Global Information Assurance Certification Paper

SANS GCWN Practical Assignment
AD Merger: Design, Application and Audit
Charles Pham
April 2004
Version 3.2 Option 1

Table of Contents

Abstract

This pager is the written to meet the practical assignment requirement for the SANS GIAC Certified Windows Administrator. The pager consists of three main parts.

The first part focused on the design of a merged domain for SANS Co. and GIAC enterprise, both fictional companies and each with its own Active Directory infrastructure. The AD design for SANS Co. was created and merged with an existing design for GIAC enterprise created and submitted to SANS by existing GCWN analysts.

The second part focused on the creation, application and testing, and evaluation of Active Directory Group Policy. Creation of the Group Policy would meet the business and security requirements of the merged design described in the first part. The Group Policy is then applied to an IIS server and tested for security and functionality compliance. Evaluation involves the review of the pros and cons of Group Policy capabilities.

The final part focused on the long term auditing of the merged AD infrastructure during its implementation and operation life cycle. The plan outlines the approach from a compliance factor and also that of exception monitoring.

Part #1: Domain Design

Merging of SANS Co. and GIAC Enterprises to expand market and consolidate operations. Develop trusts between their Active Directory (AD) infrastructure to achieve interoperability, consolidate IT overhead with no impact to existing customers.

SANS Co. Company Overview

SANS Co, a brick and mortar company that specializes in sale of widgets. Through exceptional marketing, quality products and support service that are second to none, the company has grown into a multi-million dollars business and employs approximately 100 employees. Headquartered in Canada, the company has an operation office in Taiwan with 70 employees responsible for manufacturing, research and development, human resource and distribution subdivision. The remaining 30 employees are located in Canada and spread across the finance, and sales divisions.

SANS Co. has never ventured into e-commerce due to technology immaturity, consumer adoption and security risks. Their only point of presence on the Internet is an informational website that is used mainly for marketing purpose. Recent market research indicated that e-commerce has reached a critical mass and SANS Co. has decided to explore this venue through merger with GIAC Enterprises, an e-commerce company in all perspective.

SANS Co. Active Directory Infrastructure

The SANS Co. Active Directory forest consists of a root domain with three domains reflecting the structure of the organization. In order to support decentralized administration, an empty root domain was employed with the DNS name sansad.net. Connected to the sans.net domain are the three child domains finance.sansad.net, operation.sansad.net and sales.sansad.net which represent the 3 major departments. Another forest consisting of a standalone tree and a single domain named sanswidget.com was deployed in support of the company publicly accessible server on the DMZ.

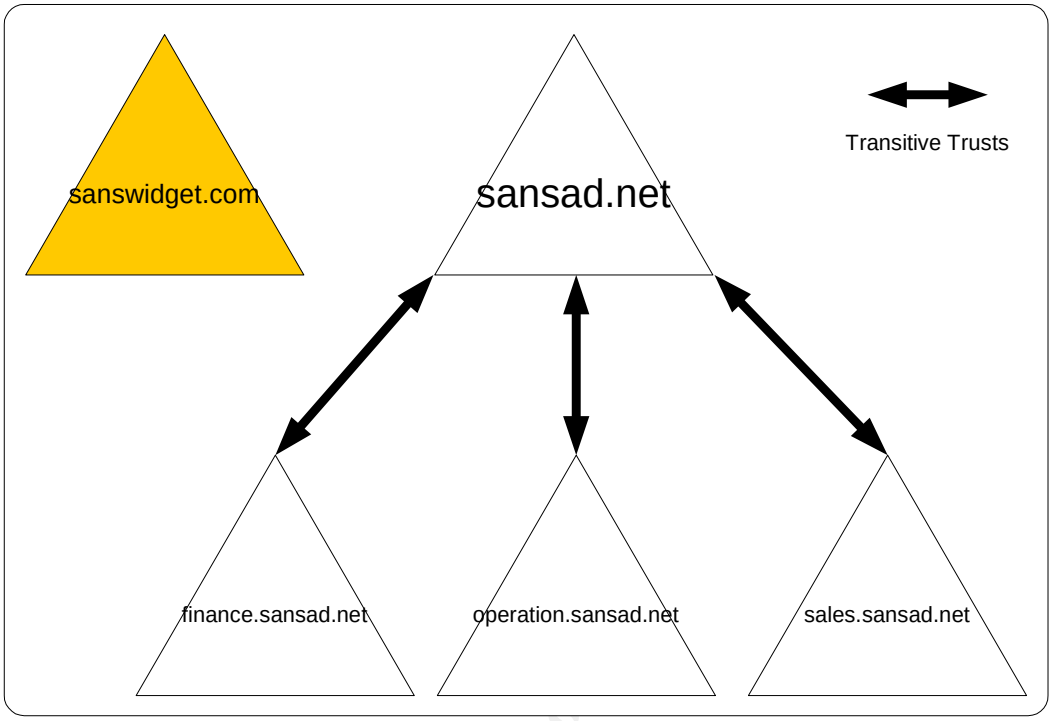


Figure 1. SANS Co. Active Directory Structure

sanswidget.com

This forest has no trust relationship with the sansad.net forest and is managed separately by onsite IT administrators. It is physically located at the company headquarter and is connected to the Internet via a T1 line. The domain sanswidget.com consists of a single Windows 2000 server running IIS providing web and email relay service. Industry best practice for securing IIS was followed in creating this bastion host. DNS records for sanswidget.com web and email services are provided by the upstream Internet Service Provider.

finance.sansad.net

This domain contains users, workstations, servers and printers for the users belonging to accounting, information technology and executive management. All workstations have standard Windows XP image with up-to-date patches and is highly managed. A Windows 2000 server act as domain controller and provides DNS and DHCP services. Another Windows 2000 server provides email via Microsoft Exchange 2000 and Intranet web service via IIS for the whole site.

operation.sansad.net

This domain contains users, workstations, servers and printers for the users belonging to production, research and development, and human resources.

Communication between this site in Taiwan and head office is provided through a VPN tunnel running 256 bit AES[1] encryption on a T1 frame-relay WAN circuit. All workstations have standard Windows XP image with up-to-date patches and his highly managed. A Windows 2000 server act as domain controller and provides DNS and DHCP services. Another Windows 2000 server provides email via Microsoft Exchange 2000 and Intranet web service via IIS for the whole site.

sales.sansad.net

This domain contains users, workstations, servers and printers for the users belonging to sales, and marketing. All workstations have standard Windows XP image with up-to-date patches and is highly managed. A Windows 2000 server act as domain controller and provides DNS and DHCP services.

Organizational Units (OUs)

Ent. Admin: The enterprise admin OU is added to the local admin group of every domain.

Admin: Contains super users that have special requirements to manage the assigned domain.

Domain controller: Contains the organization domain controllers and all are running in native mode.

Server: Contains servers that are deployed internally.

Workstation: Contains workstations that are deployed internally.

Printer: Contains printers that are deployed internally.

Privileged users: Contains group of users with access to sensitive and confidential data such as accounting, human resource, executive management, research and development"

General users: Contains group of users with no special security requirements such as production, sales, and marketing.

[1] AES, http://csrc.nist.gov/CryptoToolkit/aes/

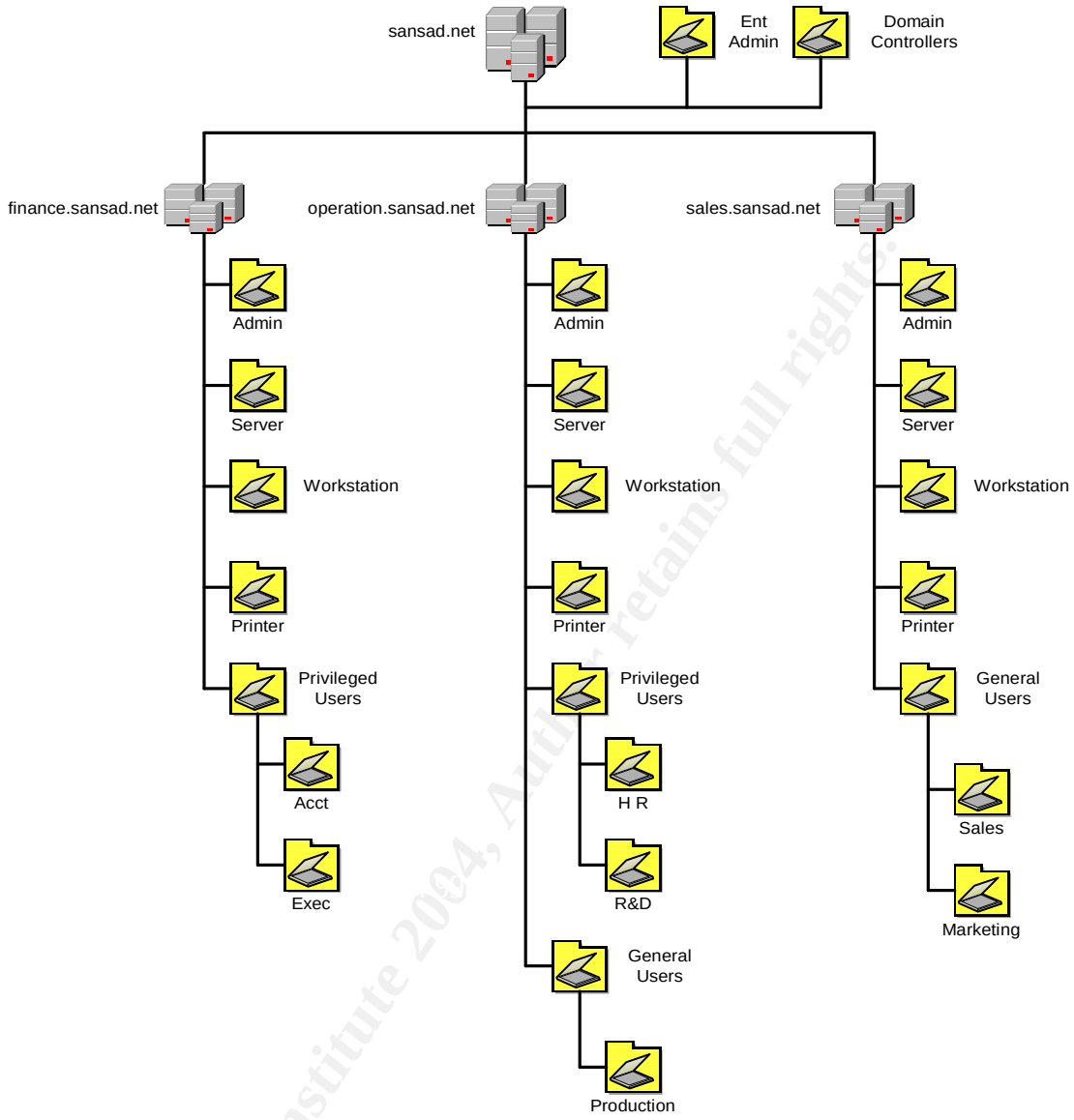


Figure 2. SANS Co. AD OU Hierarchy

Security Consideration

Perimeter security is fully observed with appropriate level of filtering on all the routers, lockdown of servers and strict control of firewall rules, strategic deployment of IDS systems, gateway, servers and workstation deployment of anti-virus software to provide a defense-in-depth approach.

