



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>

SANS Co. and GIAC Enterprises Merger

Domain Design, Security Policy and Audit

Pierre Lafortune
GCWN Practical Assignment
Version 3.2 – Option 1
April 28, 2004

Table of contents

1	Introduction	4
2	Domain Design.....	5
2.1	SANS Co overview	5
2.2	SANS Co. network design.....	5
2.3	SANS Co. AD Infrastructure and AD Design.....	6
2.3.1	SANS Co. Active Directory structure	6
2.3.2	SANS Co. Active Directory OU design.....	7
2.3.3	Active Directory Roles and Responsibilities.....	9
2.3.4	SANS Co other security aspect	13
2.4	SANS Co Web Server.....	13
2.5	GIAC Enterprises AD infrastructure	16
2.5.1	GIAC Enterprises' overview	16
2.5.2	Description of GIAC Enterprises	16
2.5.3	GIAC Network Design.....	16
2.5.4	GIAC Active Directory Design.....	17
2.6	Companies Merging.....	18
2.6.1	Physical locations	18
2.6.2	Network modifications.....	18
2.6.3	Web Servers Integration	19
2.6.4	Active Directory Structure Integration	20
2.6.5	Active Directory OU Integration	22
3	Security Policy and Tutorial.....	23
3.1	Security Policy Design	23
3.2	Application of Group Policy Objects	27
3.3	Group Policy Maintenance	30
3.4	Testing the Policies Security Settings	31
3.5	Testing the System's Functionality.....	39
4	Auditing	41
4.1	Events to audit	41
4.1.1	Logon events	42
4.1.2	Account logon events.....	42
4.1.3	Account Management	43
4.1.4	Object access events.....	43
4.1.5	Directory Service Access	44
4.1.6	Privilege use events.....	44
4.1.7	Process tracking events.....	45
4.1.8	System events	45
4.1.9	Policy change events	45
4.2	Auditing Practices	45
4.3	Monitoring and Auditing Security Events	46
4.4	Event Logs Management	51
4.5	Critical Components.....	51
5	References.....	53
6	Appendix A.....	54

7	Appendix B.....	57
8	Appendix C	58
9	Appendix D	61

© SANS Institute 2004, Author retains full rights.

1 Introduction

This document is a practical assignment for the SANS GIAC Certified Windows Security Administrator (GCWN) certification. It is based on two fictional companies, SANS Co. and GIAC Enterprises and it will describe the merger of both companies. This assignment consists of three parts:

1. Domain Design

SANS Co and GIAC enterprises have decided to merge their companies in order to expand their markets and to consolidate operations. Both companies have an extensive Active Directory so migrating one forest to another was not considered an option. Design of the GIAC Enterprises network and infrastructure was developed in a previous practical assignment by Brian Rudzonis

(http://www.giac.org/practical/GCWN/Brian_Rudzonis_GCWN.pdf).

The mandate I have been given is to develop the trusts between these two companies which will ensure interoperability, consolidate IT overhead and allow existing customer to deal with both parts of the new company seamlessly via the web.

2. Security Policy and Tutorial

Design a group policy that must encompass the needs of both companies as describe in part 1. The Group Policies will be applied and tested to demonstrate the results of the implementation.

3. Audit

This section will reveal which auditing strategy SANS Co has deployed to make sure their Active Directory is secured and remains secured. It also contains the gathering and management of Event Logs, performance data and the checking of critical settings.

2 Domain Design

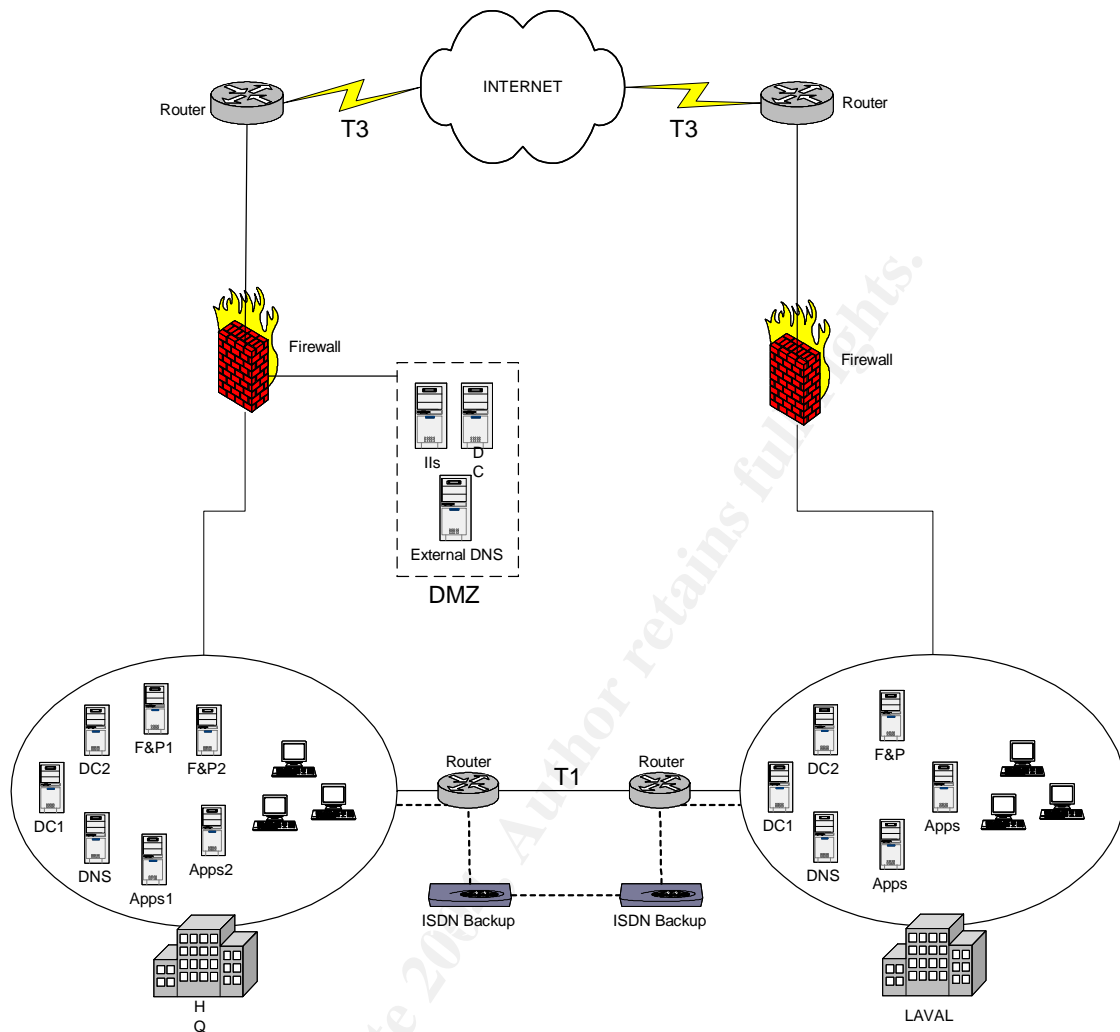
2.1 SANS Co overview

SANS Co, founded in 1994, is an enterprise that is well established in the software development. SANS Co's headquarter is located in Montreal (Quebec, CANADA) and has a remote site in Laval (Quebec, CANADA) where the developers are located. The CEO recently decided to merge with a company called GIAC Enterprises, which makes most of his business in the USA. Both enterprises see a great North American exposure and opportunity with this merger.

2.2 SANS Co. network design

The SANS Co's network is quite simple but is very efficient. Offices are connected via a T1 (1.544 Mbps) wide-area connection. In case of a wide-area provider failure, connectivity relies on the use of an Integrated Digital Network (ISDN) for backup purposes. The demilitarized zone (DMZ) contains the IIS server, a Domain Controller and an External DNS server and is connected to the Internet via a DS3 wide-area connection (44.736 Mbps). The use of a DMZ permits the egression of the Internet into the private network and still maintains the security of the network¹. The DMZ is located in the HQ building.

¹ Microsoft Corporation. Determining Network Connectivity Strategies.
<http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/deploy/part2/chapt-7.mspx>



2.3 SANS Co. AD Infrastructure and AD Design

2.3.1 SANS Co. Active Directory structure

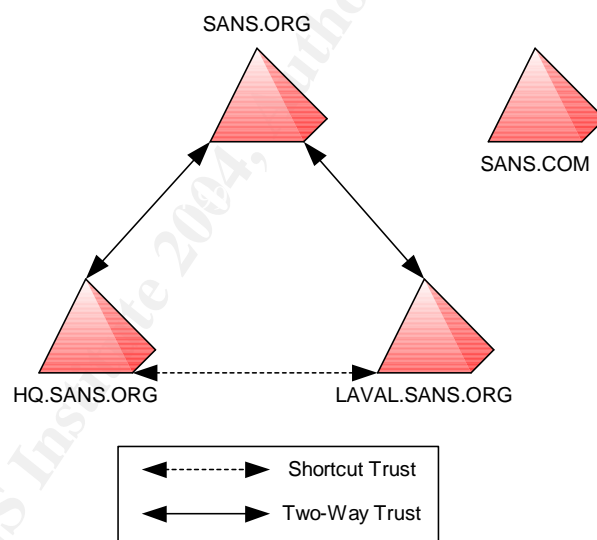
The Active Directory structure of SANS Co. consists of a single forest with four domains. SANS Co opted for a multiple domains design because of the following reasons:

- Reduces replication traffic and maintains network performance. Only the changes to the global catalogue server, configuration information, and schema, are replicated.
- Maintain separate and distinct security settings for different domains.
- Separates administrative control. Each domain may have its own administrators.

The empty root domain model was selected by SANS Co. It is in the company's objective to expand their activities all around the world. Having this model, it will allow them the flexibility required when facing countries' laws, languages, geographical, political or cultural issues differences. This will permit to set different settings through domain GPOs such as keyboard layout (French, English or bilingual), and regional options (numbers, currency, time and date formats) for each geographical domains.

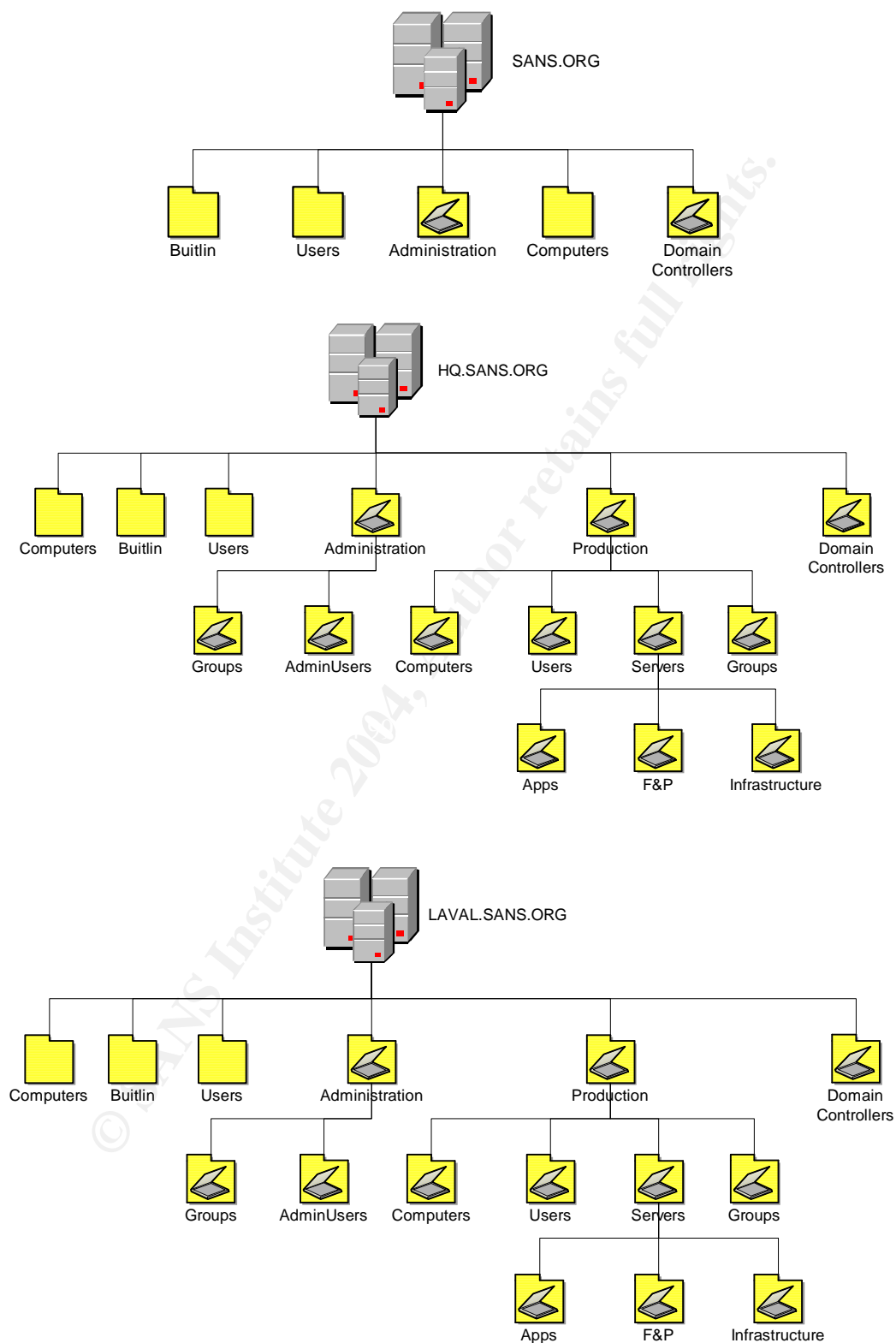
All domain trusts in Windows 2000 forest are transitive. Upon their creation, child domains, `hq.sans.org` and `laval.sans.org`, that is in a remote site, a two-way transitive trust was automatically created. Also, two-ways transitive shortcut trusts were created between `hq.sans.org` and `laval.sans.org`. Even though these shortcuts don't add any new trusting relationships; they improve authentication performance and also reduce the flood of Kerberos traffic root-level Domain Controllers would have to process otherwise.

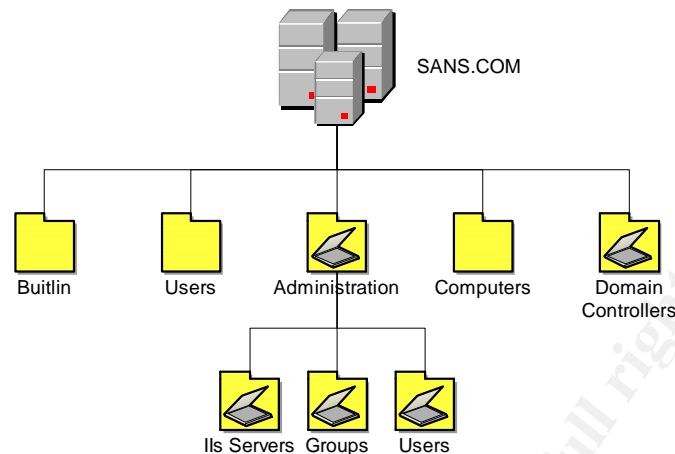
The domain `SANS.COM` hosts the web server environment. For security reasons, no trust were established between `SANS.ORG` and `SANS.COM`.



2.3.2 SANS Co. Active Directory OU design

It has been decided that the root domain, `sans.org`, will be empty. Only the two organizational units (OU), Domain Controllers and Administrators will reside on it. The containers Users, Computers and Builtin are present but not used in `sans.org`. SANS Co AD architects decided that all child domain in `sans.org` forest have common organizational units. This will make the administration of the Active Directory much easier.





2.3.3 Active Directory Roles and Responsibilities

SANS Co takes their Active Directory structure and management very seriously. A role and delegation model was implemented to make sure that IT people perform their tasks with sufficient rights and no more.

The following correlates Microsoft Active Directory (AD) tasks and responsibilities to the various SANS Co roles and teams in order to better manage Active Directory and its related services.

The majority of the teams and roles represented here currently exist at SANS Co. However, there are some new roles that will need to be delegated. Also, some of the existing roles and responsibilities will need to be adjusted and refined. In some cases, top administrative rights that were granted to users in the past will need to be curtailed.

