Global Information Assurance Certification Paper

A Secure Windows 2000 Infrastructure

GCWN
Practical Assignment Version 3.1

Option 1

Submitted by: Dan Bozicevich
October 21, 2002

Table of Contents

Section 1 – Overview of GIAC Enterprises

GIAC Enterprises is an e-commerce retailer of pumpkins and pumpkin related goods. The company is located in St. Paul, Minnesota and has 135 employees. GIAC Enterprises has one online application that interfaces with customers and business partners.

GIAC Enterprises target customer base is the residential consumer that is looking to fulfill their annual pumpkin needs for the Halloween season. In addition to selling pumpkins directly, GIAC Enterprises sells pumpkin seeds, fertilizers, vine ties, garden tools and other accessories that are targeted at the small residential pumpkin grower.

The R&D department of GIAC Enterprises focuses on seed development. Striving to create the best seed to achieve the ultimate in size, shape and color is the goal of the R&D department. Seed development is deemed crucial to the success of GIAC Enterprises and therefore the security of the R&D department is taken very seriously by management.

While GIAC Enterprises does much research surrounding seed development and sells what may be considered farm or garden related goods, it does not reside on a rolling pasture. GIAC Enterprises maintains two small facilities. One is located in downtown St. Paul, Minnesota while the second is across the Mississippi river adjacent to the downtown.

The supply of pumpkins and related goods that GIAC Enterprises sells comes from local farmers and manufacturers. Seed development is done on-site, but the knowledge is transferred to local farmers who have partnership relationships with GIAC Enterprises.

GIAC Enterprises has other departments that support the organization including, sales, finance, human resources, administration, I/T and marketing.

Section 2 – Network Design and Diagram

Network Overview

The GIAC Enterprises network consists of two physical sites. The first is the main office. This is where the employees of GIAC Enterprises report for work and where the corporate services are located. The network services at this site include file, print, messaging and directory services to support the R&D department, finance, HR, marketing, administration, I/T and sales. The second site is the e-commerce site. This site includes all of the equipment necessary to run the e-commerce application that is the underpinning of GIAC Enterprises. The network design is based around three primary goals; security, performance and redundancy.

The Internet circuits are not dedicated circuits to each site, but rather to the Internet to save money. To provide secure communications between the two sites, there is an IPSEC VPN tunnel setup between them. This IPSEC VPN tunnel is built between the Cisco PIX firewalls.

GIAC Enterprises decided to house their e-commerce infrastructure out of a physically separate facility than their main office site for several reasons. First, the main office site is located on the south bank of the Mississippi river in St. Paul, Minnesota across from the downtown which sits high on the opposing bluffs. Geographically, the office is located in a flood prone area. Second, because of market conditions created by several companies leaving the downtown area, pre-existing datacenter floor space could be found for lease relatively cheaply. It was decided that because of these two factors that a separate site would be leased for the e-commerce hardware. GIAC Enterprises decided not to move all employees to this location as the parking costs for employees was deemed as not 'employee friendly'. Because of these reasons, GIAC Enterprises operates two separate facilities.

Network Design Diagram

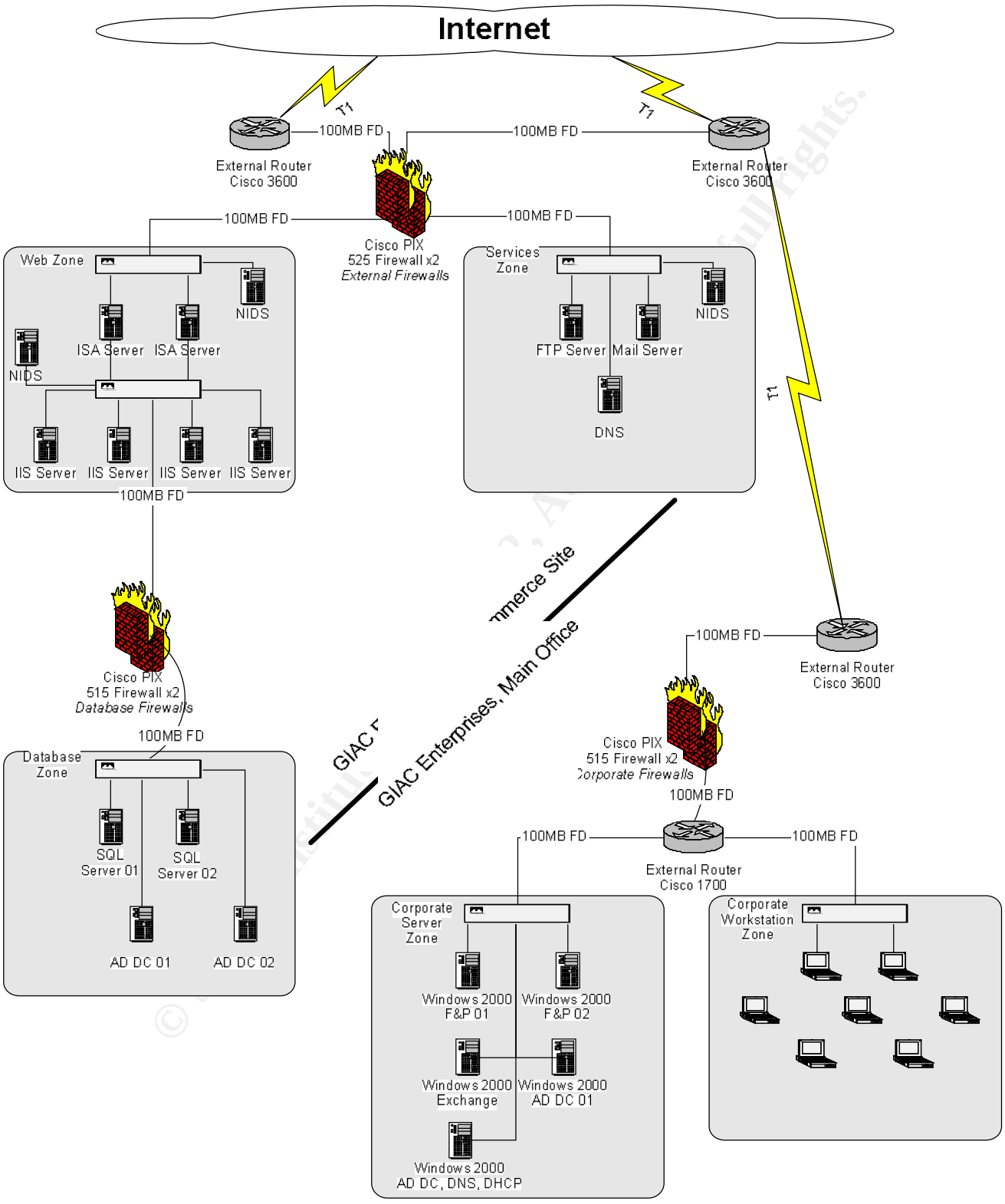


Diagram 1

Network Detail

E-Commerce Site

The e-commerce site at GIAC Enterprises is connected to the Internet via redundant T1 lines. Each of these T1 lines are connected to physically separate Cisco 3600 routers. These routers are configured with External Border Gateway Protocol (EBGP) as the connections are to independent ISPs.

The external firewall layer of GIAC Enterprises is based on a redundant pair of Cisco PIX 525s. These PIX firewalls provide for eight network interfaces, of which, six are used with redundant connections to three distinct zones. The distinct zones are; external zone, web zone, and the services zone.

The database firewall layer of GIAC Enterprises is also based on redundant Cisco PIX hardware, the 515s. The decision to use an extra set of firewalls to protect the Database Zone was based on the notion of defense in depth whereby you plan your security around the idea that the previous layer of security has failed. The database firewalls provide the database zone an extra layer of protection and are based on the assumption that the ISA and/or IIS servers have been compromised. These Cisco PIX 515s have their 'external' interface connected to the web zone while their 'internal' interface is connected to the database zone.

All servers in the e-commerce site are configured according to the checklists provided by SANS and the NSA which includes but is not limited to removing unneeded services, applying the latest service packs and hot fixes, and renaming administrative accounts.

External Zone

The external zone is comprised only of the external Cisco 3600 routers.

Web Zone

The web zone is comprised of Microsoft ISA server and Microsoft IIS server. TCP ports 80 and 443 are the only allowed ports to traverse the external firewall from the external zone to the web zone. All servers in this zone have a complete backup run on them weekly or as needed when there are application changes. Every time a new version of the application is placed onto these servers, a full backup is taken. Backups for the e-commerce site are stored at an offsite storage company that specifically handles data backups. This offsite storage scheme is applicable to all zones within GIAC Enterprises.

ISA Server

The purpose of the ISA server is to handle the SSL offload, layer 7 content filtering, load balancing and reverse proxy. The public interfaces of the ISA servers have fully routable addresses and are responsible for responding to all http and https requests. The URL for GIAC Enterprises

(http://www.bogusurl.com) resolves to the public interfaces of these servers. The ISA server cluster is the demarcation point for SSL encrypted traffic into the GIAC Enterprises e-commerce site and as such, the servers are configured with SSL offload cards to reduce the CPU load on the servers. There are two ISA servers configured as a cluster with network load balancing (NLB) running on the public interfaces of these devices. The ISA server cluster is multi-homed and has non-routable addresses on the private side of the cluster. The ISA server clusters are built for speed and redundancy. The redundancy is maintained by the cluster. The speed is maintained by utilizing IBM x335 series servers running RAID 0. The servers all run service pack 3 and are kept up-to-date on service packs and hot fixes by using an internal Windows Automatic Update server.

IIS Server

The IIS servers in the web zone are the web and application servers for the main e-commerce application. These servers are single-homed and are not directly accessible from the Internet. These servers are published via the web-publishing services in ISA. These servers all run Windows 2000 Server on the IBM x335 series servers. As these servers contain business logic, they run RAID1 for data protection; however, the servers are also in a web farm so a loss of a single server does not mean a loss to business critical data. These servers run service pack 3 and are kept up-to-date using an internal Windows Automatic Update server.

Network Intrusion Detection System

As this is the primary zone for commerce and thus attacks on GIAC Enterprises network, network intrusion detection systems are run in this zone. SNORT is the tool of choice for GIAC Enterprises. SNORT version 1.8.7 runs on a Sun LX50 server and is actively monitoring all traffic that enters the web zone.

Services Zone

The services zone consists of three devices that serve the e-commerce application. There is a public ftp server, mail server and DNS server. All servers in this zone run service pack 3 and are kept up-to-date using an internal Windows Automatic Update server. Weekly full backups are performed on these servers with daily incremental backups. The security configuration of the servers are maintained by Group Policy Objects within the external Active Directory forest. These GPOs will be described in more depth in Section 4.

DNS Server

The DNS server is an Active Directory DNS server which is maintained via the external forest of GIAC Enterprises. This DNS server provides name resolution for devices in the services and web zones. DNS for the database zone is not published to the Internet.

FTP Server

The public ftp server for GIAC Enterprises is used for downloading of pumpkin planting guides, seed charts and pumpkin history stories in PDF format. The purpose of having these downloads on a public ftp server instead of on the IIS servers that support the online sales application is to reduce load on the revenue generating portions of the network. This public ftp server is an IIS 5.0 server.

Mail Server

Exchange 2000 is the public mail server GIAC Enterprises. The purpose of this mail server is to handle outgoing mail traffic from the online application to be sent to GIAC Enterprises customers. Upon a successful sale or registration for more information, the application uses this mail server to send SMTP messages to the customers or potential customers.

Network Intrusion Detection System

Again, this is a primary zone for commerce and thus attacks on GIAC Enterprises network, network intrusion detection systems are run in this zone. SNORT is the tool of choice for GIAC Enterprises. SNORT version 1.8.7 runs on a Sun LX50 server and is actively monitoring all traffic that enters the web zone.

Database Zone

The database zone is separated from the web zone via a pair of Cisco 515 PIX firewalls. As data is the lifeblood of any modern organization, significant steps have been taken to ensure the security of the data. This includes customer and application data in Microsoft SQL servers as well as customer and network data in the external forest of Active Directory. These servers have nightly full backups as the data is highly dynamic and crucial to the success of GIAC Enterprises.

Active Directory Domain Controllers

There are two Active Directory Domain Controllers (AD DC) in the database zone. These AD DCs provide the home for customer profiles, external DNS entries and Group Policy Objects. In addition, the ISA servers in the web zone have their configurations maintained by Active Directory. The second domain controller (AD DC 02 in Diagram 1) also runs the Windows Automatic Update service. This server is then responsible for distribution of service packs and hot fixes to the rest of the servers in the e-commerce site. The Active Directory domain controllers are run on IBM x335 series servers running RAID 5 for maximum data protection.

