GIAC Certified Windows Security Administrator (GCWN) Practical Assignment

Enterprise Domain Design, Security Policy, and Auditing Guidelines

By Bryan Mabee
Document Revision Number 1.0
Practical Assignment version 3.2
Option 1
Submission Date 05/18/2004

Table of Contents

Figures

Abstract

Recently, SANS Co., a major online warehouse distributor in the US, and GIAC Enterprises, an online seller of Asian food products, merged to join in each others successes in the market. It was agreed that a committee of IT experts comprised of individuals from each company would be formed to handle the important role of creating an environment where resources and data can be shared between companies. This must be done in a manner where the core competencies of each company would remain secured from each other and all outside intervention. The Committee is comprised of network engineers, Active Directory platform engineers, security engineers, server and security operations associates, and IT leadership for each company. The project name is "Secured Partnership Infrastructure(SPI)." The charter of this project is to not only create an environment where the two companies can share resources and data but to take best practices from both companies and implement common administrative policies. These policies will also enable the IT Administrators to audit event logs, critical settings, and performance.

A survey of each company's physical, logical, and administrative infrastructure was done by this committee. The following sections detail the results.

SANS Co. Current Design Assumptions

Physical Network Layout Prior to Merger

SANS Co. has five sites. The Dallas site acts as the hub and the headquarters of the company. This site acts as the gateway of the company to the internet. The Dallas site's DMZ contains the public internet facing web servers.

The San Francisco, Chicago, and New York City sites are branch office tail sites that all connect to the Dallas site with two dedicated T1 circuits each. These major distribution centers handle sales pursuits, customer service, and distributing the product out to the region's stores and restaurants.

Atlanta is a new site attempting to get more business in the Southeast region of the United States. It is a remote site connected to the Dallas Headquarters site via a router-to-router persistent Windows 2000 implementation of VPN using Routing and Remote Access. The VPN connection is configured with the Layer Two Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec) and the Triple Data Encryption Standard (3DES). The Atlanta site is connected to the internet via a high-speed connection to an ISP.

Figure 1 - SANS Site Connectivity

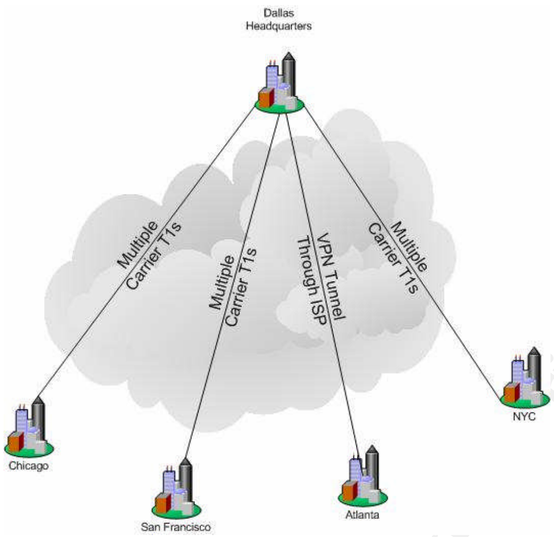
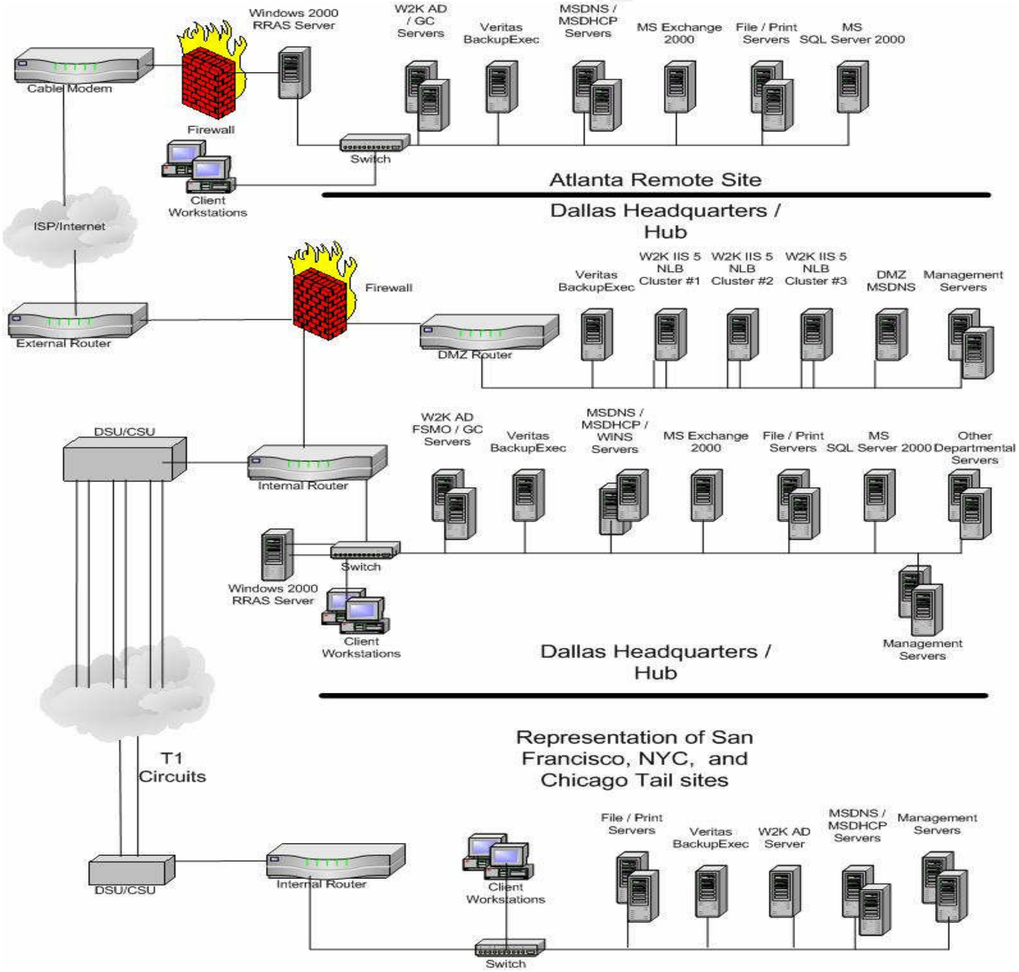


Figure 2 - SANS Network Layout



Logical Domain Design Prior to Merger

SANS Co. has standardized on Windows 2000 Active Directory. The root level domain for the SANS Co. is named SANS.COM. The child domains are NAHQ, NAEAST, NAWEST, NACTRL. All Domain Controllers are Global Catalog Servers.

The Root level domain controllers are in the Dallas Headquarters site holding the Schema Master and the Domain Naming Master FSMO roles. Dallas also has one domain controller for each of the child domains locally to provide redundancy for the sites.

The New York City site has a NAEAST domain controller holding it's domain's FSMO roles of RID master, PDC emulator, and Infrastructure daemon. Atlanta also has a local NAEAST Domain Controller.

San Francisco has a NAWEST domain controller holding it's domain's FSMO roles of RID master, PDC emulator, and Infrastructure daemon.

Chicago has a NACTRL domain controller holding it's domain's FSMO roles of RID master, PDC emulator, and Infrastructure daemon.

An Active Directory Site is created for each location. Replication is scheduled for after hours.

Administration Prior to Merger

The Services Owners for the root domain SANS.COM are located in the Dallas site. In addition to their normal user accounts in NAHQ, they have separate accounts in the SANS.COM root domain that will only be used for the additions and maintenance of the Active Directory service and configuration.

Each regional site's domain Computer resources are administered by local IT staff, On Site Support. Their local IT staff supports problems on end user computers so they would need access to the workstations.

A Central Tier 1 Customer Support group will handle the user account move, add, and change requests. This group will also handle Triage support calls of user workstation related issues and route the calls to other groups where necessary.

A Central Tier 2 Server Operations group will handle problems with the infrastructure servers and maintenance. This group will also be the recipients of problem alerts from servers.

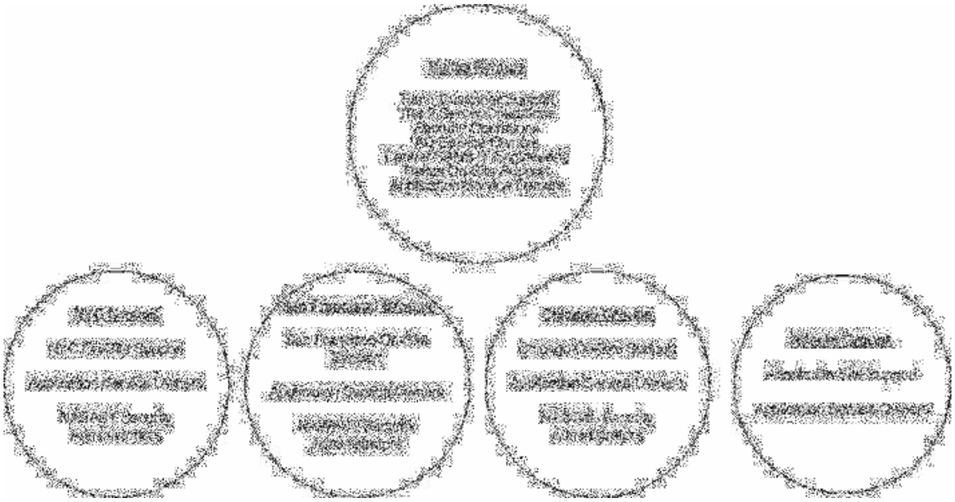
A Central Security Operations groups will be responsible for assigning group memberships. This group will receive Intrusion Detection and group membership change alerts.

A Central SANS IT Engineering group will have administrative rights over all domains but not have schema rights. This groups has rights to create and delegate Group Policy throughout the Forest.

OUs are created for functional servers in each domain (File, Print, DB, Exchange, Web, Application X, Etc.). This will allow Group Policy and data access control to be delegated to Application Service Owners responsible for their applications and services.

Each Domain will have Security Administrators responsible for their Domain's Group Policy. These are additions to the corporate policy template unique to the regional centers.

Figure 3 - SANS Administrative Groups



OU structure Prior to Merger

OUs are created to give the ability to administer resource objects separately through Group Policy and Access Control. Sub OUs are created when necessary to allow a further level of refinement of administration. Below is the OU structure created for each of the Domains.

