CompaTia2

Kerboros.
network authenication mechanism used withinwindows active directory domains and some unix environments known as realms. prvent ON PATH attacks MAN IN MIDDLE

requiuirements to work with kerboros.

a method of issuing tickets for authentification thE kEY DISTRIBUTING center uses complex process of issuing ticket granting ticket and other tickets the KDC OR TGT SERVER packages user credewntials within a ticket. tickets provide authentication for users when they access re3sources susch as files on a file server. these tickets are sometimes referred to as tokens TIme synchronozation. kereros version 5 requires al lsystems to be synchronized. "logical tokens.. not a key fab token.. like "something you have"
timestamp limits the times users try to acces

a database of subjects or users.
Kerberos is a network authentication protocol within a microsoft windows active directory domain. or a unix realm It uses a ddatabase of objects such as active directory and kdc for tgtserver to issue timestampd tickets that expire after a certain time period.

SSO AND A FEDERATION

some sso systems can connectu acuthenication mechanisms from different environments such as os or a diff network. One common methon with a federated identity management system oten integrated as a deferated database this federal database provides central authentication in a non homogeneous environment. .

a federation requires a federated identit;y management system that al members of a federation use..linkes a users credentioals from different networkds. treats it as one entity

SECURITY aSSERTION mARKUP lANGUAGE. IS AN EXTENSIBLE MARKUP LANGUAGE XML. DATA FORMAT USED FOR SSO ON WEB BROWSERS.

**many us SAML OR SSO""\

principal = user
IDP identity providor managed sthe identy information for principals.URPOS OF SSO IS FOR THE ID AND AUTHENTICATION OF USERS.

OAUTH IS AN OPEN STARTD FOR AUTHORIZATION MANY COMPANIES USE OTO PROVIDE SECURE ACCESS TO PROTECTED RESOURCES.

OAUTH FOCUSES ON AUTHORIZATION.

**OPENID AND OPENID CONNECTIONS.*
openid.

the authentication standard maintained by the OPen ID foundation. An OpenID provider holds the users credentialsand websites that support OpenId prompt users to enter OpenIdOpemID connection OICS builds on OpenID for authorization and uses OAuth2.0 framework Instead of authorization tokens OIDC uses javascriptobject((Javascript object Notation web token somethimes called an ID token.
))
SAML IS AN XML BASED STANDARD USED OT EXCHANGE AUTHENTIFCATION AND AUTHORIZATION INFORMATION BETWEEN DIFFERENT PARTIES SAML PROVIDES SSO FOR WEB BASED APPLICATIONS.

SERVICE PROVIDER....

SAML AND AUTHORIZATION .
PRIMARY P

cOMPARING ACCESS CONTROL SCHEMES.
"

```

**ROle based access Control
Rule based acces sCOntrol
Discretionary access control
Mandatory access control
attribute based access control.
---------Subjetcts are typically users or groups tha access an object.
sometimes. the subject may be a service that is using a service account to
access an object.
Objects::
 are items such as files, folders, shares, ad printers that subjects access.
the  acess control helps determine how a system grants authorization to
objects.



 ***ROLE BASED ACCESS CONROL.(ROLE-BAC)*   uses roles to manage rights and
permissions for users. this is useful for users within a specific department
who perform the same jon functions. an administrator creates the roles then
assins specific rights and permissions instread of the users.  WHEN AN
ADMISNISTRATOR ADDS THE USER TO A ROLE, THE USER HAS ALL THE RIGHTS AND
PERMISSION OF THE ROLE.
 **
```

**USING ROLES BASED ON JOBS AND FUNCTIONS. **

---ROLE BASE..   ADMINISTRATOR, EXECURITVES , PROJECT MANAGERS, TEAM MEMBERS.

DOCUMENTING ROLES WITH MATRIX.
roLE-BAC is also calle hierarchy based or job baseed.

Hierarchy based.. in the project server example you can see top level roles uch as administrator.

job,, task, or function based...... the project server example also shows how the roles are centered oon jobs or functions. that users need to perform.

Mac adress (machine)=mandatory access control.   is one of sever access control schemes. discussed. Also. Message authentication code. provides integreity similar to how a hash is used.

