Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Windows Security Architecture issues for an IT outsourcing company within a single infrastructure

GCWN - V3.2, option 1
Christian Gigandet
April 2004

1

1. Abstract

This paper is a practical work for the GIAC Certified Windows Security Administrator (GCWN). The assumption that SANS is an outsourcing company has been added in order to expose the problems faced by many outsourcing companies in the design of their windows network as well as sharing resources issues. Sharing resources is often really attractive when the discussion turns to the marketing side, however there will always be a trade-off between security and resources sharing. Recommendations based on various scenarios are provided.

This paper is divided into three parts. The first one describes the companies, their network architectures, their active directory (AD) design and the merging strategies. The second one is about security policies and group policies implementation. Auditing issues within a windows network are presented in the third part.

2. Introduction

All companies presented in this paper, SANS Co., ToBeSafe (TBS) and GIAC Enterprises, are fictional companies. SANS' domains design was driven by the giac.org (1) practical assignment version 3.2, option 1. GIAC domain has been defined in a previous practical assignment (2) and TBS has been introduced in this paper to illustrate the concept of outsourcing company.

2.1. SANS Co

One year ago, SANS Co. was founded by TBS, an US national insurance company because TBS decided to create a new company from its own IT division. This strategy allowed TBS to focus on their insurance business and gave SANS Co. a chance to generate new revenues by acquiring new clients. SANS Co. has therefore become an IT-Services company with outsourcing as their main activity.

SANS Co.'s main strengths are based on all the IT knowledge of various platforms including Solaris, Linux and Windows. However, due to the lack of a strong Sales and Marketing department which could define clear offers, they do not succeed in acquiring new clients. Nowadays SANS' main activity is to maintain and develop TBS's entire IT infrastructure and applications. From time to time, they also provide consultancy services to others.

SANS' head quarter is located in Chicago, USA, and a pool of developers is located in India.

SANS is composed of the following organizational units:
- IT infrastructure group:
  IT is composed of system, database, middleware and security

2

administrators, the back office and the helpdesk. Their tasks are to offer a strong and reliable infrastructure that can support in-house and third party applications. They are almost all located in Chicago offices. A few employees are also located in India to provide a local support to the developers.

- Development group:
  This is a pool of developers located in India which are responsible for the evolution and development of new insurance applications based the client requests.
- Sales and Marketing department:
  This is a small department composed of managers who unfortunately do not have a marketing background. They are responsible for defining products line and acquiring new clients.
- Human Resources division
- Corporate Management

As mentioned earlier, SANS has a difficult position in the market mainly due to the lack of marketing competence. Corporate Management is investigating various possibilities.

2.2. GIAC Enterprises

For two years now, the main activity of GIAC Enterprises, Michigan, is to produce fortune cookie to be sold via Internet. Progressively, they have developed their business on various e-commerce offers. In order to be strong in the market, GIAC strategy was to develop a strong Sales and Marketing division and to reduce the R&D and IT budget.

Here are the different groups within GIAC Enterprises:

- Research and Development
- Sales and Marketing
- Finance and Human Resources
- Corporate Management
- Information Systems

GIAC is well positioned in the market with lots of customers. However GIAC has reached the limit of its IT infrastructure and is currently investigating a new strategy to maintain, improve and develop their current offers. Collaboration plans with different IT-Services Company have been analyzed; SANS has been designated to be the best one.

2.3. Merging Strategy

After several weeks of negotiations, SANS and GIAC Enterprises have decided to merge on a holding structure model. SANS will benefit from GIAC's marketing experience and GIAC from SANS IT resources. The following objectives have been defined as part of the merging strategy:

3

- Both identities, SANS and GIAC, are maintained in order not to confuse the public with this merger. A holding structure has been established.
- Top management responsibilities are shared between SANS and GIAC.
- Sales and marketing tasks are going to be entirely performed by GIAC for the two entities. GIAC has already got valuable experiences and many contacts.
- SANS is going to take over the administration of the IT Infrastructure of GIAC Enterprise. GIAC R&D and IT group will join SANS IT groups.
- In the first phase, both IT infrastructures are preserved.

3. Initial Network and Domain Design

This chapter presents both network and domain design before the merging phase.

3.1. Network Design

An overview of SANS and GIAC network design is presented. Details about the implementation are not provided and are out of the scope of this paper. The goal of this overview is to simplify the comprehension of the following chapters by explaining various connection links and the topology that are part of the SANS and GIAC company.
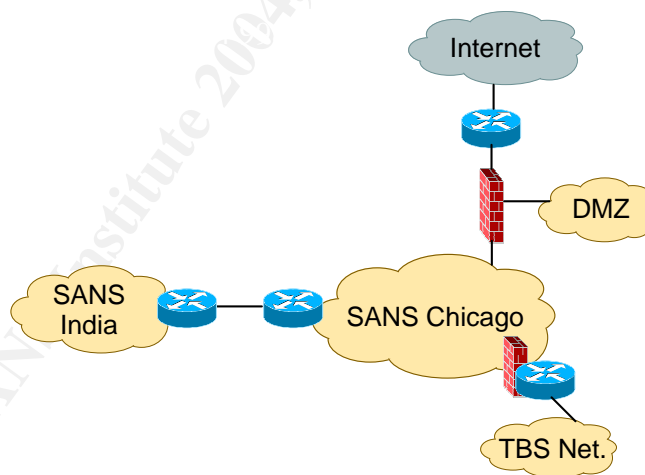
3.1.1. SANS Co

Figure 1: SANS Initial Network Design

SANS is composed of three networks: the DMZ, Sans Chicago and Sans India.

4

Network	Address Range	Descriptions
DMZ	123.123.123.0/24	Demilitarized zone hosting SANS and TBS public services: DNS for sans.org and tbs.com (Unix platform) Web Services (IIS standalone servers) Public MTA (Unix platform) VPN Servers (Cisco Equipment) External Authentication Services (RSA ACE Server)
SANS Chicago	192.168.0.0/16	This is the main Sans network containing all infrastructure resources. SANS headquarter is located in this network.
SANS India	10.1.3.0/24	This is a network located in India
TBS	10.2.0.0/16	This is the TBS network which contains servers and workstations managed by SANS administrators.

The network implementation and traffic flow control are performed on the following rules:

- All the network components and servers are doubled in order to assure redundancy and maximum services availability.
- The traffic to the DMZ from the Internet is controlled using routers with stateless access lists and statefull Firewalls rules. The traffic is restricted to the bare minimum strictly necessary (DNS, SMTP, HTTP(S) and VPN traffic).
- Each system located in the DMZ also performs OS IP filtering (ipfilter on Solaris, netfilter on Linux and ipsec rules on Windows systems)
- A statefull firewall also controls the network traffic between the SANS network and the TBS network.
- Network based intrusion detection systems are deployed to control border connection of the network.
- Strict filtering is also performed between the DMZ and backend systems located in the Chicago network
- No direct Access from Chicago and the India Network to the Internet is possible. All the traffic goes through applications proxies located in the DMZ.
- All the web traffic from inside goes through content filtering and anti-virus servers installed on Windows 2003 standalone boxes.
- Leased Line from Chicago Network to the India Network – based on Cisco equipment performing IPSec ESP in tunnel mode. A windows CA has been setup and accepts Simple Certificate Enrollment Protocol to issue certificates.
- Leased Line between Chicago Network and TBS Network.

Chicago is divided into several subnets in order to obtain fine grained network access control based on servers' roles. More details on the implementation are not provided in this document, as they would be beyond the scope of this paper.
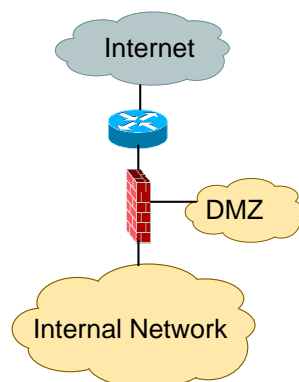
5

3.1.2. GIAC Enterprises

Figure 2: GIAC Initial Network Design

GIAC network is composed of one internal network and one DMZ for the public services. A firewall controls the flow between these different areas. For deeper configuration parameters, please refer to (2).

3.2. Domains and Active Directory Design

This section presents both domains and active directory design.

