UNIT 4 SECURITY AND MANAGEMENT - II

Structure

4.0 INTRODUCTION

This unit will introduce you to the concepts and configuration required for the management Microsoft Windows computers and you will be able to examine everything from the foundational principles of Windows 2000 security, up to the advanced issues of securing windows 2000 machines running Active Directory.

This unit covers in detail the various security methods that can be implemented in windows 2000 architecture. The unit addresses management of Windows 2000 system: Authentication (section 3); users and group security (section 4); resource security (section 5); windows network security (section 6); and encrypting file system (section 7). The section 3 of this unit deals with windows 2000 user authentication management and it covers the following areas; Subsystems components, and kerberos.

The section 4 of this unit deals with the users and group security management and it covers the topics like; configuring users accounts, windows 2000 groups (default group types, local groups, global groups, group policies etc.), security configuration tools, and configuration management and analysis tools.

The section 5 deals with resource security management and it covers the areas like; files and folder management, files/folder permissions, inheritance and propagation, moving data and permissions, shared resources, null session, printer management, and Registry management.

Section 6 the most important deals with the network management; NAT, ICS, RRAS, RAS, IAS, and IPSec are covered in this section.

The section 7 deals with encrypting file system (EFS), data recovery and EFS cryptography.

4.1 OBJECTIVES

After going through this unit you will be able to:

- learn windows 2000 authentication;
- user and group management;
- resource management;
- EFS Management; and
- windows network management.

Objectives of this unit are: Examine the basics of user authentication in Windows 2000, learn to manage User and Group Options in Windows 2000, manage and configure security options on Windows 2000 Resources, Examine the methods or management network communications in Windows 2000 Examine and configure EFS on Windows 2000.

4.2 USER AUTHENTICATION MANAGEMENT

Despite all the advancements and new components of Windows 2000, a user must be authenticated to access resources on the network. Windows 2000 can use the following for authentication: Kerberos, NTLM, RADIUS, SSL, Smart Cards, and more.

Windows 2000 uses the Security Support Interface (SPPI) to allow for these methods of authentication. The SPPI functions as a interface between the user applications, such as the Web Browser, and the authentication method, such as NTLM or Kerberos. An application developer need not create an application for each type of authentication possible, but create one that can communicate with SPPI.

Although the SPPI plays an important function in the authentication of users with no options for configuration or management involved in the SPPI. It simply performs its job of connecting authentication requests to the authentication provided by the system.

The administrator is involved more with Security Architecture of Windows 2000, which comprises of parts of both the Operating System and Active Directory. For example, in the Active Directory are the stored account information and policy settings, while in the Operating System is the security process that is and information regarding trusts to and from other areas of the network

If the Windows 2000 is installed in mixed mode, means that there can be both Windows NT 4.0 BDCs and Windows 2000 domain controllers present. This allows for maximum communication options over the network, but it is not the most secure environment. The reason behind this is an issue is that an older networking server, called LAN Manager, used the LAN Manager (LM) protocol for authentication and this protocol has weak security. Windows 9x and NT accepted LM authentication, and this is where the weakness lies and a password can be broken into 7-character pieces and cracked individually. Therefore, even though a 14-character password was implemented, the program that is trying to crack the password is cracking two 7-character blocks at once. The implementation of LM in Windows NT requires the system to not only accept LM authentication, but to store a copy of the LM version of the password in the Registry. Attackers will go after the LM password since they will almost match the NT password.

Microsoft addressed the issue with the default NTLM was to develop and release NTLMv2. There were several increases in the security provided by implementing NTLMv2; the key, or password, was now a 128-bit value, which will take much longer to crack, and MD5 (Message Digest 5) was used to verify the integrity of messages. In order for Windows NT 4.0 machines to implement NTLMv2 they must use Service Pack 4 or greater. If all your clients support NTLMv2, you may configure your Windows 2000 clients to do so also. This may be defined by creating a GPO for an OU that holds all the machines that must use NTLMv2. Then configure the response type, as per your network, in the Security Options, under Computer Configuration, in the Group Policy Editor.

4.2.1 Subsystem Components Management

The logon information is stored in the local Registry on a stand-alone machine or a machine that is part of the workgroup. The Windows 2000 logon process is the same as the Windows NT 4.0 logon process for a stand-alone machine and the Registry stores the user account data in the Security Accounts Manager (SAM). The SAM is used in NT 4.0 to store all user account information, and in Windows 2000 is what is used to store local user account information. But, if a Windows 2000 Server is promoted to be a Domain Controller, the local SAM is no longer accessible. The process for when a user tries to access a local resource is as follows: (1) the user account info is given to the Local Security Authority (LSA). The LSA is what creates the access tokens, provides an interactive environment for user authentication, controls the local security policy, and sends authentication requests to NTLM or Kerberos, as required, (2) the LSA gives the authentication request to NT LAN Manager (NTLM), and (3) the user request for the resource is validated by the Security Reference Monitor (SRM). The SRM performs the actual checks on user permissions to access objects.

4.2.2 Kerberos Management

In Windows 2000 no action is required to implement Kerberos. Kerberos will be used by default to authenticate network clients (with Windows 2000) logging onto a Windows 2000 domain.

Kerberos is an IETF standard used for authentication and the Massachusetts Institute of Technology (MIT) developed it during the 1980s. It is considered to be a secure method, and has been implemented in Operating Systems before the Windows 2000 implementation. There is a bit of controversy in the method used in Windows systems as it varies slightly from the standard created by MIT. However, it should be noted that Windows 2000 is able to intemperate with non-Windows 2000 machines running Kerberos.

When a user the log on process by entering his credentials, Windows will contact an Active Directory domain controller, and locate the Kerberos Key Distribution Center (KDC). An Authentication Server (AS) performs the actual authentication. The KDC responds by issuing a Ticket Granting Ticket (TGT) to the authenticated user. The TGT contains identification information about this user to various servers on the network, and is used to gain further access in the network.

