About permissions --> First of all, think about:
   * who: user
   * what happens (action): can/can not read (or display)/modify/create/delete/change to/run (or execute)......
   * with regard to what: file/directory (or foder)
   * why (explanation, cause): permission is/is not assigned

Example:

a) Question: Can user dacomo read the contents of file test.sh?

b) Check

```
dacomo@inf1-dacomo:/usr/bin$ ls -ls test.sh
20 -rwxr-x--x 1 root root 17654 feb 5 13:25 test.sh

dacomo@inf1-dacomo:/usr/bin$ id
uid=1000(dacomo) gid=1000(dacomo) grups=1000(dacomo),100(users),125(vboxusers)

dacomo@inf1-dacomo:/usr/bin$ cat test.sh
cat: test.sh: Permission denied
```

c) Analyse

who is the user trying to read the contents of test.sh?--> user dacomo
What is dacomo trying to do? --> Read the contents of test.sh
Is dacomo the owner of test.sh? --> No
Is dacomo member of the group with special permissions on test.sh? --> No
Is dacomo member of others? --> Yes
What are the permission of dacomo on test.sh for dacomo --> --x
What is the permission required? --> Reading
Is the reading permission set for dacomo on test.sh? --> No

d) Answer

1.- who, what happens, what,why:
who (user): dacomo
what happens (can/can not): can not read the contents of
what (file/dir): test.sh
why (permission): because the reading permission is not assigned to dacomo on test.sh

2.- Final sentence:
dacomo can not read the contents of test.sh because the reading permission is not assigned to dacomo on test.sh