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

BÁO CÁO

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

Giảng viên hướng dẫn: Vũ Minh Mạnh

Sinh viên thực hiện: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Lớp: D21CQAT03-B

Hà Nội, 2023

Môn học Thực tập cơ sở
Bài 5: Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

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 Nội dung thực hành

1.2.1 Tìm hiểu lý thuyết

- **Mạng ảo**

- Là một mô hình mạng được tạo ra và quản lý trên phần cứng và phần mềm ảo hóa. Trong mạng ảo, các tài nguyên mạng như máy chủ, bộ định tuyến, máy tính, và mạng LAN được tạo ra bằng cách sử dụng phần cứng và phần mềm ảo hóa thay vì cơ sở hạ tầng vật lý truyền thống.

- Mạng ảo cho phép giao tiếp giữa nhiều máy tính, máy ảo (VM), máy chủ ảo hoặc các thiết bị khác trên các vị trí văn phòng và trung tâm dữ liệu khác nhau. Trong khi mạng vật lý kết nối các máy tính thông qua cáp và phần cứng khác, mạng ảo mở rộng các khả năng này bằng cách sử dụng quản lý phần mềm để kết nối máy tính và máy chủ qua Internet.

- Mạng ảo cho phép các thiết bị trên nhiều địa điểm hoạt động với các khả năng tương tự như mạng vật lý truyền thống. Điều này cho phép các trung tâm dữ liệu trải dài trên các vị trí địa lý khác nhau và cung cấp cho quản trị viên mạng các tùy chọn mới và hiệu quả hơn, như khả năng dễ dàng sửa đổi mạng khi nhu cầu thay đổi mà không cần phải thay đổi hay mua mới phần cứng; linh hoạt hơn trong việc cung cấp mạng cho các nhu cầu và ứng dụng cụ thể; và khả năng di chuyển công việc trên cơ sở hạ tầng mạng mà không ảnh hưởng đến dịch vụ, bảo mật và tính khả dụng.

- **Chế độ mạng:**

- VMware và VirtualBox cung cấp các chế độ mạng khác nhau cho máy ảo, bao gồm chế độ NAT, Bridged, Host-only và Internal networking.

- **NAT (Network Address Translation)**: Máy ảo chia sẻ địa chỉ IP của máy chủ vật lý. Điều này cho phép máy ảo truy cập vào mạng bên ngoài thông qua IP của máy chủ vật lý.

- **Bridged**: Máy ảo có địa chỉ IP riêng và hoạt động như một máy tính trong mạng vật lý. Nó có thể truy cập các thiết bị trong cùng mạng với máy chủ vật lý.

- **Host-only**: Máy ảo có thể giao tiếp với máy chủ vật lý và các máy ảo khác trong cùng một mạng nội bộ, nhưng không thể truy cập mạng bên ngoài.

- **Internal networking**: Máy ảo chỉ có thể giao tiếp với các máy ảo khác trên cùng một mạng nội bộ, không thể truy cập vào mạng bên ngoài hoặc máy chủ vật lý.

❖ **Cấu hình card mạng:**

- Trong mỗi máy ảo, bạn có thể cấu hình một hoặc nhiều card mạng, mỗi card mạng có thể được gán cho một chế độ mạng khác nhau.

- Bạn có thể cấu hình các thông số mạng như địa chỉ IP, subnet mask, gateway và DNS trên mỗi card mạng.

❖ **Phân cấp DHCP:**

- VMware và VirtualBox thường cung cấp một dịch vụ DHCP để tự động cấp phát địa chỉ IP cho các máy ảo trong chế độ NAT hoặc Bridged.

❖ **Cấu hình card mạng:**

- Cả hai phần mềm đều cung cấp giao diện đồ họa và dòng lệnh để quản lý cấu hình mạng của máy ảo, bao gồm việc thêm/xóa/sửa card mạng, cấu hình các thiết lập mạng, và giám sát hoạt động mạng.

- Việc hiểu và cấu hình đúng cấu hình mạng là rất quan trọng để đảm bảo máy ảo hoạt động như mong đợi và có thể giao tiếp với các thành phần mạng khác.

❖ **PfSense.**

- Là một hệ điều hành tường lửa mã nguồn mở dựa trên FreeBSD, được thiết kế để sử dụng như một thiết bị tường lửa, định tuyến và cổng vào mạng (gateway) cho mạng máy tính. Nó cung cấp một loạt các tính năng mạnh mẽ như tường lửa, VPN, cân bằng tải, quản lý băng thông, chống vi rút và nhiều tính năng khác.

- **Tường lửa (Firewall)**: pfSense cung cấp một tường lửa mạnh mẽ cho việc kiểm soát lưu lượng mạng, cho phép người quản trị cấu hình các quy tắc để cho phép hoặc từ chối gói tin dựa trên nhiều yếu tố như địa chỉ IP, cổng, giao thức, và nhiều hơn nữa.

- **VPN (Virtual Private Network)**: pfSense hỗ trợ nhiều loại VPN bao gồm IPSec, OpenVPN, và L2TP/IPsec. Điều này cho phép người dùng kết nối mạng riêng ảo (VPN) để truy cập mạng nội bộ một cách an toàn từ xa.

- **Định tuyến (Routing):** pfSense có khả năng định tuyến mạng và quản lý các giao thức định tuyến như RIP và OSPF, cho phép nó được sử dụng như một router trong một mạng phức tạp.

- **Proxy và cân bằng tải**: pfSense cung cấp các tính năng cân bằng tải và proxy cho phép phân phối công việc mạng đồng đều và tối ưu hóa hiệu suất mạng.

- **Quản lý băng thông**: pfSense cung cấp các công cụ quản lý băng thông cho phép người quản trị kiểm soát và giám sát việc sử dụng băng thông của mạng.

- Tài liệu tham khảo:
    - Lab 7 pfsense firewall của CSSIA CompTIA Security+®
    - Advanced Penetration Testing for Highly-Secured Environments

    Second Edition
    - Giới thiệu về Pfsense: https://viblo.asia/p/network-gioi-thieu-vepfsense-N0bDM6LXv2X4

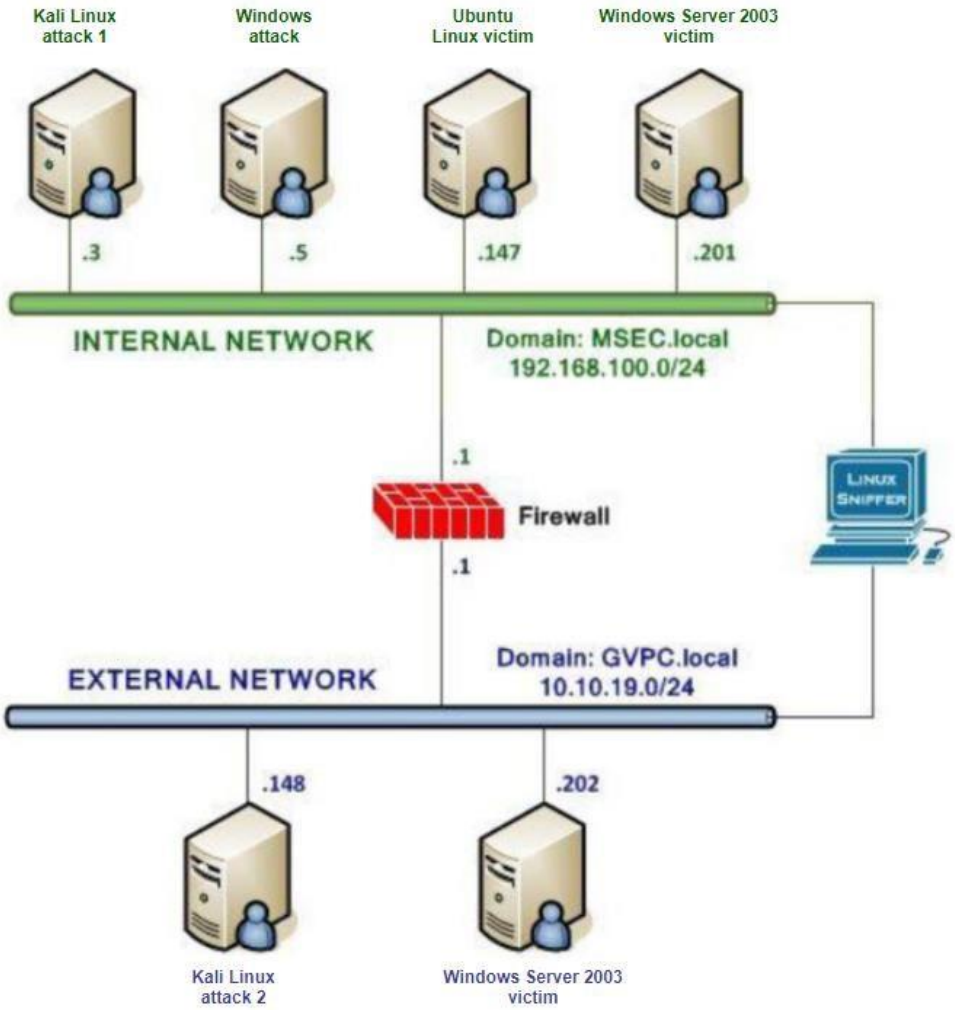
1.2.2 Chuẩn bị môi trường ○ Phần mềm VMWare Workstation. ○ Các file máy ảo VMware đã cài đặt trong các bài lab trước đó: máy trạm, máy chủ Windows và Linux. ○ File cài đặt tường lửa Pfsense

1.2.3 Các bước thực hiện và kết quả cần đạt

1.2.3.1 Cấu hình topo mạng

a) Cài đặt và cấu hình hệ thống theo topo mạng và thông tin như mô tả

dưới đây (bao gồm cài đặt các máy ảo)



