Global Information Assurance Certification Paper

GIAC:

Windows 2000 Design & Security

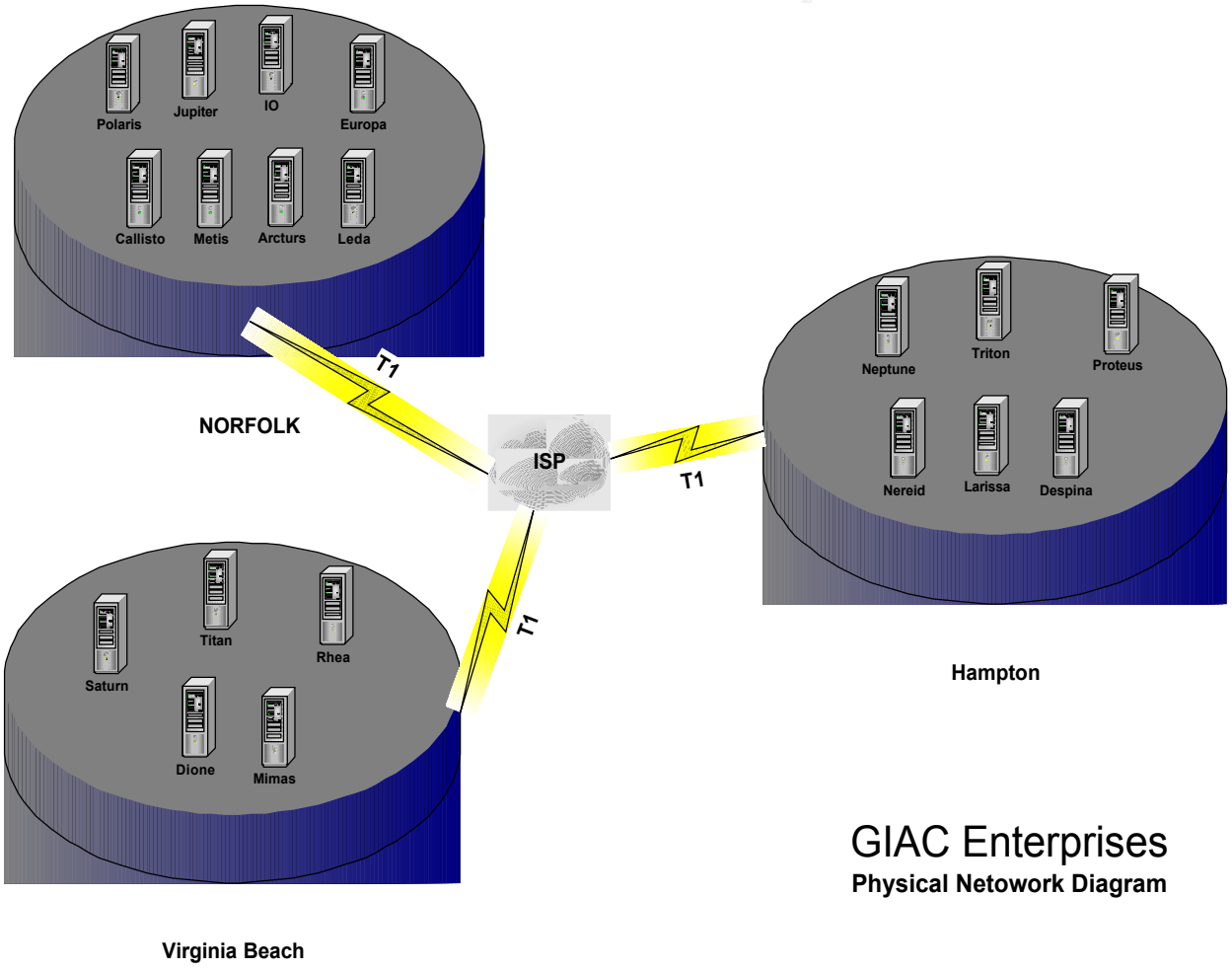
Level 2: Securing Windows
GCNT Practical Version 3.0
Option 1: Windows 2000 Design & Security

Shawn Canady
10/10/01

Shawn Canady
GCNT Practical

GIAC Enterprises is an e-business that deals in the online sale of fortune cookie sayings. GIAC is a small company consisting of 1000 employees. The company is based in Norfolk Virginia, with Branch offices in Hampton and Virginia Beach. Each office has it's own resident Information Technology (IT), staff With the IT staff in the Norfolk office setting the policies and procedures. Each of the sites has T1 access to the Internet. The goal of this paper is to document the design of a secure Windows 2000 network for GIAC Enterprises.

GIAC's Physical Network DESIGN



The above diagram shows GIAC's network layout. GIAC is split into 3 physical sites Norfolk, Virginia Beach, and Hampton. The first goal of the physical network design is to allow the users at each site 24x7 access to their workstations, departmental servers, and printers. The second goal is to keep network traffic generated by domain logins, DNS, and DHCP request local

to the site. The third is to allow each site to maintain domain operations even if connectivity is lost to the other two sites. The Fourth goal is to provide fault tolerance of critical services at each site. The Last goal is to locate each department's resources as close to the department as possible.

NORFOLK SITE (GIAC HQ)

GIAC's corporate headquarters is located in downtown Norfolk. It houses the Finance department, Human Recourses, Upper Management, and the main IT group. The Norfolk site uses a Switched Fast Ethernet for its LAN topology. It provides 10 mbps to the workstations and 100 mbps to each server. The network is divided among 5 class C subnets. A T1 connection gives the Norfolk site access to the outside world. There is also a dedicated T1 for all of GIAC's web services. Only traffic bound for the company's web services traverse this connection. The services required at this site are as follows: Active Directory, DNS, DHCP, 24x7 Domain authentication, File and Print sharing, database, web, E-mail. A number of Windows 2000 Servers were deployed to meet these needs. The following section is a description of key servers used to meet these requirements.

There are two groups of servers at the Norfolk site. One group handles enterprise wide services and the other handles services for the Norfolk site. The first group I will discuss will be the enterprise servers. These servers handle the FSMO and DNS services for the entire enterprise. I separated these services from the Norfolk services because I wanted them to be on dedicated boxes that would not see too much usage.

On of the most important decisions in a Windows 2000 implementation is the placement of the Flexible Single Master Operation (FSMO) Master Servers. In Windows 2000 all domain controllers are peers and can modify the active directory. Even though Windows 2000 is a multi-master system, some operations must be delegated to a single server. These servers are known as the FSMO Masters. There are five FSMO roles PDC emulator, RID Master, Infrastructure Master, Schema Master and Domain Naming Master. Since The Norfolk site houses the company headquarters and the main IT staff, I decided to place the first of the FISMO Servers there. The domain controller Polaris is the Schema and Domain Naming Master Server.

