Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment
Version 3.2
Option 1

The SANS Co Acquisition of GIAC Enterprises
Active Directory Design and Administration

Submitted by
Erik Peterson

March 28, 2004

TABLE OF CONTENTS

0 ABSTRACT

In this current economic market, downsizing and the movement to migrate U.S. operations to offshore sites, etc. has devalued many U.S. corporations making them "ripe for the picking". Such is the case with a lesser-known software development house called GIAC Enterprises – the developers of an online subscription based service that sells access to a database of electronic fortunes to manufactures of fortune cookies. GIAC Enterprises is based out of Maui, HI.

SANS Co is a large conglomerate that already has organizations operating in many different sectors. SANS Co, always on the lookout to purchase yet another undervalued company for pennies on the dollar, has its gaze set firmly on GIAC. For some time now, SANS Co has predicted massive product growth in the area of baking paper fortunes into all kinds of foods, such as raviolis, doughnut holes, cream-puffs and even possibly the insertion of these into fruits and some vegetables (what better way to get the kid's to eat their brussel sprouts than to look forward to finding a fortune inside?!) and sees the ability to expand GIAC's market into the leader in creation of new fortunes through these new revenue streams. GIAC Enterprises is a perfect compliment to their existing Merchandising segment, the world's largest manufacturer of vending machines and snack displays.

GIAC, though posting a small profit was struggling. The IT department had recently all just quit to take up the sport of surfing. Luckily they had the foresight to have their Active Directory Design documented here: http://www.giac.org/practical/Harpal_Parmar_GCNT.doc[1]. The purchase of GIAC was immanent. SANS Co sent down a team of crack Infrastructure and IT security guys from their corporate office to asses the situation. After careful review, and a couple days of cliff diving and eating at Luaus, the IT guys completed their report. The conclusion: Leave their existing Active Directory in place. Due to the lack of local IT support, this was the best option. A Forest trust could be implemented to facilitate administration and resource sharing in the existing Active Directory, and could be managed remotely by SANS Co staff until new IT staff could be hired at GIAC.

[1] Parmar, Harpal. "A Secure Windows 2000 Infrastructure for GIAC Enterprises." GCNT Practical Assignment. Version 3.0. 05 May 2002. URL: http://www.giac.org/practical/Harpal_Parmar_GCNT.doc (17 December 2003).

1 DOMAIN DESIGN

SANS Co has an existing Active Directory running in Windows 2003 Server functional level. GIAC Enterprises already has their Active Directory and network infrastructure documented. This section will explain how SANS Co has implemented Active Directory within their corporate network of businesses, and will touch on the design of GIAC enterprises only where necessary to explain interoperability and where changes need to be implemented to facilitate this.

1.0 SANS Co OVERVIEW

SANS Co as mentioned earlier, is a large multi-company conglomerate. SANS Co, which stands for: **S**pace Travel, **A**irplanes, **N**uclear [*research*], and **S**nacks; has four Domains in its Active Directory forest. These are SANSCO.INT, AEROSPACE, NUCLEAR, and MERCHANDISING.

Each of these Domains represents a business segment for SANS Co, and each of these business segments may contain multiple companies. Each Company Location will be primarily managed in Active Directory through Group Policy Objects at the Organizational Unit level.

Besides these four Domains, SANS Co has a corporate WEB farm where they house the Internet presence for all of their business segments. This WEB farm is contained in its own Active Directory Forest which exists outside the SANCO.INT forest.

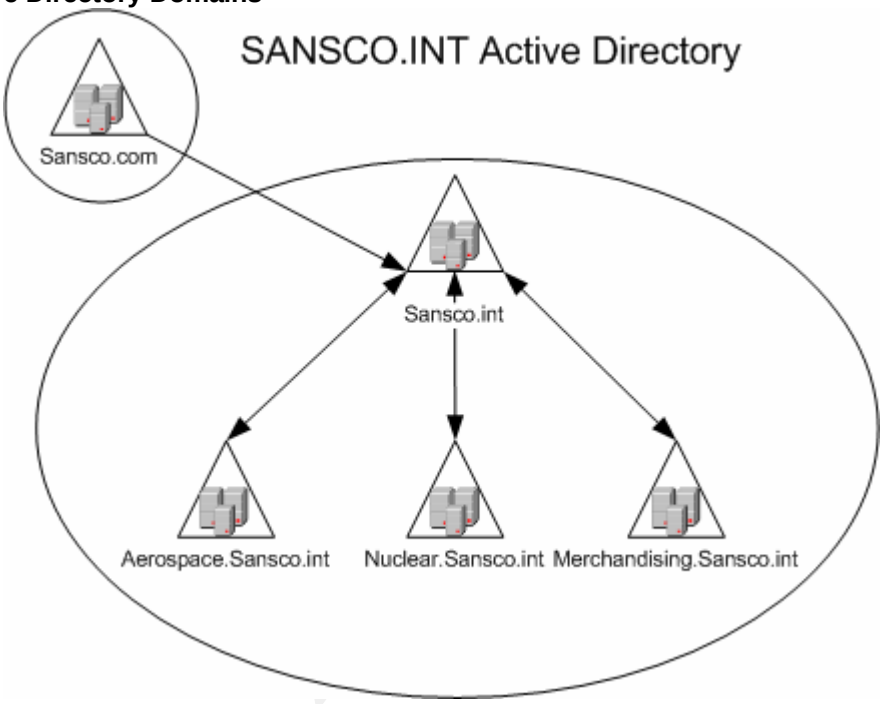
Figure 1: SANS Co Locations and office sizes within each Domain

Domain	Business Location	Size
Sansco	Stamford, CT	Large
Aerospace	Lynnwood, WA	Large
Aerospace	Burbank, CA	Large
Aerospace	Cleveland, OH	Large
Aerospace	Jacksonville, FL	Large
Aerospace	Redmond, WA	Small
Aerospace	Wichita, KS	Small
Nuclear	Springfield, OH	Large
Nuclear	Cincinnati, OH	Large
Nuclear	Long Island, NY	Small
Merchandising	St. Louis, MO	Large
Merchandising	Norwood, MA	Small

SANS Co choose to have each business segment as its own Domain, instead of in separate Forests. This single Forest model was chosen for ease of administration, use of single DNS Namespace, and to support the existing Exchange 2000 messaging organization, where delegation, public folder replication, and collaborative features are a

requirement for the entire SANS Co organization. Had SANS Co went with Multiple Forests, it would have required the installation and somewhat complex configuration of a Directory Services connector such as Microsoft Metadirectory Services[2], a tool which would allow you to integrate information from multiple directory services. SANS Co would need this tool replicate the Global Address List (GAL) and Public folders from their Exchange Organization in a multi-forest environment.

Figure 2: Active Directory Domains



1.1 INFRASTRUCTURE DESIGN

The SANS Co IT Infrastructure was based on relatively low-cost, yet reliable and robust solutions chosen to fit the requirements of the business; these being: ease of management through vendor standardization and centralized manageability, flexibility to scale within vendor product lines, reliability, interoperability through standardized implementation of well-known services and, and of course – getting a big discount for volume purchases. When discussing Active Directory particulars, Infrastructure assumptions will be based upon the following definitions.

1.1.0 NETWORKING

Active Directory Sites are TCP/IP subnets. Active Directory enabled clients use this to find the closest DC to log on to. Typically clients will log in to DCs located within their own site. Each of the SANS Co locations runs at least one IP subnet. The traffic is

[2] Microsoft Corporation. "Microsoft Metadirectory Services."
URL: http://www.microsoft.com/windows2000/technologies/directory/MMS/default.asp (08 January 2004).

routed between sites across WAN links of varying speeds. SANS Co networking equipment can be dived-up into four main categories.

I. **Routers:**
For both internal routers and border or edge routers, Cisco systems routers were selected. This was due to the large pool of trained professionals available to employ, and good proven track record in reliability. The border routers are managed and monitored by a national ISP. Internal routers are self-managed by the corporate IT staff in the corporate and smaller offices, and by the local IT staff where the networks are larger and more complex.

II. **Switches:**
Due to high costs associated with the volume of switches needed, Cisco was not selected as a switch vendor. Instead, DELL Corporation was selected. This was due in part to a volume discount purchase contract that SANS Co has awarded to DELL for corporate desktops, laptops and Microsoft OS based server purchases. All DELL switches purchased are of the managed type, and support SNMP. The switch framework, as well as the routers in the SANS Co Network are configured and access controlled, and audited. The policy for this network equipment is:

- Be access controlled with a username and password
- Have every port accurately labeled in regards to the host, vlan or next network device that is connected to it.
- Send SNMP data to authorized SNMP collectors, and have the PUBLIC community name changed to the appropriate community name for each collector site. Collectors are local at larger sites, and remote for smaller offices where they are hosted at the corporate office. All remotely located SNMP collectors will utilize IPSEC tunnels to send their data encrypted.

III. **Firewalls:**
Watchguard Corporation was selected to provide the firewalls that protect the corporate networks. Watchguard Corporation provides easy to manage firewall appliances that scale well, and provide good security, with and easy to use interface. These were selected initially because of very low cost of implementation. Firewalls that protect the corporate network will be configured using these basic assumptions:

- By default, no access is allowed inbound into private networks – no exceptions!
- By default, no access is to be allowed outbound, except:

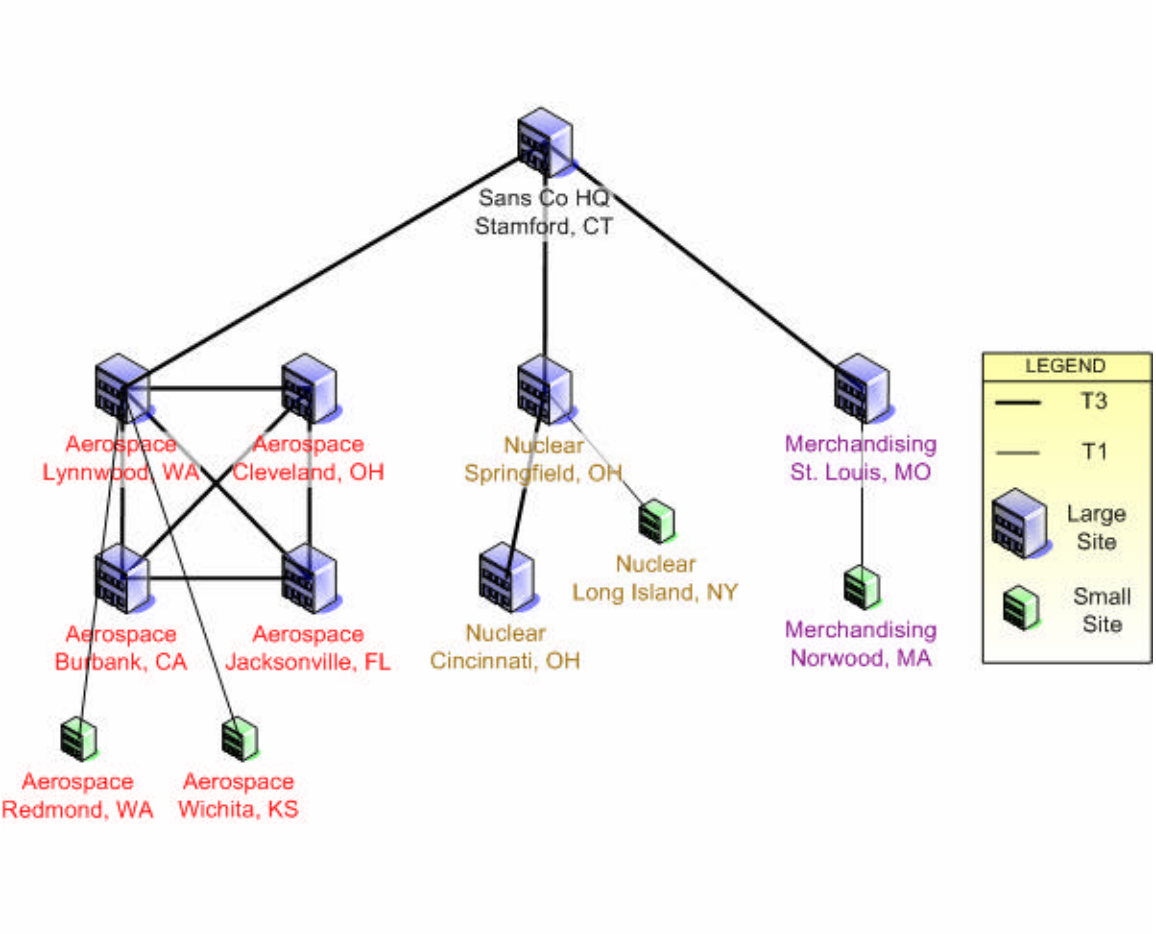
- Outbound traffic (at the port level) will only be allowed where business requires this, *and* application proxies[3] will be used wherever possible to provide the most security and tightest control over the traffic allowed out.

Firewalls protecting the sansco.com Web farm will differ in design and configuration, and will be detailed in the design description of the Web farm.

IV. **VPNs:**

Watchguard was also selected to provide WAN VPN connectivity for SANS Co due to familiarity with the product and its interface by existing SANS Co IT staff in the corporate office and within the business segments. A hardened appliance was considered a better and more secure choice to handle VPN traffic over Microsoft's implementation of IPSEC in tunnel mode. The design of the VPNs are detailed below, broken out by the different load and security requirements necessary to support the type of traffic generated by each category.

Figure 3: Site Topology



[3] WatchGuard Technologies, Inc. "Application Layer Proxies: Beyond Packet Filtering." URL: http://www.watchguard.com/products/proxy.asp (08 January 2004).

a. Large Office

A large office is considered one with a staff of five hundred users or more. For this type of office, a high-availability pair of Watchguard V60s[4] was selected for its ability to scale appropriately, cluster for redundancy, centrally manage of policies, and control traffic flow by prioritization through quality of service. All Large Offices will be fully meshed (each of connected with each other one) within a Domain (by definition, also by business segment) using IPSEC[5] in Tunnel Mode. The IPSEC policies are defined in figure 4:

Figure 4: IKE / IPSEC Policy

- Diffie-Hellman Type II[6]
- Perfect Forward Secrecy[7]
- SA Life:
  - 60 minutes / 100MB
- 168bit 3DES Encryption
- 160bit SHA-1 Hash

Authentication is accomplished through RSA certificates of 1024 bit key length. The CA for these certificates is an Issuing or Intermediate CA in the SANS Co PKI. PKI and Certificate Authorities will be discussed in detail later.

Each Domain will have designate one of their sites with a high-speed link to have a single connection to the SANS Co corporate office, in a hub and spoke design. This configuration provides for redundancy in connection amongst sites that need collaboration, and minimizes load and traffic across Domains which do not need to have frequent access with each other. Because of the design model incorporating business segments within a single domain, only locations within a Domain have a great need to access resources amongst each other.

Lastly, only WAN VPN traffic will be routed through these devices. Accessing other hosts on the internet through them is prohibited through policy.

b. Small Office

A small office is considered one with a user base of one to five hundred users. The Watchguard Firebox 1000 Appliance was selected to handle

[4] WatchGuard Technologies, Inc. "Firebox VClass: Perimeter Security." URL: http://www.watchguard.com/products/vclass.asp (10 January 2004).
[5] Kent, S. Atkinson, R. "Security Architecture for the Internet Protocol." Request for Comments: 2401. November 1998. URL: http://www.ietf.org/rfc/rfc2401.txt (13 January 2004).
[6] Microsoft Corporation. "Key exchange methods." Windows Server 2003 Product Documentation Standard Edition Help. URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_IPSECkeyexchgsm.asp (09 January 2004).
[7] American National Standard for Telecommunications. "Perfect Forward Secrecy." Telecom Glossary 2000. 28 February 2001. URL: http://www.atis.org/tg2k/_perfect_forward_secrecy.html (09 January 2004).

this duty. A Watchguard Firebox 1000 will also be deployed at the large office containing the high-speed link to the SANS Co corporate office. This Firebox 1000 will function as the DVCP Server[8], which is a Watchguard proprietary protocol that allows for utilizing the Watchguard VPN Manger[9] to configure the VPNs of the small office networks. The DVCP server contains its own CA for certificate management and deployment to VPN peers. This DVCP server will also mange the assigned addresses for home office connections as defined next.

Only WAN VPN traffic will be routed through these devices. Access to other hosts on the internet through them is prohibited through policy.

c. Home Office

The home office user has been assigned a Watchguard SOHO device to protect his home network, as well as the Corporate LAN. The SOHO will be managed centrally through the Watchguard VPN Manager by the local IT staff responsible for managing the Corporate WAN.

SOHO devices are the only VPN devices and configuration where internet traffic, other than WAN traffic is allowed. The end-user of the SOHO device is not able to modify the settings of his/her SOHO.

d. Telecommuters

Mobile users or road-warriors needing access to the corporate LAN while traveling will connect to the LAN via Microsoft PPTP v2[10]. The PPTP connectoid is pre-configured for the mobile user with the aid of the Connection Manager Administration Kit (CMAK)[11]. Split-tunneling is explicitly prohibited. User authentication is provided via Microsoft RADIUS into the Domain. The only Domain users allowed to access the PPTP server will be placed into a global security group created explicitly for this purpose.

