Global Information Assurance Certification Paper

Guide to Deploying A Windows 2000/Exchange 2000/File/Print Server In A Single Server Environment

Author:
Gary T. Pasikowski

Prepared for:
SANS GIAC GCNT Certification
Version 2.1b
June 2001 – SANS 2001 Baltimore

Table of Contents

1. Warnings

- Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 Servers and underlying components. The changes should not be applied to any other Windows 2000 versions or operating systems.
- When tested recommendations are applied to an operational environment, be sure to have a recent full backup of the server.
- Follow the rule: Test multiple times, implement once.

2. Revision History and Disclaimer

This is a living document; it by no means cover every aspect of Windows 2000 Security, but make every attempt to be accurate and complete as possible. All names used are registered trademarks of their respective companies. Recommendations and suggestions are always welcome from the security community. Changes made and credit to those who recommend the changes will be placed in the following table:

Date	***Version***	***Notes***
26 July 2001	1.0	Original document drafted

3. Introduction

Every organization that deploys a server will incur a information security risk. The main goal in mind is to minimize that risk while keeping functionality to it's fullest. One of the easiest ways to minimize that risk is to deploy many servers, each of which has one set function or task to perform. By doing that it enables administrators the ability to lock down the server to only accomplish that task and does not isolate a single point of failure. There in lies a problem in that not every organization is able to purchase, for reasons of cost, many different servers. When this happens and organizations try to use a server for many different functions, security usually suffers. When an organization is able to, multiple servers are preferred. For example a typical environment may include: a Domain Controller, a file/print server, and a messaging server. When a small organization looking to implement a network, looks at the ideal security picture, they tend to see three servers at approximately $8,000.00 each. The author of this document is a professional Network and Security Consultant and has had this scenario take place. Organizations want to save money, and with the computing power in today's world, why not implement a single server? A more robust server can be implemented to do multiple functions at a half the cost of multiple servers.

This document is designed to be a guide for Security Professionals and System Administrators to be able to deploy a single server for multiple functions safely and securely. These functions include: Windows 2000 Active Directory Domain Controller, File and Print sharing, DHCP, DNS, WINS for non Windows 2000 PCs, and Exchange 2000 Server. This guide is organized such that administrators and security professionals can utilize it in the field.

One must still be aware that deploying all of the above functions is a greater risk, and provides for a single point of failure thus much effort should be utilized to deploy a perimeter defense that provides the greatest amount of security possible and use the practice of 'Defense in Depth' wherever possible. A benefit of current servers in the amount of redundancy that can be built in, one should utilize this benefit when building a server for an organization.

It is the understanding that readers of this document will be knowledgeable of the use of the Windows 2000 Server and it's administration tools. Readers should be comfortable using Regedit, Regedt32, and all aspects of the Microsoft Management Console. This guide will not cover the theories behind the security of Windows 2000 but is rather a guide that can be utilized when deploying networks in the field.

4. Install and Harden the Operating System

Windows 2000 Server has made several advances over its previous version. While the core generally remains the same, Microsoft has made great advances in the area of security. The following statement can summarize Microsoft Active Directory Service: A means by which to store information to be provided to users and the ability to utilize access management for how the information will be distributed. Through the use of the Active Directory directory service most aspects of Windows 2000 Server mold themselves into the directory, thus sharing a common security model. This tight bond with the operating system allows services such as Exchange 2000 Server, DNS, and others to share file permissions, registry settings, password usage, user rights and other aspects of Windows 2000 security. It is a direct advantage to the administrator of the server for there is no separate security database to maintain as there was in such applications as version 5.5 of Exchange. To fully accomplish this, one must have a secure operating system from the start. The following section contains information regarding the security of the operating system of the single server domain.

4.1. Install

- Install Windows 2000 Server or Advanced Server on a clean server from the original media.
- Always use NTFS on all volumes. This will assure maximum security can be applied down to the file level.
- Do not install such things as Chat, Games, Multimedia Service, etc. Some of these options will open listening ports on the server, or at the very least waste valuable system resources. They are usually not necessary in a business environment.
- Selectively install IIS 5.0.
    - If there is a business need for services such as Outlook Web Access, one should install IIS and Exchange 2000 Server, configured as a front-end server, and on a separate server located in a DMZ.
    - Do not use this server for a web server. It is the author's belief that utilizing a multiple function server for a web server will incur too much risk. Thus one should not install such services as FTP, FrontPage 2000 Server Extensions and associated dependencies, Internet Services Manager (HTML) and Documentation (Which contains all the 'Samples' in which many exploits utilize).
    - World Wide Publishing Server Service will need to be installed but can, and should be disabled. The SMTP service depends on this service being installed, but not started.
- Install Microsoft Windows 2000 Server Resource Kit. This kit set contains many tools that one can use. Be sure to read all one can do to use the Resource Kit to it's fullest.

4.1.1. Active Directory

- Install Active Directory
    - Choose to only have permissions compatible with Windows 2000 Domain Controllers. If one chooses to install with permissions compatible with pre-Windows 2000 servers, they are allowing anonymous read access to information on the domain. With this installation being a single server install, there should be no choice but to install with permissions compatible with only Windows 2000 Domain Controllers.