2.3.3.1 Active Directory Design and Security

It is imperative to secure this environment as much as possible. This can be successfully done but SANS Co security must take an active role in vigorously restricting the membership of enterprise critical groups such as Enterprise Admins, Schema Admins and Domain Admins. No employee should ever be permitted to work on a daily basis with these elevated permissions. Enterprise Admins and Schema Admins should have no active members and Domain Admins should have a bare minimum of active members (two to four accounts used for special administrative jobs).

Guiding principles

- Users need all the rights and permissions necessary to effectively do their jobs, but nothing more.
- Security and operations both exist for the productivity of the enterprise. Where differences exist, between security measures and technical limitations, the resolution must support the ultimate goals that all SANS Co departments value and support. In some cases this means granting more rights and permissions than necessary to accomplish a task and in others less to protect the enterprise from unnecessary risks.
- The role and delegation model will apply Microsoft and industry best practices whenever possible.
- The delegation of security rights and permissions in AD, servers and workstations should be controlled centrally.
- Users who have administrative rights in AD will have two users' accounts: a regular user account and an administrative one. Users are expected to logon to their PCs with their regular account and run the tools in the context of their administrative accounts.
- When users can administer AD or servers through desktop tools they should do so. Logon locally rights and Terminal Session rights on servers should be limited to those that absolutely need those rights. Microsoft's Management Console (MMC) toolset permits almost all AD administration and most server administration to be done directly from the desktop.

Team Role Delegation Model

Help Desk (Level 1)

"Help Desk" team members are the first level support for user and computer related issues in Active Directory. They are responsible for unlocking user accounts and resetting users' passwords. They can also manage print queues to resolve blocked print jobs. Since they are responsible 7/24 for desktop support, they also do some initial problem identification and troubleshooting through either Remote Assistance (user session) or Remote Desktop Connection (local administrative session) tools. If a user or computer account needs to be deleted or disabled they must escalate the issue to a higher level. They also validate the contents of user folders without being able to open files.

Sub-Role « Help Desk Seniors »

Members of the Help Desk staff who are frequently granted special access permissions which are not granted to regular Help Desk personnel. Permissions granted are primarily file and folder permissions and not Active Directory related.

Help Desk L2 (Level 2)

“Help Desk L2” team members give level 2 support for user and computer related problems in Active Directory. They are also responsible for all non-administrative user and group security management in AD. They can create, disable and manage user accounts but the Security team is responsible to move, enable/disable and delete the accounts. They can create, delete and manage all “Production” groups which grant folder, file and resource access at SANS Co. They cannot manage administrative user accounts and groups. They can create and delete computer accounts in AD but not server accounts.

End user support includes creating and deleting printers, managing print queues and restarting the Print Spooler service on print servers. They create and delete files and folders and grant the necessary permissions to groups and users. As a part of user account management they can create, modify and delete login scripts. On certain occasions they also restore users’ personal drives. As a part of their desktop support they can do Remote Assistance (user session) or Remote Desktop Connections (local administrative session). The team can create and delete FTP site directories but must ask Security to create the FTP generic accounts. They should be able to manage all their responsibilities through desktop administrative tools on Windows 2000 or XP.

Security (Level 3 Security Support)

Security team members for Active Directory are fully responsible for all security issues related to user, computer, server, and service accounts, group management, folder and file access, printer security, security logs, and Group Policies. They are responsible for all administrative accounts and roles in AD. They need access to all servers managed by SANS Co.

AD Forest Team

The AD Forest Team is responsible for the Domain Admins, Enterprise Admins and Schema Admins roles in the root domain of the SANS.ORG forest. They are responsible for domain and forest management (Trusts, Sites and Subnets, Domain Controller deployment, Top Level OU creation, Root DFS and Link configuration, Default Domain and DC GPOs, Schema modifications, Role definitions, and expanding the SANS.ORG forest). They are responsible for all Active Directory changes, updates and hot fixes. They are also responsible for the Default Domain Policy and Default Domain Controller Policy.

Server Team - (Level 3 Server and Application Support)

Server administrators are responsible for the installation, integration, support and evolution of the server operating system and the underlying hardware. They may also be responsible for the basic application infrastructure and installation but not necessarily the procedures, configuration and management of the application. They need administrative rights and terminal server access to all servers they support. They work with Security and the AD Forest Team to deploy or remove servers and domain controllers. Security is applied as defined and prepared by the Security Team. Rights to do Domain Controller promotions and demotions are granted on a temporary basis by the AD Forest Team. They are responsible for WINS administration.

Application Servers

Application servers vary greatly in their requirements and the roles necessary to manage the application. Some vendors require the application administrator to also be an administrator of the server. Some require terminal server access for users while others don't require any user access of any type. Therefore, application server roles need to be managed on a server-by-server or application-by-application basis. The following serves as a guideline in granting rights and permissions to application servers.

- Objective: Do not grant Administrators and Server Operators rights if not absolutely necessary. The Server Team is responsible for server administration.
- BuiltIn Local Groups should be centrally administrated by GPO restricted group policy so that the Security team remains in control of who has access to the server and its applications.
- Services can be configured via GPO to grant necessary permissions to groups to avoid granting full administrative rights.
- Local User Rights can be configured via GPO in same way (e.g. Logon Locally)

DNS

In the AD Role delegation model this team is responsible for administering the DNS service on Windows 2000 servers. They can stop, start and manage the DNS service and manage the zones. They are responsible for maintaining and managing the AD service resource records.

Security DNS

This team is responsible for creating and troubleshooting DNS host and pointer records and is not responsible for the DNS service.

External Technicians (Level 2 Desktop Support)

This team is responsible for desktop support and must have administrative rights and logon locally rights on all desktops. They need the right to join computers and servers to the SANS.ORG domains.

Wins Admins

The WINS Admins team members need to be administrators of the WINS servers. They are responsible for TCP/IP name resolution for NetBios applications.

WebAdmins

The WebAdmins team members need to be administrators of the IIS servers. They are responsible for all the tasks related to the web servers.

2.3.4 SANS Co other security aspect

Physical access restrictions are implemented and administered to ensure that only authorized individuals have the ability to access or use information resources.

- Physical access to the building and immediate surroundings of computer equipment is monitored and is restricted to individuals who require such access to perform their job responsibilities. Management approval is required before access is granted.
- A badge access control mechanism is used to restrict and record access to protected areas and authority to change physical access control mechanisms is limited to appropriate personnel.

2.4 SANS Co Web Server

Upon implementation of the Web Server, SANS Co's **Server Team** applied the following guidelines:

IIS O/S and domain membership

- O/S should be running at the latest version.
 - Windows 2000 at that moment.
 - Latest patch installed.
- Web Server should be on a DMZ and is not made a member of the domain in the inside.

- Web Server is on a DMZ and is a member of the SANS.COM domain. Even though IIS is usually serving its own application, it has been decided to add a Domain Controller in the DMZ. SANS Co is planning to add more IIS servers in the future and managing these IIS servers will be easier and security will be applied through the GPO.
- For security reasons, no trust was created between SANS.ORG and SANS.COM.

Network placement

- Always ensure that any public facing IIS server be placed in a DMZ.
 - IIS server was placed in the DMZ along with a domain controller and an external DNS server. (See section 2.2)

Remote administration

- All traffic between the web server and the management station should be encrypted through IPSEC.
- We should not trust Terminal Services by itself, use encryption.

Firewall access

- Block all access except TCP 80 or TCP 443 (SSL).
 - Port TCP 80 for **World Wide Web**, HTTP opened
 - Port 3389 for **Terminal Services** opened. (See LANguard report in section 4.5 Critical Components)

IIS installation

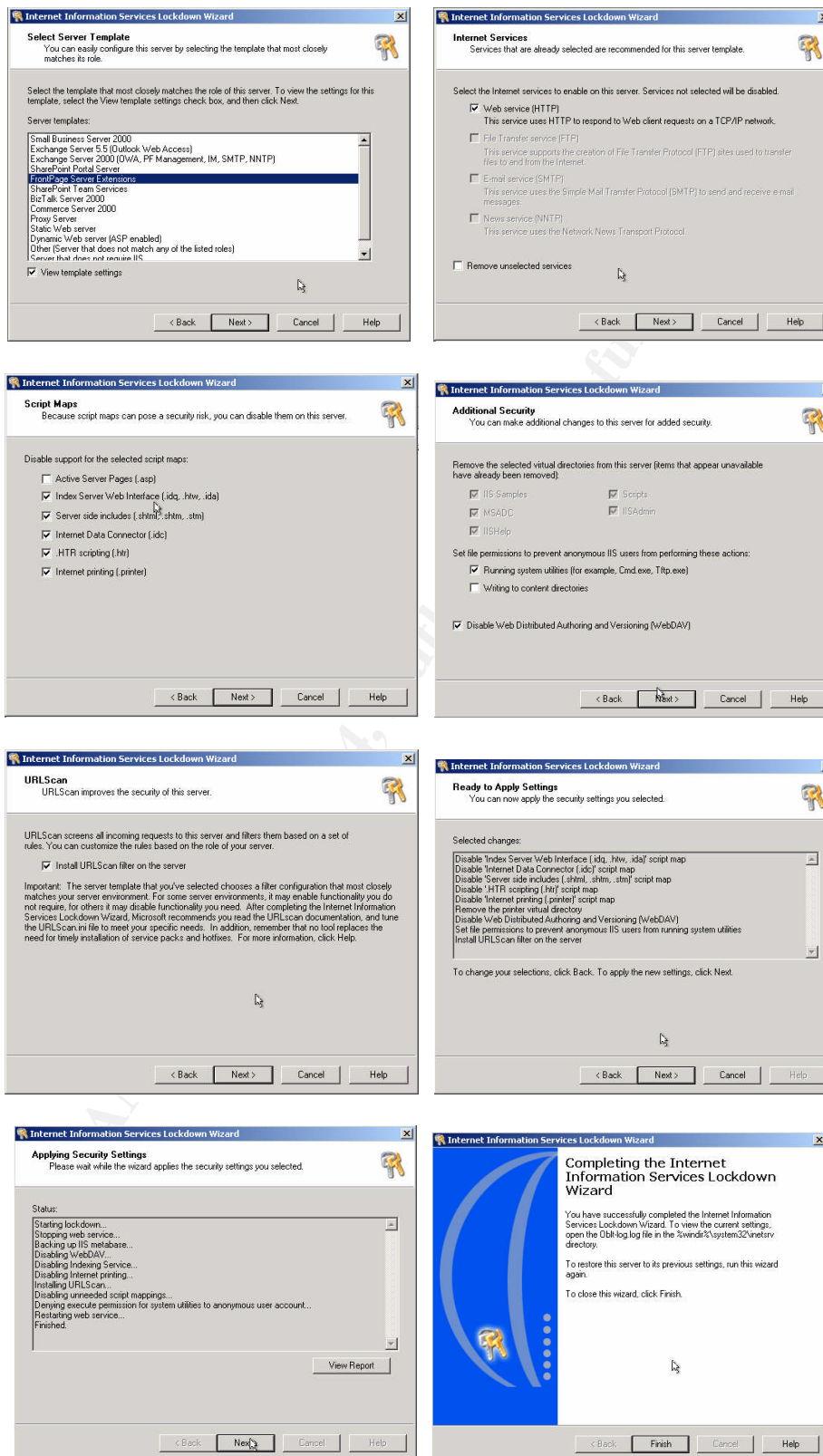
- When installing the different components, ensure that everything is unchecked except **Internet Information Services**.
 - Everything was unchecked except for **Internet Information Services** and **Terminal Services** that is needed for remote administration.
- Within **Internet Information Services**, click on details and uncheck every box except: **Common Files**, **Internet Information Services Snap-In** and **World Wide Web Server**.

IIS Lockdown Tool

IIS Lockdown Tool works by turning off unnecessary features, thus reducing attack surface available to attackers. ²

² <http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp>

Step-by-step of IIS Lockdown Tool.



2.5 GIAC Enterprises AD infrastructure

2.5.1 GIAC Enterprises' overview

The GIAC Enterprises' network and Active Directory infrastructure can be found in the practical assessment develop by Brian C. Rudzonis (http://www.giac.org/practical/GCWN/Brian_Rudzonis_GCWN.pdf). The following chapter will describe and highlight the parts of its design that are important and relevant to the issues of interoperability and consolidation.

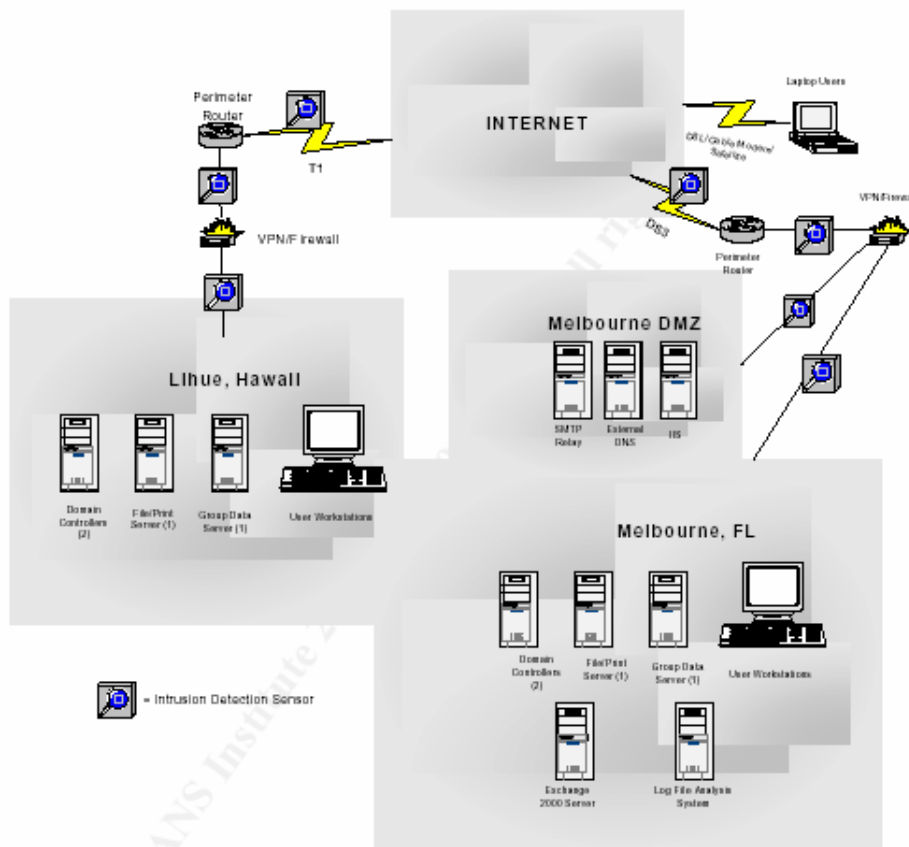
2.5.2 Description of GIAC Enterprises

GIAC Enterprises (GIAC) is a Delaware corporation, founded in 1999. The company produces and sales a test simulator with an excellent set of questions and learning tool for teaching appropriate topics.

2.5.3 GIAC Network Design³

GIAC network's sits on a single Windows 2000 domain that runs Active Directory in native mode. There are two sites, one in Melbourne (Florida, USA) and the other one in Lihue (Hawaii, USA). Both sites are connected to Internet, through a T1 in Lihue and a DS3 in Melbourne. Offices are connected through a VPN over the Internet. There is a Web server presence on GIAC's network and is the primary means for customers to download the software study tool product.

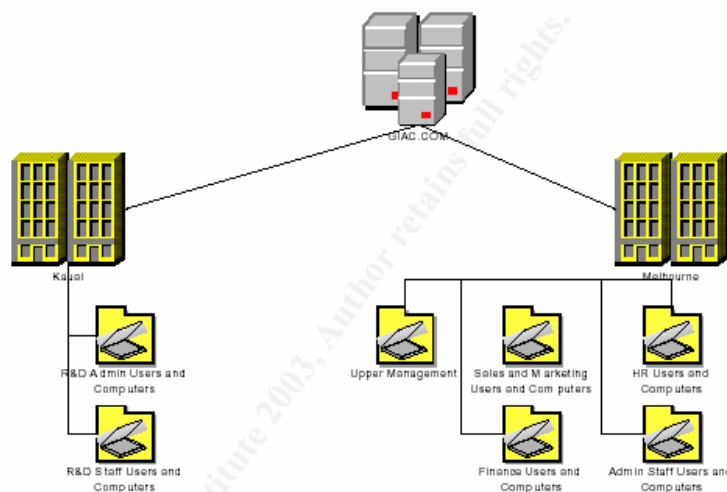
³ Rudzonis, Brian. GIAC Enterprises: Securing Windows 2000 Infrastructure Design. http://www.giac.org/practical/GCWN/Brian_Rudzonis_GCWN.pdf



2.5.4 GIAC Active Directory Design⁴

A single domain within a single forest was the choice of GIAC. Cost, simplicity and reduced overhead were the key elements in their decision. Within the domain, there are two sites. Melbourne, the first one, contains all the resources within this office. Kauai, the second site, contains the resources within this office.