NAHQ Domain
NAHQ Servers
File Servers, Print Servers, Database Servers, Web Servers, Domain Controllers, Exchange Servers, Management Servers
NAHQ Users
NAHQ Computers
Human Resources, Finance and legal, IT Administrators

NAWEST Domain
NAWEST Servers
File Servers, Print Servers, Database Servers, Domain Controllers
NAWEST Users
NAWEST Computers
Distribution, Sales, IT Administrators

NAEAST Domain
NAEAST Servers
File Servers, Print Servers, Database Servers, Domain Controllers
NAEAST Users

NAEAST Computers
Distribution, Sales, IT Administrators

NACTRL Domain
NACTRL Servers
File Servers, Print Servers, Database Servers, Domain Controllers
NACTRL Users
NACTRL Computers
Distribution, Sales, IT Administrators

**** Group Policies will be handled in Part 2 of this document, Auditing in Part 3.

GIAC Enterprises Current Design Assumptions

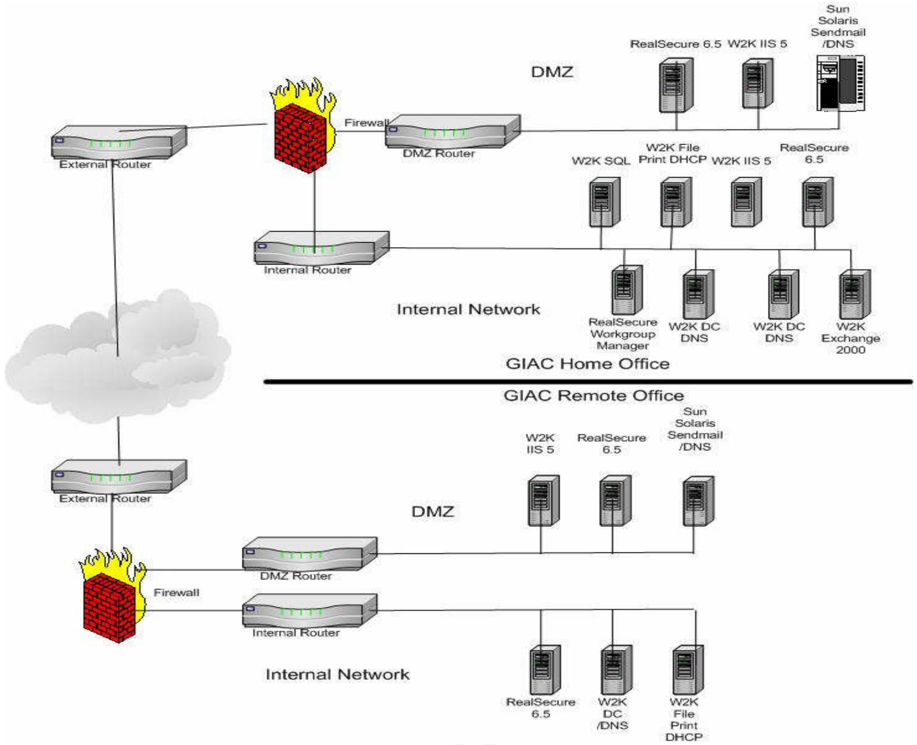
(Note: The basis of the assumptions of this section were taken from Gregory Rick's practical "GIAC Enterprises: Windows 2000 and Active Directory Design.", see References.)

Physical Network Layout Prior to Merger

GIAC Enterprise has two locations; a Remote Office and a Home Office. There is a dedicated T1 and a site to site hardware level 168-bit triple DES encryption (IPsec) VPN connecting the offices to provide fault-tolerance and load balancing. A firewall in each location protects the DMZ from the public internet by blocking all ports but the ports needed for communication. IPsec is used in the DMZ network in each location. Communication between the SQL Server in the Home Office Internal network and the IIS 5 Server is restricted to each others IP Addresses only and uses a private key from VeriSign. The firewall in each location blocks all IP Addresses that are known to be a threat.

GIAC Enterprise has different internal and external DNS. The internal DNS is an Active Directory Integrated DDNS. The external DMZ uses the Solaris implementation of DNS. Time Synchronization (SMTP) uses the US Naval Observatory for it's source to update the Domain controllers, the Domain controllers update all clients and servers in the Domain.

Figure 4 - GIAC Network Layout



Logical Domain Design Prior to Merger

The GIAC Enterprise Windows 2000 Active Directory is installed in Native Mode. There is one Forest with one Domain (Prophesy.com). There are two Active Directory Sites configured with default costs. There is a two-way trust between Prophesy.com and a parallel NT 4.0 Domain. Replication settings are configured with default replication settings.

Administration Prior to Merger

GIAC Enterprise is administered by an IT Staff at each location for the administration of computer and server objects in that location. An operations group handles client and server related support issues and administration in the Remote Office and a separate operations group handles client and server related support issues and administration in the Home Office. There is also an operations group that handles network related issues and administration that is centrally located. The company has an engineering group that handles networking projects and an engineering group that handles client and server projects that are centrally located at the Home Office.

The engineering groups have an isolated lab that is setup as a replica of the production network and logical environment on a smaller scale.

The Server and Client Engineering groups and the server and client operations groups are all Domain Administrators with the exception of one senior server engineer who is an Enterprise Administrator.

Domain Administrators and Enterprise Administrators have full control of group policies.

Global groups are used for organizing users. Domain local groups provide access to resources.

OU Structure Prior to Merger

GIAC Enterprise uses Organizational Units (OUs) in Active Directory to manage their servers, client workstations, and user accounts. OUs allow the IT staff to group objects together and delegate control of these objects to individuals responsible for the administration of those objects.

The Home Office IT staff is responsible for the administration of the printer and client workstation objects in the "Home Office" OU. The Remote Office IT staff is responsible for the administration of the printer and client workstation objects in the "Remote Office" OU. Child OUs under the "Home Office" OU and the "Remote Office" OU include "Computers", "Printers", and "Admins".

All user accounts are centrally administered in a root OU called "Domain Users". This OU has child OUs for each department. The child OUs under "Domain Users" are "IT Administrators", "Research and Development", "Sales and Marketing", and "Finance and Human Resources". Control over these OUs are delegates to administrators for those departments. All Administrative accounts will be placed in the "IT Administrators" OU.

The "Enterprise Servers" OU is administered by the centralized IT staff. Some examples of these servers are Web Servers, Database Servers and File and Print Servers.

Domain Controllers are in a default "Domain Controllers" OU.

**** Group Policies will be handled in Part 2 of this document, Auditing in Part 3.

GIAC Enterprise and SANS Co. Domain Trust Relationships

All major design changes should start with detailed designs using industry best practices and thorough lab testing. A major part of a cross-forest domain trust is ensuring security of both networks and Active Directories. Other equally important aspects are ensuring low cost management and seamless usability. This section will address the logistics of the connections between the GIAC's Prophesy.com Forest and the SANS.com Forest, as well as the testing and security assurances surrounding the connections.

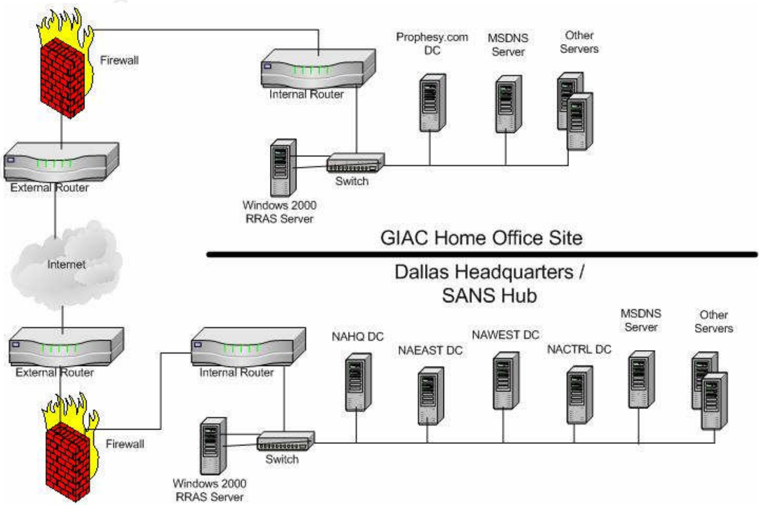
The goal of establishing the external trusts is to enable users to access resources in domains between each company's forests and enable IT Administrators to delegate control to IT Administrators in the other company's forests.

Network Configuration

The SANS Dallas Site is connected to the Home Office site in GIAC via a router-to-router persistent Windows 2000 implementation of VPN using Routing and Remote Access. The VPN connection is configured with the Layer Two Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec) and the Triple Data Encryption Standard (3DES).

As the reorganization is taking place to centralize administration and leverage across companies, the traffic over this connection will be low. If at a later date the bandwidth cannot accommodate the traffic, a new connection with higher bandwidth will be established.

Figure 5 - SANS to GIAC Connectivity



DNS Configuration

In order to create a trust and resource sharing between the companies, there needs to be name resolution. To do this, GIAC's DNS is configured to have a "Standard secondary" DNS zone of each of the SANS child Domains (NAHQ.SANS.COM, NAEAST.SANS.COM, NAWEST.SANS.COM, NACTRL.SANS.COM).

SANS Co. DNS is configured to have a "Standard secondary" DNS zone of Prophesy.com.

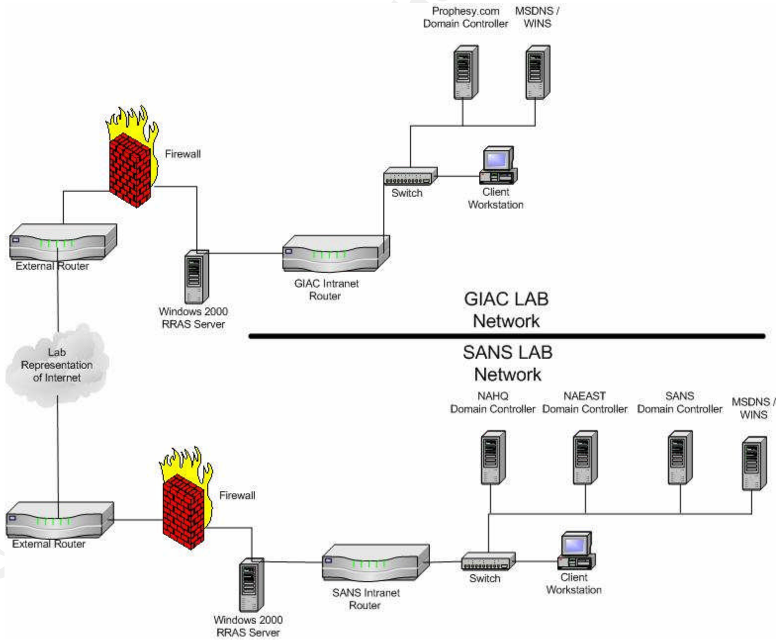
Lab Testing Approach

The lab environment consists of separate representations of the GIAC and the SANS Intranet with the following:

- A test workstation VLAN containing a workstation to test user experience.
- A test server VLAN containing an environment that would contain DNS, WINS, and the affected Active Directory servers.