"The first domain controller promoted in a forest becomes the Domain Naming Master and Schema Master" (Boswell, 493). "The Schema master Controls read/write access to the schema naming context. "All other domain controllers in the forest have a read-only replica of the schema naming context" (Boswell, 493). "The Domain Naming Master controls the addition and removal of domains in the forest" (Boswell, 493). Because of the importance of theses to FSMO services, they were placed on a dedicated machine (Polaris). Because Polaris will only be used when changes to the schema and forest are needed, I chose not to make it a powerhouse box.

POLARIS

Role	Global Domain: DC, RID Master, PDC emulator, Infrastructure Master Global Catalog
OS	Windows 2000 Server
Patch	Windows 2000 Server Service Pack 2
CPU	Pentium III Xeon 933 megahertz
RAM	1 Gigabyte
Disk	36 gig RAID array
Location	Norfolk Site

The remaining three FSMO roles reside on the same machine. Arcturus is the PDC Emulator, RID Master and Infrastructure Master for GIAC Enterprises. "All security objects in Windows 2000 have a SID. The SID is a combination of the SID of the domain and the sequential number called the relative ID (RID)" (Boswell, 494). The RID Master handles the delegation of RIDs and the creation of RID pools. The PDC emulator acts like a NT 4.0 Primary Domain Controller. All the NT 4.0 Backup Domain Controllers replicate to the PDC emulator. "Windows 2000 assigns the job of coordinating and replicating group membership changes within a domain to a single FSMO, the Infrastructure Manager" (Boswell, 496).

I decided to put the remaining three FSMO Roles on one machine because GIAC's Windows 2000 domain is a native mode domain. In a native mode domain, each domain controller is capable of being the RID Master. When a DC needs more RIDs it contacts the current RID master and is passed the RID pool. Only Windows 2000 servers and workstations can join a native mode domain. Therefore, there is no need for a PDC emulator in a native mode domain because there are no BDCs. Putting these services on one box allows me to keep control of where these services reside. Also, because these services will not be utilized, the machine has more resources that it can allocate to the Infrastructure service.

ARCTURS

Role	Global Domain: DC, RID Master, PDC emulator, Infrastructure Master
OS	Windows 2000 Server
Patch	Windows 2000 Server Service Pack 2
CPU	Pentium III Xeon 933 megahertz
RAM	512
Disk	20 gig RAID array
Location	Norfolk Site

The last of the enterprise servers is Canopus. Canopus's only job is to provide DNS fault tolerance. Canopus runs Windows 2000 Dynamic DNS. Integrating DNS with Active directory makes DNS a multi-master service. Every DNS server can have it's records updated and can receive replicated changes from other DNS servers. Native mode Windows 2000 does not require Net Bios or WINS. For this reason, I decided not to use these services for name resolution and implemented a purely DNS architecture. Going strictly DNS will reduce the amount of traffic dedicated to maintaining a consistent naming database. Since all DNS records are stored in

Active Directory, they can be replicated along with the rest of the objects.

CANOPUS

Role	**Global domain DNS server**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Pentium III Xeon 933 megahertz**
RAM	**512**
Disk	**20 gig RAID array**
Location	**Norfolk Site**

The next group of servers provides services to the Norfolk site. There are approximately 600 users located at the Norfolk site. They are split into three departments, Upper Management, Norfolk IT staff, and Human Resources. First I will discuss the servers that provide Active Directory services, DNS, and DHCP. Next I will discuss key application and file and print servers. Last I will discuss the corporate web server.

The Active Directory, DNS, and DHCP services are split between a pair of domain controllers. They are Jupiter and IO. I decided to use two machines for fault tolerance and redundancy. Both Jupiter and IO will authenticate users and hold a copy of the Active Directory. Jupiter will also serve as the Norfolk's site DNS server. It will be configured as the preferred DNS server for machines at the Norfolk site. IO will be the DHCP server for the Norfolk site. It will contain all the active DHCP scopes, for fault tolerance the scopes will be mirrored on Jupiter but not activated. The hardware configuration for these two machines is identical.

Jupiter

Role	**Child domain: DC, RID Master, PDC emulator, Infrastructure Master DNS, DHCP (scope not activated)**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Norfolk Site**

IO

Role	**Child domain: DC, DNS, DHCP, Global Catalog**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Norfolk Site**

Metis is the Norfolk site's bridgehead server. "A bridgehead server (BHS) is a DC that performs replication operations with DCs in another site" (Clark, 55). Microsoft suggest that there be at least one Global Catalog at each site. Metis also serves as the local Global Catalog for the Norfolk site Exchange Server.

METIS

Role	**Child domain: DC, Global Catalog, Bridgehead**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Norfolk Site**

Each department has it's own File server which also doubles as a print server. The configurations of these servers are identical so will discuss the basic configuration and not each individual file and print server. The file servers will be used to store user files and directories. Each user gets private space on the server. Each department will also have a common area where everyone in the department will be able to store files for other department workers can access them. Theses servers will also hold print queues for each department's printers. These servers will see a lot of activity and need to hold a lot of data.

GENERIC FILE & PRINT SERVER

Role	**Child domain: File & Print**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 1 Gigahertz**
RAM	**1 Gigabyte**
Disk	**72 gig RAID 5 array**
Location	**Norfolk, Hampton, Virginia Beach Site**

Next up is the Norfolk mail server Europa. GIAC uses Exchange 2000 as its email solution. Exchange 2000 is tightly tied to Active Directory. Its information is replicated along with the rest of active directory. Because of this there must be a Global Catalog server at each site that has an exchange server. Each of GIAC's sites has it's own Exchange server to cut down on mail access traffic. Exchange 2000 requires a powerful machine with a large amount of disk space.

EUROPA

Role	**Mail Server**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
Application	**Exchange 2000**

App Patch	Exchange 2000 Service Pack 2
CPU	Dual Pentium III Xeon 1 Gigahertz
RAM	1 Gigabyte
Disk	72 gig RAID 5 array and a 18 gig RAID 0 1 array for the transaction log
Location	Norfolk Site

The last of the application servers is Callisto, the Human Resources database server. Callisto runs SQL server 2000 Standard edition as its database engine. This database holds employee records and other HR related information for the company. The main users of this database are the HR staff.

