



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>

Willie Lui Tien Heong

GIAC Certified Windows Security Administrator (GCWN) Practical
Assignment Version 3.2 (Revised March 2003)

Assignment Option 1 – The Design and Implementation of a
Windows 2000 Multi-Forest Infrastructure

Date submitted : 10 July 2003

© SANS Institute 2003, Author retains full rights.

Abstract

Sans Co. has merged with GIAC Enterprise and the interoperability and management issues between their existing AD forest infrastructures are addressed in the first part of this paper. A group policy is designed for the merged company and implemented on one of their existing Intranet IIS servers. Finally, a full audit strategy is implemented for the long maintenance and management of the implemented group policy.

© SANS Institute 2003, Author retains full rights.

1.0 Introduction

SANS Co. and GIAC Enterprise has just completed a successful corporate merger. It is hoped that through this merger, SANGIAC the resultant company will scale to greater heights. The new combined senior management team has engaged (with immediate effect) "WL Consulting Inc" as the IT consultants responsible for making sure that the IT investments, especially the extensive Active Directory infrastructure being set up at both sites continue to function normally. In addition, due to the external linkages that both infrastructures have established with suppliers and customers, the option of migrating one forest to the other has been totally ruled out.

Given the huge payoff, WL Consulting Inc has a senior consultant to oversee the whole project to ensure the smooth execution of merger of the two forests at the technological frontline. The tasks are as follows:

- a. To design a trust relationship between the two forests such that IT resources can be consolidated and more efficiently managed. Customers and suppliers of both companies must continue to be able to deal with the companies seamlessly via the web.
- b. Based on the resulting architecture, provide a tested group policy design that encompasses the needs of the two companies.
- c. Evaluate the final group policy and analyze its effectiveness in ensuring commensurate level of security for both applications and users.
- d. Finally, conduct an audit of the Active Directory infrastructure.

1.1 Considerations

There are several important considerations:

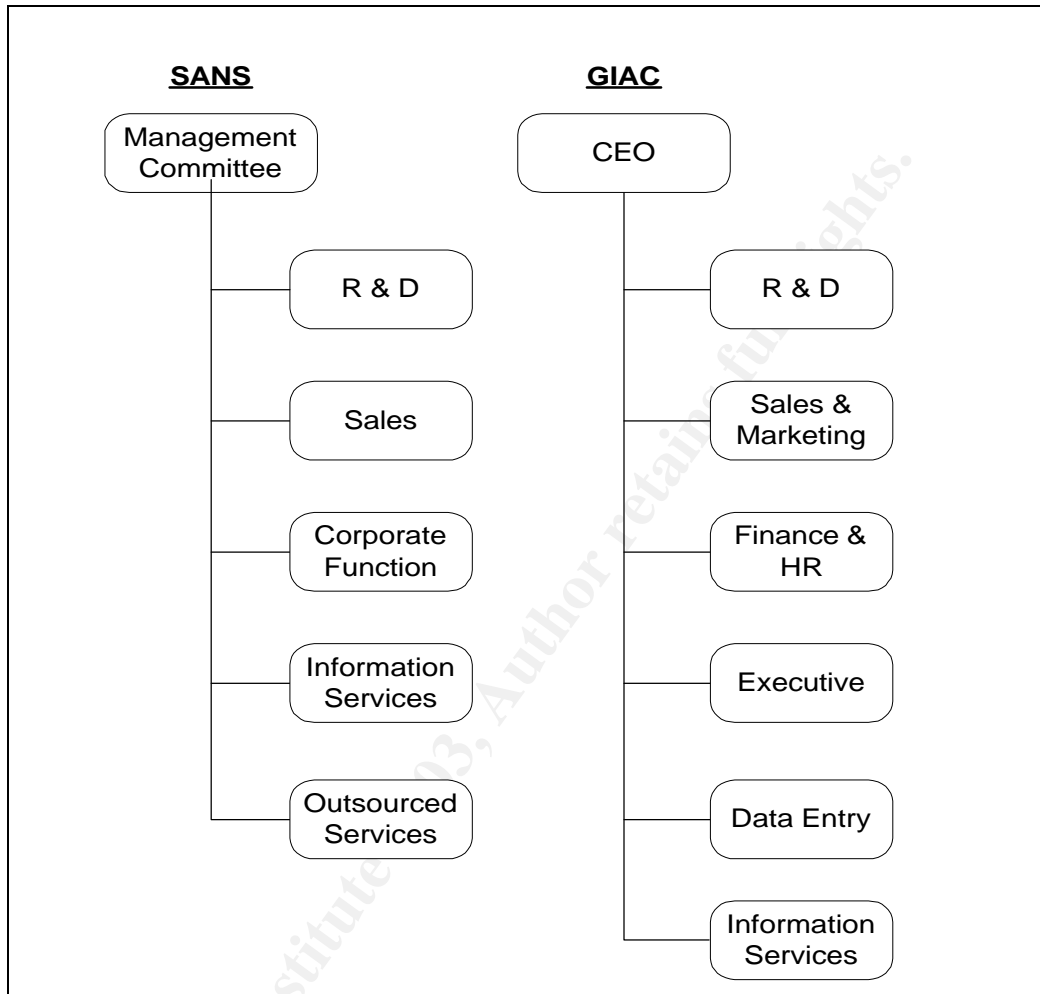
- a. Given the sensitive situation where an expected 20 % reduction of combined staff strengths, the need to establish tip top preventive, detective, deterrence and corrective IT security controls is paramount.
- b. It is important that all business activities for SANS Co. and GIAC Enterprise must not be affected in any way.

2.0 Overview

SANS Co. (SANS) is a buffet and high tea research and development company with about 100 employees. SANS conducts surveys with top-notch hoteliers, buffet food caterers and major food suppliers and compiles the research findings and data about buffet and finger food trends. However, the SANS management, recognizing that sandwiches, being the highest consumed food at buffet lunches and high teas, has decided to acquire GIAC, a sandwich research and development company for competitive reasons. For two years in a row, GIAC has been recognized by the food industry as the leading sandwich research company whose research data is considered authoritative for all types of sandwiches. SANS management, envisions that a

corporate merger GIAC will provide more cutting edge research data for the buffet and high tea industry as a whole.

The corporate structures of both companies are shown below:



I shall not attempt to discuss GIAC Enterprise corporate structure in this practical as I have based that on Matthew D. Arnold's well written GCWN [practical](#) dated 12 March 2003. Please follow the link to obtain a more detailed explanation of GIAC's corporate setup and their AD administrative requirements. However, I may use some of the materials from Arnold's practical mainly to illustrate the design of SANGIAC's AD better and the corporate/political issues that have been taken into considerations.

SANS has only about a 100 employees. Throughout their short history as a five year company, SANS management has maintained that their company will stay lean and mean. They will focus their core employees on mission critical areas and leave the day to day mundane tasks such as data entry, computer operations to outsourced services. Sensitive and important functions such as Human Resource, Finance, Sales, R & D and IT server administration and security are left in-house.

Having external contractors working within the midst of SANS employees makes it even more important that security controls such segregation of duties and least privilege is implemented.

The main departments within SANS include:

Research and Development (10 staffs): This is a team of highly experience and paid analysts who analyzes the raw data coming in from survey results. The R & D team is also responsible for constantly improving SANS own in-house developed data analysis software “CRUNCH”. Due to the highly sensitive nature of their business, the R & D department is totally isolated from the rest of the company in a different block of building and interaction is limited to the R & D manager. The R & D team boasts their own IT administrator super-user that manages their user accounts and computers.

Sales and Marketing (20 staffs): The Sales and Marketing department is highly mobile and are equipped with laptops and PDAs. Their job nature is typically to conduct market surveys and to expand the scope of their surveys to more hoteliers and food industry players so as to improve the trustworthiness of their research findings. The S & M department employees are typical IT end-users who would rather leave all messy configurations to the experts.

Corporate Functions (30 staffs): This is the biggest department in SANS. They include the Finance, HR and corporate administrative people. Their job includes hiring, buying, invoicing, building and maintaining. Although not as mobile, the corporate staffs are very much similar to the S & M staff who would rather not mess around with their computers.

Information Services (15 staffs): This department is responsible for the ensuring smooth day-to-day operation of SANS IT system. The department includes an application team, administration team and a network team. The day to day operation of the computers have been outsourced and come under the outsourced services department, but the core administrators are still within the IS department. The administration team already enjoys the greatest IT privileges among the SANS staff but would never reject the chance of having more privileges.

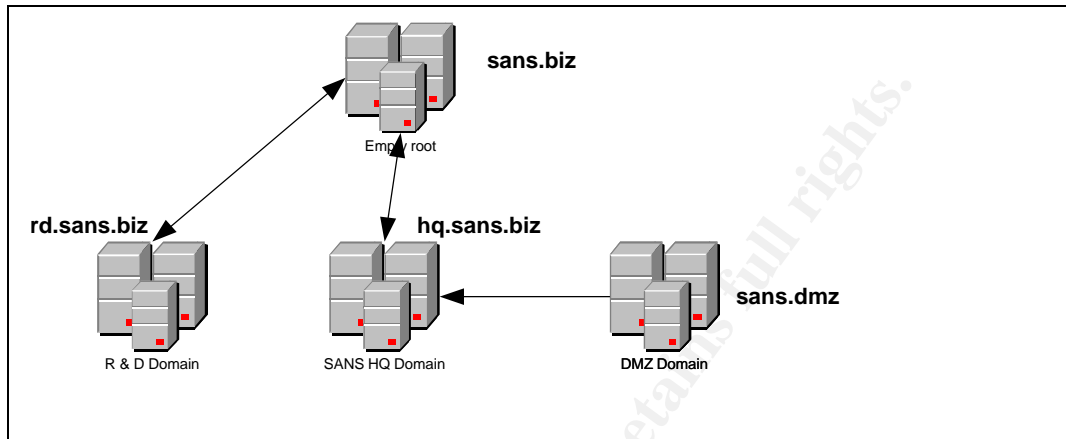
Outsourced Services (25 staffs): These people include the application developers, the 24 hour computer operations whom are in-charge of backup operations and running batch job. Basically they are outsiders who cannot be trusted fully.

Management Committee (5 staffs): SANS is really managed by a committee rather than a single person. Even though the CEO is sitting on top of the organization chart, he is only part of the management committee of 5. The management committee comprises of the CEO himself and the heads of each functional department within SANS. This is a special group of people who

need special attention in the design of the AD. Their IT needs are simple but immediate.

3.0 Existing Domain Design for SANS Co.

The figure before depicts SANS domain design:



SANS domain design is based on an empty root domain.

Due to the low-bandwidth connection between the R & D department and the main company building and the high need for self-administration, a separate sub-domain has been specially created for the R & D department. The Enterprise Admin group has been removed from the Local Administrators group of all domain controllers in the R & D sub-domain.

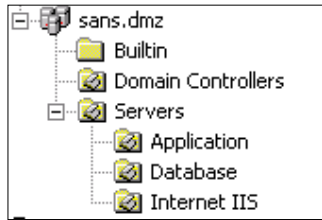
However, to ensure that forest-wide settings continue to be replicated to the sub-domain, the Enterprise Admins group is given Full Control to the Configuration NC.

The SANS HQ domain contains all Organizational Units and Objects pertaining to SANS HQ. These include two Domain Controllers, one Intranet IIS server, and an SQL database server, file and print servers, exchange email servers and the Staff Organization Unit. More details on the specific OUs will be shared in the next section.

The DMZ domain is a standalone forest that houses all DMZ machines which include one domain controller, an Internet application server, an Internet web server and a Internet database server. There are no users within the DMZ domain. However, the DMZ domain has a one-way trust with the SANS HQ domain which enable SANS web admin staff to administer the web site and applications remotely. The Internet database server is hosted in another service network segment of the corporate firewall.

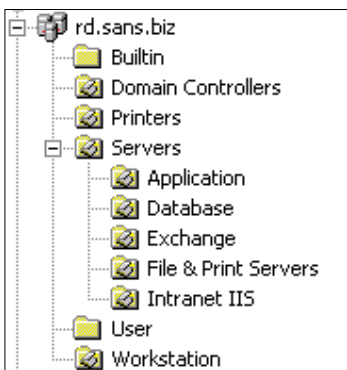
The one-way explicit trust with the SANS HQ domain ensures that if any of the DMZ machines are compromised, it will not easily filter down to the main SANS domain.

