Global Information Assurance Certification Paper

Designing a Secure Windows 2000 Infrastructure – GIAC Corporation

Ray Smith
SANS GIAC Certification – GCWN Practical Assignment
Track 5 – Version 3.1
9 Mar 2003

Table of Contents

EXECUTIVE SUMMARY

This document describes the design and practical implementation of a secure Windows 2000 Active Directory Network at GIAC Enterprises. GIAC is a small consulting business that provides specialized communications equipment and engineering services to the Department of Defense. The document is broken into four sections, each concentrating on a critical piece of GIAC's internal infrastructure.

Description of GIAC Enterprises:
This section describes GIAC's business as well as its organizational structure. It also provides the number of users and geographic locations that must be addressed by the design.

Network Design and Diagram:
This section provides descriptions and diagrams of the internal GIAC network. It concentrates on the infrastructure that the Windows 2000 Network will ride on.

Active Directory Design and Diagram:
This section lays out the Windows 2000 Active Directory design and structure. It discusses domains, sites, OUs, replication, FSMO roles and other items that must be considered in any secure AD implementation.

Group Policy and Security:
This section provides specific settings, descriptions and explanations of critical Group Policy settings that will be used by GIAC. The company uses the NSA as the source for its templates and sticks closely to their recommendations.

Additional Security:
This section lists additional measures taken to further secure GIAC's internal networks. It is a catch all for those security items that do not fall cleanly into the sections above.

1.0 DESCRIPTION OF GIAC ENTERPRISES

GIAC Enterprises is a small business located in Nashua NH. There is also a branch office in Birmingham AL. GIAC focuses primarily on providing specialized communication equipment and engineering services to the DOD. The product line consists of software and hardware that links networks and translates several protocols that weapon systems use to communicate. There is also a suite of test equipment used to certify specific weapon systems implementations of complex DOD protocols. The engineering services division provides the technicians and on site support for equipment

set-up, maintenance, analysis and trouble-shooting of systems during operations and testing. There is an external web site that offers products, contacts, information and on-line support.

Internally, there are three divisions R&D, Sales/Marketing, and Finance/Human Resources. There is a branch office in Birmingham that supports four field engineers; all other internal functions reside at the Nashua Headquarters. The IT infrastructure that supports the company is also located in Nashua and the Birmingham office requires secure access to infrastructure services. The details of the physical and logical network will be discussed in the Network Design and Diagram section.

The company is very small but growing. The approximate number of people in the enterprise:

Nashua Office – 25 people. There are a total of 29 people currently working for the company.

Executive Management – 2 people. The company is privately held and the two owners share the duties of President/CEO, Chief Technology Officer, and Chief Financial Officer.

Sales/Marketing – 4 people. Responsible for marketing and selling all products and services offered by GIAC.

R & D – 6 people. Due to the small size of the company and its relatively young age, the R & D people not only develop new products, they also have responsibility for the maintenance/bug fixes of the existing products. Once the product base increases in size, R & D will be a separate entity from the group responsible for production and fielded software.

Human Resources – 3 people. The HR and finance duties are handled within the same group. There are servers that house sensitive data much of which is required to be available in paper format for audit purposes.

Others – 10. There are also administrative people, field engineers, support and IT personnel working within the company.
Birmingham Office – 4 people. Four field engineers have a satellite office in Alabama

GIAC is in the midst of transitioning infrastructure services that have previously been outsourced, mainly mail and DNS, back inside. Mail is definitely being pulled in; the pros and cons of outsourcing DNS are being evaluated (see Additional Security Measures). In order to properly secure these services a DMZ is being implemented keeping in mind that the Birmingham office still needs access to internal resources.

GIAC although small has a wide range of customers with locations all around the world. Employees are constantly required to travel which creates the need for secure access to their mail and FTP services.