These Individual locations within the business segments that are able to utilize high-speed WAN links for secured replication of RPC traffic, will have their IP subnets grouped as Active Directory Sites for intra-site replication. Each Domain will have a secured high-speed link back to the SANS Co corporate LAN and Forest Root Domain, but not necessarily with each-other, as rich collaboration amongst the different business segments (or Domains) is not a business requirement considering that each business segment has such vastly different product lines.

[8] WatchGuard Technologies, Inc. "VPN Manager FAQ: Info Center."
URL: http://www.watchguard.com/docs/html/vpnmgr_faq.asp#dvcp (10 January 2004).
[9] WatchGuard Technologies, Inc. "VPN Manager: Firebox System." URL: http://www.watchguard.com/products/vpnmanager.asp (10 January 2004).
[10] Microsoft Corporation. "Point-to-Point Tunneling Protocol (PPTP)." Windows XP Home Edition Product Documentation
URL: http://www.microsoft.com/WINDOWSXP/home/using/productdoc/en/access_pptp.asp (09 January 2004).
[11] Microsoft Corporation "Connection Manager Administration Kit Makes Daily Internet Access Easy." January 1998.
URL: http://www.microsoft.com/technet/archive/default.asp?url=/technet/archive/ie/evaluate/ie4cmak.asp (11 January 2004).

1.1.1 COMPUTERS

SANS Co, as mentioned earlier, has finagled a good discount with DELL Corporation. Therefore, all computer hardware is sourced from DELL. This provides the support infrastructure with a common platform to maintain. Technicians are certified as DELL PC support engineers. Server administrators are likewise certified on the DELL server hardware. Servers will utilize at a minimum: mirrored root disk, and RAID 5 data disk. All raid systems are hardware based for performance and reliability. Where necessary, more redundant disk sets may be used as applications require. The corporate office has worked with DELL purchasing to create a customized portal page for purchasing DELL equipment and tracking of assets. This aids in keeping hardware similar, since purchasing is distributed at every site.

1.1.2 DATA CENTERS

Large sites with Data Centers are required to maintain access limited (and audited), climate-controlled data centers that utilize fire suppression systems such as FM-200[12], and need to be on a centralized UPS system with a generator power backup system.

1.2 DESIGN SPECIFICS

Outlined below is the Active Directory design that SANS Co has put into place. SANS Co is made up of a parent Domain: Sansco.int; three child Domains that consist of; Aerospace, Nuclear, and Merchandising; and a separate Forest for their DMZ systems: Sansco.com.

1.2.0 FOREST ROOT DOMAIN

Sansco.int is brought up as the first Active Directory Domain for SANS Co. Enterprise Administrators and Schema Administrators will be the only two forest-wide groups, and will reside in within. The users in these groups will be limited to the IT Director and the lead Microsoft systems administrator.

Three Domain controllers for the Sansco.int root Domain will be created. These will all be global catalog servers. These are physically secured in the required Data Centers. Two Domain controllers will reside at the SANS Co corporate office in Stamford, while the third will reside at the Aerospace site in Lynnwood. This will provide for redundancy, and the geographic disbursement will aid in the event of disaster recovery. In regards to recovery of your Active Directory, Microsoft acknowledges the following:

> If all of the Domain controllers for the forest root Domain are lost in a catastrophic event, and one or more Domain controllers cannot be restored from backup, the

[12] Reliable Fire Equipment Company. "FM-200 Fire Suppression Systems." 29 January 2004. URL: http://www.reliablefire.com/fm200/fm200.html (29 January 2004).

enterprise administrators and schema administrators groups will be permanently lost. There is no way to reinstall the forest root Domain of a forest.[13]

These sites are linked via the WAN with a T3, providing ample bandwidth for the RPC link (which is encrypted via the IPSEC VPN routers) over which replication data will flow. The Lynnwood site was chosen to house the third Sansco DC due to the fact that it is the single largest site, and has the most and best local IT resources.

The Forest Root Server has operations that are unique to its role. These roles are configured as follows:

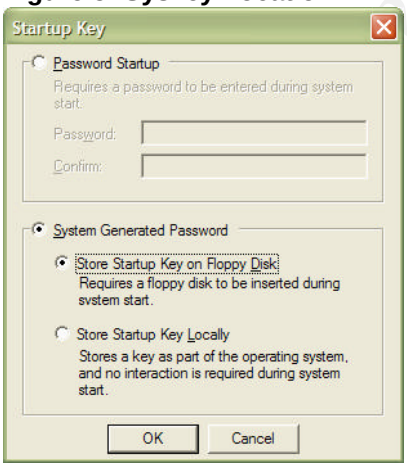
- Time Service – The Root Domain Controller will maintain the role of PDC Emulator role and will be authoritative for the entire forest. All Domain Controllers and DNS Server will sync their time with the root DC.

- Forest FSMO – Schema Master and Domain Naming Master roles are the two forest level FSMOs. These will be retained by the Root Servers.

- Root Domain FSMO – Infrastructure Master, RID Master and the PDC Emulator roles are also required on the Root Domain Controllers.

To protect passwords, the DC's master key, and service account passwords, the Forest Root DCs, as all DCs within the Sansco forest will have their System Keys stored on floppy disks.

Figure 5: Syskey Location



The first DC brought online is called SANSCODC (for clarity purposes in the writing of this document, this boorish name was chosen, a much cleverer name such as one like

[13] Microsoft Corporation, "Windows 2000 Server Deployment and Planning Guide." Windows 2000 Resource Kit. 01/19/2000. URL: http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/part3/chapt-9.asp (10 January, 2004).

Andrew D. Smith[14] would suggest, would have normally been chosen). This DC will run at the Windows Server 2003 Functional Level and Server 2003 Forest Functional Level which provides enhanced features such as renaming a Domain, and allowing for the ability to do cross-forest trusts (which will be in use with GIAC Corp). SANCODC will also be the first DNS Server for the Domain Sansco.int. It is a requirement that each Sansco Domain have at least two Domain Controllers.

1.2.0.0 CHILD DOMAINS

The three other child Domains under Sansco.int are Aerospace, Nuclear and Merchandising. At a minimum, each Domain will contain two Domain Controllers. For Domains with larger sites, a Domain controller or two will be placed at each physical location. Each Domain will contain a DC that will act as a Global Catalog Server. This will speed search operations, and minimize traffic back to HQ at SANS Co in Stamford, CT. For smaller sites within a Domain, although recommended, a Domain Controller is not necessarily a requirement as even these smaller sites are connected back up to their parent site a T1 speed WAN link.

1.2.1 SITES

In Active Directory, Sites are a collection of IP Subnets. Sites typically contain computers that are connected together with a fast and reliable network connection. Sites are defined in order to create an efficient replication topology. The mechanism that controls this replication is called the Knowledge Consistency Checker, or KCC. The KCC can automatically determine the best path to replicate using the spanning tree algorithm. This algorithm has been updated with Windows 2003 Server, and includes the ability to manage up to three thousand sites within a single Domain.

Within the SANS Co Active Directory, twelve sites are defined. These sites represent the Different IP networks that belong to each of the SANS Co physical locations.

1.2.2 DNS

Active Directory requires DNS to function. In Active Directory, Domains themselves are located using DNS. SANS Co will only host its private DNS namespace. This is an AD-Integrated zone called Sansco.int, and will run as a Windows 2003 Server, which through application partitions, allows for more finite control of DNS zone replication.

Windows 2003 DNS zone replication options are:

- All DNS servers in the Active Directory forest
- All DNS servers in the Active Directory Domain
- All Domain Controllers in the Active Directory Domain
- All Domain Controllers in a specified application directory partition

[14] Smith, Andrew "I don't want a Lime Mac, I want Names for my Servers!." 29 October 1999. URL: http://slashdot.org/features/99/10/28/1116250.shtml (16 January 2004).

The zone replication scope chosen for SANS Co will be: Replicate zone data to all DNS servers in the Active Directory Domain. This will provide for the good redundancy, without unnecessarily consuming bandwidth across WAN links.

Child Domains will be configured to use conditional forwarding to walk the Domain / DNS Tree in the most efficient manner. Each child Domain will be configured to use its Parent to lookup data in the zone for which it is authoritative. Zone lookups for which no Name Servers are configured will be configured to access external DNS servers directly, thus alleviating any extra DNS traffic across the WAN.

DNS Best Practices[15] dictates that responsible person field for the DNS zone should be used correctly with the appropriate email address of the System Administrator who is responsible for the DNS Server or zone. At SANS Co, a distribution list alias email address will be used for this entry as Admins may come and go, and the alias can be updated appropriately.

External DNS is hosted by the ISP providing Internet Access. This simplifies DNS security greatly. No DNS requests inbound from the internet will be allowed through firewall policy.

There was much debate amongst SANS Co IT over which TLD to use. Microsoft recommends using your organizations publicly registered DNS name and suffix[16], however the non-standard ".int" (for internal) was finally decided upon to keep the DNS records and IP addresses of the Sansco.com WEB farm separate and easier to manage. Secure updates will be required for hosts needing dynamic update. The Secure Cache against pollution option will also be enabled. This setting will help prevent an update returning back to the DNS server for a query which it didn't request. Another DNS server, configured similarly will be created to provide for redundancy.

1.2.3 DHCP

The SANS Co network will have desktop clients (never Servers) enabled to use DHCP. A DHCP Server will be created, and will provide secure dynamic updates in DNS for its clients. For convenience, the DHCP server is installed on the redundant DNS server. The DNSUpdateProxy global group was evaluated for usefulness, but rejected after consideration that the DHCP server being unavailable would be more than a minor inconvenience in and of itself, and the risk of DNS records becoming owner-less was not acceptable due to the fact that a rogue client could usurp control over them. The clients DHCP scope has been set to disable NetBIOS on all clients.

[15] Microsoft Corporation. "Best Practices." Windows Server 2003 Product Documentation Standard Edition Help. URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_DNS_imp_BestPractices.asp (16 January 2004).
[16] Microsoft Corporation. "Microsoft Windows 2000 Server Documentation." URL: http://www.microsoft.com/windows2000/en/server/help/sag_DNS_imp_NamespacePlanning.htm (16 January 2004).

1.2.4 WINS

No WINS Servers will be configured or running in the Sansco.int Domain. It was determined there were no legacy apps requiring the WINS service to function correctly.

1.2.5 OU

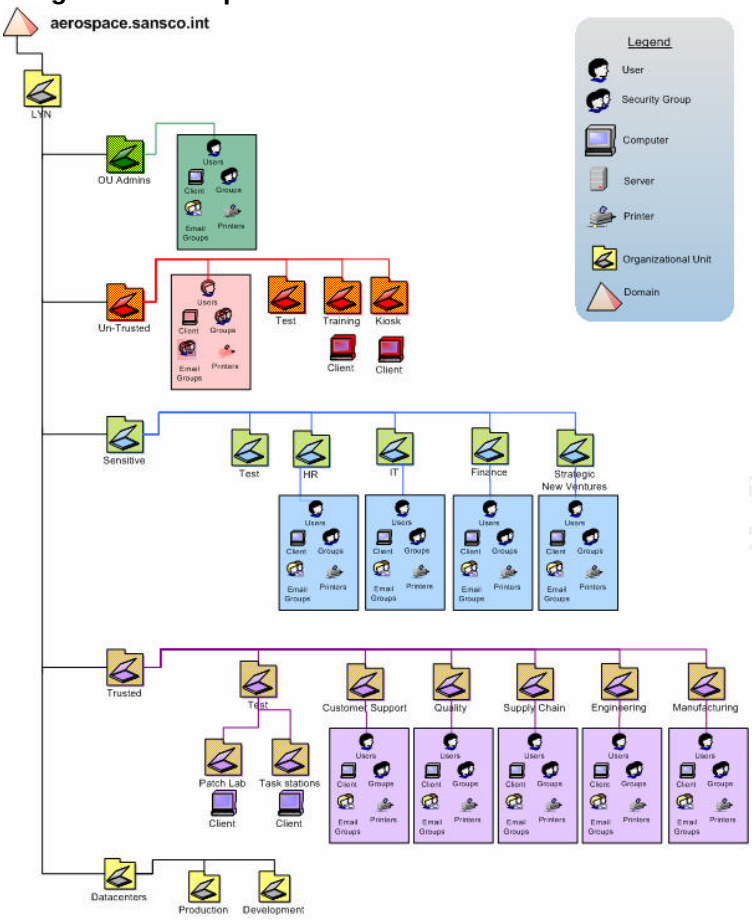
Organizational Units, though not a requirement for AD, aid in the management and structuring of your policies. The default containers: Builtin, Computers, and Users will not have any GPOs assigned to them. SANS Co policy dictates that any new users or computers added to the Domain will be moved into the appropriate OU for which they belong. Using the command line tool *netdom* you can actually add computers directly into the OU of your choosing.

When designing the OU structure for SANS Co, a hierarchical model that best reflected each business segment, and then its departmental structure within, was decided upon. The company's organizational charts were very helpful to the administrators doing the initial layout. This design incorporates first; a location based top level OU within each Domain. This OU represents a physical location or campus with multiple facilities and in most cases is synonymous with an Active Directory Site. The location name of this OU could be an airport code or the city name where the site resides. This design choice was done to allow for OU administration at the local site level, since each location has their own IT System Admins group responsible for managing the systems at their location. These site based Admins will be grouped into a location named security group such as LYN – OU Admins, and are delegated full control of their respective OU and all child objects underneath it.

Prior to the SANS Co Active Directory implementation, these Admins did not have WAN links with each other, and ran their own NT 4.0 Empires essentially independent of each other. At first they all wanted their own Domains, but under the iron-fisted guidance of the Corporate Office back at SANS Co, they eventually came around.

Underneath the site location OU, five basic OU buckets are defined. SANS Co refers to these OUs as "Trust Level" buckets. Policies applied to these buckets are representative of the level of trust applied to objects contained in those buckets. The Lynnwood location within the Aerospace Domain will be used for the following graphical example, since it is the largest location in sheer number of users, within all of Sansco.int.

Figure 6: Aerospace.Sansco.int OU structure



I. OU Admins - This will hold certain accounts and machines from the IT department. These will be the Microsoft Systems Administrators. They will have the ability to make changes within this site. OU Admins will be delegated permission to have full control over all the other OUs within the site. This OU is to remain small to ease auditing.

II. UnTrusted – Consultants, contractors, and other such undesirables (j/k you consultant types) will be placed in this bucket where strict GPOs will be in place. Training room computers and accounts as well as walk-up KIOSK Internet terminals will also belong here. This OU, along with the rest at this level, will contain a “Test” OU whereby new GPOs developed, will be applied and tested to objects in this OU. Objects will be moved in and out of the Test OU as required.

III. Sensitive – Users and systems requiring a higher level of audit, and stricter policies than that of a regular user will be placed in this bucket. The Lynnwood location has decided to put HR, Finance, and the “rest” of IT in here , among others. Some polices such as requiring 802.1X authentication for network access could be supported by machine certificate policies configured in some of these

buckets. Finance and HR may need to have an IPSEC policy for secured communications with their own file servers.

IV. Trusted – The average user and his systems are here. Standard security polices and GPOs are applied. One note of interest is the Patch Lab OU. SANS Co utilizes Microsoft Software Update Services (SUS) with Microsoft Systems Management Server (SMS) to deploy security patches to the desktop. This Patch Lab OU will be used for OS and application testing of security patches prior to generalized deployment.

V. Data Centers – Servers, both development and production are seen as having special needs, each in their own way. Security and other policies will need to be evaluated individually for each server on a case-by-case basis. For instance, a Print Server may have vastly different polices than a file server or a DHCP server. Putting these servers in their own OU bucket will help isolate them from general policies, and simplify the task of auditing them.

The OU design laid out here is used as a template for all Domains in the SANS Co Forest. Under these required OUs buckets, the OU departmental names are can be altered to fit the particular needs of the site or Business.

1.2.6 TRUSTS

Sansco.int is the Root Domain in the SANS Co Active Directory. New Domains joining the Sansco.int Domain are child Domains within the Sansco.int Tree. These child Domains are automatically linked via transitive two-way trusts. In the Microsoft Management Services Glossary, Microsoft states:

> Domains that share a common root share a contiguous namespace. Domains in a tree are joined together through two-way, transitive trust relationships. These trust relationships are two-way and transitive; therefore, a Domain joining a tree immediately has trust relationships established with every Domain in the tree.[17]

1.2.7 PKI

PKI or Public Key Infrastructure, can aid in providing better network security, logon procedures and securing of email among others. RSA Laboratories asks the question: What is a PKI?

> A public-key infrastructure (PKI) consists of protocols, services, and standards supporting applications of public-key cryptography. The term PKI, which is relatively recent, is defined variously in current literature. PKI sometimes refers simply to a trust hierarchy based on public-key certificates [1], and in other contexts embraces encryption and digital signature services provided to end-user

[17] Microsoft Corporation. "Management Services Glossary."
URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/glossary.asp#d (12 January 2004).

applications as well [OG99]. A middle view is that a PKI includes services and protocols for managing public keys, often through the use of Certification Authority (CA) and Registration Authority (RA) components, but not necessarily for performing cryptographic operations with the keys.[18]

SANS Co needed to develop a managed PKI solution. Previously, rogue Certificate Authorities had sprung-up within the various organizations within the SANS Co umbrella. These CAs were used to generate Server signing certificates for secure intranet applications, secure email, and for securing some wireless networks via EAP and 802.1X. The problem was that if an employee traveled from one site to another, he or she might not have the appropriate Trusted Root CA installed, and applications would either throw up warnings, or not function correctly or at all.