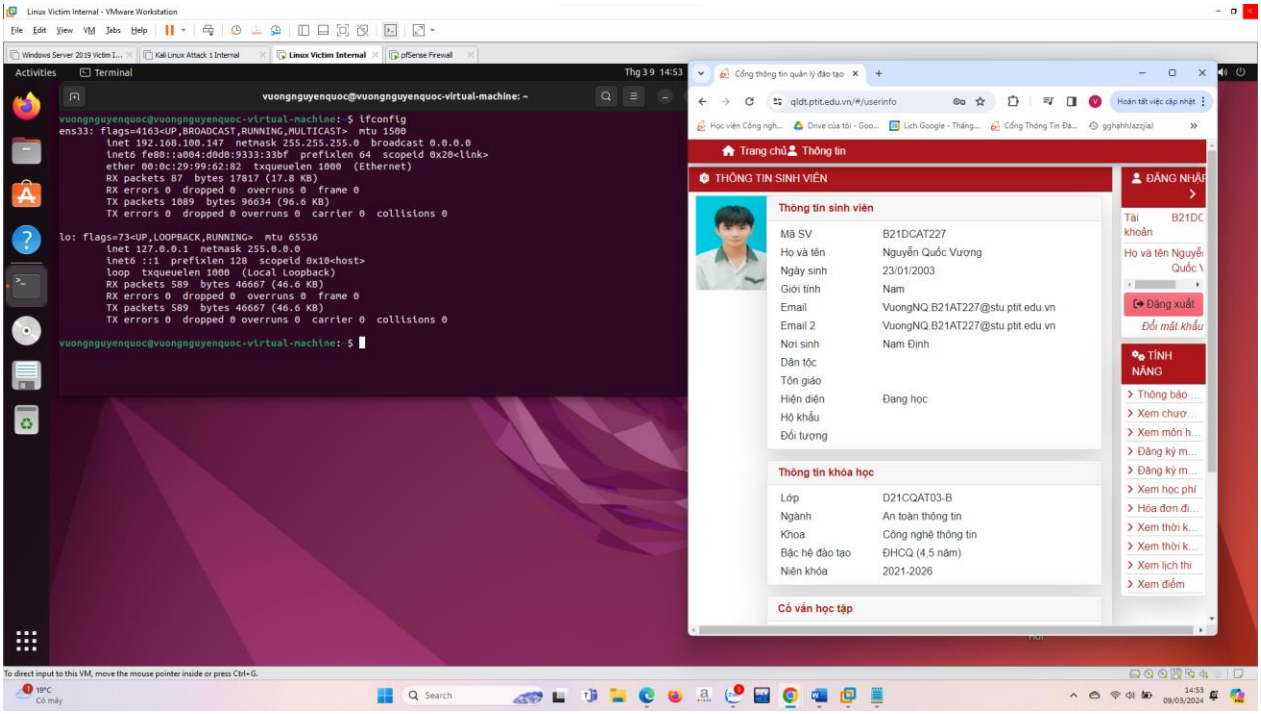
Thông tin yêu cầu cho các thiết bị trong hệ thống:

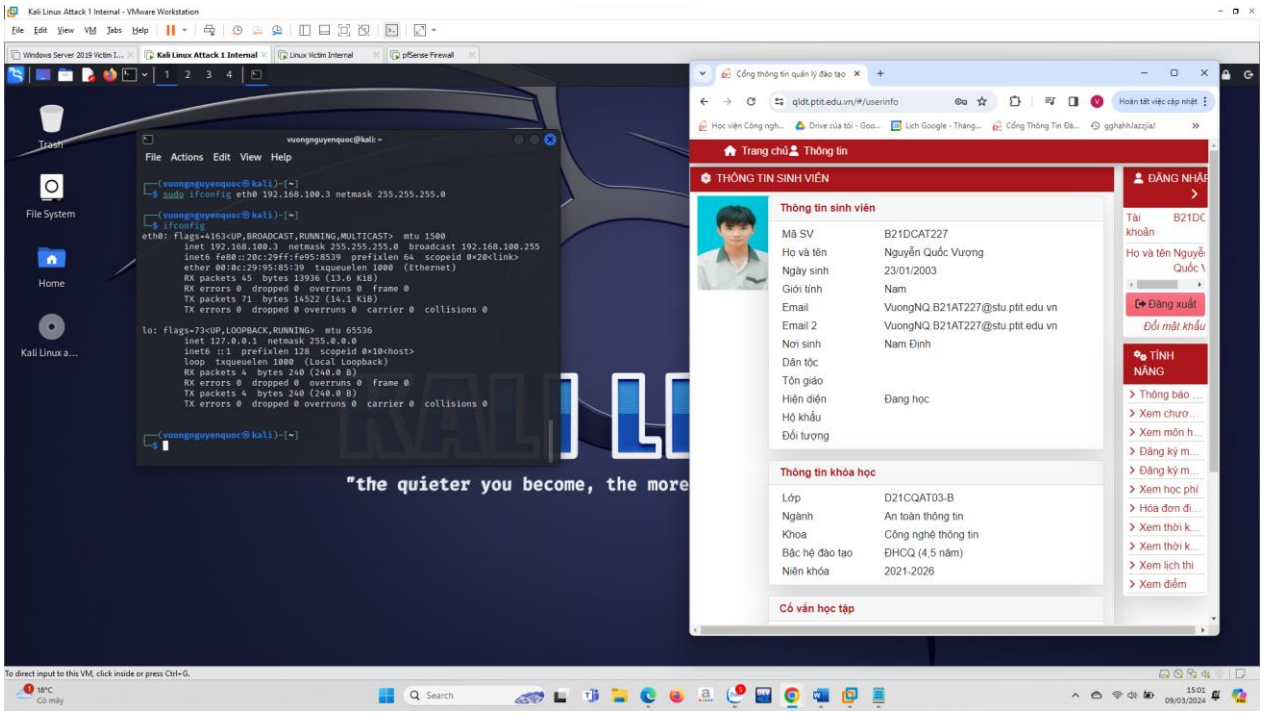
Máy Kali Linux attack 1 trong mạng Internal	IP: 192.168.100.3 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng Internal	IP: 192.168.100.201 Mật khẩu root: password
Máy Linux Victim trong mạng Internal	IP: 192.168.100.147 Mật khẩu root: password
Máy pfSense Firewall	IP: 10.10.19.1, 192.168.100.1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

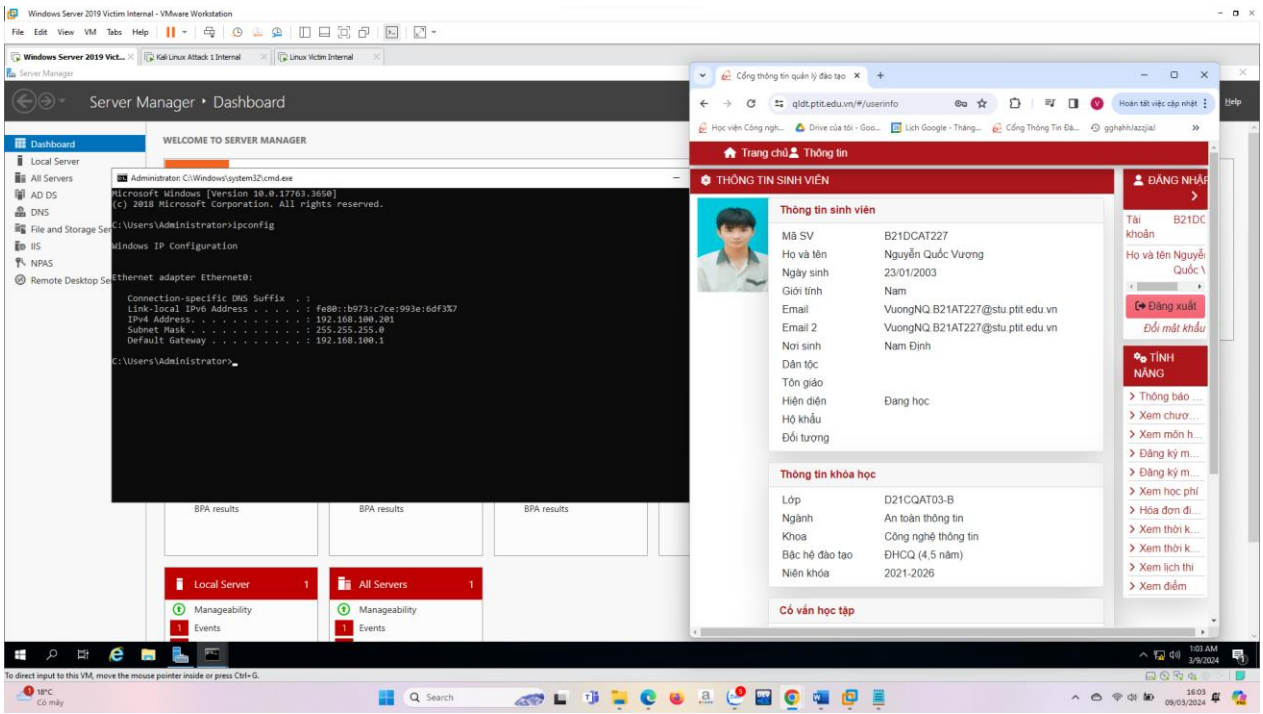
Xx`Máy Linux Attack trong mạng External	IP: 10.10.19.148 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng External	IP: 10.10.19.202 Mật khẩu root: password

Chú ý: nếu không tìm được phiên bản Windows Server 2003 thì sinh viên có thể sử dụng các phiên bản Windows Server khác cho bài này.

