Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Step-by-Step Plan for Securing Windows 2000

Catherine Sommers
February 23, 2001

GIAC Level Two
Securing Windows 2000
Capital SANS 12/2000

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

Microsoft has greatly improved the security model of Windows 2000 over its predecessor, Windows NT. All of the significant security features of Windows NT have been included in Win2K, and many of the core features of the architecture and object oriented design came from Windows NT. In addition, Win2K has some specific goals of improving the scalability, reliability and security of Windows NT along with integrating many of the add-ons into the OS. Microsoft's development of W2K was aimed at addressing the major shortcomings and vulnerabilities of WinNT. It was reported in a recent Sunbelt newsletter that WinNT is the favorite choice of hackers worldwide. NT was running on more than 50% of the compromised web servers from the period August 1999 to December 2000. Alas, as Win2K's installed base increases, its vulnerabilities are being discovered, and the number of intrusions is growing. This situation underscores the need to improve the default security settings of the OS out-of-the-box and fine-tune other security configurations. It is also essential to be as proactive as possible by keeping abreast of the revelation of potential vulnerabilities and the changing security landscape. To paraphrase the words of several security experts - security is an ongoing process, not a goal in itself.

Threats from the Internet are on the rise. In recent years the number of security incidents reported to the Computer Emergency Response Team Coordination Center (CERT-CC) has grown at a frightening rate. Since 1997 there has been a dramatic increase in the number of incidents including attempts to gain unauthorized access to a system or data, and disruption or denial of service. The security picture is actually worse than the statistics indicate since it's very likely that a large majority of the incidents are never reported. Even if an organization is running a server that does not require maximum security such as one hosting a banking site or an online shopping site, it is still necessary to take steps to secure servers that are exposed. The stakes are high since the attackers are definitely out there. They may be after your intellectual property or your computing resources or they may just want to have some fun defacing your web site.

The purpose of this paper is to provide a step-by-step guide to securing Windows 2000 from an out-of-the-box to an "Internet ready" configuration. Beginning with several good security procedures to follow in order to secure the Windows 2000 network environment against internal as well as external dangers, the new security tools and features of Windows 2000 will be described and illustrated in detail.

Standard Security Procedures

Listed below are several important security procedures that should be taken to protect the Win2K systems from internal and external threats:

- Secure computer room housing the servers and restrict access to authorized individuals.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

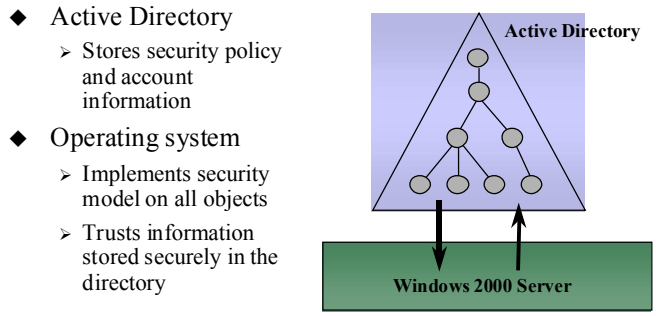
- Disable ability to use a floppy boot disk on server machines, which can allow illegal access to the system by booting to another operating system and bypassing NTFS securities.
- Keep computers up-to-date on service packs and hot fixes. Win2K's service pack slipstreaming removes the requirement to reapply a patch after installing an application. Check the Microsoft web site for new service packs and hot fixes, and subscribe to the automatic bulletin service to receive security bulletins via email. Other web sites to monitor for updates on vulnerabilities and other security information are www.sans.org, www.cert.org/advisories, www.ntbugtraq.com, www.microsoft.com/technet/security.
- Disable unnecessary services running on the server. After you have turned off all services that you are not using, a quick way to double-check that these services are actually not being used is to set the Startup Type of the services that you think are unused to Manual. Restart the server, and use all of the applications. Open the Microsoft Management Console (MMC) with the Services snap-in, and check which services are started. The services that have not started should be set to Disabled.
- See the series of white papers included in the **Best Practices for Enterprise Security** at www.microsoft.com/technet/security/bpentsec.asp for good foundation information and advice for security planning.
- Be certain that backups are performed in a secure manner and that the backup media is protected from manipulation or theft.
- Protect servers and workstations with virus protection software and keep signature files up-to-date.
- Require strong passwords and consider using a more secure level of authentication such as smart cards or biometrics since Win2K has support for these methods.
- Establish a strong perimeter defense with a correctly configured firewall that blocks dangerous and well-known vulnerable ports.
- As soon as possible, remove NetBIOS from the network and remove WINS servers. NetBIOS presents a security risk due to the well-known null session exploit.

Active Directory

Active Directory is the core of Win2K system's security. It replaces Windows NT's security accounts manager (SAM) on domain controllers as the primary repository for security information such as user accounts, passwords and groups. AD is a replicated hierarchical service that forms a trusted component of the Local Security Authority. AD holds critical security information including user and machine accounts, policy information, password hashes, certificates, permissions and privilege settings and an array of objects for the entire enterprise. AD leverages the security infrastructure for authentication and authorization in that it stores both user credentials for authentication and access control information for authorization to use system resources. AD allows easy delegation of privileges and authority based on specific functions within a given scope,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

which eliminates the necessity of granting excessive administrative privileges to a user in order to perform a single administrative function. The security infrastructure of Win2K relies on AD and without it such security related processes and tools as Kerberos, Group Policy and the audit mechanism would not work. The relationship between AD and the security system is represented in the diagram below:



The following are several AD-related security features with background information and implementation recommendations:

Security Templates

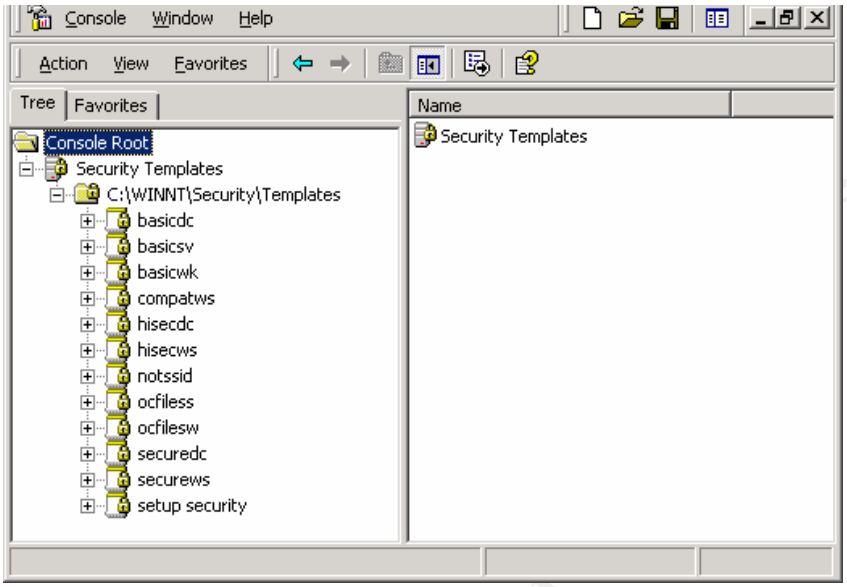
The default security settings are applied only on a clean install of Win2K onto a NTFS partition. If a server is being upgraded from a previous version of Windows NT, security is not modified, and when Win2K is installed on a FAT partition, security cannot be applied. There are three basic security templates provided that can be used to secure NTFS computers in the same way as clean-installed NTFS machines: basicwk.inf for computers running Windows 2000 Professional, basicsv.inf for computers running Windows 2000 Server and basicdc.inf for domain controllers running Windows 2000 Server. These templates specify default security settings for all security areas except User Rights and Groups.

