GIAC Certified Windows Security Administrator (GCWN) Practical Assignment Version 4.0, Option 2

Locking Down Windows2003 Servers in a Heterogeneous Environment

SANS Spring Break Conference
Orlando, Fl
April 2-7, 2004

By Joseph Kaluzny

Submitted on June 7th, 2004

Table of Contents

Abstract

Using Group Policy Objects to control access to systems within an environment provides several key benefits in the areas of both administration and security. The primary benefit in the area of administration is the ability to quickly and easily change settings on multiple systems from a single, central location. From a security perspective, Group Policies can ensure that settings put in place are not altered or overridden after they have been applied. Although the Windows 2000 and Windows 2003 architectures are more or less the same, some significant improvements have been made in the Windows 2003 release in terms of Active Directory and Group Policy. These enhancements will be identified and highlighted throughout the paper.

The focus of this paper will be to describe how the application of Group Policy Objects can be taken a step further and fully exploited to allow administrators and security personnel to tightly lock down a Windows2003 Server environment. This method of using Group Policy Objects is ideal for completely controlling access to servers in a heterogeneous environment containing different types of servers and multiple support groups. Key settings that are essential for adequate security will be discussed in detail as well as new policy objects in Windows 2003 that make significant contributions toward securing the enterprise. Underlying Network and Active Directory designs that support the Group Policy design will also be detailed within the paper with an emphasis on improvements Microsoft has made in Windows 2003 within Active Directory.

1. **Introduction – Enterprise Description**

GIAC Enterprises is a large retail company with approximately 10,000 employees operating in the South-East region of the United States. GIAC Enterprises is broken down organizationally into 2 segments, a Store segment and a Corporate/Support segment. The store segment contains all the servers, workstations, and users located in the actual stores while the corporate segment contains all systems and users for all other departments outside the stores. Retail stores are naturally critically to the operation, and they are designed to be able to operate autonomously should a network connection to the central data center fail. Since warehousing is relied on to keep an optimal level of inventory at the stores, it is also considered a key component within the business. Other support departments such as Accounting, Information Technology, Human Resources, etc. all have a varying degree of importance below stores and warehousing. There are approximately 200 store locations dispersed across several states, and 4 separate support locations where large numbers of users are consolidated.

Systems

The stores contain only a domain controller and a single member server that runs a few applications used for sales, inventory management, etc. Store servers are very static, and outside any data, all servers are the same throughout all the stores. The corporate segment contains a very diverse set of servers that run a wide variety of applications. It requires a wide variety of expertise to support these servers, making it quite complex from a support standpoint

Support Users

Stores are centrally managed by a single group located within the corporate headquarters. Due to a minimal number of applications, a single group of engineers can efficiently support servers within the stores, so access to servers can be restricted to only that one group. Servers in the corporate segment contain a wide range of functions and applications so multiple groups of support users are required to manage and maintain these systems.

Assumptions

The following assumptions have been made to allow for a design that is ideal and is secure as possible considering the latest versions of software:

- GIAC Enterprises has upgraded or will be upgrading all WindowsNT and Windows2000 Servers to Windows2003. GIAC Enterprises has upgraded or will upgrade all WindowsNT Workstation and Windows2000 Professional workstations to Windows XP.

- All applications have been upgraded to their newest versions that are able to run on Windows 2003/Windows XP.

- Part of GIAC Enterprises business is selling medication to customers; therefore HIPAA compliance is of great importance. GIAC Enterprises currently has approximately 100 Domain administrators providing support across all servers. In a desire to adhere to best security practices and limit the advanced access of support users, the number of Domain Administrators will be limited to 6. The remaining support employees who previously had domain administrator membership will continue to require varying levels of access to Domain Controllers and servers within the environment. Group Policy Objects will be utilized to grant the proper levels of access to servers at a level as minimal as possible.

- The focus of this paper is on securing the server environment. It is assumed that user account and workstation account OUs exist and have been secured according to best practices using group policy objects. Workstations and typical users and any OU's and GPO's supporting them will not be included within the scope of this paper.

.

2 Network Design

GIAC Enterprises physical network spans across 3 states. There are four areas that serve as major support locations where all of the corporate servers reside. These areas are physically connected through T-1 lines to a central data center in a hub and spoke fashion. Redundant backup connections are configured to the data center but no connections exist between other locations. As a standard, all servers consist of hardware RAID (either Raid-5 or Raid-1, depending on the number of drives), redundant fans and redundant power supplies. All domain controllers follow the same standard and additionally are configured with teamed NIC cards using load-balancing by IP address. All network server closets in all buildings are locked and protected by badge access readers as well as entry to all buildings themselves. Each physical location consists of the following:

Corporate Campus – The Corporate Campus consists of several buildings all within a 3 mile radius. These buildings include the Data Center, Corporate Headquarters, 2 Main Warehouses, an Employment office, a Transportation office, and a Branch Office, all of which are connected by 100MB speed links. All the buildings in the corporate area have been placed into a single corporate site, mainly because they are connected by high speed links. This will reduce administrative overhead by allowing the KCC to automatically manage replication between these areas. Intra-site replication delay in Windows2000 is 5 minutes; Windows2003 replication delay is now significantly smaller, only 15 seconds. The breakdown by building follows:

- Data Center Building – The Data Center is a concrete, windowless building that houses most of the servers in the Corporate Campus. The employees that work within this building are all in the IT department and number about 200. Because of its construction and location of IT and support areas, most servers are consolidated within this building. The server breakdown is as follows:
    - 3 Exchange Servers reside at the Data Center, 2 to support corporate users, and 1 to support store users.
    - All 30 intranet web servers exist in the Data Center building, 10 for development, 10 for staging and 10 for production.
    - 5 File servers hosting data for both corporate and store employees of varying departments throughout the entire corporate site.
    - 2 Print servers support the IT department within the building and have queues for 15 non-color laser printers and 1 color laser printer.
    - All 15 Database servers are consolidated within this building and provide back-end storage for both store and corporate applications throughout the enterprise.
    - All 30 Application servers reside in the Data Center that host applications used by corporate users.
    - Of the 9 Corporate Domain Controllers in the area, 6 are within the Data Center building. 2 support the empty root domain, and 4 support the corporate domain and are the FSMO role holders. Of

    the 208 Retail Domain Controllers, 8 are contained within this building, 3 are FSMO role holders, and 5 are bridgehead servers.
    - All DMZ servers, including a public web server, DNS server, and SMTP server are also located in this building since this is where the single Internet connection exists.
    - Approximately 30 non-production servers also reside in this building to be used as test servers for the IT department.
- Corporate Headquarters – The headquarters building is a large, 3 story building that contains approximately 600 Employees making up a wide variety of departments within the company. The server breakdown in this building is as follows:
    - 6 Files servers are located in this building to support the diverse user base.
    - 5 Print servers run queue's for 50 printers located through the building, approximately 40 non-color laser printers, 5 color laser printers, and 5 multi-function printers.
    - A single Exchange server resides here to support a majority of users within the building.
    - The Corporate building houses a single Domain Controller for the corporate domain, which is also configured as a Global Catalog server.
- Main Warehouses – There are 2 main warehouses that ship products to all store locations. Each warehouse operates on a 24 hour basis and contains approximately 150 users that logon to the network throughout the day and night. The servers listed are broken down evenly between the 2 warehouses:
    - 2 Domain Controllers are dedicated to the main warehouses to allow users to login and access the file and print server even in the event of a network outage. Both DC's are also Global Catalog servers.
    - 2 File Servers, one in each warehouse, support all shipping/receiving staff 24hrs a day.
    - 2 Print Servers support the warehouses and are used to print shipping labels, packing slips, and normal office documents.
- Employment Office – The employment office is located in a more convenient and public location than the Corporate Offices and contains approximately 50 employees. A Domain controller does not exist in this office, therefore a network outage between this building and the Data Center would impact these users. A low speed redundant connection can be brought up if a persistent network outage occurs The employment office contains the following:
    - 1 File Server – this single file server is used exclusively by the employment office.
- Branch Office – The branch office contains a handful of small departments totaling approximately 100 users. A domain controller was not placed in

this location but a low speed redundant connection can be brought up if a persistent network outage occurs. The server breakdown follows:

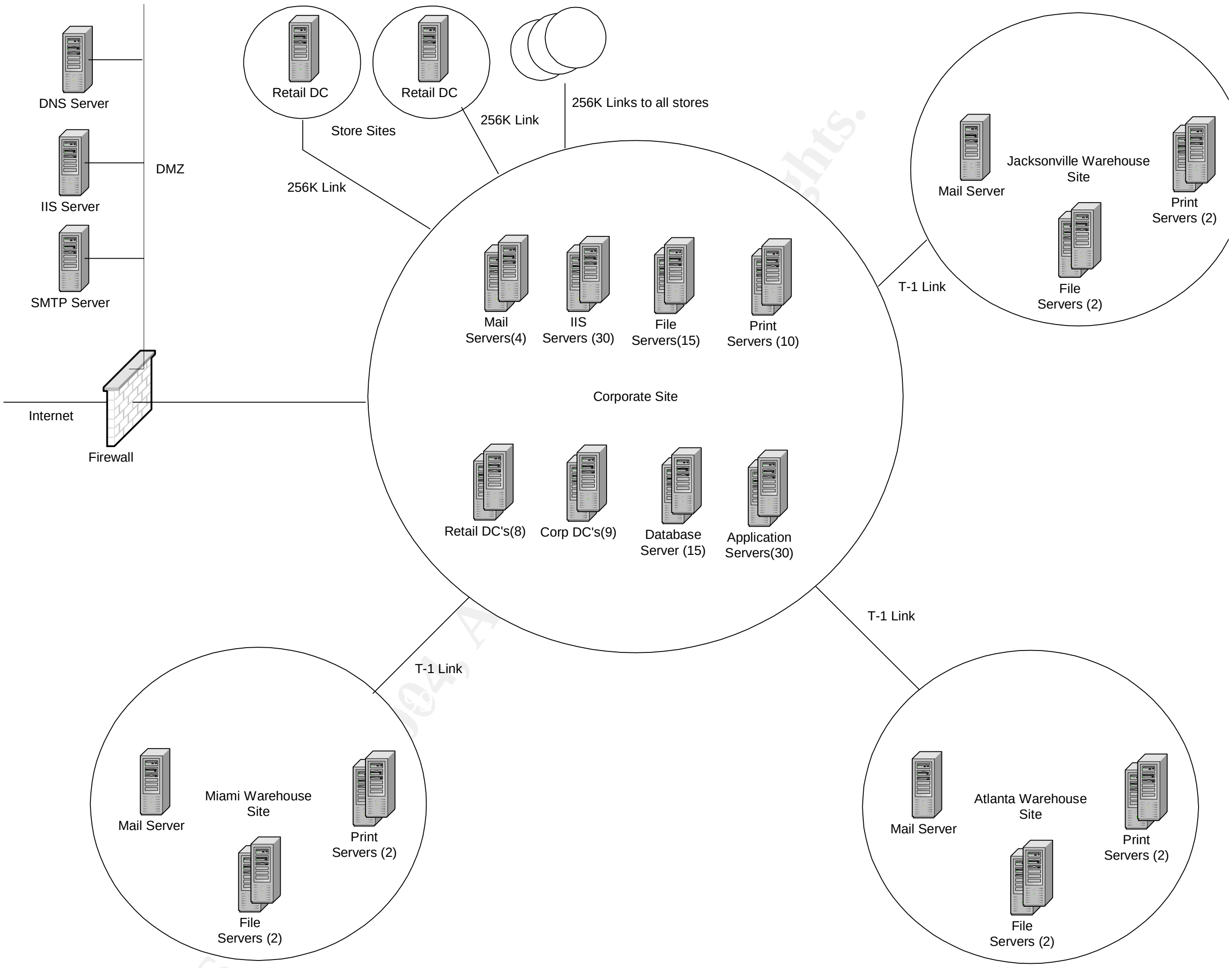
  - 1 File Server – this single file server is used exclusively by the departments located within this branch office building.
  - 1 Print Server – This print server supports 10 non-color laser printers deployed throughout the building.
- Transportation Office – The transportation office is a small office located near the fleet of trucks and maintenance shop owned by GIAC Enterprises. A domain controller does not exist at this 15 person location, and a redundant connection is not available should a network outage occur. The server breakdown follows:
  - 1 File Server – a single file server exists to contain maintenance records, shipping route information, and driver information.

Miami, Jacksonville, Atlanta Warehouse Sites – These warehouses are each single buildings that receive products from vendors and ship products to stores within their region. All warehouses operate in much the same fashion and have the same requirement from an Information Systems standpoint. Each of the three warehouse facilities is connected to the Data Center via a T-1 link, and for network bandwidth concerns, were broken down into their own sites. Each warehouse holds approximately 150 users and each warehouse contains the following servers:

  - 1 Domain Controller – due to the importance the each warehouse continue to function in the event of a network outage or data center loss, a single domain controller is placed in each warehouse.
  - 2 Files Servers – each warehouse contains 2 files servers to contain a variety of shipping/receiving data required to ship product to store locations.
  - 2 Print Servers – 2 print servers in each warehouse supports general office document printing and support printing critical to the operation of the warehouse, including shipping labels, packing slips, delivery schedules, and delivery orders. These items must be able to continue to be printed in the event of a network outage or loss of the central data center.
  - 1 Mail Server – A single mail server in each warehouse permits continued use of email within the warehouse should a network outage occur.

Store Sites – Since each store is connected to the Data Center over a low bandwidth link that would be strained by Windows 2003 intra-site replication traffic, each store will be its own site and will contain a single domain controller. Not only will this configuration improve performance by allowing for the scheduling of inter-site replication, but it also provides high availability for user logins should the network link fail.

Network/Site Diagram



Note: Although now shown in the diagram, each store site contains a single member server as well as a Store Domain Controller.

3 Active Directory Design

The Active Directory Design includes the forest, domain and Organizational Unit layout for GIAC Enterprises. The design is a culmination of several drivers, to include efficiency, administration, support, politics and security. Each component of the design that makes up the infrastructure was influenced by at least one of these factors, but all of them were impacted by considerations for security.

Forest/Domain Structure

Forest Design

GIAC Enterprises does not have any subsidiaries or partnerships that require a security boundary at the forest level. All GIAC Enterprise's domains will have a two way transitive trust between each other. There is also no anticipation for different schema requirements between portions within GIAC Enterprises since all segments of the company utilize common infrastructure applications that would extend the schema (such as Exchange 2003). For reasons of a complete trust, a common schema, and to simplify the administration of the organization, GIAC Enterprises will be made up of a single forest.

Microsoft has introduced something new in Windows 2003 in its Forest Functional Levels. These different levels depend on the Operating System of the Domain Controllers found within the Forest (regardless of domain). The three Forest Functional Levels in Windows 2003 are:

1. Windows 2000 – all DC's in the forest are WindowsNT 4.0, Windows2000, or Windows2003.
2. Windows 2003 Interim – all DC's in the forest are either WindowsNT 4.0 or Windows 2003.
3. Windows Server 2003 – all DC's in the forest are only Windows 2003.

Forest functional levels are configured within the Active Directory Domains and Trusts MMC tool. The forest functional level information can be accessed with a normal account with access to the snap in, but since this is a Forest-wide setting, can only be changed by an Enterprise Admin, or an account that has membership in the Domain Administrators group of the root domain. Once all DC's have been upgraded to Windows 2003, and all domains have been raised to Windows 2003 Domain Functional Level (covered in the next section), the forest functional level of GIAC Enterprises will be raised to Windows Server 2003, which will allow for some improved manageability of the forest above what was not available in Windows 2000. These enhancements include:

- Domain renaming – "In the Windows 2000 version of Active Directory, it was not possible to rename domains without demoting all domain controllers, which effectively destroyed the domain. In Windows Server 2003, domains can be renamed, as long as the forest in which they exist is configured as a Windows Server 2003 forest functional level"[1](DiNicolo, pg.1). Using the RENDOM utility, domains can be renamed without destroying the entire domain.

- Domain repositioning – Windows 2003 will allow the ability to reposition domains within the same forest also using the RENDOM utility. (Detailed information on the RENDOM tool and a link to download it can be found at http://www.microsoft.com/windowsserver2003/downloads/domainrename.mspx)
- Efficient replication – In Windows 2000, when you added a member to a group, the entire group was replicated. Windows 2003 will replicate only the individual user through something called Link Value Replication. In addition, global catalog replication is also less traffic intensive.
- Schema attribute de-activation – In Windows 2000, when the schema was extended with a new attribute, that attribute was a permanent addition and could not be removed in any way. Although Windows 2003 does not completely fix this problem in it still cannot delete unused items, it does improve upon it. While in this functional mode, attributes and classes that will no longer be used can be de-activated if desired.
- Forest Trusts – although this doe not affect GIAC Enterprises today, if an acquisition of another company or a partnership with another company running Windows 2003 did occur, a two way transitive trust could be created between the forests if both are in Windows 2003 forest functional mode.

Domain Design

The main political boundary within GIAC Enterprises is between its store and corporate segments. Each segment has its own, unique chain of management and its own support structure. The store environment, due to its critical nature, is kept very static and all changes made within must be tested rigorously. The corporate segment is much more dynamic and changes to that environment cannot realistically be tested as thoroughly as its store counterpart. To allow each segment to operate as efficiently as possible without affecting the other, each segment will be separated at the domain level. This will offer several advantages to both areas to include:

- Administration – each segment will be able to manage themselves independently and create the necessary OU structure, global and local domain groups, and user accounts as needed for their environment. Splitting at the domain level will also allow each domain to manage its own set of domain and default domain controller policies to its own unique needs and follow a different change management process when making changes to Group Policies.
- Performance – with a multiple domain structure, File System Replication traffic, and therefore, network traffic, is reduced. The overall size of the domain controller database is also reduced.
- Security – Creating multiple domains does create a security boundary between the two segments of the company. Each segment requires the

ability to administer itself in a decentralized fashion. Each will determine its own set of Domain Administrators and Domain and Default Domain Controller Policy can be configured to fit the unique needs of each partition.

GIAC Enterprises will create a total of three domains under their single forest. The first domain will be an empty root domain with only 3 domain/enterprise administrators in it and will be named root.GIAC.com. A dedicated child domain will be created for the store segment called stores.root.GIAC.com and a dedicated child domain called corp.root.GIAC.com will also be created for the corporate segment.