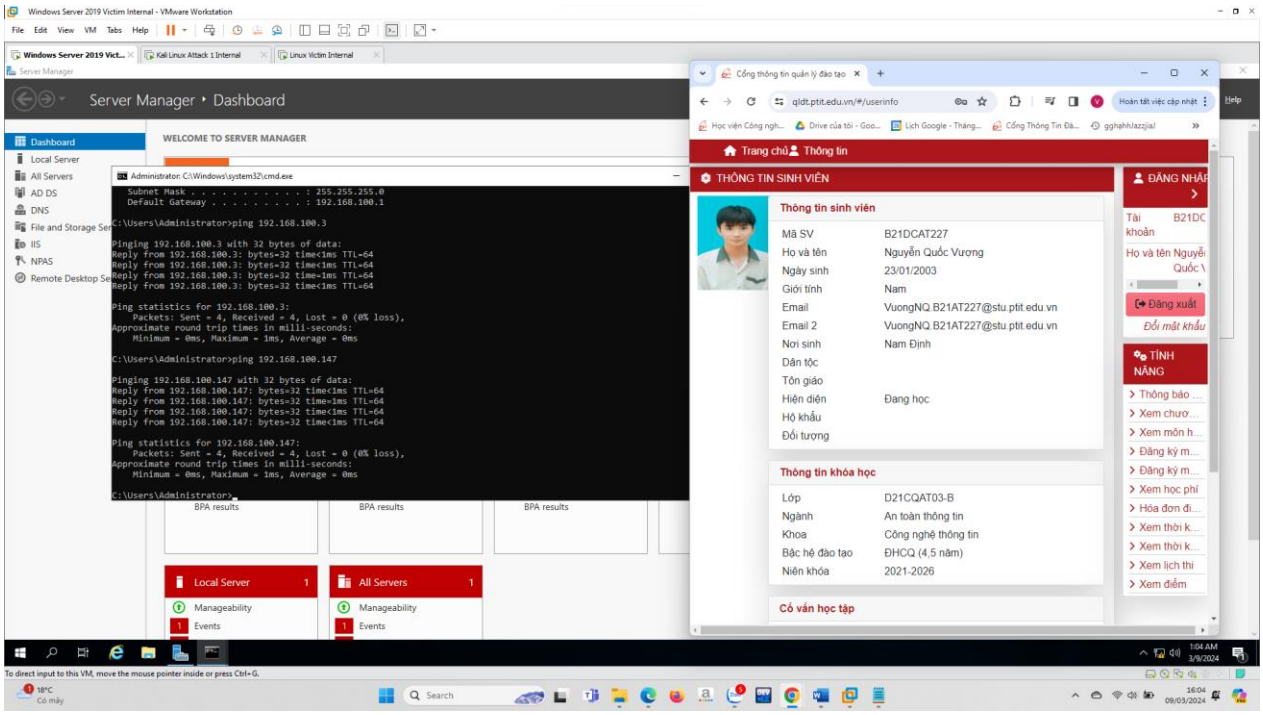
Cài đặt các máy mạng Internal:

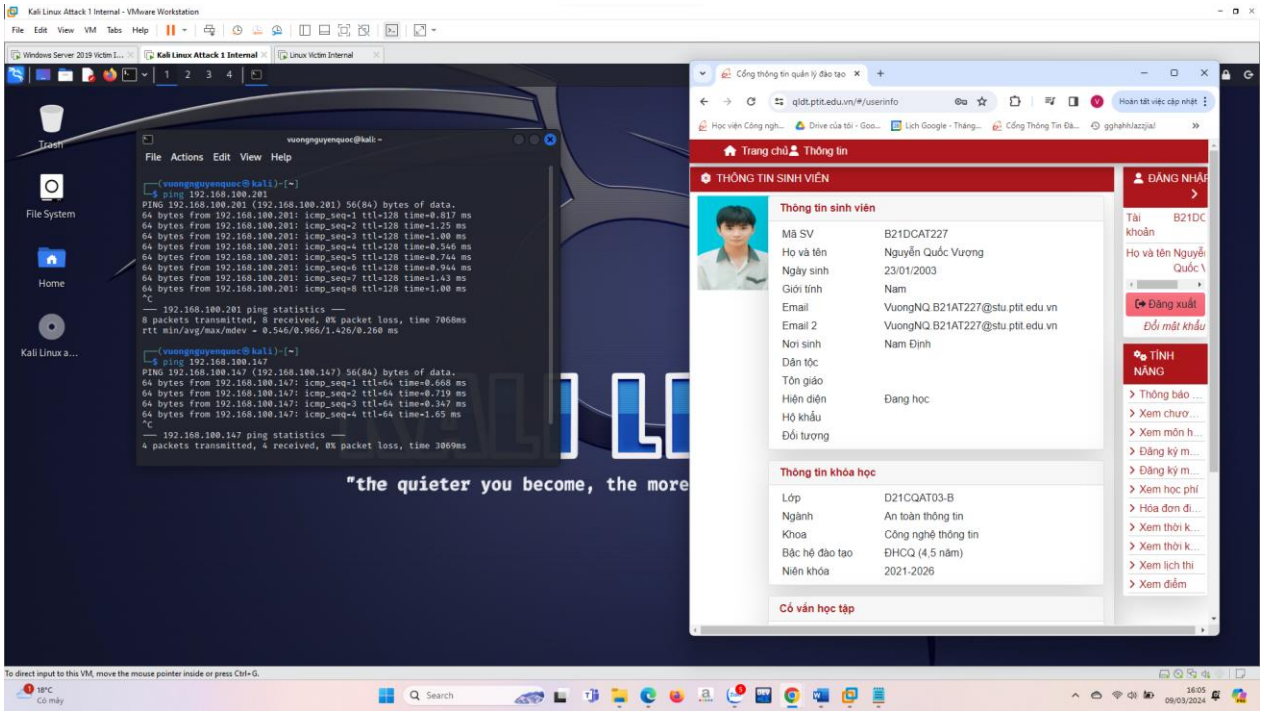


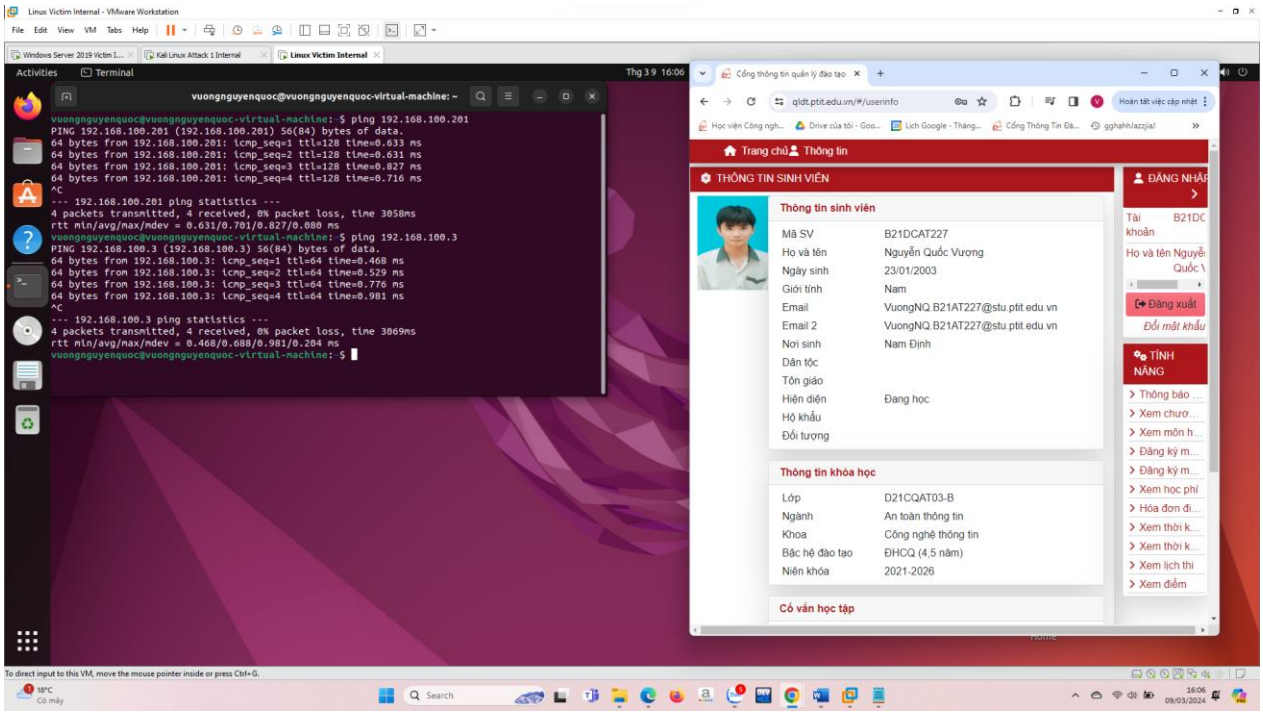




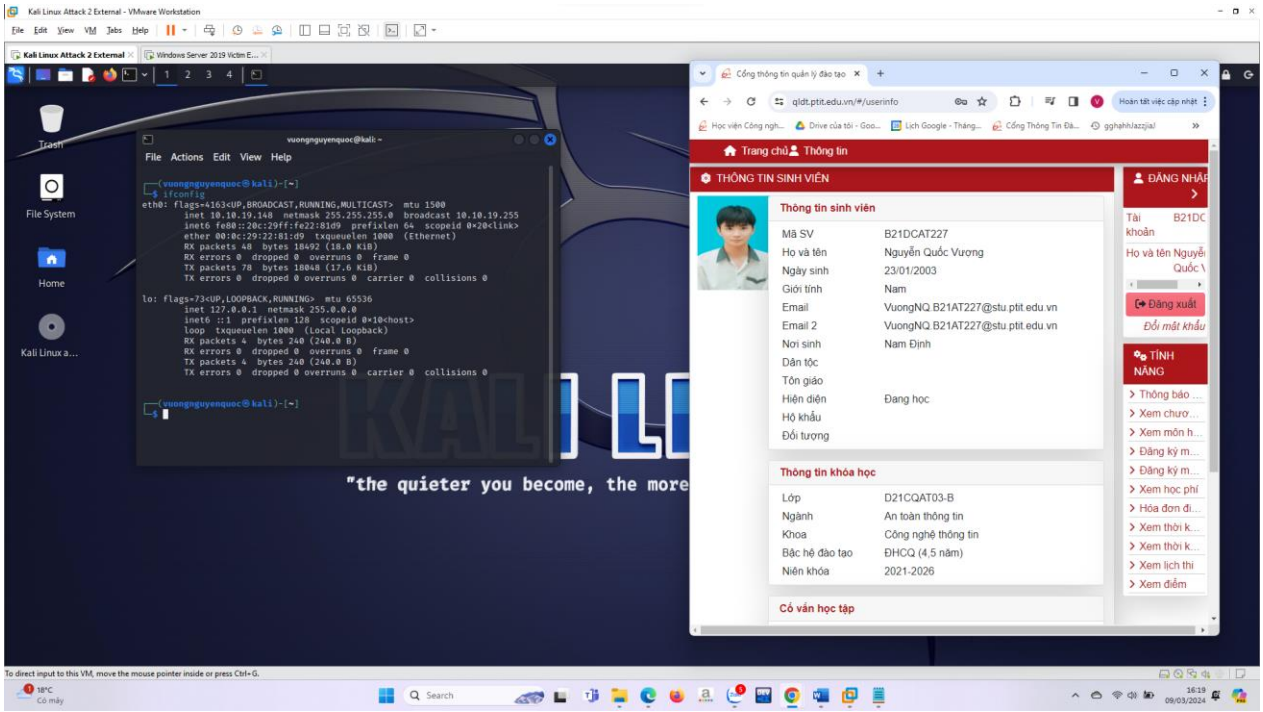
Các máy trong mạng Internal ping thông được với nhau:

