SE LINUX (Security Enhanced Linux)

Security Enhanced Linux is an additional layer of system security. The main objective of SE linux is to protect user data from un authorized system services.

SEL linux provides an additional layer of security that is object-based and controlled by more sophisticated rules known as Mandatory access control(MACL).

We have 3 Different modes in SE Linux:

1)Enforcing
2)Permissive
3)Disabled

Enforcing:

This is the default option in enforcing mode, If someting happens on the system that is against the defines policy, The action will be both blocked & Logging.

Permissive:

This mode will not actually block or deny anything from happening, However it will log anything that would have normally blocked in enforcing mode. This option is generally used for Testing or troubleshooting operations.

NOTE:

No system reboot is required when swapping between Permissive & Enforcing Modes.

Disabled:

Disabled is completely turned off, Nothing is logged at all.

In order to swap to the disabled mode. A system reboot will be required. If you are switching from disabled to either permissive or enforcing mode a system reboot is required.

#getenforce	**(Displays the SE linux current mode)**
#setenforce 0	**(Switching SE linux mode to Permissive)**
#setenforce 1	**(Switching SE Linux mode to Enforcing)**

NOTE:

- These changes are temporary for the session, To make it Permanent update in /etc/selinux/config.

- /etc/selinux/config and /etc/sysconfig/selinux are linked together.

LAB Exercise 1 : (Changing the Security Context and restoring it to default)

```
#mkdir              /virtual

#ls    -Zd    /virtual
O/P
                                    :default_t

#chcon       -t      httpd_sys_content_t       /virtual

#ls    -Zd    /virtual
O/P
                                    :httpd_sys_content_t

#restorecon   -v    /virtual

#ls     -Zd   /virtual
O/P
                                    :default_t
```

Lab Exercise 2: (understanding Security Context while moving & copying and Restoring to default context)

```
#cd    /tmp

#touch              file1   file2

#ls    -Z     file1   file2
O/P                                  :user_tmp_t         file1
                                     :user_tmp_t         file2

#mv     /tmp/file1 /var/www/html/
#cp     file2         /var/www/html/
#cd    /var/www/html

#ls    -Z     file1   file1
```

```
O/P                                 :user_tmp_t                  file1
                                    :httpd_sys_content_t                 file2

#restorecon   -Rv    /var/www/

#ls     -Z      file1    file2
O/P                                 : httpd_sys_content_t                    file1
                                    :httpd_sys_content_t                     file2
```

Lab Exercise 3: (Changing the security context to default)

```
#mkdir             /virtual

#cd    /virtual

#touch            index.html

#ls     -Z      index.html
                             :default_t              index.html

#semanage  fcontext      -a      -t      httpd_sys_content_t      '/virtual(/.*)?'

#restorecon -RFvv /virtual

#ls     -Z      /virtual
O/P
                             :httpd_sys_content_t
```