⁴ Rudzonis, Brian. GIAC Enterprises: Securing Windows 2000 Infrastructure Design. http://www.giac.org/practical/GCWN/Brian_Rudzonis_GCWN.pdf



2.6 Companies Merging

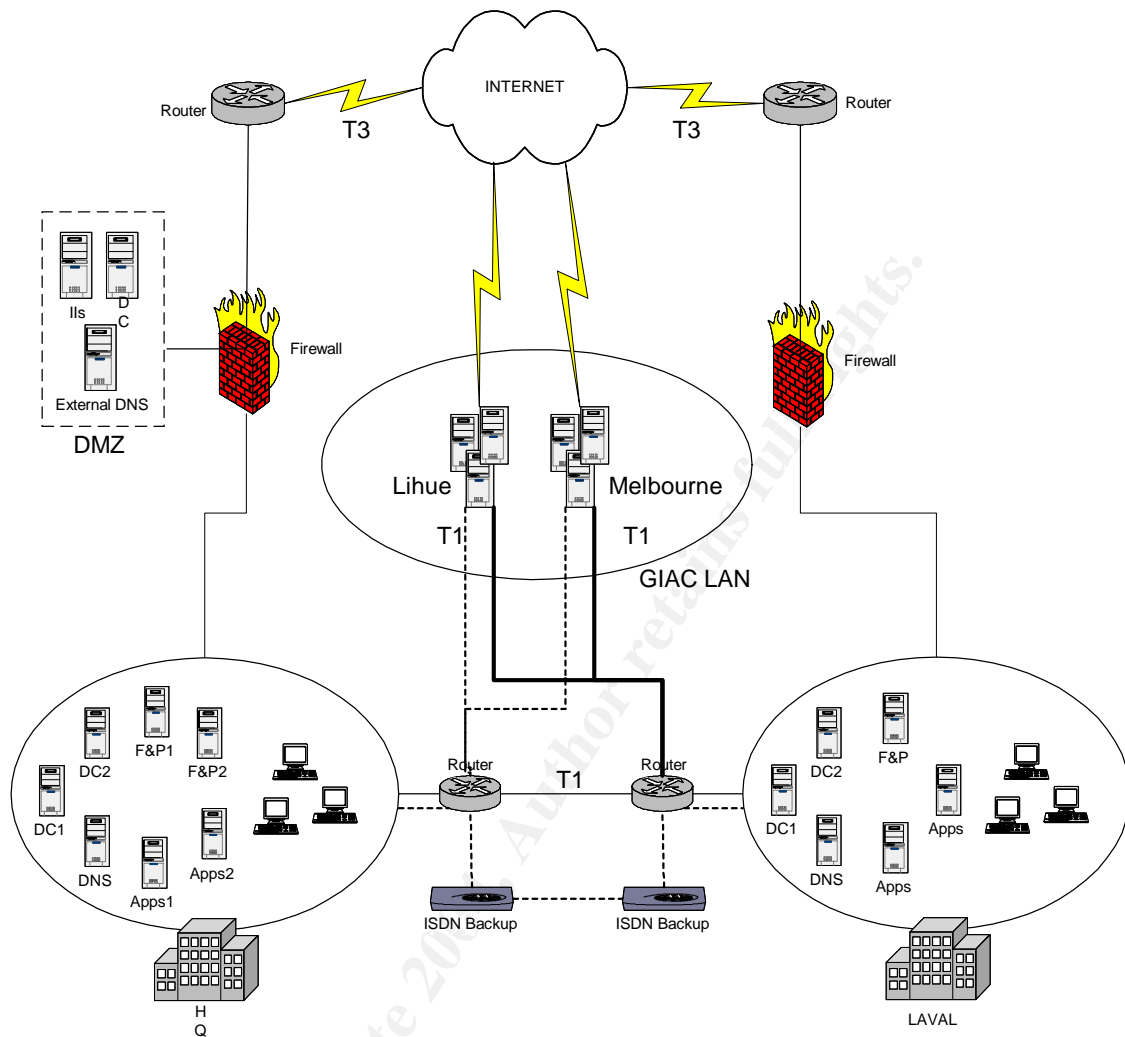
SANS Co and GIAC Enterprises merger will take place without any major changes. The merged company will operate under the new name, **S&G**. This merge will offer to the new merged company a great exposure in both Canada and the US.

2.6.1 Physical locations

S&G will not apply any changes on the location of the employees. Former GIAC and SANS Co will remain at their actual locations. This will facilitate the transition on a human perspective. Employees will not see and feel any differences and everything should be business as usual.

2.6.2 Network modifications

Both networks will maintain their actual topology. They will be connected via a T1 wide-area connection. This new configuration will permit to S&G to maintain efficient operation, interoperability



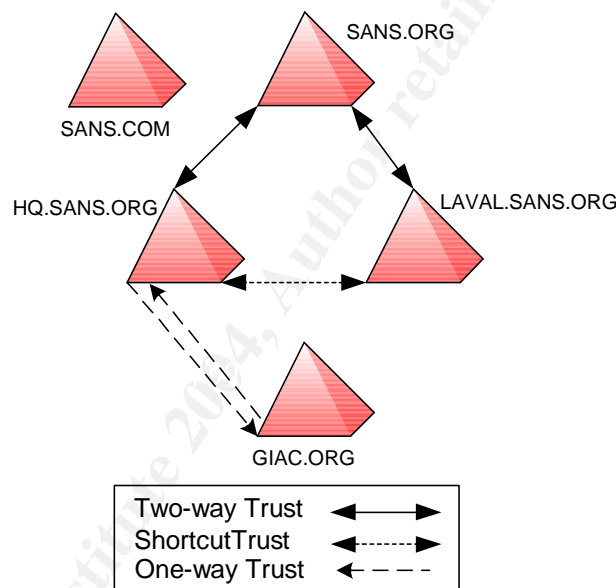
2.6.3 Web Servers Integration

Both companies' websites will remain, but will benefit from a major rebuild. They will have to make sure that products and services from one company is available on the other's website. It doesn't mean that they will have the same look, each website will retain his personal look and feel. Customers on the other hand will be able to review and buy products from any of the companies through either one of the website. IIS database will be replicated from one IIS server to another to make sure that both servers are identical and customers get the same information regardless on which site they visit. On an Active Directory point of view, the administration of GIAC web server will be very easy since it is a member of the GIAC domain.

2.6.4 Active Directory Structure Integration

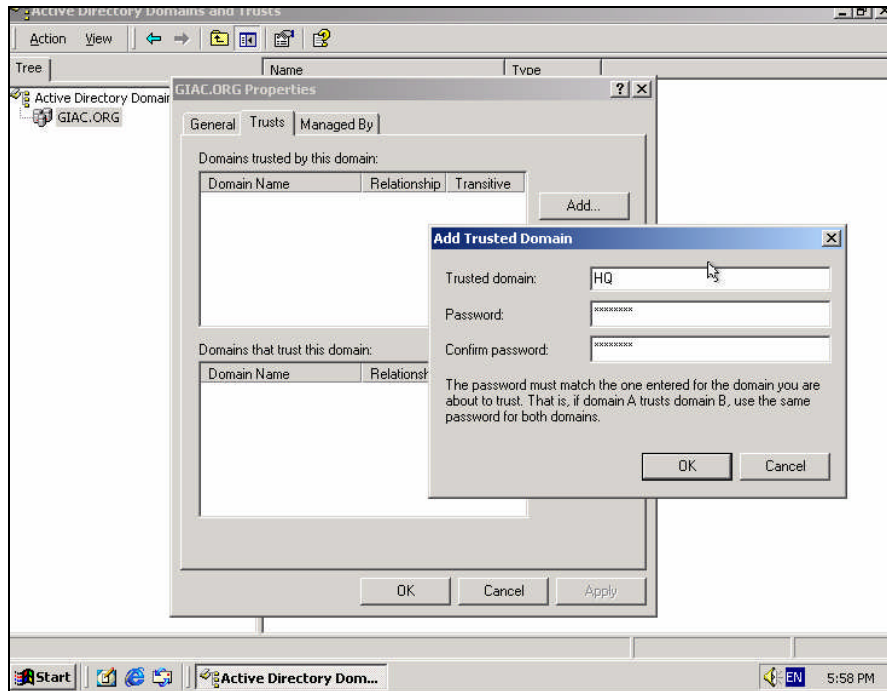
As shown below, two one-way non-transitive trusts were established between `giac.org` and `hq.sans.org`. With this type of trust, `giac.org` users will be able to have access to resources located in `hq.sans.org`, but will not be able to access the root domain `sans.org` nor `laval.sans.org` since the trusts are not transitive.

`Hq.sans.org` domain contains all the business related resources, such as HR and Management and they must be shared to the management people located in the GIAC domain. `Laval.sans.org` on the other hand contains all the developers resources and must be kept protected as much as possible. It is in S&G's projects to eventually share the resources between both groups of developers, GIAC and SANS, but until then it will remain out of GIAC's access.

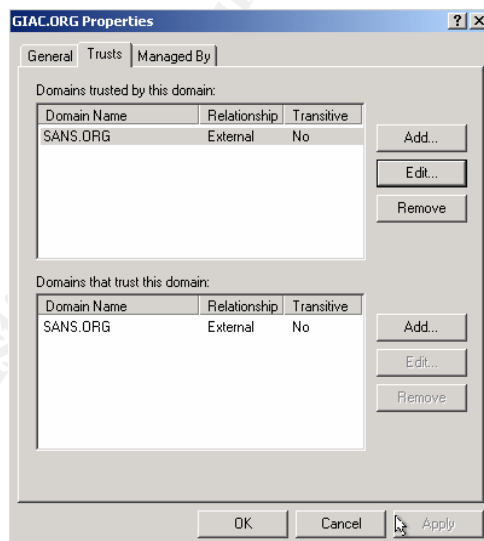


The external trusts were created using the **Active Directory Domains and Trusts** MMC. The following steps were completed:

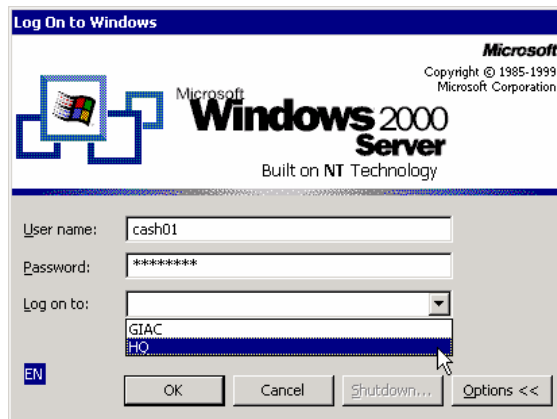
1. Right-click on the Domain you wish to create new trusts.
2. Click on Add in Domains trusted by this domain.
3. Enter the new trusted domain and password. Click OK.
4. Click on Add in Domains that trust this domain.
5. Enter the new trusted domain and password. Click OK.



6. The screenshot below shows that the new trust was created.



7. Repeat the same steps on the Domain you wish to create the two-way trust.
8. Next screenshot shows that we can connect to one domain with a trusted domain account.



2.6.5 Active Directory OU Integration

For the administration of both forests' OU, we will have to create global groups for cross-forest resource access and add these global groups to corresponding universal groups. Then create local groups with appropriate universal groups and apply security permissions to resources to provide cross-forest access.

3 Security Policy and Tutorial

S&G's domains require a set of Group Policies to help the Administrators to manage the environments in an efficient manner. Group policy for servers is a critical element of GPO design. A properly thought out configuration will harden security on the servers while still permitting the required access to resource. The easiest way to apply policies to servers is to divide them by function. All S&G's servers have a basic configuration that needs to be applied through the baseline policy. Then function servers would get a set of policies designed for them.

3.1 Security Policy Design

In order to ensure that all computers/servers are secured from internal or external attacks, settings must be applied using GPOs. S&G based their settings on the National Security Agency (NSA) recommendations⁵ and their specifics security requirements.

The following templates were used in the new merged company network.

SANS and GIAC OUs

Workstations
Member servers (other than IIS)
Web servers
Domain Controllers
Domain

Templates

W2k workstation.inf
W2k server.inf
Hisecweb.inf
W2kdc.inf
W2k Domain Policy.inf

The following group policy settings are applied across SANS.ORG, GIAC.ORG and SANS.COM.

Default domain policy **Account Policies**

Password Policy

Policy	Template Setting	Modified Setting
Enforce Password Policy	24 passwords	24 passwords
Maximum Password Age	90 days	90 days
Minimum Password Age	1 day	2 days
Minimum Password Length	12 characters	8 characters
Passwords Must Meet Complexity Requirements	Enabled	Enabled
Store Passwords Using Reversible Encryption For All Users In The Domain	Disabled	Disabled

⁵ NSA. Guide to Securing Microsoft Windows Group Policy: Security Configuration Tool Set. Version 1.1, January 22, 2002

Account Lockout Policy

Policy	Template Setting	Setting
Account Lockout Duration	15 minutes	60 minutes
Account Lockout Threshold	3 invalid attempts	3 invalid attempts
Reset Lockout Counter After	15 minutes	60 minutes

Kerberos Policy

Policy	Template Setting	Setting
Enforce User Logon Restrictions	Enabled	Enabled
Maximum Lifetime For Service Ticket	600 minutes	450 minutes
Maximum Lifetime For User Ticket	10 hours	5 hours
Maximum Lifetime For User Ticket Renewal	7 days	3 days
Maximum Tolerance For Computer Clock Synchronization	5 minutes	5 minutes

IIS Servers OU Policy Account Policies

Password Policy

Policy	Template Settings	Modified Settings
Enforce Password Policy	24 passwords	24 passwords
Maximum Password Age	42 days	90 days
Minimum Password Age	2 days	2 days
Minimum Password Length	8	8
Passwords Must Meet Complexity Requirements	Enabled	Enabled
Store Passwords Using Reversible Encryption For All Users In The Domain	Disabled	Disabled

Account Lockout Policy

Policy	Template Settings	Modified Settings
Account Lockout Duration	0 (administrator must unlock)	0 (administrator must unlock)
Account Lockout Threshold	5 invalid attempts	3 invalid attempts
Reset Lockout Counter After	30 minutes	30 minutes

IIS Servers OU Policy Local Policies

User Rights Assignments

Policy	Template Settings	Modified Settings
Access this computer from the network	Authenticated Users	Administrators SANSKOM\Backup Team
Backup files and directories	Not defined	SANSKOM\Backup Team
Log on locally	Not defined	Administrators SANSKOM\Backup Team
Shutdown the system	Not defined	Administrators

IIS Servers OU Policy Event Logs

Settings for event logs

Policy	Template Settings	Modified Settings
Maximum Application Log Size	Not defined	10240 kilobytes
Maximum Security Log Size	10240 kilobytes	10240 kilobytes
Maximum System Log Size	Not defined	10240 kilobytes
Retain Application Logs	Not defined	7 days
Retain Security Logs	Not defined	7 days
Retain System Logs	Not defined	7 days
Retention Method For Application Log	Not defined	By days
Retention Method For Security Log	Not defined	By days
Retention Method For System Log	Not defined	By days

IIS Servers OU Policy System Services

As recommended by Jason Fossen from the SANS Institute⁶, we should disable unnecessary services and subsystems.

⁶ Jason Fossen - 5.5 Securing Internet Information Server. Page 51.

