Global Information Assurance Certification Paper

Implementing and Securing the Merger of SANS Co. and GIAC Enterprises

Joseph A. Doyle
GCWN Practical Assignment
Version 3.2 - Option 1
August 21, 2003

Table of Contents

0 Summary

This paper documents the merger of SANS Co. and GIAC Enterprises. Both companies work with the United States government to provide electronic systems for use in weapons systems. As such, both companies require a high level of security across their computing environments. This paper covers the securing of the merger of these two companies in three major sections.

The Merger of SANS Co. and GIAC Enterprises
This section details both companies and their existing networks. It goes on to cover the merging of the network topologies and of the Microsoft Windows forests and domains. It ends with a discussion on the benefits provided by the merger.

The Security Polices
The second section covers the security policies that the merged company will use to provide a secure computing environment. This includes a detailed explanation of a policy suitable for Windows Server 2003 that compares to the security policies created by the NSA. The testing of the security policies is covered, followed by a plan for managing the security policy as time goes on.

Auditing the Network
The final section covers auditing of the merged networks. It provides a brief section on general auditing information, and then covers the auditing plan for the merged company, including processes and tools used.

1 The Merger of SANS Co and GIAC Enterprises

1.1 Overview of SANS, GIAC and the Merger

The SANS Company (referred to as SANS) is a leading developer of weapon systems. Last year, SANS made a strategic move by purchasing a company based in Milwaukee. That company designed long range weapons systems and had many long-term contracts with the government. SANS currently employs 2500 people. In an effort to vertically grow in their market, a merger with GIAC Enterprises (referred to as GIAC) occurred.

GIAC develops and tests communication systems for many of the weapons systems used by the government and are considered to be a top player in the field. By merging the two companies together, SANS will bring additional capabilities of product development in-house, and GIAC will gain the financial backing and support of a larger company. GIAC employs 29 people between their two offices. It is estimated that the GIAC staff will grow to approximately 500 in the first year after the merger.

Since both companies deal with government agencies on a regular basis, each has a specific set of requirements that need to be taken into account when looking to merge the two IT infrastructures. The following sections describe the current network layouts and then adjustments made to link these two companies, with minimal impact to their customers and staff, in a secure manner.

1.2 The SANS Co. Network

The corporate headquarters is located in Chicago, IL. There are 2350 employees in the Chicago office and 150 employees in the Milwaukee office. All administration and corporate decisions happen from the Chicago office. The Milwaukee office has a limited staff for local help desk support and physical server maintenance.

The SANS network is comprised of 4 internal domains and an external DMZ domain. The root domain contains the user accounts for the majority of the staff. Sub-domains exist for the research department, the Milwaukee office, and the test lab. The old *'research.sans.com'* domain still exists for the limited research that continues in Chicago.

The Chicago office has dual DS-3 connections to the internet and the Milwaukee office has a single T1 connection to the internet. SANS uses a hardware based, 256-bit VPN to secure communications from Chicago to Milwaukee. A majority of the research and development is done in Milwaukee and all communications between the two are encrypted using IPSec.

SANS prides itself in using the latest technology to stay ahead of its competitors and was an early adaptor of Microsoft Windows Server 2003. Currently all of their servers are running Windows Server 2003 and the Domain and Forest Functional

levels are set to Windows Server 2003 to take advantage of all possible features. Windows Server 2003 Functional levels are the equivalent of Windows 2000 Native mode. All of SANS workstations are running Microsoft Windows XP with Service Pack 1a.

The internal LAN is made up of all Cisco Switching products starting with Catalyst 6509 switches for the core, and Catalyst 3548 switches on the distribution layer. The distribution layer is connected to the core with fiber optic cable. Category 5e wiring is used from the distribution closets to the employee's desks. VLANs are used to create separate broadcast domains on the network.

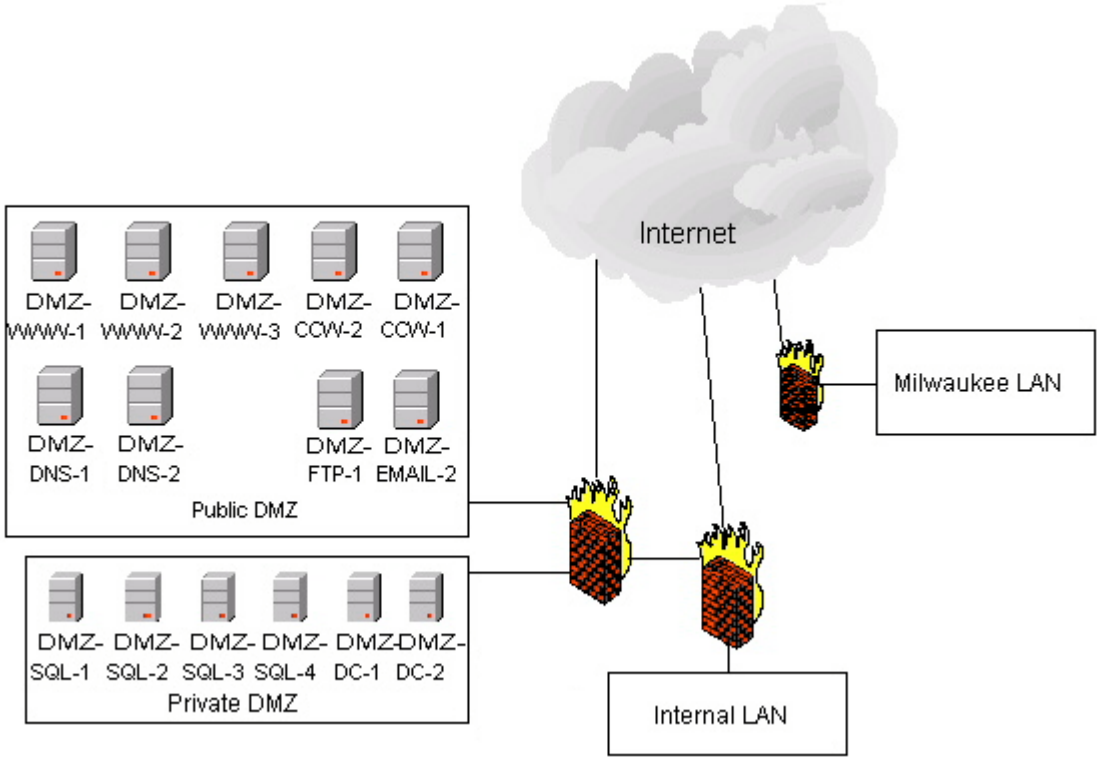

Figure 1 - Basic View of SANS Network

SANS implements it's DMZ by using a separate forest with a one-way trust to the internal domain. This helps to reduce the threat of an attacker using a DMZ server to attack the internal domain. Physically the DMZ is partitioned using Cisco PIX firewalls into two separate subnets. Access-lists are used to limit the access DMZ servers have with all subnets other than their own.

All workstations and servers in the company are configured and secured using Active Directory to keep administration as automatic as possible. For workstations, SANS follows the NSA recommendations for securing Windows XP Professional computers. Since there currently isn't an NSA recommendation for Server 2003, SANS has developed its own policy, combining the NSA Windows XP

recommendations and the Microsoft Windows Server 2003 Security Guide (Microsoft-3). A more detailed look at that policy is covered in Section 2.2.

SANS also has centrally managed anti-virus and patching for servers and workstations. They use McAfee ePolicy Orchestrator to deploy, manage, update, and audit anti-virus settings. This allows SANS to manage the anti-virus protection, globally enforce policy, and generate reports showing policy compliance. Another key element to this tool is the ability to proactively act, or to react to an occurring attack through centralized management.

Shavlik's hfNetChkPro is used to remotely deploy and audit service packs and patches to servers and workstations. This tool helps SANS ensure the computing environment is proactively defended against known vulnerabilities. A negative feature of the hfNetChkPro tool is that it requires the Task Scheduler service which is recommended to be disabled.

SANS also uses Snort and ACID as an intrusion detection system and reporting tool. Snort allows for real-time monitoring of traffic, detecting and alerting when potential attacks are occurring both in the DMZ and on the internal network. ACID provides a real-time view of the current alerts that Snort has caught and allows for flexible web-based reporting. Links to the software mentioned above are provided in the References section.

One of the most important parts of the SANS network is their corporate web site. At the site, customers can get product information, pricing, place orders, and access their order. The main site and product catalog consist of three servers running Server 2003 Web Edition. The web servers use Network Load Balancing for fault tolerance and load balancing. The site also uses a two server SQL cluster for the database back-end. SANS also has a customer collaboration site which is hosted by two load balanced web servers with a second SQL cluster as the back-end.