2.0 NETWORK DESIGN AND DIAGRAM

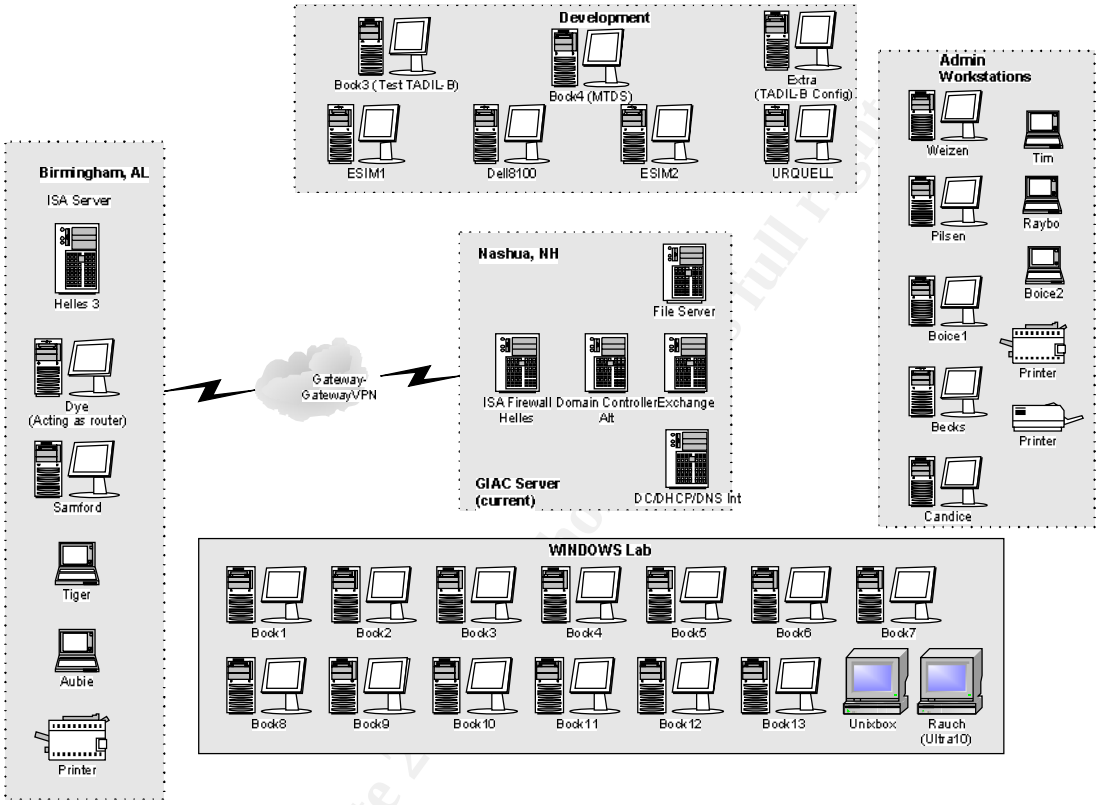

Figure 1 – Current Network Layout at GIAC

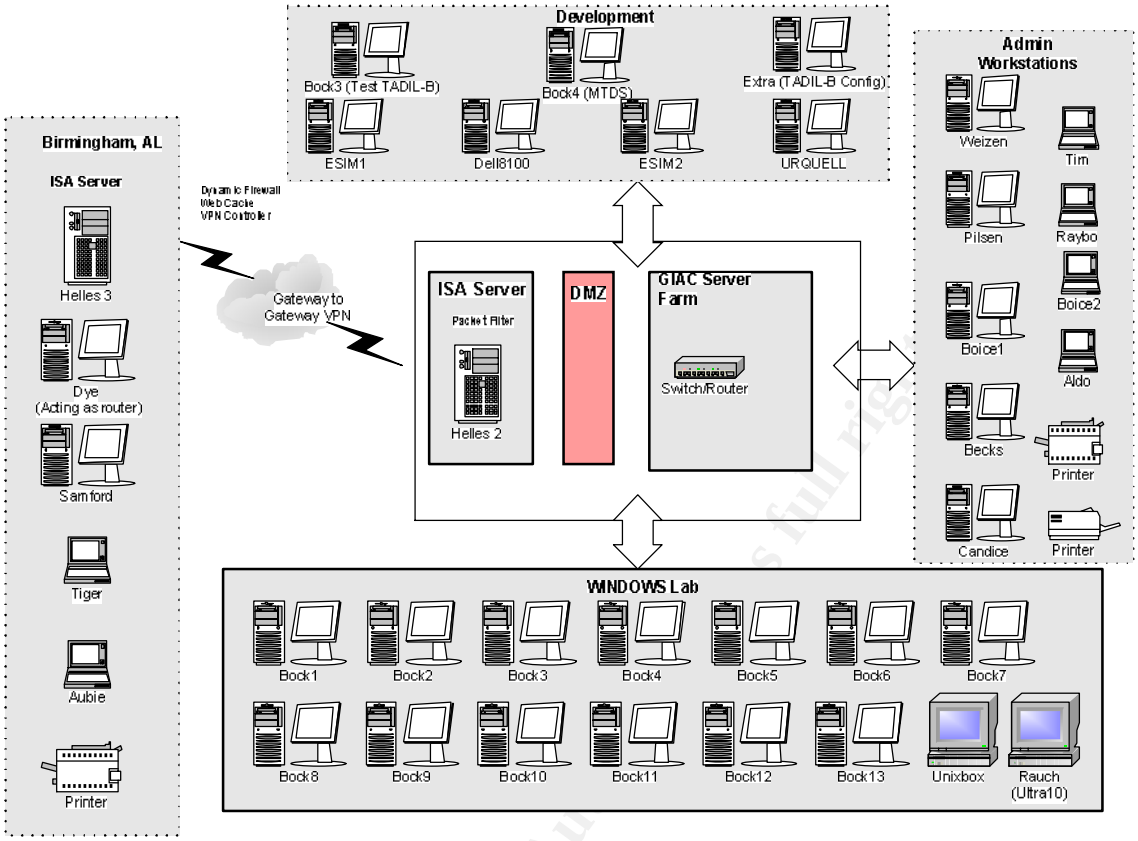

Figure 2 – GIAC Network with DMZ

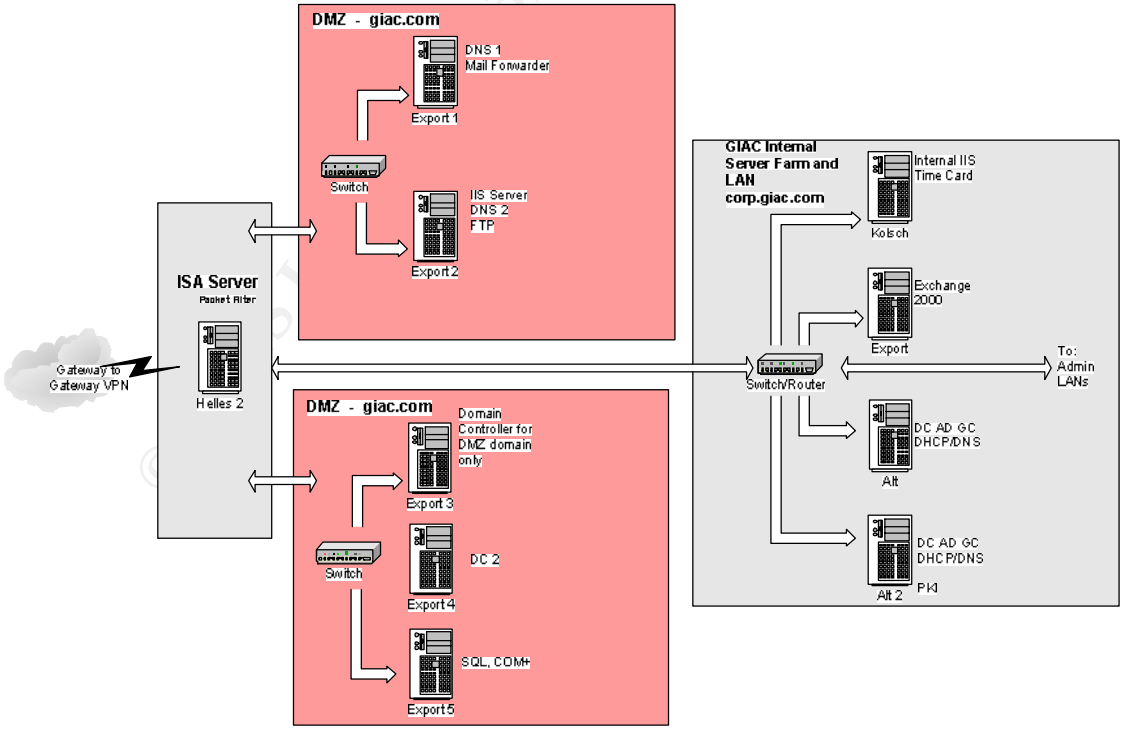

Figure 3 – Detail Breakout of DMZ

Externally, GIAC has 8 public IP addresses from its service provider. There is a T-1 connection to the Internet. The phone service is bundled with the internet service. There is a Microsoft ISA Server (combined firewall and proxy) with 4 interface cards. There are two DMZ segments, the external T-1 and the internal LAN. The internal NIC connects to a router that separates GIAC into three distinct broadcast networks or subnets for the groups of machines in Figure 1. The network runs at 100Mbs full duplex over CAT VI cable. A Cisco 3640 router and Netgear switches comprise the bulk of the hardware in the GIAC network; the last hubs have recently been upgraded to switches so each machine has a dedicated 100Mbs full duplex connection internally. The IP address blocks/gateways assigned are:

Development – The developmental or R&D LAN
Network: 192.168.1.0 255.255.255.0
Gateway: 192.168.1.1
Usable Hosts: 192.168.1.2-192.168.1.254
Broadcast: 192.168.1.255

Windows – Windows Tests and Training Suite
Network: 129.168.2.0 255.255.255.0
Gateway: 192.168.2.1
Usable Hosts: 192.168.2.2-192.168.2.254
Broadcast: 192.168.2.255

Administrative Machines – User workstations, internal servers, and printers
Network: 192.168.3.0 255.255.255.0
Gateway: 192.168.3.1
Usable Hosts: 192.168.3.2-192.168.3.254
Broadcast: 192.168.3.255

DMZ Network Segment 1 (IIS, SMTP, DNS, FTP)
Network: 192.168.4.0 255.255.255.0
Gateway: 192.168.4.1
Usable hosts: 192.168.4.2-192.168.4.254
Broadcast: 192.168.4.255

DMZ Network Segment 2 (External DCs, SQL)
Network: 192.168.5.0 255.255.255.0
Gateway: 192.168.5.1
Usable hosts: 192.168.5.2-192.168.5.254
Broadcast: 192.168.5.255

The eight public IP addresses assigned to GIAC for use on the external interface of the outside firewall:
Network x.53.30.48 255.255.255.248
Gateway x.53.30.54

Usable Hosts: x.53.30.49-x.53.30.53
Broadcast: x.53.30.55

GIAC uses a variety of Dell workstations (Precision Workstation 340s), Laptops (Inspiron 8100, 8200) and Servers (PowerEdge 1650, 2650, 4600). The larger servers use disk arrays with RAID 5. GIAC has also purchased almost half of a terabyte of IDE disk drives and is moving away from tape backups to using disk storage solutions. All of the Servers run Windows 2000 with the latest service packs and hotfixes. The clients run a mixture of Windows XP and 2000; again all machines are kept current with service packs and hotfixes and all partitions are NTFS.

Network Address Translation (NAT) is used to map the internal private IPs to the external public addresses. This adds a measure of security as it is more difficult for an attacker to discover the size and configuration of the internal network as literally hundreds of machines can at times be using the same IP address while communicating with machines across the Internet. "When the [outgoing] client packet passes the access rules that the ISA server is configured to enforce, ISA server will modify the packet changing the "from" IP address to its own IP address and pass the packet to the intended external server. The server's response packet will then be sent back to the ISA server and not the original requestor." (Pitsenbarger, 5) Security is enhanced by virtue of the fact that the internal client never actually connects to the external server. Instead, the ISA server masquerades as these boxes.

The company consists of two geographically separated units (Nashua, NH and Birmingham, AL). Currently there is no DMZ setup and GIAC publishes those services that need access and visibility from the outside internet through the firewall. These services include the mail and web server. At this time DNS is out-sourced to a company called Network Solutions.

As stated earlier, Nashua is implementing a DMZ that will be set up behind a Microsoft ISA server with four network connections. The DMZ will be used to make external services available to customers in a more secure manner. The Birmingham office also has an ISA server and connects to Nashua using a gateway-to-gateway VPN to gain access to the GIAC internal network.

There will be two separate segments within the DMZ. The first will contain three Windows 2000 servers that house two publicly accessible IIS web servers, a mail forwarder, FTP, and two external DNS servers. The firewall will allow public access only to this segment of the DMZ. The second segment of the DMZ will house two domain controllers and an SQL database. All servers in the DMZ will be members of the external domain GIAC.com that is housed on these two domain controllers. The external domain is not joined to the internal domain. It is in place so that group policy can be used to manage the external servers and also so the AD can be used for external customer accounts once GIAC is ready to implement its web based help desk and if the web becomes a viable means of selling GIAC products. Only traffic from the internal LAN or the first segment of the DMZ will be allowed onto this segment by the firewall. This will

also be enforced by using IPSec which will be discussed in greater detail under the Additional Security Measures section of this paper.