The security templates can be accessed via a snap-in to the Microsoft Management Console (MMC) as follows:

1. Click **Start**, click **Run** and then type **MMC /s** into the text box and click **OK**.
2. Click **Console** (under Console1 in the upper right of the window), click **Add/Remove Snap-in**, and click **Add.**
3. From the list of available Standalone Snap-ins, select **Security Templates.**
4. Click **Add** and then **Close**. Click **OK.**
5. Click **C:\WINNT\Security\Templates** to expand it.

The window should appear as follows:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Win2K also has incremental security templates that can be applied to Win2K computers that are configured with the new default security settings. These templates incrementally modify the default security settings and should be applied to Win2K computers that have been clean-installed into an NTFS partition or to upgraded NTFS computers that have had the basic template applied. The incremental security templates are:

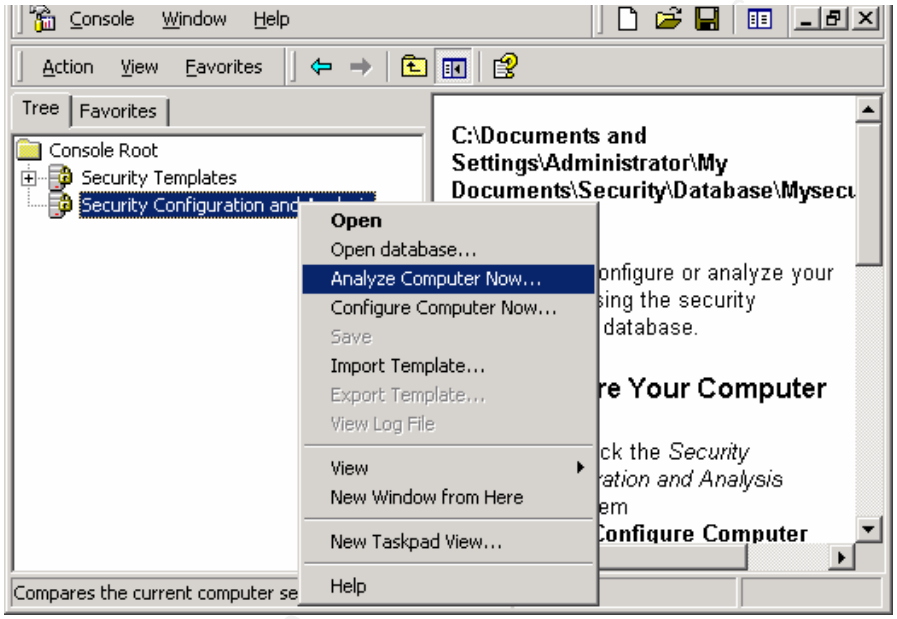
- Compatws.inf – for workstations and servers. If you do not want users to run as Power Users, this template opens the default permissions for the Users group so that legacy applications will more likely run correctly. This environment is not considered secure.
- Securews.inf – for workstations and servers (securedc.inf for domain controllers). This template provides for increased security for areas of the operating system not covered by permissions. Included are increased security settings for Auditing, Account Policy and some well-known security relevant areas of the Registry. Since it is assumed that the Win2K default security settings are in effect, access control lists are not modified. All members of the Power Users group are removed.
- Hisecws.inf – for workstations and servers (hisecds.inf for DCs). This high security configuration is for Win2K computers in native mode only and requires that all network communications be digitally signed and encrypted. Therefore, communications between a Win2K highly secure computer and a downlevel Windows client is not possible.

The Security Templates snap-in, which is a component of the Security Configuration Tool Set, also allows the modification of existing templates or the creation of custom templates containing security settings for all of the security areas supported by the Tool Set (Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry and File System). It is also possible to import a template into the Security Settings extension to configure local, domain or OU security policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

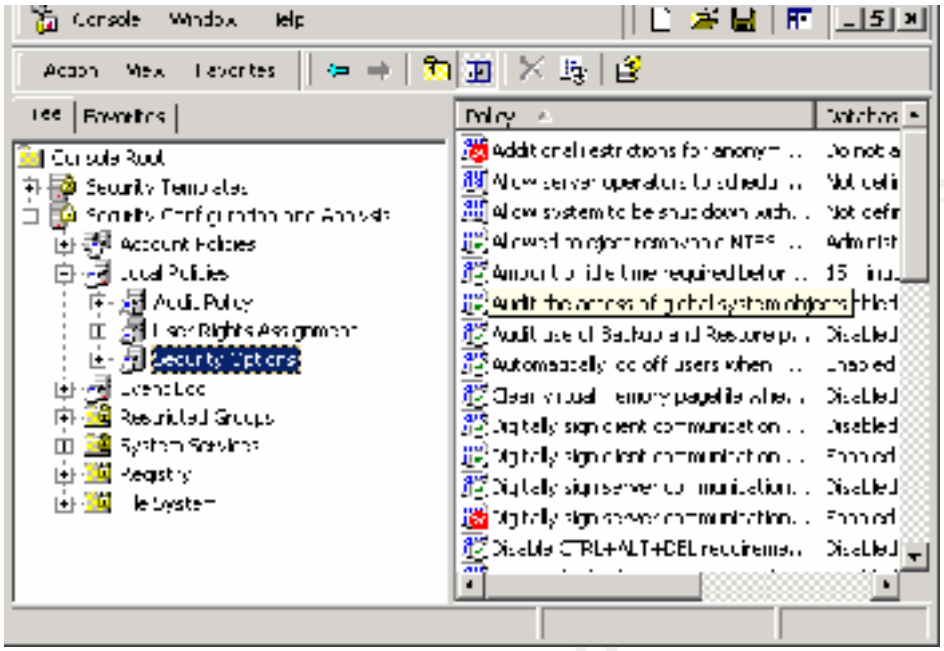
Security Configuration and Analysis Snap-in

The Security Configuration and Analysis snap-in is another standalone MMC snap-in used to configure and analyze security settings. It can be used to analyze current security settings against a baseline template to identify the following: security holes that may exist in the current configuration, changes that a potential security policy may have on a system before actually deploying the policy, and deviations from a policy that is currently imposed on a system. After the Security Configuration and Analysis snap-in is loaded in the MMC, it is necessary to create a database by opening the baseline analysis template into the database. The analysis is preformed by right-clicking on Security Configuration and Analysis and then selecting Analyze Computer Now from the context menu:



To review the results, click on View on the Security Configuration and Analysis node. Expand the Security Configuration and Analysis in the left pane, and then expand Local Policies and click Security Options:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