SQL Servers

The Microsoft SQL servers provide the relational database needs to GIAC Enterprises. These servers run a multiple Microsoft SQL instances to support the online application. SQL is not run on TCP port 1433, but rather have been moved to an undisclosed “high port” as an added measure of protection. IBM x360 series servers with four Xeon processors and 4 GB of RAM provide the

horsepower to this Windows 2000 Server. RAID 5 is used on these two servers to provide maximum data protection.

Main Office Site

According to the FBI, the majority of attacks against a corporation's network infrastructure come from inside the firewall. For this reason, all servers in the main office site are configured according to the checklists provided by SANS and the NSA which includes but is not limited to removing unneeded services, applying the latest service packs and hot fixes, and renaming administrative accounts.

Corporate Server Zone

The corporate server zone is a secure location for the internal Active Directory forest, file, print, database and messaging services for the employees of GIAC Enterprises. As stated in the overview, the R&D department does seed research and management takes very seriously the security of that research. All servers in this zone run service pack 3 for Windows 2000 and are kept up-to-date by a Windows Automatic Update server which is maintained by one of the Active Directory Domain Controllers. Weekly full backups are run on all servers in the corporate server zone and utilize off site storage in a secured vault for data protection.

Active Directory Domain Controller, DNS & DHCP Server

As there are only 135 employees of GIAC Enterprises, there are only two Active Directory Domain Controllers for the internal forest. Both of these domain controllers are DNS and DHCP servers for the corporate server and corporate workstation zone. The corporate servers do not utilize the DHCP functionality but rather have static IP addresses assigned to them. These servers run the IBM x335 series server with dual Xeon processors and utilize RAID 5 for maximum data protection. These servers have EFS enabled to secure their data and also utilize secure DDNS updates for workstations registering themselves. One of these servers is also designated as the Windows Automatic Update server and provides service packs and hot fixes to the servers in the corporate server zone and the corporate workstation zone.

Windows 2000 File and Print Server

The Windows 2000 file and print services are maintained on an IBM x345 series server to accommodate significant file storage and processing power for EFS. The server has 72GB of RAID 1 disk capacity to all departments except for the R&D department. The R&D department has an independent 72GB of disk space utilizing RAID5. As these servers are file servers, the latest McAfee anti-virus software is run on them. In addition, these servers are DAT file distribution servers for the corporate workstation zone. DAT files are updated utilizing McAfee's automatic updates.

Microsoft Exchange Server

Exchange 2000 running on Windows 2000 supported by an IBM x335 series server comprises the internal mail infrastructure for GIAC Enterprises. This server follows the same model as other servers for offsite backups. The GPOs for this server are outlined in Section 4.

Microsoft SQL Server

The SQL server in the corporate server zone is used solely by the R&D department. The R&D department has several seed development databases that are deemed vital to the success of the organization and as such, it has strict permissions from an Active Directory point of view. It does not need the horsepower that the SQL servers in the database zone have, so it is run on an IBM x345 series server running RAID 5.

Corporate Workstation Zone

The corporate workstation zone is comprised of 135 Windows XP Professional and Windows 2000 Professional workstations. These workstations all run McAfee anti-virus software and receive automatic DAT file updates from the DAT file distribution server located in the corporate server zone. The workstations also run the Windows Automatic Update service and receive their updates from the Windows Automatic Update Server which is located on a domain controller in the corporate server zone.

All workstations have their local My Documents folder redirected to shared file servers to ensure that local data is properly backed up. Workstations in the R&D department utilize EFS to further protect the files on their workstations. All workstations are subject to the password policies which are outlined in Section 4.

Section 3 – Active Directory Design and Diagram

Overview

The Active Directory layout for GIAC Enterprises is designed around two single domain forests that have a one way trust between them. The external forest trusts the internal forest. There is an external forest that houses customer profile information, GPOs for servers at the e-commerce site and is a home for future application development opportunities. The internal forest contains all employees of GIAC Enterprises, servers, workstations and GPOs.

GIAC Enterprises decided on dual single domain forests for several reasons. The first major internal debate was whether or not to actually create a forest for external computers and users. This decision came after much debate on the pros and cons of such a forest, but ultimately it was decided to do so. The primary reason in favor of creating the external forest was to house customer login accounts. One of the requirements for the online application was to maintain customer profile information. This is an ideal use of Active Directory. External customer web application logins are processed via IIS 5.0 which uses the external Active Directory forest as its user repository. In addition, being able to leverage Active Directory for management of devices in this forest greatly reduces the administrative overhead.

GIAC Enterprises did discuss the adoption of a dual domain, single forest model for its Active Directory layout and use the Sites & Services features of Active Directory to minimize replication traffic. This design was not adopted for several reasons.

First, there are multiple security concerns. The main one being that a compromise of user accounts in one domain could easily lead to a compromise of user accounts in the other domain. From there, an attacker could easily use GIAC Enterprises computers for Denial of Service attacks, deface our website or steal our data.

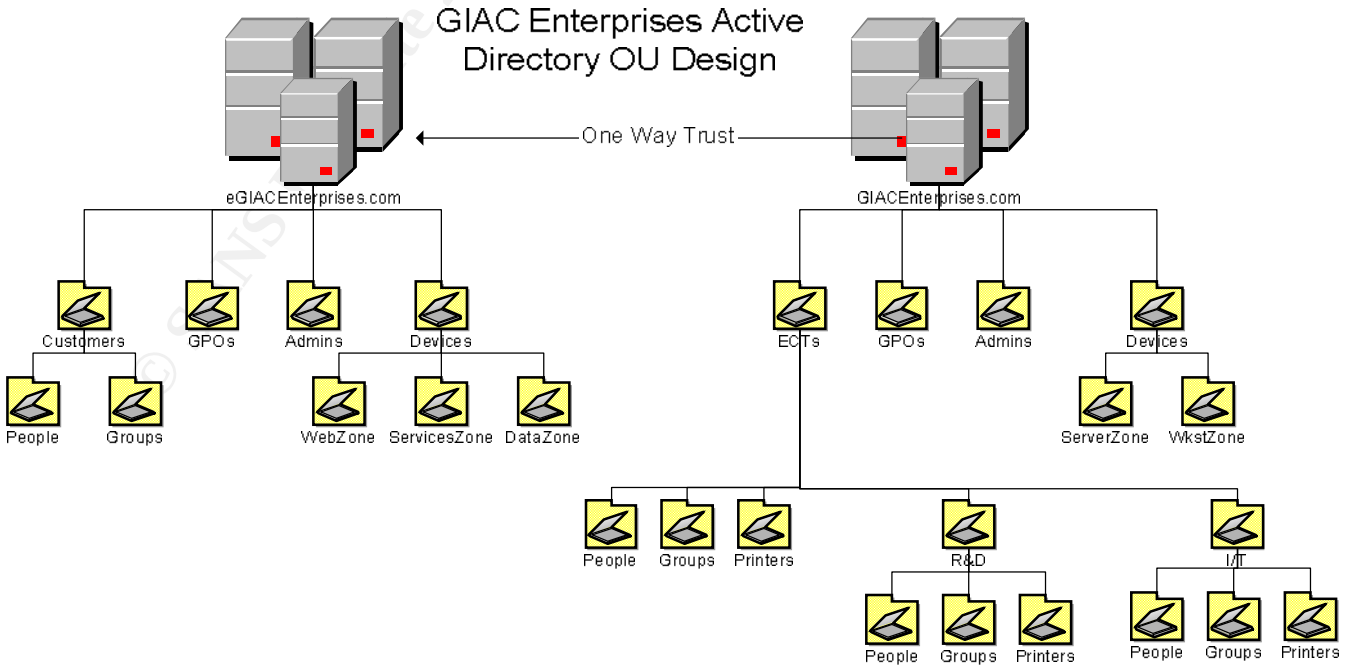
Second, there is the issue of scalability. As GIAC Enterprises' online application grows and is enhanced, the corporate direction is to leverage Active Directory whenever possible for user profile information. Because of this, this forest is to be as lean and fast as possible. The OU structure was kept relatively flat to improve performance and it is possible that future application changes could require schema modifications to hold special purpose data for the application. This was a major concern. The current release of Active Directory supports schema extensions, but there are limitations. Schema changes are one-way only. While schema changes should never be taken lightly and planned thoroughly with any directory service, this is especially true because of this

'feature' of Active Directory. The only way to back out a schema change is to restore Active Directory from tape.

In looking ahead to Windows .Net Server 2003 and the changes that are being made to Active Directory, the directory service is being made much more flexible than Active Directory for Windows 2000. GIAC Enterprises does want to research the possibility of using Active Directory in Application Mode (ADAM) as its directory service for external user authentication to the web application when it becomes available. It is very possible that the directory services architecture could be significantly overhauled at GIAC Enterprises within the next 18 months to support ADAM. Although this forest is already existent, Microsoft suggests that corporations looking to deploy Active Directory in the next year for an e-commerce purpose wait and do so with ADAM. There are several possibilities, namely to have the current corporate forest be a single domain, multi-site forest that would contain all servers and internal users. The external ADAM forest would contain only external customer account information. While not fully researched by GIAC Enterprises, this decoupling of Active Directory from the underlying operating system is believed to be good by several market journals (LDAPGuru Article and ENTMag Article) and will be followed closely by GIAC Enterprises staff.

Active Directory OU Design

Diagram



Structure Details

GIAC Enterprises is predominately a centrally managed organization. With this, the OU structure was designed primarily around the implementation of Group Policy Objects. Thought was given to delegation of control and this is seen in the user structure within the GIACEnterprises.com domain. GIAC Enterprises decided on two single domain forests for the purposes of security, administration and performance. Users and devices are first separated logically and physically with the distinction of external vs. internal. There are internal corporate policies for changing of passwords, security settings, etc. that don't necessarily apply to the external customer. For example, GIAC Enterprises has a password change policy of every 45 days. It is unrealistic to think that external customers will change their passwords this often. By creating different forests, with a one-way explicit trust from the internal to external forest whereby the external forest trusts the internal forest and a compromise of the external forest does not necessarily mean a compromise of internal data. In addition, GIAC Enterprises was looking to minimize the amount of replication traffic that traverses over the VPN tunnel connecting the e-commerce site and the main office site.

eGIACEnterprises.com

The eGIACEnterprises.com domain was created for the external or e-commerce site at GIAC Enterprises. It contains objects that are related to the e-commerce business of GIAC Enterprises including users, groups, group policy objects and servers.

In addition to the default containers, there are several OUs added to the Active Directory structure. The default containers are not used in GIAC Enterprises as they present both a security risk and they do meet the needs of GIAC Enterprises. Potential attackers know these default containers and objects within them. By not using those objects, GIAC Enterprises has removed a potential vulnerability. Default objects within the default containers have been either moved, renamed, deleted or disabled depending on the object type. eGIACEnterprises.com is a single site forest with a one way trust to it from GIACEnterprises.com.

The primary purpose of this forest is to house external customer profile information. With this in mind, the OU structure is relatively flat, having only two layers from the rootDSE to the People container. This flat structure is deemed the best fit for GIAC Enterprises as a deeper OU structure would decrease performance and frankly, there's minimal need for any other structure. All of the external users are either self-administered or administered by the I/T department of GIAC Enterprises. There is no need for delegation of control or separation of external users by OU. Generally speaking, there are two reasons to create OUs within Active Directory (which is not necessarily true in other directory services) which are to delegate control or have a different GPO.

The security design of this forest is such that only Windows 2000 or Windows XP are the only Windows computers allowed on the network. Windows 95, 98 and ME are not supported on the network. This is shown in figures 2 and 3 below as the Everyone group is not a member of the Pre-windows 2000 Compatible Access security group.

