GCWN Practical Assignment

Version 3.1 – Option 1

Design a Secure Windows 2000 Infrastructure

By
David C. Gibson
May 2003

Abstract

This document contains an overview of the design of a secure Windows 2000 infrastructure for a fictitious company called GIAC Enterprises. This company has about 600 employees located in 38 locations. This design was undertaken with the following guiding principles.

1. Network Administration – Ease of administration was a priority. They need to be able to do more with less.

2. Performance – Network and application performance is key to the business partners.

3. Security – Keeping corporate and customer information available to the right people, and out of the hands of those who don't need it or who would misuse it was essential.

This document includes a network diagram showing the logical layout of resources, an Active Directory diagram showing how these resources will be managed, and information on the four most used Group Policy Objects.

Table of Contents

Introduction

This document describes the design of a secure Windows 2000 infrastructure implemented by GIAC Enterprises. GIAC Enterprises recognized the need for a flexible, yet secure, IT infrastructure that would provide for the needs of its growing and diversifying operations. This document contains the following sections:

1. **Description of GIAC Enterprises**. This section provides a brief description of GIAC Enterprises and its business operations.

2. **Network Design and Diagram**. This section includes a diagram of GIAC Enterprises physical network, as well a discussion of the various server roles and placements.

3. **Active Directory Design and Diagram**. This section contains a diagram of the logical Active Directory structure of the network. Network administration, performance and security is discussed.

4. **Group Policy and Security**. This section covers the Group Policy Objects (GPO's) implemented in this design, as well as additional security requirements that are not managed through group policy.

Assumptions

The following assumptions were made during the development of this document:

1. Operating systems used: Unless otherwise indicated, all servers are loaded with Windows 2000 Advanced server with the latest service pack and patches applied. All workstations are loaded with Windows XP.

2. A "least privilege" security model has been implemented at GIAC Enterprises. This means that all users, from the executives to the janitorial staff have only the access that they need to do their jobs.

3. No software will be manually loaded on any production system (server or workstation). All software installed on production machines will by Group Policy or SMS issuance only.

4. Anti-Virus software will be used on all production systems. Virus definition updates will be pushed to all systems by Group Policy.

5. All servers have static IP addresses, and all workstations use DHCP assigned IP addresses.

Description of GIAC Enterprises

GIAC Enterprises was formed in 1997 when General Instruments America Corporation (GIACorp) acquired the Music World retail chain. GIACorp has been a wholesaler of quality musical instruments and accessories since 1984. In 1995 GIACorp relocated their corporate offices and main distribution facilities from Hayward, California to Reno, Nevada to take advantage of Nevada's more favorable tax structure and the location of UPS and FedEx shipping hubs. Music World started as a single, owner-operated, full-line music store in Sparks, Nevada in 1967. By the time that it was acquired by GIACorp, Music World had grown to a chain of over 30 company-owned retail stores located in 6 western states. This growth was fuelled by a very successful instrument rental program targeted to students in the primary and secondary schools. After their acquisition by GIACorp, the Music World corporate offices were consolidated into the newer GIAC Enterprises facilities.

GIAC Enterprises now has the following business units:

1. Executive Unit (10 people)

   This unit consists of the corporate executives and their staff. This unit requires access to real time sales and accounting data in order to make strategic business decisions. They are willing to abide by security related processes and procedures (the CIO is a strong proponent of information security) as long as they do not adversely affect their ability guide the corporate entity.

2. Research and Development Unit (14 people)

   This unit provides custom web-based tools that are used by the Sales and Marketing Unit and the Music World Retail Unit. They have also recently been providing new tools that expand the business monitoring and reporting capabilities used by the Executive Unit. Since this unit provides the tools that are critical to the money generating portions of the enterprise, security standards are strictly enforced in this environment. The developers in this unit have the use of an extensive test environment. The test environments (1 development and 1 simulated production) are physically isolated from the production environment and will not be discussed in this document.

3. Sales and Marketing Unit (65 people)

   The main function of this unit is to provide for the wholesale sales and marketing functions that were the mainstay of the old GIACorp entity. This includes the field sales staff that sells GIAC Enterprises merchandise to outside retail entities. Since the addition of the retail unit, the Sales and Marketing unit has added capacity to support the corporate retail entities in the Music World Retail Unit. The portion of the Sales and Marketing unit that is interesting from a security perspective is the field sales staff. They physically located throughout the United States and require limited access to the corporate network. This access is achieved through the use of VPN technology and an internet connection (either dial-up or broadband). The use of thin client web applications has allowed for much tighter controls and enhanced security for this group of people.