All sensitive areas of the main site use SSL to encrypt the data stream. Customer information and order processing along with the entire collaboration site are examples of sensitive areas that use SSL. Because their web presence is very important, SANS continually looks for way to leverage new web-based technologies to gain new customers and keep existing ones.

1.3 The GIAC Enterprises Network

GIAC has a network design very similar to SANS, only smaller in scale. The GIAC design was done by Ray Smith, Analyst Number 0226, entitled "Designing a Secure Windows 2000 Infrastructure – GIAC Corporation". Here is a quick overview of the important details of the GIAC network. For the use in this paper, it is assumed that GIAC has implemented their DMZ as planned and their web site has become an important part of their business.

Their main office is located in Nashua, NH with a small remote office in Birmingham, AL. Each site has a T1 connection and they are joined using software VPN via Microsoft's ISA Server. ISA Server is also used as the firewall product and limited IDS. All of their servers are running Windows 2000, and the workstations are a mixture of Windows 2000 Professional and Windows XP Professional. GIAC also has a second forest which is uses for its DMZ servers, securing it with access-lists and IPSec allowing controlled access to and from the DMZ.

The GIAC website is used to not only sell and showcase products; it is also used for online support. Initial numbers started low, but the site has steadily grown to become a significant portion of revenue. Customers view their web based help desk to be the feature that makes GIAC stick out from its competitors. SANS is very interested in acquiring that same process for their web site and plans to expand on that idea in the future.

GIAC also heavily uses Active Directory and Group Policy for security settings and software deployment. They have also chosen to use the NSA guides as starting points for securing their servers and workstations. GIAC utilizes a PKI which uses Verisign to allow for encrypted email to external customers. Currently, a full featured IDS is not implemented, and the design does not cover anti-virus and patch management.

1.4 Merging the Computing Environments

Merging two companies is not an easy task. Name recognition, technical and service level requirements will be just a few of the issues to overcome in the merger. To help customers identify the merger of the companies, the new name will be The SANS-GIAC Company. Due to the nature of the merger, SANS is the controlling company and will retain overall control.

The initial thought was to add GIAC.com as a sub-domain to the SANS.com domain. This was ruled out due to the extensive changes both companies have made to their Active Directory schema and the fear of extended disruption in business.

SANS-GIAC has decided to change the following major areas:

- The company's internet presence will be complete hosted in Chicago by SANS.
- GIAC will be integrated into the SANS VPN network.
- All GIAC servers will be upgraded to Windows Server 2003.
- All GIAC workstations still running Windows 2000 will be upgraded to Windows XP.
- The GIAC domain and forest will be upgraded to Windows 2003 Functional Level
- All ISA Servers will be replaced with Cisco PIX firewalls.
- GIAC will be migrated to the SANS PKI.

As much of GIAC's original configuration and domain specific policies will be retained as possible. The GIAC forest will remain as it is under the current staff's control so as to not disrupt business during the merger. SANS sees no reason to change the details of the network since both networks will still be able to access each others data.

1.4.1 Merging the Network Infrastructures

Both SANS and GIAC have a single branch office connected via VPN over a T1. Since SANS currently has dual DS-3 connections, the Chicago office will be the host for all Internet presence for the new company. All inbound traffic from the Internet will only be directed through Chicago.

The GIAC network will join new company's WAN through SANS' existing VPN. This was decided because SANS 256-bit AES encrypted VPN is superior to GIAC's 168-bit 3DES encrypted VPN. SANS-GIAC prefers to stay with the higher level of encryption to gain the slight increase in security that AES provides.

All outbound internet traffic will be sent using the office's local connection while intranet traffic will be routed over the VPN tunnel.

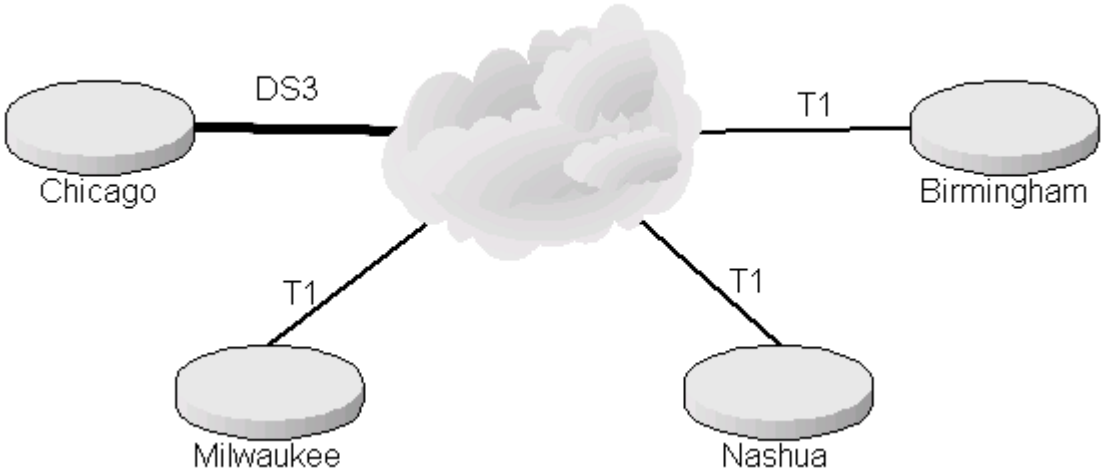

Figure 2 - Internet Connectivity Topology

The new topology creates a meshed network connecting the branch offices to each main office. This provides a high level of redundancy and multiple paths to each site. While it was determined that the Milwaukee office and the Birmingham office do not need to be connected directly to each other, the new network infrastructure does allow for a connection between them in the future if the SANS-GIAC sees the need.

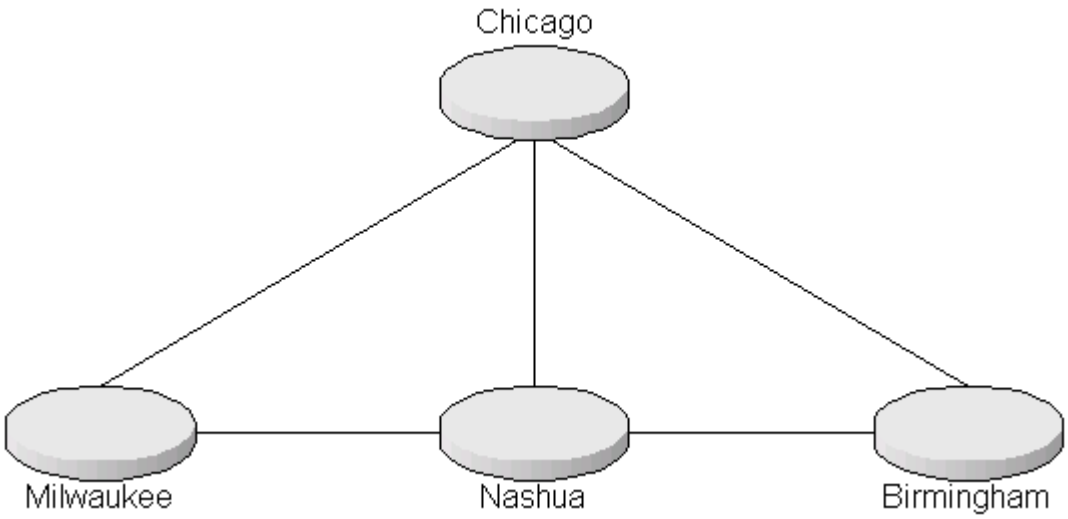

Figure 3 - VPN Site Topology

If the growth of the GIAC portion of the business occurs as expected, the T1 at Nashua will be upgraded to a DS-3. A benefit of this upgrade is that it will allow Nashua to become a disaster recovery site in the future.

1.4.2 Merging the Windows Domains

As mentioned above, the initial design was to have the GIAC domains join the SANS forest as a sub domain. After evaluating the schema changes made by both companies, it was determined that keeping the forests separate was a better option allowing operations to run as normal as possible. This means that both forests will remain unchanged with the exception of the GIAC DMZ.

To allow both companies to work together, both forests will be part of a forest trust. This is a new feature of Windows Server 2003. Traditionally, external trusts would have needed to be established to each domain that needed to be part of the authentication system. This new feature of Windows 2003 allows that, within a forest trust, you only need to setup a transitive trust to the root domains in each forest to gain complete trusts among all the domains in each forest. Since all of the domains will need to trust each other, a forest trust is the easiest method for SANS-GIAC. "When all domains in two forests trust each other and need to authenticate users, establish a forest trust between the forests" (Microsoft-1). Microsoft's Windows 2003 online documentation explains this concept very well. See reference Microsoft-2 for the link.