3.1 Organizational Units of SANS



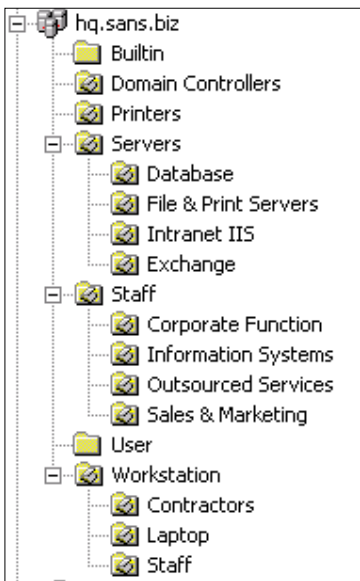
The figure on the left illustrates the OU structure of the SANS Co. The DMZ domain contains:

- **Builtin Container** containing all default group account objects such as Administrators, Server Operators etc.
- **Domain Controllers OU** which contains domain controller computer objects.
- **Servers OU** which in turn contains the database servers OU, the Internet IIS servers OU and the application servers OU.



The R & D domain contains the

- Builtin Container
- Domain Controller OU
- **Printers OU** for all printers used in the R & D department
- **User container** which contains the user account objects of all users in the R & D department
- **Workstation OU** which contains computer objects of desktops in the R & D department



The SANS HQ contains the

- Builtin Container
- Domain Controllers OU
- Printers OU for all printers used throughout SANS HQ
- Servers OU which include the database servers OU, the file and print servers OU, the mail servers OU and the IIS OU
- **Staff OU** which in turn contains the Corporate Function OU, the Information Systems OU, the Outsourced Services OU, the Sales and Marketing OU
- User Container contains default Windows 2000 user and computer group account objects.
- The Workstation OU contains the
 - o Contractors OU which in turn contain computer objects for contractors' workstations.
 - o Staff OU containing all computer objects of staff workstations.
 - o Laptop OU containing all computer objects of laptop computers.

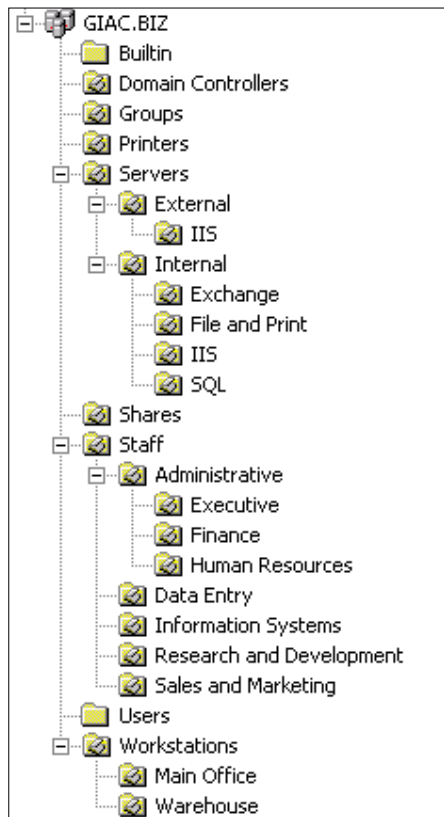
Some points to note:

User Global groups are created for each department containing all the users in the group and placed under the appropriate Staff OU.

Administrative accounts are placed in **Domain Admins** global group.

Computer Global groups are created for each department's computers and placed under the appropriate workstation OU.

3.2 Organizational Units of GIAC



This section is extracted from Matthew's practical just to let you get a flavor of the existing GIAC OU Design. I shall not go into any details and would urge you to refer to pages 16-17 of his practical.

The diagram illustrates a multi-domain Active Directory forest structure for SANS. At the top is the **sans.biz** domain, identified as the **Empty Root Domain**. Below it are four child domains: **rd.sans.biz** (labeled **R & D Domain**), **hq.sans.biz** (labeled **Main SANS employee Domain**), **sans.dmz** (labeled **DMZ Domain**), and **giac.biz** (labeled **GIAC**). Arrows show replication links from the root domain to each child domain, and bidirectional links between the child domains, indicating a fully replicated forest.

In order to facilitate the eventual consolidation of IT investments in both companies, it is necessary to establish a two-way non-transitive trusts between the SANS and GIAC forests.

3.3 Business Needs for Interoperability and Consolidation [1]

- a. Senior executives and staff of SANS and GIAC must be able share informational resources such as word documents, spreadsheets and power-point presentations. Hence it is important that the trust is setup such that SANS' executive can allow GIAC's executive access to their information residing on the SANS file servers and VICE VERSA. As the SANS file servers reside within the main SANS employee domain, a two-way trust relationship is established between the two domains.

- b. There will also be a need for printers located at each company's office to be accessible by officers from the other company. This will prove to be invaluable when senior officers from SANS need to print a document urgently while having a meeting at GIAC's locality.

Hence the domain design should take this into account, although such freedom of access to each other's computing resources must not be at the expense of security.

3.3.2 Consolidation of Computing Resources

It is important for duplicated computing resources such as Internet Web Servers, serving customers of both companies and the backend databases be consolidated at SANS within the DMZ domain. Although GIAC and SANS are not physically located within the same building, it is more cost effective to establish a T1 lease line between the two companies than to manage separate machines in the long run.

The computing resources that will be consolidated are:

- Internet IIS web server
- Internet Database server

The website from GIAC will be migrated to SANS Internet IIS Server where a virtual web site will be created to host the additional content and application. Major rework of codes may be necessary.

Some of the considerations for designing the domain application structure are:

- the submission of survey results by suppliers must not be affected as all survey results are deposited into the Internet database server
- the Finance, HR and Executive staff at GIAC needs to have read and write access to some non R & D tables in the Intranet Database server at SANS.
- The data entry staff at GIAC should be able to continue performing data entry work on the Intranet Database at GIAC.
- Application data that previously belong to SANS or GIAC should be available to both with the merger.

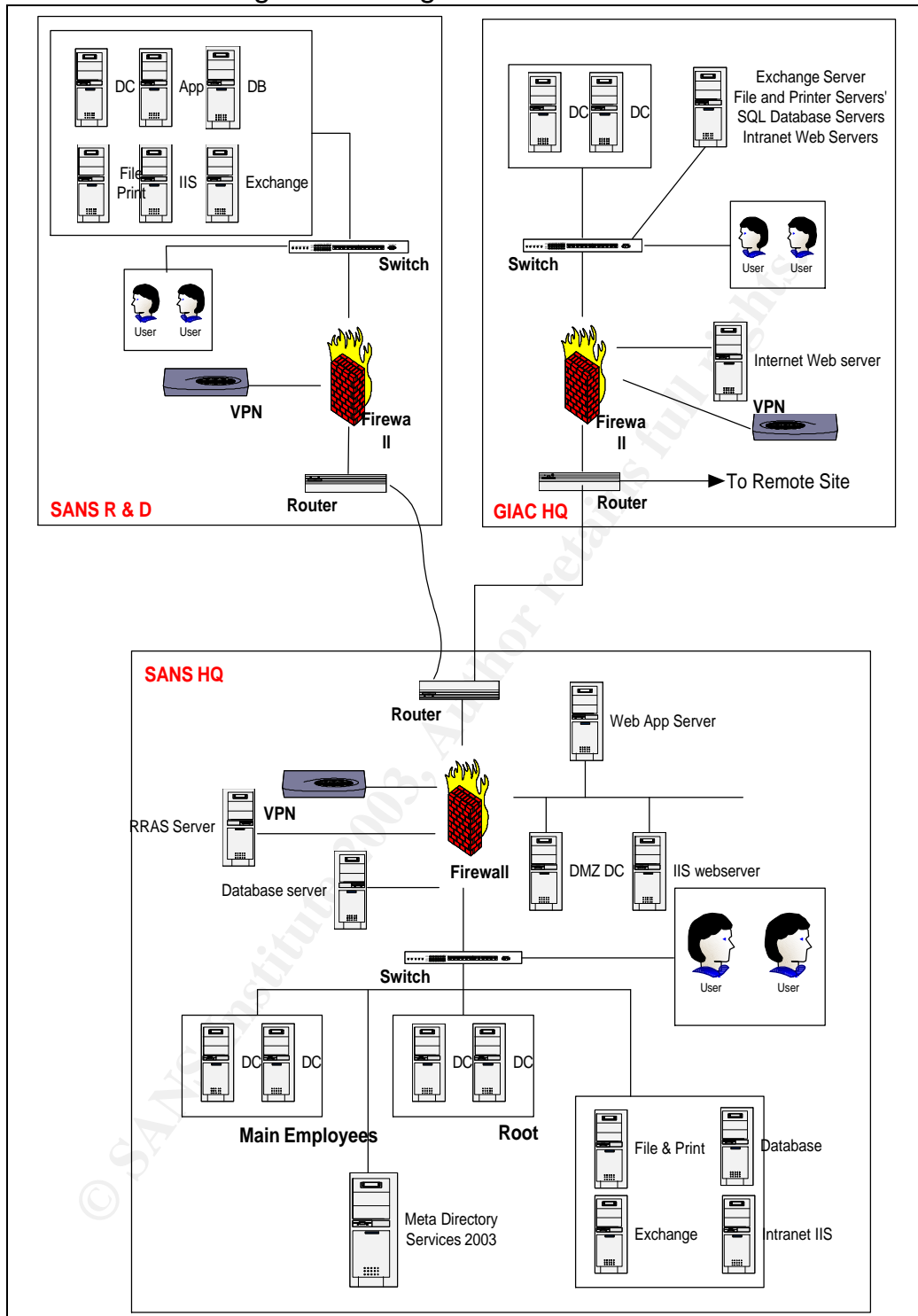
3.3.3 Single Address List for Both Forest

A single address list (containing contact information from both forests) shall be made available for all executives. This is important as a single address list facilitates easy searching for contact details such as pager, designation, department and email address.

3.3.4 Cross Forest Access to Calendars

Executive in SANS should be able to access the calendars of GIAC's executive and vice versa. Furthermore, they should be able to arrange and send meeting invitations to executives from the other company.

3.4 Network Diagram of Merged Co.



As the network diagram above depicts, the merged company will have three main sites. The R&D department will be linked to the SANS HQ over the Internet via secure router-router VPN connections. The GIAC network is connected to the SANS HQ network by a 2M dedicated leased line.

3.5 Organizational Unit, Groups and Group Policy Design for SANGIAC

Since there will not be massive migration from one forest to the other, the OU design of the two forests stay pretty much intact. However, the following needs to be implemented to ensure that the business needs for collaboration and interoperability can be achieved with efficient maintenance at the same time.

Domain, OU, Computer, Group	Effective GPO
Root Domain	Default Domain Policy GPO
Domain Controllers (OU) <ul style="list-style-type: none"> DC1 DC2 	Default Domain Controller Policy GPO
Administrators (OU) <ul style="list-style-type: none"> Domain Admins Enterprise Admins Schema Admins Administrators Server Operators Backup Operators Account Operators 	Default Domain Policy GPO

Domain, OU, Computer, Group	Effective GPO
SANS HQ	Default Domain Policy GPO
Domain Controllers (OU) <ul style="list-style-type: none"> DC1 DC2 	Default Domain Controller Policy GPO
Printers (OU) <ul style="list-style-type: none"> Printer (Corp Fn) Printer (IS) Printer (OSS) Printer (S & M) 	Default Domain Policy GPO
Servers (OU) <ul style="list-style-type: none"> Database (OU) <ul style="list-style-type: none"> Database Svr 1 File & Print Servers (OU) <ul style="list-style-type: none"> File & Print Svr 1 File & Print Svr 2 Intranet IIS (OU) <ul style="list-style-type: none"> IIS Server 1 Exchange (OU) <ul style="list-style-type: none"> Mail Server 1 Mail Server 2 Mail Server 3 	Servers GPO
Staff <ul style="list-style-type: none"> Corporate Function (OU) <ul style="list-style-type: none"> Corp Fn Grp Information Systems (OU) <ul style="list-style-type: none"> IS Grp Outsource Services (OU) <ul style="list-style-type: none"> OS Grp Sales & Marketing (OU) <ul style="list-style-type: none"> S&M Grp 	Staff GPO

Domain, OU, Computer, Group	Effective GPO
Administrators (OU) <ul style="list-style-type: none"> Domain Admins Administrators Server Operators Backup Operators Account Operators 	Admin GPO
Workstation (OU) Contractors (OU) <ul style="list-style-type: none"> Contractors Desktop Grp Laptop (OU) <ul style="list-style-type: none"> Laptop Desktop Grp Staff (OU) <ul style="list-style-type: none"> Corp Fn Desktop Grp IS Desktop Grp 	Workstation GPO Contractor GPO Laptop GPO