The Intranets connect through a firewall via VPN across a simulated internet.

Figure 6 - Testing Environment



Using GIAC's standard server builds, two servers are built in the GIAC Servers VLAN of the GIAC lab. One Workstation is built in the Workstation VLAN of the GIAC lab using the company's standard Workstation build. A share is created on the workstation.

The production DNS zones are created on the DNS / WINS server in the GIAC lab. WINS is installed.

IPs are assigned to the GIAC's Prophesy.com Domain Controller and the Workstation and hostnames are registered in the DNS server in the appropriate Zones.

The production Domain structure for GIAC's Prophesy.com, OUs, and GPOs are created on the Domain Controller in the GIAC lab. Production Functional accounts and groups are created.

The workstation and the DNS/WINS server are brought into the GIAC's Prophesy.com Domain. A test account is created in the GIAC's Prophesy.com Domain.

Using SAN's standard server builds, four servers are built in the SANS Servers VLAN of the SANS lab. One Workstation is built in the Workstation VLAN of the SANS lab using the company's standard Workstation build.

The production DNS zones are created on the DNS / WINS server in the SANS lab. WINS is installed.

IPs are assigned to the SANS.COM, NAHQ.SANS.COM, and NAEAST.SANS.COM Domain Controllers. The Workstation and hostnames are registered in the DNS server in the appropriate Zones.

The production Domain structure for SANS.COM, NAHQ.SANS.COM, and NAEAST.SANS.COM, OUs in each, and GPOs in each are created on the Domain Controllers in the GIAC lab.

The workstation is brought into the NAHQ Domain and the DNS/WINS server is brought into the SANS Domain. A share is created on the workstation. A test account is created in the NAHQ Domain and a test account is created in the NAEAST Domain.

A test account is created in NAHQ.SANS.COM. A test account is created in NAHQ.EAST.COM.

The DNS servers in each network are configured with the Standard secondary DNS zones of each other's Domains.

An External Trust is created connecting Prophesy.com and NAHQ.SANS.COM. An External Trust is created connecting Prophesy.com and NAEAST.SANS.COM.

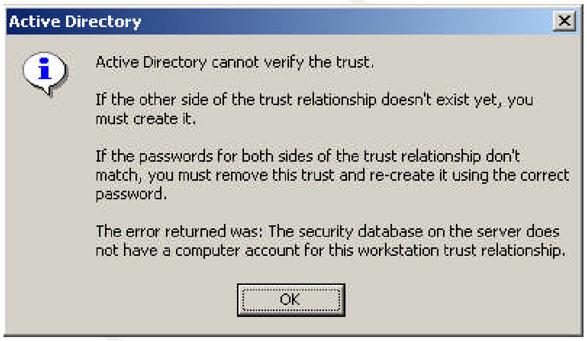
To test the trust, the following tasks were performed:

- Verify the Domain List contains all trusted domains when users login to workstations that are joined into each Domain.
- Users whose Workstation is joined into Prophesy.com can give permissions to users in NAHQ and NAEAST but not SANS.COM. Those users can access the shares. Likewise, Users whose Workstation is joined into NAHQ and NAEAST can give permissions to users in Prophesy. Those users can also access the shares.
- In Active Directory Users and Computer on the Prophesy.com domain controller, create a group, add a user from NAHQ and NAEAST to that group.
- In Active Directory Users and Computer on the Prophesy.com domain controller, create a group, add a user from NAHQ and NAEAST to that group.
- In Active Directory Users and Computer on the Prophesy.com domain controller, "Delegate Control" of the "IT Administrators" OU to the "Security Operations" group in NAHQ.

  - o Verify that a member of NAHQ\"Security Operations" group can modify group policies and manage the objects in that OU.

Trust Creation Implementation

- A member of Enterprise Admins in NAHQ.SANS.COM will perform this procedure. He will also have a separate account, created for him by the IT Administrators in GIAC that he will use. That account is a member of the Enterprise Admins group in prophesy.com.
- On a NAHQ.SANS.COM Domain Controller, logon with the user account in the NAHQ.SANS.COM Enterprise Admins group.
- Open "Active Directory Domains and Trusts".
- Right-click on NAHQ.SANS.COM and choose Properties.
- Click on the "Trusts" tab.
- Click on the [Add] button next to "Domains trusted by this domain".
- Enter Prophesy.com.
- Enter a complex password in the password box and the confirm password box.
- You will receive the following message, click [OK].



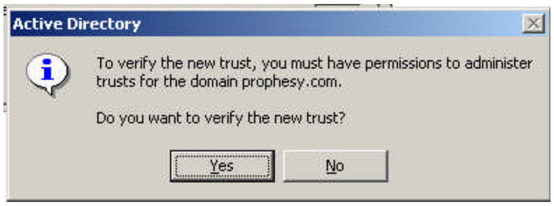
Active Directory cannot verify the trust.

If the other side of the trust relationship doesn't exist yet, you must create it.

If the passwords for both sides of the trust relationship don't match, you must remove this trust and re-create it using the correct password.

The error returned was: The security database on the server does not have a computer account for this workstation trust relationship.

- Click on the [Add] button next to "Domains that trust this domain".
- Enter Prophesy.com.
- Enter a complex password in the password box and the confirm password box.
- You will be asked the following, Click [No].



To verify the new trust, you must have permissions to administer trusts for the domain prophesy.com.

Do you want to verify the new trust?

- Click on [OK].
- On a Prophesy.com Domain Controller, logon with the user account in the Prophesy.com Enterprise Admins group.
- Open "Active Directory Domains and Trusts".
- Right-click on Prophesy.com and choose Properties.

- Click on the “Trusts” tab.
- Click on the [Add] button next to “Domains trusted by this domain”.
- Enter nahq.
- Enter a complex password in the password box and the confirm password box.
- Click [OK].
- Click on the [Add] button next to “Domains that trust this domain”.
- Enter nahq.
- Enter a complex password in the password box and the confirm password box.
- You will be asked to verify the new trust, Click [No].
- Click on [OK].

Once the trust is established, the tests performed in the lab are now performed in production to verify the trust.

Administration Consolidation

The newly created trust allows IT administration between the two companies to be consolidated. The establishment of the trusts between the domains allows administrators to delegate control over OUs and other domain administration tasks. The OU structure for both company’s domains will be modified to look similar.

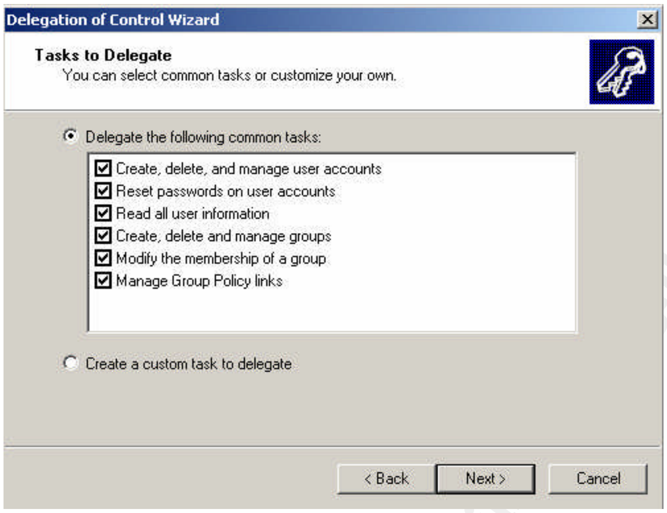
An OU is created in each domain entitled “Privileged Accounts”. This OU will contain the service accounts, Built-in administrative accounts and groups (Administrator, Domain Admins, Guest, Enterprise Admins, Etc.), and the following groups for administration:

Tier 1 Customer Support
Tier 2 Server Operations
Security Operations
<Site> On-Site Support
AD Service Owners
Central SANS IT Engineering
<Domain> Security Administrators

The following Domain Local groups are created for “User Rights Assignment. Others will be created in the future as administration becomes more granular:

ServerSysAccess-L
WksSysAccess-L
DCSysAccess-L

The “Privileged Accounts” OU will be configured to “Delegate Control” to “Domain Admins” for that domain and “<Domain> Security Administrators”. Most of the security administrators will be members of the “NAHQ Security Administrators” but there will be a few in other domain group “<domain> Security Administrators” as well. The Tasks to delegate are all of the common tasks listed.



Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

● Delegate the following common tasks:

- ☑ Create, delete, and manage user accounts
- ☑ Reset passwords on user accounts
- ☑ Read all user information
- ☑ Create, delete and manage groups
- ☑ Modify the membership of a group
- ☑ Manage Group Policy links

○ Create a custom task to delegate

*** Role Based Security will be handled later in the Group Policy section.

The “Tier 1 Customer Support” group is a group in the NAHQ domain that handles all computer related helpdesk support calls for both companies for end-user problems in all domains. This group has access to all user computers in all domains from both companies. To accomplish this, it is added to the WksSysAccess-L Domain Local group.

The “Tier 2 Server Operations” group is a group in the NAHQ domain that handles all server related issues and has role based administrative access to all servers in the domain. To accomplish this, it is added to the ServerSysAccess-L Domain Local group.

The “Security Operations” group is delegated control over the “<domain> Users” OUs. Their tasks include only the following:

- “Create, delete, and manage user accounts”
- “Reset passwords on user accounts”
- “Read all user information”
- “Create, delete and manage groups”
- “Modify membership of a group”

The “<site> On-Site Support” group has rights to certain tasks in the group policy for the computers in the “<domain> Computers” OU. They are the local System Administrators. To accomplish this, it is added to the WksSysAccess-L Domain Local group.

The “AD Service Owners” are given the rights to manage group policy in the domains. One individual from the company is put in all domain’s “AD Service Owners” group in addition to one person from that domain.

For example:

NAHQ “AD Service Owners” contains – NAHQ\bmabee
Prophesy “AD Service Owners” contains - NAHQ\bmabee, prophesy\mjones
NAEAST “AD Service Owners” contains - NAHQ\bmabee, NAEAST\kwilliams

In addition to the above rights, this group is added to the ServerSysAccess-L Domain Local group and the DCSysAccess-L Domain Local group.

The “Central SANS IT Engineering” group is a group in the NAHQ domain that handles all server related issues escalated from “Tier 2 Server Operations” and has role based administrative access to all servers in the domain. To accomplish this, it is added to the ServerSysAccess-L Domain Local group and added to the DCSysAccess-L Domain Local group.