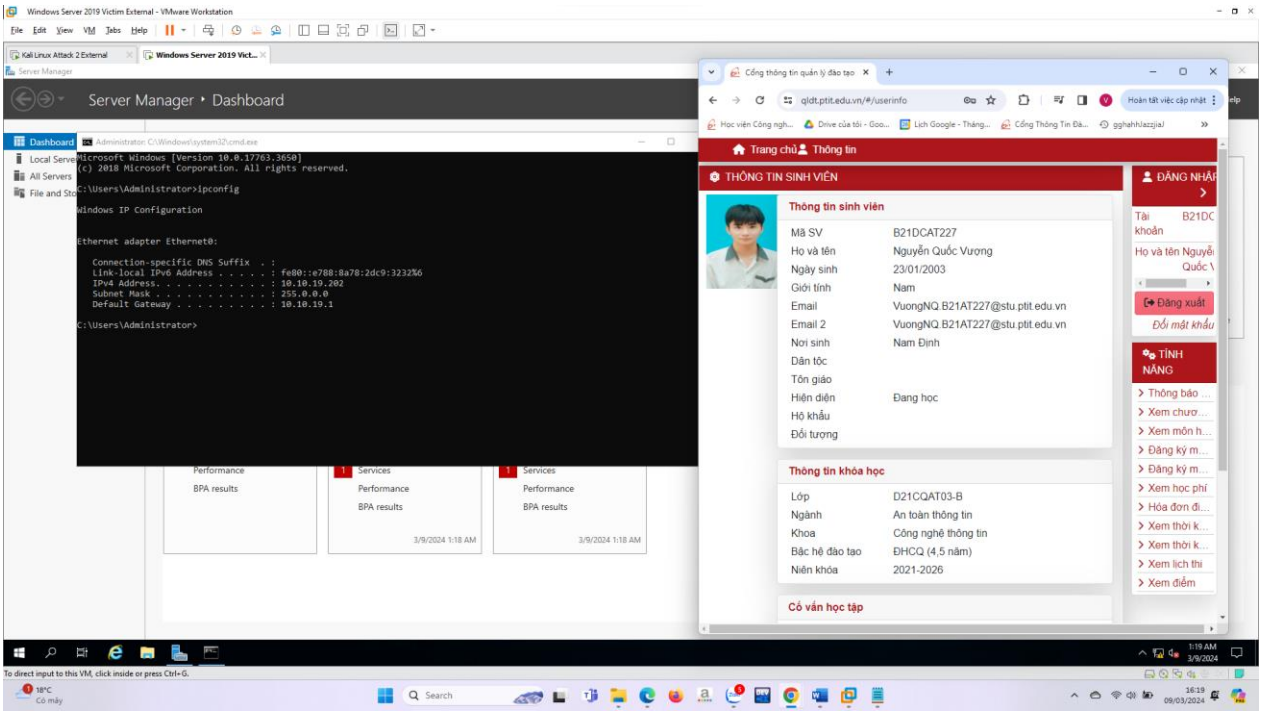

Windows Server 2019 Victim Internal - VMware Workstation
Server Manager • Dashboard
WELCOME TO SERVER MANAGER
Administrator: C:\Windows\system32\cmd.exe
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
C:\Users\Administrator>ping 192.168.100.3
Pinging 192.168.100.3 with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time<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 = 1ms, Average = 0ms
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
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>
BPA results
Local Server
All Servers
Manageability
Events
Trang chủ Thông tin
THÔNG TIN SINH VIÊN
Thông tin sinh viên
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vương
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Dân tộc
Tôn giáo
Hiện diện Đang học
Hộ khẩu
Đối tượng
Thông tin khóa học
Lớp D21CQAT03-B
Ngành An toàn thông tin
Khoa Công nghệ thông tin
Bậc hệ đào tạo ĐHCQ (4,5 năm)
Niên khóa 2021-2026
Cố vấn học tập
ĐĂNG NHẬP
Đăng xuất
Đổi mật khẩu
TÍNH NĂNG


Kali Linux Attack 1 Internal - VMware Workstation
Trash
File System
Home
Kali Linux a...
vuongnguyenquoc@kali: ~
File Actions Edit View Help
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=0.817 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=1.25 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=128 time=1.00 ms
64 bytes from 192.168.100.201: icmp_seq=4 ttl=128 time=0.546 ms
64 bytes from 192.168.100.201: icmp_seq=5 ttl=128 time=0.744 ms
64 bytes from 192.168.100.201: icmp_seq=6 ttl=128 time=0.944 ms
64 bytes from 192.168.100.201: icmp_seq=7 ttl=128 time=1.43 ms
64 bytes from 192.168.100.201: icmp_seq=8 ttl=128 time=1.00 ms
^C
— 192.168.100.201 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7068ms
rtt min/avg/max/mdev = 0.546/0.966/1.426/0.260 ms
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=0.668 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=0.719 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=0.347 ms
64 bytes from 192.168.100.147: icmp_seq=4 ttl=64 time=1.65 ms
^C
— 192.168.100.147 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
"the quieter you become, the more
Trang chủ Thông tin
THÔNG TIN SINH VIÊN
Thông tin sinh viên
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vương
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Thông tin khóa học
Lớp D21CQAT03-B
Ngành An toàn thông tin
Khoa Công nghệ thông tin
Bậc hệ đào tạo ĐHCQ (4,5 năm)
Niên khóa 2021-2026
Cố vấn học tập
ĐĂNG NHẬP
Đăng xuất
Đổi mật khẩu
TÍNH NĂNG