Policy	Template Settings	Modified Settings
Automatic Updates	Not defined	Disabled
Alerter	Disabled	Disabled
Clipboard Server	Disabled	Disabled
Computer Browser	Disabled	Disabled
DHCP client	Disabled	Disabled
Network DDE	Not defined	Disabled
Network DDE DSDM	Not defined	Disabled
Remote Access Auto Connection Manager	Disabled	Disabled
Remote Access Connection Manager	Disabled	Disabled
TCP/IP NetBios Helper	Not defined	Disabled
Telnet	Disabled	Disabled

Logon Banner

S&G are using a logon banner when a user logs on their network. This could facilitate the company in sewing an employee or an external attacker that may have caused damages. The banner is written both in French and English since Canada is officially a bilingual country and many employees of the company are francophone.

«L'accès non autorisé au réseau de S&G ainsi que l'utilisation inadéquate de l'information de l'entreprise sont strictement interdit. Veuillez noter que vous êtes responsable de toute action posée. Celle-ci pourrait faire l'objet de suivi. ~///~ Unauthorized access to the S&G network and misusing company information are strictly prohibited. Remember that you are responsible for the actions performed and as such they may be monitored.»

Audit Policies

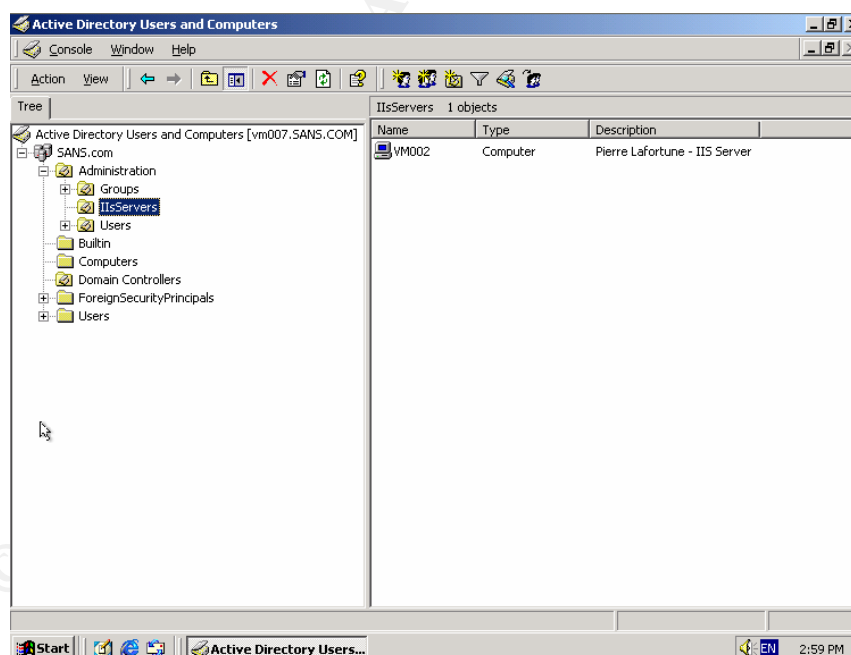
Once implemented, the number of events that policies are generating must be audited to ensure that the logs are not filling up too fast. S&G have decided to overwrite the events logs when they are full.

Policy	IIS Server	Domain Controllers
Audit Account Logon Events	Success, Failure	Success, Failure
Audit Account Management	Success, Failure	Success, Failure
Audit Directory Service Access	Not Defined	Success, Failure
Audit Logon Events	Success, Failure	Success, Failure
Audit Object Access	Failure	Failure
Audit Policy Change	Success, Failure	Success, Failure
Audit Privilege Use	Failure	Success, Failure
Audit Process Tracking	Not Defined	Not Defined
Audit System Events	Success, Failure	Success, Failure

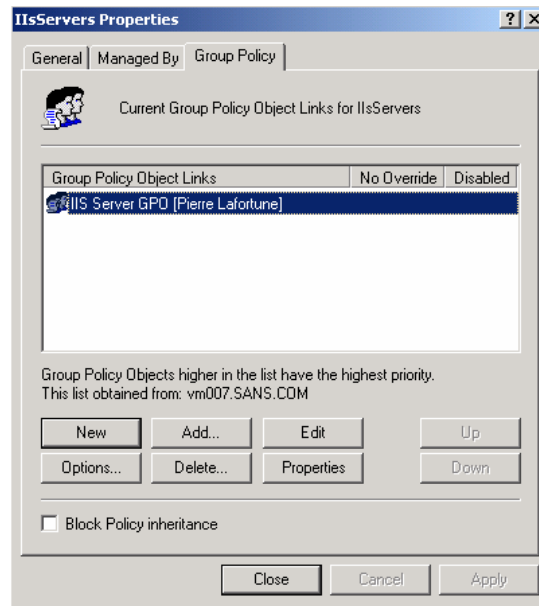
3.2 Application of Group Policy Objects

You must be connected on the SANS.COM domain controller to perform the following tasks:

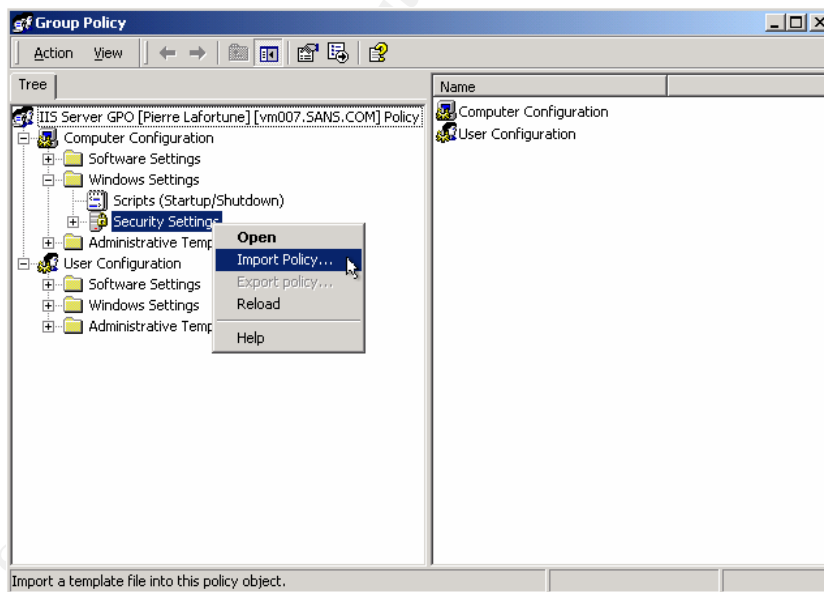
1. In **Active Directory Users and Computers**, right-click the **IIS Servers** OU, and then select **Properties**.



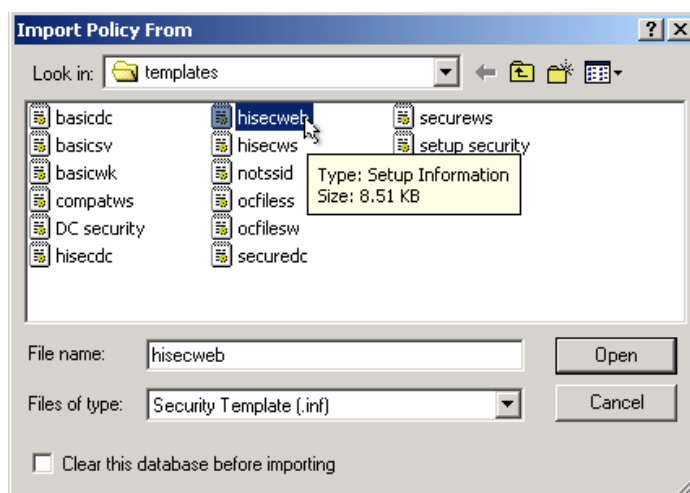
2. On the **Group Policy** tab, click New to add a new GPO.
3. Type **IIS Server GPO [Pierre Lafortune]** and press **Enter**.



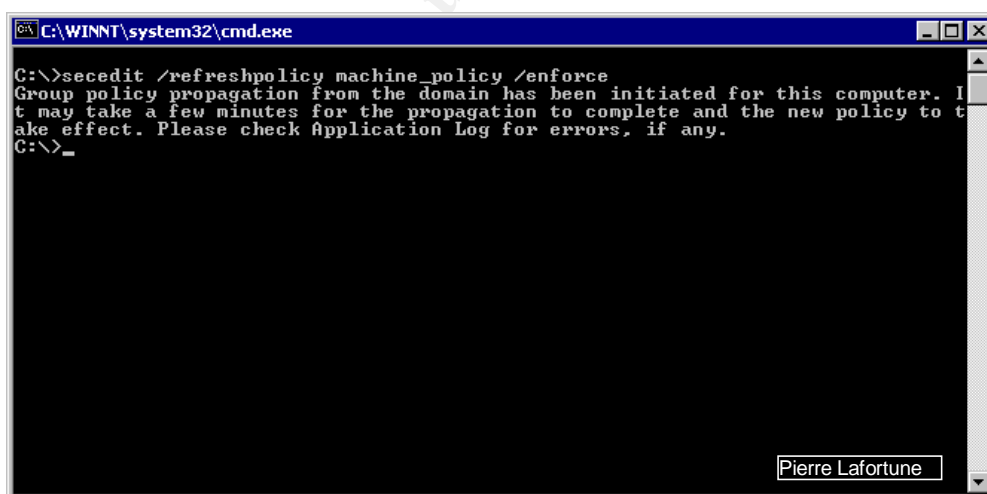
4. Select **IIS Server GPO [Pierre Lafortune]** and click **Edit**.
5. In the Group Policy Window, click **Computer Configuration\Windows Settings**. Right-click **Security Settings** and select **Import Policy**.



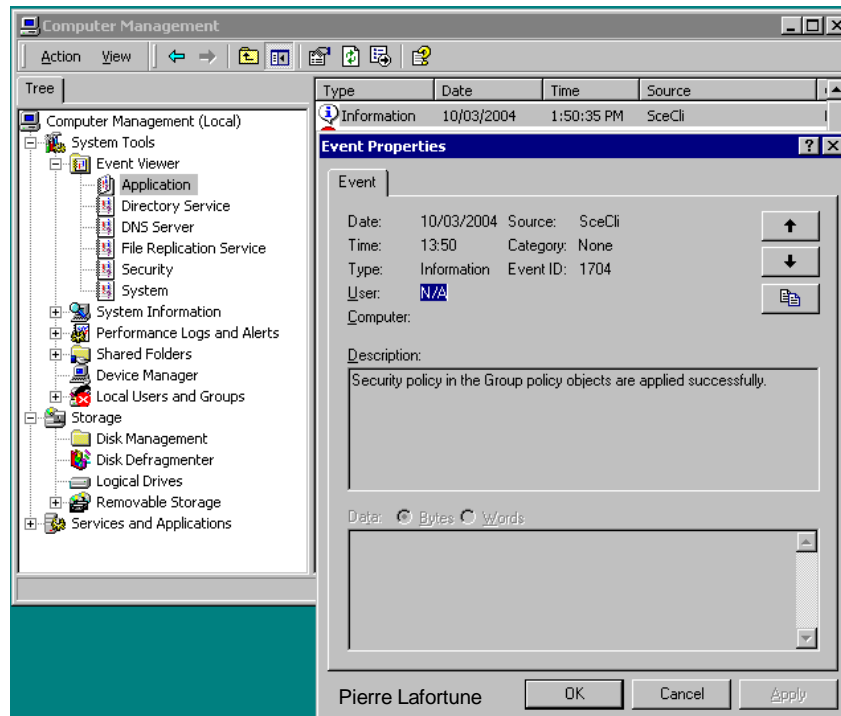
6. In the **Import Policy From** dialog box, from the **Security Template** folder, double-click **hisecweb.inf**.



7. Close the **Group Policy** that has been modified.
8. Close the **IIS Servers** OU Properties window.
9. Force the replication on the **IIS Server** so that the policy will be enforced by doing the following:
 - a. Open a command prompt and use the **Scedit.exe** command line tool to force the server to refresh the policy with the command:



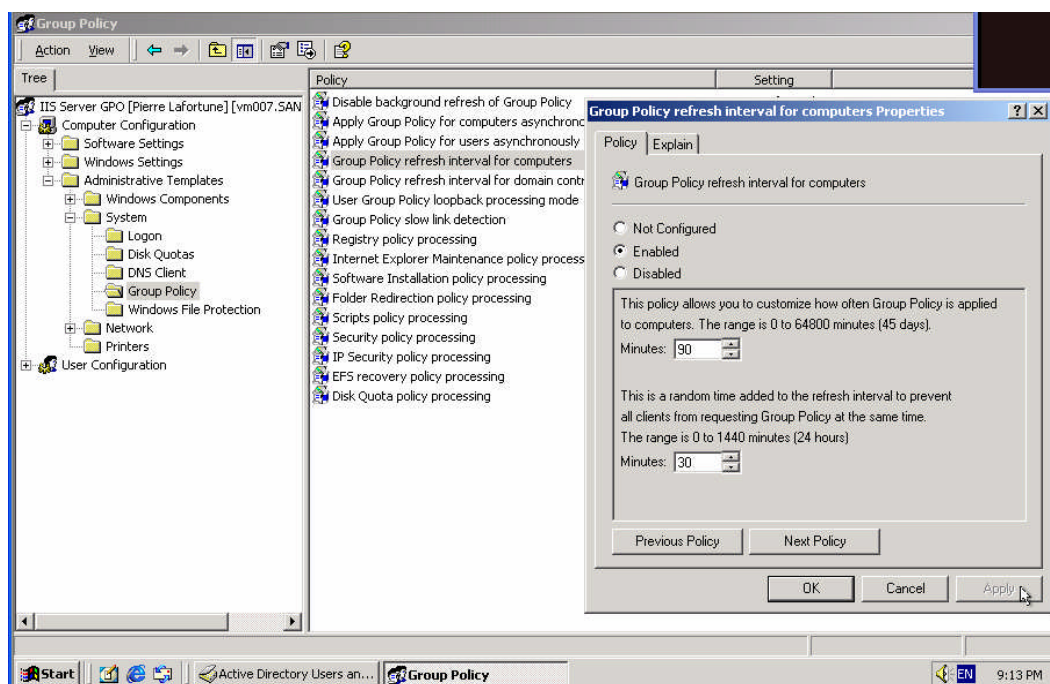
10. Verify in the **Event Log** that the policy downloaded successfully.
 - a. Open the **Computer Management** console. Expand **System Tools** and **Event Viewer**. Double-click on **Application**.
 - b. Look for an event with the following three information:
 - i. Type: **Information**
 - ii. Source ID: **SceCli**
 - iii. Event ID: **1704** (successful event)



3.3 Group Policy Maintenance

Actually the administration of all OUs and GPOs are managed by the Security team. It is in S&G's plan to delegate some of the OUs in a near future.

Group policy's refresh interval is not configured by default, it must be set through the IIS group policy. S&G opted for a 90 minutes interval with a 30 minutes offset.



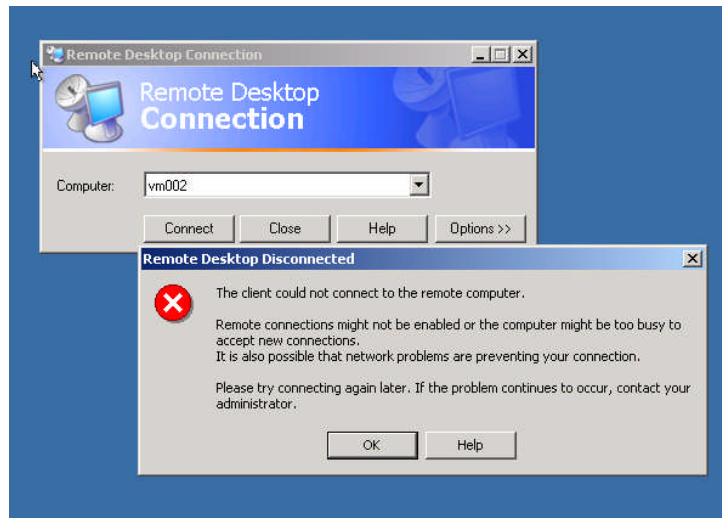
If we want to force a refresh on the IIS server, we must use the **secdit** command line. (see previous section 3.2)

3.4 Testing the Policies Security Settings

Now that the group policies were defined and applied, we must demonstrate that the security is working as expected.