CALLISTO

Role	Mail Server
OS	Windows 2000 Server
Patch	Windows 2000 Server Service Pack 2
Application	SQL 2000 Standard
App Patch	SQL 2000 Service Pack 2
CPU	Pentium III Xeon 1 Gigahertz
RAM	1 Gigabyte
Disk	72 gig RAID 5 array
Location	Norfolk Site

Leda is the GIAC IIS 5.0 web server. This server houses the company's main web site and is updated frequently with the latest company news. Leda is located on a separate subnet in GIAC's service network. Leda is a public access web server that has links to GIAC's other web services such as E-commerce. GIAC's other web services lie outside the scope of this paper. Leda does not interact with the company's internal active directory for security reasons

LEDA

Role	Web Server
OS	Windows 2000 Server
Patch	Windows 2000 Server Service Pack 2, 15 August 2001 Cumulative Patch for IIS Microsoft Security Bulletin MS01-044
Application	IIS 5.0
CPU	Dual Pentium III Xeon 1 Gigahertz
RAM	1 Gigabyte
Disk	36 gig RAID 5 array
Location	Norfolk Site

VIRIGINIA BEACH SITE (Sales & Marketing)

The second GIAC site is located in Virginia Beach, Virginia. It is home to the Sales & Marketing departments. There are approximately 300 users located at this site. The Va. Beach site uses a Switched Fast Ethernet for its LAN topology. It provides 10 mbps to the workstations and 100 mbps to each server. The network is divided between 2 class C subnets. A T1 connection gives the Va. Beach site access to the outside world.

The network design for this site follows the goals as the Norfolk site. The services at this site are a bit different from the Norfolk site in that there is no enterprise responsibility at this site. The Windows 2000 services located here only support this site. First I will discuss the servers that provide Active Directory services, DNS, and DHCP.

Like the Norfolk site Va. Beach depends on two domain controllers to provide User authentication, DNS and DHCP. Theses machine are Saturn and Titan. Like Jupiter and IO, Saturn and Titan will authenticate users and hold a copy of the Active Directory. Saturn will also serve as the Va. Beach's site DNS server. It will be configured as the preferred DNS server for machines at the Va. Beach site. Titan will be the DHCP server for the Va. Beach site. It will contain all the active DHCP scopes, for fault tolerance the scopes will be mirrored on Saturn but not activated.

Saturan

Role	**Child domain: DC, DNS, DHCP (scope not activated)**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID 5 array**
Location	**Virginia Beach Site**

TITAN

Role	**Child domain: DC, DNS, DHCP, Global Catalog**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID 5 array**
Location	**Virginia Beach Site**

Mimas is Va. Beach's Global Catalog server. It is located here to support Va. Beach's Exchange 2000 server. Dione mirrors its Norfolk counter part Metis in configuration.

Dione

Role	**Child domain: Global Catalog, Bridgehead**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**

CPU	**Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Norfolk Site**

Rhea is Va. Beach's resident Exchange 2000 server. Because it supports half as many users as it's Norfolk counter part, Rhea is not as powerful as Europa

RHEA

Role	**Mail Server**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
Application	**Exchange 2000**
App Patch	**Exchange 2000 Service Pack 2**
CPU	**Dual Pentium III Xeon 1 Gigahertz**
RAM	**1 Gigabyte**
Disk	**72 gig RAID 5 array and a 18 gig RAID 0 1 array for the transaction log**
Location	**Virginia Beach Site**

Mimas is the sales SQL 2000 database. This machine holds information such as sales statistics for fortune cookies for the U.S. for the last 5 years. The sales team uses this database for it's sales projection and profit estimations.

Mimas

Role	**Mail Server**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
Application	**SQL 2000 Standard**
App Patch	**SQL 2000 Service Pack 2**
CPU	**Pentium III Xeon 1 Gigahertz**
RAM	**1 Gigabyte**
Disk	**72 gig RAID 5 array**
Location	**Norfolk Site**

HAMPTON SITE (Research & Development)

The last GIAC site is located in Hampton Virginia. This is home to GIAC's Research and Development department. This site has approximately 230 users. The LAN topology is a Switched Fast Ethernet. It provides 10 mbps to the workstations and 100 mbps to each server. The network is divided between 2 class C subnets. A T1 connection gives the Va. Beach site access to the outside world.

The Hampton site closely mirrors GIAC's other two sites. Hampton also depends on two domain controllers to provide user authentication, DNS and DHCP. Theses machine are Neptune and Triton. Both will authenticate users and hold a copy of the Active Directory. Neptune will also serve as the Hampton's site DNS server. It will be configured as the preferred DNS server for machines at the Hampton site. Titan will be the DHCP server for the Hampton site. It will contain all the active DHCP scopes, for fault tolerance the scopes will be mirrored on Saturn but not activated. Both servers have dual Pentium III Xeon 933 megahertz processors with 1 gig of ram, and a 36 gig RAID array.

Neptune

Role	**Child domain: DC, DNS, DHCP (scope not activated)**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Hampton Site**

TRITON

Role	**Child domain: DC, DNS, DHCP, Global Catalog**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Dual Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Hampton Site**

Larrissa is the Global Catalog placed at the Hampton site. Proteus is Hampton's Exchange 2000 Server.

Larrissa

Role	**Child domain: Global Catalog, Bridgehead**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
CPU	**Pentium III Xeon 933 megahertz**
RAM	**1 Gigabyte**
Disk	**36 gig RAID array**
Location	**Hampton Site**

EUROPA

Role	**Mail Server**
OS	**Windows 2000 Server**
Patch	**Windows 2000 Server Service Pack 2**
Application	**Exchange 2000**
App Patch	**Exchange 2000 Service Pack 2**
CPU	**Dual Pentium III Xeon 1 Gigahertz**