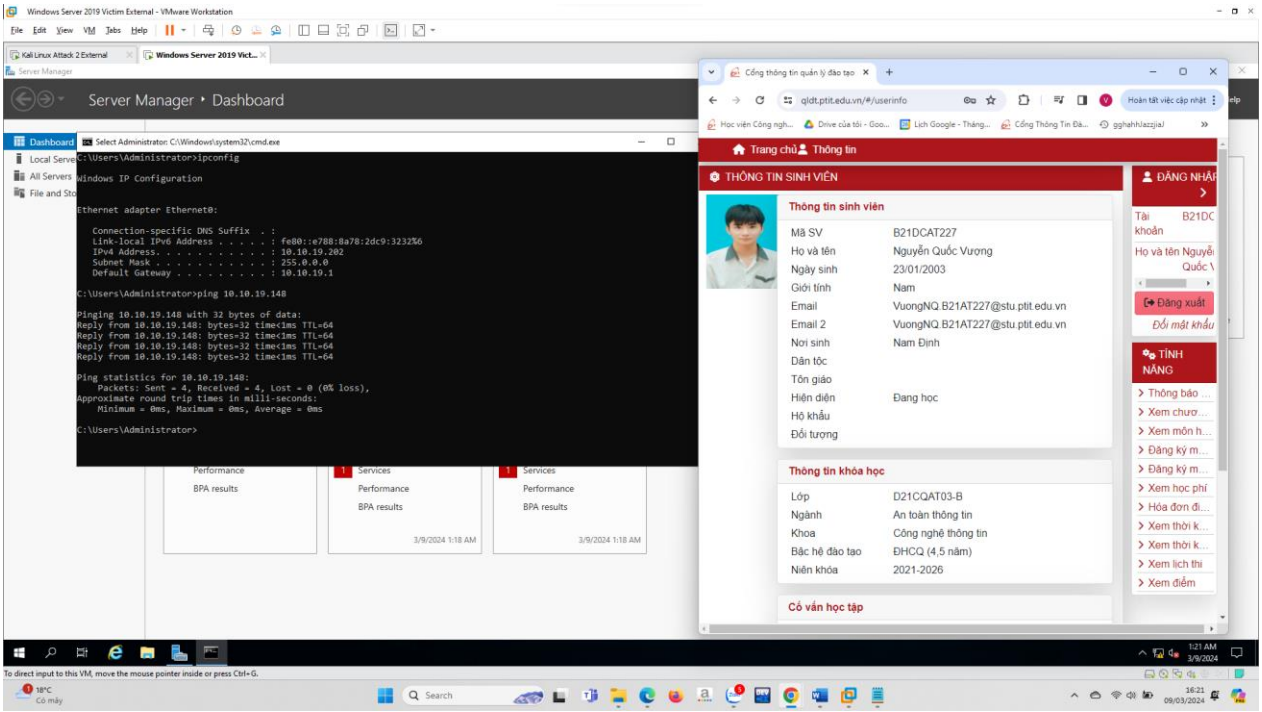


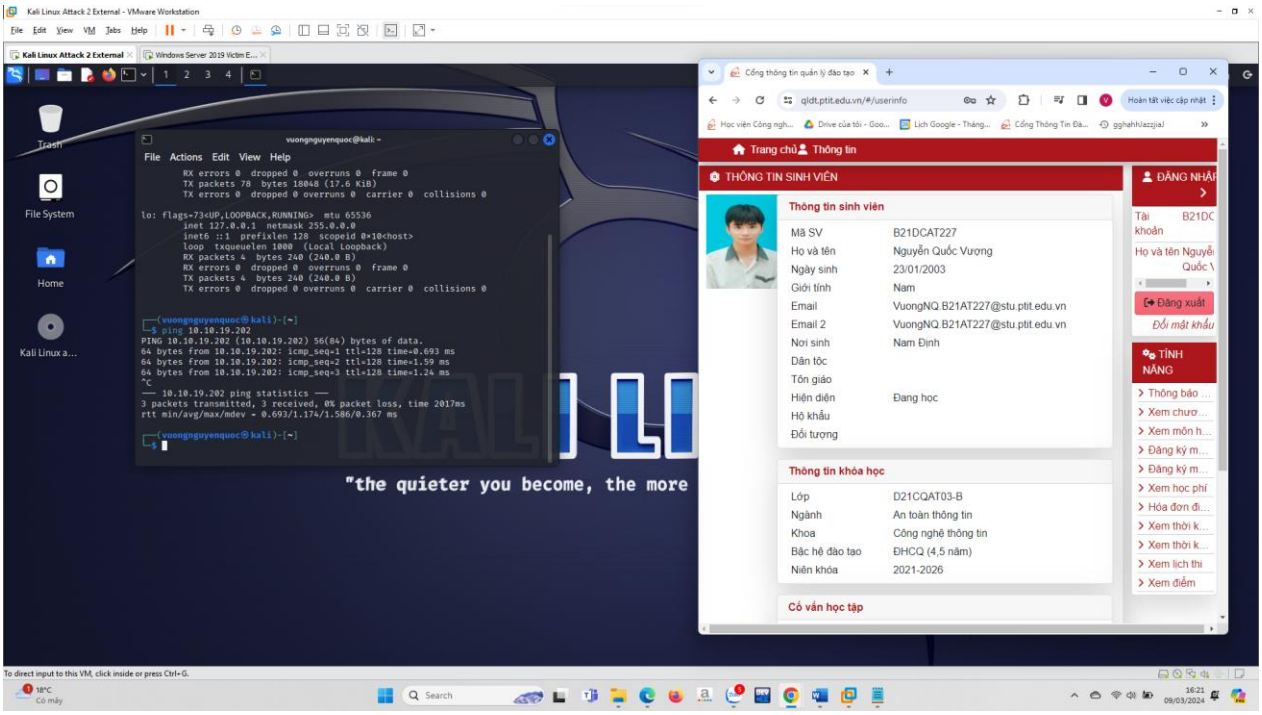
Cài đặt các máy mạng External:





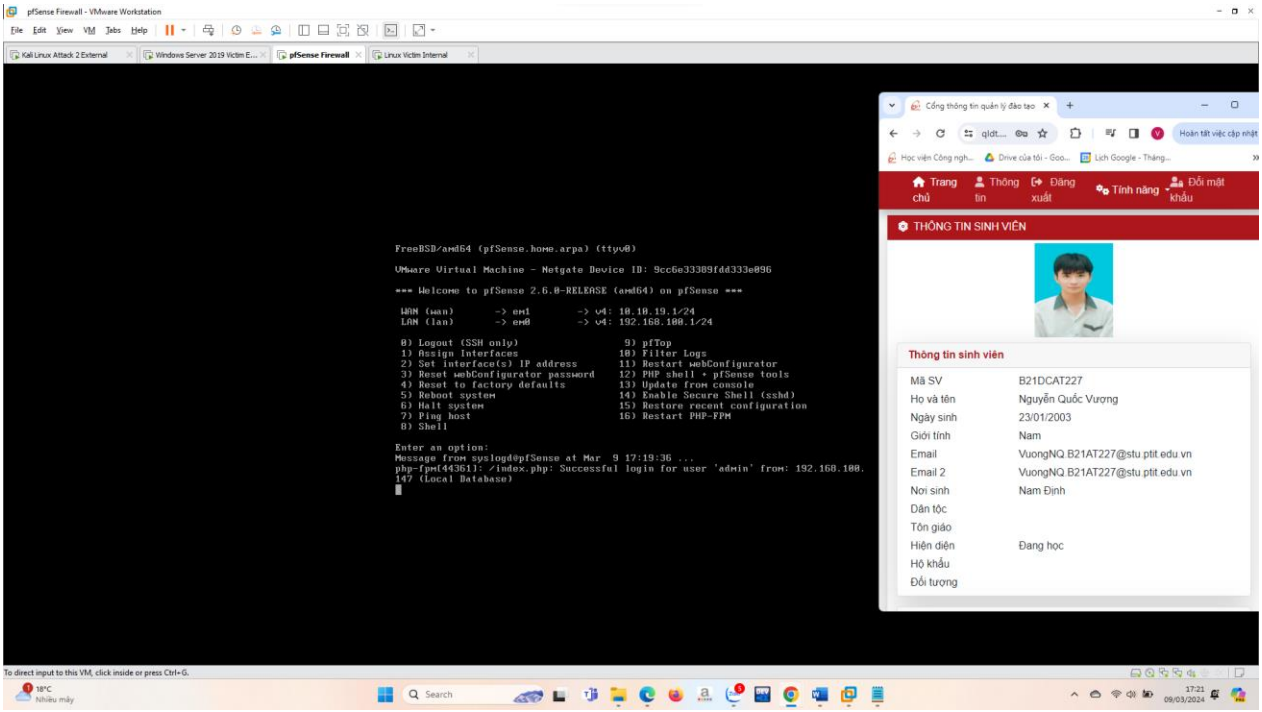
Các máy trong mạng External ping thông với nhau:





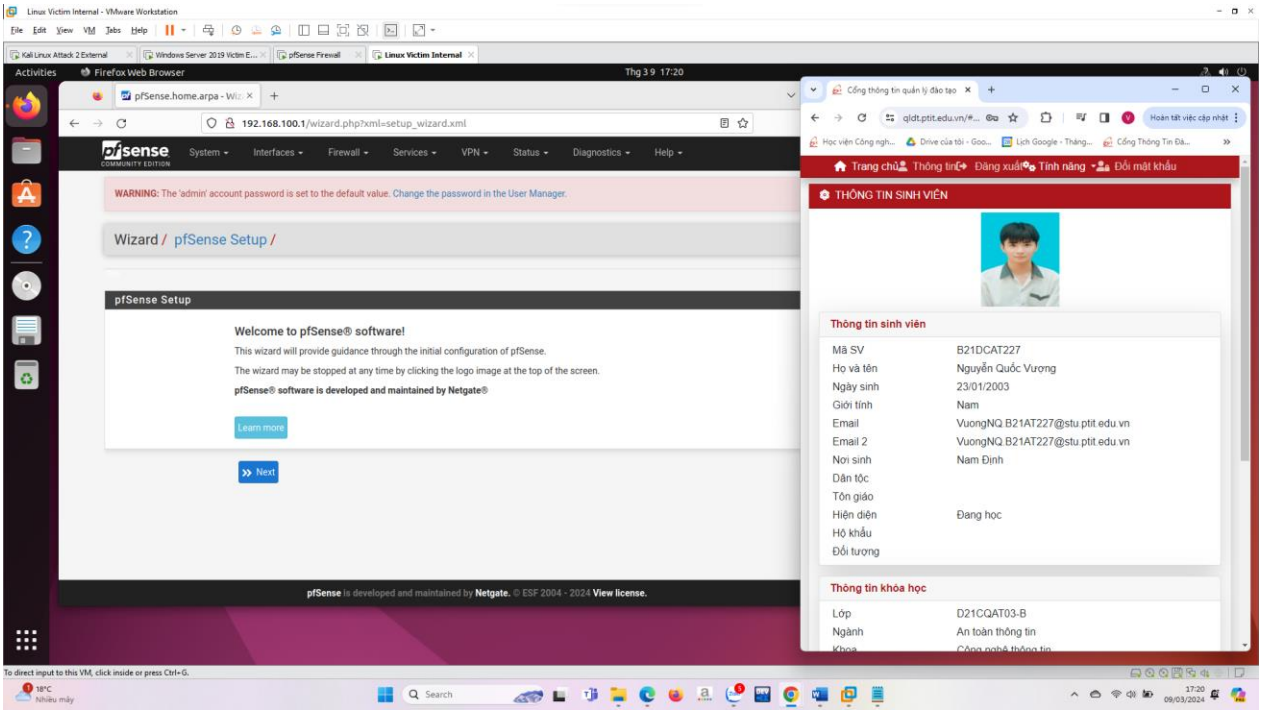
1.2.3.2 Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

Cài đặt thành công pfsense:

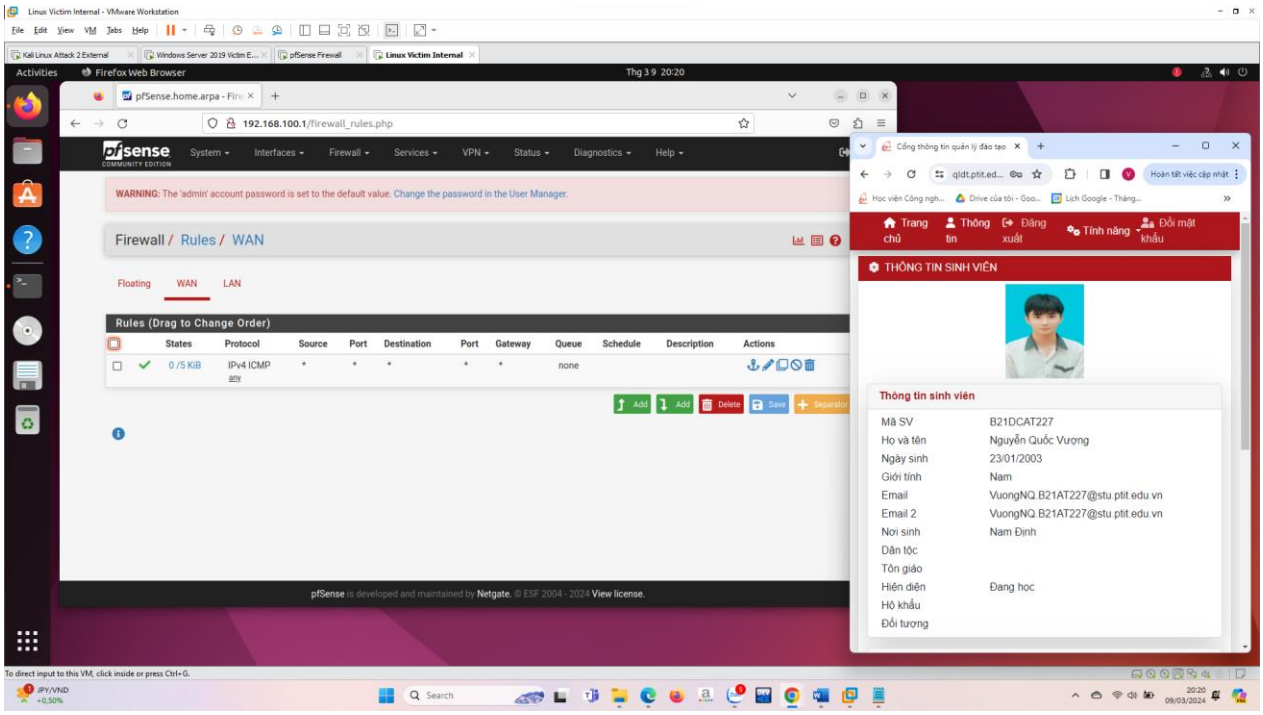


a) Cấu hình ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal. Các bước lần lượt như sau:

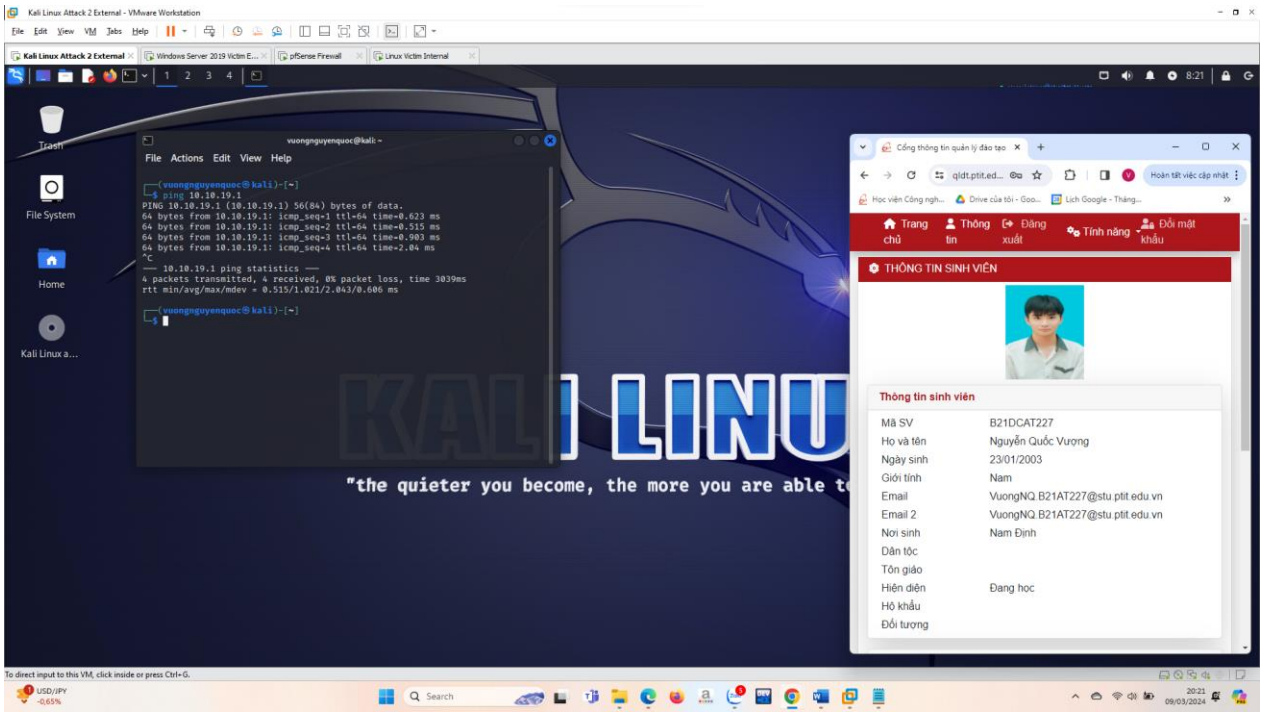
- Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình pfsense qua giao diện web.



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



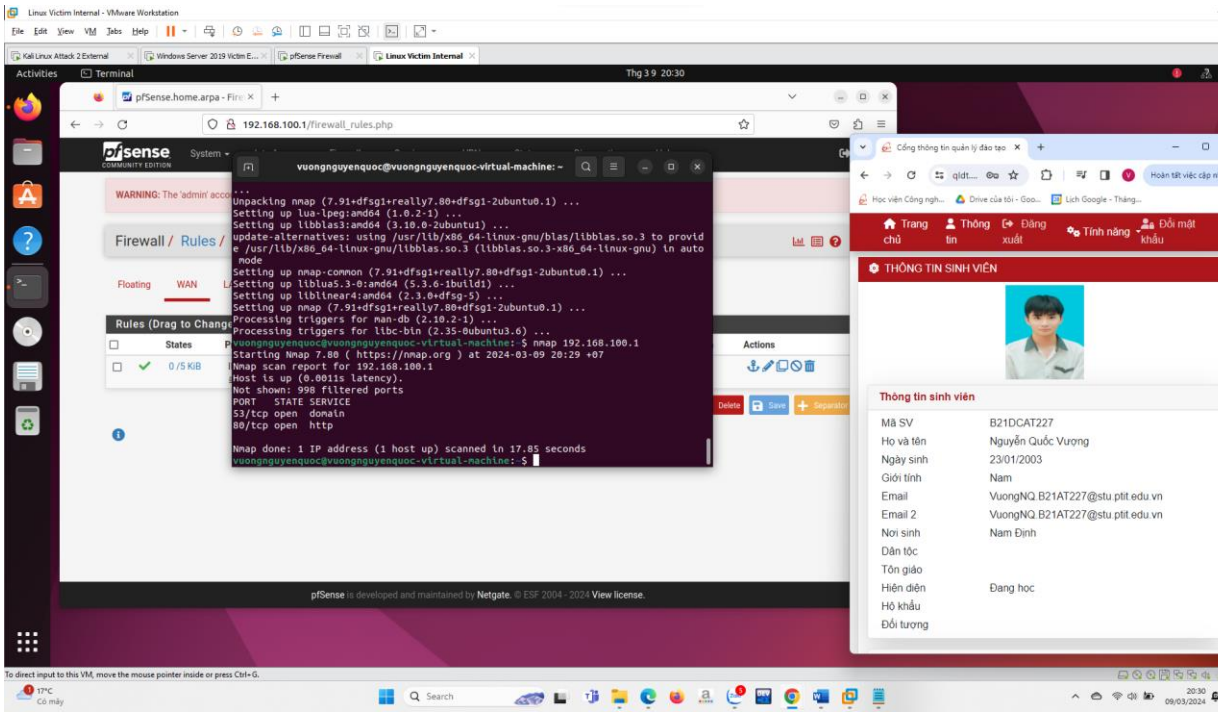
- Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài.



- Trả lời câu hỏi:

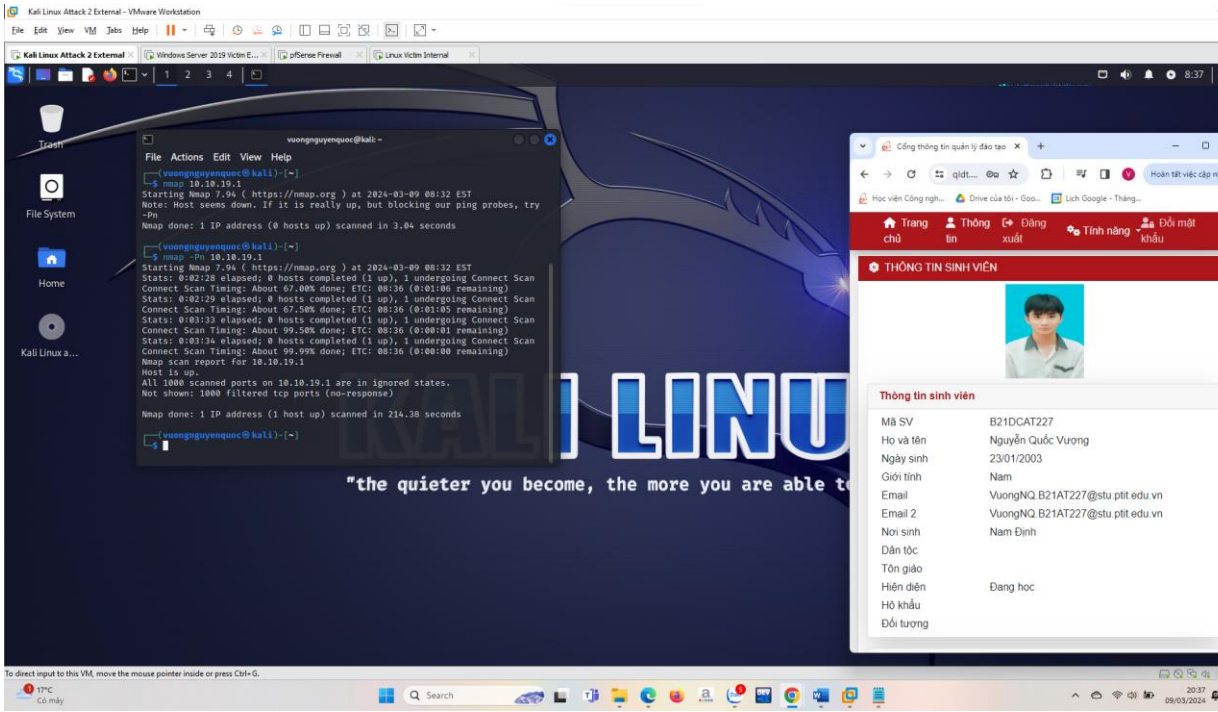
  - Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng trong của pfSense?