Note: If when installing, the mistake was made and one chose to install with permissions compatible with pre-Windows 2000 Domain Controllers, it can be fixed by typing the following command (using the quotation marks that are typed below) at the command prompt:

- *net localgroup "Pre-Windows 2000 Compatible Access" everyone /delete*

    - When prompted for a password in which Active Directory will use, always utilize proper strong password management. For Example: T1tpwd1u4m@Dss - Translated to: This is the password I use for my Active Directory Server service
    - Choose to create both a new Tree and Forest.
    - Choose to install DNS as part of the Active Directory installation.
        - DNS should be Active Directory Integrated. By doing this, it is easily configurable to who can update the DNS service.
        - Choose to enable secure dynamic updates for this zone.
        - Configure other services as needed, such as DHCP*, WINS for legacy systems, etc.

*Note: Do not allow the DHCP server to perform updates to the DNS Server records on behalf of the clients, for secure dynamic updates can be compromised according to Microsoft's online help. It is the default setting not to allow this and is best practice to keep the setting turned off. If this option is required in the organization, it is best to deploy a second server to perform DHCP functions.

4.1.2. Further Install Procedures

- Apply the latest Microsoft Service Pack, currently Service Pack 2
- For a list of the bugs fixed in Service Pack 2, see Q282522 located at http://support.microsoft.com/support/kp/articles/Q282/5/22.asp
- Install Exchange 2000 Server from original media
- Rename the built-in administrator account to something generic
- Put a strong password on the Guest account and disable it
- Create a user named 'Administrator', give it a strong password, provide it no

access rights and disable it.

- If one creates an additional partition after the install of Windows 2000, the 'Everyone' group will be given Full Control to the root of that drive. Be sure to remove the 'Everyone' group from any logical drives created.

Tip:

Before proceeding the to the next section, it is advisable to perform a full backup of the server. Also, check each subset of the Event View to fix any errors or warnings that exist. It is important to know that if a problem occurs, it resulted from a Hot Fix or possibly an error that occurred during install of Windows 2000 Server.

4.2. Disabling Unneeded Services

- Certain services within Windows 2000 Server will open ports on the system. Many of these services are unneeded for a typical installation of a File, Print and messaging server. It is advisable to disable the following services:
  - Alerter
  - Clipbook
  - Distributed File System
  - Distributed Link Tracking Systems Client
  - Distributed Link Tracking Systems Server
  - Fax Service
  - Indexing Service
  - Internet Connection Sharing
  - Intersite Messaging
  - Messenger
  - NetMeeting Remote Desktop Sharing
  - Network DDE
  - Network DDE DSDM
  - QoS RSVP
  - Remote Access Connection Manager
  - Remote Access Auto Connection Manager
  - Remote Registry Service
  - Task Scheduler
  - Telephony
  - Telnet
  - Windows Time

4.3. Removing Files and Registry Entries

Microsoft builds in support for OS2 and POSIX subsystems, into Windows 2000. There

are known exploits that can utilize vulnerabilities associated with these. One should remove the files installed to heighten the overall state of security.

- Navigate to %SystemRoot%\system32\dllcache
  - This is where Windows 2000 stores a backup copy of any files in which it will restore in the event of the originals being deleted
  - Delete os2.exe, os2ss.exe, and os2srv.exe
- Navigate to %SystemRoot%\system32
  - Delete os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe, psxdll.exe, all files in the os2 folder
- Delete the following registry entries
  - HKLM\System\CurrentControlSet\Control\Session Manager\Environment\OS2LibPath
  - HKLM\System\CurrentControlSet\Control\Session Manager\Subsystems\(Optional, OS2 and POSIX)

4.4. Patches and Hot Fixes

- Apply all relevant hot fixes that have been released since Service Pack 2 at the time you install the server.
  - See http://www.microsoft.com/security and click the link to 'Bulletins'. Choose Windows 2000 and Service Pack 2 from the drop down boxes. Download and install all fixes listed.
  - One may also use http://www.windowsupdate.com as a check for further updates.

IMPORTANT NOTE: Log all patches applied to the server. It is important as new fixes are released, to know which patches have been applied. It is suggested one keeps a short log (see Table 1), retain the files on the server (see Figure 1), as well as print the Microsoft Security Bulletin and store it in a safe place.