4. Product Distribution Unit (24 people)

   This unit provides all of the warehousing and distribution functions for the retail products that are sold through both the corporate owned stores (Music World) and the outside retail entities. A highly automated distribution system is a jewel in the corporate crown. This system allows for the efficient processing, shipping, and tracking of product orders as well as accurate inventory control. All incoming product is bar-coded (if it does not already have a bar code) for easy identification. The people fulfilling orders use proprietary software on a handheld pc with a barcode scanner to accurately fill order. This reduces the number of inaccurately filled orders, and the costs associated with them.

5. Music World Retail Unit (580 people)

   This unit consists of the management and staff of the 37 corporately owned retail establishments that operate under the Music World name. The critical nature of the systems used at 37 remote sites (spread across 6 states) with WAN links back to the corporate network in addition to the sensitive nature of the data used has forced some difficult decisions to be made. A store could not afford to be down if a WAN link was broken.

6. Finance and Human Resources Unit (32 people)

   This unit provides all accounting functions for GIAC Enterprises. This includes all of the customer billing and account tracking for both retail and wholesale customers. This unit also handles all of the human resources functions for all business units except the Music World Retail Unit. Individual retail store managers in the Music World Retail Unit require access to employee records for their particular store. These managers are also in control of employee actions for their stores.

7. Information Technology Unit (24 people)

   This unit provides the IT infrastructure and support for the entire enterprise. A small helpdesk is maintained to track and route problem tickets. A group of 6 hands-on technicians provide onsite support for the 37 retail stores. The rest of the staff maintains and implements any changes to the IT infrastructure of the corporation. The IT staff will also use the test resources described under the Research and Development Unit (above) to test all changes to the infrastructure (i.e., new software, configuration changes, etc.) before implementing in production.

Network Design and Diagram

The diagram below shows the network design for GIAC Enterprises. It has been simplified to show the placement of domain controllers and other major servers as well as Active Directory sites. IP subnet information has been omitted. The “Typical Music World Retail Location” site is duplicated for each of the 37 corporate owned retail locations.

GIAC Enterprises Network Diagram

Sites

GIAC Enterprises is divided into 38 Active Directory Sites. The main site is located at the corporate offices and contains all of the business units except the Music World Retail Unit. The Music World Retail Unit is broken into 37 separate sites (one for each retail location).

Corporate

The Corporate site houses all of the GIAC Enterprises business units except the Music World Retail Unit. When GIACorp relocated their operations to Reno, Nevada in 1995, they built a new facility with sufficient space to house their entire operation in one location.

Music World Retail Locations

There are 37 Music World retail locations located in 6 states (California, Oregon, Washington, Nevada, Arizona, and Utah). Each of these locations is connected by a T1 line to the corporate infrastructure. It was determined that the value of concentrating "live" inventory and customer data at Corporate out-weighed the cost of the connections. So far this strategy has paid dividends in reduced inventory age (limiting the "old stuff"), and fewer problem customer accounts. Due to the fact that the band/orchestra instrument rental business relies heavily on accurate customer billing and account management, the investment in IT infrastructure has more than paid for itself in the last couple of years.

Each of the Music World retail locations is designed to primarily operate with its WAN link active, but it has the capability to operate "off-line" for a time if the WAN link is unavailable. Corporate email and intranet are unavailable if the link is down, but normal retail sales can still proceed without interruption. There is a "catch-up" process that is activated when the WAN link is restored.

Field Sales Staff

The Field Sales staff members operate generally on the road. These are the sales people that sell GIAC Enterprises' wholesale merchandise to external retail entities. These people use an internet connection (either dial-up or broadband) with a VPN to connect to the corporate IT infrastructure. They have access to any internal resources that are needed efficiently perform their duties.

