Assignment 3

Name : Mohamed Khaled Ahmed atyaa

Group num : 3

Id : 16

Ques 1

**What is the SetUID, SetGID, Sticky Bit and umask command. and how to use them?**

setuid : used only for binary files (applications), this permission indicates that the file is to be executed with the permissions of the owner of the file, and not with the permissions of the user executing the file (which is the case without setuid). This is indicated by the character s in the place of the x in the owner category. If the owner of the file does not have execute permissions, a capital S reflects this fact.

We use it like that : chmod u+s <filename> (symbolic)

chmod 4755 <filename> (numeric)

setgid — used primarily for binary files (applications), this permission indicates that the file is executed with the permissions of the group owning the file and not with the permissions of the group of the user executing the file (which is the case without setgid).

If applied to a directory, all files created within the directory are owned by the group owning the directory, and not by the group of the user creating the file. The setgid permission is indicated by the character s in place of the x in the group category. If the group owning the file or directory does not have execute permissions, a capital S reflects this fact.

We use it like that : chmod g+s <filename> (symbolic)

chmod 2755 <filename> (numeric)

sticky bit — used primarily on directories, this bit dictates that a file created in the directory can be removed only by the user that created the file. It is indicated by the character t in place of the x in the everyone category. If the everyone category does not have execute permissions, the T is capitalized to reflect this fact.

Under Red Hat Enterprise Linux, the sticky bit is set by default on the /tmp/ directory for exactly this reason.

We use it like that : chmod o+s <filename> (symbolic)

chmod 1755 <filename> (numeric)

unmask:

When user create a file or directory under Linux or UNIX, she create it with a default set of permissions. In most case the system defaults may be open or relaxed for file sharing purpose. For example, if a text file has 666 permissions, it grants read and write permission to everyone. Similarly a directory with 777 permissions, grants read, write, and execute permission to everyone so to change this default permissions we use unmask value like this:

Permissions=the default value - unmask value

Ex: file with default permission 666 – unmask value 0022 =

File with permission 644 which (rw-r–r–)

To change the unmask value:

vi /etc/profile

or

umask 022