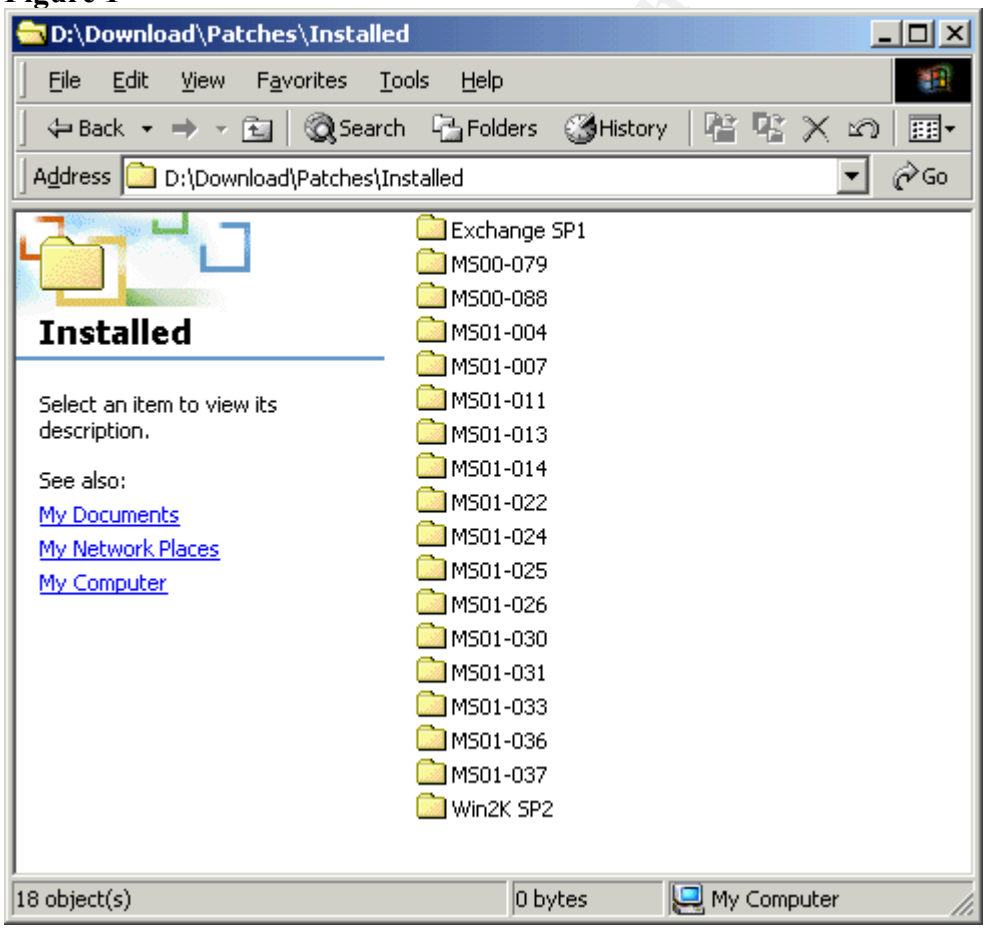
Table 1

Date:	***Server Name:***	***Vulnerability/Bug and Patch Applied:***
1 July 2001	Win2K_Server*	Windows 2000 Service Pack 2
1 July 2001	Win2K_Server*	MS00-079 – Q276471_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS00-088 – Q278523engi.exe
1 July 2001	Win2K_Server*	MS01-004 – Q285985_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-007 – Q285851_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-011 – Q287397_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-013 – Q285156_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-014 – Q286818_w2k_sp3_x86_en.exe and Q287678engi386.exe
1 July 2001	Win2K_Server*	MS01-022 – rbupdate.exe

1 July 2001	Win2K_Server*	MS01-024 – Q294391_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-025 – Q296185_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-026 – Q293826_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-030 – Q299535_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-031 – Q299533_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-036 – Q299687_w2k_sp3_x86_en.exe
1 July 2001	Win2K_Server*	MS01-033 – Q300972_w2k_sp3_x86_en.exe
5 July 2001	Win2K_Server*	MS01-037 – Q302755_w2k_sp3_x86_en.exe
9 July 2001	Win2K_Server*	Exchange 2000 Service Pack 1

*Name changed to sanitize document

Figure 1



4.5. Other Updates

It may be necessary for an organization to load additional software on the server.

It is recommended that this be kept to a minimum for certain software can contain vulnerabilities, which may be used as a means to compromise the server. It is advisable to patch the software that is bundled with the install of Windows 2000 Server, such as Internet Explorer. Most administrators will not need to, but if Microsoft Office is installed, be sure to visit http://office.microsoft.com for product updates.

4.6. Groups

Groups within Windows 2000 are a collection of users or other groups (nesting). Two types of groups exist, Distribution and Security. A Distribution Group is used for applications such as Exchange Server. This group's primary purpose is to allow a user to e-mail a number of other users with a single e-mail address. There are three main types of Security Groups that can be added or modified within Windows 2000. The first group is called Universal. This group is only available if the server is running in native mode. It is used to bring together other groups that span across multiple domains. The universal group does not apply to the deployment of the server in this paper since a single server environment would only house one domain.

The next type of group is called Global. Defined, Global groups are a way in which to create sets of users from inside the domain, to be used within or outside the domain. Global Groups are where most administrators will add their uses. The Global groups can then be nested within each other to provide manageability and options for growth.

If the organization knows for a fact that other domains will never be added, they may choose to use the Domain Local groups. These groups are similar to the Global Groups on how they provide access to resources within the domain, but unlike the Global Group, Local Domain Groups cannot traverse across domains. By assigning users to groups, and giving a group a specific right to view/change/modify/etc., management of rights the server become an easier task. Nesting is an efficient way to manage groups within an organization. It is important to note, one can only nest Distribution Groups in a mixed-mode environment, and on the same token one must run in native mode to nest Security Groups. It is important to properly plan and document a grouping strategy prior to deployment of a server.