As with its addition of the forest functional levels mentioned above, Microsoft has enhanced its domain functional levels to increase functionality. The former two levels of mixed and native have been expanded to four levels to include:

1. Windows 2000 Mixed – DC 's in the domain include a mixture of Windows NT 4.0, Windows 2000, and Windows 2003.
2. Windows 2000 Native – DC's in the domain are either Windows 2000 or Windows 2003.
3. Windows 2003 Interim – DC in the domain include either Windows NT 4.0 or Windows 2003.
4. Windows Server 2003 – DC's in the domain are exclusively Windows 2003.

Naturally, GIAC Enterprises is striving for all their domains to be placed in Windows Server 2003 mode. Since the domain functional levels can be raised independently of other domains, the root domain will be brought up in Windows Server 2003 domain functional mode. Once the other domains contain nothing but Windows 2003 domain controllers, their levels will be raised to Windows Server 2003 domain functional mode. When both child domains are in Windows Server 2003 functional mode, the forest functional mode will be raised to Windows Server 2003 mode as well. Some advantages that will be gained by being in Windows 2003 domain functional mode include:

- Domain Controller Renaming – To rename a Domain Controller in Windows 2000, it was necessary to DCPromo the system down to a member server, rename it, then DCPromo it as a new domain controller. Windows 2003 will allow the renaming of a DC in place with the NETDOM utility.
- Replicated login timestamp attribute – the last logon time of a user is replicated, which can be helpful when performing auditing and investigating account lockouts.

Organizational Unit Structure

The Organizational Unit structure is designed for the purpose of applying as much security to the servers as possible without interfering with their functionality. Certain key security setting must be applied to all servers regardless of function. These settings are applied at the top level OU. Organizational Units are nested to allow group policy settings to flow down the OU tree and enhance performance, and to simplify administration by keeping most policy settings at the top of the OU tree. A break-down of the OU's per environment follows:

Server Environment – Store

Each store location has a single Domain Controller and a single Windows 2003 server that runs various retail-type applications. Each server type is configured exactly the same, is supported by a single group of employees and requires the same group policy applied. Those same employees also support a set of domain controllers located in a central location (residing in the corporate site).

> **Domain Controllers** – 208 domain controllers (8 in the Data Center and 1 per store) support the stores.root.GIAC.com domain, all DC's are DNS servers and are Global Catalog servers (except the one holding the infrastructure master FSMO role for the store domain).
>
> **Member Server** – Includes all servers at the store locations, one in each store. This OU will have linked a computer policy intended to apply critical security settings and block local access to the server to only a single support group.

Server Environment - Corporate

A diverse array of server types can be found within the GIAC Enterprises network. Although many policy settings will be applied to all servers, each type will require specific settings adjusted to support that servers function. The types of servers within the environment have been identified and grouped as follows:

> **Domain Controller** –12 domain controllers will support the new corp.GIAC.com domain, all of which will be running DNS. 3 of the 12 will be running WINS. All will also be Global Catalogs (except the one holding the infrastructure master FSMO role for the corp domain)
>
> **Member Server** – Includes all servers within the corp domain either within itself or in a sub OU underneath it. This OU will have linked a base policy with critical computer policy settings that must be present on all systems in the domain. This OU will also will have linked numerous user policies to allow support groups various access to all servers in this OU and all sub-OU's

File Server – This OU is for servers specifically set up for file sharing.

Print Server – This OU contains servers specifically set up to run print services. Multiple groups will be given a different degree of access to these servers. Some groups will perform only queue management, while others will have rights to install drivers and software.

Database Server – GIAC has standardized their database platform on Microsoft SQL Server. The environment includes versions SQL 2000 and SQL 7. The database administrators are given access to only these servers within the domain.

IIS Server – Servers running either WWW or FTP services. These servers are locally accessible by only a small support group and the ability of IIS services to run is restricted to only the group of servers in this OU.

Application Server – This OU supports servers that can run a combination of functions and are supported by staff that maintains applications with a client/server architecture.

The Organizational Unit structure for server systems has been constructed with both the server function and support groups requiring access in mind. The following structure in corporate has been established to support this:

Support Environment

For the servers at GIAC Enterprises, certain support groups will require access to all servers, while other groups will require access to only a subset of servers. The following support groups have been identified, accompanied by the access they require.

Store Support – Support the Operating System and all applications on the Domain Controllers and Members servers in the Store domain.

System Engineers – Support the Operating System on all servers in the corporate domain, as well as various third party applications installed on servers. Require full access to all servers.

Account Administrators – Responsible for creation and maintenance of domain/local accounts and groups. Require specific access to all servers within its respective domain. There is one group in the stores domain and one in the corp domain.

Database Administrators – Responsible for database creation and maintenance, and database backup/restore. Require full access only to servers running databases in the Database Server OU.

Application Support – Responsible for client applications, some of which have a server component. Require limited access only to servers running specific applications in the Application Server OU.

Print Support – Responsible for creation of print queues and installation of printer drivers on print servers. Require full access only to print servers in the Print Server OU.

Help Desk - Receive problem calls from users. These users must logon to servers to perform basic troubleshooting and require limited access on all servers. They also will perform print queue management on the Print Servers.

Computer Technicians – Perform hardware maintenance and performance monitoring on servers. Require limited access to all servers.

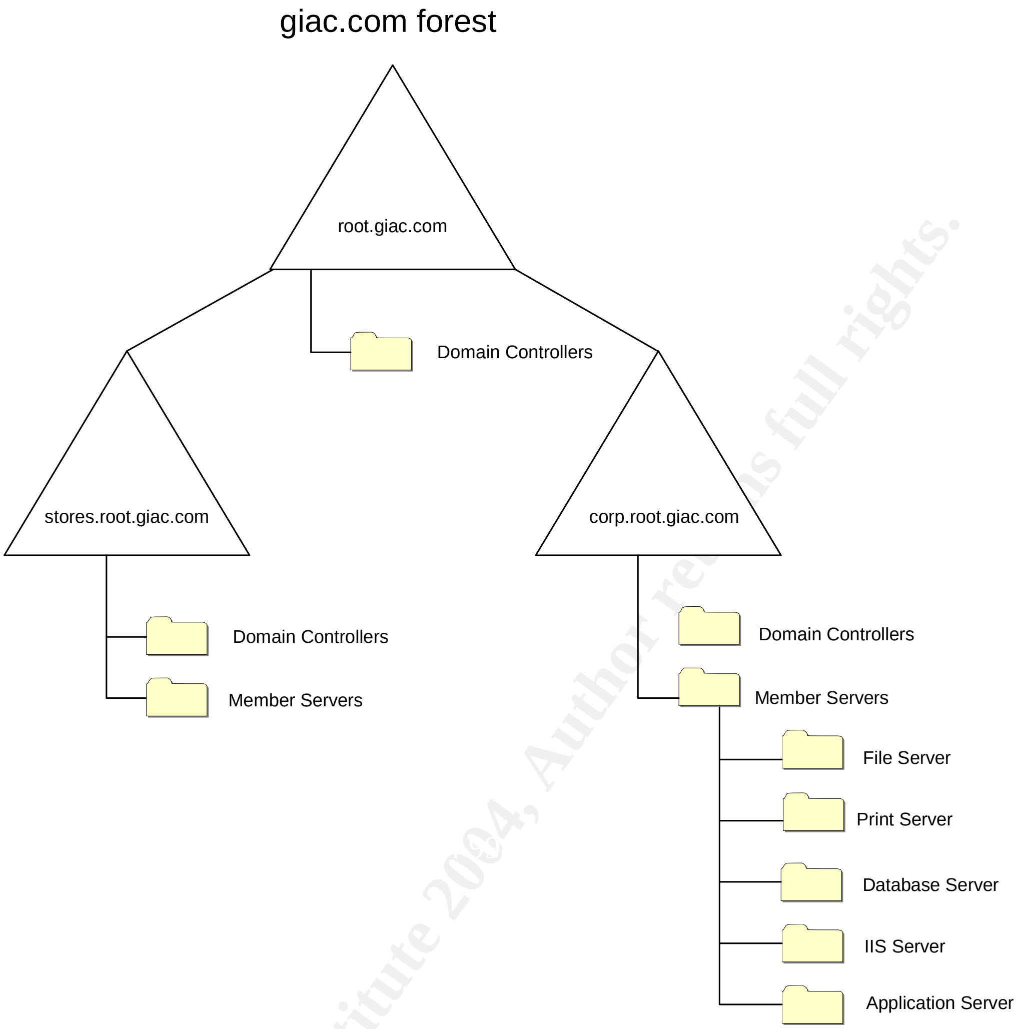
IIS Engineers – Support web applications and services. Require full access to only IIS Servers within the IIS Server OU.

To be able to refer to these users within the Policies and to apply access permission to the policies, these users will be placed into Global Groups using the names above.

Service Accounts

In addition to the accounts identified above that need direct access to servers, several service accounts have been identified within the environment that are in the Domain Admins group that need to retain their status as Domain Admins. The username and password need to be known by the members of the Server Engineers group for the configuration of software requiring these accounts with a high level of access. These accounts have frequently been misused by employees to log directly into servers for support reasons instead of using their regular user accounts. Using these common accounts for support effectively invalidates any auditing performed on servers and therefore, it is the desire of GIAC Enterprises to force support staff away from using these service accounts to log directly into servers.