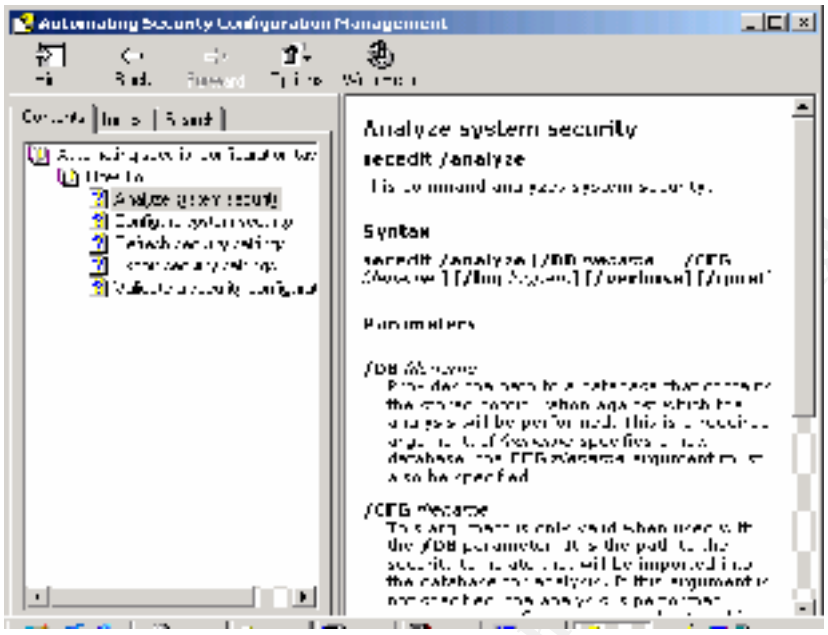


In the right pane above, both the database and the actual system settings are displayed for each object. Consistencies are marked with a green check mark, and discrepancies are highlighted with a red X flag. The settings that have no marks are ones not specified in the database. Double-click on the discrepancies in the right pane to investigate further and modify database settings, if desired. After examining the security changes indicated by the template, which are the mismatches flagged in the analysis, it is possible to configure the system with these new security settings by selecting Configure System Now after right-clicking on the Security and Analysis node. At the end of the process when the snap-in is closed down, the console settings can be saved so that the Security Configuration and Analysis snap-in will not have to be added to the console in the future.

Secedit.exe

The analysis and configuration operations that can be done with the Security Configuration and Analysis GUI can also be performed with the command line tool, secedit.exe. This tool allows security configuration and analysis to be done in conjunction with other administrative tools such as the Task Scheduler. In addition, secedit.exe provides some capabilities that are not available in the GUI version. When using a scripting tool, it's possible to configure remote analysis and security settings for all clients on the network. There is online help for this command that illustrates the syntax for configuring security and performing analysis at the command line:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Recommendations:

- Use the basic security templates to apply the default security configurations to computers that have been upgraded or to restore the security defaults to Win2K computers.
- Use Group Policy to deploy security settings to multiple computers.
- Apply incremental security templates for higher level of protection according to the needs of your environment.
- Be sure to test security settings in a lab environment before implementing in production systems.
- Avoid making users members of the Power Users group in order to run legacy applications by applying the compatws.inf template, which allows normal users to run these applications.
- Since the secure templates remove all users from the Power Users group in order to make a more secure system, it may be impractical to apply this template if there are older applications that don't meet Win2K application specifications and therefore require Power Users to run these applications.
- If the environment qualifies, apply the secure template for maximum security, which requires a native mode Win2K environment where all the clients are Win2K machines.
- Before installing your first Win2K server, consider the domain tree and forest hierarchy in terms of the DNS structure, management of users from a security and support perspective and how to protect the forest root server that contains the Enterprise Administrators group. The OU design is the key to a successful implementation.
- OUs cannot be used for security purposes since they do not have SIDs. In your AD architecture, OUs should be used for object management and groups should be used for security.

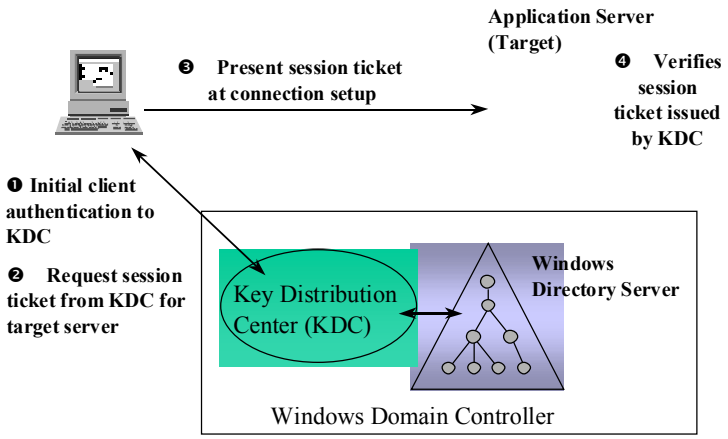
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The design structure of your AD should allow the implementation of security and application settings in a quick and easy manner without fear of breaking things by pushing down settings to unintended clients. An overly complex AD design with multiple domains created for political reasons rather than technical ones will make management much more difficult.

Kerberos

The default authentication method for Win2K clients in a Win2K domain environment is Kerberos. However, a Win2K client will automatically use a downlevel authentication method, NTLM Challenge-Response v2 or LM Challenge-Response, when accessing servers running older versions of Windows. Kerberos offers an improvement over the NT's method of authentication, NTLM. Authentication requests get resolved more quickly because Kerberos is a more efficient protocol, and member servers can validate the Kerberos ticket presented by the client without getting additional authentication from a Domain Controller. In a fashion reminiscent of callback in RAS, clients can request credentials back from member servers, which helps guard against the possibility of a renegade server infiltrating the network. Every Domain Controller is a Kerberos Key Distribution Center (KDC), which runs as a thread of the Local Security Authority Subsystem. Kerberos keeps a copy of the password hashes for all users and member servers in its realm and officiates transactions by distributing tickets. The ticket contains information known only to the KDC and is encrypted with the password hash of the validating server. The client must have a ticket for each server it wants to access. The validating server uses the ticket information to check certain key information submitted by the client, and this additional check of shared information known only to the trusted third party helps to decrease the possibility of a man-in-the-middle attack where a renegade domain controller could intercept the authentication transaction and impersonate the user on the network.

Kerberos Authentication Protocol Overview



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Recommendations:

- Eliminate the least desirable authentication method on the network by applying the DSClient patch that is on the Win2K Server CD, which will upgrade the local security package on Windows 9x machines to use NTLM v2. Then you can disable LM passwords on all domain controllers, which will help to combat password cracking.
- A special account named krbtgt is created when a Win2K Domain Controller is set up, and its password is used to create the secret key for encrypting ticket-granting tickets. This account is disabled and cannot be renamed nor deleted. The password hash of this account is used by Kerberos to validate the origin of the ticket and to identify the ticket's source domain. The password is changed by the system on a regular basis, and it should not be modified unless there is a good reason such as a requirement of integration with MIT Kerberos v5.
- Kerberos supports tiered client/server environments in which a middle server acts on behalf of the requesting client and has the ability to create an alternative security context. Win2K requires that the middle server be trusted for delegation, which can be set in the AD Users and Computers. The difference between this delegation and the NT idea of impersonation is that the delegated identity can flow from machine to machine while the impersonated account cannot leave a computer and access a remote source as the impersonated user. The server that is to be trusted for delegation should be physically protected so that unauthorized programs are not installed, and it should be removed from the Internet to avoid Trojan horse programs.
- The default settings for Kerberos are good. There are only a few policy items that can be configured, and if you do need to change the parameters, it is done in Start/Programs/Administrative Tools/Domain Controller Security Policy. The Kerberos policy is set at the domain level and is stored in AD, which means that you must be a member of the Domain Administrators group to change the policy and changes made on one Domain Controller will be replicated to the other DCs along with the other AD replication.
- KERBTRAY in the Network Management Tools folder of the Win2K Resource Kit is a handy tool that lets you view all the Kerberos tickets obtained by a client that are stored in cache plus the flags assigned to the tickets and their expiration times. Win2K Kerberos tickets expire every 10 hours. This is a helpful tool for troubleshooting authentication problems. Below is an example of the Kerbtray screen with the tab for Times displayed:

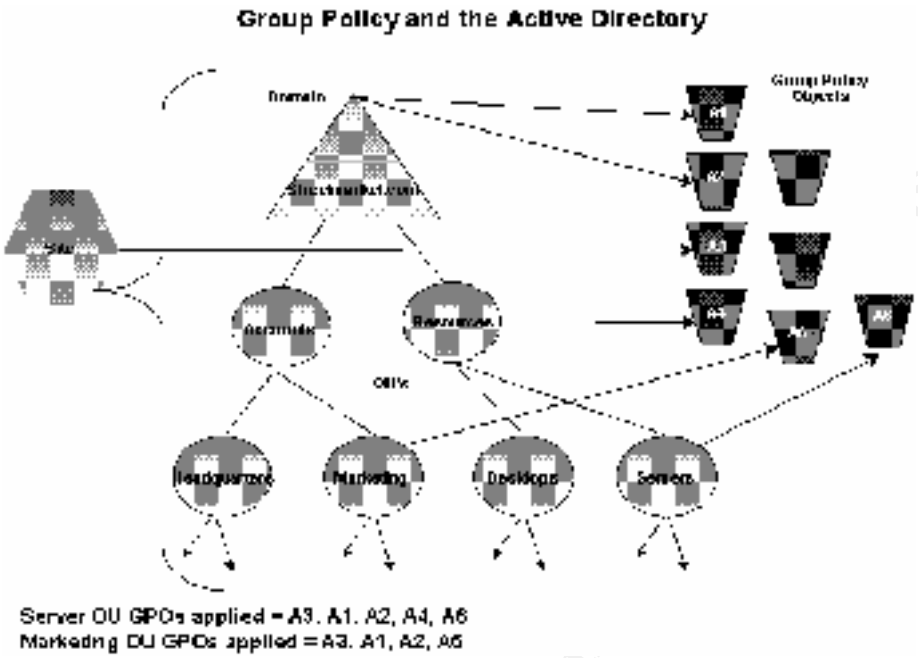
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Group Policy Objects

GPO model allows for centralized control for the creation and distribution of security settings in addition to other system and applications settings. AD enables Group Policy, and the policy information is stored in Group Policy objects, which are linked to AD containers. Group Policy can be applied centrally at the domain level or it can be applied at the OU level in a decentralized environment. The GPO will affect all computers and users in the scope to which it is applied but can be modified by the application of filters based on membership in a Win2K Security Group. Security groups can also be used to delegate control of a GPO in order to manage the group policy links and the permissions for creating and editing GPOs.

Group Policy objects are linked to containers in AD (site, domain and OU). The default order of precedence follows the hierarchical nature of AD: sites, domains and then each OU. This order of GPO processing – local, site, domain, OU – is important because policy applied later overwrites a policy applied earlier. A GPO can be associated with multiple containers or multiple containers can be linked to a single GPO. The following diagram shows how GPO can be applied to AD containers:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



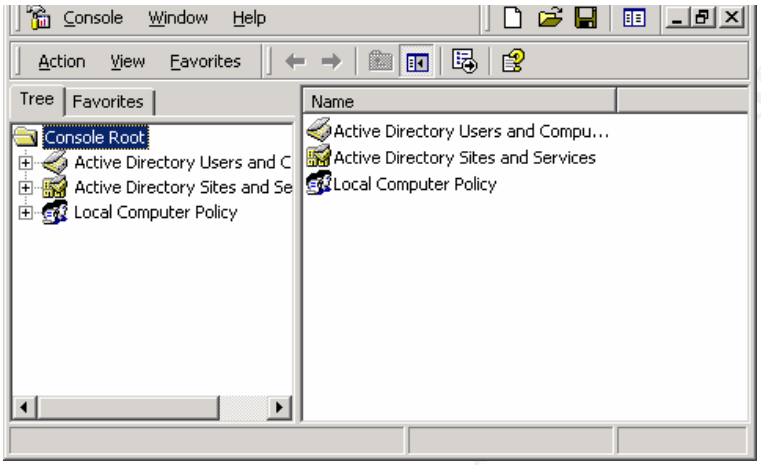
To set Group Policy for a selected Active Directory container, you must have a Win2K domain controller installed, and you must have read and write permission to access the system volume of domain controllers (Sysvol folder) and modify rights to the currently selected directory container. The system volume folder is automatically created when you install a Win2K DC (or promote a server to domain controller).

Recommendations:

- The AD snap-ins for MMC set the scope of management for GPO. To set the scope to domain and OU level, use the AD User and Computers snap-in. Use the AD Sites and Services to set the scope to a site. It is also possible to create a custom MMC console.
- By default, all GPOs affect all users and machines in a linked site, domain or OU. You can use Discretionary Access Control Lists (DACLs) to modify the effect of any GPO to exclude or include members of any security group. Modify the DACL by using the **Security** tab on the **Properties** page of any GPO. To access the GPO Properties page from the Group Policy Properties page of a Domain or OU, do the following (substituting your own domain, OU and policy):
    - Add the **Active directory user and computers snap-in** to the MMC and the double click **Active directory sites and services** snap-in from the **Available standalone snap-ins** list box. In the **Available standalone snap-ins** box, double-click **Group Policy**. In the **Select Group Policy** object dialog box, **Local computer** is selected under **Group Policy object**. Click **Finish** to edit the local Group Policy object. Click **Close** in the **Add standalone snap-in** box. In the **Add/Remove Snap-in** dialog box, click **Extensions** tab and ensure that **Add all extensions** check box is

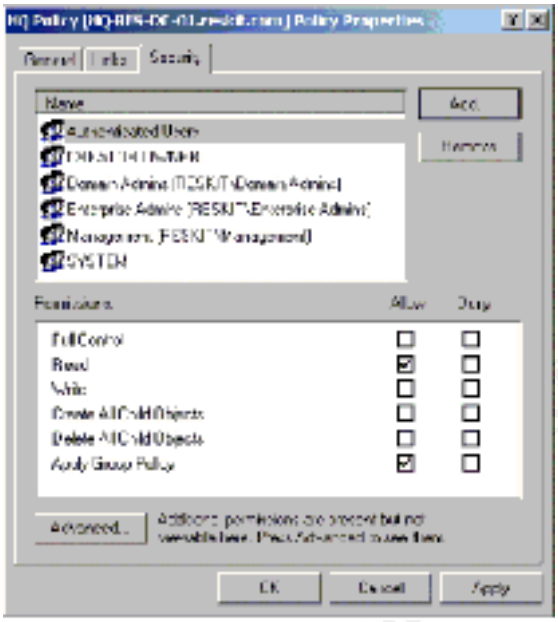
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

checked for each primary extension added to the MMC console. Click **OK**. The console should appear as follows:

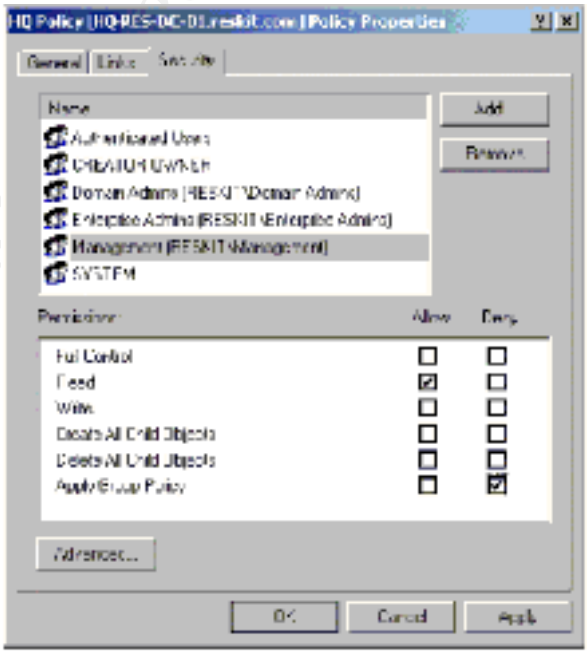


- Double-click **Active Directory Users and Computers**, double-click on the domain to use, double-click **Accounts**, right-click the OU to use and then click on **Properties**.
- In the OU **Properties** dialog, click **Group Policy**.
- Right-click the Policy to use GPO from the **Group Policy Object Links** list and select **Properties** from the context menu.
- In the **Properties** page, select the **Security** tab, which displays the standard Security parms page.
- Click **Add** on the **Security** property page.
- In **the Select Users, Computers, and Groups** dialog box, select the **Management** group. Click **Add** and **OK** to close.
- In the **Security** tab of the Policy page**,** select the **Management** group, and view the permissions. By default, only the **Read** ACE is set to **Allow** for the Management group. This means that the members of this group do not have the GPO applied to them unless they are also members of another group (they are also Authenticated Users by default) that has **Apply Group Policy** ACE selected.
- All members of the Authenticated Users group have the GPO applied, as shown below. To configure the GPO so that it applies to members of the Management group only, select **Allow** for the **Apply Group Policy** ACE for the Management group. Then remove the **Allow Group Policy** ACE from the Authenticated Users group.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