4.7. Access Control

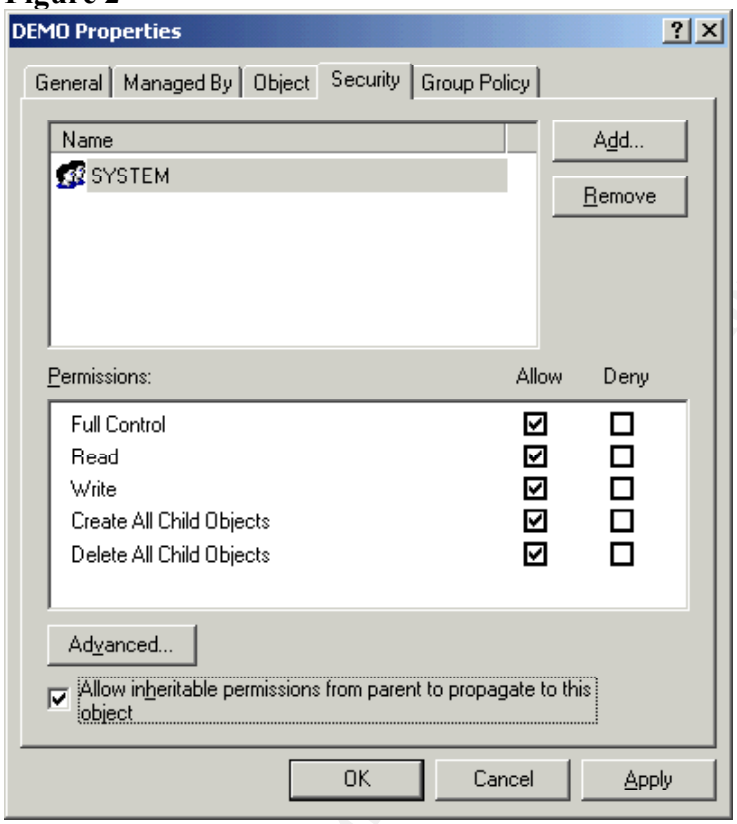
Access control in Windows 2000 applies to both file permissions and permissions within Active Directory. Every object, including those within active directory, has access control measures in place. It is to be noted that to view the Access Control measures within Active Directory, one must perform the following steps:

- Open Active Directory Users and Computers from the Administrative Tools menu.
- Click on the View menu and choose Advanced Features

When one Right Clicks and selects Properties on an object either within Active Directory

or Explorer, they should see the Security Tab as in figure 2 on the following page. With this, along with properly managed groups, administrators can properly control resources on their server. Implement the tightest possible control on files and directories according to local security policies. If one clicks on the Advanced button on the Security tab, they can see a much more in-depth view of the Access Controls in place, as well as the auditing tab and owner properties. In most cases the Access Control on the default properties page will be adequate to control permissions.

Figure 2



4.8. System Check

An administrator should use a 3rd party tool, such as ISS System Scanner or one of the many others to check for further vulnerabilities on the server. The Windows 2000 Resource Kit does come with ISS System Scanner, but is not installed as part of the Resource Kit installation. It should be noted that this is a basic version and is only updated to the point of the release of the resource kit. It is best utilized to provide a baseline configuration. To install System Scanner:

- Insert the Resource Kit CD-Rom
- Navigate to the \Apps\SystemScanner directory
- Run SysScannerSetup.exe and follow the onscreen instructions
- Run System Scanner after a restart of the server per the included documentation

As a further system check, use the IIS 5.0 Hot Fix Checking Tool (hfcinst.exe)

downloadable from http://www.microsoft.com This is a valuable tool to any administrator no matter to what extent they are using IIS 5.0, and should be run often.

Author's Note: Although it should go without saying, any administrator of a Microsoft server should subscribe to the Security Bulletin list service at http://www.microsoft.com/security .

5. Policy in Windows 2000

The next step in creating a secure single server is to use Windows 2000 policies to strengthen the security of the server, as well as desktops and user configurations. To accomplish this task one must implement policies in two areas

- Domain Policy
- Domain Controller Policy

The Domain Policy is a means by which Windows 2000 administrators can control all user, desktop, and member server settings from a centrally managed location. (Provided an Organizational Unit is not configured to block policy inheritance.) Just as most aspects of Windows 2000, such as DNS, the Group Policy Objects are Active Directory integrated. The Group Policy is an important aspect of the security of Windows 2000. One cannot have a secure environment with just a secure server; an organization must have overall security that includes users and desktop computers.

The Domain Controller policy is just as important, for it governs the security settings on which your domain controllers run. It is important to remember that the settings in the Domain Controller policy will only affect those computers in the Domain Controllers GPO.

