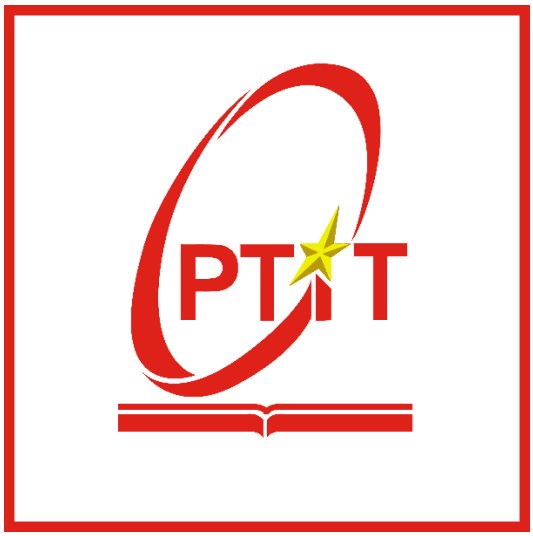
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 3

CÀI ĐẶT VÀ CẤU HÌNH UBUNTU SERVER

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 2/2024 ~

Mục Lục

BÀI 3: Cài đặt và cấu hình Ubuntu Server

1 Mục đích

Rèn luyện kỹ năng cài đặt và quản trị HĐH máy chủ Linux Server cho người dùng với các dịch vụ cơ bản.

2 Nội dung thực hành

2.1 Hệ điều hành ubuntu server

Hình 2.1: Hệ điều hành Ubuntu Server

- Là hệ điều hành dùng cho phía máy chủ, có thể cài đặt các dịch vụ phía máy chủ như: DNS, DHCP, Web, ...
- So sánh Ubuntu server với Ubuntu Desktop:

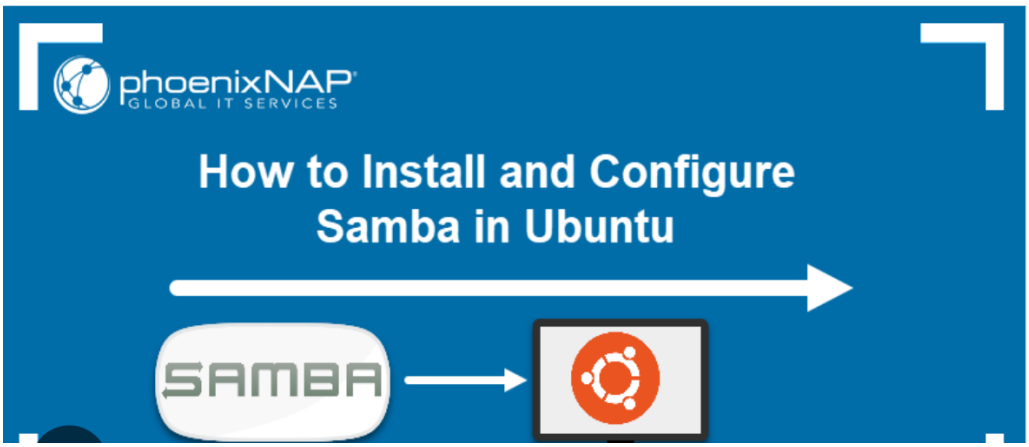
  Giống nhau:
  - Cả hai phiên bản Server và Desktop đều sử dụng cùng một kernel, có thể thêm bất kỳ gói nào vào một trong hai phiên bản.
  - Điều này có nghĩa là cho dù cài đặt mặc định có khác nhau, thì vẫn có thể tùy chỉnh phiên bản Ubuntu của mình sao cho phù hợp.

  Khác nhau:
  - Môi trường desktop: Trong khi Ubuntu Desktop bao gồm giao diện người dùng đồ họa, thì Ubuntu Server lại không có. Điều đó là vì hầu hết các máy chủ chạy mà không có GUI
  - Ứng dụng: Ubuntu Desktop chứa các ứng dụng phù hợp với mục đích sử dụng thông thường: Office, phần mềm đa phương tiện và trình duyệt web,…. Ubuntu Server cũng bao gồm các gói tiêu chuẩn. Chúng tập trung vào những

yêu cầu máy chủ, như máy chủ email, máy chủ file, máy chủ web và máy chủ samba

- Cài đặt: Cài đặt Ubuntu Desktop về cơ bản giống như cài bất kỳ phần mềm nào khác, còn Ubuntu Server sử dụng một menu điều khiển quá trình thay thế

2.2 Samba



Hình 2.2: Dịch vụ Samba

- Dịch vụ Samba trên Ubuntu là một phần mềm giúp chia sẻ tệp và máy in giữa các máy tính trong mạng thông qua giao thức SMB/CIFS (Server Message Block / Common Internet File System). Samba cho phép máy tính chạy hệ điều hành Ubuntu (hoặc bất kỳ hệ điều hành Linux nào) làm máy chủ để chia sẻ tài nguyên với các máy tính Windows, Linux hoặc macOS trong mạng LAN của bạn.

- Các tính năng chính của dịch vụ Samba bao gồm:

  - **Chia sẻ tệp**: Chia sẻ thư mục và tệp tin trên máy tính Ubuntu với máy tính khác trong mạng LAN
  - **Chia sẻ máy in**: Chia sẻ máy in nối với máy tính Ubuntu để chạy các máy tính khác có thể in qua mạng
  - **Quản lý quyền truy cập**: Samba cho phép quản lý quyền truy cập vào các tài nguyên chia sẻ, bao gồm cả quyền đọc, ghi, thực thi (w-r-x)
  - **Tích hợp với các hệ điều hành khác**: Samba hỗ trợ chia sẻ tài nguyên giữa các máy tính chạy Windows, Linux, macOS và các hệ điều hành khác.

- Nói gọn lại samba là một phần mệ miễn phí chủ yếu sử dụng để chia sẻ file giữa các nền tảng khác nhau như Windows và Linux bằng cách sử dụng giao thức SMB/CIFS.

2.3 SELinux

Hình 2.3: Hệ thống SELinux

- SELinux (Security-Enhanced Linux) là một hệ thống bảo mật được tích hợp sâu vào hệ điều hành Linux. Nó được phát triển bởi Cục Tình báo Quốc phòng Hoa Kỳ (NSA) và được phát hành dưới giấy phép mã nguồn mở. SELinux cung cấp một cơ chế kiểm soát truy cập dựa trên chính sách bảo mật để giữ cho hệ thống an toàn và đảm bảo tính toàn vẹn của dữ liệu.
- SELinux sử dụng một loạt các chính sách bảo mật để kiểm soát các hành động của các quy trình và người dùng trong hệ thống. Các chính sách này xác định quyền truy cập của các quy trình đối với các tài nguyên trong hệ thống như file, ổ đĩa và cổng kết nối mạng. Nó cũng theo dõi các hoạt động của các quy trình để phát hiện các hành vi đáng ngờ và ngăn chặn các cuộc tấn công từ các hacker hoặc phần mềm độc hại.
- Tuy nhiên, SELinux cũng có thể làm cho việc cấu hình và quản lý hệ thống trở nên phức tạp hơn đối với người quản trị hệ thống không có kinh nghiệm trong việc sử dụng SELinux.

