Global Information Assurance Certification Paper

A Secure Windows 2000 Infrastructure

Securing Windows Practical Assignment
Version 3.0 – Option 1

John Verseman

Introduction/Corporate Scenario

GIAC Enterprises is an e-business that deals in the sale of online fortune cookie sayings. The on-line fortune cookie saying industry is a relatively young industry and is currently experiencing a phase of unprecedented growth. GIAC Enterprises has benefited well from this explosion in the on-line fortune cookie saying industry with the release of some highly innovative products. As a result, GIAC Enterprises has grown significantly from being a small startup company and they are now poised to become a major player. Along with the recent boom in the industry, GIAC Enterprises has also seen a significant increase in competition. After several consecutive years of record profits, GIAC Enterprises has built up a significant amount of cash and has determined that if it is going to not only stay competitive, but dominate the on-line fortune cookie saying industry, it must overhaul it's aging NT 4.0 network infrastructure. Though GIAC Enterprises has gained a position of relative prominence in the industry through developing innovative products, their existing internal network has a number of serious problems.

The major issues with GIAC Enterprises' network infrastructure are as follows:

- Nearly all the server hardware is nearing the end of its useful life and needs to be replaced.
- There is no real support structure in place. There is an IT Team that handles both client and server issues. Responsibilities are not clearly defined. Employees learn by word of mouth who to call for support.
- There is no clear separation of development, certification and production networks.
- Corporate policy regarding the rules of the network is not clearly defined.
- The NT 4.0 infrastructure has one master user domain and numerous resource domains along with a complex web of trusts. Ownership of these domains is not clearly defined.
- All of GIAC Enterprises' users have been given a lot of freedom with their client devices and no policies have been truly enforced regarding the installation of unauthorized software, etc.
- A comprehensive security strategy is non-existent. Beyond the basics of NTFS and share permissions, trying to keep the servers up to date on their service packs and hot fixes and some simple measures regarding physical security, GIAC Enterprises does little, if anything, to ensure its network is secure.
- No service level agreements are in place. This has made it difficult to take servers down for regular maintenance. (Service Packs, Firmware upgrades, etc.)

Much of GIAC Enterprises' current problems are a result of a "get it done at all costs" cultural attitude that is the very reason for their current success. Historically, employees at GIAC Enterprises have gotten things done by using

internal relationships instead of clearly defined process and procedures. Additionally, the freedom GIAC Enterprises gave its developers helped GIAC Enterprises bring innovative products to market quickly, but resulted in a very disorganized internal network. GIAC Enterprises could get away with this as a small company, but this model does not scale well.

Management at GIAC Enterprises realizes that if they are going to be the number one player in the market, they must run their company more efficiently while preserving the "get it done at all costs" attitude that has made them successful to this point. Thus management has issued a corporate initiative to upgrade its existing network infrastructure to Windows 2000 to address issues with its aging hardware inefficient network design. Along with the network upgrade, GIAC Enterprises plans to roll out a comprehensive security strategy to address its growing security concerns, especially in an increasingly competitive industry.

GIAC Enterprises has recently completed a project upgrading all of its client devices to Windows 2000 Professional and has decided to build a pristine Windows 2000 environment as opposed to upgrading the existing NT 4.0 environment in place. This paper will concern itself with the design of the Windows 2000 network along with its supporting organizational structure, and GIAC Enterprises' Security Strategy. The specific details of the Windows 2000 migration itself are beyond the scope of this paper and will not be covered.

Corporate Structure

GIAC Enterprises is based out of Kansas City, Missouri and has five main divisions: Research and Development, Sales and Marketing, Human Resources, Finance, and Information Technology. Human Resources is responsible for recruiting, employee relations, and compensation and benefits administration. Finance handles all accounting duties. The Sales and Marketing group is tasked with the job of growing GIAC Enterprises. The Marketing group develops all collateral and corporate messaging. They are also responsible for managing the content on GIAC Enterprises' external web site. The Sales force is responsible for generating new business for GIAC Enterprises. Most of the Sales force works remotely and connects to the corporate network via a VPN connection over the Internet. Research and Development is the heart and soul of GIAC Enterprises. They are responsible for the development of new products as well as the support of their existing products. Information Technology is responsible for supporting the end user and providing the network infrastructure for GIAC Enterprises.

From an IT management perspective, Research and Development has operated as an independent entity. GIAC Enterprises began with Research and Development taking care of all the network administration duties, but as GIAC Enterprises grew a small corporate IT group was formed to manage the network resources for the other support groups: Finance, Human Resources and Sales

and Marketing as well as email. In addition to the corporate history of Research and Development maintaining control of its own network resources, the corporate IT group was small and did not have a well defined support structure and therefore has continuously struggled to keep up with the increasing support demands of the organization. As a result there has been little coordination between Research and Development and Corporate IT and this has been the root of many of the problems GIAC Enterprises is experiencing with its network infrastructure.

Support Structure and Policy

Management at GIAC Enterprises has determined unless issues with its organizational structure are addressed, the network infrastructure will collapse under the weight of its own success no matter what technology is implemented and how. Management has decided to implement a support structure to meet the increasing support demands of its user community. Additionally, management has decided to consolidate Information Technology into one group in order to better coordinate network management activities. Finally, management has decided to develop a formal policy outlining the dos and don'ts of the GIAC Enterprises network as well as service level agreements.

GIAC Enterprises will implement a three-tier support structure. The support duties will be outlined as follows:

- **Tier 1:** The Help Desk: The Help Desk is responsible for first level support. They provide one point of contact for all employees for all support issues.
- **Tier 2:** The Desktop Team: The Desktop Team is responsible for seeing any issues the Help Desk cannot fix through to their resolution. Additionally, the desktop group is responsible for providing, maintaining and configuring all user devices as well as supporting all client side software.
- **Tier 3:** The Server Team: The server team is responsible for building and maintaining GIAC Enterprises' server infrastructure. This includes all web, database, messaging, application, directory services, and network services servers.

The Server Team itself is subdivided into three groups:

- **Corporate Server Support:** This team is responsible for the corporate support infrastructure – this includes messaging, application services, directory services, print services, corporate web services, backup services, and anti-virus services for the whole company. Additionally they provide file and database services for Human Resources, Finance and Sales and Marketing.