When GIAC explored the feasibility of placing DCs in the DMZ so that the DMZ servers could be members of their own domain, it was found that although not vital at this stage of the company's development it would later be essential. For this reason GIAC plans to stand up the DMZ earlier than necessary so that its administrators can perfect security and policy by the time customers (and GIAC) will be relying heavily on the IIS servers. The external firewall itself will of course not be a member of any domain.

GIAC's internal network contains the infrastructure and services that are vital to company operation but should not be available to the general public mainly for security purposes. These include two Domain Controllers, a Microsoft Exchange Server, a file and print server, and a time card server running on Win2K. The time card server requires IIS and it also houses an internal web site that serves as a repository for employee only type items such as GIAC Policies and Procedures, internal memos, employee health care and retirement info, etc. Only the web servers, Exchange server, and TimeCard Server have IIS running on them because they require it (Exchange for OWA). IIS has been removed from all other machines and the IIS lockdown tool is used to secure all boxes that require IIS.

The two DCs serve as backups to each other by replicating all information in the directory to each other. Both are DNS servers for the internal zone (corp.giac.com) and the DNS service is Active Directory integrated so that information within the zone files can be recreated from the directory if lost. One of the DCs also servers as an intermediate/issuing Certificate Authority (CA). The root CA was stood up on a relatively old PII Win2K server; since it contains the company's root certificate the drive is pulled and kept in a safe with the private key under normal operations.

A third DC is housed at the Birmingham site in order to provide a local logon and also to allow redundancy in case the Nashua DCs become damaged or destroyed. This DC will also serve as a standby Flexible Single Master Operations (FSMO) owner mainly for disaster recovery purposes (more information provided in the next section). All of the information replicated between the two DCs in the Nashua site is also replicated to this server. The details and measures necessary to secure all replication are addressed in the next section (See Section 3 Active Directory Design and Diagram).

Certificate Authority:

GIAC uses a two-level architecture for certificate trust. The company needs to be able to send secure email to many sources outside its own domain. They also have requirements for secure web certificates that are compatible with a variety of external browsers. The most practical way to do this is to purchase an issuing CA from a large company whose certificates are trusted by the most widely used email clients and web browsers. GIAC has chosen to go with Versign for this aspect of its certificate services which will allow it

to manage and issue its own certificates. For all internal functions such as authentication to the corporate domain, GIAC can issue certificates that only trust its own root.

It is critical that Service Pack 2 or the latest Service Pack be applied so that the enhanced Cryptographic Service Provider (CSP) and the strongest keys are available. Once the Certificate Services component has been installed on a server, that computer's name and domain can not be changed without uninstalling Certificate Services first. In order to control certificate enrollment, GIAC follows SANS best practices which include:
"1. Remove the Authenticated Users group from the permissions ACL on the CA itself. Add only those groups whose users and computers will actually need to obtain certificates. Don't forget that computers can be members of groups in Windows 2000.
2. Create a local group named "CA Admins" on each CA computer. Give this group the Manage permission on the CA. Use this group to delegate authority over the CA, if necessary, without granting the delegates full administrative power on the computer or in the domain.
3. Remove all unneeded certificate templates from the Policy Settings container. Keep in mind that a template can be added temporarily when needed and then removed again. When in doubt, remove the template.
4. Assign the Everyone group Deny/No Access to all templates, then change this permission as needed to allow just the desired users and computers to request certificates. Keep in mind that permissions can be changed temporarily as needed, then reset to Everyone:Deny. In particular, be very wary of changing Everyone:Deny for the following templates: Administrator, CA, SubCA, Enrollment Agent, EFSRecovery, Code Signing, CTLSigning.
5. Audit all failed access to all certificate templates." (SANS Track 5.2, 81-82)

GIAC also pays close attention to the storage of its private keys and makes every effort to comply with the best practices located on page 92-93 of the SANS Track 5.2 book.

Email:

As stated earlier GIAC runs MS Exchange 2000 internally for email services. Currently this service is published through the ISA server. In the near future, a mail forwarder will be used as an added security layer so that the actual mail server remains hidden from the outside world. In addition, if the mail forwarder is attacked and breached, the internal mail server will not necessarily be harmed.

GIAC employees are required to travel extensively, at times only a kiosk computer or basically just a browser are available which makes Outlook Web Access (OWA) critical. As long as a person can get to a web browser, they can have access to their email, calendar, and contacts using OWA. By default OWA sends email in clear text and unfortunately sessions can often be reopened simply by hitting back on a browser that has been left open. GIAC will use a Verisign certificate to secure OWA by encrypting all sessions within an SSL tunnel. The Exchange server itself will be configured to disallow all unencrypted sessions so that only https:// is possible.

Although SSL is not a method of authentication itself, it encrypts entire sessions so that even if basic authentication is used not only the password but all of the communications will be encrypted. "Although any authentication method can be used with SSL, the most common implementation is Basic with SSL." (E2K_OWA, 9) Occasionally a browser may not be able to accept a Verisign certificate but the majority will have no problem. The added security is definitely worth the occasional hassle of not being able to use certain public kiosks for example.

Network Time:

It is important for all clients and servers in the domain to have an accurate time source. In order to authenticate using Kerberos, system time on the sending workstation must be within 5 minutes of the time on the DC or the action will fail (30 minutes for NTLMv2). DCs and the Active Directory also use time to decide which updates are written to the directory in case of conflicts so having an accurate time source is critical to maintaining a healthy directory service.

All clients and Servers will look or can be pointed to the DC with the Infrastructure Master FSMO role on it to provide time service. The Infrastructure Master in turn must have an accurate time source to pass throughout the domain. GIAC uses a time server called Truetime which gets its time from GPS using an easy to install antenna. By using an internal time source GIAC does not have to worry about receiving accurate time if the ISP goes down or if an internet time source itself becomes unavailable. Also, no ports need to be opened on the firewall to allow Network Time Protocol (NTP) through. More and more application and network services are using time as a security measure to prevent replay type attacks where packets are grabbed, modified and retransmitted. There are many reasons to have accurate time and no reasons to have inaccurate time on any network.

3.0 ACTIVE DIRECTORY DESIGN AND DIAGRAM

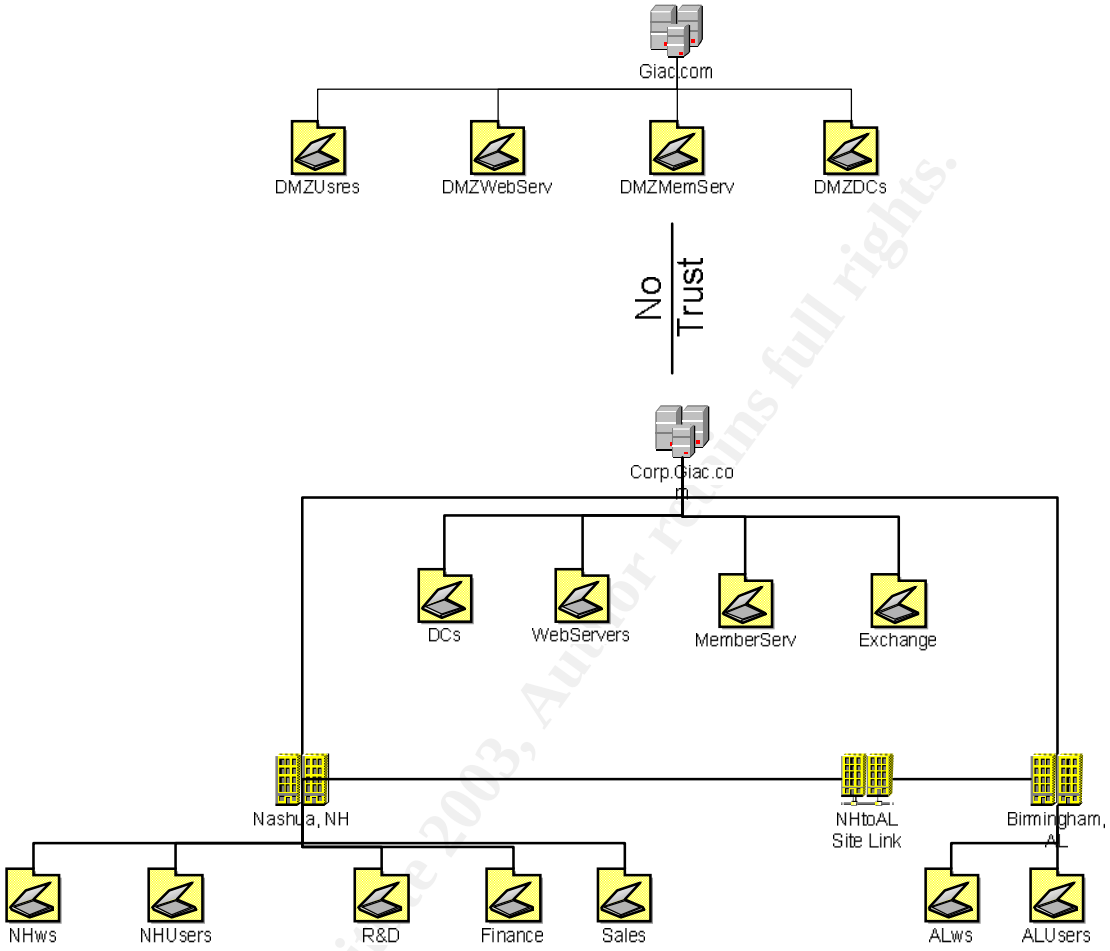

Figure 4 – GIAC Active Directory

Although GIAC currently has only one forest/domain, in the near future there will be two separate domains that have no trust relationships established with each other. This architecture is reflected in Figure 4. Externally, GIAC will use a small domain in its DMZ for the purpose of managing all the servers located in the DMZ with group policy and also to maintain a separate directory/authentication mechanism for customer accounts (the Active Directory).