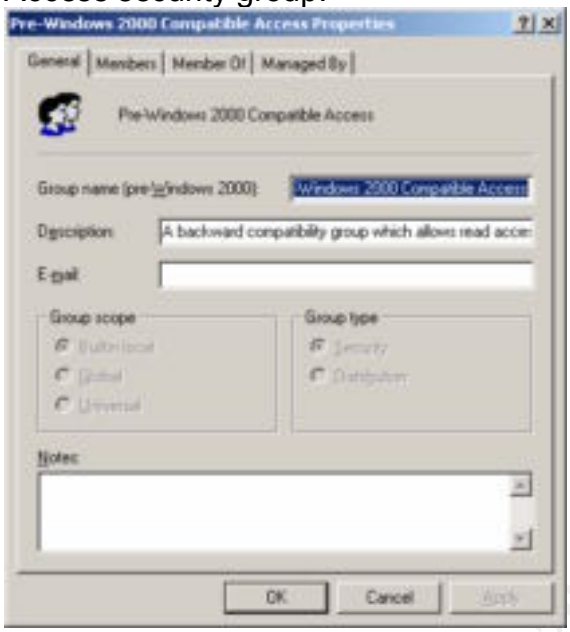


Figure 2

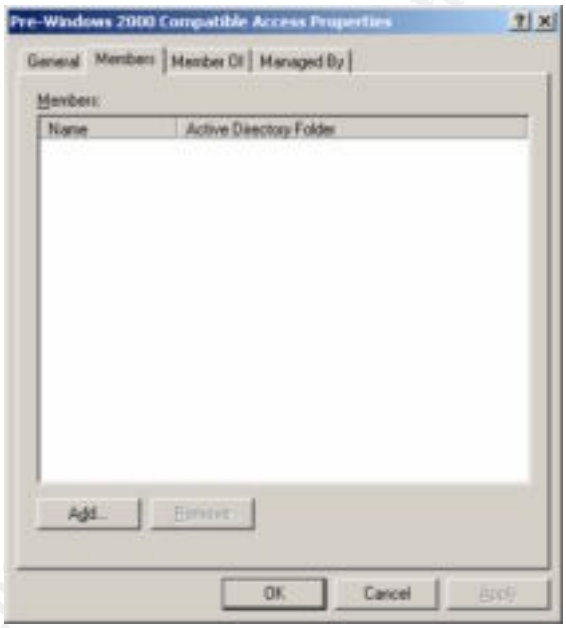


Figure 3

Also, the eGIACEnteprises.com forest is a Native mode forest. All servers are Windows 2000 and all workstations are either Windows 2000 or Windows XP. There is no need for backward compatibility with NT 4.0 and NetBIOS is disabled on the network interfaces. Figure 4 below shows the domain controller mode.

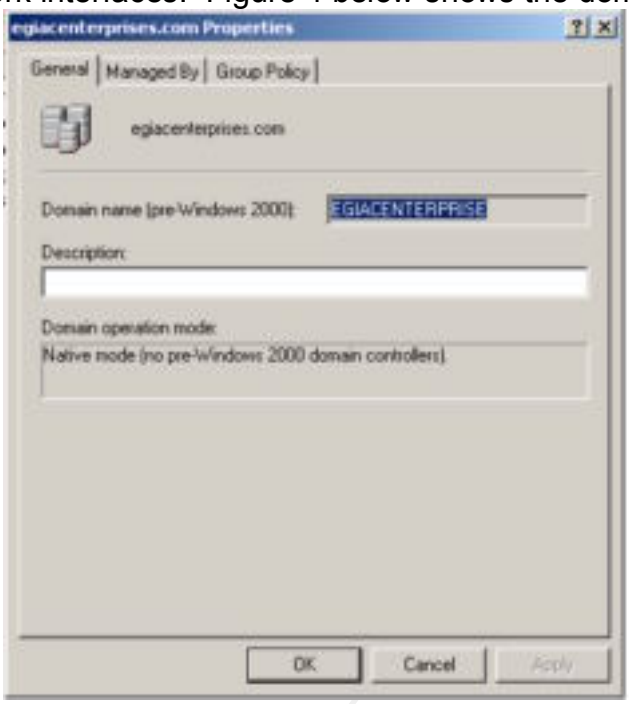


Figure 4

As the forest only has two domain controllers, the split for FSMO (Flexible Single Master Operations) roles is relatively benign. ADDC01 is both the PDC Emulator Master and the RID Master. In addition, ADDC01 is a global catalog server. ADDC02 is the Infrastructure Master, Domain Naming Master and Schema Master. ADDC02 is also a global catalog server which is defined as a best practice by the SANS Institute to have the Domain Naming Master a global catalog server. Typically, the Infrastructure Master is not a global catalog server because of problems where the Infrastructure Master will not find bad references, but this is only in a multi-domain forest. With eGIACEnterprises.com being a single domain forest, this is not an issue. Figure 5 below shows the FSMO Roles for ADDC01.egiacenterprises.com.

Figure 5

ou=GPOs, dc=eGIACEnterprises, dc=com

This organizational unit was added for placement of all Group Policy Objects within this domain. With Group Policy Objects being separate objects and not properties or attributes of other objects, their effectiveness is not reliant upon their placement within the directory tree. Group Policy Objects are enacted by simply "linking" them to other objects. For this reason, by placing Group Policy Objects in their own container, they can be easily managed. Permissions on this container are restricted to administrators only and therefore the security of the objects is increased. By default, when you create a Group Policy Object for an organizational unit, it is created in that organizational unit. In the case of external customers, the Group Policy Objects would be located in the same container as the user objects. This would violate a basic directory design principle of distributing permissions and security from a place higher in the tree than the object receiving the permission. By placing the Group Policy Objects in a

different container, they can be applied to one to many other containers and are not thought of as a Group Policy Object for a particular organizational unit. The only exception to this within the domain is the Group Policy Object for the GPO container. This GPO is located directly under the eGIACEnterprises.com domain component of the tree so as to not violate the principle of security from a location higher in the tree.

ou=Customers, dc=eGIACEnterprises, dc=com

The only purpose of this container is to add structure to the Active Directory. It contains only two objects (organizational units) which are listed below. No other objects are allowed to be created under this organizational unit.

ou=People, ou=Customers, dc=eGIACEnterprises, dc=com

This organizational unit was added to house the external customers of GIAC Enterprises. User objects are the only permissible objects within this container and only user objects for external customers. The exception to this is several test accounts for testing of the application. These accounts are disabled until needed and then are immediately disabled again when done being used. Users in this container have limited access to their own object and are allowed to update their own personal information and password through the application only. They are not allowed to modify permissions to their own object or any other object within the Active Directory forest.

ou=Groups, ou=Customers, dc=eGIACEnterprises, dc=com

This organizational unit was created to house the groups that are associated with the users in the people container. Group objects are the only objects that are permitted to be created in this container. There are a limited number of groups in this container as most groups contain most users. Because of the Active Directory limit of 5,000 users per group, group nesting is required for the online application. Group naming standards for this domain are such that the differentiating character is a numeral at the end of the object name which defines if it is a nested group or not. For example, a “1” or “2” at the end of a group name defines it to be the first and second nested groups, respectively. The decision to place groups into a separate organizational unit than the users was done for the same reason as placing GPOs into a different container than where they are being used. The basic directory design principle of gaining rights through objects above or outside of the container in which you reside. In this case, authorization to the online application is granted through one or more group memberships depending on which part(s) of the application the user may have access to. In addition, authorization to certain portions of the SQL servers is granted via group membership. If these groups were in the same container as the users, a compromise of users in that container does not necessarily lead to a compromise of the Groups container.

ou=Admins, dc=eGIACEnterprises, dc=com

The Admins organizational unit was created for the purposes of holding the local administrative accounts. As stated before, GIAC Enterprises is a centrally

managed organization. However, local accounts are maintained for purposes of disaster recovery or network problems. Primary administration is via administrative accounts located in the GIACEnterprises.com domain and thus one of the primary reasons for the trust relationship between the two forests. By having this trust relationship, the users in this container are not used except in the cases stated above (disaster recovery or network issues) and as such are audited appropriately. Users in this container are audited for successful and failed login attempts as can be seen in the GPO that is assigned to this container. In most corporations, successful logins are not audited. In this scenario, they are because administrators' primary accounts are located in the GIACEnterprises.com forest and the accounts located in this Admins container are not be used on a day in and day out basis.

ou=Devices, dc=eGIACEnterprises, dc=com
This container was built with the same intentions as the Customers organizational unit. It is a merely an organizational unit that provides structure. It contains only three objects (organizational units) which are listed below. No other objects are allowed to be created until this organizational unit.

ou=WebZone, ou=Devices, dc=eGIACEnterprises, dc=com
The Webzone organizational unit contains all devices that are located in the Web Zone on the physical network. This includes the ISA and IIS servers in addition to their administrative accounts such as the IUSR_* accounts. Normally speaking, the IUSR_* accounts would be located in the default users container which is located at the first level under eGIACEnterprises.com. However, GIAC Enterprises has elected to not use these default containers as it poses a security risk. Potential attackers know that this container exists and that these administrative and other default accounts generally reside within them. By moving them, it raises the difficulty level of them being attacked. This same scenario and line of thinking is repeated throughout the design of GIAC Enterprises network and Active Directory structure.

ou=ServicesZone, ou=Devices, dc=eGIACEnterprises, dc=com
The Services Zone organizational unit contains all devices that are located in the Services Zone on the physical network. This includes two IIS servers (acting as a public ftp server and one that also acts as a mail server) as well as a Windows 2000 DNS server. The mail server is Exchange 2000.

ou=DataZone, ou=Devices, dc=eGIACEnterprises, dc=com
The Data Zone organizational unit contains all devices that are located in the Data Zone on the physical network. This includes the domain controllers (moved from the Domain Controllers organizational unit) and the Microsoft SQL servers. The domain controllers were moved from the default Domain Controllers OU to increase the security by adding a layer of obfuscation to their location. Attackers know the default location of objects within a domain. While there are no known specific exploits today regarding the Domain Controllers OU, best practice dictates that you use the least amount of default privileges and locations as

possible. This is analogous to running SQL servers on a port other than 1433 (their default) to obfuscate their location from tools such as *sqlping*. While there certainly are differences between object placement in a directory service and services running on a server, the principle is the same.

GIACEnterprises.com

The GIACEnterprises.com domain was created for the internal or main office site at GIAC Enterprises. It contains objects that are in support of the e-commerce site but are related to corporate functions such as HR and finance. Objects within this domain include users, printers, servers, groups, workstations and group policy objects.

Just as in the eGIACEnterprises.com domain, there are several OUs added to the Active Directory structure. The default containers are not used in GIAC Enterprises as they present both a security risk and they do not meet the needs of GIAC Enterprises. According to the FBI, most attacks are from the inside of the firewall, not outside. For this reason, GIAC Enterprises follows the same stringent security model for the corporate offices as the e-commerce site. Potential attackers know these default containers and objects within them. By not using those objects, GIAC Enterprises has removed a potential vulnerability. Default objects within the default containers have been either moved, deleted or disabled depending on the object type. GIACEnterprises.com is a single site forest with a one way trust to eGIACEnterprises.com whereby eGIACEnteprises.com trusts GIACEnterprises.com.

ou=ECTs, dc=GIACEnterprises, dc=com

The Employees, Contractors and Temporaries (ECTs) organizational unit is an organizational unit of structure. This means, its purpose is to be a placeholder for each of the individual departmental organizational units. No objects other than the departmental organizational units are permitted to exist as child objects to this container. As the name implies, the child objects within this container are the organizational units in which employee, contractors and temporary employees' user accounts reside. Consideration was given to creating separate People organizational units for each of these types of accounts to apply different GPOs, but it was decided that the cost of administration and complexity outweighed the need for different policy objects.

ou=People, ou=Departments, dc=GIACEnterprises, dc=com
ou=Groups, ou=Departments, dc=GIACEnterprises, dc=com
ou=Printers, ou=Departments, dc=GIACEnterprises, dc=com
The above three containers hold the objects for people, groups and printers in the GIAC Enterprises domain. While this is not all inclusive, it is the vast majority of users. The design philosophy basically says that GIAC Enterprises is a centrally managed organization to keep administration costs down. Upon proper justification to management, a department may retain control of their users, groups and printers, otherwise, all such objects are managed by the central I/T organization.

The People organizational unit above is the organizational unit in which user objects are located. No other objects are permitted to exist in these containers.

The Groups organizational unit above is the organizational unit in which group objects are located. No other objects are permitted to exist in this container. The group objects give permissions to file shares, printers and other network resources as well as serve as distribution groups for Exchange.

