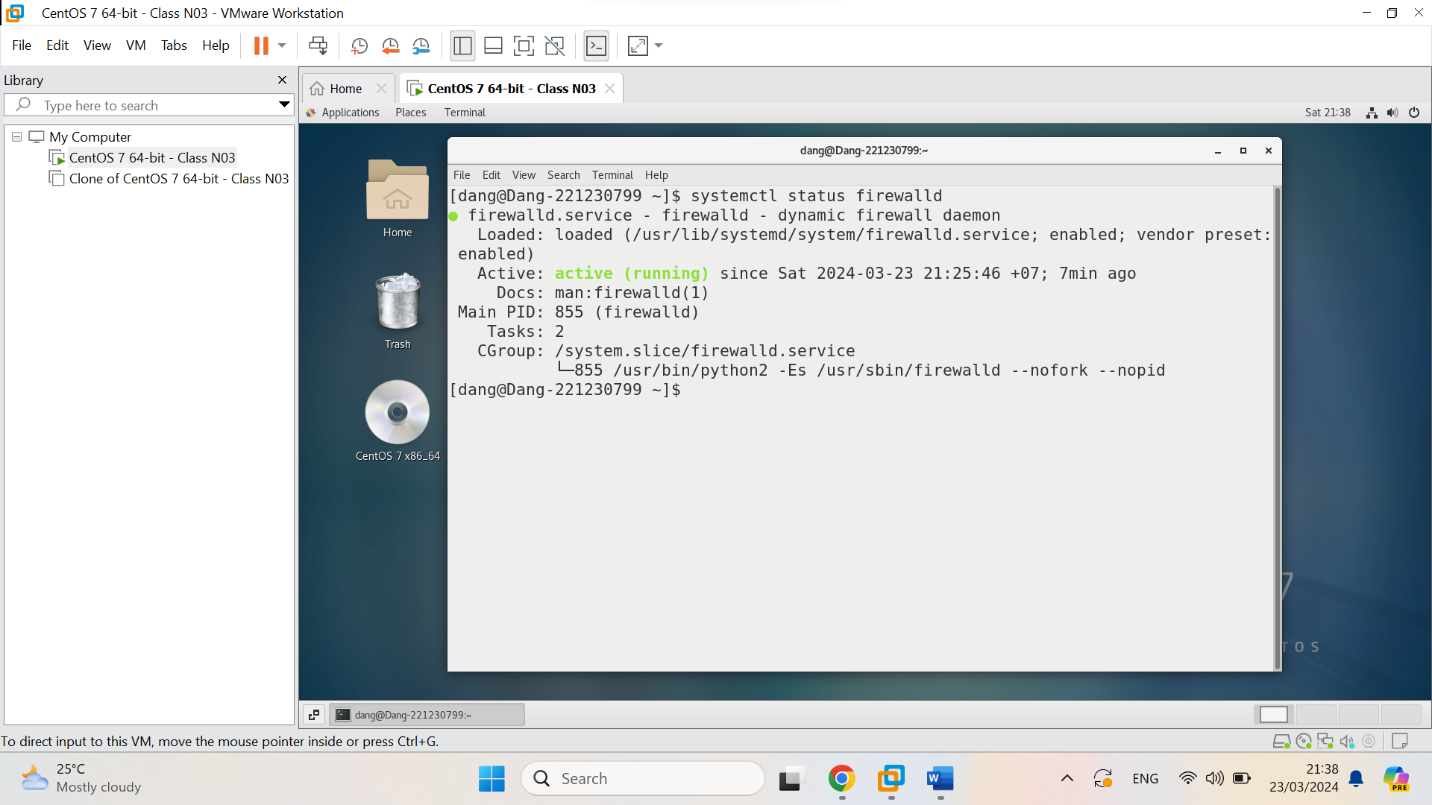
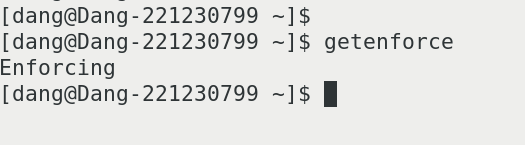
**BÀI THỰC HÀNH 4:**