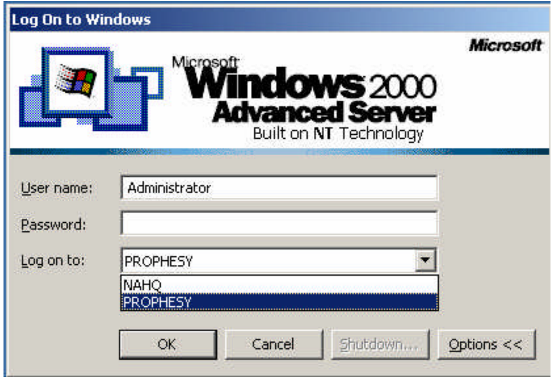
The “<Domain> Security Administrators” is the only group besides the domain build-in administrative groups and “AD Service Owners” that control the groups, account, and Group Policy for the “Privileged Accounts” OU. They can perform the following tasks.

- “Create, delete, and manage user accounts”
- “Reset passwords on user accounts”
- “Read all user information”
- “Create, delete and manage groups”
- “Modify membership of a group”

In addition to the above rights, this group is added to the ServerSysAccess-L Domain Local group and the DCSysAccess-L Domain Local group.

User Experience

- As you add trusts, the domains will show up in the “Log on to:” domain list when you login to a system in one of the trusted domains.



Log On to Windows

User name: Administrator
Password:
Log on to: PROPHESY
NAHQ
PROPHESY

- Users can give users from trusted domains rights to resources.
- If given the right to do so, users can logon to workstations joined to trusted domains.
- Users can share files.

- Data from backend databases can be connected between the companies and permissions set in active directory allowing real time information sharing for transactions over the web. The Database Administrators can be consolidated into one group allowing collaboration and leveraging.
- Administrators can Delegate Control of OUs.

Managing Systems with Group Policy

Active Directory Group Policy allows an organization to granularly apply security and other configuration settings to objects in the domains. These settings can happen at the OU, site, and/or the Domain level. This allows administration of these object to be delegated to multiple individuals or groups.

GIAC's Prophesy.com Group Policies Prior to Merger

GIAC Enterprise implemented group policies using baseline templates from the National Security Agency (NSA). The security template files downloaded from the NSA web site were the following:

- w2k_domain_policy.inf – This file was modified and imported as the Prophesy.com Group Policy. The message title and text for users attempting to log on policy, the rename Administrator account policy, and the rename Guest account policy were modified in the template to reflect the company's defined standard.
- w2k_workstation.inf – This file was modified and imported as the Group Policy for the "Computers" child OU of both the "Home Office" OU and the "Remote Office" OU.
- w2k_server.inf - This file was modified and imported as the Group Policy for the "Enterprise Servers" OU. This file was also used on the DMZ Servers as a local policy individually considering they are not part of the Domain.
- w2k_dc.inf - This file was modified and imported as the Group Policy for the "Domain Controllers" OU.

The servers in the DMZ had the w2k_server.inf template applied to them manually through the "Local Security Policy". The Web Servers in the DMZ were also locked down using the modified Hisecweb.inf template (Microsoft Knowledgebase Article Q316347).

Logon Scripts are applied to the Group Policy Object of the "Domain Users" OU. If a department needs other Logon Scripts to run, it is applied to the appropriate child OU under "Domain Users".

GIAC Enterprises distributes software using the "Software Installation" Publish or Assign Group Policy Object on the following OUs:

- "Computers" OU under "Remote Office" OU
- "Computers" OU under "Home Office" OU
- "Enterprise Servers" OU
- "Domain Controllers" OU

SANS Group Policies Prior to Merger

SANS Co. implemented Group Policies using the templates that came with Windows 2000 Server. These templates, found under c:\Winnt\Security\templates, are the following:

- securedc.inf – This was modified for specific domain needs and imported in the Domain Controllers OU in each domain.
- Securews.inf – This was modified and added to each of the computer and server OUs in each domain except for the Domain Controllers OU (File, Print, Web, Database, Etc.)

Each Domain modified account policies individually at the domain level.

Hisecdc.inf and hisecws.inf were not used because they require IPSec network communication which requires digital signatures. A CA would need to be present.

Standard Set of Group Policy Templates for GIAC and SANS Users, Servers, and Workstations

A policy is created by the "Secured Partnership Infrastructure(SPI)" Committee to apply one standard set of templates across all systems in each company. Both company's templates were reviewed. The NSA sample templates, "Windows 2000 Security Hardening Guide" sample templates, and the templates in \Winnt\Security\Templates were all used in the decision making for creating a standard set.

The Role Based Security section of this document deals with administration through "User Rights Assignment" modifications.

The following (8) standard set of templates were created.

1. "SPI Baseline Policy.INF"

Since the domain can only have one set of account policies, the advantages and disadvantages of the policies were weighed and the following were decided upon based on user experience and security requirements. These settings are saved into a template called "SPI Baseline Policy.INF that can be applied to the domains and the local policies of the standard automated server, laptop, and workstation builds. The Hardening Guide "W2KHG-baseline.inf" template settings were used with the following exceptions:

Password Policy

Maximum password age – 90 days, this setting aligns with the NSA's sample template setting. This was chosen by the SPI committee to reduce the end-user impact. Approximately 3 months was suitable for the password age.

Minimum password age – 1 day, this setting aligns with the NSA's sample template setting. One day is a sufficient amount of time to discourage users from cycling through 24 passwords to get to the desired one.

Minimum password length – 14 characters, the Minimum password length setting is longer than both the hardening guide and the NSA recommended size because the committee also chose to disable the complexity requirement. It was

decided that length was more effective than complexity when it came to hacking tools and it would reduce helpdesk calls for password resets and confusion over the complexity rules. The users are trained to use passphrases that are unique.
Password must meet complexity requirements – Disabled

Account Lockout Policy – The Account lockout duration, Account lockout threshold, and the Reset account lockout counter settings will all not be set because of the impact on service accounts (denial of service attacks) and increased helpdesk calls that it would create. The security risk is minimized by the password policies.
Kerberos Policy – No change.
Audit policy – Policies from the NSA template "w2k_server.inf" were used with the exception of "Audit directory service access". Auditing will be discussed in more detail later in this document.

Audit account logon events - Success, Failure
Audit account management - Success, Failure
Audit directory service access - 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

Security Options – The interactive logon text and title are changed.
Interactive logon: Message title for users attempting to log on -
"WARNING! Use of this system is restricted and monitored."
Interactive logon: Message text for users attempting to log on -
"Use of this system is restricted to authorized users. User activity is monitored and recorded by system personnel. Anyone using the system expressly consents to such monitoring and recording. BE ADVISED: If possible criminal activity is detected, system records along with certain personal information may be provided to law enforcement officials."

To create this template the following steps were performed:

- Rename the Hardening Guide "W2KHG-baseline.inf" template to "SPI Baseline Policy.INF" and copy it to c:\winnt\security\templates directory on a Windows 2000 test server.
- In the "Security Templates" MMC snap-in, expand "C:\WINNT\Security\Templates".
- Expand "SPI Baseline Policy.INF" and make the above modifications.
- The modified template is then saved.

2. SPI Secured Laptops.INF
The Windows 2000 Hardening Guide template "W2KHG-MemberLaptop.inf" was leveraged to create this template. Some portable computer specific concerns are

handled in this template. To create this template, rename the Hardening Guide "W2KHG-MemberLaptop.inf" template to "SPI Secured Laptops.INF" and copy it to c:\winnt\security\templates directory on a Windows 2000 test server.

3. SPI Secured Workstations.INF
   The Windows 2000 Hardening Guide template "W2KHG-MemberWKS.inf" was leveraged to create this template. Some workstation computer specific concerns are handled in this template. To create this template, rename the Hardening Guide "W2KHG-MemberWKS.inf" template to "SPI Secured Workstations.INF" and copy it to c:\winnt\security\templates directory on a Windows 2000 test server.
4. SPI Secured Domain Controllers.INF
   The NSA template "w2kdc.inf" was leveraged to create this template. Some Domain Controller specific concerns are handled in this template. Some of those concerns include defining only certain groups to have rights of certain tasks in "User Rights Assignment". To create this template, rename the Hardening Guide "w2kdc.inf" template to "SPI Secured Domain Controllers.INF" and copy it to c:\winnt\security\templates directory on a Windows 2000 test server.
5. SPI Secured Servers.INF
   The NSA template "w2k_server.inf" was leveraged to create this template. Some server specific concerns are handled in this template. Server specific concerns are addressed in this template. To create this template, rename the Hardening Guide "w2k_server.inf" template to "SPI Secured Servers.INF" and copy it to c:\winnt\security\templates directory on a Windows 2000 test server.
6. SPI Secured DMZ Servers.INF
   The Windows 2000 Hardening Guide template "W2KHG-StandaloneServer.inf" was leveraged to create this template. Some server specific concerns are handled in this template. To create this template, rename the Hardening Guide "W2KHG-StandaloneServer.inf" template to "SPI Secured DMZ Servers.INF" and copy it to c:\winnt\security\templates directory on a Windows 2000 test server. Changes to the template are identified below:
   - Local Policies | Security Options | Interactive logon: Message title for users attempting to log on - "WARNING! Use of this system is restricted and monitored."
   - Local Policies | Security Options | Interactive logon: Message text for users attempting to log on - "Use of this system is restricted to authorized users. User activity is monitored and recorded by system personnel. Anyone using the system expressly consents to such monitoring and recording. BE ADVISED: If possible criminal activity is detected, system records along with certain personal information may be provided to law enforcement officials."
7. SPI Secured DMZ IIS 5 Servers.INF
   "hisecweb.inf" included with Windows 2000, was used for creating the DMZ IIS server template. To create this template, rename the Hardening Guide "hisecweb.inf" template to "SPI Secured DMZ IIS 5 Servers.INF" and copy it to

c:\winnt\security\templates directory on a Windows 2000 test server. Changes to the template are identified below:

- Removed the “everyone” group from access to the “c:\inetpub\mailroot” and the “c:\inetpub\ftproot” directories under file system.
- Local Policies | Security Options | Accounts: Guest account status – Disabled
- Local Policies | Security Options | Accounts: Rename administrator account – spiadmin
- Local Policies | Security Options | Accounts: Rename guest account – spiguest
- Local Policies | Security Options | Interactive logon: Message title for users attempting to log on - “WARNING! Use of this system is restricted and monitored.”
- Local Policies | Security Options | Interactive logon: Message text for users attempting to log on - “Use of this system is restricted to authorized users. User activity is monitored and recorded by system personnel. Anyone using the system expressly consents to such monitoring and recording. BE ADVISED: If possible criminal activity is detected, system records along with certain personal information may be provided to law enforcement officials.”