The Printers organizational unit above is the organizational unit in which printer objects are located. Originally, GIAC Enterprises had a single printers container located as a child object to the Devices organizational unit so that they could be centrally administered, however, to properly delegate authority to the departmental administrator of R&D and I/T, it was decided to create a printers organizational unit under the R&D and I/T departmental organizational units. To maintain consistency and provide for future delegation of authority, a similar printers container was as a child to ECTs.

ou=R&D, ou=Departments, dc=GIACEnterprises, dc=com
ou=IT, ou=Departments, dc=GIACEnterprises, dc=com
The above two containers are the only two departments that have justified reasons for being separated from the larger group.

The R&D Department separated from the rest of the organization so that they may be managed by their own staff and not the central I/T group. This was decided because of the extreme sensitivity of the work that this group does. As you may recall from the opening section, the R&D Department was to be handled with increased security from the rest of the organization. By separating their Active Directory objects and delegating control of those objects to several select users in that department, GIAC Enterprises is able to secure those objects more granularly.

The I/T department also has a separate container from the rest of the organization. Again, this was done for increased security, but with a twist. While the R&D department was separated to keep other users out of the R&D department, the I/T department was separated out so as not to allow users to

escalate privileges beyond their current allotment. The difference is scope. There are varying degrees of administrators and administrative accounts within the forest. While domain and enterprise admins are located in the Admins OU, there are administrative accounts (such as the help desk) that have rights to other people's accounts for password resets, etc. that aren't necessarily domain admins. If the I/T accounts were to remain with the rest of the organization, then it is possible that users may be able to escalate their privileges if they were to obtain access to an I/T user's account. While this is still possible, it is less likely that this type of mistake can be made across OUs.

People, groups and printers are the only three child objects to each of the above organizational units. Within each container they each serve the same purpose, to provide a logical separation of objects by which different group policy objects can be applied and different rights can be granted.

ou=GPOs, dc=GIACEnterprises, dc=com
For the same purposes as in the eGIACEnterprises.com domain, this organizational unit was added for placement of all Group Policy Objects in the GIACEnterprises.com domain. With Group Policy Objects being separate objects and not properties of other objects, their effectiveness is not reliant upon their placement within the directory domain. Group Policy Objects are enacted by simply "linking" them to other objects. For this reason, by placing Group Policy Objects in their own container, they can be easily managed. Permissions on this container are restricted to administrators only and therefore the security of the objects is increased. By default, when you create a Group Policy Object for an organizational unit, it is created in that organizational unit. In the case of external customers, the Group Policy Objects would be located in the same container as the user objects. This would violate a basic directory design principle of distributing permissions and security from a place higher in the tree than the object receiving the permission. By placing the Group Policy Objects in a different container, they can be applied to one to many other containers and are not thought of as a Group Policy Object for a particular organizational unit. The only exception to this within the domain is the Group Policy Object for the GPO container. This GPO is located directly under the eGIACEnterprises domain component of the tree so as to not violate the principle of security from a location higher in the tree.

ou=Admins, dc=GIACEnterprises, dc=com
The Admins organizational unit was created for the purposes of holding the administrative accounts. In this container reside the domain and enterprise administrators for the GIACEnterprises.com and eGIACEnteprises.com domains. As stated before, GIAC Enterprises is centrally managed organization. As GIAC Enterprises is not a large company from an employee perspective and its domain administrators are also enterprise administrators. The users in this container are a primary reason why the trust relationship was created between the two forests. By enabling the one way trust from the GIACEnterprises.com domain to the

eGIACEnterprises.com domain, administrators do not have to re-authenticate to the external forest when they want to do administrative work in that forest. The user IDs in the giacenterprises.com forest are members of groups for authorization and distribution in the egiacenterprises.com forest.

ou=Devices, dc=GIACEnterprises, dc=com
The Devices organizational unit is an organizational unit of structure. This means, its purpose is to be a placeholder for the ServerZone and WkstZone organizational units. No objects other than these two organizational units are permitted directly underneath this container.

ou=ServerZone, ou=Devices, dc=GIACEnterprises, dc=com
The Server Zone organizational unit is the container that contains all servers in the Corporate Server Zone on the physical network. This includes two Windows 2000 file and print servers, an Exchange 2000 server, a SQL server and two Domain Controllers that also are acting as DNS and DHCP servers. Because the GIACEnterprises.com domain is a single domain forest, the FSMO roles are split between the two domain controllers. Without the implications of a multi-domain forest, there are no issues with having the domain controller being an Infrastructure Master as well as a global catalog server. The FSMO roles are split just as they are in the eGIACEnterprises.com forest. ADDC01 maintains the RID and PDC Emulator Master roles while ADDC02 maintains the Infrastructure, Schema and Domain Naming Master roles. Also, since all workstations and servers are Windows 2000 or higher, this forest runs in Native mode. Internal testing was done to verify that all attached products such as ARCServe 2000 would function appropriately when the domain controllers were in Native mode. After this was done, the one way switch was made. Also, since all workstations are Windows 2000 or Windows XP, the group Pre-Windows 2000 Compatible Access does NOT have the Everyone group as a member.

ou=WkstZone, ou=Devices, dc=GIACEnterprises, dc=com
The WkstZone organizational unit is the container that contains all of the workstations at GIAC Enterprises. There was significant discussion at GIAC Enterprises whether to have a single organizational unit for workstations or to have an individual one underneath each of the departmental organizational units. It came to be decided that a single workstation organizational unit was most appropriate so that a base level of security could be applied to all workstations across the enterprise. All workstations at GIAC Enterprises are either Windows 2000 or Windows XP. The Windows XP rollout was started several months ago and is being done on completely new hardware. To manage the ever increasing amount of fixes and now SP1 for XP, Group Policy Objects are used for distribution. This is explained in greater detail in the next section.

Section 4 – Group Policy Object Design

Group Policy Objects are the most important new feature in Windows 2000 Active Directory. They allow administrators to centrally manage hundreds and thousands of users with complete uniformity. Group Policy allows administrators to manage many functions within a Windows 2000 network including registry values, NTFS permissions, auditing functions, manage scripts and desktops.

It's been said that without Group Policy Objects, security in Windows 2000 could not be controlled. In addition to Group Policy, the [i]"…Group Policy Snap-In provides an integrated tool with which to manage the Group Policy…" This is an important point. The Group Policy Objects' effectiveness at securing a Windows 2000 site is well documented; however, it is not as much talked about how the tools were improved. Microsoft very much improved the management tools (MMC) in Windows 2000 and made it very modular. Snap-ins allow an administrator to easily define custom consoles for OU Admins, help desk personnel, or whomever.

GIAC Enterprises defines a default domain policy for both domains, as well as OU policies for each of the major organizational unit differences. These Group Policy objects are outlined below.

eGIACEnterprises.com

Default Domain Policy

The default domain policy for eGIACEnterprises.com is based on the [ii]National Security Agency's domain policy but is modified for use at GIAC Enterprises. The policy was modified in Notepad and then imported into the Default Domain Policy object. As the great majority of the rationale behind this forest is for external customers, there is very little in terms of Group Policy to be examined for this forest. Users in the People OU take on the settings of the default domain policy.

Figure 7 below shows the Password Policies maintained by the Default Domain Policy while the table describes more detailed information and explains the deviation from the NSA recommendations.

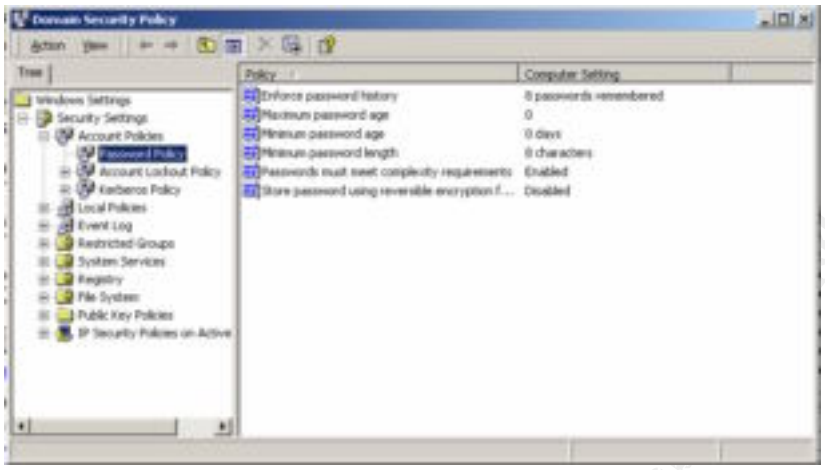


Figure 7

Account Policies

Option	GIAC Enterprises Setting	Notes
MinimumPasswordAge	0	Modified from W2K_DOMAIN_POLICY.INF.
MaximumPasswordAge	0	Modified from W2K_DOMAIN_POLICY.INF.
MinimumPasswordLength	8	Modified from W2K_DOMAIN_POLICY.INF.
PasswordComplexity	Enabled	Taken from W2K_DOMAIN_POLICY.INF.
PasswordHistorySize	8	Modified from W2K_DOMAIN_POLICY.INF.
LockoutBadCount	3	Taken from W2K_DOMAIN_POLICY.INF.
ResetLockoutCount	15	Taken from W2K_DOMAIN_POLICY.INF.
LockoutDuration	600	Modified from W2K_DOMAIN_POLICY.INF.
Store Password Using Reversible Encryption	Disabled	Taken from W2K_DOMAIN_POLICY.INF.
MaxTicketAge	10	Taken from W2K_DOMAIN_POLICY.INF.
MaxRenewAge	7	Taken from W2K_DOMAIN_POLICY.INF.
MaxServiceAge	600	Taken from W2K_DOMAIN_POLICY.INF.
MaxClockSkew	5	Taken from W2K_DOMAIN_POLICY.INF.
TicketValidateClient	1	Taken from W2K_DOMAIN_POLICY.INF.

As is shows in the notes and in the preceding paragraphs, the template used for the Default Domain Policy is the W2K_DOMAIN_POLICY.INF template. Setting the 'MaximumPasswordAge' to 0 effectively states that users in this domain do not have to reset passwords. While this is usually looked on by security personnel as abhorrent, it was not done without considerable attention. The primary use of this forest is to house external users. As the majority of the customers for GIAC Enterprises use the site once a year, the business decision was made to not require them to change their passwords. Doing so was felt to turn away a great majority of customers. This is another reason for the trust relationship. By using this setting, the external users do not have to change passwords, while internal administrators will be bound by the account policies in the GIACEnterprises.com domain. GIAC Enterprises decided to significantly increase the lockout duration. The application will automatically unlock the account after re-verification of personal information. If the user does not re-verify the information, they cannot attempt to access the site again until 10 hours later.

WebZone Group Policy

The Web Zone is arguably the most dangerous place in GIAC Enterprises network. This is the most attacked portion of the network from the outside "black hats". With this in mind, the security of the individual servers is extremely important. Servers in this zone include ISA and IIS servers. To accommodate both types of servers, a customized Group Policy Object was created that is a combination of HISECWEB.INF and NSA's ISA.INF policies. The following four lines,

```
[File Security]
1="d:\microsoft isa server", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
2="d:\microsoft isa server\clients", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
3="d:\urlcache", 0, "D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
```

were added to the HISECWEB.INF file to provide additional security to Microsoft ISA server. In addition, HISECWEB.INF was modified in the following ways to meet the needs of GIAC Enterprises.

Option	GIAC Enterprises Setting	Reason
NewAdministatorName	Coke	The default administrator account is renamed on all of these devices to Coke.
NewGuestName	Pepsi	The default guest account is renamed on all of these devices to Pepsi.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	1	Added logon message to comply with corporate policy. "This computer system is owned and operated by GIAC Enterprises. If you do not have explicit permission from GIAC Enterprises to be here, LEAVE! Your actions will be watched and you will be prosecuted if you are not supposed to be here."

In addition to the Group Policy objects, the IIS lockdown tool is run on both the ISA and IIS servers in this zone. For the IIS servers, the tool is run with the dynamic web server option selected. For the ISA server, the proxy server option is chosen. The HFNetCheck tool is also run against these servers on a monthly basis and a report is generated which is sent to the domain administrators email box. The tool is scheduled using a combination of DOS batch files and task scheduler.

ServicesZone Group Policy

The Services Zone is the other zone on the eGIACEnterprises.com network that is exposed to the Internet. This zone contains a public ftp server, an Exchange 2000 mail server and an Active Directory DNS server. A combination of security templates are used to secure these servers. Because the server's functions are unique and very different from each other, agreement on Group Policy settings were extremely difficult to come to. A combination of HISECWEB.INF from Microsoft and W2K_DC.INF from the NSA were used to secure these servers. Because of functionality issues[iii], Microsoft explicitly states to not use the HISECWEB.INF security template on a domain controller because of problems between domain controllers and IIS. With both IIS (ftp server) and a domain controller (DNS server) in this zone, the HISECWEB.INF file is the best file to implement. To date, GIAC Enterprises has not encountered issues with this configuration. Customizations were made to the file to however to comply with corporate policy.