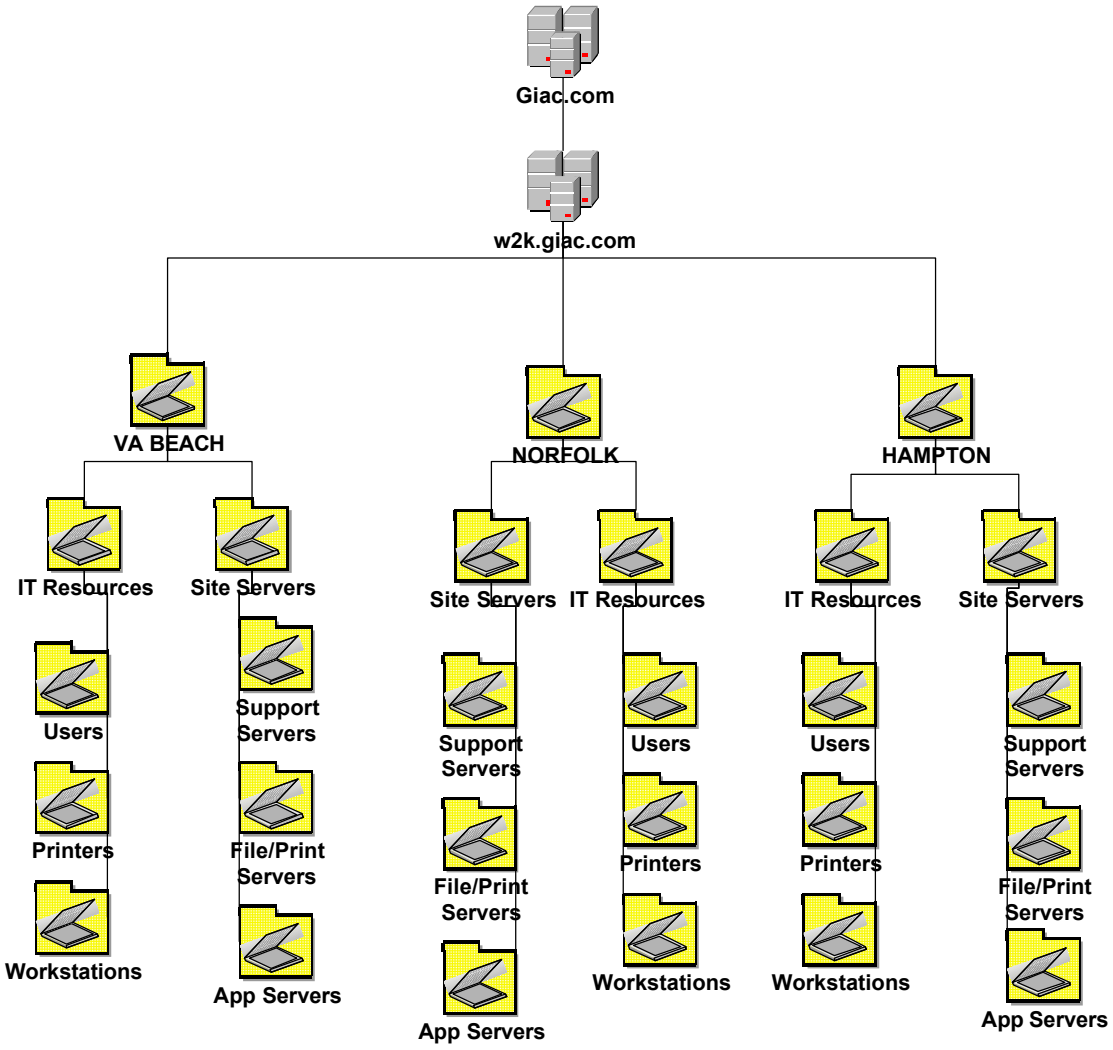
RAM	**1 Gigabyte**
Disk	**72 gig RAID 5 array and a 18 gig RAID 0 1 array for the transaction log**
Location	**Hampton Site**

Network Design Recap

The GIAC Windows 2000 network servers are divided into two groups. One group handles services for the entire enterprise and domain. The other group handles services for each site. Two servers handle the FSMO Master rolls. These servers reside at the Norfolk site. Each GIAC site has a pair of domain controllers. This enables user authentication to occur locally instead of over the WAN connection. Having two domain controllers at each site also provides fault tolerance for user authentication and DHCP. DNS is fault tolerant by configuring each client with Canopus as the secondary DNS server. Each site also has a Global Catalog and Exchange 2000 server. Having theses five servers at each site keeps traffic such as user authentication, DNS lookups, DHCP requests and user email access local instead of using the WAN link. This frees up bandwidth for Active Directory and makes accessing these services faster for the user. Each site also has the resident departments application and file & print servers. This gives GIAC users access to departmental resources even if the site looses WAN connectivity. The next section focuses on GIAC's Active directory.

ACTIVE DIRECTORY DESIGN

The heart and soul of Windows 2000 is Active Directory. Its design is the most critical part of a Windows 2000 rollout. The design goals for GIAC's Active directory are ease of administration, performance, and security. The following section covers GIAC's Active Directory structure, sites, administrative benefits, performance issues, and security. I will discuss the Active Directory structure in three sections. The first section will cover the tree level. Next I will discuss the domain level. Then I will cover the OU level. Below is a diagram of GIAC's Active Directory.



TREE DESIGN

GIAC's divisions all share the same parent DNS domain name (giac.com). Therefore I organized them into a tree rather than a forest. "A tree is two or more domains in a hierarchical domain structure where one domain serves as a DNS root domain for the others" (Fossen, 57). If at some time in the future, there becomes a need for part of GIAC to have it's own tree, then it will be easy to add the new tree to form a forest. "A Forest is two or more domains where one domain is not a DNS sub domain of the other(s), but they are still joined with two-way transitive trusts and they still replicate a shared Schema, configuration NC and Global Catalog" (Fossen, 57).

A single tree has less administrative overhead than a forest. In a single tree design, administrators do not have to manage trust relationships at the forest level. There is also no replication of the active directory at the forest level.

DOMAIN DESIGN

"A domain is a single partition of the Active Directory" (Microsoft Corporation, Best Practice Active... 28). Domains in Windows 2000 act as replication boundaries. The domain structure for GIAC consists of a dedicated root domain and a single, global child domain. "A single global child domain of the forest root domain has all user, computer, and group accounts in a single child domain, except those of directory administrators residing in the forest root." (Microsoft Corporation, Best Practice Active... 33). The single root domain is giac.com and the global child domain is w2k.giac.com. The users, computers, and group accounts all exist in the child domain. The root contains the directory administrators accounts and the root domain DC, GC and DNS servers.

Using a dedicated root domain limits membership of the administrators in the root domain. This reduces the likelihood that an administrator could make a change that would affect the entire tree. The dedicated root domain never becomes obsolete because it acts only as the forest root.

Because the root domain will only contain the administrator's accounts and 3 servers it will relatively small in size. "A small root domain can easily be replicated anywhere on your network to provide protection against geographically centered catastrophes" (Microsoft Corporation, Best Practice Active... 32). So, having a dedicated root domain will not heavily impact Active Directory replication performance.

This design also simplifies administration. Instead of having to manage trust with peer domains, one group of administrators can be given control of the root domain and have reign over the whole tree. It also allows for the centralization of the IT staff with distributed administrative responsibility. The tree/forest administrators set the policy for the entire tree with administrators of the child domain taking their direction.

On the security end, only administrators in the root domain will be able to make enterprise changes. This adds another layer of protection to the Enterprise Admins and Schema Admins groups. Having a dedicated root domain allows an organization to have a stricter security policy on members of the root domain.

ORGINIZATIONAL UNIT DESIGN

"OUs are containers within domains that can contain other OUs, users, groups, computers, and other objects" (Microsoft Corporation, Best Practice Active... 72). For the OU structure I chose a design based on location and then by user resources and servers. Each of the three sites has a dedicated OU which contain child OUs containing user resources and site resources.