Another benefit to Windows Server 2003 forests is the ability to later merge the GIAC forest into the SANS forest. Server 2003 allows for the merging and rearranging of domains into and within a forest. The capability of renaming a domain has also been added. This allows for the GIAC domain to someday become giac.sans.com inside the SANS forest. Although it is not in the current plans, this functionality will be required in the future.

The biggest change to the domain design to be implemented will be to merge the DMZ forests of both companies. The new DMZ forest will house all internet facing servers retaining a similar configuration to the way they are currently set up. GIAC will still be able to administer the servers that contain their content just as they do now. The DMZ will have one-way external trusts from the DMZ to the *'corp.sans.com'* and *'corp.gaic.com'* domains. This will allow for easier administration of the DMZ servers while not compromising the security benefits of a DMZ forest.

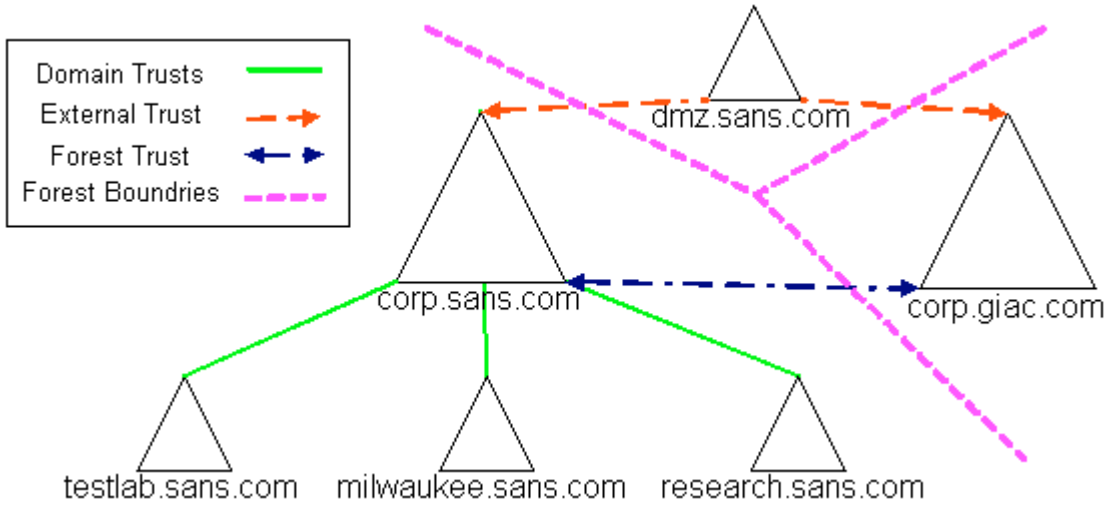

Figure 4 - SANS-GIAC Trusts and Forests

As shown in Figure 3, the new SANS-GIAC enterprise will consist of three forests joined together by trusts to allow for maximum security and flexible administration.

1.5 Benefits of the Merged Environment

The main goal of creating SANS-GIAC is to create a company which better meets the needs of current and future customers. This gets translated down to the computing environment in three main points:

- Reduce the costs of maintaining two separate companies.
- Allow for easily administered resources.
- Have minimal impact on existing business processes.

Costs will be reduced by relocating GIAC's DMZ servers to Chicago, allowing GIAC to stop paying to have its external DNS hosted by another company, moving them to SANS internally hosted DNS servers. This move will allow the Nashua office to reduce the load on their T1 allowing for better performance for inter-office communication. This additional load will be hardly noticed on Chicago's DS-3 pair.

Licensing costs will also be reduced as services and servers are consolidated or removed, such as the decommissioning of the ISA Servers GIAC uses. GIAC Windows licensing will also be absorbed into the SANS Microsoft Enterprise Agreement. This will allow for the licensing of workstation OS and the Office Suite to be almost significantly less.

With the two-way transitive forest trust in place, the newly merged IS department will be able to administer any server or workstation on the network, although complete access to both sides will not be granted to allow for accountability. The main benefit will be having the Chicago staff now manage the GIAC DMZ servers allowing either a reduced staff position in Nashua, or reallocation of a position.

Initially, the forest trust will create no changes to the SANS-GIAC workflow process. This will allow the newly merged company to slowly grow into its new form. The employees will immediately be able to securely share data and the company can start to evaluate future changes. It also provides the ability for permissions to be assigned for users from the GIAC domains to resources from any domain in the SANS forest.

Both the SANS and GIAC web sites will remain as separate sites with the only change being that the GIAC web site's hosts will be physically relocated to Chicago, but still keep existing functionality and design. This is very important to the management of SANS-GIAC because they don't want to lose existing GIAC customers due to major changes to the GIAC web site. This also keeps processes the same for the content maintainers allowing them to continue publishing new content to the site. SANS will start to incorporate the web help desk features that currently exist on the GIAC site. Similarly, the GIAC site will add a customer collaboration site just as it exists on the SANS site.

The end result is SANS-GIAC gaining access to all of the resources of each separate company in a manner that allows them to grow at a controlled rate into a single company. The merged network design will allow for money to be saved, administrative costs and overhead reduced, and each department to keep existing business processes during the merger.

2 The Security Policies

2.1 Requirements for the New Company

Although both companies shared a similar view on security, the introduction of Windows Server 2003 forces a review of the existing policy. SANS-GIAC wants to stay with the NSA recommendations for Windows Security policies. Both SANS and GIAC have been using the NSA Windows XP (NSA-XP) guide prior to the merger, so there are no issues in continuing to use it in the future. The problem is the NSA has not released a recommendation for Server 2003. Since management still requires security policies at a level that the NSA would recommend, SANS-GIAC has developed one.

2.2 Details of the Server 2003 Security Policy

The starting point SANS-GIAC used was the NSA Windows XP template. From there, they examined the higher level security templates policies that come with Server 2003 such as hisecdc.inf and securedc.inf. Additionally, Microsoft has released their own security guide[1] which provides a comparison for three levels of security based on the required security a company desires. The result is a hybrid policy explained below.

To create the SANS-GIAC Server 2003 template, the Security Templates MMC snap-in was used to modify a copy of the NSA Windows XP template. This policy will then be imported into Active Directory as the Security Settings portion of the Group Policy Object when the policy is created. Importing the policy is as simple as right clicking on the Security Settings folder in the Group Policy Object Editor, and choosing “Import Policy…”. A dialog box then allows you to select the template to import.

[1] A link to the guide is listed in the References section under Microsoft-3.

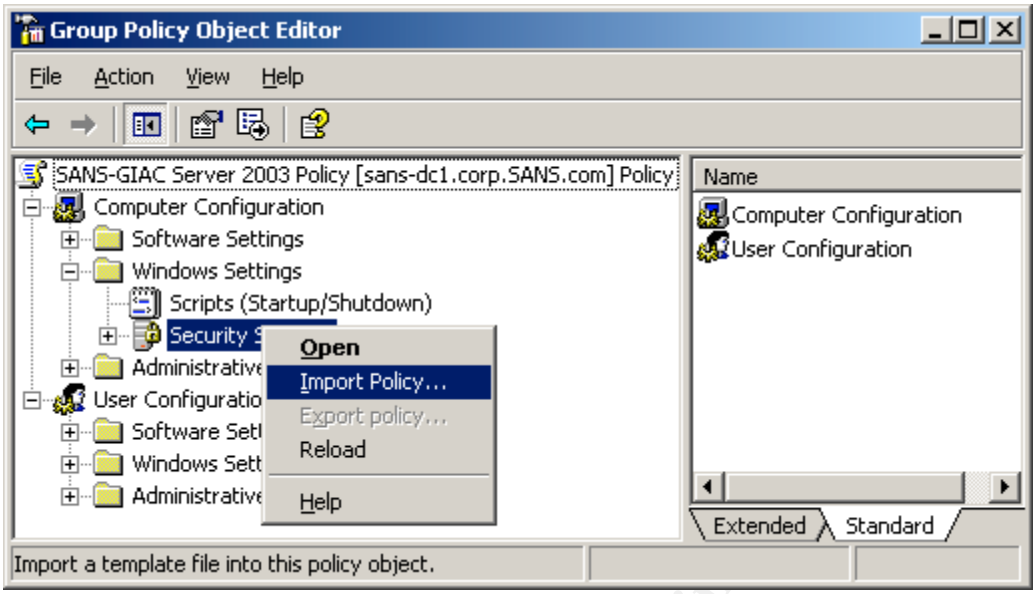

Figure 5 - Importing the Security Template into the GPO

Below are the settings that SANS-GIAC has developed for its Server 2003 template.