- **Write** access is required to make modifications to the ACEs. **Read** and **Allow** Group Policy ACE are required for a policy to apply to a group. **Deny** ACE setting for any group has precedence over **Allow** ACE given to a user or group because of membership in another group. Use **Deny** with caution. Below is example of security settings allowing everybody to be affected by the GPO except the Management group. Note that if a member of the Management group was also a member of a group that had an explicit **Allow** setting for the **Apply Group Policy** ACE, the **Deny** would take precedence and the GPO would not affect that user.



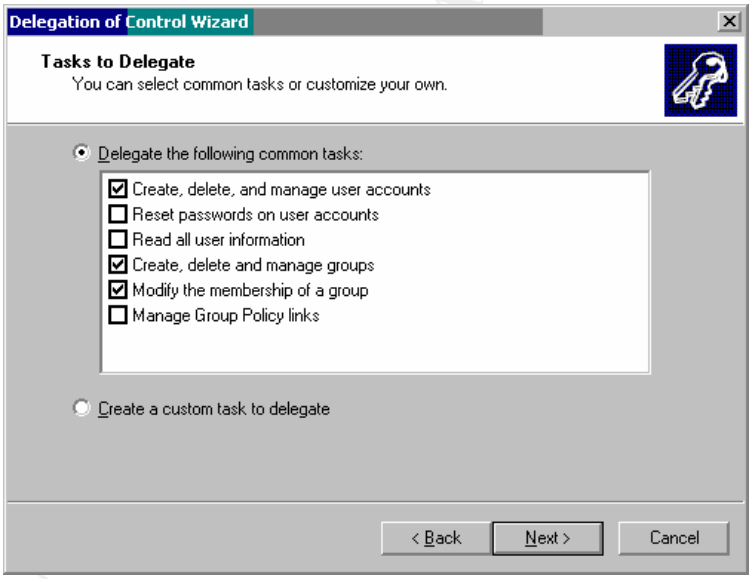
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Use the **No Override** option to enforce the Group Policy settings in a specific Group Policy object so that GPOs in lower-level AD containers are prevented from overriding that policy. For example, if you have defined a specific GPO at the domain level and specified the **No Override** option, the policies that the GPO contains apply to all OUs under that domain; that is, the lower-level containers (OUs) cannot override that domain Group Policy. You can also block inheritance of Group Policy from parent AD containers by using the **Block policy inheritance** option.
- The Security Settings extension of the Group Policy snap-in complements existing system security tools such as the **Security** tab on the **Properties** page (of an object, file, folder, and so on), and **Local Users** and **Groups** in **Computer Management**. The security areas that can be configured for computers include the following:
    - **Account Policies** - includes Kerberos policy in Win2K domains.
    - **Local Policies -** includes security settings for audit policy, user rights and security options and allows configuration of local and network access and the auditing of local events.
    - **Event Log** -security settings for Application, Security and System event logs.
    - **Restricted Groups** -configuration of restricted group membership and ability to enforce security policies for sensitive groups such as Enterprise Administrators or Payroll.
    - **System Services -**control of startup mode and security options (security descriptors) for system services such as network services, file and print services, telephone and fax services, Internet and intranet services, etc.
    - **Registry** - This is used to configure security settings for registry keys including access control, audit, and ownership. When you apply security on registry keys, the Security Settings extension follows the same inheritance model as that used for all tree-structured hierarchies in Win2K (such as the Active Directory and NTFS). Use inheritance capabilities to specify security only at top-level objects, and redefine security only for those child objects that require it. This approach greatly simplifies the security structure and reduces the complexity of the access control structure, which reduces administrative overhead.
    - **File System** - used to configure security settings for file-system objects, including access control, audit, and ownership.
    - **Public Key Policies** – use these settings to specify that computers automatically submit a certificate request to an enterprise certification authority and install the issued certificate, establish a common trusted root CA, add encrypted data recovery agents and change the recovery policy settings.
    - **IP Security Policies** – IPSec policy can be applied to the GPO of an AD object, and this will propagate that IPSec policy to any computer accounts affected by the GPO.
- Win2K has corrected NT's lack of granular administrative rights. With Win2K it is possible to delegate rights down to the property types on a specific class of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

object. The security for object creation and deletion is managed independently from the modification of object attributes. You can grant an individual or group the right to modify an object without granting that same individual or group the right to create or delete the object. When object permissions are set to allow or deny, all subordinate objects inherit these permissions by default.

- For access control rely on inheritance from group assignments and avoid assigning rights on an individual user account basis. Assign rights high in the tree to get the maximum breadth of effect with the least administrative effort.
- The extended rights and other features further add to the array of access permissions to be managed. Considering this wide range of objects and attributes available, management would be a daunting task without a tool such as the Delegation of Control Wizard. Use the **Delegation of Control Wizard t**o consolidate the permissions into permissions sets which can be used to delegate permissions, and delegate these permissions as high in the tree as possible to avoid overlapping permissions lower down in the tree:
    - In the **Active Directory Users and Computers** display, right-click on the OU to be affected, the click on **Delegate Control** on the context-sensitive menu. Click **Next** on the Welcome screen.

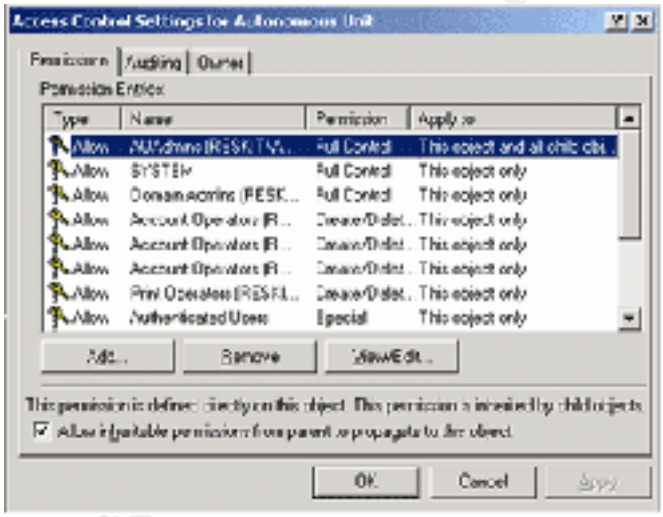


    - The **Users or Groups** window will be active, and the selected users and groups portion of this window will always be blank.
    - Click **Add** to display **Select Users, Computers or Groups** window. Here you can select users and groups from the entire directory, the active domain or another domain including WinNT4 domains from the **Look** in the drop down box.
    - Double-click on the group(s) and/or individual(s) to receive delegation and the wizard will display the selections in the lower portion of the window. Click **OK**.
    - Click **Next** to see the display of **Tasks to Delegate**. The **Delegate the following common tasks** option is enabled by default. Select the tasks

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

you wish to delegate from the list. If the common task list doesn't include the task you wish to delegate, use the **Create a custom task to delegate** option for further options.