Administrator security is provided through specially assigned admin hosts where administration tasks can be performed and can only be accessed by authorized

administrators via a two factors authentication mechanism. In addition, extensive logging and auditing of users and services are enabled on these hosts.
Domain security required that all domain controllers to use IPSec VPN tunnel for end-to-end replication.

Server security required that all servers are properly hardened and maintained with up-to-date patching process. Servers hosting services such as web, DNS, and DHCP will follow industry best practice on service lockdown.

GIAC Enterprise Active Directory Infrastructure

Design of GIAC Enterprise corporate network is documented in

http://www.giac.org/practical/Lenny_Zeltser_GCWN.doc

GIAC Enterprise is an e-commerce company with majority of its revenue from online sales and has approximately 50 employees. Its corporate office and e-commerce systems are located in Canada, however, are physically separated. The e-commerce systems do not utilize Windows OS due to design requirements and hence do not need to be taken into consideration in the AD integration.

On the corporate network DMZ, a standalone Windows 2000 server provides public web, and mail relay services running on IIS. DNS records for web and mail services are hosted on the ISP. Administration of this server is provided via SMB over IPSec authentication from the internal corporate network.

Internal services are categorized under three departments:

- Research and Development
- Sales and Marketing
- Finance and Human Resources

Research and Development servers and workstations have been segregated from the rest of the internal machine through a Hogwash[2] packet-filtering device as these machines contain data with higher security classifications.

Machines in on the internal network are configured as followed:

- Workstations running on Windows 2000 have since been upgraded to Windows XP.
- Internal servers running on Windows 2000 are scheduled to be upgraded to Windows 2003 sometime in the near future.
- Domain controllers running on Windows 2000 double as DNS servers for all internal hosts.
- Internal mail server runs Microsoft Exchange 2000

[2] Hogwash, http://sourceforge.net/projects/hogwash/

- User's files are stored on departmental servers, as well as a central file server which double as the print server.
- Workstations have been upgraded to use MS Office XP applications running Word, Excel and PowerPoint. MS Access is installed on workstations in the Research and Development department.
- Anti-virus protection is provided through Norton AntiVirus corporate edition
- Large numbers of internal applications are hosted on the internal web server and are accessed via Internet Explorer.

Active Directory Structure

GIAC Enterprise AD design consists of a single Windows 2000 domain supported by two domain controllers with five first-level OUs and three second-level OUs.

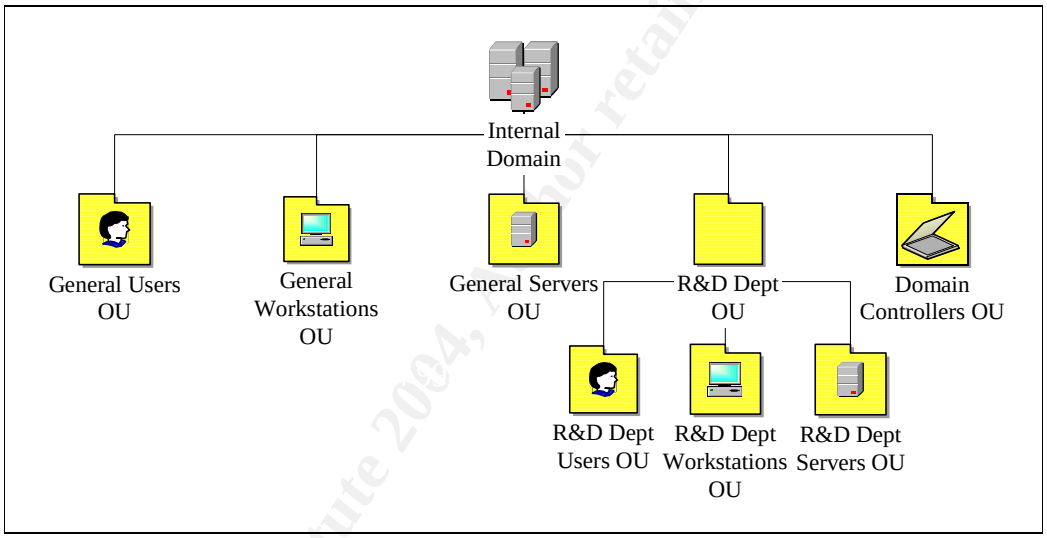


Figure A – AD Hierarchy at GIAC Enterprises

All users, with the exception of R&D department falls under a generic classification and are categorized by the General Users, General Workstations, and General Servers OUs. These OUs are managed by the Domain Admins group.

Management of the R&D Dept OU is delegated to the two local administrators due to differing security policies requirements. Furthermore, enterprise delegations of user password reset and unlock user accounts are granted to two local Help Desk personnel.

The Merger

In order to support the objectives of the merger, the two most significant infrastructure changes were to that of the network and the active directory structure. In addition, cost savings were realized by physically relocating staffs in the GIAC corporate head into the empty offices at the SANS Co. headquarters just a few blocks away.

Network changes

Although physically relocated, GIAC logical network remains relatively intact with a few minor changes.

- Connectivity and segregation of GIAC and SANS Co. was achieved through VLAN implementation.
- DNS records of publicly accessible web and email services for SANS Co. and GIAC are now served by the same internet service provider.
- Hosting of both SANS Co. and GIAC web and email relay are now implemented on the same server with the free-up server running in parallel to provide redundancy. Although hosted on the same server, the contents of the two sites remain independent. As a result, the changes were transparent to customers of both companies. These servers will remain independent of the AD structure within SANS Co. and GIAC enterprise and industry best practice on securing IIS remains fully observed. Administrations of these servers are provided via SMB over IPSec authentication from the GIAC internal corporate network.
- Contents of the new SANS Co. e-commerce venture are hosted on the same e-commerce facility for GIAC enterprise. Due to its robust design, this addition did not affect existing production. It was also decided that this e-commerce facility remains in its current physical location.

AD infrastructure changes

In order to allow customize access privileges, monitor activity and limit the scope of authenticated access between the SANS Co. forest and the GIAC forest, explicit external trusts was created between the domains in these forests. Since external trusts only give one-way trust, both domains must create external trusts to each other.

SANS Co. and GIAC will continue to have their distinct security boundary with separate administration. Administrators in each of the domain can add users and groups in the other domain to the permission lists for resources within their domain. Kerberos authentication protocol referral path must be followed when resources are accessed.

The newly merged company will utilizes security policies that are based on SANS Co.'s security policies. However, some of GIAC's security policies will be adopted where it is deemed advantageous.

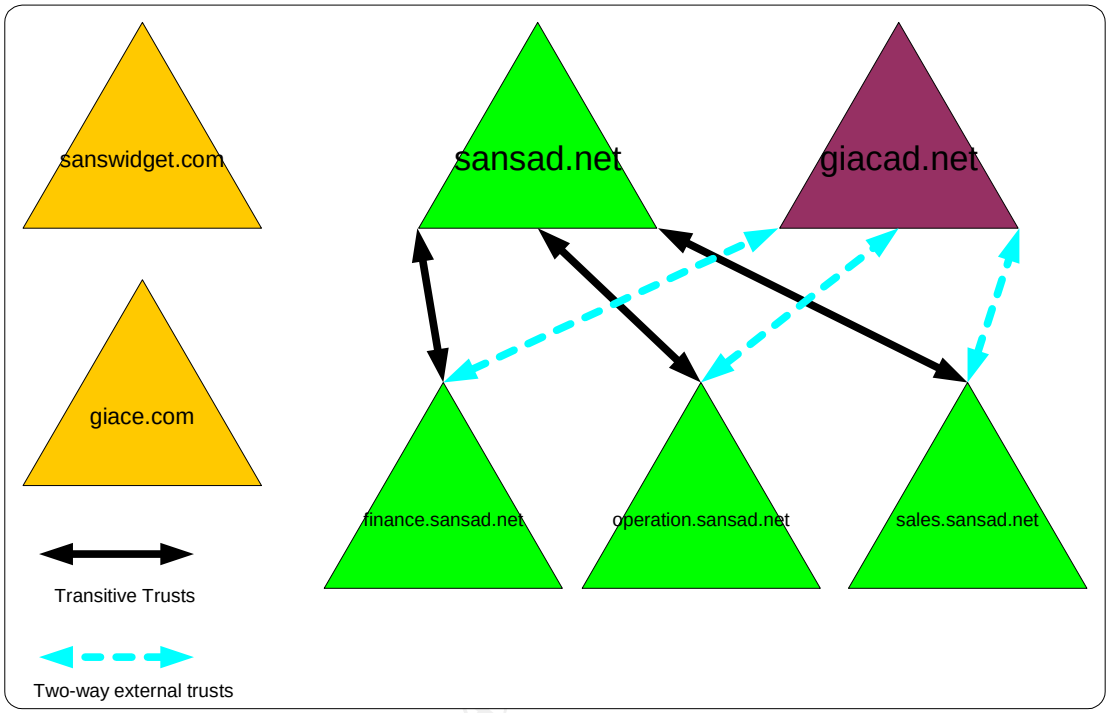


Figure 3. SANS Co. & GIAC Active Directory Structure

Additionally, DNS name resolution is enabled between the two forests to allow users and computers to locate resource in the other company. This can be achieves through DNS zone transfer.