Domain, OU, Computer, Group	Effective GPO
SANS DMZ	Default Domain Policy GPO
Domain Controllers (OU) <ul style="list-style-type: none"> DC1 	Default Domain Controller Policy GPO
Servers (OU) Application (OU) <ul style="list-style-type: none"> Application Svr 1 Database (OU) <ul style="list-style-type: none"> Database Svr 1 Internet IIS (OU) <ul style="list-style-type: none"> IIS Svr 1 RRAS Server	DMZ Servers GPO
Administrators (OU) <ul style="list-style-type: none"> Domain Admins Administrators Server Operators Backup Operators Account Operators 	Admin GPO

Domain, OU, Computer, Group	Effective GPO
R & D	Default Domain Policy GPO
Domain Controllers (OU) <ul style="list-style-type: none"> DC1 	Default Domain Controller Policy GPO
Servers (OU) Application (OU) <ul style="list-style-type: none"> Application Svr 1 Database (OU) <ul style="list-style-type: none"> Database Svr 1 Intranet IIS (OU) <ul style="list-style-type: none"> IIS Svr 1 Exchange (OU) <ul style="list-style-type: none"> Mail Svr 1 File & Print Server (OU) <ul style="list-style-type: none"> File Svr 1 	Servers GPO
Staff (OU) <ul style="list-style-type: none"> User Account 1 User Account 2 	Staff GPO

Domain, OU, Computer, Group	Effective GPO
Administrators (OU) <ul style="list-style-type: none"> Domain Admins Administrators Server Operators Backup Operators Account Operators 	Admin GPO
Printers (OU) <ul style="list-style-type: none"> Printer 1 	Default Domain Policy GPO
Workstation (OU) <ul style="list-style-type: none"> Workstation 1 Workstation 2 	Workstation GPO

Domain, OU, Computer, Group	Effective GPO
GIAC	Default Domain Policy GPO
Domain Controllers (OU) <ul style="list-style-type: none"> DC1 DC2 	Default Domain Controller Policy GPO
Groups (OU)	Default Domain Policy GPO
Printers (OU)	Default Domain Policy GPO
Servers (OU) <ul style="list-style-type: none"> SQL (OU) <ul style="list-style-type: none"> Database Svr 1 IIS (OU) <ul style="list-style-type: none"> IIS Svr 1 Exchange (OU) <ul style="list-style-type: none"> Mail Svr 1 File & Print Server (OU) <ul style="list-style-type: none"> File Svr 1 	Servers GPO
Shares (OU)	Default Domain Policy GPO
Staff (OU) <ul style="list-style-type: none"> Administrative (OU) <ul style="list-style-type: none"> Executive (OU) Finance (OU) Human Resources (OU) Data Entry (OU) Information Systems (OU) Research and Development (OU) Sales & Marketing 	Staff GPO Admin (OU)
Workstations (OU) <ul style="list-style-type: none"> Main Office (OU) Warehouse (OU) 	Workstation GPO

3.5.2 Domain Name Service [2]

Closely related to the sharing of resources across the two forests, how does AD know which IP address to go to when a user located in GIAC types [\\servername](#) in the “Start – Run” command box to access the file shares available on servername which exists in SANS forest.

Domain Name Resolution across different forests is the most important and fundamental capability to provide in order to allow cross forest collaboration. Without this capability, every user, application and server will have to know the IP address of the target machine to be accessed.

The SANS root DNS server (DNS server responsible for the “.” zone) has been identified to be the root DNS for the combined forests. New delegations are created within this root zone for each of the DNS namespaces for SANS and GIAC. Also the root hints of all the DNS servers in the forest are added with the new root DNS server. This is the method documented at Microsoft.

3.5.3 Sharing of Resources [1]

To allow for cross-forest sharing of resources, the following grouping scheme is used.

- Create global groups in a domain that contains the set of users who need to access a particular type of resource. For example, in the hq.sans.biz domain, a global group named “file server user group” may be created and all the users that need cross domain/forest access to file servers are placed in this global group.
- Corresponding universal groups (since both forests’ domains are all in native mode) are then created and the global group is assigned as members. For our example, a “uni file server user group” is created and the “file server user group” is added as a member to this universal group.
- At the resource end, we create resource domain local groups for each of the resources that will be accessed from outside the forest. For example, a “local file server user group” can be created in giac.biz. The universal groups are then added to these resource domain local groups which are in turn added to the ACL of the resource. So for giac.biz, the File and Print OU may have the “local file server user group” added to its ACL.

This scheme, recommended in Microsoft white paper “Multiple Forest Considerations” allows users to access resources across forests in the most efficient manner.

When new user accounts need to access a resource in another forest, the user account is simply added to the relevant global group. When a new resource is available for sharing, then the relevant resource domain local group can be added to its ACL.

3.5.4 Address List Synchronization [1]

GIAC and SANS HQ use Exchange 2000 mail servers. However, GIAC users cannot see fellow SANS users in their address list and so similarly SANS users cannot see GIAC users on theirs. The address lists must be synchronized. Synchronization can be achieved using a directory synchronization product such as Metadirectory Services.

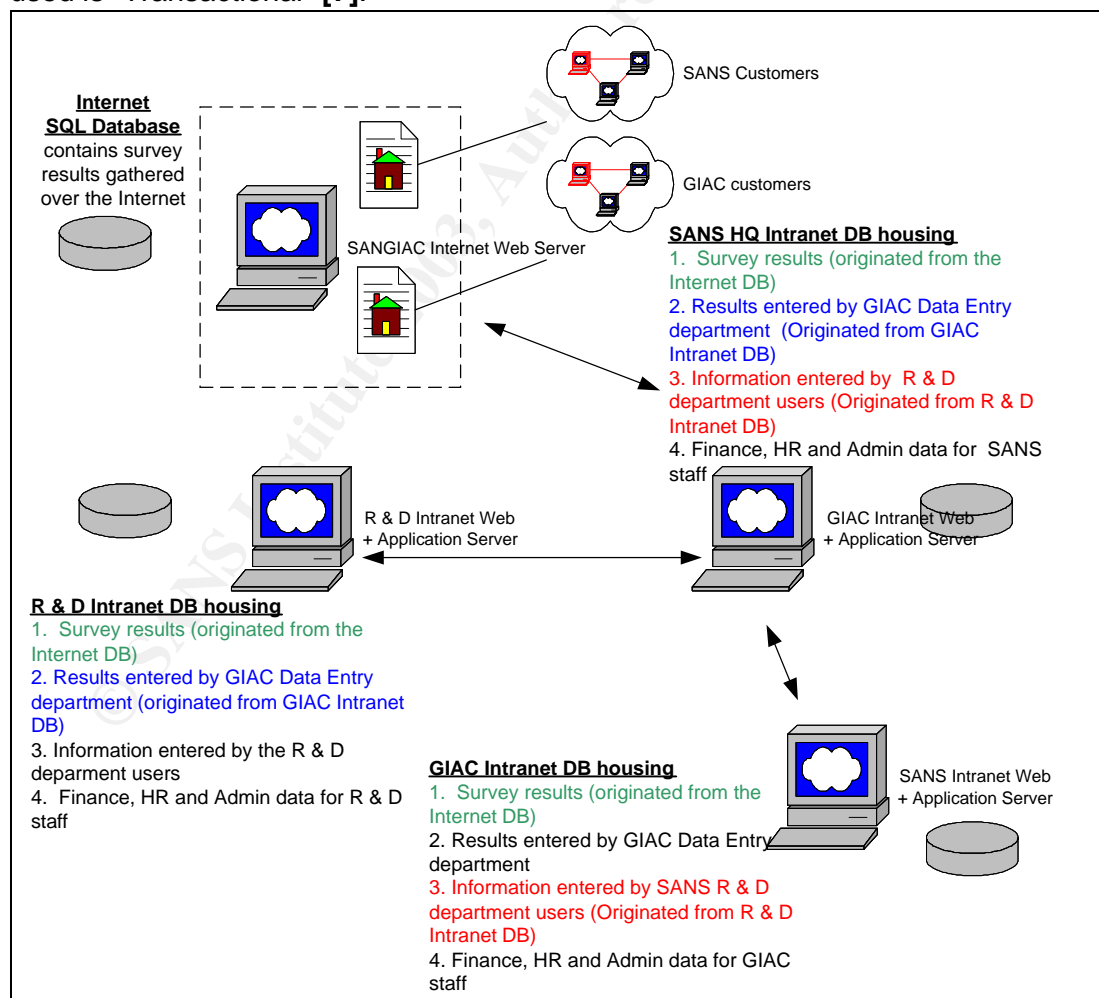
For every user in GIAC, a ‘shadow’ user account (contact object) is created in SANS and vice versa. One-way synchronization using Metadirectory Services can be scheduled on a periodic basis to dynamically update all ‘shadow’ user

accounts with deletions, additions, modifications transactions from the source forest. Hence all changes to the mail-enabled objects must be initiated from the source forest and never from the target.

For SANGIAC, a central Metadirectory Services hosted at SANS is used to synchronize the directory information between the two forests. The Metadirectory Services server is a fully hardened server due to the potentially devastating impact if this server is compromised.

3.5.5 Synchronizing Application Data

SANS R & D executive needs to access GIAC's R & D department analysis application data and vice versa. As we do not want to have users in one forest going all the way to the other forest to access the data, it is important that a duplicate copy of the data be hosted in another database server there. However, this is only restricted to the Intranet database server where the full set of application data is residing. This application data can be replicated across the two forests to ensure that they are the same on a periodic basis. Since data updates can be carried out from both forests, the replication type used is "Transactional" [7].



4.0 Group Policy Design

All guest accounts are disabled on all servers in SANGIAC. A random password is entered for the guest account and the account is disabled and expired. This will ensure that no hackers will be able to exploit this well-known loophole in Windows security.

4.1 Computer Configurations [8], [10]

4.1.1 Password, Account Lockout and Kerberos Policies

Password, account lockout and kerberos policies affect all computers and user accounts in the domain.

The following group policy settings are applied across for the SAN HQ and GIAC domain:

Policy	Value	Explanation
Password Policy (Windows Settings / Security Settings / Account Policies / Password Policies)		
Enforce Password History	24 passwords	Prevents users from using any of their previous 24 passwords
Maximum Password Age	90 days	Users must change their passwords every 90 days
Minimum Password Age	1 day	Prevents users from changing their password 10 times in a row with a day in order to use back an old password. With this setting, users need to change their passwords 10 days in a row before using an old password.
Minimum Password Length	8	Make sure that all passwords are at least 8 characters long
Password must meet complexity requirements	Enabled	To ensure that passwords are not easily guessed or cracked
Store Passwords using Reversible Encryption for all users in the Domain	Disabled	This is not necessary in the SANGIAC network
Account Lockout Policies (Windows Settings / Security Settings / Account Policies / Account Lockout Policies)		
Account Lockout Threshold	5	Lockout accounts when there are five consecutive login failures
Account Lockout Duration	30 minutes	Accounts are unlocked after 30 minutes.
Reset account lockout	30 minutes	Account lockouts are

counter after		remembered up to 30 minutes.
Kerberos Policies (Windows Settings \ Security Settings \ Account Policies \ Kerberos Policy)		
Enforce user logon restrictions	Enabled	Ensures that every request from the user account is validated by checking the user rights policy.
Maximum Lifetime for Service Tickets	480 minutes	Service Tickets are cached for 480 minutes
Maximum Lifetime for User Tickets	8 hours	User tickets will be cached for 8 hours
Maximum Lifetime for user ticket renewal	7 days	We can use the default here as we felt that this setting is reasonable.
Maximum Tolerance for Computer Clock Synchronization	5 minutes	Left as default. Anything less than this may generate much problems.