Considering the current mess, SANS Co wanted to start over with PKI for their organization. They had a need to issue personal certificates for electronic signing of internal documents, as well as to issue Smart Cards to some employees in the Aerospace and Nuclear Domains where security was a big concern. Using certificates for the application of encrypting data using the Encrypting File System[19], or EFS was also an appealing use of the technology.

SANS Co decided to create an Enterprise CA. Every CA Server will run Windows 2003 Server. This would entail creating four intermediate signing certificates to issue to Intermediate issuing CAs – one for the Corporate Office, and one for each Domain. These CAs create a chain of trust. After these certificates were issued, the Stand Alone Root CA was shutdown and backed-up. Its Hard Disks were also removed and sent to an off-site storage facility. The back-ups were also sent offsite, but to a different secured location – just in case. The Root CA was configured with a ten year lifespan. This is considered more than adequate due to technology lifecycles.

The location of Certificate Revocation List (CRL), and the Certificate Distribution Point (CDP) is re-directed to a SANS Co Intranet Web Server. The DSSTORE utility is used to publish the TRC to the AD.

Figure 7: Syntax used for publishing the certificate to the AD
dsstore.exe DC=sansco,DC=int –addroot sanscorca.crt "SANS Co Trusted Root CA"

This information is then replicated to Active Directory, and the subordinate CAs are ready to be created.

[18] RSA Laboratories. "What is a PKI?." Cryptography FAQ.URL: http://www.rsasecurity.com/rsalabs/faq/4-1-3-1.html (17 January 2004).
[19] Microsoft Corporation. "Components of EFS." Microsoft Windows XP Professional Resource Kit, Chapter 17. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prnb_efs_jjvx.asp (18 January 2004).

Each Domain could now issue certificates as it saw fit, to the users in its own Domain via auto-enrollment or else wise. In addition to re-deploying new certificates to applications under the older PKI, the new SANS Co PKI is used to secure and encrypt the Intranet based time and attendance application, providing the server signing certificate, as well as client authentication certificates.

1.2.8 SANSCO.COM WEB FARM OVERVIEW

After careful consideration, SANS Co decided that the only way to truly have a security boundary between itself and its Servers that reside in the Private DMZ (which are systems that allow connections directly from the Public Network), was to put them into their own Active Directory Forest. Certainly, they could run these systems without being in a Domain at all, however for more seamless administration, and to take advantage of the management capabilities of Active Directory services, the Sansco.com Active Directory Forest was created.

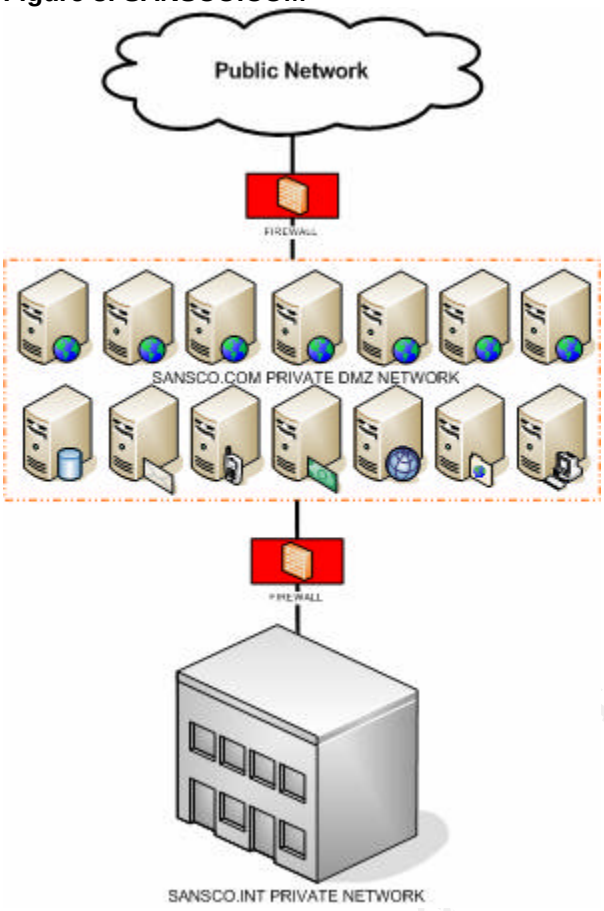
Inside the WEB Farm, sit all the systems providing externally facing services. These include corporate informational websites for each division of SANS Co., the SMTP gateways that act as virus and spam filters and protect the Exchange email systems that reside in the SANS Co private network from direct connections. They also house a WEB based collaboration site for project management with remote locations, an application portal for SANS Co suppliers into their ERP systems, mobile information servers for PDA and Blackberry users, and WEB enabled email servers. These systems are all integral to SANS Co for providing customers, suppliers and employees with vital information. Microsoft SQL Server, Oracle, and eRoom, are among the technologies used to implement these services.

1.2.8.0 NETWORKING

The SANS Co WEB Farm lives in its own network segment, but is physically located at the SANS Co corporate headquarters. This network is in the private IP space[20], and completely separated from any other IP networks at SANS Co. The WEB Farm sits sandwiched between firewalls. The rulesets on these firewalls are quite different. The externally facing one's job is to protect the Servers themselves from intruders on the public network, while still allowing them to provide their essential function to customers, suppliers, and employees. At the same time, the internally facing firewall needs to protect the SANS Co network from intrusions or compromises to these more vulnerable systems, while still providing administrative and development access.

[20] Y. Rekhter., B. Moskowitz., D. Karrenberg., G. J. de Groot., E. Lear. "RFC 1918 - Address Allocation for Private Internets." February 1996. URL: http://www.faqs.org/rfcs/rfc1918.html (20 January 2004).

Figure 8: SANSCO.COM



1.2.8.0.0 DNS

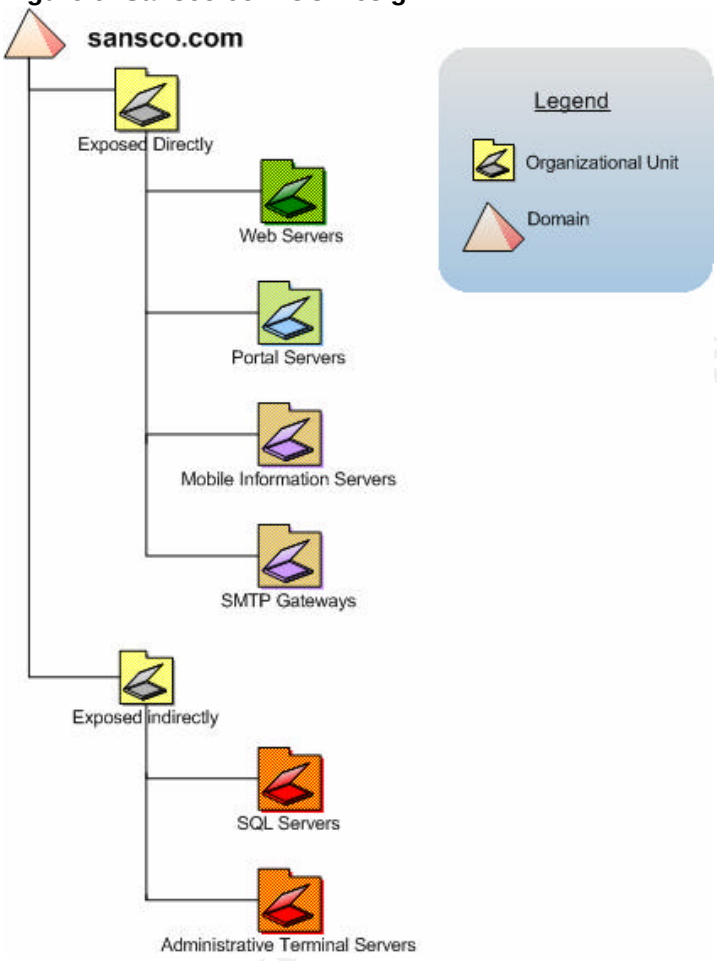
Since Sansco.com is an Active Directory enabled Domain, it of course uses DNS, but this DNS namespace is only for the private use of the Domain, and no inbound DNS requests are allowed via firewall policy. Port 53 is denied for all inbound requests. The publicly registered addresses of the externally facing systems are handled by the Internet Service Provider (ISP). This was seen as an advantage, both from a security and management standpoint. Since DNS changes such as adding or changing A, CNAME, or MX records for systems publicly accessible is done infrequently, letting the ISP handle those DNS records was deemed better than opening up a DNS server for inbound queries. The ISP already has an advanced and secure DNS infrastructure, and SLAs were provided to guarantee accuracy and uptime.

1.2.8.1 OU

The OU structure defined in the WEB Farm is quite different, and less complex than the one created for Sansco.int. OU buckets at the top level are defined by level of exposure. Those systems accessed directly through firewall rules are placed in the Exposed Directly OU. Systems that are access indirectly, such as a SQL server that provides data for a dynamic website, are placed in the OU Exposed Indirectly. These systems

are not exposed via firewall ruleset, but are access from systems that are. Underneath these are buckets defined around common types of servers in the WEB Farm to take advantage of common baseline policies.

Figure 9: Sansco.com OU Design



1.2.8.2 TRUSTS

In order to simplify management Sansco.com, an external trust was created. This Trust is one-way, with Sansco.com trusting Sansco.int, but not the other way around. This is by design. If a machine in the Sansco.com Domain was compromised, this configuration makes it more difficult for a would-be attacker to gain access into the Sansco.int corporate network. By default, when a Windows 2003 DC creates an external Trust such as has been created here, SID Filtering is enabled.

SID Filtering is an important part of securing your Domain against malicious users who have administrative privileges. Because of a feature called SID History[21], (one that

[21] Microsoft Corporation. "Using SID History to Preserve Resource Access." Windows Server 2003 Deployment Kit. URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dssbi_reer_qdhe.asp (January 24 2004).

administrators take legitimate advantage of when migrating users from one domain to another to simplify administration of access to resources) malicious administrators could setup a packet sniffer on the network to sniff the SID of administrative users during an authentication request in the trusting Domain. This evil Admin could then add the SID of this high-level user to the SIDHistory attribute of his (or another's) account, in order to surreptitiously gain full access to the trusting Domain. SID Filtering combats this by removing the SIDs from any authentication attempts where said SID is not of the trusted domain. Microsoft Security Bulletin MS02-001[22] details this exploit.

1.2.8.3 PKI

Because all the systems in the SANS Co WEB Farm are for access from the public network, it was decided that PKI would come from external sources that were more widely trusted. Because SANS Co doesn't discriminate where they spend their money, they choose the VeriSign Corporation to issue them their server signing certificates for SSL encryption on their secure WEB applications.

1.3 GIAC Corp OVERVIEW

When GIAC Enterprises implemented Active Directory, they were running on the Windows 2000 Server platform. This worked well for GIAC Enterprises, since GIAC has only a single site, and a single Domain called corp.giac.com for the corporate network.

GIAC has a similar OU structure to the one defined in the SANS Co Active Directory. GIAC also has a WEB Farm, running their internet presence. This is also based on WINDOWS 2000 Server.

In order to better facilitate management of the GIAC, since they no longer have any internal IT support, an infrastructure team from SANS Co flew down to GIAC, and upgraded the Domain from Windows 2000, to Windows 2003 Server. Forest and Domain functional levels were also set to the 2003 level, as is the case with the Sansco Domain. This was done in order to take advantage of the forest trust capabilities of this product, allowing for cross forest authentication and authorization. These capabilities allow for users perhaps visiting from the Sansco Domain, to login their own Domain while at GIAC. This also facilitates the sharing of resources between the sites, allowing for SANS Co users to give GIAC Enterprises users access to common files and resources in the their Domain, and visa-versa.

1.4 SANS Co and GIAC Corp TRUST

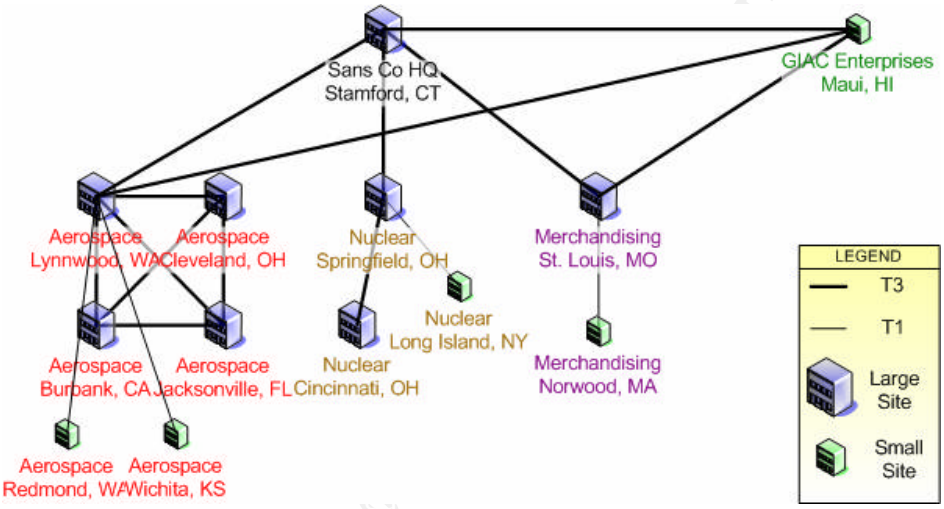
Before the Forest trust can be established, physical connectivity needs to be in place. SANS Co decided to use the technology they were already familiar with to accomplish this. GAIC Enterprises already has ample bandwidth to support a VPN connection, so a Watchguard V60 IPSEC VPN end-point router solution was put into place. A high-

[22] Microsoft Corporation. "Microsoft Security Bulletin MS02-001." Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data. 09 MAY 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS02-001.asp (February 02 2004).

availability pair of these IPSEC routers was configured as defined in section 1.1.0 Figure 4.

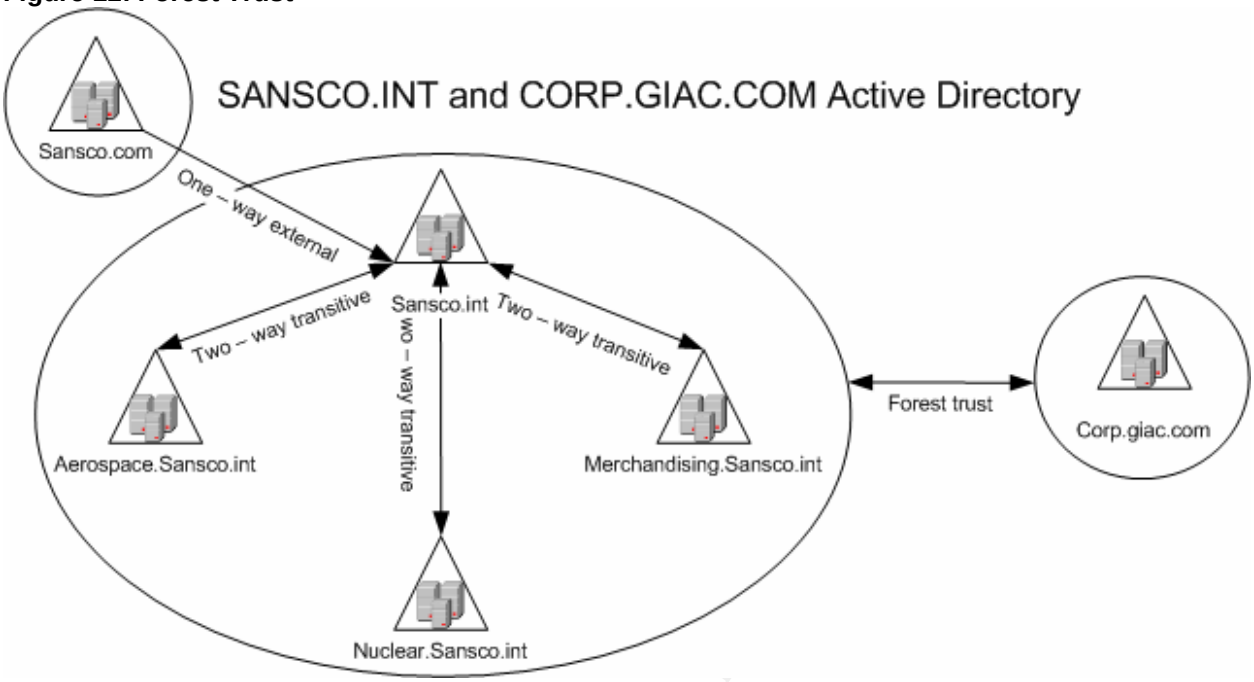
The IPSEC VPN routers at GIAC Enterprises will participate in the SANS Co VPN mesh, with the exception of the SANS Co Nuclear division. No IP routes will be defined for the Nuclear division network at the GIAC site, nor will any IPSEC peers be defined in the VPN policy on the routers, effectively cutting of network access at the IP layer from GIAC to Nuclear. The Nuclear site will also not contain any routing table information for the GIAC Enterprises Network.

Figure 10: SANCO and GIAC VPN MESH



With the GIAC Enterprises Active Directory running at the highest functional levels, the Forest Trust is ready to be created.