3.2.1. SANS Co

SANS Windows infrastructure is exclusively based on Windows 2003 Servers in native mode and Windows XP workstations.
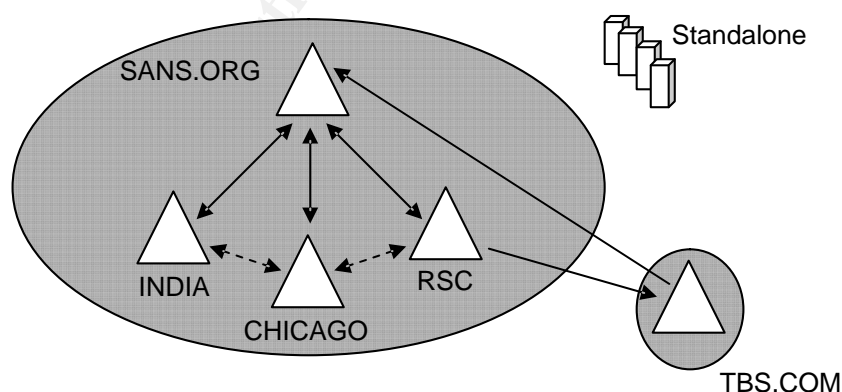

Figure 3: SANS Domains architecture

6

SANS forest is composed of a four-domain tree. Each domain has an implicit transitive trust with each other, which is automatically created when installing the domains (15). A special function is assigned to each domain:

- SANS.ORG, the root domain:
  This domain contains all the administrative accounts that are used to manage the entire forest as well as TBS.COM forest. Only the administrative tasks that need privileges are performed with those accounts. Account criteria are stricter than the on the others domains. Unidirectional trust has been established between TBS.COM and SANS.ORG domain in order to allow SANS administrators to manage TBS.COM domain. SANS.ORG is the "windows administration domain".

  This unidirectional trust between SANS.ORG domain and TBS.COM does not imply that the entire SANS.ORG forest has a trust with TBS. In fact, the external trust is intransitive, thus only users from SANS.ORG domain can access TBS domain. There is no implicit trust with the the external trust. In addition to the trusting restriction, there is also a filter on the IP level provided by the firewall that only allows SANS.ORG member servers to access TBS.COM network.

- CHICAGO.SANS.ORG:
  This represents the majority of SANS windows resources. Each SANS employee located in Chicago owns an account on this domain which is used for daily logon. Almost all workstations of the forest belong to this domain, excepted those located in India which represent a minority.

- INDIA.SANS.ORG:
  This domain is used by SANS employees located in India. Development resources that are only accessed by developers are members of this domain.

- RSC.SANS.ORG:
  All resources that need to be accessed from external clients' domain are members of this domain. For the time being, only TBS.COM has a unidirectional external trust with RSC domain. This external trust is not transitive, thus only resources of this domain can be accessed from TBS.COM domain.

On Figure 3, a schema of SANS and TBS domains is available. Figure 4 shows the trust configuration of SANS.ORG root domain. IT is possible to verify the implicit transitive trusts with the subdomain. The external intransitive trust with TBS.COM which has been manually setup is not transitive.
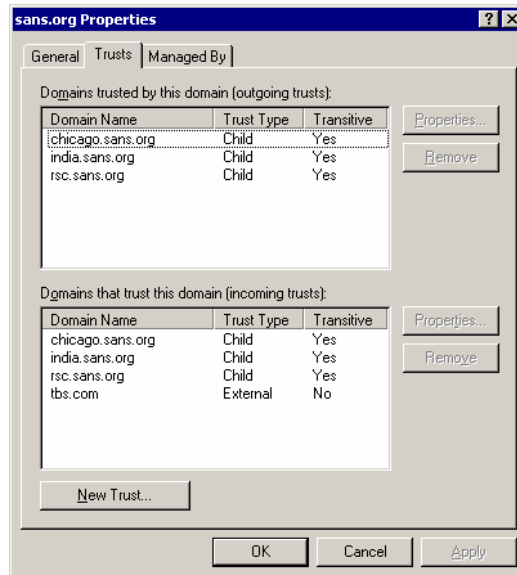
Figure 4: SANS Domains Trust

The motivations for installing multiple domains within the forest were the following:

- India and Chicago network are linked with a leased line. In order to keep the maximum bandwidth for the business traffic, a separate domain has been chosen. In fact, only the global catalogue is replicated between domains and this represents about 55% of the AD database. At that time architects who have designed the network did not want to manage various windows sites, neither AD replication tuning.
- The India domain needs different local setting than the others and this is a domain wide parameter.
- The administrative accounts need particular attention and special password policies are applied domain wide. Custom password policies filters have not been retained because of the management decisions to rely only on windows default functionalities.
- RSC.SANS.ORG domain need to have unidirectional trust with external domains, but only with it! External trusts are not transitive as already mentioned in this paper.
- There were some unexplained management/architects reasons not to have several forests that could provide a better enhancement of the security level, particularly for RSC.SANS.ORG. In fact, if the RSC.SANS.ORG domain gets compromised, access to the others is possible due to the implicit trust. They stated that SANS would feel more comfortable with a domain logical separation and that several forest was too much for the need.

In addition to the SANS.ORG forest, SANS windows IT infrastructure is also composed of several standalone Windows servers. For example two IIS web servers those are located inside the DMZ. Due to the exposure factor it has been decided not to integrate them into the internal forest, nor to create a new forest

8

for them. The DMZ also contains two windows servers with a web content filtering application responsible for analyzing and filtering the web traffic. Others standalones within Chicago network have been installed for special needs. Thus, the DMZ servers do not belong to any domain in order to minimize the access level between the exposed DMZ servers and the internal network. If one of those servers get corrupted, the attacker will not have access to the entire internal forest, to all members and to the internal Active Directory. The corporate security policy states that no AD query is allowed from external network. Due to the small number of windows servers located within the DMZ, it has been decided not to setup a separate forest. The cost to administer and maintain an external forest has been evaluated higher than the individual administration and maintenance of each server. Please note that this individual administration can cost a lot if the number of DMZ windows servers gets higher. In this case, it will be more efficient to set up a separate external forest

Between the different domains, Kerberos is the primary authentication method used. By default, interdomain Kerberos keys are only exchanged between adjacent name domains. The name of the domains determines the trust path. To prevent SANS.ORG to be "flooded" by unnecessary traffic, a shortcut trust is established between INDIA.SANS.ORG and CHICAGO.SANS.ORG as well as between CHICAGO.SANS.ORG and RSC.SANS.ORG. This improves authentication performances and has no drawbacks on the security level.

Figure 5 shows the shortcut trusts that have been established between subdomains. These trusts only have a meaning for Kerberos authentication.
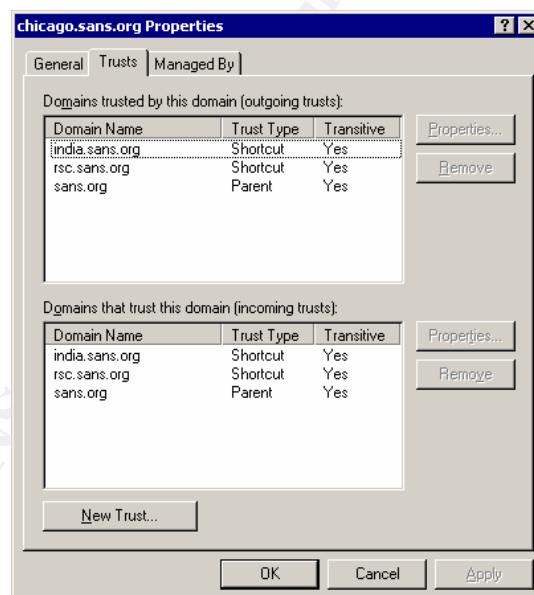

Figure 5: Chicago Domain Trust

As already mentioned above, SANS.ORG has the administrative domain function for the entire forest as well as for the external forest. Of course, this is not a windows technical function, but it makes sense on an organizational point of

9

view. That simply means that all administrative tasks for the entire forest are going to be performed from SANS.ORG domain. No Windows administrative accesses privileges are assigned to other domain accounts. Actually there are no technical reasons that could prevent administration tasks to be performed from an account of another domain. This would simply require the correct privileges and domain trust. This is up to a corporate security policy that forces the centralize administration from a single domain.

Of course, different permissions are defined and assigned based on job functional roles. A role can be a security administrator, a Windows administrator, a Windows integrator, the helpdesk and others. Theses roles are technically represented with SANS domain global groups which contains all the administrative accounts. As every domain under SANS administration scope is managed from SANS.ORG domain, it is important to have enough flexibility to assign a specific role only regarding a specific client. In fact, a security administrator for client X does not necessary get the security administrator privilege for the client Y and it must not be the case. This will lead to a kind of authorization creeping! A naming convention for the SANS administrative group is defined. This simplifies the administration of those groups and avoids misconfigurations. Naming convention is an important issue and often neglected. Table 1 presents the convention for the SANS.ORG admin groups.