The Norfolk site OU contains child OUs containing user resources and site servers. The User Resources OU contains an account OU for users in Upper Management and Human Resources. The other two children of the User Resources OU contain the printers and workstations located at the Norfolk site. The Norfolk OU also contains the Site Servers OU. The Hampton and Virginia Beach OUs are structured like the Norfolk OU. All three OUs are detailed in the next three tables.

NORFOLK ORGANIZATIONAL UNIT

OU	Parent OU	Purpose
Norfolk	**NA: Parent OU**	**Contains accounts and resources located at the Norfolk site**
Site Servers	**Norfolk each**	**Contains site server OUs**
Support Servers	**Site Servers**	**Contains server used to support the Norfolk site (dc,gc,dns, email, etc…)**
File&Print Servers	**Site Servers**	**Contains File & Print servers Located at the Norfolk site.**
App Servers	**Site Servers**	**Contains application servers located at the Norfolk site.**
User Resources	**Norfolk**	**Contains users, workstation, and printer OUs for the Norfolk**
Users	**IT Resources**	**Contains user accounts and groups located at the Norfolk site**
Printers	**IT Resources**	**Contains printers located at the Norfolk site**
Workstations	**IT Resources**	**Contains Workstations located at the Norfolk site**

The VA. Beach Site OU contains sub OUs For the resources and users of the Sales and Marketing department and Beach IT.

Virginia BEACH ORGANIZATIONAL UNIT

OU	Parent OU	Purpose
VA_Beach	**Parent OU**	**Contains accounts and resources located at the VA, beach site**
Site Servers	**VA_Beach**	**Contains site server OUs**

Support Servers	**Site Servers**	**Contains server used to support the VA Beach site (dc,gc,dns, email, etc…)**
File&Print Servers	**Site Servers**	**Contains File & Print servers Located at the VA. Beach site.**
App Servers	**Site Servers**	**Contains application servers located at the VA. Beach site.**
User Resources	**VA_Beach**	**Contains users, workstation, and printer OUs for the VA. Beach site**
Users	**IT Resources**	**Contains user accounts and groups located at the VA. Beach site**
Printers	**IT Resources**	**Contains printers located at the VA. Beach site**
Workstations	**IT Resources**	**Contains Workstations located at the VA. Beach site**

The Hampton Site OU contains sub OUs For the resources and users of the Research and Development department and Hampton IT.

HAMPTON ORGANIZATIONAL UNIT

OU	Parent OU	Purpose
Hampton	**Parent OU**	**Contains accounts and resources located at the Hampton site**
Site Servers	**Hampton**	**Contains site server OUs**
Support Servers	**Site Servers**	**Contains server used to support the Hampton site (dc,gc,dns, email, etc…)**
File&Print Servers	**Site Servers**	**Contains File & Print servers Located at the Hampton site.**
App Servers	**Site Servers**	**Contains application servers located at the Hampton site.**

User Resources	**Hampton**	**Contains users, workstation, and printer OUs for the VA. Beach site**
Users	**IT Resources**	**Contains user accounts and groups located at the VA. Beach site**
Printers	**IT Resources**	**Contains printers located at the Hampton site**
Workstations	**IT Resources**	**Contains Workstations located at the Hampton site**

Before I discuss the impact on administration this OU design has, I will give a brief description of GIAC's IT organization. GIAC's IT organization is a centralized department with distributed administration. GIAC's IT staff is separated into two main groups enterprise support and site support. The enterprise group is located at the Norfolk site. The enterprise support group is responsible for the forest and domain operation and maintenance. This group sets the over all IT policy with input from the site support administrators. The Site Support group is divided into three teams. Each of the teams is located at and responsible for one of the sites. A site administrator heads each site group up. The site admin take direction from the Enterprise group on site security and group policy. The enterprise group is responsible for developing the group policy.

Taking into account the GIAC IT staff's structure, the OU were designed with centralized control with delegated responsibility in mind. By breaking the domain into Site OUs, it is possible to give each Site Administrator complete control over the users and resources at his site but not at any other site. By breaking each site into user resources and site servers, each site administrator can give specific groups in his staff rights to manage specific resources at the site. For example, the Helpdesk staff can be given full admin rights to the site's Workstation and Printers OUs, and only the rights to change user passwords on the Users OU.

The following is a description of the delegation of IT responsibility through out GIAC's Active directory. The Enterprise Admins group has total control over GIAC's tree. At the w2k.giac.com domain level, the domain admins group has complete control over everything in the w2k domain. The w2k domain admins are a sub team in the enterprise group. They are responsible for the domain level operations. The domain admins assign permissions to manage the site OUs.

The site admins do not belong to a built in administrators group, instead they have regular user accounts that are given full control over a site OU. They posses the ability to create, delete, and manage user accounts and groups within the site OU. They also have the ability to reset, passwords on user account, read all user information, modify group membership, and manage

group policy links. Site admins are limited to two IT staff members per site.

Each site has a group of IT staff dedicated to the day-to-day administration of the site servers. These individuals have the right to manage only the computer objects in the Site Servers OU. To further distribute the authority, the server support staff is divided into three groups, the support servers group, the file/print servers group and the application servers group. Each group has right to manage servers located in their respective OUs. The support servers group manages the domain controllers and global catalogs and Exchange servers located at each site. The File/Print servers group manages the file and printer servers at each site. This group also has the right to manage printer objects in the Printers OU. The Application Servers group has administrative rights to all computers and shared folder objects under, the app server OU. The members of this group also specialize in the applications that the servers host. Each site has a group of IT staffers that provide helpdesk services. This group has the ability to reset passwords on user accounts in the Users OU. Each site's IT staff follows this structure.

This design increases security in the Active Directory by limiting the scope of the helpdesk, server support, site support and domain support IT staff. Each group has control over the resources necessary to carry out their jobs. Only the domain administrators have full control over the domain. Only the enterprise administrators have complete control over the entire tree.

Because the OU are only nested three deep, Active Directory searches are not too costly. The performance of active directory replication is also an issue. To increase the performance of inter-site replication, Active Directory sites are used. A site is a set of well-connected IP subnets. Each physical GIAC site constitutes an Active Directory site. Sites are use to optimize replication between domain controllers and locate the closet domain controller to a client. Site links connect Active Directory sights. Sight links have a cost, schedule and interval associated with them. The cost of the link is based on the available bandwidth on the link. The higher the available bandwidth, the lower the cost. The schedule defines the length of time that replication can take place between sites. The interval is the frequency that replication takes place between sites. You can also choose the protocol used for replication (TCP/IP or SMTP). The following two charts describe the GIAC Active directory sites and site links.