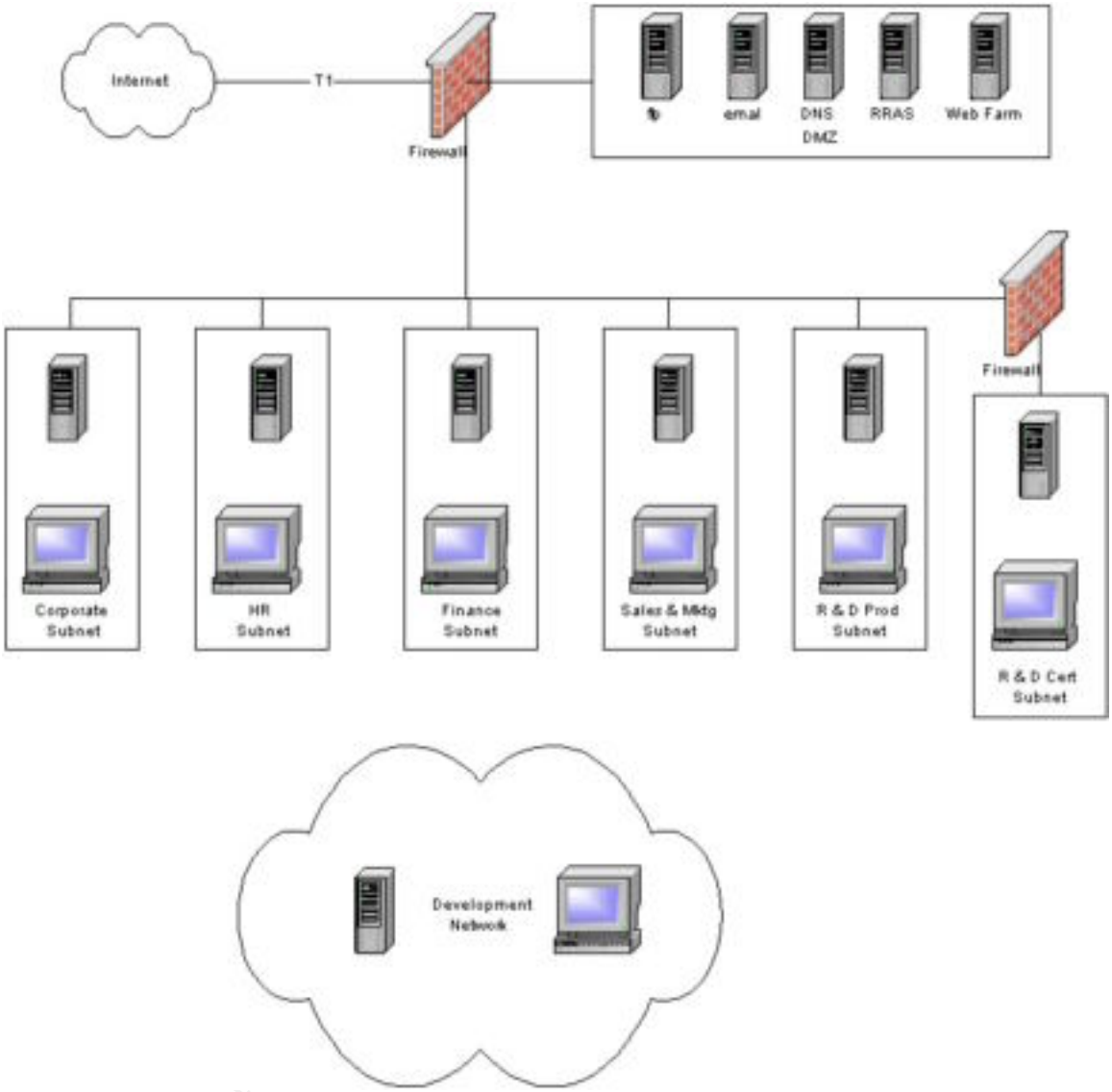
- **Production and Certification R&D Server Support:** This team is responsible for all services on the production and certification Research and Development networks. Additionally this group also is responsible for ensuring the certification network accurately models the production network.
- **Development R&D Server Support:** This team is responsible for all services on the development Research and Development network.

Finally there is a small team called Auditing and Research. This team's primary responsibility is monitoring all the security logs and investigation of any security breaches. This team is responsible for periodically reviewing GIAC Enterprises' corporate security strategy and determining its effectiveness. Additionally, this team also monitors for new virus threats and security bulletins and determines the appropriate Service Pack and Patch level for all servers and desktops.

In addition to implementing an improved organizational support structure, GIAC Enterprises has developed a formal policy regarding the rules of the corporate network as well as service level agreements. The corporate network policy outlines acceptable behavior and use of the network, and reminds users that their actions will be monitored without any prior notices. Additionally the corporate network policy states that the philosophy behind the policy is "That which is not expressly allowed is denied." Service Level Agreements have been put in place so all servers can be put on a regular maintenance schedule so service packs, hot fixes, firmware updates, etc can be applied in a timely manner with little or no unplanned interruption in service.

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

Network Design



Overview

GIAC Enterprises has chosen a mostly standard design for it's corporate network. GIAC Enterprises has one full T1 line connected to a router that connects GIAC Enterprises to the Internet. A firewall routes packets either to a screened subnet (DMZ) or the GIAC Enterprises corporate network. The DMZ contains external DNS, email and ftp servers as well as a web farm which hosts GIAC Enterprises' corporate web site and an RRAS server. The internal network is sub-netted out by business unit and contains all internal email, DNS, web, database, and network and directory service servers. Lastly the development

environment for the Research and Development group exists as an untrusted Active Directory forest on an isolated subnet that is not physically connected to the GIAC Enterprises network or the Internet.