Group name	Function
Admin_Security	Security administrator role included in all domain and forest under SANS responsibility. This group is included in all other domain global group that represents a security role.
Admin_*domainname*_Security	Security administrator role for *domainname* domain.
Admin_helpdesk	Helpdesk role included in all domain and forest under SANS responsibility.
Admin_ *domainname*_helpdesk	Helpdesk role for *domainname* domain.
...	...

Table 1: Domain Global groups that are mapped to job function

The SANS administrative domain global groups defined are not directly used to grant permissions on resources. Instead they are included in domain local groups of each domain and permissions on resources are granted on those domain local groups. This allows setting minimum permissions on resources. Using only domain local group to assign permissions is always an advantage when migrating or modifying the trust model. A similar naming convention is also defined for those groups. It is presented in Table 2.

10

Group name	Function
Grant_Security	Domain local group created in each domain. Necessary permissions based on security administrator role (AD attributes, user rights…) are granted on those local groups. They include the corresponding SANS domain global group (Admin_*domainname*_Security)
Grant_helpdesk	Similar to Grant_Security, but for the helpdesk
…	…

Table 2: Domain local groups that are used to grant resource permissions

Universal groups are not used in this administrative model as there is up to now, no need to add accounts from others domain. Planning permissions assignment deployment based on group types can be found in (3).

This naming standard allows fine granular access based on roles that can be different for each domain/forest. A similar model is followed on other domain to assign user permission based on their job functions (role). Group like Grant/User_humanressource, Grant/User_management … are defined.

The consequence is that a SANS employee who needs windows administrative privilege has two accounts. One in the CHICAGO.SANS.ORG that is used for daily logon and tasks that do not require administrative access, and one in the SANS.ORG domain which is his admin account. The administrative accounts are accessed through terminal services on dedicated terminal servers. On the network level, only specific subnet accesses are authorized. The runas command can also be used from all domains to perform administrative tasks

The active directory design of CHICAGO.SANS.ORG is presented below. Other domains have similar design. Basically, three top levels OU are created for the members, the accounts and the groups:

- OU_members contains all members of the domain. It is divided in sub OU depending on the servers or workstation role. This facilitates the implementation of specific security policy. This will be approached in more details later in this paper. The current OU defined for servers are the followings: OU_MailServers, OU_FileServers, OU_IISServers, OU_PrintServers and OU_TSServers
- OU_Accounts for the accounts of the domain. This OU is also divided in several OU, but the motivation is a little bit different from the one for the members. The idea is not to separate accounts base on their role, but based on the delegation that will be applied to them. As example, the helpdesk will be delegated the task to reset password on standard user, but not on management users.
- OU_Groups that contains both groups used to set ACL and the group containing the user as discussed above.

In Figure 6, you can see the Active Directory Users and computers of cg2.chicago.sans.org, a DC. It illustrates the OU structure of the AD
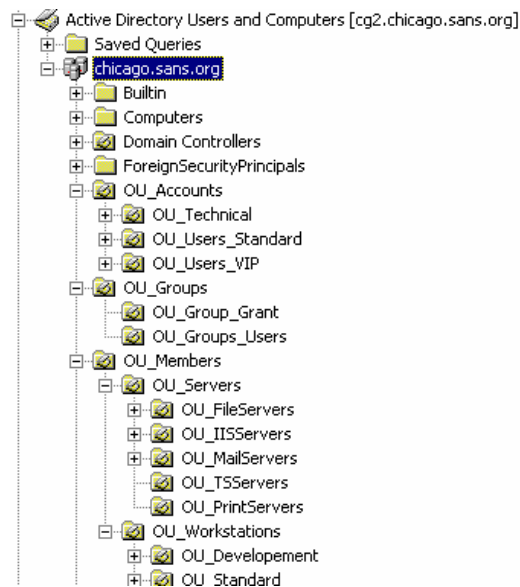
11

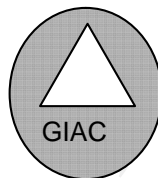Figure 6: Chicago AD design

3.2.2. GIAC Enterprise

Figure 7: GIAC Domain architecture

GIAC windows architecture is a windows 2000 single domain (Figure 7). The AD design follows the organizational structure with about one OU per entities. Each department in GIAC has specific OU, although no distinction is made between information systems users except for the helpdesk Operators. For deeper configuration parameters, please refer to (2).

4. SANS and GIAC integration design

The merging plan includes both the establishment of IP connectivity based on Cisco equipment and establishment of a new trust. This will allow the SANS IT department to take over GIAC domain administration tasks and GIAC employees to access resources from RSC domain.

12

4.1. Network Design

It has been decided to keep both SANS and GIAC Internet connectivity. However, a project will start in a few months to study the migration phase in order to rely only on SANS internet connectivity by moving all the GIAC public services into the SANS DMZ infrastructure.

A leased line will assure the network connection between SANS Chicago network and GIAC Internal network. The implementation relies on Cisco network equipment.

Schema is not provided, but it can easily be derived from a merger of Figure 1 and Figure 2.

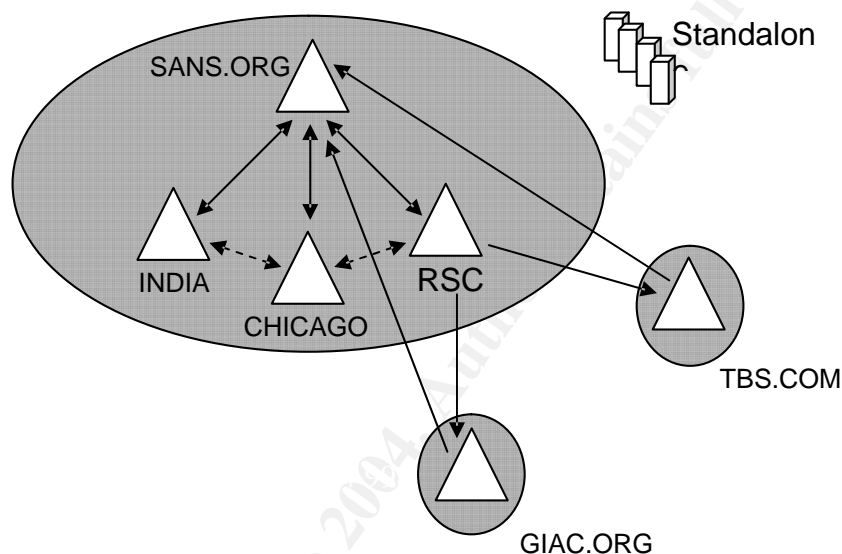## 4.2. Domains and Active Directory Design

Figure 8: SANS and GIAC trust implementation

Figure 8 illustrates the new windows trust between SANS and GIAC. Two external unidirectional trusts have been established. The first one allows SANS administrator to access and administer GIAC domain. The second one allows GIAC employees to access future resources that will be included in the RSC domain. Figure 9 shows SANS incoming trusts and GIAC outgoing trust configuration.

13

Domains that trust this domain (incoming trusts):				Domains trusted by this domain:		
Domain Name	Trust Type	Transitive		Domain Name	Relationship	Transitive
chicago.sans.org	Child	Yes		sans.org	External	No
giac.org	External	No				
india.sans.org	Child	Yes				
rsc.sans.org	Child	Yes				
tbs.com	External	No				

Figure 9: SANS and GIAC unidirectional external trust

In order to follow the administrative model presented, several domain local groups were defined in GIAC domain and appropriated permissions affected. Corresponding SANS domain global group were defined and included on GIAC groups.

5. Sharing resources recommendations

SANS and GIAC motivations are to offer services on a low cost basis by doing a maximum of resource sharing for themselves as well as for their clients. Resources can be servers' hardware as well as applications.

Marketing and management inputs are always to produce and offer solutions at the lowest possible cost. Here are typical scenarios from the highest client isolation and associated implications. High level recommendations are provided below and of course followed by SANS administrators:

- No sharing at all. Each client has its dedicated hardware. This offers a strong and reliable client logical isolation. Do not forget that even if the hardware is dedicated to one client, isolation between different kinds of applications is also an issue! In fact, it is rare to dedicate a hardware server to a single application, but various applications require different security level. Securing every applications within an entire windows network can be time consuming and not all businesses require strong security configuration for each applications. However in a high security environment, each application should be configured correctly and should only be permitted to read and modify its configuration and necessary data files. As a minimum, you should think of grouping low level security application requirement in a farm of servers and high level security requirements (or well controlled applications) on another farm of servers. Applications isolation for a single customer can lead to the same reflection provided below for multi customers and should not be neglected. This is part of the minimum privilege principle.
- Hardware sharing, but one dedicated application per client. This is also an acceptable scenario, but only if there is a logical separation between the applications. Practically, it implies that the execution account of each application (service account) has to be unique in order to prevent an ill-

14

intentioned, corrupted or misconfigured application to access other clients' data. This of course also means that there are strict and well defined file system permissions.