The R & D and the DMZ domains have the following password, account lockout and Kerberos policies:

Policy	Value	Explanation
Password Policy (Windows Settings / Security Settings / Account Policies / Password Policies)		
Enforce Password History	24 passwords	Prevents users from using any of their previous 24 passwords
Maximum Password Age	30 days	Users must change their passwords every 90 days
Minimum Password Age	2 day	Prevents users from changing their password 24 times in a row within a day in order to use back an old password. With this setting, users need to change their passwords 48 days in a row before using an old password.
Minimum Password Length	14	Make sure that all passwords are at least 8 characters long
Password must meet complexity requirements	Enabled	To ensure that passwords are not easily guessed or cracked
Store Passwords using Reversible Encryption for all users in the Domain	Disabled	This is not necessary in the SANGIAC network
Account Lockout Policies (Windows Settings / Security Settings / Account Policies / Account Lockout Policies)		
Account Lockout	3	Lockout accounts when

Threshold		there are five consecutive login failures
Account Lockout Duration	2 hours	Accounts are unlocked after 30 minutes.
Reset account lockout counter after	2 hours	Account lockouts are remembered up to 6 hours. This can effectively deter even the most patient of hackers.
Kerberos Policies (Windows Settings \ Security Settings \ Account Policies \ Kerberos Policy)		
Enforce user logon restrictions	Enabled	Ensures that every request from the user account is validated by checking the user rights policy.
Maximum Lifetime for Service Tickets	300 minutes	Service Tickets are cached for 480 minutes
Maximum Lifetime for User Tickets	5 hours	User tickets will be cached for 8 hours
Maximum Lifetime for user ticket renewal	3 days	We can use the default here as we felt that this setting is reasonable.
Maximum Tolerance for Computer Clock Synchronization	5 minutes	Left as default. Anything less than this may generate much problems.

Also the R & D Department is totally autonomous and has removed the Enterprise Admins group from the Local Administrators group of every DC in their domain.

4.1.2 Audit Policies

The following audit policies here are implemented for all default domain and domain controller policy GPOs in all domains. This is not defined in other GPOs.

Policy	Value	Explanation
Audit Policy (Windows Settings \ Security Settings \ Local Policies \ Audit Policy)		
Audit Account Logon Events	Success, Failure	
Audit Account Management	Success, Failure	
Audit Directory Service access	Success, Failure	
Audit Logon Events	Success, Failure	
Audit Object Access	Success, Failure	
Audit Policy Change	Success, Failure	

Audit Privilege Use	Failure
Audit Process Tracking	Not Defined
Audit System Events	Success, Failure

4.1.3 Event Log Settings

At SANS HQ, all logs are fully backed up on a weekly basis. We initially increased the size of the security logs to the maximum of 4 GB but eventually scaled down the size settings to 500 MB as we average about 50 MB of security logs per week normally. Not obvious from the settings here is that SANS HQ implements a central logging system (near real time dispatch of log information) to remotely capture the logs for all domain servers on a log server.

This policy is applied to the Default Domain Controllers Policy and Servers GPO for all SANGIAC domains.

Policy	Value	Explanation
Event Log Settings (Windows Settings \ Security Settings \ Event Log \ Settings for Event Log)		
Maximum application log size	75 MB	
Maximum security log size	500 MB	
Maximum system log size	75 MB	
Restrict guest access to application log	Enabled	
Restrict guest access to security log	Enabled	
Restrict guest access to system log	Enabled	
Retention method for application log	Overwrite events by days	
Retention method for security log	Overwrite events by days	
Retention method for system log	Overwrite events by days	
Retain application logs	3 days	
Retain security logs	3 days	
Retain system logs	3 days	
Shut down the computer when the security audit log is full	Disabled	

For the DMZ Servers GPO, the following settings are used.

Policy	Value	Explanation
Maximum application log size	4 GB	
Maximum security log size	4 GB	
Maximum system log size	4 GB	
Restrict guest access to application log	Enabled	
Restrict guest access to security log	Enabled	
Restrict guest access to system log	Enabled	
Retention method for application log	Overwrite events by days	
Retention method for security log	Overwrite events by days	
Retention method for system log	Overwrite events by days	
Retain application logs	14 days	
Retain security logs	14 days	
Retain system logs	14 days	
Shut down the computer when the security audit log is full	Disabled	

Event Log Settings are left “Not Defined” in the Default Domain GPO.

4.1.4 User Rights Assignment

Policy	Servers GPO + DMZ Servers GPO	Default Domain Policy	Domain Controller Policy
Access this computer from the network	Administrators Backup Operators Authen. Users	Not Defined	Administrators Authenticated Users
Act as part of the operating system	None	Not Defined	None
Add workstations to domain	Administrators	Not Defined	Domain Admins
Back up files and directories	Administrators Backup Operators	Not Defined	Administrators Backup Operators
Bypass traverse checking	Administrators	Not Defined	Administrators
Change the system time	Administrators Power Users	Not Defined	Administrators Server

Policy	Servers GPO + DMZ Servers GPO	Default Domain Policy	Domain Controller Policy
			Operators
Create a pagefile	Administrators	Administrators	Administrators
Create a token object	None	Not Defined	None
Create a permanent shared objects	None	Not Defined	None
Debug programs	Administrators	Not Defined	Administrators
Deny access to this computer from the network	None	Not Defined	None
Deny logon as a batch job	None	Not Defined	None
Deny logon as a service	None	Not Defined	None
Deny logon locally	None	Not Defined	None
Enable computer and user accounts to be trusted for delegation	None	Not Defined	Administrators
Force shutdown from a remote system	Administrators	Administrators	Administrators
Generate security audits	None	Not Defined	None
Increase quotas	Administrators	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators	Administrators
Lock pages in memory	None	Not Defined	None
Log on as a batch job	None	Not Defined	None
Log on as a service	None	Not Defined	None
Log on locally	Administrators	Not Defined	Administrators
Manage auditing and security log	Administrators	Administrators	Administrators
Modify firmware environment values	Administrators	Administrators	Administrators
Profile single process	Administrators	Not Defined	Administrators
Profile system performance	Administrators	Administrators	Administrators
Remove computer from docking station	None	Not Defined	None
Replace a process level token	None	Not Defined	None
Restore files and directories	Administrators	Not Defined	Administrators
Shut down the system	Administrators	Not Defined	Administrators
Synchronise directory service data	None	Not Defined	Administrators
Take ownership of files or other objects	Administrators	Administrators	Administrators

4.1.5 Security Options

Policy	Setting	Server GPO + DMZ	Default Domain Policy	Default Domain Controller Policy
Additional restrictions for anonymous connections	No access without explicit anonymous permissions.	•	•	•
Allow server operations to schedule tasks (domain controllers only)	Disabled			•
Allow system to shut down without having to log on	Disabled	•	•	•
Allowed to eject removable NTFS media	Administrators	•	•	•
Amount of idle time required before disconnecting session	-	15 minutes	15 minutes	15 minutes
Audit the access of global system objects	Enabled	•	•	•
Audit the use of Backup and Restore privilege	Enabled	•	•	•
Automatically log off users when logon time expires (both)	Enabled	•	•	•
Clear virtual memory pagefile when system shuts down	Enabled	•	•	•
Digitally sign client communication (always)	Disabled	•	•	•
Digitally sign client communication (when possible)	Enabled	•	•	•
Digitally sign server communication (always)	Disabled	•	•	•
Digitally sign server communication (when possible)	Enabled	•	•	•
Disable CTRL+ALT+DEL requirement for logon	Disabled	•	•	•
Do not display last user name in logon screen	Enabled	•	Not Defined	•
LAN Manager Authentication Level	Send NTLMv2 responses only and refuse LM and NTLM protocols	•	•	•
Message text for users attempting to log on	"To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this	•	•	•

Policy	Setting	Server GPO + DMZ	Default Domain Policy	Default Domain Controller Policy
	system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties."			
Message title for users attempting to log on	"Authorized users only".	•	•	•
Number of previous logons to cache (in case of domain controller is not available)	-	3 (0 for DMZ)	3	0
Prevent system maintenance of computer account password	Disabled	•	•	•
Prevent users from installing printer drivers	-	Not Defined	Enabled	Enabled
Prompt user to change password before expiration	10 days	•	•	Not Applicable
Recovery Console: Allow automatic administrative logon	Disabled	•	•	•
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	•	•	•
Rename Administrator account	Enabled	•	Not Defined	•
Rename guest account	ANIMAL	•	•	•
Restrict CD-ROM access to locally logged-on user only	Enabled	•	•	•
Restrict floppy access to locally logged-on user only	Enabled	•	•	•
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	•	•	•
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	•	•	•
Secure channel: Digitally sign secure channel data (when	Enabled	•	•	•

Policy	Setting	Server GPO + DMZ	Default Domain Policy	Default Domain Controller Policy
possible)				
Secure channel: Require session key	Disabled	•	•	•
Send unencrypted password to connect to third-party SMB servers	Disabled	•	•	•
Shut down system immediately if unable to log security audits	Disabled	•	•	•
Smart card removal behaviour	Lock Workstation	•	•	•
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	•	•	•
Unsigned driver installation behaviour	Do not allow installation	•	•	•
Unsigned non-driver installation behaviour	Warn but allow installation	• (Do not allow for DMZ)	•	•

4.1.6 Restricted Groups

The following groups are added to the Restricted Groups:

Enterprise Admins
Domain Admins
Schema Admins
DnsAdmins
Administrators
Account Operators
Backup Operators
Server Operators

4.1.7 System Services

Service Name	Default Domain Policy	Default Domain Controller Policy	DMZ Servers GPO
Alerter	Disabled	Disabled	Disabled
Application Management	Manual	Manual	Disabled
ClipBook	Disabled	Disabled	Disabled
COM+ Event System	Manual	Manual	Disabled
Computer Browser	Automatic	Automatic	Disabled
DHCP Client	Automatic	Automatic	Disabled
Distributed File System	Disabled	Automatic	Disabled
Distributed Link	Disabled	Disabled	Disabled









Service Name	Default Domain Policy	Default Domain Controller Policy	DMZ Servers GPO
Transaction Client			
Distributed Link Tracking Server	Disabled	Manual	Disabled
Distributed Transaction Coordinator	Manual	Manual	Disabled
DNS Client	Automatic	Automatic	Automatic
Event Log	Automatic	Automatic	Automatic
Fax Service	Disabled	Disabled	Disabled
File Replication	Manual	Automatic	Disabled
IIS Admin Service	Disabled	Disabled	Automatic
Indexing Service	Disabled	Disabled	Disabled
Internet Connection Sharing	Disabled	Disabled	Disabled
Intersite Messaging	Disabled	Disabled	Disabled
IPSEC Policy Agent	Manual	Manual	Disabled
Kerberos Key Distribution Center	Disabled	Automatic	Disabled
License Logging Service	Automatic	Automatic	Automatic
Logical Disk Manager	Automatic	Automatic	Manual
Logical Disk Manager Administrative Service	Manual	Automatic	Manual
Messenger	Disabled	Disabled	Disabled
Net Logon	Automatic	Automatic	Disabled
Netmeeting Remote Desktop Sharing	Disabled	Disabled	Disabled
Network Connections	Automatic	Automatic	Automatic
Network DDE	Disabled	Disabled	Disabled
Network DDE DSDM	Disabled	Disabled	Disabled
NT LM Security Support Provider	Manual	Manual	Disabled
Performance Logs and Alerts	Manual	Manual	Disabled
Plug and Play	Automatic	Automatic	Automatic
Print Spooler	Disabled	Automatic	Disabled
Protected Storage	Automatic	Automatic	Automatic
QoS RSVP	Disabled	Disabled	Disabled
Remote Access Auto Connection Manager	Disabled	Manual	Disabled
Remote Access Connection Manager	Disabled	Manual	Disabled
Remote Procedure Call (RPC)	Automatic	Automatic	Automatic
Remote Procedure Call (RPC) Locator	Manual	Automatic	Disabled
Remote Registry Service	Disabled	Automatic	Disabled
Removable Storage	Disabled	Disabled	Disabled
Routing and Remote	Disabled	Disabled	Disabled

Service Name	Default Domain Policy	Default Domain Controller Policy	DMZ Servers GPO
Access			
RunAs Service	Disabled	Disabled	Disabled
Security Accounts Manager	Automatic	Automatic	Automatic
Server	Automatic	Automatic	Automatic
Simple Mail Transport Protocol (SMTP)	Disabled	Disabled	Not Install
Smart Card	Disabled	Disabled	Disabled
Smart Card Helper	Disabled	Disabled	Disabled
System Event Notification	Automatic	Automatic	Disabled
Task Scheduler	Disabled	Disabled	Disabled
TCP/IP NetBIOS Helper Service	A	A	Automatic
Telephony	Disabled	Disabled	Disabled
Telnet	Disabled	Manual	Disabled
Terminal Services	Disabled	Disabled	Disabled
Uninterruptible Power Supply	Automatic	Automatic	Disabled
Utility Manager	Disabled	Disabled	Disabled
Windows Installer	Manual	Manual	Manual
Windows Management Instrumentation	Manual	Automatic	Automatic
Windows Management Instrumentation Driver Extensions	Manual	Manual	Manual
Windows Time	Automatic	Automatic	Disabled
Workstation	Automatic	Automatic	Automatic

4.1.8 Administrative Templates

The following is configured in Workstation GPO in SANS HQ and R & D domains. In GIAC domain, it is set at the Workstation OU level.