Các chế độ SELinux

- SELinux có ba chế độ hoạt động chính: Enforcing, Permissive và Disabled. Mỗi chế độ có mục đích và tác động khác nhau đến việc kiểm soát truy cập của hệ thống
    - Enforcing mode: Đây là chế độ mặc định của SELinux. Trong chế độ này, SELinux sẽ kiểm soát và hạn chế các hành động của các quy trình và người dùng trên hệ thống dựa trên chính sách bảo mật đã được định nghĩa. Khi một hành động vi phạm chính sách được phát hiện, SELinux sẽ ghi log và ngăn chặn hoạt động đó. Chế độ Enforcing giúp bảo vệ hệ thống khỏi các cuộc tấn công và xâm nhập.
    - Permissive mode: Trong chế độ này, SELinux sẽ ghi log các hoạt động vi phạm chính sách, nhưng không ngăn chặn chúng. Chế độ Permissive được sử dụng

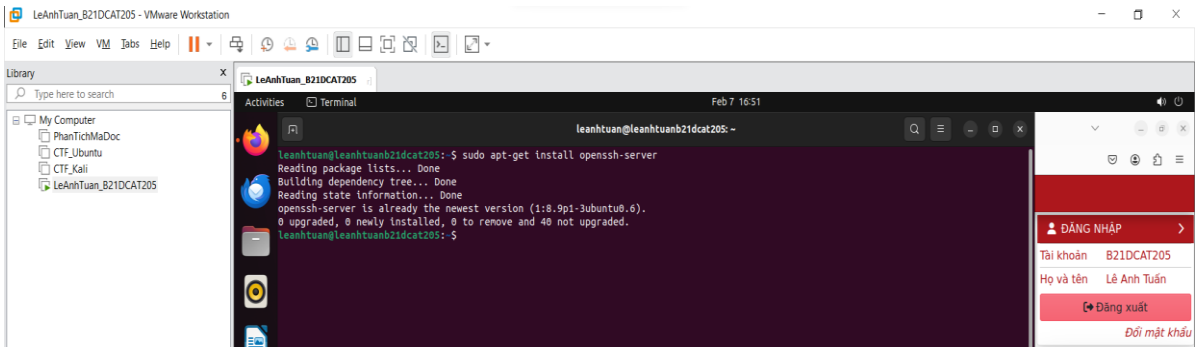
để giám sát các hoạt động của hệ thống và xác định các hoạt động mà các chính sách bảo mật cần được cập nhật hoặc điều chỉnh. Chế độ này cũng hữu ích để giảm thiểu các vấn đề tương thích và sửa lỗi SELinux trên hệ thống.

- Disabled mode: Trong chế độ này, SELinux không hoạt động và không có kiểm soát truy cập của SELinux trên hệ thống. Chế độ này được sử dụng khi người dùng muốn tắt hoặc gỡ bỏ SELinux hoặc khi cần tạm thời vô hiệu hóa SELinux để giải quyết các vấn đề tương thích. Tuy nhiên, việc sử dụng chế độ Disabled là không khuyến khích vì nó sẽ làm giảm tính toàn vẹn và bảo mật của hệ thống