- Application sharing. This scenario is possible when applications have been designed to support multi-client hosting. This scenario has to be accepted with caution. In fact, the logical separation between clients only relies on the application level and the correct behavior of the application itself. If the application gets compromised, the entire environment will too! The recommendation would rather be not to accept this scenario. If the associated risks are accepted, be sure that the "multi-client" binding on the application is applicable and allows you to set different configuration per client. This seems quite implicit, but there are lots of applications claiming to support multi-client, but are so inflexible that this becomes unfeasible. Always double check your requirements as well as your client's ones.
- The last scenario is definitely to be prohibited on high level security infrastructure. This is the case were one single hardware is shared between clients running application under the same execution account. This will typically be the case for applications requiring SYSTEM account. If an application needs to have local administration privileged, it also falls under this case.

Resources sharing are not always easy to implement because of poor vendor feedback regarding the privilege requirement in order to have the application running. You will often hear that the service account needs administrative privilege. Be sure to ask twice because it often is unnecessary! Event worst, some installation guide will claim to need domain admin privileges!

Before being implemented into a production environment, all applications must first go through an integration process were you can actually test their behavior. You can of course use utilities like NTFSmon and Regmon (4), however be sure and ask your vendor about the support clauses. A non default installation is rarely supported!

On the network side, as soon as there is resource sharing, be sure that it is possible to bind the application on a specific logical interface. That will help you to configure proper IP filtering, either on a network level or on the OS level. Some application also support IP filter rules on the application level.

6. Future migration plans

While doing this migration plan, the SANS administrators and management admitted that this multi domain forest has got a poor security value added. Basically beside the administrative rigor that allows proper functional separation, we only rely on SID security and the criticality of SANS.ORG domain will become higher and higher with the number of clients managed from this domain. It has

15

been decided to migrate the SANS.ORG domain in another forest that will have the same role.

The Internet access between SANS and GIAC will also be merged by moving all GIAC servers that need Internet connectivity into the SANS DMZ. Actually several DMZ will be defined based on the type of service they provide (web servers, VPN connection, email server, dns…).

The Network architecture also needs some improvement, by defining dedicated sub network segment for front servers and others for back-end servers. The connectivity between the different locations is also going to be migrated on a VPN over Internet with ISDN as backup.

7. Security Policy

Security policy is a vast subject and it would be possible to write entire books about it. Implementation design for both companies, SANS and GIAC are presented in this section. The aim is not to provide full implementation detail on each parameter that can be set on windows servers, but rather to present a clear overview about the design with some precise samples configurations.

Group policy (GPO), introduced since Windows 2000, is the mandatory tool while speaking about Windows security policies (16). Group policy is used to automatically set lots of parameters for users and computers. Different scopes can be defined which are by order of treatment: local, site, domain and OU. Some parameters can only be applied at the domain level. Group policy allows defining a standard and coherent configuration for the entire network. Domain, OU and local policies are defined and used for SANS and GIAC forests.

Following the "due care" and least privilege principle, each company has its own security level requirements depending on business needs and the risks acceptance. Thus, windows security policy will be defined based on the high level corporate security policy and the means (budget and human resources) allocated for the security. Note that even in the same company, different security requirements can depend on the system criticality. For example, in our case the SANS.ORG domain is an administration domain. If this domain gets compromised, the entire infrastructure could be damaged, as well as the client's infrastructure. It is important to remember: 100% security does not exist.

As mentioned, member domains of SANS and GIAC forest are grouped based on their role and thus form a hierarchy. This allows linking GPO on different stages (OU) and defining precise parameters depending on the role. This member separation into various OU allows being flexible enough without additional cost by the administration of windows group of servers. Consider that a group of servers is an OU. Of course there will always be some special case where only one server has a particular role that requires a specific configuration

16

and it would be overkill to define an OU for one servers. GPO permissions resolve this issue and are discussed below.
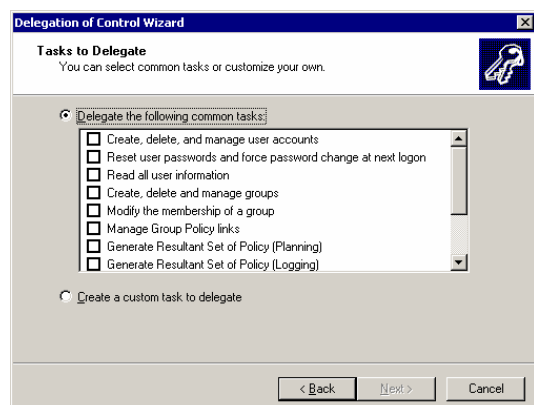

Figure 10: Delegation Wizard

Definition of different groups for users is more implicit as this has to be done in any case for resource permissions. OU separation for servers seems logical; however OU primary function is not to reflect the business organization. The main OU purpose is to enable delegation of some kind of tasks based on OU. This can be done directly by assigning correct permissions on the Active Directory or using the delegation wizard represented in Figure 10.

Actually, three OU have been defined for the accounts: one for the technical accounts, one for the standard users and one for the VIP's. This allows delegating several tasks like resetting the password to the helpdesk, but of course only for the standard user OU! Tasks on the VIP OU (e.g. Management accounts) will still require the intervention of a SANS security administrator. Please note that this is not a technical limitation, but this restriction is only due to a corporate security policy. VIP accounts are more sensible because of the confidentiality level of information they can access and this is the reason why the intervention of a security administrator is require to reset password for VIP accounts.

Even with a unique OU it is still possible to have different GPO applied to the objects based on the permission settings. All SANS and GIAC domains will rely on GPO permissions regarding the user configuration parameters.

Figure 11 represents the permissions on the GPO_IE6_Standard_With_Proxy GPO which contain Internet proxy definition. GPO permissions determine who is able to read and manage the GPO, but a permission that allows lots of flexibility is the "apply" permission. The GPO will only apply to someone who has at minimum read and apply permission.
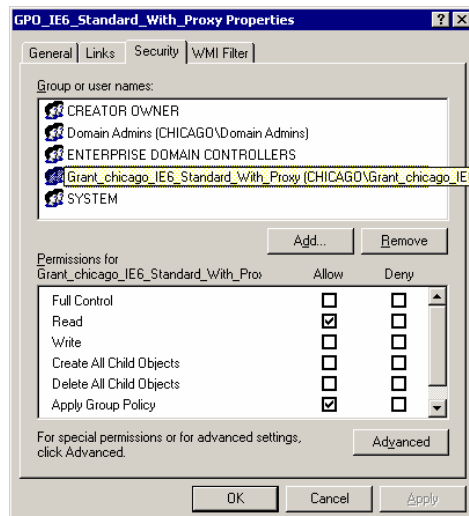
17

Figure 11: GPO Proxy permissions

Similar GPOs' address different needs. For example, as soon as a user gets local administrator rights on this workstation for whatever reason, he is assigned another group Grant_chicago_IE6_Standard_WithOUT_Proxy and thus cannot surf on the web (poor guy!). Web Surfing must never be done with a privileged account. Even if your Internet Explorer is up to date, there are still ActiveX issues. ActiveX are running under the user context privilege and can be used to read/write data, set registry value or access databases. This is often used by attacker to penetrate a network. Internet Explorer parameters under "Tools – Internet Options – Security" can be set by zone to control ActiveX download and execution. By default there are 4 different zones which are; Internet, Trusted Sites, Intranet and sensible sites. Theses zones must be configured according to your requirements. Internet Explorer Administrative Kit (IEAK) that can be used, but in an Active Directory domain, you should rather push these parameters through a GPO. Since this is an important issue, I would also mention to take care of the "save for scripting" tag that can be bind to an ActiveX. This tag means that the developer guarantees that no script can cause damage to the user's computers and that no unauthorized information can be obtained or corrupted to the user's computer. Unfortunately, it is quite common that the developers mark their ActiveX as safe for scripting to avoid all the IE setting issues! In fact, it is only up to the developers to decide whether or not its ActiveX is safe or unsafe! Adding with the permission to download ActiveX, this can be a powerful tool in possession of malintentioned hacker. Be sure to cover all aspect of IE parameters security settings.

There is a last point to mention: GPO is a powerful tool, but it can also be a very destructive one! You should always think twice before adding a GPO to an OU as it will automatically apply (see 7.2 for more details when GPO are actually applied). A good practice is to disable the new GPO while editing it. Once it is ready, think twice before you enable it. Of course a testing environment is used by SANS administrators to prepare the new configuration that will be applied on the production systems. Adding to the testing environment, don't forget that you

18

can easily create a sub-OU and move the computer or account into this OU for the final validation into the production environment.