Standard applications on individual workstations are adopted from SANS Co.'s deployment where all machines are equipped with the following applications:

- Microsoft Office XP Word
- Microsoft Office XP Excel
- Microsoft Office XP PowerPoint
- Microsoft Office XP Outlook
- Microsoft Internet Explorer 6
- Mozilla 1.6 as an alternative browser
- McAfee VirusScan Enterprise 7.1 with automated update
- Adobe Acrobat Reader

The following additional applications on the workstations also adopted from SANS Co.'s deployment are available on a need basis:

- Microsoft Office XP Access
- Microsoft Visio
- Visual C++
- Visual Basic

Transitioning of GIAC's users to the above application image was seamless and some users training were required on the changes to McAfee AntiVirus from Norton AntiVirus.

Finally, there is the issue of user visibility of both MS Exchange 2000 systems across the two forests as there is no database replication. The solution was to implement MS Identity Integration Server 2003 Enterprise Edition with MS SQL Server 2000 Enterprise Edition as its back-end store. This enables synchronization and provision of identity information including Exchange 2000 global address lists across the two forests.

Part #2: Security Policy and Tutorial

Provide a Group Policy design to reflect the business needs and security considerations for SANS Co. and GIAC Enterprises. Apply the policy to an IIS server in SANS Co. for further testing and evaluation.

Group Policy Design

The two AD directory infrastructures are managed independently based on the forest separation and by the local on-site administrators but will be based on the same security policies. This means that the policies, although common, can not be applied across the forest. This will be accomplished via the redevelopment of SANS Co. group policy templates that are based on existing sample security templates from the National Security Agency[3]. The newly designed security templates will also try to incorporate existing GIAC security templates whenever possible in order to best avoid potential problem.

The following SANS Co. security templates are re-defined for the application to SANS Co. / GIAC infrastructure:

- Domain.inf – default domain GPO
- Dc.inf – default domain controller GPO
- I_server.inf – default internet server GPO
- Server.inf – default internal server GPO
- Workstation.inf - default workstation GPO
- Admin.adm – default administrator GPO
- Priv_user.adm – default privileged users GPO
- User.adm – default general users GPO

Of the eight security templates, the five *.inf templates are applied to the computers while the three *.adm are applied to the users. This separation of users and computers allows more flexibility in system administration. Computers tend to be static in their purpose while users role are more dynamic. This minimizes the amount of changes required should a user from one group moves to another group which was assigned a different privileges.

SANS Co. management has asked 3rd party companies to provide a RFP for desktop support outsourcing and the initiative will apply to the newly merged company as well. As such, maintaining the separation of users and computers policies would facilitate the handoff should the company decide to go through with the outsourcing provider.

[3] Nation Security Agency Security Recommendation Guides, http://nsa1.www.conxion.com/

The application of the users security policies is new for GIAC's employees and resulted in the loss of control for some of the privileges these employees has previously enjoyed. Although there were some lockdown on the GIAC's employees' computer, the adoption of SANS Co.'s security templates was more restrictive. There was an initial outcry from those not being able to personalize their computer system. However, these users come to accept the restrictions as they were not able to provide the business justifications of being able to personalize their machine. This would not have been entirely possible if it was not for management support and buy-in of highly-managed workstation solution.

Domain.inf

Account Policies -> Password Policy

Settings are based on the SANS Co.'s adoption of the NSA security template w2k_domain_policy.inf with the following exceptions as per GIAC's requirements.

Policy options	Settings
Enforce password history	10 passwords
Minimum password age	5 days
Minimum password length	10 characters

Lowering the enforce password history from 24, as per SANS Co. adoption of NSA recommendation, to 10 passwords allows users to re-use historical password as per GIAC's requirements. This in effect lowers the security level but increases user's friendliness. Increasing minimum password age prevent users from temporarily changing the password as per GIAC's requirement. For SANS Co.'s users, this was a non-issue as these users have already embraced this practice without enforcement. Lowering the minimum password length from 12 to 10 characters, as per GIAC's requirement, lowers the security level but increased user's friendliness. This increases the security of SANS Co.'s existing policies of 8 characters minimum password. Training users to use passphrase instead of password continues to be a challenge.

Account Policies -> Account Lockout Policy

Policy options	Settings
Account lockout duration	15 minutes

Lowering account lockout duration from GIAC's 2 hours to the SANS Co. adoption of the NSA's default 15 minutes to achieve better balance between brute-force password attack protection and usability during "off-hours". Since the new merged company has offices in conflicting time zones, it would be a business impediment to not be able to access resource in the remote domain in a timely manner.

In addition, the following security options are adopted from SANS Co. from the NSA's recommendations at the domain level:

Local Policies -> Security Options

Policy options	Settings
Interactive logon: Message text for users attempting to log on	This system and data belong to SANS Co. / GIAC company. Use of this system constitutes consent to monitoring.
Interactive logon: Message title for users attempting to log on	Warning – Authorized Users Only.

Consultation with legal and human resources department brought about the logon message settings. The preference was to use SANS Co.'s message and add GIAC name to the text. The message serves as a warning to users attempting to connect to the merged company resources that their actions might be audited and that trespassers will not be tolerated.

Dc.inf

Adopted from SANS Co.'s interpretation of the NSA's security template w2kdc.inf with the following exceptions:

Local Policies -> Security Options

Policy options	Settings
Automatically log off users when logon time expires	Not defined
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key.	Enabled
LAN Manager Authentication Level	Send NTLMv2 only\refuse LM & NTLM

The option of log off users when logon time expires as per GIAC's settings was reset to "not defined" as the restriction would impose administrative overhead when considering remote office connectivity. The cost associated with the overhead was deemed to overweight the security benefit offered by this setting.

Force secure channel communications to use strong encryption and further enhance the security of all data passing through the channel even though it might affect performance. This was adopted from the SANS Co. settings and was imposed on GIAC's without any resulting problem.

Update LAN manager authentication level for GIAC's setting to SANS Co.'s adoption of the NSA's recommended setting as all GIAC's computers have been upgraded and can support NTLMv2 natively. The settings were default on SANS Co.'s computers as they were all capable of supporting NTLMv2 natively and no changes were required after the merger.

Event Log -> Settings for Events Logs

Policy options	Settings
Maximum application log size	524280KB
Maximum security log size	524280KB
Maximum system log size	524280KB
Retention method for application log	Overwrite events as needed
Retention method for security log	Overwrite events as needed
Retention method for system log	Overwrite events as needed
Shut down the computer when the security audit log is full	Disabled

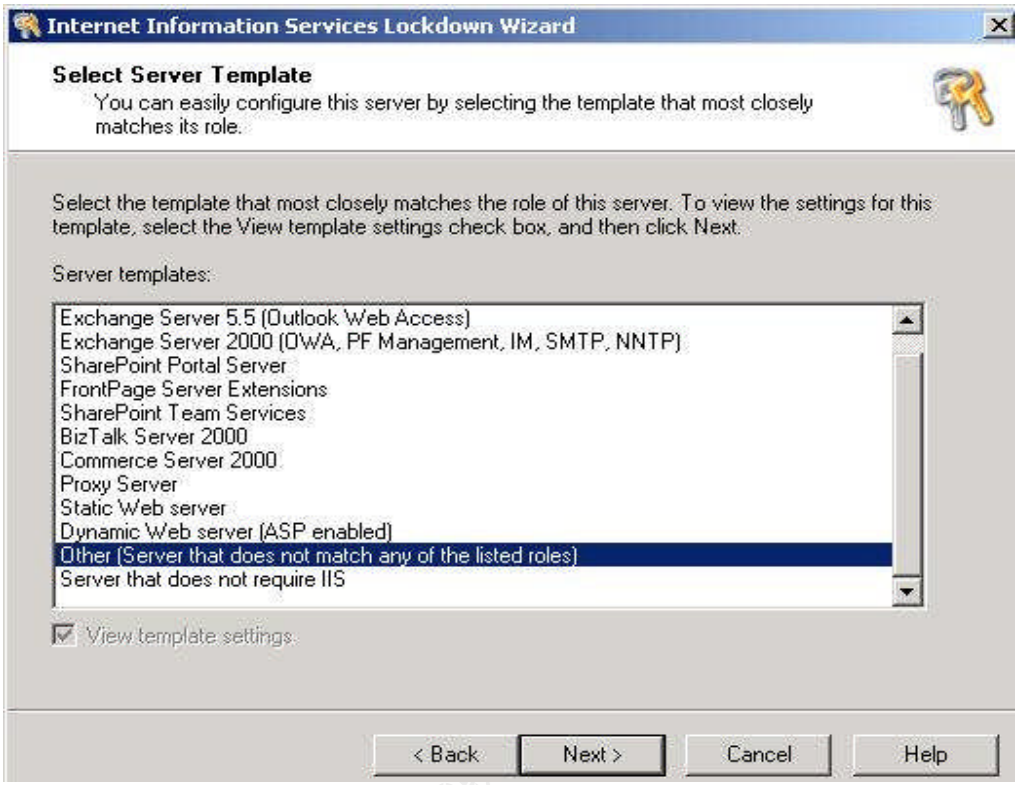
Using GIAC's establish solution for log archival, the above settings were modified from the SANS Co.'s adoption of the default NSA's recommended settings. The logs are automatically incorporated into a dedicated database for archival and reporting purposes using ELM Enterprise Manager[4]. Prior to the merger SANS Co.'s has no additional cost associated with the handling of the logs based on NSA's recommended settings. As part of the merger review, the ELM Enterprise Manager was deemed far superior and a more secure solution, hence this off-load archival solution was expanded to includes SANS Co.'s servers as well. The associated cost was manageable considering the benefits associated.

