Linux Quiz-2

1. What command would list all files (except . and ..) in the current working directory?

Ans:

ls

2. What is the simplest command for adding execute permission to file ~/foo, for all users (without changing any other permission)

Ans:

chmod +x ~/foo

3. Explain what execute permission means/allows when it is associated with a directory. So that I can execute and see results in my terminal.

Ans:

```
[vkosaraju@localhost Desktop]$ ls -l
total 4
drwxrwxr-x. 2 vkosaraju vkosaraju 260 Mar  1 06:27 Assignment4
drwxrwxr-x. 4 vkosaraju vkosaraju 164 Mar  1 14:10 Assignment7
drwxrwxr-x. 2 vkosaraju vkosaraju 174 Mar  1 00:58 classwork
-rwxrw-r--. 1 vkosaraju vkosaraju 129 Mar  1 04:04 delOlderFiles.sh
drwxrwxr-x. 2 vkosaraju vkosaraju  60 Mar  1 04:29 forQue12
drwxrwxr-x. 2 vkosaraju vkosaraju  33 Mar  1 04:05 forQue9
[vkosaraju@localhost Desktop]$ chmod -x *
[vkosaraju@localhost Desktop]$ ls -l
total 4
drw-rw-r--. 2 vkosaraju vkosaraju 260 Mar  1 06:27 Assignment4
drw-rw-r--. 4 vkosaraju vkosaraju 164 Mar  1 14:10 Assignment7
drw-rw-r--. 2 vkosaraju vkosaraju 174 Mar  1 00:58 classwork
-rw-rw-r--. 1 vkosaraju vkosaraju 129 Mar  1 04:04 delOlderFiles.sh
drw-rw-r--. 2 vkosaraju vkosaraju  60 Mar  1 04:29 forQue12
drw-rw-r--. 2 vkosaraju vkosaraju  33 Mar  1 04:05 forQue9
[vkosaraju@localhost Desktop]$ cd Assignment4
bash: cd: Assignment4: Permission denied
[vkosaraju@localhost Desktop]$ cd classwork
bash: cd: classwork: Permission denied
[vkosaraju@localhost Desktop]$ ls
Assignment4  Assignment7  classwork  delOlderFiles.sh  forQue12  forQue9
[vkosaraju@localhost Desktop]$ ls Assignment4
ls: cannot access Assignment4/delEmpLines.sh: Permission denied
ls: cannot access Assignment4/newfile.tmp: Permission denied
ls: cannot access Assignment4/a4q2: Permission denied
ls: cannot access Assignment4/a4q5.sh: Permission denied
ls: cannot access Assignment4/casePing.sh: Permission denied
ls: cannot access Assignment4/delDir.sh: Permission denied
ls: cannot access Assignment4/delDupLines.sh: Permission denied
ls: cannot access Assignment4/finalfile.tmp: Permission denied
ls: cannot access Assignment4/process.sh: Permission denied
ls: cannot access Assignment4/replace.sh: Permission denied
```

The permissions on regular files differs to that of directories:

a) **The read command enables us to list the files with in the directory**
b) **The write command enables us to create, delete, rename files within the directory.**
c) **The execute bit enables user to enter the directory, and access files and directories inside.**

4. Suppose that you wanted all users on the machine to be able to see the contents of the file ~/public/software/instructions. text. Explain the minimum set of permissions for files and directories needed to allow this, and any security issues that arise.

Ans: **chmod 444 ~/public/software/instructions.text**

5. Suppose that you want to allow (only) other users bob and chuck to be able to access the above file. Explain what you would have to do differently from what you described above. (You are not allowed to consider the use of ACLs.)

Ans:

Create a group for bob and chuck. Let's name it as friends
groupadd friends
useradd bob -g friends
useradd chuck -g friends
Chmod 770 ~/public/software/instructions.text

6. How would your answer to the previous problem change if you were to use ACLs (access control lists)?

Ans:

```
[vkosaraju@localhost Desktop]$ setfacl -m g:friends:rwx 1.txt
```

```
[vkosaraju@localhost Desktop]$ getfacl 1.txt
# file: 1.txt
# owner: vkosaraju
# group: vkosaraju
user::rw-
group::rw-
group:friends:rwx
mask::rwx
other::r--
```

7. What are set UID (SUID) files, and when are they typically used?

Ans:

Set User ID is a special permission which is given to user that allows user to execute the file, which is normally not given to the user. For example, let us consider a sudo command like useradd when we set S permission to it. Then, a non-root user can execute the command and add users.

8. Find one SUID file on a Linux system, and show its "long listing" (permissions, owner, etc.).

Ans:

```
[vkosaraju@localhost Desktop]$ find . -perm /6000
./1.txt
[vkosaraju@localhost Desktop]$ ls -l 1.txt
-rwSrwxr--+ 1 vkosaraju vkosaraju 12 Mar  1 18:44 1.txt
[vkosaraju@localhost Desktop]$
```

9. Why are SUID root files considered a security issue?

Ans:

This special permission is considered to be a security risk, because some of the users can misuse the permissions given and they maintain the permissions that are granted to them by the setid process even after the assigned work is done.

.

10. What command would be used to set a file foo to be SUID, and how exactly would it be done?

Ans:

chmod u+s foo

chmod 4* foo (octal method)**

11. What command could determine the process ID (PID) of a running SSH server (sshd)?

Ans:

ps aux | grep sshd | head -1

12. What command would best identify which process is using excessive CPU resources?

Ans:

'top' command can be used to look at the %CPU resources used.

13. What command that should definitely terminate the process identified above?

Ans:

Kill -9 {pid}

14. What file contains the list of valid user ID's (UID's) and their associated usernames?

Ans:

/etc/passwd

15. What file contains passwords on a Linux system (if that system is using local authentication rather than NIS, etc.)?

Ans:

/etc/shadow or /etc/shadow-

But the password is salted and hashed.

16. What is difference between telnet and ssh. When will you use each command? give examples.

Ans:

Secure shell, often referred as SSH and Telnet are two network protocols that have been used to connect to remote servers. The primary difference between them is security. SSH offers security measures whereas telnet doesn't offer any security whatsoever.

Telnet is designed to operate in private network, not I public network. Telnet also doesn't offer authentication, whereas, SSH does. Telnet sends data as a plain text. SSH uses public key for authentication. SSH adds bit more overhead to the bandwidth as it should accommodate security mechanisms along with the data in the packets.