Figure 11: Forest Trust



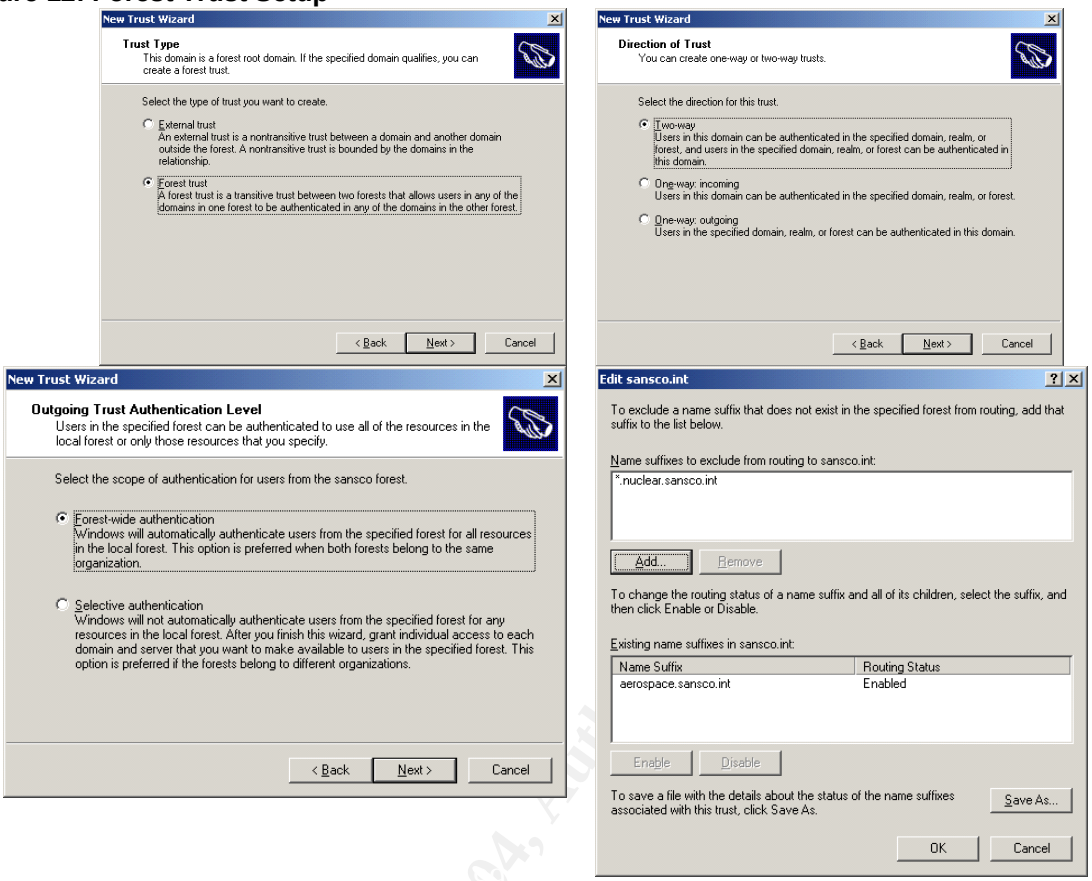
A Windows 2003 forest trust is created between the Domains Sansco.int and corp.giac.com. This is a two-way trust, allowing users from either Domain to be authenticated in each others Domains. Forest trusts can also be setup to work unidirectional, like an external trust. This direction can be specified as incoming or outgoing.

The Outgoing trust authentication level is set to Forest-wide authentication. Since SANS Co and GIAC have merged, they are now under a single management umbrella, and can be considered a single organization – from a trust standpoint. This choice was seen as the best option to alleviate a lot of up-front work with the other authentication option: Selective authentication. This method requires ACLs be set for every individual requiring access to every resource in the other Domain.

Because the forest trust is transitive, users in the corp.giac.com Domain would also be able to access resources in the child Domains within Sansco.int. This is fine, with the exception of the Nuclear Domain. SANS Co did no want anyone within GIAC Enterprises to access the Nuclear Domain, so a name suffix exclusion was added[23]. This prevents name lookups to route to the Nuclear Domain.

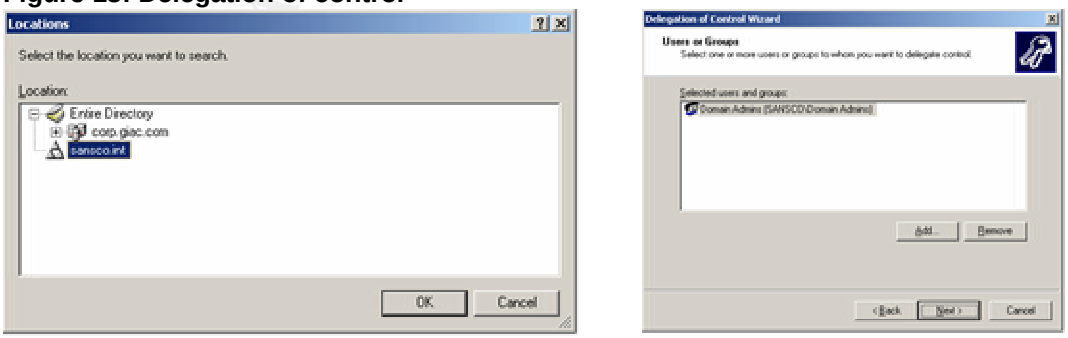
[23]Microsoft Corporation. "To exclude name suffixes from routing to a local forest." Windows Server 2003 Product Documentation. URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/x_routename.asp (20 January 2004).

Figure 12: Forest Trust Setup



The Domain Administrators from the Sansco.int Domain are delegated control over managing the corp.giac.com Domain. The first order of business is to create the same top-level OU buckets for the GIAC AD, as defined in section 1.2.5 OU. The Domain Admins will work with the GIAC management to define which departments needed to move into which buckets.

Figure 13: Delegation of control



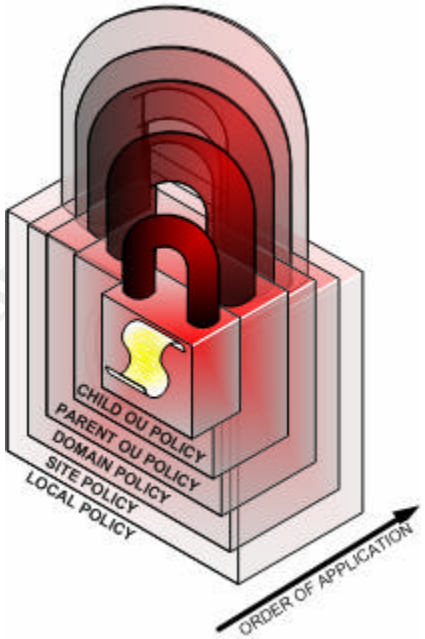
Now that the connectivity has been established and the trust is created, SANS Co and GIAC Enterprises can begin sharing system resources. The Admins at SANS Co can start to create the GPOs for the GIAC OUs and get the GIAC policies in line with the SANS Co standards.

2 SECURITY POLICY

If you want to be able to simplify deployment of common settings to your Active Directory clients, Group Policy is a necessary component. Group Policy can enable an Administrator to specify which security settings a system will inherit, or what software is made available to a user. SANS Co and GIAC Enterprises use Group Policy Objects (GPOs) to designate security and settings for computers and users in a Site, Domain, and OU. Broad polices are site at the highest levels, and increasingly more specific policies are set at the OU level. These GPOs could be different for each OU as required by the objects contained in that OU. For example, the desktop settings for the “OU Admins” group OU in the “Lynnwood OU” of the Aerospace Domain, will be much less stringent than that of the “Manufacturing Group” OU in the “Trusted OU” of the same Domain. In this way, GPO deployment can be simplified by applying these policies to systems and users with like requirements.

GPOs can be applied at many different levels. Managing and keeping track of which GPOs settings are the ones to be applied can be difficult and confusing if multiple GPOs are applied to the same object at multiple levels. Figure 14 shows the order of application for GPOs.

Figure 14: GROUP POLICY APPLICATION ORDER



The innermost layer is the last GPO to be applied. The exception to this rule would come through the followings settings: Block Inheritance, and No Override. Block Inheritance means that any parent containers are blocked from applying their GPOs to the object (and all child objects) where this is set. No Override is actually a property of the Link object, and not that of the GPO itself. By setting No Override on the Link to the

container where the GPO is applied, you are enforcing the settings in this policy to all nested objects, even if there is a conflicting setting from a child GPO. No Override will be used by SANS Co on the Default Domain GPO, and on GPOs that contain the common security settings for all buckets referred to as “Trust Level” buckets; See section 1.2.5 OU, Figure 6. These Trust level buckets should not have their more specific settings overwritten by higher-level OU GPOs, or by the default Domain or Site GPOs.

2.0 SANS Co and GIAC GPO

SANS Co has implemented baseline GPOs to secure its Domains. SANS Co and GIAC Enterprises will use the same Domain level GPO. Sansco.int child Domains are permitted to use different Domain level GPOs as are required by the different business segments. Sansco.com will use its own unique Domain GPO do to the nature of the Domain being exposed directly to the internet.

In each case, the default Domain Policy is left in place, set with a lower priority, and then disabled. This is done in case a problem is discovered with the new Domain Policy, the default can easily be restored. SANS Co and GIAC will not use GPOs linked to the Active Directory Site object. The Domain Policy used by aerospace.sansco.int is used as the example GPO.

2.0.0 DOMAIN GPO

Since each Domain under Sansco.int is managed by it’s own IT group, the Domain GPO will vary. This section will cover the Domain GPO for the aerospace.sansco.int Domain.

The new Domain GPO will not have extensive modification over the default Domain GPO. Only where a security baseline needs to be set, will any settings be applied. This will allow the Administrators that manage their sites from the OU level to best apply the settings appropriate for their site. The exception to this is the Account policy. Account polices which include Kerberos, lockout, and password polices are set at the Domain level, so these were agreed upon by the Aerospace administrators, and will be applied as listed in the tables below:

Figure 15: Domain Account Policies – Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	2 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Enforce password history was left at the default of twenty-four passwords remembered. This setting ensures that users will not be able to reuse the same passwords too often. When used in conjunction with the Minimum password age setting of two days, a user in the aerospace Domain would not be able to reuse a password for forty-eight days.

Maximum password age was bumped-up to ninety days. This was done to coincide with other existing application password policies inside SANS Co. The business systems have long been set with a ninety day expiration, and it was deemed that this was the shortest amount of time acceptable to the users. Any more frequent changing of passwords had shown to lead to bad practices such as the posting of passwords underneath keyboards and on monitors.

Minimum password length was set at eight characters. This was deemed long enough when combined with complexity requirements. Complexity requirements enforce the following:

- No part of the account name is used in the password, and that the password meets three out of four of the following requirements:
  - Upper case characters (A – Z).
  - Lower case characters (a – z).
  - Numbers (0 – 9).
  - Special characters (! • Ü •, for example.).

Store passwords using reversible encryption will not be allowed, and disable in the Default Domain policy for Aerospace. One would enable this when needing to authenticate with the old CHAP over RAS or using Digest authentication with IIS.

Figure 16: Domain Account Policies – Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout after	30 minutes

The account lockout policy was a source of much debate amongst the Aerospace Administrators. Trying to balance protection and supportability while preventing Denial of Service attacks against your Domain accounts can be difficult to manage. The settings agreed upon in Figure 16 seemed to support a symmetry of protection and supportability. Too stringent of a policy can drastically drive up support and cause serious problems due to denial of service type attacks, while to loose of a policy would provide opportunity for malicious users to access unauthorized accounts.

Account lockout duration and Reset both set to thirty minutes, seemed sufficient enough to deter crackers using brute-force methods. When combined with allowing for only five invalid logon attempts, any attempts to login with five or more bad passwords could be construed as a real attack on an account. Good auditing and alerting practices should notify administrators of such a situation. Typically, a problem such as having the caps-

lock key on, or a bout of Monday morning forgetfulness, is resolved in less than five attempts.

Figure 17: Domain Account Policies – Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	480 minutes
Maximum lifetime for user ticket	480 minutes
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 days

Kerberos is the authentication mechanism used in the SANS Co and GIAC Active Directory. Kerberos provides a secure method for authentication and authorization of resources in the Domain.

Enforcing user logon restrictions ensures that the user account attempting to logon has not been deleted or disabled, and also has the appropriate rights to logon to resource for which it is requesting access. This is enabled.

By setting a maximum lifetime for service tickets, you are enforcing that a new ticket exchange happens for any new connection requests to a server after the time defined within the policy setting has expired. This is set to eight hours. The maximum lifetime for user tickets refers to the Ticket Granting Ticket (TGT). The TGT is what the client presents to the Ticket Granting Service (TGS) in order to be able to receive session tickets to other servers.[24] This is also set to eight hours. The maximum lifetime for a user to renew their ticket is defined as the maximum time allowed to renew any session ticket. Once this time has passed, a new ticket must be exchanged. This is left at the default setting of seven days.

In Active Directory, computers clocks need to be synchronized. Setting a maximum tolerance for a difference between the client and the KDC will help limit the effectiveness of replay attacks against the KDC[25]. This was kept at the default setting of five minutes.

Any other policies and settings applied will be done through the appropriate OU or builtin container GPOs.

2.0.1 OU GPO

This section will focus on the settings and configuration of a GPO applied to an OU in the Lynnwood site OU of the aerospace.sansco.int Domain. See section 1.2.5 Figure 6 for the Aerospace Domain - Lynnwood Site - OU design. This OU is under the

[24] Fossen, Jason. “Kerberos and NTLMv2.” Active Directory. SANS Institute. May 2000. 38-39, 43.
[25] Haney, J. “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set.” National Security Agency Security Recommendation Guides. 03 December 2002. URL: http://nsa2.www.conxion.com/win2k/guides/w2k-3.pdf (02 February 2004)

"UnTrusted" bucket, and is labeled "Training". This Training OU contains both machines and user accounts. This OU was created around the company's various training rooms. These training rooms are used by groups within the organization to hold in-house training sessions on the use and function of various applications that are deployed within the organization. These training rooms are not physically secured, and are used by any number of different individuals in the company. The training rooms are however placed on their own LAN segment.

These training rooms are seen as high-risk environments due to the following factors: Applications are continuously installed and uninstalled; the usernames and passwords of the training room accounts are actually posted right on the monitors of the training room computers! These computers still need access to the test and/or development versions of the company's business applications, however due to the fact that the login information is readily accessible, a new security group was created for these training room user accounts.

The global security group created is called: LYN – Training Users. This group is not a member of any other groups, including the AEROSPACE\Domain Users builtin group, to aid in controlling access to resources. The GPO for this OU will have to be created to function within the requirements for providing training, while still keeping the network safe from malicious users who could simply walk-up to a training room computer and login using the information posted right on the monitor. It should be noted that the local Administrators protested this blatant breech of standard security practices.

2.0.1.0 SECURITY POLICY

The Microsoft policy template hisecws.inf, version 05.10.HW.0000 was used as a baseline for this security policy. This template was then modified to fit the requirements of the training room computers and users. The template was imported in to the GPO assigned to the OU. The notable differences between the default Microsoft policy and the modified policy are illustrated as follows.

Software installation needs to be managed on these training rooms systems. Software is installed and uninstalled continually on these computers to support training and functionality testing of newly published or soon to be published applications. The default package location is set to a common folder on a file server where these application packages are staged for installation.

Startup and shutdown scripts to do not vary from the standard startup and shutdown scripts applied to typical Domain computers.

Account polices are set at the Domain Level. Local polices are enforced. Since the number of settings to configure through GPO can number in the thousands, only the more interesting ones are listed in the following table. Descriptions of many of these settings have been explained in the previous GPO example.

Figure 18: Training Rooms GPO - Local Polices

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit system events	Success, Failure
Access this computer from the network	Administrators, AEROSPACE\LYN – Training Users
Allow logon locally	Administrators, AEROSPACE\LYN – Training Users
Deny logon locally	Aerospace\Domain Users
Audit: Shutdown the system immediately if unable log security audits	Enabled
Domain member: Require strong session key	Enabled
Network security: Force logoff when logon hours expire	Enabled

Training Rooms GPO – Event Log

Maximum security log size	65536 kilobytes
Retain security log	30 days
Restricted groups	Administrators

Training Rooms GPO – System Services

Alerter	Disabled
Application Layer Gateway Service	Disabled
Automatic Updates	Disabled
DNS Server	Disabled
Internet Connection Firewall	Disabled
NetMeeting Remote Desktop Sharing	Disabled
Routing and Remote Access	Disabled
Telnet	Disabled
Terminal Services	Disabled

Training Rooms GPO – Administrative Templates – Windows Components – Internet Explorer

Security Zones: Do not allow users to change policies	Enabled
Security Zones: Do not allow users to add/delete sites	Enabled

Training Rooms GPO – Administrative Templates – Windows Components – IIS

Prevent IIS installation	Enabled

Training Rooms GPO – Administrative Templates – Windows Components – Task Scheduler

Prohibit new task creation	Enabled
Prohibit task deletion	Enabled

Training Rooms GPO – Administrative Templates – Windows Components – Windows Installer

Always install with elevated privileges	Enabled
Enable user control over installs	Disabled
Logging	Enabled
Prohibit user installs	Enabled

Training Rooms GPO – Administrative Templates – System - Scripts

Run logon scripts synchronously	Enabled
Maximum wait time for Group Policy scripts	Enabled, 120 Seconds

Training Rooms GPO - User Configuration - Administrative Templates – Network

Prohibit access to properties of a LAN connection	Enabled
Enable Windows 2000 Network Connections settings for Administrators	Enabled

Training Rooms GPO - User Configuration - Administrative Templates – System

Prevent access to registry editing tools	Enabled

The goal of this policy is to tightly control the access that this untrusted user has to both the computer and the Domain. This policy needs to limit the ability of the user to change critical settings on the computer while still providing means to access training resources without impacting functionality.