I_server.inf

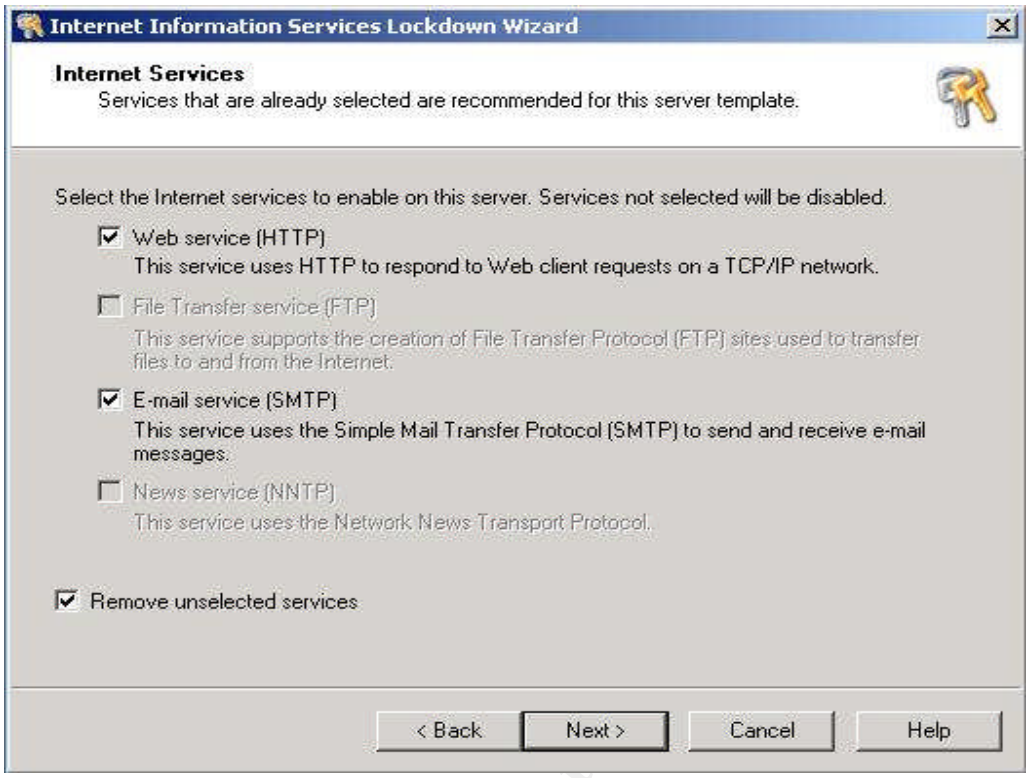
The IIS server was locked down according to Microsoft IIS 5.0 Baseline Security Checklist[5]. The IIS Lockdown[6] tool disables and uninstalls unneeded services, removes default script mappings, disables sample applications, installs URLScan

[4] ELM Enterprise Manager, http://www.tntsoftware.com/Products/EEM/
[5] IIS 5.0 Baseline Security Checklist, http://www.microsoft.com/technet/security/chklist/iis5cl.mspx
[6] IIS Lockdown Tool, http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC

and a more to harden IIS. The following screen shots illustrated the selected options for the IIS Lockdown tool:

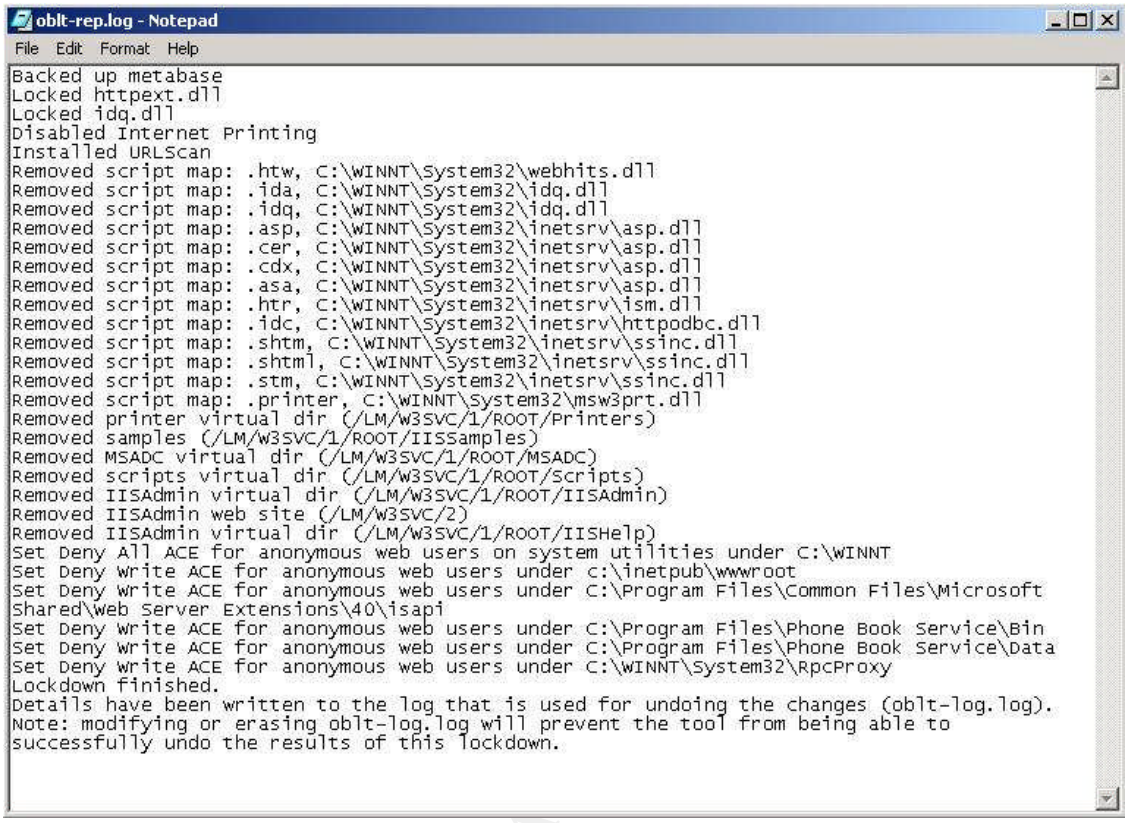


The “Other (Server that does not match any of the listed roles)” was selected and clicking on next brought about the services offered in IIS as shown in the screen below:



The two services HTTP and SMTP are selected as required and clicking on next bring about the “Script Maps” screen. All the options were selected for disabling on this screen as well as the subsequent screen “Additional Security”. In the next screen, enable the URLScan filter and clicking on next to go to the application screen.

Verification of a successful application of the Lockdown tool is done by viewing the log file which is shown below:



In addition NetBIOS protocol was disabled to force the system to use SMB over TCP port 445 as previously set in GIAC's public server. The above application of using SMB over TCP port 445 to the SANS Co.'s server did not cause any problem as it did not conflict with previously set services.

This security template is applied to the standalone HTTP and SMTP server that is accessible to Internet users. Its security settings are based on the internal server "server.inf" security template described below with the following exceptions:

Local Policies -> User Rights Assignment

Policy options	Settings
Access this computer from network	Administrators Web Anonymous Users and Web Applications
Log on as a batch job	Web Anonymous Users and Web Applications
Log on locally	Administrators Web Anonymous

	Users Web Applications

Web Anonymous Users and Web Applications groups are created by IIS Lockdown Tool. Access for these two user groups are severely limited through NTFS permissions. This will help protect the server from a complete compromise in the event of exploitation of an unknown vulnerability. This was the default settings on SANS Co.'s server and its application on GIAC's services was seamless.

Local Policies -> Security Options

Policy options	Settings
Network Security: Maximum number of half-open retired TCP sockets to maintain	160
Network Security: Maximum number of half-open TCP sockets to maintain	200
Network Security: Protect against SYN attacks	Best protection

Enabled Syn DoS attacks protection though limiting the resources associated with half-open TCP sockets and by controlling the timeout associated with the retransmission of SYN-ACKs. However, this protection comes at a slight cost to performance but will have no noticeable impact to the users through excellent performance capacity management. Again, originally set on SANS Co.'s server, these settings did not cause any problem on GIAC's services.

Event Log -> Settings for Events Logs

Policy options	Settings
Maximum application log size	4194240KB
Maximum security log size	4194240KB
Maximum system log size	4194240KB
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually
Shut down the computer when the security audit log is full	Enabled

Set events log size to maximum and shutdown the server if the audit log is full. As the retention method for the logs is set to manual and the computer to shutdown when the log is full, the system will required extra care and maintenance. Adopted by SANS Co.'s from the NSA's recommendation, these settings has did not cause any problem on the GIAC's services. However, it should be noted that the logs are now locally contained rather than being off-loaded to the ELM Enterprise Manager. This was deemed necessary to reduce the number of open ports through the firewall and to ensure that should the server becomes subjective to a DoS attack, it would not cause performance

problem on the firewall. The policy as adopted from the SANS Co.'s policy is that the server can be the sacrificial lamb should the question of company connectivity versus web and email presence ever arises. A downtime of a day or less for web and email is deemed acceptable. However, connectivity to the remote office or the Internet can not be interrupted for more than 3 hours before productivity is impacted.

System Services

Policy options	Settings
IIS Admin Service	Automatic
IPSEC Policy Agent	Automatic
RPC Locator	Automatic
Server	Automatic
SMTP	Automatic
World Wide Web Publishing Service	Automatic

The IIS Admin Service is required for the SMTP and WWW server administration. The IPSEC Policy Agent is required for providing secure communications, managing IPSec policy, and to act as a packet filtering firewall. RPC Locator is required for remote administration. Server service is required for SMTP service. SMTP service is required for email relaying and World Wide Web Publishing Service is required to provide HTTP. Again, these lockdown settings are adopted from SANS Co.'s security policies and do not impose any additional problem on GIAC's existing services.

SANS Co.'s policy follows the principle of least privileges and is adopted for use across the newly merged company. As such, services that are not explicitly listed below are disabled:

Policy options	Settings
Application Management	Not defined
COM+ Event System	Not defined
Distributed Link Tracking Client	Not defined
DNS Client	Not defined
Event Log	Not defined
Indexing Service	Not defined
Kerberos Key Distribution Center	Not defined
License Logging Service	Not defined
Logical Disk Manager	Not defined
Logical Disk Manager Administrative Service	Not defined
Net Logon	Not defined
Network Connections	Not defined
NT LM Security Support Provider	Not defined
Performance Logs and Alerts	Not defined
Plug and Play	Not defined

Protected Storage	Not defined
Remote Access Auto Connection Manager	Not defined
Remote Access Connection Manager	Not defined
Remote Procedure Call (RPC)	Not defined
Routing and Remote Access	Not defined
RunAs Service	Not defined
Security Account Manager	Not defined
SNMP Service	Not defined
SNMP Trap Service	Not defined
System Event Notification	Not defined
Telephony Service	Not defined
Uninterruptible Power Supply	Not defined
Utility Manager	Not defined
Windows Installer	Not defined
Workstation Service	Not defined

The Application Management service provides software maintenance capability on the server and disabling this service will severely impede server administration. The COM+ Event System is required to support the System Event Notification used to monitors and tracks system event.