DAC Discretionary Access Controll uses a new file system "ntfs' windows. proveds secuirty by restinging acess.   is based on a DAC
SCHEME "
SIDS/DACL
MICROSOFT SYSTEM iDENTIFYERS... instead of a system displaying a sid(f-1-11-2-3l884009479098-)example   it looks up the name associated with the SID Nd displays the name

DIRECTORY ACCESS CONTROL LIST. identfifies who can access a system using the dac scheme. THE DACL IS   list of access control entries. ACEs each ACE composted of a SID and the permissiond grand=ted to the SID.

**The DAC SCHEME SPECIFIES THAT EVERY OBJECT HAS AN OWNER AND THE OWBNER HAS FULL EXPLICITY CONTROL OF THE OBJECT. MICROSOFT. NTFS USES THE DAC SCHEME.

MANDATORY ACCESS CONTROL SCHEME USES LABELS. SENSITIVE, AND SECURITY TO DETERMINE ACCESS **
the dac scheme is significantly more flexible than the mac scheme . MAC has predefined access privileges and the administrator is required to make the changes. with DAC   if you want to grant another user access to a file you

```
own.  you simply make the change .




 **selinux policy is a set of rules that override standard linux permissions
however even if a selinux polisy is in place it isnt necessarily enforced
selinux has 3 modes.

 1.  enforming mode will enforce selinux policy and ignore permissions.
 Permissive mode does not enforce the selinux policy but instead uses
permissions.

 disbabled mode does not enforce the selinux policy and dows not log
anything related to the policy**

 **THE DAC SCHEME SPECIFIES THAT EVERY OBJECT HAS AN OWNER AND THE OWNER HAS
FULL EXPLICIT CONROL OF THE OBJECT . mICROSOFT NTFS USES THE DAC SCHEME.**

 LABELS AND LATTICE.
  THE mac SCHEME USES DIFERENT LEVELS OF SEURITY TO CLASSIFY BOTH THE USER
AND THE DATA the levels are defined in lattice which can be a complex
relationship between different ordered set of labels. eac \h of these levels

  ::: **THE MAC SCHEME **USES SENSITIVITY LABESLS FOR USERS AND DATA.. IS
COMMONLY USED WHEN ACCESS NEEDS TO BE RESTRICTED BASED ON A NEED TO KNOW.
SENSITIVITY LABELS OFTEN REFLECT CLASSIFICATION LEVES OF DATA CLEARANCES
GRANTED TO INDIVIDUALS



  *attribute based access control.
 *evaluates attributes and grants access based on the value of those
attributes.
 **


 attributes can be almost any charachteristic of user, the environment or
the resource.. abac uses policies to evaluate attributes and grant access
when the system detects a match..
 many software defined networks.  (SDNS  us AMAC schemes  instead of rules
on a physical routers, policy through the amac system conrol the traffic.
these policies typically use plain language and statements.
 )

 SUBJECT---- THIS IS TYPICALLY THE USER
```

OBJECT --- this is the resource (such as file, database or application)that is attempting to be accessed.
ACTION=---- THIS IS THE ACTION the user is attempting to do ,such as readying, modifying
ENVIRONMENT---the environment includes everything outside of the subject and object attributes. this is often referrred as the context of access request

------tHE ABAC scheme uses attributes defined in policies to grant access to resources its commonly used in software defined networkssdns.

a ABAC system has a lot of lexibility and can enforce both a DAC and a MAC scheme. there are also many similarities between the ABAC dac mac .
DAC scheme owners ove control over the access..
ABAC scheme. owneres can create policies to grant access.
MAC ses labels assined to both subjects and objects and grants access when a policy idnetifies a match.

CONDITIONAL ACCESS
mICROSOFT HAS IMPLEMENTED CONDITIONAL ACCESS WITHIN AZURE ACIVE DIRECTORY ENVIRONMENT IT CAN BE USED WITH TRADITIONAL ACCESS CONTROL SCHEMES BUT ADDS ADDITIONAL CAPABILITES TO ENFORCE ORGANIZATIONAL POLICIES, CONTDITIONAL POLICIES