After the user account has been authenticated, the TGT is used to request further Kerberos tickets in order to access network services. The machine that provides the tickets for the network resources to the authenticated client is known as a Ticket Granting Server (TGS).

The benefits to end-users of a network running Kerberos are that a Single Sign On (SSO) will be maintained and the users are not required to authenticate with each resource they wish to access in the network, and since Trusts in Windows 2000 are transitive, once a user logs on to one domain user, s/he will have access to the other domains of the network. Another key benefit of Kerberos is that it has a mechanism for verifying the identity of the user, not just authentication. This means that in a Kerberos network, if a message says it came from User X, you can be very confident it did indeed come from User X.

4.3 USERS AND GROUP MANAGEMENT

In earlier sections we examined the infrastructure of Windows 2000, including the concepts relating to the Group Policy. The following sections builds off those foundational issues, introducing users and groups into the network.

4.3.1 Configuring User Accounts

The focal point of Windows system is the users and without users being able to access the network, there is no point in having a network. There are two basic types of user accounts that may be created in Windows 2000, domain and local. A domain user account has the ability to log on to the network and access authorized resources throughout the domain. A local user account has the ability to log on to a specific computer and access authorized resources on that computer.

The default accounts in Windows 2000 server are the Guest and Administrator. Securing the Guest account and Administrator should happen right away. These steps are as follows: (1) remove the description, (2) disable all logon hours, (3) create a very complex password, (4) and allow the account to only access the network from a nonexistent machine.

4.3.2 Creating Domain User Accounts

The steps for creating domain user accounts are:

a. Open the management console MMC.

b. Open or add the Active Directory Users and Computer Snap-In.

c. Expand domain listing, to view the console tree.

d. In the Action down menu, select option New User.

e. Create new users, user1, user2, user3, user4, etc.

4.3.3 Managing Logon Hours

Once you have created several users, the next step is to restrict logon hours. That means restricting the hours in which a user can logon to the server. The steps are:

a. Open the Active Directory Users and MMC Snap-in

b. Expand domain listing, to view console tree.

c. Select user folder.

d. Double click user1.

e. In the Property Window, choose Account Tab, and select the Logon Hours Option.

f. Limit user1 so that this account can log on to the network during 10 AM to 5 PM during week days (i.e Monday to Friday).

g. Press OK to close the Logon Hours dialog box.

h. Again press OK to close the User1 Property Window.

4.3.4 Managing Expiry Date for a User Account

You can further control the access to network resources by setting a limit or expiry date for a user account.

a. Open Active Directory Users and Computers MMC Snap-In.

b. Expand domain listing to view the console tree.

c. Select user folder.

d. Double click user3 and in pr. ıerty window select the Account tab.

e. In the Account Expires Option, and select End of option, and enter a expiry date.

f. Press OK.

4.3.5 Windows 2000 Groups Management

While working with Windows 2000 you will most likely want to implement and configure a full Active Directory structure, to gain all the benefits afforded by doing so. However, when you first install a windows 2000 server, it is nothing more than a stand alone server, not even part of a domain, let alone a domain controller.

Once the machine has become a domain controller (by running DCPROMO), as the administrator there are several groups for you to manage. These groups include the Domain Administrators and Domain Users.

There are two group types, a Security Group and a Distribution group. The Distribution Group is used to manage lists, such as email lists.

4.3.6 Default Group Types

On Windows NT 4.0 that groups can be either Global or Local, in Windows 2000 this concepts is expanded. In Windows 2000 the group types are: (1) Domain Local,

(2) Computer Local, (3) Global, and (4) Universal.

Domain Local group is one that may have members from any domain in the network. These groups are only created on Domain Controllers, and can be used to provide resource access throughout the domain. The Computer Local group is used provides access to resources on the local machine only, and cannot be created on a Domain Controller.

Global group is one that combines users who often share network resources use and access needs. Global groups may contain members from the domain in which the group was created.

Universal groups are used in a multi-domain environment where groups of users from different domains have similar resource use and access needs. To implement Universal groups, the network must be running in Native mode, meaning only Windows 2000 computers.

It is also possible to combine groups together, such as Global Groups in Universal Groups. There may be a resource you are trying to control; in this case a Universal group will work for controlling access across the network. You may also place Universal Groups in Domain Local Groups, and control access lo the resource by placing permissions on the Domain Local Group.

These groups can be used for controlling access to resources; both allowing and denying permissions based on your security needs. If you are trying to secure the computer, user, and network environments, you will use Group Policies, as discussed in the previous sections.

Group Policies Management

Two of the issues that must be discussed are the options associated with Policy Inheritance and Overrides. The Group Policy Objects are implemented in the following order: Local GPO, Site GPO, Domain GPO, and OU GPO. And when there is multiple GPOs assigned lo an object such as a Domain that the highest GPO on the list takes priority over the rest of the list. You can change the order of implementation on this list by simply choosing a GPO and pressing the Up or down button to re-order the list as you desire. However, you may need to have further control than what the Up and Down option provides you.

Policy Inheritance

Policy Inheritance is the name of the process of a user or computer inheriting the final policy configuration from multiple policies, depending on where the object may be in the Active Directory hierarchy and configured GPOs. To track the policies that may be implemented as a user logs onto a computer, use the following list: (1) a Computer Policy is enabled when the computer is first turned on, (2) a User Policy is applied, (3) when a user logs onto the system, (4) the Local GPO is applied, (4) the site GPO is applied, (5) the Domain GPO is applied, and (6) the OU GPO is applied.

It is not uncommon for Sites, Domains, and OUs to have more than one GPO configured. It is also not uncommon then for there to be conflicting settings in locations throughout the policies.