Administrative Templates\Windows Components\Netmeeting\Disable remote Desktop Sharing = Enabled

 Security Zones: Use only machine settings	Enabled
 Security Zones: Do not allow users to change policies	Enabled
 Security Zones: Do not allow users to add/delete sites	Enabled
 Make proxy settings per-machine (rather than per-user)	Enabled
 Disable Automatic Install of Internet Explorer components	Not configured
 Disable Periodic Check for Internet Explorer software updates	Enabled
 Disable software update shell notifications on program launch	Not configured
 Disable showing the splash screen	Enabled

All items under Administrative Templates\Windows Components\Task Scheduler\ are “Enabled”

All other items under Administrative Templates are left as “Not configured”

4.2 User Configuration

These user configuration settings are application to all the Staff GPOs in SANS HQ, R&D and GIAC domains. These restrictions do not apply to the Admin GPO.

All user configuration settings under Administrative Template\Windows Components\Netmeeting are left as “Not configured”

Administrative Template\Windows Components\Internet Explorer\

Search: Disable Search Customization	Not configured
Search: Disable Find Files via F3 within the browser	Not configured
Disable external branding of Internet Explorer	Enabled
Disable importing and exporting of favorites	Not configured
Disable changing Advanced page settings	Enabled
Disable changing home page settings	Not configured
Use Automatic Detection for dial-up connections	Not configured
Disable caching of Auto-Proxy scripts	Not configured
Display error message on proxy script download failure	Not configured
Disable changing Temporary Internet files settings	Enabled
Disable changing history settings	Not configured
Disable changing color settings	Not configured
Disable changing link color settings	Not configured
Disable changing font settings	Not configured
Disable changing language settings	Not configured
Disable changing accessibility settings	Not configured
Disable Internet Connection wizard	Not configured
Disable changing connection settings	Enabled
Disable changing proxy settings	Enabled
Disable changing Automatic Configuration settings	Enabled
Disable changing ratings settings	Not configured
Disable changing certificate settings	Not configured
Disable changing Profile Assistant settings	Not configured
Disable AutoComplete for forms	Enabled
Do not allow AutoComplete to save passwords	Enabled
Disable changing Messaging settings	Not configured
Disable changing Calendar and Contact settings	Not configured
Disable the Reset Web Settings feature	Not configured
Disable changing default browser check	Enabled
Identity Manager: Prevent users from using Identities	Not configured

Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

 Disable the General page	Not configured
 Disable the Security page	Enabled
 Disable the Content page	Not configured
 Disable the Connections page	Enabled
 Disable the Programs page	Not configured
 Disable the Advanced page	Enabled




Settings on Administrative Templates\Windows Components\Internet Explorer\Offline Pages are left as “Not configured”

The setting “Administrative Templates\Windows Components\Internet Explorer\Browser Menus\Disable Save this program to disk option” is set to “Enabled”

All other settings under Internet Explorer is left as “Not configured”

All settings on Administrative Templates\Windows Components\Windows Explorer are left as “Not configured”

Administrative Templates\Windows Components\Microsoft Management Console:

 Restricted/Permitted snap-ins	
 Restrict the user from entering author mode	Not configured
 Restrict users to the explicitly permitted list of snap-ins	Enabled

Administrative Templates \ Windows Components \ Microsoft Management Console \ Restricted/Permitted snap-ins:





All MMC are set to “Not configured” under

“Administrative Templates\Windows Components\Microsoft Management Console\Group Policy” and

“Administrative Templates \ Windows Components \ Microsoft Management Console\Extension snap-ins”

























 Active Directory Users and Computers	Not configured
 Active Directory Domains and Trusts	Not configured
 Active Directory Sites and Services	Not configured
 Certificates	Not configured
 Component Services	Not configured
 Computer Management	Enabled
 Device Manager	Enabled
 Disk Management	Enabled
 Disk Defragmenter	Enabled
 Distributed File System	Enabled
 Event Viewer	Enabled
 FAX Service	Enabled
 Indexing Service	Not configured
 Internet Authentication Service (IAS)	Not configured
 Internet Information Services	Not configured
 IP Security	Enabled
 Local Users and Groups	Enabled
 Performance Logs and Alerts	Enabled
 QoS Admission Control	Enabled
 Removable Storage Management	Enabled
 Routing and Remote Access	Not configured
 Security Configuration and Analysis	Not configured
 Security Templates	Not configured
 Services	Enabled
 Shared Folders	Enabled
 System Information	Enabled
 Telephony	Enabled
 Terminal Services Configuration	Not configured
 WMI Control	Not configured

Administrative Templates\Windows Components\Windows Installer:













 Always install with elevated privileges	Disabled
 Search order	Enabled
 Disable rollback	Not configured
 Disable media source for any install	Enabled

Administrative Templates\Windows Components\Windows Update\Remove access to use all Windows Update features : Enabled











Administrative Templates\Start Menu & Taskbar:

 Remove user's folders from the Start Menu	Not configured
 Disable and remove links to Windows Update	Enabled
 Remove common program groups from Start Menu	Enabled
 Remove Documents menu from Start Menu	Not configured
 Disable programs on Settings menu	Not configured
 Remove Network & Dial-up Connections from Start Menu	Not configured
 Remove Favorites menu from Start Menu	Not configured
 Remove Search menu from Start Menu	Not configured
 Remove Help menu from Start Menu	Not configured
 Remove Run menu from Start Menu	Enabled
 Add Logoff to the Start Menu	Not configured
 Disable Logoff on the Start Menu	Not configured
 Disable and remove the Shut Down command	Not configured
 Disable drag-and-drop context menus on the Start Menu	Not configured
 Disable changes to Taskbar and Start Menu Settings	Not configured
 Disable context menus for the taskbar	Not configured
 Do not keep history of recently opened documents	Not configured
 Clear history of recently opened documents on exit	Not configured
 Disable personalized menus	Not configured
 Disable user tracking	Not configured
 Add "Run in Separate Memory Space" check box to Run dialog box	Not configured
 Do not use the search-based method when resolving shell shortcuts	Not configured
 Do not use the tracking-based method when resolving shell shortcuts	Not configured
 Gray unavailable Windows Installer programs Start Menu shortcuts	Not configured




















Administrative Templates\Desktop:

 Hide all icons on Desktop	Not configured
 Remove My Documents icon from desktop	Not configured
 Remove My Documents icon from Start Menu	Not configured
 Remove Properties from the My Documents context menu	Not configured
 Remove Properties from the My Computer context menu	Enabled
 Hide My Network Places icon on desktop	Enabled
 Hide Internet Explorer icon on desktop	Not configured
 Do not add shares of recently opened documents to My Network ...	Not configured
 Prohibit user from changing My Documents path	Enabled
 Disable adding, dragging, dropping and closing the Taskbar's tool...	Not configured
 Disable adjusting desktop toolbars	Not configured
 Don't save settings at exit	Enabled











Administrative Templates\Control Panel\Add/Remove Programs:

 Disable Add/Remove Programs	Enabled
 Hide Change or Remove Programs page	Enabled
 Hide Add New Programs page	Enabled
 Hide Add/Remove Windows Components page	Enabled
 Hide the "Add a program from CD-ROM or floppy disk" option	Enabled
 Hide the "Add programs from Microsoft" option	Enabled
 Hide the "Add programs from your network" option	Not configured
 Go directly to Components wizard	Not configured
 Disable Support Information	Not configured
 Specify default category for Add New Programs	Not configured

Administrative Templates\Control Panel\Display:











 Prohibit deletion of RAS connections	Not configured
 Prohibit deletion of RAS connections available to all users	Not configured
 Prohibit connecting and disconnecting a RAS connection	Not configured
 Prohibit enabling/disabling a LAN connection	Enabled
 Prohibit access to properties of a LAN connection	Enabled
 Prohibit access to current user's RAS connection properties	Enabled
 Prohibit access to properties of RAS connections available to all u...	Enabled
 Prohibit renaming LAN connections or RAS connections available t...	Not configured
 Prohibit renaming of RAS connections belonging to the current user	Not configured
 Prohibit adding and removing components for a LAN or RAS conne...	Not configured
 Prohibit enabling/disabling components of a LAN connection	Not configured
 Prohibit access to properties of components of a LAN connection	Not configured
 Prohibit access to properties of components of a RAS connection	Not configured
 Prohibit access to the Network Connection wizard	Enabled
 Prohibit viewing of status statistics for an active connection	Not configured
 Prohibit access to the Dial-up Preferences item on the Advanced ...	Enabled
 Prohibit access to the Advanced Settings item on the Advanced m...	Enabled
 Prohibit configuration of connection sharing	Enabled
 Prohibit TCP/IP advanced configuration	Enabled

Administrative Templates\Network\Network and Dial-up Connections:

 Disable Display in Control Panel	Enabled
 Hide Background tab	Not configured
 Disable changing wallpaper	Not configured
 Hide Appearance tab	Not configured
 Hide Settings tab	Enabled
 Hide Screen Saver tab	Enabled
 Activate screen saver	Enabled
 Screen saver executable name	Enabled
 Password protect the screen saver	Enabled
 Screen Saver timeout	Enabled

For the screen saver timeout, it is set to 600 seconds

Administrative Templates\System:

 Don't display welcome screen at logon	Not configured
 Century interpretation for Year 2000	Not configured
 Code signing for device drivers	Not configured
 Custom user interface	Not configured
 Disable the command prompt	Enabled
 Disable registry editing tools	Enabled
 Run only allowed Windows applications	Not configured
 Don't run specified Windows applications	Not configured
 Disable Autoplay	Not configured
 Download missing COM components	Not configured

Administrative Templates\System\Logon\Logoff\Disable Task Manager = Enabled.

4.3 DMZ Domain

There are no user accounts within the DMZ domain. Rather, users from the SANS HQ, R & D and GIAC domains access resources in the DMZ domain via one-way explicit trusts. This domain contains the corporate IIS Internet server (only one server currently) and so allows anonymous access for operational purposes.

Typically, the IIS web server is the doorway into the DMZ Domain (via port 80 and 443). Hence it must be fully hardened and patched up-to-date to deter external attacks.

4.3.1 TCP Hardening [13], [14]

The registry key below contains subkeys that control the behaviour of the TCP/IP stack.

Key Path:	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip
Key:	Parameters

Add the following values to increase system security.

- **SynAttackProtect** REG_DWORD: 2

Synattack protection involves reducing the amount of retransmissions for the SYN-ACKS, which will reduce the time for which resources have to remain allocated. The allocation of route cache entry resources is delayed until a connection is made. If synattackprotect = 2. Also note that the actions taken by the protection mechanism only occur if TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are exceeded.

- **TcpMaxHalfOpen** REG_DWORD

Controls the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate. If SynAttackProtect is set to 1, ensure that this value is lower than the AFD listen backlog on the port you want to protect.

Value = 100

- **TcpMaxHalfOpenRetried** REG_DWORD

Control the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN sent, before SYN-ATTACK attack protection begins to operate.

Value = 80

- **EnablePMTUDiscovery** REG_DWORD: 1

When this parameter is set to 1 (True), TCP attempts to discover the Maximum Transmission Unit (MTU) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and network congestion. Setting this parameter to 0 causes an MTU of 576 bytes to be used for all connections that are not to hosts on the local subnet.

- **NoNameReleaseOnDemand** REG_DWORD: 1

Parameter that determines whether the computer releases its NetBIOS name when it receives a name-release request from the network. It was added to allow the administrator to protect the machine against malicious name-release attacks.

- **KeepAliveTime** REG_DWORD: 300,000

Parameter controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote system is still reachable and functioning, it acknowledges the keep-alive transmission. Keep-alive packets are not sent by default. This feature may be enabled on a connection by an application.

- **PerformRouterDiscovery** REG_DWORD: 0

Parameter controls whether Windows 2000 attempts to perform router discovery per RFC 1256 on a per-interface basis.

- **EnableICMPRedirect** REG_DWORD: 0

Parameter to control whether Windows 2000 will alter its route table in response to ICMP redirect messages that are sent to it by network devices such as routers.

4.3.2 Remove all Sample and Help files

All sample and help files are deleted. Sample and help files are extremely prone to be exploited by hackers if left lying around on the server.