Distributed Link Tracking Client service maintains local and remote links within NFTS files by tracking object ID to ensure that shortcuts and OLE continues to work after the file is renamed or moved. This is useful for file administration and the setting was enabled, inheriting from SANS Co.'s setting rather than GIAC's setting, as there was no known vulnerability associated with this service. DNS client service is required to resolves DNS name resolution.

Event Log service is required for viewing of log through Event Viewer. Without this service, events will not be tracked in Application log, Security log and System log. Indexing Service is needed to speedup searching and access to contents on the system. The setting on the GIAC's server was replaced with the SANS Co.'s setting as the associated vulnerabilities were mitigated with up-to-date patches.

Kerberos Key Distribution Center service is needed to allow user to logon to the network via Kerberos v5 authentication protocol. This is potentially useful for administration from the local network. License Logging Service monitors and records client accessing licensing for things such as IIS. Not an absolute must have service but is useful for troubleshooting in case of access problem.

Logical Disk Manager and Logical Disk Manager Administrative Service are required for dynamic disk administration. Not an absolute must have but is useful nevertheless. Net Logon service is required to authenticate users and services on the computer. Network Connections service is required to client side configuration of the network and its media.

NT LM Security Support Provider service is required to provide logon authentication via NTLM authentication on stand-alone system. This is needed for local server administration. Performance Logs and Alerts service is needed to collect information on server performance. This is needed to ensure that the server will be able to provide service at a satisfactory level. Also act as a useful metric to monitor in the event of a DoS attack.

Plug and Play service is required to automatically recognize and adapt to new hardware changes. Not absolute requirement but is very useful for server administration activities such as hardware swap. Protected Storage service is required to protect sensitive information such as private keys, certificates, Secure Multipurpose Internet Mail Extensions (S/MIME) and Secure Socket Layer (SSL).

Remote Access Auto Connection Manager and Remote Access Connection Manager service allow automatic administration of the network connection such as the VPN. Remote Procedure Call (RPC) service is required to provide inter-process communications (IPC) and provides support to a large number of system services. The operating system needs this service to be enabled in order to load.

Routing and Remote Access service is required to provide support for the VPN connection. RunAs Service is useful for system administration by allowing commands to temporarily run as Administrator from a restricted user account.

Security Account Manager service is a core operating system service and is used by the system to manage user and group account information. This service also supports other system services. SNMP Service and SNMP Trap Service are useful in monitoring and auditing network performance and usage. Network fault in local network routing device can be detected and forwarded to the local server for contingency action.

Telephony Service is required to support Remote Access Service. The setting is enabled as per SANS Co.'s setting rather than GIAC's setting with no impact to GIAC's services. Uninterruptible Power Supply is required to support the UPS device connected to the serial port for contingency purpose. Utility Manager service is a useful administrative tool that control accessibility.

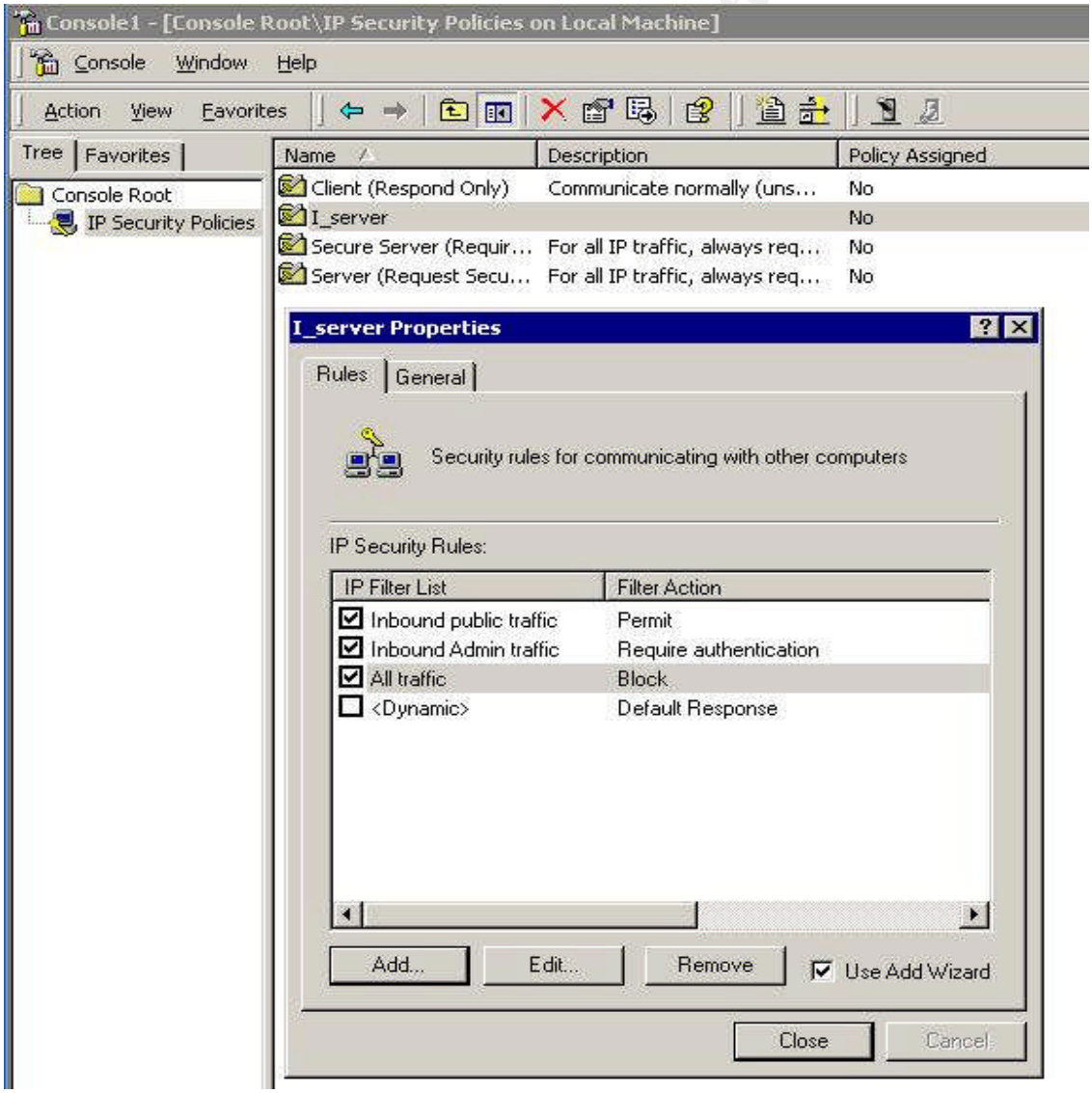
Windows Installer service is required for system administration task such as installation and removal of applications. Workstation Service is required to create and maintains client network connections. The setting is enabled as per SANS Co.'s setting as the associated vulnerabilities were mitigated with up-to-date patches with no impact on GIAC's services.

The Winalysis software was removed from all GIAC's servers as the administrative cost of maintaining and supporting this software out-weight the benefits. A lot of the associated benefits were already offered through the

security policies and settings and although might not be as comprehensive, they are deemed sufficient.

The final lockdown involves using IPSec filtering, through IP Security Policies on Local Machine snap-in for MMC, to provide another layer of defense. As previously discussed in GIAC's design documentation, the following filters are created to meet the business and administration needs:

- inbound with mirrored TCP port 25 and 80
- inbound with mirrored TCP port 445 from specifics admin workstation and required authentication using MD5 protocol.
- Block all other traffic.



Server.inf

Settings for server security template are derived SANS Co.'s policy adopted from the NSA's security template w2k_server.inf with the following exceptions:

Account Policies -> Password Policy and Account Lockout Policy are left undefined as these shall be inherited from the default domain policy.

Event Log -> Settings for Events Logs

Policy options	Settings
Maximum application log size	524280KB
Maximum security log size	524280KB
Maximum system log size	524280KB
Retention method for application log	Overwrite events as needed
Retention method for security log	Overwrite events as needed
Retention method for system log	Overwrite events as needed
Shut down the computer when the security audit log is full	Disabled

Again, the options are set to support ELM Enterprise Manager as previously mentioned under the domain controller security template. This was adopted from the GIAC's setting and application to the SANS Co.'s servers was without problem as previously mentioned.

Although re-using the domain controller security policy is entirely possible for the internal server, separation of this policy and the domain controller policy provides much flexibility at a minimal cost to administration.

Production servers in the R&D department will abide by the same security template without exception. This was changed according to SANS Co.'s setting which make the distinction between production servers and test servers. Test servers in the R&D department will be managed locally by the developer groups as per development project. These servers are not interconnected with the production servers and will be localized to the test environment. This allows developers greater flexibility in testing and quicker turnaround time as the project proceeds through the various development life cycle. The GIAC's R&D team will no longer be able to test their codes on production servers; however, this is more than compensated for through dedicated test environment.

Workstation.inf

Adopted from the SANS Co.'s interpretation of the NSA's security template workstation.inf with the following exceptions:

Account Policies -> Password Policy and Account Lockout Policy are left undefined as these shall be inherited from the default domain policy.

Local Policies -> Audit Policy

Policy options	Settings
Audit system events	Failure

Since log space is at a premium, only log system events failure. This setting is adopted from the SANS Co.'s policy and application of this setting on GIAC's workstation was seamless.