8. SPI Secured IIS 5 Servers.INF
“hisecweb.inf” included with Windows 2000, was used for creating the Secured IIS 5 server template. To create this template, rename the Hardening Guide “hisecweb.inf” template to “SPI Secured IIS 5 Servers.INF” and copy it to c:\winnt\security\templates directory on a Windows 2000 test server.

Applying Security Templates to Stand-alone Servers

Once the template is created, it will be used to secure the servers, laptops, and workstations based on their role during the automated install of the standard builds. The “SPI Baseline Policy.INF” is applied first and then the role based security template is applied. In addition to having the security templates in the automated builds, the existing servers, laptops, and workstations will be retrofitted with these templates. This can be done through login scripts, software distribution, or manually.

To apply these templates, perform the following:

- Copy c:\WINNT\Security\Database\secedit.sdb to c:\WINNT\Security\Database\copy.sdb
- Run “*C:\winnt\system32\secedit.exe /configure /db* c:\WINNT\security\Database\copy.sdb /CFG “SPI Baseline Policy.INF”
- Run “*C:\winnt\system32\secedit.exe /configure /db* c:\WINNT\security\Database\copy.sdb /CFG <role security template>.INF

Lockdown of DMZ IIS5 Servers

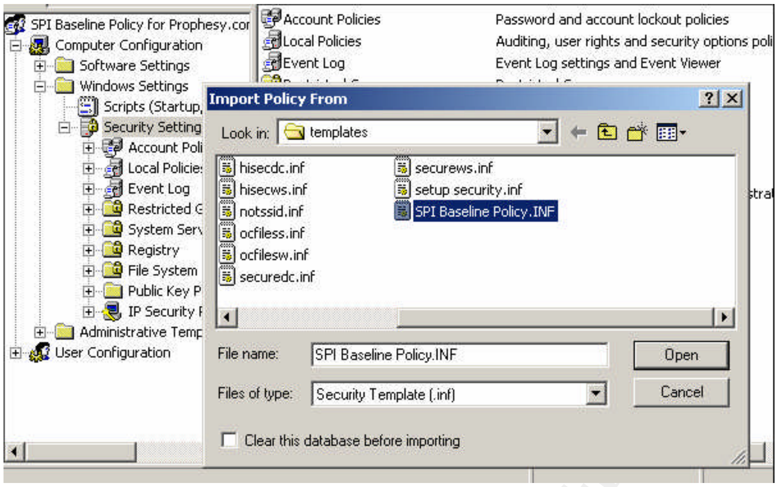
In addition to applying the “SPI Secured DMZ IIS 5 Servers.INF” (modified hisecweb.inf) security template to the server, the following steps were taken to lockdown the DMZ web servers. The “From Blueprint to Fortress: A Guide to Securing IIS 5.0” whitepaper was referenced for these settings.

- Install all current security hotfixes related to IIS and the Operating System.
- Delete the contents of the web samples directories
  - c:\inetpub\iissamples
  - c:\winnt\help\iishelp
  - c:\program files\common files\system\msadc
- Modify the following registry value to prevent SYN Flood Attacks.
  - HKLM\System\CurrentControlSet\Services\Tcpip\Parameters[SynAttackProtect]=2
- Delete Web Printing
  - HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting
- Remove Administrative shares
  - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters[AutoShareServer]=0
- Restrict NULL Session Access
  - HKLM\System\CurrentControlSet\Services\LanManServer\Parameters[RestrictNullSessAccess]=1

Applying Security Templates to the Domains

Prophesy.com, SANS.COM, NAHQ, NAWEST, NAEAST, NACTRL

- Perform the following steps to the Prophesy.com, SANS.COM, NAHQ.COM, NAWEST.COM, NAEAST.COM, and NACTRL.COM on the “PDC Emulator” Domain Controllers for each Domain.
  - Copy “SPI Baseline Policy.INF” to the c:\WINNT\Security\Templates directory.
  - Open “Active Directory Users and Computers”.
  - Right-click on the domain name and choose “Properties”.
  - Click on the “Group Policy” tab.
  - Right-click on “Default Domain Policy” and choose “Rename”.
  - Change the name to the name to “SPI Baseline Policy for <domain name>” (e.g. “SPI Baseline Policy for prophesy.com”).
  - Click on the [Edit] button.
  - Expand “Computer Configuration” | “Windows Settings” | “Security Settings”.
  - Right-click on “Security Settings” and choose “Import Policy ...”.
  - Choose “SPI Baseline Policy.INF” and click on [Open].



Look in: templates

File name: SPI Baseline Policy.INF

Files of type: Security Template (.inf)

☐ Clear this database before importing

- o Close “Group Policy” and click on [OK].

Applying Security Templates to OUs

*** See Role Based Security section for “User Rights Assignment” modifications for details on how administration is accomplished through Group Policy.

- For the “NAHQ Servers”, “NAEAST Servers”, “NAWEST Servers”, and “NACTRL Servers” OUs in SANS and the “Enterprise Servers” OU in Prophesy.com, the “SPI Secured Servers.INF” security template is applied as the group policy for these OUs. Perform the following steps to the OUs on the “PDC Emulator” Domain Controllers for each of their respective Domains.
  - o Copy “SPI Secured Servers.INF” to the c:\WINNT\Security\Templates directory.
  - o Open “Active Directory Users and Computers”.
  - o Right-click on the OU name and choose “Properties”.
  - o Click on the “Group Policy” tab.
  - o Click on the [New] button.
  - o Change the name to “SPI Server Policy for <OU name>” (e.g. “SPI Server Policy for NAHQ Servers”).
  - o Click on the [Edit] button.
  - o Expand “Computer Configuration” | “Windows Settings” | “Security Settings”.
  - o Right-click on “Security Settings” and choose “Import Policy ...”.
  - o Choose “SPI Secured Servers.INF” and click on [Open].
  - o Close “Group Policy” and click on [OK].
- Perform the above steps for the “Domain Controllers” OUs in SANS.COM, NAEAST.COM, NAHQ.COM, NAWEST.COM, NACTRL.COM, and Prophest.com using the “SPI Secured Domain Controllers.INF”.

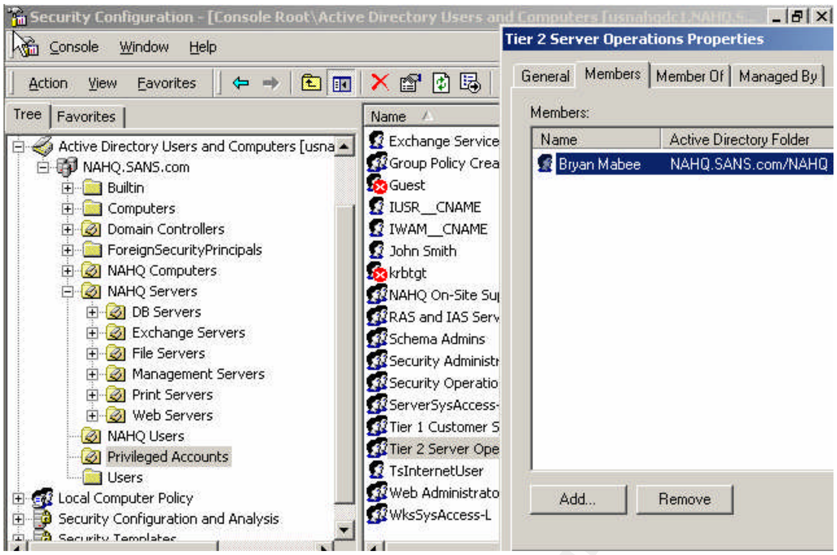
- Perform the above steps for the “Computers” OU under the “Home Office” OU in Prophesy.com using the “SPI Secured Workstations.INF”.
- Perform the above steps for the “Computers” OU under the “Remote Office” OU in Prophesy.com using the “SPI Secured Workstations.INF”.
- Perform the above steps for the “<Domain> Computers” OU in NAEAST.COM, NAHQ.COM, NAWEST.COM, NACTRL.COM using the “SPI Secured Workstations.INF”.
- Perform the above steps for the “Web Servers” OU in NAEAST.COM, NAHQ.COM, NAWEST.COM, NACTRL.COM using the “SPI Secured IIS 5 Servers.INF”. The “Web Servers” OU is under the “<domain> Servers” OU so the Group Policy of “<domain> Servers” OU will be applied first then the Group Policy applied to the “Web Servers” OU will be applied, overwriting common settings between the two.
- The other server type sub OUs (i.e. File Servers, Print Servers, Database Servers, Web Servers, Domain Controllers, Exchange Servers, Management Servers, etc.) and Computer OUS (i.e. Computers under the Prophesy.com Home Office and Remote Office OUs, etc.), can be used to define management and security options through Group Policy like logon scripts, software distribution. Control can be delegated to IT Administrators responsible for that area of business.

Role Based Security

Once the Security Templates have been applied, role based security is applied to the “<domain> Servers” OU Group Policy, the “Domain Controllers” OU Group Policy, and the “<domain> Computers” OU Group Policy.

The ServerSysAccess-L, WksSysAccess-L, and DCSysAccess-L Task Domain Local groups were used to assign rights to and Global groups are added to those Domain Local groups. Users are assigned to the Global groups.

Figure 7 – OUs, Groups, Roles, an Memberships



Name	Active Directory Folder
Bryan Mabee	NAHQ.SANS.com/NAHQ

The “User Rights Assignment” Group Policy for the “<domain> Servers” OU is modified with the following changes:

Policy	Computer Setting
Access this computer from the network	Users,NAHQ\ServerSysAccess-L,Administrators
Back up files and directories	NAHQ\ServerSysAccess-L,Administrators
Change the system time	NAHQ\ServerSysAccess-L,Administrators
Create a pagefile	NAHQ\ServerSysAccess-L,Administrators
Force shutdown from a remote system	NAHQ\ServerSysAccess-L,Administrators
Increase quotas	NAHQ\ServerSysAccess-L,Administrators
Increase scheduling priority	NAHQ\ServerSysAccess-L,Administrators
Load and unload device drivers	NAHQ\ServerSysAccess-L,Administrators
Log on locally	NAHQ\ServerSysAccess-L,Administrators
Manage auditing and security log	NAHQ\ServerSysAccess-L,Administrators
Modify firmware environment values	NAHQ\ServerSysAccess-L,Administrators
Profile single process	NAHQ\ServerSysAccess-L,Administrators
Profile system performance	NAHQ\ServerSysAccess-L,Administrators

Restore files and directories	NAHQ\ServerSysAccess-L,Administrators
Shut down the system	NAHQ\ServerSysAccess-L,Administrators
Take ownership of files or other objects	NAHQ\ServerSysAccess-L,Administrators

The “User Rights Assignment” Group Policy for the “Domain Controllers” OU is modified with the following changes:

Policy	Computer Setting
Access this computer from the network	NAHQ\DCSysAccess-L,ENTERPRISE DOMAIN CONTROLLERS,Authenticated Users,Administrators
Back up files and directories	NAHQ\DCSysAccess-L,Administrators
Bypass traverse checking	Authenticated Users
Change the system time	NAHQ\DCSysAccess-L,Administrators
Create a pagefile	NAHQ\DCSysAccess-L,Administrators
Enable computer and user accounts to be trusted for delegation	NAHQ\DCSysAccess-L,Administrators
Force shutdown from a remote system	NAHQ\DCSysAccess-L,Administrators
Increase quotas	NAHQ\DCSysAccess-L,Administrators
Increase scheduling priority	NAHQ\DCSysAccess-L,Administrators
Load and unload device drivers	NAHQ\DCSysAccess-L,Administrators
Log on locally	NAHQ\DCSysAccess-L,Administrators
Manage auditing and security log	NAHQ\DCSysAccess-L,Administrators
Modify firmware environment values	NAHQ\DCSysAccess-L,Administrators
Profile single process	NAHQ\DCSysAccess-L,Administrators
Profile system performance	NAHQ\DCSysAccess-L,Administrators
Restore files and directories	NAHQ\DCSysAccess-L,Administrators
Shut down the system	NAHQ\DCSysAccess-L,Administrators
Take ownership of files or other objects	NAHQ\DCSysAccess-L,Administrators

The “User Rights Assignment” Group Policy for the “<domain> Computers” OU is modified with the following changes:

Policy	Computer Setting
Access this computer from the network	Users, NAHQ\WksSysAccess-L,Administrators
Back up files and directories	NAHQ\WksSysAccess-L,Administrators
Change the system time	NAHQ\WksSysAccess-L,Administrators
Create a pagefile	NAHQ\WksSysAccess-L,Administrators
Force shutdown from a remote system	NAHQ\WksSysAccess-L,Administrators
Increase quotas	NAHQ\WksSysAccess-L,Administrators
Increase scheduling priority	NAHQ\WksSysAccess-L,Administrators
Load and unload device drivers	NAHQ\WksSysAccess-L,Administrators
Log on locally	NAHQ\WksSysAccess-L,Administrators
Manage auditing and security log	NAHQ\WksSysAccess-L,Administrators

Modify firmware environment values	NAHQ\WksSysAccess-L,Administrators
Profile single process	NAHQ\WksSysAccess-L,Administrators
Profile system performance	NAHQ\WksSysAccess-L,Administrators
Restore files and directories	NAHQ\WksSysAccess-L,Administrators
Shut down the system	NAHQ\WksSysAccess-L,Administrators
Take ownership of files or other objects	NAHQ\WksSysAccess-L,Administrators

These settings will be added to the respective standard set of Group Policy templates ("SPI <dc, wks, or server>.inf").

Policy Maintenance

Group Policy, once applied, tattoos the system with the settings but Active Directory refreshes these settings every 90 minutes. For those systems that are not in the domain, a script is created which runs locally every 45 minutes using the security template defined for that system (i.e. "SPI Secured DMZ IIS 5 Servers.INF", SPI Secured DMZ Servers.INF, etc). This script includes the following two commands:

- **secedit /configure /DB** <local database location> **/CFG** <location of security template created of that system type> **/overwrite /log** <log file location> **/quiet**
- **secedit /refreshpolicy machine_policy /enforce**

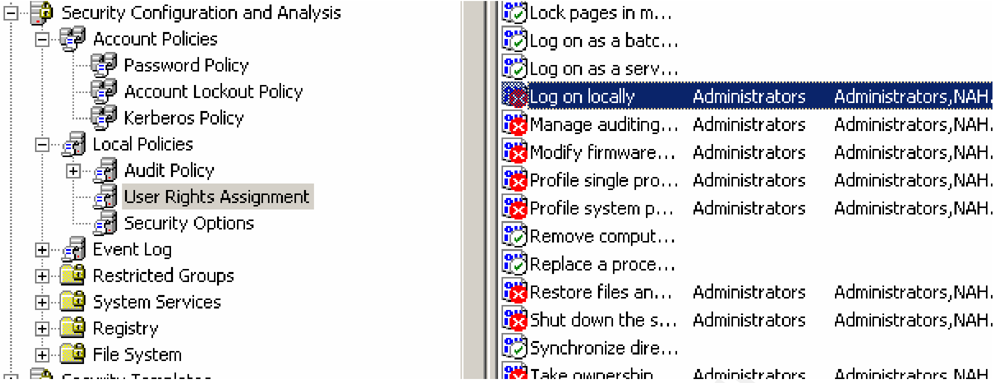
Testing Group Policy

Once the Group Policy settings have been modified, you will need to test the objects in each one of the OUs. To do this, in the test lab discussed in Part 1 of this document, apply the GPOs to group policy in each of the domains.

Create a computer account under the "NAHQ Servers" OU. Bring a Windows 2000 Advanced server into the NAHQ Domain with that computer account. Verify the settings on the server match what is in the "SPI Secured Servers.INF". To do this, you can use the MMC Snap-in "Security Configuration and Analysis".

- Copy C:\WINNT\Security\Database\secedit.sdb to C:\WINNT\Security\Database\secedittemp.sdb.
- Right click on "Security Configuration and Analysis" and choose "Open Database …".
- Navigate to C:\WINNT\Security\Database\secedittemp.sdb and click on [Open].
- Right click on "Security Configuration and Analysis" and choose "Import Template …".
- Navigate to "SPI Secured Servers.INF" and click on [Open].
- Right click on "Security Configuration and Analysis" and choose "Analyze Computer Now …".
- On the right verify the settings on the server against your template. Note that under "User Rights Assignment", you will see exceptions. This is because of

the Role Based Security you have applied to Group Policy (for example "Logon Locally" in NAHQ has NAHQ\ServerSysAccess-L).

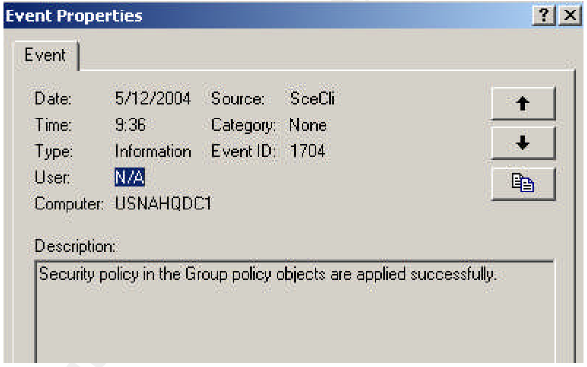


Lock pages in m...		
Log on as a batc...		
Log on as a serv...		
Log on locally	Administrators	Administrators,NAH.
Manage auditing...	Administrators	Administrators,NAH.
Modify firmware...	Administrators	Administrators,NAH.
Profile single pro...	Administrators	Administrators,NAH.
Profile system p...	Administrators	Administrators,NAH.
Remove comput...		
Replace a proce...		
Restore files an...	Administrators	Administrators,NAH.
Shut down the s...	Administrators	Administrators,NAH.
Synchronize dire...		
Take ownership	Administrators	Administrators,NAH

Perform the same steps as you did with the Advanced Server with a workstation in the "NAHQ Computers" OU. Validate settings using the "SPI Secured Workstations.INF" and "NAHQ Computers" User Rights Assignments.

Install a Domain Controller and make sure the server shows up in the "Domain Controllers" OU. Validate settings using the "SPI Secured Domain Controllers.INF" and "Domain Controllers" User Rights Assignments.

Verify on all systems the existence of the following application event log entry.



Date: 5/12/2004 Source: SceCli
Time: 9:36 Category: None
Type: Information Event ID: 1704
User: N/A
Computer: USNAHQDC1

Description:
Security policy in the Group policy objects are applied successfully.

Testing System Functionality

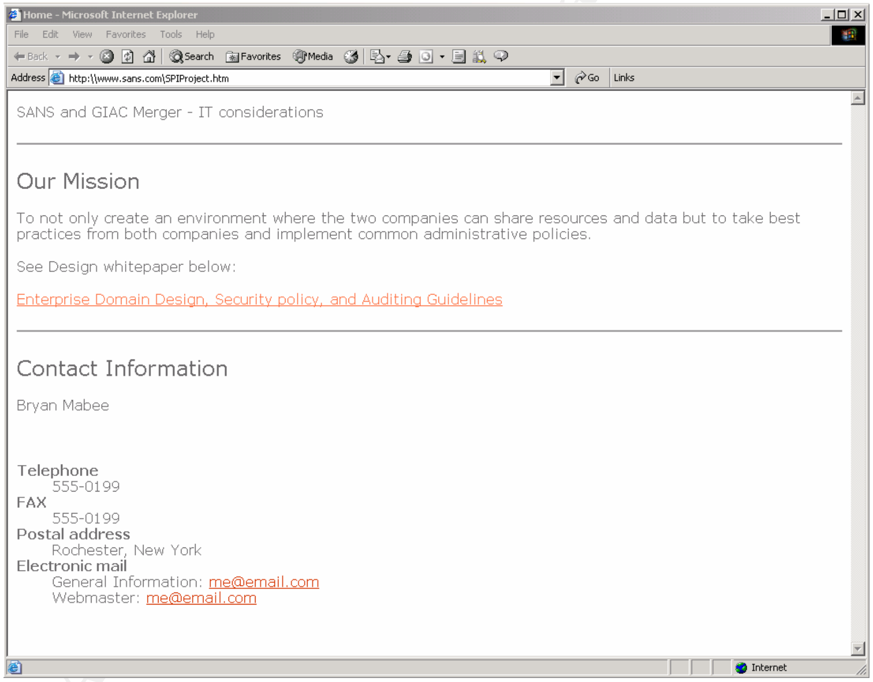
All major functions on the servers and workstations in the environment should be tested against the new policies prior to implementing them in production. These functions were put into test cases and executed in the lab. In addition to testing these in the lab, after the new policies have been applied to production, they should be tested in production. A back out plan should always be ready in case of test failures. In the case of Group Policy, the default policies can be reapplied to the systems that failed from the new policies. Below are two examples of the test cases:

Test 1 – Systems IIS Server functions Properly

One of the web sites on the SANS web servers is a page for the SPI team to review this paper and get updated information on the project. To test the policies against web pages in production, the following tasks are performed:

- The production web pages for the “Secured Partnership Infrastructure” (SPI) team page are copied to a lab IIS server built as a replica of the production Intranet IIS server.
- The server is moved over to the “Web Servers” OU under the “NAHQ Servers” OU.
- The page is tested.
- The result was the page displayed and the links are active.
- The production web pages for the “Secured Partnership Infrastructure” (SPI) team page are copied to a lab IIS server built as a replica of the production DMZ IIS server.
- The server is locked down with the procedure outlined in the “Lockdown of DMZ IIS5 Servers” section of this document.
- The page is tested.
- The result was the page displayed and the links are active.

