



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

Securing Sans Co. and GIAC Enterprises
GCWN v.3.2
Matt Parks
March 12, 2004

© SANS Institute 2004, Author retains full rights.

Introduction

This paper is for certification of SANS/GIAC GCWN – Securing Windows. In this paper, two fictional companies, Sans Co. and GIAC-Enterprises (GIACE from here on out) have merged and are looking for ways to ensure technical interoperability, economies of scale, consolidate IT overhead, and to allow customers to deal with both companies via a web presence. The paper consists of three sections. The first describes Sans Co.'s network and Active Directory architecture. Additionally, I have taken from a previous GCWN Practical, architecture for GIACE, which shows its network and Active Directory structure. This structure will merge with Sans Co. to form one company. In this section, I provide assumptions on the setup of Sans Co.'s network and AD structure, which provides an infrastructure that focuses on security as well as allows Sans Co. and GIACE the ability to leverage each other's resources.

The second section is a description and tutorial, which includes specific Group Policies that will implement to allow interoperability between the two forests, seamless integration as seen by the external customers. The main emphasis of this Group Policy will of course be the security of the company as a whole. The discussion will not only apply Group Policies, but also test (audit) the policies and show why they are appropriate for the company. This section also provides company policy that will apply to all internal employees that will require adherence. The Group Policy that is in place will back up this company policy from a technical standpoint; however, it is also the responsibility of the employees themselves to follow the policy set forth.

In the third section, I provide methods for auditing and verifying the integrity of the AD infrastructure as a whole. This will contain specific information on how IT staff will handle the audit and why I need to audit the AD infrastructure.

Sans Co. Forest Description and Domain Design

Sans Co. is a Denver based company that for years has been well known and respected in the public eye for producing a quality product as well as for technical innovation. The company employs 150 personnel in the areas of Executives, marketing, sales, finance, IT staff, and manufacturing. As a leader in the USA in the niche of producing the finest quality accessories for Chinese and Japanese restaurants, Sans Co. has expanded rapidly by acquiring similar niche companies. Sans Co. started producing chop sticks (which it still does today); however, through acquisitions, the company has gone on to expand its business and product offering through the companies listed below. Sans Co. was also the first chopstick manufacturer to have a web presence for its customers, which enabled customers to place orders over the internet, and created the ability to offer each of the companies' products online via an integrated web server. This has drastically increased sales and profitability.

Fortune Co. Sans Co. purchased this fortune cookie manufacturer several years ago. They are physically located in Denver as well and employ approximately 25 people in IT Staff, manufacturing, and sales/marketing. Starting off as a small “mom and pop” company, they have been able to expand to their current size via the sales boost from the web presence, as well as being able to expand due to business gained by existing Sans Co. customers.

Boxes Co. was the premier maker of the boxes used in takeout orders and was also purchased by Sans Co. recently. Boxes Co. also never had any web presence before being bought out by Sans Co., but has seen an increase in sales since going “online.” Also physically located in Denver, Boxes Co. employs approximately 15 people in IT staff and Operations (including sales, marketing, finance, and manufacturing).

Little Soy, Inc. was the leading maker and distributor of soy sauce packets, also mainly for delivery orders. They had prior web presence but were able to merge web orders with Sans Co. several months ago after being bought out. Little Soy is located in Denver, where it has approximately 50 employees in manufacturing, sales and marketing, and IT Staff.

Since the acquisition of these three companies, Sans Co. has been able to merge each company into one main forest with the exception of the external web servers in the DMZ. They have however retained the domain structure at each company so there are currently five domains (www.sansco-mp.com, www.boxscompany.com, www.littlesoy.com, and www.fortunecookie.com). The fifth domain is isolated from the rest of the Sans Co. forest as it is merely for their web server(s) in the network DMZ. The Sans Co. forest is depicted on the following page, with sansco-mp.com being the root domain. Each of the four domains within the forest contains two Domain Controllers (DC’s) although in a Windows 2000 AD Structure and with multi-master replication, there is no such thing as primary and back up DC’s. Still, it is important to have redundant DC’s for each domain as they provide the framework for security in the Sans Co. environment.

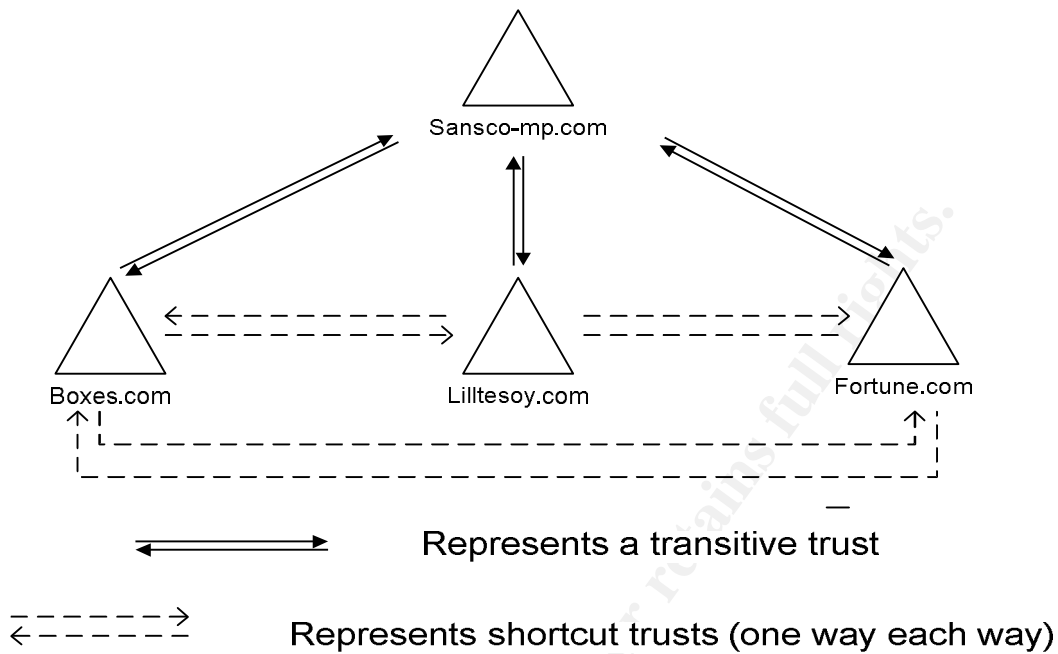
Sans Co.’s Organizational Unit (OU) structure was designed under the assumption that different types of users in different functional areas would require different types of access and security controls. For this reason, we have created different OU’s to be able to manage not only these varying user types, but also different OU’s for workstations within the functional areas. For example, IT Staff is in charge of administering the network, servers, databases, and creating/deleting users. Human Resources have access to confidential information about employees that should not be available to just anyone. Manufacturing has limited need for network resources, aside from internet access (for researching product development) and email (to contact vendors, suppliers, and communicating internally with other employees.) Additionally, OU’s were created for general servers, which can for the most part be

administered as a whole by Group Policy. Web servers (internal) are categorized in another OU because they require security that is more stringent. The OU structure of Sans Co. is further broken into Users and Workstations for the IT Staff to be able to apply Group Policy to user accounts and to workstations within each functional area.

The external web server domain was set up to allow us to use Active Directory and Group Policy to manage users as well as to be able to apply Group Policy and more easily secure the web servers. With the growth that Sans Co. has seen recently experienced and with the addition of GIACE, additional web servers will be needed for customers to place orders. This domain will allow us to easily replicate the security settings and group policies to the new servers, as well as to manage customer accounts. In the AD diagram(s) below, also notice that there have been external one way trusts set up between the web server domain and each domain in the forest, with the external domain being *trusting* and the four internal domains being *trusted*. Likewise, there is a similar trust set up between GIACE and the web server domain, again with the web server domain being *trusting* and GIACE being *trusted*. This is done for security purposes as well as for functionality. This is crucial for IT Staff to manage the servers, sales and marketing employees to be able to track orders, and executives should they need to access the web servers directly. Additionally, this is done as a business requirement for employees, both internally and the external sales force, to be able to authenticate to the web servers to be able to place orders for customers, track orders and run reports if necessary. The applications in the web servers domain includes software that performs these critical business functions, which is the lifeblood of Sans Co. and directly correlates to the bottom line of the company. Because of this we have set up the one way trust as mentioned above, which balances functionality (being able to authenticate and access the applications housed in the DMZ) with security (having a one way trust allows access from the protected network out to the web server domain, but not vice versa. Additionally there is no replication of Global Catalog, Naming Context or Schema.)

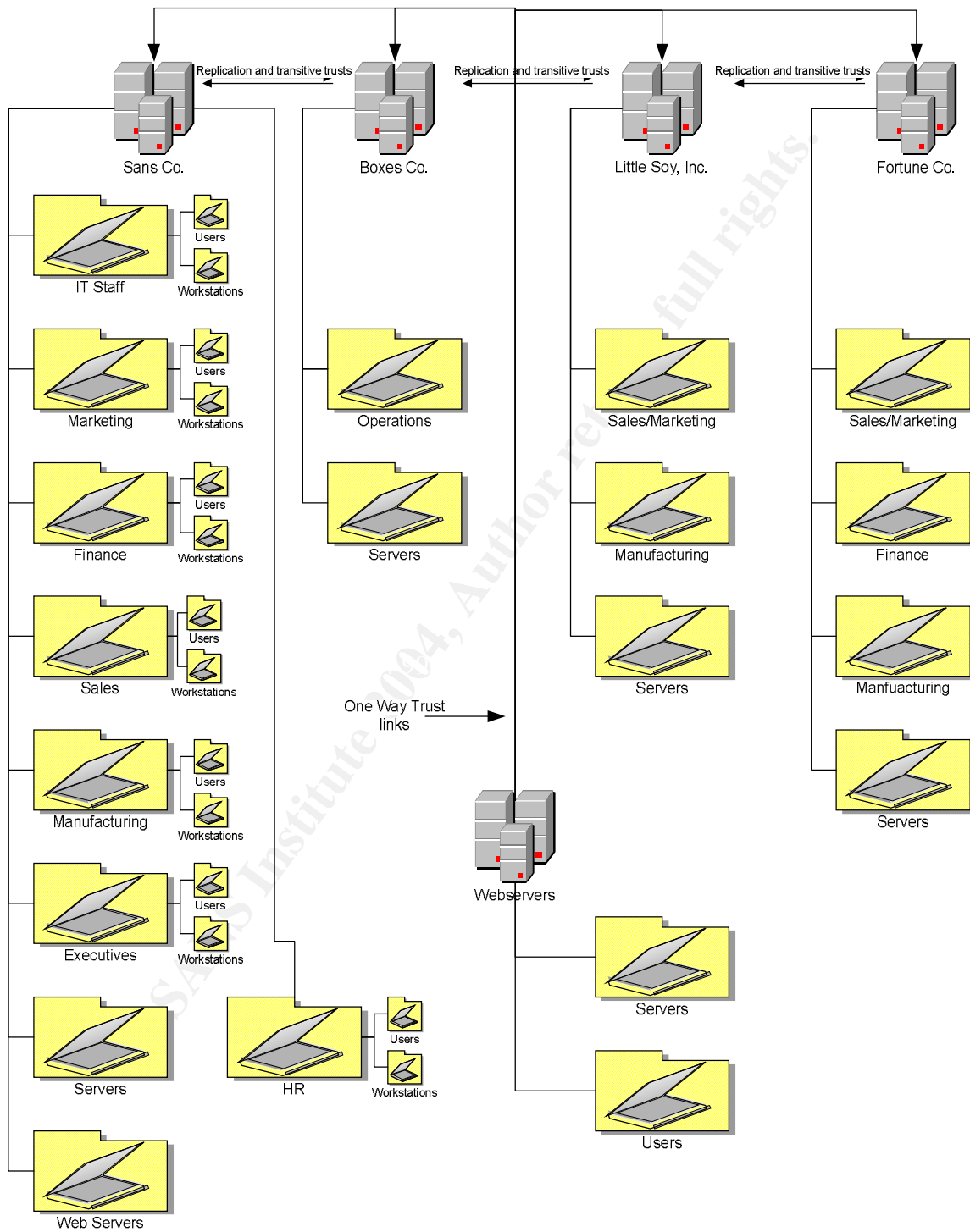
Additionally below, I have shown a high-level design of the domain structure, which shows sansco-mp.com as the root domain. Note that the one-way trusts set up between the web servers' domain and each of the internal network domains has been excluded from this diagram, as its purpose is to show the relationship and replication channels between the four domains within the Sans Co forest. As Sans Co. grew and added companies (and domains), they were installed under the root domain sansco-mp.com. Because of this, transitive trusts are automatically set up between the root and the subsequent domains. However in order to reduce the overhead of Kerberos referrals between the sub-domains (and so they could directly share referral TGT's to each others DC's) we have added shortcut trusts between each of the sub-domains. "Shortcut trusts simply exist to make Kerberos referrals more efficient, but they don't really add

any new trusting relationships...” (Fossen. Windows 2000/XP/2003 Active Directory, p. 170).



Sans Co. AD Structure

Sans Co. Active Directory Structure



Assumptions

The Sans Co. network is set up in one physical location in Denver, CO. Upon their latest acquisition of Little Soy, Inc. Sans Co. was able to consolidate the physical locations of all 4 companies; however, due to political reasons and so that each company under Sans Co. could retain its company name, email addresses, and a semblance of autonomy, they retained the 4 domain structure under one forest, in one consolidated network. All servers and workstations, both internally and remote users laptops, have been upgraded to Windows 2000, SP 4. This is important to note because W2K SP2 and higher support 128-bit RC4 encryption for non-authentication purposes (i.e. the generation of session keys) and provides for the most stringent security for W2K. It is also important from a patching perspective that everything is at the latest Service Pack possible.

The local area network (LAN) was set up in the manner shown in the diagram below. At the edge, there is a router connecting the internet to a dual PIX firewall with failover. Each of these firewalls is configured identically for the purpose of redundancy. The PIX has a VPN module installed, which has an accelerator card for enhanced processing of encrypted data, and in fact handles all the processing for VPN connections from remote users. Remote users connect via the Windows VPN client installed on laptops or home computers using PPTP. A Cisco ACS server on the internal network allows these remote users to authenticate to the ADS structure. Since PPTP is less secure than L2TP and the password hashes can be sniffed and run through a password cracker like L0phtcrack or John the Ripper, all remote users machines have been set up so Microsoft Point to Point Encryption (MPPE) uses 128 bit RC4 encryption. Additionally, Sans Co. has established a strong password policy, as the ultimate strength of a password in this configuration lies on the password itself. A copy of this password policy is in Appendix A, and the group policy tutorial covers technical controls for enforcing this policy.

Additionally, there is a DMZ established off the PIX, which controls packets going in and coming out. The DMZ contains external DNS and SMTP servers, as well as an external web server (a fully patched IIS 5.0 server) for customers to be able to place orders and verify/check their status. This web server is becoming the backbone of the sales teams and the meat and potatoes of sales to customers; thus, it is extremely important to the bottom line success of Sans Co. The web server collects customer information; however, no sensitive data is stored locally. Instead, a SQL 2000 server on the internal network that acts as a data store for all private and confidential information such as customer names, phone numbers, email addresses, credit card numbers, purchases, etc. The web server is set up in its own domain with Active Directory and Group Policy used to adhere to security standards. As mentioned above, there is a business need for the internal users and external sales forces to be able to access the web servers, usually to be able to place and track orders for customers. Customer service and quick response to customer inquiries about orders is imperative in this industry

as many of Sans Co's. customers are small "mom and pop" type restaurants with limited internet access, if any at all.

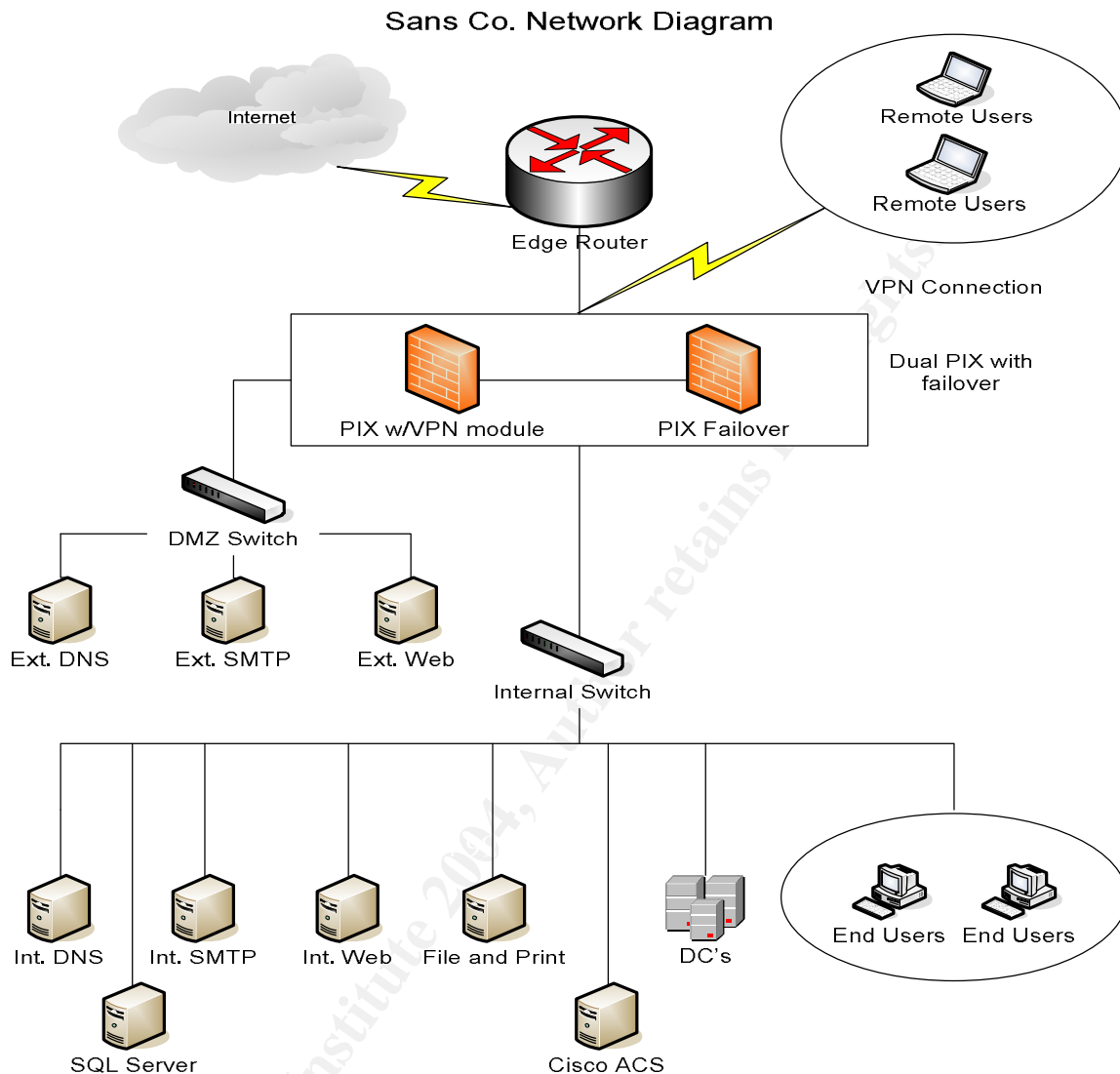
Additional requirements at the DMZ firewall are to open ports for Kerberos authentication. To do this, the following ports must be open. To enhance security, we developed firewall rules that specify that only traffic to and from specific IP addresses (namely the internal and DMZ DC's) is allowed on these ports.

