**Đề**

1. Простой вариант (обе):

* Настроить Apparmor для мониторинга сложного приложения и продемонстрировать его работу при ограниченных правах (оконное приложение или веб-сервер)
* Настроить selinux в режиме мандатного доступа (CentOS и др.) и продемонстрировать работу в двухуровневой модели.

2. Сложный вариант (или):

* Придумать и написать свой LSM-модуль (сложная авторизация действий)
* Придумать и написать свой PAM-модуль (сложная авторизация действий)

Задание

apparmor-profiles

apparmor-utils

aa-status

aa-complain - режим мониторинга

aa-enforce - режим защиты

aa-autodep - новый профиль

aa-genprof - обновить профиль

сгенерировать свой профиль для ncat

**Tiếng anh:**  
1. Simple option (both):

Configure Apparmor to monitor a complex application and demonstrate how it works with limited rights (windows application or web server)

Configure selinux in mandatory access mode (CentOS, etc.) and demonstrate how it works in a **two-tier model.**

2. Complex option (or):

Design and write your own LSM module (complex action authorization)

Design and write your own PAM module (complex authorization of actions)

Exercise

apparmor-profiles

apparmor-utils

aa-status

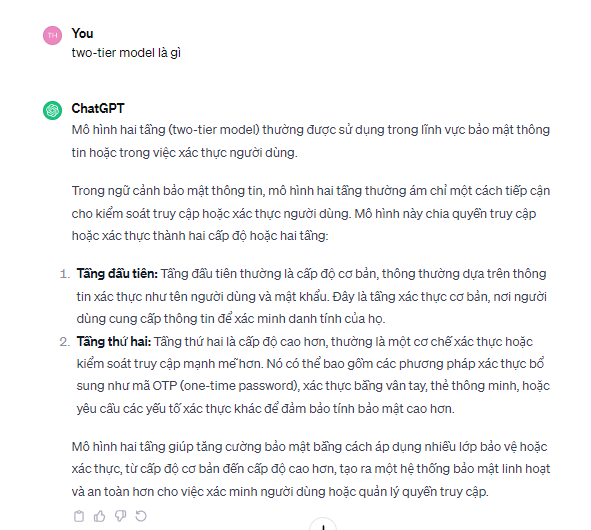
aa-complain - monitoring mode

aa-enforce - protection mode

aa-autodep - new profile

aa-genprof - update profile

generate your profile for ncat



**Tiếng Việt:**

1. Tùy chọn đơn giản (cả hai):

Định cấu hình Apparmor để giám sát một ứng dụng phức tạp và chứng minh cách nó hoạt động với các quyền hạn chế (ứng dụng windows hoặc máy chủ web)

Định cấu hình selinux ở chế độ truy cập bắt buộc (CentOS, v.v.) và trình bày cách hoạt động của nó trong mô hình hai tầng.

2. Tùy chọn phức tạp (hoặc):

Thiết kế và viết mô-đun LSM của riêng bạn (ủy quyền hành động phức tạp)

Thiết kế và viết mô-đun PAM của riêng bạn (ủy quyền hành động phức tạp)

AppArmor là một công cụ bảo mật trong hệ điều hành Linux

—-------------------------------------------------------------------------------------------------------------

Đầu tiên cài AppArmor

touch example2.sh

Viết file bash

#!/bin/bash

echo "This is an apparmor example."

