Global Information Assurance Certification Paper

MERGING SANS CO. AND GIAC ENTERPRISES INFRASTRUCTURES

GCWN Practical Assignment
Option 1
Version 3.2

BY
Richard L. DuClos
02/15/2004

MERGING SANS CO. AND GIAC ENTERPRISES INFRASTRUCTURES

TABLE OF CONTENTS

1 ABSTRACT

The purpose of this document is to describe the merger of SANS Co. and GIAC Enterprises into one organization. This document will deal with the specifics of merging the two infrastructures, securing them, and what is required for routine audits.

The first section of this document will include an overview of the current network and Active Directory designs of each company including the newly formed organization. A new Active Directory forest will be discussed along with how the two network infrastructures will be merged. Both companies have an e-business existence on the Internet via a DMZ.

Next, once the two domains are merged a group policy will need to be applied that effectively reflects business and security needs. Before the policy is actually implemented it will be exhaustively tested in the SANS Co. test lab. The section will discuss, with regards to the test lab implementation, the application of the policy, testing the functionality, security settings and evaluating applied the policy.

The final section of this document will discuss ways of auditing the newly formed infrastructure. Once this new Active Directory forest is implemented SANS Co. / GIAC Enterprises needs a way to audit the infrastructure. A method for gathering of the Event Logs, routine checking of critical setting, and user account audits will be discussed.

2 DOMAIN DESIGN

2.1 Overview of SANS Co. and GIAC Enterprises

These two companies operate specifically in the food sector. SANS Co. is a wholesale food distributor selling products though out Texas and abroad via its e-business web site. GIAC Enterprises is an e-business, which produces fortune cookie sayings. SANS Co. has recently decided to merge with GIAC Enterprises to increase its e-business customer base.

SANS Co. will host the GIAC web site so that there is only one existence on the Internet. GIAC recently underwent an extensive rebuild of there Windows implementation, they upgraded from NT 4.0 to Windows 2000 with Active Directory. SANS Co. also uses Windows 2000, which will enable ease of merging the companies. Both of these companies have very extensive Active Directory implementations, which is why the decision of setting up a trust with GIAC existing AD implementation.

2.2 SANS Co.

SANS Co. corporate office is located in Houston, Texas with remote offices in Austin, Dallas and Galveston. Each of these separate locations deals with sales to restaurants. The Houston, Austin, and Dallas offices handle food products for the Italian, Mexican and Asian food restaurants. The Galveston office specifically handles all seafood restaurant sales. The SANS Co. currently has about 500 employees through out the state, and the corporate office handles all accounting, human resource, and information technology resources. SANS Co. also sells world wide via there web site, which prompted the merger with GIAC to increase e-business exposure.

2.2.1 SANS Co. Network Design

2.2.1.1 SANS Co. Corporate Office Network Design

SANS Co. took the approach of having a standardized network configuration. This standardized design consisted of using switches and routers from Cisco, and IBM workstations and servers.

SANS Co. uses a Cisco PIX 535 firewall to protect the corporate network from the DMZ and Internet connections. This Cisco PIX also acts as the VPN concentrator for the organization allowing mobile users to securely access the network remotely. The Internet comes in to a Cisco 2612 router with two interfaces and terminates at the firewall. The DMZ also is connected to the firewall on a separate interface and uses a Cisco Catalyst 2950 switch with VLANs defined. The servers and workstations at this location user separate Catalyst switches with VLANs defined according to function or department. The

workstation and server switches are connected to the firewall via separate interfaces. The final interface on the firewall is utilized by a Cisco 7609 router used to connect the three remote offices to the corporate office. This router will need to have an additional interface for the GIAC connection.

There are approximately 100 IBM workstations at the corporate office that currently connected to the corporate network all running Windows 2000 Professional. SANS Co. also use Norton Anti-Virus 2002 scanning software on these workstations. The DMZ is located at this office, which hosts the companies IIS 5.0 web site runs on an IBM 230 xSeries server. This server is a domain controller and runs Window 2000 server. For this network the domain controller is the DNS server. This office has Exchange 2000, Oracle 9 server, IIS intranet server, and a domain controller all running on IBM 230 Windows 2000 servers with Norton Anti-Virus protection.

SANS Co. has a T1 connection to its ISP and T1 connections to the three offices in Austin, Galveston, and Dallas. There will be an additional T1 connection for the link to GIAC. There are also plans of upgrading the Internet to a T3 since there will be increased bandwidth requirements.

2.2.1.2 SANS Co. Remote Office Network Design

The offices in Austin, Galveston, and Dallas all share the SANS Co, standardized network and hardware requirements by using Cisco and IBM hardware. It is assumed that these offices also have two servers with about 50 employees each.

These offices use a smaller Cisco 515 PIX firewall to protect them and the corporate network. This connection from the corporate office is connected to a Cisco 2612 series router. This Cisco router has a separate interface on the firewall. The workstations and servers use the same Cisco Catalyst 2950 switch with separate VLANs determined by function and department.

The remote offices each have a Windows 2000 domain controller and Exchange 2000 server using IBM 230 xSeries hardware. These servers also use Norton Anti-Virus software for virus protection. The workstations at these offices are also Windows 2000 Professional IBM machines. It can be assumed that the domain controller is also the DNS server.

The connection to the corporate office Cisco router is done via a T1 connection. Each location has one T1 running between them and the corporate office. There is also a bit of redundancy that comes from having a T1 connection from the Cisco 2612 router at the Dallas location connected to an interface at the Galveston office. The Austin office also has a T1 connection to the Galveston office. These are considered redundant links and are configured as such because of the possibility of the connection with the corporate office failing. The

following diagram, Figure 1, depict the network infrastructures at the corporate and remote locations.

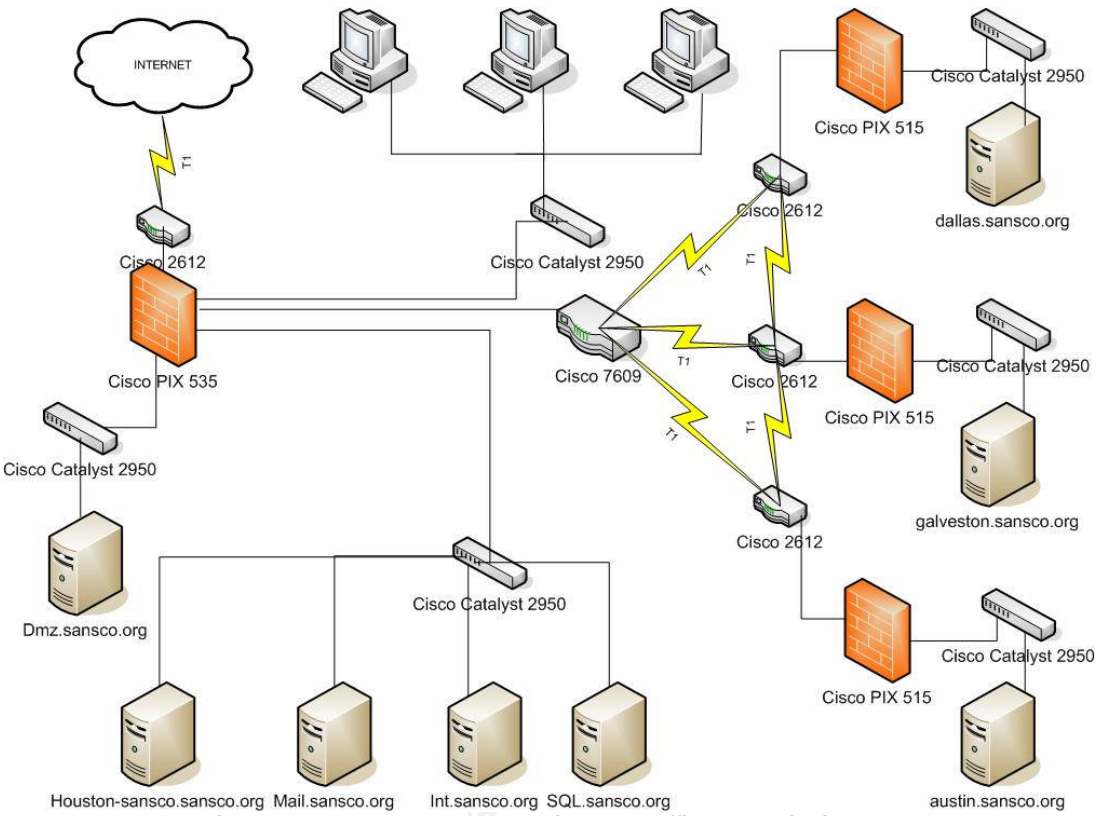

Figure 1 – SANS Co. Corporate and Remote Office Network Diagram

2.2.2 SANS Co. Active Directory Design

SANS Co. uses Windows 2000 Active Directory on all its servers. This design consists of a forest with three domains. The root domain sansco.org domain controller will be the root domain controller, tree root domain controller, and forest domain controller (Sanderson, 19). For this implementation it was decided to use multiple domain architecture rather tan and "Empty Root" designs (Fossen, 175). This is due to security concerns with the DMZ and that the root domain has most of the users and servers. It is also assumed that each location has its own domain controller and mail server.

The sansco.org forest has three domains dallas.sansco.org, Galveston.sansco.org, and Austin.sansco.org. Each one of these domains has a two-way transitive Parent-Child trust with sansco.org. The domain dmz.sansco.org is used for all the web access and is connected to sansco.org via a one-way non-transitive Tree-Root trust. Having a DMZ separate from the sansco.org domain provides an extra level of security for the root domain without the increasing the difficulty of administration (Sanderson, 19). The Active Directory forest design and trusts between the domains can be seen below in Figure 2.

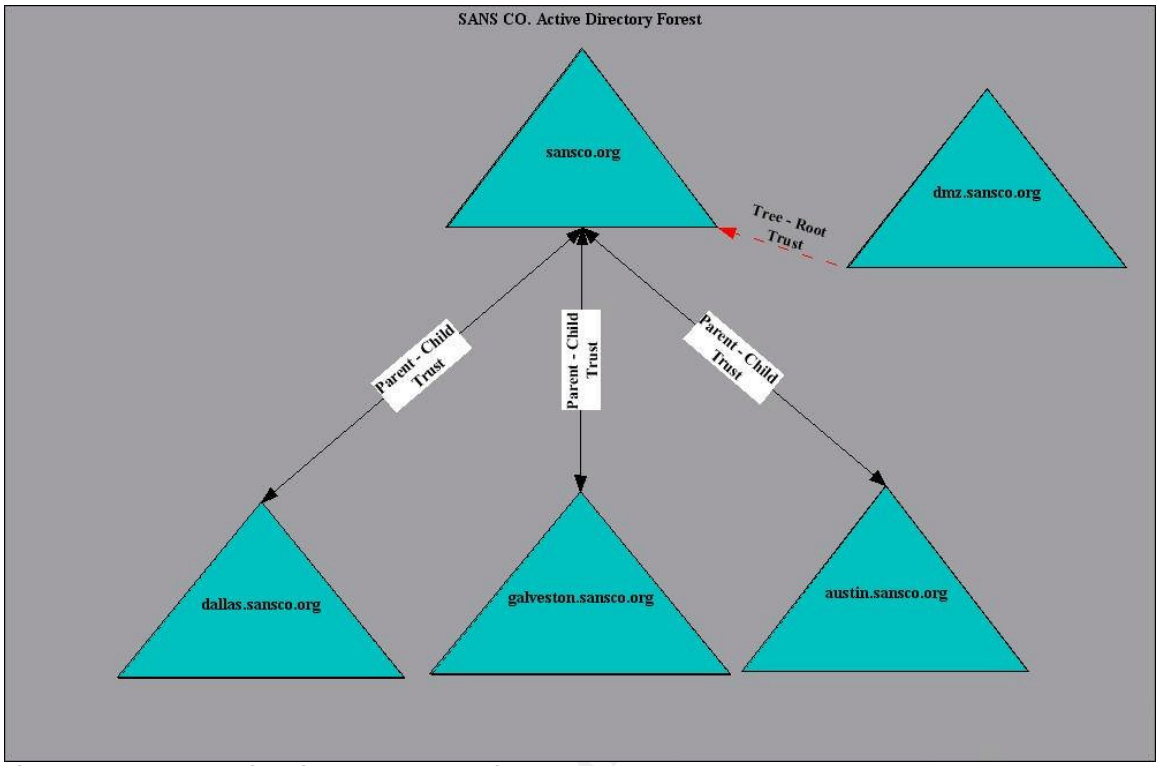

Figure 2 – SANS Co. Active Directory Forest Design

The NSA "Guide to Securing Windows 2000 Active Directory" was used when the sansco.org domain and OUs were designed. The sansco.org domain also has separate OUs for added security; this will allow each OU to have a separate GPO. According to the NSA's suggestions on securing Active Directory the following was taken in account when creating the sansco.org domain. (Sanderson, 14)

- A separate OU for each subdivision of the domain.
- Move default user and computer objects into OUs.
- Management of user and groups are performed by GPOs that are linked or applied to an OU or site object.

