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

Ans: ls command

Ls-l for the long list.

2. What is the simplest command for adding execute permission to file ~/foo, for all users

(without changing any other permissions)?

Ans: Chmod 777 ~/foo No restrictions on permissions. Anybody may do anything. Generally not a desirable setting.

Chmod 755 ~/foo The file's owner may read, write, and execute the file. All others may read and execute the file. This setting is common for programs that are used by all users.

3. Explain what execute permission means/allows when it is associated with a directory.

Ans: The ability to cd into this directory, and access the files in this directory.

For example, if the file was a binary executable, write access would allow you to modify it,

read access would allow you to view it, but without execute permissions you would not be able to run the program.

In the case of a script, its a little more complicted, because you don't necessarily need to 'run' the program,

you can just read its contents into an interpreter, which itself has the execute privilege,

but you do not need execute permissions on the script itself.

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 744 filename. The owner may read and write,execute a file, while all others may only read the file. A common setting for data files that everybody may read, but only the owner may change.

If we give only read permissions, users unable to change or delete the file security issues will be little less when compare to write and execute permissions.

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: Chmod 744 instructions.text

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

control lists)?

Ans: # setfacl -m "u:username:permissions" or # setfacl -m "u:uid:permissions"

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

Ans: SUID (Set owner User ID up on execution) is a special type of file permissions given to a file. Normally in Linux/Unix when a program runs, it inherits access permissions from the logged in user. SUID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file owner rather that the user who runs it.

In simple words users will get file owner’s permissions as well as owner UID and GID when executing a file/program/command.

8. Find one SUID file on a Linux system, and show its “long listing” (permissions, owner,

**Ans**:

Sample Output

-rwsr-xr-x 1 root root 42856 2009-07-31 19:29 /usr/bin/passwd.

We Use “S” instead of “X” while giving pernissions.

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

Ans: A attacker can exploit setuid binaries using a shell script or by providing false data. Users normally should not have setuid programs installed, especially setuid to users other than themselves. For example, you should not find setuid enabled binary for root under /home/vivek/crack. These are usually **Trojan Horses** kind of programs.

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**

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

Ans:

pidof {process name}

or

ps aux | grep {process-name}

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

Ans: $ Top to see all the process

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

Ans : Kill {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 authen-

tication rather than NIS, etc.)?

Ans: /etc/shadow

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

## Ans : Telnet

1. Telnet is the joint abbreviation of Telecommunications and Networks and it is a networking protocol best known for UNIX platform.
2. Telnet uses the port 23 and it was designed specifically for local area networks.
3. Telnet is not a secure communication protocol because it does not use any security mechanism and transfers the data over network/internet in a plain-text form including the passwords and so any one can sniff the packets to get that important information.
4. There are no authentication policies & data encryption techniques used in telnet causing huge security threat that is why telnet is no longer used for accessing network devices and servers over public network.

SSH

1. SSH stands for Secure Shell and it is now only major protocol to access the network devices and servers over the internet.
2. SSH runs on port 22 by default; however it can be easily changed.
3. SSH is a very secure protocol because it shares and sends the information in encrypted form which provides confidentiality and security of the data over an un-secured network such as internet.
4. Once the data for communication is encrypted using SSH, it is extremely difficult to decrypt and read that data, so our passwords also become secure to travel on a public network.
5. SSH also uses a public key for the authentication of users accessing a server and it is a great practice providing us extreme security.
6. SSH is mostly used in all popular operating systems like Unix, Solaris, Red-Hat Linux, CentOS, Ubuntu etc.