Option	GIAC Enterprises Setting	Reason
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	1	The following text was added, "This computer system is owned and operated by GIAC Enterprises. If you do not have explicit permission from GIAC Enterprises to be here, LEAVE! Your actions will be watched and you will be prosecuted if you are not supposed to be here."
NewAdministatorName	Coke	The default administrator account is renamed on all of these devices to Coke.
NewGuestName	Pepsi	The default guest account is renamed on all of these devices to Pepsi.
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Removed	This value is removed from the Group Policy Object. By removing this value, the automatic password changing feature for machine accounts is enabled. If this were to be disabled, a compromised password could lead to total control of the domain by the attacker.

Data Zone Group Policy (Includes Policy for Domain Controllers)

The Data Zone is considered to be the "gold" of the network. A compromise at this level would constitute a complete failure in the security plan for GIAC Enterprises. Servers in this zone consist of two Active Directory domain controllers and two SQL servers. The domain controllers were moved from their default container of 'Domain Controllers'. The servers in this zone use the W2K_DC.INF security template as their baseline. From there, modifications are made. Listed below are those modifications and highlights from the security policies.

Account Policies

Option	GIAC Enterprises Setting	Notes
MinimumPasswordAge	Not Defined	This setting is defined at the Domain level.
MaximumPasswordAge	Not Defined	This setting is defined at the Domain level.
MinimumPasswordLength	Not Defined	This setting is defined at the Domain level.
PasswordComplexity	Not Defined	This setting is defined at the Domain level.
PasswordHistorySize	Not Defined	This setting is defined at the Domain level.
LockoutBadCount	Not Defined	This setting is defined at the Domain level.
ResetLockoutCount	Not Defined	This setting is defined at the Domain level.
LockoutDuration	Not Defined	This setting is defined at the Domain level.
ClearTextPassword	Not Defined	This setting is defined at the Domain level.
RequireLogonToChangePassword	Not Defined	This setting is defined at the Domain level.

Even though these settings are defined by W2K_DC.INF, they are ineffectual because the Account Policy settings are also defined at the Domain level. For this reason, they are return to 'Not Defined' for the Data Zone.

Auditing Policies

Option	GIAC Enterprises Setting	Notes
AuditSystemEvents	Success/Failure	Taken from W2K_DC.INF.
AuditLogonEvents	Success/Failure	Taken from W2K_DC.INF.
AuditObjectAccess	Failure	Taken from W2K_DC.INF.
AuditPrivilegeUse	Success/Failure	Modified from W2K_DC.INF.
AuditPolicyChange	Success/Failure	Taken from W2K_DC.INF.
AuditAccountManage	Success/Failure	Taken from W2K_DC.INF.
AuditProcessTracking	No auditing	Taken from W2K_DC.INF.
AuditDSAccess	Failure	Taken from W2K_DC.INF.
AuditAccountLogon	Success/Failure	Taken from W2K_DC.INF.

For the most part, these settings are taken directly from the W2K_DC.INF template. These settings will audit all critical events on the domain controller. GIAC Enterprises decided to modify the AuditPrivilegeUse setting to include the auditing of successful uses. This will enable tracking of administrative access to the domain controllers.

User Rights Assignment Policies

Option	GIAC Enterprises Setting	Notes
Access this computer from the network	Administrators Authenticated Users	Taken from W2K_DC.INF.
Act as part of the operating system	None	Taken from W2K_DC.INF.
Add workstations to domain	Administrators	Taken from W2K_DC.INF.
Back up files and directories	Backup Operators Administrators	Taken from W2K_DC.INF.
Bypass traverse checking	Authenticated Users	Taken from W2K_DC.INF.
Change the system time	Administrators	Taken from W2K_DC.INF.
Create a pagefile	Administrators	Taken from W2K_DC.INF.
Create a token object	None	Taken from W2K_DC.INF.
Create permanent shared objects	None	Taken from W2K_DC.INF.
Debug programs	None	Taken from W2K_DC.INF.
Deny access to this computer from the network	Not defined	Taken from W2K_DC.INF.
Deny logon as a batch job	Not defined	Taken from W2K_DC.INF.
Deny logon as a service	Not defined	Taken from W2K_DC.INF.
Deny logon locally	Not defined	Taken from W2K_DC.INF.
Enable computer and user accounts to be trusted for delegation	Administrators	Taken from W2K_DC.INF.
Force shutdown from a remote system	None	Modified from W2K_DC.INF.
Generate security audits	Not defined	Taken from W2K_DC.INF.
Increase quotas	None	Modified from W2K_DC.INF.
Increase scheduling priority	Administrators	Taken from W2K_DC.INF.
Load and unload device drivers	Administrators	Taken from W2K_DC.INF.
Lock pages in memory	None	Taken from W2K_DC.INF.
Log on as a batch job	None	Taken from W2K_DC.INF.
Log on as a service	None	Taken from W2K_DC.INF.
Log on locally	Administrators	Taken from W2K_DC.INF.
Manage auditing and security log	Administrators	Taken from W2K_DC.INF.
Modify firmware environment values	Administrators	Taken from W2K_DC.INF.
Profile single process	Administrators	Taken from W2K_DC.INF.
Profile system performance	Administrators	Taken from W2K_DC.INF.
Remove computer from docking station	None	Taken from W2K_DC.INF.
Replace a process level token	None	Taken from W2K_DC.INF.
Restore files and directories	Administrators	Taken from W2K_DC.INF.
Shut down the system	Administrators	Taken from W2K_DC.INF.
Synchronize directory service data	None	Taken from W2K_DC.INF.
Take ownership of files or other objects	Administrators	Taken from W2K_DC.INF.

As with the Auditing Policies, the majority of these settings are taken directly from the W2K_DC.INF template. There are two modifications to the template that need to be discussed. First, the 'Force shutdown from a remote system' is defined by the W2K_DC.INF template to be Administrators. GIAC Enterprises has decided to change that to none. While this could pose a support issue by having administrators physically drive into the office to reboot a system, it does remove the risk of someone (either maliciously or accidentally) shutting down the

system when not at the console. Second, the 'Increase Quotas' setting is defined by the W2K_DC.INF template to be administrators. While this is not necessarily an incorrect setting, none of the servers in this forest are file servers (especially the domain controllers) and as such, users do not store files on them. GIAC Enterprises operates under the presumption of least privileged access which essentially means that users have the minimum access to do their jobs, no more…no less.

Security Options Policies

Option	GIAC Enterprises Setting	Notes
Additional restrictions for anonymous connections	No Access Without Explicit Permissions	Taken from W2K_DC.INF.
Allow server operators to schedule tasks (domain controllers only)	Disabled	Taken from W2K_DC.INF.
Allow system to be shut down without having to log on	Disabled	Taken from W2K_DC.INF.
Allowed to eject removable NTFS media	Administrators	Taken from W2K_DC.INF.
Amount of idle time required before disconnecting session	10 minutes	Modified from W2K_DC.INF.
Audit the access of global system objects	Enabled	Taken from W2K_DC.INF.
Audit use of Backup and Restore privilege	Enabled	Taken from W2K_DC.INF.
Automatically log off users when logon time expires	Not defined	Taken from W2K_DC.INF.
Automatically log off users when logon time expires (local)	Enabled	Taken from W2K_DC.INF.
Clear virtual memory pagefile when system shuts down	Enabled	Taken from W2K_DC.INF.
Digitally sign client communication (always)	Disabled	Taken from W2K_DC.INF.
Digitally sign client communication (when possible)	Enabled	Taken from W2K_DC.INF.
Digitally sign server communication (always)	Disabled	Taken from W2K_DC.INF.
Digitally sign server communication (when possible)	Enabled	Taken from W2K_DC.INF.
Disable CTRL+ALT+DEL requirement for logon	Disabled	Taken from W2K_DC.INF.
Do not display last user name in logon screen	Enabled	Taken from W2K_DC.INF.
LAN Manager Authentication Level	Send NTLMv2 responses only\Refuse LM & NTLM	Taken from W2K_DC.INF.
Message text for users attempting to log on	This computer system is owned and operated by GIAC Enterprises. If you do not have explicit permission from GIAC Enterprises to be here, LEAVE! Your actions will be watched and you will	Modified from W2K_DC.INF.

	be prosecuted if you are not supposed to be here.	
Message title for users attempting to log on	A GIAC Enterprises Owned and Operated Computer	Modified from W2K_DC.INF.
Number of previous logons to cache (in case domain controller is not available)	0 logons	Taken from W2K_DC.INF.
Prevent system maintenance of computer account password	Disabled	Taken from W2K_DC.INF.
Prevent users from installing printer drivers	Enabled	Taken from W2K_DC.INF.
Prompt user to change password before expiration	0 Days	Modified from W2K_DC.INF.
Recovery Console: Allow automatic administrative logon	Disabled	Taken from W2K_DC.INF.
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Taken from W2K_DC.INF.
Rename administrator account	Coke	Taken from W2K_DC.INF.
Rename guest account	Pepsi	Taken from W2K_DC.INF.
Restrict CD-ROM access to locally logged-on user only	Enabled	Taken from W2K_DC.INF.
Restrict floppy access to locally logged-on user only	Enabled	Taken from W2K_DC.INF.
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Taken from W2K_DC.INF.
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Taken from W2K_DC.INF.
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Taken from W2K_DC.INF.
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Taken from W2K_DC.INF.
Send unencrypted password to connect to third-party SMB servers	Disabled	Taken from W2K_DC.INF.
Shut down system immediately if unable to log security audits	Disabled	Modified from W2K_DC.INF.
Smart card removal behavior	Not Defined	Modified from W2K_DC.INF.
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Taken from W2K_DC.INF.
Unsigned driver installation behavior	Warn but Allow Installation	Taken from W2K_DC.INF.
Unsigned non-driver installation behavior	Warn but Allow Installation	Taken from W2K_DC.INF.

As per the previous sections, the majority of the settings are taken directly from W2K_DC.INF. Several settings were modified from those to meet the needs of GIAC Enterprises. The setting 'Amount of idle time required before disconnecting session' is set to 30 minutes by the template. GIAC Enterprises has chosen to set this to 10 minutes to reduce the risk of unattended connections to domain controllers. Some other notable changes from the template including adding a logon message, renaming the administrator and guest accounts,

modifying the smart card behavior, the shutting down of the system due to security audits not being logged appropriately and the notification of an expired password. The last two notables require some discussion. First, the 'Shut down system immediately if unable to log security audits' is disabled. This is enabled in the template. It was decided to disable this and enable a repeating script that monitors for the event and simply pages the administrator on duty for further investigation. This option is less invasive up front and can still be carried out by the administrator if he/she feels it necessary. Furthermore, this could be a potential attack or way to have a back door activated on a reboot if the attacker could make a security audit fail. Second, the 'Prompt user to change password before expiration' was set to 0 days because the default domain policy does not require users to change their passwords.

Event Log Policies

Option	GIAC Enterprises Setting	Notes
Maximum application log size	500,000 Kilobytes	
Maximum security log size	500,000 Kilobytes	
Maximum system log size	500,000 Kilobytes	
Restrict guest access to application log	Enabled	
Restrict guest access to security log	Enabled	
Restrict guess access to system log	Enabled	
Retain application log	7 Days	
Retain security log	7 Days	
Retain system log	7 Days	
Retention method for application log	Overwrite Events by Days	
Retention method for security log	Overwrite Events by Days	
Retention method for system log	Overwrite Events by Days	
Shutdown the computer when the security audit log is full	Disabled	

While the majority of the other sections were taken from the W2K_DC.INF template, this section is mostly different. The goal of the event logs for GIAC Enterprises is to retain the three logs for a period of one week after which they are automatically overwritten and archived to tape. To accomplish this, the maximum log sizes are set fairly high (500MB) and the above settings are made. In addition, GIAC Enterprises does not agree with the NSA on the last setting regarding shutting down the computer when the security audit log is full. This is an extreme action to an event and could be used by an attacker to disable a system through the filling of logs. Again, GIAC Enterprises monitors this and pages an administrator for further investigation but does not automatically shutdown servers.

