Q1. What is Data Security?

Ans: Choosing the data set each user or group of users can see is one of the key decisions that affects the security of your Salesforce org or app. Once you've designed and implemented your data model, give some thought to the kinds of things your users are doing and the data they need to do it.

Q2. How data security is implemented in Salesforce?

Ans: The salesforce platform makes it easy to specify which users can view, create, edit, or delete any record or field in the app. You can control access to your whole org, a specific object, a specific field, or even an individual record. By combining security controls at different levels, you can provide just the right level of data access to thousands of users without having to specify permissions for each user individually.

Q3. What are the different levels of security?

Ans: Organization

Object

Field

Record

Q4. What is Organization Level Security?

Ans: For your whole org, you can maintain a list of authorized users, set password policies, and limit logins to certain hours and locations.

Q5. What is Object level security? And how is it implemented?

Ans: Access to object-level data is the simplest thing to control. By setting permissions on a particular type of object, you can prevent a group of users from creating, viewing, editing, or deleting any records of that object. For example, you can use object permissions to ensure that interviewers can view positions and job applications but not edit or delete them.

Q6. What is a Profile? How many types of Profile in Salesforce?

Ans: A profile is a collection of settings and permissions. Profile settings determine which data the user can see, and permissions determine what the user can do with that data.

- The settings in a user's profile determine whether she can see a particular app, tab, field, or record type.

- The permissions in a user's profile determine whether she can create or edit records of a given type, run reports, and customize the app.

Q7. What is the difference between Profile and Permission sets?

Ans: Profile's are like global, and permission sets are local.

When we assign a profile to a user, whatever securities we defined in that profile are assigned to that user and many users too who are having assigned to this profile.

comes to permission sets these will give more flexibility, means if one user among them need more security or accessibility, we define a permission set and assign it to the particular user, this work's with appropriate user only.

Q8. Can a user be associated with 2 profiles?

Ans: No, a user can be associated with only one profile.

Q9. Can a single profile be assigned to users?

Ans: Yes

Q10. What is field level security?

Ans: You can restrict access to certain fields, even if a user has access to the object. For example, you can make the salary field in a position object invisible to interviewers but visible to hiring managers and recruiters.

Q11. Can we delete a user from the organization?

Ans: No, we can deactivate and freeze a user.

Q12. What is the difference between freeze and activate user in salesforce?

Ans: **Freezing** a user in Salesforce means that only stops the user from being able to login.

Deactivating a user in Salesforce means that user will not be deleted from the system but will no longer be able to log in to Salesforce and their records can be transferred to another user. They cannot be part of workflows or part of any automated processes.

Q13. What is Record level security?

Ans: You can allow particular users to view an object, but then restrict the individual object records they're allowed to see. For example, an interviewer can see and edit her own reviews, but not the reviews of other interviewers.**Q14. What are the ways of Record level security?**

Ans: You can manage record-level access in these four ways.

- Organization-wide defaults
- Role hierarchies
- Sharing rules
- Manual sharing

Q15. What is OWD? What all access levels are in OWD?

Ans: Organization-wide defaults specify the default level of access users have to each other’s’ records. You use org-wide sharing settings to lock down your data to the most restrictive level, and then use the other record-level security and sharing tools to selectively give access to other users.

Access levels are Private, Public Read Only, Public Read/Write.

Q16. What is the difference between Public read only and private OWD access level?

Ans: Public Read Only

All users can view and report on records, but only the owner, and users above that role in the hierarchy, can edit them.

Private

Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.

Q17. What is controlled by the parent access level?

Ans: Asume A1 is Master object and B1 is child object in a master detail relationship.
OWD for A1 is private & OWD for B1 is controlled by parent & user has edit access on A1(custom object). So, if user shares A1 records with access level=Read/write, then other users can will be able to edit B1 records

Q18. What is the difference between role and profile?

Ans: profile - profile is basically an object level access and field level access and it is required for the users.

role - role is basically a record level access and it is not required for users.

Q19. What is the Governor limit of sharing rules?

Ans: You can define up to 300 total sharing rules for each object

Q20. What is the sharing rule?Types of manual sharing?

Ans: Sharing rules are automatic exceptions to organization-wide defaults for particular groups of users, so they can get to records they don’t own or can’t normally see. Sharing rules, like role hierarchies, are only used to give additional users access to records. They can’t be stricter than your organization-wide default settings.

Only these 4 users can share the record:

- Record Owner
- A user in a role above the owner in the role hierarchy.
- Users granted “Full Access” to record.
- Administrator

Q21. What is a public group?

Ans: Public groups is to assign things or resources to it which are meant to be seen or used by everyone in the organization. Making a data or resource to everybody in an organization may be cumbersome and time consuming but by assigning it to a public group it can be done with 1 click.

Q22. If the Owd access level of the account is set to private then what will be the default access level of opportunity?

Ans: Private