DMZ

The Demilitarized Zone (DMZ) contains the resources that are accessible from the internet. These resources are an external DNS server (configured for manual update only) and the web farm. The web farm consists of 3 Windows 2000 servers running IIS. These 3 IIS servers are attached to a hardware based load balancing appliance. These web servers allow customers to access their account information. They are able to make account updates, make payments, request account pay off information and a number of other functions using SSL encryption.

Associated with the DMZ, but not a part of it is the ISA server. The ISA server provides for Network Address Translation (NAT) as well as a software firewall. Like the servers in the DMZ, the ISA server is not a member of the domain.

Server Types

GIAC Enterprises uses eight different server types. These types are defined by their function in the network. Each server type will be briefly discussed in the following paragraphs.

Domain Controllers

The Corporate site has two domain controllers for redundancy and load sharing. They are configured as follows:

Corporate DC #1	
Processor	4 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 3 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Schema Master PDC Emulator Relative ID (RID) Master Global Catalog AD integrated DNS DHCP

Corporate DC #2	
Processor	4 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 3 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Domain Naming Master Infrastructure Master AD integrated DNS DHCP

Each Music World Retail location has a domain controller. This server is configured as follows:

Music World Domain Controller	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Global Catalog AD integrated DNS DHCP SMS Secondary

IIS Servers

GIAC Enterprises has two web farms. One is internet facing, and the other is for intranet applications. The internet web farm consists of three Windows 2000 servers running IIS. These IIS servers are attached to a hardware-based load balancing appliance. The internet IIS servers are all configured as follows:

Internet IIS Server (DMZ)	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Internet Information Server (IIS) Stand-alone (Not a domain member)

The intranet web farm consists of four Windows 2000 servers running IIS. They are also attached to a hardware-based load balancing appliance. The intranet IIS servers are configured as follows:

Intranet IIS Server	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Internet Information Server (IIS) Domain member

Exchange Servers

GIAC Enterprises uses two Exchange 2000 email servers. These servers handle all email for the enterprise, including the retail locations. These servers are configured as follows:

Exchange Server #1 and #2	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Exchange 2000

File/Print Servers

Each business unit in GIAC Enterprises has its own File/Print server with a couple of exceptions. The Product Distribution Unit had minimal file server requirements, but fairly extensive print server needs. These functions were combined with the Sales and Marketing Unit’s File/Print server. The other exception is the Music World Retail Unit. This unit has minimal file and print server needs and are distributed at 37 locations. The file and print server needs are handled by the Retail Location Application Servers discussed in the next section. The number of File/Print servers located at corporate is probably more than needed and some of them definitely could have been combined, but politics won this battle. This is one of the few legacy items that came across when the new Windows 2000 infrastructure was designed and implemented. The File/Print servers located at corporate are configured as follows:

Executive File/Print Server	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 3 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Only used as a file/print server

R&D File/Print Server	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 5 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Only used as a file/print server

Sales & Marketing File/Print Server	
Processor	2 X P4 1.8 GHz
RAM	4 GB (memory increased to accommodate heavy printing load)
Hard Drives	2 X 18 GB (RAID 1) 5 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Only used as a file/print server

Finance & HR File/Print Server	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 3 X 18 GB (RAID 5) 3 X 18 GB (RAID 5) Separate RAID array implemented to ensure financial is not commingled with HR data.
Roles/Functions/Services Configured	Only used as a file/print server

IT File/Print Server	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 36 GB (RAID 5)
Roles/Functions/Services Configured	Only used as a file/print server

Retail Location Application Servers

The Retail Location Application Servers are a multi-purpose server that handles the diverse requirements of the small retail locations. They are configured as follows (all 37 retail locations have identically configured systems):

Retail Location App Server	
Processor	2 X P4 1.8 GHz
RAM	4 GB (memory increased for performance)
Hard Drives	2 X 18 GB (RAID 1) 3 X 18 GB (RAID 5) 3 X 18 GB (RAID 5)
Roles/Functions/Services Configured	Internet Information Server (IIS) SQL 2000 Server Custom Point of Sale Application file/print server

SQL Servers

SQL servers are used in support of the internet and intranet applications used by all of the business units as well as the customers of GIAC Enterprises. The SQL servers located at corporate are configured in a clustered pair. They are configured identically as follows:

SQL Server #1 and #2 (Clustered)	
Processor	4 X P4 1.8 GHz
RAM	5 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 36 GB (RAID 5) 4 X 36 GB (RAID 5) 4 X 36 GB (RAID 5)
Roles/Functions/Services Configured	SQL 2000 Server Cluster Service