touch data/sample.txt

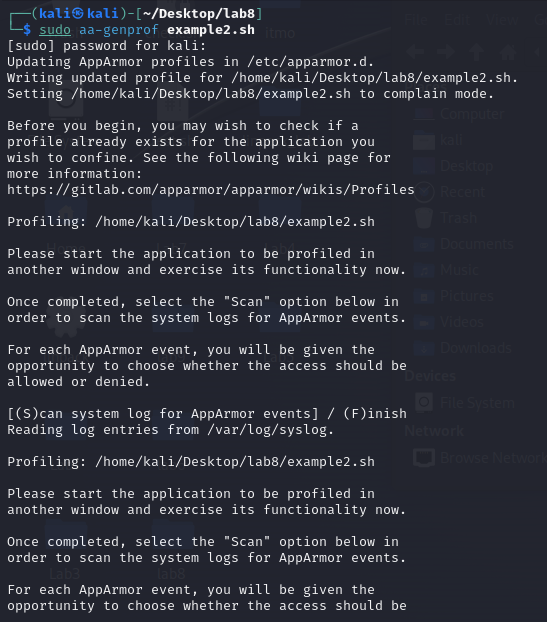
echo "File created"

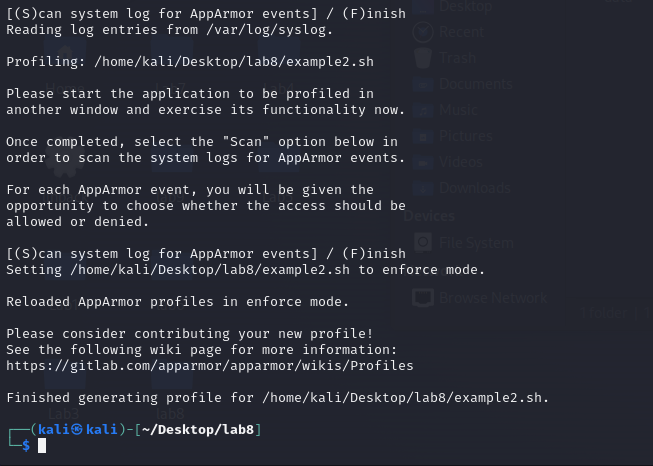
rm data/sample.txt

echo "File deleted"

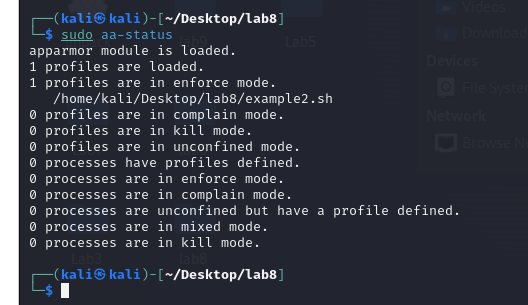
Cấp quyền file bash: chmod u+x example2.sh

aa-genprof - update profile

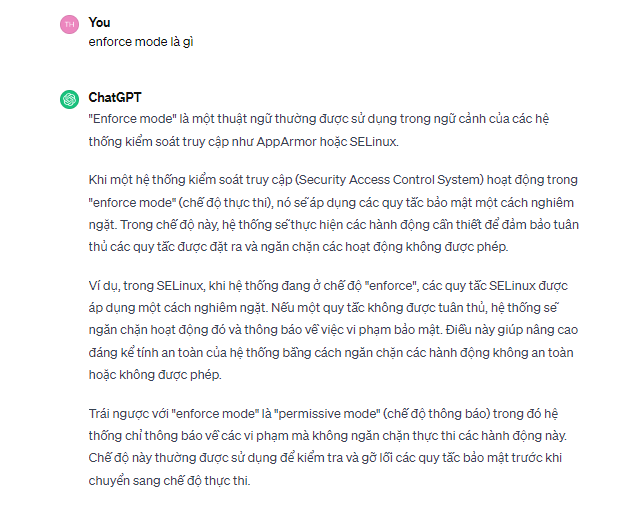
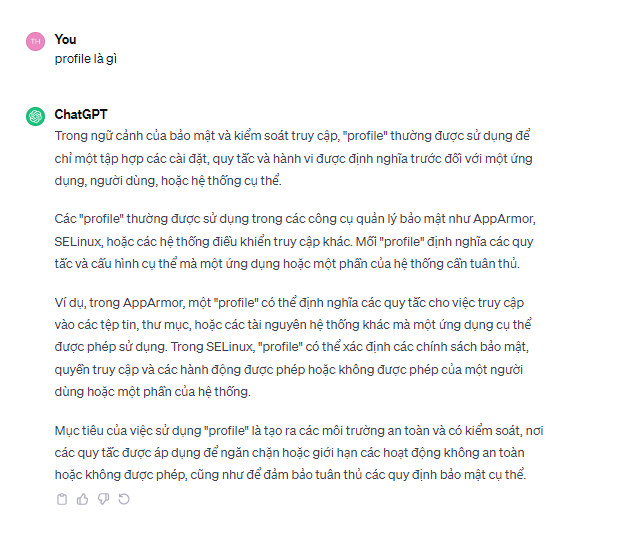