Registry Policies

Object Name	Permission	Audit
CLASSES_ROOT	Replace	Replace
machine\software	Replace	Replace
machine\software\microsoft\netdde	Replace	Replace
MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT	Replace	Replace
machine\software\microsoft\protected storage system provider	Ignore	Ignore
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands	Replace	Replace
machine\software\microsoft\windows nt\currentversion\perflib	Replace	Replace
machine\software\microsoft\windows\currentversion\group policy		
machine\software\microsoft\windows\currentversion\installer		
machine\software\microsoft\windows\currentversion\policies		
machine\system	Replace	Replace
machine\system\clone	Ignore	Ignore
machine\system\controlset001		
machine\system\controlset002		
machine\system\controlset003		
machine\system\controlset004		
machine\system\controlset005		
machine\system\controlset006		
machine\system\controlset007		
machine\system\controlset008		
machine\system\controlset009		
machine\system\controlset010		
machine\system\currentcontrolset\control\securepipeservers\ winreg	Replace	Replace
machine\system\currentcontrolset\control\wmi\security	Replace	Replace
machine\system\currentcontrolset\enum	Ignore	Ignore
machine\system\currentcontrolset\hardware profiles		
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers	Replace	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities	Replace	Replace
users\.default	Replace	Replace
users\.default\software\microsoft\netdde	Replace	Replace
users\.default\software\microsoft\protected storage system provider	Ignore	Ignore

The above table are the registry values that will be put in place by the W2K_DC.INF template and used by GIAC Enterprises.

File System Policies

Object Name	Permission	Audit
%ProgramFiles%	Replace	Replace
%SystemDirectory%	Replace	Replace
%SystemDirectory%\appmgmt		
%SystemDirectory%\config	Replace	Replace
%SystemDirectory%\dllcache	Replace	Replace

%SystemDirectory%\DTCLog		
%SystemDirectory%\GroupPolicy		
%SystemDirectory%\ias	Replace	Replace
%SystemDirectory%\Ntbackup.exe	Replace	Replace
%SystemDirectory%\NTMSData		
%SystemDirectory%\rcp.exe	Replace	Replace
%SystemDirectory%\regedt32.exe	Replace	Replace
%SystemDirectory%\ReinstallBackups	Ignore	Ignore
%SystemDirectory%\repl		
%SystemDirectory%\repl\export		
%SystemDirectory%\repl\import		
%SystemDirectory%\rexec.exe	Replace	Replace
%SystemDirectory%\rsh.exe	Replace	Replace
%SystemDirectory%\secedit.exe	Replace	Replace
%SystemDirectory%\Setup		
%SystemDirectory%\spool\printers	Replace	Replace
%SystemDrive%\		
%SystemDrive%\autoexec.bat	Replace	Replace
%SystemDrive%\boot.ini	Replace	Replace
%SystemDrive%\config.sys	Replace	Replace
%SystemDrive%\Documents and Settings		
%SystemDrive%\Documents and Settings\Administrator	Replace	Replace
%SystemDrive%\Documents and Settings\All Users		
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson	Replace	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log	Replace	Replace
%SystemDrive%\Documents and Settings\Default User	Replace	Replace
%SystemDrive%\Inetpub	Ignore	Ignore
%SystemDrive%\IO.SYS	Replace	Replace
%SystemDrive%\MSDOS.SYS	Replace	Replace
%SystemDrive%\My Download Files	Replace	Replace
%SystemDrive%\ntdetect.com	Replace	Replace
%SystemDrive%\ntldr	Replace	Replace
%SystemDrive%\Program Files\Resource Kit	Replace	Replace
%SystemDrive%\System Volume Information	Ignore	Ignore
%SystemDrive%\Temp	Replace	Replace
%SystemRoot%	Replace	Replace
%SystemRoot%\$NtServicePackUninstall$	Replace	Replace
%SystemRoot%\CSC	Replace	Replace
%SystemRoot%\debug		
%SystemRoot%\debug\UserMode		
%SystemRoot%\NTDS		
%SystemRoot%\Offline Web Pages	Ignore	Ignore
%SystemRoot%\regedit.exe	Replace	Replace
%SystemRoot%\Registration		
%SystemRoot%\repair	Replace	Replace
%SystemRoot%\security	Replace	Replace
%SystemRoot%\SYSVOL		
%SystemRoot%\SYSVOL\domain\Policies		
%SystemRoot%\Tasks	Ignore	Ignore
%SystemRoot%\Temp	Replace	Replace
c:\autoexec.bat	Replace	Replace
c:\boot.ini	Replace	Replace

c:\config.sys	Replace	Replace
c:\ntbootdd.sys	Replace	Replace
c:\ntdetect.com	Replace	Replace
c:\ntldr	Replace	Replace

Also, as stated previously, the W2K_DC.INF template was used as the baseline for security of the servers in the Data Zone. This includes the above file system permissions that were put in place on these servers.

Restricted Groups Policy

The W2K_DC.INF template does not define any Restricted Groups. GIAC Enterprises adds several groups to this list for the external forest. The Enterprise Domain Administrators, Administrators, Schema Administrators, Domain Administrators and Account Operators are all added as Restricted Groups. Individual administrators from the GIACEnterprises.com forest are added to these as allowed members. This effectively eliminates the possibility of external users escalating privileges.

Services Policy

Service	Startup	Permission
Alerter	Disabled	Configured
Application Management	Not defined	Not defined
Automatic Updates	Automatic	Configured
Background Intelligent Transfer Service	Automatic	Configured
ClipBook	Disabled	Configured
COM+ Event System	Disabled	Configured
Computer Browser	Automatic	Configured
DHCP Client	Disabled	Configured
DHCP Server	Disabled	Configured
Distributed File System	Disabled	Configured
Distributed Link Tracking Client	Not defined	Not defined
Distributed Link Tracking Server	Not defined	Not defined
Distributed Transaction Coordinator	Not defined	Not defined
DNS Client	Automatic	Configured
DNS Server	Automatic	Configured
Event Log	Automatic	Configured
Fax Service	Disabled	Configured
File Replication Service	Disabled	Configured
FTP Publishing Service	Disabled	Configured
IIS Admin Service	Disabled	Configured
Indexing Service	Disabled	Configured
Internet Connection Sharing	Disabled	Configured
Intersite Messaging	Disabled	Configured
IPSEC Policy Agent	Automatic	Configured
Kerberos Key Distribution Center	Automatic	Configured
License Logging Service	Automatic	Configured
Logical Disk Manager	Automatic	Configured
Logical Disk Manager Administrative Service	Not defined	Not defined
Messenger	Disabled	Configured
Net Logon	Not defined	Not defined

NetMeeting Remote Desktop Sharing	Disabled	Configured
Network Connections	Automatic	Configured
Network DDE	Not defined	Not defined
Network DDE DSDM	Not defined	Not defined
Network News Transport Protocol (NNTP)	Disabled	Configured
NT LM Security Support Provider	Not defined	Not defined
Performance Logs and Alerts	Not defined	Not defined
Plug and Play	Not defined	Not defined
Print Spooler	Disabled	Configured
Protected Storage	Not defined	Not defined
QoS RSVP	Not defined	Not defined
Remote Access Auto Connection Manager	Disabled	Configured
Remote Access Connection Manager	Disabled	Configured
Remote Procedure Call (RPC)	Not defined	Not defined
Remote Procedure Call (RPC) Locator	Not defined	Not defined
Remote Registry Service	Disabled	Configured
Removable Storage	Not defined	Not defined
Routing and Remote Access	Disabled	Configured
RunAs Service	Not defined	Not defined
Security Accounts Manager	Not defined	Not defined
Server	Disabled	Configured
Simple Mail Transport Protocol (SMTP)	Disabled	Configured
Smart Card	Disabled	Configured
Smart Card Helper	Disabled	Configured
SNMP Service	Not defined	Not defined
SNMP Trap Service	Not defined	Not defined
System Event Notification	Not defined	Not defined
Task Scheduler	Automatic	Configured
TCP/IP NetBIOS Helper Service	Disabled	Configured
Telephony	Disabled	Configured
Telnet	Disabled	Configured
Terminal Services	Disabled	Configured
Uninterruptible Power Supply	Not defined	Not defined
Utility Manager	Not defined	Not defined
Windows Installer	Not defined	Not defined
Windows Management Instrumentation	Not defined	Not defined
Windows Management Instrumentation Driver Extensions	Not defined	Not defined
Windows Time	Automatic	Configured
WMDM PMSP Service	Not defined	Not defined
Workstation	Disabled	Configured
World Wide Web Publishing Service	Disabled	Configured

The above table identifies the 71 services that on a Windows 2000 Domain Controller running Service Pack 3. The table outlines the removal of unnecessary services as of the 71 total, only 13 are started automatically while 31 are disabled automatically.

GIACEnterprises.com

Default Domain Policy

The default domain policy for GIACEnterprises.com is based on the [iv]National Security Agency's domain policy (W2K_Domain_Policy.inf) but is modified for use at GIAC Enterprises. The policy was modified in Notepad and then imported into the Default Domain Policy object.

Account Policies

Option	GIAC Enterprises Setting	Notes
MinimumPasswordAge	1	Taken from W2K_DOMAIN_POLICY.INF.
MaximumPasswordAge	45	Modified from W2K_DOMAIN_POLICY.INF.
MinimumPasswordLength	8	Modified from W2K_DOMAIN_POLICY.INF.
PasswordComplexity	Enabled	Taken from W2K_DOMAIN_POLICY.INF.
PasswordHistorySize	8	Modified from W2K_DOMAIN_POLICY.INF.
LockoutBadCount	3	Taken from W2K_DOMAIN_POLICY.INF.
ResetLockoutCount	15	Taken from W2K_DOMAIN_POLICY.INF.
LockoutDuration	60	Modified from W2K_DOMAIN_POLICY.INF.
Store Password Using Reversible Encryption	Disabled	Taken from W2K_DOMAIN_POLICY.INF.
MaxTicketAge	10	Taken from W2K_DOMAIN_POLICY.INF.
MaxRenewAge	7	Taken from W2K_DOMAIN_POLICY.INF.
MaxServiceAge	600	Taken from W2K_DOMAIN_POLICY.INF.
MaxClockSkew	5	Taken from W2K_DOMAIN_POLICY.INF.
TicketValidateClient	1	Taken from W2K_DOMAIN_POLICY.INF.

The 'MaximumPasswordAge' was modified from the template to comply with corporate policy of change passwords every 45 days. In addition, the 'MinimumPasswordLength' was reduced from 12 to 8 which was thought to be more applicable to the organization given the increased frequency of changes. The 'PasswordHistorySize' was reduced from 24 to 8 to accomplish the goal of restricting users to not using the same password more than once in any given calendar year. While this could be fooled by modifying your password everyday, it was deemed that that level of risk was low.

Server Zone OU Group Policy (Includes Default Domain Controllers)

Objects in the Server Zone consist of domain controllers, file and print servers, an Exchange 2000 server, and an SQL server. These servers all use the W2K_DC.INF policy from the NSA as opposed to the HISECDC.INF policy from Microsoft as it is much more comprehensive.

There are two schools of thoughts on having the all of these varying types of servers managed by one GPO. First, it can be looked at as security of the least common denominator. This means that security is only as good as the least

secure piece of the chain. An example would be if there were an IIS server in this zone, that the GPO would need to allow for the IIS service to be running while typically with a DC policy, that service would be disabled. The second school of thought says you bring security up to the highest level possible for all components. Domain controllers typically have a higher security valuation placed on them versus web or file servers. For this reason, those web or file servers have lower security or more places to attack. This school of thought says that you bring the security on those servers up to the level of the domain controller by managing it with the same GPO.

GIAC Enterprises believes that both schools of thought are right and wrong. While they are both good arguments, GIAC Enterprises has elected to manage all of the varying types of servers in this zone with a single GPO (listed as the Default Domain Controller GPO) believing that while the DC may have some additional vulnerabilities, those are considered to be minor compared with the higher level of security on the rest of the servers and the consistency that is brought. Also, given the fact that there are less than a dozen servers and not hundreds as in a large organization, this tradeoff can be easily justified. The time it takes to create and manage multiple GPOs can be justified with additional staff and servers to manage.

The individual settings for each section are outlined below with the corresponding modifications made for GIAC Enterprises internal forest.