Certificate Authority

GIAC Enterprises actually has two Certificate Authorities. The Root Certificate Authority is powered down and locked away. The subordinate Certificate Authority is configured as follows:

Certificate Authority Server	
Processor	2 X P4 1.8 GHz
RAM	1 GB
Hard Drives	2 X 18 GB (RAID 1)
Roles/Functions/Services Configured	Certificate Services

SMS Server

The primary SMS server is located in the corporate datacenter, and is used to issue software to all of the servers and workstations in the corporate location. All software distribution functions are shared between SMS and group policy. This server is configured as follows:

Primary SMS Server	
Processor	2 X P4 1.8 GHz
RAM	2 GB
Hard Drives	2 X 18 GB (RAID 1) 4 X 18 GB (RAID 5)
Roles/Functions/Services Configured	SMS server

Secondary SMS servers are located at each retail location and are loaded as part of the Retail Location Application Server discussed previously.

Active Directory Design and Diagram

The Active Directory design for GIAC Enterprises was developed with following requirements in mind:

1. Network Administration: Ease of administration was one of the primary concerns that management brought forth during the planning stages for this environment. The need to do more with less has been drilled into all levels of the organization, but nowhere as strongly as in the IT unit. It is imperative that the support staff is responsive to the needs of the customer facing business units.

2. Performance: Network and application performance are also of utmost importance. Proper site management in Active Directory can minimize replication traffic, and proper domain controller (and other server) location can improve network performance.

3. Security: Increased security is the primary benefit of a well designed and implemented Windows 2000 infrastructure. The implementation of the "Least Privilege" security model could only occur with a correctly designed active directory. Advanced rights can be granted in a much more granular fashion, and the number of users with domain wide administrative access can be minimized.

GIAC Enterprises Active directory design is illustrated in the following figure.

GIAC Enterprises Active Directory Design

Domains

GIAC Enterprises' Active Directory was designed using a single domain model. It was determined the size and nature of the business could easily be accommodated by this model, and there were no security (or other) reasons to use a multiple domain model.

Sites

A Site is defined as a collection of one or more subnets. The subnets in a site should have comparatively high bandwidth network connections (i.e., LAN). Often sites are used to define groups of physically separated AD elements (OU's, users, etc.). The physical locations used by GIAC Enterprises led to an AD design using a total of 38 sites. The main (and largest) site contains the resources and users that are at the corporate location in Reno, Nevada. The remaining 37 sites are the 37 retail locations spread out across 6 states. Defining the sites in this manner allows for better control of replication traffic across the WAN links to these remote locations.

Organizational Units (OU)

The discussion of the Organizational Units (OU's) and the OU structure used in the AD implementation for GIAC Enterprises can be divided into two parts. The first part will address the use of the default (or built-in) OU's that are automatically created in the Windows 2000 Active Directory. The second, and more complex, part will cover the OU's and OU structure that were design specifically for this implementation.

Default Organizational Units and Containers

The following table lists the default AD containers and how they are used in this implementation.

Container Name	Purpose
Builtin	Contains the Windows 2000 built-in groups (i.e., Account Operators, Administrators, Backup Operators, etc.)
Domain Controller	Contains the computer accounts for all of the domain controllers. Allows for delegation of advanced security rights to all domain controllers. This OU also allows for GPO(s) to be applied to all DC's.
ForeignSecurityPrincipals	Not Used.
Users	Contains the default user objects – GIAC Enterprises' user accounts have been created in a Users OU under each business unit's OU.

Custom Organizational Unit Structure

The following table details the specific OU structure that was implemented for GIAC Enterprises and lists the purpose of each OU. Please refer to the diagram above for the logical structure of these OU's.