- Click **Next** to go to the **Permissions** page where you can set the permissions to be delegated from the sets that appear.
- Click **Next** to finish, which will return you to the **Active Directory Users and Computers** window.
- To view the ACL entries for the OU you just set, you need to enable Advanced Features on the **View** menu and right-click on the group you delegated. Click on **Properties** and then click on the **Security** tab to display the OU's properties. When you highlight an entry in the Name list, the **Permissions** section shows the permissions that group has for the OU. The sample screen shot below shows the **Permissions** tab of the **Access Control Settings**. Double-click on an entry to display more information, which displays the permissions and the access control.



- The Delegation of Control Wizard cannot undo delegations. If you need to make a change, you will have to manually edit all the relevant ACEs. If you rerun the wizard on the same object and change the group or tasks you previously delegated, the wizard will keep all the previous entries. Until Microsoft adds support to revoke the delegation of control wizard settings, it is probably easier to modify the existing ACEs rather than deleting the old ones and adding new ones with the wizard.

Auditing

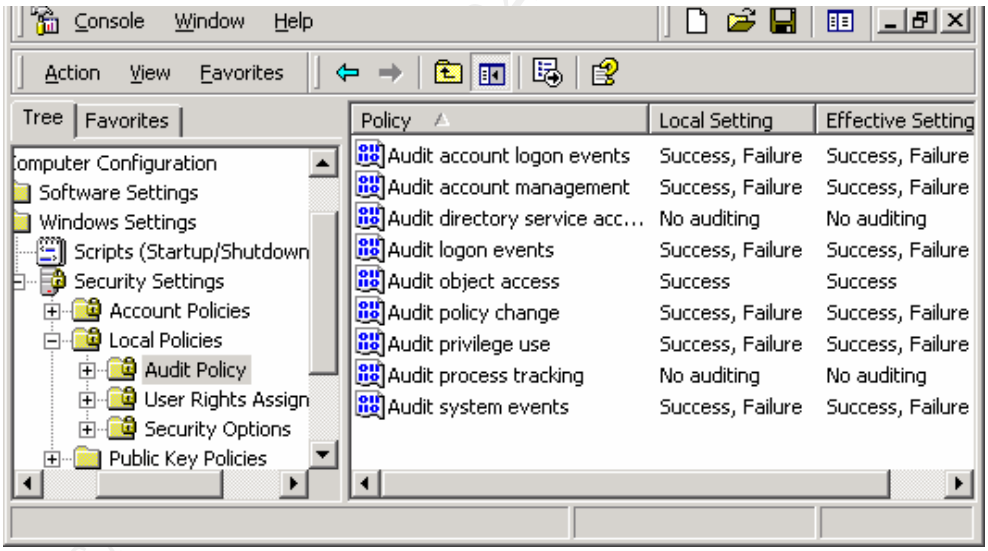
The Win2K auditing subsystem supports six logs. The first three are present in all Win2K systems: Application, System and Security. The last three are present only if you have installed the service: Directory Service, File Replication and DNS. By default, the Security audit log is turned off and must be enabled with the Group Policy. This log

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

contains information regarding security events such as the activity of users and processes, and whether a security service failed to start. The system is the only entity allowed to write to the log, which safeguards the log from being overflowed by misconfigured or rogue applications. The audit log file properties can be controlled with the Event Viewer MMC snap-in, which is handy for controlling both the local audit log settings and those of another system.

Recommendations:

- The Group Policy is the recommended method of setting audit log configuration for a range of systems. When Win2K applies GP, it creates a composite of all the GPOs that link to a computer's site, domain and OUs. It can be confusing when you try to browse the GPOs using the **Active Directory Users and Computers** snap-in, and it can be easy to miss settings. To help determine a system's current audit policy, open the MMC **Local Security Policy** snap-in, and go to **Security Settings/Local Policies/Audit Policy**. This window displays the system's GPO settings in the **Local Settings** column. The **Effective Settings** column shows the system's current settings after all the relevant GPOs have been applied. The new category, *audit logon events*, is used to track logon events in the same manner as NT's *Logon and Logoff*. The other two new categories, *Audit account logon events* and *Audit directory service access*, apply to DCs.



- Security auditing helps you to determine if your system has been attacked and the method and time of the attack. The following best practices table lists some audit events you should audit and the specific security threat that the event monitors:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Audit Event	Potential Threat
Failure audit for logon/logoff	Random password hack
Success audit for logon/logoff	Stolen password break-in
Success audit for user rights, user and group management, security change policies, restart, shutdown and system events	Misuse of privileges
Success and failure audit for file-access and object-access events. File Manager success and failure audit of Read/Write access by suspect users or groups for the sensitive files	Improper access to sensitive files
Success and failure audit for file access printers and object-access events. Print Manager success and failure audit of print access by suspect users or groups for the printers	Improper access to printers
Success and failure write access auditing for program files (.EXE and .DLL extensions). Success and failure auditing for process tracking. Run suspect programs; examine security log for unexpected attempts to modify program files or create unexpected processes. Run only when actively monitoring the system log.	Virus outbreak

- It is very important to have a security auditing policy for domain controllers. Security auditing for workstations, member servers and DCs can be enabled remotely only by domain administrators via Group Policy.
- Auditing of objects involves enabling the policy and then setting the auditing on individual objects. The security descriptor for each object contains the DACL and auditing information called system access control list (SACL). The types of access that you can audit depends on whether you are attempting to audit directory objects or the file system objects, files and folders. Auditing can only be done on NTFS file systems.
- There are numerous events that can be logged, and since the log is limited in size, you should carefully select the categories to be audited and the amount of disk space you want to use for the log.
- It is a good idea to monitor the audit policy to prevent a rogue Administrator from turning off auditing to perform an illegal activity and be virtually undetected.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Since a determined administrator can manipulate the system to cover his tracks, be sure that you grant administrative access only to trusted individuals.

Protocols

TCP/IP

TCP/IP is robust under normal circumstances but in situations where a Win2K server is going to be exposed to the Internet, it is necessary to harden the TCP/IP stack. Denial of Service attacks are hard to defend against. It is important to keep up on the latest DoS attack information in addition to the latest security information on all the products that you are using on your Win2K servers and workstations. Microsoft's web site will automatically send security bulletins on issues as they are discovered. Go to http://www.microsoft.com/technet/security to see previous bulletins and sign up for the automatic bulletin email service.

In the white paper *Data Security and Data Availability for End System* from the Best Practices for Enterprise Security series produced by Microsoft, the following Registry settings are recommended in order to harden TCP/IP against various attacks. All of the TCP/IP parameters are under the Registry key –

HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services

SynAttackProtect

Key:	Tcpip\Parameters
Value Type:	REG_DWORD—Boolean
Valid Range:	0, 1, 2
Default:	0
Description:	When enabled, this parameter causes TCP to adjust the retransmission of SYN-ACKS to cause connection responses to time out more quickly if it appears that there is a SYN-ATTACK in progress. This determination is based on the TcpMaxPortsExhausted parameter.
Parameters:	
0:	**Default Value** – Normal protection against SYN Attacks.
1:	**Better Protection** - This parameter causes TCP to adjust the retransmission of SYN-ACKS to cause connection responses to time out more quickly if it appears that there is a SYN-ATTACK in progress. This determination is based on the TcpMaxPortsExhausted, TCPMaxHalfOpen, and TCPMaxHalfOpenRetried.
2:	**Best Protection** – Adds in additional delays to connection indications to quickly timeout TCP connection requests when a SYN=Attack is in progress. This is the recommended setting. When using this setting, note that the following socket options will no longer work on any

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

socket: Scalable windows (RFC 1323) and per adapter configured TCP parameters (Initial RTT, window size).