Figure 8 - Sample Web Page Functionality Test


Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Internet

http:\\www.sans.com\SPIProject.htm

SANS and GIAC Merger - IT considerations

Our Mission

To not only create an environment where the two companies can share resources and data but to take best practices from both companies and implement common administrative policies.

See Design whitepaper below:

Enterprise Domain Design, Security policy, and Auditing Guidelines

Contact Information

Bryan Mabee

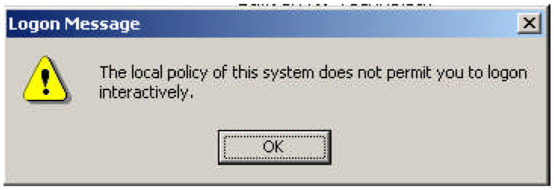
Telephone
555-0199
FAX
555-0199
Postal address
Rochester, New York
Electronic mail
General Information: me@email.com
Webmaster: me@email.com

Test 2 – Administrative Support of systems under the Role Based Security defined

It is important to test administrative access to systems after the application of Role Based Security Group Policy. An Administrator cannot afford to be surprised to find out that they do not have access when issues arise. To test this access, do the following:

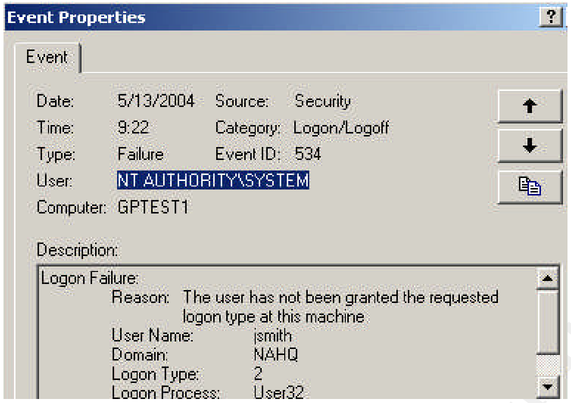
- Install a Windows 2000 Professional workstation
- Bring it into the NAHQ domain under the “NAHQ Computers” OU.
- Attempt to logon locally to the Workstation using accounts from each one of these groups:
    - Tier 1 Customer Support
    - Tier 2 Server Operations

    - Security Operations
    - <Site> On-Site Support
    - AD Service Owners
    - Central SANS IT Engineering
    - <Domain> Security Administrators
- Only users from the groups “Tier 1 Customer Support” and “NAHQ On-Site Support” should have rights to logon locally of the groups tested.
- Install a Windows 2000 Advanced Server
- Bring it into the NAHQ domain under the “NAHQ servers” OU.
- Attempt to logon locally to the Server using accounts from each one of these groups:
    - Tier 1 Customer Support
    - Tier 2 Server Operations
    - Security Operations
    - <Site> On-Site Support
    - AD Service Owners
    - Central SANS IT Engineering
    - <Domain> Security Administrators
- Only users from the groups “Tier 2 Server Operations”, “Security Operations”, “AD Service Owners”, “Central SANS IT Engineering”, and “NAHQ Security Administrators” should have rights to logon locally of the groups tested.
- Install a Windows 2000 NAHQ Domain Controller
- Bring it into the NAHQ domain under the “Domain Controllers” OU.
- Attempt to logon locally to the Server using accounts from each one of these groups:
    - Tier 1 Customer Support
    - Tier 2 Server Operations
    - Security Operations
    - <Site> On-Site Support
    - AD Service Owners
    - Central SANS IT Engineering
    - <Domain> Security Administrators
- Only users from the groups “AD Service Owners”, “Central SANS IT Engineering”, and “NAHQ Security Administrators” should have rights to logon locally of the groups tested.
- Below is an example of the user who was attempting to login to a server they do not have rights to.



The local policy of this system does not permit you to logon interactively.

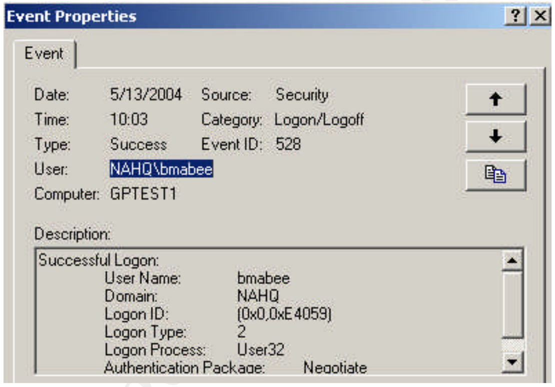
- Security Log Event of an unsuccessful login. John Smith was a member of Tier 1 Customer Support and attempted to login to a server.



```
Date:      5/13/2004   Source:    Security
Time:      9:22        Category:  Logon/Logoff
Type:      Failure     Event ID:  534
User:      NT AUTHORITY\SYSTEM
Computer:  GPTEST1

Description:
Logon Failure:
         Reason:   The user has not been granted the requested
                   logon type at this machine
         User Name:          jsmith
         Domain:             NAHQ
         Logon Type:         2
         Logon Process:      User32
```

- Security Log Event of a successful login. Bryan Mabee (me) was a member of Tier 2 Server Operations and attempted to login to a server.



```
Date:      5/13/2004   Source:    Security
Time:      10:03       Category:  Logon/Logoff
Type:      Success     Event ID:  528
User:      NAHQ\bmabee
Computer:  GPTEST1

Description:
Successful Logon:
         User Name:          bmabee
         Domain:             NAHQ
         Logon ID:           (0x0,0xE4059)
         Logon Type:         2
         Logon Process:      User32
         Authentication Package:      Negotiate
```

Evaluation of Policies

There are areas where the Group Policy can become stronger but impact needs to be carefully evaluated. One can make Group Policy lockdown all objects in the domain disabling all unneeded services, tasks, and applications but this would require more administration and cause troubleshooting of problems to be much more difficult. On the other hand, one can be the hero by locking down something that prevented a vulnerability to be spread through the organization.

Some examples of how the SPI Group Policy can become more locked down are service startup states, permissions on registry keys, and permissions on portions of the file system.

Windows 2000 has many services that start by default but are not needed. A future vulnerability may take advantage of one of these services. If these services will not be used by the functional server, they can be disabled. This can be kept consistent through Group Policy. Some examples of services that can be disabled on most servers are Clipbook, Fax Service, Indexing Service, Internet Connection Sharing, License Logging Service, Messenger Service, NetMeeting Remote Desktop Sharing, Removable Storage, Smart Card, Smart Card Helper, Telephony, Utility Manager, Etc.

Restricting permissions on the registry prevent individuals who need access to the server from changing settings and installing software. Changes to these permissions will require a more granular approach to Role Based Security.

Restricted access to the file system comes in handy when there are operational tools on the servers that only some individuals should be using. It also gives a slight advantage to protect from viruses who damage system files.

If, in the future, projects are created to expand the scope of lockdown through Group Policy, new OUs may need to be created. For instance, web services will be disabled on all servers but web servers. Another example is special permissions can be put on data locations of legal and finance file servers through Group Policy. Group Policy is such a powerful security and administrative tool that the options seem limitless.

Auditing Your Environment

Auditing Events

Auditing events can be a very labor intensive task. When Auditing events one needs to determine how to extract from the Event Logs, how to collect them centrally, how to sift through to get the events important to you, how to interpret, and what to do with that information.

By default the baseline template logs the following:

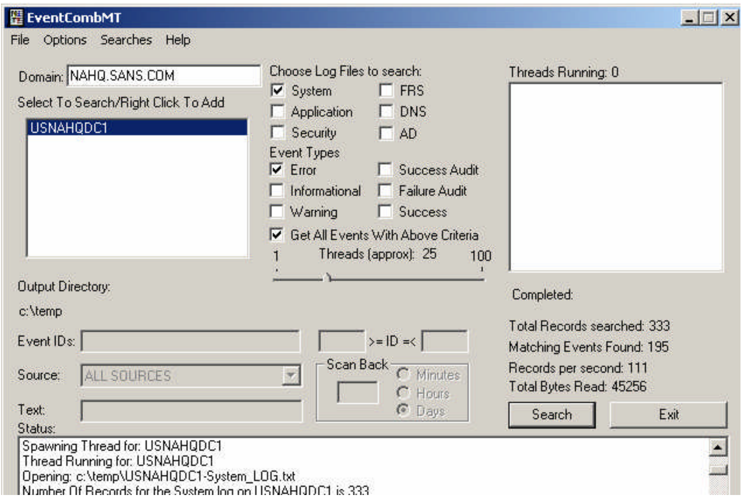
Audit account logon events - Success, Failure
Audit account management - Success, Failure
Audit directory service access - Failure
Audit logon events - Success, Failure
Audit object access - Failure
Audit policy change - Success, Failure
Audit privilege use - Failure
Audit process tracking - No auditing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

A free utility from Sysinternals (http://www.sysinternals.com/ntw2k/freeware/psloglist.shtml) called *Psloglist.exe* can remotely extract the eventlogs to a comma delimited text file and clear the log when finished. It is important to save the text file with a descriptive name. Include the server name, Domain name and the date. These logs will get pretty big, but if compressed won't take up much room. A task run from a management server using a service account can be scheduled at a frequency that would provide the most data.

The group policy design mentioned in this document handles audit polices. "Audit account management" is particularly important for the "Privileged Accounts" OU for it contains many sensitive accounts that should infrequently change. Event IDs 624 – 644 deal with account management. It is important for these event IDs corresponding to the accounts in the "Privileged Accounts" OU to be audited.

Another tool that Microsoft offers with it's Windows 2003 Resource Kit is the *EventCombMT.exe* tool. This tool allows an administrator to choose domain, choose which Event Log files to search, choose Event Type and Event ID, choose Source, and choose text to search for. You can save the output to a comma delimited file or in .csv format. This tool has a number of useful built-in searches and you can also create custom searches. Reports can be run periodically.