SANS Co. decided to use the "Windows 2000 Security Harding Guide" and the NSA's "Guide to Securing Microsoft Windows 2000 Group policy" for developing the GPOs to use in each of the OUs. SANS Co. originally tried to use the "Empty Root" design but since most of their user and groups were at the corporate office it was deemed impossible (Fossen, 175**)**. SANS Co. has the following OUs defined under its sansco.org domain for its corporate office:

- **Domain Controllers** – this container will have all the domain controllers for sansco.org
- **Member Servers** – Container for sansco.org general use servers.
- **Database Servers** – container for sansc.org database servers.
- **Web servers** – container for corporate office Intranet servers
- **Workstations** – container for all workstations in the corporate office

- **Remote Users** – Container for users that access the system remotely through the VPN.
- **Users** – container for users at the corporate office.

Each of the remote offices has containers for their domain controllers, member servers, computers, and users using the same GPOs that the corporate office implemented. The DMZ domain has only OUs for its domain controllers and web servers; it too uses the same type of GPO as the sansco.org domain uses.

The following diagram, Figure 3, shows the design of sansco.org OUs. This diagram also displays each of the GPOs used in the forest and their inheritance.

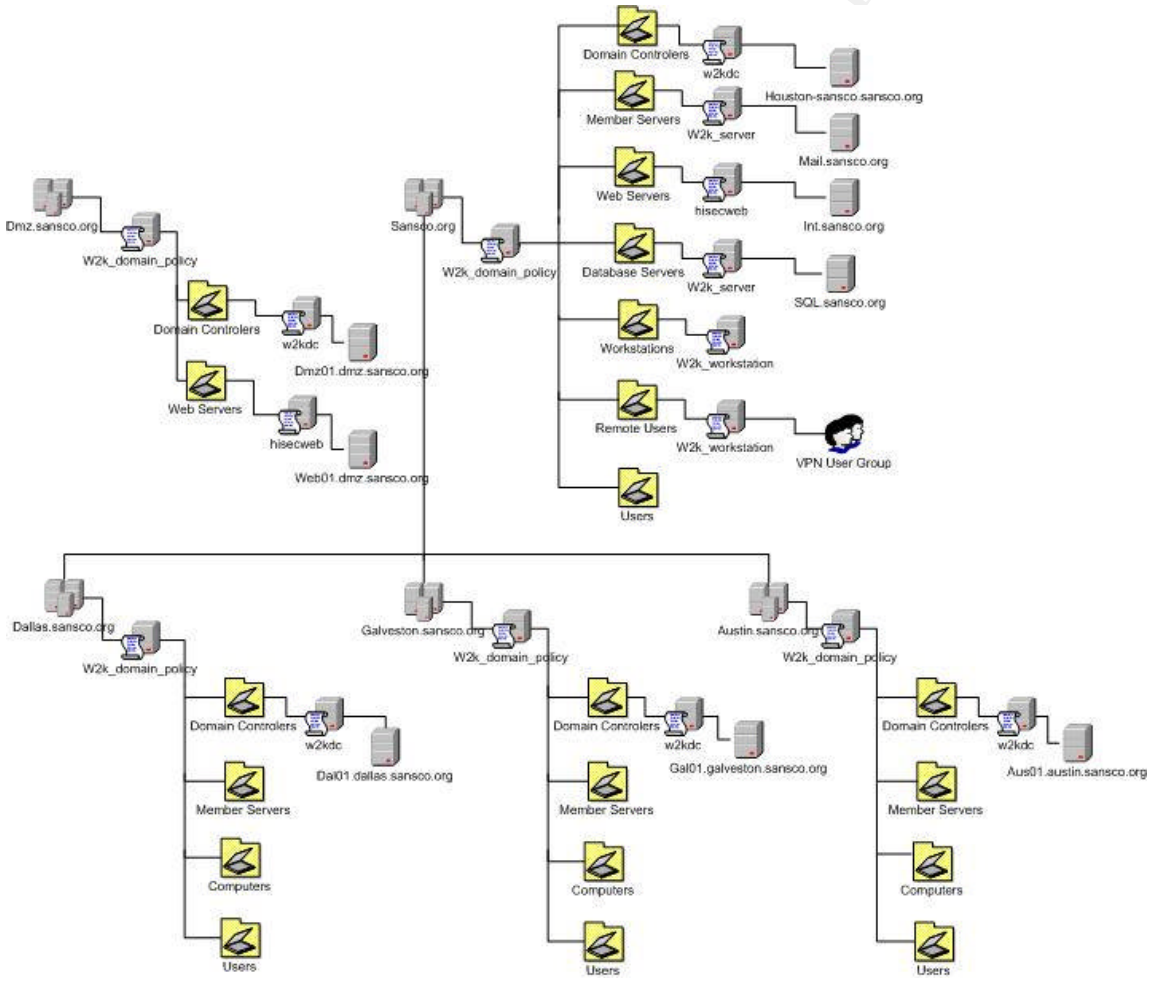

Figure 3 – SANS Co. Active Directory and OU Design

SANS Co. uses the following template to create its GPOs according to the OUs:

- Domain uses the NSA w2k_domain_policy template
- Member and Database Servers use the NSA w2k_server template
- Web Servers use the Microsoft hisecweb template
- Workstations use the NSA w2k_workstation template
- Remote Users use the NSA w2k_workstation template

2.3 GIAC Enterprises

GIAC Enterprises also is located in Texas and currently only has one remote office. GIAC is an e-business, which sells fortune cookie sayings to makers of fortune cookies, which SANS Co. will benefit from since their web. This company only has about 150 employees and with the two offices this merger will be quite easy. The network design for GIAC Enterprises is referenced from the design by Gregory Rick GCWN analyst # 0182.

2.3.1 GIAC Enterprises Network Design

2.3.1.1 GIAC Enterprises Main Office Network Design

GIAC Enterprises also uses Cisco hardware, which will aid in the administration of the merged network. It is also assumed that GIAC has a standard for its servers on its networks. The GIAC Main Office is connected to the internet with an external router connected to its firewall. The "Internal Network" has a connection to the firewall through what is referenced as the "Internal Router". The firewall also has a DMZ connected through a router (Rick, 4). This DMZ network will be removed from the merged implementation. This network also has a RealSecure 6.5 IDS system on each of the segments.

The GIAC Main Office has a mixture of servers, specifically Windows NT 4, Window 2000, and Sun Solaris. GIAC currently has Windows NT 4.0 servers that are due to be phased out and will not be considered in the merged implementation. GIAC has IIS 5, Exchange 2000, SQL, DNS, and file servers using Windows 2000. Similarly to SANS Co. remote users, GIAC Enterprises uses a Cisco VPN to connect the remote office to the main office using 168-Bit Encryption over a dedicated T1 connection (Rick, 4). The VPN is only used for connecting the Main and Remote offices. GIAC uses Window 2000 on all its workstations.

This location has a T1 connection for the link between the Main Office and Remote office. There is a separate T1 for internet access at the Main Office. The connection to SANS Co will occur by adding a new T1 interface to the Main Office external router.

2.3.1.2 GIAC Enterprises Remote Office Network Design

GIAC Remote Office also uses Cisco PIX firewalls for both its internal, external and DMZ networks, and these networks also have Cisco routers. The Remote office connects to the Main Office through a Cisco router using VPN.

Like the Main Office the Remote Office has a RealSecure IDS system, IIS 5, DNS, and file servers. The DMZ and Windows NT servers at the Remote Office will not be part of the merged design. The following is a diagram of GIAC Enterprises network.

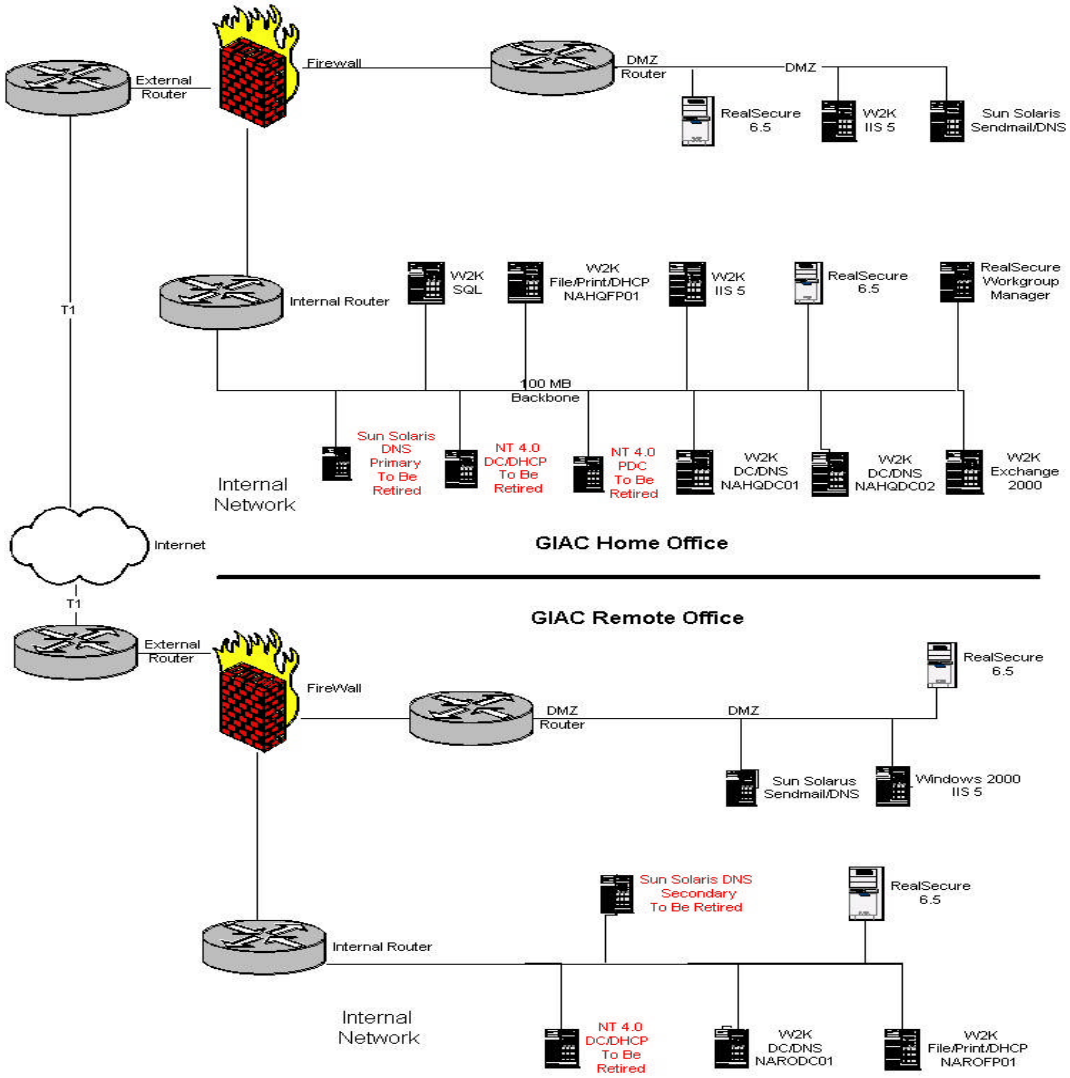

Figure 4 – GIAC Enterprises Network Design
Source: Gregory Rick GCWN Analyst # 0182

2.3.2 GIAC Enterprises Active Directory Design

GIAC has implemented Active Directory on Windows 2000 Servers. Their AD forest contains only one AD domain. OUs are also used here for security and management (Rick, 16). The domain name for GIAC Enterprises is "prophesy.com". This domain also has a DMZ but GIAC has not implemented AD and has no plans to do so on this network segment. This is why their web site will be hosted on SANS Co's DMZ.