3 Kết quả thực hành

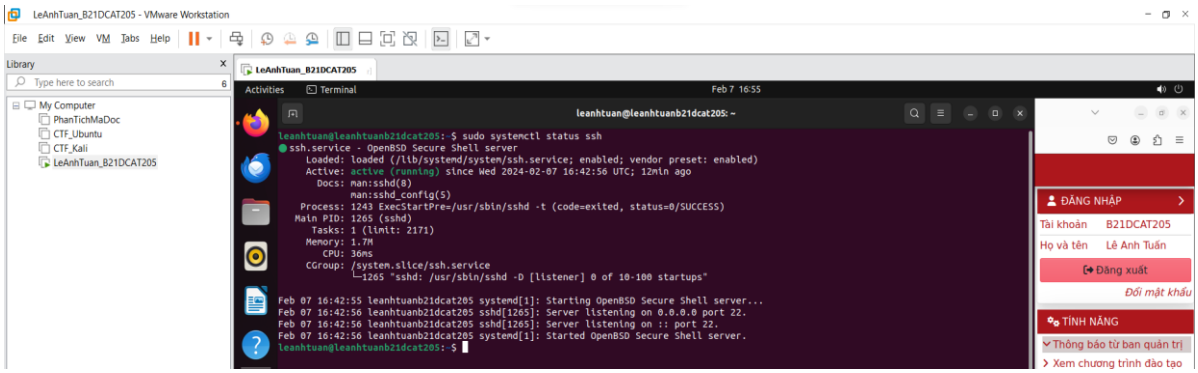
3.1 Cài đặt OpenSSH

Sử dụng câu lệnh **sudo apt-get install openssh-server** để tiến hành cài đặt



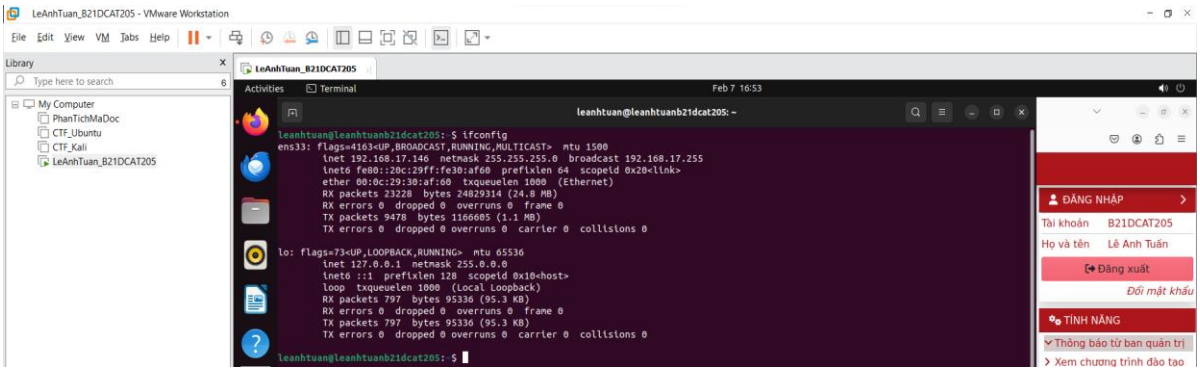
Hình 3.1: Cài đặt OpenSSH

Kiểm tra trạng thái ssh: **sudo systemctl status ssh**



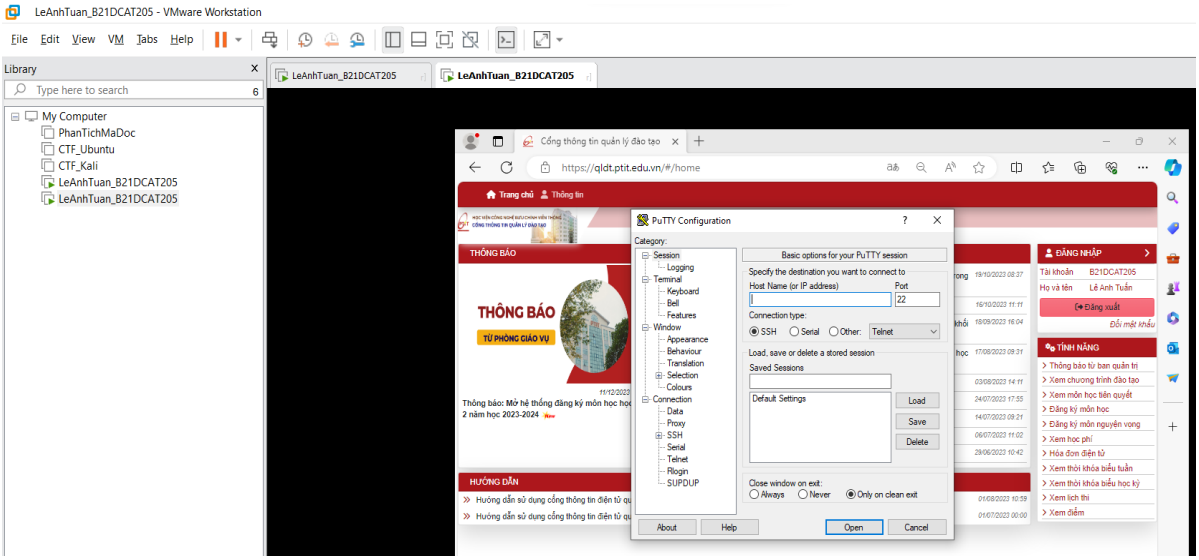
Hình 3.2: kiểm tra trạng thái ssh

Kiểm tra địa chỉ IP máy server với câu lệnh **ifconfig**



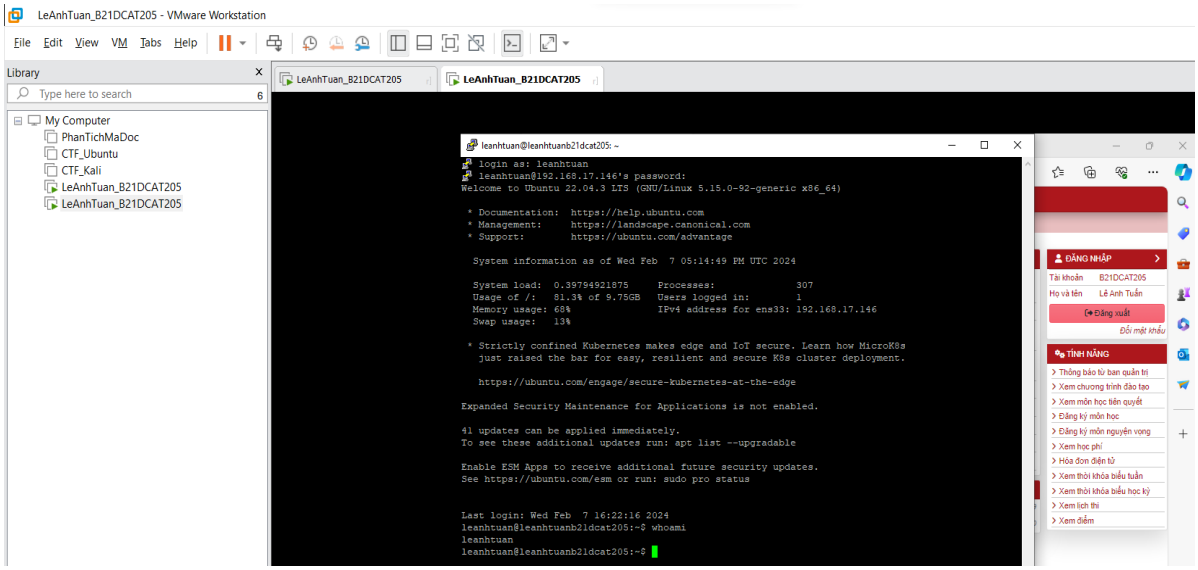
Hình 3.3: Địa chỉ IP là 192.168.17.146

Cài đặt thành công **Putty** trên máy trạm Windows 10.



Hình 3.4: Giao diện Putty

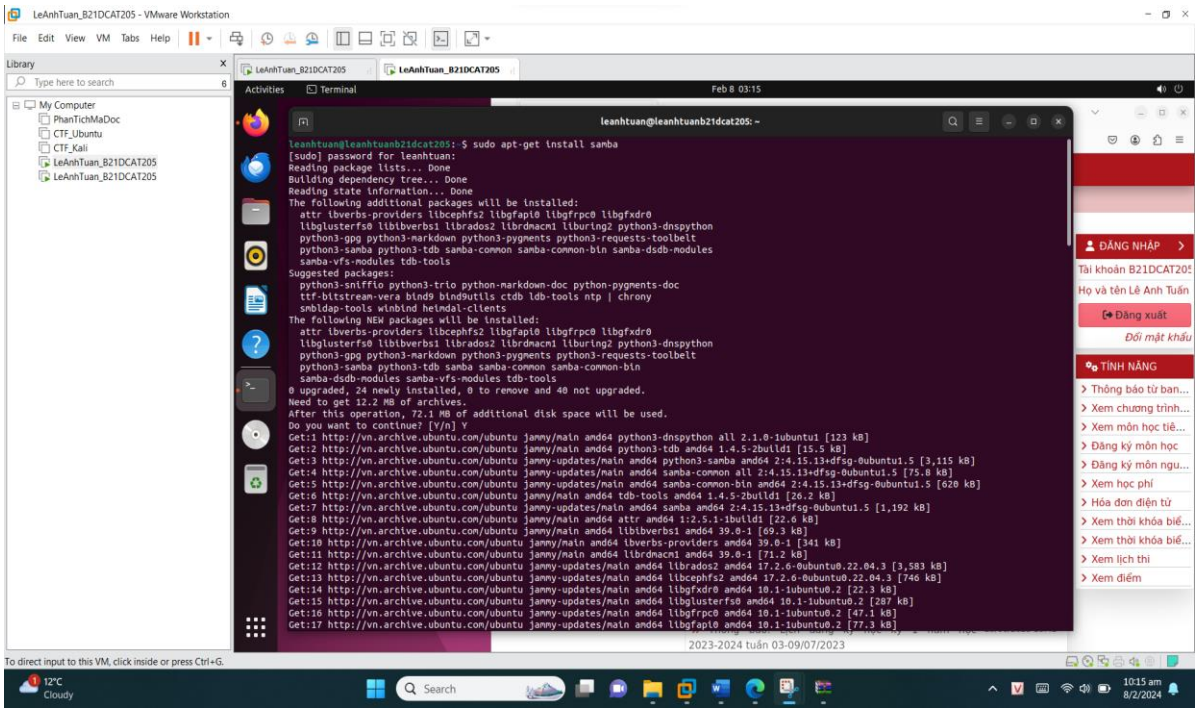
Dùng **Putty** truy cập vào địa chỉ Ip (của máy server vừa kiểm tra ở trên) là **192.168.17.146** truy cập thành công vào Ubuntu Server 22.04, kiểm tra lại bằng câu lệnh: **whoami**