Account Policies

Although these have the most impact on domain accounts only, SANS-GIAC will also enforces these settings onto the member servers and workstations. This will keep all accounts, local and domain, uniform in security settings.

Password Policy

Enforce password History	24 passwords remembered
Maximum Password age	90 days
Minimum password age	1 day
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

These settings are identical to the NSA-XP settings. Microsoft only recommended 42 day password age, but agree with the NSA on minimum password length of 12 for high security environments. Microsoft does suggest a minimum password age of 2 days which seems to offer very little additional security to SANS-GIAC.

Account Lockout Policy

Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes

Again, the NSA-XP settings will be used. Microsoft also recommends the 15 minute window for counter and lockout, but recommend 10 invalid attempts

citing the fact that accounts can be locked out if a user changes their password while logged into another computer. (Microsoft-3 pg.39) SANS-GIAC does not view this as an issue and will stay with the NSA setting.

Kerberos Policy	
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	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Microsoft does not provide a recommendation for Kerberos settings. The interesting part is that default settings when enabling this section are very close to the NSA recommendations listed, with the exception of Maximum lifetime for ticket renewal. Microsoft's default is 34 days. The reasoning is that lower settings can provide more security at the cost of increased server utilization. (Microsoft-3 pg.41)

Local Policies

On servers where a variety of applications are installed, the User Rights Assignment section of the policy starts to get complex to implement. Some applications such as Microsoft SQL Server and IIS modify the local settings to allow the application to perform lower-level functions such as debugging. Sometimes the modifications made by an application are required just for that application to operate. The settings provided here will be used as the starting point for the incremental policies since this section will become server dependant based on the applications installed. This is taken into account with the design of the Active Directory OU hierarchy and the use of incremental Group Policies.

Audit Policy	
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	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

In this section, there seems to be a little confusion between the NSA and Microsoft as to what each of these items actually do. SANS-GIAC has come up with the following settings based on common sense trusting Microsoft's explanation of each item. The main discrepancy is the Audit Directory

Service Access field. The NSA comments that this is not used on workstations and member servers, but Microsoft says it is. (Microsoft-3 pg.55) SANS-GIAC, following the NSA's advice, has decided to enable Success and Failure since there will be no overhead if they aren't used on workstations and member servers.

User Rights Assignment

SANS-GIAC used the NSA-XP settings here with the following exceptions.

- Allow logon through Terminal Services – Administrators
- Deny logon through Terminal Services – Guests

The NSA-XP guide mentions that Administrators need to be added if you are going to use Terminal Services for remote administration. SANS-GIAC will be using this feature across all servers.

Security Options

The NSA-XP recommendations and Microsoft's recommendations actually line up very similarly in this section. For most of the differences, the NSA chooses to set Not Defined, whereas Microsoft has a value assigned. Here are the settings that Microsoft recommends that the NSA chooses not to configure.

- Audit: Audit the access of global system object – Disabled
- Audit: Audit the use of Backup and Restore privilege – Disabled
- Microsoft network client: Digitally sign communications(always) – Enabled
- Microsoft network server: Digitally sign communications(always) – Enabled

Additional settings for the Domain Controller policy:

- Domain Controller: Allow server operators to schedule tasks – Disabled
- Domain Controller: LDAP server signing requirements – Require signing
- Domain Controller: Refuse machine account password changes – Disabled
- Domain Controller: Digitally encrypt or sign secure channel data – Enabled

All of the digital signing policies are set to "Always" because all of the computers in SANS-GIAC are Server 2003 and Windows XP. This forces all secure channel traffic to be encrypted and signed in a manner that is incompatible with down-level clients such as NT4 and Windows 9X.

Event Viewer

The Event Viewer is one of the most critical parts of Windows security. All operating system events get captured here. Because of that fact, this section has a very

aggressive policy towards the retention of the logs. The NSA-XP policy is suitable for workstations as far as retention goes, but it is inadequate for servers. Knowing this, a foot note has been added to the NSA guide:

> "NOTE: This recommendation applies to workstations only. Server logs should be cleared manually." (NSA, pg.55)

Following that piece of advice, here are the settings SANS-GIAC uses:

Maximum application log size	4194240 kilobytes
Maximum security log size	4194240 kilobytes
Maximum system log size	4194240 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually

These settings will allow for up to 4GB per log file or the remaining space on the System Root drive, which ever should occur first. As part of SANS-GIAC auditing policy, these logs will be cleared when they are exported to the log management server. This will be covered more in depth in Section 3.2.1.

System Services

The Microsoft guide includes a list of services to configure, while the NSA-XP guide does not. Included in this list are the services that can be disabled across all servers and workstations. SANS-GIAC follows the best practice of not installing services if they are not needed on servers, hence there are no servers running web services or FTP services where they are not needed. The security for all services is set to local Administrators and SYSTEM, both with full control which limits the ability of users to alter these services. This is the list of services that SANS-GIAC configures:

- Alerter – Disabled
- Application Layer Gateway Server – Disabled
  - This service is used in conjunction with Internet Connection Sharing and Internet Connection Firewall. SANS-GIAC doesn't use these features.
- Automatic Updates – Disabled

    - SANS-GIAC uses a patching tool to distribute patches after testing them. We do not want the users to install patches that aren't tested first.
- Clipbook – Disabled
- Distributed File System – Disabled
    - SANS-GIAC currently doesn't use DFS
- Distributed Link Tracking Client – Disabled
- Distributed Link Tracking Server – Disabled
    - These two services allow for shortcuts to automatically update when they move. SANS-GIAC deems this feature unnecessary.
- Error Reporting Service – Disabled
    - SANS-GIAC doesn't wish to send these error reports to Microsoft.
- Fax Service – Disabled
- File Replication Service – Disabled
    - This service is set to Automatic for Domain Controllers since it is used as part of Active Directory replication.
- Help And Support Service – Disabled
    - SANS-GIAC has a help desk capable of answering any questions end users would have, and there is no need for this on the servers.
- IMAPI CD-Burning COM Service – Disabled
    - Any user with a CD-Burner will use 3rd party software that doesn't require this service.
- Indexing Service – Disabled
- Infrared Monitor – Disabled
    - This service only applies to workstations. SANS-GIAC doesn't want users to be able to do file sharing through their infrared port.
- Internet Connection Sharing/Firewall – Disabled
    - All internet connections go through the corporate firewall. There is no need for a server or workstation to become a gateway or run a firewall. Servers on the DMZ will be using IPSec policies instead of the Firewall service.
- Kerberos Key Distribution Center – Disabled
    - This service is only needed on Domain Controllers where it is set to Automatic.
- License Logging Service – Disabled
    - SANS-GIAC does not need this functionality.
- Messenger – Disabled
- Netmeeting Remote Desktop Sharing – Disabled
- Network DDE – Disabled
- Network DDE DSDM – Disabled
    - Network DDE and DSDM services aren't used in any applications at SANS-GIAC.
- Portable Media Serial Number Service – Disabled
- Removable Storage – Disabled

    - This service is only needed if using ntbackup.exe, and SANS-GIAC doesn't.
- Routing and Remote Access – Disabled
- Task Scheduler – Automatic
    - Even though most security guides recommend disabling this service, it is used by the centralized patching tool to deploy patches.
- Telnet – Disabled
- Upload Manager – Disabled
    - This service provides data to Microsoft to allow the correct driver to be downloaded and installed from Windows Update. SANS-GIAC doesn't require this feature.
- Windows Image Acquisition – Disabled
    - This service is used to interact with digital cameras and scanners.
- Wireless Zero Configuration – Disabled
    - Wireless networks aren't implemented at SANS-GIAC

Compared to a list the NSA would have released, SANS-GIAC recognizes itself as being liberal in allowing services to remain running. It was determined, however, that disabling additional services would start to reduce functionality that is either required or desired.

Registry and File System Security
SANS-GIAC uses the settings from the NSA-XP policy. The NSA-XP provided settings provide the appropriate amount of security to the file system and registry to meet SANS-GIAC's requirements.