The DMZ

The DMZ is considered to be the area where GAIC Enterprises' network is most vulnerable to outside attack. To mitigate this risk, GIAC enterprises has taken numerous steps in the design and build of all servers in the DMZ. First and most notably, none of the servers in the DMZ participate are members of GIAC Enterprises' Active Directory infrastructure, nor are they any part of any domain. All servers in the DMZ are currently managed individually. Second, all servers in the DMZ are designed and built for one specific purpose. The DNS servers only provide DNS, the email servers only route email to and from GIAC Enterprises' internal email servers, the web servers only host GIAC Enterprises' external web site and the FTP server only provides FTP services. This design was chosen so as few ports and services are open to the Internet as possible on any one system. (Anthes, A Secure Windows 2000 Infrastructure Design, p. 3.) There are two DNS servers in the DMZ for redundancy purposes. Also, the web servers all participate in a web farm, so the web site can maintain 24X7 availability but servers that host the web site can be taken down individually for maintenance if necessary. All servers in the DMZ run either Windows 2000 Server, except for the web servers, which run Windows 2000 Advanced Server in order to make use of network load balancing capabilities. All are also loaded with Service Pack 2 and the latest hot fixes. All machines use dual power supplies. All drives are hot swappable with RAID-1 used on all system drives and RAID-5 used on all data drives. Drives are formatted with NTFS with permissions strictly controlled and audited. All servers have been hardened by having unnecessary services disabled. All accounts have strong passwords, guest accounts are disabled and renamed, and administrator accounts have also been renamed.

Finally, GIAC has taken a few extra steps to harden its IIS Servers in the DMZ. All unused ISAPI extensions and filters have been removed; all http and ftp root folders have been moved from the system drive to their own drive. Security logs have also been relocated to their own drive and their size has been set to 500MB with a retention period of 15 days. In order to protect the IIS metabase, NTFS permissions have been set on the metabase.bin file and the metaback folder to full control for system and administrators and modify for operators. (Fossen, Securing Internet Information Server 5.0 p. 183)

The Internal Network

GIAC Enterprises' primary internal network is roughly divided into two distinct parts: the corporate production network, and the certification network. Each of these halves is separated by a firewall. Additionally, a development network exists as an untrusted domain on an isolated subnet with no physical connection to the GIAC Enterprises product or certification network or the Internet. GIAC Enterprises chose this design to give the developers more freedom to try radical new ideas in online fortune cookie saying design and delivery on the development network without having any adverse impact on the production network. The development network is very chaotic compared the production and certification networks. It is a holdover from GIAC Enterprises' roots where the Research and Development group could make changes rapidly without having to follow lots of processes and procedures. Policies and process will be put in place to provide a minimal amount of control, but the development network is intended be a "playground" for developers to experiment freely with new ideas and is intentionally left wide open – which is why it is not connected to the Internet or the primary internal network. Roughly speaking the development network will run parallel to the production network, and developers will have two machines at their desks: one connected to the internal corporate network and one connected to the development network. Management believes that this network design will give them the compromise they are looking for: the production network will be more efficient in its design and tightly controlled thus more stable, reliable and manageable, but the isolated development network will still give GIAC Enterprises' developers the freedom they had in the early days to explore new ideas and rapidly develop new products as well as enhancements to existing products.

GIAC Enterprises decided to further segregate its internal network by business unit. Thus HR, Finance, IT and Sales and Marketing each have their own subnet. There is a subnet for common network resources such as the internal web servers, application servers, email servers, print servers and an SMS Server for software distribution and inventory purposes. Research and Development has two subnets: production and cert. The cert network is separated from the rest of the network by a firewall and has its own domain with a one way trust set up to the production network. All other subnets can communicate freely with each other. GIAC Enterprises has decided to go with this design in anticipation of future growth. Eventually these groups can easily be separated by firewalls if necessary and IP traffic between business units could easily be filtered and controlled if necessary.

Human Resources, Finance, and Sales and Marketing each have a file server and a database server that resides on their respective subnets. The production Research and Development network also has two file servers, two database servers, a web farm and an application server in each of its environments

The certification network exists on its own separate subnet and it is designed to accurately model the production network. Thus it is treated with the same respect as the production network with regards to its configuration and any changes made to that configuration. It exists a separate domain under giacenterprises.com with a one-way trust to the production network. It is important to note here that primary purpose of the certification network is intended to model the Research and Development production subnet. However a smaller scale certification network does also exist for the HR, Finance, and Sales & Marketing subnets to test upgrade and rollouts of new and existing applications for those groups. The biggest difference with regards to scale is that the certification network exists as a single subnet whereas the production network exists as six subnets.

All servers and workstations in all these subnets run either Windows 2000 Professional or the appropriate variation of Windows 2000 Server with the latest service packs and hot fixes applied. On server class machines, all system drives are configured as RAID-1 volumes with all other drives using a RAID-5 configuration and all drives are formatted with NTFS. Dual power supplies are also used in all server class machines. All internal systems are also hardened – unnecessary services have been disabled or removed guest accounts are disabled and renamed and administrator passwords have been renamed.

Hardware Strategy

GIAC Enterprises has chosen to use a single hardware vendor in an effort to promote uniformity across its network. GIAC Enterprises has chosen Compaq as its hardware provider and as a result uses Compaq's Insight Manager solution to monitor the health of its server hardware. Insight Manager provides administrators with information about the health of their hardware from a central console. Use of this tool will allow administrators to proactively monitor for potential hardware issues. In this same vein, wherever possible on server class machines, fault tolerance is implemented, through the uses of RAID configurations, redundant power supplies, etc. Finally, all corporate servers are connected to a UPS so the servers can shut down gracefully in the event of a power failure. A backup generator would provide complete protection from a power failure, but management has determined that implementing such a measure at this time would be cost prohibitive.

Backup Strategy

Client machines based out of headquarters are configured to use home directories on the network and off-line file synchronization. With all information being stored on the servers, servers are then backed up on a weekly basis. Full backups are done Friday nights, so impact on the network is minimal.

Cumulative incremental backups are done Monday through Thursday. GIAC Enterprises also stores its backups off site. To help manage the cost of tapes, GIAC Enterprises recycles it's tapes every thirteen weeks. In order to make sure older data is available is necessary GIAC Enterprises also designates the first full week of every month as an archive week. Backups during archive week are not part of the thirteen-week rotation and are saved off site for one year. Additionally, unless tapes are needed for a restore GIAC Enterprises only keeps the current and the previous week's backups on site. Everything else is stored in an off-site storage facility.