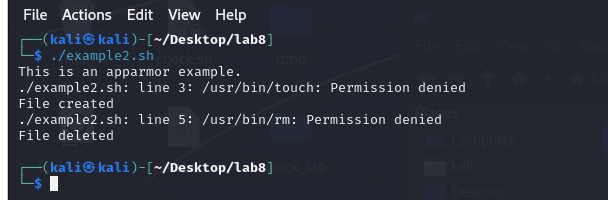


aa-status -tình trạng

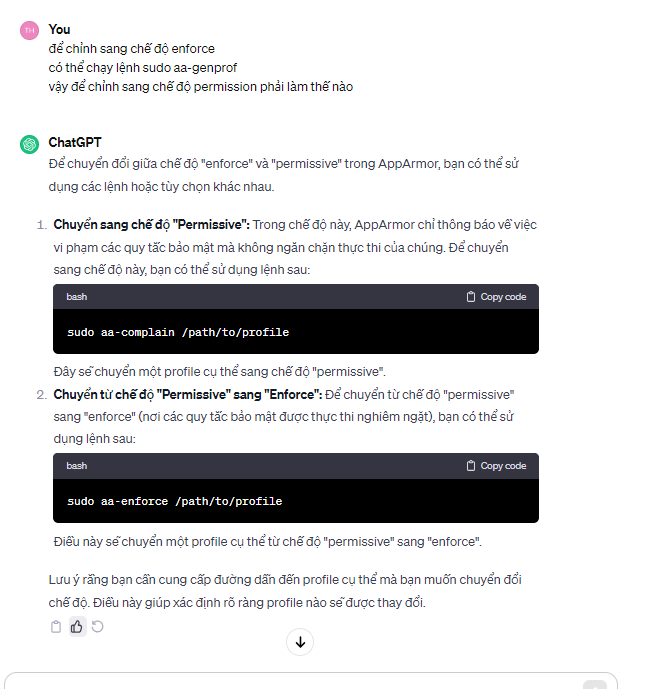


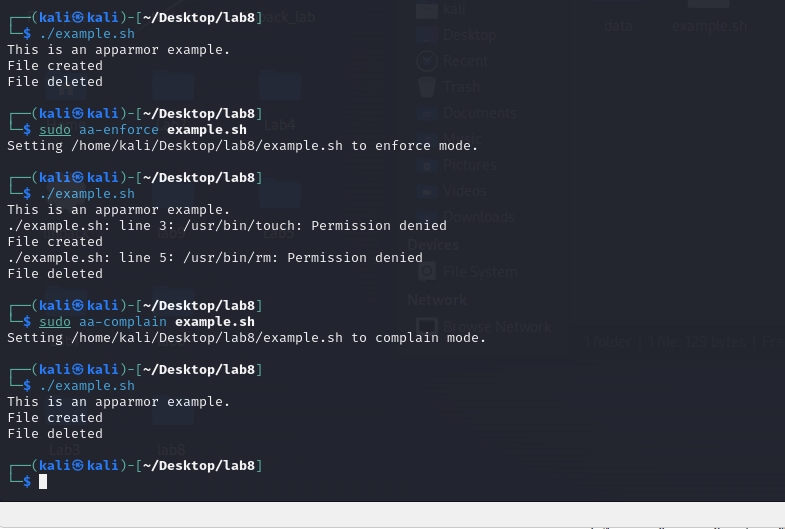
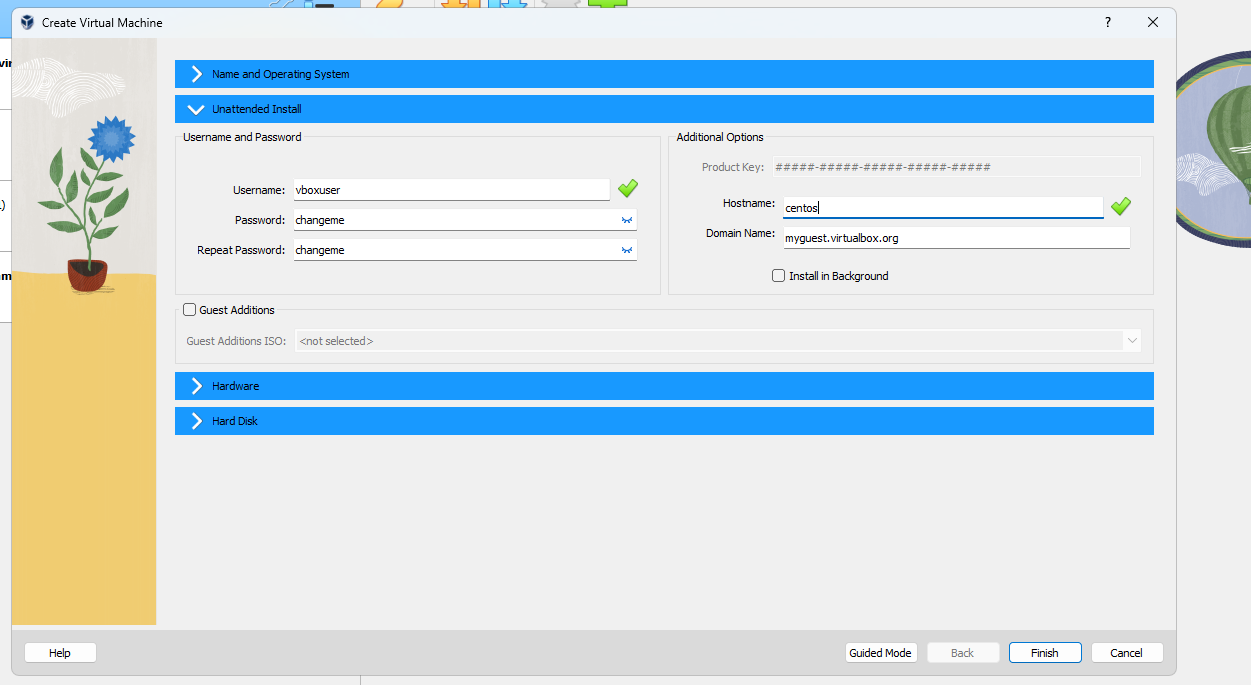
Sau khi mà nó thành enforce mode thì