The GIAC domain has a Main Office that consists of domain controllers, DNS, mail, file, and SQL servers. The remote office also has a DMZ, domain controller, DNS, and a file server. GIAC uses OUs for the delegation of administration and the application of group policy (Rick, 16).

Gregory Rick states that OU structure focus is to "delegate administration, apply group policy and hide objects"(Rick 16). This justifies why there are OUs for each office and separate OUs for user and severs. The OU structure of the "prophesy.com" domain consists of the following logical structure:

- **Home Office** – Consitst of Printers, Computers, and Admin OUs
- **Remote Office** - Consitst of Printers, Computers, and Admin OUs
- **Users** – IT Admin, Resarch and Development, Sales and Marketing, Finance and HR
- **Enterprise Servers** – OU for member servers
- **Domain Controllers** – OU for domain controller

Figure 5 below show this OU design for "prophesy.com"

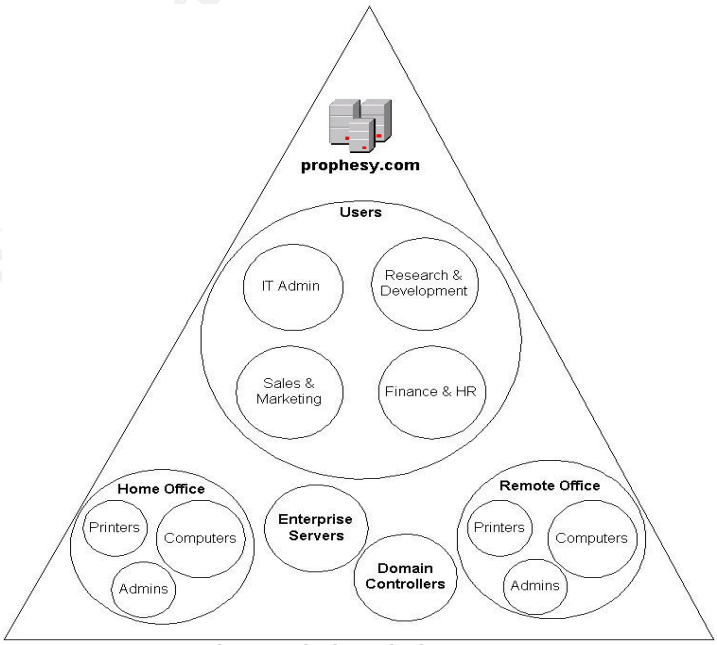

Figure 5 – GIAC Enterprises Logical OU design
Source: Gregory Rick GCWN Analyst #0182

GIAC currently only uses four GPOs (Domain Policy, Workstation Policy, Server Policy, and Domain Controller) and they were adopted from the NSA. Like SANS Co. GIAC uses GPOs for management and security considerations utilizing readily and proven security templates (Haney). The NSA templates that GIAC uses are located below:

- Domain policy uses the w2k_domain_policy.inf template
- Workstation Policy uses the w2k_workstation.inf template
- Server policy uses the w2k_server.inf template
- Domain controller uses the w2k_dc.inf template.

2.4 SANS Co. / GIAC Enterprises Merger

This section will discuss the merger of the two organizations specifically network and Active Directory design. As explained in the preceding two sections show that the merger should be easy due to the similarities of network hardware and Windows 2000 AD designs. But since the networks rely on their extensive AD designs they will remain separate with trusts. The merger will also make administration of the network easier and cheaper since all administration will occur at the SANS Co. corporate office. This merger should:

- Increased and/or maintained security and reliability
- Customer satisfaction and employee work performance will not suffer.
- Provide customers with a single Internet presence
- Verification of AD security configuration
- All administration will be performed at the SANS Co. corporate office to reduce IT overhead.

2.4.1 SANS Co. / GIAC Merged Network Design

The merged network design of SANS Co. / GIAC Enterprises will consist of the current configuration of each, with the exception of modifying GIAC's external router with a new T1 interface. A new T1 interface will be added to SANS Co. Cisco 7609 router and the phase out of the GIAC DMZ domain will be performed. The firewalls at both locations will need to be reconfigured with new rules to allow the traffic between the two sites. The diagram located below, Figure 6, shows how GIAC will be connected to the SANS Co infrastructure.

GIAC had not allowed users to remotely access the corporate network through VPN, but now since SANS Co. has that infrastructure in place they will be allowed to do so. The GIAC remote office for the time being will be connecting through VPN to the GIAC Main Office but will soon be connected to the Cisco at SANS Co. This will remove the need of having a dedicated connection at GIAC for VPN and all web access will come from SANS Co. The current T1 Internet connection at SANS Co. might need to be upgraded due to the new bandwidth requirements of hosting the prophesy.com site and added web traffic.

Since the DMZ at the GIAC Main Office is going to be decommissioned, so will the remote office DMZ. The IDS sensors will be used in other locations on the merged network. The current GIAC web servers will be physically moved to SANS Co. and located on that DMZ. This will be seamless to the customers, because they will access the web site the same way as they currently do. Since SANS Co. does not currently have a IDS system this will provide an opportunity for SANS Co. to develop their IDS infrastructure.

The only servers that will exist at GIAC will be the domain controllers, IDS, file, SQL, and mail servers. This is justified since the GIAC office will be treated, as a SANS CO remote office with the temporary exception of GIAC remote office connection requires the security of VPN; this can be seen below in Figure 6.

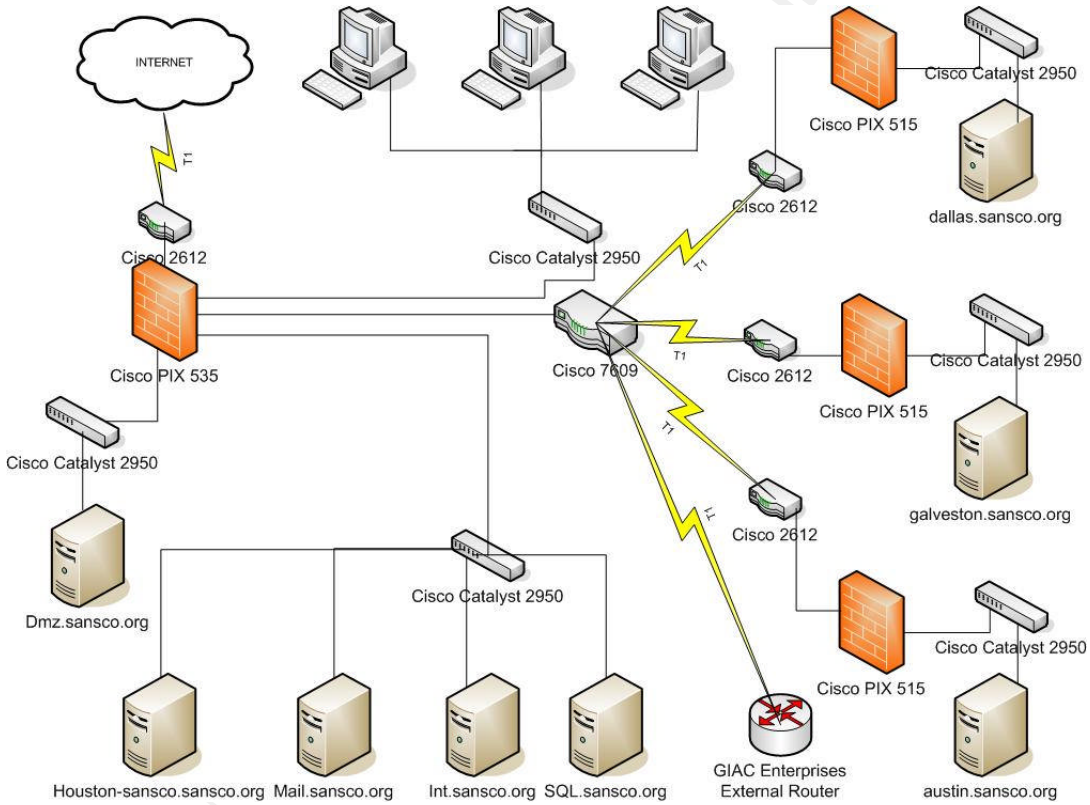

Figure 6 – Merged SANS Co.. / GIAC Enterprises Merged Networks

2.4.2 SANS Co. / GIAC Merged Active Directory

As previously discussed, it is possible to see that both of these companies have very extensive AD designs. It was decided since SANS Co. has a separate DMZ domain for management and security reasons that the "prophesy.com" domain will be a separate forest as well.

The AD design of each existing network will stay mostly unchanged, specifically OUs, and security templates. The DNS servers at each location will need to be changed to reflect the merger and also to act as redundant DNS servers. The

will prevent the single DNS server from being a single point of failure (Sanderson, 6). With the AD merger design out of the way, the trust between SANS Co. and GIAC need to be configured.

The trust will be configured to be a two-way external Tree – Root trust between prophesy.com and sansco.org. All the OUs and GPOs contained in prophesy.com will not be modified. The only drastic change to the prophesy.com domain is the decommissioning of their DMZ. All web sites that existed on this GIAC DMZ will be ported to the dmz.sansco.org. All customers will still be able to access their web sites with out any problems.