<u>Port</u>	<u>Protocol</u>	<u>Description</u>
464	TCP/UDP	Kerberos Passwords
88	TCP/UDP	Kerberos Secure Authentication
636	TCP	LDAP SSL
3269	TCP	Global Catalog with LDAP and SSL

Internally, there is another DNS server, an SMTP server, and several file and print servers set up with file and print shares for users located throughout the office. Additionally, there is a server dedicated to the collection of security event logs. The software installed acts as a data store for reporting on security events in the network, as well as a tool to notify (via SMTP) administrators on security events that indicate possible attacks to servers in the network. As previously mentioned, each server is set up with Windows Server 2000 SP4.

Because all domains exist within the same network (except for the web server domain), multi-master replication between domain controllers occurs internally between sites via RPC over the secure channel for the Global Catalog, Schema, and Naming Context. Since all replication occurs internally, IPSec is used to provide encryption between the DC's. Additionally, IPSec offload cards have been installed on all DC's, which handles processing for replication only and allows the CPU to be utilized for the other functions of each DC. IPSec is also configured to secure replication traffic and ignore everything else. There is no replication between the web server domain and any of the other four domains within Sans Co. since there are only one-way (intransitive) external trusts between them.

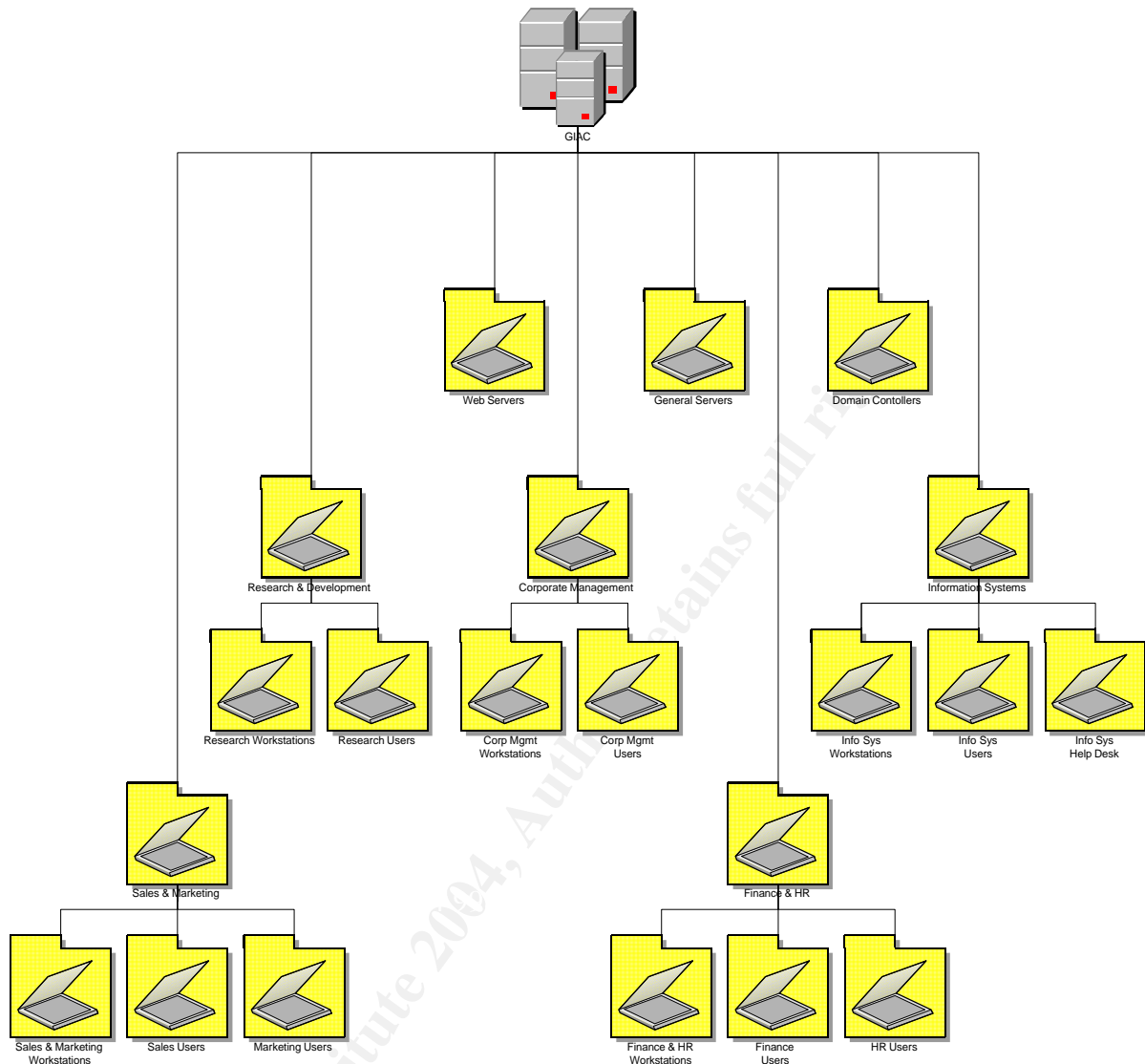
Sans Co. Network Diagram



GIAC Enterprises

Forest Description

The GIACE network is designed based on the GCWN paper "GIAC Enterprises Windows 2000 Layout" by Mike McCabe. A diagram of the GIACE forest is shown below. It is a single domain structure with redundant DC's, similar to the setup of Sans Co. AD structure.

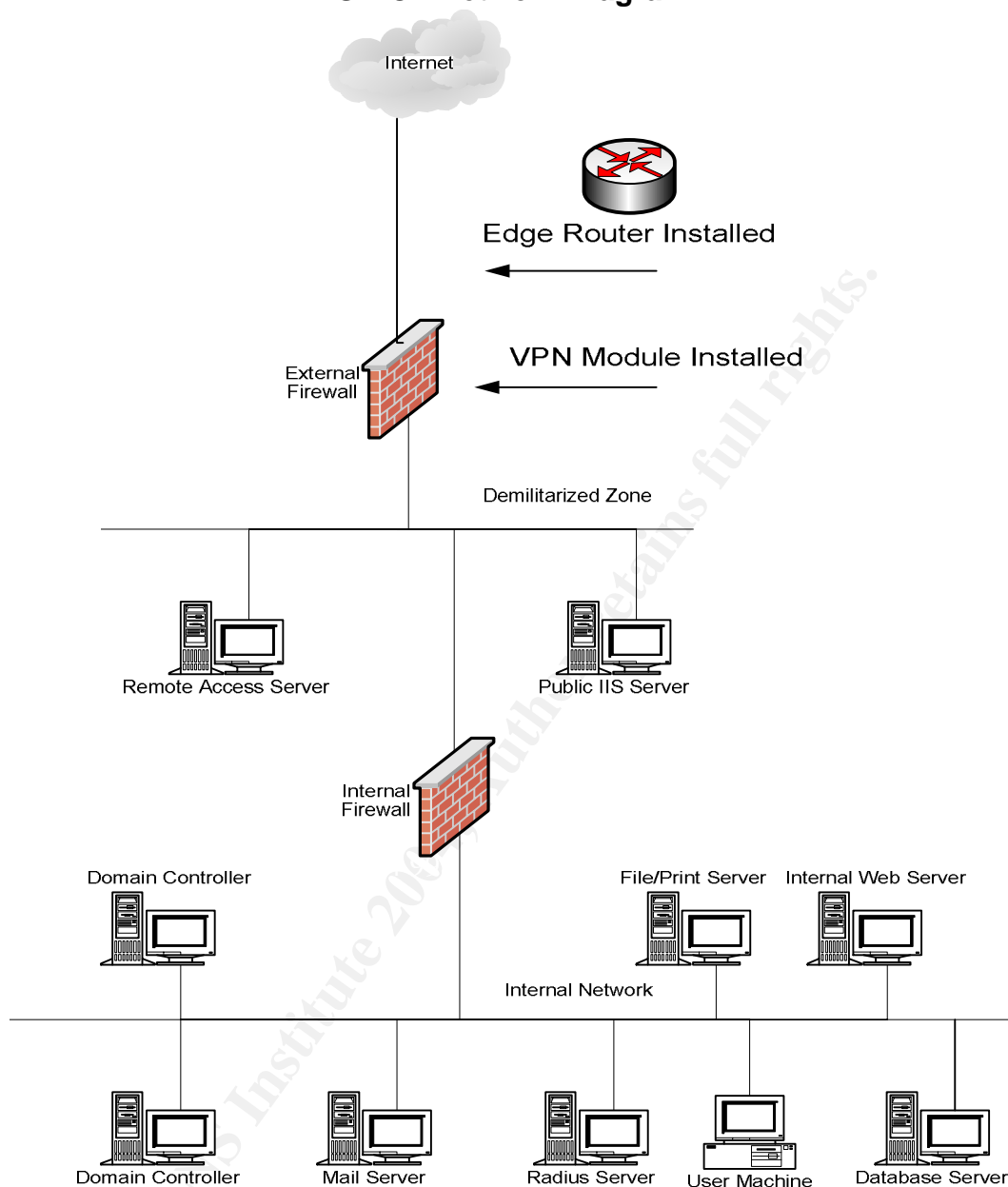


(McCabe, p. 5)

Network Diagram

This network consists of a DMZ containing a remote access server for authentication and authorization of GIACE's remote sales force. Additionally there is an IIS server in the DMZ for a public web presence. Following the merger of GIACE and Sans Co., an edge router was installed between the GIACE external firewall and WAN (shown as Internet below). Additionally a VPN module was installed on the GIACE external firewall. This will allow for a router-to-router VPN between GIACE and Sans Co. Because of this, we are able to set up an L2TP VPN over the WAN between networks, which allows for strong authentication (MS-CHAPv2) and the strongest possible encryption (168 bit 3DES).

GIACE Network Diagram

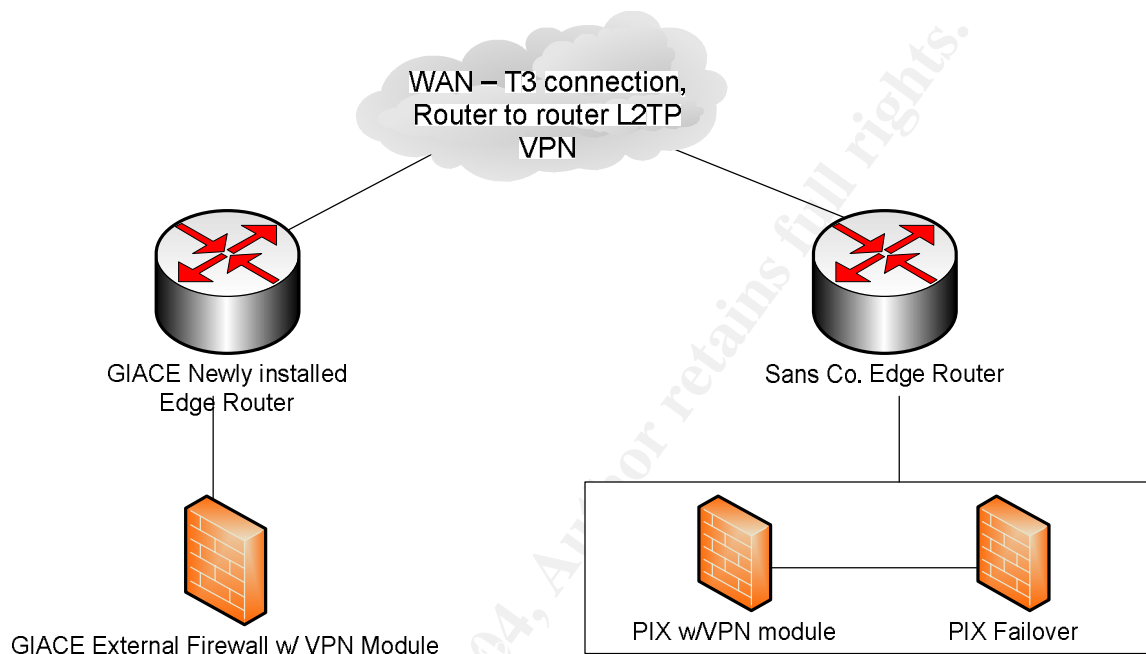


(McCabe, p. 3)

Additionally, I have attached a diagram representing the newly established WAN link between, which is a T3 connection between GIACE's Ann Arbor, MI location and the Denver, CO location of Sans Co. You may think that because this is a private T3 connection between Sans Co. and GIACE, there is no need for a VPN between the two physical sites. Sans Co., however, is highly concerned with layered security and employs a defense in depth strategy wherever possible. The T3 connection allows for enough bandwidth that creating a VPN does not significantly degrade or slow down connectivity. Additionally, since we do not know where the physical link goes once off our site(s), questions arise as to the security measures taken by the vendors supplying the T3 connection. Possible

exploits could easily include man in the middle attacks, thus management at Sans Co. thought it best to allow for the additional level of security. Finally, the cost of deploying this technology is small in both administrative overhead and hardware costs, so it made business sense to employ this technology.

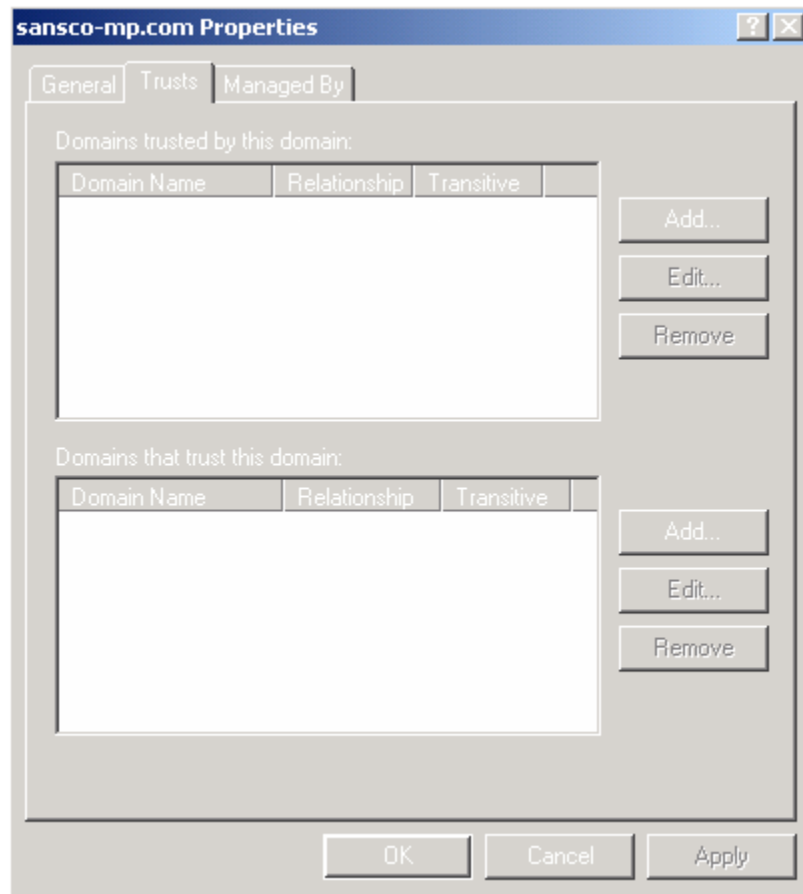
GIACE and Sans Co. WAN



Trusts

External one way (intransitive) trusts have been established between GIACE and Sans Co., which allows for authentication of GIACE and Sans Co. employees across the WAN link. As sansco-mp.com is the root domain, the trusts are established between GIACE.com and sansco-mp.com. There is no transitive trust between forests in Windows 2000; therefore, the Active Directory Global Catalog, Naming Contexts and Schema are not replicated across the WAN connection. Since this is an intransitive trust however, the other three domains in the Sans Co. AD structure must create external intransitive trusts between GIACE if users in these three domains are to be allowed to access GIACE resources and vice versa. This would allow for any of the four Sans Co. domain users to authenticate to GIACE and, for example, be able to access and share marketing, financial, or Human Resource data between the two forests. This would also allow the remote sales forces of both GIACE and Sans Co. to access web servers as well as internal database servers located in the other forest. Below is a screen shot taken from the Sans Co. DC on how this trust is set up on Sans Co.'s DC. In order for Sans Co. employees to be able to access GIACE's resources, the same trust relationship will be set up on GIACE's DC's; only

sansco-mp.com will be in the “domains trusted by this domain” window, and giace.com will be in the “domains that trust this domain” window.