7.1. Security Policies Configuration

The security policies implemented in SANS and GIAC define a baseline configuration for members and for users' configuration. This baseline has been designed to have the most restricted level as possible while meeting the common requirements functionality. More specific policies based on role or job function have the tasks to apply a fine grained control in order to reflect each specific parameter. Practically this baseline is a GPO with computer setting only applied to the OU_members and a GPO with user settings only applied to the OU_Users. The idea is to harden the systems as much as possible with the baseline policy without having to reopen everything on the next GPO OU level.

Each domain has a specific user setting configuration. SANS.ORG settings are stricter in terms of password policies and all IE parameters are blocked with no proxy configuration. Please be aware that a user having access to the registry (regedit for example), can set the proxy configuration values himself in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings. Actually, much more that just the proxy or proxy automatic configuration (PAC) file can be set in this location. This is the reason why the proxy servers also implement a network filter in order not to accept requests from SANS.ORG workstations and servers. This is only possible as strict range definition are defined and used for each windows domain. This prevents administrators to surf with their privileged account (poor dude!). CHICAGO.SANS.ORG is similar to INDIA.SANS.ORG, but developers have different settings specific to their tasks functions. For example, IE settings for developers will also "trust" development web sites which is not the case for standard users.

While the user settings have different parameters depending on the domain and the job function they have they have, the server setting is more common as this is the minimum setting in order to have the servers performing their tasks.

NSA recommendations (5) are followed for the implementation of GPO for GIAC.ORG Windows 2000 domain. Concerning Windows 2003, the Microsoft Windows 2003 Recommendations (6) have been chosen for the SANS.ORG forest. Actually, even the NSA will point you to Microsoft Recommendations regarding Windows 2003. That does not mean that these proposed setting must be blindly applied. SANS.ORG administrators have chosen those standards as a template, but additional settings and modifications have been necessary in order to fulfill SANS requirements. Examples are presented below. There are lots of public available templates for securing a windows Active Directory domain. Do not reinvent the wheel; there is nothing bad in acquiring public template to start defining your own template.

In adding to that, each application deployed on a windows server requires additional configuration on different levels (NTFS, Registry, Services…). This is

19

for example the case for domino and exchange MTA servers that have been secured on a NTFS and Service level. As discussed in chapter 5, isolation between applications is an important issue. This is the reason why the integration process must always define proper settings following the least privilege in terms of user service, NTFS permission, registry…

Generally, whatever was the source of the templates was, SANS administrators have applied the "minimum privilege" principle. On tables 3, 4 and 5, the modifications applied to the high-level security of Microsoft Recommendations (6) regarding the domain policy, the baseline policy and the IIS policy are described. Those three policies were chosen in this paper as they have been applied in the next part. The modifications main goal is to support SANS administrative model. In fact several tasks are not performed by the administrator, but by dedicated groups. For example adding a member or performing a restore.

As every domain managed by SANS is AD domain with XP as workstation, no big issues are faced because of old NT4 or windows 95/98 clients.

Descriptions of the parameters are not provided in this paper. Plenty of other sources discuss the advantages and disadvantages of the different settings (7).

	Settings	Comment
Account Policies – Password Policy		
Maximum password age	60	
Minimum password length	8 characters	Corporate Global Policies (platform alignment)
Account lockout threshold	5 invalid logon attempts	
Microsoft network server. Disconnect clients when logon hours expire	Disable	No official logon hours are defined.

Table 3: Default domain policy – customization to the High Security Microsoft recommendations

	Settings	Comment
Local Policies – Audit Policy		
Audit privilege use	Failure	Many events are generated. Failure has been decided to be sufficient.
Local Policies – User Rights Assignment		
Add workstations to domain	Administrators and Grant_domain_backoffice	This task has been delegated to another group (backoffice)
Debug programs	Administrators	Avoid conflict with SUS which use windows update
Lock pages in memory	Not Defined	Avoid degradation of system performance
Restore files and directories	Administrators and Grant_domain_Restore	This task has been delegated to another group (Restore)

20

Shutdown the system	Administrators and Grant_domain_backoffice	Backoffice group has to perform some shutdown
Local Policies – Security Options		
Audit: Shut down system immediately if unable to log security audits	Disable	
Shutdown: Clear virtual memory pagefile	Disable	Laptop issue with hiberfil will be addressed in a laptop focused GPO
Accounts: Rename administrator account	SuperAccess	
Accounts: Rename guest account	DevNull	
Services		
SNMP Service	Enable	Used within the Enterprise for Surveillance – tools migration is evaluated due to SNMP issues
SNMP Trap Service	Enable	Used within the Enterprise for Surveillance – tools migration is evaluated due to SNMP issues

Table 4: Member Server Baseline policy – customization to the High Security Microsoft recommendations

	Settings	Comment
Account Policies – User Rights Assignment		
Deny access to this computer from the network	Not Defined	Member Server Policy will apply. Only windows authentication is wanted on the domain Web server. Thus Guest account has not to be removed. IIS on the DMZ does not apply this policy.

Table 5: IIS Servers policy – customization to the High Security Microsoft recommendations

In addition to the custom parameters, it is also necessary to import some domain dependent information like the built-in Administrator, Guest or support_388945a0 built-in account whose SID is specific for each domain. Figure 12 is a snapshot of this task. More detailed explanations about the template importation are provided in the next section.
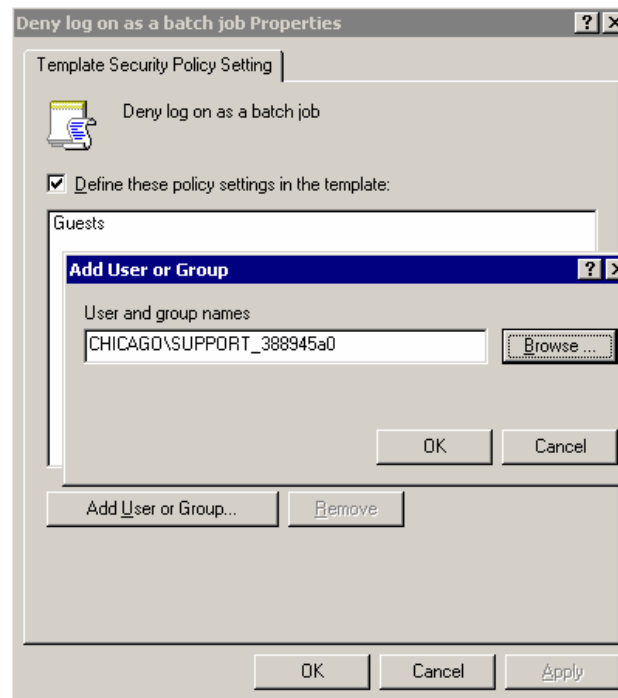
Figure 12: Domain dependant parameters

As presented in Table 4, SANS is currently using management software that is using Simple Network Management Protocol (SNMP). Short explanations about security issues and threat mitigation are presented below. SNMP has been the defacto standard for network management. SNMP agents reside on each device. The set of objects that can be managed using SNMP are described in a Management Information Base (MIB). The majority of software management are using the version 1 of SNMP (9). SNMPv1 lacks in confidentiality and integrity in it's implementation and thus is vulnerable to several threats. SNMPv1 authentification relies on a community strings sent in clear over the network. Community strings are often leaving to the defaults one (public for read and private for write) and, in any case, can be sniffed. You must change the default value! IP address access lists are rarely used but should be implemented even if it can potentially be spoofed.

SNMPv2 and v3 definitions aim to improve these security issues from the previous version. Information is not provided in this paper but can be found in (10). Those standard are not wildly deployed.

The software management used within the SANS network relies on SNMPv1 and administrators are currently evaluating two possibilities in order to mitigate this exposure factor. The first one is to require IPSec between each host agents and the central management console for the SNMP traffic. Some https capabilities from the new version of this software management is also reviewed and analyzed with SANS's need.

22

Please note that the next versions of security management software will probably integrate Windows Management Instrumentation (WMI) which is "the Microsoft implementation of the Distributed Management Tasks Force's (DMTF) Common Information Model (CIM) for Web-Based Enterprise Management (WEBM)" (20) (SANS scriptable). To simplify, you can consider this a new version of SNMP where you can get simple requests, but also manage computers. For more information please refer to (11).

7.2. Application of policies on a IIS Server

This section presents the application of the three policies discussed above. A testbed has been setup in order to verify the accuracy of the proposed settings. It will be demonstrated that policy have hardened the systems and that policies even allow detecting misconfigured systems.

