Ques:

Consider the following scenario where we have certain sales people in the organization. Each of the team member needs to be provided access to a printer, a file 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 Twitter 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 changes bits into electromagnetic signals
b. THIS layer has responsibility for process-to-process delivery of the entire message
c. Mail services are available to network users through THIS layer
d. THIS is process to process protocol which adds only port addresses, checksum error control, and length information to the data from the upper layer
e. THIS address also known as the link address, is the address of a node as defined by its WAN or LAN

Ans:

a. Physical layer

b. Transport Layer

c. Application layer

d. UDP

e. Physical

Ques:

a. Suppose you have an interface on a router with the IP address of 192.168.192.04/29, now including router interface, how many hosts can have IP addresses on the LAN attached to the router interface? Explain

b. Suppose you have network address of 152.26.0.0/19, this network can provide how many subnets and hosts? Explain

c. For a network which requires 29 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   [2 + 2 + 2 = 6]

Ans:

(a) **6 hosts,** A /29 (255.255.255.248), regardless of the class of address, has only 3 host bits. Six hosts is the maximum number of hosts on this LAN, including the router interface.

(b) 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.

(c) **5 bits,** A 240 mask is 4 subnet bits and provides 16 subnets, each with 14 hosts. We need more subnets, so let's add subnet bits. One more subnet bit would be a 248 mask. This provides 5 subnet bits (32 subnets) with 3 host bits (6 hosts per subnet).