No Override

One of the methods for you to manage a GPO implementation is through the No Override option and this option is available on any Site, Domain, or OU GPO. When this option selected, this option means that none of the policy settings in this GPO can be overridden. In the event that more than one GPO is set to No Override, the highest GPO takes priority.

Block Inheritance

The other choice for managing policy implementation is called **Block Policy inheritance** and this choice is also available to any Site, Domain, or OU GPO. This option means that any policy that is higher will not be inherited. Enabling this option will ensure that the settings of the current GPO will be implemented and not the policies of a higher priority policy.

Block Inheritance and No Override options must be used with proper care and if used with incomplete planning can cause serious disruptions to the overall policies that are implemented throughout the organization.

4.3.7 Security Configuration Management Tools

In Windows 2000, there are with a variety of tools and resources for the configuration and management of security options on both individual computers, and the network itself. These tools include The **Security Template Snap-In**, The Security Configuration and Analysis Snap-In, and Secedit.exe. Secedit.exe is a command line tool that can be used for analyzing the security of computers in a domain.

Security Templates

The task of configuring all the options in the GPO can be quite complex at times. To help with defining how the security should be configured for given situations, Microsoft has included Security Templates that can be used in the Group Policy Editor. These templates are .in files and can be opened with a text-editor, for viewing.

Templates are stored in the % system root%\security\templates. These templates can be applied to a GPO, and any user or computer that is controlled by that GPO will implement the security template. A template itself is a set of pre-configured options and Microsoft has included a full set of templates designed to cover most of the standard scenarios that are possible. User can use the default templates as-is, or modify them to suit his requirements. In addition to modifying a template, a user can create his oven template from scratch.

Predefined Security Templates

The list of common Security Templates are given below:

- BASICDC.INF – used to configures default Domain Controller security settings.
- BASICSV.INF – used to configures default Server security settings.
- BASICWK.IN – used to configure default Workstation security settings.
- COMPATWS.INF – used to configures compatible Workstation or Server security settings.
- SECUREDC.INF - This template configures secure Domain Controller security settings.
- SECUREWS.INF - This template configures secure Workstation security settings.
- HISEDC.INF - This template configures highly secure Domain Controller security settings.

- HISECWS.INF — This template configures highly secure Workstation security settings.
- SETUP SECUR1TY.INF - This template configures out of the box default security settings.

There are several general security levels in the templates: Basic, Compatible, Secure, and Highly Secure. The following sections define the general purpose and function of each of the security levels.

Basic templates (BASIC*.INF): These templates allow for an administrator to reverse an earlier implementation of a security configuration and configure Windows 2000 security settings that are not related to user rights.

Compatible templates (COMPAT*.INF) are often only run in a mixed environment. This template configures the system so that local Power Users have security settings that are compatible with Windows NT 4.0 users.

Secure templates (SECURE*.INF) configure security settings for the entire system, but not on files, folders, and Registry keys.

Highly Secure template (HISEC*.INF) is used to secure network communications on Windows 2000 computers and it allows for the highest level of protection on traffic sent to and from Windows 2000 machines. This template requires that a computer configured to use a HISEC template can only communicate with another Windows 2000 computer.

Dedicated Domain Controller (DEDICADC.INF) is used to secure a machine running as a Domain Controller. The reason you may wish to implement this template is that by default the security on a DC is designed to allow for legacy applications, and as such is not as secure as it could be. If your DC is not required to run any of these programs, it is suggested that the Dedicated DC template be implemented.

The final predefined template we will discuss is one that is very important in today's world, but is not included with the other preconfigured templates — the HISECWEB.INF template.

Microsoftat:http;//microsoft.com/default.aspx?scid=kb;en-us;Q316347& This template is discussed in the Microsoft article: "IIS 5: HiSecWeb Potential Risks and the IIS .lookdown Tool (Q3I6347)". The implementation of the HISECWEB.INF template is a requirement for any US 5.0 Web Server that wishes to be locked down.

HISECWEB.INF is designed to configure an US 5.0 machine running the WWW service. Although not in the list of default templates, this can be found and downloaded for free, directly from.

Analysing Password Security Policy of Templates

Open MMC management console, and select Add/Remove Snap-In option. Press Add and add the Security Templates Snap-In. Expand and review the password policy of following templates: Hisecdc, Basicsv, etc.

It is evident from above that the security templates provide a range of configuration. And if default or available templates does not quit fit to your needs, you can simply create a new template altogether.

Creating a Custom Template

a. Open MMC and select Add/Remove Snap-Ins.

b. Click on Add button, and add Security Templates Snap-In.

c. View all templates by expanding Security Templates.

d. Right Click Directory Location (e.g. :\Winnt\Security\Templates) and press New Template.

e. Enter template name: Custom Template.

f. Enter Description: Template for highly secure passwords.

g. Press OK

h. Apply following configuration settings to Custom Template.

- Password History 30 passwords
- Maximum Password age of 15 days and Minimum password age of 3 days.
- Minimum password length 12 characters.
- Account Lockout duration 0 minutes
- Account Lockout Threshold of 4 invalid Logon attempts.
- Reset Account Lockout Counter after 70 minutes.
- Right Click and press Save.

Advance Security Management- Through Security Configuration and Analysis Snap-In Tool.

After creating the policy and making changes in the predefined templates, the templates are applied to the network. As mentioned earlier, templates can be applied (also called Imported) to GPOs and importing a template to a GPO is a straightforward procedure, and uses a tool called **Security Configuration and Analysis Snap-In**.

The Security Configuration and Analysis Snap-In is another of the advances in security management provided by Windows 2000. Through this tool, you are able to implement templates and configure the security of your system. In addition to implementation, this tool allows for a complete security analysis of the operating system.

This tool is compares the security settings of a template to the current configuration of the operating system. During this analysis, this tool will highlight items that are in compliance with the settings with a green checkmark, and highlight those items that are not in compliance with a red X. Implementing the security configuration with an analysis tool is a time consuming process.

