Experiment No. 4

Managing Security in a Small Business Network

Objectives

Server/client networks are important to establish when the number of computers in your network increases and therefore it becomes impossible for peer to peer networks to handle all the computing. In such model, security is maintained easier, since the server is responsible for managing all the other users. In server based environment, users and computers are created and granted access according to the administrator's needs. Different rights are assigned to users and computers, giving the ability for the users/computers to print, use internet etc …

In this lab, a small business network is established in which an active directory is installed and users and computers are added to form a base for the network security. In order to acquire a better understanding of how an active directory works.

Active Directory

Active directory is a tool created by Microsoft windows that provides a variety of network services which include DNS naming, secure access to resources, Kerberos based authentication, LDAP directory and many more other services. It is mainly used to create users, computers, groups, sites etc. and stores all the information related to these entities, in addition to security policies and trusts. Active directory can occur in different environments with different types. It can be local or global.

The structure of active directory is a hierarchy which starts with forests, domain, organizational units and individual users or computers as shown in fig 1. It contains also trusts, groups, sites replication and global catalog as its building block. Everything that the active directory is responsible for and tracks is called objects. Objects can be either resources (printer (or security principals) user/computers. Every object has its own characteristics that identify the kind of object that can be stored in the Active directory. The hierarchy can consist of multiple domains which are under each other, or connected parallel to each other establishing trusts between them.

Fig.1 Active Directory Hierarchy
Active Directory objects are:

*Site* is an object that represents a subnet which is classified according to geographical location. It can be used to assign group policies. Multiple sites can be connected to each other to provide reliability and availability of the resources.

*Domains:* are the heart of the active directory, that basically consists of the internet naming. It can contains multiple nested OU’s.

*Tree* is a collection of one or more domains or domains trees link in a transitive trust hierarchy.

*Organizational Unit* is a container that contains all the objects in the domain. Organizational units can be divided according to geographical, organizational or logical locations of users and computers. It mainly eases the administration and simplifies the structure of AD so security rights can be assigned to certain OU’s.

*Groups* are divided into two types: security and distribution. Security groups which contain accounts controlled by security policies. While a distribution group is.

**Note:** It is so important to plan the architect of your network before starting to build the hierarchy of active directory. If the architect is not well built from the beginning it can be a whole mess going down the road. In addition, it is recommended to limit the number of domains and instead increase the number of organizational units to

### Before installing Active Directory

- Configure static IP address
- If your server contains two network cards configure the networks cards as shown in the figure below:

![Fig.2 ET-111 Lab Network](image-url)
Note: When configuring two network adapters on the server, you need to add a DNS forwarder. Go to DNS > Forwarder > Add DNS. Add the DNS provided by your ISP.

Installing Active Directory

1. Click **Start > Run > dcpromo > Ok**, to start the installation Wizard then click **Next**
2. Choose **Domain Controller for a new domain > Next**
3. Choose **Domain in a new forest > Next**
4. Enter the full DNS name for the new domain (for example: ET111.local)
5. Accept the default domain NetBIOS name (ET111)
6. Accept the default database and log file location
7. Accept the Sysvol folder location on
8. **Install and configure the DNS server on this computer**
9. Check **Permissions compatible only with Windows 2000 or Windows Server 2003 servers or operating systems.**
10. Enter a password for the directory service restore mode.
11. Review and confirm the options that you selected > **Next**.
12. Restart your computer when prompted.

Confirm the installation of Active directory

- Confirm that the active directory administrative tools are installed.
- Confirm that the DNS service location records have been created

  a. **Start > Administrative Tools > DNS > DNS**
  b. Expand :Server name > Forward Lookup Zones > domain.
  c. Verify that the _msdcs, _sites, _tcp, and _udp folders are present.

Creating users and computers

Users and accounts are also active directory objects that we will manage to enable individuals to logon into the network and access resources.

Users’ accounts can be either domain users or local users. Domain users are users that are given the permission to access all the resources on the domain while local users are given the access only to logon and access resources on that computer you linked the user to.

To create a domain user account:

1. Go to **Administrative tools > Active directory users and computers**
2. Right click the **OU > New > User**
3. Fill out the user information (first name, last name, initials, logon name)
4. Type the user **password**
5. Select the appropriate password option > **Next > Finish**.

To create a local user account:
1. Go to **Administrative tools > computer Management**
2. Expand Local users and groups
3. Fill out the user information (first name, last name, initials, logon name)
4. Type the user **password**
5. Select the appropriate password option > **Next** > **Finish.**

**Conclusion**

Creating users and computers enhances the security by providing an ease of management and facilitating the management of rights and trusts. Only authenticated users are able to access computers and therefore data. If a hacker was able to connect to the external interface network, the access of information would be unreachable since his computer is not added to the domain and he doesn’t have a user account that is authenticated. So, active directory users and computers play a very important role in isolating and managing the network more efficiently and securely.

**Future work**

The next lab will focus more on managing the security inside the small business, to do so we will introduce group policies in details. We will implement groups on different active directory objects, test the policies, and have a clear understanding of the hierarchy of policies and rights.