Public Key Policies
SANS-GIAC has a policy in place to have workstations and servers retrieve the following certificates:

- IPSec – Allows computers to use IPSec for encrypted communications
- Computer – Allows computers to digitally sign client and server authentication

IP Security Policies
These polices are configured specifically for each OU depending on what type of access is required. Currently, the only two types of policies are for accessing the DMZ and accessing resources in the Milwaukee office.

This policy is applied to the top level of the Domain Servers OU in Active Directory. SANS-GIAC follows Microsoft's recommendation of assigning generic policies at the top levels of Active Directory, and then applying more specific policies as needed further down the OU tree.

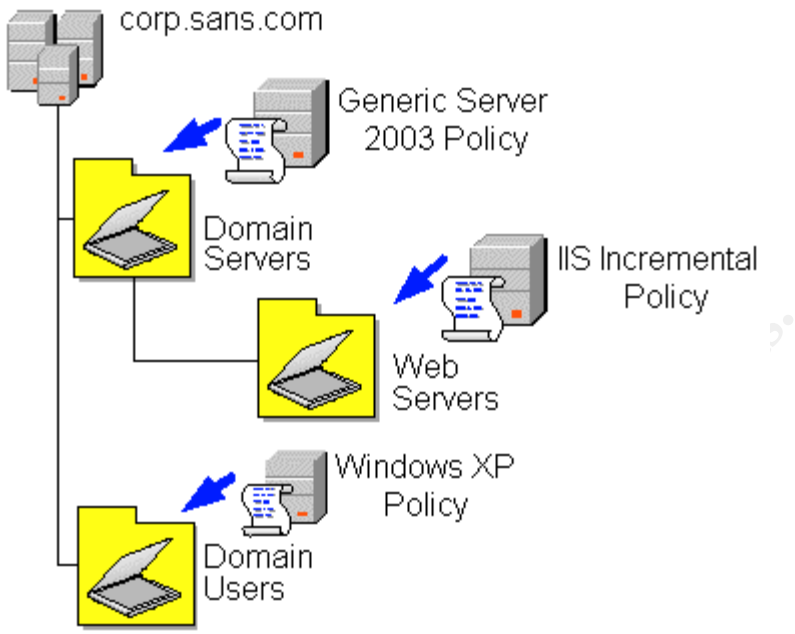

Figure 6 - Example of Incremental Policies

An example of this in action is demonstrated in the next section were we will take a close look at an example web server, how the security policies are applied to it, and the effects of those policies.

2.3 The Security Policies in Action

The security policies are applied through Active Directory Group Policy Objects. Central administration is the greatest benefit to using Active Directory and GPOs to apply the security policies are that they are centrally administered. Also, enforcement and application of the policies is automatic for all of the systems in the company. "Group Policy is your most important security tool" (Fossen, p56).

2.3.1 Applying the Group Policies

As mentioned above, the application of Group Policy is actually an automatic process. Every 90 minutes, plus or minus 30 minutes for randomization, computers in the domains will contact a domain controller and refresh their Group Policy settings. This is an acceptable timeframe for applying our settings enterprise wide to a large number of computers. However, for or testing the application of these settings, however, a possible two hour wait is a little long. Knowing there would be times that administrators would need more control in refreshing Group Policy, Microsoft has provided the GPUPDATE.EXE tool.

GPUPDATE is a new tool for Windows XP and Server 2003. It offers extended functionality compared to the Windows 2000 command of SECEDIT /refreshpolicy. Most of the additional options are to allow more control for Group Policy refreshes via scripting. Some of the more useful new options are:

- /Force – refresh and reapply the all of the policies, not just what has changed.
- /Logoff – refresh the policies, and then log the current user off.
- /Boot – refresh the policies, and then reboot the computer.

A complete list of the command line switches can be found by using the /? switch at a command prompt.

With a method for quickly applying the Group Policies, the test plan can be started in the Development Lab using the testlab.sans.com domain.

2.3.2 Verifying and Testing the Settings on a Web Server

In the Development Lab, they will test the impact of the security policies on a web server.

In addition to the base Server 2003 Policy, SANS-GIAC has an incremental IIS policy that adds IUSR_*[ServerName]* and IWAM_*[ServerName]* to the "Access this computer from the network", "Logon as a batch job", and "Logon Locally" settings.

The policy also applies the correct NTFS security to D:\LogFiles and D:\Inetpub. These are static locations that are identical for every web server in SANS-GIAC enterprise and configured in IIS as server defaults. Additional IPSec policies are added to allow for secure access to the server for publishing new content and gathering the IIS log files.

First, Group Policies are applied to the OU tree. The policy is then refreshed on the web server and on a test workstation by going to a command prompt and using GPUPDATE /Force command. Next, verification must occur to ensure that the polices have actually applied, and that the web server is still functional. By checking the Application Event Log, it can be determined if the policy has successfully applied. If it has, there should be an event that looks similar to Figure 7. Testing can then begin.

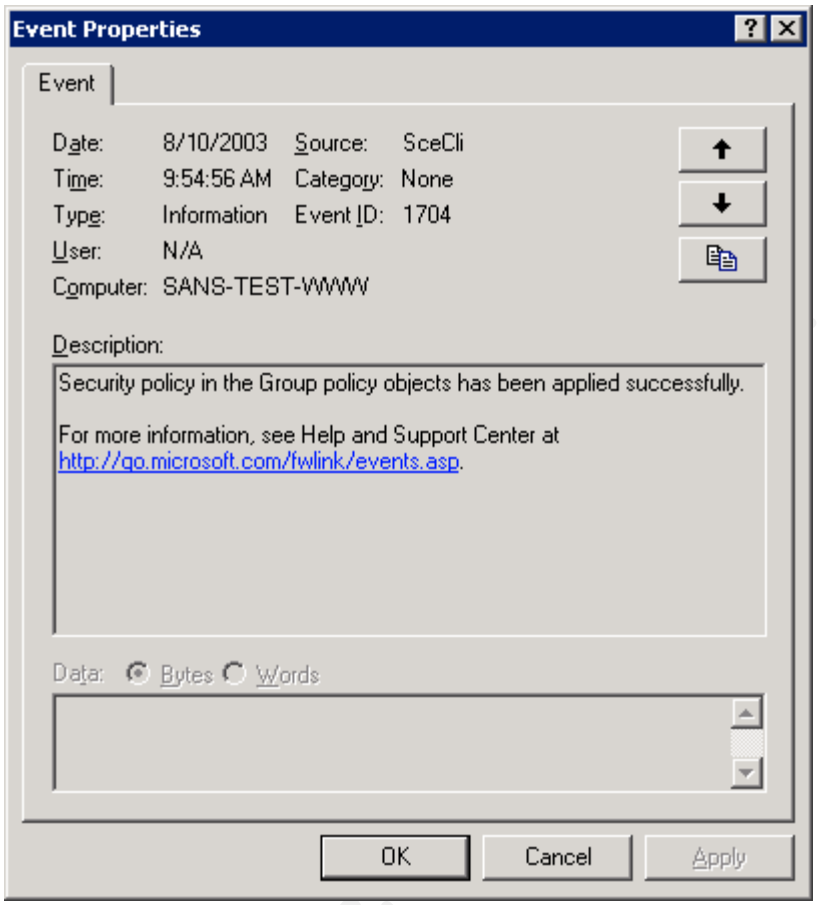

Figure 7 - A successful Group Policy event

Once the policy has been applied to the server, the easiest way to verify that all of the settings have been applied is to use the Security Configuration and Analysis MMC snap-in.

To start, right click on the root of the snap-in and choose Open Database. It is recommended to save the database to a location other than inside the current user profile so that it can be easily retrieved later.