The following actions were performed on a CHICAGO.SANS.ORG internal IIS server. After the application of these 3 policies, the functionality of an IIS server will be controlled by using a non privilege account CHICAGO\christian. In order to do this task, three different kind of web servers' configuration have been reproduced:

- A static web server
- A web server relying on ASP. Actually a simple ASP which only write file on hard drive has been used.
- A WebDAV server

The Microsoft Security template has been added on the "Security Templates" mmc snap-in and customized based on the configuration available on table 3, 4 and 5.

It is then possible for an analysis on the IIS server to show all parameters that do not match the defined policy. That can be used to perform last verification before the policies are applied. Figure 13 shows the results, the member's default setting (Computer Setting) and the policy definitions (Database Setting) are displayed. It is also possible to verify that the customized parameters have been taken into account (eg: Audit privilege use - Failure)

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

Figure 13: Security Configuration and Analysis (before)

23

Once all customizations have been made and are estimated to be correct, the template can be imported into a GPO. All parameters of the security template will be reflected in the Computer Configuration – Windows Settings – Security Settings section. Figure 14 and 15 illustrate these steps.

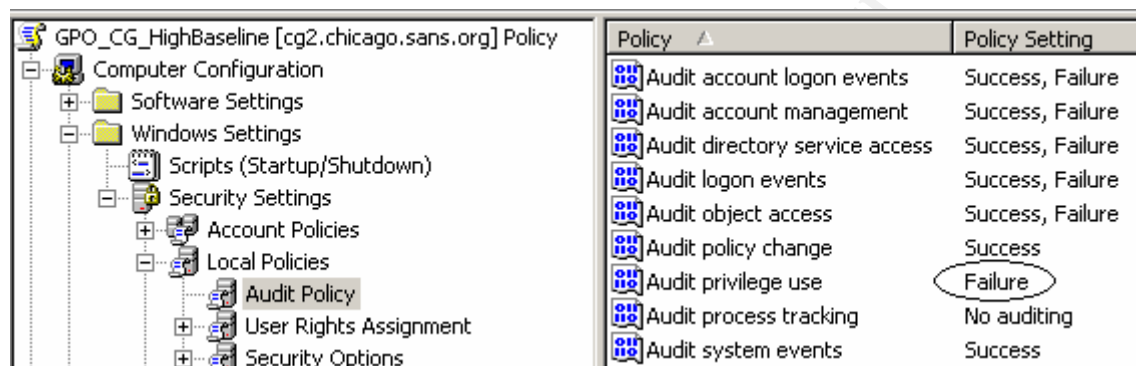

Figure 14: Import a template into a GPO

Figure 15: GPO parameters set through the imported template

Once the GPO is linked to an OU, the members will not modify immediately their setting according to the GPO. In fact, "by default, the computer Group Policies are updated every 90 minutes with a random offset of 0 to 30 minutes"[1]. This interval can be customized depending on your need via Group Policy
(Computer configuration – Administrative templates – System – Group Policy – Group Policy refresh interval for computers).

For the purpose of the testing, group policy update has been forced with the "gpupdate /Target:computer /Force".

Then, the correct application of the GPO has been verified on the IIS Servers with the ">gpresult /scope computer" command and through the security event log (figure 16). The gpresult command shows that the two additional GPO "GPO_CG_HighIIS and GPO_CG_HighBaseline" have been added to the default ones.

---

[1] See Explain tab of Group Policy refresh interval for computer Properties

24

Figure 16: Verification of the correct appliance of a GPO

In case of any doubts, you can also perform another security analysis on the IIS server and check that all the Computer Settings are equivalent to the Database Settings (Figure 17)

Figure 17: Security Configuration and Analysis (after)

The defined security parameters have been applied and it is now important to verify the behavior of the system functionalities which is to offer three different types of web server access to specific domain users. The three types of web servers will be accessed using the non privilege account Chicago\Christian.

While accessing the static web server, the following message immediately appears: "You are not authorized to view this page" (figure 18). It means that the web server has successfully started as configured on the GPO_CG_HighIIS GPO, but also that there is an issue with the parameter applied by one of the two GPO.
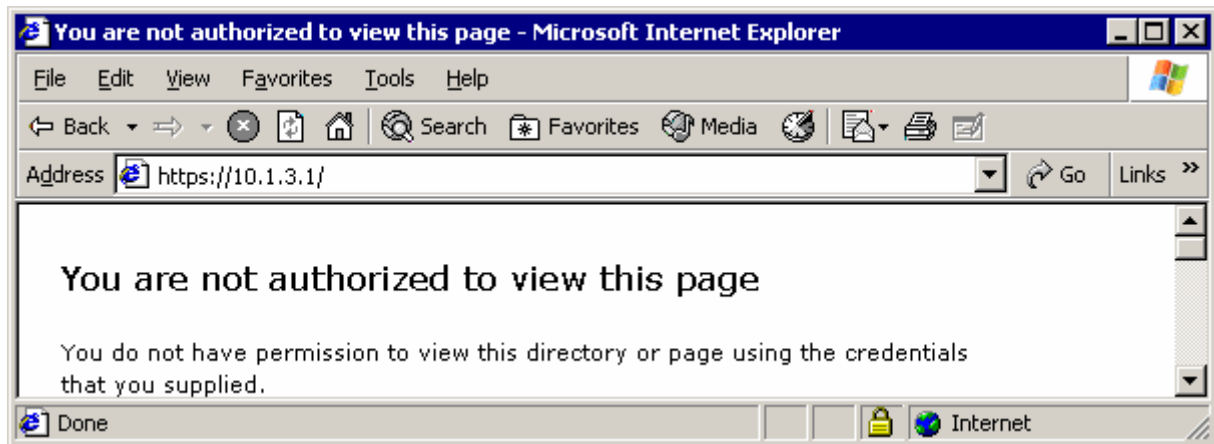
25

Figure 18: Static Web Site Failure Access

As the auditing has just been turned on, the first place to look at is the security event log before doing any other investigation. This was the right place to look at as a Failure Audit message has been generated. It shows "IUSR_CG8 user has not been granted the right to log on to this machine". (Figure 19)
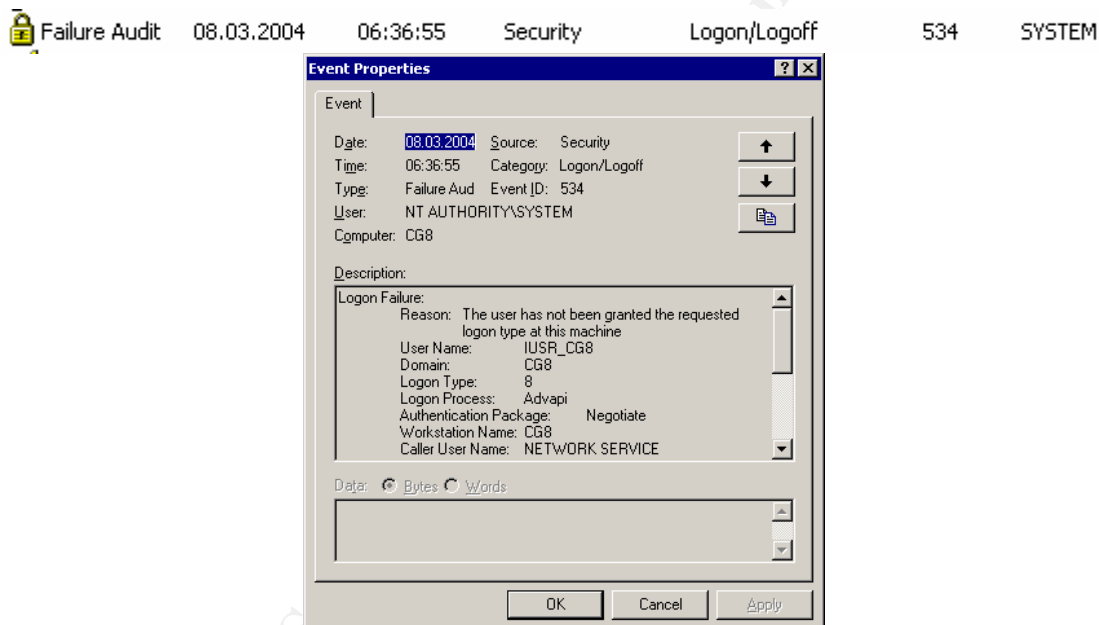

