**SELinux**

SELinux is a set of security policies/modules which are going to apply on the machine to improve the overall security of the machine. These are the Linux security modules(LSM) which are loaded in to kernel to improve security on accessing services/files which improve security. **SELinux** is short form of Security Enhanced Linux.

**SELinux is set in three modes.**

* **Enforcing** – SELinux security policy is enforced. IF this is set SELinux is enabled and will try to enforce the SELinux policies strictly
* **Permissive** – SELinux prints warnings instead of enforcing. This setting will just give warning when any SELinux policy setting is breached
* **Disabled** – No SELinux policy is loaded. This will totally disable SELinux policies.

**And SELinux is set in two levels**

* **Targeted** – Targeted processes are protected,
* **Mls** – Multi Level Security protection.

**Ex 1**: Is SELinux enabled or not on your box? use below command to get the status.

**# getenforce**

**Ex 2**: To see SELinux status in simplified way you can use sestatus

**# sestatus**

**Ex 3:** To get elobrated info on difference status of SELinux on different services use -b option along sestatus

**# sestatus –b**

**Ex 4**: How to disable SElinux

**We can do it in two ways**

**1)** Permanent **way : edit /etc/selinux/config**

change the **status** of SELINUX from **enforcing** to **disabled**

SELINUX=enforcing

to

SELINUX=disabled

Save the file and exit. And Restart The System

**2) Temporary way :** Execute below command

**echo 0 > /selinux/enforce**

or

setenforce 0

**Ex 5:** Switch back disable to **enforcing**:

#setenforce enforcing