Internally, GIAC Enterprises uses a single forest, tree and domain. Since the company is relatively small and domains have been tested with loads greater than 16 million objects there is no a size constraint. There are also no political boundaries or factions of administrators controlling the setup of the AD structure. Also, "It is easier to manage and trace Active Directory object access control and group policy inheritance since

permissions are contained within the domain boundary." (Sanderson, 20) For these reasons a single domain which utilizes Organizational Units (OUs) is ideal for GIAC.

The small size of the company and the fact that it is only a few years old will enable the implementation of a native Windows 2000/XP environment; at no time should a Windows 9x or NT client be placed on the network. Using a native Win2K (soon XP and .Net) allows the company to take advantage of the built in security and administration features without having to allow backwards compatibility for legacy NT or Windows OSs. For example Kerberos authentication and NTLMv2 can be used for authentication – they are built into the OS and nothing further need take place in order to take advantage of these improved features. Additional benefits in the areas of centralized administration and increased performance make this design the best option for GIAC.

Organization Units:

OUs are the extremely handy containers that basically comprise the building blocks or subdivisions within domains. They can contain users, computers, groups, printers, contacts, shared folders, and other OUs according to the delegation and group policy requirements within a company. Despite popular opinion, it is not recommended that the organizational structure be reflected in the OU architecture. Microsoft does not recommend nesting OUs deeper than 5 levels because it becomes cumbersome to apply group policy across many layers of OUs and begins to effect performance. GIAC attempts to maintain the simplest architecture possible on all levels of its design and at this time does not expect to have to go deeper than one or two levels of nested OUs.

Keeping in mind that OUs are created with group policy (security is included with group policy) and delegation as the focus, GIAC has created containers for R&D, Human Resources (finance), and Sales and Marketing. There are also OUs or domain containers required for certain infrastructure servers that have different security needs and therefore also require tailored Group Policy Objects (GPOs) to be associated to them. Windows 2000 DCs creates some OUs by default and others need to be set up by administrators. The OUs of note include but are not limited to Domain Controller (default container), Computer Container (default container), Exchange Server, Internet Web Server, and Intranet Web Server.

Flexible Single Master Operation (FSMO) Role placement:

Since GIAC is a small company that contains only one domain. All five FSMO roles will be placed on the same DC. When a company has more than one domain it is often recommended to place the Infrastructure Master role on a DC that does not contain the global catalog. This does not matter when only one Active Directory domain is involved because there are no "phantoms" which means there is no work for the infrastructure master to perform. In the future if roles are separated onto multiple boxes it is necessary that "the domain naming master operations master must also be a global catalog server". (BPADDPLY, 50)

It is important however to select local primary and standby FSMO domain controllers in case a failure occurs on the primary FSMO owner. The Alabama branch office will be used as an off site standby owner in case disaster strikes the main office in New Hampshire. Since the standby will be a remote site the connections will be configured for "continuous replication over a persistent link". (MS, Q223346)

Sites and Replication:

Microsoft defines a site as a group of well connected subnets GIAC is divided into two sites (Nashua and Birmingham). The DCs at the Nashua office are contained on the same subnet and site. Each subnet (or subnets) must be specifically associated with a site using the Active Directory Sites and Services snap-in to the MMC. On that local subnet, changes are propagated as soon as they occur. Although, both of these domain controllers sit on the internal GIAC network all updates between domain controllers are done via an IPSec Tunnel.

An intersite link is used to connect the two sites. Since both sites are part of the same domain, they are required to use the RPC over IP transport when replicating over the WAN. The intersite replication traffic is sent through the ISA Server Gateway to Gateway VPN (also uses IPSec) to secure communications between the Nashua and Birmingham sites when stored changes propagate across the WAN according to the schedule (every 15 minutes) set up using the Sites and Services snap in.

DNS and Naming:

Since Windows 2000 has replaced WINS with DNS it is a vital part of the Active Directory design and securing it becomes a very important task. GIAC will use what is known as "split" or "split-brain" DNS where internally there is a private namespace (corp.giac.com) and name servers that contain all the internal clients and services that do not need to be published to the internet. Internally Active Directory can dynamically and securely publish all of its services so that corporate users can look up other internal clients, servers and services. This makes it much more difficult for anyone on the outside to "discover" infrastructure and network information about GIAC since under ordinary circumstances it is not visible to the outside world.

Any lookup that can't be resolved will be forwarded to the external DNS servers in the DMZ (or at an outsourced location) for resolution or a recursive search if necessary. Externally or in the DMZ a public zone is established for those machines and services that must be available to external users such as mail, ftp, and web servers. Again, all internal lookups that can not be resolved are forwarded.

The internal DNS machines are Active Directory integrated which basically means the objects or records are stored in the Active Directory instead of in zone files. Changes within the zones such as the addition of a new client are all handled by Active Directory replication. This allows DNS to take advantage of the security features that are built into

AD. In addition it is much easier to recover from a disaster as all of the DNS records can be recovered from the directory in the case that a DNS server is lost.

Physical Security:

Perhaps the most fundamental element of securing AD, replication and any other important network infrastructure servers/services is physical security. The New Hampshire GIAC office is located in a building that is basically open to all during business hours and only to employees who lease space during off-hours. There is a lock on the office door and there is also a secure server room that houses all of GIACs servers, back-up devices, network infrastructure and Telco equipment. The servers are all mounted in a standing rack (also locked). Each server is on a UPS and all servers share a single monitor and keyboard through the use of a KVM switch. Only the owners and administrators have keys to the room. There are of course administrator accounts and groups set up on the boxes to maintain them but only after the administrator has gained physical access to the room which is seldom necessary since terminal services are used for the bulk of server maintenance.

Although the room is currently secured only by lock and key it sits in the center of the office so it is highly visible. GIAC plans to implement a combination smart/proxy card that will log all access not only to the server room but also through the front office door. The Birmingham office contains only a front door lock but there are only a handful of employees at this site most of which are field engineers or administrators. As more employees are hired it will be necessary to evolve physical security with infrastructure. Currently the use of surveillance equipment is not planned for either office.

4.0 GROUP POLICY AND SECURITY

Group Policy is probably the most important security feature of Windows 2000. Group Policy is used to change/control the configuration of computers and user preferences across a single machine or an entire enterprise. These policies or Group Policy Objects (GPOs) can be attached to containers including sites, domains, or OU using tools or snap-ins available through the Microsoft Management Console (MMC). Although a GPO exists separately as an object it must be attached to a container in order to be applied to computers and/or users. GIAC uses a Windows test suite (See Figures 1 & 2) to import, modify and test all group policies before they are applied to operational networks, machines and users.

All group policies are split into two parts. The first part, computer configuration, controls settings that are applied to all computers regardless of what user is logged in. The second section, user configuration, controls a user's environment wherever that person logs in. An example of how a setting in group policy might be applied is included below.

If a box was built for the purpose of running a certain application such as the protocol translation s/w product produced at GIAC, whenever a user logs in that s/w should be running. Under the computer configuration in the local machine's group policy the setting "Run These Programs at User Logon" (located under Administrative Templates, System, Logon) can be enabled and the fully qualified path for the application can be added so that no matter who is logged in on the machine that application will run. This setting is also available under user configuration and will launch an application no matter what user logs on. Basically this accomplishes the same thing however the list of applications under the computer configuration will be processed before those under user configuration.