**SECURITY TRONG HĐH CENTOS 7 - MỨC CƠ BẢN**

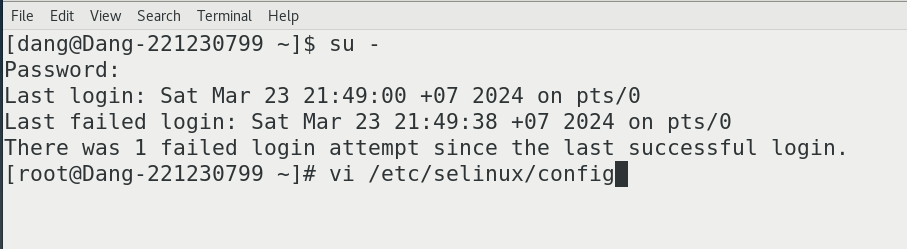
- Hiển thị trạng thái của firewall sau khi khởi động máy:

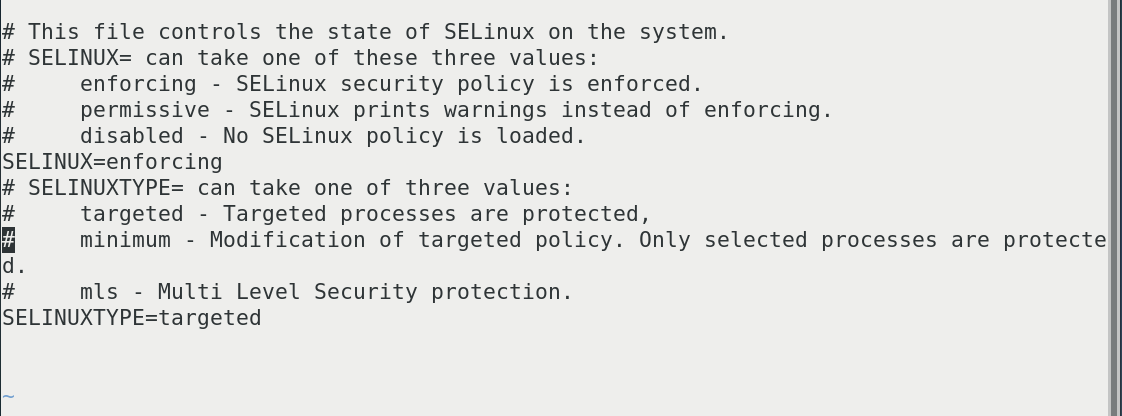


- Hiển thị trạng thái của SELinux sau khi khởi động máy



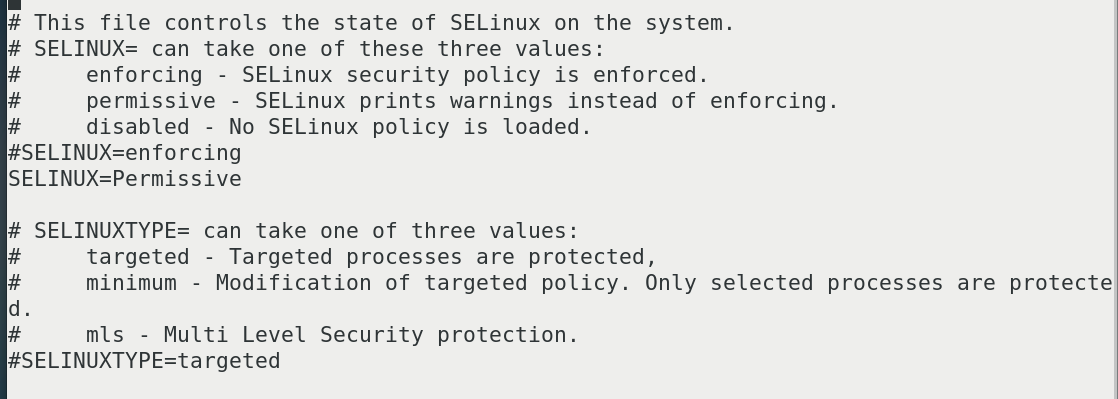
- Chuyển sang chế độ người dùng root, mở file /etc/selinux/config bằng công cụ vi hoặc

Vim

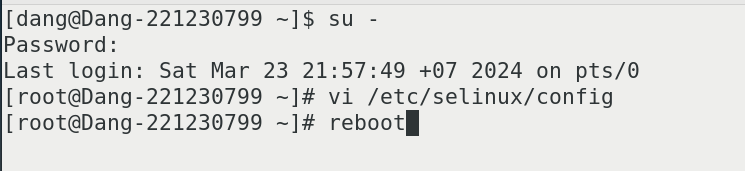


- Sửa giá trị biến SELINUX trong file cấu hình /etc/selinux/config (SELINUX=Permissive).