Xem và kiểm tra: nmap 192.168.100.1



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

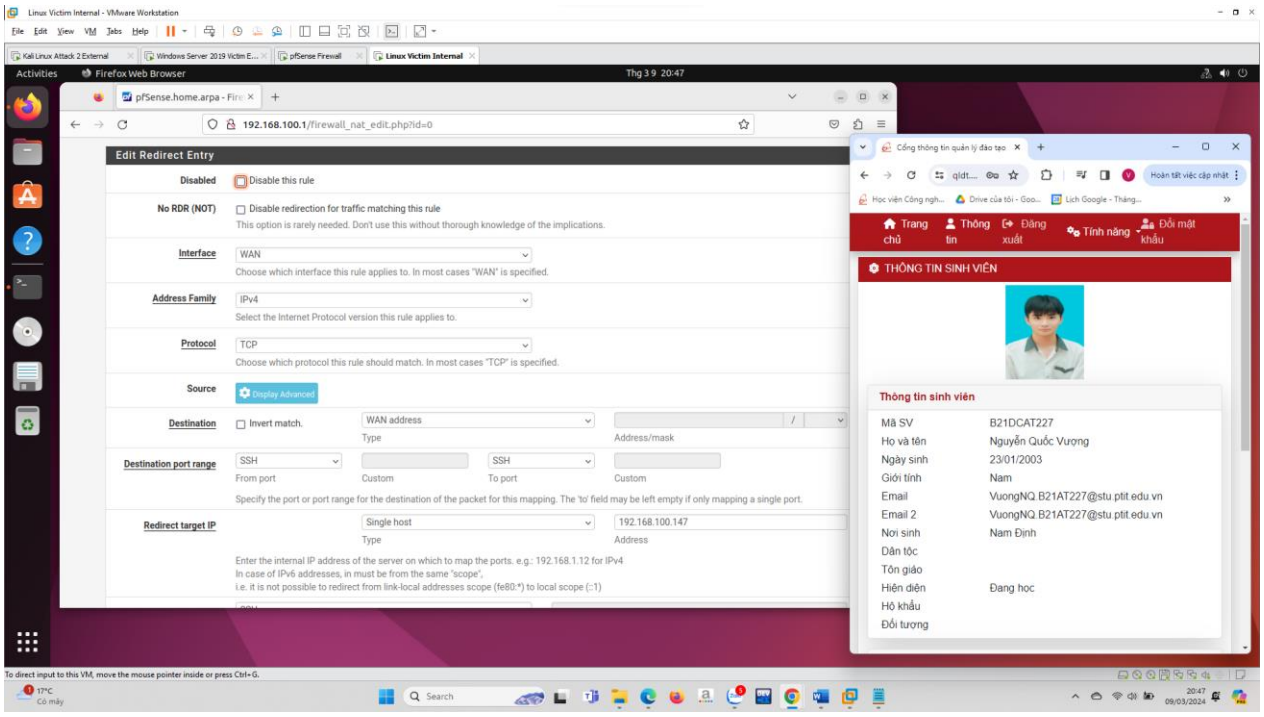
Xem và kiểm tra: nmap -Pn 10.10.19.1

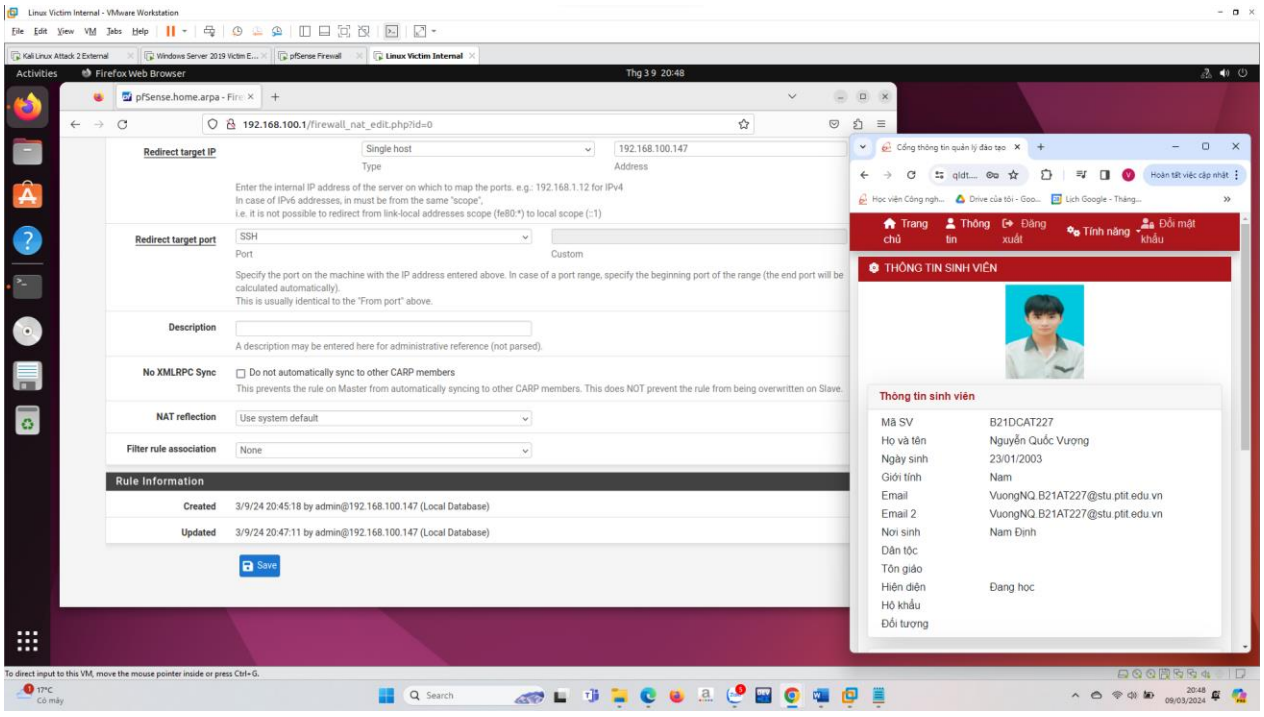


1.2.3.3 Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

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

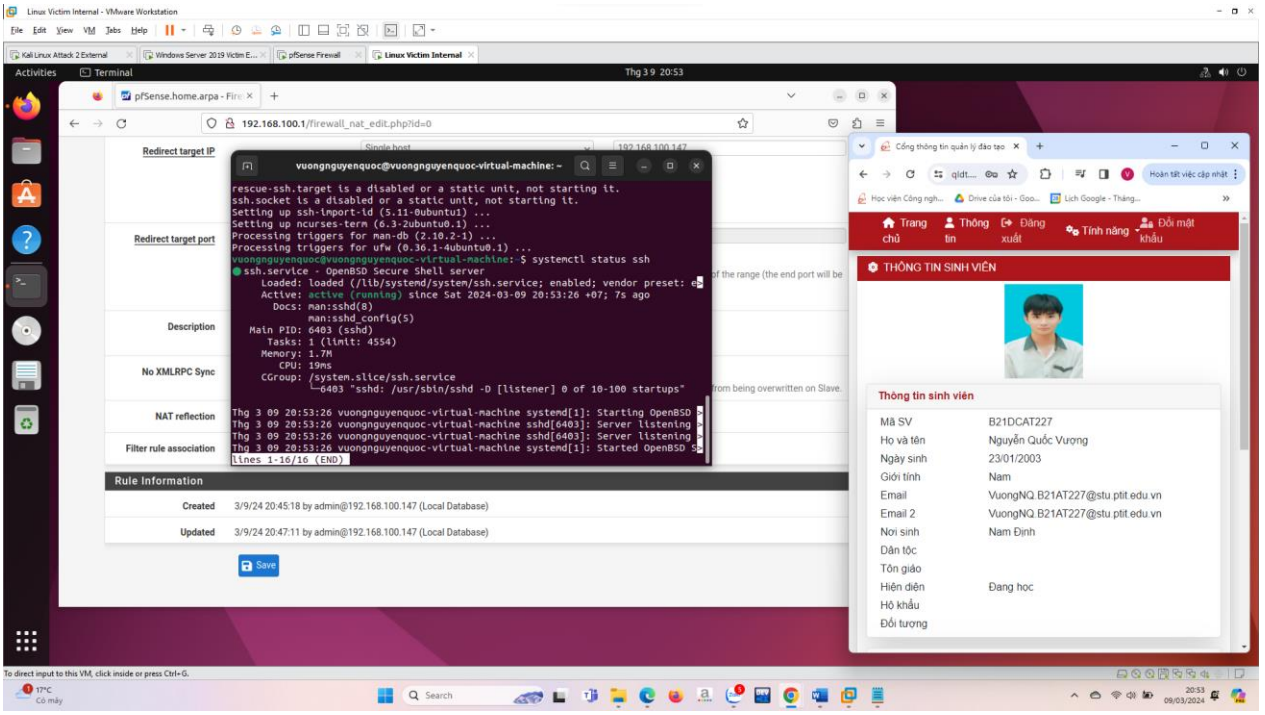
- Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình NAT trên pfsense qua giao diện web.



