Ques:

Consider the following scenario where we have people in the marketing department of an organization. Each member of this group needs to be provided access to a copier machine, a web server, and several folders and files. What kind of access control model best suits to handle this scenario. Explain the access control model in question using the scenario as example. Describe the advantages of this model and disadvantages if this access control model is not used using the scenario as example. [1 + 2 + 2 + 2 = 7]

Ans:

a) RBAC

b), c) and d) Answers will be evaluated when given scenario-based explanation is provided

Ques:

Consider that a subject means a user or process and an object means a file or other resources that subjects can access.
Describe the characteristics of per-object access control list. Using an example, explain the advantage(s) of using per-object access control list. What might be a disadvantage of using such access control list? Suggest an alternative means of handling this particular disadvantage. [2 + 2 + 2 = 6]

Ans:

a) ACL's mechanism works on subject and object; and definition of such parameter changes from system to system, like in an operating system a file tries to access a resource, here; the file is the object while resource is the subject.

The per-subject ACL creates the access list directory for each subject with their specified access by different objects.

Per Subject ACL Characteristics:

- It works on a subject (in our case, user/process) and an object (in our case, files/other resources)
- It creates an access directory list for each subject with their specified access by different objects
- While an object tries to access a resource, its compatibility with the resource in terms of the user is being checked
- To delete access by the subject the entries that correspond to that object is omitted from the access list.

b) and c) answers will be evaluated when given scenario-based explanation is provided

Ques:

a. Develop an attack tree to gain access into someone's corporate account.
b. For any two of the components, discuss attack strategies.
c. What is the purpose of attack tree in the context of security management? [2 + 2 + 2 = 6]

Ans:

Since attack tree can be created in multiple way, hence we are not providing one answer, evaluation will be done on answers provided, and necessary comments will be provided.

Ques:

For below questions you need to fill THIS value [1 X 5 = 5]
a. THIS layer is responsible for moving frames from one hop to next
b. THIS layer adds a header to packet comes from upper layer that includes the logical addresses of the sender and receiver
c. THIS layer is responsible for the delivery of a message from one process to another
d. THIS layer changes bits into electromagnetic signals
e. THIS layer has responsibility for process-to-process delivery of the entire message

Ans:

1. **Data Link layer**
2. **Network layer**
3. **Transport layer**
4. **Physical layer**
5. **Transport layer**

Ques:

a. Suppose you have network address of 162.26.0.0/19, this network can provide how many subnets and hosts? Explain
b. For a network which requires 28 subnets while maximizing the number of hosts addresses available on each subnet, how many bits one must borrow from the host field to provide the correct subnet mask? Explain
c. Suppose we have a local subnet that uses the 255.255.255.224 subnet mask, what is the maximum number of IP addresses that can be assigned to it? Explain [2 + 2 + 2 = 6]

Ans:

(a) 8 subnets, 8,190 hosts each, A CIDR address of /19 is 255.255.224.0. This is a Class B address, so that is only 3 subnet bits, but it provides 13 host bits, or 8 subnets, each with 8,190 hosts.

(b) We need to borrow 5 bits, The number of subnets can be calculated using this formula, 2^n (where n is the number of host bits borrowed)
We need a network that requires 28 subnets, so 2^n >= 28
To calculate this, we need to figure out n which satisfies 2^n >= 28
Let's consider n as 4, we get 2 ^ 4 = 16 which is not >= 28 so n=4 isn't correct
Let's consider n as 5 , we get 2 ^5 = 32, since 32 >=28 is true, hence the number of bits to borrow from host field to provide correct subnet mask is 5

(c) 30 IP addresses, A /27 (255.255.255.224) is 3 bits on and 5 bits off. This provides 8 subnets, each with 30 hosts.