Để thoát khỏi chế độ enforce ta set nó sang chế độ complain



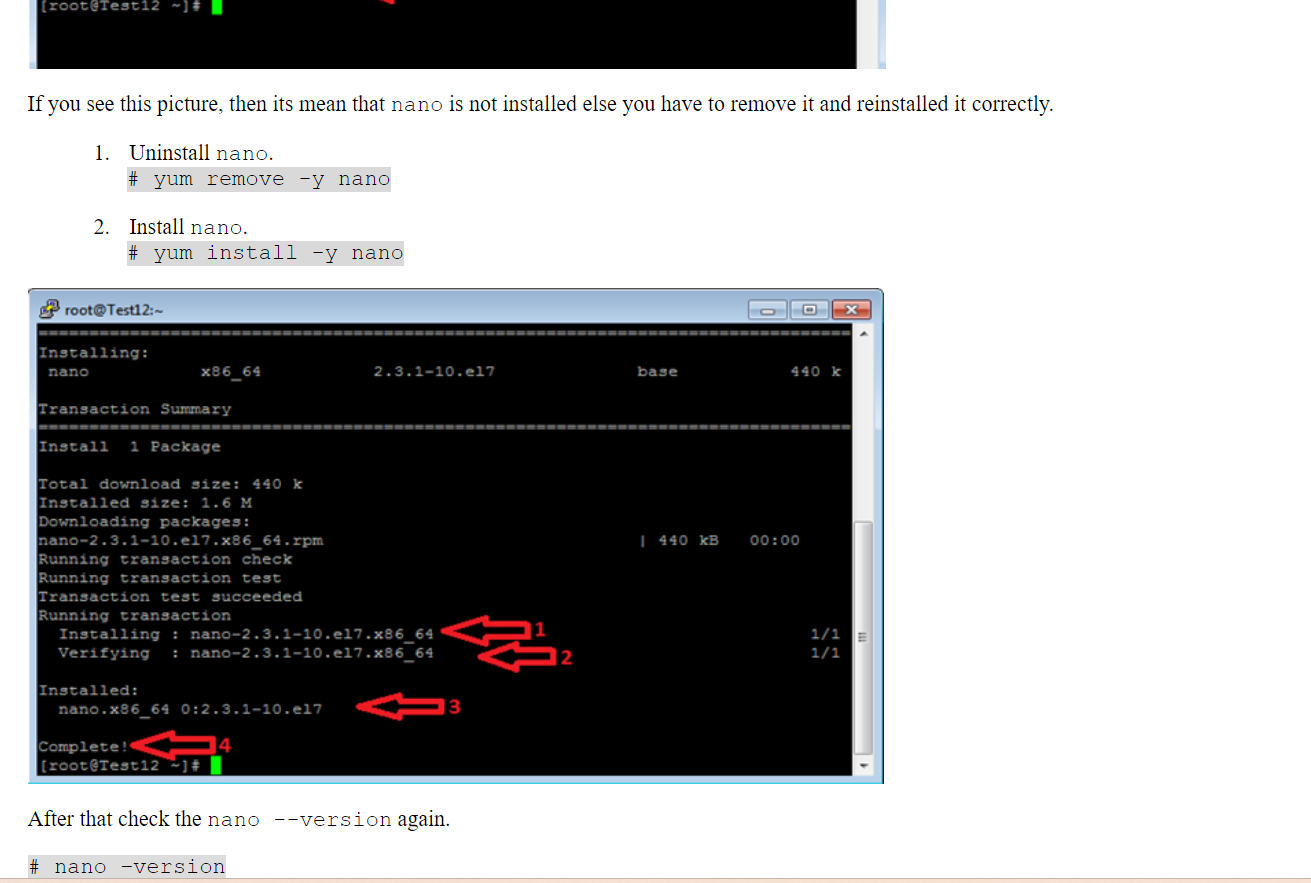
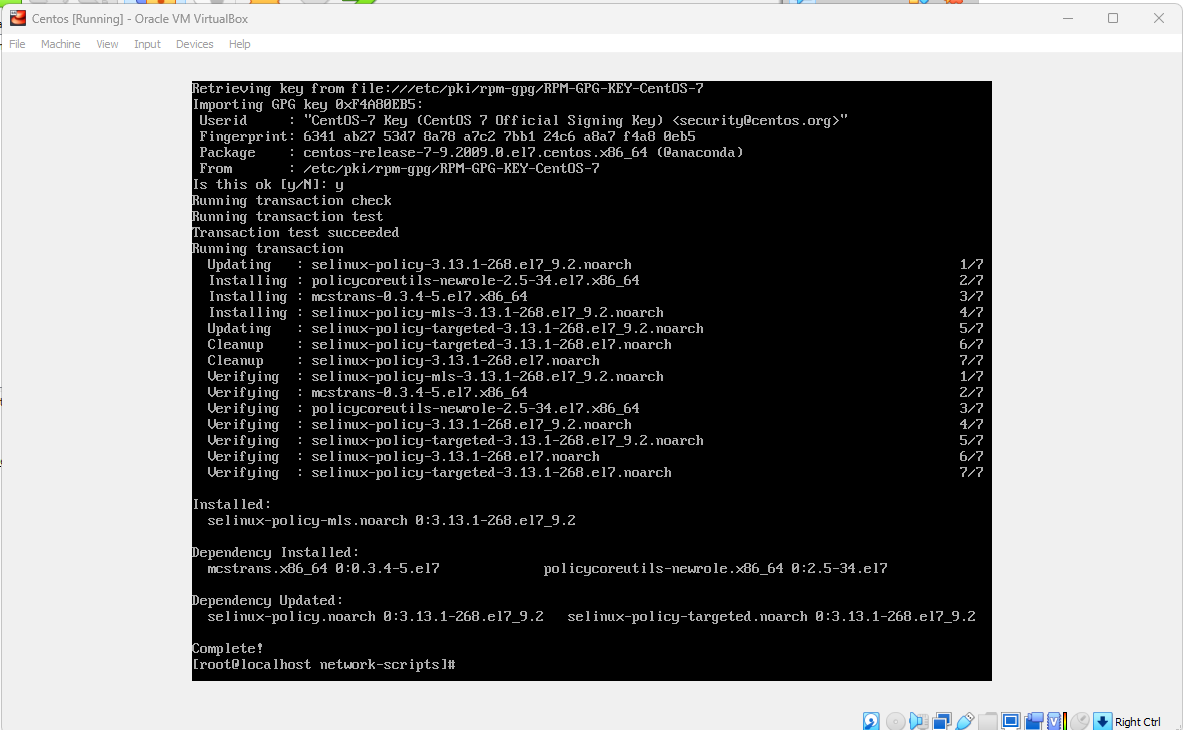
  