We will now test the following policy: Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignments\Log on Locally. The actual settings permits to **Local Administrators** and **Backup Team** members to log one the IIS server. (see section 3.1.1)

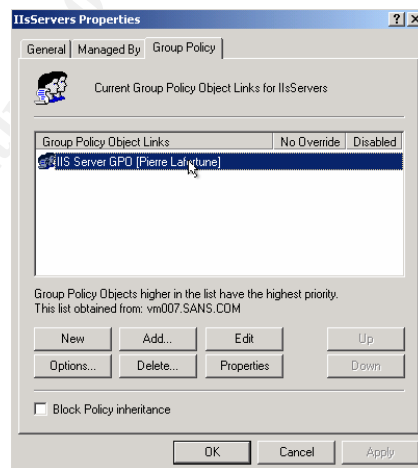
The following tasks were performed using a user member of the **WebAdmins** team from the SANS.COM domain. WebAdmins are members of IIS server's **Local Administrators** group.



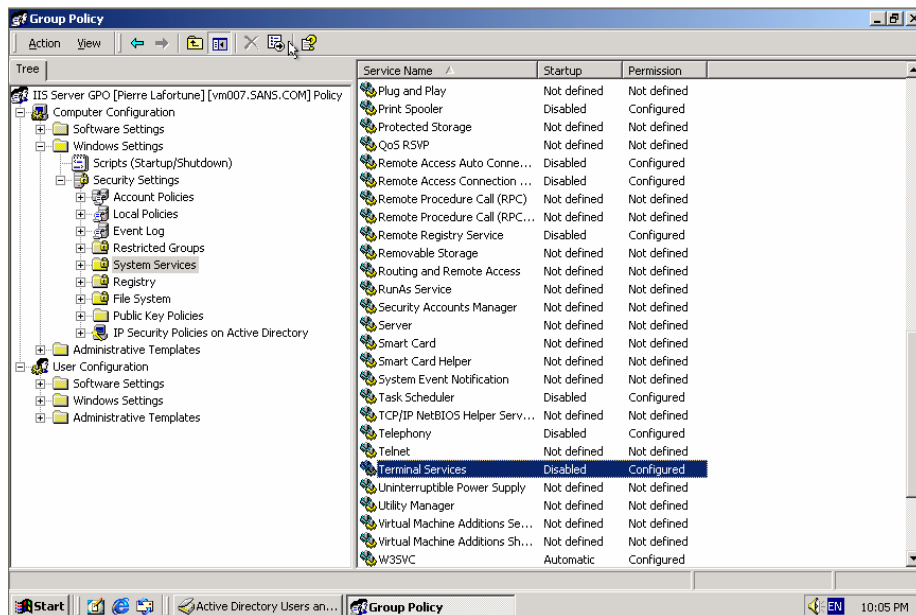
As seen above, connection to IIS Server (vm002) failed. Let's go look in the GPO to try to locate and fix the problem.

Connected on the SANSCOM domain controller, the following tasks must be performed:

1. In **Active Directory** Users and Computers, right-click the **IIS Servers** OU, and then select **Properties**.
2. On the **Group Policy** tab, select the GPO **IIS Server GPO [Pierre Lafortune]** and click Edit.

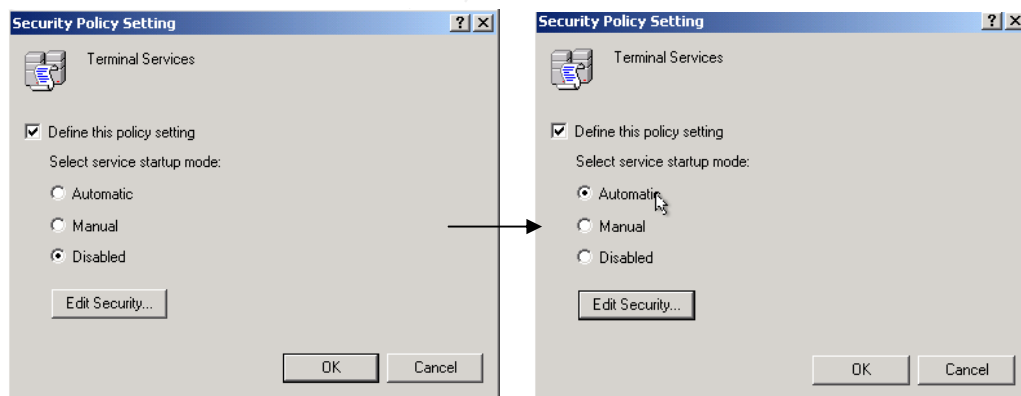


3. In the **Group Policy** window, select **Computer Configuration > Security Settings > System Services**. Double-click on **Terminal Services**.

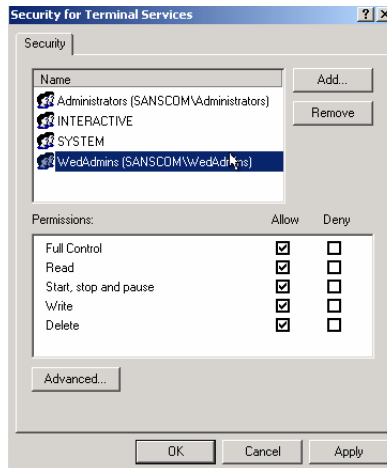


As we can see on the screenshot above, the GPO defined the **Terminal Services** policy setting to **Disabled**. Since it is needed for remote administration, we must modify the GPO to make the service available.

4. In the **Security Policy Settings** window, select **Automatic**.



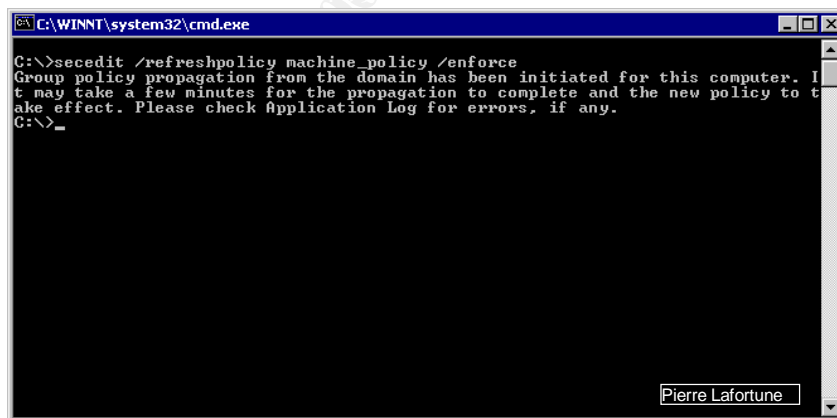
5. Click on **Edit Security**.



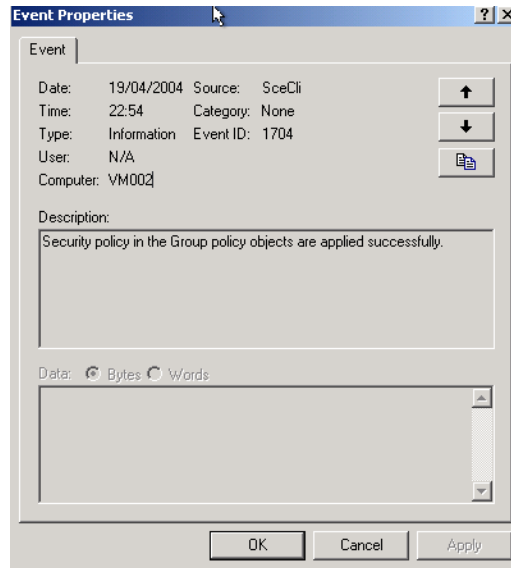
6. Add the **WebAdmins** group and grant full control. This will allow the WebAdmins the ability to manage the service.
7. Close the **Group Policy** that has been modified.
8. Close the **IIS Servers** OU Properties window.

Force the replication on the **IIS Server** so that doing the following will enforce the policy:

1. Open a command prompt and use the **Scedit.exe** command line tool to force the server to refresh the policy with the command:
 - **Scedit /refreshpolicy machine_policy /enforce**

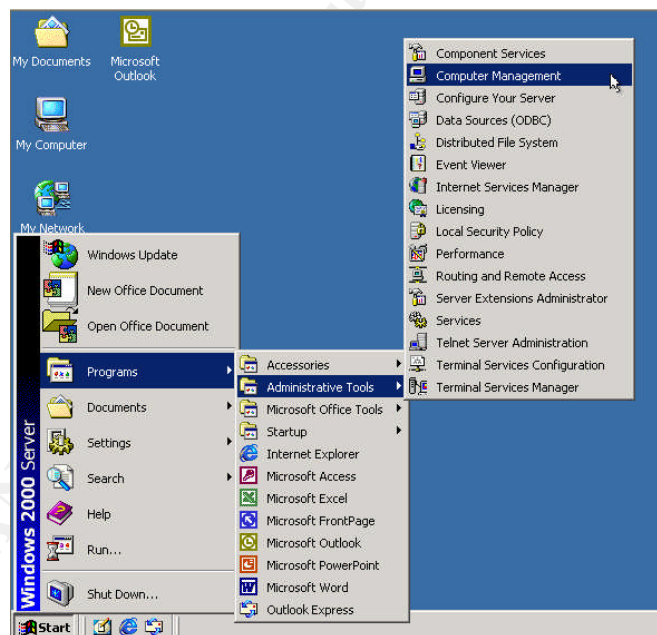


2. Verify in the **Event Log** that the policy downloaded successfully.
 - a. Open the **Computer Management** console. Expand **System Tools** and **Event Viewer**. Double-click on **Application**.
 - b. Look for an event with the following three information:
 - iv. Type: **Information**
 - v. Source ID: **SceCli**
 - vi. Event ID: **1704** (successful event)

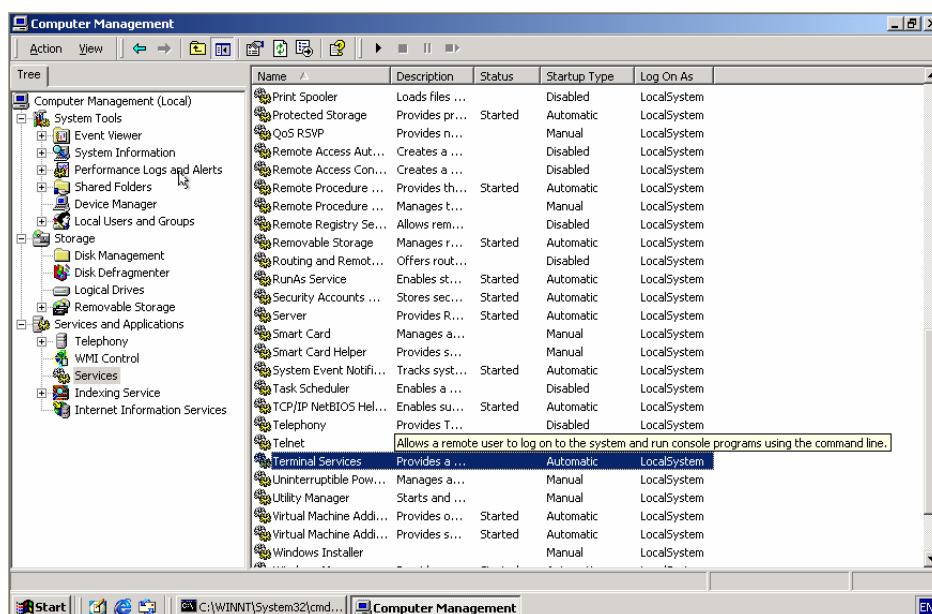


We can verify that the Group Policy changed the **Terminal Services** settings. Connected on the **ILS server** do the following tasks:

1. Open the Computer Management console.

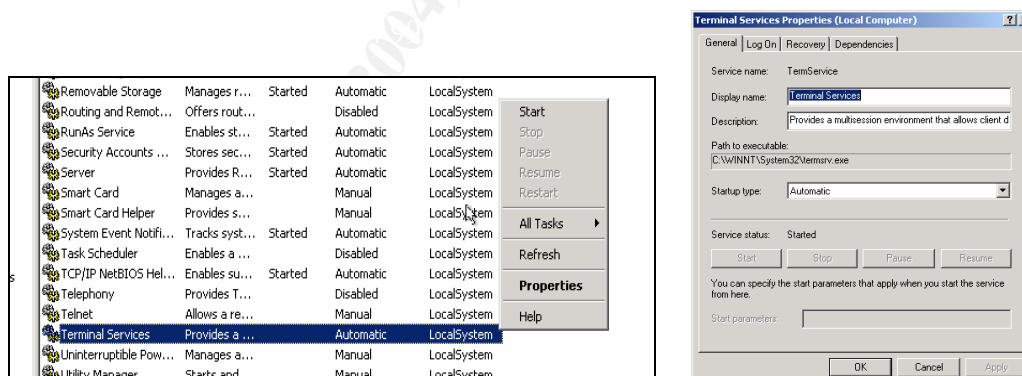


2. Expand **Services and Applications**. Double-click on **Services**.



Above screenshot shows that the GPO did take place. The only thing left to do is to start the service.

3. Right-click on the **Terminal Services** and click on **Start** or double-click on **Terminal Services** and click on **Start** in the **Terminal Services Properties** window.



4. Next screen shows that the service started.

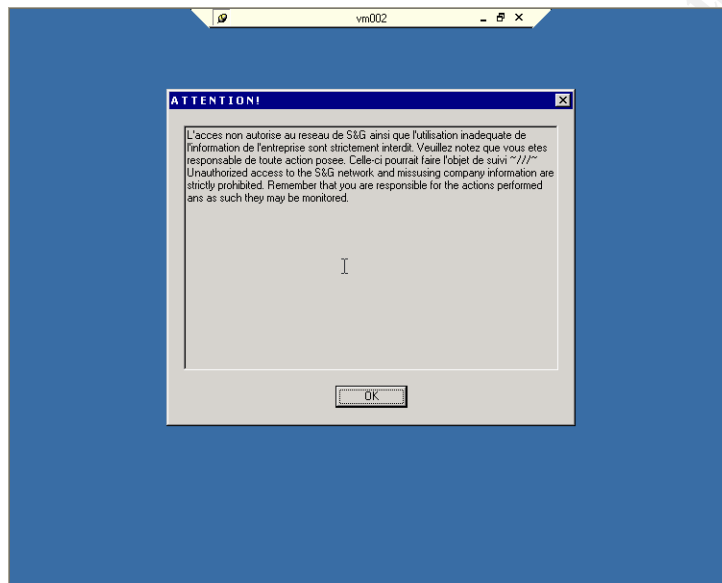
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	LocalSystem
Telephony	Provides T...	Disabled	Automatic	LocalSystem
Telnet	Allows a re...	Manual	Automatic	LocalSystem
Terminal Services	Provides a ...	Started	Automatic	LocalSystem
Uninterruptible Pow...	Manages a...	Manual	Manual	LocalSystem
Utility Manager	Starts and ...	Manual	Manual	LocalSystem
Virtual Machine Addi...	Provides o...	Started	Automatic	LocalSystem

Take note that the **Terminal Services** service can't be stopped. This is by design; stop/restart of the service can do unpredictable things to the system environment on **Terminal Services**. To be able to disable remote logon, we

simply have to issue the following command from a console prompt: **change logon/disable**

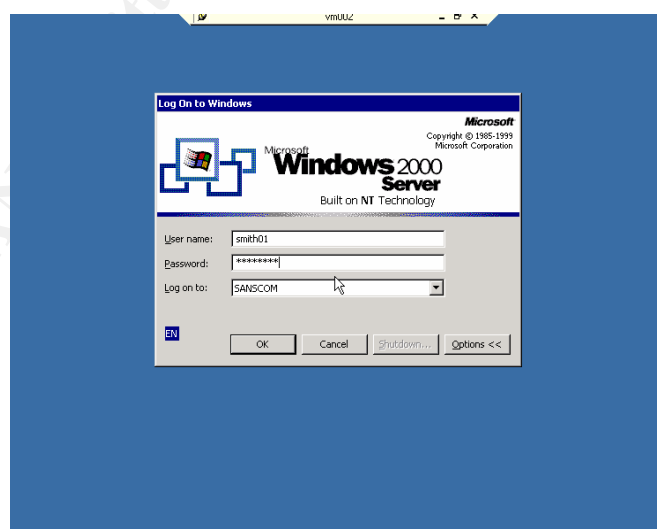
To enable logon again, we have to issue the **change logon/enable**. This has the advantage of not doing anything to the current connection.