Active Directory Diagram



4 Group Policy Objects – Base Policy

The Default Domain policies for all the domains in the forest are the same and are limited to Account policy settings. Microsoft recommends not changing the Kerberos Policy settings in the Account Policy section of the Default Domain policy and since there were no specific requirements for GIAC Enterprises to do so, these setting were left as 'Not Defined'. Other settings were made as follows:

Default Domain Policy – All domains

Password Policy

Enforce Password history – Set to 24. This policy prevents users from reusing previously used passwords. The setting in this policy will require the user make a new password 24 times before using a password once again.
Maximum Password Age – Set to 30. Users will be required to change their password every 30 days.
Minimum Password Age – Set to 29. The password set cannot be changed again for 29 days. The recommended setting for this is one day less than the maximum password age setting. The basis of this recommendation is that it "ensures that intruder will be noticed if he changes the password as he will lock out the real user and then the password will not be able to be changed by the user exposing the intruder"[2](Magalhaes, pg. 1). In addition to this benefit, GIAC Enterprises will prevent users from finding out the password history and cycling through a number of passwords all at once only to return to their original password, effectively defeating the password history setting.
Passwords must meet complexity requirements – Enabled. This policy will require that when a password is first set, or changed to a new one that complexity requirements are met. The complexity of the password ensures it is a minimum of 8 characters long and includes 3 of the following:

- Uppercase letters
- Lowercase letters
- Numeric and non-alphanumeric characters.

The password also cannot contain the account name or the user's name.

Account Lockout Policy

Account lockout duration – Set to 1 week, which means when an account is locked out it will not automatically unlock itself for 1 week. Under most circumstances it is expected that the help desk will need to get involved whenever an account is locked out. GIAC Enterprises views the additional help desk expense as worth the increase in security this setting yields.

Account lockout threshold – Set to 3, which will lock an account after 3 failed attempts.

Reset account lockout counter after – set to 120 minutes. This will reset the account lockout threshold counter after 2 hours. Without the reset, the counter will increment to 3 over a long period of time and eventually lock out a legitimate user.

Default Domain Controller Policies

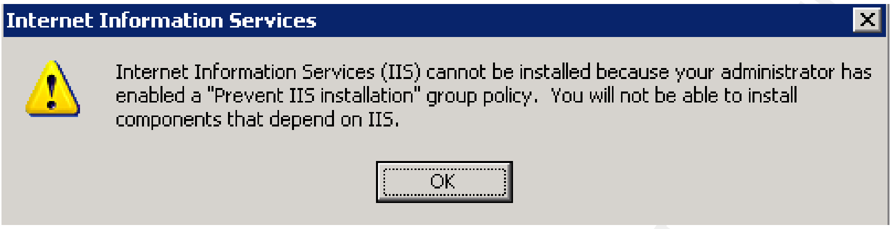
It is the goal of GIAC Enterprises to limit direct access to domain controllers as much as possible in both store and corporate segments of the network. In the store environment, the employees in the Store Support group will need full access to install, upgrade and troubleshoot the domain controllers. In the Corporate environment, only the employees in the Systems Engineers group will be able to gain access to the Domain Controllers. To raise the level of protection on the Domain Controllers above that of normal servers, Help Desk or Computer Technicians will not have any ability to access the domain controllers directly; all support will be performed by only the Store Support and System Engineers groups.

Restricted Groups

To ensure only those groups will have administrative access to the DC's, the group membership of the Administrators group will be dictated by the Group Policy Setting - Computer Configuration, Windows Settings, Restricted Groups. The Administrators group will be populated using this setting on store DC's with only the Store Support global group and on corp DC's with only the System Engineers global group. Should a non-administrative user be added to the Administrators group either deliberately or by accident, they will be removed the next time the group policy settings are refreshed (default is 90 minutes). In conjunction with the restricted group, GIAC wants to ensure only those users defined in the restricted groups can log on to the Domain Controllers. The default setting for the right to log on locally is Administrators, Account Operators, Backup Operators, Print Operators, and Server Operators. This right will be restricted using the setting 'Computer Configuration\Windows Settings\Local Policies\Security Settings\User Rights Assignment\Allow Logon Locally', which will be set to only Administrators.

IIS Restrictions

Because of the vulnerabilities inherent with web services in general, it is essential that GIAC Enterprises keep these services from running on the Domain Controllers within the domain. To ensure the DC's in both domains are not running IIS, multiple settings will be made in the Default Domain Controller policy. The first setting to be made is new in Windows 2003 and will prevent the installation of IIS altogether on all DC's. The setting is found in Administrative Templates\Windows Components\Internet Information Services\Prevent IIS installation and will be set to Enabled. With this setting in place, whenever an attempt is made to install IIS, the users will receive the following message:



Internet Information Services

Internet Information Services (IIS) cannot be installed because your administrator has enabled a "Prevent IIS installation" group policy. You will not be able to install components that depend on IIS.

The next settings will be to disable the World Wide Web Publishing Service, as well as the IIS Admin Service and the FTP Publishing service. If a server with IIS was installed and later promoted to a Domain Controller, the first setting made above would not impact the already installed components and that Domain Controller would be open to IIS attacks. The best scenario is to not have IIS components installed at all, but with these settings in place the worse case is the components will be on the system but not usable over standard IIS ports.

System Services

Following security best practices, any Windows services not required specifically by the organization will be disabled by default. In Windows 2003, Microsoft has set the default for many services, such as Alerter and Telnet to be disabled by default. Some other services found not to be required by GIAC Enterprises will be disabled as well through the Default Domain Controller Policy to include: Indexing, Portable Media Serial Number, Remote Access Auto Connection Manager, Remote Access Connection Manager, Remote Desktop Help Session Manager, Removable Storage, Telephony, Windows Audio, and Wireless Configuration. Microsoft has improved its security in the Services area with Windows 2003 by allowing a smaller number to run under the local system account. "Almost all services used this account in Windows 2000. Programs that run in this context have unlimited privileges on the local computer, which presents an obvious security risk."[3] (Shinder, pg. 1) Although some services still use Local System in Windows 2003, many common ones use the Local Service or Network Service account, which has a much lower level of privileges.

User Rights Assignment

Due to Kerberos's heavy reliance on a reliable system time, it is very important that all the Domain Controllers have the correct time that is completely synchronized across the entire domain. "A domain controller configured with a system time that is out of synch with the system time on other domain controllers in the environment could interfere with the operation of domain services. Allowing only administrators to modify system time minimizes the possibility of a domain controller being configured with an incorrect system time."[4]. (A general overview of Kerberos can be found at http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/security/kerberos.mspx). The default setting allows Administrator and Server Operators to change the system time. Using the setting 'Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time', a restriction will be made to just Administrators.

Security Options

In an increased focus on security, Microsoft has set new default levels within their security options in group policy. Some of these settings will have a direct impact on down-level clients and 3rd party applications that are assuming a more open level of communications will be available with the Domain Controllers. One such example of this in Windows 2003 is the setting 'Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)'. This setting is enabled on DC's by default and disabled on member servers. Any third party application authenticating users against the domain may have problems if it cannot sign the connection. Another setting, 'Computer Configuration\Windows Settings\Local Policies\Security Settings\Security Options\Microsoft network server: Digitally sign communications (if client agrees)' is also enabled by default on DC's and disabled on member servers. To allow 3rd party application to continue to work, it may be necessary to disable the 'always' setting. Making this change will cause communication to be signed if it's possible but not require it. Making a change such this as will lower security to some degree but may be necessary as a temporary measure to keep older applications working until they can be upgraded to be more compatible with the Windows 2003 out of the box configurations.

One security option Microsoft did not enable on DC's by default but GIAC Enterprises will, is the setting 'Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Do not store LAN Manager hash value on next password change'. When accounts are created, a LAN Manager hashed version of the password will be created and unfortunately, this cannot be changed. But with this setting in place, all new passwords changes will not generate this hashed version of the password so as long as accounts are created with the option to "change password on next login" a usable LAN Manager hashed version of the password will only be available for a short period of time. The implication of enabling this setting is minimal. It will affect the ability of Windows95 clients to change passwords, and will affect older DOS-based network boot disks that may be relied upon by applications such as Norton's Ghost. There is no workaround to get Windows95 clients to be able to change their own passwords, but the network boot disk problem can be eliminated by using a Windows PE boot CD, which has no problem with this setting. These are the only legacy applications being effected at GIAC.

Audit Policy

Audit Policy provides a limited version of an Intrusion Detection System on servers that can be used as a basis for evidence should it be needed in a legal forum. By default, Windows 2000 sets all audit events to 'No Auditing', which is improved upon in Windows 2003 which sets a minimum level of auditing by default. The following table lists the auditing events available, the defaults put in place in Windows 2003, and the alterations made by GIAC Enterprises based on the recommendations in the "Microsoft Windows 2003 Security Guide, Chapter 3"[5].

Setting	Default	GIAC Setting
Audit account logon events	Success	Success Failure
Audit account management	Success	Success Failure
Audit directory service access	Success	Success Failure
Audit logon events	Success	Success Failure
Audit object access	No Auditing	Success Failure
Audit policy change	Success	Success
Audit privilege use	No Auditing	Success
Audit process tracking	No Auditing	No Auditing
Audit system events	Success	Success

Most settings above were changed from success to both success and failure to allow GIAC administrators to determine unauthorized attempts into the domain. The Windows 2003 Security Guide is sensitive to the fact that over-auditing will bloat the logs with uninteresting data, therefore their High Security recommended settings were used with the expectation it will provide a large amount of relevant data.