4.3.4 Other Hardening Steps

- Disable Posix and Os2 subsystems
- Disable 8Dot3 Name Creation
- Disable WebDAV
- Disable Indexing Service for each of the system drive.

5.0 Group Policy Application and Maintenance

For this part of the assignment, I have managed to source for one machine with Windows 2000 Active Directory and IIS installed. I will use this setup to explain how the group policy I have created would be applied to existing systems and maintained/refreshed over time.

5.1 Application of Group Policy to SANGIAC's system

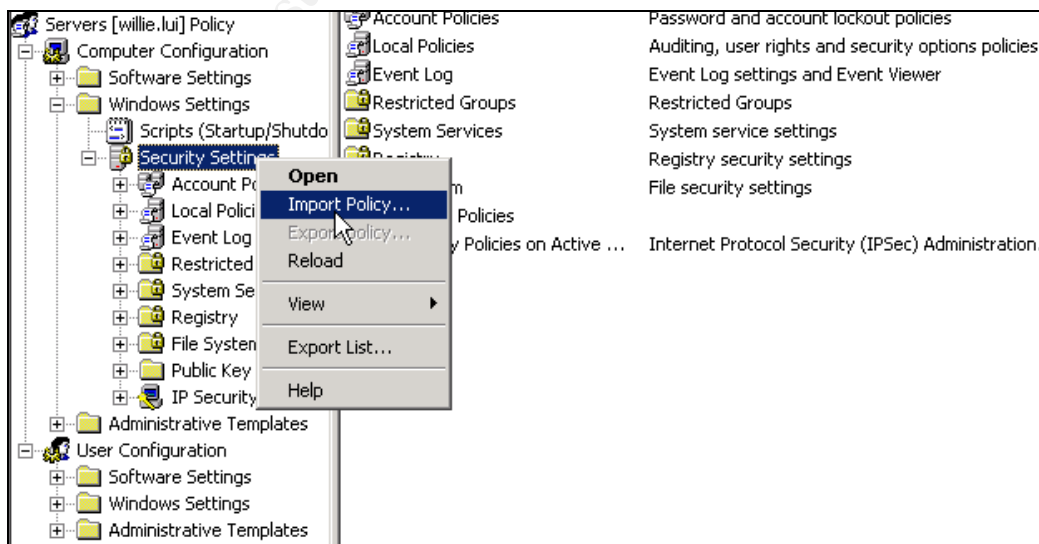
Group policies are domain specific. With five domains (root, R&D, SANS HQ, DMZ and GIAC) the group policies would normally have to be implemented five different times.

We use security templates to minimize the amount of configuration work needed. However, security templates only cover the following areas:

- password policies
- account lockout policies
- Kerberos policies
- Audit policies
- User rights assignment
- Security options
- Event log settings
- Restricted groups
- System services
- Registry Key Permissions
- File system permissions

User security settings are not included.

To apply the security template to a group policy object, we “edit” the group policy object and right-click the “Computer configurations\Windows Settings\Security Settings” and select “Import Policy...”



By making use of the security template mechanism to manage the group policy objects used in SANS, it is possible to systematically refresh and maintain the security settings over time efficiently and effectively.

The distinct security settings across the SANS forest are

- a. Default domain, servers and domain controllers for **SANS HQ**,
- b. Default domain, servers and domain controllers for **R & D**,
- c. DMZ Servers and domain controllers for **DMZ** and
- d. Domain controllers for **Root**.
- e. Domain controllers, servers, default domain policies for **GIAC**

Effectively, we need to maintain 9 different security template files (.inf) on each of the domain controllers where we are managing the forest-wide Active Directory. By importing the relevant security templates to the relevant group policy object from one server, we can efficiently manage the security settings of all servers in the forest.

For the user configuration settings, the same tasks to configure the workstations in each domain must be repeated for the R & D, SANS HQ and GIAC domains. There are no users or workstations in the DMZ and Root domains.

One interesting way to efficiently update the user configuration is to find out exactly which registry keys are added, modified or deleted by the user configuration portion of the GPO and the corresponding registry values that are set. This can be simply found by using third party tools such as RegSafe from ImagineLAN or the free RegDiff.

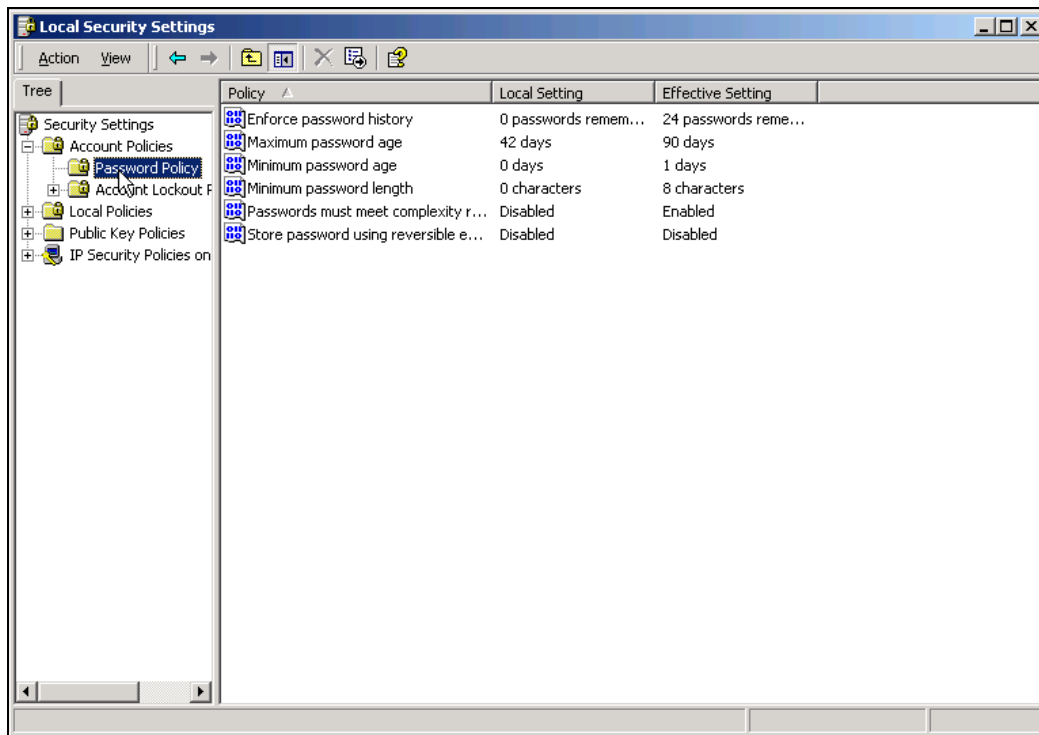
Using this knowledge, configure a login script to set the registry settings for the users and assign the script accordingly in the group policy.

5.2 Testing the Policies' Security Settings

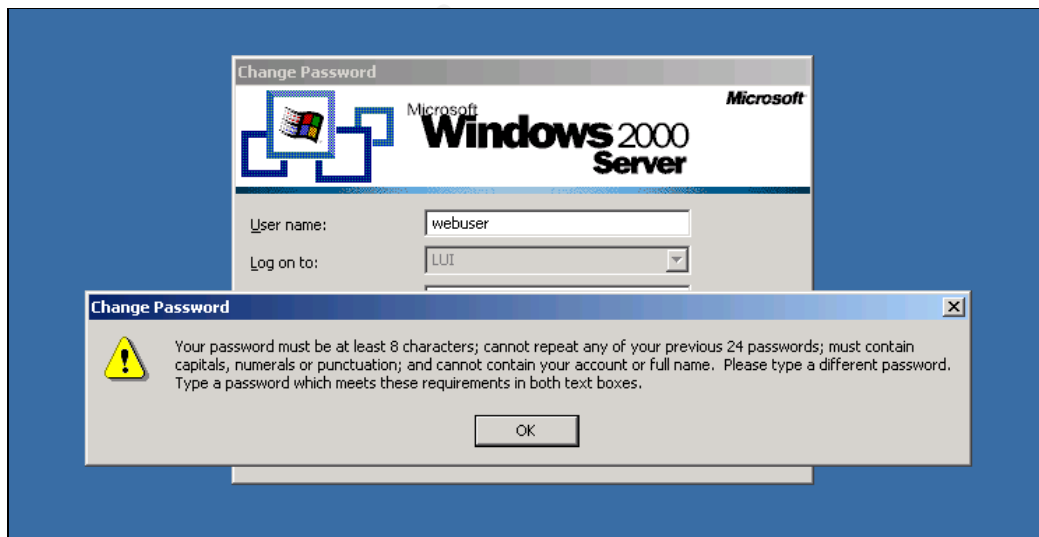
To verify that the policies' security settings are working correctly, we selected three items to be tested as below:

- a. Password must meet complexity requirements
 - b. Account Lockout threshold
 - c. Do not display last user name in logon screen
- A. Password must meet complexity requirements

We test this policy by first checking if the effective setting for the Local Security Policy at the IIS Server is the same as the domain password policies.

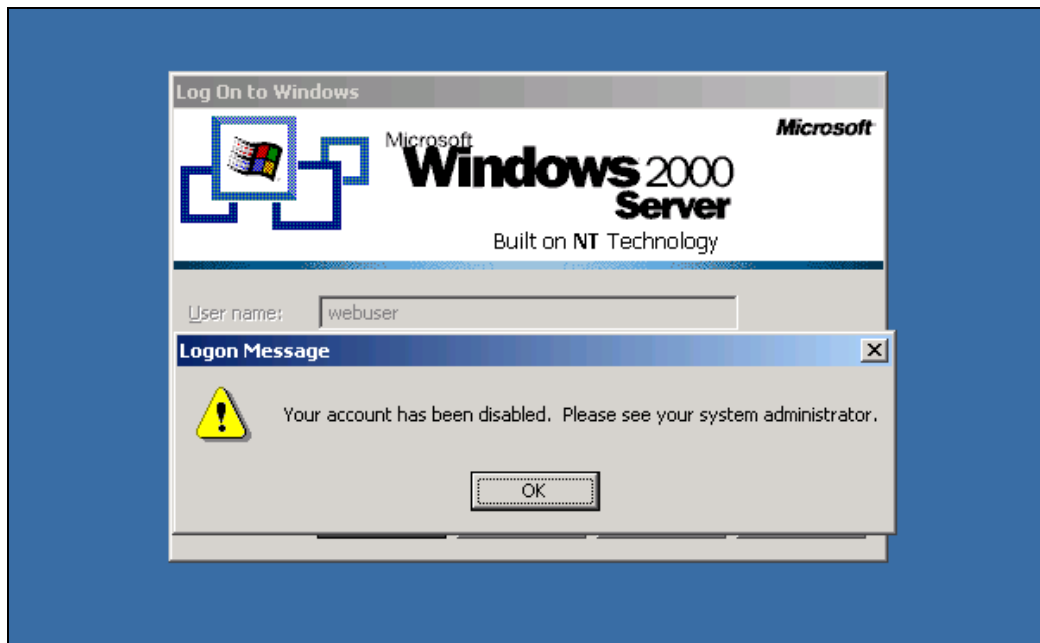


Next we test out the feature by enforcing a user to change password at the next logon. The simple password we entered for the new password was truly rejected.



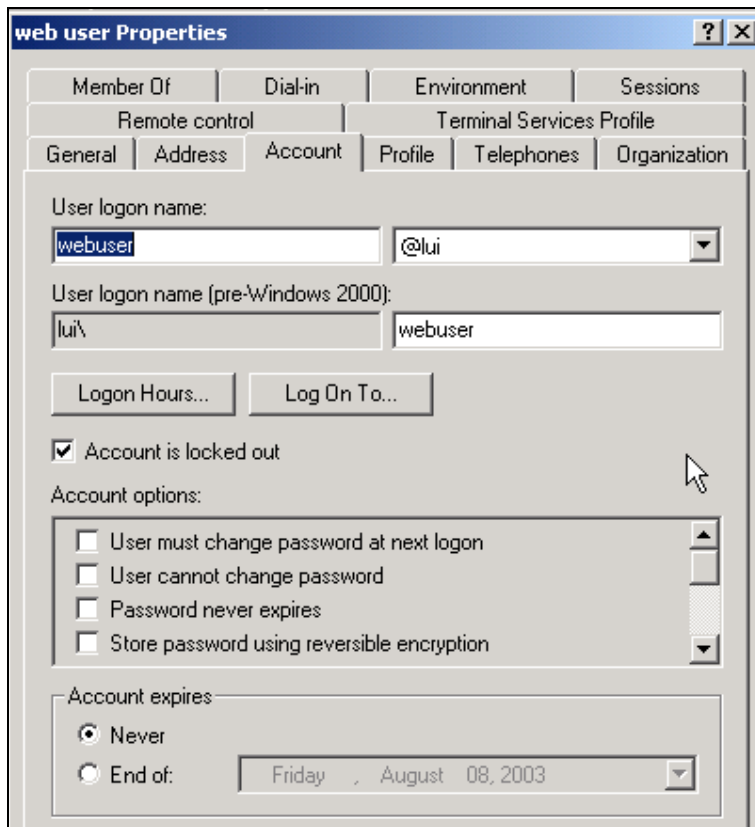
B. Account Lockout Threshold

We intentionally entered the wrong passwords for five consecutive times.