Now let's test the **Remote Desktop Connection** again and see the result.



Good work, the connection is back! We can also see that the **Logon Banner** appears correctly.

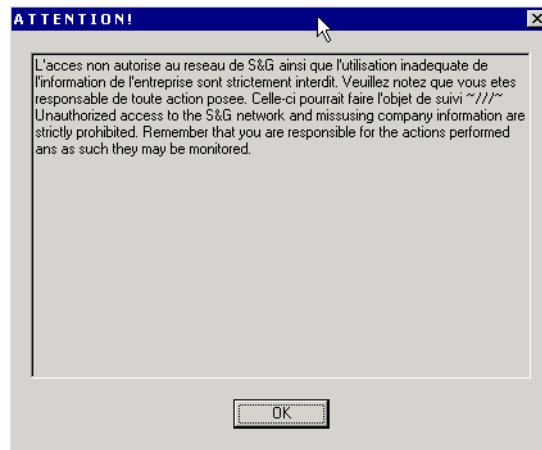
Let's finish our connection.



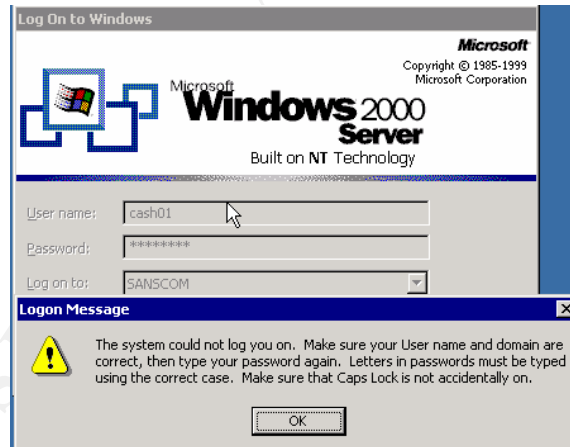
Connection worked perfectly.

We will now try to log on with a regular user account to the IIS server.

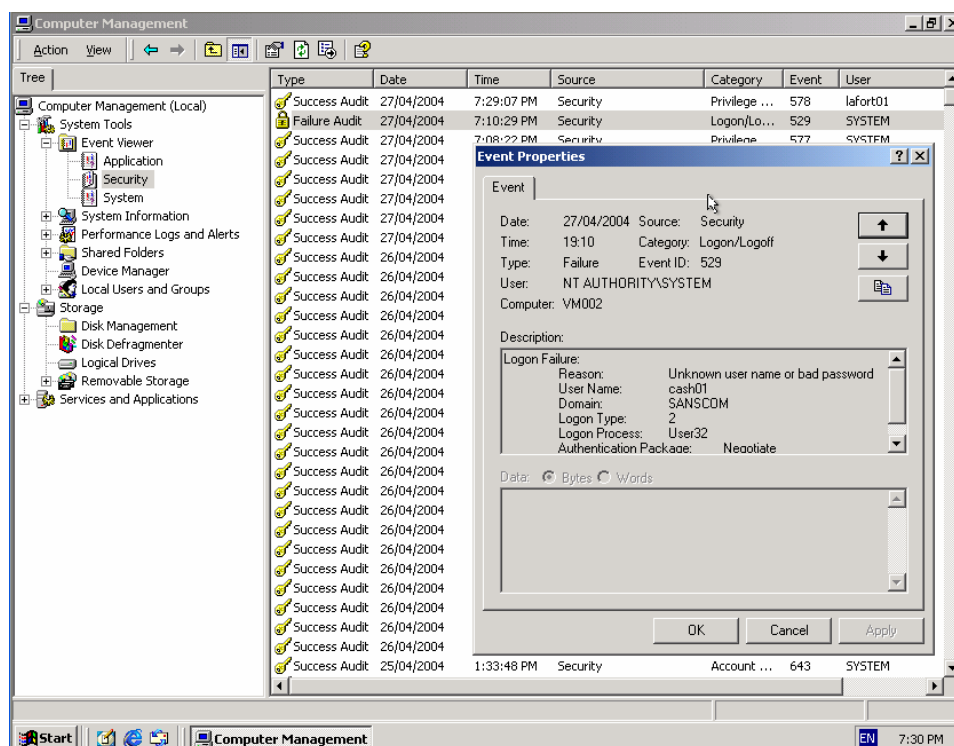
The first screen that the user sees is the Log on banner that the Administrator have put in the GPO. (See image below)



After the message, the user has the choice to Cancel or try to connect even though he knows he doesn't have the permissions to do it. For test purposes, we will continue and try to connect.



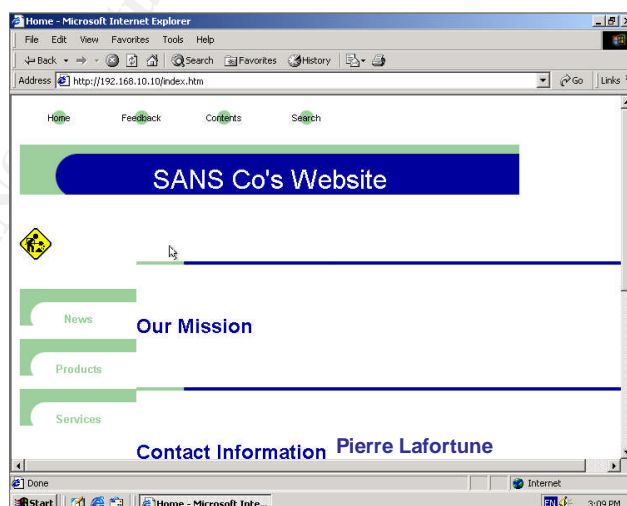
The above image shows that the policy in place is working just fine. Now let's connect on the IIS server as an administrator and view the event log to locate the logon failure.



3.5 Testing the System's Functionality

The following tasks will be performed to verify that the security policies settings are working properly and in a functional way.

A user member of the SANS.ORG domain will try to connect to the SANS Co's website.

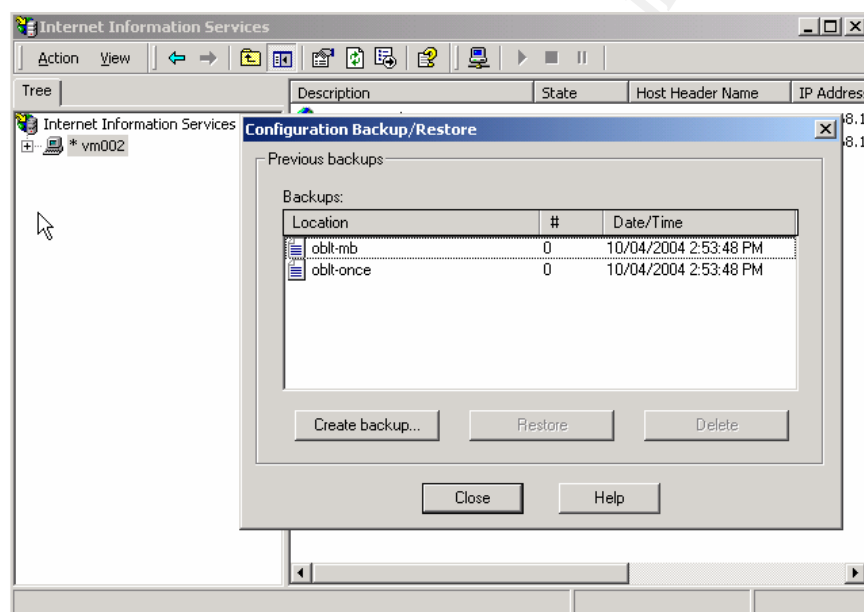


Screenshot above confirms that SANS Co's website is still available.

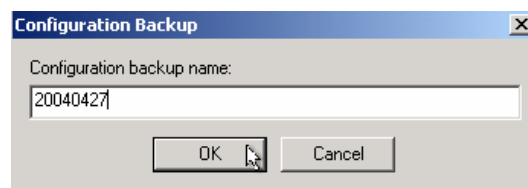
The next test is to verify that members of the **WebAdmins** group can backup/restore the Metabase.

Connected to the IIS server with a **WebAdmins** group user account, the following tasks were performed:

1. Start the Microsoft Management Console (MMC) Internet Information Services (IIS) Manager snap-in (go to Start, Programs, Administrative Tools, then click Internet Information Services Manager).
2. Right-click the name of the machine that hosts the IIS services, then select Backup/Restore from the menu.



3. Click Create Backup.
4. Enter a name for the backup as the image below shows.



5. Click OK.
6. Click Close on the main Backup/Restore Configuration window.

This test was also conclusive and prove that the security policy was applied and is fully functional.

4 Auditing

Part of a good security practice is the audit of the event logs. There are three different logs that need to be audited: System, Security and Application. The System log contains events related to operating system performance and are mainly used for troubleshooting. The Security log records the authentication events, access to resources, invocations of user rights, and other items for intrusion detection and incident response. The application log is for events application developers would like to register. S&G realizes that monitoring and auditing for intrusion are very important. The following reasons influenced greatly their decision to be pro-active in auditing:

- Any functional computer environment is potentially open to attack. Your level of security may be at a high but you still can be attacked.
- Successful attacks happen often after a series of unsuccessful ones. If attacks are not monitored they will not be detected before they are successful.
- It is much easier to contain the possible damage, if a successful attack is detected earlier. It also helps in determining what network resources are compromised.
- Knowing what damage was done, it will be easier to recover from the attack.
- Auditing will help in determining who was responsible for the attack.
- Reviewing the security logs on a regular base helps to identify security configuration issues (incorrect permissions, lax account lockout settings).

S&G Co's Group Policy is not configured to shut down the systems if the security log reaches capacity. Instead, it is configured to overwrite event logs older than 7 days (see section 3.1 - IIS Servers OU Policy - Event Logs). This will help avoiding attackers to flush out log files with meaningless entries.

The members of **Security** team are responsible for the auditing.

On the hardware side, S&G followed Jason Fossen⁷ recommendations and ensured that there was adequate free space in the Boot partition for both the log files and a paging file. Additional paging files were placed in other partitions, a RAID 0 volume dedicated to the paging file was implemented.

4.1 Events to audit

Microsoft Windows 2000 has several categories of auditing for security events. The following will list the available events, a short description of the event and the ones that S&G Co decided to include in their auditing:

⁷ Jason Fossen - 5.2 Windows 2000/XP/2003 Group Policy and DNS. Page 111.

4.1.1 Logon events

When a user logs on or off a computer or a remote server an event is generated in the Security log of the computer where the logon attempt occurs.

S&G audit strategy

Auditing for large numbers of logon attempts failure and large number of accounts lockouts.

The following security events can be identified using logon events:

- A local logon attempt failure:
Events 529, 530, 531, 532, 533, 534 and 537. Events 529 and 534 if an attacker unsuccessfully tries to guess a username and password.
- An account misuse:
Events 530, 531, 532 and 533. The username and password were correctly entered but restrictions are preventing a successful log on.
- An account logout:
Event 539 shows that an account was locked out. This could mean that a password attack has failed.
- A Terminal Services attack:
Event 683, when a user does not log out from a session. Event 682, when a connection to a previously disconnected session has occurred.

4.1.2 Account logon events

When a user logs on to a domain, the domain controller processes the log on. This logon attempt is recorded at the domain controller that validates the account. Since the event can be recorded in any valid domain controller, the security log is consolidated across domain controllers to analyze all Account Logon events in the domain.

S&G audit strategy

S&G is monitoring for high numbers of domain logon attempt failure.

The following security events can be identified using logon events:

- A domain logon attempt failures:
Events 675 and 677 show failed attempts to logon to the domain.
- Time synchronization issues:
Event 675. When a time difference occurs between a client computer and the domain controller by more than 5 minutes.

- Terminal Services attacks:
Event 682. A user has reconnected to a disconnected Terminal Services session. This event indicates that a previous Terminal Services session was connected to.
Event 683. A user disconnected a Terminal Services session without logging off. This event is generated when a user is connected to a Terminal Services session over the network.

4.1.3 Account Management

Account Management is used to determine when users or groups are created.

S&G audit strategy

S&G doesn't have that many accounts activities. So the monitoring of these events wouldn't cause too many alerts and make it easy to track these activities.

The following Account Management events can be identified using security log events.

- Creation of a user account:
Events 624 and 626. A user account was created and enabled.
- User account password changed:
Events 627 and 628. The password was successfully changed, it is important to verify that somebody else than the user itself did not change the password. This could indicate that another user has taken the account.
- Modification of security groups:
Events 632 and 633. Global groups memberships modification.
Events 632 and 633. Domain local groups memberships modification.
- Account logout:
Events 642 and 644. Will indicate that an account was locked out.

4.1.4 Object access events

It is possible to audit all objects in a Windows 2000-based network with a system control list (SACL). SACL contains a list of users and groups for which actions on the object are to be audited. Files and folders on NTFS file system drives, printers and registry keys are object that are auditing when a user manipulate them. To have the event appear in the security log, Auditing for Object Access must be enabled and the SACL must be defined for each object to be audited.

S&G audit strategy

S&G is monitoring for failure object access events. It has been decided to audit only the sensitive files.

4.1.5 Directory Service Access

Active Directory objects have SACLS associated with them, which mean they can be audited. This is useful to audit the modification of objects in other naming convention like the Configuration and Schema naming contexts.

S&G audit strategy

S&G is not monitoring for any directory service access object. It has been decided to audit object access only the sensitive files.

4.1.6 Privilege use events

Tracks unsuccessful attempts to use privileges. Auditing for success will generate a very large number of entries in the security log. This is why we should only audit for failure.

S&G audit strategy

S&G is monitoring for any events that indicate a normal shutdown or a forced shutdown from a remote system. The Security team monitors any events that indicate that the auditing and security log have been modified.

- Act as part of the operating system.
Events 577 or 578 with the **SeTcbPrivilege** access privilege indicated.
- Change the system date.
Events 577 or 578 with the **SeSystemtimePrivilege** access privilege indicated.
- Force the shutdown from a remote system.
Events 577 or 578 with the **SeRemoteShutdownPrivilege** access privilege indicated.
- Load an unload device drivers.
Events 577 or 578 with the **SeLoadDriverPrivilege** access privilege indicated. Can indicate a user's attempt to load an unauthorized or Trojan horse version of a device driver.
- Manage auditing and security log.
Events 577 or 578 with the **SeSecurityPrivilege** access privilege indicated. Will occur both when the event log is cleared and when events for privilege use are written to the security log.

- Shut down the system.
Events 577 or 578 with the **SeShutdownPrivilege** access privilege indicated. Will occur when an attempt to shut down the computer happens.
- Take ownership of files or other objects.
Events 577 or 578 with the **SeTakeOwnershipPrivilege** access privilege indicated. Can indicate an attacker is attempting to bypass actual security settings by taking ownership of an object.

4.1.7 Process tracking events

Detailed tracking information for events such as program activation and exits.

S&G audit strategy

Not monitored.

4.1.8 System events

Events that affect the entire system or the Audit log, such as restart or shutdown.

S&G audit strategy

S&G is monitoring both computer shutdown and restarts.
--

4.1.9 Policy change events

Tracking of changes in security policy. Activities like assignment of privileges or changes in the audit policy are audited.

S&G audit strategy

These events are not monitored but are available for consulting for any troubleshooting or incident response.

4.2 Auditing Practices

S&G implemented the following practices to effectively audit the security of their server environment:

- Scheduling regular review of the event logs.

Experience shows that reviewing the event logs is the most frequently missed auditing step. S&G ensured that at least one person member of the **Security (Level 3 Support)** team is responsible for reviewing the logs as a regular task. The actual plan is to schedule an audit of the event logs every week. This was based on the actual level of auditing. If the amount

of data collected in the security log should increase (more events audited), the schedule would be changed to a daily base.

S&G sees great benefits in scheduling the events logs reviews. They will be able to detect faster the security issues and repair the security vulnerabilities. The person identified of reviewing the log files can ultimately be responsible for identifying potential attacks.

- Reviewing Internet Information Services (IIS) log files.