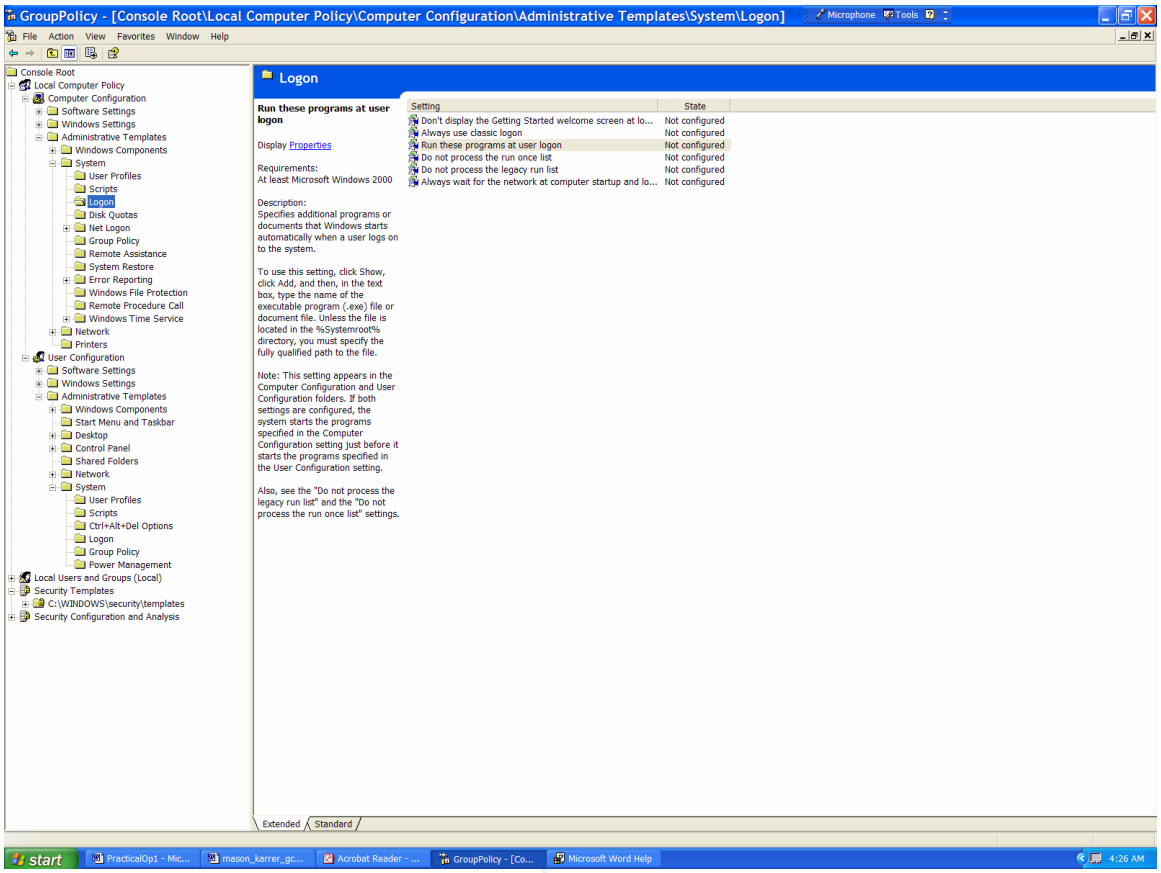

Figure 5 - MMC Group Policy Snap In; Example of editing group policy on a local machine.

There are several sources of group policy security templates available to use as a starting point for GIAC's tailored policy. These templates contain recommended settings depending on the desired security level of the box. Since GIAC has many DoD customers, the company chooses to use the templates put out by the National Security Agency (NSA) as a starting point for its internal GPOs. There are literally thousands of settings that can be controlled through group policy. This section addresses the settings of concern or those that are relevant to securing GIAC's networks. When discussing more restrictive policies only the differences and reasons for those differences will be addressed.

Access to MMC snap-in should be limited to administrators. Permissions on who can change a group policy as well as who can link a policy to a container are also limited to administrators only.

Group policy is processed in the following order within an enterprise:

1. Group policy objects linked to sites
2. Group policy objects linked to domains

3. Group policy objects linked to OUs. In the case of nested OUs, GPOs in parent OUs are applied first.

The order listed above is significant in that those policies applied later over write those applied earlier. No override options can be used to ensure that lower level policies do not overwrite those applied before them. In the case of GIAC this will not be necessary due to the small size of the organization. Only one OU will be delegated and the on Site administrator is known to be extremely knowledgeable and security conscious. Any conflicts can be worked out without having to use no override or block inheritance to manipulate the application or non-application of policies.

GAIC attempts to keep the number of GPOs attached to objects to a minimum. GIAC also tries to avoid redundancy within the policies to the greatest extent possible. Attaching many complex GPOs to containers throughout a domain can erode performance as policy settings are applied, reapplied, over written through each layer of the precedence list above.

BASIC GROUP POLICY

Default Domain Policy

It is good to start with domain policy to ensure consistent password and lock out policy across all servers (including domain controllers) and workstations. Currently this template should be the final policy that end users experience as far as password, account lockout and Kerberos are concerned. Certain OUs (that house servers) will have policies that differ in other areas and they will be discussed further in those sections.

Password Policy:

1. Enforce Password History – should be set to 12 passwords to prevent users from immediately reverting back to their same password or toggling between a few favorites.
2. Maximum Password Age – should be set to 120 days in order to make sure users are not unnecessarily inconvenienced but are forced to change passwords at a reasonable interval.
3. Minimum Password Age – should be set to 1 day (range from 0 to 998). The default setting for this is 0 which allows users to immediately change passwords as many times as they like. Setting it to 1 prevents anyone from rapidly changing their passwords until they exceed the history and can return to their favorites.
4. Minimum Password Length – should be set to at least 12 characters. Although Windows 2000 supports passwords up to 127 characters in length however the Windows Security Template interface will not allow passwords in excess of 14 characters (Guide to Securing W2K Group Policy, SNAC at NSA).
5. Password Must Meet Complexity Requirements – Enabled.
Enforces strong password requirements for all users by using a dynamic link library called passflt.dll. Stronger passwords provide some measure of defense against password

guessing and dictionary attacks launched by outside intruders. Passwords must contain characters from 3 of 4 classes and cannot be the same as a logon name.
NOTE: NSA provides an enhanced password complexity filter, ENPASFLT.DLL that can be used in place of the Microsoft provided PASSFLT.DLL however it is only available to government agencies. Several of GIACs customers in the command and control sector choose to use this filter instead of the default.
6. Store Password Using Reversible Encryption For All Users in the Domain – Disabled. This option allows passwords to be stored using a two way hash so that they can be provided to some applications. It becomes similar to storing the password in clear text and should not be enabled.

Account Lockout Policy:

1. Account Lockout Duration – 15 minutes. Account lockout policy should be set to 15 minutes to slow down dictionary attacks. A value of 0 will keep the account locked until it is unlocked by an administrator. Setting the value to 0 can open systems up to a denial of service attack. It is important to note that the built-in administrator account can not be locked out.
2. Account Lockout Threshold – 3. Helps prevent brute force password guessing attacks. A value of 0 means the account will never be locked out.

Kerberos Policy:

1. Enforce user Logon Restrictions – Enabled. Checks whether the user has the right to log on locally or over the network. If the proper permission is not in place a ticket will not be issued. This provides added security but may slow down a busy network. GIAC's network is not overloaded and can easily accommodate the extra traffic.
2. Maximum Lifetime for a Service Ticket – 600 minutes. Determines length of time a Kerberos ticket remains valid (10 minutes – Max Lifetime for User Ticket). Default setting is fine.
3. Maximum Lifetime for a User Ticket – 10 hours. Determines the life time of a TGT – default 10 hours is fine.
4. Maximum Lifetime for User Ticket Renewal – 7 days. Sets the max number of days that a TGT can be renewed.
5. Maximum Tolerance Computer Clock Synchronization – 5 minutes. Sets the maximum amount of time that the KDC's clock can differ from any client machine. All Win2K clients should automatically obtain the time via the W32Time Service. The PDC that has been elected as the master time server should be configured to get the time from a reliable external time source such as the US Naval Observatory (ntp2.usno.navy.mil). (Heywood, 583)

Local Machine Policy includes audit policy, user rights assignment, and security options.

Audit Policy:

Although auditing can become processor intensive and can consume a large amount of disk space, GIAC has a relatively small network and user base so it is practical and manageable to enable auditing on all workstations and servers. Auditing must be turned on since it is not enabled by default. Audit logs are kept on a separate partition. GIAC sticks to NSA's recommendations which are summarized below.

1. Events audited for both success and failure.
    a. Audit Account Logon
    b. Audit Account Management
    c. Audit Logon Events
    d. Audit Policy Change
    e. Audit System Events
2. Events Audited for failure
    a. Audit Directory Services Access (only audited on a DC)
    b. Audit Object Access
    c. Audit Privileged use
    d. Audit Process Tracking

Perhaps more critical than tweaking what is to be audited is the actual checking of the event logs in event viewer. GIAC security administration policy calls for the logs to be checked each morning and saved off weekly. Any suspicious anomalies are addressed at the weekly staff meeting unless they constitute an emergency.