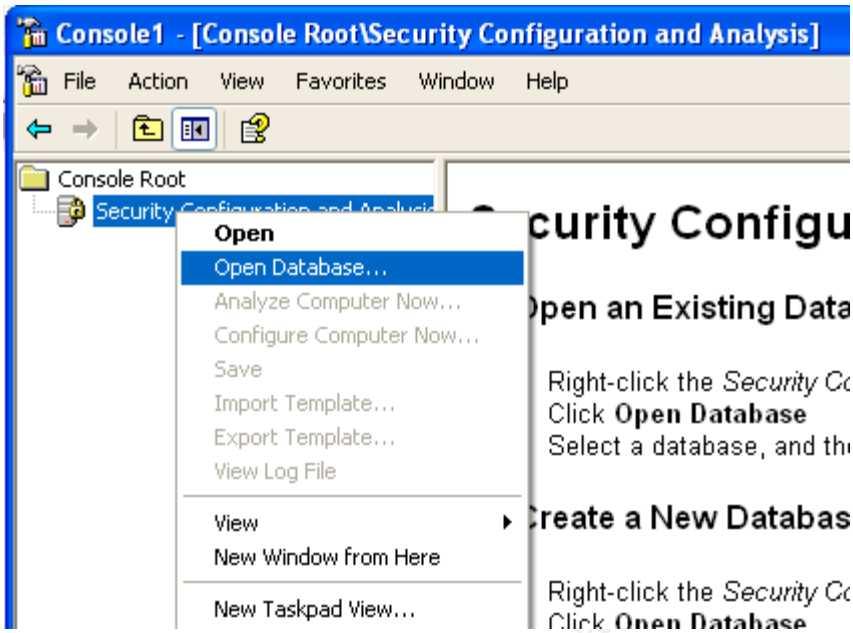

Figure 8 - Creating the Database

The next window prompts for a security template to use as the basis of our database. Since the engineers are interested in comparing the net result of our GPOs applied to the server, all templates that will be applied via Group Policy will need to be added into the database. The Import dialog box only allows the addition of a single template at a time and there are multiple to add. The Security Configuration and Analysis tool was designed for just such a situation. The tool allows us to import multiple templates into a single database, but only one at a time.

In creating the database, the end-result needs to mimic the way that Active Directory applies and merges multiple GPOs. The first template to import will be the generic Server 2003 template that was created above, which in Active Directory is applied at the top level OU.

At this point, the tool gives instructs on how to start the analysis, but all of the templates have not been imported yet; the IIS specific template still remains. This is done by again right clicking on the root of the snap-in and choosing Import Template. Selecting the IIS template will merge it into the database. Be sure that the check box at the bottom of the dialog box is cleared. If it's not, then the database will be reset using only the IIS template, losing the Server 2003 settings. It is also important to know that if there are any conflicts between the two policies, the last template applied will determine the setting used. This is how the server will combine multiple policies from Active Directory, and that's how this tool to works as well.

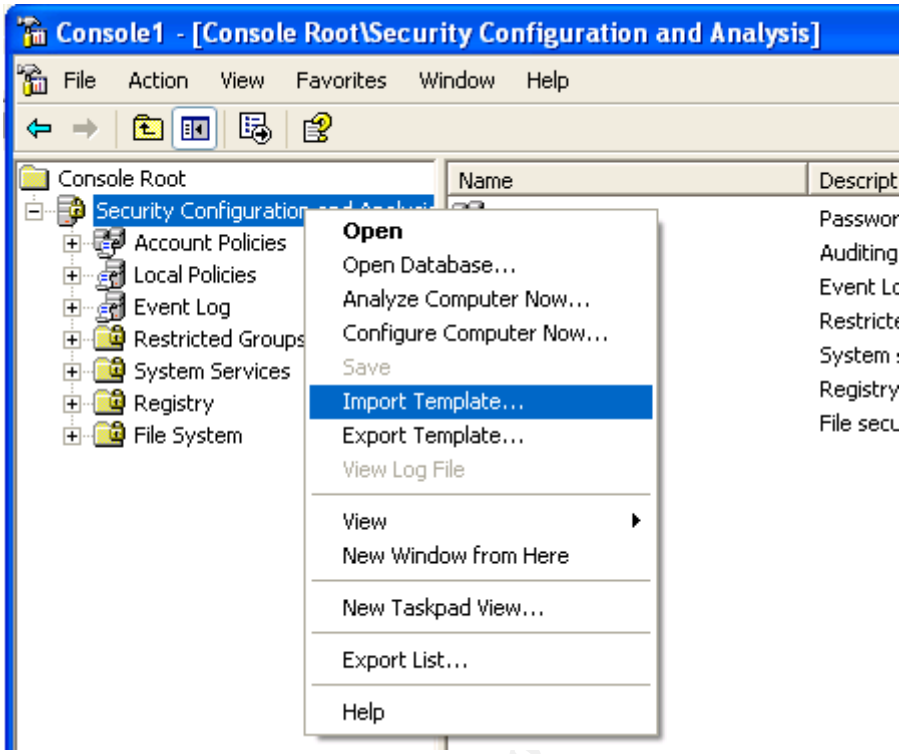

Figure 9 - Importing the second template

Now our database is ready to analyze the server. Once more right click on Security Configuration and Analysis snap-in, and this time choose Analyze Computer Now. It is recommended to save the log file into the same folder that we saved the database into for quick access afterwards.

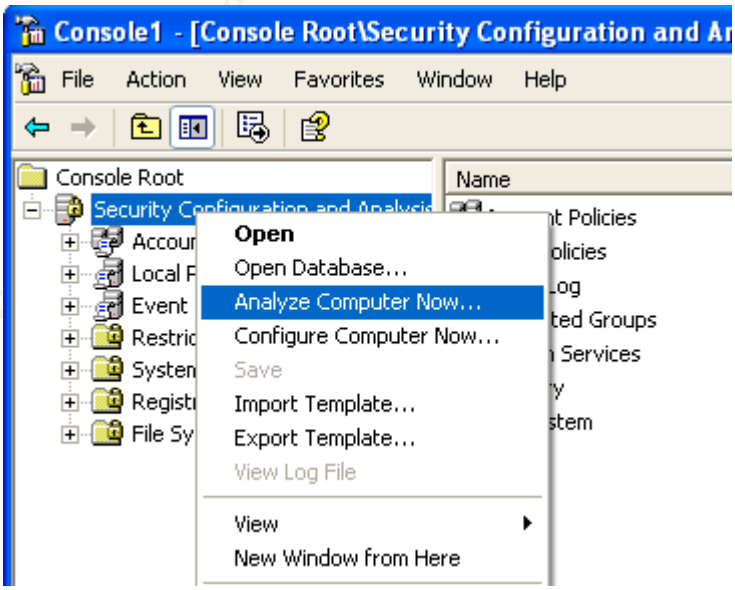

Figure 10 - Starting the analysis

The tool will now compare all of the settings in the database with the current settings applied to the server. This process can take anywhere from one minute to ten minutes depending on how many settings are actually in the database being compared and the speed of the system. When finished, the tool allows us to browse through the database to see where the settings are the same and where they are different. When the computer settings match the database, a green check mark icon is shown. When they differ, a red 'X' icon will be displayed. In addition to browsing for differences, the log file also has a list of all the settings and their status.

After the analysis is finished, we see that our settings have indeed taken affect. The log file shows a few errors for configuring items that do not exist on our server, but those can be safely ignored. The log file shows us that the Group Policy Objects have been applied via Active Directory and we are now ready to test the server for functionality and the effects of the policy.

2.4 The Effects of the Security Policy

Once the application of the policy has been verified on the web server, it's time to verify that the web server is still functional, and that the restrictions applied are being enforced. Since the engineers are dealing with a server that is exclusively a web server, the functionality list is relatively short. The engineers only care that the web site is serving all of its web pages correctly, and that the server can be administered.

2.4.1 Evaluating the Security Settings

Since there are hundreds of individual changes made to the server, only one of them will be covered here for the sake of brevity.

Two critical areas on a web server are the actual content, and the IIS log files. By default in Windows Server 2003, the permissions allow Users to have read access to an entire, non-system hard drive. SANS-GIAC prefers that only Administrators have any access to the logs, so in the security policy they have changed the permission on the log files folder to only allow access to Administrators and SYSTEM. As shown in Figure 11, the NTFS permissions have been correctly applied via the GPO.