© SANS Institute 2003, Author retains full rights.

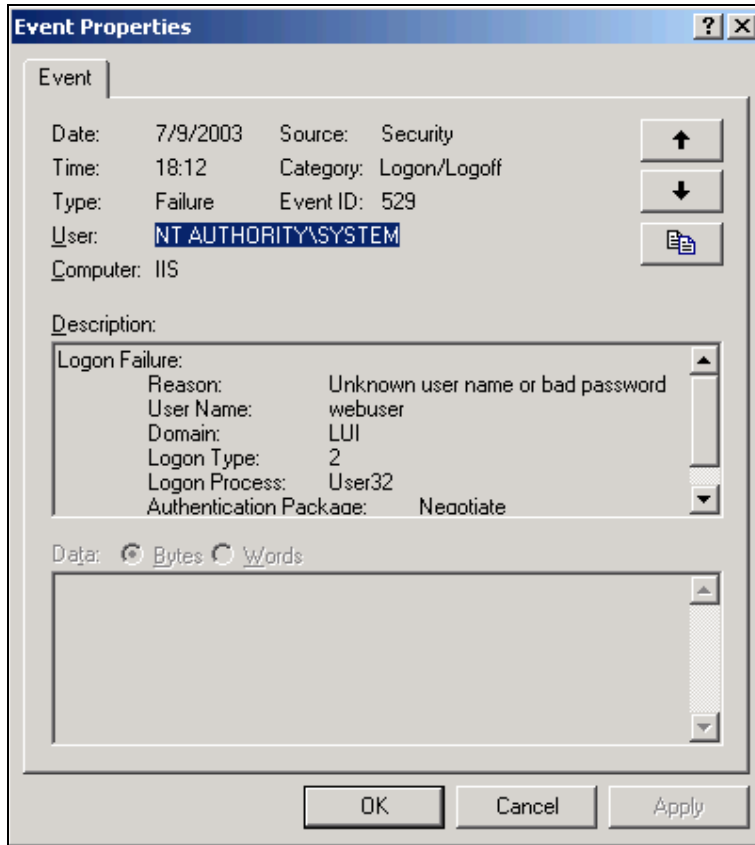
At the domain controller, we found that the user account is indeed locked out.



Finally, the security event log records also checks that the audit log settings are in effect.

Type	Date	Time	Source	Category	Event	User	Cor
Success Audit	7/9/2003	6:01:38 PM	Security	Logon/Lo...	538	SYSTEM	WII
Failure Audit	7/9/2003	6:01:32 PM	Security	Account ...	676	SYSTEM	WII
Success Audit	7/9/2003	6:01:30 PM	Security	Account ...	642	Everyone	WII
Success Audit	7/9/2003	6:01:30 PM	Security	Account ...	644	Everyone	WII
Failure Audit	7/9/2003	6:01:30 PM	Security	Account ...	675	SYSTEM	WII
Failure Audit	7/9/2003	6:01:29 PM	Security	Account ...	675	SYSTEM	WII
Failure Audit	7/9/2003	6:01:28 PM	Security	Account ...	675	SYSTEM	WII
Failure Audit	7/9/2003	6:01:27 PM	Security	Account ...	675	SYSTEM	WII
Failure Audit	7/9/2003	6:01:26 PM	Security	Account ...	675	SYSTEM	WII
Success Audit	7/9/2003	6:01:11 PM	Security	Logon/Lo...	540	Administrator	WII
Success Audit	7/9/2003	6:01:11 PM	Security	Account ...	673	SYSTEM	WII

This is the record shown on the IIS server for the failed logon event.

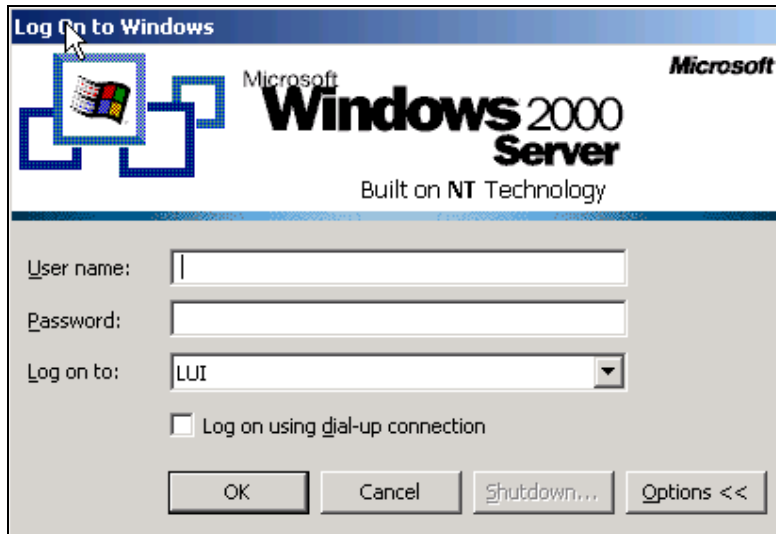


© SANS Institute 2003, All rights reserved.

C. Do not display last user name in logon screen

It is easy to test for this by just executing a “secdit /refreshpolicy machine_policy” at the IIS Server. When a new application log event for the “SceCli” Source appears, we check the local security policy and find that the Effective Setting for “Do not display last user name in logon screen” is indeed set to “Enabled”.

A test by just logging out from the IIS Intranet Server shows that the user name field is blank.



5.3 Test the System's Functionality

The server in question is an IIS server. Hence the two most commonly used functions of the server will be:

- a. Uploading of web pages via ftp to the webserver by the webmasters group
- b. Browsing of web pages by the Intranet users

A. Uploading of web pages to IIS Server via FTP

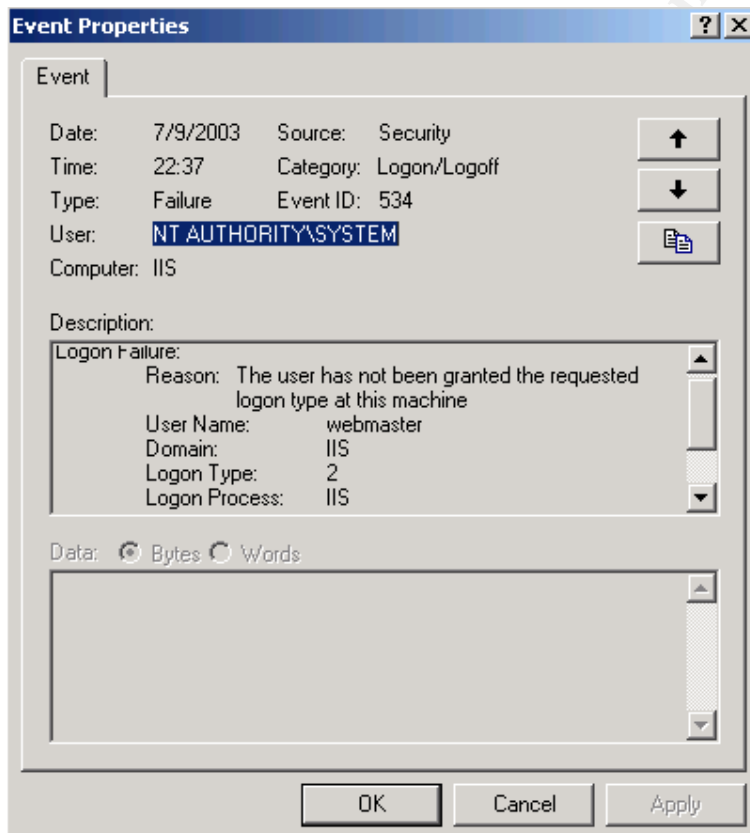
We encounter the following problem when the webmaster account attempts to ftp to the server.



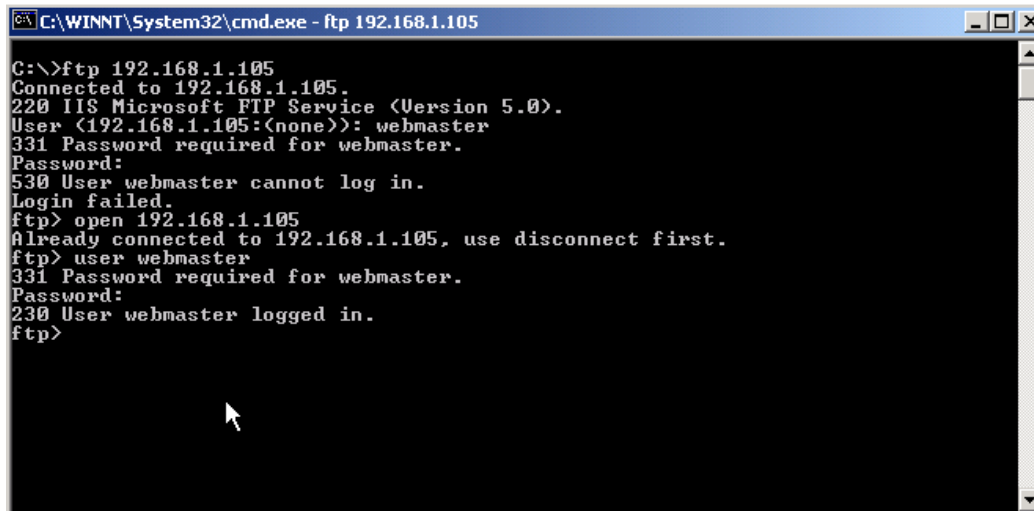
```
C:\WINNT\System32\cmd.exe - ftp 192.168.1.105
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ftp 192.168.1.105
Connected to 192.168.1.105.
220 IIS Microsoft FTP Service (Version 5.0).
User (192.168.1.105:(none)): webmaster
331 Password required for webmaster.
Password:
530 User webmaster cannot log in.
Login failed.
ftp> _
```

We look up the Security Log to see what is the problem.



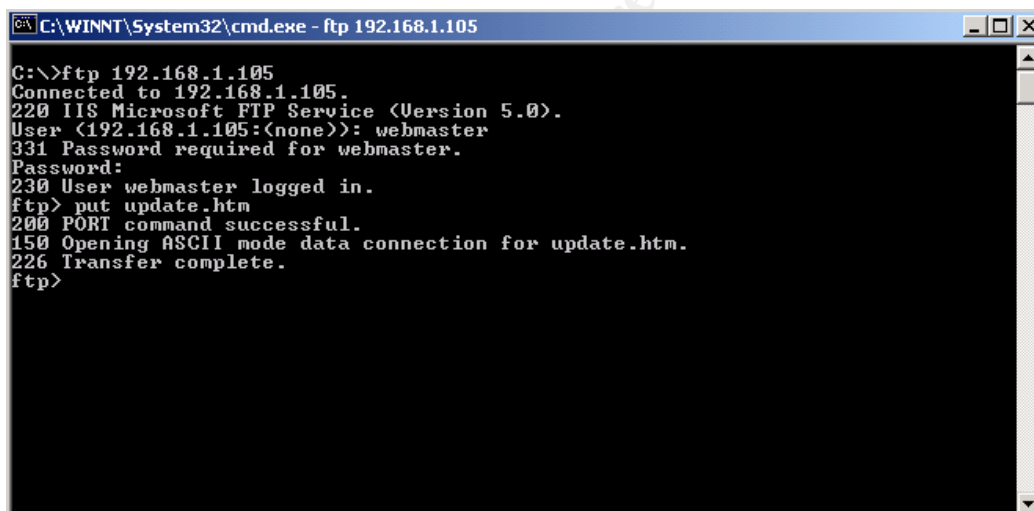
Logon Type 2 is found to be "Interactive Logon". We then assign the Local Group Webmaster with the user right to "Logon On Locally" and tried again. Success!



```
C:\WINNT\System32\cmd.exe - ftp 192.168.1.105

C:\>ftp 192.168.1.105
Connected to 192.168.1.105.
220 IIS Microsoft FTP Service (Version 5.0).
User (192.168.1.105:(none)): webmaster
331 Password required for webmaster.
Password:
530 User webmaster cannot log in.
Login failed.
ftp> open 192.168.1.105
Already connected to 192.168.1.105, use disconnect first.
ftp> user webmaster
331 Password required for webmaster.
Password:
230 User webmaster logged in.
ftp>
```

Next we need to attempt to upload files to the designated wwwroot folder. The wwwroot has been shared out and the ftproot is configured to point to this share.



```
C:\WINNT\System32\cmd.exe - ftp 192.168.1.105

C:\>ftp 192.168.1.105
Connected to 192.168.1.105.
220 IIS Microsoft FTP Service (Version 5.0).
User (192.168.1.105:(none)): webmaster
331 Password required for webmaster.
Password:
230 User webmaster logged in.
ftp> put update.htm
200 PORT command successful.
150 Opening ASCII mode data connection for update.htm.
226 Transfer complete.
ftp>
```

B. Normal browsing by users to the web pages/use of the Finance, HR applications

We did not encounter any problems with normal browsing of the web sites.