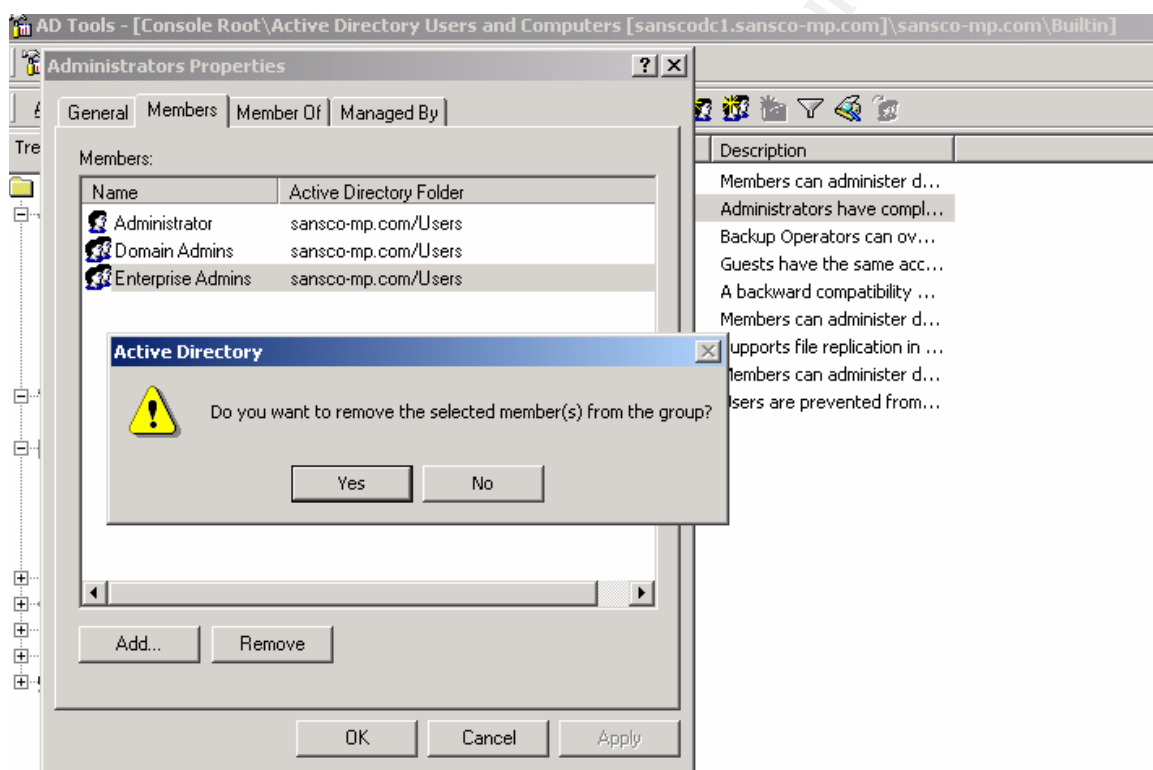


In addition, as mentioned previously, there also exist external (intransitive) one-way trusts between the web server domain and all other domains within Sans Co. and GIACE. These trust connections would all be one way in that the web server domain would trust the other domains, but the other domains would not trust the web server domains. It is established in this manner so the appropriate users at Sans Co. and GIACE can access the web server domain and the web servers themselves.

Managing multiple forests

Management of multiple forests ultimately rests on the shoulders of IT departments in both GIACE and at Sans Co. Political pressures have dictated this, as each company IT Staff is wary of allowing “those guys” from the other company administrative access to their networks. However, in order to gain economies of scale and to reduce overhead, the IT departments have been consolidated under one management structure and into one OU on the sansco-mp.com domain. The Sans Co.’s CIO has been named the CIO of the entire organization. This does not mean that either IT staff has lost control over “their”

systems however. Additionally the new CIO of the organization has been established as the Enterprise Administrator (EA) for each forest. However, the power of the EA has been restricted in each forest to being able to authorize new domains. The individual domain administrators still have power over changes within their domains, to Group Policy, etc. This is done by removing the EA group from the local administrators group on the Domain Controllers as shown below. One advantage to doing this is that it IS reversible, meaning that you can back out of the change if need be. Another advantage is that it politically, only the CIO is in charge of all forests and domains; however, each domain still may have its own respective domain administrator. This allows a sense of control over the domain and network (Fossen. Windows 2000/XP/2003 Active Directory, p.140.)

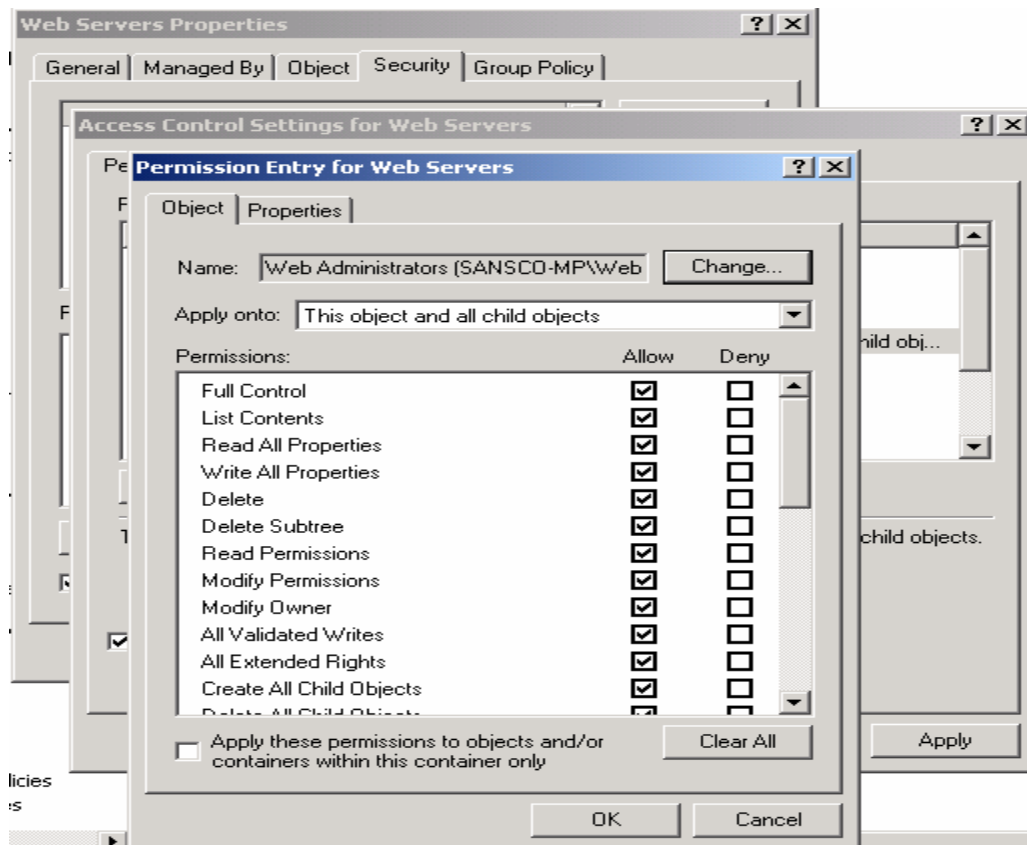


Delegation

At the highest level, there is the Enterprise Administrator, which we have stripped of relative power in the Sans Co. and GIACE domains. Below the Enterprise Administrator, there are Domain Administrators, and below this is the bulk of where the authority is delegated – at the OU level. Granted, in an organization that is relatively small such as Sans Co. or GIACE, there will be some overlap as the OU Administrators may in fact administer several OU's; however this structure and policy is in place specifically to allow us to separate authority amongst our different OU's. It also provides a framework for future growth, should there be more acquisitions, or should there be an increase in the size of the existing company. For example, our internal Web Server OU was created to

be able to apply Group Policies, and add/remove users and computers to the OU. Because these servers are so mission critical, it is important to delegate authority to them to only a select few administrators who can be trusted to maintain both the functionality of and security of these servers. Furthermore, as authority is delegated over OU's, it is important to assign permissions based on Global Group membership, and not specifically to users themselves. By doing this we can merely edit the group membership, which will automatically edit the administrators of the OU where that group was given permissions. The only time we would do this is in the event of gaining or losing an employee performing the function of a Web Administrator. If this were the case, it would need to follow a set procedure for adding or deleting a user. Human Resources would coordinate this effort through a well-defined process for granting access to new employees or system deleting access. The owner of that process for the IT Staff then either creates the new user and adds permissions or assigns the task to the owner of the Web Administrators OU to grant access. Specifically we need to create the initial Global Group and put it into the OU it will have permissions on. In this case, the Global Group "Web Administrators" is the group given control over the Web Servers OU. Following that, I give the group full control over the OU by right clicking the OU, then going to Properties, Security Tab, adding the Web Administrators group, then clicking on the Advanced Tab. At this point, the Web Administrators are only given Read access to this object; however, selecting this group and then clicking view/edit will give us the option to set permissions, as shown below. I will give full control over this object and all child objects in both the Object and Properties tabs of the Permission Entry for Web Servers window, then click OK 3 times to have the changes take effect. Taking this one step further, the Web Administrators group can be added to the local administrators group on every computer within the OU if desired.

© SANS Institute



Consolidated IT Overhead and Economies of Scale.

As stated, a main goal of consolidating and creating this network and AD structure is to consolidate IT operations, which will allow for reduced overhead. This reduction occurs not only in actual costs, but also in administrative overhead. As Sans Co. joined and added companies and domains one by one, the need for separate IT staff at each company and in each domain was reduced. Furthermore, as the locations physically merged the need for additional onsite technicians lessened. Because of this, Sans Co. was able to reduce IT Staff, which saved on cost and reduced overhead. In terms of reduced administrative costs, we were able to remove IT Staff OU's from each domain at Sans Co. except in the sansco-mp.com domain. Sans Co. technicians now handle IT support and administration for the entire forest. Furthermore, the merger of Sans Co. and GIACE and the trusts set up between the domains allowed for further reduction of IT Staff and for more centrally managed technical support and administration. There still exists IT Staff on-site at GIACE however. This is required for physical access to servers and workstations, and hands-on support. However, due to the way the WAN and AD structure has been set up, administration of moves, adds and changes can now centrally be handled at Sans Co's. headquarters.

Reduced overhead also needs to be looked at from a technical perspective. The addition of shortcut trusts between the domains at Sans Co. has reduced Kerberos traffic and therefore reduced overhead in the form of authentication traffic. This is discussed above on the section regarding the AD structure at Sans Co. Further reduction in IT overhead occurred when the DC's of Little Soy, Boxes, and Fortune Co. were added into the Sans Co. forest. Upon promoting these new servers to Domain Controllers, there is a question in DCPROMO.EXE asking whether you want to create a new forest or join an existing one. Since sansco-mp.com already exists as the root domain, we merely need to add these to the existing forest, which allows for the following:

- New domain will not create its own Schema and Configuration Naming Context and will instead copy from sansco-mp.com. The Schema represents the blueprint of AD. The Configuration NC holds information about sites, subnets, replication transports, trusts, and other services; which means that this information is only entered once and will then replicate across the different DC's in the forest.
- The Global Catalog replicates automatically between sansco-mp.com and the new domain(s). The Global Catalog is a subset of the AD database (approximately 55% (Fossen. Windows 2000/XP/2003 Active Directory, p. 86)) which consists of all objects in AD, but not all properties of all objects. In our forest, there are two Global Catalog Domain Controllers. Because all of our internal users are physically located in the same space, this is all we require to allow for redundancy and still allows for fast speeds on object searches. Additionally, it minimizes replication traffic and reduces overhead bandwidth being used for replication when it can be utilized in other ways.
- Enterprise Admins group is automatically added to the Administrators group on the DC's (however, we have shown how that power is delegated/limited).

Physical Security

A discussion of Windows security or security in general would be lacking if there were no mention of physical security. For this reason, I am listing some physical and technical controls that have been implemented at Sans Co. to ensure that physical security of the DC's is in place.

- Syskey.exe is being used on DC's at Sans Co. This program creates a 128-bit RC4 encrypted system key, which in this implementation is stored on a floppy disk with backups of the key kept, secured in off-site locations. The floppy method was chosen to allow administrators to complete unattended reboots. Additionally it takes the system key off the local hard drive, therefore off any backup media as well.

- DC's at Sans Co. are kept in a room that is always locked with keycard access. Access is granted by the HR department who are in charge of the keycard system.
- DC's are furthermore in a keycard accessed room with cables reaching into the outer room for access to the keyboard, monitor and mouse. This is due to the system key being stored on a floppy that is continually inserted into the floppy drive. DC's are connected to a KVM to better utilize space.
- DC's and all servers are located in locked cabinets and on a raised floor, which mitigates risk against water damage from flooding, or sprinklers for example.
- The Network Control Center had redundant UPS and AC units to ensure power and climate are regulated accordingly.
- There is a well-documented process for backups of DC's and all servers, with backup copies sent to a secure off site location.

Security Policy and Tutorial

Group Policies on IIS Server

Description

There are several ways to use Group Policy to help secure a server. At Sans Co., security is stressed for both external Sales personnel as well as on its web servers. Because of this, Sans Co. has developed two specific group policies to address these security needs.

Password Policy

The first policy to be discussed is the password policy, which affects not only the Sales force working remotely, but also any user, system, etc., which requires authentication against the domain. The password policy is further affected by the fact that PPTP is used as the VPN for remote users and PPTP encryption can be sniffed and then run through a password cracker like L0phtcrack. Additionally, even though we use Kerberos v.5 for authentication, this traffic can be sniffed and brute forced as well to reveal passwords. "Kerberos authentication traffic can be "sniffed" and a brute-force attack can be mounted to attempt to reveal the user's password. This is possible because, ultimately, the user's master key is derived from the user's password, and this key is used to encrypt sniffable data during the AS Exchange." (Fossen. Windows 2000/XP/2003 Active Directory, p. 34). Kerberos authentications use an MD4 hash of a users password to generate the master key, which is used in the AS exchange granting that user a TGT. KerbSniff captures this traffic, and KerbCrack attempts to break the MD4 hash of the user's password. Ntsecurity offers a tool for this called KerbCrack,

which includes KerbCrack and KerbSniff programs. Find it at <http://ntsecurity.nu/toolbox/kerbcrack/>.

To demonstrate this point, I downloaded and installed KerbCrack and KerbSniff into a test environment. The programs themselves are small and surprisingly (or scarily) easy to use. This demonstration shows KerbSniff and KerbCrack attempting to sniff then subsequently crack someone logging into the Administrator account in a test domain named GIAC. The first step after installing the software is to start the KerbSniff program, shown below:

```
C:\KerbCrack>kerbsniff kerb_sniff_results.txt
KerbSniff 1.2 - (c) 2002, Arne Vidstrom
               - http://ntsecurity.nu/toolbox/kerbcrack/

Available network adapters:
    0 - 10.1.1.2
    1 - 192.168.249.1
    2 - 192.168.24.1

Select the network adapter to sniff on: 0
Captured packets: * _
```

The program determines enabled network adapters on the machine, and prompts your input as to on which adapter you would like to capture packets. Subsequently, it will display the "Captured packets:" text. This will remain blank until there is actual Kerberos traffic (as described above). Upon capturing packets, it displays an asterisk. This will then populate the information in the file established upon executing the program (kerb_sniff_results.txt in this case). The result will be the account name, domain, and MD4 hash value of the password. This illustration is below:

```
Administrator
GIAC
37EA97A067EF210D54E62049BB72A45909E1545A9E19E82DC459781F20CF05BDFDDE1C2
C70EF9F32010F35E4A8D642A87A057AB1
#
```

We then run KerbCrack, which has the following options:

```
C:\KerbCrack>kerbcrack
KerbCrack 1.2 - (c) 2002, Arne Vidstrom
               - http://ntsecurity.nu/toolbox/kerbcrack/

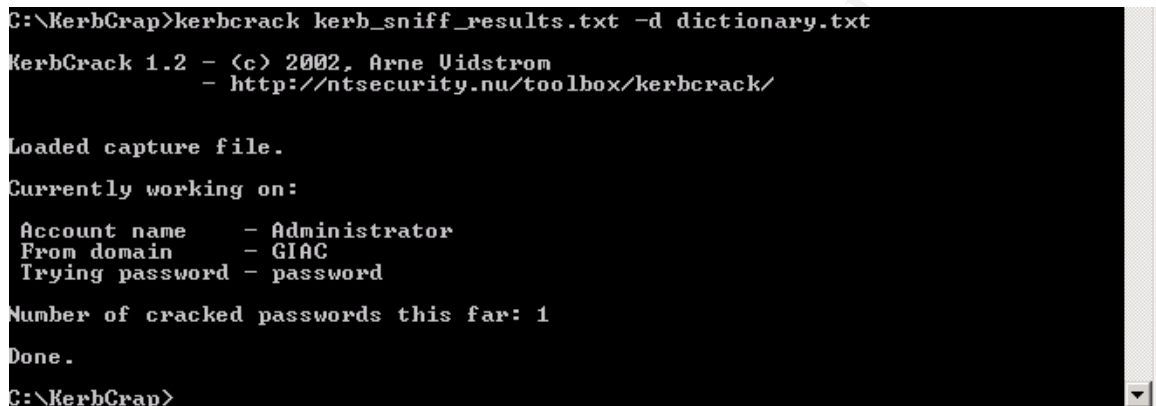
Usage: kerbcrack <capture file> <crack mode> [dictionary file] [password size]

crack modes:
    -b1 = brute force attack with <a-z, A-Z>
    -b2 = brute force attack with <a-z, A-Z, 0-9>
    -b3 = brute force attack with <a-z, A-Z, 0-9, special characters>
    -b4 = b1 + swedish letters
    -b5 = b2 + swedish letters
    -b6 = b3 + swedish letters
    -d  = dictionary attack with specified dictionary file

C:\KerbCrack>
```

In this example (and to simplify the demonstration), I have chosen the password "password," and created a sample dictionary (dictionary.txt) with only the word password in it. As you can see, there are various other options to KerbCrack including various brute force attacks and a dictionary attack. A simple Google search reveals several dictionaries available online. A site with free downloads is <http://www.accessdata.com/dictionaries.htm>. Openwall (the makers of password cracker John the Ripper) offers a CD for purchase at <http://www.openwall.com/wordlists/>.