Windows 2000 provides a simple way to implement policies using the Microsoft Management Console and pre-defined policy templates. Windows 2000 Server is installed with some of these templates available to use by administrators. If one chooses not to use the templates provided by Microsoft, one can download templates from such organizations as the National Security Agency (http://www.nsa.gov) or create their own policies to implement. For this paper the author has chosen to use the templates provided by the NSA, and modify them slightly to conform to local security policies.

Caution: Certain settings in the policy regarding LAN Manager Authentication Level will break functionality with legacy systems. Be sure to implement the LAN Manager patch on the legacy systems to allow them to use NTLMv2 (recommended) or lower the restriction regarding LAN Manager.

The following will illustrate how to implement and configure the Domain and Domain Controller policies.

- Download and save the desired security template to: C:\Winnt\Security\Templates where C: is the System Root (only necessary if an organization is going to use other's security policy templates)
- View the template prior to implementing it. This will ensure that the security template will conform to the policies in which an organization sets forth. One can make any changes necessary prior to implementing the policy.
    - Choose Run from the Start menu and type *MMC*

    - Choose Add/Remove Snap-in from the Console Menu
    - Click Add
    - Choose Security Templates and click Add
    - Click Close and OK
- Export the Default Domain Policy and Default Domain Controller Policy prior to implementing a new policy. This gives an administrator a safe guard for going back in the event the implemented policy does not work as an organization wishes.
- Implement the Domain policy
    - Start Active Directory Users and Computers from the Start menu, Administrative Tools
    - Highlight the Organization, right-click and select properties
    - Click the Group Policy tab
    - Highlight the Default Domain Policy and click Edit
    - Navigate to Computer Configuration/Widows Settings/Security Settings
    - Right-click Security Settings and select Import Policy
    - Highlight the policy in which to implement on the domain and click Open
    - After verifying the template has been imported, close the Group Policy window, click OK on the organization properties page
- Implement the Domain Controller policy
    - Start Active Directory Users and Computers from the Start menu, Administrative Tools
    - Highlight the Domain Controllers container, right-click and select properties
    - Click the Group Policy tab
    - Highlight the Default Domain Controllers policy and click Edit
    - Navigate to Computer Configuration/Widows Settings/Security Settings
    - Right-click Security Settings and select Import Policy
    - Highlight the policy in which to implement on the domain and click Open
    - After verifying the template has been imported, close the Group Policy window, click OK on the organization properties page
- Rename default accounts
    - Rename the administrator and guest accounts on both the Domain and Domain Controller policies
    - Optional: Create a decoy Administrator and Guest account with no access but be sure to disabled the accounts
- Additional Changes
    - Certain settings will have to be modified to ensure Exchange works properly on the server. Those changes are the following:
        - If the Exchange server is used as for a POP3 or IMAP server set

the client to use Secure Password Authentication

- Ensure the Exchange Enterprise Servers group is given the right to manage audit and security logs in the Domain Controller Policy
- Allow Exchange Domain Servers Group full control access to the following registry entry:
    - HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg

Tech Note:

Shortly after installing the policies, the author of this document encountered the following two error messages in the Application Log: See Figure 3 and 4.
For the reader of this document who may encounter the same problem, the fix is as follows:

- Add the ExtensionDebugLevel DWORD with the value data 2 to the following registry key:

  HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\GPExtension\{827…}*

  *Any GUID starting with {827}

- Type cmd from the Start menu, Run, Open dialog box
- Type "secedit /refreshpolicy machine_policy /enforce" exactly as stated without the quotes followed by the Enter key
- Browse to \Winnt\Security\Logs and open the Winlogon.log file
- Read through the log file looking for errors
- In the authors case, a setting in the User Rights Assignments was granted to a security group which did not exist
- Either remove the setting in the policy or create the user/group
- See Microsoft Knowledgebase article Q234237 for further details