Phần 2 CENTOS

<https://www.7host.vn/huong-dan-cai-dat-centos-7-toan-tap/>

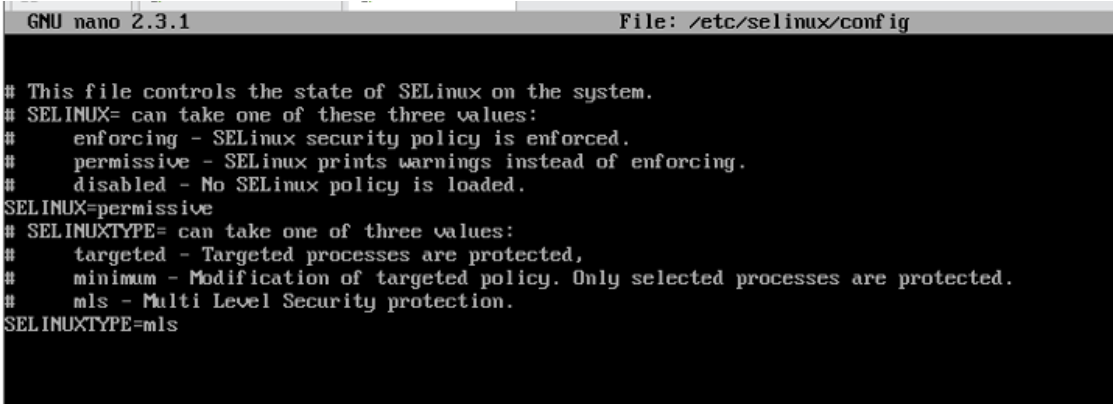
<https://www.youtube.com/watch?v=IxookDRgOZM>