Organizational Unit Name	Purpose
Member Servers	Contain child OU's for each of the member server types. It is used to delegate advanced security rights and apply GPO settings to all member servers.
- SQL	Contains computer objects for each SQL servers at Corporate. (This does not include the Retail App servers that are located in the individual retail locations and have SQL loaded.) It is used to delegate advanced security rights (IT support groups) and apply GPO settings to SQL servers.
- Exchange	Contains computer objects for each of the Exchange servers in the enterprise. It is used to delegate advanced security rights (IT support groups) and apply GPO settings to Exchange servers.
- File/Print	Contains computer objects for each of the File/Print servers in the enterprise. It is used to delegate advanced security rights (IT support groups) and apply GPO settings to File/Print servers.
- SMS	Contains the computer object for the SMS Primary server. It is used to delegate advanced security rights (IT support groups) and apply GPO settings to SMS servers.
- Intranet IIS	Contains computer objects for each of the Intranet IIS servers in the enterprise. (This does not include the Retail App servers that are located in the individual retail locations and have IIS loaded.) It is used to delegate advanced security rights (IT support groups) and apply GPO settings to

	Intranet IIS servers.
- CA	Contains a computer object for the Certificate Authority server. It is used to delegate advanced security rights (IT support groups) and apply GPO settings to CA servers.
- Retail App	Contains computer objects for each of the Retail App servers in the enterprise. It is used to delegate advanced security rights (IT support groups) and apply GPO settings to Retail App servers. The GPO's for SQL and IIS are linked to this OU.
Corporate Site Container	Contains OU's for each of the business units at Corporate.
- Executive Unit	Contains child OU's for Executive Unit user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
- R&D Unit	Contains child OU's for R&D Unit user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
- Sales & Marketing Unit	Contains child OU's for Sales & Marketing Unit user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
- Product Distribution Unit	Contains child OU's for Product Distribution Unit user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
- Finance & HR Unit	Contains child OU structures for Finance and HR. Due to regulatory and oversight requirements, Finance accounts needed to be separated from the HR accounts. It is used to delegate

	advanced security rights (IT support groups) in this unit.
- Finance	Contains child OU's for Finance user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
- HR	Contains child OU's for HR user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
- IT Unit	Contains child OU's for IT Unit user and computer accounts. It is used to delegate advanced security rights (IT support groups) in this unit.
- Users	Contains user accounts.
- Workstations	Contains computer account.
Music World Retail Unit	Contains the child OU structures for the Retail Unit. It is used to delegate advance security rights (IT support groups) in this unit. Due to regulatory issues and varying state laws, sites in each state need to be logically grouped together.
- California	Contains the site containers for the retail locations in California. Each site container holds a user and a workstation OU for the user accounts and computer accounts in that site.
- Arizona	Contains the site containers for the retail locations in Arizona. Each site container holds a user and a workstation OU for the user accounts and computer accounts in that site.
- Oregon	Contains the site containers for the retail locations in Oregon. Each site container holds a user and a workstation OU for the user accounts and computer accounts in that site.
- Washington	Contains the site containers for the retail locations in Washington. Each site container holds a user and a workstation OU for the user accounts

	and computer accounts in that site.
- Nevada	Contains the site containers for the retail locations in Nevada. Each site container holds a user and a workstation OU for the user accounts and computer accounts in that site.
- Utah	Contains the site containers for the retail locations in Utah. Each site container holds a user and a workstation OU for the user accounts and computer accounts in that site.

Group Policy and Security

Group policies are used to control many aspects of GIAC Enterprises' Windows 2000 environment. It is used to grant or deny user access to resources. It is also used for software distribution, and is even used to control how a workstation looks and behaves. In the following sections several of the Group Policy Objects (GPO's) that are used by GIAC Enterprises will be outlined. Following the GPO discussion, additional security requirements will be covered.

It is important to understand the order that GPO's are applied and how that affects the priority. When conflicting GPO settings are applied the one that is applied last wins. Therefore, it can be said that GPO's are applied from low priority to high priority. They are applied in the following order:

1. Local GPO(s) – These are stored on the local machines, and not in AD.

2. Site GPO(s)

3. Domain GPO(s)

4. OU GPO(s) – These are applied from the parent OU then from the child OU.

In the following group policies, only settings that have been changed from the default will be discussed. It can be assumed that if a policy is not covered here, that the default setting applies

Basic Group Policy

Default Domain Policy

The default domain policy is applied to domain wide. The following tables provide details to some of the settings in this policy.