Site	IP addresses
Norfolk	**197.16.1.0, 197.16.2.0, 197.16.3.0, 197.16.4.0, 197.16.5.0**
Hampton	**197.16.6.0, 197.16.7.0**
Virginia Beach	**179.16.8.0, 197.16.9.0**

Site Link	Available bandwidth	Cost	Schedule	Interval
Norfolk1	**500 kbps/sec**	**379**	**Always**	**4 hours**
Hampton1	**760 kbps/sec**	**355**	**Always**	**4 hours**
VABeach1	**760 kbps/sec**	**355**	**Always**	**4 hours**

As the table shows the T1 links between the sites are not heavily utilized. The cost is calculated by dividing 1024 by the log (available bandwidth (Kbps)). This equation was taken from Microsoft's "Best Practice Active Directory Design for Managing Windows Networks" web document. The schedule is set to replicate every 4 hours 7 days a week. Replication takes place using the TCP/IP protocol. By using sites and site links, the performance of active directory replication is increased. If the available bandwidth on the links were to change, the site links can be reconfigured to maintain the best performance possible.

GROUP POLICY & SECURITY

Group Policy is the primary tool used to secure a windows 2000 network. It gives administrators the ability to manage system security, user settings, and application deployment. Group Policy Objects (GPOs) contain the settings that are applied to systems and users. GPOs are applied by linking them to domain, OUs and sites. The following section details GIAC's Group Policy and security settings. Because there are 400 some settings that can be set in-group policy, I will only discuss significant settings.

GIAC.COM GROUP POLICY

Since giac.com is the dedicated root directory, it has a stronger security policy than its child domain. First I will discuss the account Policies. The only accounts that exist in the giac.com domain are administrator accounts. Because these accounts have the ability to make changes that affect the entire tree, the domain account policy must be strict.

Account Policies

Policy	Computer Setting
Enforce password history	**10**
Maximum password age	**60 days**
Minimum password age	**1**
Minimum password length	**10**
Password must meet complexity Requirements	**Enabled**
Store Passwords using reversible encryption	**Disable**

As shown in the above table, the password history is set to 10. This causes Windows to keep track of the users last to passwords. The max password age is set to 60 days. Theses two settings guarantee that a user will not be able to reuse a password for at least 600 days. The Minimum password length is set to ten characters. The longer a password is the longer it takes to crack. Requiring long passwords increases the chance that a hacker might get caught trying to crack a password. Enabling the complexity requirement requires that all passwords contain characters from three of the following groups (uppercase alpha, lowercase alpha, numeric, and special characters). Passwords are not stored using reversible encryption.

Account Lockout Policy

Policy	Computer Setting
Account lockout duration	**480 minutes**
Account lockout threshold	**3 invalid logon attempts**
Reset account lockout counter after	**480 minutes**

Because of the strict security requirement of the root domain, the account lockout duration is 480 minutes or 8 hours. The same goes for the reset counter. The lockout threshold is 3 invalid attempts. If a hacker were to attempt to guess a password, after the third invalid attempt the account would be locked for 8 hours. This reduces the likely hood that an account will be compromised.

Kerberos Policy

Policy	Computer Setting
Enforce user logon restrictions	**Enabled**
Maximum lifetime for service ticket	**600 minutes**
Maximum lifetime for user ticket	**10 hours**
Maximum lifetime for user ticket renewal	**3 days**
Maximum tolerance for computer clock synchronization	**5 minutes**

The above chart shows the kerberos policy settings. “Session tickets are validated by checking the user rights policy on the destination computer. The user must have Log on Locally or Access This Computer From Network rights before a session ticket is granted” (Bragg, 331). The max life for the service ticket and the maximum lifetime for the user ticket are both 10 hours. The user ticket stays active for the normal day (9-10 hours). The ticket can be renewed for 3 days.

W2K.GIAC.COM GROUP POLICY

The w2k domain holds all the user accounts, workstations, and printers. Because the domain users have varying need for access, the domain security policy will be general..

The w2k domain will have two GPO applied to it. One GPO will be accessed by the users the other will be accessed by the IT and R&D departments. Because the IT staff accounts have more privileges in the domain than regular user accounts, the IT GPO has stricter settings. Because the information that the R&D department works with is so crucial to GIAC’s success, the R&D users require a stricter GPO. They will have the same GPO as the IT department.

W2K.GIAC.COM GROUP POLICY (User)

Account Policies

Policy	Computer Setting
Enforce password history	10
Maximum password age	180 days
Minimum password age	1
Minimum password length	8
Password must meet complexity Requirements	Enabled
Store Passwords using reversible encryption	Disable

Account Lockout Policy

Policy	Computer Setting
Account lockout duration	60 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	60 minutes

Kerberos Policy

Policy	Computer Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600
Maximum lifetime for user ticket	12 hours
Maximum lifetime for user ticket renew	5 days
Maximum tolerance for computer clock synchronization	5 minutes

As the above charts show, the user's GPO contains more relaxed security settings. Because users will only be able to access IT resources needed to perform their jobs, their security policy can be relaxed a bit. Users needing access to high security resources will have a stricter GPO applied. This GPO will be accessible to the Human Resources, Upper Management, and Sales & Marketing user groups.

In order to make the user GPO accessible to only the previously mentioned groups, the GPO's discretionary access control lists (DACLs) must be changed. To include or exclude a group from the effects of a GPO, the Access Control Entries (ACEs) within the DACLs must be modified. By unchecking the Allow Group Policy for Authenticated Users check box and removing the Read ACE, a GPO can be made invisible to a group of users. By taking these actions, the user will not be able to process the GPO. This will improve logon performance when using multiple GPOs at the domain level. Using this method for assigning access to GPOs, The IT and R&R departments can be given stricter security settings than the rest of GIAC's users. Below are the GPO settings for the IT and R&D departments.

W2K.GIAC.COM GROUP POLICY (IT/R&D)

Account Policies

Policy	Computer Setting
Enforce password history	10
Maximum password age	60 days
Minimum password age	1
Minimum password length	10
Password must meet complexity Requirements	Enabled
Store Passwords using reversible encryption	Disable

Account Lockout Policy

Policy	Computer Setting
Account lockout duration	480 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	480 minutes

Kerberos Policy

Policy	Computer Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	5 days
Maximum tolerance for computer clock synchronization	5 minutes

Next, I will discuss the default domain controller GPO. Because every domain controller in windows 2000 holds a read/write copy of the Active Directory database, their security policies must be very strict. The following GPO applies to domain controllers in the giac.com and w2k.giac.com domains.

DOMAIN CONTROLLER GROUP POLICY

Account Policies

Policy	Computer Setting
Enforce password history	10
Maximum password age	60 days
Minimum password age	1
Minimum password length	10

Password must meet complexity Requirements	**Enabled**
Store Passwords using reversible encryption	**Disable**

Account Lockout Policy

Policy	Computer Setting
Account lockout duration	**480 minutes**
Account lockout threshold	**3 invalid logon attempts**
Reset account lockout counter after	**480 minutes**

Kerberos Policy

Policy	Computer Setting
Enforce user logon restrictions	**Enabled**
Maximum lifetime for service ticket	**600**
Maximum lifetime for user ticket	**10 hours**
Maximum lifetime for user ticket renewal	**3 days**
Maximum tolerance for computer clock synchronization	**5 minutes**

The account and kerberos policies have the same settings as the IT department's GPO.

