Review Question Chapter 4:

4.8)
A Family of Role-Based Access Control Model $RBAC_0$ is the minimum requirement for an RBAC system. $RBAC_1$ adds role hierarchies and $RBAC_2$ adds constrains. $RBAC_3$includes $RBAC_1$and $RBAC_2$

RBAC (Role-Based Access Control)

- The control access is defined based on the roles of the user
  i) The user roles are defined within the system and the access allowed in a given roles

RBAC Models:

1) $\boldsymbol{RBAC_0}$: Base model
2) $\boldsymbol{RBAC_1}$: Role Hierarchies
3) $\boldsymbol{RBAC_2}$: Constrains
4) $\boldsymbol{RBAC_3}$: Consolidated model

$RBAC_0$ - Base model
$RBAC_0$ has the minimum functionality for the RBAC system, it has 4 types of entities.

User:
1) User has the access right of computer system
2) Each user is associated with a user ID

Role:
1) Role is named job function to control the computer system in the organization
2) Role is a description of the authority and the responsibility

Permission:
1) The approval process for a particular mode of access to one or more object

Session:
1) It is a mapping between the user and an activated subset set of roles assigned to user

$RBAC_1$ – Role Hierarchies:
1) It includes the $RBAC_0$ functionalities
2) Role hierarchies reflecting the hierarchical structure roles of an organization
3) It enables one role to inherit permissions from another
   (1) Greater responsibility job functions have a greater authority to access the source
   (2) A secondary job functions have subset of access rights to the superior job functions

$RBAC_2$ – constraints:
1) The roles or a condition related roles defines the constraint relationship
2) It has three roles
   a. Cardinality – set a maximum number based of roles

b. Mutually exclusive roles – The limit might be static or dynamic and the user can be decided only one role in the set

c. Prerequisite roles – Particular role will only assign to a user if it is already assigned to some other specified role

$RBAC_3$ – Consolidated model:
This model contains the functionality of $RBAC_0$, $RBAC_1$, $RBAC_2$

Problems Chapter 4:

4.8)

a) For a traditional DAC, there will be 1 possible relationship between users and permissions must be defined
b) For RBAC scheme, there will be $U \times P$ relationship between users and permission must be defined.
   Because U is a set of individuals, P is a set of permissions required,
   P $\Rightarrow$ h one or more roles of user
   User roles $\Rightarrow$ one or more P

4.12)
RBAC:
A RBAC enable a system administrator or an organization administrator to control the user access to the system or database, and let uses perform after they login. The administrator privileges and roles with the login accounts for implementing the RBAC.

Roles: (See page. 131)
We can define the roles as the groups of permissions those can be linked with or granted to the users. It offers an appropriate way for packaging the permission needed to do a job. Roles can be applied to the entities that they are created. For example, it can be applied only to the system if a role is created at the system level.
We can think the **online entertainment store** example,

a) Adult (age ≥ 13)
b) Juvenile (age < 17 and age ≥ 13)
c) Children (age < 13)

Privileges:
This control each and every action in the online entertainment store. The actions are allowed within the online entertainment store. We can think that each role is assigned with certain permissions/privileges to the user while they are registering.

a) Can watch the R-rated movies
b) Can watch PG-13 rated movies
c) G-rated movies

In above example, adult can watch all movies. Juvenile can watch PG-13 rated movies. Children can watch G-rated movies