IIS creates log files that track connection attempts to Web, File Transfer Protocol (FTP), network time protocol (NTP), and Simple Mail Transfer Protocol (SMTP) services. The review of the logs is the **WebAdmins** team responsibility and they are located on C:\WINNT\system32\LogFiles\W3SVC2 (See log sample in Appendix A)

4.3 Monitoring and Auditing Security Events

Monitoring for intrusion and security events includes both passive and active tasks. Difference is quit simple; passive intrusion are attacks that already took place and are visible in the logs and active intrusion can be detected as the attack takes place. The following section will look at tools that can be used to implement both types of intrusion detection to protect the network from attack.

Passive detection methods

These detection systems involve the manual review of event logs and application logs. We must look for an attack pattern in event log data. Many tools are available to help review the event logs.

- Windows 2000 Event Viewer MMC Console
The Windows 2000 security log can be viewed using the Windows 2000 Event viewer MMC console. It allows us to view application, security, and system logs. Filters helps us to find specific events in the Event Viewer. (See screenshot below)

Type	Date	Time	Source	Category	Event	User	Comput
Success Audit	24/04/2004	4:25:52 PM	Security	Privilege Use	578	lafort01	VM002
Success Audit	24/04/2004	4:25:21 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	4:24:35 PM	Security	Privilege Use	578	lafort01	VM002
Success Audit	24/04/2004	4:23:48 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:49:12 PM	Security	Login/Logoff	538	1USR_VM002	VM002
Success Audit	24/04/2004	3:49:12 PM	Security	Login/Logoff	538	1USR_VM002	VM002
Success Audit	24/04/2004	3:32:08 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:32:07 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:30:08 PM	Security	Privilege Use	578	lafort01	VM002
Success Audit	24/04/2004	3:29:24 PM	Security	Privilege Use	578	lafort01	VM002
Success Audit	24/04/2004	3:28:52 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:24:39 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:24:39 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:17 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:17 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:12 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:08 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:06 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:03 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:23:01 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:22:59 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:22:18 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:22:18 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:21:12 PM	Security	Privilege Use	577	lafort01	VM002
Success Audit	24/04/2004	3:21:08 PM	Security	Privilege Use	577	lafort01	VM002

- **Dump Event Tool (Dumpel.exe)**
Dump Event is an utility tool that runs from a command line. It is included in the Windows 2000 Server Resource Kit. It dumps an event log into a tab separated text file. The text file could be imported into a spreadsheet or database for future investigation. The use of filters allows us to search for certain event types.

Dump Event Log Syntax:

dumpel -f file [-s \\server] [-l log [-m source]] [-e n1 n2 n3...] [-r] [-t] [-d x]

Where:

-f file

specifies the file name for the output file. there is no default for **-f**, so you must specify the file.

-s server

specifies the server for which you want to dump the event log. leading backslashes on the server name are optional.

-l log

specifies which log (system, application, security) to dump. if an invalid *logname* is specified, the application log will be dumped.

-m source

specifies in which source (such as rdr, serial, ...) to dump records. only one source can be supplied. if this switch is not used, all events are dumped. if a source is used that is not registered in the registry, the application log will be searched for records of this type.

-e n1 n2 n3 ...

filters for event id *nn* (up to ten can be specified). if the **-r** switch is not used, only records of these types are dumped; if **-r** is used, all records except records of these types are dumped. if this switch is not used, all events from the specified *sourcename* are selected. you cannot use this switch without the **-m** switch.

-r

specifies whether to filter for specific sources or records, or to filter them out.

-t

specifies that individual strings are separated by tabs. if **-t** is not used, strings are separated by spaces.

-d x

dumps events for the past x days.

- Microsoft Operations Manager (MOM)
MOM 2000 offers a comprehensive set of tools that allow thoroughly analyze the built-in event reporting and performance monitoring of Windows 2000. MOM 2000 can collect, store, and report events and performance data to a single location.
- **EventCombMT**. SANS Co opted for this tool.

Event Comb (EventCombMT) is a GUI tool that searches event logs on multiple DCs/Servers and collects Event ID records matching the specified criteria.

Tool's options:

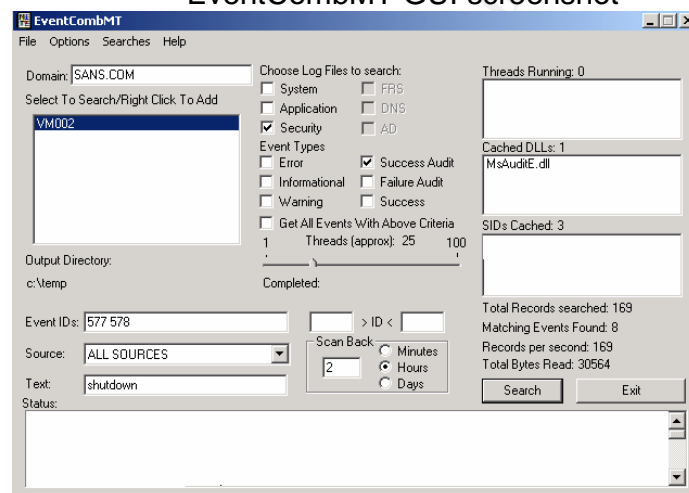
- Define either a single Event ID, or multiple Event Ids to search for.
- Define a range of Event Ids to search for.
- Limit the search to specific event logs.
- Limit the search to specific messages types.
- Limit the search to specific event sources.
- Search for specific text within an event description.
- Define specific time intervals to scan back from the current date and time.

Scenario: Customers recently complained that SANS Co's Web site was not responding. **WebAdmins** team contacted the **Security** team and asked them to trace in the logs the IIS server shut down, if possible. They would like to know who performed the shut down since they were not advised through the change control process. According to the customers the problem occurred within the last hour.

Connected on the IIS server, the **Security** team member will perform the following tasks using **EventCombMT**:

1. Add the IIS computer name in the *Select To Search* field.
2. Click on the server to be scanned. *VM002* in this example.
3. Select *Security* in the *Choose Log Files to search*.
4. Select *Success Audit* in the *Event Types*.
5. Type *577 578* in the *Event Ids* field.
6. Since we are looking for a shutdown, type *shutdown* in the *Text* field.
7. The event occurred one hour ago, lets give us a larger time frame. Type *2* and select *hours* in the *Scan Back*.
8. Click *Search*.

EventCombMT GUI screenshot



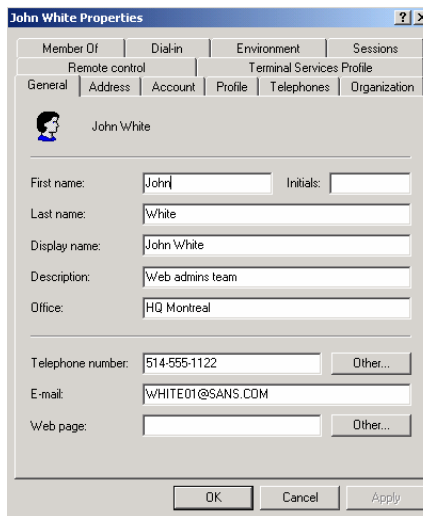
9. **EventCombMT** will scan the server(s) and save the result in a text file. A windows will open and the file will be available from there. Format is *servername-EventLogName_LOG* (*VM002-Security_LOG* for this example).
10. Open the file. (See log sample in Appendix B)
11. Locate the Event ID 578, the date and time, and the user account and Domain name.

Information located in log are in bold:

578,AUDIT SUCCESS,Security,**Sat Apr 24 20:09:00**

2004,**SANSCOMWHITE01**,Privileged object operation: Object Server: Security Object Handle: 0 Process ID: 200 Primary User Name: VM002\$ Primary Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: **white01** Client Domain: SANSCOM Client Logon ID: (0x0,0x426CE) Privileges: **SeShutdownPrivilege**

12. With the above information, we now can tell who did the shutdown. In this case the user **WHITE01** from the **SANSCOM** Domain is responsible for the shutdown. We can simply use **Active Directory Users and Computers** to track the user's information.



13. Last thing to do is transmit the information to the **WebAdmins** team.

Active detection methods

Active intrusion detection systems analyze incoming network traffic at the application level. It looks for well known attacks method or suspicious application layer payloads. The intrusion system will drop any suspicious packet received and log an entry in a log file (see Appendix C). An alert is also available in some intrusion detection systems, it will alert an administrator if a severe attack is detected.

S&G IIS servers receives incoming HTTP traffic, and not all traffic is legitimate. To protect themselves from these attacks, S&G opted for **URLScan** (comes with IISLockdown). URLScan is an ISAPI filter that analyzes incoming HTTP packets and can reject any suspicious traffic.

URLScan protects S&G's servers from attacks by filtering and rejecting HTTP requests for selected IIS service features. By default, URLScan is configured to accept requests for only static HTML files, including graphics. It will reject the following types of requests:

- CGI pages
- WebDAV
- FrontPage Server Extensions
- Index Server
- Internet printing
- Server side includes

URLScan is configured using a file called UrlScan.ini. It can be found in the %WinDir%\system32\inetsrv\UrlScan folder. S&G opted to keep the default configuration since it respected their security needs. (See Appendix D)

4.4 Event Logs Management

S&G are archiving all log files from all machines to one central location. A directory structure and a naming convention was implemented which clearly indicates the time frame covered by the log file and from which computer it came from. A scheduled task resides on each server which calls a WMI script that will backup the event logs and copy them to the centralized location. The schedule is set to run every Saturday between 1:00 AM and 4:00AM, and starting time is different from one server to another to avoid having too much traffic at the same time.

4.5 Critical Components

Attackers will often perform a port scan to identify any known services running on the target computer. Since our IIS server can be accessed from a public network, the port scan is performed from an external computer to ensure that the firewall software allows access to desired ports. The port scanning is **Server Team's** responsibility. They're using **LANguard Network Scanner** (GFI Software Ltd) to perform their scanning. The interface is very easy to use and the reports formats are easy to read. Also, it comes with helpful security guidelines showed in the Alerts section.

GFI LANguard Network Scanner is a Freeware security scanner for networks. It searches the network for hosts, shares and user names. Amongst many other functions it recognizes operating systems, as well as registry problems and tests password security. The scanner also provides comprehensive reports in HTML format on request. The **GFI LANguard Network Scanner** is a comprehensive and easy-to-use tool.

The following guidelines are stated word for word in **GFI LANguard Network Scanner's** help file and we believe that all system administrators should follow read it and memorize it.

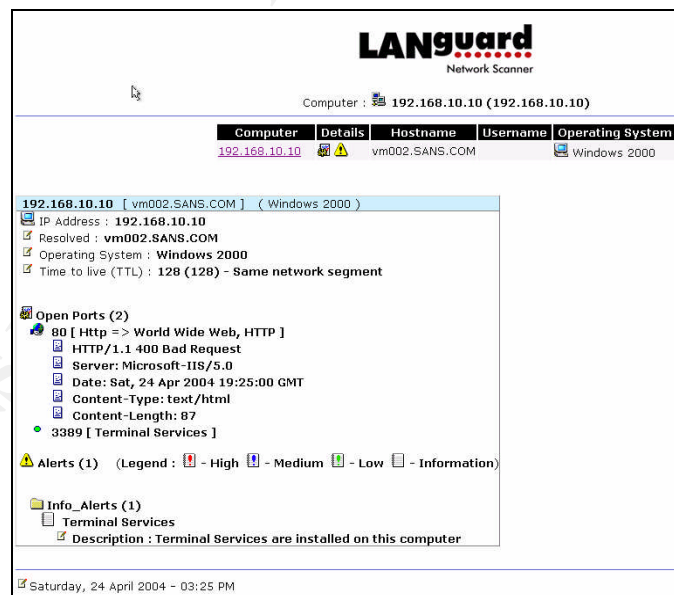
"Why care about Internal Network Security ?

Many normal users, such as employees within a company, should not have access to each other's machines, to administrative functions, to network devices or similar rights. Of course in practice this is usually not achieved, and a user with minimal skills will be able to do a successful penetration and achieve remote administrative rights of your network within a few minutes of exploration.

Because of the amount of flexibility needed for normal operation, Internal networks cannot afford maximum security. However with no security at all, internal users can be a major threat for many corporate internal networks. A user within the company already has access to many resources and does not need to bypass firewalls or other security mechanisms which prevent non-trusted sources, such as internet users, to access the internal network. Such internal users can also make sure that it is hard enough to identify or even detect.

Other than internal users, poor network security will mean that once a hacker gets hold of a computer which is within your network, he or she also has access to the rest of the Internal Network. Many holes exist which allow hackers to tunnel through different protocols, such as SMTP (e-mail) and HTTP, to bypass security mechanisms such as firewalls and bastion hosts. Such attacks will allow a more sophisticated attacker to easily penetrate and get administrative rights over an internal network, meaning confidential e-mails and documents can be read, computers can be trashed leading to loss of information, possible business information leakage and other problems.”

S&G implemented a process to audit their vulnerabilities. Every week a member of the **Server** team performs a scan on each server on the network and takes appropriate measures when a weakness or a breach is discovered.



The report above confirms that the firewall policy, stated in section 2.4 Firewall Access, was applied properly. Only ports 80 and 3389 are opened to the public network.

5 References

Rudzonis, Brian. GIAC Enterprises: Securing Windows 2000 Infrastructure Design. http://www.giac.org/practical/GCWN/Brian_Rudzonis_GCWN.pdf

Microsoft Corporation. Determining Network Connectivity Strategies. <http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/deploy/part2/chapt-7.mspx>

Microsoft Corporation. Microsoft Windows 2000 Network and Operating System Essentials. 2151AC. Released: 2/2000.

Microsoft Corporation. Implementing a Microsoft Windows 2000 Network Infrastructure. 2153BC. Released: 3/2002

Microsoft Corporation. Designing a Secure Microsoft Windows 2000 Network. 2150AC. Released: 6/2000

Microsoft Corporation. Microsoft Solutions for Security. Windows 2000 Server Security Solution. 2003

NSA. Guide to Securing Microsoft Windows Group Policy: Security Configuration Tool Set. Version 1.1, January 22, 2002

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

Fossen, Jason. Track 5.2 – Windows 2000/XP/2003 Group Policy and DNS. SANS Institute. 2003

Fossen, Jason. Track 5.5 –Securing Internet Information Server. SANS Institute. 2003

Microsoft Corporation. Microsoft Prescriptive Guidance. Security Operations Guide for Windows 2000 Server.