2.1 SANSCO.COM WEB SERVERS GPO

Sansco.com runs multiple IIS servers. Although the Sansco.com AD is running Windows 2003 Domain Controllers, the IIS servers are still running Windows 2000 and IIS 5.0. Windows 20003 with IIS 6 provides a more secure and stable platform, and Sansco.com plans on upgrading their IIS servers as time allows and applications are officially supported. The IIS systems here serve up sites that range from simple static pages for informational purposes, to IIS servers running 3rd party applications that allow for secured project collaboration and issue tracking.

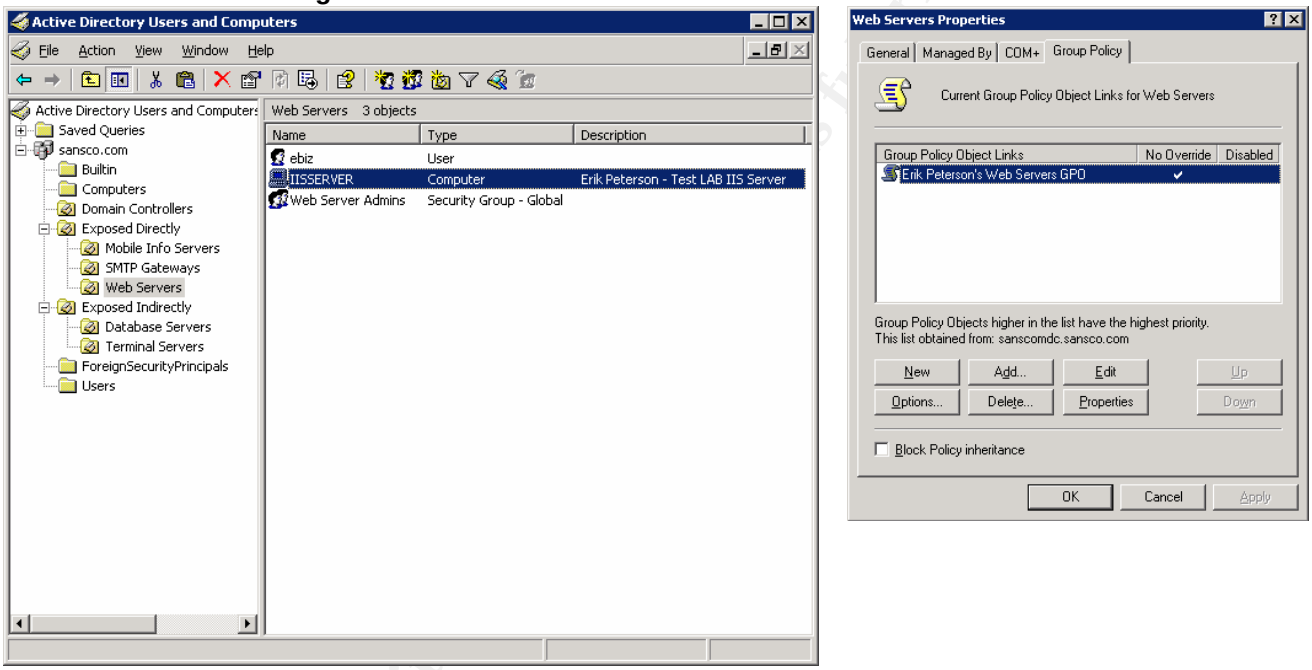
The GPOs applied to the Servers that reside in the Sansco.com AD are different than the typical GPO applied to a typical user's workstation within the Sansco.int Domain. For the most part, these are systems that typically do not run with anyone logged into them locally. These systems also need to be hardened more stringently due to the fact that they are purposely publicly accessible. The security of these systems cannot rely solely on the security settings applied to them through GPO. These WEB servers need to be protected through defense-in-depth at each layer. This starts with the edge routers, extends to the firewalls behind them, and then on to the servers themselves where OS hardening is the first step, prior to any application installation. Microsoft provides some excellent resources and guides for securing IIS. These can be found at the Microsoft TechNet site online, in the Securing IIS 5.0 Resource Guide[26]. The

[26] Microsoft Corporation. "Securing IIS 5.0 Resource Guide." URL: http://www.microsoft.com/technet/security/chklist/iis50srg.asp (02 February 2004).

application and methods for implementing end to end security is in itself a lengthy discussion, and is only noted here that this is acknowledged and implemented at SANS Co.

For the purpose of defining one of the GPOs, the baseline IIS Server GPO will be described. It should be noted that a mostly generic default Domain GPO does exist, and that the last child OU GPO is mostly responsible for securing the resources contained within it. This particular GPO outlined for this exercise is applied at the OU level named "Web Servers", which exists under "Exposed Directly" OU.

Figure 19: Sansco.com IIS Web Servers OU and GPO



We will start with the Windows 2000 resource kit security template: SecureInternetWebServer.inf. This template is then modified using sectemplates.msc to fit the requirements of these systems. Only the modifications and more important settings are listed in the tables below.

Figure 20: Sansco.com IIS Web Server Security Template – Account Policies – Password Policy

Policy	Setting
Enforce password history	12 passwords remembered
Maximum password age	30 days
Minimum password age	1 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Password stored using reversible encryption	Enabled

These settings require a strong password with a twelve character minimum, and require that the password be changed every thirty days. Although security is loosened, passwords will need to be stored using reversible encryption to support Digest Authentication on the OWA web server.

Sansco.com IIS Web Server Security Template – Local Policies – Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit policy change	Success, Failure
Audit system events	Success, Failure

We want to track all logon events, and also want to know when any account or policy is added, removed or changed. By auditing system events, we will know when the system is shutdown or restarted, or when the security log has filled up.

Sansco.com IIS Web Server Security Template – Local Policies – User Rights Assignment

Access this computer from the network	Everyone
Allow logon locally	Administrators, Web Server Admins
Back up files and directories	Administrators, Backup Operators
Force shutdown from a remote system	Administrators, Web Server Admins
Take ownership of files or other objects	Administrators

Sansco.com IIS Web Server Security Template – Local Policies – Security Options

Accounts: Guest account status	Disabled
Audit: Audit the use of Backup and Restore privilege	Enabled
Audit: Shut down system immediately if unable to log security audits	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Interactive logon: Message text for users attempting to log on	This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring.
Interactive logon: Message title for users attempting to log on	SANS CORPORATION - AUTHORIZED USERS ONLY
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM
Shutdown: Clear virtual memory pagefile	Enabled

Sansco.com IIS Web Server Security Template – Computer Configuration – Administrative Tem…	
Turn off Autoplay	Enabled, All Drives

Although these Servers are physically access controlled behind a locked server room with mag-readers, extra measures should still be taken to audit and limit access through means that could more easily be compromised. Restricting network access to removable drives could aid in this by helping to prevent a rogue administrator or other malicious person from placing unwanted or dangerous software in a removable drive, to be remotely executed at a later time.

We do not want unprivileged users to be able to get a list of users or shares on any of these systems, so "Do not allow anonymous enumeration of SAM accounts and shares" is enabled to prevent this.

Adding banner text is an important legal requirement[27], especially for machines exposed to external untrusted users. Lack of any logon banner, or worse, a banner welcoming users to your system could hinder any attempts to prosecute intruders.

Sansco.com IIS Web Server Security Template – Local Policies – Event Log	
Maximum application log size	524288 kilobytes
Maximum security log size	524288 kilobytes
Maximum system log size	524288 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	7 days
Retain security log	7 days
Retain system log	7 days

All systems in the "Exposed Directly" OU have incremental backups done every night. These systems also all have their event logs centralized on a log consolidation server. The log file sizes were set to 512MB since disk space is not a concern. Seven day retention of logs keeps local copies around longer, to be able to more quickly troubleshoot issues.

Sansco.com IIS Web Server Security Template – Local Policies – Restricted Groups
Administrators, Web Server Admins

Restricted Groups is a feature that allows you to enforce who should be members of sensitive groups. The Administrators group, Domain Admins group, and the Web Server Admins group all are configured as restricted groups, and have their membership explicitly defined.

[27] Rohrer, Mark. "Neohapsis Archives." 23 March 2002.
URL: http://archives.neohapsis.com/archives/incidents/2002-03/0117.html (03 February 2004).

Sansco.com IIS Web Server Security Template – System Services

Service Name	Startup
Alerter	Disabled
ClipBook	Disabled
DNS Server	Disabled
Indexing Service	Disabled
Irmon	Disabled
Messenger	Disabled
NetMeeting Remote Desktop Sharing	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
TCP/IP NetBIOS Helper	Disabled
Telnet	Disabled
Terminal Services	Disabled

The above listed services are all either unnecessary for running the Sansco.com IIS servers or can be deemed a security risk, so they have all been disabled.

It should also be noted that the SecureInternetWebServer.inf template secures access to numerous sensitive registry keys and system files.

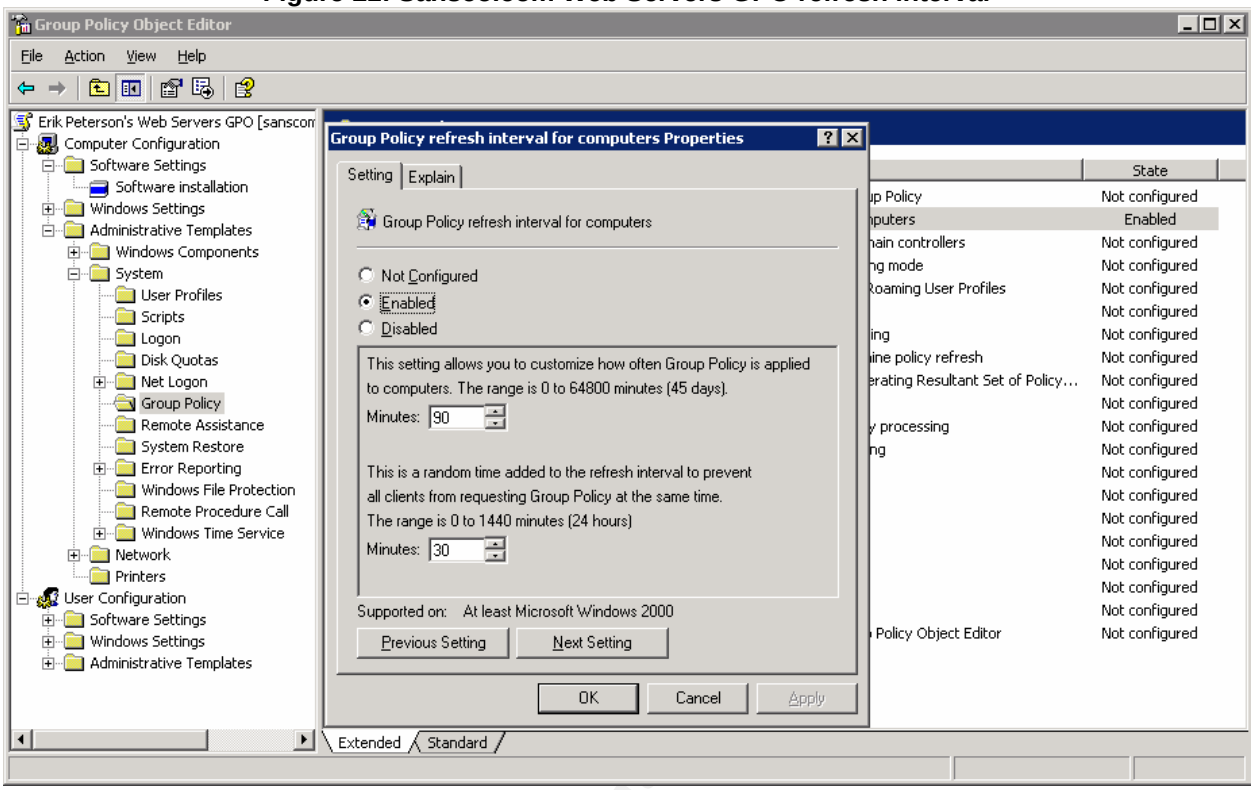
The finished template is now imported into the GPO for the “WEB Servers” OU in the Sansco.com Domain. The Web Servers GPO is set to “no override”.

2.2 POLICY APPLICATION and MAINTENANCE

The “Web Servers” OU has its administration delegated to the Web Server Admins group for continued management of the OU and GPOs linked to it.

The refresh interval for this GPO is set to every 90 minutes with a 30 minute offset. This is often enough considering this GPO will not change much once it is in place.

Figure 21: Sansco.com Web Servers GPO refresh interval



In order to force a refresh on the IIS server used for testing, the command line utility *secedit* was run. We will run this with the */refreshpolicy* {user_policy and machine_policy} */enforce* switches to force an update on our system.

The Windows 2000 resource kit utility *gpresult* was then run to validate that the policy truly had been applied. This shows which GPOs were applied to the local system and logged-in user, and when.

Figure 22: gpresult output

```
Microsoft (R) Windows (R) 2000 Operating System Group Policy Result tool
Copyright (C) Microsoft Corp. 1981-1999


Created on Tuesday, February 10, 2004 at 7:43:45 PM


Operating System Information:

Operating System Type:          Server
Operating System Version:       5.0.2195.Service Pack 4
Terminal Server Mode:           Remote Administration

#############################################################

  User Group Policy results for:

  CN=ebiz,OU=Web Servers,OU=Exposed Directly,DC=sansco,DC=com

  Domain Name:          SANSCOCOM
  Domain Type:          Windows 2000
  Site Name:            SANSCOCOM
```

```
  Roaming profile:      (None)
  Local profile:        C:\Documents and Settings\ebiz.SANSCOCOM

  The user is a member of the following security groups:

        \Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        NT AUTHORITY\Authenticated Users
        \LOCAL

###################################################################

Last time Group Policy was applied: Tuesday, February 10, 2004 at 7:42:07 PM

###################################################################

  Computer Group Policy results for:

  CN=IISSERVER,OU=Web Servers,OU=Exposed Directly,DC=sansco,DC=com

  Domain Name:          SANSCOCOM
  Domain Type:          Windows 2000
  Site Name:            SANSCOCOM


  The computer is a member of the following security groups:

        BUILTIN\Administrators
        \Everyone
        BUILTIN\Users
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users

###################################################################

Last time Group Policy was applied: Tuesday, February 10, 2004 at 7:27:59 PM
Group Policy was applied from: sanscomdc.sansco.com
=====================================================================

The computer received "Registry" settings from these GPOs:

        Local Group Policy
        Default Domain Policy
        Erik Peterson's Web Servers GPO
=====================================================================

The computer received "Security" settings from these GPOs:

        Default Domain Policy
        Erik Peterson's Web Servers GPO
=====================================================================

The computer received "EFS recovery" settings from these GPOs:

        Local Group Policy
        Default Domain Policy
```

Another way to get detailed information regarding the application of group policy is to enable verbose logging of the user environment[28]. We will enable verbose logging by adding a new DWORD value to the following registry key:

Figure 23: Enable User Environment Debug Logging
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

[28] Microsoft Corporation. "How to Enable User Environment Debug Logging in Retail Builds of Windows." 23 September 2003. URL: http://support.microsoft.com/default.aspx?scid=kb:EN-US:221833 (03 February 2004).

New DWORD: *UserEnvDebugLevel*
Value: 10002

A value of 10002 will set the log level to verbose with log file. The output of this file can be found in the directory: %SystemRoot%\Debug\UserMode\ with a filename of userenv.log.

Once a GPO has been created, thoroughly tested, and placed into production, it needs to fall under standard change management controls to provide for maintenance of the GPO. SANS Co has developed production change management policies for both their Infrastructure and Development groups. GPOs, since they are managed primarily by infrastructure staff, will fall into the infrastructure category. These change management polices define procedures that have to be followed in order to implement a change to a production system, or in this case, a production GPO. After being validated in a test environment, the change will need to have a risk and impact assessment done, have a back-out procedure defined, and be authorized by the appropriate management level approver before it can be placed into production.

2.3 POLICY VALIDATION

Something interesting happened when I went to test the results of the GPO being applied to the Member Server, IISSERVER in the "Web Servers" OU. I was getting strange error messages in the userenv.log file, as well as some errors being generated in the application log of the affected machine. These errors seemed to point to a problem accessing the SysVol share on the DC. Oddly enough, *gpresult* did not indicate any problems.

One quick test I did to see if the user policy was being applied was to check the screen saver settings. I had enabled this in the GPO, set it to a time-out of two minutes, and specified logon.scr as the screen saver to use. A quick check once logged in, showed no screen saver set.

Userenv.log repeated a few specific errors during each logon process, and during manual GPO updates using *secedit*. These errors seemed to point to access or permissions problems. Due to the large file size, I have listed only one section for the user and machine policies during the application process, with the interesting errors highlighted.