Event Log -> Settings for Events Logs

Policy options	Settings
Maximum application log size	20480KB
Maximum security log size	20480KB
Maximum system log size	20480KB
Retention method for application log	Overwrite events as needed
Retention method for security log	Overwrite events as needed
Retention method for system log	Overwrite events as needed

As mentioned in GIAC's documentation, workstations have less disk space than servers and hence log size shall be set to a maximum size of approximately 20MB. In addition, setting the retention method for log to overwrite as needed means events will be kept for as long as possible given other constraints. Previous settings for SANS Co. abided by the NSA's recommendations and no impact is expected as a result of the adoption of this policy.

Application of EFS and Folder Redirection was adopted from GIAC as SANS Co. did not have such policy in place. However, based on the associated security benefits, management has given the blessing to have the complete rollout in the newly merged company. There was slight performance hit to the SANS Co.'s machines after EFS was deployed but was not significant enough to impact productivity. Deployment of Folder Redirection on SANS Co.'s machines required users awareness training but for most was a non-issue as the changes was seamless. It should be noted that network bandwidth utilization did increase by 15% as a result of increase network traffic but was within acceptable limit.

Software management is adopted from SANS Co.'s deployment of IBM Tivoli Configuration Manager[7] as it is more robust. The transition of GIAC's users onto Tivoli was completed without major complications.

Admin.adm

Inherited from the SANS Co.'s template, this group consists of domain administrators, excluding the enterprise admin which does not have a GPO applied, required special privileges to perform their duties. For administrators previously from GIAC's, these lockdown was a bit more restrictive. However, did not interfere with their job duties. The settings are too numerous to list and only highlights are listed below:

- Enable access to Task Scheduler
- Enable access to Windows Update
- Disable Active Desktop
- Allow access to the Control Panel
- Allow changing wallpaper
- Password protect the screen saver
- Allow access and modification of LAN connection properties
- Allow access to the command prompt and run menu
- Allow access to registry editing tools
- Prompt for password on resume from hibernate / suspend

Priv_user.adm

Inherited from the SANS Co.'s template, these users are restricted from making changes to their machine although not quite as severe as the general users. The R&D dept and other in this group required the flexibility to make certain changes to their machine. For the GIAC's R&D users, this lockdown was a bit more restrictive and at the same time allows them more freedom to in controlling their Internet Explorer settings. The settings are too numerous to list and only highlights shall be listed below:

- Disable access to remote Desktop Sharing
- Restrict user from entering author mode for MMC
- Disable Active Desktop
- Password protect the screen saver
- Prevent access to registry editing tools
- Prompt for password on resume from hibernate / suspend

[7] IBM Tivoli Configuration Manager 4.2.1, http://www-306.ibm.com/software/tivoli/products/config-mgr/enhancements-4-2.html

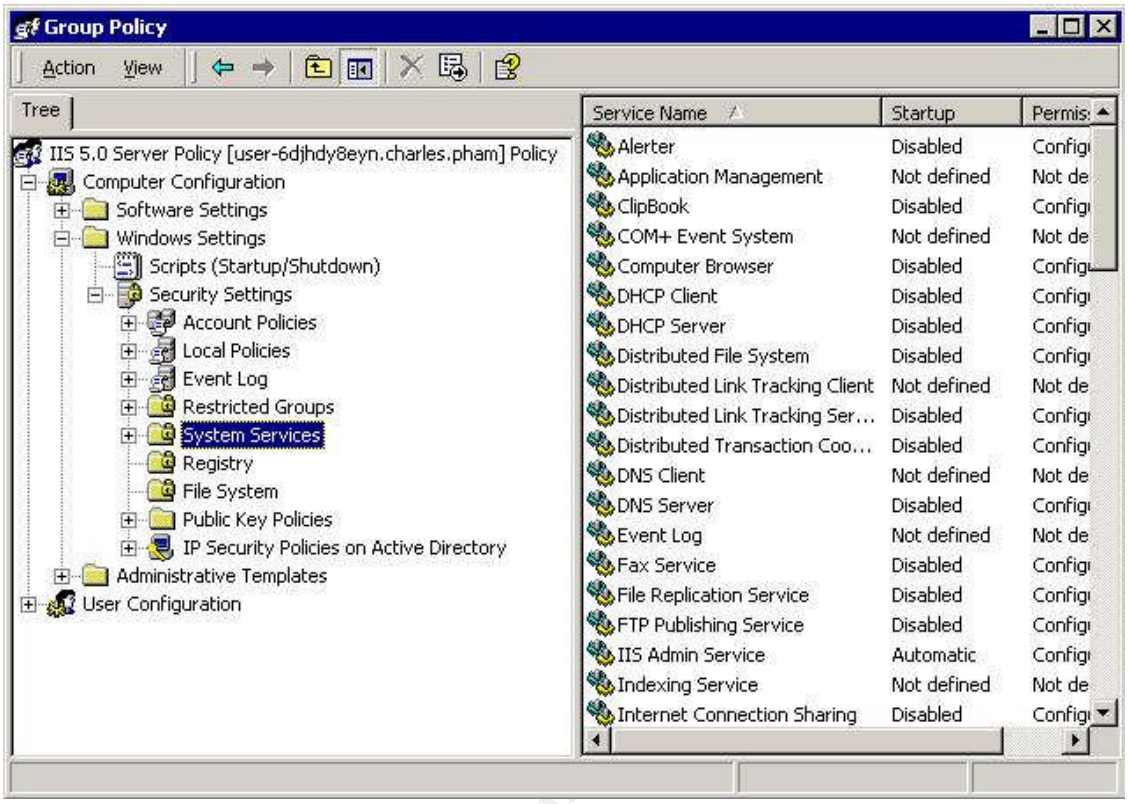
User.adm

Inherited from the SANS Co.'s template, these users are severely restricted from making any changes to their machine. The vast majority of the users are placed in this group. For GIAC's users, this lockdown was more restrictive than they previously experienced. There settings are too numerous to list and as such only highlights shall be listed below:

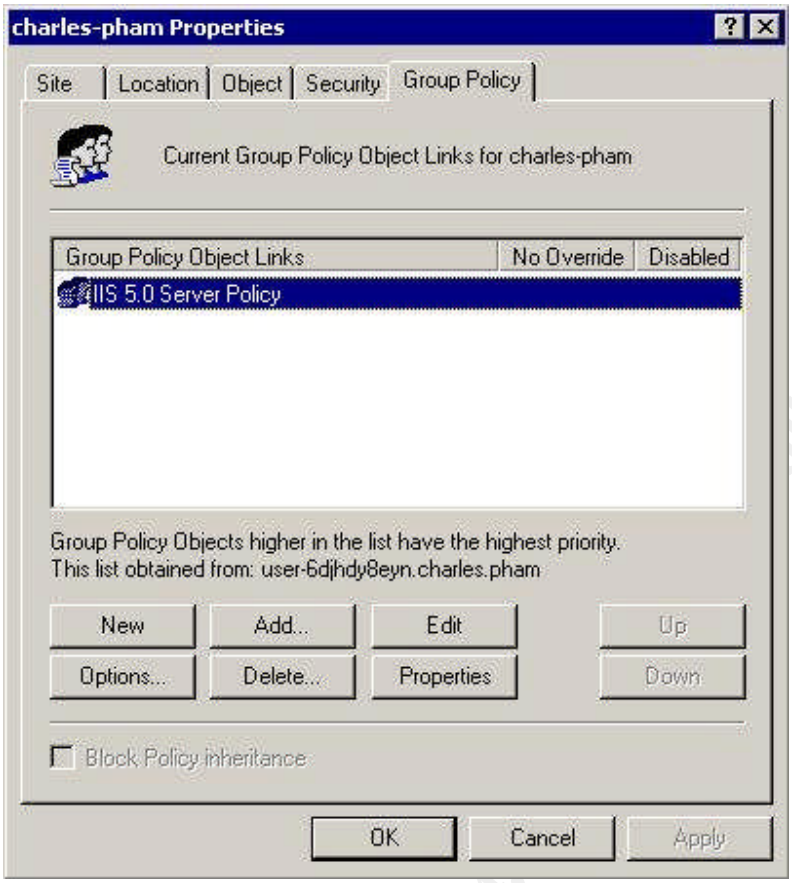
- Disable access to remote Desktop Sharing
- Disable user's ability to make changes to Internet Explorer's security and configurations.
- Disable access to Task Scheduler
- Prohibits user installs
- Disable access to Windows Messenger
- Prevent use of offline files
- Disable NetMeeting chat
- Restrict user from entering author mode for MMC
- Disable user access to Windows Update
- Don't save Desktop settings at exit
- Disable Active Desktop
- Prohibit access to the Control Panel
- Prevent changing wallpaper
- Password protect the screen saver
- Remove Theme option
- Prevent addition and deletion of printers
- Prohibit access and modification of LAN connection properties
- Prevent access to the command prompt and run menu
- Prevent access to registry editing tools
- Remove Task Manager
- Prompt for password on resume from hibernate / suspend

Apply the Group Policy

Apply the policy to the IIS Server accessible from the Internet in SANS Co. To start, the templates need to be imported into the GPO for this IIS Server.



Once the GPO is ready, it can be applied through the Active Directory Sites and Services or Active Directory Users and Computers MMC snap-ins. The GPO can be linked to the site, domain, or OU by selecting its properties through right-clicking then going to the group policy interface. However, since the Internet accessible IIS server is not part of any AD domain, application of the GPOs will be made on the local machine using MMC snap-ins for tutorial purpose. Applications and screen shots of the AD tools are for the tutorial purpose and do not reflect actual implementation. Given the resource limitations, i.e. lack of machines for infrastructure test lab, improvisation of certain setups were required. In this test environment, screen-shots of the AD tools were captured on the IIS server which was also temporary promoted to a Domain Controller.



