PES UNIVERSITY

(Established under Karnataka Act No.16 of 2013)

100-ft Ring Road, BSK III Stage, Bangalore – 560 085

Department of Computer Science

Session: Jan-May 2021

UE19CS254: Operating Systems

Assignment 5

Assignment 5 is based on protection: Access matrix, access control

1. **Explore the functions/working of setuid()/ setuid bit in Unix operating system.**

```
root@DESKTOP-8MFSNVJ:~# which sudo
/usr/bin/sudo
root@DESKTOP-8MFSNVJ:~# ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 166056 Feb  3  2020 /usr/bin/sudo
root@DESKTOP-8MFSNVJ:~# ls -l /usr/bin/crontab
-rwxr-sr-x 1 root crontab 43720 Feb 14  2020 /usr/bin/crontab
root@DESKTOP-8MFSNVJ:~#
```

2. **Explore Configuring ACL(Access Control Lists) in Linux File System**
   1) Installing ACL
      # yum install acl

   2) Configuring ACL on a file system
      # mount -t ext3 -o acl [device-name] [mount-point]

3. Explore the commands for ACL Support in Linux Systems

1) To add permission for user

   setfacl -m "u:user:permissions" /path/to/file

2) To allow all files or directories to inherit ACL entries from the directory it is within
   setfacl -dm "entry" /path/to/dir

3) To remove a specific entry
   setfacl -x "entry" /path/to/file

4) To show permissions:
   # getfacl filename

5) To remove the set ACL permissions,

   use setfacl command with -b option.

Multiple-Choice Questions

1. What does the access matrix represent?
   - **A. Rows-Domains, Columns-Objects**
   - B. Rows-Objects, Columns-Domains
   - C. Rows-Access List, Columns-Domains
   - D. Rows-Domains, Columns-Access list

2. The setuid permission on a file:
   - A. Causes the file to always run as root
   - B. Causes the file to never run as root
   - **C. Causes the file to run under the owner's identity**
   - D. Causes the file to run under the user's identity

3. Using the setgid permission on a directory:
   - A. **Causes new files created in the directory to be owned by the group that owns the directory**
   - B. Causes the directory to be writable to members of the group that owns the directory
   - C. Causes files existing in the directory to be made executable by the group
   - D. Causes files existing in the directory to be owned by the group that owns the directory

4. Which permission is used to make a directory so that only root, the owners of files, or the owner of the directory can remove them?
   - A. sticky bit
   - B. **setgid**
   - C. write
   - D. setuid

5. A file owner does not have permission to edit the file but the group to which the file owner belongs does have the permission to edit it. Can the owner edit the file?
   - **A.** Yes
   - **B.No**
   - **C.** Cannot be defined
   - **D**. Error will be encountered

Additional links:

1. https://www.liquidweb.com/kb/how-do-i-set-up-setuid-setgid-and-sticky-bits-on-linux/#:~:text=Setuid%2C%20Setgid%20and%20Sticky%20Bits,write%20or%20execute%20the%20file.
2. https://www.tecmint.com/secure-files-using-acls-in-linux/
3. https://www.geeksforgeeks.org/access-control-listsacl-linux/