EnableDeadGWDetect

Key:	Tcpip\Parameters
Value Type:	REG_DWORD—Boolean
Valid Range:	0, 1 (False, True)
Default:	1 (True)
Description:	When this parameter is 1, TCP is allowed to perform dead-gateway detection. With this feature enabled, TCP may ask IP to change to a backup gateway if a number of connections are experiencing difficulty. Backup gateways may be defined in the Advanced section of the TCP/IP configuration dialog in the Network Control Panel. See the "Dead Gateway Detection" section in this paper for details.
Recommended:	0 – an attack could force use to switch gateways and thus making up switch to non-intended gateways

EnablePMTUDiscovery

Key:	Tcpip\Parameters
Value Type:	REG_DWORD—Boolean
Valid Range:	0, 1 (False, True)
Default:	1 (True)
Description:	When this parameter is set to 1 (True) TCP attempts to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and network congestion. Setting this parameter to 0 causes an MTU of 576 bytes to be used for all connections that are not to hosts on the local subnet.
Recommended:	0– an attacker could force MTU to something tiny and over-work the stack

KeepAliveTime

Key:	Tcpip\Parameters
Value Type:	REG_DWORD—Time in milliseconds
Valid Range:	1–0xFFFFFFFF
Default:	7,200,000 (two hours)
Description:	The parameter controls how often TCP attempts to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	verify that an idle connection is still intact by sending a keep-alive packet. If the remote system is still reachable and functioning, it acknowledges the keep-alive transmission. Keep-alive packets are not sent by default. This feature may be enabled on a connection by an application.
Recommended:	300,000 (5 minutes)

NoNameReleaseOnDemand

Key:	Netbt\Parameters
Value Type:	REG_DWORD—Boolean
Valid Range:	0, 1 (False, True)
Default:	0 (False)
Description:	This parameter determines whether the computer releases its NetBIOS name when it receives a name-release request from the network. It was added to allow the administrator to protect the computer against malicious name-release attacks.

PerformRouterDiscovery

Key:	Tcpip\Parameters\Interfaces\<interface>
Value Type:	REG_DWORD--BOOLEAN
Valid Range:	0: Disabled 1: Enabled 2: Off by default, DHCP-controlled
Default:	2
Description:	This parameter controls whether Windows NT attempts to perform router discovery per RFC 1256 on a per-interface basis.
Recommended:	0 – This will prevent bogus router advertisements
Note:	Use the value in Tcpip\Parameters\Adapters to figure out which value under Interfaces matches the network adapter.

IP Security

IPSec is a modification of the IP protocol at the network layer to provide security. It can be used to secure computers, sites, domains, application communications and dial-up communications. IPSec ensures protection of the transmitted data; it cannot secure the data that is stored on the disk. In the Win2K environment, Encrypting File System technology should be used to secure the data stored on disk.

IPSec addresses the concerns over trusting data sent over the wire with regard to authenticity, nonrepudiation, integrity, and confidentiality. Win2K provides administration in which IPSec policies can be associated with OUs, domains, sites or

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

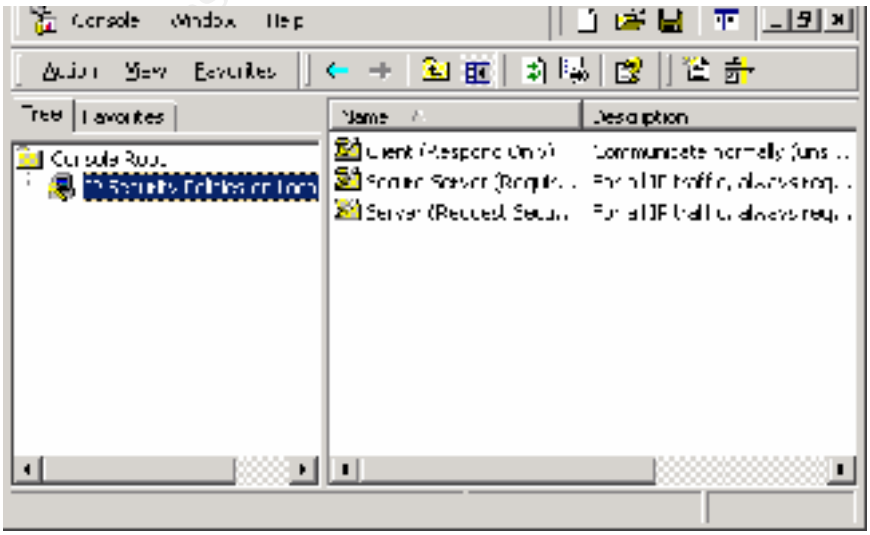
computers. Previously, securing servers that needed a high degree of security often required segmenting the intranet since using different physical segments prevented security violations. With IPSec groups of secure computers can reside within the same physical intranet and still receive the desired protection.

Rules control the implementation of IPSec policy, and they govern when and how IPSec is used based on source, destination and type of IP traffic. When setting up a rule, you can specify which traffic will be secured, the security action to take place when the filter matches, whether to use Kerberos, certificates or shared secrets to authenticate, the scope of the connection for the rule and whether the rule applies to a tunnel.

Win2K comes with three predefined policies: Client, Secure Server and Server. The policies are as follows:

- *Client (Respond Only)* - the client responds to other computers requesting security according to the settings in the default response rule. With this policy active, the client never requests security, but will negotiate IPSec based on the connecting host. You can configure workstations to respond to requests for secure communication but not initiate requests.
- *Secure Server (Require Security)* - server requires IPSec negotiation prior to allowing a connection. This policy will allow unsecured incoming communications, but outgoing traffic will always be secured. You would use this policy in situations where data must always be secure.
- *Server (Request Security)* - server requests IPSec negotiation, but will allow unsecured communications if the other computer is not IPSec aware. You would use this policy to implement security between IPSec enabled computers without sacrificing interoperability with non-IPSec-enabled computers.

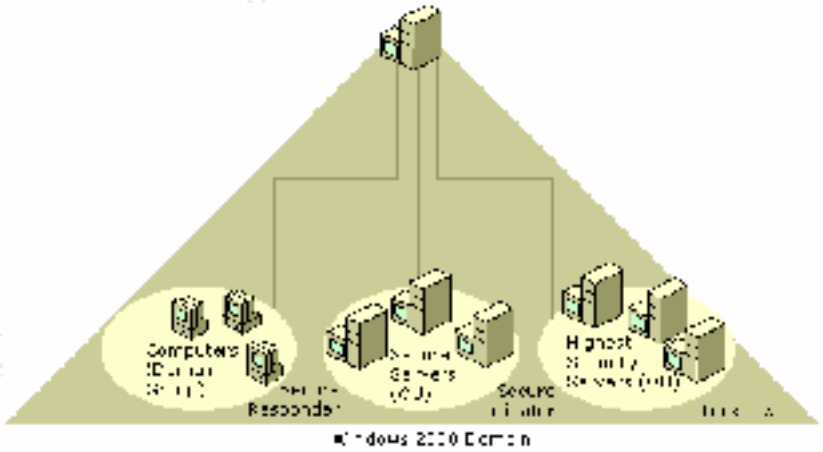
To view the local IPSec policies, open the MMC with the IP Security Policy Management snap-in:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Recommendations:

- In most cases, the default policies will provide the needed security; however, it is possible to modify existing policies or create new ones, if necessary. For example, you can change the authentication method to another method such as an internal certificate authority by modifying the default response filter action of the policy and selecting a new authentication method from the list of Certificate Authorities. Once you have added the CA you want to use, be sure that it appears before Kerberos in the list so that unnecessary validation attempts are minimized.
- Design, create, and test the IPSec policies for each scenario in your security plan. By doing this you will clarify and refine what policies and policy structures you actually need. Before implementing IPSec, consider the features desired, the overhead involved in deployment, the impact on performance and the effect on the existing network. Implementing IPSec will increase CPU utilization, IP traffic and IP packet size. Dedicated network cards can help if performance does become an issue.
- Place the computers to receive the same IPSec policy in an OU and use Group Policy to apply the policy to this container. In the diagram below, servers that store highly sensitive data are placed in the Highest Security OU. Servers that use unsecured communication to exchange data with non-Win2K computers in the domain belong to the Secure Servers OU. Clients that need to respond appropriately when secure communications is required are in the default Computers OU. By using GP the IPSec policies can be easily distributed to these groups in their OUs, which allows the appropriate level of security to be assigned to only those machines needing it, thereby avoiding unnecessary security overhead.



PKI and SmartCards

Pubic Key Infrastructure is at the center of much of Win2K's new security functionality with certificates being used for many security related functions. PKI allows many applications to provide strong asymmetric-cryptography-based security, and this security can be established within an organization or between organizations

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

through the use of trusts. As part of the Win2K Server, PKI can scale to millions of certificates and can be used to enhance security for many types of applications that can be built on top of the Win2K's PKI. Secure web, secure email, the Encrypting File System, code signing to protect against downloads of altered or hacker code from web sites, smart card logon, VPN and remote access authentication are some of the applications that utilize PKI. The Certificate Authority can be customized for different security needs, and user-related PKI administration can be simplified with the use of Group Policy objects.

One of the important security benefits provided by PKI in terms of locking down a Win2K server environment is the support for smart cards. Smart cards can be used to log onto a local or remote computer and reduce the possibility of intruders infiltrating the network by intercepting the logon sequence. Smart card's two-factor authentication is more secure than the traditional password only authentication since it is based on both the possession of the card and the knowledge of the PIN in order to log on. Since smart cards perform private key operations internally, the private key is never exposed during log on, email signatures, TLS/SSL key exchanges and remote card authentication for VPN and DUN. Logging on with a smart card replaces all occurrences of the user's password with the public key credentials, and AD holds a mapping between the certificate and the Win2K account. In Win2K smart card authentication can be required for any account, and the GP can be used to force a logoff when the smart card is removed.

Recommendations:

The following are recommended best practices from the *MS Windows 2000 Server Manual*:

- Be sure to plan your PKI infrastructure before deploying certificate authorities. The *MS Windows Server Manual* section on Certificate Services Concepts and the resources listed in Resources: Public Key Infrastructure will help you with planning a PKI.
- In order to minimize potential for key compromise, the root CA should be offline and its signing key should be secured by hardware and kept in a vault.
- If you are going to use a custom policy module for a Win2K CA, you should first install Certificate Services using stand-alone policy and then replace stand-alone policy with your custom policy. Replacing enterprise policy is not supported and may have unpredictable results.
- Use the Certification Authority MMC snap-in to change security permissions for the CA. Setting permissions using other mechanisms (such as the Active Directory Sites and Services snap-in) may create problems for users attempting to access and request certificates from the CA.
- Organizations should not issue certificates to users or computers directly from the root CA but rather should use at least a three-tier CA hierarchy composed of Root-Intermediate-Issuer CAs to provide flexibility and insulate the root certification authority from attempts to compromise its private key by malicious individuals.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Backing up the CA database, the CA certificate and the CA keys is essential to protect against the loss of critical data. The CA should be backed up on a regular basis based on the number of certificates issued in a period. The more certificates issued, the more frequently you should back up the CA.
- Review the concepts of security permissions and access control, since enterprise certification authorities issue certificates based on the security permissions of the certificate requester.
- When you install the Certificate Server on an AD domain controller, there is an option to select standalone mode or enterprise mode. These modes install different CA policy modules. The standalone mode is geared for the issuance of certificates for external users and will allow you to issue only SSL and S/MIME certificates. Enterprise mode integrates the Certificate Server with AD, which means that you can set ACLs on the certificate templates just as you do on any other AD object and control the distribution of certificates based on group or container membership.

Summary

To paraphrase one of the Ten Immutable Laws of Security published on Microsoft's web site (http://www.microsoft.com/technet/security), if a bad guy gets into your computer, it's not your computer anymore. This paper has attempted to cover several of the essential new Win2K security tools that will help you prevent both the bad guys (the purposeful hackers) and the good guys (the legitimate users in your organization) from using your machines in ways you never intended. Microsoft has paid a lot of attention to security in Win2K, and the integration with AD means that system administrators will have an easier time configuring, administering and monitoring security. In addition, because Win2K relies heavily on industry standards and protocols such as LDAP, Kerberos, PKI, X.500, DNS and IPSec instead of proprietary technologies such as NTLM, the SAM, PPTP and WINS, Win2K is more interoperable than previous versions of Windows and offers the flexibility of replacing Microsoft components with better solutions if the need arises.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Best Practices for Enterprise Security. Microsoft Solutions Framework. http://www.microsoft.com/technet/security/bpentsec.asp.

Boswell, William. *Inside Windows 2000 Server*. Indianapolis, Indiana: New Riders, 2000.

Boswell, William. *Windows 2000: How It Works*. Washington, DC: The SANS Institute, December 2000.

Building Enterprise Active Directory Services: Notes from the Field. Microsoft Consulting Services. Redmond, Washington: Microsoft Press, 2000.

DeClerq, Jan. "Kerberos in Win2K." *Windows NT Magazine*, October 1999, p. 75-81.

Fossen, Jason. *Windows 2000: Active Directory and Group Policy*. Washington, DC: The SANS Institute, Version 2.1.1, July 2000.

Fossen, Jason. *Windows 2000: PKI*. Washington, DC: The SANS Institute, Version 1.0, October 2000.

Iseminger, David. *Active Directory Services for Microsoft Windows 2000: Technical Reference*. Redmond, Washington: Microsoft Press, 2000.

Microsoft Windows 2000 Security Technical Reference. Redmond, Washington: Microsoft Press, 2000.

Microsoft Windows 2000 Server Manual. Microsoft TechNet, December 1999.

Scambray, Joel, McClure, Stuart and Kurtz, George. *Hacking Exposed: Network Security Secrets & Solutions*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

Secure Networking Using Windows 2000 Distributed Security Services. Microsoft TechNet, July 1999.

Securing Windows 2000 Network Resources: Scenario Guide. Windows 2000 Server Technical NotesWhite Paper. Microsoft TechNet, February 2000.

Sharick, Paula. "The Active Directory Delegation of Control Wizard." *Windows 2000 Magazine*, September 2000, p. 75-79.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Step-by-Step Guide to Configuring Enterprise Security Policies. Microsoft TechNet, March 2000.

Step-by-Step Guide to Understanding the Group Policy Feature Set. Microsoft TechNet, January 2000.

Step-by-Step Guide to Using the Security Configuration Tool Set. Microsoft TechNet, February 2000.

"WinNT: Hacker Target # 1". *Win2Knews Electronic Newsletter:* Vol. 6, #3, Issue 237, January 15, 2001. www.sunbelt-software.com.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: October 24th, 2017

Upcoming Training

San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Univ. of California - SEC505: Securing Windows and PowerShell Automation	**Los Angeles, CA**	**Jan 29, 2018 - Feb 03, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**