Account Policies

Option	GIAC Enterprises Setting	Notes
MinimumPasswordAge	Not Defined	This setting is defined at the Domain level.
MaximumPasswordAge	Not Defined	This setting is defined at the Domain level.
MinimumPasswordLength	Not Defined	This setting is defined at the Domain level.
PasswordComplexity	Not Defined	This setting is defined at the Domain level.
PasswordHistorySize	Not Defined	This setting is defined at the Domain level.
LockoutBadCount	Not Defined	This setting is defined at the Domain level.
ResetLockoutCount	Not Defined	This setting is defined at the Domain level.
LockoutDuration	Not Defined	This setting is defined at the Domain level.
ClearTextPassword	Not Defined	This setting is defined at the Domain level.
RequireLogonToChangePassword	Not Defined	This setting is defined at the Domain level.

Even though these settings are defined by W2K_DC.INF, they are ineffectual because the Account Policy settings are also defined at the Domain level. For this reason, they are return to 'Not Defined' for the Server Zone.

Auditing Policies

Option	GIAC Enterprises Setting	Notes
AuditSystemEvents	Success/Failure	Taken from W2K_DC.INF.

AuditLogonEvents	Success/Failure	Taken from W2K_DC.INF.
AuditObjectAccess	Failure	Taken from W2K_DC.INF.
AuditPrivilegeUse	Failure	Modified from W2K_DC.INF.
AuditPolicyChange	Success/Failure	Taken from W2K_DC.INF.
AuditAccountManage	Success/Failure	Taken from W2K_DC.INF.
AuditProcessTracking	No auditing	Taken from W2K_DC.INF.
AuditDSAccess	Failure	Taken from W2K_DC.INF.
AuditAccountLogon	Success/Failure	Taken from W2K_DC.INF.

These settings are taken directly from the W2K_DC.INF template. These settings will audit all critical events on the domain controllers, file servers, SQL server, etc. In the eGIACEnterprises.com forest, you'll notice that the 'AuditPrivilegeUse' setting was modified but not here in the GIACEnterprises.com forest because of fewer security concerns and increased traffic on the internal Active Directory.

User Rights Assignment Policies

Option	GIAC Enterprises Setting	Notes
Access this computer from the network	Administrators Authenticated Users	Taken from W2K_DC.INF.
Act as part of the operating system	None	Taken from W2K_DC.INF.
Add workstations to domain	Administrators	Taken from W2K_DC.INF.
Back up files and directories	Backup Operators Administrators	Taken from W2K_DC.INF.
Bypass traverse checking	Authenticated Users	Taken from W2K_DC.INF.
Change the system time	Administrators	Taken from W2K_DC.INF.
Create a pagefile	Administrators	Taken from W2K_DC.INF.
Create a token object	None	Taken from W2K_DC.INF.
Create permanent shared objects	None	Taken from W2K_DC.INF.
Debug programs	None	Taken from W2K_DC.INF.
Deny access to this computer from the network	Not defined	Taken from W2K_DC.INF.
Deny logon as a batch job	Not defined	Taken from W2K_DC.INF.
Deny logon as a service	Not defined	Taken from W2K_DC.INF.
Deny logon locally	Not defined	Taken from W2K_DC.INF.
Enable computer and user accounts to be trusted for delegation	Administrators	Taken from W2K_DC.INF.
Force shutdown from a remote system	None	Modified from W2K_DC.INF.
Generate security audits	Not defined	Taken from W2K_DC.INF.
Increase quotas	None	Modified from W2K_DC.INF.
Increase scheduling priority	Administrators	Taken from W2K_DC.INF.
Load and unload device drivers	Administrators	Taken from W2K_DC.INF.
Lock pages in memory	None	Taken from W2K_DC.INF.
Log on as a batch job	None	Taken from W2K_DC.INF.
Log on as a service	None	Taken from W2K_DC.INF.
Log on locally	Administrators	Taken from W2K_DC.INF.
Manage auditing and security log	Administrators	Taken from W2K_DC.INF.
Modify firmware environment values	Administrators	Taken from W2K_DC.INF.
Profile single process	Administrators	Taken from W2K_DC.INF.
Profile system performance	Administrators	Taken from W2K_DC.INF.
Remove computer from docking station	None	Taken from W2K_DC.INF.

Replace a process level token	None	Taken from W2K_DC.INF.
Restore files and directories	Administrators	Taken from W2K_DC.INF.
Shut down the system	Administrators	Taken from W2K_DC.INF.
Synchronize directory service data	None	Taken from W2K_DC.INF.
Take ownership of files or other objects	Administrators	Taken from W2K_DC.INF.

Security Options Policies

Option	GIAC Enterprises Setting	Notes
Additional restrictions for anonymous connections	No Access Without Explicit Permissions	Taken from W2K_DC.INF.
Allow server operators to schedule tasks (domain controllers only)	Disabled	Taken from W2K_DC.INF.
Allow system to be shut down without having to log on	Disabled	Taken from W2K_DC.INF.
Allowed to eject removable NTFS media	Administrators	Taken from W2K_DC.INF.
Amount of idle time required before disconnecting session	10 minutes	Modified from W2K_DC.INF.
Audit the access of global system objects	Enabled	Taken from W2K_DC.INF.
Audit use of Backup and Restore privilege	Enabled	Taken from W2K_DC.INF.
Automatically log off users when logon time expires	Not defined	Taken from W2K_DC.INF.
Automatically log off users when logon time expires (local)	Enabled	Taken from W2K_DC.INF.
Clear virtual memory pagefile when system shuts down	Enabled	Taken from W2K_DC.INF.
Digitally sign client communication (always)	Disabled	Taken from W2K_DC.INF.
Digitally sign client communication (when possible)	Enabled	Taken from W2K_DC.INF.
Digitally sign server communication (always)	Disabled	Taken from W2K_DC.INF.
Digitally sign server communication (when possible)	Enabled	Taken from W2K_DC.INF.
Disable CTRL+ALT+DEL requirement for logon	Disabled	Taken from W2K_DC.INF.
Do not display last user name in logon screen	Enabled	Taken from W2K_DC.INF.
LAN Manager Authentication Level	Send NTLMv2 responses only\Refuse LM & NTLM	Taken from W2K_DC.INF.
Message text for users attempting to log on	This computer system is owned and operated by GIAC Enterprises. If you do not have explicit permission from GIAC Enterprises to be here, LEAVE! Your actions will be watched and you will be prosecuted if you are not supposed to be here.	Modified from W2K_DC.INF.

Message title for users attempting to log on	A GIAC Enterprises Owned and Operated Computer	Modified from W2K_DC.INF.
Number of previous logons to cache (in case domain controller is not available)	0 logons	Taken from W2K_DC.INF.
Prevent system maintenance of computer account password	Disabled	Taken from W2K_DC.INF.
Prevent users from installing printer drivers	Enabled	Taken from W2K_DC.INF.
Prompt user to change password before expiration	0 Days	Modified from W2K_DC.INF.
Recovery Console: Allow automatic administrative logon	Disabled	Taken from W2K_DC.INF.
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Taken from W2K_DC.INF.
Rename administrator account	Coke	Taken from W2K_DC.INF.
Rename guest account	Pepsi	Taken from W2K_DC.INF.
Restrict CD-ROM access to locally logged-on user only	Enabled	Taken from W2K_DC.INF.
Restrict floppy access to locally logged-on user only	Enabled	Taken from W2K_DC.INF.
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Taken from W2K_DC.INF.
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Taken from W2K_DC.INF.
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Taken from W2K_DC.INF.
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Taken from W2K_DC.INF.
Send unencrypted password to connect to third-party SMB servers	Disabled	Taken from W2K_DC.INF.
Shut down system immediately if unable to log security audits	Disabled	Modified from W2K_DC.INF.
Smart card removal behavior	Not Defined	Modified from W2K_DC.INF.
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Taken from W2K_DC.INF.
Unsigned driver installation behavior	Warn but Allow Installation	Taken from W2K_DC.INF.
Unsigned non-driver installation behavior	Warn but Allow Installation	Taken from W2K_DC.INF.

Event Log Policies

Option	GIAC Enterprises Setting	Notes
Maximum application log size	500,000 Kilobytes	
Maximum security log size	500,000 Kilobytes	
Maximum system log size	500,000 Kilobytes	
Restrict guest access to application log	Enabled	
Restrict guest access to security log	Enabled	
Restrict guess access to system log	Enabled	

Retain application log	7 Days	
Retain security log	7 Days	
Retain system log	7 Days	
Retention method for application log	Overwrite Events by Days	
Retention method for security log	Overwrite Events by Days	
Retention method for system log	Overwrite Events by Days	
Shutdown the computer when the security audit log is full	Disabled	

Registry Policies

Object Name	Permission	Audit
CLASSES_ROOT	Replace	Replace
machine\software	Replace	Replace
machine\software\microsoft\netdde	Replace	Replace
MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT	Replace	Replace
machine\software\microsoft\protected storage system provider	Ignore	Ignore
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands	Replace	Replace
machine\software\microsoft\windows nt\currentversion\perflib	Replace	Replace
machine\software\microsoft\windows\currentversion\group policy		
machine\software\microsoft\windows\currentversion\installer		
machine\software\microsoft\windows\currentversion\policies		
machine\system	Replace	Replace
machine\system\clone	Ignore	Ignore
machine\system\controlset001		
machine\system\controlset002		
machine\system\controlset003		
machine\system\controlset004		
machine\system\controlset005		
machine\system\controlset006		
machine\system\controlset007		
machine\system\controlset008		
machine\system\controlset009		
machine\system\controlset010		
machine\system\currentcontrolset\control\securepipeservers\winreg	Replace	Replace
machine\system\currentcontrolset\control\wmi\security	Replace	Replace
machine\system\currentcontrolset\enum	Ignore	Ignore
machine\system\currentcontrolset\hardware profiles		
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers	Replace	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities	Replace	Replace
users\.default	Replace	Replace
users\.default\software\microsoft\netdde	Replace	Replace
users\.default\software\microsoft\protected storage system provider	Ignore	Ignore

File System Policies

Object Name	Permission	Audit
%ProgramFiles%	Replace	Replace
%SystemDirectory%	Replace	Replace
%SystemDirectory%\appmgmt		
%SystemDirectory%\config	Replace	Replace
%SystemDirectory%\dllcache	Replace	Replace
%SystemDirectory%\DTCLog		
%SystemDirectory%\GroupPolicy		
%SystemDirectory%\ias	Replace	Replace
%SystemDirectory%\Ntbackup.exe	Replace	Replace
%SystemDirectory%\NTMSData		
%SystemDirectory%\rcp.exe	Replace	Replace
%SystemDirectory%\regedt32.exe	Replace	Replace
%SystemDirectory%\ReinstallBackups	Ignore	Ignore
%SystemDirectory%\repl		
%SystemDirectory%\repl\export		
%SystemDirectory%\repl\import		
%SystemDirectory%\rexec.exe	Replace	Replace
%SystemDirectory%\rsh.exe	Replace	Replace
%SystemDirectory%\secedit.exe	Replace	Replace
%SystemDirectory%\Setup		
%SystemDirectory%\spool\printers	Replace	Replace
%SystemDrive%\		
%SystemDrive%\autoexec.bat	Replace	Replace
%SystemDrive%\boot.ini	Replace	Replace
%SystemDrive%\config.sys	Replace	Replace
%SystemDrive%\Documents and Settings		
%SystemDrive%\Documents and Settings\Administrator	Replace	Replace
%SystemDrive%\Documents and Settings\All Users		
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson	Replace	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log	Replace	Replace
%SystemDrive%\Documents and Settings\Default User	Replace	Replace
%SystemDrive%\Inetpub	Ignore	Ignore
%SystemDrive%\IO.SYS	Replace	Replace
%SystemDrive%\MSDOS.SYS	Replace	Replace
%SystemDrive%\My Download Files	Replace	Replace
%SystemDrive%\ntdetect.com	Replace	Replace
%SystemDrive%\ntldr	Replace	Replace
%SystemDrive%\Program Files\Resource Kit	Replace	Replace
%SystemDrive%\System Volume Information	Ignore	Ignore
%SystemDrive%\Temp	Replace	Replace
%SystemRoot%	Replace	Replace
%SystemRoot%\$NtServicePackUninstall$	Replace	Replace
%SystemRoot%\CSC	Replace	Replace
%SystemRoot%\debug		
%SystemRoot%\debug\UserMode		
%SystemRoot%\NTDS		
%SystemRoot%\Offline Web Pages	Ignore	Ignore
%SystemRoot%\regedit.exe	Replace	Replace
%SystemRoot%\Registration		
%SystemRoot%\repair	Replace	Replace

%SystemRoot%\security	Replace	Replace
%SystemRoot%\SYSVOL		
%SystemRoot%\SYSVOL\domain\Policies		
%SystemRoot%\Tasks	Ignore	Ignore
%SystemRoot%\Temp	Replace	Replace
c:\autoexec.bat	Replace	Replace
c:\boot.ini	Replace	Replace
c:\config.sys	Replace	Replace
c:\ntbootdd.sys	Replace	Replace
c:\ntdetect.com	Replace	Replace
c:\ntldr	Replace	Replace

The majority of the settings for the previous sections (User Rights Assignment Policies, Security Options Policies, Event Log Policies, Registry Policies and File System Policies) were taken from the W2K_DC.INF template. These settings are identical to the corresponding settings in the eGIACEnterprises.com domain and as such the modifications will not be discussed here.