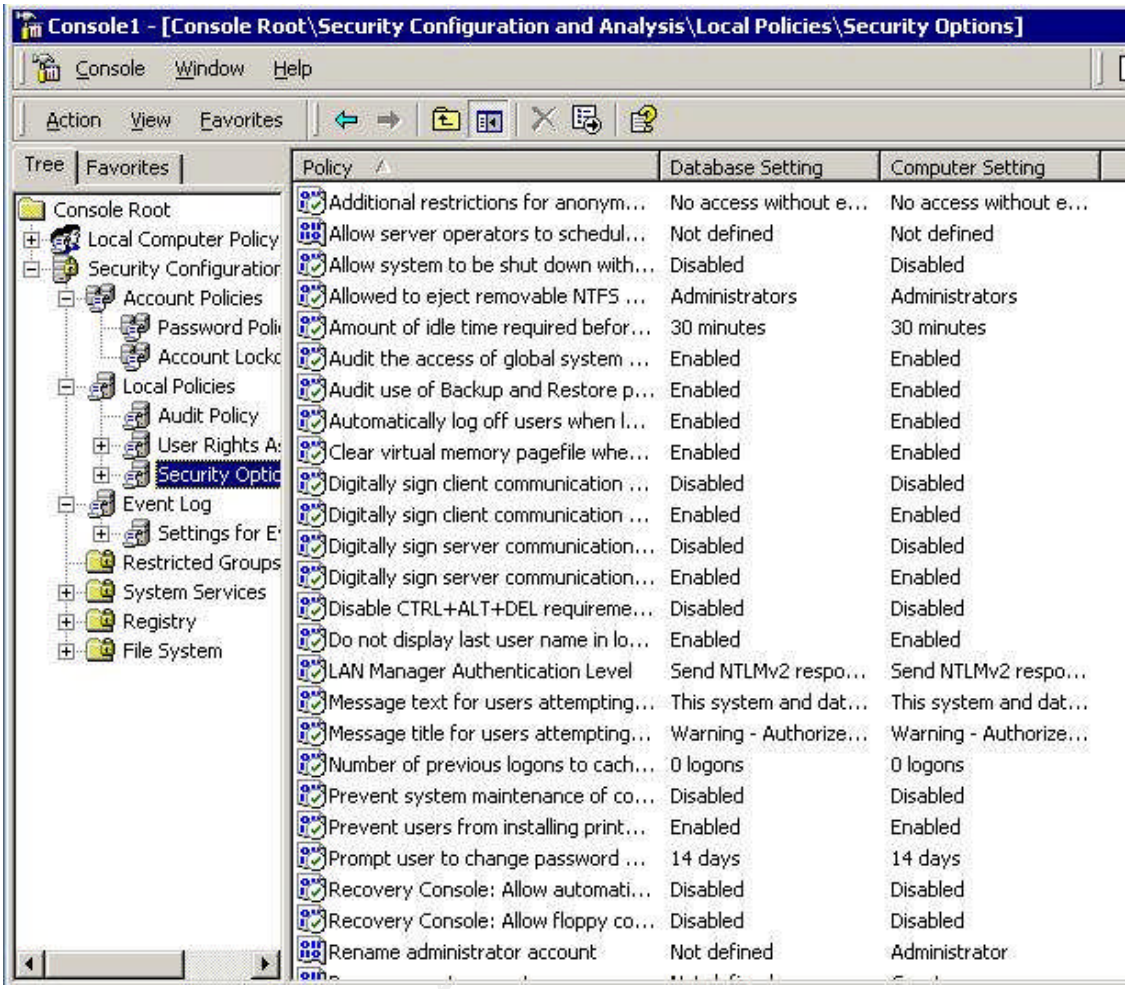
Group Policy settings will use the default refresh rate of every 90 minutes with 30 minutes randomized offset for member servers. The 30 offset help ensures that Group Policy refresh will not congest the network. As such, Group Policy refresh can occur from 90 to 120 minutes apart.

In situation where a forced refresh is desired, the following command line program can be executed on the client machine:

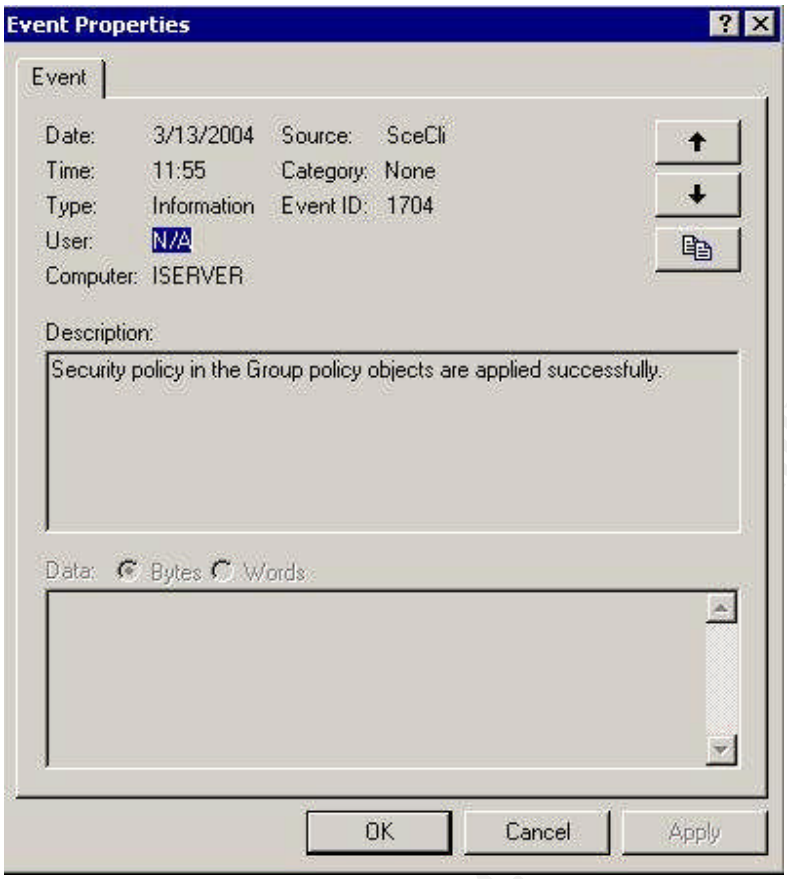
- Secedit /refreshpolicy

Test the policies' security settings

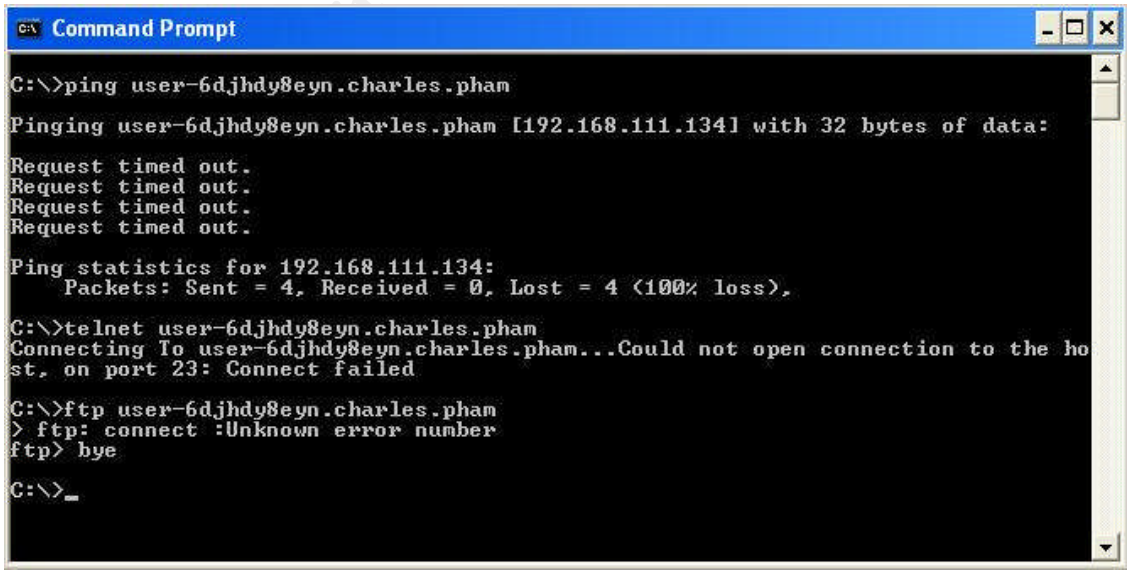
Once the GPO has been applied, the Security Configuration and Analysis MMC snap-in tool was used on to verify that the group policy security settings were applied to the server. The I_server.inf security template was imported for analysis. Going through the results, a green checkmark is shown beside all matching entries compared between the template and what is on the computer. Seeing that there is no red cross displayed in any of the categories indicated that the settings have been applied successfully.



Successful application of the Group Policy is also verified in the application log as below:

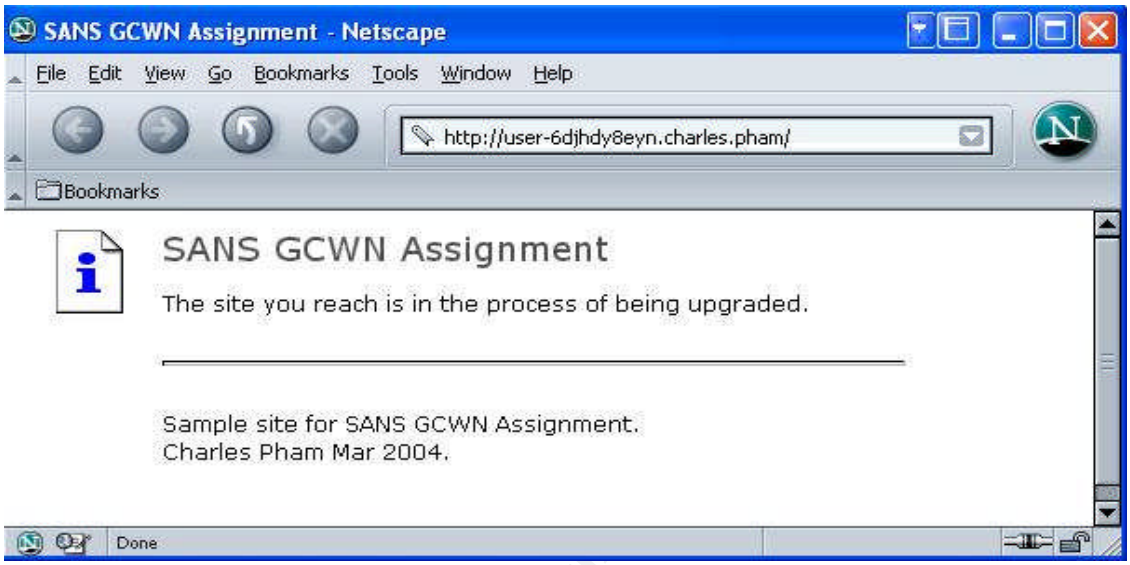


Ping (ICMP protocol), telnet (service provided by the OS), and ftp (service provided by IIS) were used to verify that the IPSec filter is functioning as per the system security settings.