Hình 3.5: Truy cập thành công vào Ubuntu Server 22.04

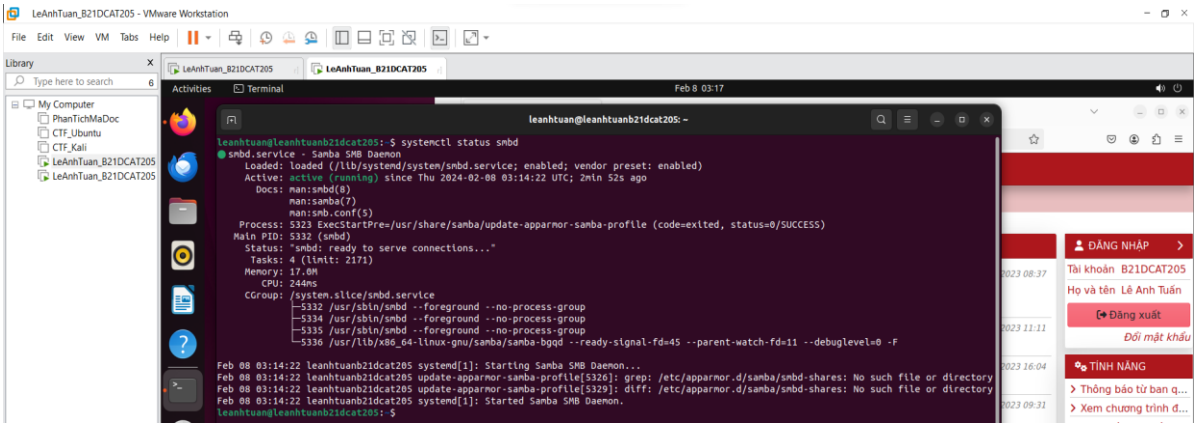
3.2 Cài đặt thành công Samba

Sử dụng câu lệnh: **sudo apt-get install samba** để cài đặt samba



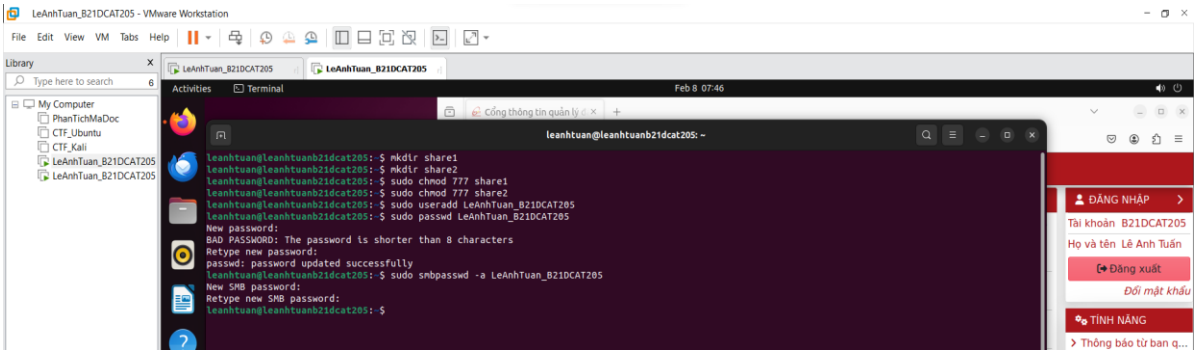
Hình 3.6: Cài đặt samba

Kiểm tra lại máy chủ samba hoạt động không: **systemctl status smbd**



Hình 3.7: Kiểm tra trạng thái máy chủ samba

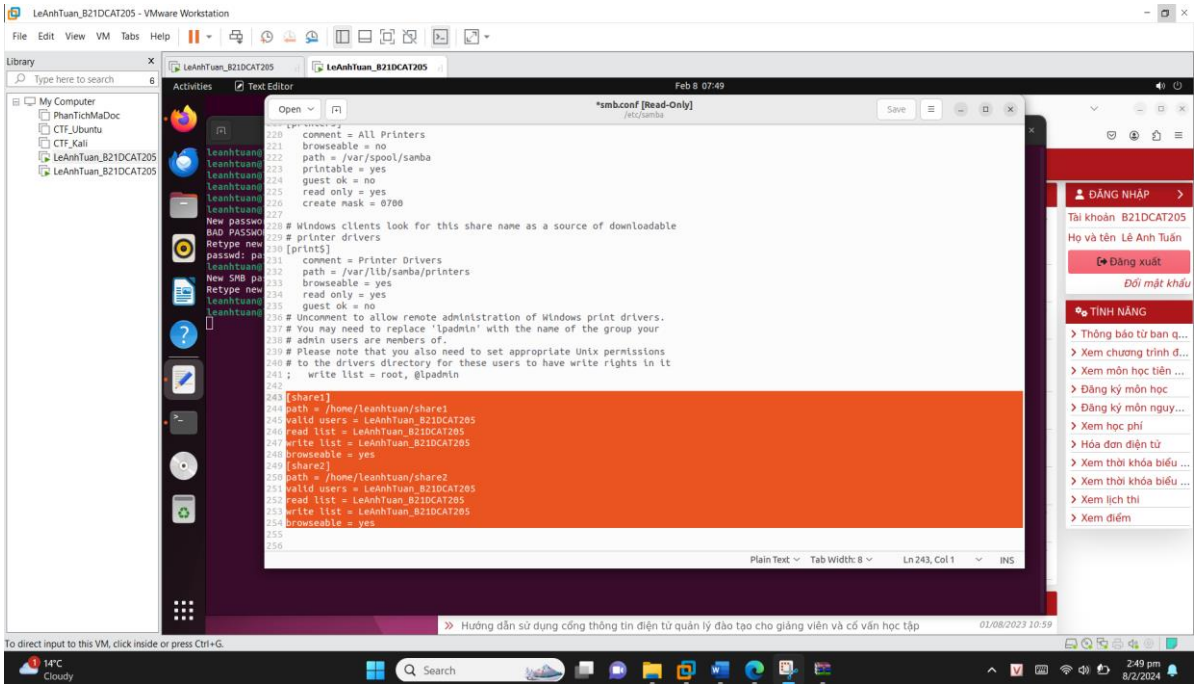
Tạo 2 thư mục **share1** và **share2** => tạo user **LeAnhTuan_B21DCAT205** và cài đặt mật khẩu cho user. => sử dụng câu lệnh **sudo smbpasswd -a LeAnhTuan_B21DCAT205** để cập nhật mật khẩu cho người dùng " **LeAnhTuan_B21DCAT205**" trong hệ thống Samba.