5.4 Evaluate the Group Policy

There were two areas in the group policy where I felt are potential weakness and overkill areas. These are

A. Allowing previous logons to be cached

Allowing previous logons to be cached permits global domain accounts such as Domain Admins to be able to log on to perform administrative tasks even when the domain controllers are not available. If this setting is set to 0 and the domain controllers are not available for some reasons, the Domain Admins will not be able to log on to the server at all.

This is also necessary for the laptop GPO. As laptops are meant to be mobile, laptop users often have to log on to the laptop in an offline mode. Caching previous logons allows users to do so before they establish the VPN tunnel back to the HQ network. Enabling caching of passwords effectively reduce calls to the helpdesk since the majority of users are not very good at remembering to switch the domain to LUI when online and (this computer) when offline.

Enabling this feature has security dangers tied to it. Malicious people who gain physical contact or obtain possession of the machine in question can take their time to crack the passwords, especially the Administrator account.

B. Account Lockout Threshold

The security policy to lockout an account after 3 attempts at logon seems too strong and could be relaxed to about 5 or even 8 times. This is given that other mitigating controls such as the requirement to use passwords that meet complexity requirements and a password length of 8.

A Microsoft knowledgebase article has also explained that under some circumstances, a single failed attempt by a user to logon to his/her account could generate two parallel failed logon attempt count on the system, one for Kerberos and one for NTLM.

It is therefore highly possible to extend the account lockout threshold to 5 or 8 for the SANS HQ personnel.

6.0 Audit

There are several steps involved in developing a system audit plan.

Firstly, an audit policy and strategy should be endorsed by management. This policy and strategy should spell out the objectives of system audit and the major type of system/security events to be captured. For example, possible objectives of the audit policy may be to detect unauthorized changes and operations by malicious system administrators, to detect unauthorized password guessing or to detect suspect logons during office hours.

After getting management's endorsement for the audit policy and strategy, the next logical step will translate into the type of log information to capture on the systems to help achieve the objectives.

One of the most important mechanisms to implement in any security-conscious organization is a central logging system. With a "near realtime" central logging system, it highly negates the possibility that the logs on the system is tampered with.

The other mechanism to implement is a host-based intrusion detection system that will closely monitor events as they are happening.

One other mechanism that we learnt from the GCWN is the security configuration and analysis tool that allows us to perform a comparison between the actual configuration and the template configuration.

Finally, host configuration scanning tools and password crackers can be used to perform a thorough scan of the host configuration for potential loopholes and weak passwords. Some of the host-based configuration scanners such as ISS Scanners and Symantec ESM have best practices configuration files that can be downloaded and imported into the scanners. The reports generated by the scanners can then be studied carefully and new security configurations can be incorporated into the corporate template if found to be good.

6.1 Audit Policy and Strategy [9]

A. Audit Objectives

- i. To detect unauthorized attempts to access to sensitive accounts such as Domain Admins, the Enterprise Admins, and Schema Admins.

Repeated account login failures as a result of wrong user names or passwords may be a good indication that Admin accounts are being targeted. Typically, this will be one of the first places to target, given the huge payoff if successful. If the system is not audited well, such attempts will go undetected as administrative accounts are normally not configured to be locked out.

- ii. To detect unauthorized configurations to the Local Active Directory Schema at a domain controller.

Local administrators logging onto domain controllers at the console can configure such that the local copy of the schema can be modified therein. To deter local administrators from doing so, the fact that this is monitored should be made known.

iii. To detect deviated changes to the endorsed group policy settings that may lead to a breach of information security.

Administrators can play hell on the security of the organization by simply changing password, account and Kerberos settings. We would like the audit mechanisms to detect these type of changes.

iv. To detect successful modifications and accesses to sensitive executables and files on servers.

Successful modifications and executions of sensitive files on the system may be an indication either that a loophole in the file system permissions has been exploited or that a malicious privilege officer (administrators) has abuse his/her powers.

It will also be a good indication of virus attacks because modern virus writers like to target such innocent looking system files.

v. To detect successful logon sessions during off-office hours.

We would like to know when someone logs on during weird office hours. This will enable the IS team to conduct investigations based on such information if the need ever arises.

The above audit objectives are very focus on Active Directory configuration, management and use. It does not cater to application specific objectives which may be applicable for IIS, Exchange or MS SQL. These are out of scope of this exercise.

vi. To detect denial of service attacks on the domain

By running an automated password cracker on all domain user accounts, a denial of service attack can be effectively carried on an organization. We would like to be able to detect or minimize the impact of such malicious actions when it happens to the organization.

B. Audit Strategy

We will develop audit strategies to achieve the above objectives.

i. To detect unauthorized attempts to access to sensitive accounts such as Domain Admins, the Enterprise Admins, and Schema Admins.

Host-based IDSes will be installed on every domain controllers and will be configured to closely monitored login failures to the sensitive accounts. The

number of login failures encountered daily for every account will be tabled and sent as a report to the security officer whom will monitor the trend. If a pattern is encountered and upon further questioning, no valid attempts has been made by the affected account, malicious attempts at access sensitive accounts can be confirmed.

ii. To detect unauthorized configurations to the Local Active Directory Schema at a domain controller.

Whenever, the "Schema may be modified on this Domain Controller" checkbox is set to 1, the following registry value is updated:

Key = HKLM\System\CurrentControlSet\Services\NTDS\Parameters
Value = Schema Update Allowed

This value can be monitored by a host-based IDS installed on every domain controller. When this value is set to 1, a page should be sent to the security team.

iii. To detect deviated changes to the endorsed group policy settings that may lead to a breach of information security.

Audit policy settings changes are audited by the Windows 2000 event log. By configuring "Audit policy change" to log both success and failure events under "Default Domain Policy \ Computer Configurations \ Windows Settings \ Security Settings \ Local Policies \ Audit Policy", it is possible to record all changes to the audit policies, Kerberos policies, ipsec policies and user rights assignments.

Domain policies changes such as password and account lockout policies are detected by configuring "Audit Account Management" under the same tree and watching out for event 643.

There are also a whole other chunk of security options that can be monitored via registry keys and values as long as you know where to find them. These include:

- installation of print drivers
- restricting CD ROM/floppy access to only locally logged-on users
- enabling of admin shares (C\$, D\$)
- displaying last user name in logon screen

iv. To detect successful modifications and accesses to sensitive executables and files on servers.

There are some sensitive executables and files residing on servers that should be closely watched. These include the

%SystemRoot%\
- regedit.exe

- poledit.exe
- all files in "inf" folder
- all files under "security\templates" folder
- all files under "system" folder
- system32\cacls.exe
- system32\cipher.exe
- system32\command.exe
- system32\convert.exe
- system32\cscript.exe
- system32\dcpromo.exe
- system32\dns.exe
- system32\ftp.exe
- system32\gpedit.msc
- system32\secpol.msc
- system32\cmd.exe
- system32\ipsecmon.exe
- system32\irftp.exe
- system32\regsvr32.exe
- system32\regsvr.exe
- system32\regedt32.exe
- system32\recover.exe
- system32\secedit.exe
- system32\runonce.exe
- system32\runas.exe
- system32\telnet.exe
- system32\tftp.exe

There are many others, especially in the Support folder if the support tools are installed. These should be closely watched for file size changes and executions.

To do so, trip wires can be installed on the servers to send alerts when file hashes changed. To detect for access, the "audit object access" success and failures must be first enabled.

Then at the object, the relevant type of accesses and by which party are configured.

Once object accesses are configured properly, we can now make use of our host-based IDS to alert us on accesses to critical files. An example may be lpd.exe which should not be accessed at all during normal circumstances.

Another huge amount of accesses that is not audited by the above setting is the access to directory service objects. User and groups are AD objects and very often, we would like to be able to know what our administrators are doing to some sensitive accounts. For example, we may want to be alerted whenever a sensitive user account's information is modified or accessed.

- v. To detect successful logon sessions during off-office hours.

We would also like to log all successful logon sessions, especially the ones during off-office hours. To be complete, we also want to know when a particular user logs off.

This information is captured by the "Audit Account Logon Events".

vi. To detect denial of service attacks on the domain

Most IDSes are able to detect certain events and kept a counter for the same events happening within a certain time frame. So for this case, if the IDS is configured to raise an alert when 50 account are locked with 20 seconds, then we know that we are the victim of some sort of denial of service attack.

At SANGIAC, the IDS is configured to block off the source ip if the above situation happens, thus minimizing the damage.

6.2 Periodic Group Policy Security Setting Assessment

Apart from implementing on-the-fly/real time auditing on the servers, it is also important to perform a periodic assessment of the server's group policy security settings to "take stock" or "stock take" of the deviations and update some system documentations to reflect the deviations and the reason behind them.

ISS System Scanner is a wonderful tool for doing so. Running on an agent-server architecture, one can schedule security configuration assessments to determine what are the deviations from best practices.

A scanning console/server machine is used to communicate with agents that are installed on every server. Before starting the scan, the latest system policies (best practice type) can be downloaded from the ISS web site and imported into the scanning server. The configurations can then be reconfigured to better suit SANGIAC's security settings. Servers can be scanned in parallel and reports are generated for each.

In addition to using commercial system scanners, other alternatives will be to download the latest security templates from Microsoft, NSA or even SANS and studying them. According to the study results, update the SANGIAC security templates. Using the Security Configuration and Analysis snap-in, perform analysis on each server and see the differences. This will give a pretty good idea as to what are the security deviations on the servers.

===== END =====

References

- [1] Multiple Forest Considerations:
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/plan/mtfstwp.asp>
- [2] Checklist: Creating a forest trust
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/enterprise/x_checklist.asp
- [3] Outline for Group Policy Design Readiness
<http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/gpdesout.asp>
- [4] Best Practice Active Directory Design for Managing Windows Networks
<http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp>
- [5] Designing the Active Directory
<http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/activedi.asp>
- [6] MSDN Microsoft SQL Server 2000 Replication Articles -
http://msdn.microsoft.com/library/en-us/replsql/repllover_694n.asp
- [7] Implementing Nonpartitioned, Bidirectional, Transactional Replication
http://msdn.microsoft.com/library/en-us/replprog/rp_replsamp_3ve6.asp
- [8] Hardening Windows 2000,
Philip Cox, Version 1.3, March 14, 2002,
<http://www.systemexperts.com/win2k/hardenW2K13.pdf>
- [9] Auditing the Windows 2000 Authentication Process
Julio Silveira, April 01, 2001, <http://www.sans.org/rr/papers/66/184.pdf>
- [10] Microsoft Windows 2000 Security Configuration Guide
<http://www.microsoft.com/technet/security/issues/W2kCCSCG/default.asp>
- [11] Designing a Secure Windows 2000 Infrastructure, GCWN Practical Assignment
Matthew D. Arnold, March 12 2003,
http://www.giac.org/practical/GCWN/Matthew_Arnold_GCWN.pdf
- [12] Security Templates were downloaded from NSA website at
<http://www.nsa.gov/snac/win2k/download.htm>
Date : 5 Mar 2003, W2k Server.INF and W2kDC.INF
- [13] HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000
<http://support.microsoft.com/?kbid=315669>

[14] Hardening Systems and Servers Checklists and Guides
<http://www.microsoft.com/technet/security/topics/hardsys/default.asp>

© SANS Institute 2003, Author retains full rights.