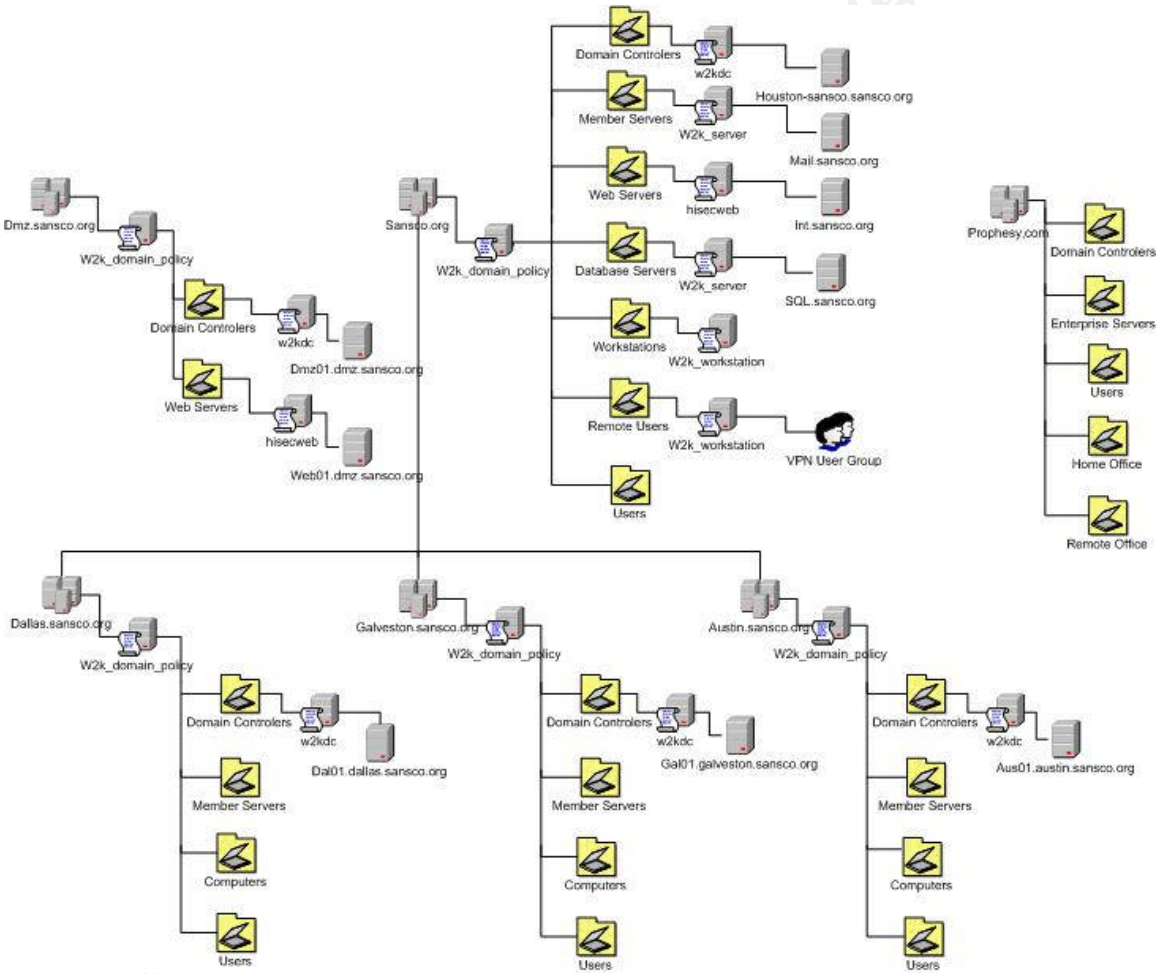

Figure 7 – SANS Co. / GIAC Merged Active Directory OU Design

The OUs of each network will remain the same since they are basically identical and were implementing to represent each organization. GPOs of each organization came from Microsoft's hardening guidelines and NSA; they will remain in place and be updated accordingly.

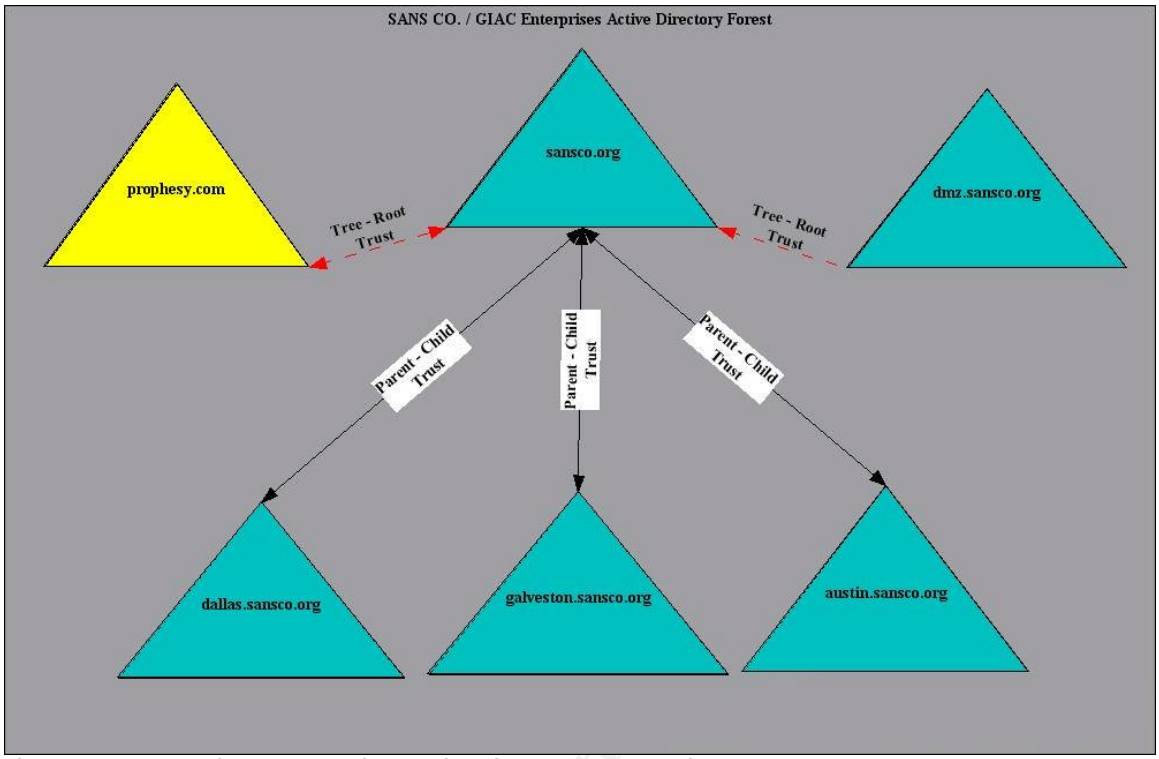

Figure 8 – SANS Co. / GIAC Enterprises Active Directory Forest Design

The preceding diagram, Figure 8, shows what the final merged AD domains look and how trusts will be used. The trusts in this diagram are Tree-Root and Parent-Child trusts.

2.5 Other Merger Considerations

With the networks and Active Directory domains complete it is time to address some other considerations of the merged companies. These concerns include IIS 5.0 security, VPN usage, and Active Directory backup / recovery considerations. The concerns with IIS and Active Directory backup / recovery should be dealt with immediately and the VPN usage concerns can be implemented over a period time.

2.5.1 IIS 5.0 Security

According to John Davis' document titled "From Blueprint to Fortress" there are some specific needs with regards to IIS 5.0 security that needs to be addressed. The following lists are those considerations:

- **File System** – ACLs are set on the OS files and folders.
- **Active Directory** – Since AD gives centralized administration, group policy and access controls.
- **Security Configuration Manager** – this a tool used to set security settings for servers.

- **Hot Fixes and Service Packs** – many attacks can be prevented by making sure all appropriate patches and service packs are installed.
- **Removing Samples** – remove all sample web pages since they are well known to hackers.
- **Registry Hardening** – the following should be done to help secure IIS
    - **SYN Flood Attack Protection** – protect against DDOS attacks.
    - **Disabling Internet Printing** – this new feature of Windows 2000 it should be disabled to prevent a large hole in a web server.
    - **Restricting Anonymous Login** – this will prevent someone from mallicously learning about the system.
    - **Removing Administrative Shares**
    - **Restrict Null Sessions**

A checklist like Microsoft document titled "Secure Internet Information Services 5 Checklist" needs to be followed when the DMZ IIS servers are configured. Regarding the configuration of SANS Co. DMZ the following were deemed necessary:

- Use of the hisecweb.inf template
- Configuration of IPSec – will be performed in the future
- Limiting use of the Telnet service to developers
- Set appropriate ACLs on virtual and log file directories
- Enabling logging on IIS servers

The Microsoft IIS lockdown tool will be used to verify the overall configuration of the DMZ IIS servers. According to Microsoft the IIS Lockdown Tool works by shutting down "unnecessary features" (Microsoft - IIS, 1). The lockdown tool does not make changes to the base Operating System.

2.5.2 VPN Usage

The VPN at the SANS Co. corporate office is currently configured to accept connections from mobile users via the Internet and GIAC only uses VPN for its remote office connection. Gregory Rick stated that GIAC does not use their VPN for remote users but has the capabilities. With this in mind it can be assumed the merged company will have not only the SANS Co. mobile users but the GIAC mobile users as well. So this could lead to also having the GIAC Remote Office connecting to the SANS Co. corporate office VPN and removing the need of having a VPN concentrator and dedicated T1 connections at GIAC's Main Office.

2.5.3 Active Directory Backup / Recovery Considerations

The need for a backup / restore methodology is needed for this AD design. This is especially true since the newly merged environment is assumed not to have a backup / restore procedure in place. Active Directory backup/restore is important to include in an organizations disaster recovery policy (Sanderson, 45).

The backup / restore can be performed by backing up the system state information. The backup feature included with Windows only backups the system state information of the local machine. This means that each server will have to run the backup wizard on at least the system state data.
Restores can be authoritative or non- authoritative, meaning that for a non-authoritative restore the AD data will go back to its state when the backup occurred. An authoritative allows the Admin to fix the data so that it does not get overwritten. Authoritative restores are performed after non- authoritative restores (Sanderson, 45). The previous information shows how easy backing up AD can be and the restore feature gives some flexibility.

2.6 Domain Design Conclusion

With the discussion of the merger now complete, it is time to discuss some of the benefits of the combined network. The combined network will provide SANS Co. / GIAC Enterprises the ability of centralized administration, reduced IT overhead, and a single web presence.

Since SANS Co. / GIAC Enterprises use AD and there is a two-way trust between the two sites AD administration will occur at the SANS Co. corporate office, therefore this will eliminate the need to have two separate IT departments. All the old Windows NT 4.0 servers at GIAC are going to be phased out immediately to insure not having to configure trusts with AD and NT 4. All web development will occur at SANS Co. on their DMZ and all web servers from GIAC will be moved to that location. This too will provide the need for only one web development department. The company will also look at in the future using IPSec to further secure the link between DMZ and corporate networks.

Now without the need of the GIAC IT department a larger sales staff can utilize space at the GIAC location that was occupied by the IT department. The IT overhead will certainly be further reduced when the GIAC remote office connects directly to the SANS Co. network rather than through GIAC's Main Office. The Internet connection at GIAC also will no longer be needed. Since SANS Co. is now joined with a company that utilizes an intrusion detection system, it will provide an increased level of security.

All the web servers and web development team will be at the SANS Co. corporate location, which will also free up more office space at GIAC. It was decided to use the SANS Co. DMZ rather that GIACs DMZ because GIAC did not use AD on their IIS servers. SANS Co. uses AD and furthermore have the DMZ on a separate domain. Customers will continue to connect to their respective web sites just as they have in the past and should not notice the difference.

The new organization will incur some expenses when moving all needed GIAC personnel to the SANS Co. corporate office, buying needed interfaces for Cisco

routers to connect the two locations, moving IIS servers from GIAC to SANS Co, the possible need of purchasing more IDS sensors for the SANS Co network.

3 SECURITY POLICY AND TUTORIAL

This section of this document will discuss the GPOs that are used in this network. The IIS server will be discussed specifically. A tutorial will be performed in a test lab environment on the GPOs before they are implemented in the actual network. These policies will also be tested for functionality.