User rights:

1. Access this computer from the network – Administrators, users. Allows users to connect over the network to computers.
2. Add Workstations to a Domain – No One. Allowing users to add their own machines to a domain could pose a security risk and is not necessary.
3. Act as Part of the Operating System – No One. This right should not be granted on any machine.
4. Change the System Time – Administrators. There should be no need to change the system time as all computers on the network are synchronized with a reliable time source via the DC.
5. Logon as a Service – No One. Allows a process to register with the system as a user. There are exceptions to this – see Exchange section below.
6. Logon Locally – Users, Administrators. Both users and administrator should be able to logon locally to a workstation.
7. Shutdown – Users, Administrators. Users should be able to shut down their own machines especially since most of them are laptops that are not shared and are used for traveling. Along the same lines both users and administrators need to be able to undock their machines from docking stations.

Security Options:

There are numerous security options some of the more important ones and the recommended settings for the GIAC network are discussed below.

1. Allow Automatic Logon for Administrators – Disabled. This setting allows a system to automatically logon as administrator when the machine is started. Although this setting is disabled by default, if it has ever been enabled a Default Password registry value may exist in the same key. If it does it contains a clear text password and should be deleted.
2. Additional Restrictions for Anonymous Connections – No Access without Explicit Permissions. Requires "Anonymous" be given explicit permissions to access resources by removing the everyone and network groups from the anonymous user token. It is possible that this may cause some problems when setting up trust relationships or running certain services or applications. If this setting has negative effects, "Do not allow enumeration of SAM accounts and shares" should be selected.
3. Automatically Logoff SMB Users When Logon Time Expires – Enabled. Causes client SMB sessions to be forcibly disconnected when users logon hours expire.
4. LAN Manager Authentication Level – Send NTLMv2 response only, refuse LM and NTLM. This setting only affects networks with non-Windows 2000 clients but there is no harm in setting it to ensure that only the most secure challenge/response protocol is used which is NTLMv2.
5. Message Text For Users Attempting to Logon (logon banner) – GIAC's message informs any potential user that the network and systems are private and also monitored. Attempting to gain unauthorized access is illegal and GIAC will hold those attempting to gain access without authorization liable for their actions.
6. Number of Previous Logons to Cache – 0 logons. The default setting is ten logon credentials. A setting of 0 will not allow logons when no DC is available however GIAC has an excellent availability and disaster recovery plan so it is not necessary.
7. Rename Administrator Account; Rename Guest Account – Both the administrator and guest accounts are created by default. Associating their SIDs with different names may thwart potential attackers who attempt to target these built in accounts.
8. Send Unencrypted Password to Third Party SMB Servers – Disabled. Some non-Microsoft vendors only support unencrypted password exchange. Enabling the option allows passwords to be sent in the clear when requested. This significantly reduces the overall security disposition of the environment and should never be enabled.
9. Smart Card Removal Behavior – Lock Workstation. Determines behavior of workstation after smartcard is removed. Should never be set to "no action" as pulling the smartcard indicates the user has left the immediate area. "Force Logoff" is no less secure but it is also no more secure so there is no need to inconvenience users for no additional gain in security practice.

Default Domain Controller Policy:

No settings are defined for password, account lockout and Kerberos. The settings in these areas defined in the default domain policy discussed above do not need to be modified or reset. In fact not defining them will allow the GPOs to be applied more quickly and efficiently.

The auditing defined in the default domain policy will suffice for the DCs with the exception of the Audit Directory Service Access setting should be audited for "Failures". Audits users' access to AD objects that have System ACLs (SACLs) defined. Similar to the Audit Object Access setting except it only applies to the Active Directory objects, not the registry and file objects. Since the object applies only to Active Directory it has no meaning on workstations or member servers.

User Rights:

1. Access this computer from the network – Administrators, Authenticated Users, Enterprise Domain Controllers. Allows users to connect over the network to computers.
2. Add Workstations to a Domain – No One. Authenticated users on a domain controller are granted this right by default.
3. Enable Computer and User Accounts to be Trusted for Delegation – Administrators. Allows the user to set the "Trusted for Delegation" setting on a user or computer object. This right should only be granted to admins on DCs and should be granted to no one on all other servers and workstations.
4. Logon Locally – Administrators. There is no need for anyone besides an administrator to logon to a DC locally. Even this should rarely be necessary as most administration is accomplished through the use of terminal services.
5. Shutdown the System – Administrators. Only Administrators need to shutdown domain DCs.

Security:

Other than the exception below all security settings discussed above in the default domain policy will have the same values for the DCs as they do for the workstations and member servers.
1. Allow Server Operator to Schedule Tasks – Disabled. This setting need not be defined on a workstation or member server but only administrators should be allowed to schedule tasks on a DC.

Event Logs:

1. Maximum Application Log Size, Maximum Security Log Size, Maximum System Log Size – 4,194,176K. This is the maximum size for an event log. Since large amounts

of disk space are available the size is set to the max to prevent administrators from having to frequently clear the log files.
2. Restrict Guest Access to Application, Security, and System Log – these three options set to Enable. By default guests and null logon sessions are allowed to view these logs. Enabling these options disallow that privilege.
3. Retain Application, Security, and System Log – Not Defined. This setting dictates how long log files will be kept before they are overwritten. Since these logs should not automatically be overwritten the option is not defined.
4. Retention Method for Application, Security, and System Log – Manually. Forces the method of clearing logs to manual instead of automatic after a certain size or number of days. In the case of a security breach it is vital to have the old logs in order to figure out what happened. This setting ensures they will be available.
5. Shut Down the Computer When the Security Log is Full – Disabled. Although the system should not be running if security events can not be recorded, GIAC will rely on the vigilance of administrators to stay on top of this and will not shut down systems automatically.

ADDITIONAL GROUP POLICY

Below are some of the differences or exceptions between the policies applied to some of the other OUs vice the default domain and DC policy. In addition some of the other uses of group policy at GIAC are discussed in general terms.

Modifying Registry Settings:

In order to effectively implement security in Windows 2000 it is necessary to change the permissions on some registry keys. This can of course be accomplished using tools such as Regedit32.exe however it can also be done through Group Policy. Performing this task through group policy is quicker and less error prone than doing it manually.

Software distribution and configuration management:

Administrators can efficiently deploy and remove software from machines or groups of machines throughout their Enterprise by using the Software Settings section of group policy. This feature is not only handy for mass deployments such as Service Packs or .msi packaged applications but it is great to enforce a configuration management baseline. This allows administrators to know what is on each machine and more importantly control what can be loaded by non-administrators. The intent is to make it much harder for a user to unwittingly install harmful software or to violate corporate licensing agreements by loading too many copies of an application.

Scripts – logoff, logon, startup and shutdown:

Most organizations have some type of logon/logoff and/or startup/shutdown scripts used to do a variety of things related to specific users and to the systems themselves. GIAC

scripts are controlled by group policy under User Configuration and Computer Configuration – Windows Settings.

Specific Examples of tailored OU group policy at GIAC:

There are literally thousands of settings in group policy. In general terms many of the settings will be similar across companies hence templates have been developed which provide excellent guidelines for administrators. Security policy must then be tailored to balance the needs of the users and administrators. What follows are some specific examples of tweaking policy settings within GIAC.

The R&D OU contains field engineers and technical people; many work as windows consultants and are constantly troubleshooting customer machines and networks. They are allowed more access to their machines than users in the other OUs. They have access to the registry, command prompt, NIC card and other items/tools that are usually reserved for administrators. Access to the registry tools (Regedit.exe, regedit32.exe) and command prompt are controlled through group policy under User Configuration, Administrative Templates, System. The ability to view and change properties of the NIC card is also under Administrative Templates in the network folder. For the R&D OU these settings will not be configured so the engineers can have access. However, for the sales/marketing and finance/HR OUs these settings will be enabled so that the less technical people working in these areas do not inadvertently reconfigure or break their company machines.

Both the New Hampshire and Alabama sites have now gone to ISA server which handles proxy services. However, in the past the Alabama site used the Squid proxy server available in Linux as do many of GIAC's customers. Group policy has a handy setting that configures proxy settings in Internet Explorer. Using this setting drastically cuts down on trouble calls as it is often the culprit when users report they can not get out on the network. GIAC uses the Internet Explorer Maintenance section of group policy to set all users default homepage to www.corp.giac.com. There are lots of useful announcements and information on the company's internal web server so GIAC provides incentive for employees to check it by having it come up as soon as they launch their browsers.