KerbCrack, once run, will both display the results on screen;



```
C:\KerbCrack>kerbcrack kerb_sniff_results.txt -d dictionary.txt
KerbCrack 1.2 - <c> 2002, Arne Uidstrom
               - http://ntsecurity.nu/toolbox/kerbcrack/

Loaded capture file.
Currently working on:
Account name    - Administrator
From domain     - GIAC
Trying password - password
Number of cracked passwords this far: 1
Done.
C:\KerbCrack>
```

As well as save it to a text file with a .crk extension:

```
Account name - Administrator
From domain  - GIAC
Password     - password
```

Of course, this test was trivial and took less than a second to crack, however KerbCrack has the ability to go through one million words in less than 10 minutes with a 533 MHz. Celeron processor (KerbCrack FAQ).

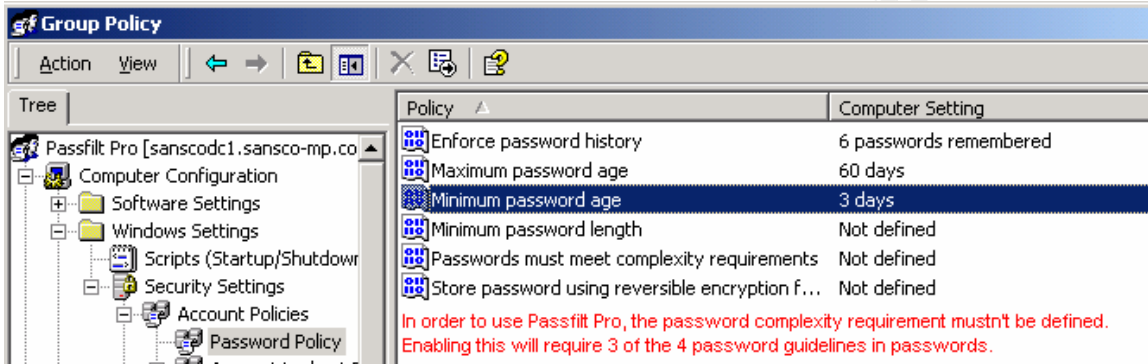
Because of this, it is imperative to have a strong password policy, but also to educate end users and to provide technical controls that require strong passwords. Several resources are available to enforce strong passwords, either in complexity or length, or in both. Microsoft includes this functionality to some degree in Windows 2000; however, there are some limitations. These limitations are described below:

- Even though Windows 2000 supports passwords/passphrases up to 127 characters long, Group Policy does not allow more than a 14-character password length.
- Enabling the registry key (Passwords must meet complexity requirements - below) that requires complexity does NOT necessarily mean that a

password is strong. It does mean that passwords must meet 3 of the 4 requirements:

- Contains uppercase letters.
- Contains lowercase letters.
- Contains numbers
- Contains non-alphanumeric symbols.

This coupled with a short password length requirement equates to a weak password, for example, the password “Ball11” would be trivial to brute force.



For this reason, a custom password filter should be used to enforce the company policy, which will ultimately increase the security at Sans Co. In this example, I have chosen Passfilt Pro, which retails at \$295 per DC. Changes need only be made to one DC; since replication will ensure that the other DC's are updated with the password filter.

Passfilt Pro is an excellent tool, which is user friendly and allows you to be very specific with the policy you set for passwords. To use, you need to disable the option for “Passwords must meet complexity requirements” from above. For our policy, I have listed below the portion of our policy, and then listed how Passfilt Pro provides the technical control to apply the policy.

- POLICY: Our network requires passwords of at least 16 characters long
 - Passfilt sets the maximum number of characters, then you apply minimum number of each of the 4 required sets of characters (upper, lower, special and numbers). Here the minimum for each is 4 and the maximum is 12, that way you always have at least 16 character passwords, but nothing longer than 30. ***Please note that Passfilt Pro did not allow a password longer than 30 characters long, which is why our policy states 30 as the maximum password length. Otherwise with these password rules you could have a password of 48 characters long.
- POLICY: Contain at least 4 but no more than 12 of both upper and lower case characters (e.g., a-z, A-Z)

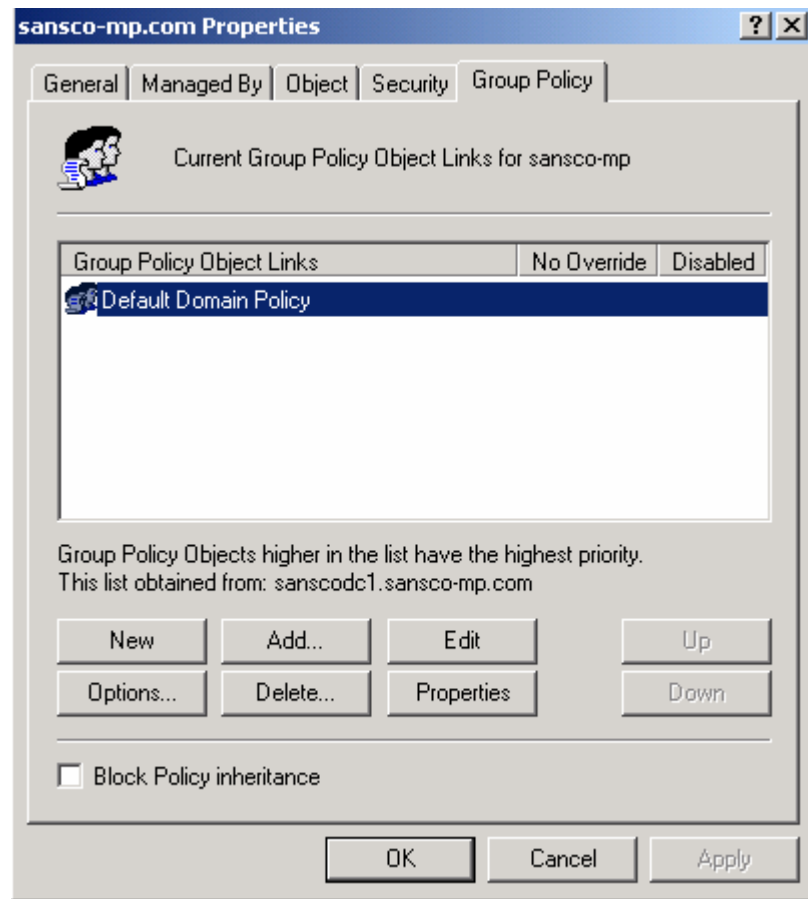
- Passfilt allows you to set minimum and maximum levels of upper and lower case numbers.
- POLICY: Have at least 4 but no more than 12 of both digits and special characters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:~';<>?,./)
 - Passfilt allows you to set minimum and maximum levels of numbers and special characters
- POLICY: Are not words in any language, slang, dialect, jargon, etc.
 - Passfilt can check the user's proposed new password against a customizable dictionary.
- POLICY: Passwords should not contain your username.
 - Passfilt Pro has a checkbox that allows you either enable or disable this function.
- POLICY: Are not based on personal information, names of family, birthdates, etc.
 - Passfilt can check the user's proposed new password against a customizable dictionary.

The document "Passfilt Pro Documentation" contains detailed information on how to set up and apply the custom password template, so I will not rehash that information here. I will explain how that policy can be applied specifically to the Domain, which will inherently apply it to all OU's within the domain. Per Microsoft KB Article 255550, Windows 2000 allows only one domain account policy per domain. This applies to policies such as password policy and account lockout policy.

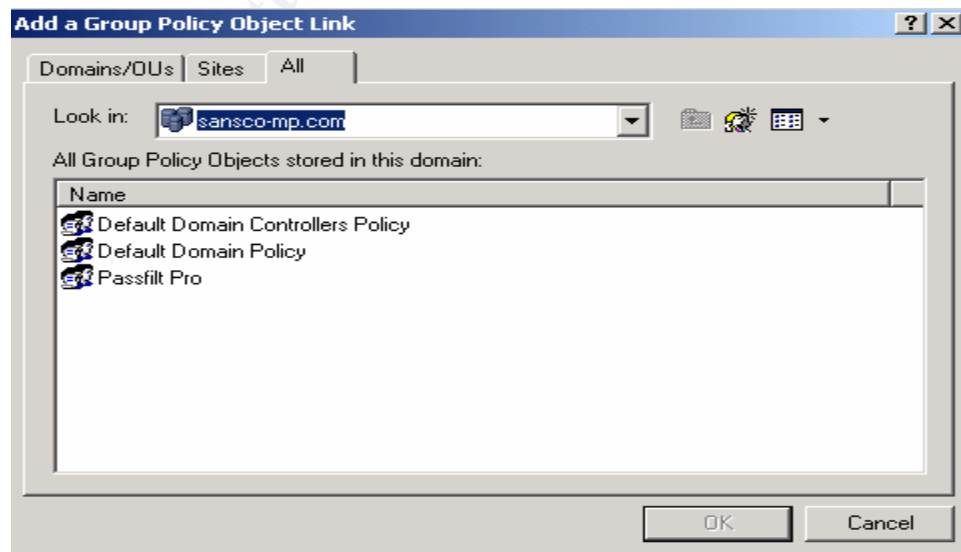
In our example, we are assuming that it is imperative for not only the Sales force, but also all end users to use strong passwords, so we will apply the policy to the entire Domain (which will apply it for both users and workstations).

To do this we perform the following:

1. Browse to the Active Directory Users and Computers MMC snap-in, expanding it and then browsing to the sansco-mp.com domain.
2. Right click on sansco-mp.com, and then browse to the Group Policy Tab.



3. Click Add, and then click the "All" tab, which will show our Passfilt Pro Group Policy (that has been added through the installation of Passfilt Pro).



4. Click Passfilt Pro, and then press OK.

5. Make sure to move the Passfilt Pro Group Policy UP so it takes precedence over the Default Domain Policy.
6. Click OK once more to apply the policy.

Through this, the custom password filter has been added to the sansco-mp.com domain.

Custom Password Filter Policy Evaluation

In order to verify that our policy has been applied and is in fact working, we need to audit the policy. This is done by performing a stimulus and response test and verifying that the results match the intention of the group policy.

Stimulus 1

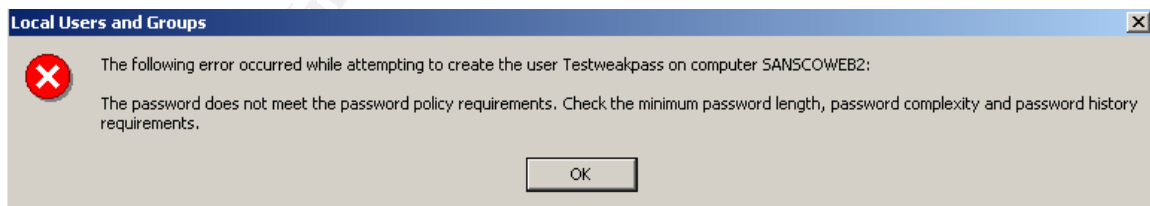
Create a user account with a password that is considered weak (does not comply with password policy), and see what the result is. Our expected response will be that we will not be able to create the account without complying with the password policy (and technical controls that enforce it). The password we will test is "Password123" which does not meet complexity requirements or password length.

Stimulus 2

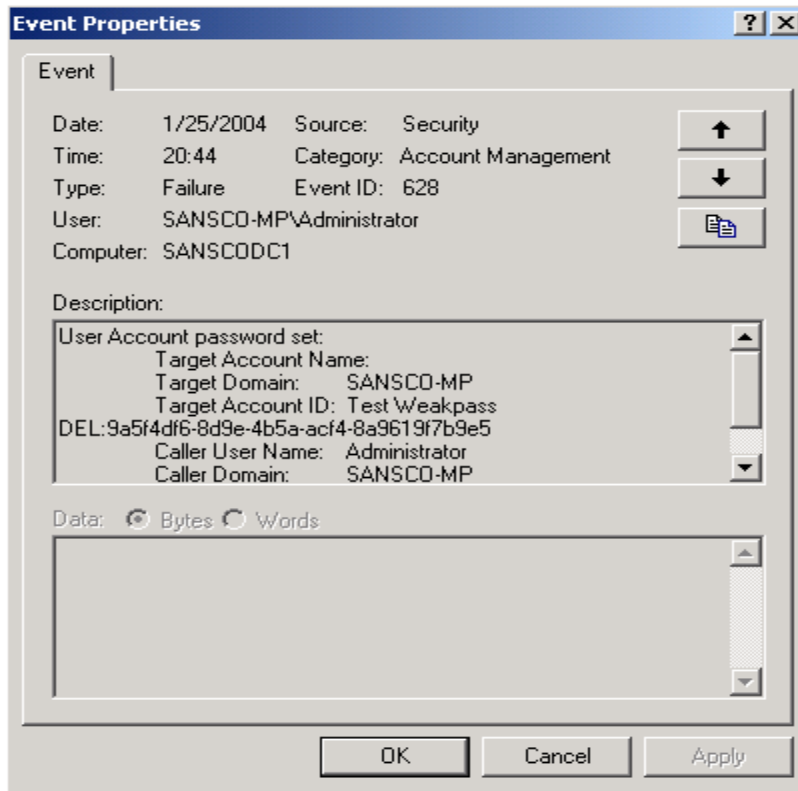
Create a user account with a strong password (one that complies with our password policy) and see what the result is. Our expected response will be that we will be able to create the account. The password we will test is "1q@W3e\$R5t^Y7u*I9o" which meets the requirement of length and complexity in our Passfilt Pro Group Policy as well as in our password policy.

Response 1

The user could not be created because the password did not meet complexity requirements or password length.

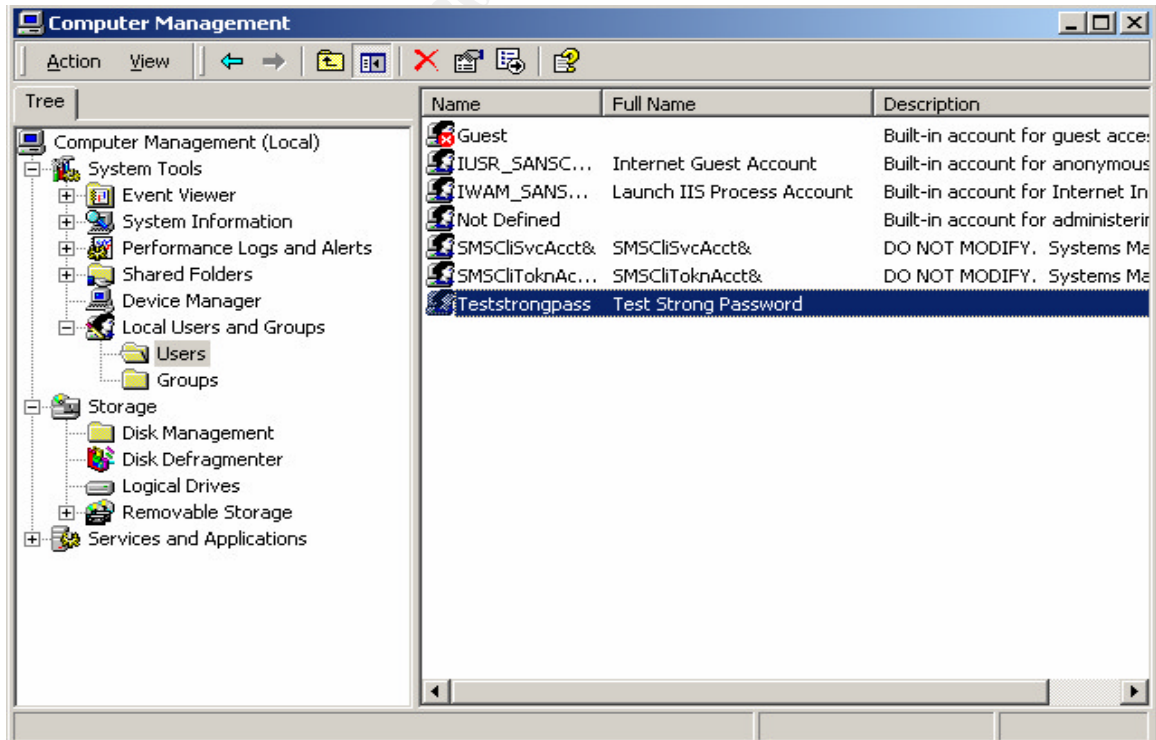


Additionally, a security event (ID 628) is generated when a password is (attempted to be) created for a new user that does not meet complexity requirements. This is shown below:



Response 2

The user (Teststrongpass) was created successfully as the password met requirements for complexity and length and history.



Microsoft Internet Information Services (IIS)

Brief overview of IIS "Security"

Windows web servers running IIS 5.0 (or any version of IIS) can be very susceptible to attack for several reasons. The most obvious is that they are directly connected to the internet and can easily be accessed from anywhere on the internet. Furthermore, IIS has long been the scourge of security for network administrators. This is of course not to say that IIS cannot be reasonably secured!