Anti-Virus Strategy

GIAC Enterprises selected Trend Mirco for it's anti-virus solution because of the software architecture. All machines receive their updates from an internal server that is configured to get its updates directly from Trend Micro. This means that all clients and servers can be managed centrally. This is especially important on the client side because clients are not responsible for getting their own updates. Rather all client software is configured and updated centrally from the server. In additional to running anti-virus software on its client and server systems, GIAC Enterprises also runs anti-virus software on its email systems as well. This software is configured to scan incoming and outgoing messages for viruses. In addition, GIAC Enterprises also uses Trend's content filtering and attachment blocking capabilities. Emails that contain inappropriate language are blocked as well as the following attachments: .exe, .vbs, .scr, .htm, .html, .xml, .eml, .asp, .ocx, rm, .ram, .asf, .avi, .qt, .mpeg, .mp3 and .bat. Finally, GIAC Enterprises blocks access to public email sites (hotmail, yahoo, etc) to prevent users from circumventing its attachment blocking policy and accidentally or deliberately downloading infected files on to the network.

Special considerations for remote users

Remote users' client devices also have a few extra standard configurations to make them more secure. BIOS passwords are enabled so a separate password is required to get a laptop to even boot. Laptops are also loaded with personal firewall software, so users are protected when they aren't connected to the GIAC Enterprise's network. Also, the drives on the laptops are partitioned into a system drive and a data drive. All program files are stored on the data drive and client side caching for offline folder synchronization is configured to use the data drive. This is done so EFS can be used on the data drive to further protect data on laptops without adversely affecting system performance. Laptops are also configured to use L2TP over IPSec and use the strongest authentication and encryption methods possible. Finally a special account has been created to serve as the recovery agent and laptops have been configured to use the

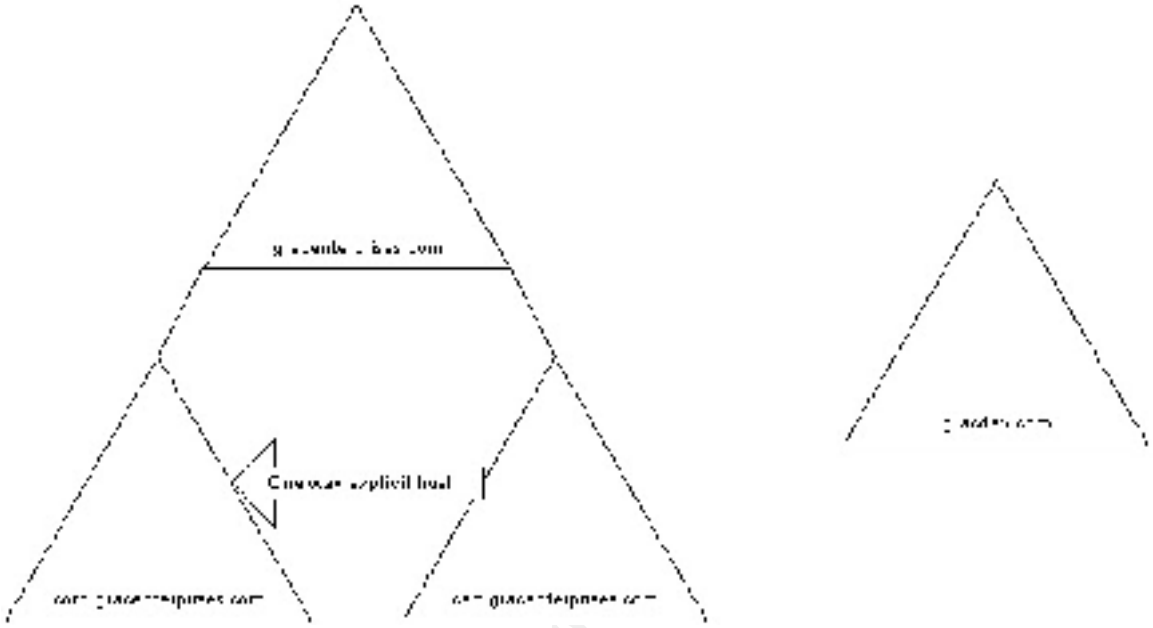
recovery agent account as the recovery agent instead of the administrator account, which is the default recovery agent.

Other Physical Security Considerations

It is important to note here that physical security is also an important consideration. The security options in Windows 2000 aren't nearly as effective if someone can walk out your front door with one of your domain controllers. GIAC Enterprises has taken numerous steps to help ensure physical security. All servers are stored in a physically secure location and access is restricted to administrators only. A card reader access system has been put in place so access can be logged and monitored for suspicious activity. Additionally all networking equipment is in a physically secure location with access restricted only to those who need it. All employees undergo a basic background check before they are officially hired at GIAC Enterprises and all employees are required to wear their photo ID's on their person while in the GIAC Enterprises Facility. Additionally all guests and contractors must be escorted by a GIAC Enterprises Employee at all times.

Active Directory Design

DNS/Domain Design



Because GIAC Enterprises wants to segregate its production and certification networks, they have decided to use a multiple domain model. GIAC Enterprises followed recommendations from Microsoft and constructed an empty forest root domain – giacenterprises.com, with two sub domains: corp.giacenterprises.com and cert.giacenterprises.com. Again, servers in the DMZ do not participate in the domain. The development network currently uses a single domain model and is named giacdev.com. Since the development environment is completely isolated and is subsequently a loosely controlled and rapidly changing environment, its design will not be discussed in any significant detail.

Control of, and access to the empty forest root domain, giacenterprises.com is granted only to the directory services team in corporate IT. They are assigned a special account with privileges that is a member of the Schema Admins and Enterprise Admins group. This account is separate from their regular network sign on and separate from their administrative sign on.

FSMO (Flexible Single Master Operations) Placement

Because GIAC Enterprises is a large network, Operations Master roles have been separated out to improve performance. There are five Operations Master roles: Schema Master, Domain Naming Master, Infrastructure Master, RID

Master, and PDC Emulator. The Schema Master and Domain Naming Master are forest wide roles, which means that only one of each exists for the whole forest. The other roles domain roles and must exist in each domain.