The NSA recommends the following changes to DC Policy when it is being applied to IIS and Exchange servers. In order to ease administration, these servers will be placed in the DC or Server OU. The settings below and some other settings may need to be manipulated for all of the servers to run correctly. Some of these changes may slightly weaken the DCs but GIAC believes the overall security posture of the company will remain excellent. As GIAC grows and the number of servers increase i.e. the web server becomes a farm of servers, separate OUs will be created to accommodate the growth and the new administrators that are hired for each discipline. The difference in group policy between the DCs and IIS/Exchange are:

IIS:

1. Logon Locally – Administrators. In addition to Administrators the IWAM_xxx, IUSR_xxx (anonymous web user account) needs to be assigned this right.

Exchange
User Rights:

1. Logon as a Service – No One. Exchange requires a service account which should have this right. The users/groups that have this right should be noted before the application of this template so that the accounts that require it can keep it. The NSA templates will remove
2. Manage Auditing and Security Log – Administrators, Exchange Enterprise Managers. When running Exchange, the Exchange Enterprise Managers Group must be added in addition to Administrators.

As discussed earlier there are many security templates to choose from and there are literally thousands of different settings that can be configured. Administrators may choose to import templates that come from Windows 2000 or other sources such as SANS or NSA. They can apply these templates as they are or make modifications as necessary. The security templates are .inf files and can be custom made from scratch if necessary. Templates can be created, copied or modified independently from GPOs at any time using the Security Template snap-in.

Templates have a cumulative effect, building on one another to achieve a certain level of security. For example to get to the highest security state on a DC using the templates provided by Microsoft it is necessary to apply the default DC template, the Secure DC template and finally the Highly Secure DC template in that order. Once a template or set of templates are decided upon, the Security Configuration and Analysis snap-in can be used to configure or analyze the system. The tool is also very useful for troubleshooting changes to security settings that may be the cause of problems. A database is created into which a security template can be brought in. Once the security template is added it can be applied to the system or an analysis can be done to show what the state of the system would be were it applied. The definitions in Figure 5 apply to the example output of the tool shown in Figure 6:

Visual flag	Meaning
Red X	The entry is defined in the analysis database and on the system, but the security setting values do not match.
Green check	The entry is defined in the analysis database and on the system and the setting values match.
Question mark	The entry is not defined in the analysis database and, therefore, was not analyzed. If an entry is not analyzed, it may be that it was not defined in the analysis database or that the user who is running the analysis may not have sufficient permission to perform analysis on a specific object or area.

Exclamation point	This item is defined in the analysis database, but does not exist on the actual system. For example, there may be a restricted group that is defined in the analysis database but does not actually exist on the analyzed system.
No highlight	The item is not defined in the analysis database or on the system.

Figure 5 – Security Configuration and Analysis Output Definitions (www.microsoft.com, #15)

Whether an analysis is conducted prior to applying a template or not one must still be performed in order to view the changes.

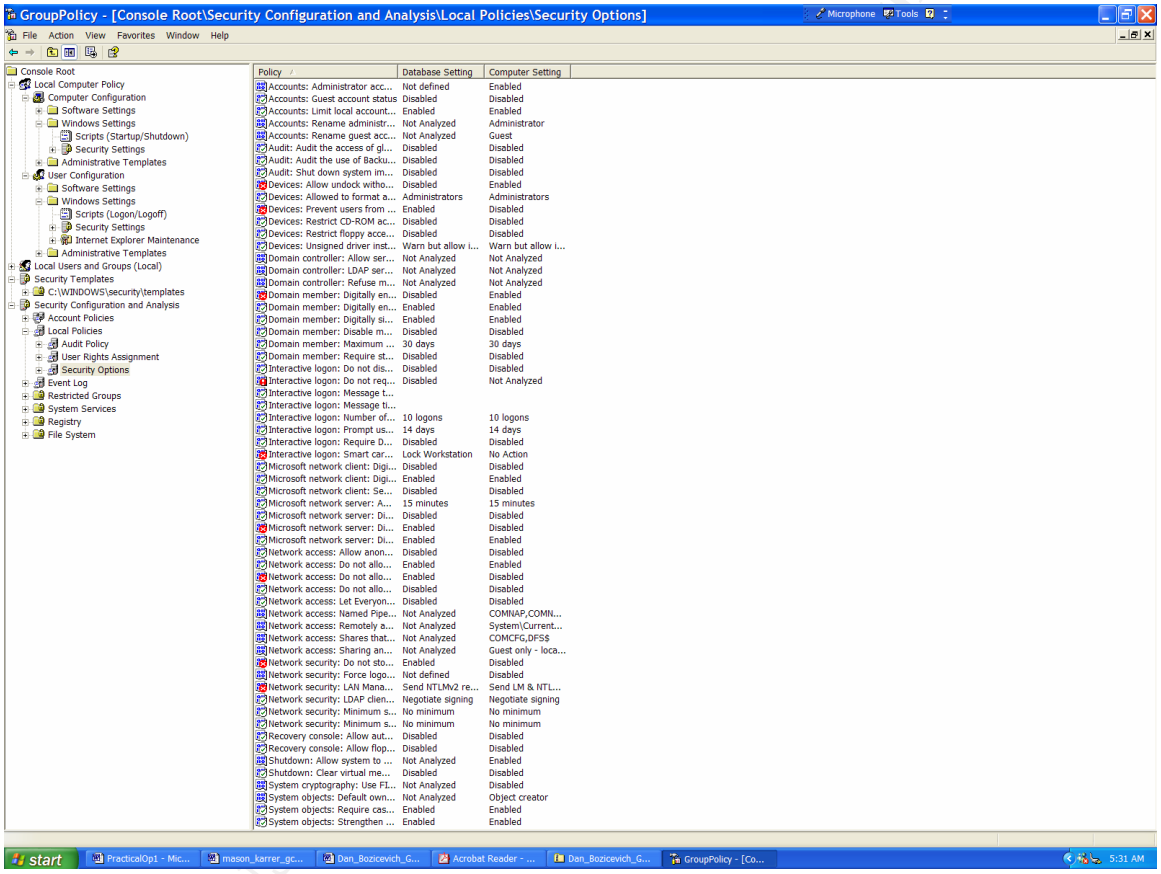

Figure 6 – Security Configuration and Analysis snap-in

5.0 ADDITIONAL SECURITY

GIAC chooses to use some additional security measures in an attempt to supplement the policies, configurations, and procedures already discussed.

Intrusion Detection System:

Although GIAC does not have a full blown Intrusion Detection System, the company does use the somewhat limited capability embedded in the Microsoft ISA Server. The ISA Server is capable of monitoring traffic for a number of well know attacks. Although it is by no means all encompassing it does provide an added level of security and should be configured on all ISA Servers.

Smartcard:

GIAC is transitioning to a single smartcards solution that will control access to both the front door and also to each user's machine. GIAC plans to issue certificates using its own CA (for the purpose of authentication with smartcards); "Smart card certificates must be issued by a Windows 2000 Enterprise CA, using either the Smart Card User or Smart Card Logon templates". (SANS Track 5.2, 150) The company will purchase USB card readers for each employee's computer.

The card itself will be a combination proxy and smart card so it will work with the locking system, server and logs as well as with the Active Directory (Kerberos) when used for authentication. In Windows 2000 a user's logon certificate can be bound to their user account so that Kerberos will use the certificate instead of a password. This can be accomplished through the AD Users and Computers snap-in. Also, Group Policy needs to be set to lock the workstation if the user removes the card.

Since GIAC has some accounts that are security sensitive, it is necessary to limit the power of the enrollment agents so that it will not be possible for an agent to issue certificates for these accounts to themselves. The following procedure will be used in accordance with SANS best practices:

1. "Create a group named "Enrollment Agents". The user accounts that are given Enrollment agent certificates should be members of this group, Users, and no others. Enrollment agents do not need to be administrators.
2. Create an organizational unit in Active Directory named "Security Sensitive Accounts". Add the accounts of all administrators, purchasing managers, executives, and any other account that you do not wish to issue certificates for.
3. Deny the Enrollment Agents group any access to the Security Sensitive Accounts OU. Do the same for any other OU desired. Enrollment Agents must be able to read some of a user's account information in order to issue a smart card certificate on behalf of that user. (This can also be done on a per-user basis." (SANS Track 5.2, 154)

The card not only controls physical access to the office space but also adds a device to the authentication process so that both the card itself and the password/pin have to be compromised in order to gain access to the system. Finally the card will also be used as the company ID so it will have company information as well as an employee picture. This should provide a more secure and convenient (since it is one card) way for users to access both the physical office and their computer resources.