Back as far as the year 2000, IIS has been on the radar for security, network administrators, and hackers in the black hat community. When the SANS Institute published their list of top 10 vulnerabilities in July 2000 (<http://www.sans.org/top20/top10.php>), IIS (or components of) were the number two and 4 vulnerabilities. When the October 2001 list was published (http://www.sans.org/top20/top20_oct01.php), an IIS web traversal vulnerability was number one on the list, and three of the top five Windows vulnerabilities were IIS as well. The following year's list of October 2002 (<http://www.sans.org/top20/oct02.php#W1>) finally stopped just listing specific components of IIS as vulnerabilities, but merely listed IIS 4.0 for Windows NT and Windows 2000's IIS 5.0 as the number one vulnerability. Lucky for all those administrators and security professionals that in October of 2003 (<http://www.sans.org/top20/#w1>), IIS was able to retain its place as the most dangerous security threat for Windows systems! Looking into the future, I would think the chance of IIS remaining the biggest security vulnerability for Windows machines is good. For reference, I have attached in Appendix B the Sans/FBI entry into the top 20 list for IIS, which contains various CVE entries, links to Microsoft, and other very helpful remediation tactics.

Finally, there are several ways to stay on top of IIS security, such as signing up for different mailing lists that warn you of new vulnerabilities, as well as patch information and/or mitigation strategies. A couple of the best to keep you abreast are:

Microsoft:

<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/notify.asp>

SANS Institute:

Create an account on the www.portal.sans.org website, and then subscribe to "@RISK: The Consensus Security Alert".

Minimal IIS 5.0 Server Security

In order to secure IIS, various things need to be done. At Sans Co., web servers exist both internally and externally. The external web server(s) are administered

via Group Policy through Active Directory in their own domain and do not replicate within the Sans Co. forest. Because of this, any changes made to secure these servers must take place independent of changes made to the web servers on the internal network. For the sake of this paper, I will apply changes via Group Policy to the internal web servers since I am unable to replicate the web server domain; however, these changes would be made and IIS would be secured in the same way to the web server domain as they are in the Sans Co. domain.

We have already established delegation of authority over the web servers OU to the Web Administrators Global Group. From there, how do we secure IIS? Sans Co. has a policy in which web servers are brought into the network and secured at a bare minimum in the following manner:

1. Web Servers are built as Windows 2000 Server with the latest Service Pack (SP4) applied. Service Packs contain the appropriate hot fixes and patches for IIS as well.
2. Most up to date (post SP4) hot fixes are installed from CD via a qchain (qchain.exe).
3. Web servers are first built as standalone, not connected to the network or internet in any way, and remain standalone until fully secured.
4. IIS is installed (a default installation at first)
5. Latest IIS hot fixes (usually they come out one by one or in a cumulative patch containing several of the latest) are installed from CD, via a qchain (qchain.exe) if necessary.
6. IIS lockdown tool is run, providing the highest, most restrictive level possible with the lockdown tool. This includes disabling WebDAV, which is not used in the environment.
7. UrlScan is installed to lock down and protect against incoming requests.
8. All sample, help, and script files are removed.
9. Operating System tools such as cmd.exe are removed and stored on a CD, which can be loaded when these are required for administration of the server or applications residing on the server.
10. Resource kits and Software Development Kits are removed or never installed on the server itself. Instead, CD's with them are used when needed.
11. Internet printing is disabled (this is also enforced by using hisecweb.inf – see below)
12. Unnecessary services are disabled. This of course depends on exactly what is being run on the server and is the decision of the system and security administrators. (This is also enforced by using hisecweb.inf – see below)

Once these steps are completed, the server can be brought into the network and from there on out managed by Group Policy and a patch management policy. As of yet, there is no way to deploy hot fixes via Group Policy; however, new Service

Packs (via .msi files) can be deployed via Group Policy. As we saw with the brief overview of IIS, there are always new vulnerabilities found with IIS that require patches to be installed and because of this, I have added a brief section on patch management at the end of this section.

IIS Group Policy – Security Templates

Earlier I had mentioned that password strength was imperative in our environment, and we deployed Passfilt Pro to assist us with enforcing a custom password filter requiring a strong password. We duplicate (but not replicate) this policy in our DMZ, ensuring that we apply it and move it ahead of our Default Domain Policy. This will ensure that the password rules set by Passfilt Pro take precedence over the Default Domain Policy, which will be effected by the use of our template. Additional steps still need to be taken and applied directly to our web servers AD domain in the DMZ. Additionally, in the next section I will discuss auditing of our environment, to which the cornerstone is our Audit Policy and Event Logs (especially Security Event Logs). So how can we tie in web server security, password policy, and event logging? The easy answer is with a security template. Microsoft offers Hisecweb.inf as its answer, and this is available from the NSA at <http://nsa1.www.conxion.com/>. Microsoft also offers it for download in KB Article 316347. It is possible to apply these templates through Group Policy, which will automatically update every web server in the OU where we apply it (as opposed to updating one server at a time as we do upon a new server build. If we did want to apply templates upon the server build, this is also possible through the Security Configuration and Analysis MMC snap-in.).

Hisecweb.inf is the template recommended by the NSA for Windows 2000 systems to help secure IIS 5.0 web servers; however, in our configuration, we will need to modify the file before applying it to ensure we are meeting Sans Co.'s security standards.

The original Hisecweb.inf file is located in Appendix C, and the complete modified version (hisecweb_v2.inf) is attached in Appendix D. Below, I recap the changes we have made from the original to our v2 and the reasoning for these changes. Finally, I will show how the template is applied via Group Policy to our Web Servers OU and how we know that the template changes (and our Group Policy) have been applied and enforced.

One more note on using templates and Hisecweb.inf: these templates have been known to cause problems. Please be careful when applying and know exactly how they will change your configuration. Specifically, the hisecweb.inf template automatically sets the "Startup Type" to "Disabled" for the Routing and Remote Access Service (RRAS) and the Telephony Service. In our implementation, our web servers do not need the RRAS service as the VPN set up between the remote workforce's workstation client and the VPN modules

handles that function. The telephony service is used for control of telephony devices using IP, such as in VoIP implementations. This is an unnecessary service as well and disabling it only further tightens the security of these servers. Finally, neither of these services have dependencies, meaning that no services rely on these in order to function, so we know that by disabling them we are not effecting any other applications or implementations on our web servers. More information on Hisecweb.inf is available from Microsoft at the following locations. The References section at the end of the paper notes this as well.

<http://support.microsoft.com/?kbid=272978> – Knowledge Base article 272978 on how Hisecweb.inf prevents the RRAS service from starting.
<http://support.microsoft.com/default.aspx?kbid=316347> – Knowledge Base article 316347 on Hisecweb.inf potential risks (and the IIS Lockdown Tool)
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/seconfig.asp> - Guide to using the Security Configuration Toolset.

Hisecweb v2.inf

Below is a section from the version of Hisecweb.inf that I have reconfigured to apply password policy, enable auditing (security, application and system), and control event logs. The **bold** sections are the sections where changes were made. The parenthesized notes are the justification for and analysis of each policy setting). Two things of note: one, these changes can be made through the Security Configuration and Analysis Tool (GUI) once the Hisecweb.inf file is saved to c:\%windir%\security\templates; two, we are still using our Passfilt Pro custom password filter in addition to the password settings in hisecweb_v2.inf.

[System Access]

MinimumPasswordAge = 2 (**This ensures that users don't merely keep changing a password until they get back to their original password. If this were set to 0 this would be much easier to accomplish**)

CHANGED: MaximumPasswordAge = 60 (To comply with Password Policy)

CHANGED: MinimumPasswordLength = 14 (This is actually controlled by our Passfilt Pro GPO, however we set it to 14 – the maximum possible, in the event that something were to happen to Passfilt Pro. Another reason for setting this here instead of leaving it off is that if left off it would inherit the setting of the local machine, which may be set low.)

CHANGED: PasswordComplexity = 0 (To comply with Passfilt Pro GPO)

PasswordHistorySize = 24 (**Will save 24 passwords, so passwords are rarely if ever reused**)

LockoutBadCount = 3 (Changed from 5 to 3 which will lock out users after three failed attempts. Protects against brute force attacks.)

ResetLockoutCount = 30 (minutes)

LockoutDuration = 0 (Requires administrator to unlock accounts)

RequireLogonToChangePassword = 0 (Does not require a logon to change the password since administrator is resetting)

ClearTextPassword = 0

[System Log]

ADDED: MaximumLogSize = 25024 (in Kb.)

ADDED: AuditLogRetentionPeriod = 1 (Means log is retained for days (below) then cleared).

ADDED: RetentionDays = 15

RestrictGuestAccess = 1 (Restricts Guest users from accessing the System Logs)

[Security Log]

CHANGED: MaximumLogSize = 50000 (in Kb. - increased log file size setting)

ADDED: AuditLogRetentionPeriod = 1 (Means log is retained for days (below) then cleared).

ADDED: RetentionDays = 15

RestrictGuestAccess = 1 (Restricts Guest users from accessing the System Logs)

[Application Log]

ADDED: MaximumLogSize = 25024 (in Kb.)

ADDED: AuditLogRetentionPeriod = 1 (Means log is retained for days (below) then cleared).

ADDED: RetentionDays = 15

RestrictGuestAccess = 1 (Restricts Guest users from accessing the System Logs)

```
-----  
; Local Policies\Audit Policy  
-----
```

[Event Audit]

AuditSystemEvents = 3

AuditLogonEvents = 3

AuditObjectAccess = 2

AuditPrivilegeUse = 3

AuditPolicyChange = 3

AuditAccountManage = 3

AuditAccountLogon = 3

ADDED: AuditDSAccess = 2 (auditing failures of access to AD)

ADDED: CrashOnAuditFull = 0 (Computer will NOT shut down if Security Logs fill)

;PLEASE NOTE

```
-----  
;for the above Local Policies\Audit Policy parameters the following applies  
;3 - both success and failure events are logged  
;2 - only failure events logged  
;1 - only success events logged  
;0 - or not included, means not logged or disabled  
-----
```

[Service General Setting] **(These automatically disable the following services)**

**Dhcp,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDT
LOCRSDRCWDWO;;;WD)"** (will require a statically set IP address which is useful in
forensics. Additionally, the IP's will be NAT'ed via the router configuration.

**Fax,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;WD)"** (Disables the Fax service, a good example of an unnecessary
service which is not required by any applications, therefore needs to be disabled in the
event of current or future vulnerabilities associated with it.)

**Messenger,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;WD)"**

RemoteRegistry,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)" (Requires registry changes be made by a user logged on locally. Users allowed this access will be restricted on this server to Web Administrators)

Schedule,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)" (Disables Task Scheduler, which could be used to launch scripts or batch files detrimental to the health of the server.)

TermService,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)" (Restricts remote access into the system and will require users log on locally to administer the server).

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit\Reg Values\MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect]
"ValueType"=dword:00000004
"DisplayType"=dword:00000000
"DisplayName"="TCP/IP: Syn Attack Protection"

;(This registry entry will provide protections from Syn Attacks)

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2

**;(This registry entry restricts anonymous access to those with explicit permissions only.
;This was the number 5 Windows vulnerability in the SANS-FBI Top 20 in 2002-2003.)**

Of course, hisecweb_v2.inf (our iteration of the template) allows for more than what is listed above. There are additional services and registry edits that the template effects, including RRAS and Telephony Services as mentioned earlier. For a comprehensive description of hisecweb.inf, please see the paper "Hisecweb.inf – An Analysis" by Colleen L'Abbe. This is located at <http://www.sans.org/rr/papers/66/212.pdf>.

Applying the template via Group Policy

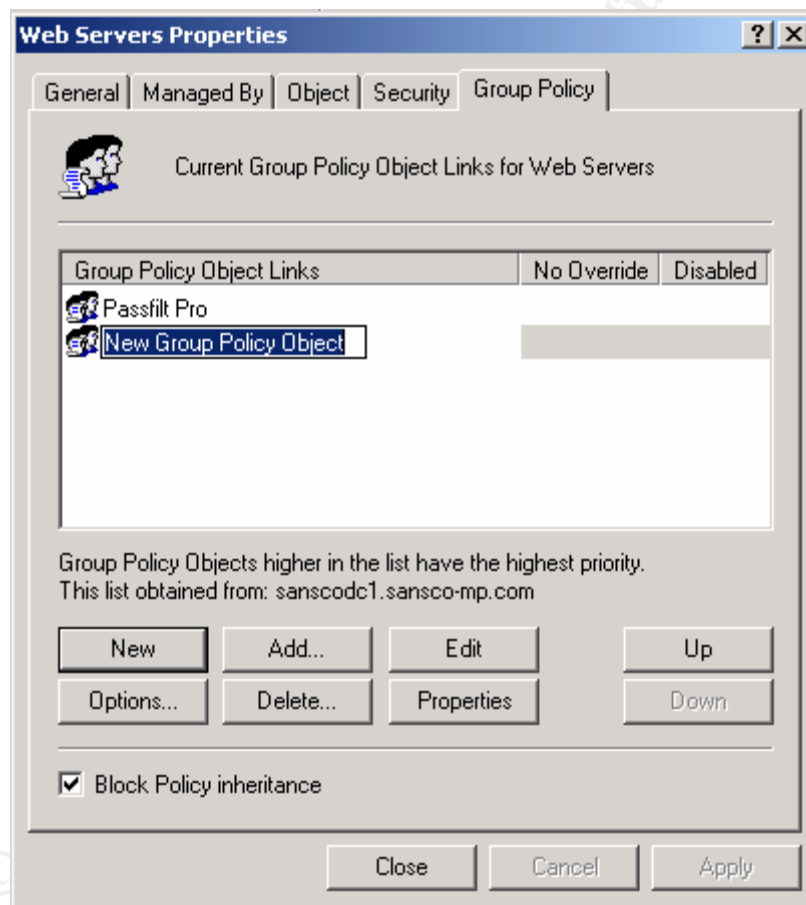
When applying any Group Policy, the GPO can be configured by right clicking on the specific OU you want the GPO to apply to, then selecting Properties, and then the Group Policy tab. You can also create the GPO on another OU or on the Domain itself in the same way. Regardless of where you create it, the GPO is available to any OU, site or domain. In the event that there are conflicting being applied to a single object, remember that the order of precedence is as follows:

1. Local GPO (stored on the machine, not in AD)
2. Site GPO's
3. Domain GPO
4. Organizational Unit GPO's in nested order (outermost to innermost) (Fossen. Group Policy and DNS, p. 66)

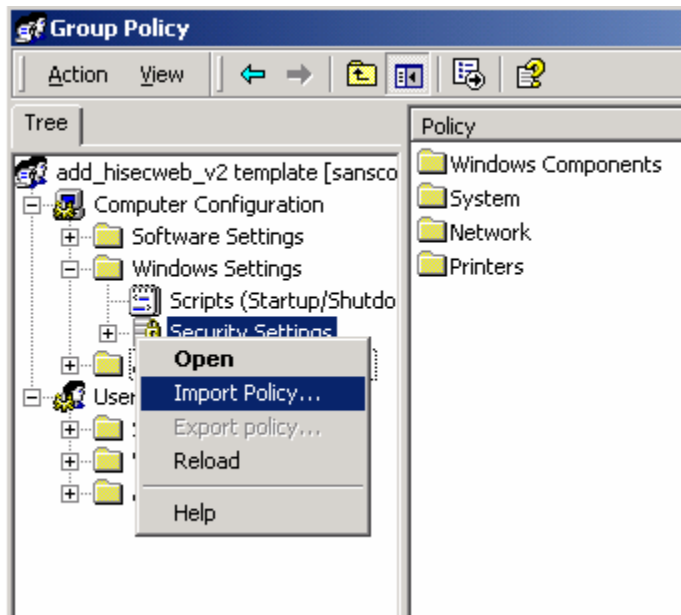
That being said, we will install this Group Policy for the hisecweb_v2.inf template directly to the Web Server Domain. This is done because as before, there are settings in hisecweb_v2.inf that relate specifically to account and local policies, and these may only be set once at the domain level.

Please note that I was unable to replicate this domain in a test environment, so in the following screen shots where the window name is Web Servers, this is actually our Web Servers Domain, not an OU within sansco-mp.com.

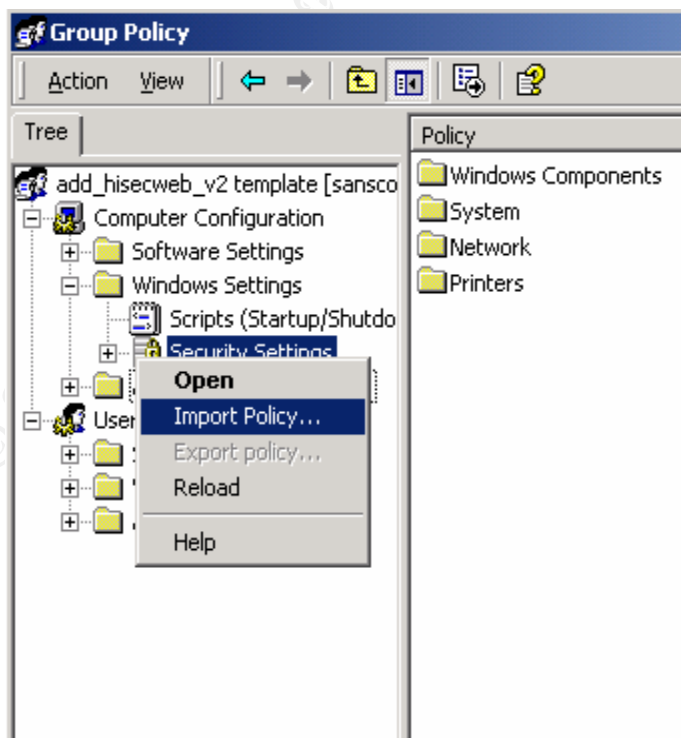
First, we would right click the web server domain (in Active Directory Users and Computers MMC snap-in) and select Properties. Next, we click on the Group Policy tab, then New. I then called the new Group Policy “add_hisecweb_v2 template,” typed where “New Group Policy Object” is highlighted below.