Figure 19: Failure Audit Event Log

Actually this event has occurred due to a misconfiguration in the IIS server. It should have been configured to accept only Windows integrated authentication, but was set for anonymous access with the IUSR_CG8 account. This misconfiguration has been corrected. This error could have been detected sooner if the NTFS permissions of the document root were set appropriately to allow only the designated windows domain local group Grant_Intranet_read. The NTFS permissions were adjusted to the correct ones and it is now possible to access the Intranet site (Figure 20)
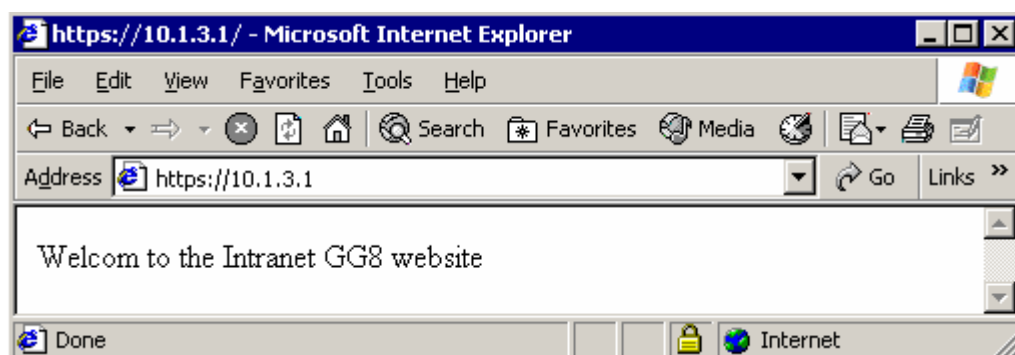
26

Figure 20: Static Web Site Success Access

This was an important issue to discover. In fact it demonstrates that the security policies can also help to find misconfigured servers. It is really important to have security policies in accordance to your environment and not just blindly apply some high level security just because someone stated they are high. If we would have applied the default Microsoft recommendation with no modification, this error would not have been detected. In fact Microsoft IIS specific policies would have had authorized this logon using the anonymous IIS authentication. Having policies implementing YOUR requirement can only be of benefit.

The two other web sites, asp and webdav, were accessible successfully without having detected any functionality regression due to the policies just applied. Apart from the log on of the webdav server presented in Figure 21, no more snapshot is provided for this testing functionality because it would have poor value added.

```
PROPFIND /cg/salut - 80 chicago\christian 10.1.1.55 Microsoft-WebDAV-MiniRedir/5.1.2600 207 0 0
```

Figure 21: WebDav serveur access log

While accessing the cg8 servers, it has also been possible to verify that the logon banner configured on the policies had been applied. Please refer to Figure 22. Each single parameter set though the policies can be verified, but as it has been discussed above, the two additional GPO have been applied, so that the risk for the parameters not to be set is unprobable. The biggest issue is the functionality testing that has been conducted on each of the three web servers of the testbed.
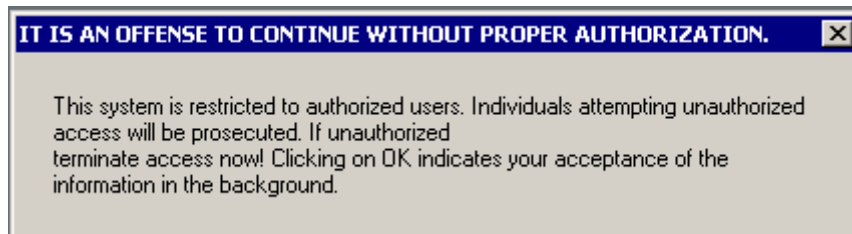
27

IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION.

This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. If unauthorized
terminate access now! Clicking on OK indicates your acceptance of the information in the background.

Figure 22: logon banner

7.3. Evaluation of the Group Policy

According to the functionality tests performed, the defined policies have raised up the security level of the infrastructure without altering system functionalities. Of course, the only the service offered has been tested and all administrative tasks that must be performed on the servers have not yet been tested with different privileges according to the role. The policies applied are maybe to strict. Full tests of the services as well as of the administrative tasks should be done in order to state that a policy is not too strict.

On the other hand, it has been discovered that the policies applied were not strong enough regarding the NTFS rights that are not addressed. New policies should be defined related to the web server running that put the correct permissions, of course still applying the privilege minimum principle.

8. Audit plan

Auditing is an important part of information security. Everybody is speaking about it, but only a few percentages of the companies are actually treating the entire generated events correctly. The level of auditing and the response action of some kind of event always depend on the security levels that want to be achieved. As stated in the previous chapter, even in a single company we can have various auditing level depending on the systems importance. It is not easy to determine what to audit. To help define the level required, it is important to remember the goal. Here are the functions that should be offered by an auditing system:

- First, this is the worst case scenario where nobody wants to be faced with, however planning and preparing it is very important. Auditing system must collect the proof of evidence in the case a security incident has occurred. There is nothing worst than having been compromised with no clue about what was changed and occurred. There are also some legal issues that require some kind of auditing on various systems.
- Preferably an auditing system should alert when something is going wrong in order to react with appropriate responses. This is actually what is offered by a lot of host based Intrusion Detection System (knowledge-based) whose task is to monitor event logs and provide a passive or

28

active response. By developing a correct auditing plan you can have your own IDS at a lower cost!

- The auditing system role is to detect misconfigured systems that generate a lot of event even before you are being called by the helpdesk!
- An auditing system must allow having a global view on your network activities.
- The auditing system must not be an overkill of administration tasks. Automatic procedures must be implemented.
- Finally this is maybe the argument that could allow you to be given a budget to spend some money and times in auditing: to provide statistics report for your management. Who has never been asked for one?

An auditing system can collect events from various sources. The most common one on a Windows system is the event log, but we can also get events from various application log files, from the registry and others. Depending on the configuration, some auditing events will be automatically created by the operating system or by an application, but there are also lots of events that need to be gathered.

8.1. Auditing models

Various theories are discussed about the ideal auditing system, but it is generally agreed by all parties that a centralized treatment of audit events can help and improve the responses actions. Advanced techniques like event correlation can be performed but are not discussed deeply in this paper. Correlation of events can for example allows you to be alerted only if event A occurs after event B in a five minutes time slot. You can benefit from correlation by reducing the number of alerts and give them more importances. This technique is used by the Intrusion Detection Systems in order to reduce the number of false positive alerts. Taken the hypothesis there would be a common centralized audit repository were the events would be stored and treated, there are two different models that can be followed:

- The pull model
- The push model

The pull model means that the centralized auditing systems has to contact each system to be audited in order to get the relevant information that will be stored and treated in the centralized repository. Issues with this model are:

- An up-to-date inventory of all systems to be audited needs to be maintained. This is quite an easy task for all the domain members as the AD can inform you, but don't forget you will have standalone servers and non windows systems. In any case, the AD repository is an excellent start for windows systems.

29

- As this model does not support real time auditing, there is a chance that an attacker has already deleted the proof of evidence. Thus you will not know that your system has been compromised.

The push model means that every event generated is directly sent through the network to the central repository. The major advantage is that even if your system gets compromised, there is a chance for you to notice it because the attacker is not yet in possession of your auditing system. Of course, this model does not prevent an attacker to flood your centralized system once a compromised system is under his control! Such flooding aims to confuse you with the high number of alerts generated and thus reduce your efficiency by doing your job much more complicated and time consuming.

8.2. Auditing Strategy adopted and planned

In this section an audit plan for SANS and GIAC network is presented. The windows security event log and the verification of the patches applied are discussed below.

In order to treat different kinds of events, an application has been developed that can take events from a text file or directly from a SQL database. Up to now the treatment of the event is run each hour and can run different kind of responses based on the events that occurred. The responses rules are currently based on a simple pattern matching. There is no flag that can be set in order to determine that there is an action if event B occurs after event A. This is something planed.

Scripts have been created in order to collect security event log information. These scripts are using dumpel.exe (8) from the resource kit which allows getting event log information from local and remote machine. Thus the pull model is adopted. The role of the scripts is to import the event log into an SQL database where the application is producing reports and adequate responses. The development has been stopped in order to first see the capabilities of Microsoft Auditing Collection Systems (MACS) that will probably be integrated in the Windows Server 2003 SP1.

MACS beta2 (9) has been installed on a SANS testbed. MACS is composed of three components: an agent, a central collector and a SQL databases. The agents need to be installed on each system to be audited. This can be done either manually or through a GPO. Once installed the agent is a windows service stated automatically on the system and will send the entire security event log to the collector. The agents and the collector can communicate across forests. In this beta version, collectors are found based on a SRV record (_adtserver). The collector also consists of a windows service. Figure 23 represents those services.