Figure 24: userenv.log Errors

```
USERENV(270.3d4) 21:05:49:458 ======================================================
USERENV(270.61c) 21:05:49:529 ApplyGroupPolicy: Entering. Flags = 6
USERENV(270.61c) 21:05:49:529 ProcessGPOs:
USERENV(270.61c) 21:05:49:529 ProcessGPOs:
USERENV(270.61c) 21:05:49:529 ProcessGPOs: Starting user Group Policy processing...
USERENV(270.61c) 21:05:49:529 ProcessGPOs:
USERENV(270.61c) 21:05:49:529 ProcessGPOs:
USERENV(270.61c) 21:05:49:529 EnterCriticalPolicySection: User critical section has been claimed.
```

```
Handle = 0x1f0
USERENV(270.61c) 21:05:49:529 ProcessGPOs:  Machine role is 2.
USERENV(270.61c) 21:05:49:529 PingComputer: PingBufferSize set as 2048
USERENV(270.61c) 21:05:49:529 PingComputer:  First time:  0
USERENV(270.61c) 21:05:49:529 PingComputer:  Fast link.  Exiting.
USERENV(270.61c) 21:05:49:529 ProcessGPOs:  User name is:
CN=Administrator,CN=Users,DC=sanscocom,DC=com, Domain name is:  SANSCOCOM
USERENV(270.61c) 21:05:49:529 ProcessGPOs: Domain controller is:  \\sanscomdc.sanscocom.com
Domain DN is sanscocom.com
USERENV(270.61c) 21:05:49:539 MyGetDomainDNSName:  Successfully determined fqdn
CN=Administrator,CN=Users,DC=sanscocom,DC=com
USERENV(270.61c) 21:05:49:539 MyGetDomainDNSName:  Successfully obtained domain dns name
sanscocom.com
USERENV(270.61c) 21:05:49:539 GetOldSidString:  Failed to open profile profile guid key with
error 2
USERENV(270.61c) 21:05:49:539 ProcessGPOs: Calling GetGPOInfo for normal policy mode
USERENV(270.61c) 21:05:49:539 GetGPOInfo:  ********************************
USERENV(270.61c) 21:05:49:539 GetGPOInfo:  Entering...
USERENV(270.61c) 21:05:49:549 GetGPOInfo:  Server connection established.
USERENV(270.61c) 21:05:49:769 GetGPOInfo:  Bound successfully.
USERENV(270.61c) 21:05:49:779 SearchDSObject:  Searching <DC=sanscocom,DC=com>
USERENV(270.61c) 21:05:49:779 SearchDSObject:  Found GPO(s):  <[LDAP://CN={31B2F340-016D-11D2-
945F-00C04FB984F9},CN=Policies,CN=System,DC=sanscocom,DC=com;0]>
USERENV(270.61c) 21:05:49:779 ProcessGPO:  ==============================
USERENV(270.61c) 21:05:49:779 ProcessGPO:  Deferring search for <LDAP://CN={31B2F340-016D-11D2-
945F-00C04FB984F9},CN=Policies,CN=System,DC=sanscocom,DC=com>
USERENV(270.61c) 21:05:49:789 SearchDSObject:  Searching <CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=sanscocom,DC=com>
USERENV(270.61c) 21:05:49:789 SearchDSObject:  No GPO(s) for this object.
USERENV(270.61c) 21:05:49:789 EvaluateDeferredGPOs:  Searching for GPOs in
cn=policies,cn=system,DC=sanscocom,DC=com
USERENV(270.61c) 21:05:49:789 ProcessGPO:  ==============================
USERENV(270.61c) 21:05:49:789 ProcessGPO:  Searching <CN={31B2F340-016D-11D2-945F-
00C04FB984F9},CN=Policies,CN=System,DC=sanscocom,DC=com>
USERENV(270.61c) 21:05:49:799 ProcessGPO:  User has access to this GPO.
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found functionality version of:  2
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found file system path of:
<\\sanscocom.com\sysvol\sanscocom.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}>
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found common name of:  <{31B2F340-016D-11D2-945F-
00C04FB984F9}>
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found display name of:  <Default Domain Policy>
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found user version of:  GPC is 1, GPT is 0
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found flags of:  0
USERENV(270.61c) 21:05:49:799 ProcessGPO:  Found extensions:  [{3060E8D0-7020-11D2-842D-
00C04FA372D4}{3060E8CE-7020-11D2-842D-00C04FA372D4}]
USERENV(270.61c) 21:05:49:799 ProcessGPO:  ==============================
USERENV(270.61c) 21:05:49:799 GetGPOInfo:  GPO Local Group Policy doesn't contain any data since
the version number is 0.  It will be skipped.
USERENV(270.61c) 21:05:49:819 GetGPOInfo:  Leaving with 1
USERENV(270.61c) 21:05:49:819 GetGPOInfo:  ********************************

USERENV(e0.4a4) 10:20:48:624 ProcessGPOs:  Starting computer Group Policy processing...
USERENV(e0.4a4) 10:20:48:624 ProcessGPOs:
USERENV(e0.4a4) 10:20:48:624 ProcessGPOs:
USERENV(e0.4a4) 10:20:48:624 EnterCriticalPolicySection: Machine critical section has been
claimed.  Handle = 0x76c
USERENV(e0.4a4) 10:20:48:624 ProcessGPOs:  Machine role is 2.
USERENV(e0.4a4) 10:20:48:624 PingComputer: PingBufferSize set as 2048
USERENV(e0.4a4) 10:20:48:624 PingComputer:  First time:  0
USERENV(e0.4a4) 10:20:48:624 PingComputer:  Fast link.  Exiting.
USERENV(e0.4a4) 10:20:48:744 ProcessGPOs:  User name is:  CN=IISSERVER,OU=WEB Servers,OU=Exposed
Directly,DC=sanscocom,DC=com, Domain name is:  SANSCOCOM
USERENV(e0.4a4) 10:20:48:744 ProcessGPOs: Domain controller is:  \\sanscomdc.sanscocom.com
Domain DN is sanscocom.com
USERENV(e0.4a4) 10:20:48:744 ProcessGPOs: Calling GetGPOInfo for normal policy mode
USERENV(e0.4a4) 10:20:48:744 GetGPOInfo:  ********************************
USERENV(e0.4a4) 10:20:48:754 GetGPOInfo:  Entering...
USERENV(e0.4a4) 10:20:48:764 GetGPOInfo:  Server connection established.
USERENV(e0.4a4) 10:20:48:774 GetGPOInfo:  Bound successfully.
USERENV(e0.4a4) 10:20:48:774 SearchDSObject:  Searching <OU=WEB Servers,OU=Exposed
Directly,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:774 SearchDSObject:  Found GPO(s):  <[LDAP://CN={2DE77B00-2084-4585-
B74B-53ACC134E883},CN=Policies,CN=System,DC=sanscocom,DC=com;0]>
USERENV(e0.4a4) 10:20:48:774 ProcessGPO:  ==============================
USERENV(e0.4a4) 10:20:48:774 ProcessGPO:  Deferring search for <LDAP://CN={2DE77B00-2084-4585-
B74B-53ACC134E883},CN=Policies,CN=System,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:774 SearchDSObject:  Searching <OU=Exposed Directly,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:774 SearchDSObject:  No GPO(s) for this object.
USERENV(e0.4a4) 10:20:48:774 SearchDSObject:  Searching <DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:774 SearchDSObject:  Found GPO(s):  <[LDAP://CN={31B2F340-016D-11D2-
```

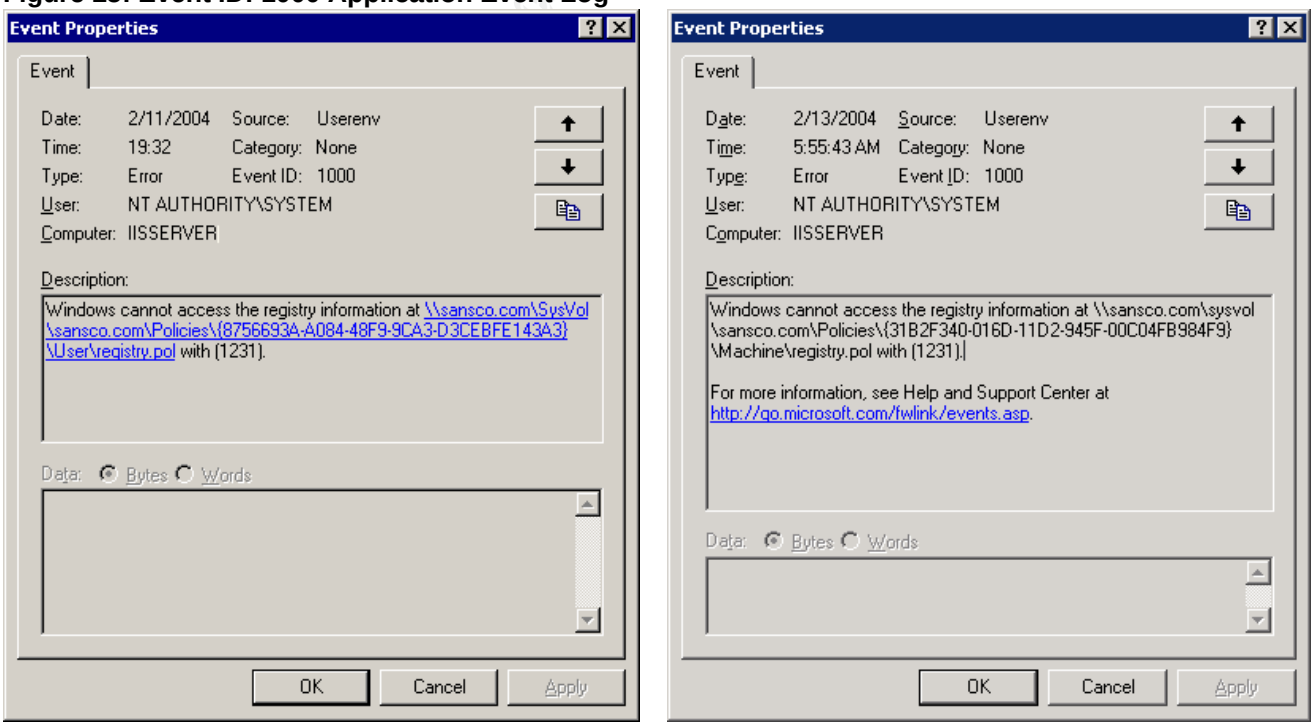
```
945F-00C04FB984F9},CN=Policies,CN=System,DC=sanscocom,DC=com;0]>
USERENV(e0.4a4) 10:20:48:774 ProcessGPO:  ==============================
USERENV(e0.4a4) 10:20:48:774 ProcessGPO:  Deferring search for <LDAP://CN={31B2F340-016D-11D2-
945F-00C04FB984F9},CN=Policies,CN=System,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:794 SearchDSObject:  Searching <CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:794 SearchDSObject:  No GPO(s) for this object.
USERENV(e0.4a4) 10:20:48:794 EvaluateDeferredGPOs:  Searching for GPOs in
cn=policies,cn=system,DC=sanscocom,DC=com
USERENV(e0.4a4) 10:20:48:794 ProcessGPO:  ==============================
USERENV(e0.4a4) 10:20:48:794 ProcessGPO:  Searching <CN={31B2F340-016D-11D2-945F-
00C04FB984F9},CN=Policies,CN=System,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:794 ProcessGPO:  Machine has access to this GPO.
USERENV(e0.4a4) 10:20:48:794 ProcessGPO:  Found functionality version of:  2
USERENV(e0.4a4) 10:20:48:794 ProcessGPO:  Found file system path of:
<\\sanscocom.com\sysvol\sanscocom.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}>
USERENV(e0.4a4) 10:20:48:814 ProcessGPO:  Found common name of:  <{31B2F340-016D-11D2-945F-
00C04FB984F9}>
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found display name of:  <Default Domain Policy>
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found machine version of:  GPC is 3, GPT is 3
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found flags of:  0
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found extensions:  [{35378EAC-683F-11D2-A89A-
00C04FBBCFA2}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}][{827D319E-6EAC-11D2-A4EA-
00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-
00C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}]
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  ==============================
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  ==============================
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Searching <CN={2DE77B00-2084-4585-B74B-
53ACC134E883},CN=Policies,CN=System,DC=sanscocom,DC=com>
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Machine has access to this GPO.
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found functionality version of:  2
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found file system path of:
<\\sanscocom.com\SysVol\sanscocom.com\Policies\{2DE77B00-2084-4585-B74B-53ACC134E883}>
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found common name of:  <{2DE77B00-2084-4585-B74B-
53ACC134E883}>
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found display name of:  <Erik Peterson IIS Web Server
GPO>
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found machine version of:  GPC is 3, GPT is 3
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found flags of:  0
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  Found extensions:  [{827D319E-6EAC-11D2-A4EA-
00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
USERENV(e0.4a4) 10:20:48:824 ProcessGPO:  ==============================
USERENV(e0.4a4) 10:20:48:824 GetGPOInfo:  Leaving with 1
USERENV(e0.4a4) 10:20:48:824 GetGPOInfo:  ********************************
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: OpenThreadToken failed with error 1008, assuming thread
is not impersonating
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Registry
USERENV(e0.4a4) 10:20:48:834 CompareGPOLists:  The lists are the same.
USERENV(e0.4a4) 10:20:48:834 CheckGPOs: No GPO changes and no security group membership change
and extension Registry has NoGPOChanges set.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Folder Redirection
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Extension Folder Redirection skipped with flags
0x10007.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Microsoft Disk Quota
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Extension Microsoft Disk Quota skipped with flags
0x10007.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Scripts
USERENV(e0.4a4) 10:20:48:834 CompareGPOLists:  The lists are the same.
USERENV(e0.4a4) 10:20:48:834 CheckGPOs: No GPO changes but couldn't read extension Scripts's
status or policy time.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Extension Scripts skipped because both deleted and
changed GPO lists are empty.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Security
USERENV(e0.4a4) 10:20:48:834 CompareGPOLists:  The lists are the same.
USERENV(e0.4a4) 10:20:48:834 CheckGPOs: No GPO changes and no security group membership change
and extension Security has NoGPOChanges set.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Internet Explorer Branding
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Extension Internet Explorer Branding skipped with flags
0x10007.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension EFS recovery
USERENV(e0.4a4) 10:20:48:834 CompareGPOLists:  The lists are the same.
```

```
USERENV(e0.4a4) 10:20:48:834 CheckGPOs: No GPO changes and no security group membership change
and extension EFS recovery has NoGPOChanges set.
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Processing extension Application Management
USERENV(e0.4a4) 10:20:48:834 ProcessGPOs: Extension Application Management skipped with flags
0x10007.
USERENV(e0.4a4) 10:20:48:844 ProcessGPOs: ----------------------
USERENV(e0.4a4) 10:20:48:844 ProcessGPOs: Processing extension IP Security
USERENV(e0.4a4) 10:20:48:844 CompareGPOLists:  The lists are the same.
USERENV(e0.4a4) 10:20:48:844 CheckGPOs: No GPO changes but couldn't read extension IP Security's
status or policy time.
USERENV(e0.4a4) 10:20:48:844 ProcessGPOs: Extension IP Security skipped because both deleted and
changed GPO lists are empty.
USERENV(e0.4a4) 10:20:48:844 LeaveCriticalPolicySection: Critical section 0x76c has been
released.
USERENV(e0.4a4) 10:20:48:844 ProcessGPOs: Computer Group Policy has been applied.
USERENV(e0.4a4) 10:20:48:844 ProcessGPOs: Leaving with 1.
USERENV(e0.4a4) 10:20:48:844 GPOThread:  Next refresh will happen in 111 minutes
```

As you can see from the excerpt above, it appears that the Member Server knows where to contact the DC, and knows about the GUIDs containing the appropriate policies, but is either unable to contact the DC, or does not have the appropriate access. I couldn't get any valid hits of my searches on the two errors showing up, so I started do some investigation on my own.

The application event log errors show here, indicate perhaps a slightly more definitive problem. It is clear that the client is having difficulty accessing the .pol files for both the user policy, and the machine policy.

Figure 25: Event ID: 1000 Application Event Log



Further investigation of these errors turn up many known problems related to the Event ID: 1000. The findings from Microsoft TechNet searches are listed here, and each one is investigated for a possible resolution. I have listed my conclusions (as a.) after each finding.

I. Microsoft Knowledge Base Article – 278316. ESENT Event IDs 1000, 1202, 412, and 454 Are Logged Repeatedly in the Application Event Log. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;261007

   a. This article outlines the steps to re-create a corrupted local Group Policy database. I went through the steps as outlined, and did re-create them. This however did not resolve the problem.

II. Microsoft Knowledge Base Article – 261007. Event ID 1000 Is Logged in the Application Event Log. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;261007

   a. This article points to an invalid or missing primary DNS Server entry on your client. The DNS server setting on the Member server was checked, and found to be configured correctly.

III. Microsoft Knowledge Base Article – 259398. SceCli Event ID 1001 and UserEnv Event ID 1000 When Dfs Client Is Disabled. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;259398

   a. The DFS client being disabled or DNS A records for the Domain or DC missing from the DNS server could also cause the error I was receiving. I checked the running services, and found the DFS client to be running. I also checked the DNS server for the appropriate A records, and validated they were pointing to the correct IP address. The four "_" records were also checked for good measure, and found to be valid on the DNS server.