LOCAL POLICIES

Audit Policy

Policy	Computer Setting
Audit account logon events	**Success, Failure**
Audit account management	**Success, Failure**
Audit directory service access	**Success, Failure**
Audit logon events	**Success, Failure**
Audit object access	**Success, Failure**
Audit policy change	**Success, Failure**
Audit privilege use	**Success, Failure**
Audit process tracking	**No auditing**
Audit system events	**Success, Failure**

The audit policy is set to keep track of all major events on the domain controller. It keeps track of who is accessing the machine, making changes to the directory service and who is making changes to user rights.

User Rights Assignment

Policy	Computer Setting
Access this computer from the network	**Domain Users**
Act as part of the operating system	**None**
Add workstations to domain	**Administrators**

Back up files and directories	**Backup Operators Administrators**
Bypass traverse checking	**Server Operators Backup Operators Administrators**
Change the system time	**Administrators**
Create a pagefile	**Administrators**
Create a token object	**None**
Create permanent shared objects	**Not defined**
Debug programs	**None**
Deny access to this computer from the network	**Not defined**
Deny logon as a batch job	**Not defined**
Deny logon as a service	**Not defined**
Deny logon locally	**Not defined**
Enable computer and user accounts to be trusted for delegation	**Not defined**
Force shutdown from a remote system	**Not defined**
Generate security audits	**Not defined**
Increase quotas	**Not defined**
Increase scheduling priority	**Not defined**
Load and unload device drivers	**Not defined**
Lock pages in memory	**Not defined**
Log on as a batch job	**Not defined**
Log on as a service	**Replicators**
Log on locally	**Server Operators Backup Operators Administrators**
Manage auditing and security log	**Administrators**
Modify firmware environment values	**Server Operators Backup Operators Administrators**
Profile single process	**Not defined**
Profile system performance	**Not defined**
Remove computer from docking station	**Not defined**
Replace a process level token	**None**
Restore files and directories	**Backup Operators**
Shut down the system	**Server Operators Administrators**
Take ownership of files or other objects	**Administrators**

As shown in the User Rights Assignment portion of the GPO, Regular users have very limited right on the domain controller. Domain users only have the right to access the computer from the network. The administrators do no have every right on the domain controller. By

limiting the Administrators right to those that they need to do their jobs, you create a more secure system. Note that only the Administrators can shutdown the machine, manage security logs, take ownership of files and directories, and add workstations to the domain. The administrator is not given the right to access the domain controller from the network to force them to make changes on the local system.

Security Options

Policy	Computer Setting
Additional restrictions for anonymous connections	No Access Without Explicit Permissions
Allow server operators to schedule tasks (domain controllers only)	Disable
Allow system to be shut down without having to log on	Disable
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Disabled
Automatically log off users when logon time expires	Not defined
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Enabled
Digitally sign client communication (when possible)	Disabled
Digitally sign server communication (always)	Enabled
Digitally sign server communication (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Enabled
Do not display last user name in logon screen	Disabled
LAN Manager Authentication Level	Send NTLMv2 responses only\Refuse LM & NTLM
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled

Prompt user to change password before expiration	**14 days**
Recovery Console: Allow automatic administrative logon	**Disabled**
Recovery Console: Allow floppy copy and access to all drives and all folders	**Disabled**
Rename administrator account	**Stimpy**
Rename guest account	**Ren**
Restrict CD-ROM access to locally logged-on user only	**Enabled**
Restrict floppy access to locally logged-on user only	**Enabled**
Secure channel: Digitally encrypt or sign secure channel data (always)	**Enabled**
Secure channel: Digitally encrypt secure channel data (when possible)	**Disabled**
Secure channel: Digitally sign secure channel data (when possible)	**Disabled**
Secure channel: Require strong (Windows 2000 or later) session key	**Enabled**
Send unencrypted password to connect to third-party SMB servers	**Disabled**
Shut down system immediately if unable to log security audits	**Disabled**
Smart card removal behavior	**Lock Workstation**
Strengthen default permissions of global system objects (e.g. Symbolic Links)	**Enabled**
Unsigned driver installation behavior	**Do Not Allow**
Unsigned non-driver installation behavior	**Do Not Allow**

The above chart shows the settings for the security options of the GPO. The settings in red text will be discussed in more detail. The Allow system to be shutdown with out having to log on option has been disabled. This ensures that only users that have the right to log into the server can safely shut it down. The page file can contain user account and passwords and should be cleared before the server is shutdown. Because GIAC runs a native mode Windows 2000 domain, all clients and servers are capable of SMB signing. To maintain the high security, clients and servers are always required to digitally sign communication.

The Control + Alt + Delete requirement is enabled to force the warning box to pop up when a user tries to log in. By default the last user that successfully logs into the server, will be displayed in the login box. Allowing the last user name to be displayed, opens up the possibility that a hacker could obtain a valid user name to the server. To prevent this form happening, the display last user name in logon screen is disabled. By setting the LAN MANAGER AUTHENTICATION LEVEL to send NTLMv2 responses only\Refuse LM & NTLM, the server

will only use the more secure NTLMv2 when Kerberose authentication fails. Again, because GIAC is a Native mode domain, NTLMv2 can be exclusively used. Windows 9x clients may have compatibility issues with NTLMv2.

The administrator and guest account names should be changed to make it harder for hackers to compromise the accounts. The CD and floppy drives are only accessible to users logged on locally. The secure net logon channel is set to always be encrypted and the secure channel requires a strong session key. These settings provide the highest security on the communication between domain controllers and can be set with Windows 2000 running in native mode. To maintain high security on authentication and server communication the unencrypted password to connect to third-party SMB servers has been disabled. To prevent poorly written drivers from causing system failures, the installation of unsigned drivers and unsigned non-drivers is not allowed.

Event Log

Policy	Computer Setting
Maximum application log size	10,240 Kilobytes
Maximum security log size	10,240 Kilobytes
Maximum system log size	10,240 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	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed
Shutdown the computer when the security audit log is full	Not Defined

The above table shows the settings for the event log portion of the GPO. The max log size is ten megabytes and events are over written as needed. This allows enough space to store multiple days worth of events. If the logs were to become full, events will be overwritten as needed so that you don't loose valuable history data in the event of a system failure or a hack. Guest access is restricted to all logs for obvious reasons.

