UNIVERSITY INSTITUTE of COMPUTING
Asia's Fastest Growing University

NAAC GRADE A+ ACCREDITED UNIVERSITY

# Experiment No. 3.1

**Student Name:** Rishav Kumar
**UID:** 22MCC20039
**Branch:** MCA - CCD
**Section/Group:** MCD-1/ Grp B
**Semester:** I
**Date of Performance:** 05th Jan 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. **Code for practical:**

- Create a file using ***touch ABC.txt*** command.
- Now, to create backup, use ***tar Mybackup.tar ABC.txt*** command.
- 

```
┌──(kali㉿kali)-[~/Desktop]
└─$ setenforce 0
setenforce: SELinux is disabled
```

**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)**.

********** THE END **********