3.1 Security Policy Design

The templates used in the merged network GPOs have been adopted from NSA and Microsoft. The GPOs that will be used are the following and can be found in on the NSA and Microsoft website

- W2kdc, NSA
- W2k_domain_policy, NSA
- W2k_server, NSA
- W2k_workstation, NSA
- Hisecweb, Microsoft

The hisecweb template will be tested in a test lab environment before actually rolling the policies out. The hisecweb template is supplied by Microsoft to help secure IIS at the OS level (Microsoft - IIS, 1). It is also mentioned that this policy should not be installed before applications are installed, since it could prevent proper installation. The hisecweb template will currently be the only one that undergoes any modification on the merged network. The changes to this template are reflected below.

The templates used by SANS Co. / GIAC Enterprises will be broken down by OU. The following information illustrates what template each SANS Co. / GIAC Enterprises OUs will utilize:

SANS Co. / GIAC Enterprises OUs	Template
Domain Controllers	**W2kdc.inf**
Member / Enterprise Servers	**W2k_server.inf**
Web Servers	**Hisecweb.inf**
Database Servers	**W2k_server.inf**
Remote users	**W2k_workstation.inf**
Workstations	**W2k_workstation.inf**

The GIAC servers will continue to use the NSA templates that they were originally designed to utilize. Using GPOs will allow centrailized management, flexablity, reliability, and security (Microsoft - Windows 2000, 4).

To apply the policy the snap-in tool for GPOs will be used to take the textbased template file and apply the security settings of the security areas (Microsoft, 4).

3.1.1 Building the Security Policy

Since a test needs to be performed before implementing policy on the DMZ. A test of the hisecweb template will be performed. A copy of this template can be found in Appendix A. This template will be used on SANS Co. DMZ web servers; the test lab has been configured with a replica of the sansco.org domain and dmz.sansco.org domain. A new copy of the hisecweb template was downloaded from Microsoft's web site into the test lab for testing. Using the snap-in "Security Templates" the settings for the Account Policies, Local Policies, Event Log, and System Services were checked to make sure they meet the needs of SANS Co. DMZ servers, according to the NSA guide to Group Policy.

The following changes were made to the Account Policies:

- The maximum password age was changed from 42 days to 90 days.
- Account lockout threshold was changed from 5 attempts to 3 attempts.

The following changes were made to the User Rights Assignments:

- Administrators group can be the only ones to shutdown the system
- Developers, Administrators, Internet groups can access the machine via the network, i.e. the telnet service.
- Developers and Administrators can login locally.

The following changes were made to the event log settings:

- The Maximum application and system log size was changed to 10240 kilobytes to reflect the maxiumum size of the security log.
- The retention method for the application and system log was also changed to overwrite events as needed.

The systems services needed the following changes:

- Automatic Updates were set to disabled
- BITS were set to disabled.
- The Windows Time service was set to automatic.
- The Telnet service is set to automatic

There were no more changes made to the hisecweb template before it is to be applied to a GPO.

3.2 Applying the Group Policy

The application of the test policy will be performed in the SANS Co. test lab on a Windows 2000 IIS server named TEST-WEB. There will be a host record was created in DNS named WEB-RichardDuclos that will resolve to the TEST-WEB

address. The part of the test will explain how the policy is applied and how it can be maintained over time.

Since the template is ready to be imported to a GPO, selecting the new button and then naming it “Web Server Policy – Richard Duclos”, created a new GPO. The following, Figure 9, is screen shot of the GPO name and how the procedure was completed.

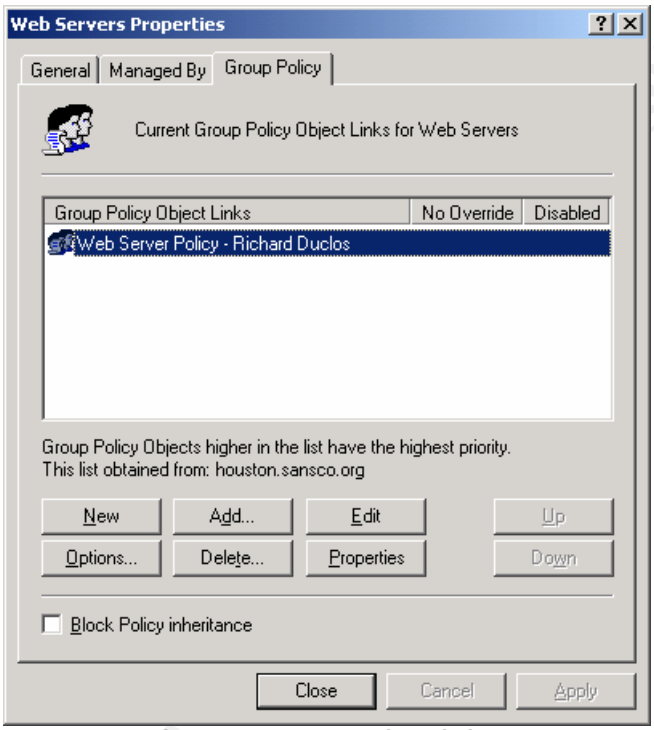

Figure 9 – GPO Properties Window

Since using the No Override and Block Policy Inheritance can lead to complicated troubleshooting, it was decided to not use these options at this time (Haney, 9). Now with the GPO created it can now be edited by clicking the edit button. The following, Figure 10, is a display of what the edit window for the GPO looks like. Any changes to the local policies, password policies, etc… are to be done in this window.

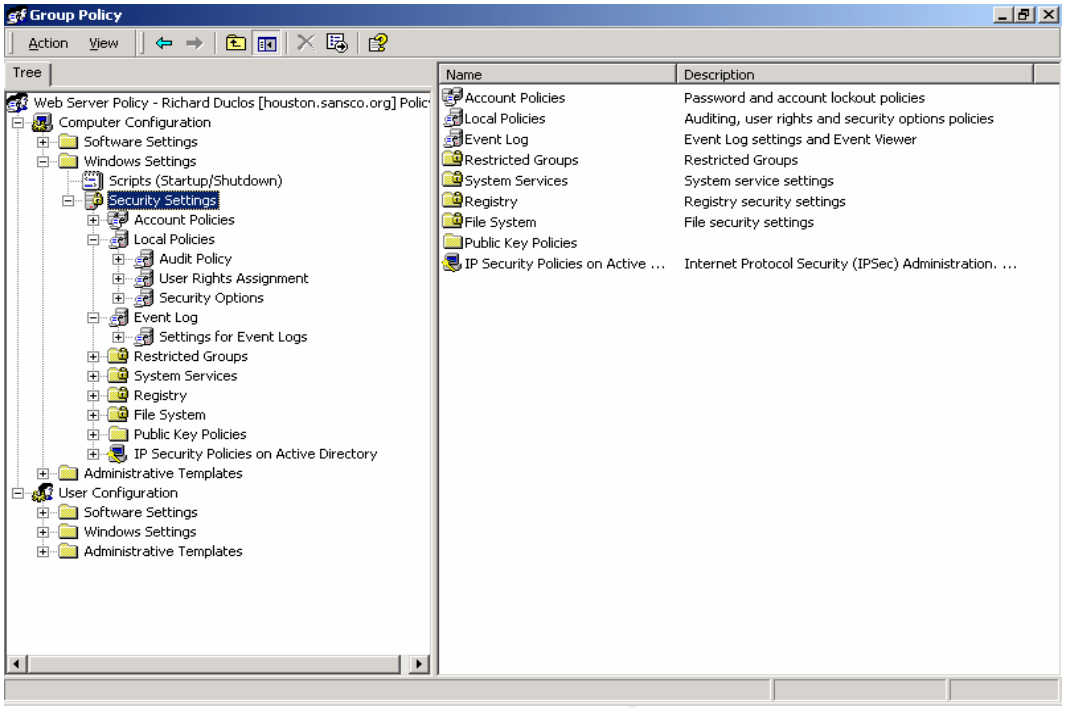

Figure 10 – Web Server policy – Richard Duclos Edit Window

After any editing the policies the GPO according to the data from section 3.1.1, the policy is ready to be applied. Currently the GPOs update every 90 minuites but for this test it is not sufficient. The secedit /refreshpolicy machine_policy /enforce command is used to speed up the process (Haney 2, 95). Once the policy is applied there should be a message in the application log, the following, Figure 11, is what appeared in the application log after running secedit.

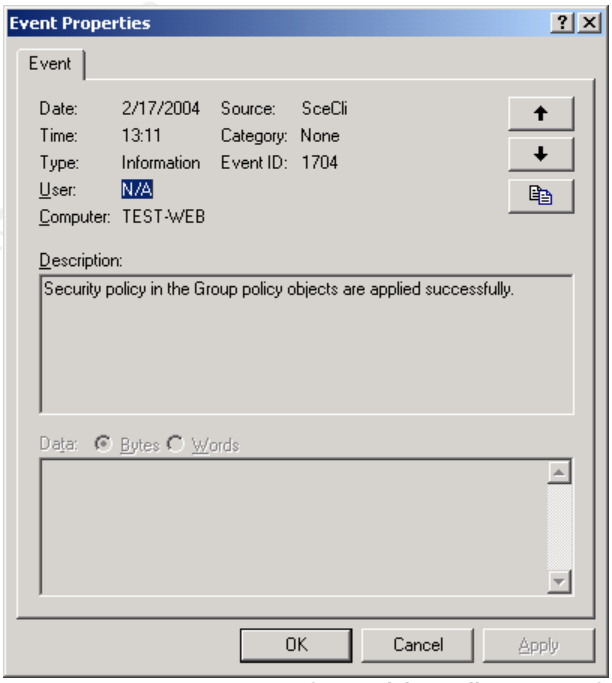

Figure 11 – Event Log message after applying policy successfully

The Security Configuration and Analysis tool snap-in will be used to verify successful application of the security policy and used for maintenance over time. It is said by the NSA that this procedure be completed every time a new security policy is implemented on a local system (Haney, 95). The following steps from the NSA were followed when using the tool:

- Start the snap-in in the MMC
- Open or Create a new database
- Select import template and specify which inf file to import.
- Right click the database node and select Analyze Computer Now.
- Specify location of error log file
- Select Configure computer now

Output from running this snap-in can be found in Appendix B. The image below, Figure 12, is how the window appears once a database is but and the computer is analyzed.