Steps are:

a. Open MMC and select Add/Remove Snap-Ins.

b. Press Add button, and add Security Configuration and Analysis Snap-Ins.

c. Right Click Security Configuration and Analysis Snap-Ins and select open database.

d. Open Password_Check.sdb.

e. Select your earlier created Custom Template, and press open.

f. Right Click Security Configuration and Analysis Snap-In and choose Analyze Computer Now and press OK.

g. Right Click Security Configuration and Analysis Snap_ins and examine whether or not your system is up to policies in respect of passwords.

Implementing a Template

a. Open MMC, Right Click Security Configuration and Analysis Snap_ins, and click on Configure Computer Now.

b. Press OK. This process will take several minutes and no message will be displayed.

c. Run the analysis again to confirm the configuration.

☞ Check Your Progress 1

1) State True or False T□ F□

a. Kerberos is an IETF standard used for privacy. □

b. SPPI is Server Support Interface. □

c. The SPPI functions as a interface between the user applications, such as the Web Browser, and the authentication method, such as NTLM or Kerberos. □

d. MD5 is Mirror Domain 5. □

2) Name various methods of authentication available in windows operating system.

....

....

....

3) Describe kerberos management in windows operating system.

....

....

....

4.4 RESOURCE MANAGEMENT

In this section we are highlighting resource management related issues.

4.4.1 Files and Folder Management

Windows NT 4.0 had the ability to work with only FAT and NTFS file systems, Windows 2000 can also work with FAT32. Further, NTFS should be used for Windows Security Options. NTFS in Windows 2000, technically called NTFS version 5, is required as an administrator wishes to use Active Directory, Domains, and the advanced file security that is provided. Further, the addition of file encryption and disk quotas require NTFS. It is suggested that all partitions that are still running FAT or FAT32 be converted to NTFS in order to effectively secure Windows 2000 resources. If you need to convert a partition to NTFS, the command is (using the C:\ drive as the example): convert volume /FS: NTFS /C. Any new partitions either created or converted to NTFS will, by default, allow everyone group Full Control access. As this includes the Guest and Anonymous accounts, strict security must be implemented before user accounts, which are able to access the system, are added.

In Windows 2000 some additional steps have been added to prevent users from making changes to the system files of Windows itself. Those changes are to hide the folders in the Winnt folder and the System32 folder by default. However, a quick click on the Show File option and all is revealed. There is a built-in mechanism that is working to keep system files from being modified, called the Windows File Protection (WFP) system, and its job is to ensure that system files installed during the setup of Windows are not deleted or overwritten. Only files that have been digitally signed by Microsoft will be able to make these changes.

4.4.2 Files and Folder Permissions

To view permissions, Right-click the object, Select properties, and view the information on the Security tab. One can view more detailed data in advanced option. File permissions are different in Windows 2000 over NT 4.0. Some of the File Permissions available are defined in the following list:

- Traverse Folder/Execute File: The Traverse Folder (Applied to folders only) permission manages a users ability to move "through" a folder to reach other files and folders, regardless of the permissions on the folder. The Execute File (Applied to files only) permission manages a users ability to run program files.
- List Folder/Read Data: The List Folder (Applied to folders only) permission manages a users ability to view file names and folder names. The Read Data permission manages a users ability to read files. (Applied to files only).
- Create Folders/Append Data: The Create Folders (Applied to folders only) permission manages a users ability to create folders within a folder. The Append Data (Applied to files only) permission manages a user's ability to make changes to the end of a file.
- Create Files/Write Data; The Create Files (Applied to folders only) permission manages a user's ability to create files within a folder. The Write Data (Applied to files only) permission manages a user's ability to modify and/or overwrite a file.
- Delete: This permission manages a user's ability to delete a file or a folder.
- Read Permissions: This permission manages a user's ability to read the permissions of a file or a folder.
- Change Permissions: This permission manages a user's ability to change the permissions of a file or a folder.
- Take Ownership: This permission manages a user's ability to take ownership of a file or folder.
- Read Attributes: This permission manages a user's ability to read the attributes of a file or folder.
- Write Attributes: This permission manages a user's ability to modify the attributes of a file or folder.

	Read (Display Data, attributes, owner, pemissions)	Executive (run or execute the file or files in the folder)	Write (to the folder or to the file or change the file attribute)	Delete (the directory or file)	Change Permisson (i.e., the permission to change permissions)	Take Ownership	
FOLDER SECURITY	R	X	W	D	P	O	**FILE SECURITY**
No Access							No Access
List Folder	*	*					
Read	* *	* *					Read
Add		*	*				
Add & Read	*	*	*				
Change	*	*	*	*	*	*	Change
Full Contro	*	*	*	*	*	*	Full Control
Special Access	? ?	? ?	? ?	? ?	? ?	? ?	Special Access

Figure 1: Files and Folder Permissions

These permissions alone are not considered to allow or deny access; the administrator must define on each object. It is not required to specify each of these unique permissions when securing resources. User will most likely use the defined permissions of: Full Control, Modify, Read and Execute, List Folder Contents, Read, and Write. The specific abilities of each of these Permissions are defined in the chart shown in *Figure 1.*

When you apply the Read permission, for example, to a folder, the folder gets the List Folder / Read Data, Read Attributes, and Read Extended Attributes. NTFS file permissions are similar, with the difference of no List Folder Contents as an option, as the permissions are applying to a file.

4.4.3 Inheritances and Propagation

When a user creates a new file, this new file will inherit the permissions of its parent folder, or parent partition on a root level folder. Therefore, if a parent folder is set: Everyone Modify, the file you create in that folder will have everyone modify as its permissions. User can alter this behaviour, create a folder apply the permissions to the This Folder Only option, which means that new data created in the folder will not inherit the permissions of the folder and new objects will inherit the permission that is set one level higher. Therefore, if you have a folder D:\Secure\Self, and this folder has had permissions applied to it only, when you create a file D:\Secure\Self\test.txt, this file will inherit its permissions from the D:\Secure object.