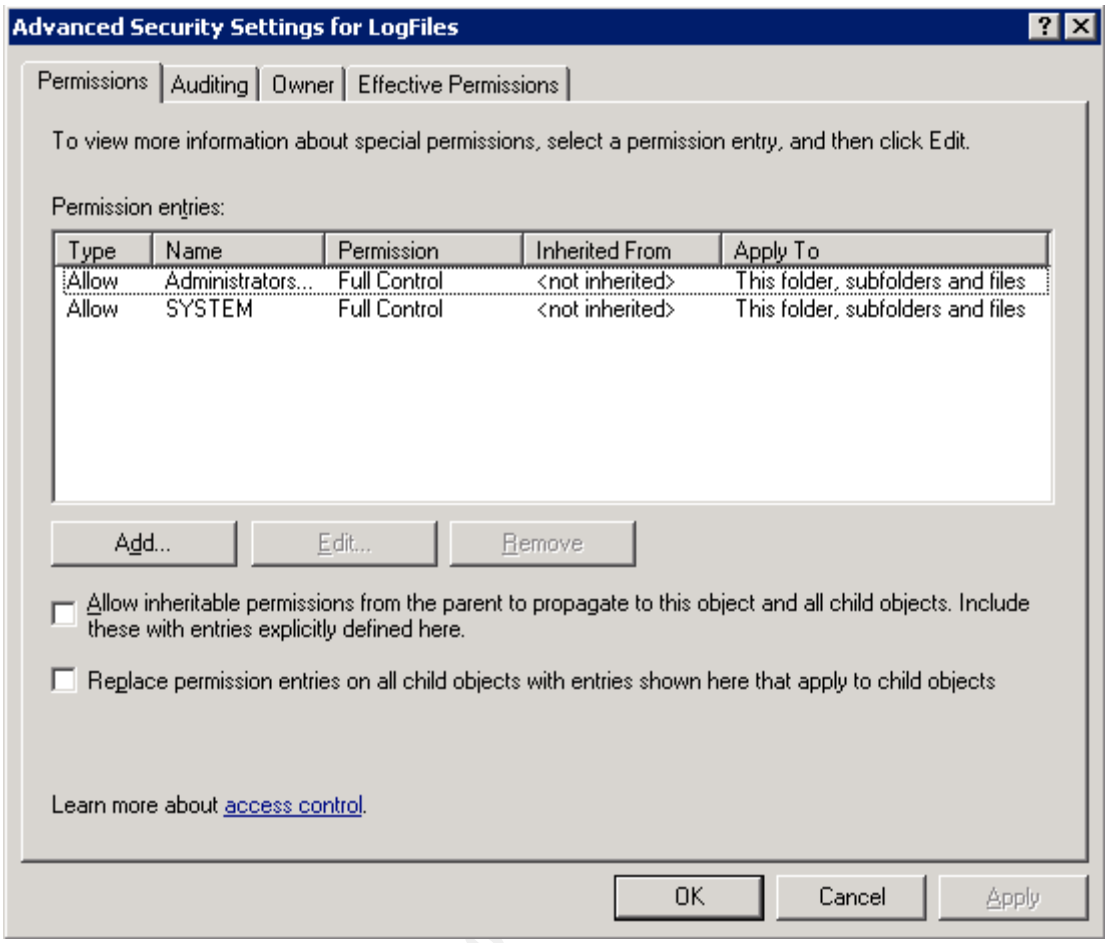

Figure 11 - Security on LogFiles folder

The engineers are also interested in access to the server. An important method of administering the server will be the use of Terminal Services for remote administration. The security policy enforces the use of IPSec encryption for Terminal Server sessions based on certificates. The test plan required that a workstation that is part of the Development Lab and has matching IPSec policies connect to the web server using the Remote Desktop Connection client; verify the ability to connect, and that IPSec is active. The test was a success.

In Windows 2000, a tool called IPSECMON was used to get information about IPSec usage and connections. In Windows XP and Server 2003 there is a new tool to get IPSec information: the IP Security Monitor MMC snap-in. It provides the same basic information IPSECMON does, but also allows administrators to see more of the specifics for each IPSec association. When this snap-in is run on the test workstation after connecting to the web server, it displays the active IPSec association (see Figure 12). Notice that the Destination Port is 3389 which is used for Terminal Services, and the two IP addresses were the test workstation and web server respectively, demonstrating the success of the security policies in allowing appropriate functionality.

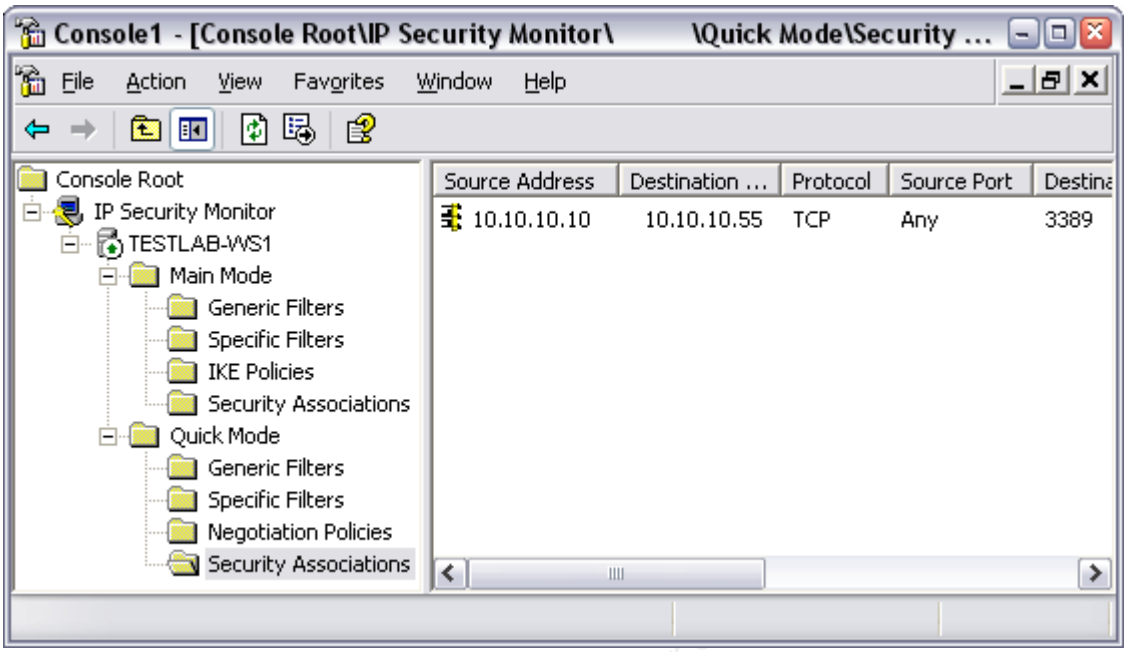

Figure 12 - An active IPSec association

The next thing tested was the IIS service itself. First, verification was performed to ensure that the World Wide Web Publishing Service had started. The next step was to attempt to retrieve content from the server. The test workstation was used to launch Internet Explorer and then browse to the URL of the server. The web server was able to send the page as shown in Figure 13. Again, the engineer's tests were successful.

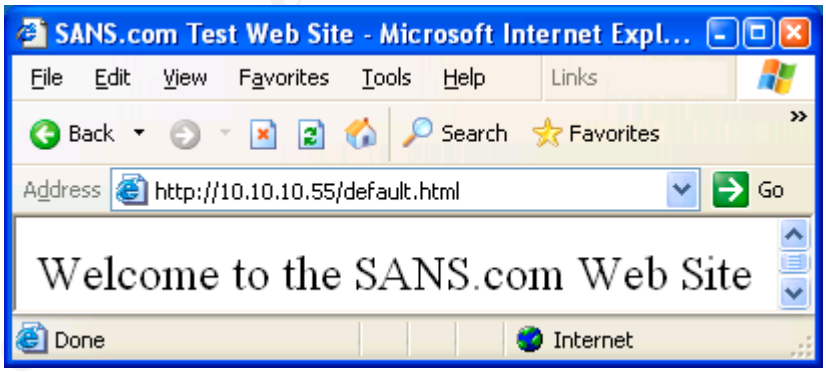

Figure 13 - Web Site for the Test WWW Server

2.4.2 Changes to the Policies

After the policies on a web server had been tested, the test plan continued with the other Development Lab servers. Any changes that needed to be made to the security policies to either fix broken applications or to correctly apply the required

security were to be determined during that testing so the production environment was not disrupted.

For SANS-GIAC, the testing went smoothly with no unexpected results. No changes needed to be made to any of the policies.

2.5 Managing the Security Policies Over Time

As with any process, changes and modifications to the security policies must be made over time. Since SANS-GIAC is expecting to grow significantly in the next year, planning must be done to ensure the security policies are not only enforced, but applicable. SANS-GIAC is large enough that they can dedicate staff to the administration of Active Directory which allows a smaller number of people to manage the policy.

The biggest threat to the security policies are new applications, such as Exchange Server 2003, which may require changes to the policy to function. SANS-GIAC is hoping to catch any of those problems through the use of their Development Lab. As part of any project, time must be spent evaluating the compatibility of the application with the current security policies. If needed, changes are documented and tested before the new systems go into production.

2.5.1 Growth Planning for the Policies

Active Directory and the automation of Group Policy will ensure that the deployment of the policies is scalable, although growth is easily handled by adding more domain controllers to distribute the load. The need for additional policies also scales in a efficient manner. The benefit to having a base policy with incremental policies is that it allows administrators to simply add a new OU then add the incremental policy.