6 Appendix A

Internet Information Services (IIS) sample log file

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2004-04-24 18:47:41
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status
cs(User-Agent)
2004-04-24 18:47:41 192.168.10.20 - 192.168.10.10 80 GET /index - 404
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:47:56 192.168.10.20 - 192.168.10.10 80 GET /index.html - 404
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET /index.htm - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/home_cmp_capsules000_gbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/feedback.htm_cmp_capsules000_gbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/search.htm_cmp_capsules000_gbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/toc.htm_cmp_capsules000_gbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/index.htm_cmp_capsules000_bnr.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET /images/undercon.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/news.htm_cmp_capsules000_vbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/products.htm_cmp_capsules000_vbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:00 192.168.10.20 - 192.168.10.10 80 GET
/_derived/services.htm_cmp_capsules000_vbtn.gif - 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 18:48:01 192.168.10.20 - 192.168.10.10 80 GET /_themes/capsules/capsepd.gif
- 200 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /msadc/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /scripts/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cgi-bin/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /bin/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /samples/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /_vti_cnf/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /_vti_bin/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /iisadmpwd/ - 404 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /index.htm - 200 -
2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
~///lanscan.ida 404 -
```

2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///lanscan.idq 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cfdocs/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cfide/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /_vti_inf.html - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /tsweb - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /_vti_bin/_vti_aut/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///default.asp::\$DATA 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /default.asp. - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cgi-bin/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /index.htm - 200 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /carbo.ddl - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /technote/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /iisadmpwd/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cgi-dos/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /scripts/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /mall_log_files/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /Admin_files/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cgi-bin/a1stats/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /quote.html - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cgi-bin/ikonboard/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /foldoc/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /cgi-bin/adcycle/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /ROADS/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 HEAD /way-board/ - 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /index.php
 chemin=..%2F..%2F..%2F..%2F..%2F..%2Fetc 404 -
 2004-04-24 19:00:04 192.168.10.20 - 192.168.10.10 80 GET /edit_image.php
 dn=1&userfile=/etc/passwd&userfile_name=%20ls;%20 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /msadc/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /scripts/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /bin/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /samples/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_cnf/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_bin/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /iisadmpwd/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /index.htm - 200 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///lanscan.ida 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///lanscan.idq 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cfdocs/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cfide/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_inf.html - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /tsweb - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_bin/_vti_aut/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///default.asp::\$DATA 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /default.asp. - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /index.htm - 200 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /carbo.ddl - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /technote/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /iisadmpwd/ - 404 -

2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-dos/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /scripts/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /mall_log_files/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /Admin_files/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/a1stats/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /quote.html - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/ikonboard/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /foldoc/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/adcycle/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /ROADS/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 HEAD /way-board/ - 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /index.php
 chemin=.%2F.%2F.%2F.%2F.%2F.%2Fetc 404 -
 2004-04-24 19:02:35 192.168.10.10 - 192.168.10.10 80 GET /edit_image.php
 dn=1&userfile=/etc/passwd&userfile_name=%20;ls;%20 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /msadc/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /scripts/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /bin/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /samples/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_cnf/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_bin/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /iisadmpwd/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /index.htm - 200 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///lanscan.ida 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///lanscan.idq 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cfdocs/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cfide/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_inf.html - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /tsweb - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /_vti_bin/_vti_aut/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /<Rejected-By-UrlScan>
 ~///default.asp::\$DATA 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /default.asp. - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /index.htm - 200 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /carbo.ddl - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /technote/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /iisadmpwd/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-dos/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /scripts/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /mall_log_files/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /Admin_files/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/a1stats/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /quote.html - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/ikonboard/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /foldoc/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /cgi-bin/adcycle/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /ROADS/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 HEAD /way-board/ - 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /index.php
 chemin=.%2F.%2F.%2F.%2F.%2F.%2Fetc 404 -
 2004-04-24 19:25:15 192.168.10.10 - 192.168.10.10 80 GET /edit_image.php
 dn=1&userfile=/etc/passwd&userfile_name=%20;ls;%20 404 -

7 Appendix B

EventCombMT log sample

577,AUDIT SUCCESS,Security,Sat Apr 24 20:15:19 2004,SANSCOM\lafort01,Privileged
Service Called: Server: Security Service: - Primary User Name: VM002\$ Primary
Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: lafort01
Client Domain: SANSCOM Client Logon ID: (0x0,0x6D2F) Privileges:
SeShutdownPrivilege
577,AUDIT SUCCESS,Security,Sat Apr 24 20:15:19 2004,SANSCOM\lafort01,Privileged
Service Called: Server: Security Service: - Primary User Name: VM002\$ Primary
Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: lafort01
Client Domain: SANSCOM Client Logon ID: (0x0,0x6D2F) Privileges:
SeShutdownPrivilege
578,AUDIT SUCCESS,Security,Sat Apr 24 20:09:00 2004,SANSCOM\WHITE01,Privileged
object operation: Object Server: Security Object Handle: 0 Process ID: 200
Primary User Name: VM002\$ Primary Domain: SANSCOM Primary Logon ID:
(0x0,0x3E7) Client User Name: white01 Client Domain: SANSCOM Client Logon ID:
(0x0,0x426CE) Privileges: SeShutdownPrivilege
577,AUDIT SUCCESS,Security,Sat Apr 24 20:08:47 2004,SANSCOM\WHITE01,Privileged
Service Called: Server: Security Service: - Primary User Name: VM002\$ Primary
Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: white01
Client Domain: SANSCOM Client Logon ID: (0x0,0x426CE) Privileges:
SeShutdownPrivilege
577,AUDIT SUCCESS,Security,Sat Apr 24 20:08:47 2004,SANSCOM\WHITE01,Privileged
Service Called: Server: Security Service: - Primary User Name: VM002\$ Primary
Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: white01
Client Domain: SANSCOM Client Logon ID: (0x0,0x426CE) Privileges:
SeShutdownPrivilege
577,AUDIT SUCCESS,Security,Sat Apr 24 19:07:35 2004,SANSCOM\lafort01,Privileged
Service Called: Server: Security Service: - Primary User Name: VM002\$ Primary
Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: lafort01
Client Domain: SANSCOM Client Logon ID: (0x0,0xB65B) Privileges:
SeShutdownPrivilege
577,AUDIT SUCCESS,Security,Sat Apr 24 19:07:35 2004,SANSCOM\lafort01,Privileged
Service Called: Server: Security Service: - Primary User Name: VM002\$ Primary
Domain: SANSCOM Primary Logon ID: (0x0,0x3E7) Client User Name: lafort01
Client Domain: SANSCOM Client Logon ID: (0x0,0xB65B) Privileges:
SeShutdownPrivilege
578,AUDIT SUCCESS,Security,Sat Apr 24 18:59:17 2004,SANSCOM\WHITE01,Privileged
object operation: Object Server: Security Object Handle: 0 Process ID: 1280
Primary User Name: VM002\$ Primary Domain: SANSCOM Primary Logon ID:
(0x0,0x3E7) Client User Name: white01 Client Domain: SANSCOM Client Logon ID:
(0x0,0x18D022) Privileges: SeShutdownPrivilege
c:\temp\VM002-Security_LOG.txt contains 8 parsed events.

8 Appendix C

URLScan sample log file

```
[04-24-2004 - 15:00:05] ----- Initializing UrlScan.log -----
[04-24-2004 - 15:00:05] -- Filter initialization time: [04-20-2004 - 21:20:37] --
[04-24-2004 - 15:00:05] Client at 192.168.10.20: URL contains extension '.ida', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///lanscan.ida'
[04-24-2004 - 15:00:05] Client at 192.168.10.20: URL contains extension '.idq', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///lanscan.idq'
[04-24-2004 - 15:00:05] Client at 192.168.10.20: URL contains sequence ':', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///default.asp::$DATA'
[04-24-2004 - 15:02:35] Client at 192.168.10.10: URL contains extension '.ida', which is d
isallowed. Request will be rejected. Site Instance='2', Raw URL='///lanscan.ida'
[04-24-2004 - 15:02:35] Client at 192.168.10.10: URL contains extension '.idq', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///lanscan.idq'
[04-24-2004 - 15:02:35] Client at 192.168.10.10: URL contains sequence ':', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///default.asp::$DATA'
[04-24-2004 - 15:25:16] Client at 192.168.10.10: URL contains extension '.ida', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///lanscan.ida'
[04-24-2004 - 15:25:16] Client at 192.168.10.10: URL contains extension '.idq', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///lanscan.idq'
[04-24-2004 - 15:25:16] Client at 192.168.10.10: URL contains sequence ':', which is
disallowed. Request will be rejected. Site Instance='2', Raw URL='///default.asp::$DATA'
[04-24-2004 - 19:00:08] ----- UrlScan.dll Terminating -----
[04-24-2004 - 19:04:44] ----- Initializing UrlScan.log -----
[04-24-2004 - 19:04:44] -- Filter initialization time: [04-24-2004 - 19:04:44] --
[04-24-2004 - 19:04:44] ----- UrlScan.dll Initializing -----
[04-24-2004 - 19:04:44] UrlScan will return the following URL for rejected requests:
"/<Rejected-By-UrlScan>"
[04-24-2004 - 19:04:44] URLs will be normalized before analysis.
[04-24-2004 - 19:04:44] URL normalization will be verified.
[04-24-2004 - 19:04:44] URLs must contain only ANSI characters.
[04-24-2004 - 19:04:44] URLs must not contain any dot except for the file extension.
[04-24-2004 - 19:04:44] Only the following verbs will be allowed (case sensitive):
[04-24-2004 - 19:04:44] 'GET'
[04-24-2004 - 19:04:44] 'HEAD'
[04-24-2004 - 19:04:44] 'POST'
[04-24-2004 - 19:04:44] 'OPTIONS'
[04-24-2004 - 19:04:44] Requests for following extensions will be rejected:
[04-24-2004 - 19:04:44] '.exe'
[04-24-2004 - 19:04:44] '.bat'
[04-24-2004 - 19:04:44] '.cmd'
[04-24-2004 - 19:04:44] '.com'
[04-24-2004 - 19:04:44] '.htw'
[04-24-2004 - 19:04:44] '.ida'
[04-24-2004 - 19:04:44] '.idq'
[04-24-2004 - 19:04:44] '.htr'
[04-24-2004 - 19:04:44] '.idc'
[04-24-2004 - 19:04:44] '.shtm'
[04-24-2004 - 19:04:44] '.shtml'
[04-24-2004 - 19:04:44] '.stm'
[04-24-2004 - 19:04:44] '.printer'
[04-24-2004 - 19:04:44] '.ini'
```

```

[04-24-2004 - 19:04:44] '.log'
[04-24-2004 - 19:04:44] '.pol'
[04-24-2004 - 19:04:44] '.dat'
[04-24-2004 - 19:04:44] Requests containing the following headers will be rejected:
[04-24-2004 - 19:04:44] 'if:'
[04-24-2004 - 19:04:44] 'lock-token:'
[04-24-2004 - 19:04:44] Requests containing the following character sequences will be
rejected:
[04-24-2004 - 19:04:44] '..'
[04-24-2004 - 19:04:44] '/'
[04-24-2004 - 19:04:44] '\'
[04-24-2004 - 19:04:44] ':'
[04-24-2004 - 19:04:44] '%'
[04-24-2004 - 19:04:44] '&'
[04-24-2004 - 20:09:42] ----- UrlScan.dll Terminating -----
[04-24-2004 - 20:15:06] ----- Initializing UrlScan.log -----
[04-24-2004 - 20:15:06] -- Filter initialization time: [04-24-2004 - 20:15:06] --
[04-24-2004 - 20:15:06] ----- UrlScan.dll Initializing -----
[04-24-2004 - 20:15:06] UrlScan will return the following URL for rejected requests:
"/<Rejected-By-UrlScan>"
[04-24-2004 - 20:15:06] URLs will be normalized before analysis.
[04-24-2004 - 20:15:06] URL normalization will be verified.
[04-24-2004 - 20:15:06] URLs must contain only ANSI characters.
[04-24-2004 - 20:15:06] URLs must not contain any dot except for the file extension.
[04-24-2004 - 20:15:06] Only the following verbs will be allowed (case sensitive):
[04-24-2004 - 20:15:06] 'GET'
[04-24-2004 - 20:15:06] 'HEAD'
[04-24-2004 - 20:15:06] 'POST'
[04-24-2004 - 20:15:06] 'OPTIONS'
[04-24-2004 - 20:15:06] Requests for following extensions will be rejected:
[04-24-2004 - 20:15:06] '.exe'
[04-24-2004 - 20:15:06] '.bat'
[04-24-2004 - 20:15:06] '.cmd'
[04-24-2004 - 20:15:06] '.com'
[04-24-2004 - 20:15:06] '.htw'
[04-24-2004 - 20:15:06] '.ida'
[04-24-2004 - 20:15:06] '.idq'
[04-24-2004 - 20:15:06] '.htr'
[04-24-2004 - 20:15:06] '.idc'
[04-24-2004 - 20:15:06] '.shtm'
[04-24-2004 - 20:15:06] '.shtml'
[04-24-2004 - 20:15:06] '.stm'
[04-24-2004 - 20:15:06] '.printer'
[04-24-2004 - 20:15:06] '.ini'
[04-24-2004 - 20:15:06] '.log'
[04-24-2004 - 20:15:06] '.pol'
[04-24-2004 - 20:15:06] '.dat'
[04-24-2004 - 20:15:06] Requests containing the following headers will be rejected:
[04-24-2004 - 20:15:06] 'if:'
[04-24-2004 - 20:15:06] 'lock-token:'
[04-24-2004 - 20:15:06] Requests containing the following character sequences will be
rejected:
[04-24-2004 - 20:15:06] '..'
[04-24-2004 - 20:15:06] '/'
[04-24-2004 - 20:15:06] '\'
[04-24-2004 - 20:15:06] ':'

```

[04-24-2004 - 20:15:06] '%'
[04-24-2004 - 20:15:06] '&'

© SANS Institute 2004, Author retains full rights.

9 Appendix D

IIS server's UrlScan.ini file

```
[options]
UseAllowVerbs=1          ; if 1, use [AllowVerbs] section, else use [DenyVerbs] section
UseAllowExtensions=0     ; if 1, use [AllowExtensions] section, else use
[DenyExtensions] section
NormalizeUrlBeforeScan=1 ; if 1, canonicalize URL before processing
VerifyNormalization=1    ; if 1, canonicalize URL twice and reject request if a change
occurs
AllowHighBitCharacters=0 ; if 1, allow high bit (ie. UTF8 or MBCS) characters in URL
AllowDotInPath=0         ; if 1, allow dots that are not file extensions
RemoveServerHeader=0     ; if 1, remove "Server" header from response
EnableLogging=1          ; if 1, log UrlScan activity
PerProcessLogging=0      ; if 1, the UrlScan.log filename will contain a PID (ie.
UrlScan.123.log)
AllowLateScanning=1      ; if 1, then UrlScan will load as a low priority filter.
PerDayLogging=1          ; if 1, UrlScan will produce a new log each day with activity in
the form UrlScan.010101.log
RejectResponseUrl=       ; UrlScan will send rejected requests to the URL specified here.
Default is /<Rejected-by-UrlScan>
UseFastPathReject=0      ; If 1, then UrlScan will not use the RejectResponseUrl or allow
IIS to log the request
; If RemoveServerHeader is 0, then AlternateServerName can be
; used to specify a replacement for IIS's built in 'Server' header
AlternateServerName=

[AllowVerbs]
;
; The verbs (aka HTTP methods) listed here are those commonly
; processed by a typical IIS server.
;
; Note that these entries are effective if "UseAllowVerbs=1"
; is set in the [Options] section above.
;
GET
HEAD
POST
OPTIONS

[DenyVerbs]
;
; The verbs (aka HTTP methods) listed here are used for publishing
; content to an IIS server via WebDAV.
;
; Note that these entries are effective if "UseAllowVerbs=0"
; is set in the [Options] section above.
;
PROPFIND
```

PROPPATCH
MKCOL
DELETE
PUT
COPY
MOVE
LOCK
UNLOCK
SEARCH

[DenyHeaders]

;
; Request headers listed in this section will cause UrlScan to
; reject any request in which they are present.
;
; Headers should be listed in the form
; Header-Name:
;
;

If:
Lock-Token:

[AllowExtensions]

;
; Extensions listed here are commonly used on a typical IIS server.
;
; Note that these entries are effective if "UseAllowExtensions=1"
; is set in the [Options] section above.
;
;

.asp
.cer
.cdx
.asa
.htm
.html
.txt
.jpg
.jpeg
.gif

;.idq
;.htw
;.ida
;.idc
;.shtm
;.shtml
;.stm
;.htr
;.printer

[DenyExtensions]

;
; Extensions listed here either run code directly on the server,

```

; are processed as scripts, or are static files that are
; generally not intended to be served out.
;
; Note that these entries are effective if "UseAllowExtensions=0"
; is set in the [Options] section above.
;

; Deny executables that could run on the server
.exe
.bat
.cmd
.com

; Deny infrequently used scripts
.htw ; Maps to webhits.dll, part of Index Server
.ida ; Maps to idq.dll, part of Index Server
.idq ; Maps to idq.dll, part of Index Server
.htr ; Maps to ism.dll, a legacy administrative tool
.idc ; Maps to httpodbc.dll, a legacy database access tool
.shtm ; Maps to ssinc.dll, for Server Side Includes
.shtml ; Maps to ssinc.dll, for Server Side Includes
.stm ; Maps to ssinc.dll, for Server Side Includes
.printer ; Maps to msw3prt.dll, for Internet Printing Services

; Deny various static files
.ini ; Configuration files
.log ; Log files
.pol ; Policy files
.dat ; Configuration files

.asp
.cer
.cdx
.asa
[DenyUrlSequences]
.. ; Don't allow directory traversals
./ ; Don't allow trailing dot on a directory name
\ ; Don't allow backslashes in URL
: ; Don't allow alternate stream access
% ; Don't allow escaping after normalization
& ; Don't allow multiple CGI processes to run on a single request

```