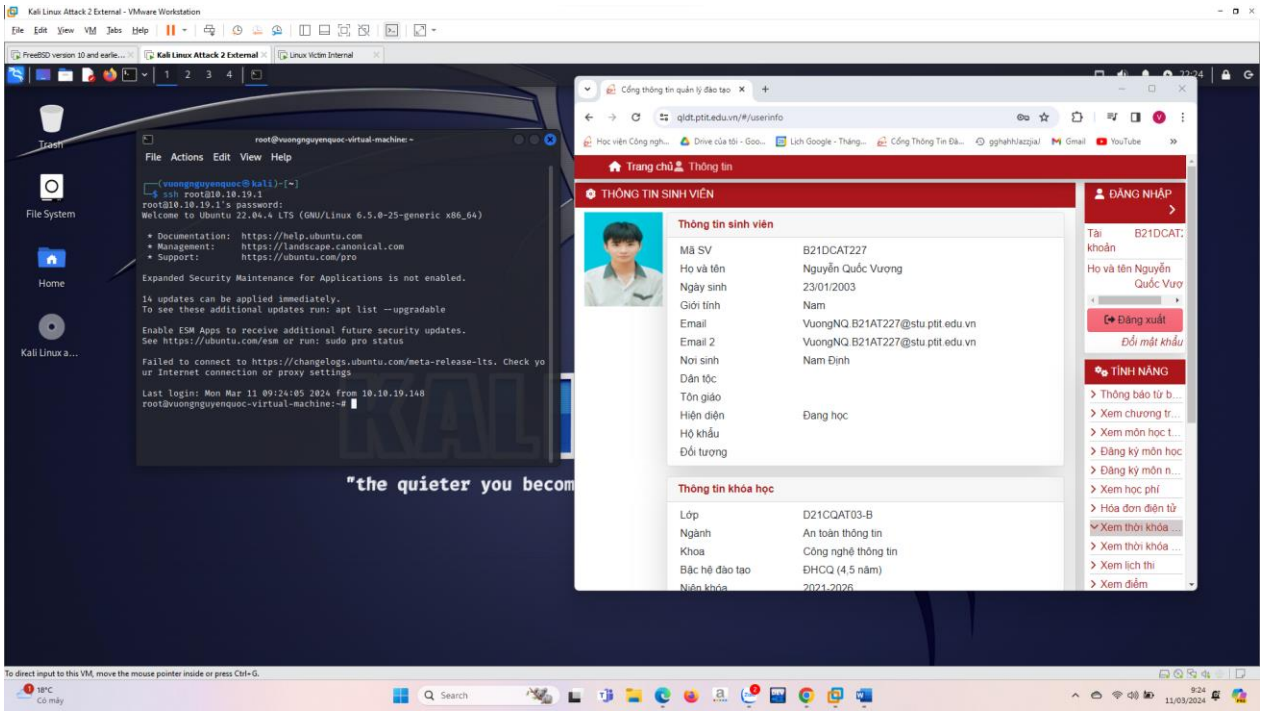


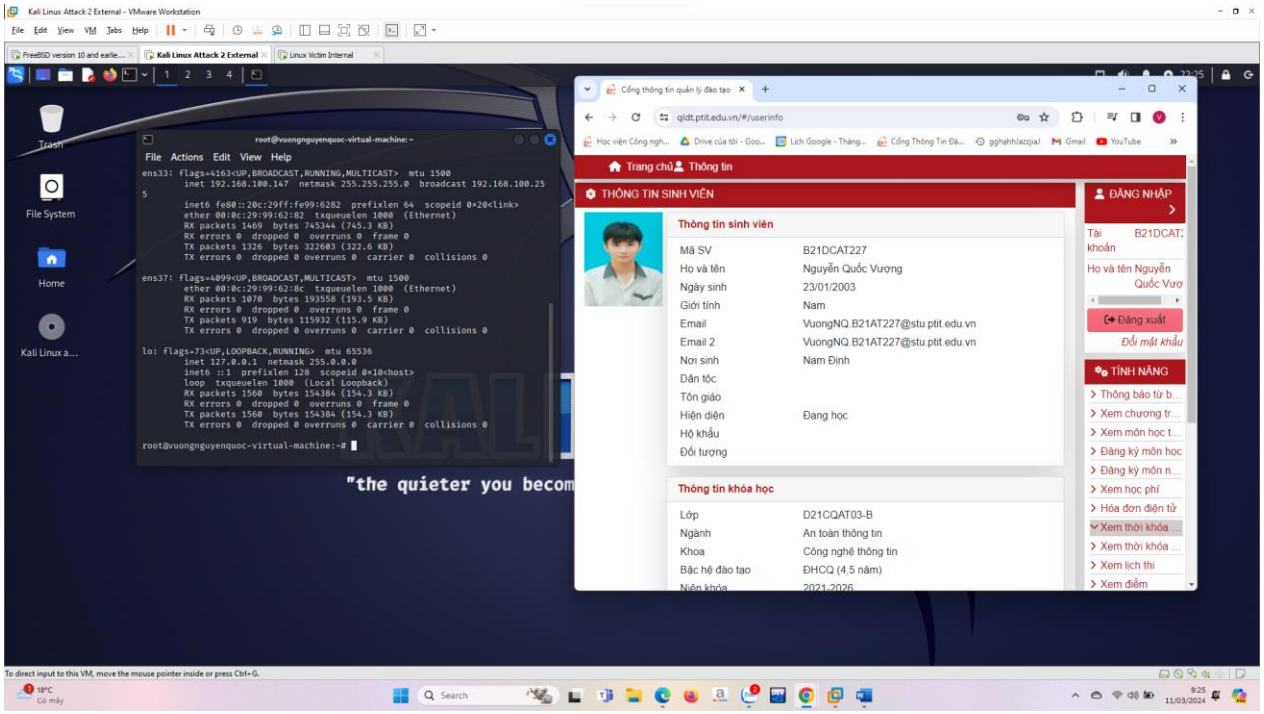
- Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy Linux victim mạng Internal) được truy cập từ bên ngoài thông qua port forwarding.

  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.

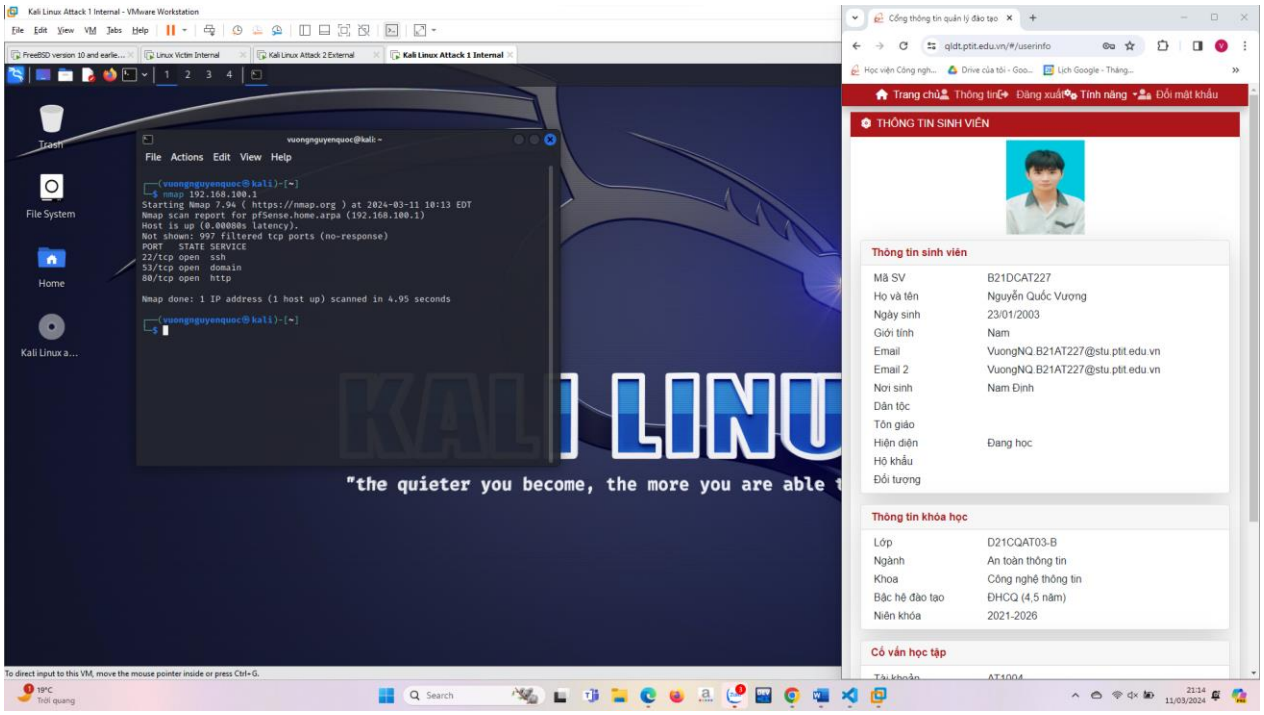


- Kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?





- 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


Kali Linux Attack 1 Internal - VMware Workstation
File Edit View VM Tabs Help
FreeBSD version 10 and earlie...
Linux Victim Internal
Kali Linux Attack 2 External
Kali Linux Attack 1 Internal
Trash
File System
Home
Kali Linux a...
vuongnguyenquoc@kali: ~
File Actions Edit View Help
(vuongnguyenquoc㉿kali)-[~]
$ nmap 192.168.100.1
Starting Nmap 7.94 (https://nmap.org) at 2024-03-11 10:13 EDT
Nmap scan report for pfSense.home.arpa (192.168.100.1)
Host is up (0.00080s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
(vuongnguyenquoc㉿kali)-[~]
$
"the quieter you become, the more you are able
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
19°C
Trời quang
Search
21:14
11/03/2024
Cổng thông tin quản lý đào tạo
qldt.ptit.edu.vn/#/userinfo
Trang chủ
Thông tin
Đăng xuất
Tính năng
Đổi mật khẩu
THÔNG TIN SINH VIÊN
Thông tin sinh viên
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vượng
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Dân tộc
Tôn giáo
Hiện diện Đang học
Hộ khẩu
Đối tượng
Thông tin khóa học
Lớp D21CQAT03-B
Ngành An toàn thông tin
Khoa Công nghệ thông tin
Bậc hệ đào tạo ĐHCQ (4,5 năm)
Niên khóa 2021-2026
Cố vấn học tập