Figure 3

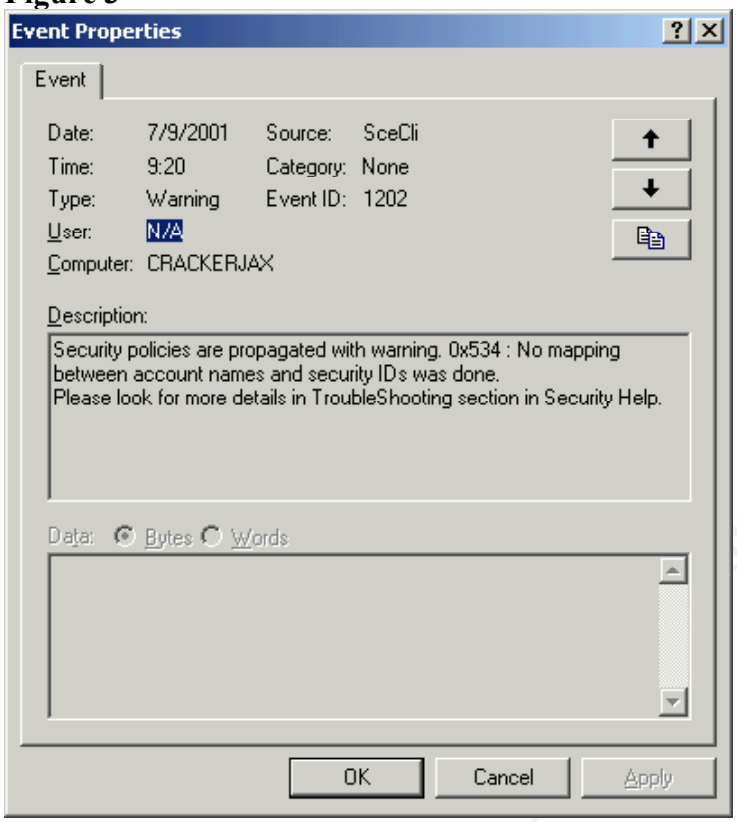
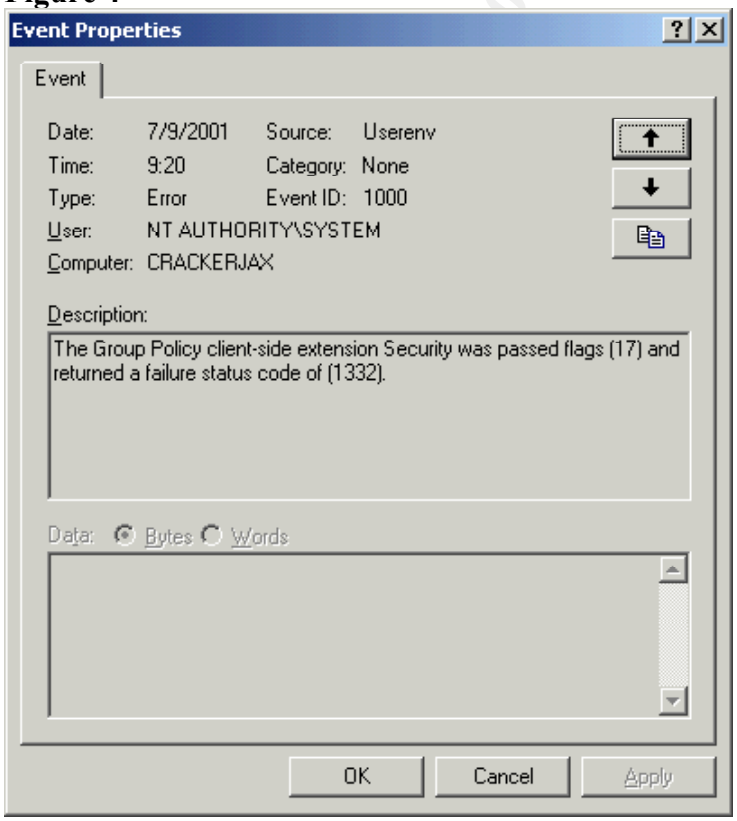


Figure 4



6. Viruses

This section is going to cover the aspect of viruses. One must protect their Windows 2000 servers from viruses. Email viruses in particular are more dangerous and numerous then ever, and the numbers are continuing to rise. One cannot rely on desktop or server protection alone. Protecting the network, and the server from viruses should be a 3-fold process, otherwise known as defense in depth.

- Protection at the Internet Gateway
- Protection at the server
- Protection at the desktop

NOTE: The author of this paper is not endorsing any of the products mentioned in the following section. Rather, he is using them as an example to illustrate the ability to use different vendors to achieve the best aspect of defense in depth.

6.1. Gateway Protection

The first layer of defense should be your gateway to the world. One should install a product such as eSafe Gateway from Aladdin Knowledge Systems. (http://www.esafe.com) One of the benefits the author has found with this product is that it can be installed on a standard workstation, and does not need any special hardware. It can be configured to not only scan and block viruses, but also any attachments that the local security policy does not allow, for example: *.exe, *.jpg, *.mpg, etc.

6.2. Server Level Protection

Next, install two forms of anti-virus protection at the server level. The first form should be an anti-viral program that only scans files. For example one could use ServerProtect from Trend Micro (http://www.antivirus.com) to provide the file level anti-virus protection. The other program should be one that incorporates itself into the messaging system, typically called a groupware anti-virus application. For example one could use GroupShield from Network Associates (http://www.nai.com) to provide this aspect.

6.3. Desktop Protection

Finally install an anti-virus program at the desktop level like Norton Anti-virus from Symantec (http://www.symantec.com). If the desktops are Windows 2000 Professional based, some anti-virus programs can utilize the group permissions on the desktop, enabling only administrators to make changes to the anti-virus program. We in the security community know how much users like to "Play".

6.4. Virus Protection in closing

It is no shock that viruses continue to become a problem. It is critical that all levels of defense be maintained. To prove that aspect one just has to look at the W32.Sircam.worm virus that is wreaking havoc on the Internet at the time this paper is being written. According to an article at ComputerWorld.com (http://www.computerworld.com/storyba/0,4125,NAV47_STO62470,00.html) not all commercial antiviral scanning engines are identifying the worm as harmful. With that said, one can understand the importance of having virus protection at the gateway, groupware, server, and desktop level from different software vendors.