Once that is created, we select our new GPO and click Edit, where the following screen is shown.

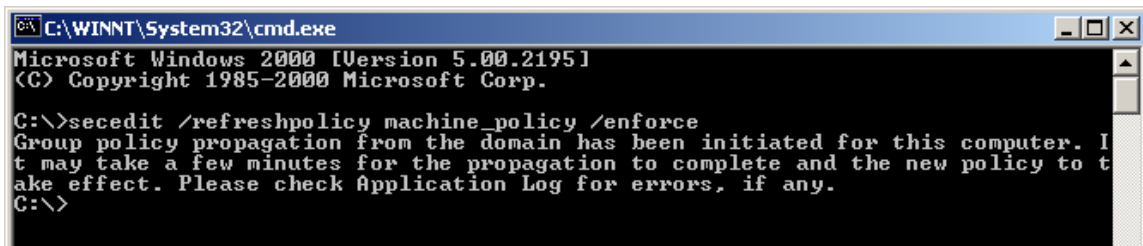


We then browse to Computer Configuration > Windows Settings, then right click Security Settings and Import Policy. From here, the C:\%windir%\security\template folder appears, and since we had already added the hisecweb_v2.inf file, it shows up as a template. Select that template, then Open, and then close the Group Policy window. Click Apply, then OK, which adds this template and will therefore add our settings to the computers in this OU.



Web Server Policy Evaluation

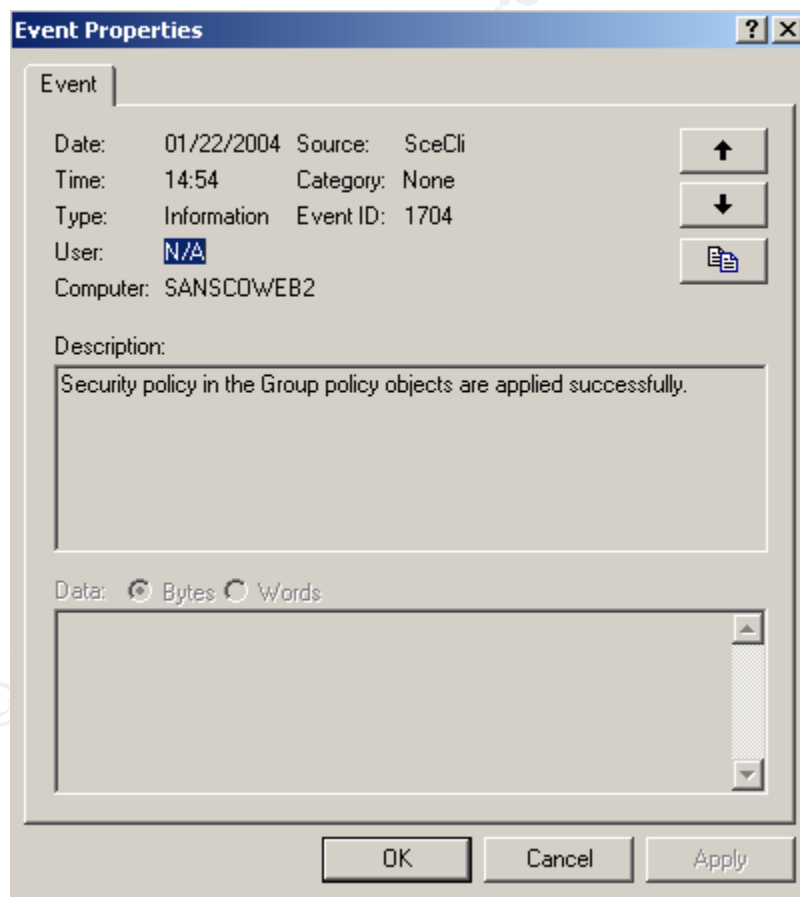
So how do we know that this group policy was applied correctly? We can do two things. The first is to immediately apply the GPO to the web server, and the second is to verify that the policy has been applied by checking the Application Event Log for event ID 1704. To immediately apply the Group Policy, we can use `secedit.exe` from the command line, as shown below.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

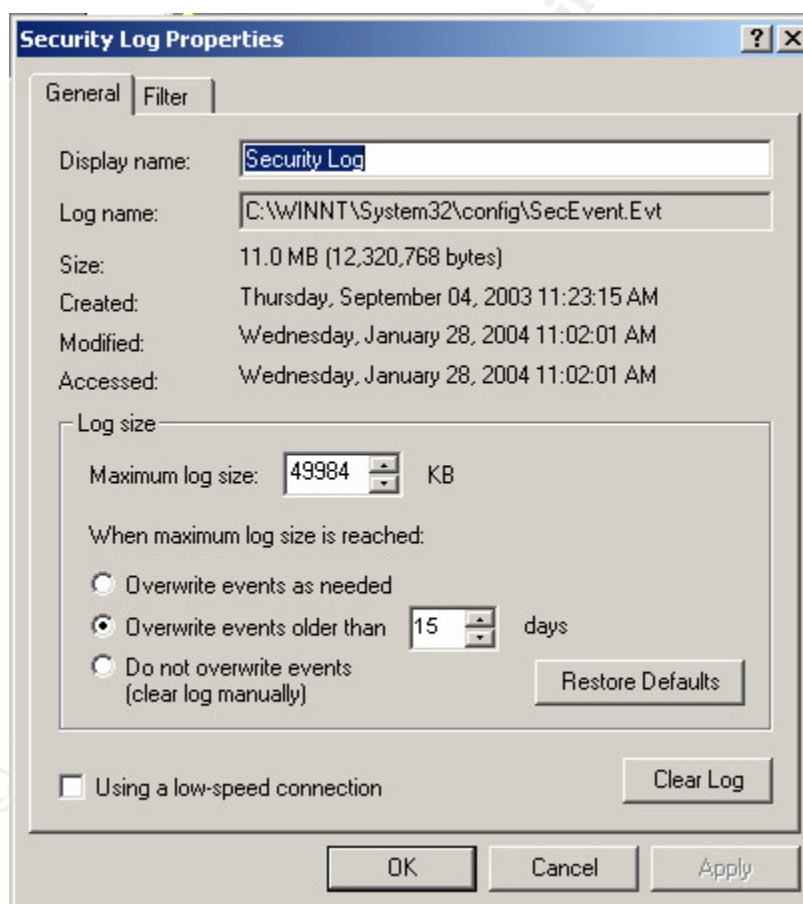
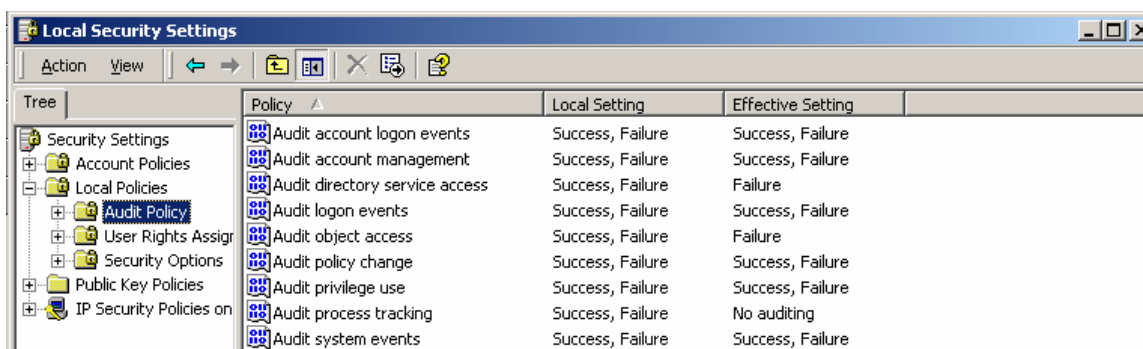
C:\>secedit /refreshpolicy machine_policy /enforce
Group policy propagation from the domain has been initiated for this computer. It
may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>
```

Then we check our event logs and find the following that verifies the successful application of the GPO to our web server.



Finally, we can actually check our Local Security Policy (for password, account policy, and audit policy changes) and the Event Viewer properties (for System, Application and Security event log changes) to verify that the settings we

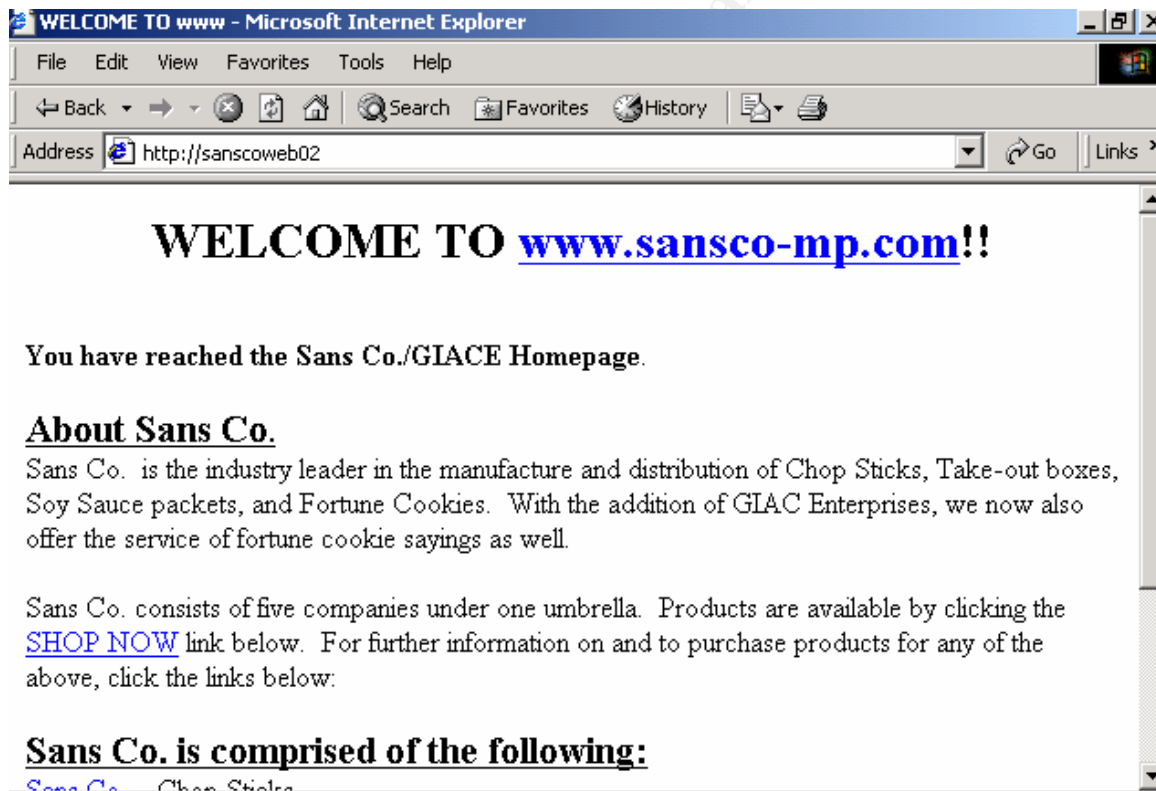
configured (the ones we are particularly concerned with) have been applied. Below are screen shots taken from our Web Server on the audit policy and the Security Log Properties, which represent two of the areas where we made changes using hisecweb_v2.inf. Notice that the effective setting is what we are concerned with as this is the setting set by our Group Policy template.



**In the initial draft of the paper, the settings were verified on the web server, however in the second version; I did not have the resources and could not test the actual application of the template. There were merely minor changes to the template and the application would be similar. The screen shots are taken from the original application of the template, and the Security Log Properties shot was altered to reflect the new setting of overwriting events older than 15 days.

Test for Functionality

Ultimately, any policy setting we change, template we use, or configuration setting will need to undergo a test for functionality. With a web server such as this, the test that speaks the most to retaining functionality is to see that we can still access the web site. To do this, I created a sansco-mp default web site, and then attempted to connect to it from another machine. A result that we see our web page means that we are able to connect. Since users and customer's ability to access our web site is mission critical, this is the most vital test of functionality. In this case, we want to make sure that hisecweb_v2.inf did not alter any registry entries that would hinder access, disable necessary services, or apply any other policy changes that would adversely affect access to our site. Below is the screen shot taken from another server, which shows that we successfully were able to connect to the sansco-mp web site.



Patch Management (IIS or any server)

Due to the problems inherent in IIS especially, and in the Windows 2000 OS in general, patch management requires special attention. Because of this, I would like to touch briefly on this issue.

Patch management requires a few things; the first of course is knowing when new vulnerabilities are released, and furthermore knowing when Microsoft has released a patch for that vulnerability. Since we have signed up for Microsoft's mailing list, we are aware of new patches that are released.

Additional tools can and will be used, such as Microsoft's Hotfix Check Tool, hfnetchk.exe, which is a command line utility that is included with the GUI version, Microsoft Baseline Security Analyzer (MBSA). MBSA performs some basic windows vulnerabilities checks, weak password check (although not even closed to being as good as L0phtcrack or John the Ripper), as well as informing you of security updates not installed on the OS, IIS, SQL, Internet Explorer, and Windows Media Player. In order to use this utility, you would need administrative access to the machine you would like to scan. Additionally, the command line utility (mbsacli.exe) used with hfnetchk.exe provides additional functionality such as ways to handle the outputted results, creation of batch files and automation of the task. Please note that there are several Microsoft Patches that hfnetchk.exe is NOT capable of checking for. KB Article 30640 (<http://support.microsoft.com/default.aspx?scid=kb;en-us;306460>) describes these.

Finally, it is strongly recommend that you always test patches in test environments before applying to production servers. At a bare minimum, apply them first to servers that are less business critical but offer similar functionality (such as first on an internal web server that's used for the Marketing department's intranet site as opposed to the DMZ web server where customers place and verify orders).

Audit

Security Event Logs

In the previous section, we created and applied a template that amongst other things overwrites Security Event Logs every 15 days. There are three main reasons to use a 15 day overwrite policy:

1. The first reason is that we have set our event log size to 50,000 Kb. (with an effective setting of 49,984 Kb. – the maximum log file size). This will ensure that we are not overwriting data due to lack of disk space on the server(s) themselves. In 15 days, we should not go over this size limit therefore will not lose any valuable log information.
2. Secondly, this allows us to collect event logs onto a separate server, running Event Log management software, at a minimum of once every two weeks. Since we overwrite every 15 days, this will allow us an extra day of leeway to collect the logs should an issue arise. Some examples of this software are GFI's LANGuard S.E.L.M. and Aelita. Microsoft Operations Manager (MOM) is also software that collects Event Logs over

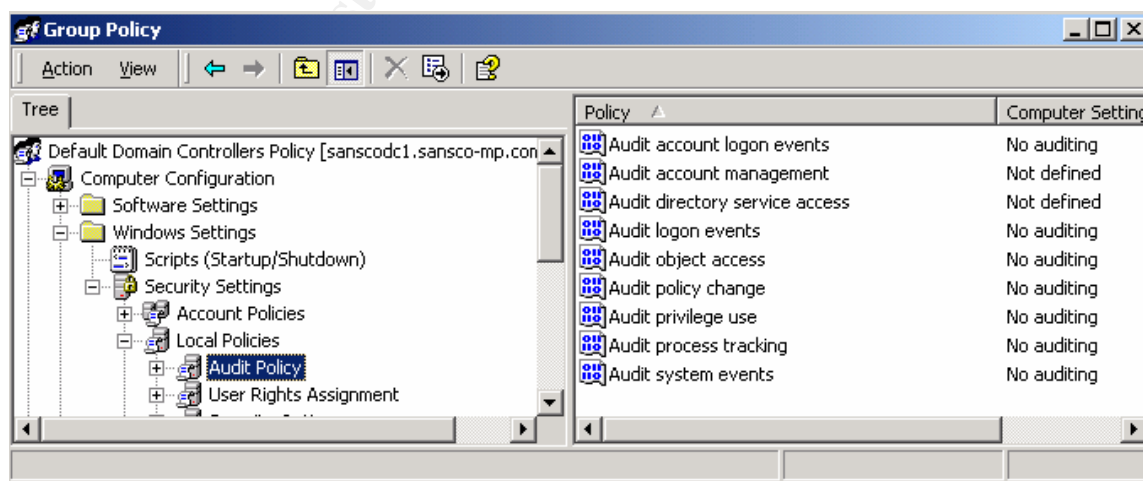
time. The benefit of this is that you have a data warehouse of all Security Event Logs kept in a repository that is searchable and reportable. Each of these offers reporting capabilities for management, as well as a resource for incident handling and forensics.

3. Thirdly, Sans Co. uses a backup cycle of 7 days for its servers. This means that each server and the information stored on it is backed up (by policy) once every week. This allows the event logs (as well as everything else) to be backed up twice before being overwritten, and ensures that we are retaining event logs.

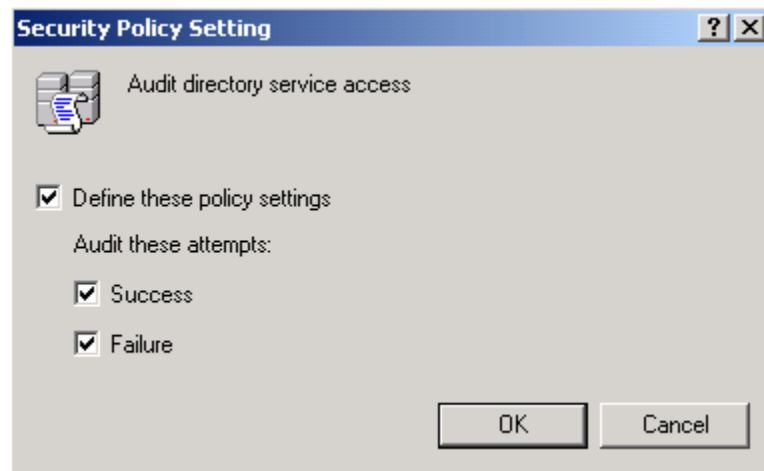
“Avoid the situation where a log fills to capacity before it has been exported to a storage server or backed up to tape.” (Fossen. Windows 2000/XP/2003 Group Policy and DNS, p. 111). Per Sans Co. policy, we are both backing up the servers and backing up event logs to a dedicated storage server. This doubly protects us from losing Security Event Logs and allows for historical audits.

Auditing AD Infrastructure

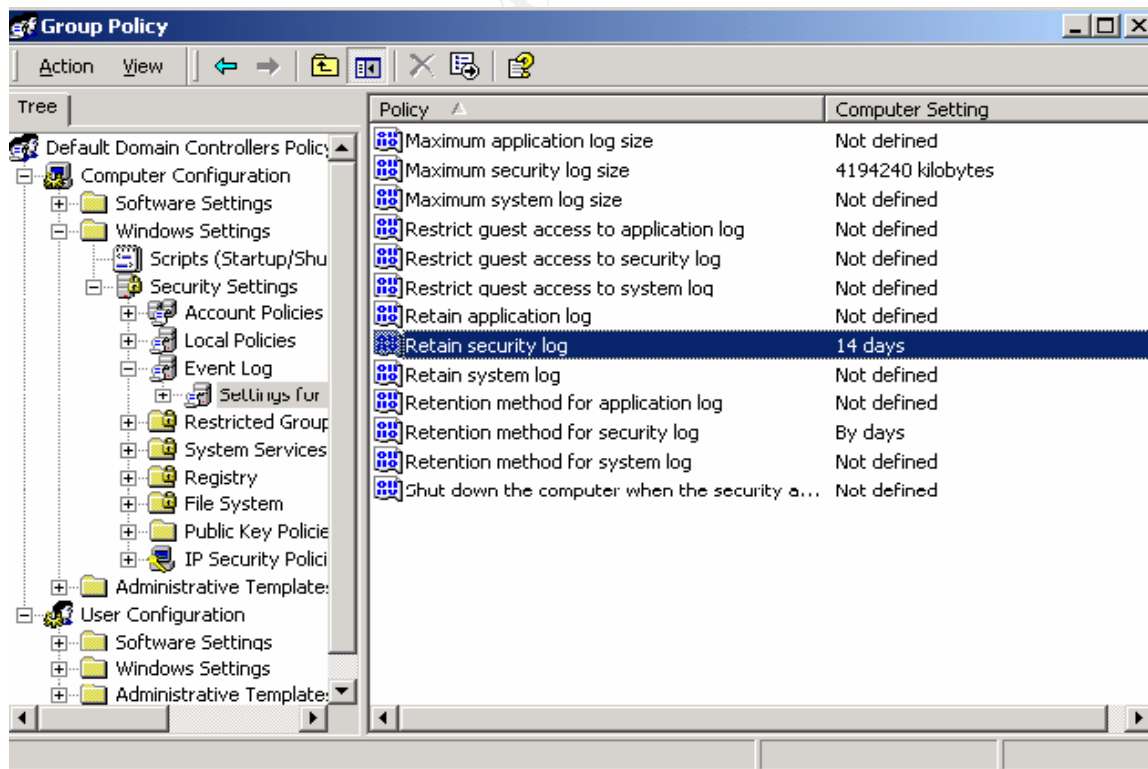
Now that Sans Co. has applied various strategies for securing their infrastructure, how do we ensure that going forward we comply with our security policies and that our actual AD infrastructure is intact? Since AD is the “registry” for the network and because so much critical information is stored here, it is imperative that we audit AD to ensure its security. In Windows 2000 does NOT enable AD auditing by default, so we must first enable auditing. To do this, open the AD Users and Computers MMC snap-in, then right click on the Domain Controllers OU and select properties. Then click on the Group Policy tab, select the “Default Domain Controllers Policy” and Edit. From here, we expand the following: Computer Configuration > Windows Settings > Security Settings > Local Policy > Audit Policy. Notice (below) by default the settings are either Not Defined or No Auditing.



In order to audit access to specific objects in AD, we need to, minimally, enable both success and failure of “Audit directory service access.” Do this by double clicking (or right click) on the Policy, and check each of the three boxes to define both success and failure events.



We should also change the Security Event Log size to the maximum of 4,194,176 KB, reset the Security Event Log every 14 days, and change the Retention Method to “By Days.” Do this under the Default Domain Controller Policy: Computer Configuration > Windows Settings > Security Settings > Local Policy > Event Log.

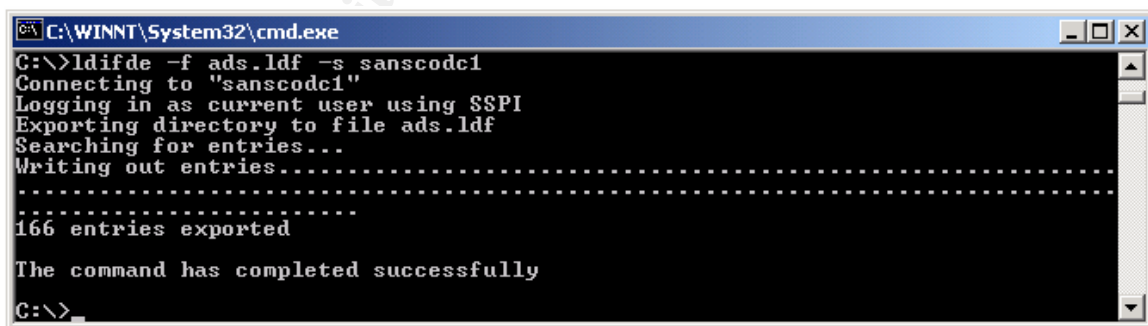


From here, we can proceed to audit specific AD objects and containers via their System Access Control Lists (SACL's). In our example, it would be beneficial to audit the Web Servers OU, so we would right click on Web Servers (in the AD Users and Computers MMC snap-in) and click Properties > Security Tab > Advanced button > Auditing. This shows us what groups/users we are auditing for access to the OU. By default, the Everyone group is audited and we can then choose to audit different types of access to Web Servers. In the case of Web Servers, we would check the box for "Full Control" which will audit all access to this OU.

As mentioned earlier in the paper, we can then program our audit log collection software to collect our logs, and email administrators any alerts that generate that we deem necessary.

AD Infrastructure Integrity

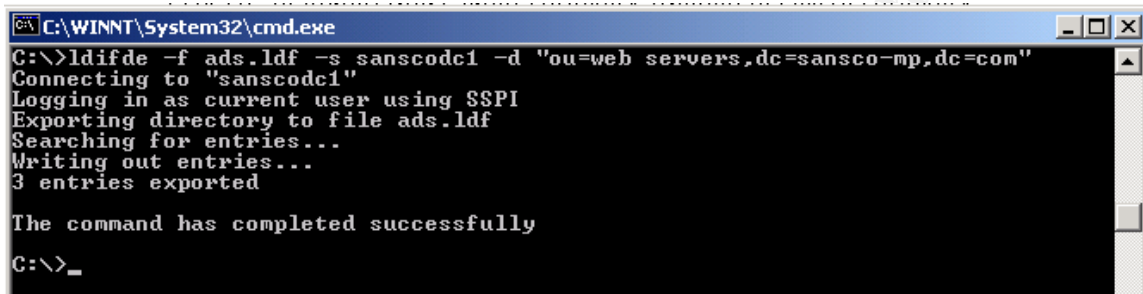
There are several methods of verifying the integrity of our AD infrastructure. A host based IDS system can be used to baseline AD and verify from day to day, week to week, month to month, etc. whether there have been any unauthorized changes. Several third party vendors make such software, and there are some available in Windows 2000. One such program is LDIFDE.EXE, which is a tool that can be used for bulk import and export of AD data, but can check for changes to AD ongoing. To do this we can combine its use with the use of a file comparison tool, such as FC.EXE and create batch files (or through scripting) which can provide detailed information as to what has changed in our AD infrastructure. On a basic level, we can use the tool to export the whole of AD into a text file (in the form of an .ldf file) from day to day; then run the FC.EXE tool to compare the differences. Use LDIFDE in this manner with the commands shown in the screen shot below.