Password Policy	Setting	Reason
Enforce Password History	13 remembered	Sufficient to prevent users from toggling between favorite passwords. 13 also makes date references less likely.
Maximum Password Age	90 days	Longer password ages encourage better passwords, fewer password resets are required, and fewer people will resort to writing the passwords down to remember them.
Minimum Password Age	2 Days	Prevents user from repeatedly changing passwords until they can use their “favorite one” again.
Minimum Password Length	8 characters	This also is a concession to the users. Longer passwords are better, but can be harder to remember. Administrative accounts require longer passwords.
Complexity Requirements	Enabled	Stronger passwords are a must. Since additional length is not required, the use of complex passwords will be.

Account Lockout Policy	Setting	Reason
Account Lockout Duration	60 minutes	60 minutes will be sufficient to discourage a password guessing attacker.
Account Lockout Threshold	6 invalid tries	This will cut down on helpdesk calls for password resets, caused by weekends, etc.
Reset Account Lockout Counter After	60 minutes	This is a reasonable setting for those with “fat finger” problems.

Local Policies / Security Options	Setting	Reason
Additional Restrictions for anonymous connections	No Access without explicit anonymous permissions	Prevents NULL sessions.
Message Text for Users attempting to log on	This system is to be used by authorized GIAC	Legal notice is required.

	Enterprises Employees only. This system is subject to monitoring. Unauthorized use of this system will be prosecuted.	
Message title for users attempting to log on	GIAC Enterprises – Authorized use only.	
Disable CTRL+ALT+DEL requirement at log on	Disabled	CTRL+ALT+DEL is required.
LAN Manager Authentication Level	Send NTLMv2 – refuse LM and NTLM.	Less secure Authentication methods are not required.
Do Not display last user name in logon screen	Enabled	Username is half of Username/Password.

Default Domain Controller Policy

The default domain controller policy is applied to all domain controllers. Due to the critical function provided by the DCs, this policy provides the additional security settings that are needed. The following tables provide details to some of the settings in this policy.

Account Lockout Policy	Setting	Reason
Account Lockout Duration	0 minutes	This requires administrative action when an account is locked out on a domain controller.

Setting the audit policies takes some care due to performance issues and space requirements for large logs. It was determined that the following events (or actions) needed to be audited on the domain controllers and sufficient log space has been allocated.

Audit Policies	Setting
Audit Account Logon Events	Success, Failure
Audit Account Management	Success, Failure
Audit Directory Service Access	Failure
Audit Logon Events	Success, Failure
Audit Object Access	Failure
Audit Policy Changes	Success, Failure
Audit Privilege Use	Failure
Audit System Events	Success, Failure

User Rights Assignments	Setting	Reason

Add Workstations to Domain	Administrators	Only administrators are authorized to add workstations.
Change the System Time	Administrators	Due to the importance of time synchronization for Kerberos, this right needs to be restricted.
Logon Locally	Administrators	Logging on directly to a DC is restricted.
Shut Down the System	Administrators	This function also needs to be restricted.

Security Options	Setting	Reason
Allow Server Operators to Schedule Tasks	Disabled	Only Administrators are able to schedule tasks on domain controllers.
Allow system to be shutdown without having to log on	Disabled	This effectively means that only administrators can shut down the domain controllers.
Audit use of backup and restore privilege	Enabled	It was deemed desirable to log backup and restores to the DCs.

Event Logs	Setting	Reason
Restrict Guest Access to Application Log	Enabled	Even though the Guest account is disabled, this provides additional protection.
Restrict Guest Access to Security Log	Enabled	Same as above.
Restrict Guest Access to System Log	Enabled	Same as above.
Retention Method for Application Log	Manually	Requires administrator action, but the importance of log files warrants this action.
Retention Method for Security Log	Manually	Requires administrator action, but the importance of log files warrants this action.
Retention Method for System Log	Manually	Requires administrator action, but the importance of log files warrants this action.
Shut Down the Computer When the Security Log is Full	Disabled	This will prevent a “Denial of Service” situation if the log filled up.

Additional Group Policy

It is beyond the scope of this document to enumerate all of the group policy objects that are used throughout the AD structure of GIAC Enterprises. I have chosen to cover the default workstation GPO that is applied to all workstations in the enterprise, and the default member server GPO that is applied to all member servers.