User can also block the inheritance of permissions by clearing the Allow Inheritable Permissions from Parent to Propagate to this Object option on the Security tab of the Properties windows for an object. When you clear this option, you will be presented with three options: (1) Copy the permissions that this object has inherited, (2) Remove all permissions except for those that have been specifically applied, and (3) Cancel the operation and keep the permissions as they were.

The process of configuring/setting permissions in Windows 2000 is similar to that of Windows NT 4.0, with the exception that you will specifically allow or deny access. If you wish to give a user or a group what was called No Access in Windows NT, you would, in Windows 2000, give that user or group Deny to the Full Control permission.

The attacker can get around your NTFS security, if they are able to get physical access to the computer by using MS-DOS etc. User may think that using DOS will not have an effect on any files that are on an NTFS partition, and that DOS will not even be able to recognise the NTFS partition. In most situations this is true; however there are tools and utilities on the market that are designed to access NTFS from DOS. One of the most common of these tools is simply called NTFSDOS.

Steps for assigning permissions

a. Open Windows Explorer, and select any NTFS partition.

b. Create a new folder, called protected_folder and right click this folder and select properties.

c. Select Security tab and clear the Allow inheritable permissions from parent to propagate to this folder, and choose copy option.

d. Add the user3 and give this account Deny- Full Control permission.

e. Add the user2 and give this account Allow- Modify permission.

f. Add the user4 and give this account Allow- Read and Execute permission.

g. Press Advance button and select User1 and press View/Edit.

h. Modify security settings to Apply onto: This folder only (i.e., protected_folder).

4.4.4 Moving Data and Permission

When data /files are moved from one folder to the another, what will happen to the security permissions that were set to secure these files. When files that are secured on an NTFS partition, how their security settings may be altered if those files are moved. In other words, if a file is defined as having everyone — allow — Read & Execute permissions, what will happen to those permissions if the file is moved to another folder? The rules in Windows 2000 regarding copying and moving files are the same as they were in Windows NT 4.0 and by default, a file will keep the permissions that are assigned to it when moving the file to another folder on the same NTFS partition. If the file is moved to another NTFS partition the file will inherit the permissions of the destination folder or partition. If a file is copied to any location, it will inherit the permissions of the destination folder or partition.

4.4.5 Shared Resources Management

Windows 2000 is designed to provide extensive network services; the security of resources via the network must be a high priority. The normal users of the system are not granted the permission to create shares on their local machines. Only Administrators and Power Users have this right to do so.

Three permissions are available for a shared folder, which may be applied to a user or a group; (1) Full Control, (2) Change, and (3) Read. These permissions are independent of the permissions set using NTFS security options. Windows 2000 uses both NTFS permissions and Share level permissions to decide the access a user will have to an object. When there are conflicting levels of permission for an object. Windows will determine the least restrictive permission both for the NTFS security and the share security. It will then compare those two permissions and the more restrictive of the two will be the resultant permission for the user. The exception to this rule is if a user has been given the Deny - Full Control permission, this takes precedence over the other permissions.

4.4.6 The NULL Session

For a system to provide shared resources it must communicate with the network and this communication is done via anonymous connections from system to system. If the system is not connected to Internet, this may not present a problem, but if the machine is directly connected lo the Internet, this operation may allow an attacker to learn about the inside network without authorisation.

This is called a NULL session connection, and is when an attacker connects as the anonymous logon. User should disable the NULL session and this can be done via any of the Security Templates. The steps for this are as follows: (1) Open any one of the security templates in the MMC, (2) Navigate to Local Policies, (3) Navigate to Security Options, and (4) Set the Additional Restrictions for Anonymous Connections to No Access Without Explicit Anonymous Permissions'.

4.4.7 Registry Management

The Windows 2000 Registry stores the configuration data for the computer, and as such is obviously a critical item to secure properly. The Registry in Windows 2000 can be directly updated with the tools like Regedit.exe and Regedt32.exe. As mentioned earlier it is recommended that Regedt32.exe be used as permissions can be applied to individual keys as you see fit. When setting the primary permissions in the Registry, however, you only have Read and Full Control to choose from.

The following lists are the permissions that are available for Registry:

- Query Value - Ask for and receive the value of a Key

- Set Value - Change a Key Value
- Create Subkey - Create a Subkey
- Enumerate Subkey - List the Subkey
- Notify - Set Auditing
- Create Link - Link this Key to some other Key
- Write DAC - Change Permissions
- Read Control - Find the Owner of a Key
- Write Owner - Change Ownership of a Key
- Delete - Delete the Key.

The permission "Full Control" is equivalent to all permissions listed above and the "Read" permission is equivalent to the Query Value.

4.4.8 Default Registry Configurations

There are systems in place to protect the Registry by default. Administrator SYSTEM account should have Full Control to all areas of the Registry. Power users are given permission to create subkeys in the HKEY__LOCAL_ MACHINE\SOFTWARE\ key, which allows them to install new software packages. Power users then have Full Control over the subkeys they create, as does the CREATOR OWNER Account. The extent of control for power users does not expand into all areas of the Registry. For example, in the Hardware hive of the Registry power users are not on the list to set permissions, by default. While making changes to areas of the Registry, be sure to have planned out the changes very carefully, as unintended actions can happen very easily and quickly.

Steps for Configuring Registry Permissions are given below:

a. Logon as Administrator.

b. Open Regedt32

c. Select HKEY_LOCAL_MACHINE

d. Expand SAM and leave the Greyed out SAM selected, choose Security from drop-down option and select permissions.

e. In this give Administration Full Control permission.

f. Expand SAM and notice that user and account information is now visible.

4.4.9 Registry Backup Management

To Secure the Registry, a backup strategy for the organization should be implemented.