7. Physical Security

When it comes to the aspect of physical security, the main weapon of choice is common sense. If an intruder does not have any usernames or passwords but can physically touch the machine, you are compromised. There are tools in which one can boot to a different operating system using the floppy drive and access any files located on that server.

- Keep the server stored in a locked room with limited access.
- Use the floppy-lock utility found in the resource kit to restrict unauthorized use of the floppy drive.
    - Open a command prompt window by typing 'cmd' at the Run window
    - Type the following command, assuming the Resource Kit was installed to the default location:
        - *instsrv FloppyLock "c:\Program Files\Resource Kit\Floplock.exe"*
    - Open the Computer Management snap-in.
    - Start the service and configure it to start automatically on startup.
- For organizations that require enhanced security, modify the system using the SYSKEY utility. The default installation of Windows 2000 will have SYSKEY enabled, but with no password and it stores the binary key locally. If one would like to change this, follow the following steps:
    - Click 'Start', 'Run' and type 'syskey.exe'
    - Click on the 'Update' button
    - Click the radial button next to 'Store Startup Key on Floppy Disk'
    - Insert a floppy disk into the drive when prompted
    - Make a copy of the disk and store both in secure, safe place, preferably one on-site and one off-site
    - The author of this paper recommends that one take the data from the disk and place it on a CD-ROM, since they have a history of being more reliable.
    - If one is not comfortable with having to use media to start their server, they may apply the password startup feature.
    - Click 'Start', 'Run' and type 'syskey.exe'
    - Click the radial button next to 'Startup Password'
    - Type in and confirm a strong password in the boxes provided
- Disable or remove all removable boot media devices.

- Lock the server case if possible, especially important if the server contains 'Hot-Plug' drives.
- Implement a BIOS password.

8. Auditing

Auditing is a means by which to check events that have occurred on the server. In other word it is a way to determine whether your system has been attacked. It by no means should be the only way to determine this. To provide the complete picture on an external attack, one should have logging on their firewall as well as Intrusion Detection in place. Auditing on Windows 2000 does however give an excellent means to determine what internal users are attempting to do. It is important to remember that one should set up Auditing based on their local Security Policies. When completing section 5 of this paper, auditing and permissions relating to auditing may have been set up on the domain controller, but this will depend on what was modified on the security template prior to importing it. Be sure to review these settings by doing the following:

- Open Active Directory Users and Computers
- Right click on Domain Controllers and select Properties
- Click on the Group Policy tab and click Edit
- Expand Windows Settings\Security Settings\Event Log\Settings for Event Log
- Review all settings listed. Some important points to make are:
    - Ensure the maximum size is sufficient for the organization
    - Do allow the system to clear or overwrite any events
        - Backup the logs on a regular basis then clear them manually. The logs provide forensics value in the event the organization is attacked.
    - Restrict access to all logs
    - Set the server to shutdown in the event the security audit log is full. Setting this is a means to foil any attacker that tries to fill the security log with false information prior to executing his true motive. Use caution with this setting. One can monitor the size of the any log by navigating to %SystemRoot%\system32\config*.evt
- Perform the above steps on the Domain Policy as well. This will ensure that in the event that a member server is added to the domain, the server will already be in regulation to the local security policy

The next aspect relating to auditing is the configuration relating the auditing of files and folders on the server. One must specify which files and folders that will be audited as well as what actions will trigger the audit response. To choose how files and folders are audited perform the following actions:

- Open Windows Explorer
- Right click on the File or Folder that will be audited and select properties

- Click on the Security tab and click the Advanced button
- Click Add
- Choose the users or groups to which the audit policy will apply
- Choose how the auditing will be done per the user or group selected

Auditing can get very difficult to manage thus it is imperative that proper documentation be accomplished to easily track and manage what is being audited.

9. Protecting Sensitive Data

9.1. Encrypting File System

When deploying a single server to do so many functions, one concern may be the ability of users to read sensitive/unauthorized data, for example employee records containing sensitive data that may have been placed in the wrong folder. One of the easiest ways to add a layer of protection to this type of data is the Microsoft Encrypting File System (EFS). It should be noted that using EFS does create an additional burden on the server as well as clients accessing the encrypted files, thus discretion should be used when choosing which files/folders will be encrypted. One feature of EFS is that if the folder/file is moved, the encryption will follow it. To deploy EFS, follow the following simple steps:

- Open Windows Explorer
- Right click on the folder or file one would like protected and choose Properties
- Click the Advanced button
- Click the checkbox next to 'Encrypt contents to secure data'
- Click OK, and OK again and if an entire folder was selected, one will be prompted to choose whether they would like to apply the changes to the folder only or the folder, all sub-folders and files.
- One can also export and delete the private key on the recovery agent if local security policies permit this.

Those steps can be reversed if one ever wants to remove the encryption from the file/folder.