Services

Service Name	Startup	Permission
Alerter	Disabled	Configured
Application Management	Not defined	Not defined
ClipBook	Disabled	Configured
COM+ Event System	Not defined	Not defined
Computer Browser	Disabled	Configured

DefWatch	**Not defined**	**Not defined**
DHCP Client	**Disabled**	**Configured**
Distributed Link Tracking Client	**Not defined**	**Not defined**
Distributed Transaction Coordinator	**Not defined**	**Not defined**
DNS Client	**Not defined**	**Not defined**
Event Log	**Not defined**	**Not defined**
Fax Service	**Disabled**	**Configured**
Indexing Service	**Not defined**	**Not defined**
Internet Connection Sharing	**Disabled**	**Configured**
IPSEC Policy Agent	**Automatic**	**Configured**
LicenseService	**Automatic**	**Configured**
Logical Disk Manager	**Not defined**	**Not defined**
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	**Not defined**	**Not defined**
Network DDE	**Not defined**	**Not defined**
Network DDE DSDM	**Not defined**	**Not defined**
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	**Automatic**	**Configured**
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**
Smart Card	**Not defined**	**Not defined**
Smart Card Helper	**Not defined**	**Not defined**
SMTPSVC	**Automatic**	**Configured**
System Event Notification	**Not defined**	**Not defined**
Task Scheduler	**Automatic**	**Configured**
TCP/IP NetBIOS Helper Service	**Not defined**	**Not defined**
Telephony	**Disabled**	**Configured**
Telnet	**Not defined**	**Not defined**
TermService	**Disabled**	**Configured**

The above chart shows the service settings of the GPO. To increase security, unneeded services are disabled on the domain controller.

Registry settings not covered in the GPO

Disable Autorun on CD-Rom Drives	**Hive: HKEY_LOCAL_MACHINE** **Key: System\CurrentControlSet\Services\CDRom** **Value Name: Autorun** **Type: REG_DWORD** **Value: 0**
Restrict Null User access to Named Pipes	**Hive: HKEY_LOCAL_MACHINE** **Key:System\CurrentControlSet\Services\LanManServer\Parameters** **Value Name: NullSessionPipes** **Type: REG_ MULTI_SZ** **Value: (list of pipe names permitted anonymous registry access)**

	Hive: HKEY_LOCAL_MACHINE **Key:System\CurrentControlSet\Services\LanManServer\Parameters** **Value Name: RestrictNullSessAccess** **Type: REG_DWORD** **Value: If this value exists and is set to 0, the NullSessionPipes value above is disregarded and null sessions are allowed to all pipes. Thus, in a secure system,RestrictNullSessAccess should either not exist or be set to 1. If this key does not exist, its value is assumed to be 1.**
Restrict Null User access to Shares.	**Hive: HKEY_LOCAL_MACHINE** **Key:** **System\CurrentControlSet\Services\LanManServer\Parameters** **Value Name: NullSessionShares** **Type: REG_ MULTI_SZ** **Value: (list of share names permitted anonymous registry access)**
Remove the AEDebug Key.	**Hive: HKEY_LOCAL_MACHINE** **Key: Software\Microsoft\WindowsNT\CurrentVersion\AEDebug** **Value Name: Debugger**
Remove Administrative Shares.	**Hive: HKEY_LOCAL_MACHINE** **Key:** **System\CurrentControlSet\Services\LanmanServer\Parameters** **Value Name: AutoShareServer** **Type: REG_DWORD** **Value: 0**
Disable 8.3 Filename Creation.	**Hive: HKEY_LOCAL_MACHINE** **Key: System\CurrentControlSet\Control\Filesystem** **Value Name: NTFSDisable8dot3NameCreation** **Type: REG_DWORD** **Value: 1**

The information in the above table was taken from the SANS "Securing Windows 2000 Step-by-Step Guide". Restricting null user access to named pipes prevents null sessions from accessing named pipes. "The registry is remotely accessed through a named pipe, as well as other services" (The SANS Institute, 42). By changing this registry setting, null access to the registry is disabled. Null access to shares is also restricted. The administrative shares are disabled to remove them, as a target for would be hackers.

Additional Security Measures

Because each domain controller holds a read/write copy of the Active Directory, the machine should be kept in a secured location. The location should have a lockable entrance and only be accessible by authorized personal. By physically securing the machines you reduce the risk that an internal hacker can gain consol access to the domain controllers.

There are additional security measures you can take above and beyond GPO. Insure that all partitions are NTFS formatted. Without NTFS you cannot assign file access rights. Also remove the unsecure OS/2 and Posix sub systems.

Do not allow administrators to login to the domain with their admin accounts unless they need admin rights to perform tasks. Every administrator should have a non-administrative account that is used for every day access to the windows 2000 environment. This cuts down on the number of accidental errors and lowers the chance that a hacker could use a logged in admin account while the administrator is away form his or her machine. Also force users and IT staff to have a password protected screen saver enabled.

Do not allow modems or RRAS on high security systems. Dial up through a modem opens up a hole to your network behind your firewall. You do not want to allow this vulnerability on your domain controllers.

Establish daily, weekly, monthly, and yearly backup routines for your critical servers. Backups provide disaster recovery for your environment. It will allow you to restore valuable data and systems in the case of a disaster. In addition, keep a copy of back up data off site incase of a fire or other building disaster.

Require real time virus protection for all systems to combat malicious code attacks. Routinely update virus definition files and software to provide protection form the most current virus threats. Also perform weekly or bi-weekly scans of all servers on the network.

Lastly, ensure that the latest security and service packs are applied to your windows 2000 systems. Applying the latest patches strengthens the security of your systems and safeguards them from the latest threats.

Conclusion

This document details GIAC Enterprise's Windows 2000 design and security. It covers the physical network design, the active directory design and Group Policy. Using Active directory with group policy greatly increases the ease of administration and security of Windows 2000 networks.

Bibliography

Boswell, William. Inside Windows 2000 Server. Indianapolis: Indiana, 2000

Bragg, Roberta. Windows 2000 Security. Indianapolis: Indiana, 2001

Clark, David, ed Building Enterprise Active Directory Services: Notes form the Field. Redmond: Washington, 2000.

Fossen, Jason. Windows 2000 Active Directory and Group Policy. The SANS Institute, 2001.

Microsoft, Corporation. "Best Practice Active Directory Design for Managing Windows Networks". 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/bpaddply.asp (9 Oct. 2001)

Microsoft, Corporation. "Developing a Group Policy Implementation Strategy." "Change and Configuration Management Deployment Guide." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/ccmdepl/ccmch05.asp (9 Oct. 2001)

Microsoft, Corporation. "How Group Policy Works." "Change and Configuration Management Deployment Guide." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/ccmdepl/ccmch04.asp (9 Oct. 2001)

SANS, Institute. Windows 2000 security Step by Step. The SANS Institute, 2001