IV. Microsoft Knowledge Base Article – 258296. Cannot Access Group Policy Objects--Event ID 1000 and Event ID 1001 Logged. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;258296

   a. This article refers to a multi-homed (more than one network card installed) DC where MS file and print are not bound to an adapter. This one was easy to troubleshoot since my DC only has one NIC!

V. Microsoft Knowledge Base Article – 271213. Event ID 1000 and 1001 Repeat Every 5 Minutes in the Event Log. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;271213

a. If the SysVol directory structure is missing, corrupted or altered, a similar error is logged. The SysVol directory and share on my DC were checked, and found to be functioning and setup correctly.

VI. Microsoft Knowledge Base Article – 290647. Event ID 1000, 1001 Is Logged Every Five Minutes in the Application Event Log. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;290647

a. If the SysVol directory or Share has permission set too tightly, or the wrong groups have the Bypass Traverse Checking User Rights Assigned, the problem could also occur. These were all checked according to the article, and were shown to be setup correctly.

At this point, some further testing and analysis needed to be done to resolve this issue since none of the knowledge base articles were getting me in the right direction.

2.3.0.0 TESTING METHODS

The first test that seemed obvious was to check to see if the Member Server could contact the DC. A ping of the DC's IP address came back just fine, verifying physical connectivity. Next, an *nslookup* from the command prompt was done, showing that both the Domain Controller and the Domain Name itself would resolve at the Member Server to the correct IP address:

Figure 26: nslookup

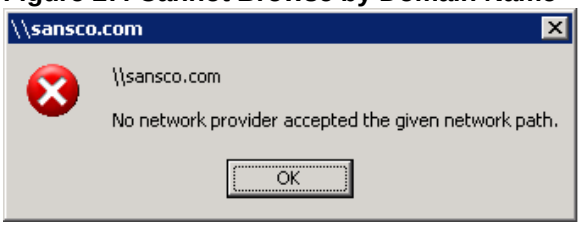
```
Default Server:  sanscomdc.sansco.com
Address:  10.100.251.1

> sansco.com
Server:  sanscomdc.sansco.com
Address:  10.100.251.1

Name:    sansco.com
Address:  10.100.251.1
```

The next test was to try to browse to the DC from my affected client, first via Network Neighborhood, and then from *Start > Run* *\\sanscomdc* . Both of these tests came back with the result I had expected, the DC was resolved correctly! I was then able to drill down into the SysVol share, and into the unique GUID directories without any problems. This proved that the DC and SysVol share and directories were accessible.

These results prompted a closer look at the event log errors. I noticed these error events actually have UNC hyperlinks to the SysVol share and policy location. I also noticed that it is not the name of the Domain Controller that is in this UNC path, but the

Domain Name itself. I opened one of the error events up while logged into the Member Server, and tried to click on the link to the policy, nothing happened. This prompted an attempt to simply try to browse to the Domain Name via UNC via *Start > Run* [\\sansco.com](\\sansco.com) :

Figure 27: Cannot Browse by Domain Name

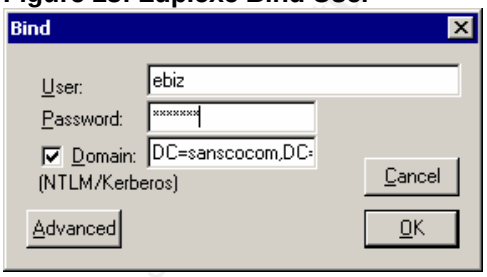


As per the screen shot, the test failed. This same test was then tried on the DC itself. An explorer window came right up without any problems, and I was able to browse the SysVol share – I was on to something.

The next thing I wanted to try was to see if I could browse the Active Directory itself from the Member Server. Using the *ldp.exe* utility located on the Windows 2000 Server CD, you can connect to your Active Directory database and browse the objects within. This would tell me whether or not the AD database was accessible to the user and computer.

Using *ldp.exe* I was able to connect to the Domain Controller, and then bind using the Domain account that was designated as a local administrator. This worked!

Figure 28: Ldp.exe Bind User



Next I enabled tree view, and was able to drill down into the individual policy locations: System > Policies > {GUID} . They were all accessible. I had actually hoped this would fail, but it did not. I was stumped again, so I went back to more carefully examine my OU GPO for the IISSERVER. The problem was discovered.

I'm certain, that had I caught this early enough, that the exact cause of the problem would have shown-up in the userenv.log file, but because my troubleshooting process actually spanned multiple days, the userenv.log file and userenv.bak file had both

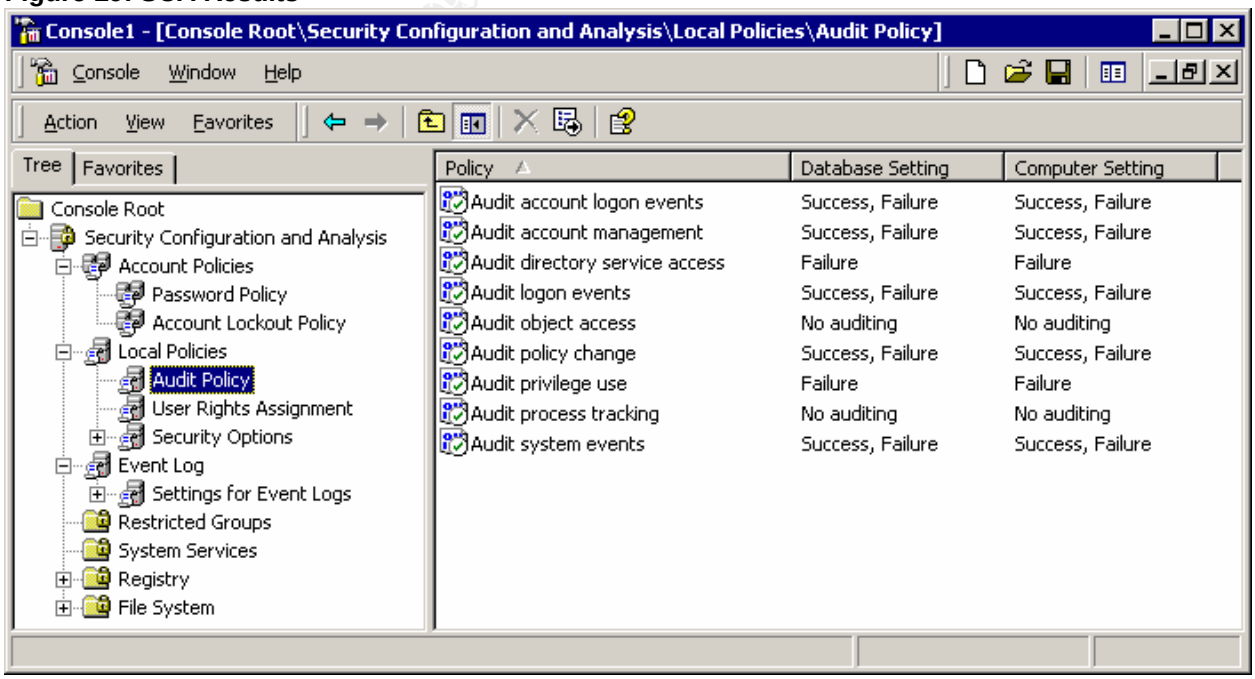
overwritten the earliest events. In a “real” production environment, this file could easily be restored from the backup tape to be examined; however no backup system was readily available for my test lab environment.

A single policy setting that disabled a single service, turned out to be the root of the problem. The TCP/IP NetBIOS Helper service was disabled via the GPO I had created. It was verified that this service was stopped, by checking the services on the affected Member Server. After some investigation, it was found that this service is disabled by default, in the security template: SecureInternetWebServer.inf. This was the template used as a basis for the security policy of this GPO.

My research on this matter showed conflicting conclusions. I read articles by both Microsoft and independent parties that suggested disabling this service for IIS servers, yet also found articles stating the contrary. My own conclusion is that the TCP/IP NetBIOS Helper service is required to be enabled and running on all clients that are required to have Group Policies applied correctly.

Lastly, we will run the Security and Configuration Analysis tool via the SCA snap-in to audit if our policy adheres to the security template we defined. On the target computer, IISSERVER, we will open the MMC console, and select the Security and Configuration Analysis snap-in. Next, we will create a new database, and import our customized security template based on the template: SecureInternetWebServer.inf. Once this is imported, we can run the analysis.

Figure 29: SCA Results

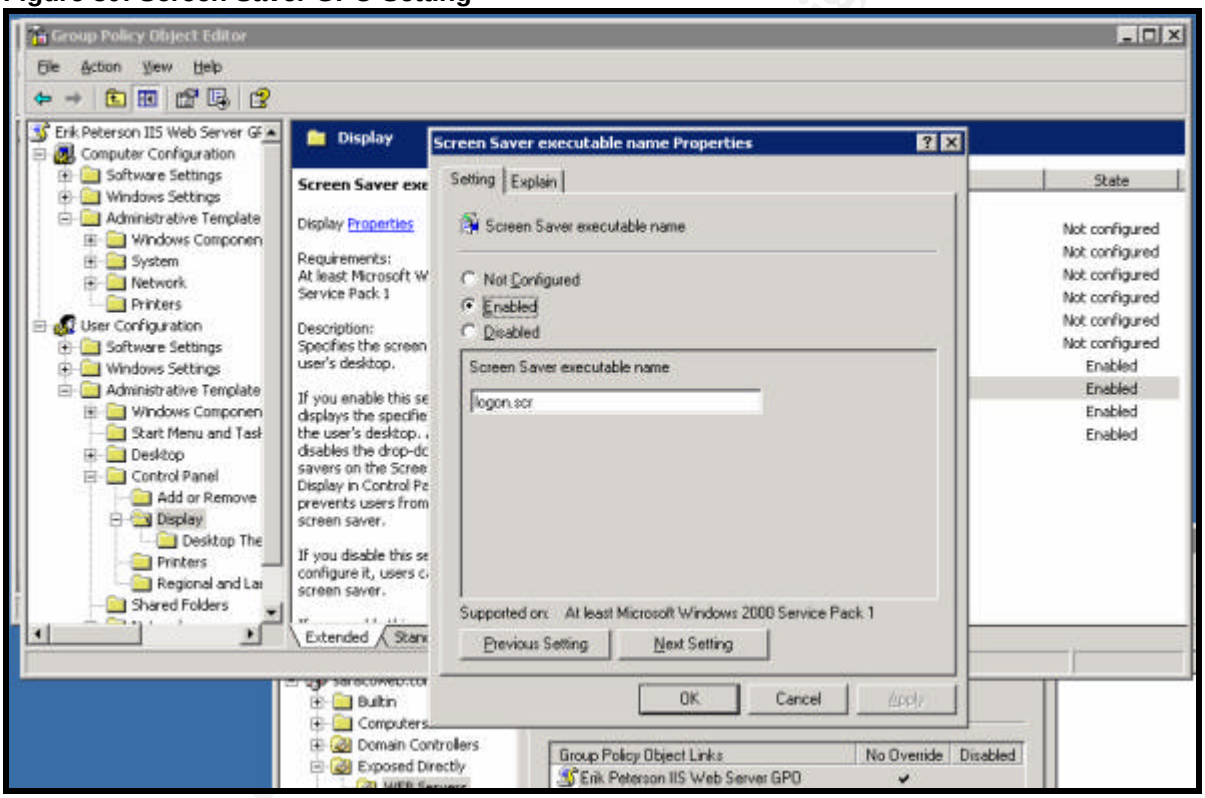


As you can see from the screenshot above, the SCA analysis has validated that the security policy is now being applied appropriately.

2.4 FUNCTIONALITY TESTS

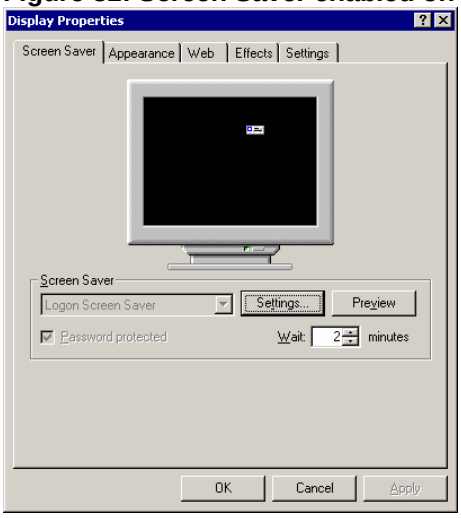
With Group Policy now applying correctly to the IISSERVER Member Server, we can begin to test the functionality of the policy. As mentioned earlier, a quick test to see if the policy was applied was to check the application of the screen saver and timeout period. This was set to the logon.scr with a timeout of two minutes.

Figure 30: Screen Saver GPO Setting



A quick check when logged into the IISERVER does indeed show that the logon.scr screen saver is enabled with a two minute timeout.

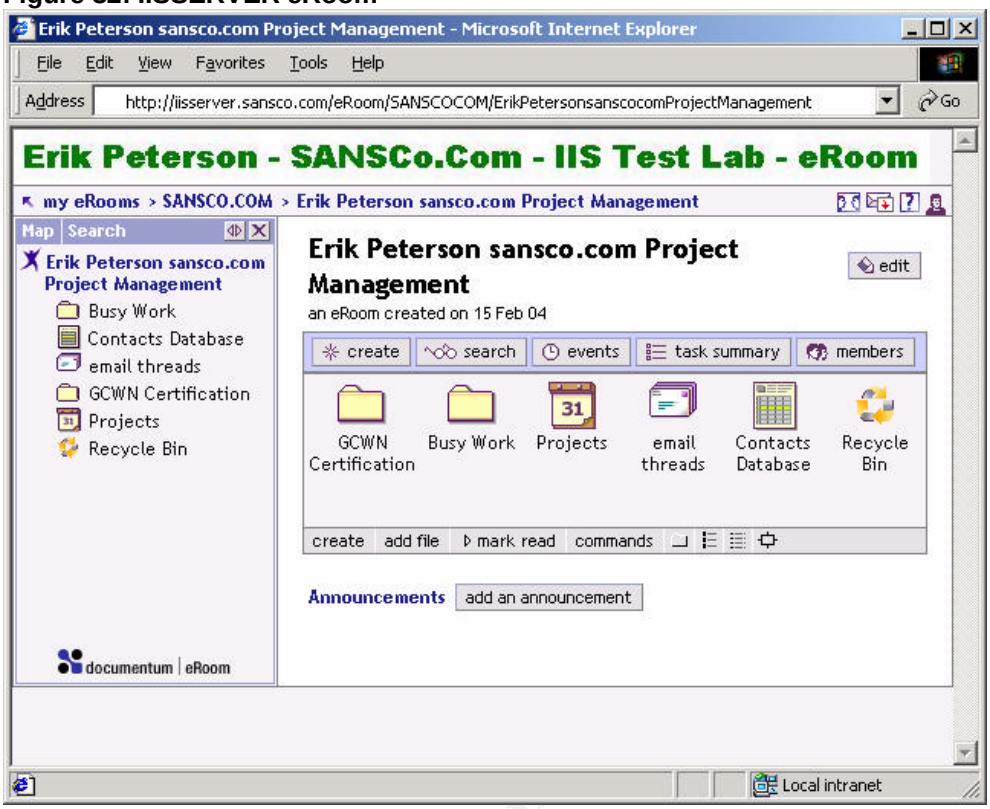
Figure 31: Screen Saver enabled on Client



Next, we would like to test for application functionality. This IIS server will be running a 3rd party application called eRoom. This is a browser-based project collaboration tool that installs on top of IIS. This product can hook into your Active Directory Domain or other LDAP directory for user authentication into the system.

ERoom was installed on this same lab web server, IISSERVER. I was able to successfully log in as an authenticated user in the Domain to my test lab eRoom:

Figure 32: IISSERVER eRoom



With the application running, and tested to be fully functional, we know that our GPO has not interfered with our applications functionality.

2.5 POLICY EVALUATION

This GPO applied to the WEB Servers OU will aid in providing security through defense in depth to the IIS Servers in the SANS Co WEB Farm. This policy allows full functionality to the necessary components and services of the Web Servers where it is applied. The default security template used proved incompatible with the application of the Group Policy and had to be modified, otherwise functionality remained intact.

Group Policy requires thorough planning and testing prior to its application. A good test lab environment that simulates your real environment is invaluable to your development of group policies.

3 AUDIT

Auditing can be a doubled-edged sword. On the one side, you need to collect enough information to be able to accurately assess valuable information. On the other, collecting too much information (or not being able to process this data efficiently), can lead to headaches, or worse, simply ignoring this data because the volume it is simply overwhelming. When evaluating this conundrum, there is one easy answer: only audit what you will examine.