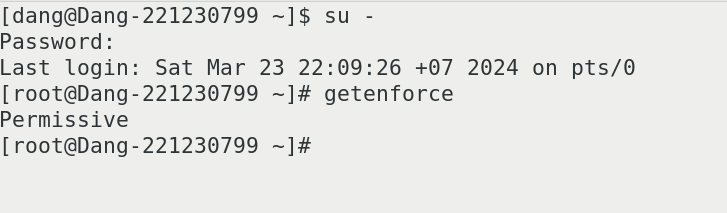
- Lưu file và thoát



- Reboot hệ thống

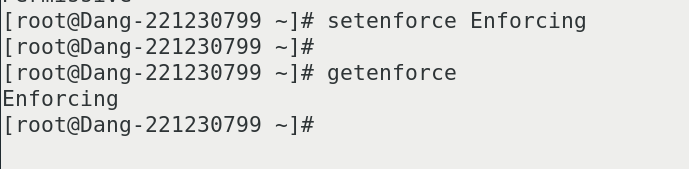


-Kiểm tra chế độ hoạt động của SELinux (vẫn là Permissive)

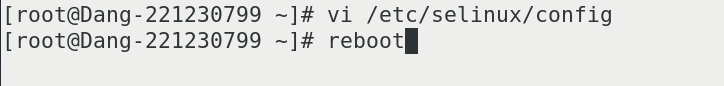


-Chuyển chế độ hoạt động của SELinux từ Permissive sang Enforcing bằng lệnh (~]#

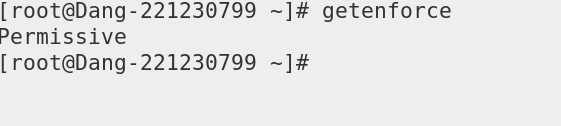
setenforce Enforcing)

- Hiển thị trạng thái của SELinux (~]# getenforce) 

-Reboot hệ thống (~]# reboot)