5 Group Policy Objects – Additional Group Policy

The goal of the group policies within GIAC is not only to restrict access to the servers as much as possible, but also to reduce the attack surface that is presented to hackers. This is done by disabling unused services, restricting user rights, and enabling new security features found in Windows 2003 - all done within the computer configuration section of the GPO. The caveat of implementing every feature possible is it will likely break legacy applications and hinder older clients from communicating with servers or participating in the domain. For GIAC, all servers will be upgraded to Windows2003 and all clients to Windows XP but the settings made in their policies must still be sensitive to down-level clients to ensure functionality is not lost during migration. Microsoft has provided some help with anticipating which settings may cause problems with legacy systems in their "Windows2003 Security Gudie"[6]. This guide provides recommendations on policy settings within 3 types of environments; Legacy, Enterprise Client, and High Security. The guide is also organized to provide hardening of server by function (File, Print, IIS, etc.) which proves helpful. From an informational standpoint, the Windows 2003 Security Guide offers an excellent explanation of the settings, but is best coupled with the "Threats and Countermeasures Guide"[7], which is also a product of the Microsoft Solutions for Security Group. This document will fully describe the vulnerabilities and impact associated with each setting, and provides a recommendation in the form of a countermeasure. This document also covers the Administrative Templates section of the Computer Policy (which the Windows 2003 Security Guide does not). Some of the key settings found in these guides (with an emphasis on new items introduced in Windows 2003), applied at the Member Server OU are detailed in this section.

Group Policy Management Console (GPMC)

In conjunction with Windows 2003, Microsoft released a Group Policy Management tool to replace the original Group Policy Editor originally integrated with Windows 2000. The GPMC introduced some significant enhancements over the original tool and in addition to its ease of use, its abilities include:

- Backup and Restore group policy objects
- Import/export and copy/paste of GPO's.
- Application of WMI filters.
- Perform reporting on GPO settings and Resultant Set of Policy Data.

As of the date of this writing, the GPMC with Service Pack 1 can be obtained from http://www.microsoft.com/downloads/details.aspx?FamilyId=C355B04F-50CE-42C7-A401-30BE1EF647EA&displaylang=en

Once installed, the GMPC will actually replace the original Policy Editor tool and will launch either directly from the Start menu or when clicking the Edit Policy button when in the properties or an OU.

User Rights Assignment

The first level of login restriction to servers will be within the User Right 'Log on Locally'. This setting is found at 'Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment, Allow logon locally'. The first server policy to be created, called Member Server, will have this setting configured with Administrators, Account Admins, Help Desk, and Computer Technicians – all those groups (other than administrators) needing some limited access to servers. Servers within sub OU's needing additional users to access them, such as the Database Servers OU, will have policies created and linked to them with additional groups assigned the logon locally right. In the Database Servers policy, it will be the Database Administrators. The ability of some users only having access to some servers was one of the drivers of the OU design described earlier.

User Interface – Desktop

Across 2 domains and many different server types, GIAC Enterprises has a large number of support personnel that need to log into servers and manipulate them with a varying degree of privileges. To reduce the requirement to maintain multiple accounts and remember multiple passwords, GIAC would prefer to allow server support employees to use a single account to access their own workstation and resources as a normal user and to log onto and manipulate servers. The challenge presented in using a single account is the rights and desktop settings these employees have on their workstation is not the same that they would have on the servers they login to. It is the desire of GIAC to leave the user's desktop fairly open while at the same time, restricting the server interface as much as possible. This will be accomplished using the Loopback Processing GPO setting on the member server OU and applying user policies directly on the server OU and the sub OU's. This, in combination with access control lists, will allow workstation and server policies to be created and maintained independently. In a nutshell, this setting will force user policies that are applied on the Server OU's rather than those on a User OU found somewhere else in the domain. This will ensure that servers are locked down appropriately without interfering with support personnel's ability to maintain user workstations within the domain or use their own system.

Loop Back Processing Setting

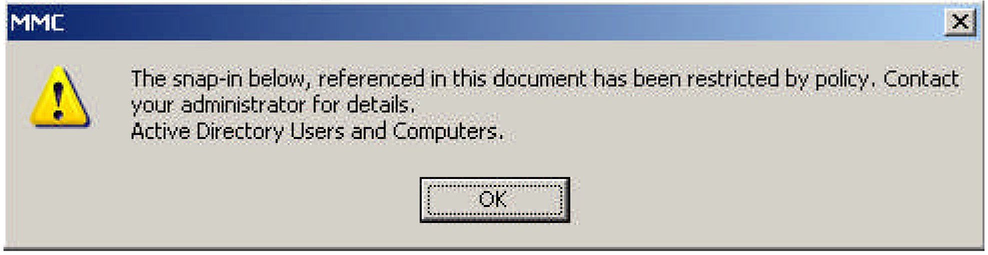
When a user logs on to a system, the User policy settings that are applied are those that are linked to the OU that the users account resides in. User

Configuration settings configured to OU's only containing computers are generally not applied.
The Loopback Processing setting (found at Computer Configuration, Administrative Templates, System, Group Policy, User Group Policy loopback processing mode), will force the application of User Configuration settings in GPO's linked to computer OU's regardless of the location of the Users account..

There are 2 modes of LoopBack processing when it is enabled, Merge mode and Replace mode. Merge mode will apply the User Configuration settings configured on both the users OU and the computers OU and if there is a conflict, the policy tied to the computer OU will override. Replace mode will apply only the User policy setting linked to the computers OU and will ignore the settings linked to the Users OU. GIAC's desire is to only apply user policies linked directly to server OU's, so the Replace setting will be used. A Policy will be created called Member Servers and will be linked to the Member Servers OU. In addition to policy settings found to improve security (as recommended in the "Windows2003 Security Gudie"[6] , the "Threats and Countermeasures Guide"[7]), the loopback processing setting will be made in this policy.

User Policy

With Loopback Processing set, Additional policies are then added with user settings specific to the type of user logging into the server. For example, a User Policy (the Computer configuration section of the policy is disabled) will be created called Help Desk. GIAC will restrict the help desk to only a few MMC snap-ins by Enabling the setting 'User Configuration, Administrative Templates, Windows Components Microsoft Management Console, Restrict users to the explicitly permitted list of snap-ins'. When enabling this, users who have this policy applied will only be able to access snap-ins set to enabled under 'User Configuration, Administrative Templates, Windows Components Microsoft Management Console, Restricted/Permitted snap-ins'. Attempting to add a restricted snap-in or access it through an administrative program will result in an error similar to the following:

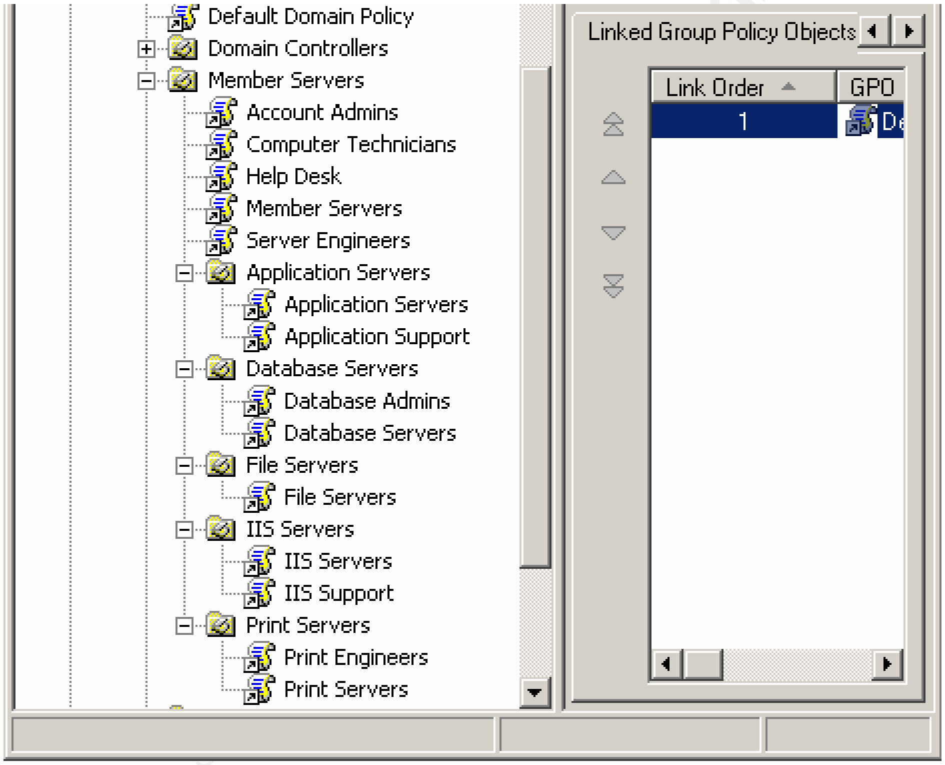


The snap-in below, referenced in this document has been restricted by policy. Contact your administrator for details.
Active Directory Users and Computers.

Several other settings will be made in the User Configuration section to limit the desktop of the help desk users. Other policies will be configured and linked to the Member Server OU to tailor access of those other groups that access all servers in the environment. User policies will also be created and linked to sub-OU's for support staff logging into servers in specific OU's (ie. a Database Administrators User policy linked to the Database Server OU). To ensure a user does not get the wrong policy, the policies will be filtered using Access Control lists so only the users global group will have the Apply Group Policy right on the policy ACL.