Restricted Groups Policy

The W2K_DC.INF template does not define any Restricted Groups. GIAC Enterprises adds several groups to this list for the internal forest. The Enterprise Domain Administrators, Administrators, Schema Administrators, Domain Administrators and Account Operators are all added as Restricted Groups. Individual administrators from the GIACEnterprises.com forest are added to these as allowed members. This effectively eliminates the possibility of internal users escalating privileges. This same policy exists on the eGIACEnterprises.com forest.

Services Policy

Service	Startup	Permission
Alerter	Disabled	Configured
Application Management	Not defined	Not defined
Automatic Updates	Automatic	Configured
Background Intelligent Transfer Service	Automatic	Configured
ClipBook	Disabled	Configured
COM+ Event System	Disabled	Configured
Computer Browser	Automatic	Configured
DHCP Client	Disabled	Configured
DHCP Server	Automatic	Configured
Distributed File System	Disabled	Configured
Distributed Link Tracking Client	Not defined	Not defined
Distributed Link Tracking Server	Not defined	Not defined
Distributed Transaction Coordinator	Not defined	Not defined
DNS Client	Automatic	Configured
DNS Server	Automatic	Configured
Event Log	Automatic	Configured
Fax Service	Disabled	Configured
File Replication Service	Disabled	Configured
FTP Publishing Service	Disabled	Configured
IIS Admin Service	Disabled	Configured
Indexing Service	Disabled	Configured

Internet Connection Sharing	Disabled	Configured
Intersite Messaging	Disabled	Configured
IPSEC Policy Agent	Automatic	Configured
Kerberos Key Distribution Center	Automatic	Configured
License Logging Service	Automatic	Configured
Logical Disk Manager	Automatic	Configured
Logical Disk Manager Administrative Service	Not defined	Not defined
Messenger	Disabled	Configured
Net Logon	Not defined	Not defined
NetMeeting Remote Desktop Sharing	Disabled	Configured
Network Connections	Automatic	Configured
Network DDE	Not defined	Not defined
Network DDE DSDM	Not defined	Not defined
Network News Transport Protocol (NNTP)	Disabled	Configured
NT LM Security Support Provider	Not defined	Not defined
Performance Logs and Alerts	Not defined	Not defined
Plug and Play	Not defined	Not defined
Print Spooler	Disabled	Configured
Protected Storage	Not defined	Not defined
QoS RSVP	Not defined	Not defined
Remote Access Auto Connection Manager	Disabled	Configured
Remote Access Connection Manager	Disabled	Configured
Remote Procedure Call (RPC)	Not defined	Not defined
Remote Procedure Call (RPC) Locator	Not defined	Not defined
Remote Registry Service	Disabled	Configured
Removable Storage	Not defined	Not defined
Routing and Remote Access	Disabled	Configured
RunAs Service	Not defined	Not defined
Security Accounts Manager	Not defined	Not defined
Server	Automatic	Configured
Simple Mail Transport Protocol (SMTP)	Disabled	Configured
Smart Card	Disabled	Configured
Smart Card Helper	Disabled	Configured
SNMP Service	Not defined	Not defined
SNMP Trap Service	Not defined	Not defined
System Event Notification	Not defined	Not defined
Task Scheduler	Automatic	Configured
TCP/IP NetBIOS Helper Service	Disabled	Configured
Telephony	Disabled	Configured
Telnet	Disabled	Configured
Terminal Services	Automatic	Configured
Uninterruptible Power Supply	Not defined	Not defined
Utility Manager	Not defined	Not defined
Windows Installer	Not defined	Not defined
Windows Management Instrumentation	Not defined	Not defined
Windows Management Instrumentation Driver Extensions	Not defined	Not defined
Windows Time	Automatic	Configured
WMDM PMSP Service	Not defined	Not defined
Workstation	Disabled	Configured
World Wide Web Publishing Service	Disabled	Configured

Other than the DHCP Server, Terminal Services and Server services, the above list is identical to that of the eGIACEnterprises.com forest. These services were set to Automatic on the GIACEnterprises.com forest to support internal processes.

WkstZone OU Group Policy

Objects in the WkstZone consist of Windows XP Professional and Windows 2000 Professional workstations.

The WkstZone Group Policy does folder redirection for purposes of maintaining files on the file servers instead of on local workstations. This ensures that data is backed up and secured appropriately. Figure 8 below shows the redirection. Redirection is done using the advanced feature of My Documents redirection to ensure that space is adequately allocated. For example, R&D and I/T share file server 1 (GEFP01) while the rest of the organization is on file server 2 (GEFP02) by way of group memberships.

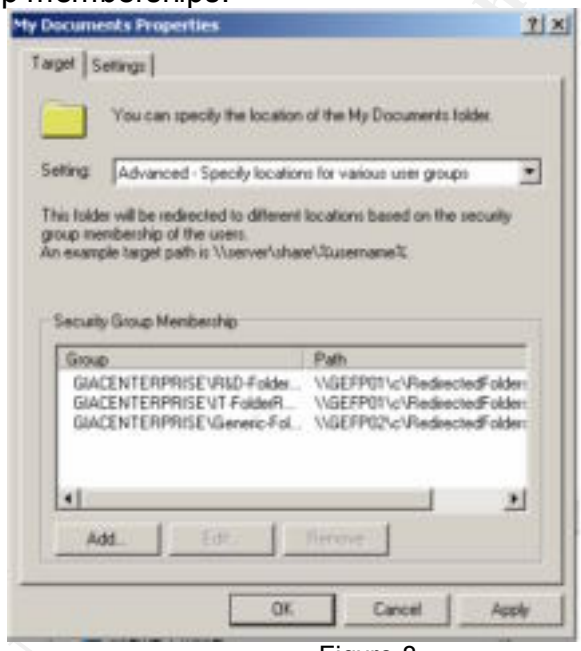


Figure 8

In addition to redirecting folders, distribution of the recent release of SP1 for Windows XP Professional is deemed critical to the security of the infrastructure. To quickly distribute this application, it was determined that Group Policy would do the distribution.

To do this, the update.msi file that comes with SP1 was added to a newly created share on the file server. A Group Policy Object was created specifically for this deployment and is setup to be distributed as machine-assigned, not user-deployed. The Group Policy Object is linked to the WkstZone OU as secondary under the WkstZone Group Policy Object.

To minimize load on the server, workstations are divided into three different groups and only one group has the appropriate permissions to install the package. The total distribution is scheduled to take five days. The first three days will cover the bulk of the users while the remaining two days for users who did not boot their machines on their assigned day.

Finally, the WkstZone Group Policy specifies some Administrative Template settings. The highlights from these settings are outlined below.

Policy	Setting	Notes
Code signing for device drivers	Enabled: Block	Ensures device drivers are digitally signed
Disable Registry editing tools	Enabled	Ensures that users cannot modify registry settings through regedit or regedt32
Disable Auto-Play	Enabled	Aids in prevention of viruses spreading through auto-played CDs
Disable Add/Remove Programs	Enabled	Another tool to ensure that users cannot add/remove programs from their workstations
Prohibit user from changing My Documents path	Enabled	This setting ensures that the folder redirection above works appropriately
Screen Saver Timeout	Enabled: 600 Seconds	This setting along with the following one will ensure that corporate policy of having a locked screen when the user is not at the desk is followed.
Password Protect the Screen Saver	Enabled	See above.

Section 5 - Additional Security Components

Network Time

Although not usually considered to be a security component, network time is critical to the security plan of any Windows 2000 network. By having the correct time on all servers and workstations on the network, Active Directory will function correctly. In addition, the timestamps in the log files will be synchronized. For any basic level of forensic work to take place, correct log entry times are needed.

From a cost perspective, this requires GIAC Enterprises to purchase and maintain two radio atomic clocks. This is viewed as a worthwhile expense so as to not open additional ports on the firewall.

Servers in the Data Zone and Corporate Server Zone each have a domain controller acting as the FSMO Infrastructure Master. As far as network time is concerned, all of the servers are a member of either GIACEnterprises.com or eGIACEnterprises.com domain. By default they are configured to receive time updates from the domain controller that has the FSMO role of Infrastructure Master. The Infrastructure Master receives its time from an atomic radio clock. This allows accurate network time to be distributed to the member servers without punching holes in the firewall to allow NTP traffic to pass. Workstations in the Corporate Workstation Zone will receive their time from whichever domain controller they are authenticated against.

From an Active Directory perspective, accurate, or at least consistent, network time must be established across all domain controllers. As Active Directory is a multi-master directory service (meaning any replica of the domain can be written to) accurate time is critical. For example, if two administrators are making changes to an attribute of a user object on two separate domain controllers, the decision on which one is enacted is based on the last change timestamp. This is done at the attribute level, not the object level, and therefore Active Directory data is kept valid by accurate timestamps.

ADAM

Although not implementing at GIAC Enterprises at this point, and to continue the discussion from Section 3, Active Directory in Application Mode (ADAM) is a hot topic at GIAC Enterprises. ADAM offers functionality above and beyond that of Windows 2000 Active Directory which should be of interest to directory and security professionals.

First, ADAM allows for two-way schema changes. In Windows 2000 Active Directory a schema change is a one-way change, meaning any additions to the schema cannot be backed out. With ADAM, those changes are reversible.

Second, ADAM is not hooked into the operating system in the way that Windows 2000 or even .Net Active Directory is. It is not reliant upon Active Directory DNS/DHCP and since it is not tied to the OS, multiple can be run. Microsoft envisions having multiple ADAMs running on a Windows .Net Server to service multiple applications. From a security point of view, if you can run multiple types of the same application on the same server, that means that that application can be run on multiple TCP/UDP ports. By default, LDAP runs on TCP 389. Attackers know this as well and will try to access Active Directory via this port or through tunneled access to this service. By moving the Active Directory service to a different port, the directory service can be obfuscated from a potential attacker.

Third, since domain policies dictate the account policies for an entire domain, this can be somewhat limiting when dealing with web applications. For example, a domain may contain a mix of internal, corporate users and external customers. These two sets of users are very likely to have different password change intervals, length and complexity requirements. In addition, there may be multiple web applications that belong to different parts of large organizations. While the organization may define a corporate policy for password changes, it may leave the web application password policy to each individual department or application. With Windows 2000, to accomplish multiple password policies, there would need to be multiple domains which isn't always an ideal scenario. By using ADAM, multiple single domain forests could be created that share information via Microsoft's Meta-Directory service to ensure the appropriate level of data sharing amongst applications.

Sources

In addition to the endnotes listed below.

Windows XP Service Pack 1 Deployment Guide, URL: http://www.microsoft.com/windowsxp/pro/downloads/servicepacks/sp1/spdeploy.asp

Windows 2000 Registry Guide, URL: http://www.winguides.com/registry/display.php/209/

MCSE Training Kit, Microsoft Windows 2000 Server, 2000, Microsoft Press

---

[i] Microsoft Windows 2000 Security Technical Reference, 2000, Microsoft Press

[ii] National Security Agency, Windows 2000 Domain Policy, URL: http://nsa2.www.conxion.com/win2k/guides/inf/w2k_domain_policy.inf

[iii] Microsoft Note on using HISECWEB.INF on a domain controller. URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q316347&

[iv] National Security Agency, Windows 2000 Domain Policy, URL: http://nsa2.www.conxion.com/win2k/guides/inf/w2k_domain_policy.inf

Introduction to Active Directory in Application Mode, URL, http://www.microsoft.com/windows.netserver/techinfo/overview/adam.mspx

LDAPGuru.org Article, URL, http://www.ldapguru.org/modules/news/article.php?item_id=187

ENTMag Article, URL, http://www.entmag.com/news/article.asp?EditorialsID=5472