GIAC Enterprises used the following rules/guidelines for FSMO placement.

- The Schema Master and Domain Naming Master Roles should be located on the same Domain Controller (Pg 186)
- The Domain Naming Master should be located on a Global Catalog Server
- The Infrastructure Master should not be located on a Global Catalog Server

(Fullerton & Hudson, Using Microsoft Active Directory, p. 185-186)

With these recommendations in mind, GIAC Enterprises has placed its operations Masters as follows:

Forest Root Domain (giacenterprises.com)

- DC1: Schema Master/Domain Naming Master/Global Catalog
- DC2: Infrastructure Master, RID Master, PDC Emulator

Production Domain (corp.giacenterprises.com)

- DC1: Infrastructure Master
- DC2: RID Master/Global Catalog
- DC3: PDC Emulator/Global Catalog

Certification Domain (cert.giacenterprises.com)

- DC1: Infrastructure Master
- DC2: RID Master/Global Catalog
- DC3: PDC Emulator/Global Catalog

Development Domain (giacdev.com)

- DC1: Schema Master/Domain Naming Master/Global Catalog
- DC2: RID Master/Global Catalog
- DC3: PDC Emulator/Global Catalog
- DC4: Infrastructure Master

Since there is only one Schema and Domain Naming master for the entire forest and the Schema and Domain Naming master roles are installed on the first domain controller in the forest by default, the Schema Master and Domain Naming Master reside in the forest root domain. All other operations master roles will exist on the other domain controller. Since only the Schema Admins and Enterprise Admins have direct access to the empty forest root domain, there

is very little logon traffic and changes are infrequent thus only two domain controllers are necessary mostly so the infrastructure master for the domain can reside on a domain controller that is not a global catalog.

By comparison, the other domains handle a large amount of logon traffic and thus more domain controllers are necessary. Additionally, each domain controller handles only one Operations Master role for load balancing purposes. Multiple global catalogs exist in these domains to speed up logon times. Because the network is all 100mb and there is only one site, GIAC Enterprises is not concerned with controlling replication traffic at this time. However replication traffic will be proactively monitored as the network grows so potential problems can be addressed early. Finally all Domain Controllers only function as Domain Controllers. All other unnecessary services have been disabled.

OU Design

OU's exist for two main reasons, to delegate administration, and to facilitate the implementation of group policy. GIAC Enterprises wants to keeps its OU structure as flat as possible and wants to avoid nesting. This strategy will speed up the application of group policy and simplify its administration. All OU's have been created at the top level of the OU structure. A summary of the groups created follows:

- **GIAC Users:** Contains all corporate user accounts and any groups whose membership is administered by IT
- **Help Desk:** Contains all administrative accounts and groups for the Help Desk Team.
- **Desktop Support:** Contains all administrative accounts and groups for the Desktop Support team.
- **Servers:** Contains all computer accounts for all of GIAC Enterprises' serves.
- **Workstations:** Contains all computer accounts for all GIAC Enterprises' workstations
- **Printers:** Contains all printer objects.
- **Human Resources:** Contains all groups and shares that HR administers
- **Finance:** Contains all groups and shares that Finance administers
- **Sales and Marketing:** Contains all groups and shares that Sales and Marketing administers
- **Research and Development:** Contains all groups and shares that research and development administers.

All user and computer accounts in corp.giacenterprises.com are centrally administered by IT along with all corporate printers. Specific tasks within IT are delegated out to the Help Desk and Desktop support teams. Group membership and share management are delegated out to the individual business units within

GIAC Enterprises. Thus HR has its own OU that contains shares and groups and manages membership to all groups and permissions on all shares in its OU. The same thing goes for Finance, Research and Development, and Sales and Marketing.

Since all user accounts are centrally administered and group policy, as it is applied to users, will be applied to all users equally, GIAC Enterprises chose not to locate user accounts in their corresponding business unit OU's. Instead, GIAC Enterprises created a separate user's OU for all user accounts in corp.giacenterprises.com. There is also a Help Desk OU and a Desktop support OU. These OU's contain administrative accounts and groups for the Help Desk and Desktop support groups. These groups have their own OU's for the purposes of delegating authority. Custom mmc's and task pads are configured and maintained for each of these groups by the server team. This is done so these groups only have the privileges they need to perform their necessary job functions. Administrative accounts for the server team are located in the default users OU. All administrative user accounts are located outside the GIACUsers OU so a user configuration policy can be applied to the GIAC Enterprises Users without those settings being applied to administrative accounts. All administrative groups are required to sign on with a regular user sign on located in the GIACUsers OU and use the "run as" feature to perform any administrative tasks.

The OU structure of cert.giacenterprises.com is configured to mirror that of corp.giacenterprises.com. Obviously the contents of the OU's are different, but the structure of the OU's and groups and group membership is configured to accurately model corp.giacenterprises.com

OU Design – giacdev.com

Since giacdev.com is completely isolated from the rest of the world, the Research and Development group has decided to make use of the built-in groups. All user and computer accounts need to be centrally managed. Giacdev.com does not require the complex support structure that the production and certification networks the delegation of administration is not a real issue. Beyond that, OU structure and group policy is created, changed, and reorganized as necessary depending on the direction of GIAC Enterprise's development efforts.

Group Policy Design

Overview

Group policy is an effective to tool for security and configuration management, however because group policy can be applied at multiple levels and in multiple layers, the application of group policy not only can quickly get confusing, but can also slow down logon times. GIAC Enterprises wants to avoid a group policy nightmare of a complex web of multiple policies but at the same time take advantages of the features of group policy. One way GIAC Enterprises has tried to address this issue is through OU structure. What follows is how group policy is applied via that structure.