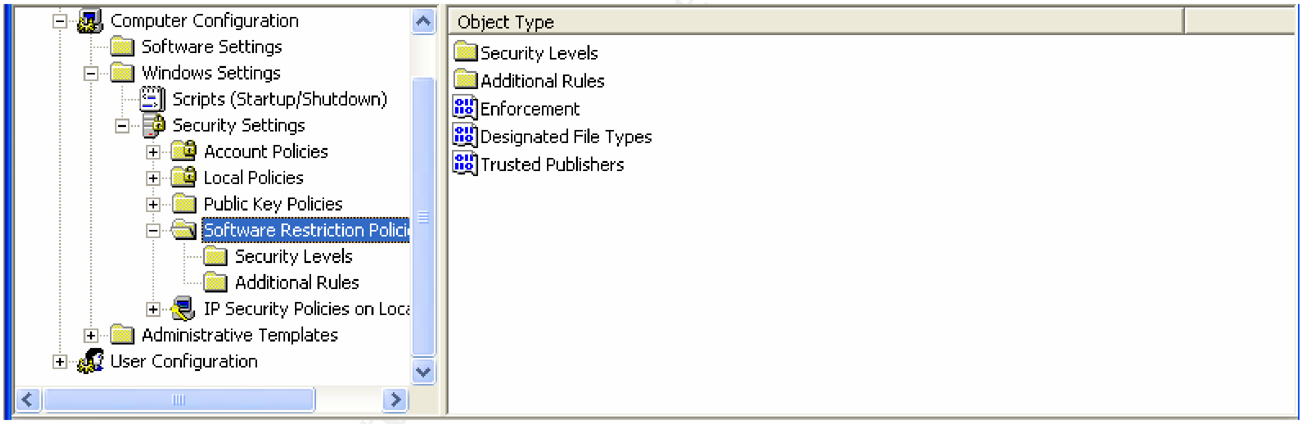
It is here that the service account problem mentioned in section 3 will be dealt with. Although the service accounts need elevated rights on servers and at times across the domain, these accounts do not need access to most components on the desktop. To discourage staff from logging in with these accounts, a user policy will be created and linked to the Member Server OU and filtered using ACL's to apply to only the service accounts. This policy will restrict as many things as possible on the desktop and will essentially leave it in a state where only the logoff button is available.

An example of the common policies and the OU's as they are linked to within the corp domain follows:



Software Restrictions Policy

A new item in Windows2003 within Group Policy is the ability to place restrictions on specific software to prevent it from running. Since the server systems are subject to a wide range of direct user access, GIAC would like to place some restrictions on what is allowed to run on the servers within the corp domain. The software restriction setting can be found in the Computer section of the group policy under Computer Configuration, Windows Settings, Security Settings, Software Restriction Policies. To apply restrictions to all servers in the corp domain, GIAC will create a new software restriction policy in the Member Server group policy which is linked to the Member Server OU. When you right click on the Software Restriction Policies item and create a new policy, a number of configuration items will become available. By default, the software restriction policy will apply to all users, including Administrators. This can be changed in the Enforcement properties to exclude administrators, but GIAC will keep the default setting to ensure the restrictions are always in place. Also by default, the security level is set to Unrestricted, which will allow all software from running except what is specified in the Additional Rules section of the policy. The alternative is to set the security level to Disallowed, which will restrict all software unless purposely allowed to run under the Additional Rules section. To avoid a state of complexity, GIAC will keep the default setting of Unrestricted and focus on restricting specific areas of concern. The following policies will be put into place based on methods supplied by Microsoft in their article "Using Software Restriction Policies to Protect Against Unauthorized Software" [8]. The following screenshot shows an example of what the Software Restriction Policies look like.



Installing software from web sites

The first area of concern is installing software made available through internet sites. Some internal web sites have been developed to easily load software that is standard across all systems, so allowing software to install from internal sites is required, but installing from internet sites should be prohibited. This restriction can be made by right clicking on the Additional Rules Item and selecting New Internet Zone Rule. Within the properties of the new rule, Internet zone will be selected from the Internet zone dropdown box, and the Security level will be set to Disallowed.

Email software

To limit the exposure of servers to email based worms and Trojans and any other security vulnerabilities found within those products, GIAC will restrict the use of Outlook and Outlook Express on servers. Since Outlook Express is installed as a default component with Windows, its path is predictable and it needs to be restricted regardless of version (which may change due to service pack upgrades or other updates to the OS) a New Path Rule will be added to the additional rules where the path is C:\Program Files\Outlook Express\msimn.exe and the Security Level set to disallowed. Outlook can be installed off a network share which is accessible to all employees, so a support staff member could choose to install it anywhere on a server. Since the version of Outlook available on the network is known and does not change often, a New Hash rule will be created to restrict Outlook from running if installed (since Outlook is part of the MS Office install package, and some components from office do need to be installed on servers, a policy could not be created to prevent the installation of Outlook entirely). In the Hash Rule properties box, the File hash value can be gotten by browsing to the Outlook executable, then the security level will be set to Disallowed.

Remote Access

GIAC wishes to control remote access to servers as much as possible and prevent unauthorized remote sharing of server resources and desktop access. To support this, software restrictions will be used to prevent running the NetMeeting application. The file C:\Program Files\Netmeeting\conf.exe will be restricted using a Path Rule as done with Outlook Express.

WMI filtering

> In Windows 2003, you can use WMI Filters in addition to group filtering. WMI filters contain the WQL based queries, which are evaluated dynamically at the computer startup or user logon, and depending on their outcome, allow or disallow the GPO settings to be applied. As you can imagine, the number of possible conditions is huge, since you can test values of any property available via WMI.(Policht, pg. 2)

As critical patches are released for IIS, GIAC Enterprises would like to use WMI filtering to ensure that patch is applied before the WWW service is started. To do this, a WMI filter could be placed on the policy linked to the IIS Server OU. Then the WWW service would only be allowed to start if the IIS server was in that organizational unit AND had the critical patch installed since the policy would only be applied if the filter query resulted as true. A WMI filter that could detect if patch Q12345 was installed would look like:

```
Root\CimV2; SELECT * FROM Win32_QuickFixEngineering  WHERE Hotfix ID =
"Q12345"
```

In an effort to reduce the risk of a virus from installing on a File Server, A policy for the File Server OU could be added and set to run first in the link order that would Disable the Server service. A second policy could be linked to the same OU that enables the Server service based on a WMI filter that tests for the presence of antivirus software. Such a filter would look like this:

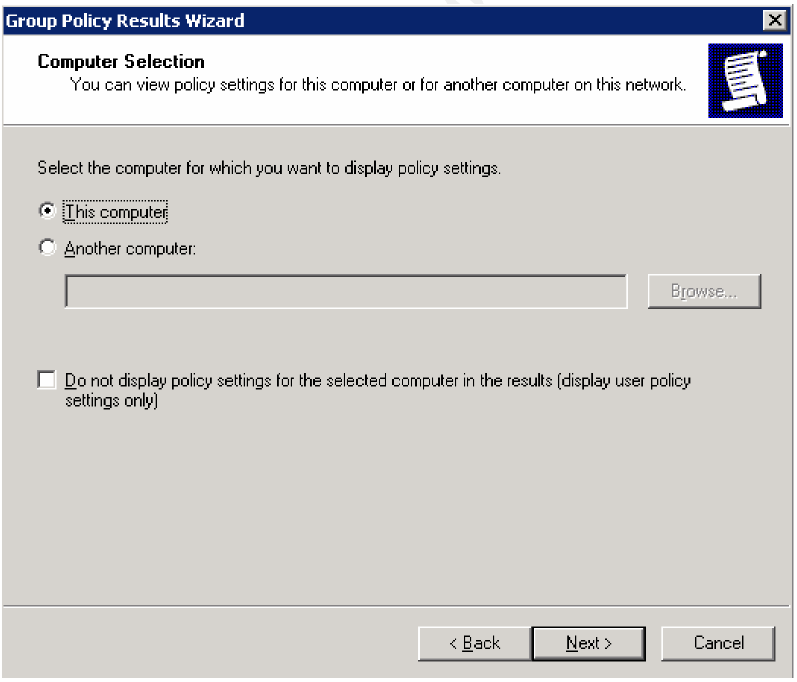
```
Root\CimV2; SELECT * FROM Win32_SoftwareElement  WHERE Name =
"Norton_Antivirus"
```

Note: It is important to ensure that all systems in the OU (and sub OU's) the policy is applied to only contain Windows 2003 servers. On Windows 2000 based computers, the WMI filter is ignored and the policy is always applied. In this case, the server service would be disabled on any Windows 2000 system even if they were running the proper version of the AV software.

Microsoft has provided some help with creating WMI filters with its WMI Administrative tools, including CIM Studio and Object Browser Tools. These tools will allow the viewing and editing of classes and properties and is a good source of documentation for creating WMI filters. These tools can be downloaded at http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6430F853-1120-48DB-8CC5-F2ABDC3ED314.