Hình 3.8: Tạo 2 folder, user và cập nhật user vào hệ thống Samba

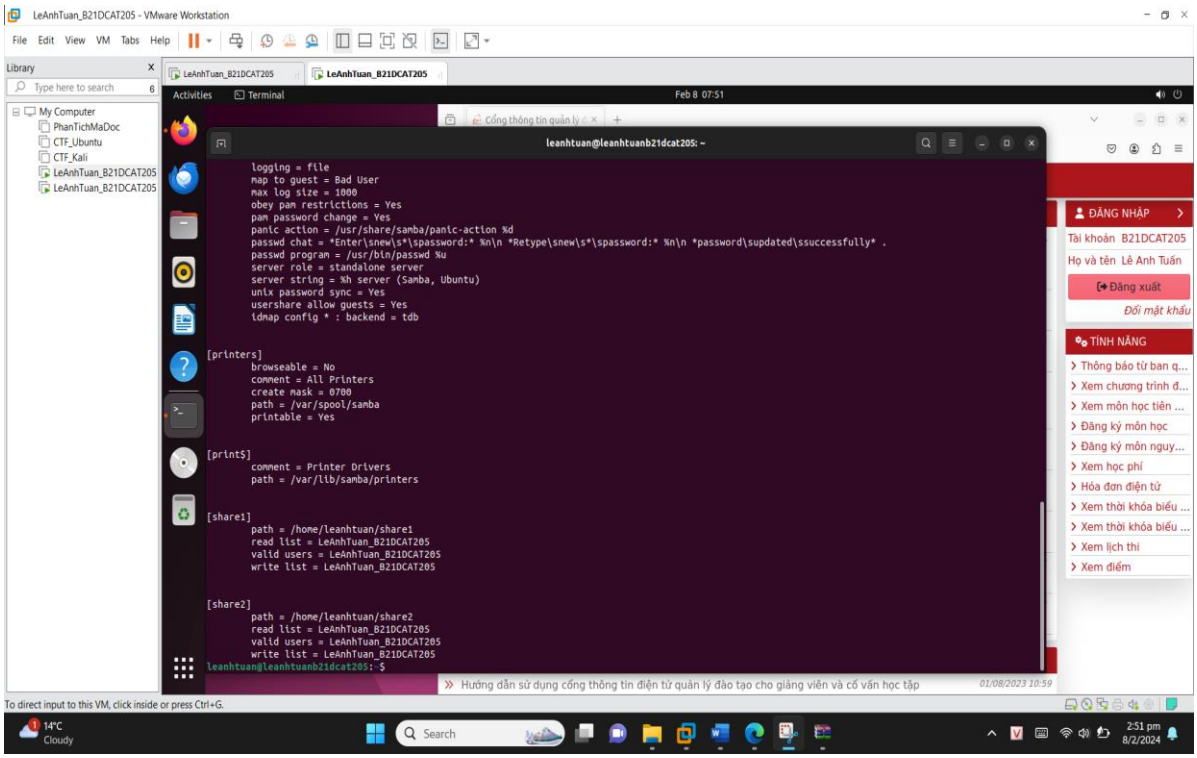
Dùng lệnh **sudo gedit /etc/samba/smb.conf** để chỉnh sửa các quyền truy cập file cho user vừa tạo:

- **path**: Xác định đường dẫn đến thư mục muốn chia sẻ.
- **valid users**: Chỉ định người dùng hoặc danh sách người dùng được phép truy cập chia sẻ.
- **read list**: Xác định danh sách người dùng được phép đọc (xem nội dung của thư mục).
- **write list**: Xác định danh sách người dùng được phép ghi (thay đổi, xóa tệp).
- **browseable**: Cho biết liệu chia sẻ có hiển thị trong danh sách khi người dùng duyệt qua mạng hay không. Nếu đặt là "yes", thì chia sẻ sẽ xuất hiện.



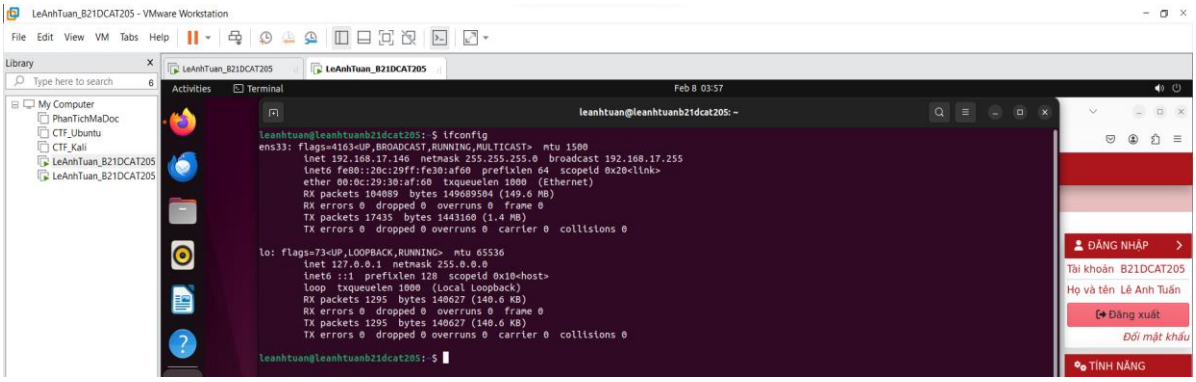
Hình 3.9: Chỉnh sửa quyền truy cập file

Dùng câu lệnh **sudo testparm** để kiểm tra lại:

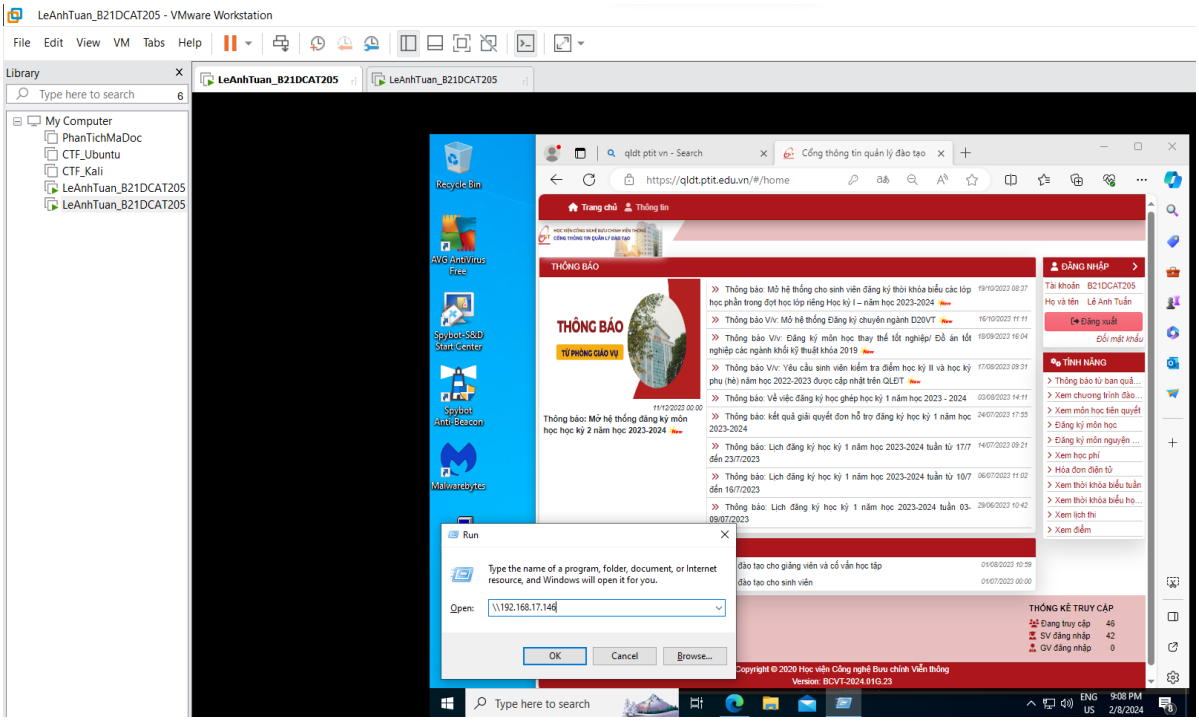


Hình 3.10: Kiểm tra lại với sudo testparm

Kiểm tra địa chỉ ip máy server và dùng máy windows và truy cập vào địa chỉ ip đó:

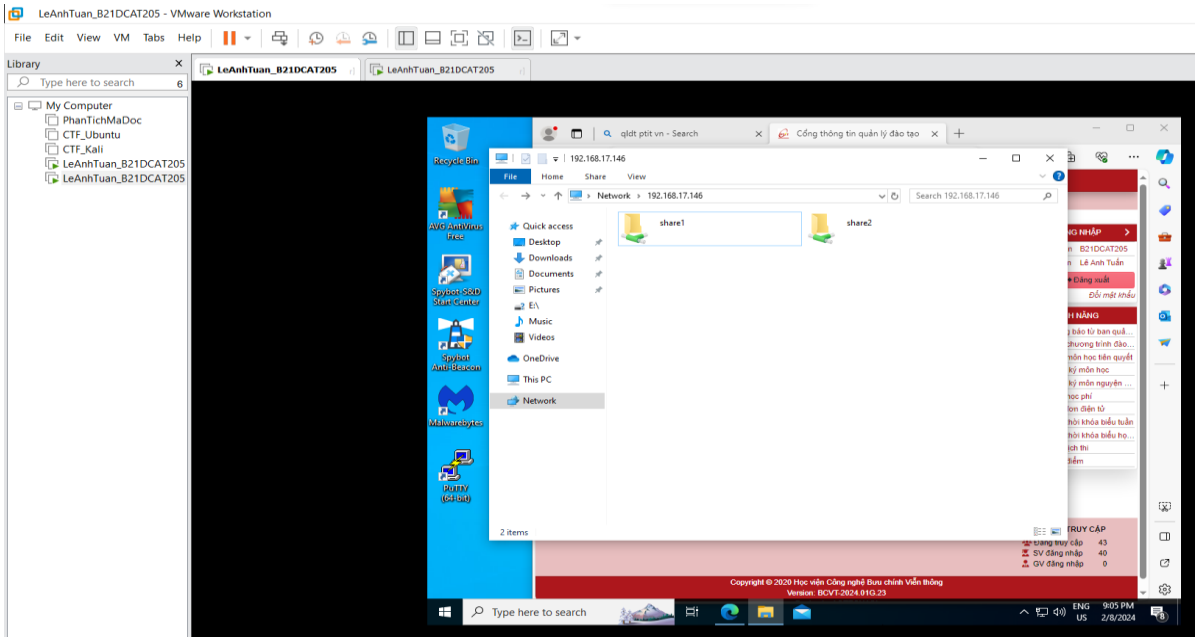


Hình 3.11: Địa chỉ IP máy server là 192.168.17.146.



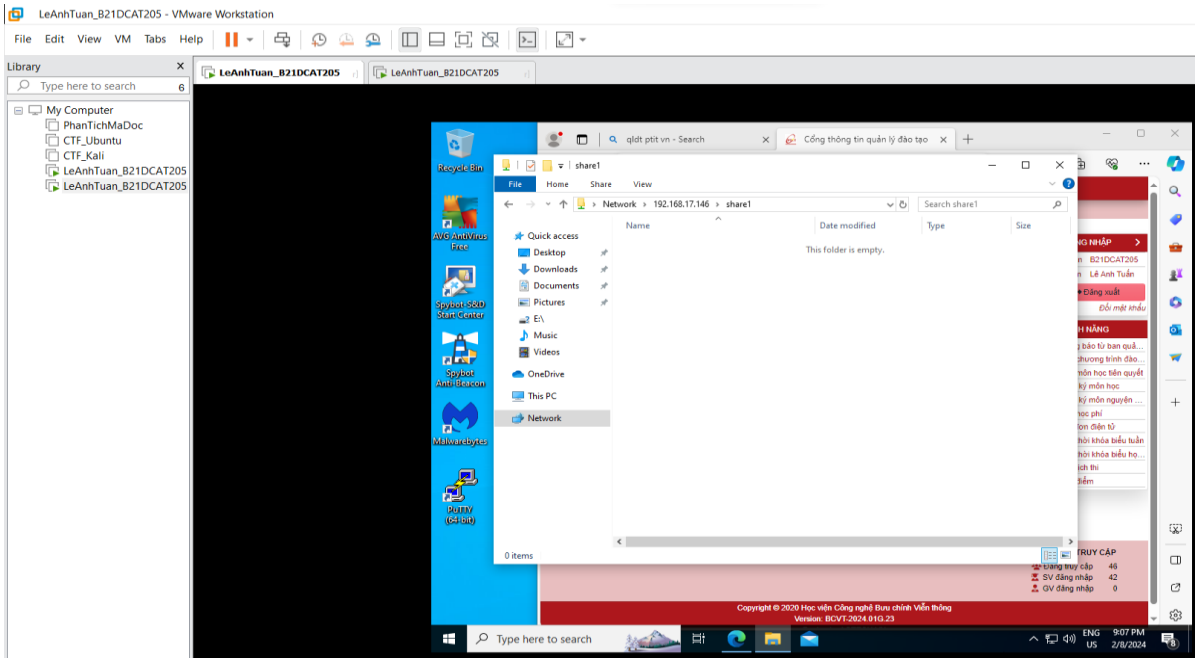
Hình 3.12: Sử dụng tổ hợp phím Windows+R và nhập như hình.