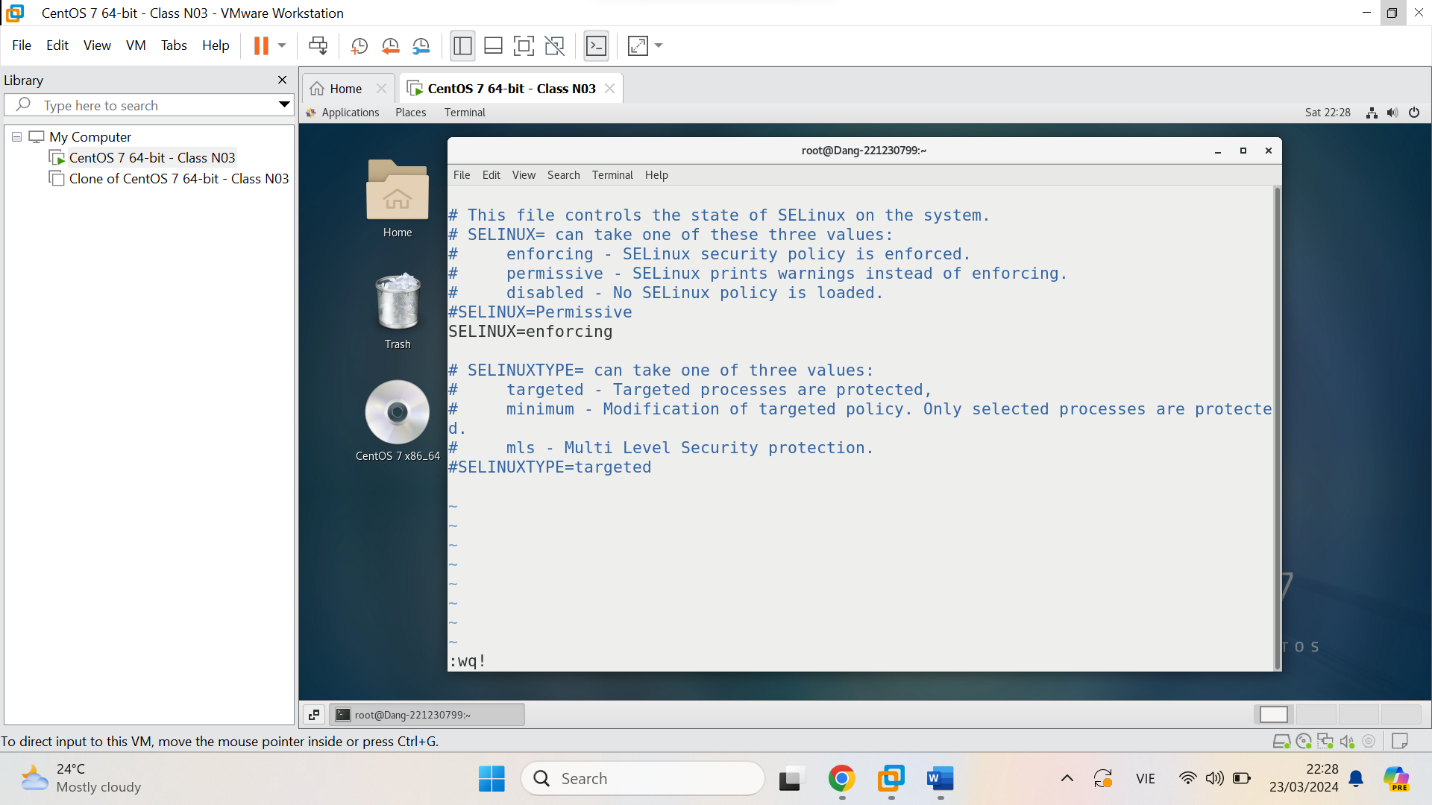


-Hiển thị trạng thái của SELinux sau boot (~]$ getenforce). Vẫn là Permissive

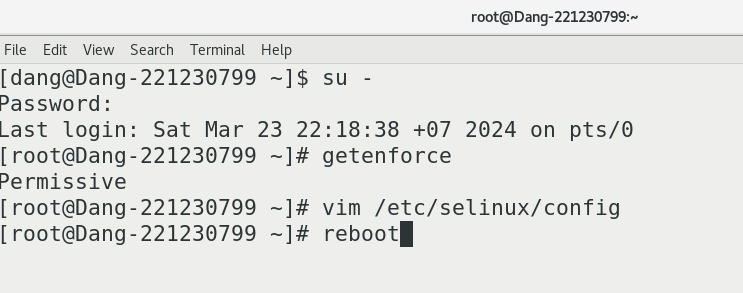


-Dùng lệnh (~]# vim /etc/selinux/config) sửa giá trị biến SELINUX trong file cấu hình

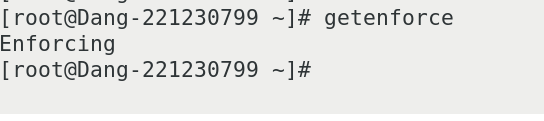
(SELINUX=Enforcing)



-Lưu file cấu hình và thoát



-Reboot hệ thống và kiểm tra chế độ hoạt động của SELinux (là Enforcing)

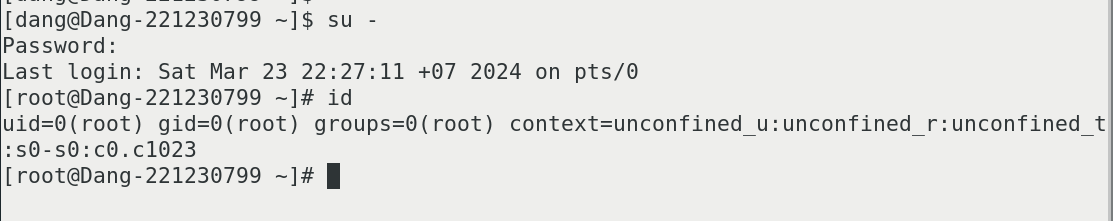
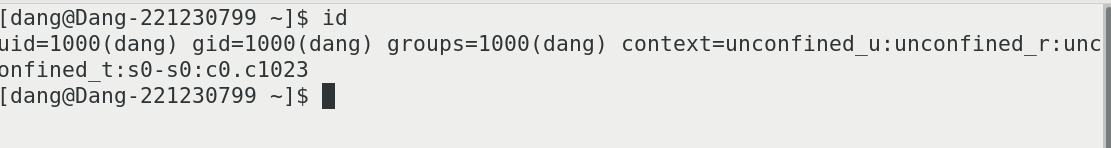