Default Workstation Group Policy

There are a number of group policy settings that are used for workstations enterprise wide. These settings are covered in the following tables. These settings are based on the Windows 2000 Professional Operating System Level 2 Benchmark (Consensus Baseline Security Settings) published by the Center for Internet Security, and have been modified to fit the exact needs of GIAC Enterprises.

Local Policies / Security Options	Setting	Reason
Additional Restrictions for anonymous connections	No Access without explicit anonymous permissions	Prevents NULL sessions.
Allow System to be Shut Down Without Having to Log On	Disabled	Effectively means that only Authenticated Users can shut down the workstation.
Allowed to Eject Removable NTFS Media	Administrators	
Amount of Idle Time Required Before Disconnecting Session	30 Minutes	
Automatically Log Off Users When Logon Time Expires	Enabled	Provides better enforcement of user logon times.
Clear Virtual Memory Pagefile When System Shuts Down	Enabled	
Digitally Sign Client Communication (When Possible)	Enabled	
Digitally Sign Server Communication (When Possible)	Enabled	
CTRL+ ALT+ Delete Requirement for Logon	Disabled	
Do Not Display Last User Name in Logon Screen	Enabled	
LAN Manager Authentication Level	Send NTLMv2 response only	This is a homogenous W2K/XP environment,

		NTLMv2 is required.
Message Text for Users attempting to log on	This system is to be used by authorized GIAC Enterprises Employees only. This system is subject to monitoring. Unauthorized use of this system will be prosecuted.	Legal notice is required.
Message title for users attempting to log on	GIAC Enterprises – Authorized use only.	
Number of Previous Logons to Cache	1	This allows laptop users to work with cached credentials.
Prevent System Maintenance of Computer Account Password	Disabled	
Prevent Users from Installing Printer Drivers	Enabled	
Prompt User to Change Password Before Expiration	14 Days	
Recovery Console: Allow Automatic Administrative Logon	Disabled	
Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders	Disabled	
Rename Administrator Account	"Da1!Man"	Local Administrator account is a regular target.
Restrict CD- ROM Access to Locally Logged- On User Only	Enabled	
Restrict Floppy Access to Locally Logged- On User Only	Enabled	
Secure Channel: Digitally Encrypt Secure Channel Data (When Possible)	Enabled	
Secure Channel: Digitally Sign Secure Channel Data (When Possible)	Enabled	
Secure Channel: Require Strong (Windows 2000 or later) Session Key	Enabled	Windows 2000 domains are capable of supporting strong session keys.

Send Unencrypted Password to Connect to Third- Party SMB Servers	Disabled	
Smart Card Removal Behavior	Lock Workstation	This setting is included for future planned smart card use by remote users.
Strengthen Default Permissions of Global System Objects (e. g. Symbolic Links)	Enabled	
Unsigned Driver Installation Behavior	Warn, but allow installation	
Unsigned Non- Driver Installation Behavior	Warn, but allow installation	

User Rights Assignment	
Access this computer from the network	Administrators, Workstation Support Group
Act as part of the operating system	None
Back up files and directories	Administrators
Bypass traverse checking	Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	None
Create permanent shared objects	None
Debug Programs	None
Deny access to this computer from the network	Guests
Deny logon as a batch job	None
Log on as a batch job	None
Log on as a service	None
Log on locally	Users, Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Users, Administrators
Replace a process level token	None
Restore files and directories	Administrators
Shut down the system	Users, Administrators
Synchronize directory service data	None
Take ownership of file or other objects	Administrators

Default Member Server Group Policy

Just as all of the workstations in the enterprise start with same default workstation GPO, all of the member servers in the enterprise have their basic GPO settings applied through the default member server group policy. The features of this GPO are detailed in the following tables. These settings are based on the Windows 2000 Server Operating System Level 2 Benchmark (Consensus Baseline Security Settings) published by the Center for Internet Security, and have been modified to fit the exact needs of GIAC Enterprises.