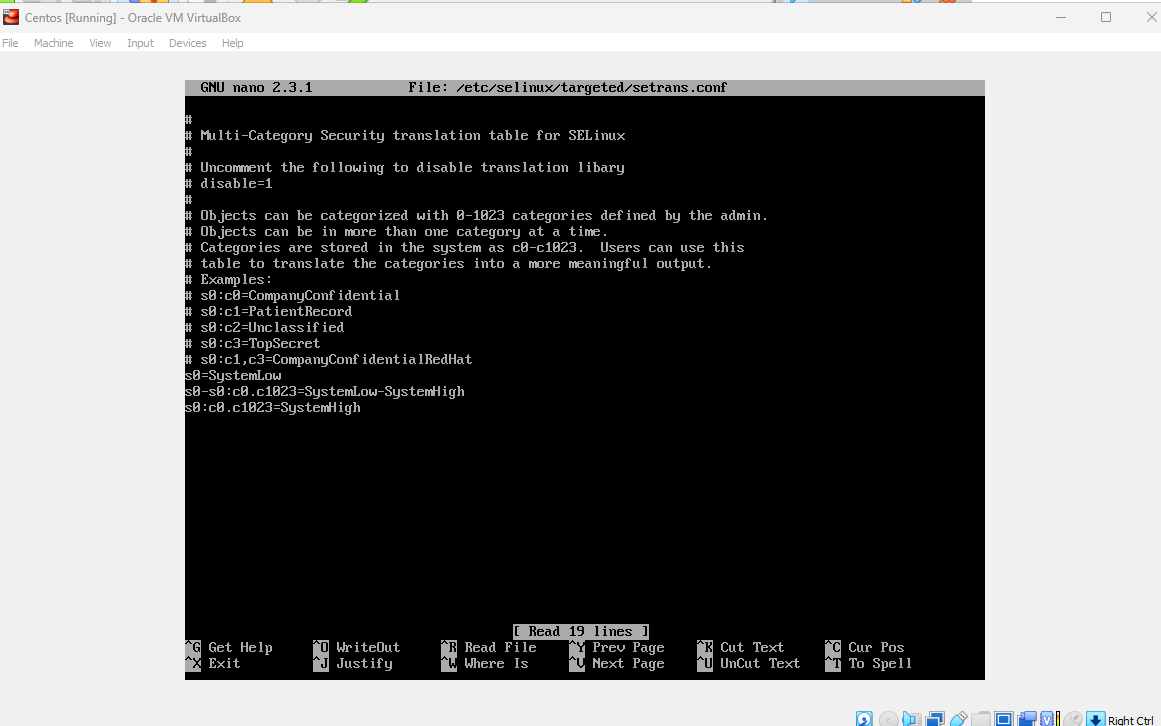
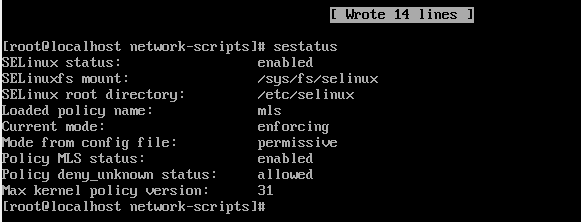
Password: theviet