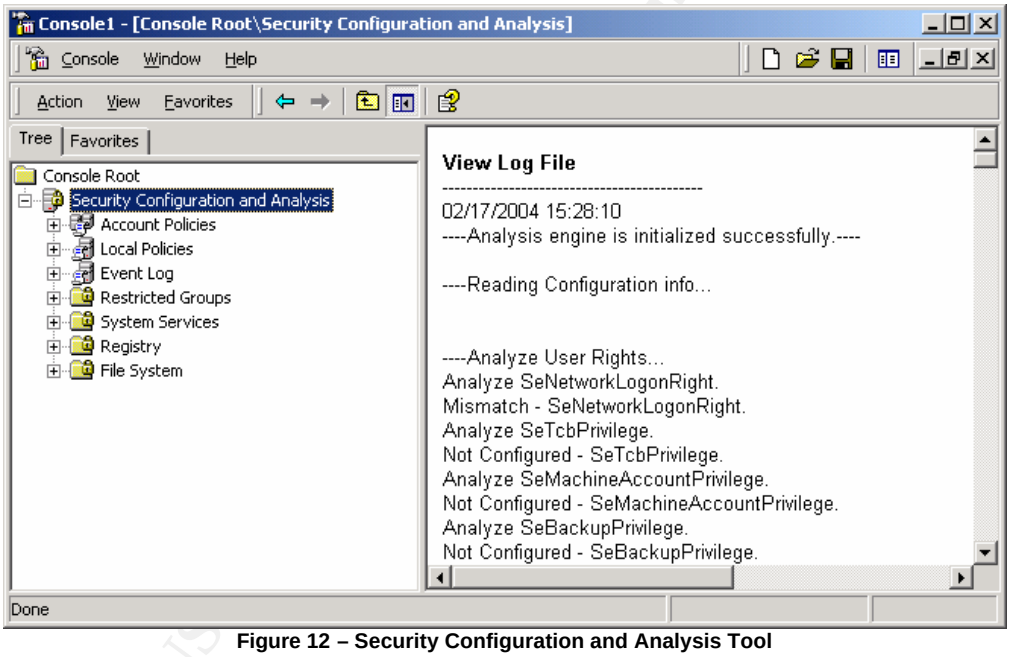

Figure 12 – Security Configuration and Analysis Tool

3.3 Testing the system's functionality

This part of the tutorial will deal with verifying that there are no problems associated with applying the policy. To test that the applied policies' security settings are working as expected, especially functionality, the website built for this tutorial will be used. The policies that have been applied to the system should have no effect for access to this website. The image below, Figure 13, show the web page running on WEB-RichardDuclos.

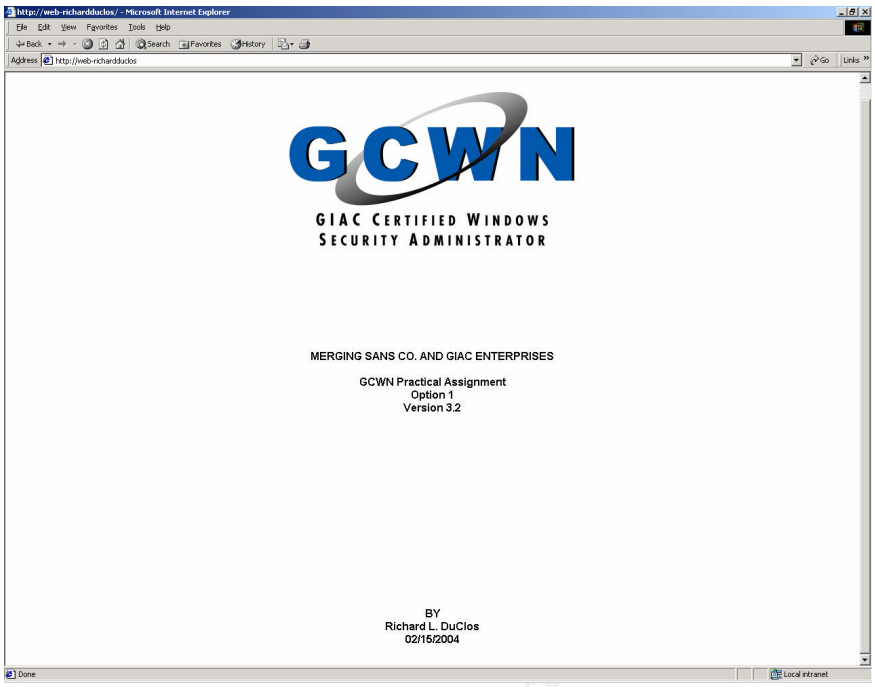

Figure 13 – WEB-RichardDuclos home page

As can be seen in the above image the web page opens, as it should with out any problems since the policies were correctly applied.

The final functionality test is to verify that members of the Developers group can login over the network using telnet. On a system logged in the user rduclos, access to telnet should not be allowed since the policy only allows Developers and Administrators access over the network. Rduclos only belongs to the User group.

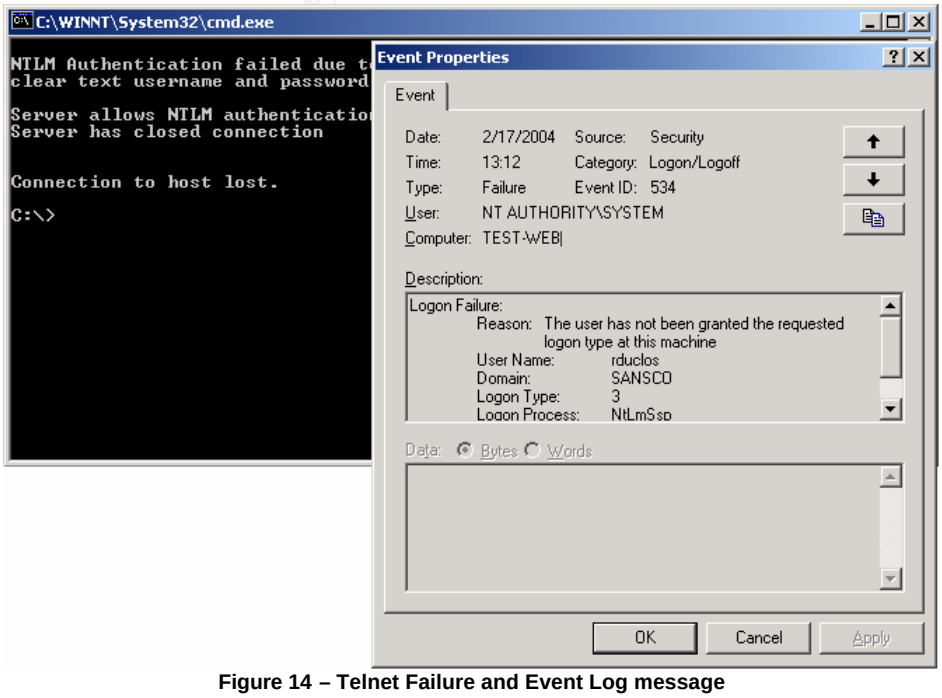

Figure 14 – Telnet Failure and Event Log message

With the user rduclos logged in telnet to WEB-RichardDuclos is not allowed. The resulting message from the event log is also displayed in the preceding Figure 14. This test further proves that the security policy is working as expected. Next, the user Richard who belongs to the Development group will login and try to telnet to the server WEB-RichardDuclos.

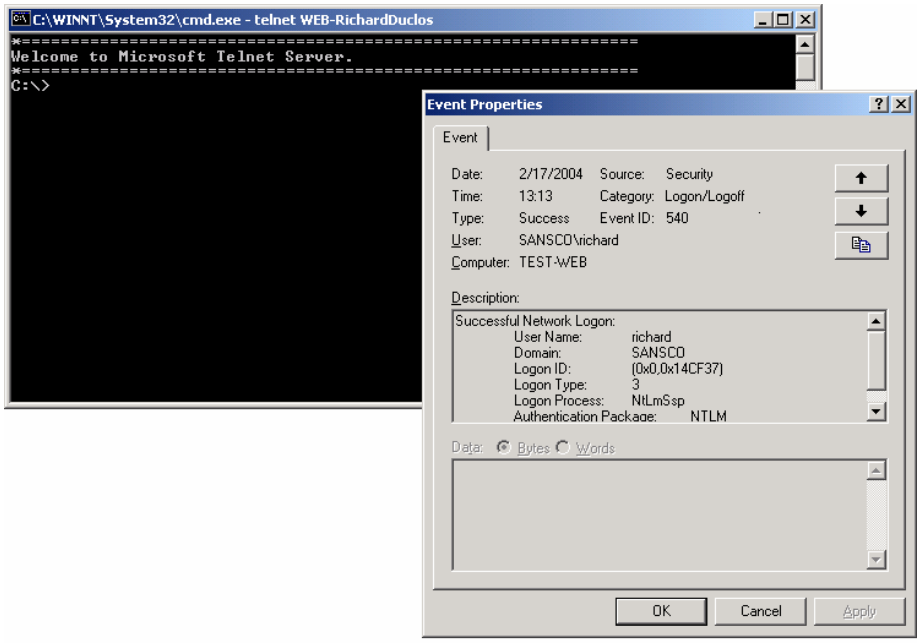

Figure 15 – Telnet Success and Event Log message

When the user Richard logged in the telnet session is opened. The resulting message from the event log is also displayed here in Figure 15. This test also proves that the policy is working correctly and there is not loss of functionality.

These two tests and use of the Security Configuration and Analysis snap-in prove that the security policy was applied and are functioning successfully. The next step is to test the policies security settings for proper configuration and operation.

3.4 Testing the policies security settings

With the policy built and applied now comes time to test the settings on the IIS server in the test lab. This test will include trying to connect to the web server locally as a general user and trying to shutdown the server. The only option available to the user should be log off and nothing else, but the administrator should be able to shutdown the system. The other test will include trying to add a printer as a user and then as the Administrator. As set in the policy users may not add print drivers to the machine, so this should work as planed.

For the first test will involve performing a login locally as a general user. The user for the experiment will be richard, which belongs to the development and

user groups. Once logged in the user richard will attempt to shutdown the system.

Figure 16 – Shutdown failure by general user

As depicted in the preceding figure, Figure 16, the shutdown option is not available as user Richard, so the policy did not fail. Next the Administrator attempts to login and shutdown the system. If the policy is configured correctly the administrator should have the option of shutting down the system.

Figure 17 – Shutdown success by Administrator

Again, as Figure 17 displays, with the Administrator login the option to shutdown the system is available once again. This is the result that was expected since the policy only allows administrators to shutdown the system.

The final test for verifying the security policies settings will be to try to add a printer as a user and then as the Administrator. With the user Richard logged in

again, the user attempts to open the printer folder and add a local printer. As depicted in Figure 18 below, the only option to the user is to add a network printer. The outcome of this test verifies that the policies settings are appropriate.

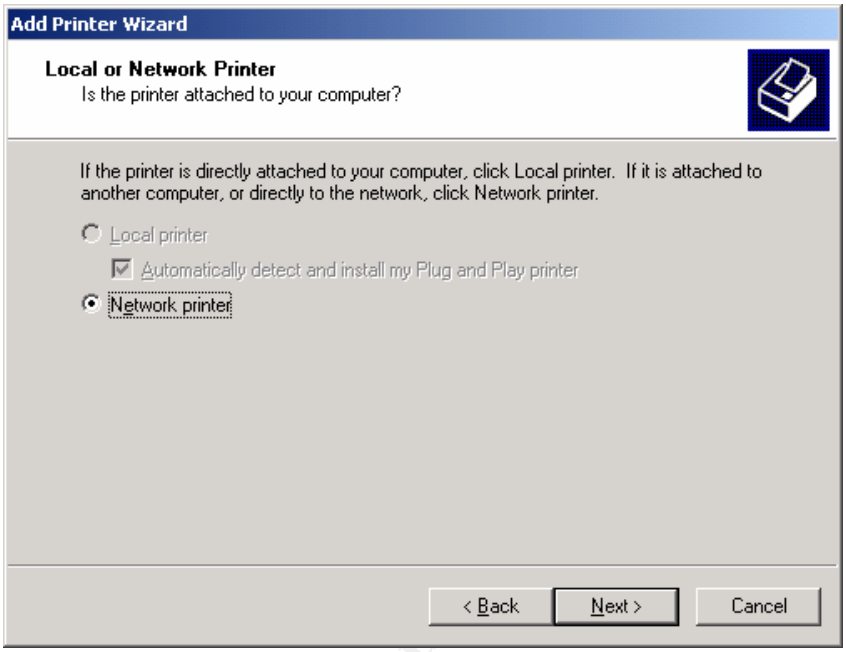

Figure 18 – User failure adding a printer

With the Administrator logged and attempts to add a printer to the local machine the option is now available to do so. Figure 19 below shows the window the Administrator saw and the available options.