There are several methods in which to backup the Registry; the first of these is to go through the Registry itself to save Subkeys/files, use the Microsoft Backup program. The Microsoft Backup utility can create a full backup of the System State, which includes the Registry configuration information. The storage option for backups is critical and a compromised system state backup is dangerous. The main files to secure, in regards to Registry Backup, is in the Operating System files, and stored in the % system root%\repair folder are the settings that must be secured. This folder contains the Registry configuration information that is needed in the event the system needs to be repaired.

Steps for saving the Registry information are given below:

a. Open Regedt32 and select software subkey of HKEY_LOCAL_MACHINE.

b. From drop-down option select Save Key.

c. Create a folder Reg_keys_folder in NTFS partition and create soft_1 as the file name and press save and close the Registry Editor.

d. Again go to Reg_keys_folder, right click and select security tab. Configure the security such that only user3 has Full Control, and remove any access to any other user account or group.

4.4.10 Printer Security Management

Printer Security in Windows 2000 provides three permissions: Print, Manage Printers, and Manage Documents. The Print option is the default level of security provided to users. This means they are provided the right to print, pause, resume, restart, and cancel documents they have submitted to a printer. To provide more control to a user, you can give them the permission of Manage Documents. With this level of permission, they are able to get the right to pause, resume, restart, and cancel all documents that have been submitted to this printer. You can also give Manage Printer permission and this level of permissions means they are given the right to share the printer, change printer permissions, change printer properties, and delete printers.

More control still over the printer can be acquired through advanced setting of printers. In the advanced settings of a printer, you can define the hours in which the printer is available. If the printer is to be used during only business hours, there is no reason to have the hours of the printer state it may be used 24x7. This type of control helps to keep the device used for official purposes only. You should secure the spooler that holds print jobs waiting to print and if the spooler is left at the default, it is in the % system root %, allows Everyone Full Control. This location should be moved to a secure NTKS location and should be managed individually.

☞ Check Your Progress 2

1) a. Create three domain user accounts: trainee1, trainee2, trainee3

b. Limit trainee1 so that this account can log on to the network during 10 AM to 5 PM during week days (i.e., Monday to Friday).

c. Set expiry date for trainee3 from 3 days from the today's date.

2) Describe policy inheritance.

....

....

....

3) Create security template with following parameters.

- Password History 30 passwords
- Maximum Password age of 15 days and Minimum password age of 3 days.
- Minimum password length 12 characters.
- Account Lockout duration 0 minutes
- Account Lockout Threshold of 4 invalid Logon attempts.
- Reset Account Lockout Counter after 70 minutes

4.5 WINDOWS 2000 NETWORK- SECURITY AND MANAGEMENT

4.5.1 NAT and ICS

In the previous section all of the security systems and methods are for securing operating system and data on physical hard disk. This security system is of no use if an attacker is able to sniff network packets.

Network Address Translation (NAT), is used to mask internal IP addresses with the IP address of the external Internet connection. Networks require NAT in their security policies to add an additional security "layer" between the Internet and the intranet. NAT functions by taking a request from an internal client and making that request to the Internet on behalf of the internal client. In this configuration clients on the internal network, on local LAN, are not required to have a public IP address, thus conserving public IP addresses. The internal clients can be provided with an IP address from the private network blocks. Private IP addresses are not routed on the Internet and the address ranges are:

Private IP Addresses

10.0.0.0- 10.255.255.255

172.16.0.0- 172.31.255.255

192.168.0.0-192.168.255.255

However, Microsoft has designated a range for private addressing, 169.254.0.0 - 169.254.255.255.

NAT is an integral part of Routing and Remote Access Services (RRAS), as well as part of Internet Connection Sharing (ICS). The version of NAT used by ICS is scaled down form the full version, and does not allow for the level of configuration that the RRAS NAT allows. ICS is for a small office or for a home network, where there is one Internet connection that is to be shared by the entire network. All users connect via a single interface, usually connected via a modern, DSL, or cable access point.

4.5.2 RRAS, RADIUS, and IAS

The Windows 2000 RRAS is made of several components, including: (1) Network Address Translation (NAT), (2) Routing protocols (RIP, OSPF), (3) VPN support (L2TP and PPTP), and (4) Demote Authentication Dial-In Service (RADIUS).

The Remote Access Server of RRAS allows for PPP connections and accomplish required authentication. For authentication, RRAS can use the Remote Authentication Dial-In User Service (RADIUS), or Windows Authentication. If RRAS is using RADIUS, when a user request for authentication is made to the RRAS server, the dial-in credentials are passed to the RADIUS server. The RADIUS server then performs the authentication and authorisation to access for the client to access the network.

The Remote Access Policy is controlled via the Internet Access Server (IAS), which is the Microsoft version of RADIUS. The RRAS server itself does not control the Remote Access Policy. The IAS performs several functions for remote users of the network, including authentication, authorization, auditing, and accounting to those users who connect to the network via dial-up and VPN connections. For authentication, IAS allows for great flexibility, accepting PAP, CHAP, MS-CHAP, and EAR EAP is Extensible Authentication Protocol, and is used in conjunction with technologies such as: Smart Cards, Token Cards, and One-time passwords.

4.5.3 IPSec

IPSec is a framework for ensuring secure private communications over IP networks. IPSec provides security for transmission of critical and sensitive information over unprotected networks such as the Internet. Ipsec VPNs use the services defined within Ipsec to ensure confidentiality, Integrity, and authenticity of data communications over the public network, like Internet. IPSec operates at the network layer, protecting and authenticating IP packets between participating IPSec devices. The IPSec provides the following network security services.

- Data Confidentiality – The IPSec sender can encrypt packets before transmitting them across a network.
- Data Integrity – The receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- Data Origin Authentication – The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- Anti-Replay – The IPSec receiver can detect and reject replayed packet.