Resultant Set of Policy

A final improvement worthy of mention in Windows 2003 group policy is the Resultant Set of Policy tool which will allow you to verify policy settings based on a specific computer, user, or both. This MMC snap-in will run in 2 modes, logging and planning. Logging mode shows the actual setting while planning mode allows you to "perform what-if analysis as though the user had actually logged onto the server...to test GPO combinations before actually deploying them." (Fossen, pg.80).This tool can also be used within the GPMC by Right clicking Group Policy Results, and selecting the Group Policy Wizard. The wizard will ask you to select the computer you're running the tool on, browse to another machine to test, or not to display computer settings (if only interested in user settings).


Group Policy Results Wizard

Computer Selection

You can view policy settings for this computer or for another computer on this network.

Select the computer for which you want to display policy settings.

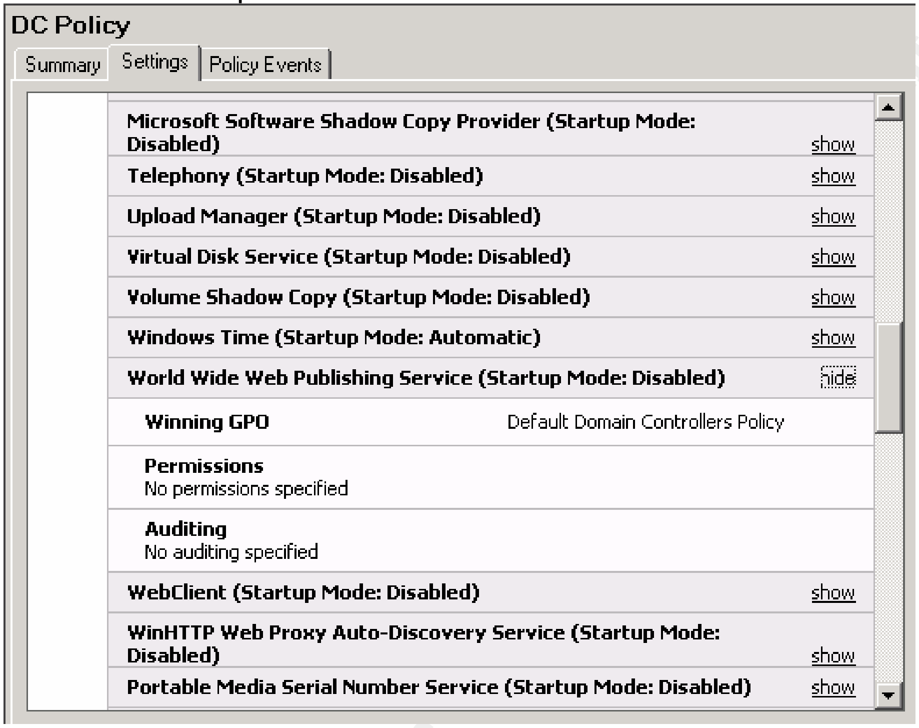
● This computer

○ Another computer:

□ Do not display policy settings for the selected computer in the results (display user policy settings only)

On the next screen you can choose the current user, select one in the domain, or not show any user settings if only interested in the computer configuration. The results of the query will be displayed in the right pane of the GPMC in an html format that will even display which policy applied each setting. This will help determine where a setting is coming from when a set of complex policies are being linked and used.

Here is an example of the results.



DC Policy

Microsoft Software Shadow Copy Provider (Startup Mode: Disabled)	show
Telephony (Startup Mode: Disabled)	show
Upload Manager (Startup Mode: Disabled)	show
Virtual Disk Service (Startup Mode: Disabled)	show
Volume Shadow Copy (Startup Mode: Disabled)	show
Windows Time (Startup Mode: Automatic)	show
World Wide Web Publishing Service (Startup Mode: Disabled)	hide
Winning GPO	Default Domain Controllers Policy
Permissions No permissions specified	
Auditing No auditing specified	
WebClient (Startup Mode: Disabled)	show
WinHTTP Web Proxy Auto-Discovery Service (Startup Mode: Disabled)	show
Portable Media Serial Number Service (Startup Mode: Disabled)	show

The Query can be refreshed to verify policy changes by right clicking on the results report that gets created under the Group Policy Results container and selecting Rerun Query.

Although RSOP is not a group policy effecting security itself, it is a valuable tool that will provide effective troubleshooting assistance as well as a platform for pre-deployment testing. Such a tool encourages the use of Group Policies and their application granularly which will amount to a raised level of security.

Additional Security

DMZ Systems

So far, GIAC has been able to apply a variety of Group Policy settings to all the systems that are part of each of its three domains, which excludes those systems not joined to the domain and perhaps its most vulnerable systems – those located on their DMZ. As described in section 2 (Network Design) there are 3 publicly accessible servers on the DMZ to include a DNS server, SMTP server, and an IIS 6.0 server, all of which run Windows 2003. Since these servers are all stand alone systems, Group Policy cannot be deployed to them at all.

The first level of defense for these systems against malicious attack will be the firewall, which will only allow in-bound traffic into the DMZ over ports 80, 443, 25, and 53 to support the http, https, smtp, and dns protocols to their respective servers. In addition to this, IP filtering will be configured on all 3 servers so they will only listen on those ports needed for them to perform their function. This will protect them from each other in the event one is compromised and used to attack another over any chosen port. This will not impact the ability to support and maintain these systems since administrator access to these servers is out of band via a HP Remote Insight Board (RIB).

Above the firewall and IP filtering, many settings can be configured to 'harden' the servers against attack. Best security practices include disabling all unused services, uninstalling unneeded components, keeping updated with the latest patches and setting and reviewing strong audit logs. Although Group Policies created within the domain cannot be deployed to these servers, many of the settings found in group policy are available through security templates. Each system will be hardened specifically tailored to its function, but there are a common set of important setting that will be detailed here that will be applied to all systems from a standard DMZ security template. These setting are important because they help prevent some sources of footprinting that hackers seek when they are in the reconnaissance phase of targeting your systems. These settings as recommended in the text "Hacking Exposed, Windows 2003"[11] include:

Setting	**Configuration**
Network Access:Allow anonymouse SID/Name translation	Disabled
Network Access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network Access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network Access: Let Everyone permissions apply to anonymous users	Disabled
Network Access: Named Pipes that can be accessed anonymously	Empty
Network Access: Remotely accessible Registry paths and subpaths	Empty
Network Access: Restrict anonymous access to named pipes and shared	Enabled

These, plus other settings as recommended in the "Windows 2003 Security Guide"[6] will be applied through a single common security template. Of note are a large security audit log, account policies, and a renamed Administrator account. With SID/Name translation off it will be more difficult for a hacker to identify the true admin account and the rename should limit brute force password guessing on that account. A copy of all the settings made with the template has been included in Appendix B for review.

Finally, a .vbs script will be run on the servers in the DMZ to make some adjustments to the TCP/IP parameters that cannot be made through the security templates. These adjustments will help defend against SYN floods and other denial of service attacks that may impact the system as described in "Hacking Exposed Windows 2003 Server"[12]. The script used to apply these setting has been included in Appendix C.

Patch Deployment

A final area of security in addition to group policy settings/security templates that is critical to GIAC enterprises is patch management. GIAC desires a high level of control over which patches are deployed to their production systems and attempts to ensure a patch will not affect the OS or applications by performing thorough testing before deployment. To best support this, the Automatic Update service will not be enabled on the Windows2003 Servers in the enterprise. Recent developments made by Microsoft allow the downloading of patches from their web site to a local deployment server, which can then be granularly deployed to servers at a time of GIAC's choosing. This will allow sufficient testing to take place before a patch or set of patches are deployed in an automatic fashion. Microsoft's Software Update Service (SUS) and new Windows Update Services (WUS) provide exactly this ability, as does an add on component for SMS 2.0, the Software Update Services Feature Pack. SUS/WUS and documentation can be downloaded from the Microsoft site at http://www.microsoft.com/windowsserversystem/sus/default.mspx. GIAC will deploy SUS and develop a testing and deployment strategy to keep their systems as up to date as possible with new security patches released by Microsoft.

Summary

It was the effort of this paper to introduce an Active Directory Design and application of Group Policies that could effectively lock down a Windows 2003 server environment given a heterogeneous set of support staff. Using previous Windows 2000 settings along with new Windows 2003 settings, it was demonstrated that a wide variety of users with a varying degree of responsibility can be given granular access to perform their jobs without giving them much more than standard User access on a server, or even a separate account. Windows 2003 yields several significant improvements over Windows 2000 from a directory, policy, and administrative standpoint. The key advancements were highlighted within each area of the paper, all improving upon the ability to tailor the security of Windows 2003 to fit into a large and dynamic environment.