Chia sẻ file thành công từ máy Ubuntu Server đến máy Window 10.



Hình 3.13: Chia sẻ thành công 2 file từ máy Ubuntu Server sang máy Windows 10

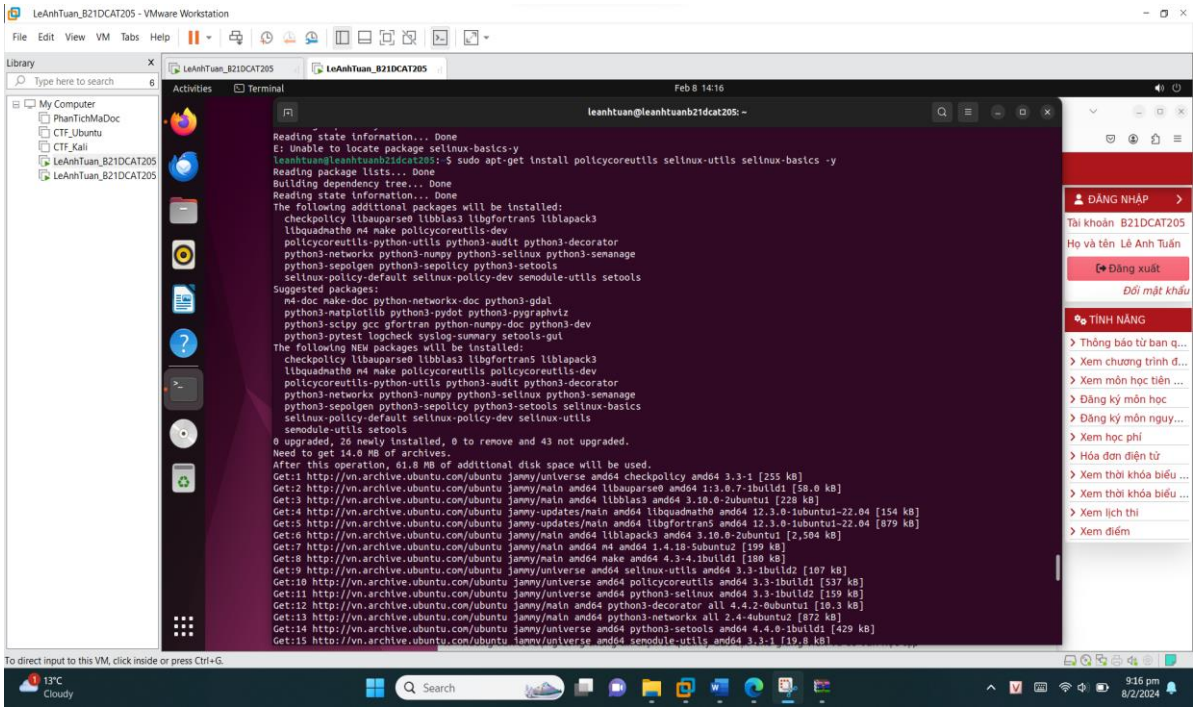
Thử mở file **share1**



Hình 3.14: Kiểm tra xem có quyền mở file chia sẻ hay không.

3.3 Cài đặt thành công SELinux

Cài đặt các module của **SELinux**

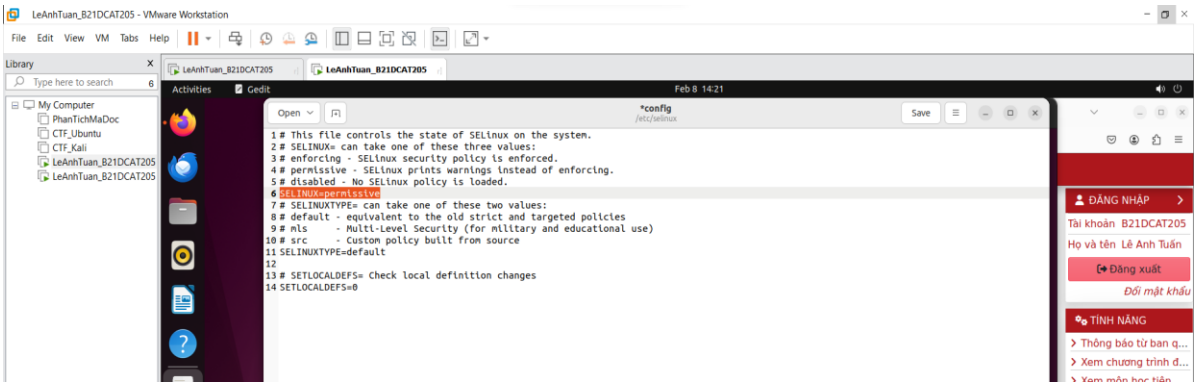


Hình 3.15: Cài đặt SELinux

```
leanhtuan@leanhtuanb21dcat205:~$ sudo selinux-activate
Activating SE Linux
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.15.0-92-generic
Found initrd image: /boot/initrd.img-5.15.0-92-generic
Found memtest86+ image: /memtest86+.elf
Found memtest86+ image: /memtest86+.bin
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
SE Linux is activated.  You may need to reboot now.
leanhtuan@leanhtuanb21dcat205:~$ sudo selinux-config-enforcing
Configured enforcing mode in /etc/selinux/config for the next boot.
This can be overridden by "enforcing=0" on the kernel command line.
leanhtuan@leanhtuanb21dcat205:~$
```

Hình 3.16: Kích hoạt SELinux.

