UNIVERSITY INSTITUTE of COMPUTING
Asia's Fastest Growing University

NAAC GRADE A+ ACCREDITED UNIVERSITY

Experiment No. 3.1

Student Name: Gaurav Kumar **UID: 22MCC20177**
Branch: MCA – CCD **Section/Group: 22MCD-1 / Grp B**
Semester: I **Date of Performance: 21st December 22**
Subject Name: Linux Administration Lab **Subject Code: 22CAP-648**

1. **Aim/Overview of the practical:**

   How to temporarily turn off enforcing mode without having to reboot?
   What are the access control attributes used by SELinux type enforcement security to control access?

2. **Task to be Done/Concept Used:**
   The basic concepts and ideas of SE Linux is used here.

3. **Commands for experiment/practical:**

How do I temporarily turn off enforcing mode without having to reboot?

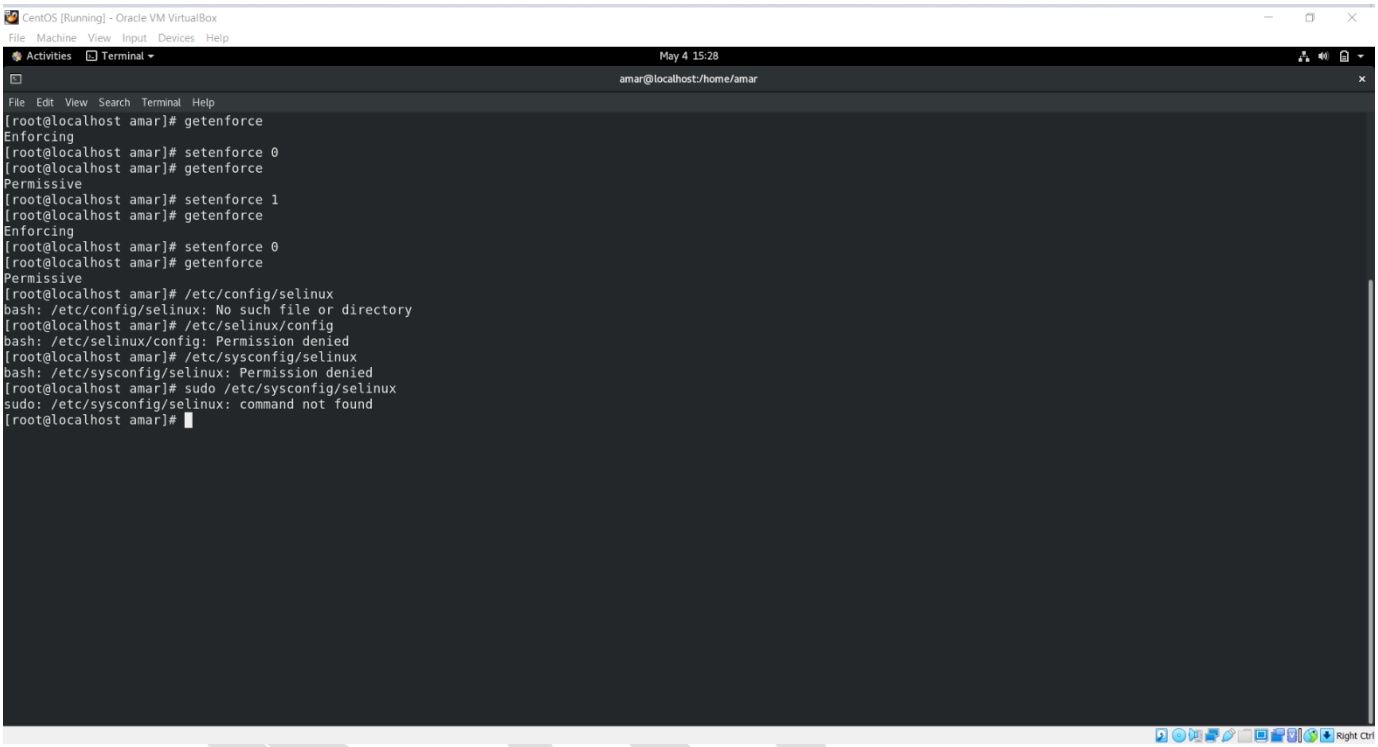
⇨ To temporary turn off the enforcing mode without rebooting, we can use setenforce command. That is: **setenforce 0**

What are the access control attributes used by SELinux type enforcement security to control access?

⇨ SE Linux provides **MAC (Mandatory Access Controls)**.
MAC takes a hierarchical approach to controlling access to resources. Under a MAC enforced environment access to all resource objects (such as data files) is controlled by settings defined by the system administrator. As such, all access to resource objects is strictly controlled by the operating system based on system administrator configured settings. It is not possible under MAC enforcement for users to change the access control of a resource.

The SELinux implementation **also uses role-based access control (RBAC)**, which provides abstracted user-level control based on roles, and **Type Enforcement (TE)**.

4. **Result/Output/Writing Summary:**



Learning outcomes (What I have learned):

1. Learned about SE Linux.

2. Learned to use enforcing commands to enabling & disabling SE Linux & enforcing mode.

3. Learned to use different concepts and commands of SE Linux.