Encrypting File System:

Encryption is now available natively within the newer Windows operating systems (Windows 2000 and XP). Many GIAC employees travel extensively and have a laptop for both office and road use. It is highly encouraged that GIAC employees use EFS to encrypt sensitive materials on their computer. It is corporate policy that all travelers use the SYSKEY.EXE Startup Password option in conjunction with EFS. "The BIOS password on a laptop is usually trivial to circumvent. The SYSKEY password, on the other hand, can not be circumvented, and, when combined with the correct use of EFS file encryption can secure a laptop's data against even against sophisticated and well funded adversaries." (SANS Track 5.1, 74) A simple way to incorporate EFS is to keep all folders and files in My Documents or a single folder and encrypt the folder itself. That way all documents written to the folder will be encrypted and no clear text trace of them will exist on the hard drive. Also, the temporary folder should be encrypted to ensure that no plain text copies of files are deposited there.

"EFS will automatically enroll a user for an EFS certificate with a Windows 2000 CA, if one is available, or it will generate its own self-signed certificates. EFS will not automatically enroll against a third party CA." (PKI, 4) As stated earlier GIAC uses a Microsoft CA. Given that, there will be one administrator as well as the head of each division who will be designated recovery agents for the domain. The senior administrator and the Chief Technology Officer will be enterprise wide recovery agents. All recovery certificates issued will require a password for use on the stand alone recovery PC. After EFS Recovery certificates are issued, permissions on the EFS Recovery certificate template should be set to deny access to everyone. Administrators can take ownership back whenever necessary. At no time should the private key of a recovery agent be on any machine other than the one designated for recovery. At no time should a recovery agent account be used for anything but recovery. The passwords will be stored in the safe along with the keys since in theory they will not have to be used extensively and may be forgotten. (SANS Track 5.2, 140)

RRAS and VPNs:

GIAC has requirements for a secure and functional method of accessing the network remotely. They have many individuals who travel regularly and also have a branch office in AL - all need access to resources located in NH. GIAC uses ISA server which basically rides on top of RRAS. The ISA server is not part of the internal domain and therefore does not have access to an internal DC. Since external users dialing in need to

be authenticated the most practical solution is to use a RADIUS server to access the Active Directory. The Internet Authentication Server ((IAS), not to be confused with ISA) is the Microsoft implementation of RADIUS and it comes bundled in Windows 2000 so it is used to provide authentication information to the RRAS server. In other words the RRAS server will actually be a client that outsources its own authentication to the RADIUS server (IAS). The IAS box in turn needs permission to access account information in AD. "This is accomplished by "registering" the IAS server, which simply adds the server's account to the "RAS and IAS Servers" group in Active Directory". (SANS Track 5.3, 121)

Individuals can access the network using a Host-to-Router VPN. They simply connect locally to the internet and then initiate an encrypted tunnel to a firewalled VPN router on the company LAN. Authentication to the company domain is accomplished using their GIAC username and password. Once authenticated the user has access to company resources (files, email, etc.). A Router-to-Router VPN will connect the NH site to the AL site. This method of connection is simple to set up and completely seamless to users.

Initially, GIAC will use Point-to-Point Tunneling Protocol (PPTP) as its VPN protocol for remote Host-to-Router connections. Although it is not as secure as Layer 2 Tunneling Protocol (L2TP), it can be brought to a level that will more than meet GIAC's security requirements. The reason for not using L2TP at this time is the fact that it uses Encapsulating Security Payload (ESP) in transport mode. Currently ESP can only pass through a NAT router in tunnel mode. GIAC uses NAT and since a DMZ using two ISA servers is planned, PPTP will be used due to its compatibility with NAT servers. PPTPs main weakness arises from the fact that it is susceptible to password hash sniffing. GIAC will counter this through the use of group policy. GIAC requires a reasonably strong password be used by all employees (See Section 4 Group Policy, Password Policy). Although it is still possible to extract the password and load into a password cracker, making it long and complex helps to combat this known weakness within PPTP.

The Router-to-Router VPN should be able to use L2TP with no problem as there are only two hosts involved and both must have a public email address on the interface connected to the Internet.

Test Suite and DNS Example:

GIAC owns several domain names and maintains a very active Windows/network test suite. In order to simulate the most realistic environment, a miniature stand alone enterprise containing a web server, mail server, DCs, workstations, etc. is constantly up and running. It is connected to the internet via a separate (and slower) network connection than the one regularly used by GIAC. On this suite GIAC out sources external DNS services using Verisign's servers and web based tool which allow customers to control their own DNS records (A-records, MX record's, aliases, etc.). The service costs $24 per year per domain; for that price a customer completely off loads the cost of maintaining the two servers (technically two IP addresses) required by the registrar. In addition the somewhat intangible but significant costs and headaches of

maintaining the security posture of the services are off loaded to Verisign. An SLA guarantees 100% uptime while allowing the customer to maintain their own zone files.

The DNS service offered by Verisign seems like an excellent value. Currently DNS is out sourced at a cost of $10/month and there is no control over GIAC zone files. Minimal changes are possible through a help desk but support in the past has been mediocre. GIAC had planned to stand up internal DNS servers. However, if the Verisign service which is currently being evaluated is a success, the operational external DNS will continue to be outsourced. If the Verisign service works as advertised it will serve to improve GIAC's security posture for a very minimal cost.

DNS is just one example of the many on-going projects that are continually being evaluated on the test network. The test environment is also used to evaluate and understand next generation Windows servers and technologies for the purpose of implementation. In addition all GIAC group policy and architectural changes are proven here before they go out to the live corporate network. GIAC uses the test network to ensure that the company maintains a solid security posture while impacting performance as little as possible over both the short and long term.

IPSec:

IPSec will be used to further increase the security of the DMZ once implemented. The ISA server Gateway to Gateway VPN is already taking advantage of IPSec in order to encrypt all traffic between the NH and AL sites. The firewall will allow traffic from the outside to the public segment of the DMZ but never from the outside to the management segment containing the DMZ DCs. All traffic from the internal LAN or from the public DMZ statement will use IPSec Authentication Header (AH). The firewall and all hosts will be configured to enforce this policy. AH does not supply encryption however, it does provide integrity and authentication. In this case encryption is not necessary since the traffic is never leaving the protected network and would; "ESP encryption would incur needless CPU overhead." (SANS Track 5.4, 14)

Perhaps the most beneficial security measure may be to get employees (besides administrators) interested in security. This is no small task but GIAC makes the effort to do so by having a quarterly security stand down where all employees attend a one hour briefing and discussion. Employees are encouraged to understand the company's security architecture and also taught how to ensure their own workstations and laptops remain secure. The meeting is always held on a Friday after which employees are let off work an hour early. Prizes and T-Shirts are awarded for answering questions. The intent is to remove some of the tedium of security by making it fun.

There is also a security section on the internal GIAC webpage that posts security holes/fixes pertaining to the GIAC network. The website offers cash prizes to employees who discover security holes and report them to the security administrators. GIAC believes that its security posture is greatly increased by making each employee responsible for security and not just relying on a handful of administrators. Maintaining

an up-to-date secure enterprise is relentless endeavor that requires everyone to do at least a small part.

6.0 REFERENCES

1. Exchange User Education. Microsoft Outlook Web Access in Microsoft Exchange Server 2000. Exchange Core Documentation. Microsoft Corporation. Mar 2000, updated May 2002.
2. Fossen, Jason. Track 5.1 – Windows 2000/XP Active Directory, Group Policy and DNS. SANS Institute. 2002.
3. Fossen, Jason. Track 5.2 – Windows 2000/XP PKI, Smart Cards and EFS. SANS Institute. 2002.
4. Fossen, Jason. Track 5.3 – Windows 2000/XP IPSec and VPNs. SANS Institute. 2002.
5. Fossen, Jason. Track 5.4 – Windows 2000/XP Securing Internet Information Server. SANS Institute. 2002.
6. Hanley, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. NSA SNAC. 7/22/2002.
7. Heywood, Drew. Windows 2000 Network Services. Sans Publishing. 2001.
8. Microsoft Windows Product Group. Best Practice Active Directory Deployment for Managing Windows 2000. Microsoft Press. 1985-2001
9. Pitsenbarger, Trent. Guide to the Secure Configuration and Administration of Microsoft ISA Server 2000 v1.4. NSA SNAC. 7/18/01.
10. Rice, David C. Group Policy Reference v1.08. NSA SNAC. 3/2/02.
11. Sanderson, Michael J. Guide to Securing Microsoft Windows 2000 Active Directory v1.0. NSA SNAC. Dec 2000.
12. Spealman, Jill. MCSE Training Kit Microsoft Windows 2000 Active Directory Services. Microsoft Press. 2000.
13. White Paper: Windows 2000 Server Public Key Interoperability. Microsoft Corporation. 1999.
14. www.microsoft.com; Microsoft Knowledge Base Article – Q223346; FSMO Placement and Optimization on Win2K DCs 10/10/2002
15. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SCMUsingAnalysis.asp Security Configuration and Analysis Tool Output.