Audit Policies	Setting
Audit Account Logon Events	Success, Failure
Audit Account Management	Success, Failure
Audit Directory Service Access	Not Defined
Audit Logon Events	Success, Failure
Audit Object Access	Failure
Audit Policy Changes	Success, Failure
Audit Privilege Use	Failure
Audit Process Tracking	Not Defined
Audit System Events	Success, Failure

Event Logs	Setting
Application Log	
Maximum Event Log Size	80Mb
Restrict Guest Access to Logs	Enabled
Log Retention Method	Overwrite Events As Needed
Log Retention: Not Defined	
Security Log	
Maximum Event Log Size	80Mb
Restrict Guest Access to Logs	Enabled
Log Retention Method	Overwrite Events As Needed
Log Retention: Not Defined	
System Log	
Maximum Event Log Size	80Mb
Restrict Guest Access to Logs	Enabled
Log Retention Method	Overwrite Events As Needed
Log Retention: Not Defined	

Local Policies / Security Options	Setting
Allow System to be Shut Down Without Having to Log On	Disabled
Allowed to Eject Removable NTFS Media	Administrators
Amount of Idle Time Required Before Disconnecting Session	30 Minutes
Audit the access of global system	Not Defined

objects	
Audit the use of backup and restore privilege	Not Defined
Disable CTRL+ ALT+ Delete Requirement for Logon	Disabled
Do Not Display Last User Name in Logon Screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only
Number of Previous Logons to Cache	0
Prevent System Maintenance of Computer Account Password	Disabled
Prevent Users from Installing Printer Drivers	Enabled
Prompt User to Change Password Before Expiration	14 Days
Recovery Console: Allow Automatic Administrative Logon	Disabled
Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders	Disabled
Restrict Floppy Access to Locally Logged- On User Only	Enabled
Secure Channel: Require Strong (Windows 2000 or later) Session Key	Enabled
Send Unencrypted Password to Connect to Third- Party SMB Servers	Disabled
Smart Card Removal Behavior	Lock Workstation
Strengthen Default Permissions of Global System Objects (e. g. Symbolic Links)	Enabled
3.2.1. 37 Unsigned Driver Installation Behavior	Warn, but allow installation
3.2.1. 38 Unsigned Non- Driver Installation Behavior	Warn, but allow installation

User Rights Assignment	
Access this computer from the network	Administrators, Server Support Group
Act as part of the operating system	None
Back up files and directories	Administrators
Bypass traverse checking	Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	None
Create permanent shared objects	None
Debug Programs	None

Deny access to this computer from the network	Guests
Deny logon as a batch job	None
Deny logon as a service	None
Deny logon locally	None
Enable computer and user accounts to be trusted for delegation	None
Force shutdown from a remote system	Administrators
Generate security audits	None
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators, Server Support Group
Lock pages in memory	None
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Log on locally	Administrators, Server Support Group
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators, Server Support Group
Profile single process	Administrators
Profile system performance	Administrators
Replace a process level token	None
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	None
Take ownership of files or other objects	Administrators

Additional Security

Disaster Recovery Plan

GIAC Enterprises has implemented an extensive disaster recovery plan. This includes duplicate power feeds into the data center with UPS backup, and complete backup tape sets that are stored offsite. A server can be rebuilt from an image in only a couple of hours. Additional plans are currently underway to implement a secondary datacenter that will be located in another facility. The lessons learned from disasters like September 11th have been taken to heart since GIAC enterprises relies very heavily on its IT infrastructure.

Physical Security

Implementing physical security is a very important part of secure Windows 2000 infrastructure. If a hacker (or disgruntled employee) can gain physical access to an infrastructure server (like a domain controller) all of the group policy settings in the enterprise will not be able to protect your network. So, in keeping with this, GIAC Enterprises built a very nice data center to protect their corporate servers. This data center uses card key access. A security guard is at the entrance to verify that no unauthorized hardware enters (or more importantly, leaves) the facility. In addition, all servers are locked in rack mount cabinets with console access through KVM (Keyboard-Video-Mouse) switches.

References

1. The Center of Internet Security “Windows 2000 Server Operating System Level 2 Benchmark - Consensus Baseline Security Settings - (Stand-alone and Member Servers)”, URL – http://www.cisecurity.org

2. The Center of Internet Security “Windows 2000 Professional Operating System Level 2 Benchmark - Consensus Baseline Security Settings - (Stand-alone and Member Servers)”, URL – http://www.cisecurity.org

3. Fossen, Jason “Securing Windows” SANS Course Material.

4. National Security Agency “Security Recommendation Guides”, URL – http://nsa1.www.conxion.com

5. McLean, Ian “Windows 2000 Security – Little Black Book” Coriolis, 2000