8.1.6 Trusts and Transitive Access Facts

A *trust* is an established relationship between different domains that allows mutual authentication, communication, and access to resources between the domains. *Transitivity* defines whether or not the trust between domains flows to other trusted domains.

Be aware of the following details about trusts:

- The direction of trust is typically identified with an arrow.
  - A *one-way* trust is a unidirectional authentication path created between two domains. For example, if Domain A trusts Domain B, the arrow would point from Domain A to Domain B. Domain A is the *trusting* domain, and Domain B is the *trusted* domain.
  - A *two-way* trust is the same as two one-way trusts in opposite directions. In other words, authentication requests are passed between the two domains in both directions.
- Resource access is granted in the direction of trust. For example, if Domain A trusts Domain B, users in Domain B have access to resources in Domain A. Remember that users in the trusted domain have access to resources in the trusting domain.
- Transitivity is implemented as follows:
  - A *transitive* trust allows the trust relationship to flow among domains. For example, suppose we have established a two-way transitive trust between Domain A and Domain B. If we now establish a two-way trust between Domain B and Domain C, then Domain A will also trust Domain C. This is based on the principle of transitivity.
  - With a *non-transitive* trust, trust relationships must be explicit between domains. In other words, non-transitive trust relationships restrict trust to just the two domains. The trust relationship does not flow through to any other domains in the forest. By default, non-transitive trusts are one-way. However, you can create a non-transitive two-way trust, which is, essentially, two one-way trusts that go in opposite directions.
- By default, Active Directory creates two-way transitive trusts between parent and child domains in the tree or forest. These are known as Active Directory trusts or Kerberos trusts.

A transitive access attack involves threat agents acquiring more trust than they should by joining the domain. Therefore, they have unauthorized access to resources.