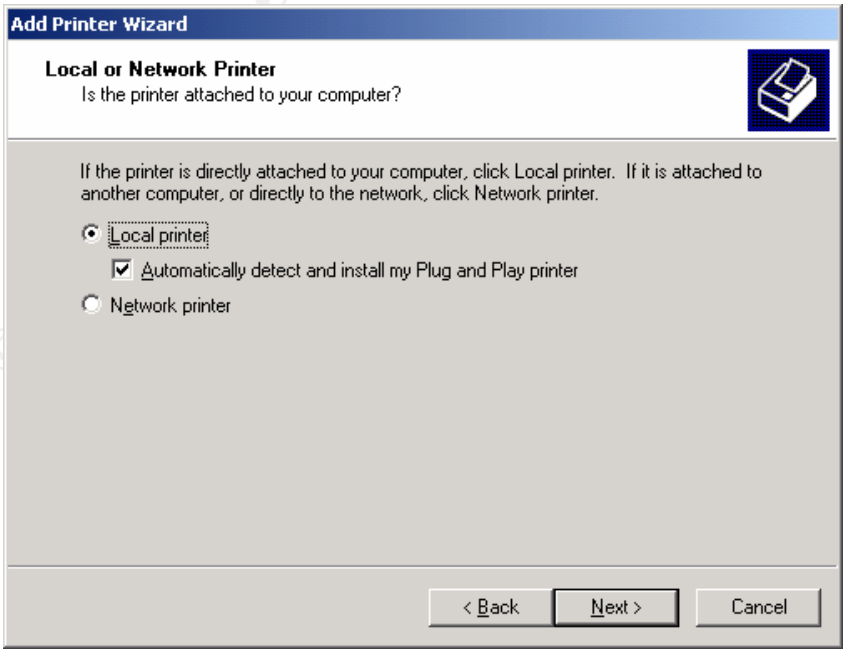

Figure 19 – Administrator success adding a printer

The final part of the printer settings test is to make sure members of the user group can print. The following print queue, Figure 20, show that the job was successfully submitted and status is printing.

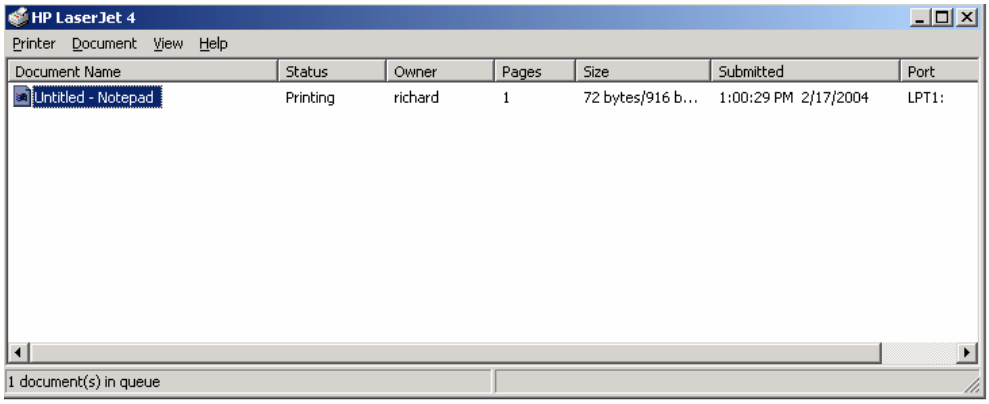

Figure 20 – User successful print job

These preceding two tests proved that the settings applied to the policy are performing as they were intended. No problems were encountered, with regards to security policy, during these tests.

3.5 Security Policy Evaluation

With the policies applied and tested evaluation of the applied policy is necessary to properly analyze it effectiveness. The only area of the policy that might be ineffective is allowing developers to login locally. This setting was implemented for easier administration of web applications but might be a security risk. This decision to allow developers to login would be locally considered an omission due to special circumstance. The policy should have the log settings and improved password policies already in place.

The only effect by having this setting disabled would be to the developers, if they need access, would need log in via the network rather than locally. It might be necessary for the developers to login locally to check code and setting of their web applications. There would be no impact to security by limiting their access would be, it would only be strengthened.

4 AUDITING

Now with the Active Directory design is complete and policies are tested it is time to develop an auditing strategy. The following sections will discuss gathering event logs and performance data, and checking of critical settings on a routine basis.

4.1 Gathering and Management of Event Logs and Performance data

SANS Co. / GIAC Enterprises will needs to utilize a utility that will enable the administrators to retrieve, and analyze logs. There are several options to do this, one use a tool in the Windows 2000 Resource Kit called dumpel. This utility can be configured to execute every morning on the domain controller to collect the logs and store them for future needs. The other option is to use the WMI_Dump_log.vbs, or WMI_Backup_clear_log.vbs scripts. Bill Boswell referenced these scripts in the GCWN course materials.

Dumpel is an utility that runs from command line and dumps the specified event log on local or remote computers. It stores the retrieved information in a tab-dilimted text file. It can also be used to filter on certain event. SANS Co. / GIAC could use dumpel to retrieve the logs from each member server and store them on the domain controller with out filtering on events (Microsoft - dumpel, 2).

These two WMI VBscripts can dump the information to text, or even back the log up and then clear the logs. Dumpel is a command line tool and these WMI scripts can be scheduled task and utilize Windows native VBScript support.

For example the logs on the IIS server are configured to overwrite as necessary, by using this utility daily it will enable logs will be retained for longer periods of time. This may not be the best solution since there are syslog applications for Windows, which might lead to better log retention results.

4.2 Checking of Critical Settings

Once the logs are gathered and retained a frequency for evaluating the system settings should be determined. This should be done on routine basis, perhaps quarterly. The event logs and GPOs should be evaluated during these reviews.

The retained eventlogs should undergo further forensic analysis to see is any hazardous or malicious changes have occurred. Scripts could be written to check the files and report any such findings to the administrators. The GPOs should be checked using the Security Configuration and Analysis snap-in to verify the current settings are the intend settings. The logs produced by the tool should too be kept on a long-term basis.

4.3 Checking of User Accounts

During these reviews the user accounts should be reviewed for any anomalies or users that are no longer part of the organization. It should be verified that these accounts have been disabled or deleted. User rights and groups assignments should also be verified for any mis-configurations.

After reading the GCWN material the best way to do this is using the ADSI (Active Directory Services Interface). For example, the script ADSI_Accounts_With_Old_Passwords.vbs, according to Bill Boswell, this script will show a list of user's passwords that have not been changed "in iMaxPasswordAge days". Using the ADSI_Auditing_Tool.vbs script can check the strength of user passwords.

5 CONCLUSION

In conclusion this document has described the merger of SANS Co. and GIAC Enterprises into one organization, SANS Co. / GIAC Enterprises and has specifically dealt with the merger of the two network and Active Directory infrastructures, and a basis for auditing the new infrastructure.

This document also provided an overview of the current network and Active Directory designs of each company, newly formed organization and other consideration that need to be considered. It was also described how the newly implemented network will be secured using templates and GPOs and the use of the SANS Co. DMZ.

Next, the document discussed the different policies that can be utilized, specifically policy for the IIS servers. It was also mentioned that the policies need to be tested in a test lab before using them in production. The test that SANS Co. used for the hisecweb template dealt with the implementation, application, and testing of the security policy. This test also generated many screen shots and event log data

Finally, this document discussed a set of routine activities to audit the infrastructure. The ways of auditing the newly formed infrastructure included gathering of the event logs, checking of critical setting and checking user accounts.

6 REFERENCES

Boswell, Bill. SANS Institute. "Windows 2000/XP Scripting For Security and Auditing ". February 13, 2003.

Davis, John. "From Blueprint to Fortress: A Guide to Securing IIS 5.0". June 2001. http://www.microsoft.com/technet/prodtechnol/iis/iis5/deploy/depovg/securiis.asp

Fossen, Jason. SANS Institute. "Active Directory ". January 24, 2003.

Haney, Julie M. "Guide to Securing Microsoft Windows 2000 Group Policy". September 13, 2001. http://www.nsa.gov/snac/win2k/guides/w2k-2.pdf

Haney, Julie M. "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set". December 3, 2002. http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf

Howard, Michael. "Secure Internet Information Services 5 Checklist". June 29, 2001. www.microsoft.com/technet/security/chklist/iis5chk.asp

Microsoft Corporation. "Introduction to Windows 2000 Group Policy". 1999. http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.asp

Microsoft Corporation. "IIS 5 HiSecWeb Potential Risks and the IIS Lockdown Tool". http://support.microsoft.com/default.aspx?scid=kb;en-us;316347

Microsoft Corporation. "Windows 2000 Security Hardening Guide". May 15, 2003. http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en

Rick, Gregory. "GIAC Enterprises Windows 2000 and Active Directory Design". GCWN Practical Assignment. May 24, 2002. http://www.giac.org/practical/Gregory_Rick_GCWN.doc

Sanderson, Mark J. "Guide to Securing Microsoft Windows 2000 Active Directory". December 2000. http://www.nsa.gov/snac/win2k/guides/w2k-5.pdf

7 APPENDIX A
Hisecweb.inf template

```
; (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 accept 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]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = 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"="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;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
ClipSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
Browser,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
Dhcp,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;WD)"
Fax,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDW
O;;;WD)"
SharedAccess,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLO
CRSDRCWDWO;;;WD)"
Messenger,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;WD)"
mnmsrvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
Spooler,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
RasAuto,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
RasMan,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)"
RemoteRegistry,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDT
LOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;WD)"
TapiSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
TermService,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOC
RSDRCWDWO;;;WD)"
PolicyAgent,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSW
RPWPDTLOCRSDRCWDWO;;;SY)"
```

```
W3SVC,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSWRPWPDT
LOCRSDRCWDWO;;;SY)"
IISADMIN,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;SY)"
Irmon,4,"D:AR(A;;RPWPDTRC;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)(A;;CCDCLCSWRPWPDTLOCR
SDRCWDWO;;;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\EnableSecuritySign
ature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPas
sword=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\TcpMaxConnectResponseRetransmi
ssions=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,A
T T E N T I O N !
```