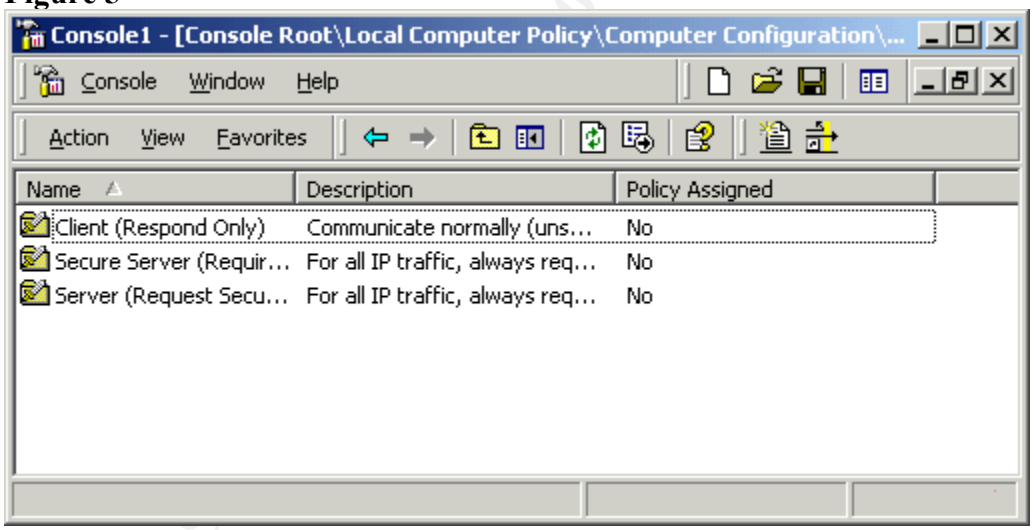
9.2. Internet Protocol Security

If an organization is concerned with risks such as man-in-the-middle attacks, they should deploy Internet Protocol Security (IPSec). IPSec can only be implemented between Windows 2000 versions, thus one would not be able to implement the Secure Server policy if any other version of Windows existed on the network. Once again it should be noted that utilizing IPSec would incur an additional load upon the network. Careful planning should be done prior to implementing IPSec. The proper means to deploy IPSec is to create a specific Organizational Unit within Active Directory and move

computers that must have secure communication into that OU. Figure 5, on the following page shows the default policies that are included with Windows 2000. If one would like more information regarding creating a custom policy, please read the chapter regarding Network Security, IPSec, in the book *Microsoft Windows 2000 Security Technical Reference*, from Microsoft Press. If one of the pre-defined policies meeting the needs of the local security policy, simply follow the following steps to implement it:

- Open Active Directory Users and Computers
- Create a new Organizational Unit (i.e. SecureComm)
- Move computers that require secure communications into the new OU
    - Highlight computers, right click, select move, and choose the new OU
- Right click the new OU and select Properties
- Click the Group Policy tab and click Add
- Navigate to the root, choose the Domain Policy and click OK
    - The author then prefers to block policy inheritance, this is optional and is only for management reasons
- Choose to edit the policy
- Navigate to Computer Configuration/Windows Settings/Security Settings/IP Security Policies on Active Directory
- Right click the policy and choose Assign

Figure 5



10. Protecting Exchange

With the way that Microsoft has embedded Exchange 2000 Server into Windows 2000, very little must be done to protect the services other that what has been accomplished above. If one wishes to protect the content of messages, they can explore such avenues as PGP (http://www.pgp.com) on client workstations or the Secure/Multipurpose Internet Mail Extensions (S/MIME) format, which in the author's opinion will soon become the standard for e-mail communications. Some actions to be

taken to ensure a secure Exchange environment include:

- User education
  - Do not open e-mail from unsolicited sources
  - If a questionable e-mail is received, contact an administrator by phone. Do not forward it on.
- Ensure all anti-virus definitions are current
- Monitor message logs

11. Conclusion

Once again this document's intended purpose is to be used as guide for field engineers and security administrators to be able to deploy a secure server for small organizations utilizing a single server. This guide only scratches the surface on all the possibilities that can be done to secure a Windows 2000 Server. The author hopes that this guide will assist everyone when it comes to deploying a secure single server for an organization.

References:

1. Madden, Jeff (Program Manager). MCSE Training Kit Microsoft Windows 2000 Server. Redmond, WA: Microsoft Press, 2000.
2. Internet Security Systems, Inc. Microsoft Windows 2000 Security Technical Reference. Redmond, WA: Microsoft Press, 2000.
3. Risk, Allan (Group Program Manager). Microsoft Exchange 2000 Server Resource Kit. Redmond, WA: Microsoft Press, 2000.
4. National Security Agency. "Windows 2000 Security Recommendation Guides." Windows 2000 ".inf" Files. June 2001. URL: http://nsa1.www.conxion.com/win2k/download.htm.
5. Weiss, Todd R. "Sircam worm spreading; vendor warnings upgraded." July 23, 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62470,00.html
6. Sanderson, Mark J., Rice, David C. "Guide to Securing Microsoft Windows 2000 Active Directory." December 2000. URL: http://nsa1.www.conxion.com/win2k/r1/guide_to_securing_microsoft_windows_2000_act.pdf.
7. "MSDN Library October 2000." 1999-2000 Microsoft Corporation. Three CD-ROM set, MSDN Subscription.