Figure 23: MACS agent and server Services

During the installation of the Collector, the SQL database is configured. It consists of several tables that will contain each event log (Figure 24)
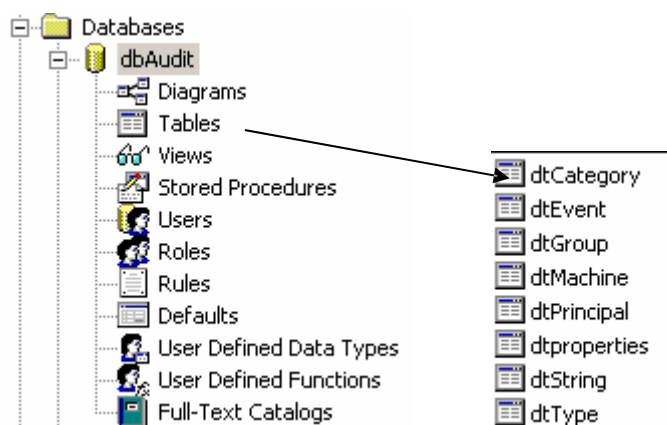

Figure 24: SQL dbAudit database and Tables

The agent has been installed on a server cg5.chicago.sans.org and security event log generated with a success logon from cg6.chicago.sans.org. Of course, it is possible to see the event in the local security log of cg5 (Figure 25). Thanks to the date in which the event occurred, it has been possible to see the corresponding entry in the SQL database. The table dtEvent contains "CreationTime" column (Figure 26). Having a look on the other tables, especially the dtString, it has been possible to check that this was really the corresponding entry. The event have been generated on cg5 at 18:00:11 and received by the collector at 18:00:19.
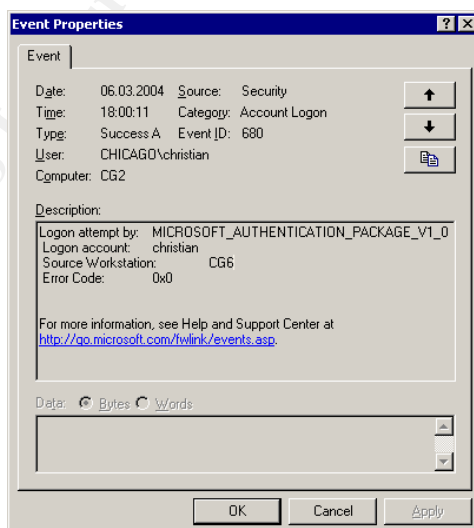

Figure 25 Local security log of CG5: Account Logon from CG6

31

Id	Event	SequenceNo	TypeNo	CategoryNo	CreationTime	CollectionTime	AgentMachineId	AuditMachineId	SourceId	UserId	PrimaryUserId
7695	540	400	8	2	06.03.2004 18:00:11	06.03.2004 18:00:19	1	1	2	8	3

Figure 26 MS SQL database, dtEvent table

This current beta version only collects event logs, and no further automatic treatment is possible out of the box depending on the events generated. To the knowledge of the author, there is no documentation describing the structure of the SQL database, or the predefined views. This version will certainly be completed and it has been decided not to spend too much time in reverse engineering this application. The Service Pack 1 for windows 2003 should be put on the market in the middle of 2004. This will be the time to evaluate it closer, and to see if it can fulfill the need of the SANS infrastructure in terms of functionality and bandwidth issues. SANS administrators have decided to wait for the next release.

Here are the minimum functionalities that the SANS administrators are expecting from the events treatment:
- Classification possible of the events based on various levels
- Different responses possible depending on the classification. Basically, send an email, a pager message; trigger a custom scripts or just logging.
- Possible integration of other event sources with a predefined format

The typical events that are going to produce an immediate response are the unsuccessful application of a GPO, a server shutdown, computer resources limits, new application installed and failed privilege used.

Collecting and analyzing events logs are an important task which has to done to monitor what is occurring on the systems, but this is not enough. You also have to make sure that your servers and workstations remain secure as you go forward in time. A patch management strategy needs to be defined and implemented in every windows network. New vulnerabilities are discovered each days and this is the reason why it is so important to have your systems up to date with the recent patches. Don't blindly rely on firewalls and access control lists. These are important for the overall network security, but you have to apply security in depth, by maintaining your operating systems and applications up to date. Patch management can be implemented in various ways using a SUS server (13), third party software or others. This is not discussed in this paper. What is important is that this has to be done and verified.

The verification of systems patch level is part of the auditing system. Microsoft Baseline Security Analyzer (14) has been installed and runs periodically in SANS network. It is run in hfnetchk mode using the AD databases and produces a text file that is imported into the auditing application for analyzing and alerting. Using MBSA in conjunction with a SUS server, allows you to audit only the patches that have been applied by a security administrator. Such function can also be implemented on the application level of your home made auditing systems.

32

Other information like installed programs, listening port, anti-virus updates, ACL with everyone permissions, alternate data stream files list and others need to be collected and analyzed by your collecting systems.

The next step once the window auditing system is in place is to integrate it as much as possible with other auditing systems, in order to get a global view on the entire network security of your company.

9. Conclusion

Interaction capabilities between various windows AD domains have been presented in this paper. Domains and Forests design are important issues that need to be addressed for each Windows network. Roles and responsibilities definitions are one of the key success while speaking about security and access right. These are important factors to consider in the design of Windows security architecture. Many security mechanisms depend on correct access rights and are only worth implementing if the below level is set up correctly.

The applications integration process, in a single client as well as in multi clients environment, needs to be closely followed in terms of security. Once the applications are installed and running it is more difficult and often too late for any modifications. Some recommendations about the sharing of resources have been proposed and should be followed.

The Group Policy Object is a toolkit that each security and system administrator needs to be comfortable with. It provides extensive capabilities because almost each configuration parameters can be set with a GPO. Sample configuration based on the Microsoft High level recommendation have been presented, discussed and applied into a testbed environment with success. GPO helps a lot in implementing the global organization security policy and are powerful

Security is a process that involves techniques, people and procedures. Auditing is a big part of the security measures that need to be addressed and implemented in order to maintain and control the system security level. Auditing need constant development based on the new technical and business requirements. Auditing can help to identify weak points and determine points to react on. After this step has been identified, a procedure must be in place that can be followed to solve this problem. Patch management is one of this issues that has grown and needs to be addressed clearly

Finally I want to recommend the SANS Securing windows track to anyone involved in securing a windows security infrastructure. This class and documentations cover a lot of aspect of windows security with lots of value added.

33

10. References

1. GCWN practical assignment, 2004:http://www.giac.org/GCWN_assign_32.php

2. Mike McCabe practical, 2004:
http://www.giac.org/practical/Mike_McCabe_GCNT.doc

3. Microsoft TechNet, Understanding User and Group accounts, 2004:
http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/07w2kada.mspx

4. SysInternals Utilities, 2004: http://www.sysinternals.com/win9x/98utilities.shtml

5. NSA Operating System guidelines, 2004:
http://www.nsa.gov/snac/downloads_os.cfm?MenuID=scg10.3.1.1

6. Microsoft Solutions for Security, Windows Server 2003 Security Guide, 2004:
http://www.microsoft.com/downloads/details.aspx?FamilyID=8a2643c1-0685-4d89-b655-521ea6c7b4db&displaylang=en

7. Microsoft, Threats and Counter measures: Security Settings in Windows Server 2003 and Windows XP, 2004:
http://www.microsoft.com/technet/security/topics/hardsys/tcg/tcgch00.mspx

8. Windows Resource Kit, Dump Event Log, 2004:
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp

9. RFC 1157, A Simple Network Management Protocol, IETF 2004:
http://www.ietf.org/rfc/rfc1157.txt?number=1157

10. RFC 2271, An Architecture for Describing SNMP Management Frameworks, IETF 2004: http://www.ietf.org/rfc/rfc2271.txt?number=2271

11. Windows Management Instrumentation Download, microsoft, 2004:
http://msdn.microsoft.com/library/default.asp?url=/downloads/list/wmi.asp

12. Microsoft Windows Server 2003, Beta Release: Microsoft Auditing Collection System (MACS) Planning and Deployment Guide, Jen Bayer, June 2003

13. Microsoft, Deployment of the SUS components
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dmebh_sus_vtzp.asp

14. Microsoft Baseline Security Analyzer, 2004:
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

15. SANS Institute Track 5 – Securing Windows, 5.1 Windows 2000/XP/2003 Active Directory, Jason Fossen

16. SANS Institute Track 5 – Securing Windows, 5.2 Windows 2000/XP/2003 Group Policy & DNS, Jason Fossen

17. SANS Institute Track 5 – Securing Windows, 5.6 Windows 2000/XP/2003 Scripting for Secrurity, Jason Fossen

35