```
C:\WINNT\System32\cmd.exe
C:\>ldifde -f ads.ldf -s sanscodc1
Connecting to "sanscodc1"
Logging in as current user using SSPI
Exporting directory to file ads.ldf
Searching for entries...
Writing out entries.....
.....
166 entries exported
The command has completed successfully
C:\>
```

The -f switch names our export file name, which will save the .ldf file into the directory from which the program is run, in this case C:\. The -s switch tells the program on which server to collect information. To find additional information on LDIFDE, use Microsoft Knowledge Base Article 237677, "Using LDIFDE to Import and Export Directory Objects to Active Directory"

As you can see in the command prompt screen shot above, a successful result will show how many entries exported 166 entries in an AD infrastructure that is not extensive at all. This results in a 139 KB text file. If AD were much larger, the amount of data exported could become very large, and in a large environment with many changes, there could easily be an enormous amount of information to sort through. To rectify this, LDIFDE allows us to export very specific information, which means that we can audit and track changes to specific objects, or even down to specific attributes. For example, the following shows how to use LDIFDE to export information on a specific OU.



```

C:\WINNT\System32\cmd.exe
C:\>ldifde -f ads.ldf -s sanscodc1 -d "ou=web servers,dc=sansco-mp,dc=com"
Connecting to "sanscodc1"
Logging in as current user using SSPI
Exporting directory to file ads.ldf
Searching for entries...
Writing out entries...
3 entries exported

The command has completed successfully
C:\>_

```

Notice that three entries were exported. The resulting text file shows the three entries (dn=xxxxxx) and their specific attributes.

dn: OU=Web Servers,DC=sansco-mp,DC=com (this is the first entry)

```

changetype: add
dSCorePropagationData: 20040116042433.0Z
dSCorePropagationData: 16010101000001.0Z
gPLink:
[LDAP://CN={41F87355-78A3-416D-BCFD-92509756E815},CN=Policies,CN=System,DC=sansco-mp,DC=com;0][LDAP://CN={52874DA7-1D96-413F-8E78-043A8F7F7C19},CN=Policies,CN=System,DC=sansco-mp,DC=com;0]
gPOptions: 1
instancetype: 4
distinguishedName: OU=Web Servers,DC=sansco-mp,DC=com
objectCategory:
CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=sansco-mp,DC=com
objectClass: organizationalUnit
objectGUID:: 0cWuSW/I/0GLXf1TAvtBbQ==
ou: Web Servers
name: Web Servers
uSNChanged: 3697
uSNCreated: 2793
whenChanged: 20040122235136.0Z
whenCreated: 20040116011302.0Z

```

dn: CN=Web Administrators,OU=Web Servers,DC=sansco-mp,DC=com (this is the second entry)

```

changetype: add
member: CN=Web Admin2,CN=Users,DC=sansco-mp,DC=com
member: CN=Web Admin1,CN=Users,DC=sansco-mp,DC=com
cn: Web Administrators
description: Web Server Administrators

```

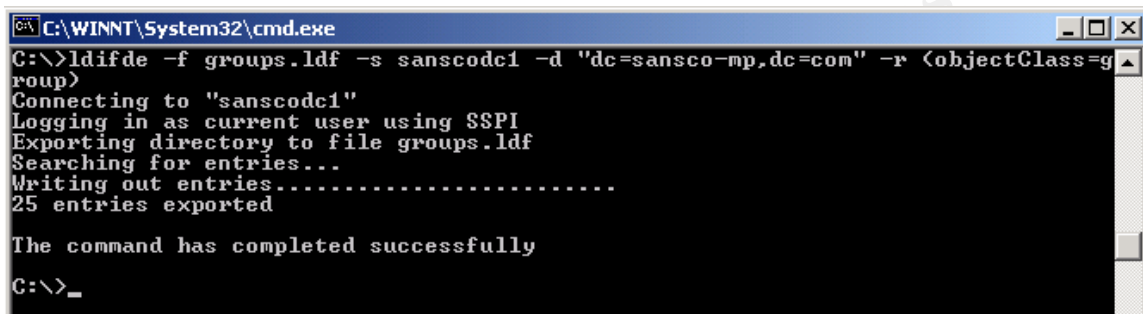
dSCorePropagationData: 20040116044759.0Z
dSCorePropagationData: 20040116042433.0Z
dSCorePropagationData: 16010101000417.0Z
groupType: -2147483646
instanceType: 4
distinguishedName: CN=Web Administrators,OU=Web Servers,DC=sansco-mp,DC=com
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=sansco-mp,DC=com
objectClass: group
objectGUID:: gdAW2WLJyEaSlE+vnhiCQQ==
objectSid:: AQUAAAAAAAAUVAIAI19ja74EPjKKpzI/WQAAAA==
name: Web Administrators
sAMAccountName: Web Administrators
sAMAccountType: 268435456
uSNChanged: 2849
uSNCreated: 2833
whenChanged: 20040116041246.0Z
whenCreated: 20040116033957.0Z

dn: CN=SANSCOWEB2,OU=Web Servers,DC=sansco-mp,DC=com (this is the third entry)

changetype: add
accountExpires: 9223372036854775807
badPasswordTime: 127191183288419600
badPwdCount: 0
codePage: 0
cn: SANSCOWEB2
countryCode: 0
dNSHostName: SANSCOWEB2.sansco-mp.com
dSCorePropagationData: 20040121233338.0Z
dSCorePropagationData: 16010101000001.0Z
instanceType: 4
isCriticalSystemObject: FALSE
lastLogoff: 0
lastLogon: 127193608013703328
logonCount: 10
distinguishedName: CN=SANSCOWEB2,OU=Web Servers,DC=sansco-mp,DC=com
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=sansco-mp,DC=com
objectClass: computer
objectGUID:: oa8koN86YEqnFBeeXQK0MQ==
objectSid:: AQUAAAAAAAAUVAIAI19ja74EPjKKpzI/YAQAAA==
operatingSystem: Windows 2000 Professional
operatingSystemServicePack: Service Pack 3
operatingSystemVersion: 5.0 (2195)
primaryGroupID: 515
pwdLastSet: 127191185872635520
name: SANSCOWEB2
sAMAccountName: SANSCOWEB2\$
sAMAccountType: 805306369
servicePrincipalName: HOST/SANSCOWEB2
servicePrincipalName: HOST/SANSCOWEB2.sansco-mp.com
userAccountControl: 4128
uSNChanged: 3563
uSNCreated: 3352
whenChanged: 20040121233338.0Z
whenCreated: 20040120235130.0Z

In order to monitor that no new users, groups, computers, etc. have been added to our Web Servers OU on a weekly basis, we could set up a batch file, schedule with autosys on a weekly basis, then set up another batch file to run FC.EXE weekly.

Another way that we could use LDIFDE is to run the command as shown below, which exports a specific object class (objectClass=X) from the domain. In this example, we are exporting anything that is a group in our AD structure.