In Windows 2000, you have two options for IPSec implementation, Transport Mode, and L2TP Tunnel Mode. Transport mode is designed for securing communication, between nodes on an internal network. L2TP Tunnel Mode is designed for securing communications between two networks.

IPSec Features

Two high level features of IPSec are the Authentication Header (AH) and the Encapsulated Security Payload (ESP). The AH is used to provide data communication with both integrity checking and source authentication and ESP is used to provide confidentiality. When using IPSec to secure communication, both the sender and the receiver (and only those two) know the security key used. Once authenticated, the receiver knows that the communication in-fact comes from the sender, and that the data has not been modified.

Since IPSec is works at the IP layer, it is able to secure communications with multiple protocols, including TCP, UDP, and ICMP. From a user viewpoint, the implementation of IPSec is transparent; the user is not required to modify user's environment in any way to use IPSec.

Windows 2000 IPSec Components

The Windows 2000 implementation of IPSec uses three components; (1) IPSec Policy Agent Service, (2) Internet Key Exchange (IKE), and Security Associations (SA). The IPSec Policy Agent Service gets the IPSec policy as configured in Active Directory, or the Registry, and provides that information to the IKE. Every Windows 2000 machine runs the IPSec Policy Agent Service, and the policy is pulled when the system starts as Active Directory settings are applied.

The IKE manages Security Associations (SA) and creates and manages the actual authentication keys that are used to secure the communications. This happens in two distinct steps; (1) in the first step is the establishment of a secure authenticated channel of communication, and (2) the second step the Security Associations are determined. The as are used to specify both the security protocol and the key that will be implemented.

IPSec Implementation Options

The configuration may be applied in Active Directory or directly to the Registry. IPSec policies may be applied to to computers, domains, OUs, or other GPOs in the Active

Directory. The IPSec options are in Group Policy, under Security Settings.

There exist three policy options that are predefined for IPSec implementations. They are: Client (Respond Only), Server (Request Security), and Server (Require Security).

- **Client (Respond only)** – As per this policy the secure communications are nct secured most of the time. Computers with this policy respond to a request for secure communication by using a default response. If a client needs to access a secured server, it can use normal communications.
- **Server (Request Security)** - Communication must be secured most of the time, and will allow unsecured communications from non IPSec-computers. It will request IPSec from the client first, and open a secured communication channel is the client can respond securely.
- **Server (Require Security)** - This policy states that communication must always be secured and all traffic must use IPSec or it will not be accepted, and the connection will be dropped.

4.6 ENCRYPTING FILE SYSTEM MANAGEMENT

In this section we will discuss about the encryption of file system.

4.6.1 Encrypting File System (EFS)

The main benefits of personal computers are that it provides you the flexibility to boot into multiple Operating Systems for desired use. But this flexibility poses great difficulty in the world of security. In addition to the security risks of multiple Operating Systems, there are security risks introduced with the use of laptop computers. Laptops often get stolen or misplaced, and the data on that computer is vulnerable to compromise as soon as the location of the laptop is changed. With NTFS security you are able to solve the issues of security to a certain extent. As detailed there are tools available to access data even properly secured on an NTFS partition.

The concept of encryption has been introduced to solve this problem. Data encryption works to make the files on the computer only useful to the authorised owner of the data. Some of these methods provide a password for each encrypted file, which while effective, is not practical for large volumes of files. Another method is to use a key to unlock each file that has been encrypted, with only one user holding the key and Microsoft's EFS uses this approach. EFS use "public key cryptography" for encryption/ decryption of data. Public key cryptography is the use of two keys, one performs encryption and another performs decryption. The keys are keys are mathematically related. The files are encrypted by DES encryption algorithm in EFS. EFS supports file encryption for both on a local hard drive and on a remote file server. But, any files encrypted on the remote server will be transmitted over the network in clear-text by default. So, the file is decrypted at the file server, and then sent to the user. In order to maintain the high level of security, a mechanism should be implemented to secure the network traffic, such as IPSec.

The implementation of EFS works directly with NTFS and data can only be encrypted on an NTFS partition. EFS can encrypt any temp files created along with the original, and the keys are stored in the kernel using non-paged memory, so they are never vulnerable to attackers.

4.6.2 EFS and Users Management

One of good or bad point of EFS is that its use does not require any administrative effort and keys are created automatically, if the user does not already have a public key pair to use. Files and Folders are encrypted on a single file or single folder basis, each with a unique encryption key and as they are encrypted uniquely, if you move an encrypted file to an unencrypted folder on the same partition, the file will remain encrypted. If you copy an encrypted file to a location that allows for encryption, the file will remain encrypted.

The EFS is a very transparent in use and user may have encryption enabled without aware of it.

4.6.3 Data Recovery Management

EFS designed to be implemented by a user, and is designed to be transparent; it can be used where it was not initially intended. EFS allow for Recovery Agents and the default Recovery Agent is the Administrator. These agents have configured public keys that are used to enable file recovery process. But, the system is designed in such a way that only the file recovery is possible and the recovery agent cannot learn about the user's private key.

Data Recovery for those companies and organisations that have the requirement of accessing data if an employee leaves, or the encryption key is lost.

The policy for implementing Data Recovery is defined at a Domain Controller. And this policy will be enforced on every computer in that domain. In case EFS is implemented on a machine that is not part of a domain, the system, will automatically generate and save Recovery Keys.

4.6.4 EFS Cryptography Management

As mentioned in the previous sections EFS uses public key cryptography, based on the DES encryption algorithm. Data is encrypted by what is called a File Encryption Key (FEK), which is randomly generated key. The FEK itself is then encrypted using a public key, which creates a list of encrypted FEKs. The list is then stored with the encrypted file in a special attribute called the Data Decryption Field (DDF). When a user needs to decrypt the file, he or she will use the private key that was part of the key pair. User performs encryption from the command line, or from Explorer. In Explorer, the option to encrypt is under the advanced option on the properties Window. When using the command line version, the command is, cipher, with a/e switch for encryption and a/d switch for decryption.