3.0 OVERVIEW

Within SANS Co, an overall audit strategy is in place. Auditing is performed at some, or all of the following levels depending upon the requirements of the specific location:

- Physical: This includes magnetic readers logging access on the entrances to all buildings, and to secured rooms within certain buildings, and Video surveillance where appropriate.
- Network devices: SNMP logs are collected for critical switches and routers.
- Firewalls and VPNs: This is the only category where all logs are centrally collected at SANS Co corporate headquarters. Each sites firewalls and VPN routers and VPN RAS servers will use the WAN to send the logs from these systems to a central log server at SANS Co corporate. Backup logs servers are also placed locally to collect logs in the event of a WAN failure (this is doubly important do to the fact that a local log server may be needed to help track down the problem causing the WAN link to be down.).
- Servers: Events and logs are centrally collected at a level equal to the sensitivity of the system. Dell OpenManage agents are used on servers to send SNMP data regarding the system hardware state to OpenManage servers at each site.
- Desktops: Events and logs are recorded only on the local system. Microsoft Systems Management Server (SMS) is deployed at each site. SMS allows for among others, the audit of hardware configuration, and software installation.

The auditing of systems can have different requirements, depending upon the type of system, sensitivity of information contained within, and exposure of these systems. Analysis needs to be done up front regarding what level of auditing is pertinent for a given system. For instance, a file server in the R&D department or an externally exposed DNS server may much more detailed audit events collected than say, a marketing users desktop PC. Since each Domain in SANS Co is also a separate business segment, SANS Co will leave it up to each Domain to come up with its own auditing policy. The product that best fit this plan was Microsoft Operations Manager (MOM).

MOM is highly customizable, and can gather all kinds of information. With MOM, you can also write rules and setup alerts. This could allow you to receive notification for

things like attempts to log into sensitive accounts with a bad password. MOM will be used for alerting, performance data gathering, and reporting metrics.

3.1 LOG MANAGEMENT

SANS Co needed a way to be able to centralize event logs and other pertinent system logs centrally where possible, and locally where necessary. It was decided that in order to keep the cost down on the expensive WAN links, that logs would be gathered from within a given physical site only.

Microsoft has tools readily available that allow you to pull in information from the event logs. These tools include utilities such as EventQuery.vbs and Dumpel.exe. While both tools may provide the necessary collection of event logs, SANS Co has decided to use MOM for event log collection.

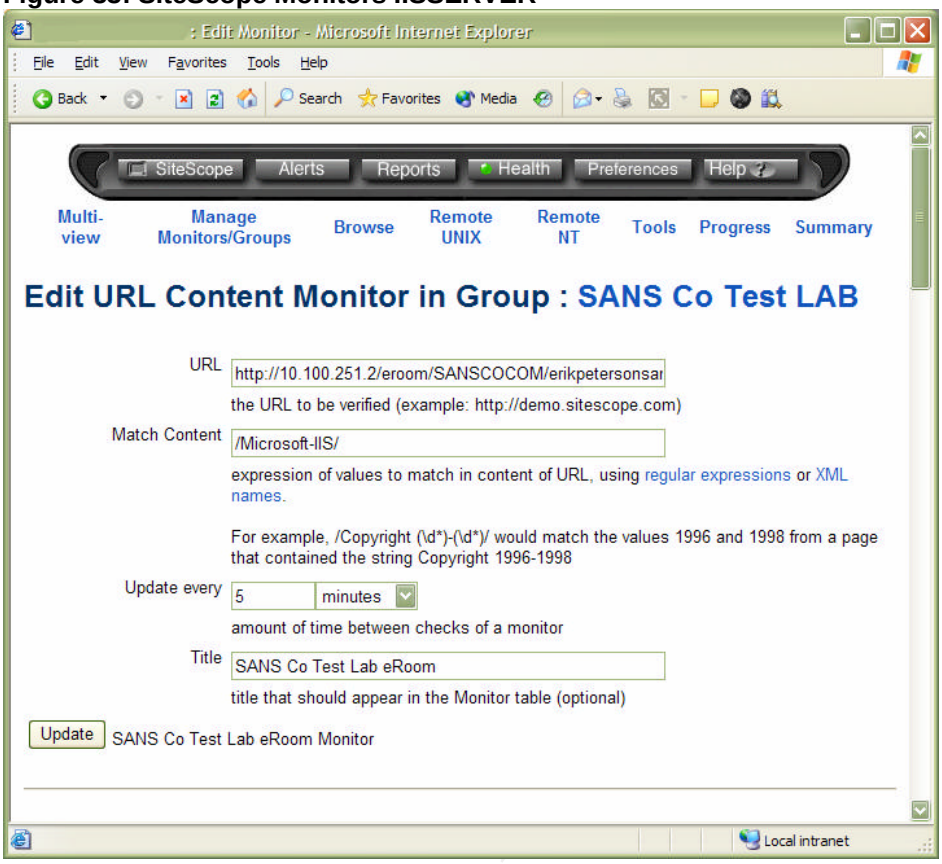
3.2 METRICS

Metrics are important to help gauge the availability of your systems, and to help in the evaluation of load and performance. Besides MOM, SANS Co also utilizes an agent-less monitoring tool called SiteScope[29], a product of the Mercury Interactive Corporation. SiteScope can monitor and report on many of the same things MOM can, such as Windows Services, Disk utilization, performance thresholds and system availability. SANS Co uses SiteScope to compliment Microsoft MOM. SiteScope has also greatly aided in the monitoring of systems availability at GIAC. SANS Co infrastructure admins have setup a SiteScope monitoring group to monitor the availability of the Domain controllers, and all the device dependencies required to gain access to those Domain controllers at GIAC. This monitoring group looks first at all the critical WAN components, such as the routers, switches and VPN routers involved in getting connectivity between SANS Co DCs and the GIAC DCs. This group then monitors the actual DCs themselves, and the critical services required for the DCs to function appropriately.

We will configure SiteScope to monitor our IISSERVER on port 80, to make sure our eRoom application is running. It will do this by validating URL content by string matching some text that is returned in the HTTP header from the IIS Server.

[29] Mercury Interactive. "SiteScope How It Works." URL: http://www.mercuryinteractive.com/products/sitescope/works.html (15 February 2004).

Figure 33: SiteScope Monitors IISSERVER



By having SiteScope gather this information, we can easily run reports to see the percent of uptime, and percent in error of any of the systems we use it to monitor. SiteScope, because it is agent-less also does not require us to install anything on the clients it monitors. This is also beneficial because SANS Co can quickly add monitors for practically anything in their network, such as the VPN IPSEC routers at each location.

3.3 CRITICAL COMPONENTS

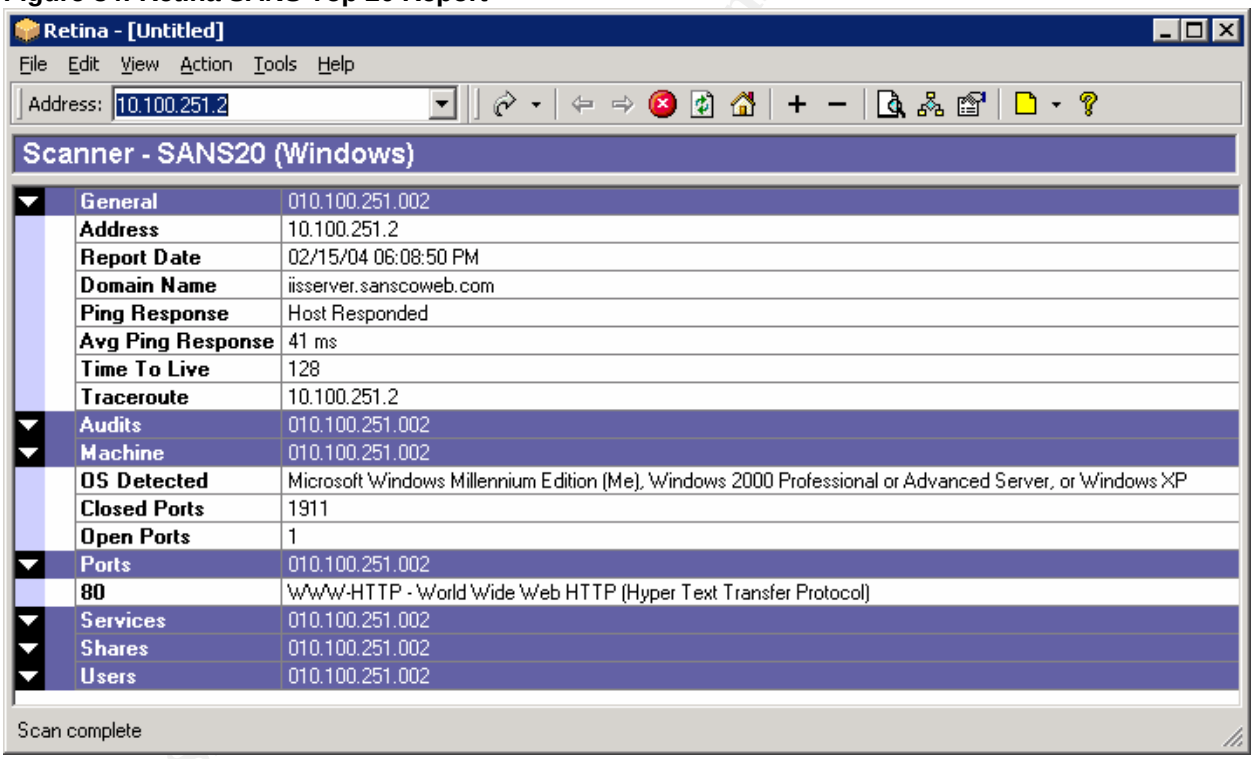
SANS Co also needed a way to audit the vulnerabilities of a given system. This is a daunting task when all the possibilities are considered. It was decided that a 3rd party auditing tool would be used to asses these vulnerabilities. The tool that was selected was the Retina Network Security Scanner from eEye Digital Security Corporation[30]. This tool provides a good means of auditing for known vulnerabilities, and general misconfigurations that could lead to a vulnerability. Retina continually updates the product as new vulnerabilities are discovered, and allows for scheduled scans to be run, and the data collected to be stored in a database of your choosing. SANS Co stores all of these audit scans on a Microsoft SQL database.

[30] eEye Digital Security Corporation. "Retina Network Security Scanner." URL: http://www.eeye.com/html/Products/Retina/ (02/13/2004).

Within SANS Co, the systems that are in the DMZ have a vulnerability scan scheduled to run nightly. This scan is run from a system that is outside of the firewalls protecting the DMZ, and therefore audits both the firewalls and the systems behind them at the same time. This is done to audit any on authorized changes to firewall rulesets, and unauthorized services running on these systems. For instance, this audit scan would catch an unauthorized FTP service running on a compromised WEB server, most likely before any administrator would notice it.

For test lab purposes, a packet filtering firewall will be placed in front of the IISERVER running the eRoom application to simulate the real production environment. We will then have Retina perform a SANS Top 20 vulnerability scan on it. The firewall will be configured to only forward port 80.

Figure 34: Retina SANS Top 20 Report



The results of the report show only one port open, port 80. Based on the HTTP header information returned, Retina corrected fingerprinted a web server running a Microsoft OS, but could not pinpoint the exact operating system.

These sorts of nightly scans will enable the Administrators of these systems to sleep better knowing that this audit tool is backing up the effort they have made to keep their systems secured.

4 SUMMARY

SANS Co has greatly benefited from the administrative capabilities of Active Directory. Active Directory has allowed them to increase their network systems security and simplify management of systems and user accounts.

Active Directory compliments the infrastructure design at SANS Co and GIAC. Sites and departments requiring higher levels of security can implement policies supporting these requirements while still maintaining connectivity to system-wide resources where required.

Through the use of Group Policies, SANS Co is more easily able accomplish systems management tasks that would have been daunting to undertake prior to its inception. SANS Co can now quickly safeguard similar types of resources in a manageable and extremely configurable manner. The support infrastructure has an easier job now that group policies help define what the end-users can and cannot do to their desktops, creating less work for them when a user cripples their system.

Thanks to Active Directory, GIAC has been able to hand over the administration of their Windows systems to the IT staff at SANS Co with minimal impact to their supportability. The forest trust relationship between the two organizations has enabled users to quickly and easily share resources amongst themselves.

Active Directory will continue to play an important role in securing the system at SANS Co and GIAC, and has made the job of managing security much easier for all involved.

5 REFERENCES

Parmar, Harpal. “A Secure Windows 2000 Infrastructure for GIAC Enterprises.” GCNT Practical Assignment. Version 3.0. 05 May 2002. URL: http://www.giac.org/practical/Harpal_Parmar_GCNT.doc (17 December 2003).

Microsoft Corporation. “Microsoft Metadirectory Services.”
URL: http://www.microsoft.com/windows2000/technologies/directory/MMS/default.asp (08 January 2004).

WatchGuard Technologies, Inc. “Application Layer Proxies: Beyond Packet Filtering.”
URL: http://www.watchguard.com/products/proxy.asp (08 January 2004).

WatchGuard Technologies, Inc. “Firebox VClass: Perimeter Security.”
URL: http://www.watchguard.com/products/vclass.asp (10 January 2004).

Kent, S. Atkinson, R. “Security Architecture for the Internet Protocol.” Request for Comments: 2401. November 1998.
URL: http://www.ietf.org/rfc/rfc2401.txt (13 January 2004).

Microsoft Corporation. “Key exchange methods.” Windows Server 2003 Product Documentation Standard Edition Help.
URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_IPSECkeyexchgsm.asp (09 January 2004).

American National Standard for Telecommunications. “Perfect Forward Secrecy.” Telecom Glossary 2000. 28 February 2001. URL: http://www.atis.org/tg2k/_perfect_forward_secrecy.html (09 January 2004).

WatchGuard Technologies, Inc. “VPN Manager FAQ: Info Center.”
URL: http://www.watchguard.com/docs/html/vpnmgr_faq.asp#dvcp (10 January 2004).

WatchGuard Technologies, Inc. “VPN Manager: Firebox System.”
URL: http://www.watchguard.com/products/vpnmanager.asp (10 January 2004).

Microsoft Corporation. “Point-to-Point Tunneling Protocol (PPTP).” Windows XP Home Edition Product Documentation
URL: http://www.microsoft.com/WINDOWSXP/home/using/productdoc/en/access_pptp.asp (09 January 2004).

Microsoft Corporation “Connection Manager Administration Kit Makes Daily Internet Access Easy.” January 1998.
URL: http://www.microsoft.com/technet/archive/default.asp?url=/technet/archive/ie/evaluate/ie4cmak.asp (11 January 2004).

Reliable Fire Equipment Company. “FM-200 Fire Suppression Systems.” 29 January 2004.
URL: http://www.reliablefire.com/fm200/fm200.html (29 January 2004).

Microsoft Corporation, “Windows 2000 Server Deployment and Planning Guide.” Windows 2000 Resource Kit. 01/19/2000.
URL: http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/part3/chapt-9.asp (10 January, 2004).

Smith, Andrew “I don't want a Lime Mac, I want Names for my Servers!.” 29 October 1999.
URL: http://slashdot.org/features/99/10/28/1116250.shtml (16 January 2004).

Microsoft Corporation. “Best Practices.” Windows Server 2003 Product Documentation Standard Edition Help.
URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_DNS_imp_BestPractices.asp (16 January 2004).

Microsoft Corporation. “Microsoft Windows 2000 Server Documentation.”
URL: http://www.microsoft.com/windows2000/en/server/help/sag_DNS_imp_NamespacePlanning.htm (16 January 2004).

Microsoft Corporation. “Management Services Glossary.”
URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/glossary.asp#d (12 January 2004).

RSA Laboratories. “What is a PKI?.” Cryptography FAQ.URL: http://www.rsasecurity.com/rsalabs/faq/4-1-3-1.html (17 January 2004).

Microsoft Corporation. “Components of EFS.” Microsoft Windows XP Professional Resource Kit, Chapter 17.
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prnb_efs_ijvx.asp (18 January 2004).

Y. Rekhter., B. Moskowitz., D. Karrenberg., G. J. de Groot., E. Lear. “RFC 1918 - Address Allocation for Private Internets.” February 1996. URL: http://www.faqs.org/rfcs/rfc1918.html (20 January 2004).

Microsoft Corporation. “Using SID History to Preserve Resource Access.” Windows Server 2003 Deployment Kit.
URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dssbi_reer_qdhe.asp (January 24 2004).

Microsoft Corporation. "Microsoft Security Bulletin MS02-001." Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data. 09 MAY 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS02-001.asp (February 02 2004).

Microsoft Corporation. "To exclude name suffixes from routing to a local forest." Windows Server 2003 Product Documentation. URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/x_routename.asp (20 January 2004).

Fossen, Jason. "Kerberos and NTLMv2." Active Directory. SANS Institute. May 2000. 38-39, 43.

Haney, J. "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." National Security Agency Security Recommendation Guides. 03 December 2002. URL: http://nsa2.www.conxion.com/win2k/guides/w2k-3.pdf (02 February 2004)

Microsoft Corporation. "Securing IIS 5.0 Resource Guide." URL: http://www.microsoft.com/technet/security/chklist/iis50srg.asp (02 February 2004).

Rohrer, Mark. "Neohapsis Archives." 23 March 2002.
URL: http://archives.neohapsis.com/archives/incidents/2002-03/0117.html (03 February 2004).

Microsoft Corporation. "How to Enable User Environment Debug Logging in Retail Builds of Windows." 23 September 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;221833 (03 February 2004).

Mercury Interactive. "SiteScope How It Works." URL: http://www.mercuryinteractive.com/products/sitescope/works.html (15 February 2004).

eEye Digital Security Corporation. "Retina Network Security Scanner." URL: http://www.eeye.com/html/Products/Retina/ (02/13/2004).