**BÀI THỰC HÀNH 5:**

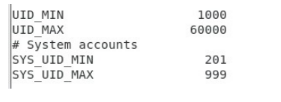
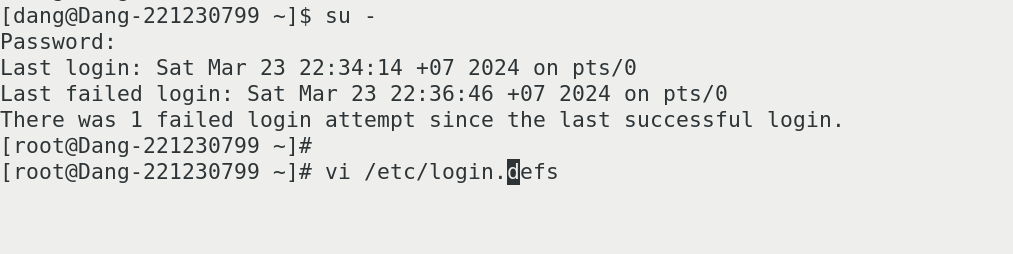
**QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG TRONG CENTOS 7 -**

**MỨC CƠ BẢN**

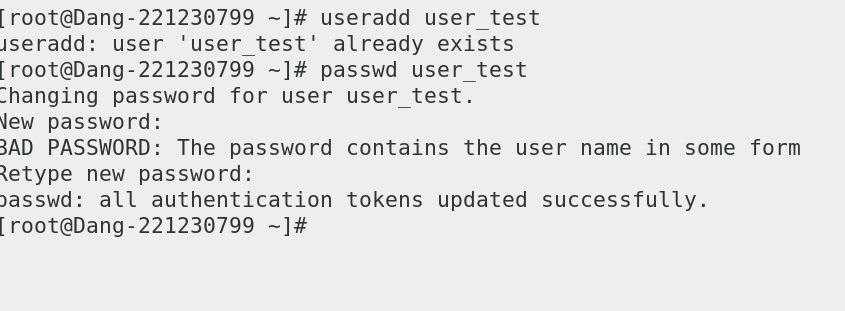
- Kiểm tra UID với account thường vừa truy cập

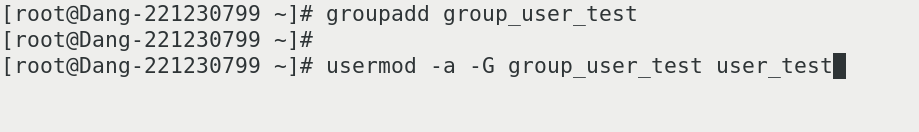


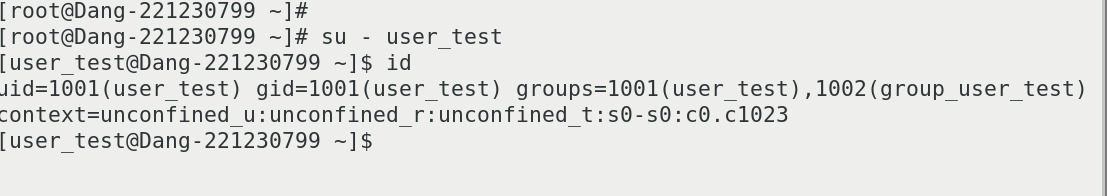
-Mở file login.defs bằng lệnh “vi /etc/login.defs”



-Tạo người dùng mới có thông tin user / pass là user\_test / user@test



-Tạo nhóm group\_user\_test và thêm người dùng user\_test vào nhóm vừa tạo này

-Từ root chuyển sang người dùng user\_test, kiểm tra UID của người dùng này

-Từ người dùng user\_test chuyển sang người dùng thường đc tạo khi cài máy