List of References

1. DiNicolo, Dan - "New Active Directory Features in Windows 2003, Part 1", - ServerWatch, 2003.
URL: http://www.serverwatch.com/tutorials/article.php/2213281

2. Magalhaes, Ricky – "Using passwords as a defense mechanism to improve Windows security (Part 2)" – Windows Security.com, 2003.
URL: http://www.windowsecurity.com/articles/Passwords_Improve_Windows_Security_Part2.html

3. Shinder, Debra – "Changes to Default Settings Make Windows Server 2003 More Secure (Part 2)" – Windows Security.com, 2003.
URL: http://www.windowsecurity.com/articles/Settings_Windows_Server_2003_Secure_Part2.html

4 "Windows 2003 Security Guide", April 23rd, 2003. Chapter 4.
URL: http://www.microsoft.com/technet/Security/prodtech/win2003/w2003hg/sgch04.mspx#top

5 "Windows 2003 Security Guide", April 23rd, 2003. Chapter 3.
URL: http://www.microsoft.com/technet/Security/prodtech/win2003/w2003hg/sgch03.mspx

6. Dillard, Maldonado, Warrender - "Windows2003 Security Gudie" - Microsoft Corporation, April 23rd, 2003
URL: http://go.microsoft.com/fwlink/?LinkId=14845

7. Dillard, Kurt – "Threats and Countermeasures: Security Settings in Windows 2003 and WindowsXP" – Microsoft Corporation, 2003.
URL: http://go.microsoft.com/fwlink/?LinkId=15159

8. "Using Software Restriction Policies to Protect Against Unauthorized Software", January 1st, 2002.
URL: http://www.microsoft.com/windowsxp/pro/techinfo/articleindex.asp

9. Policht, Marcin - "Examining Windows 2003 Group Policy Enhancements, Part II", - ServerWatch, 2003.
URL: http://www.serverwatch.com/tutorials/article.php/10825_2205741_1

10. Fossen, Jason – "Windows2000/XP/2003 Group Policy and DNS" – SANS Institute, 2004

11. Scambray, Joel, and McClure, Stuart, Hacking Exposed Windows Server 2003, New York, McGraw Hill/Osborne Publishing, 2003. pg 100.

12. Scambray, Joel, and McClure, Stuart, Hacking Exposed Windows Server 2003, New York, McGraw Hill/Osborne Publishing, 2003. pg 427-439.

Appendix A

Windows 2003 Group Policy Additional Settings (Setting documented in these tables were taken from the ServerWatch article "Examining Windows Server 2003 Group Policy Enhancements")[9]

Computer Configuration

Setting	Benefit
Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies	Control security (e.g. authentication and encryption methods used in wireless networks),
Windows Settings\Security Settings\Software Restriction Policies	Prevent or allow applications to be run on target computers, based on a number of configurable criteria, such as file paths, hashes, certificates, Internet zones they originated from, or registry keys they use. This can be extremely useful in preventing virus infections and unauthorized software use.
Administrative Templates\Windows Components\Application Compatibility	Determine the ability to run applications that were designed for legacy operating systems (including preventing access to all 16-bit applications),
Administrative Templates\Windows Components\Internet Information Services	Control the ability to install IIS
Administrative Templates\Windows Components\Terminal Services	Provide the ability to control practically every single aspect of Terminal Services functionality,
Administrative Templates\Windows Components\Windows Messenger	Prevent or allow the use and automatic launch at startup of Windows Messenger
Administrative Templates\Windows Components\Windows Media Digital Rights Management	Control Digital Rights Management Internet Access
Administrative Templates\Windows Components\Windows Media Player	Affect several aspects of Windows Media Player operations, such as automatic updates, desktop shortcut creation, etc.
Administrative Templates\Windows Components\Windows Update	Critical from the management and security point of view, allow you to control frequency, time, and source of Windows updates
Administrative Templates\System\User	Determine different aspects of local

Profiles	and roaming profiles behavior, such as impact of slow links, permissions, etc.
Administrative Templates\System\Scripts	Contained previously (in Windows 2000 group policies) in Administrative Templates\System\Logon folder, controlling the way machine startup and shutdown scripts are executed
Administrative Templates\System\Net Logon	Control Active Directory features that are intended to optimize domain login process, such as site membership, DC Locator DNS records, or caching domain controller information on the client workstation
Administrative Templates\System\Remote Assistance	Affect solicited and offered Remote Assistance options and their security configuration such as level of control, helper list, or maximum ticket time
Administrative Templates\System\System Restore	Allows you to disable user configuration of System Restore or turn it off altogether
Administrative Templates\System\Error Reporting	Used mainly for troubleshooting and monitoring, affect level of error message notifications
Administrative Templates\System\Remote Procedure Call	Affect how RPC errors are handled
Administrative Templates\System\Windows Time Service	Allow configuration of NTP server and client settings
Administrative Templates\Network\DNS Client	Expanded well beyond what was available in Windows 2000 (in Administrative Templates\System\DNS Client folder which allowed only mandating the suffix used to identify the computer in DNS). With these settings you can control practically all DNS related features, such as client's DNS suffix search order, registration of PTR records, connection-specific DNS suffix, etc.
Administrative Templates\Network\QoS Packet Scheduler	Affect Quality of Service parameters, such as maximum reservabe bandwidth or timer resolution.
Administrative Templates\Network\SNMP	Determine SNMP communities, permitted SNMP managers, and SNMP traps for public commmunities.

User Configuration

Setting	Benefit
Administrative Templates\Windows components\Application Compatibility	Prevent or allow access to 16-bit applications
Administrative Templates\Windows Components\Help and Support Center	Used to eliminate annoying "Did you know" messages
Administrative Templates\Windows components\Terminal Services	User specific Terminal Services settings, such as a program to be started once the RDP connection is established or level of remote control allowed
Administrative Templates\Windows components\Windows Messenger	Just as equivalent settings on the computer level, these control whether Windows Messenger is allowed to run (or run at startup)
Administrative Templates\Windows components\Windows Media Player	Affect user specific options of Windows Media Player functionality, such as user interface, playback options, and networking options (such as proxy settings)
Administrative Templates\Shared Folders	Control publishing shared folders and DFS roots in Active Directory.
Administrative Templates\System\User Profiles	Control profile size and directories excluded from roaming profile (included in Administrative Templates\System\Logon/Logoff folder in Windows 2000 Group Policy)
Administrative Templates\System\Scripts	Control synchronous and visible execution of user login and logoff scripts (also included in Administrative Templates\System\Logon/Logoff folder in Windows 2000 Group Policy)
Administrative Templates\System\Ctr+Alt+Del Options	Allow removing individual buttons in the Windows Security dialog box
Administrative Templates\System\Logon	The settings grouped previously (in Windows 2000 Group Policy) in Administrative Templates\System\Logon/Logoff folder, control list of programs running at logon
Administrative Templates\System\Power Management	Determines whether the logged-on user is prompted for passwords when computer resumes from hibernate or suspend state

Appendix B

The following is the Windows2003 Security template that was created and applied to all three servers in the GIAC DMZ.

```
Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordAge = 30
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
NewAdministratorName = "TempUser"
LSAAnonymousNameLookup = 0
EnableGuestAccount = 0
[System Log]
AuditLogRetentionPeriod = 0
[Security Log]
MaximumLogSize = 99968
AuditLogRetentionPeriod = 1
RetentionDays = 30
[Application Log]
AuditLogRetentionPeriod = 0
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditAccountLogon = 2
[Service General Setting]
ALG,4,""
AppMgmt,4,""
wuauserv,4,""
BITS,4,""
EventSystem,4,""
COMSysApp,4,""
```

```
Browser,4,""
Dfs,4,""
TrkWks,4,""
TrkSvr,4,""
MSDTC,4,""
Dnscache,4,""
DriverManager,4,""
ERSvc,4,""
NtFrs,4,""
helpsvc,4,""
HTTPFilter,4,""
cisvc,4,""
SharedAccess,4,""
LicenseService,4,""
Spooler,4,""
RasAuto,4,""
RasMan,4,""
RDSessMgr,4,""
RemoteRegistry,4,""
NtmsSvc,4,""
RSoPProv,4,""
SENS,4,""
Schedule,4,""
TermService,4,""
Tssdis,4,""
Themes,4,""
AudioSrv,4,""
W32Time,4,""
WZCSVC,4,""
Messenger,4,""
lanmanserver,4,""
[Registry Values]
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateCDRoms=1,"1"
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateFloppies=1,"1"
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous
=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNo
ticeText=7,WARNING! By accessing and using this system you are consenting to
```

```
system monitoring for law enforcement and other purposes. Unauthorized use of
this computer system may subject you to criminal prosecution and penalties.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"Legal Notice for all Users"
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"0"
[Profile Description]
Description=Apply to Windows2003Servers on the DMZ
```

Appendix C

The following is the source code of the .vbs script that is applied to GIAC servers on the DMZ.

```
'******************************
'Name: HardenDMZ.vbe
'Author: GIAC Server Engineer
'Purpose: This script will strengthen servers on the GIAC DMZ against DOS attacks
'******************************

Dim value
Dim IIsObject

Set WSHShell = CreateObject("WScript.Shell")
Set WSHDir = CreateObject("Scripting.FileSystemObject")
On error resume next

'Harden against DOS Attacks
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect",2,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen",100,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxPortsExhausted",1,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions",2,"REG_DWORD"
```

```
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers\TcpMaxHalfOpenRetried",80,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers\EnablePMTUDiscovery",0,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers\KeepAliveTime",300000,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBt\Paramet
ers\NoNameReleaseOnDemand",1,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers\EnableICMPRedirects",0,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers\DisableIPSourceRouting",1,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers\TcpMaxDataRetransmissions",3,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Paramete
rs\EnableDynamicBacklog",1,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Paramete
rs\MinimumDynamicBacklog",20,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Paramete
rs\MaximumDynamicBacklog",20000,"REG_DWORD"
WSHShell.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Paramete
rs\DynamicBacklogGrowthDelta",10,"REG_DWORD"


WSHShell.Popup "DMZ TCPIP Hardening Complete"
```