8 APPENDIX B

Output from Security Configuration and Analysis snap-in for hisecweb.inf

```
-------------------------------------------
02/17/2004 15:28:10
----Analysis engine is initialized successfully.----

----Reading Configuration info...


----Analyze User Rights...
       Analyze SeNetworkLogonRight.
Mismatch       - SeNetworkLogonRight.
       Analyze SeTcbPrivilege.
Not Configured - SeTcbPrivilege.
       Analyze SeMachineAccountPrivilege.
Not Configured - SeMachineAccountPrivilege.
       Analyze SeBackupPrivilege.
Not Configured - SeBackupPrivilege.
       Analyze SeChangeNotifyPrivilege.
Not Configured - SeChangeNotifyPrivilege.
       Analyze SeSystemtimePrivilege.
Not Configured - SeSystemtimePrivilege.
       Analyze SeCreatePagefilePrivilege.
Not Configured - SeCreatePagefilePrivilege.
       Analyze SeCreateTokenPrivilege.
Not Configured - SeCreateTokenPrivilege.
       Analyze SeCreatePermanentPrivilege.
Not Configured - SeCreatePermanentPrivilege.
       Analyze SeDebugPrivilege.
Not Configured - SeDebugPrivilege.
       Analyze SeRemoteShutdownPrivilege.
Not Configured - SeRemoteShutdownPrivilege.
       Analyze SeAuditPrivilege.
Not Configured - SeAuditPrivilege.
       Analyze SeIncreaseQuotaPrivilege.
Not Configured - SeIncreaseQuotaPrivilege.
       Analyze SeIncreaseBasePriorityPrivilege.
Not Configured - SeIncreaseBasePriorityPrivilege.
       Analyze SeLoadDriverPrivilege.
Not Configured - SeLoadDriverPrivilege.
       Analyze SeLockMemoryPrivilege.
Not Configured - SeLockMemoryPrivilege.
       Analyze SeBatchLogonRight.
Not Configured - SeBatchLogonRight.
       Analyze SeServiceLogonRight.
Not Configured - SeServiceLogonRight.
       Analyze SeInteractiveLogonRight.
Not Configured - SeInteractiveLogonRight.
       Analyze SeSecurityPrivilege.
Not Configured - SeSecurityPrivilege.
       Analyze SeSystemEnvironmentPrivilege.
Not Configured - SeSystemEnvironmentPrivilege.
       Analyze SeProfileSingleProcessPrivilege.
Not Configured - SeProfileSingleProcessPrivilege.
       Analyze SeSystemProfilePrivilege.
Not Configured - SeSystemProfilePrivilege.
       Analyze SeAssignPrimaryTokenPrivilege.
Not Configured - SeAssignPrimaryTokenPrivilege.
       Analyze SeRestorePrivilege.
Not Configured - SeRestorePrivilege.
       Analyze SeShutdownPrivilege.
Not Configured - SeShutdownPrivilege.
       Analyze SeTakeOwnershipPrivilege.
Not Configured - SeTakeOwnershipPrivilege.
       Analyze SeDenyNetworkLogonRight.
Not Configured - SeDenyNetworkLogonRight.
       Analyze SeDenyBatchLogonRight.
Not Configured - SeDenyBatchLogonRight.
```

```
       Analyze SeDenyServiceLogonRight.
Not Configured - SeDenyServiceLogonRight.
       Analyze SeDenyInteractiveLogonRight.
Not Configured - SeDenyInteractiveLogonRight.
       Analyze SeUndockPrivilege.
Not Configured - SeUndockPrivilege.
       Analyze SeSyncAgentPrivilege.
Not Configured - SeSyncAgentPrivilege.
       Analyze SeEnableDelegationPrivilege.
Not Configured - SeEnableDelegationPrivilege.

       User Rights analysis completed successfully.

----Reading Configuration info...


----Analyze Group Membership...
       Analyze Users.
Not Configured - *S-1-5-32-545__Members.
       Analyze Replicator.
Not Configured - *S-1-5-32-552__Members.
       Analyze Guests.
Not Configured - *S-1-5-32-546__Members.
       Analyze Backup Operators.
Not Configured - *S-1-5-32-551__Members.
       Analyze Administrators.
Not Configured - *S-1-5-32-544__Members.
       Analyze Power Users.

       Group Membership analysis completed successfully.

----Reading Configuration info...


----Analyze Registry Keys...
Not Configured - CLASSES_ROOT.
Not Configured - USERS.
Not Configured - MACHINE.

       Registry keys analysis completed successfully.

----Reading Configuration info...


----Analyze File Security...
Not Configured - C:.

       File security analysis completed successfully.


----Analyze General Service Settings...
       Analyze wuauserv.
Not Configured - wuauserv.
       Analyze Wmi.
Not Configured - Wmi.
       Analyze WMDM PMSP Service.
Not Configured - WMDM PMSP Service.
       Analyze WinMgmt.
Not Configured - WinMgmt.
       Analyze W3SVC.
       Analyze W32Time.
Not Configured - W32Time.
       Analyze UtilMan.
Not Configured - UtilMan.
       Analyze UPS.
Not Configured - UPS.
       Analyze TrkWks.
Not Configured - TrkWks.
       Analyze TlntSvr.
Not Configured - TlntSvr.
       Analyze TapiSrv.
```

```
Mismatch       - TapiSrv.
       Analyze SysmonLog.
Not Configured - SysmonLog.
       Analyze Spooler.
Mismatch       - Spooler.
       Analyze SMTPSVC.
Not Configured - SMTPSVC.
       Analyze SharedAccess.
Mismatch       - SharedAccess.
       Analyze SENS.
Not Configured - SENS.
       Analyze seclogon.
Not Configured - seclogon.
       Analyze Schedule.
Mismatch       - Schedule.
       Analyze SCardSvr.
Not Configured - SCardSvr.
       Analyze SCardDrv.
Not Configured - SCardDrv.
       Analyze SamSs.
Not Configured - SamSs.
       Analyze RSVP.
Not Configured - RSVP.
       Analyze RpcSs.
Not Configured - RpcSs.
       Analyze RpcLocator.
Not Configured - RpcLocator.
       Analyze RemoteRegistry.
Mismatch       - RemoteRegistry.
       Analyze RemoteAccess.
Not Configured - RemoteAccess.
       Analyze RasMan.
Mismatch       - RasMan.
       Analyze RasAuto.
Mismatch       - RasAuto.
       Analyze ProtectedStorage.
Not Configured - ProtectedStorage.
       Analyze PolicyAgent.
       Analyze PlugPlay.
Not Configured - PlugPlay.
       Analyze NVSvc.
Not Configured - NVSvc.
       Analyze NtmsSvc.
Not Configured - NtmsSvc.
       Analyze NtLmSsp.
Not Configured - NtLmSsp.
       Analyze Netman.
Not Configured - Netman.
       Analyze Netlogon.
Not Configured - Netlogon.
       Analyze NetDDEdsdm.
Not Configured - NetDDEdsdm.
       Analyze NetDDE.
Not Configured - NetDDE.
       Analyze MSIServer.
Not Configured - MSIServer.
       Analyze MSFTPSVC.
Not Configured - MSFTPSVC.
       Analyze MSDTC.
Not Configured - MSDTC.
       Analyze mnmsrvc.
Mismatch       - mnmsrvc.
       Analyze Messenger.
Mismatch       - Messenger.
       Analyze McShield.
Not Configured - McShield.
       Analyze LmHosts.
Not Configured - LmHosts.
       Analyze lanmanworkstation.
Not Configured - lanmanworkstation.
       Analyze lanmanserver.
```

```
Not Configured - lanmanserver.
        Analyze IISADMIN.
        Analyze Fax.
Mismatch        - Fax.
        Analyze EventSystem.
Not Configured - EventSystem.
        Analyze Eventlog.
Not Configured - Eventlog.
        Analyze Dnscache.
Not Configured - Dnscache.
        Analyze dmserver.
Not Configured - dmserver.
        Analyze dmadmin.
Not Configured - dmadmin.
        Analyze Dhcp.
Mismatch        - Dhcp.
        Analyze ClipSrv.
Mismatch        - ClipSrv.
        Analyze cisvc.
Not Configured - cisvc.
        Analyze Browser.
Mismatch        - Browser.
        Analyze BITS.
Not Configured - BITS.
        Analyze AvSynMgr.
Not Configured - AvSynMgr.
        Analyze Ati HotKey Poller.
Not Configured - Ati HotKey Poller.
        Analyze AppMgmt.
Not Configured - AppMgmt.
        Analyze Alerter.
Mismatch        - Alerter.

        General Service analysis completed successfully.


----Analyze available attachment engines...
        Load attachment LanManServer.
LanManServer: Query configuration information

        Attachment engines analysis completed successfully.

----Reading Configuration info...


----Analyze Security Policy...
Mismatch        - MaximumPasswordAge.
        Analyze password information.
Mismatch        - LockoutBadCount.
        Analyze account lockout information.
Not Configured - NewAdministratorName.
Not Configured - NewGuestName.
        Analyze other policy settings.

        System Access analysis completed successfully.
Not Configured - MaximumLogSize.
Not Configured - AuditLogRetentionPeriod.
Not Configured - MaximumLogSize.
Not Configured - AuditLogRetentionPeriod.
        Analyze log settings.
Not Configured - AuditProcessTracking.
Not Configured - AuditDSAccess.
        Analyze event audit settings.
Not Configured - CrashOnAuditFull.

        Audit/Log analysis completed successfully.
        Analyze machine\software\microsoft\driver signing\policy.
        Analyze machine\software\microsoft\windows
nt\currentversion\winlogon\allocatecdroms.
        Analyze machine\software\microsoft\windows
nt\currentversion\winlogon\allocatedasd.
```

```
       Analyze machine\software\microsoft\windows
nt\currentversion\winlogon\allocatefloppies.
       Analyze
machine\software\microsoft\windows\currentversion\policies\system\disablecad.
       Analyze
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername
.
       Analyze
machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption.
       Analyze
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
Mismatch       -
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
       Analyze
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon.
       Analyze machine\software\policies\microsoft\windows
nt\printers\disablewebprinting.
       Analyze
machine\system\currentcontrolset\control\filesystem\ntfsdisable8dot3namecreation.
       Analyze machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
       Analyze machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel.
       Analyze machine\system\currentcontrolset\control\lsa\restrictanonymous.
       Analyze machine\system\currentcontrolset\control\print\providers\lanman print
services\servers\addprinterdrivers.
       Analyze machine\system\currentcontrolset\control\session manager\memory
management\clearpagefileatshutdown.
       Analyze machine\system\currentcontrolset\control\session manager\protectionmode.
       Analyze
machine\system\currentcontrolset\services\afd\parameters\dynamicbackloggrowthdelta.
       Analyze
machine\system\currentcontrolset\services\afd\parameters\enabledynamicbacklog.
       Analyze
machine\system\currentcontrolset\services\afd\parameters\maximumdynamicbacklog.
       Analyze
machine\system\currentcontrolset\services\afd\parameters\minimumdynamicbacklog.
       Analyze
machine\system\currentcontrolset\services\lanmanserver\parameters\autoshareserver.
       Analyze
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff.
       Analyze
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature
.
       Analyze
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpas
sword.
       Analyze
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysign
ature.
       Analyze
machine\system\currentcontrolset\services\netbt\parameters\nonamereleaseondemand.
       Analyze
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange.
       Analyze
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel.
       Analyze
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\disableipsourcerouting.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\enabledeadgwdetect.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\enableicmpredirect.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\enablepmtudiscovery.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\enablesecurityfilters.
       Analyze machine\system\currentcontrolset\services\tcpip\parameters\keepalivetime.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\synattackprotect.
```

```
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxconnectresponseretransmi
ssions.
       Analyze
machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxdataretransmissions.
       Analyze
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey.
Not Configured -
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey.
       Analyze
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal.
Not Configured -
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal.
       Analyze
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySig
nature.
Not Configured -
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySig
nature.
       Analyze
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignatur
e.
Not Configured -
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignatur
e.
       Analyze
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect.
Not Configured -
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect.
       Analyze MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl.
Not Available  - MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl.
       Analyze MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail.
Not Configured - MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail.
       Analyze MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects.
Not Configured - MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects.
       Analyze MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScRemoveOption.
Not Configured - MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScRemoveOption.
       Analyze MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning.
Not Configured - MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning.
       Analyze MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\CachedLogonsCount.
Not Configured - MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\CachedLogonsCount.
       Analyze MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand.
Not Configured - MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand.
       Analyze MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel.
Not Configured - MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel.
       Analyze MACHINE\Software\Microsoft\Non-Driver Signing\Policy.
Not Configured - MACHINE\Software\Microsoft\Non-Driver Signing\Policy.

       Registry values analysis completed successfully.


----Analyze available attachment engines...

       Attachment engines analysis completed successfully.


----Un-initialize analysis engine...
```