In this report I have mentioned all the learnings of today. I have learnt about Directory, difference between a directory and a relational database, LDAP, Web access management, Header based authentication, SAML, OAuth 2.0 and OpenID.

**Directory:**

* Directory is a hierarchical structure that is used for searching and reading information.
* It is more optimized for reading rather than writing. It means that in a directory maximum operation performed will be of type read.
* The major purpose of directory is store attributes such as name, location, user id etc. It not only stores info about people but also about physical devices on a network such as printers, routers, PC’s etc.

**Directory Vs Database:**

* Directory provides a simple way of accessing resources whereas Database are used for transactions with more write to read ratio.

**Importance of Directory in IAM:**

* Directories are used to store the identities attributes such as first name, last name, mobile number etc.
* They provide a common way to authenticate the identity by using the LDAPstandard protocol.

**LDAP:**

* LDAP stands for Lightweight Directory Access Protocol.
* As the name suggests the operations are much faster as compared to Relational databases.
* It is a client server based standard protocol which is used to connect with directory.

**LDAP Tree:**

* A hierarchical structure is used to represent the entries of organization in a directory.
* It is also called as a namespace or a directory information tree.

1. Organization: It is the topmost level of a LDAP tree. Generally, company name is given in Organization. Eg. o=Deloitte.
2. Country: It provides the geographical location. Eg. c=India
3. Organizational Units: It allows us to store other containers such as users and groups.
4. Person: It is a type of an object class in a directory. cn=Chirag Gaur, UID=123
5. Group of unique names: It allows us to group objects to allow performing operations simultaneously.

**LDAP Schema:**

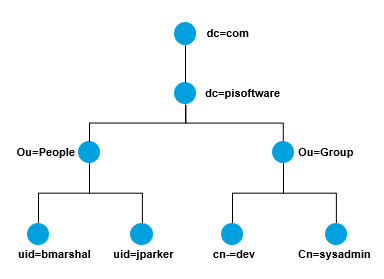
* LDAP schema defines the type of objects that a directory may have. It may include mandatory and optional attributes of each object.

**Object Class:**

* Object class is used to group related information.
* It maps real world entities to objects such as Person or a printer**.**
* Eg: object class: Person
* cn: Chirag; c: India

**Distinguished Name:**

* In a directory every object must have unique name. It includes unique attribute values as well as Path going back to tree.



* In above diagram distinguished name example can be:

Cn=dev, ou=group, dc=pisoftware, dc=com

**LDAP operations:**

Common LDAP operations are

* Bind
* Search
* Add, modify and delete

**LDAP Bind operation:**

* A client initiates a connection with the LDAP server by sending the server a “bind” operation that contains the authentication information.
* An LDAP request sent by a client without doing a “bind” is treated as an anonymous client.

**LDAP Search operation:**

* Search operation can be performed using command line tools or LDAP browser.
* It is the most common operation.

**Web Access Management:**

* Web access management controls the access to web resources.
* It provides authentication management, policy-based authorizations and single sign on.

**Header based Authentication:**

* In header-based authentication, users are authenticated based on the user’s information received in the HTTP headers.
* It allows users to log in automatically based on a request header.

**SAML:**

* SAML stands for Security Assertion Markup Language. It is a standard which allows users to log into multiple applications using single sign on option.
* As the user’s identity is stored in directory so it would make more sense to fetch those identities from the active directory and log users into different applications.
* Eg: In Deloitte username and password remains stored in the directory and the target applications such as Skype, outlook, teams etc will be logged in automatically using the same credentials for all of them.
* SAML transfers the user’s identity among the two parties. These two parties are identity provider and service provider.
* **Identity Provider** — It authenticates the user's identity and authorizes to the service provider.
* **Service Provider** — It authorizes the given user to access the requested resource.

**Advantages of SAML:**

* Enhanced user experience
* No need to remember passwords
* Increased Security

**OAuth 2.0:**

* OAuth stands for Open Authorization. It is a standard protocol which allows an application or website to have access to resources which are hosted by some other application.
* It allows a client application to perform some actions on the resources on behalf on user without having user’s credentials.
* The principle of OAuth 2.0 is based on authorization. It uses access tokens.
* Access token is a data which allows to perform authorization in order to gain access of resource.

**OAuth 2.0 Roles:**

1. *Resource Owner* is the one who grants access to resources.
2. *Client* is the one who wants to get the access of some resources.
3. *Authorization server* receives the request for access token from client and after successful authentication, it grants them the access token.
4. *Resource server* protects the user’s resources.

**OpenId:**

* It is an extra identity layer added on top of the OAuth. It allows to check the identity of the user based on authorization done by authorization server.
* In this we can fetch additional info about end user

**Identity Access Management: is a very big part of it.**

Managing identities is a very imp thing.

IAM is about creating an acc in AD and use that identity to provision to end points (i.e laptops, databases,

WAM uses that identities and grants access to web resources. We need to write correct set of policies such that an user have only access to allowed web pages.

Whenever accessing any web page, It will go and check attributes from LDAP.

Authentication: verification. Proving that you are the one who u r proving to be.

Authorization: giving access to right set of identities. Least privileged access.

Auditing: whatever some one is doing on web access and then there should be annual audit or review

SSO: Single sign on

How to protect security in SSO?

User id and password is not sufficient these days so adding extra layer of security is very imp.

First layer of authentication is something that we know such as user id and password. It is not a safer option.

Second layer of authentication is something we have. Ex. Tokens, Authenticator, smart card, badge

Third layer of authentication is something we are. Ex. Biometric, Retinal Scan, Voice Print

MFA is about adding additional layer to single sign on option. It is a two-factor authentication.

Web access mgt is divided into web, access and mgt. We provision access to app

Load Balancer is distributing the load on different servers

Server is a machine running some program and we can utilize that program.

Load balance can act as a

1. Forward Proxy: it has some firewalls. It checks for request and returns the response accordingly.
2. Reverse Proxy: It check the user request when accessing any application

External network requests can be handled by external servers. So, these external servers are known as DMZ (demilitarized zone)

AWS has its own servers and own tools.

Onpron servers are those servers which we have ownership of.

Majority of servers are used along with Linux,