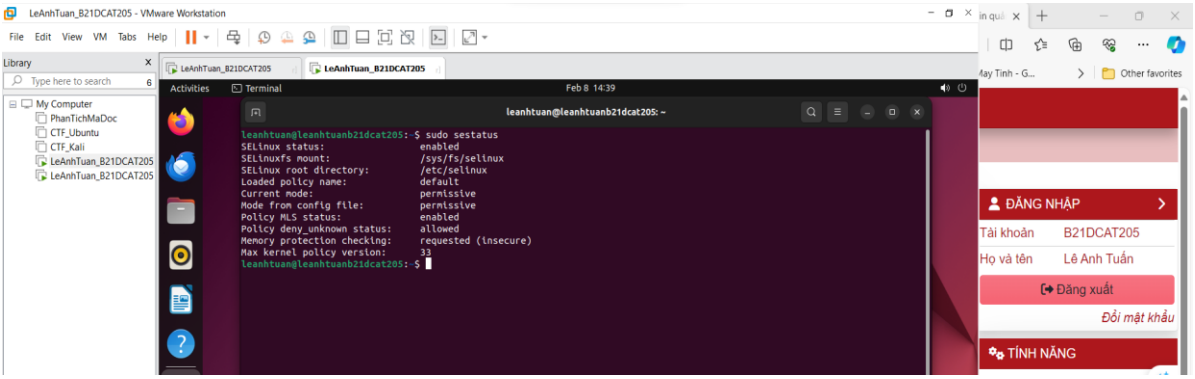
Dùng câu lệnh: **sudo gedit /etc/selinux/config**, để chỉnh sửa chế độ của SELinux



Hình 3.17: Chuyển sang chế độ permissive(như hình).

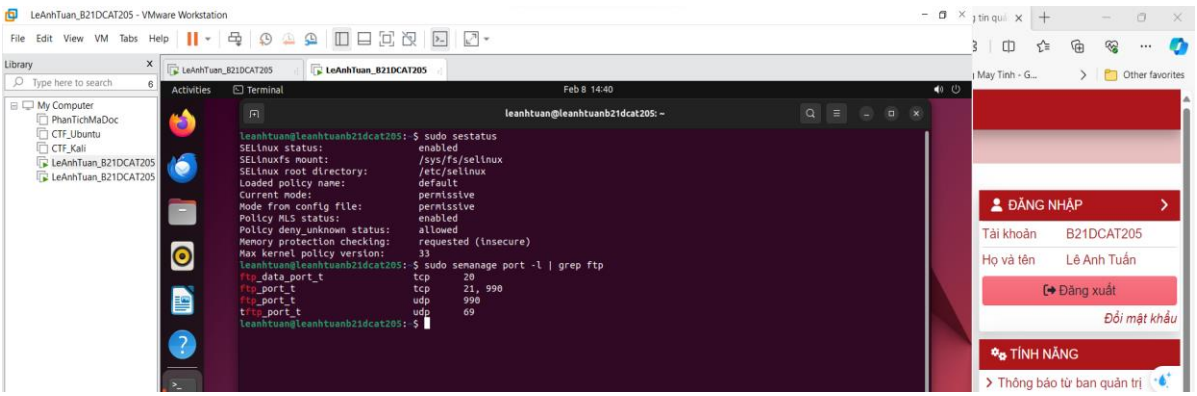
Sau đó tiến hành khởi động lại máy ảo

Kiểm tra lại xem **SELinux** đã hoạt động chưa, ta thấy **SELinux status: enabled**



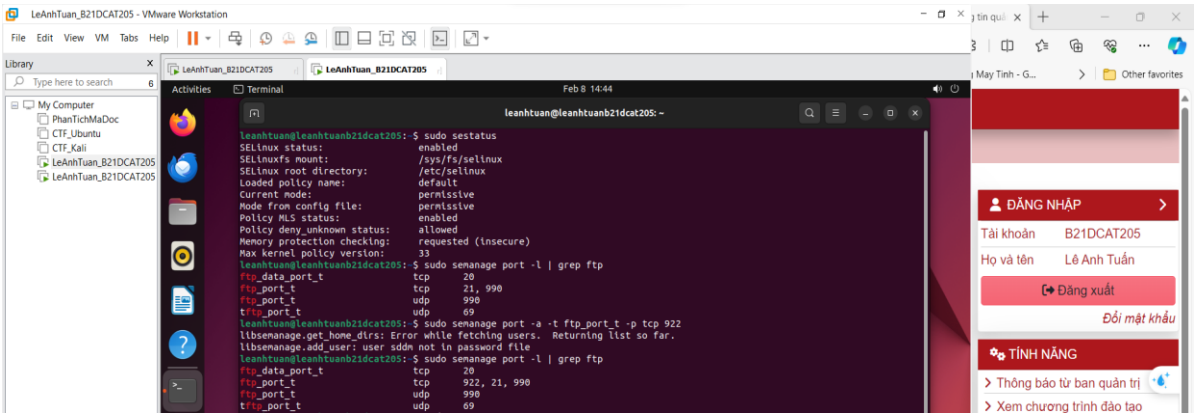
Hình 3.18: SELinux đã sẵn sàng hoạt động

Trước khi thêm cổng ta kiểm tra xem các cổng dịch vụ ftp bằng câu lệnh: **sudo semanage port –l | grep ftp**, ta thấy ftp_port_t có hai cổng 21 và 990



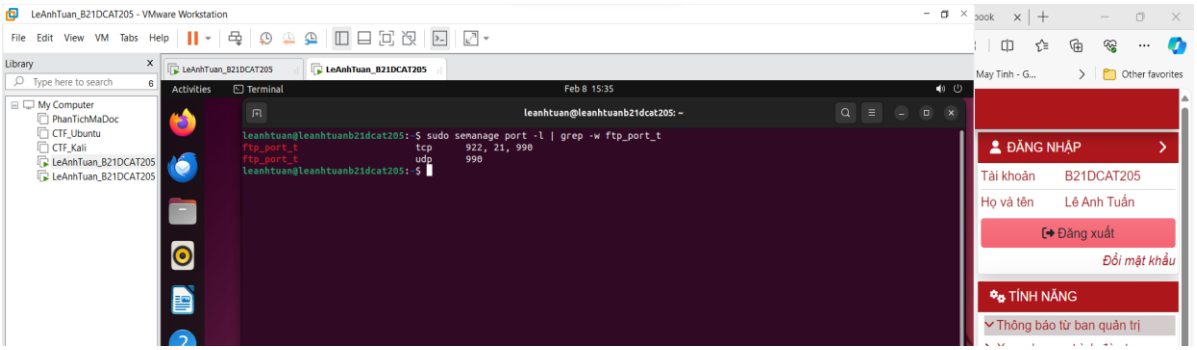
Hình 3.19: Kiểm tra cổng dịch vụ ftp

Dùng câu lệnh **sudo semanage port –a –t ftp_port_t –p tcp 922** để thêm cổng 992



Hình 3.20: Thêm cổng 922

Kiểm tra thành công bằng câu lệnh: **semanage port -l | grep -w ftp_port_t**



Hình 3.21: Kiểm tra và thành công thêm cổng 922

4 Kết luận

- Sinh viên cài đặt và quản trị thành công hệ điều hành Linux Server
- Sinh viên cài đặt và sử dụng thành thạo một số dịch vụ cơ bản của Linux Server

5 Tài liệu tham khảo

- Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
- Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012