```
C:\WINNT\System32\cmd.exe
C:\>ldifde -f groups.ldf -s sanscodc1 -d "dc=sansco-mp,dc=com" -r <objectClass=group>
Connecting to "sanscodc1"
Logging in as current user using SSPI
Exporting directory to file groups.ldf
Searching for entries...
Writing out entries.....
25 entries exported

The command has completed successfully
C:\>_
```

We could set up the same type of scheduled batch jobs and file comparison to audit the groups in our AD structure for Sans Co. to determine on a weekly basis whether or not any groups are added or removed each week as well as whether any attributes were changed in any group. We then verify this with our system administrators to determine if these were valid changes or not. Additional "objectClass" that we would want to audit would include domainPolicy, organizationalUnit, computer, groupPolicyContainer, trustedDomain, LostAndFound, and user.

Furthermore, we could take the results from our LDIFDE runs and import them into an Access (or SQL for more scalability) database. Parse the text results and import into the database, which then gives each run of LDIFDE it's own timestamp (in the DB) and allows us the ability to historically track changes and compare results month to month, or back to any previous month to see when a specific change was made. This is extremely useful for ad-hoc management requests as to who did what and when.

Conclusion

Sans Co. and GIACE have both merged and were looking at ways to connect their networks to reduce overhead and still maintain security in their network and AD infrastructure. The web presence is imperative to the success of the company and because of this; we take extra precautions in order to ensure the security. To do this, I first established the trust relationships between the companies and formed the network infrastructure that would allow for secure communications between Sans Co. and GIACE. Then I proceeded to provide group policies that would further the security of these companies and ensure adherence to company policy. These policies have been tested and in fact do

provide the level of security required to protect vital business resources. Finally, I presented a method for auditing the AD infrastructure to ensure its integrity ongoing.

© SANS Institute 2004, Author retains full rights.

Appendix A – Password Policy

(SANS Institute, Track 5 CD-ROM – Policies. Modified.)

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Sans Co.'s entire corporate network. As such, all Sans Co. employees (including contractors and vendors with access to Sans Co. systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Sans Co. facility, has access to the Sans Co. network, or stores any non-public Sans Co. information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on monthly basis.
- All production system-level passwords must be part of the IT Staff administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every two months.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Sans Co. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. Since very few systems have

support for one-time Tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Sans Co.", "LittleSoy", "BoxesInc.", "FortuneCo." or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics, and are enforced by this policy and via technical controls in our network. These are must have requirements for your password:

- Contain at least 4 but no more than 12 of both upper and lower case characters (e.g., a-z, A-Z)
- Have at least 4 but no more than 12 of both digits and special characters e.g., 0-9, !@#\$%^&*()_+|~-=-\`{}[]:;'\<>?,./)
- Are at least eight alphanumeric characters long. Our network requires passwords of at least 16 characters long, but not to exceed 30.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, birthdates, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Passwords should not contain your username.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Sans Co. accounts as for other non-Sans Co. access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Sans Co. access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share Sans Co. passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Sans Co. information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

Remember that IT Staff, Administrative Staff, or vendors (Microsoft, Compaq, etc.) will NEVER ask for your password. If someone does ask for a password they are likely trying to social engineer you into giving them access to the system. Please refer any inquiries of this nature to your respective IT Staff.

If someone demands a password, refer them to this document or have them call someone in the Information Technology Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption and the approval of the IT Staff.

Change passwords at least once every two months (except system-level passwords which must be changed monthly). The recommended change interval is every two months, and the system will prompt you to do so every 60 days if you do not initiate the change yourself.

If an account or password is suspected to have been compromised, report the incident to your IT Staff and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the IT Staff or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Use of Passwords and Passphrases for Remote Access Users

Access to the Sans Co. Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix B – SANS/FBI top 20 entry for IIS vulnerabilities

W1 Internet Information Services (IIS)

W1.1 Description

Default installations of Internet Information Services (IIS) have proven vulnerable to a number of serious attacks over time. The impact of these vulnerabilities can include:

- Denial of service
- Exposure or compromise of sensitive files or data
- Execution of arbitrary commands
- Complete compromise of the server

IIS uses a programming hook known as ISAPI to associate files having certain extensions with DLLs (known as ISAPI filters). Preprocessors such as ColdFusion and PHP use ISAPI, and IIS includes many ISAPI filters to handle functions such as Active Server Pages (ASP), server-side includes, and web-based printer sharing. Many ISAPI filters installed with IIS by default are not required in most installations, and many of those filters are exploitable. Examples of malicious programs which use this type of propagation mechanism include the well-known Code Red and Code Red 2 worms.

Like many web servers, IIS includes sample applications that were designed to demonstrate the functionality of the web server. These applications were not designed to operate securely in a production environment. Some IIS sample applications have allowed remote viewing or overwriting of arbitrary files as well as remote access to other sensitive server information, including the administrator's password.

An IIS installation that is not maintained is also subject to vulnerabilities discovered since the software release date. Examples include the [WebDAV](#) ntdll.dll vulnerabilities in IIS 5.0, which enabled denial of service attacks and could allow any web site visitor to create and execute scripts on the server, and the Unicode exploit vulnerability, which allowed any web site visitor to execute arbitrary commands on the web server merely by requesting carefully crafted URLs.

Third-party web add-ons such as ColdFusion and php can introduce further vulnerabilities in an IIS installation, either through misconfiguration or through vulnerabilities inherent in the product.

Additionally: More information on the latest WebDAV specific vulnerabilities ([CAN-2003-0109](#) [CA-2003-09](#)) can be found at the following sites.

<http://www.cert.org/advisories/CA-2003-09.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109>

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q241520>

W1.2 Operating Systems Affected

Windows NT 4 (any flavor) running IIS 4

Windows 2000 Server running IIS 5

Windows XP Professional running IIS 5.1

At the time of this writing, no vulnerabilities have been reported in Windows 2003 running IIS 6; however, it is reasonable to anticipate that vulnerabilities will be found and reported as production environments adopt the new platform in significant numbers.

W1.3 CVE/CAN Entries

[CVE-1999-0264](#), [CVE-1999-0278](#), [CVE-1999-0874](#), [CVE-1999-0237](#), [CVE-1999-](#)

[0191](#),
[CVE-2000-0770](#), [CVE-2000-0778](#), [CVE-2000-0884](#), [CVE-2000-0886](#), [CVE-2000-0226](#),
[CVE-2001-0151](#), [CVE-2001-0241](#), [CVE-2001-0333](#), [CVE-2001-0500](#), [CVE-2001-0507](#)

[CAN-1999-0509](#), [CAN-1999-0736](#), [CAN-1999-1376](#), [CAN-2002-0071](#), [CAN-2002-0073](#),
[CAN-2002-0079](#), [CAN-2002-0147](#), [CAN-2002-0149](#), [CAN-2002-0150](#), [CAN-2002-0364](#),
[CAN-2002-0419](#), [CAN-2002-0421](#), [CAN-2002-0422](#), [CAN-2002-0869](#), [CAN-2002-1180](#),
[CAN-2002-1181](#), [CAN-2002-1182](#), [CAN-2002-1309](#), [CAN-2002-1310](#), [CAN-2003-0109](#),
[CAN-2003-0223](#), [CAN-2003-0224](#), [CAN-2003-0225](#), [CAN-2003-0226](#), [CAN-2003-0227](#),
[CAN-2003-0349](#)

W1.4 How to Determine if You Are Vulnerable

Default or unpatched IIS installations should be presumed vulnerable.

System and network administrators in charge of IIS deployments should familiarize themselves with Microsoft's extensive collection of tools and security documents relating to the proper administration of Internet Information Server.

The main repository for IIS related security documentation is the [Internet Information Sever \(IIS\) Security Center](#).

It is suggested that you download and run the [Microsoft Baseline Security Analyzer](#) which contains detection procedures specifically tailored to IIS.

Administrators should compare their systems against the many [checklists](#), [hardening guides](#), and [vulnerability remediation](#) documentation that Microsoft offers to get a sense of vulnerability status.

W1.5 How to Protect Against It

Patch the system and keep it current.

Patching a server on installation is necessary but not sufficient. As new IIS weaknesses are uncovered, you will need to patch accordingly. Windows Update and AutoUpdate are options for single-server installations. [HFNetChk](#), the Network Security Hotfix Checker, assists the system administrator in scanning local or remote systems for current patches. The tool works on Windows NT 4, Windows 2000, and Windows XP. The current version can be downloaded from Microsoft at <http://www.microsoft.com/technet/security/tools/hfnetchk.asp>.

If you use third-party add-ons such as ColdFusion, PerlIIS, or PHP, remember to check the third-party vendors' web sites for patches and configuration tips as well. For obvious reasons, Microsoft does not include third-party patches in Windows Update and related update services.

Use IIS Lockdown Wizard to harden the installation

Microsoft has released a simple tool to aid in securing IIS installations known as the IIS

Lockdown Wizard. The current version can be downloaded from Microsoft at <http://www.microsoft.com/technet/security/tools/locktool.asp>.

Running the IIS Lockdown Wizard in "custom" or "expert" mode will allow you to make the following recommended changes to an IIS installation:

- Disable WebDAV (unless your environment absolutely requires it for web content publishing).
- Unmap all unnecessary ISAPI extensions (including .htr, .idq, .ism, and .printer in particular).
- Eliminate sample applications.
- Forbid the web server from running system commands commonly used in a compromise (e.g., cmd.exe and tftp.exe).

Use URLScan to filter HTTP requests

Many IIS exploits, including Code Blue and the Code Red family, use maliciously formed HTTP requests in directory traversal or buffer overflow attacks. The URLScan filter can be configured to reject such requests before the server attempts to process them. The current version has been integrated into the IIS Lockdown Wizard, but can be downloaded separately from Microsoft at <http://www.microsoft.com/technet/security/tools/urlscan.asp>.

[back to top ^](#)

(SANS FBI Top Vulnerabilities to Windows Systems – W1 Internet Information Services (IIS), URL: <http://www.sans.org/top20/#w1>.)

© SANS Institute 2004, 1/1/04

Appendix C – hisecweb.inf

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:      HiSecWeb.INF
; Template Version:   05.00.HB.0000
;
; -----
; Revision History
; -----
; Date           Comment
; 03-Sep-1999    Original, based on the following assumptions:
;                Machine is a not a Domain Controller
;                DC's should not be web-servers
;                Machine is a standalone server
;                - If machine is joined to a domain,
;                  then domain-level policies may (or may not)
;                  overwrite these settings.
;                - If machine is joined to a domain,
;                  it should be in it's own OU, and you would
;                  apply this template at the OU level.
;                Machine is a dedicated web-server and physically protected
;                Machine has the Windows 2000 clean-install defaults
;                - No modifications have been made to ACLs, User Rights etc.
;                No one is allowed to log on locally to the machine except an admin
;                Admins are not allowed to log on over
;                the network (they have to go to the Web server to administer it)
;                Admin\Guest accounts are not renamed via this template
; 24-Jan-2000    Updated registry entries
; 23-May-2000    Updated to reduce SMB/Secure channel signing requirements.
; -----

[version]
signature="$CHICAGO$"
Revision=1

[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1
RequireLogonToChangePassword = 0
ClearTextPassword = 0

[System Log]
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 10240
```

AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1

; Local Policies\Audit Policy

[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditAccountLogon = 3

[Strings]
ScelnfAdministrator = Administrator
ScelnfAdmins = Administrators
ScelnfAccountOp = Account Operators
ScelnfAuthUsers = Authenticated Users
ScelnfBackupOp = Backup Operators
ScelnfDomainAdmins = Domain Admins
ScelnfDomainGuests = Domain Guests
ScelnfDomainUsers = Domain Users
ScelnfEveryone = Everyone
ScelnfGuests = Guests
ScelnfGuest = Guest
ScelnfPowerUsers = Power Users
ScelnfPrintOp = Print Operators
ScelnfReplicator = Replicator
ScelnfServerOp = Server Operators
ScelnfUsers = Users

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit\Reg
Values\MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect]
"ValueType"=dword:00000004
"DisplayType"=dword:00000000
"DisplayName"="TCPIP: Syn Attack Protection"

[Privilege Rights]
SeNetworkLogonRight = *S-1-5-11
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Service General Setting]
Alerter,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Browser,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Dhcp,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Fax,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

SharedAccess,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Messenger,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

mnmsrvc,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Spooler,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

RasAuto,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

RasMan,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

RemoteRegistry,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Schedule,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

TapiSrv,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

TermService,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

PolicyAgent,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

W3SVC,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

IISADMIN,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

Irmon,4,"D:AR(A;;RPWPDTLOC;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

[Registry Values]

MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2

MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1

MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1

MACHINE\Software\Microsoft\Driver Signing\Policy=3,2

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting=4,1
MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,This is a private computer system. <add your own text using the MMC Security Templates tool>
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,ATTENTION!

Appendix D – hisecweb v2.inf

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:      HiSecWeb_v2.INF
; Template Version:   05.00.HB.0000
;
; -----
; Revision History
; -----
; Date          Comment
; 03-Sep-1999   Original, based on the following assumptions:
;               Machine is a not a Domain Controller
;               DC's should not be web-servers
;               Machine is a standalone server
;               - If machine is joined to a domain,
;                 then domain-level policies may (or may not)
;                 overwrite these settings.
;               - If machine is joined to a domain,
;                 it should be in it's own OU, and you would
;                 apply this template at the OU level.
;               Machine is a dedicated web-server and physically protected
;               Machine has the Windows 2000 clean-install defaults
;               - No modifications have been made to ACLs, User Rights etc.
;               No one is allowed to log on locally to the machine except an admin
;               Admins are not allowed to log on over
;               the network (they have to go to the Web server to administer it)
;               Admin\Guest accounts are not renamed via this template
; 24-Jan-2000   Updated registry entries
; 23-May-2000   Updated to reduce SMB/Secure channel signing requirements.
; -----

[version]
signature="$CHICAGO$"
Revision=1

[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 60
MinimumPasswordLength = 14
PasswordComplexity = 0
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 30
LockoutDuration = -1
RequireLogonToChangePassword = 0
ClearTextPassword = 0

[System Log]
MaximumLogSize = 25024
AuditLogRetentionPeriod = 1
RetentionDays = 15
RestrictGuestAccess = 1
```

[Security Log]
MaximumLogSize = 50000
AuditLogRetentionPeriod = 1
RetentionDays = 15
RestrictGuestAccess = 1

[Application Log]
MaximumLogSize = 25024
AuditLogRetentionPeriod = 1
RetentionDays = 15
RestrictGuestAccess = 1

; Local Policies\Audit Policy

[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditDSAccess = 2
AuditAccountLogon = 3
AuditProcessTracking = 0
CrashOnAuditFull = 0

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAccountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit\Reg
Values\MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect]
"ValueType"=dword:00000004
"DisplayType"=dword:00000000
"DisplayName"="TCP/IP: Syn Attack Protection"

[Privilege Rights]

```

SeNetworkLogonRight = *S-1-5-11
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Service General Setting]
Alerter,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Browser,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Dhcp,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Fax,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SharedAccess,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Messenger,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
mnmsrvc,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Spooler,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RasAuto,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RasMan,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RemoteRegistry,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TapiSrv,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TermService,4,"D:(A;;CCLCSWLOCRRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
PolicyAgent,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
W3SVC,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
IISADMIN,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
Irmon,4,"D:AR(A;;RPWPDTRC;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1

```

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
 MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
 MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
 MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
 MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
 MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
 MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
 MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
 MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
 MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
 MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
 MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
 MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting=4,1
 MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
 MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer=4,0
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,1
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
 MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
 MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=4,1
 MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
 MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
 MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20
 MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
 MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1
 MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,This is a private computer system. <add your own text using the MMC Security Templates tool>
 MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,ATTENTION!

References

1. Fossen, Jason. Track 5 – Securing Windows. The SANS Institute, 2003.
2. McCabe, Mike. “GIAC Enterprises Windows 2000 Layout.” Modified 8 January 2002. URL: http://www.giac.org/practical/Mike_McCabe_GCNT.doc
3. Garner Jr., George. “Securing Microsoft Internet Information Server 5.0 Using the Windows 2000 Internet Server Security Configuration Tool.” 15 August 2000. URL: www.giac.org/practical/George_Garner_Jr.doc
4. L’Abbe, Colleen. “Hisecweb.inf – An Analysis.” 23 November 2001. URL: <http://www.sans.org/rr/66/212>.
5. “Passfilt Pro Documentation.” Altus Network Solutions. Version 2.0.6 for Windows 2000. Updated 12/15/2003. URL: <http://www.altusnet.com/passfilt/>
6. Microsoft Knowledge Base Article 151082. “HOW TO: Password Change Filtering & Notification in Windows NT.” 8 November 2003. Version 2.2. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;151082>
7. Microsoft Knowledge Base Article 306460. “Microsoft Security Baseline Analyzer (MBSA) Returns Note Messages for Some Updates.” Microsoft. 23 January 2004. Version 13.0. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;306460>
8. Microsoft Knowledge Base Article 272978. “Applying a Hisecweb.inf Template to a Web Server Prevents the Routing and Remote Access Service From Starting.” Microsoft. 21 October 2003. Version 2.0. URL: <http://support.microsoft.com/?kbid=272978>
9. Microsoft Knowledge Base Article 316347. “IIS 5.0: HiSecWeb Potential Risks and the IIS Lockdown Tool.” Microsoft. 3 December 2003. Version 1.2. URL: <http://support.microsoft.com/default.aspx?kbid=316347>
10. Microsoft Knowledge Base Article 314977. “HOW TO: Enable Active Directory Access Auditing in Windows 2000.” Microsoft. 4 November 2003. Version 2.0. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q314977&sd=tech>
11. Microsoft Knowledge Base Article 237677. “Using LDIFDE to Import and Export Directory Objects to Active Directory.” Microsoft. 13 November 2003. Version 2.0. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;237677&sd=tech>
12. Microsoft Knowledge Base Article 255550. “How to Configure Account Policies in Active Directory.” Microsoft. 26 December 2003. Version 3.0. URL: <http://support.microsoft.com/?kbid=255550>.
13. Microsoft Knowledge Base Article 179442. “How to Configure a Firewall for Domains and Trusts.” Microsoft. February 2004. Version 5. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;179442>. 6
14. “Step-by-Step Guide to Using the Security Configuration Toolset.” URL: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/seconfig.asp>

15. "UrlScan Security Tool." URL:
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/urlscan.asp>
16. "Microsoft Baseline Security Analyzer v1.2." URL:
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp>
17. "IIS Lockdown Tool." URL:
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp>
18. "Secure Internet Information Services 5 Checklist." URL:
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/iis5/tips/iis5chk.asp>
19. "NSA Security Recommendation Guides." URL:
<http://nsa1.www.conxion.com/>
20. "KerbCrack FAQ." <http://ntsecurity.nu/toolbox/kerbcrack/faq.php>
21. "The Twenty Most Critical Internet Security Vulnerabilities." The SANS Institute. 8 October 2003. Version 4. URL: <http://www.sans.org/top20/>
22. "SANS FBI Top Vulnerabilities to Windows Systems – W1 Internet Information Services (IIS)." The SANS Institute. 8 October 2003. Version 4. URL: <http://www.sans.org/top20/#w1>
23. "The Twenty Most Critical Security Vulnerabilities." The SANS Institute. 29 May 2003. Version 3.2.3. URL:
<http://www.sans.org/top20/oct02.php#W1>
24. "The Twenty Most Critical Security Vulnerabilities (Old)." The SANS Institute. 2 May 2002. Version 2.504. URL:
http://www.sans.org/top20/top20_oct01.php
25. "How to Eliminate the Ten Most Critical Internet Security Threats." 25 June 2001. Version 1.33. URL: <http://www.sans.org/top20/top10.php>
26. Aelita EventAdmin. URL: <http://www.aelita.com/products/>
27. GFI LANGuard S.E.L.M. URL: <http://www.gfi.com/lanselm/>
28. Microsoft Operations Manager. URL: <http://www.microsoft.com/mom/>
29. Access Data password dictionaries. URL:
<http://www.accessdata.com/dictionaries.htm>
30. Openwall Project password dictionaries. URL:
<http://www.openwall.com/wordlists/>