GIAC Enterprises will use four group polices: The Default Domain Policy, the Default Domain Controller Policy, a Server Policy and a User Policy. The Default Domain Policy will be the primary policy that pushes down security configurations applicable to both servers and workstations and will only contain computer configurations. The Server Policy will contain those configurations necessary for Servers only, and will be applied only to the servers OU. The Domain Controller Policy will contain all the necessary configurations to secure the domain controllers. The User configuration portion of the Default Domain, Domain Controller and Server policy will be disabled. The User Policy will be applied to the GIACUsers OU and will contain only user configurations. The Computer Configuration portion of this policy will be disabled.

Group Policy will look exactly the same in the production and certification domains. The empty forest root domain will contain the Default Domain Policy and the Default Domain Controller policy but will not have a Server Policy or User Policy since it will only contain the domain controllers and does not contain Server or User OU's as they exist in the production and certification domains.

The giacdev.com domain will use the same Default Domain Controller configurations that are outlined for the production and certification domains below. The Default Domain Policy will contain only the password configurations outlined below. Since the giacdev.com domain is completely isolated, security is not as much of a concern as it is on the production and certification domains. Additionally, users on the giacdev.com domain are allowed much more freedom and thus their actions do not need to be controlled through group policy like they need to be on the production and certification domains.

Default Domain Policy

This policy sets computer configurations for the entire domain and contains the majority of group policy configurations user will receive.

Computer Configuration | Windows Settings | Security Settings | Account Policies | Password Policy

Password History	10
Max Password Age	60 Days
Min Password Age	5 Days
Password Length	8 Char
Password must meet complexity requirements	Enabled

These settings define the password policy for the whole domain. Because password authentication is the only method of gaining access to the network, strong passwords are an absolute necessity. These settings are designed to enforce a strong password policy. Password history is set to 10 so users are forced to cycle through ten passwords before they reuse passwords. Users are also required to change their passwords every 60 days. The minimum password age is set to 5 days to keep users from cycling through their passwords too quickly. The password length is set to eight characters and passwords are required to meet complexity requirements to harden GAIC Enterprises' systems against brute force password cracking attempts.

Computer Configuration | Windows Settings | Security Settings | Account Policies | Account Lockout Policy

Lockout Duration	30 minutes
Lockout Threshold	5 attempts
Reset Account Lockout	30 minutes

Again, these settings exist to protect against brute force password cracking attempts. Accounts will be locked out for 30 minutes after 5 failed attempts to enter a correct password. After thirty minutes, if the password is not reset, accounts will no longer be locked out.

Computer Configuration | Security Settings | Local Policies | Security Options

Additional Restrictions for anonymous connections	No access without explicit permissions

This setting is in place so no anonymous users can connect to the network. All users who connect must have a valid account on the domain.

Clear pagefile when system shuts down	Enable

This setting is in place as an added security measure and is in place primarily for GIAC Enterprises' mobile users because they have a higher risk of getting their devices stolen. However, if there were break-in and desktop devices were stolen, this policy would also add an extra layer of protection. With the pagefile

being cleared when the system shuts down, sensitive data that is contained in the pagefile is deleted and anyone who might steal a device and try to hack into the pagefile for information will not find anything.

Disable ctrl-alt-del for login	Disable

This setting is in place to keep users from setting their computers to automatically log them into the network.

Do not display last user name	Enable

This setting is in place to make life a little harder for would-be hackers. Anyone who is able to get unauthorized access to a device will also have to guess not only the password, but the user account as well. This setting is very valuable when it comes to accounts with administrative privileges and works well with the next configuration we will discuss.

Rename Administrator Account	GIACEntSUser1542

Because of their elevated level of privilege, Administrator accounts are a prime target for password cracking attempts. This setting is intended make life harder for would-be hackers by renaming the administrator account to something that is not readily obvious to someone on the outside of the organization. The "GIACEntSUser" portion of the account is intended to make the account name difficult for an outsider to guess, but not impossible for an administrator to remember. The "1542" portion of the account is intended to add an extra layer of complexity for anyone trying to guess the username.

LanManager Authentication Level	Sent NTLM v2 responses only/refuse LM

GIAC Enterprises is an all Windows 2000 shop so Kerberos Authentication will almost always be used. This setting is in place in case a need arises to attach a down level client or server to the network. GIAC Enterprises will need to make sure that if such a need arises, the down level client has DSCLient.exe loaded on it if it is a Win9x system or service pack 4 loaded if it is an NT system.

Message text for users logging on	You are about to enter GIAC Enterprises' private network. All system use is monitored. By logging on, you acknowledge and consent to the rules of this network as outlined by corporate policy.
Message Title for users attempting to logon	GIAC Enterprises' Private Network

This setting does not serve any critical security function, but is in place to remind corporate users that they are on a private network and therefore they are expected to adhere to a corporate policy and their actions will be monitored.

Secure channel: Digitally encrypt or sign secure channel data (always)	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) sessions key	Enabled

These settings are in place to provide the maximum amount of security possible for all communications between client computers and domain controllers. These settings will help protect GIAC Enterprises from both external and internal threats of anyone who might try and gather information by using packet sniffers.

Restricted Groups	Administrators Desktop Team Help Desk

Because members of these groups have an elevated level of privilege on the network, they are configured as restricted groups. Thus users are prevented from adding accounts to these groups and elevating their privileges.

Change System Time	Administrators Desktop Team Help Desk

Only the administrative groups should be allowed to change the system time. With Kerberos authentication being used on the network, it is critical that all systems are synchronized because Kerberos drops all packets that are outside its time synchronization threshold.

Load and unload device drivers	Administrators Desktop Team Help Desk

Only administrative users should be allowed to load and unload device drivers.

Shut down the system	Authenticated Users

This ensures that only users who have been authenticated can shut down a system. This setting is a safeguard in case a would-be attacker somehow gains

anonymous access to the network the attacker would not be able to shut down any systems.

Take ownership of files or other objects	Administrators Desktop Team Help Desk

This setting ensures that only administrative users can take ownership of objects and modify permissions on them.