☞ Check Your Progress 3

1) Expand the following:

   a. RADIUS

   b. NAT

   c. ICS

   d. RRAS

2) What do you understand by VPN? Discuss IPSec security.

   ……………………………………………………………………………………………

   ……………………………………………………………………………………………

   ……………………………………………………………………………………………

3) Discuss in detail EFS (Encrypting File System)]

....

....

....

4) What do you understand by a null session? How null session can be disabled?

....

....

....

4.7 SUMMARY

This unit covers in detail the various security and management issues that can be implemented in windows 2000 architecture. The unit address broad sweep of security and management related issues: User Authentication Management- users and group management; resource management; windows network management ; and encrypting file system management. Windows 2000 authentication covers the Subsystems components, and kerberos.

The users and group security in unit covers the topics like; configuring users accounts, windows 2000 groups (default group types, local groups, global groups, group policies etc), security configuration tools, and configuration and analysis tools. In unit covered the resource management in detail and it covers the areas like; files and folder management, files/folder permissions, inheritance and propagation, moving data and permissions, shared resources, null session, printer management, and Registry management.

The network management has been covered in detail in this unit and various network security methods like NAT, ICS, RRAS, RAS, IAS, and IPSec are covered. The unit also talks about the EFS (Encrypting File System) management of Windows 2000 systems and it covers topics like data recovery and EFS cryptography. This unit introduced the management of configuration required to secure Microsoft Windows Computer Systems and now you will be able to examine everything from the foundation principles of Windows 2000 security and management, upto to the advanced issues of securing windows 2000 running Active Directories.

4.8 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) (a) False , (b) False, (c) True (d) False.

2) Windows 2000 can use the following for authentication: Kerberos, NTLM, RADIUS, SSL, Smart Cards, and more.

3) When a user the log on process by entering his credentials, Windows will contact an Active Directory domain controller, and locate the Kerberos Key Distribution Center (KDC). An Authentication Server (AS) performs the actual authentication. The KDC responds by issuing a Ticket Granting Ticket (TGT) to the authenticated user. The TGT contains identification information about this user to various servers on the network, and is used to gain further access in the network. After the user account has been authenticated, the TGT is used to

request further Kerberos tickets in order to access network services. The machine that provides the tickets for the network resources to the authenticated client is known as a Ticket Granting Server (TGS).

Check Your Progress 2

1) a. Open the management console MMC.

b. Open or add the Active Directory Users and Computer Snap-In.

c. Expand domain listing, to view the console tree.

d. In the Action down menu, select option New User.

e. Create new users, trainee1, trainee2, trainee3, etc.

b) i. Open the Active Directory Users and MMC Snap-in

j. Expand domain listing, to view console tree.

k. Select user folder.

l. Double click trainee1.

m. In the Property Window, choose Account Tab, and select the Logon Hours Option.

n. Limit trainee1 so that this account can log on to the network during 10 AM to 5 PM during week days (i.e Monday to Friday).

o. Press OK to close the Logon Hours dialog box.

p. Again press OK to close the trainee1 Property Window,

c) g. Open Active Directory Users and Computers MMC Snap-In.

h. Expand domain listing to view the console tree.

i. Select user folder.

j. Double click trainee3 and in property window select the Account tab.

k. In the Account Expires Option, and select End of option, and enter desired expiry date.

l. Press OK.

2) Policy Inheritance is the name for the process of a user or computer inheriting the final policy configuration from multiple policies, depending on where the object may be in the Active Directory hierarchy and configured GPOs.

3) • Open MMC and select Add/Remove Snap-Ins.

- Click on Add button, and add Security Templates Snap-In.
- View all templates by expanding Security Templates.
- Right Click Directory Location(e.g. :\Winnt\Security\Templates. and press New Template.
- Enter template name: Custom Template
- Enter Description: Template for highly secure passwords.
- Press OK
- Apply following configuration settings to Custom Template:
- Password History 30 passwords

- Maximum Password age of 15 days and Minimum password age of 3 days.
- Minimum password length 12 characters.
- Account Lockout duration 0 minutes
- Account Lockout Threshold of 4 invalid Logon attempts.
- Reset Account Lockout Counter after 70 minutes.
- Right Click and press Save.

Check Your Progress 3

1) RADIUS – Remote Authentication Dial in Service, (b) NAT- Network Address Translation, (c) ICS- Internet Connection Sharing, (d) RRAS- Routing and Remote Access Services.

2) Virtual Private Network. IPSec is a framework of pen standards for ensuring secure private communications over IP networks. IPSec provides security for transmission of critical and sensitive information over unprotected networks such as the Internet.

3) EFS works directly with NTFS and data can only be encrypted on an NTFS partition. EFS can encrypt any temp files created along with the original, and the keys are stored in the kernel using non-paged memory, so they are never vulnerable to attackers.

4) For a system to provide shared resources it must communicate with the network and this communication is done via anonymous connections from system to system. If the system is not connected to Internet, this may not present a problem, but if the machine is directly connected lo the Internet, this operation may allow an attacker to learn about the inside network without authorization. This is called a NULL session connection, and is when an attacker connects as the anonymous logon.

Disabling null session:

c) Open any one of the security templates in the MMC,

d) Navigate to Local Policies,

e) Navigate to Security Options, and

f) Set the Additional Restrictions for Anonymous Connections to No Access Without Explicit Anonymous Permissions'.

4.9 FURTHER READINGS

1) Windows 2000 Professional Resource Kit, Microsoft Press.

2) *Cryptography and Network Security, Principles and Practice,* SE, PE., William Stallings

3) *Security in Computer,* Charles P. P fleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education.

4) *Windows 2000 Commands* by Aleen Frisch.

5) Microsoft Web Site http://www.microsoft.com.