Figure 9 - EventCombMT



Domain: NAHQ.SANS.COM

Select To Search/Right Click To Add

USNAHQDC1

Choose Log Files to search:

☑ System ☐ FRS
☐ Application ☐ DNS
☐ Security ☐ AD

Event Types

☑ Error ☐ Success Audit
☐ Informational ☐ Failure Audit
☐ Warning ☐ Success

☑ Get All Events With Above Criteria

1 Threads (approx): 25 100

Threads Running: 0

Output Directory:
c:\temp

Event IDs: >= ID =<

Source: ALL SOURCES

Scan Back ○ Minutes ○ Hours ● Days

Text:

Completed:

Total Records searched: 333
Matching Events Found: 195
Records per second: 111
Total Bytes Read: 45256

Status:

```
Spawning Thread for: USNAHQDC1
Thread Running for: USNAHQDC1
Opening: c:\temp\USNAHQDC1-System_LOG.txt
Number Of Records for the System log on USNAHQDC1 is 333
```

To check if and when the correct Group Policy is being applied to the system in question, a resource kit tool called *gpresult* can be used. A script can be run and sent to a Security Administrator to review. This reports displays useful information like the following:

Figure 10 - Output of *gpresults* Execution

```
Microsoft (R) Windows (R) 2000 Operating System Group Policy Result tool
Copyright (C) Microsoft Corp. 1981-1999
Created on Friday, May 14, 2004 at 11:02:58 AM
Operating System Information:
Operating System Type:              Server
Operating System Version:   5.0.2195.Service Pack 4
Terminal Server Mode:               None
#################################################################
 User Group Policy results for:
 CN=Bryan Mabee,OU=NAHQ Users,DC=NAHQ,DC=SANS,DC=com
 Domain Name:               NAHQ
 Domain Type:               Windows 2000
 Site Name:                 Default-First-Site-Name
 Roaming profile:           (None)
 Local profile:     C:\Documents and Settings\bmabee
 The user is a member of the following security groups:
      NAHQ\Domain Users
      \Everyone
      BUILTIN\Users
      NT AUTHORITY\INTERACTIVE
      NT AUTHORITY\Authenticated Users
      \LOCAL
      NAHQ\Tier 2 Server Operations
#################################################################
```

```
Last time Group Policy was applied: Friday, May 14, 2004 at 10:57:00 AM
############################################################
  Computer Group Policy results for:
  CN=GPTEST1,OU=NAHQ Servers,DC=NAHQ,DC=SANS,DC=com
  Domain Name:            NAHQ
  Domain Type:            Windows 2000
  Site Name:              Default-First-Site-Name
  The computer is a member of the following security groups:
          BUILTIN\Administrators
          \Everyone
          BUILTIN\Users
          NT AUTHORITY\NETWORK
          NT AUTHORITY\Authenticated Users
          NAHQ\GPTEST1$
          NAHQ\Domain Computers
############################################################
Last time Group Policy was applied: Friday, May 14, 2004 at 11:00:28 AM
Group Policy was applied from: usnahqdc1.NAHQ.SANS.COM
============================================================
The computer received "Registry" settings from these GPOs:
          Local Group Policy
          NAHQ policy
============================================================
The computer received "Security" settings from these GPOs:
          Local Group Policy
          SPI Baseline Policy for NAHQ
          NAHQ Servers
============================================================
The computer received "EFS recovery" settings from these GPOs:
          Local Group Policy
          SPI Baseline Policy for NAHQ
```

Audit policy change needs to be watched carefully also. Only a limited number of individuals should make changes with a strict approval process.

In the long term, a product like GFI LanGuard Event Monitor or ISS RealSecure Intrusion Detection would help protect the environment. This will reduce the amount of administrators necessary for evaluating logs and give security administrators a quicker response time.

Auditing Critical Settings

On occasion, settings critical to the security of the workstations, servers, and DCs change from the template as a result of tempering or incorrect configuration. A method of auditing this needs to be in place to assure Security Administrators are aware of the situation and can correct it in a timely manner.

Some key policy settings considered to be critical to the organization are the Account Policies, the Audit Policies, and a subset of the User Rights Assignments. To check the server template against the local configuration, perform the following:

The manual way for checking these setting is through the Security Configuration and Analysis MMC Snap-in.

- Copy C:\WINNT\Security\Database\secedit.sdb to C:\WINNT\Security\Database\secedittemp.sdb.
- Right click on “Security Configuration and Analysis” and choose “Open Database …”.
- Navigate to C:\WINNT\Security\Database\secedittemp.sdb and click on [Open].
- Right click on “Security Configuration and Analysis” and choose “Import Template …”.
- Navigate to “SPI Secured Servers.INF” and click on [Open].
- Right click on “Security Configuration and Analysis” and choose “Analyze Computer Now …”.
- Verify settings.

Scripts can be written using the *secedit* command to compare exported local policies and security templates. These scripts can send the ‘difference’ reports to a central location at a periodic basis.

A more automated and comprehensive approach to critical settings auditing and management is the Full Armor FAZAM 2000 Version 3 product (http://www.fullarmor.com/solutions/group/). This is a much more expensive solution and will require leadership’s commitment to policy management. A highlight of the benefits of this product include tracking changes to Group Policy, allowing offline modifications, ‘difference’ reporting, rollback, documentation, etc.

Auditing Performance Data

SNMP should be configured with a private string on all servers. Auditing of performance data is done through the use of Tivoli Distributed Monitoring. Agents will be put on all enterprise servers and data will be collected on Disk capacity, CPU utilization, Memory utilization, and heartbeat (general availability).

The “Tier 2 Server Operations” group will be sent alerts if the agent detects changes beyond the threshold that was set. Action will be taken by that team accordingly.

IBM, HP (Compaq), and Dell all have free management tools that monitor system performance and send alerts for imminent failures. These centralized consoles should be configured to collect these events. They should be monitored by the “Tier 2 Server Operations” group. An initiative is in place to begin standardizing on one hardware platform vendor so that only one console will be needed.

Merging SANS and GIAC Infrastructure Design

The focus of this paper was the merging of SANS and GIAC in a way to enable both companies to continue functioning and allow growth in leveraging each others resources. This was done in a way that included security best practices from both companies and the industry. At risk to both companies, if done incorrectly, is the information that keeps them competitive and the ability to operate uninterrupted by vulnerabilities.

There is a vast amount of features that can be locked down in the topics discussed. In some cases, the more you lock down, the more complex the support of the environment becomes. Automation reduces the amount of manual labor but increases the cost in software/hardware and expertise. The key is to cover as much as possible and mature over time.

Many topics involving security were not discussed in this paper including physical security of assets, disaster recovery, antivirus, Intrusion Detection, social engineering, perimeter security, patch management, OS and application hardening, etc. These also need to be considered on their own.

GIAC’s domains and SANS’ domains were joined by external trusts, connecting domains together where users needed to collaborate. Administration, as a result, needed to be consolidated. This saved both companies a lot of IT administration overhead and provided a consistent security approach.

A standard set of templates were created using best practices from both companies and the industry. These templates were applied and verified in an orderly way. These standards were documented so that support of the environment is easier. These templates will mature over time as issues are worked out and vulnerabilities are identified.

An auditing plan of events, performance, and critical settings has been put in place. This will allow administrators to detect bottlenecks, vulnerabilities, exploits, indiscretion, and other mischief. This information will allow administrators to tweak the environment in order to keep it going smoothly.

The key to this transformation is to make this merged company a more profitable and efficient business in the marketplace.

Appendix A – Security Templates

Group Policy.zip

References

Rick, Gregory. “GIAC Enterprises: Windows 2000 and Active Directory Design.” Securing Windows Practical Assignment Version 3.0 – Option 1. 24 May 2002. URL: http://www.giac.org/GCWN_200.php (2 January 2004) .

Author Unknown. “Multiple Forest Considerations.” Abstract. 1.0.0. 18 November 2002. URL: http://www.microsoft.com/downloads/details.aspx?familyid=71242e3a-ec89-480a-8df5-2c379a1e560f&displaylang=en (2 January 2004).

Hanley, J. “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset.” Version 1.2. 3 December 2002. URL: http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf (24 January 2004).

Author Unknown. “Windows 2000 Security Hardening Guide.” Version 1.0. 15 May 2003. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en (February 2004).

Fossen, Jason (multiple contributors). “Windows 2000/XP/2003 IPSEC and VPNs.” Version 7.4. 26 August 2003. SANS Institute Track 5 “Securing Windows” Course Material.

Author Unknown. “Enabling Resource Sharing Between Windows 2000 Forests.” Windows 2000 Resource Kit Deployment Scenarios. URL: http://www.microsoft.com/windows2000/techinfo/reskit/deploymentscenarios/scenarios/trust_enable_resshare_w2000_forests.asp (February 2004)

Mason, Andrew. “Active Directory Branch Office Deployment Guide.” Version 1.0. 9 August 2001. URL: http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/branchoffice/default.asp (February 2004)

Bartock, Paul F Jr; Donahue, Paul L; Duesterhaus, Daniel J; Haney, Julie M; Hayes, Pentice S; Pitsenbarger, Trent H; Stephens, Robin G; Ziring, Neil L. “Microsoft Windows 2000 Network Archetecture Guide.” Version 1.0. 19 April 2001. URL: http://nsa2.www.conxion.com/win2k/download.htm (February 2004)

Haney, Julie M. “Guide to Securing Microsoft Windows 2000 Group Policy.” Version 1.1. 13 September 2001. URL: http://nsa2.www.conxion.com/win2k/download.htm (February 2004)

Haney, Julie M. “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set.” Version 1.2. 3 December 2002. URL: http://nsa2.www.conxion.com/win2k/download.htm (February 2004)

Rice, David C. “Group Policy Reference.” Version 1.0.8. 2 March 2001. URL: http://nsa2.www.conxion.com/win2k/download.htm (February 2004)

Fossen, Jason (multiple contributors). “Windows 2000/XP/2003 Group Policy and DNS.” Version 1.5.2. 26 August 2003. SANS Institute Track 5 “Securing Windows” Course Material.

Rice, David C; Sanderson, Mark J. “Guide to Securing Microsoft Windows 2000 Active Directory.” Version 1.0. December 2000. URL: http://nsa2.www.conxion.com/win2k/download.htm (February 2004)

Walker, William E IV; Christman, Sheila M. “Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0.” Version 1.4. 29 October 2003. URL: http://nsa2.www.conxion.com/win2k/download.htm (February 2004)

Davis, John, “From Blueprint to Fortress: A Guide to Securing IIS 5.0.” Version 1.0. June 2001 URL: http://www.microsoft.com/serviceproviders/security/iis_security_p73766.asp (May 2004)

Seguis, Steve. “Windows Scripting Solutions” URL: http://www.winnetmag.com/Articles/ArticleID/27574/pg/2/2.html (May 2004)

Unknown. “Tivoli Distributed Monitoring User’s Guide” Version 3.7. URL: http://publib.boulder.ibm.com/tividd/td/dist_mon/GC31-8382-04/en_US/HTML/ (May 2004)

Author Unknown. “Eliminating the Management Challenges of Group Policy with FAZAM 2000” Version 1.1. January 19, 2001. URL: http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges_v11_010119.pdf (May 2004)