User: root



Nano /etc

Chỉnh thành

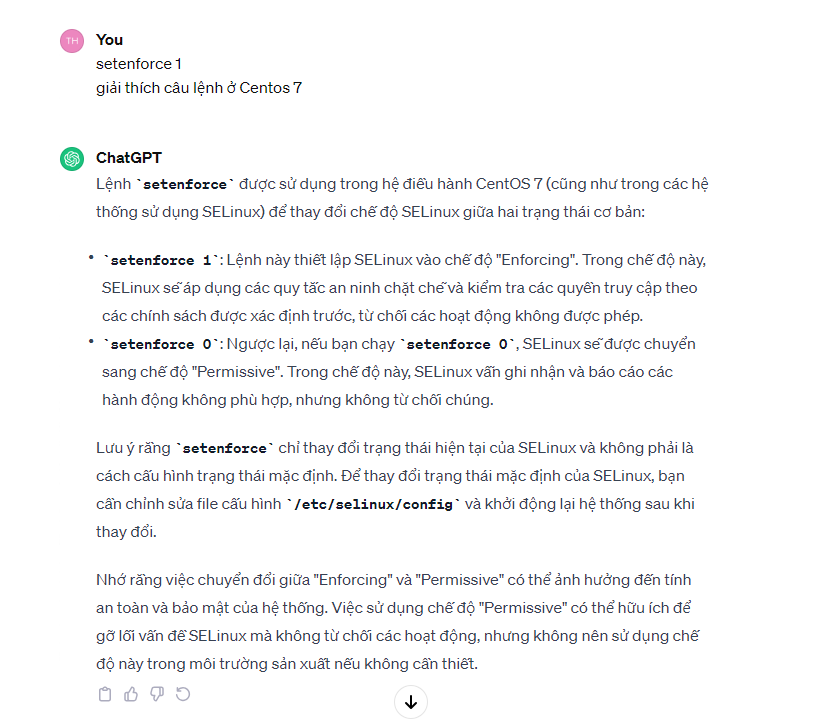


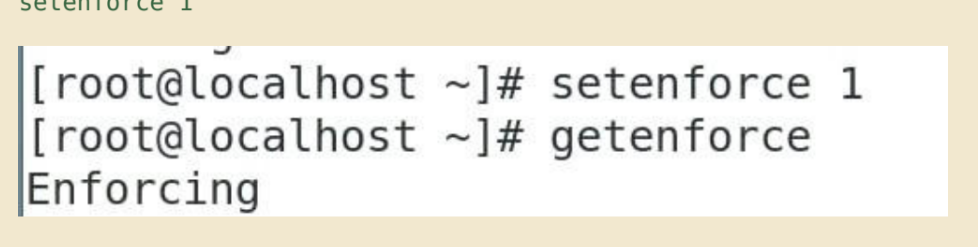
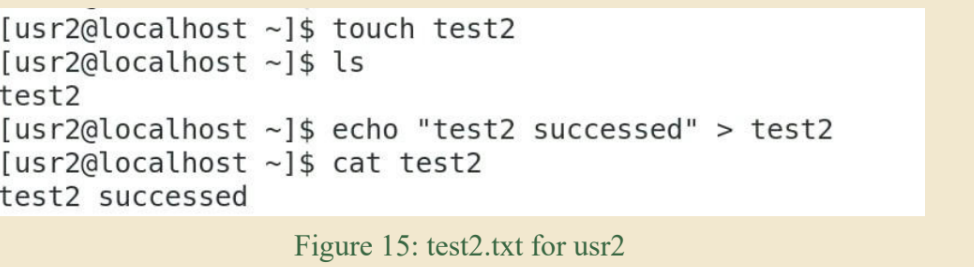
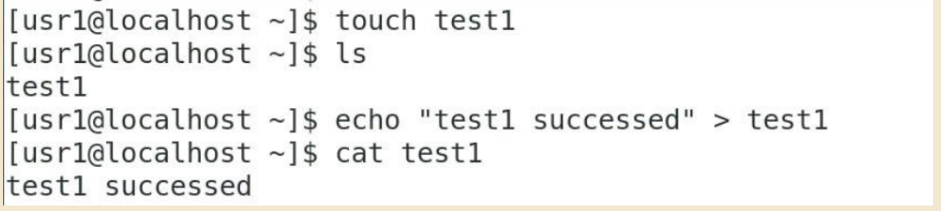
yum install dnf

dnf provides /usr/sbin/semanage

Tải semanage

<https://www.itzgeek.com/how-tos/linux/centos-how-tos/semanage-command-not-found-in-centos-7-rhel-7-quick-fix.html>



<https://access.redhat.com/documentation/vi-vn/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-confining_users-confining_existing_linux_users_semanage_login>