Computer Configuration | Windows Settings | Event Logs | Settings for Event Logs

Maximum Log Size - Application Log	5120 KB
Maximum Log Size - Security Log	5120 KB
Maximum Log Size - System Log	5120 KB
Restrict Guest access to Application Log	Enable
Restrict Guest access to Security Log	Enable
Restrict Guest access to System Log	Enable
Retention Method for Application Log	Overwrite as needed
Retention Method for Security Log	Overwrite as needed
Retention Method for System Logs	Overwrite as needed

Since disk space is not generally an issue, the size of all the logs is set to 5MB and the retention method on the logs is set to overwrite as needed. These settings are in place so GIAC Enterprises has a maximum amount of information in its logs. To help protect that information, guest access to the logs is restricted.

Server Policy

Not all the settings in the default domain policy provide for the appropriate level of security for GIAC Enterprises' servers. Therefore and additional server configuration policy is applied to the servers OU. Since the servers OU inherits all the settings from the default domain policy, only those options that require a different setting or are not configured in the default domain policy are configured in the server policy. Again, the user configuration portion of this policy has been disabled to help speed up the processing of group policy.

Computer Configuration | Windows Settings | Local Policies | User Rights Assignment

Logon Locally	Domain Admins
Shut down system	Domain Admins

These configurations are set so that only domain admins can log on to the servers locally and shut down the system.

Computer Configuration | Windows Settings | Event Logs | Settings for Event Logs

Maximum Log Size - Security Log	10240KB
Retention Method for Security Log	Clear logs after 21 days

Security logs on the servers are of high importance to the server team. Thus their settings are different than found in the default domain policy. The size of the security logs is set to 10MB and data is kept for 21 days. Event logs get backed up weekly so old data is available if it is needed.

Computer Configuration | Windows Settings | Security Settings | Local Policy | Security Options

Shut down system immediately if unable to log security audits	Enabled

This setting is configured because GIAC Enterprises has placed a high level of importance on the security logs. This setting can cause a server to go down unexpectedly if the security log fills up which is why the maximum size of the security log is set to 10MB in the server policy instead of the 5MB setting in the default domain policy.

Default Domain Controller Policy

The settings in the Default Domain Controller Policy are configured to be the same as the cumulative effect of the Default Domain Policy and the Server Policy. In other words, the Default Domain Policy has all the same settings as the Default Domain Policy with exception of the configurations in the Server Policy. Again, security requirements are slightly different on Domain Controllers than they are on member servers, so there are a few additional differences. These differences are outlined below.

Computer Configuration | Windows Settings | Local Policies | User Rights Assignment

Access this computer from the network	Domain Users (Administrators are removed from this right)

"Stolen Administrator accounts can be used over the network. Removing this right from the administrator accounts forces these users to have physical access to the system in order to access resources." (SANS Institute, Securing Windows 2000 Step by Step, p. 22). This setting is set on domain controllers to make them that much harder to hack over the network.

Add workstations to the domain	Administrators Desktop Team

Only Domain Administrators and members of the Desktop support group are allowed to add workstations to a domain. Note that in the giacdev.com domain, only Administrators have this right as the Desktop Team does not support the giacdev.com domain.

Audit Policy

GIAC Enterprises has decided to address the issue of auditing on two fronts. The first front is technological – this is how auditing is set up and configured in group policy. What objects and events will be audited as well as where the logs are stored, and how long information is kept. The second front is organizational and this addresses the policies in place for reviewing the information and what is done as a result.

To help ensure the integrity of the logs and prevent tampering, all security logs are configured to write to a central location on the network. Access to this drive is granted only to the Auditing group. This ensure that there is limited access to the logs and those individual with the power on the network do not have access to the information the network records about their activities.

Basic Audit Policy Settings – These settings are applied in the Default Domain Controller Policy and Server Policy and are also set on all servers in the DMZ. Audit settings are not applied to workstations because it would generate too much information for the auditing group to reasonably handle, thus these settings are not configured in the Default Domain Policy. Instead, GAIC Enterprises will focus on auditing the use of its server infrastructure.

Computer Configuration | Windows Settings | Security Settings | Local Policies | Audit Policy

Event Category	Success	Failure
Audit Account Logon Events	X	X
Audit Account Management	X	X
Audit Directory Service Access		X
Audit Logon Events	X	X
Audit Object Access		X
Audit Policy Change	X	X
Audit Privilege use		X
Audit System Events		X

Audit Account Logon Events: These events are audited for two reasons, first success events are audited so a record of what accounts logged on and when

can be kept. Failure events are audited because they can be an indication of attempted break-ins.

Audit Account Management: These events are audited again for record keeping purposes so management can tell when privileges on accounts were changed and failures are audited because they can indicate an attempted attack on the system.

Audit Directory Service Access: Failures of this type of event are audited again because they can indicate an attack on the system. Success events are not audited because the amount of data generated from this would be too much to be meaningful.

Audit Logon Events: Again auditing success and failure of these events serves two purposes. Success events generate a record of who/what was logged on and when, and failures can indicate an attempted attack on the system.

Audit Object Access: Only failures of this type of event are audited because they can indicate an attack on the system. Like directory service access, if successes were audited, the amount of information generated would be too much to be meaningful.

Audit Policy Change: Success events are audited to generate a record of changes on the system and failure events are audited for the purposes of intrusion detection.

Audit Privilege Use: Failure events are audited for intrusion detections purposes. Success events could be audited for record keeping purposes, but again information overflow can result in critical information being missed. Since account management is audited and logon events are already audited for record keeping purposes, the risks associated with not auditing privilege use success events are mitigated.

Audit System Events: Again only failures of System Events are audited for intrusion detection purposes. If success events were audited, the amount of data generated would be too much to provide any meaning.

Currently, GIAC Enterprises does not have any host based intrusion detection software implemented and this can pose a potentially serious problem. While Windows 2000 provides the infrastructure necessary to audit important system events, intrusion detection software makes the management of all the information generated from auditing much easier by further organizing the data and providing an automated system of alerting the necessary parties of potential break-ins. Once the network infrastructure has been upgraded to Windows 2000 GIAC Enterprises will evaluate current intrusion detection systems on the market and implement a solution.