3 Auditing the Network

3.1 The Reason for Auditing Security Settings

One of the junior members of the department asked these questions: "Audit our security settings? Shouldn't Active Directory and Group Policy be taking care of that for us?"

The simple answer is yes, it should be. The problem is Active Directory doesn't have a method for telling you if a policy or parts of a policy have failed to apply to a computer. It also isn't able to notify you if someone has changed or blocked the policies on a computer.

Auditing answers the question "Is Active Directory and Group Policy doing its job?" Not only does it provide that answer, but it also allows administrators to know where it is failing and react to that failure. Auditing is also your proof to the management that your security settings have been applied, and are staying applied. Quantitative results can be provided as feed-back and are the easiest way to compare current success to future successes.

3.1.1 General Rules for Auditing

While the need for auditing is clear, there are some general rules that will help employees keep focused on the reason for auditing. These are meant to help identify the reason for auditing a particular setting, and how to be successful with setting up an auditing process.

1. If you aren't going to look at it, don't monitor it.
   - Event logs and performance data can take up a lot of space and additional processing power. There's no point in collecting 50GB of data if no one will ever look at. Hone your processes so that all data being captured is worthy of being examined and not just stock piled.
2. Have a schedule for auditing.
   - Don't get caught in the trap of auditing once, then forgetting about it. Determine the frequency that works for your situation. A weekly audit of every computer on the network might be excessive for some companies, but just right for others.
3. Be sure to have an external audit at least once a year.
   - External audits can help not only help point out your weaknesses, but also validate your policies. Security consulting companies are also typically more current with the latest methods of attack than the average IT employee.

While some IT professionals may laugh at these rules as common sense, they are important and sometimes forgotten never the less.

3.1.2 Reacting to Variances Found

Inevitably, you will find variances to your security policy when performing an audit. It's important to have a plan on how to deal with them. Will the machine be removed from production until it can be fixed? Or will it be allowed to stay on the network until a technician can troubleshoot it? Having a plan will allow you to quickly handle each incident and continue with the audit.

In an Active Directory environment, variances are usually found due to a problem with the offending system not being configured correctly and thereby, not being able to retrieve the policy or subsequent updates. A problem with the DNS settings of a computer can have a drastic impact when using Group Policy. Using the GPUPDATE tool and the Event Logs, you can usually isolate the cause of the problem.

3.2 Security Items to Audit

With all the settings that have been configured, choosing what to audit can become a challenge. SANS-GIAC has determined that the following categories should be audited on a regular basis:

- Server Event Logs
- Server Security Settings
- Changes to the Group Policy Objects
- Spot checks of Workstation Settings
- Enterprise Wide Patch Status
- Enterprise Wide Anti-Virus Status

Enterprise wide patch status and anti-virus status are handled by the respective vendor's management tools and won't be covered in this paper.

3.2.1 Server Event Logs

The Event Log is the home to every important event on a system and the security policies in place generate a lot of logged data. In order to help with the management and processing of all that data, SANS-GIAC uses the Kiwi Syslog Daemon for all of its log management. Not only does it gather Windows event log data, but also events generated by SANS-GIAC's PIX firewalls. This data is quite large and SANS-GIAC uses 4 servers to collect all of the server logs. All of the servers at SANS-GIAC are divided based on IP address to balance the load across the syslog servers.

Syslog is setup so that it will clear the logs on the servers when the information has been archived. SANS-GIAC has also setup processing rules to alert administrators when excessive failure events occur. This helps to allow for proactive responses to incidents as they are happening. Many times, this will allow the administrators to solve a problem before it noticeably affects the production environment.

3.2.2 Server Security Settings

Once a quarter, SANS-GIAC will perform a security audit on all servers. This is to ensure that the policy has successfully been applied to all servers and that unauthorized changes aren't being made. Extra care is taken to verify that DMZ servers remain unaltered. Although SANS-GIAC is confident that appropriate security precautions have been taken, DMZ servers are at higher risk of a security incident due to their exposure to the Internet.

The administrators use the SECEDIT command line tool to script the running of the audit. This provides the administrators with a way to always compare the current settings with a known-good baseline. The log files from SECEDIT are stored in common location and then analyzed via a script to look for variances. The script then generates a report that is emailed to the administrators and used to report back to the management detailing the status of the audit.

3.2.3 Changes to the Group Policies

Also using the Kiwi Syslog Daemon, the SANS-GIAC administrators have scripted a monitor to send an email notification whenever an event is generated indicating that someone has modified the GPOs in Active Directory. This allows SANS-GIAC to track possible rogue administrators who might undo portions of the security policy. Without this tracking, it would be possible for a rogue administrator to alter or remove policies without anyone knowing. SANS-GIAC is a high security company, so changes of any kind to the security policy must be authorized and monitored.

3.2.4 Spot checks of Workstation Settings

Since there are over 2500 workstations at SANS-GIAC, it was deemed excessive to continually audit all of them. Instead, a random group of machines from each department will be audited to verify that the security settings continue to match those being applied via Group Policy. The same process and scripts which use the SECEDIT tool are used from the Server audit to keep the process and reports consistent.

3.3 Long-term Planning for Auditing

Auditing is a task that doesn't scale very well. SANS-GIAC has mainly focused on capacity planning for its Syslog servers. The load on the four current servers is acceptable, but plans for a fifth have already been made to handle future growth. The use of scripts to perform the security settings audit make that task simpler to modify since it only requires the addition of more servers to the list.

Since auditing, even with scripts, is a process which requires staff hours to complete, SANS-GIAC has formed a group to control and run the audits. With staff dedicated to the process, a consistent approach can be developed and followed and

time will always be committed to the audit. If there was a reliance on over-burdened staff, the possibility arises for an audit to be skipped due to lack of time. SANS had seen that occur in past years before its focus on security had been established. Now they are at a level where the proper staffing can be assigned to this task.

4 Conclusions

In a world where new viruses and worms can bring a company to its knees by exploiting holes less than two weeks old, security of a computer system can never be taken for granted. SANS-GIAC understands and appreciates that fact and proactively works to keep all of its practices and policies current.

In dealing with the merger, SANS-GIAC has utilized the enhanced out-of-the-box security of Windows Server 2003 to upgrade its new partner to a higher level of security. Both companies have been taking advantage of the power of Active Directory and will continue to do so not only for administration, but also for applying its security policies. The new network design will allow them to cut some of the costs of administration and services by consolidating redundant resources, while allowing them the greatest flexibility.

SANS-GIAC continues to be proactive by auditing their network to ensure that the policies are being enforced as required. They have implemented tools such as centralized anti-virus control, enterprise-wide patch management, and intrusion detection systems to maintain active control of all systems. Consistent auditing will allow them to verify that all corporate policies are still being applied and enforced.

5 References

DiNicolo, Dan. "New Active Directory Features in Windows Server 2003, Part 1", Posted 5/23/2003. http://www.serverwatch.com/tutorials/article.php/2213281, (8/21/2003)

Fossen, Jason. Track 5.2 – Windows 2000/XP Group Policy and DNS. SANS Institute. 2003

Smith, Ray – Designing a Secure Windows 2000 Infrastructure – GIAC Corporation http://www.giac.org/practical/GCWN/Ray_Smith_GCWN.pdf, (8/21/2003)

Limoncelli, Thomas. Hogan, Christine. The Practice of System and Network Administration. Addison Wesley, 2002

Microsoft-1 – Microsoft Corporation, "Establishing Interforest Authentication", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dsscc_aut_hirq.asp, (8/20/2003)

Microsoft-2 – Microsoft Corporation, "Forest Trusts", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/x_c_foresttrusts.asp, (8/20/2003)

Microsoft-3 – Microsoft Corporation, "Windows Server 2003 Security Guide", Version 1.0. Posted 8/15/2003. http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en, (8/20/2003)

NSA-XP – Bickel, R. Cook, M. Haney, J. Kerr, M. Parker, T. Parkes, H. Guide to Securing Microsoft Windows XP. National Security Agency, 2002

Software Links

ACID - http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html, (8/21/2003)

Kiwi Syslog Daemon - www.kiwisyslog.com, (8/21/2003)

McAfee ePolicy Orchestrator - http://www.nai.com/us/products/mcafee/antivirus/fileserver/epo.htm, (8/21/2003)

Microsoft Windows Home Page- http://www.microsoft.com/windows/, (8/21/2003)

Shavlik hfNetChkPro - http://www.shavlik.com/pHFNetChkPro.aspx, (8/21/2003)

Snort – http://www.snort.org/, (8/21/2003)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**