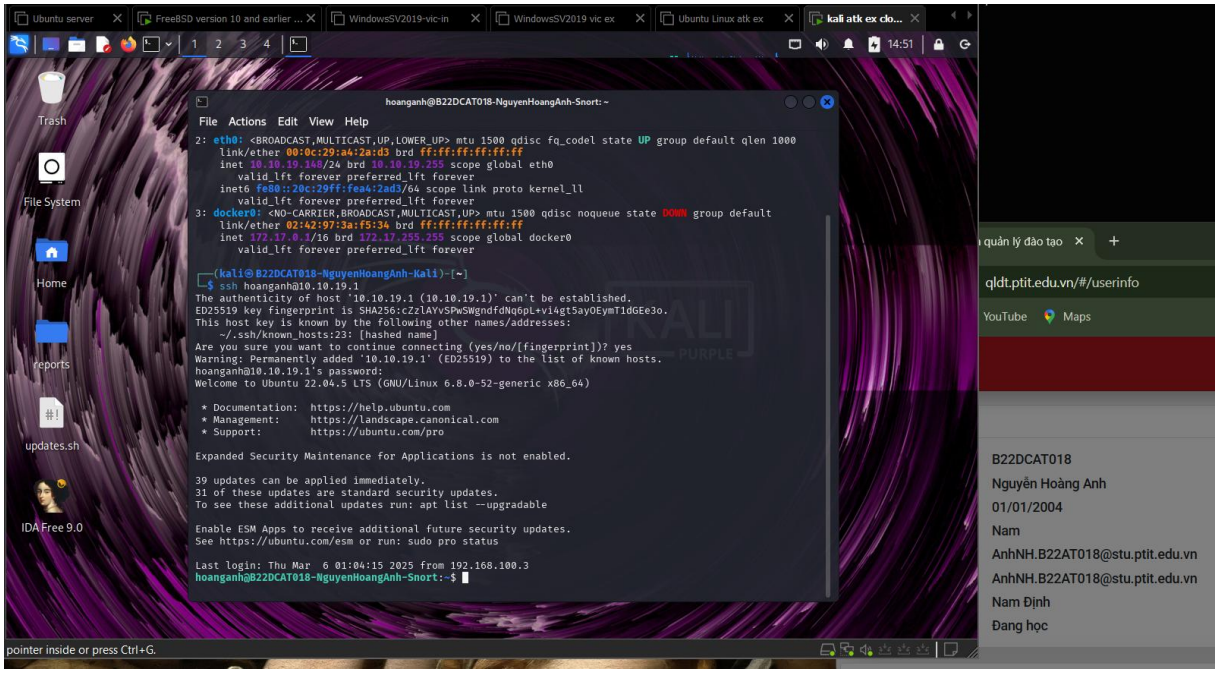
Hình 23 - cấu hình rule mới

Apply rule mới thành công:



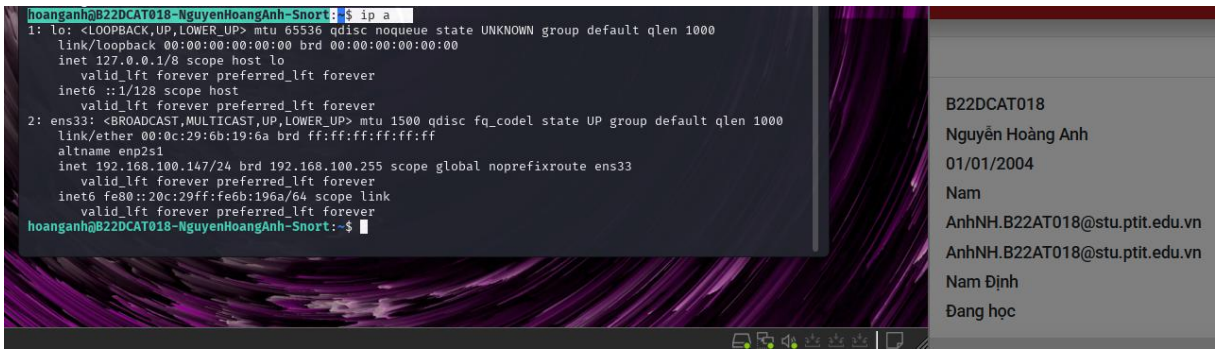
Hình 24 - apply rule mới

Ssh từ máy kali external tới máy linux victim internal



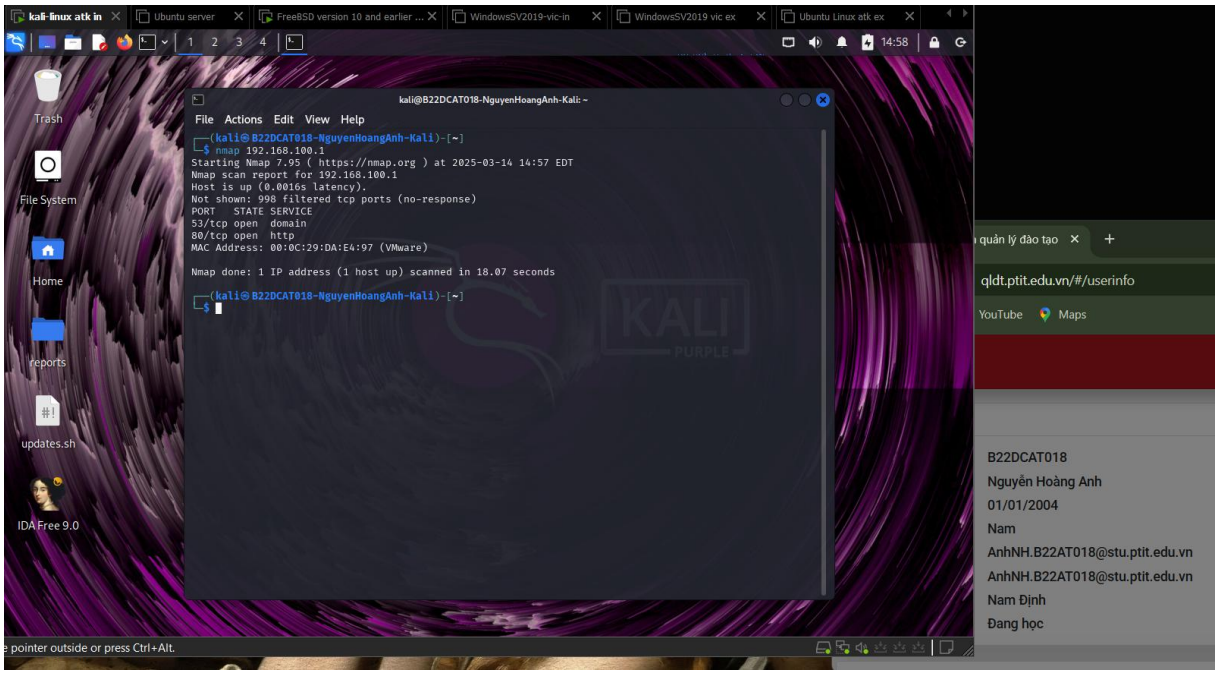
Hình 25 - ssh từ máy kali external tới máy linux victim internal

- Kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?



Hình 26 - kiểm tra ip của máy linux vừa được ssh đến

- Kiểm tra các cổng được phép truy cập trên mạng Internal bằng cách gõ lệnh trên máy Kali Linux trong mạng Internal: nmap 192.168.100.1



Hình 27 - kiểm tra các cổng

TỔNG KẾT

Qua bài thực hành này, chúng ta đã tìm hiểu và áp dụng các bước để xây dựng một mạng doanh nghiệp với pfSense firewall nhằm kiểm soát lưu lượng truy cập. Cụ thể, sinh viên đã:

- Cài đặt và cấu hình pfSense firewall để kiểm soát truy cập, từ việc thiết lập topo mạng, điều chỉnh các quy tắc firewall, đến cấu hình lưu lượng ICMP

- Thiết lập chính sách bảo mật nhằm cho phép hoặc chặn lưu lượng trong mạng nội bộ, đồng thời định tuyến lưu lượng đến các thiết bị trong mạng internal

Bài thực hành giúp sinh viên có cái nhìn thực tế về cách một tường lửa hoạt động trong môi trường mạng doanh nghiệp. Những kiến thức này sẽ là nền tảng quan trọng để tiếp tục nghiên cứu về bảo mật mạng, quản trị hệ thống, và kiểm thử xâm nhập trong các bài lab ATTT sau này

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. VirtualBox Network Settings: Complete Guide: https://www.nakivo.com/blog/virtualbox-network-setting-guide/

4. Lab 7 pfsense firewall của CSSIA CompTIA Security+®

5. Advanced Penetration Testing for Highly-Secured Environments

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