Since system administrators have the highest level of privilege on the network, then it is imperative that whomever is doing the auditing not be a member the systems administrators group. (Cox & Sheldon, Windows 2000 Security Handbook, p. 397). Thus auditing is it's own separate division within IT. Separating auditing into its own function also serves another purpose: it helps to ensure that audit logs are reviewed daily. A person who's primary job function is to review and manage security logs is naturally going to be in a position to pay attention to the logs, notice important security alarms, and act on those alarms in a timely manner that a system administrator who is also responsible for managing disk space, installing service packs, troubleshooting network problems and doing any one of a number of other tasks.

Finally, the audit policies themselves are proactively reviewed biannually to assess their effectiveness and implement any changes/improvements in policy. Additionally, policies are also reviewed after any security breaches or incidents to determine where the failure was and implement the necessary corrective action. This combination of proactive and reactive measures will ensure that as the company grows and changes, audit policy will adapt to meet GIAC Enterprises' needs.

User Configuration Policy

This policy is applied to the GIAC Enterprises Users at the OU level. The function of these settings is to limit user access to administrative tools. Only a few configurations have been made here. GIAC Enterprises wants to limit the use of administrative tools by its users, but at the same time does not want to limit its users to the point where they can't do their jobs.

User Configuration | Windows Components | Administrative Template | MMC

Restrict Users from entering author mode	Enable
Restrict users to the explicitly permitted use of snap-ins	Disk Management Event Viewer Performance

These settings are intended to restrict user access to MMC's. These settings primarily protect GIAC Enterprises from its internal users. With access to the majority of mmc snap-ins restricted, there is less chance of the average user intentionally or accidentally causing harm to their device or the network.

User Configuration | Windows Components | Administrative Templates | Start Menu & Tool Bar

Disable & Remove links to Windows	Enable

Update	

While it is always nice to see users that desire to have their systems up to date with the most recent patches, GIAC Enterprises does not want to get its users in the habit of pulling their patches down from windows update individually. Furthermore, since users are prevented from installing software on their local machines, windows update would not be very helpful anyway. Instead GIAC Enterprises pushes out hot fixes, service packs and programs via SMS.

User Configuration | Windows Components | Administrative Templates | Control Panel

Hide Specified Control Panel Applets	Add/Remove Hardware Add/Remove Programs Administrative Tools Internet Options System

GIAC Enterprises wants to prevent users from installing unauthorized programs and hardware. Hiding the administrative tools applet works in conjunction with restricting the use of mmc's policy outlined above. Also GIAC Enterprises does not want users to change their Internet options or modify information in the system applet. GIAC Enterprises also uses permissions and group membership to help prevent unauthorized access, however these setting add an extra layer of security by hiding certain options from the user.

User Configuration | Windows Components | Administrative Templates | Add/Remove Programs

Disable Add/Remove Programs	Enable

Again this setting is intended to enforce the policy that users are not allowed to add any unauthorized software to their devices.

Conclusion

Security naturally brings with it an extra layer of complexity to network management as well as a certain level of inconvenience for users. For these reasons, security cannot truly be enforced unless it has buyoff from the highest levels of management and is part of the corporate culture. GIAC Enterprises has won half the battle here, because upper management has determined that they need to make security on their network a priority. Thus they are committed to providing the monetary and human capital necessary to properly implement an effective security strategy. An example of this commitment is creation of a new position devoted primarily to auditing. Which brings up another key point: network security goes beyond just implementing technology. Organizational structure, policies and procedures must also be in place to support that technology and use the information generated by it appropriately.

Because GIAC Enterprises has never really enforced a strict security policy, their most significant challenges will likely be twofold. First, they have to understand the ramifications of what they just implemented. There is now an extra layer of complexity when troubleshooting network issues and security policies now need to be taken into consideration during the day-to-day administration of the network. The IT staff must have a thorough understanding of these policies and how they affect their day-to-day tasks. This issue is why GIAC Enterprises delayed implementing an intrusion detection system until after the upgrade is complete. Once the infrastructure is in place and GIAC Enterprises understands the issues surrounding the new infrastructure, they will be in a better position to implement an effective solution. Second, GIAC Enterprises is likely to see significant pushback from their users. Many users will not have the freedom on their machines that they used to have and of those users, a few will most likely try and circumvent security in some way. The pain from this can be alleviated mostly through communication. Communication about the changes in security policy in the Windows 2000 environment needs to come from upper management well in advance of the actual implementation of Windows 2000. The rationale behind these security changes should be clearly communicated to the user community. The Auditing and Research team should also provide regular security updates, such as information about new viruses, to the user community. These efforts to educate the user community on the security policy itself and the reason's behind it will help create a culture of security conscious users.

As we can see, there is no magic bullet for security. The best way to describe any effective security strategy is "defense in depth." We can clearly see that group policy by itself will not make your network secure, nor will simply just keeping up to date on your hot fixes and service packs. The best solution is a multi-dimensional strategy that is implemented in layers and is reviewed on a regular basis to assess its effectiveness. A security strategy should include not only technological and physical solutions such as firewalls, permissions, OS

configurations, a secure data center, etc, but should also include organizational policies and structure, as well as political and financial backing from upper management. A security strategy is most effective only when all these different pieces work together.

References

1. Securing Windows 2000 Step by Step. Version 1.5. SANS Institute, July 1, 2001.

2. Anthes, Mary A. "A Secure Windows 2000 Infrastructure Design." September 26, 2001. URL: http://www.sans.org/y2k/practical/Mary_Anthes_GCNT.zip (December 26, 2001)

3. Lewis, Brett. "Security Considerations for Windows 2000 Infrastructure Design." December 11, 2001. URL: http://www.giac.org/practical/Brett_Lewis_GCNT.doc (December 26, 2001)

4. Fossen, Jason. "Securing Windows 2000." GIAC training course from San Diego SANS, 2001.

5. Fossen, Jason. "Securing Internet Information Server 5.0." SANS Institute: 2001.

6. Cox, Philip and Tom Sheldon. Windows 2000 Security Handbook. Berkeley, CA: Osborne/McGraw-Hill. 2001.

7. Fullerton, Sean and James Hudson. Using Microsoft Active Directory. Indianapolis, IN: Que. 2001.

8. Windows 2000 Server Resource Kit. Supplement 1. Redmond: Microsoft Press, 2001.

Last Updated: September 25th, 2017

Upcoming Training

Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**