Test the system's functionality

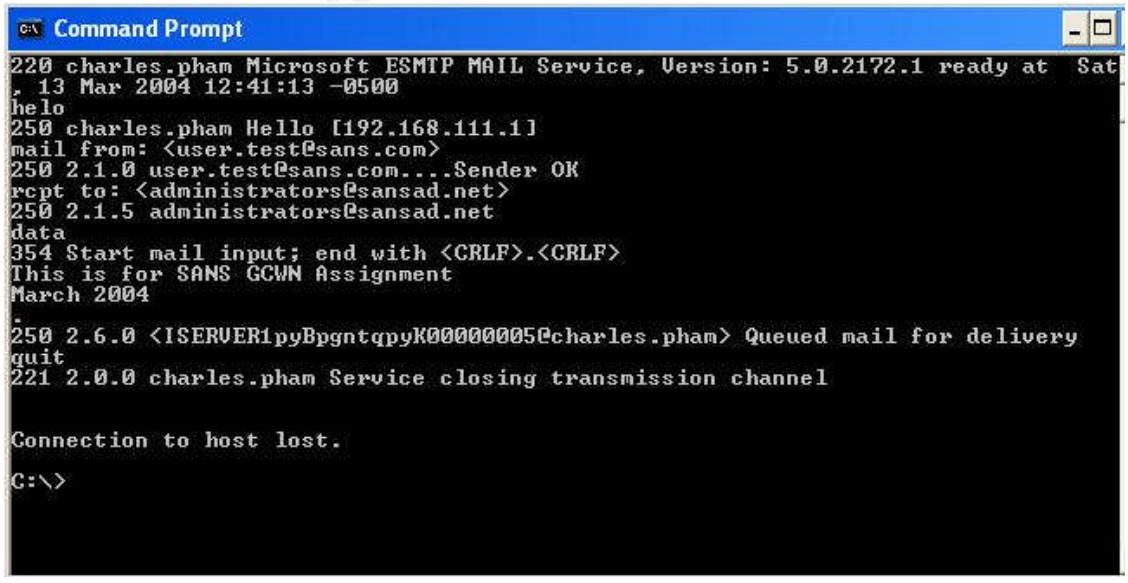
The first functionality test is to the web server. As shown below, it is working as expected.



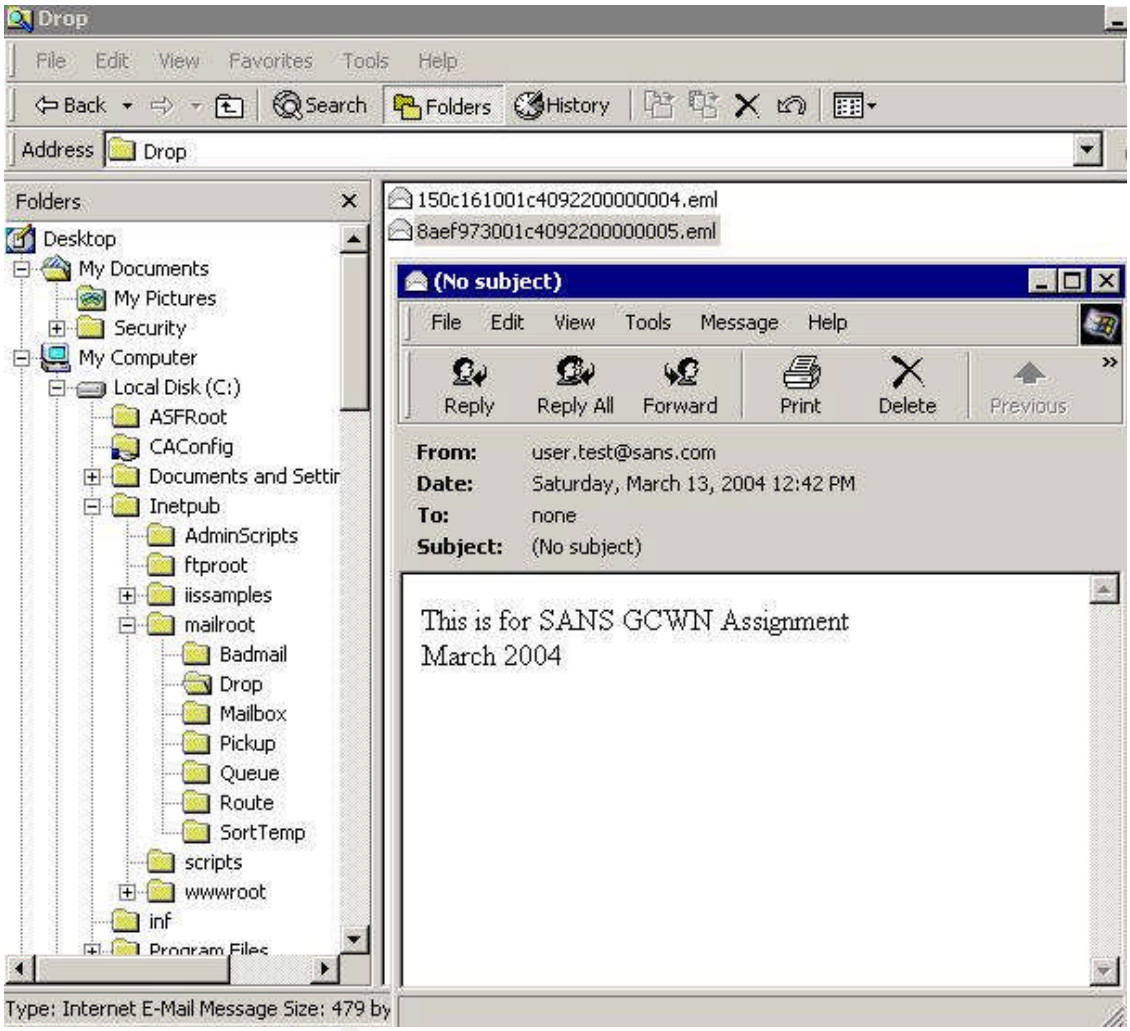
Access was logged on the web server as followed:

2004-03-13 16:34:11 192.168.111.1 - 192.168.111.134 80 GET /iisstart.asp - 200 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.4)+Gecko/20030624+Netscape/7.1+(ax)

The second functionality test is to the mail relay server. As shown below, it is working as expected.



Checking the mail drop on the server revealed:



As the test revealed, the server is functioning as expected.

Evaluate the Group Policy

Domain GPO is used to apply security to settings such as Password, Account, Kerberos Policy, and Public Key Trust List. Domain controller GPO is used to apply security, applications, user environment to settings such as User Rights, File/Registry Discretionary Access Control Lists, Audit/Event Logs, Local Policies, Administrative Tools, and Standard user settings. At the OU level, there is Computer GPO that can set security and applications controls. In addition, there is Users GPO that can set security, applications, and user environment controls.

GPO inheritance is a double edge sword in that when used properly can significantly reduce the amount of administration. On the other hand, it can create problems that will require significant amount of troubleshooting. Extensive planning and foresight is required to ensure that the lowest level OU will function without flaws. GPO at the highest level should contain the settings that are common to the infrastructure and progress to be more specific down the levels. The needs to be specifics will come at a cost of greater administration as there will be more GPOs required per OU. Hence, it is without doubt that certain sacrifice must be made to settings in order to simplify administration.

It should be noted that Group Policy is one part of the security solution. Other part of the security solution such as system hardening, network level filtering and intrusion detection system should be considered as well.

It is without doubt that Group Policy is extremely useful as a centralized domain management solution. However, proper planning and design must take place prior to actual deployment.

Group Policy applied to the Internet accessible IIS servers did not interfere with its operation. If the same Group Policy were to be applied to other servers with differing services, it is highly probable that the settings might break some functionality.

The Group Policies that was applied to the IIS servers were highly restrictive due to its exposure to the Internet. The Group Policies that are designed for the Internal Servers and Workstations are less restrictive in order to accommodate their dynamic nature. This meets the typical egg-shell security policies that the newly merged company has adopted. The adoption of SANS Co.'s Group Policies and its redesign for the Internal Servers and Workstations were granular, modular and flexible enough to meet the political and administrative requirements for both GIAC and SANS Co.

There were compromises from both GIAC's and SANS Co.'s original security policies. However, the resulting policies incorporated the best of both policies and since they were based on the same security templates (NSA's), the changes were doable without significant impact. SANS Co.'s extensive policies in the use of administrative templates complements GIAC's high-grade security in the use of policies templates and this is demonstrated in the combined policies in the merged company.

Part #3: Audit

Requirements

In an effort to ensure that the Active Directory infrastructure is secured after the merger and throughout its life cycle, a plan was created to provide the level of assurance. Given the size and complexity of the new infrastructure, it is essential that the audit system be as automated as possible. The alternatives of not auditing or hiring lots of administrators to manually perform the tasks would be too costly for the business.

The plan was to have an audit system that can be easily managed by leveraging a network centric design. Other considerations are the ease of deployment, operation, and maintenance; capable of capturing data for forensic analysis, performs self integrity check and raising real-time alerts.

Approach

The audit will be limited to two stages in a project life cycle: that of during implementation prior to production and during operation after production launch. However, since the two infrastructures were already in production, the definition for implementation applies to the Active Directory merge and also stretches to capture the existing designs. The operation phase is then defined as the time at which no further changes are made to the complete the merger of the Active Directory structure and after the completion of the implementation audit.

Implementation Audit:

In this phase, the concern is around compliance of the design and that of the system. Verification is required to ensure that what was designed and documented is what actually is in place. The assurance can be perform by internal information security staffs to review the design for possible security gaps and using tools such Security Configuration and Analysis, GPOTool, GPResult (with /z option), Secedit (with /analyze /db <db template name> option), Microsoft Baseline Security Analyzer[8], Port Reporter[9] and ACLDIAG.EXE. Other tools such as network (eEye Retina[10]) and application (Sanctum Inc. AppScan Audit Edition[11]) level vulnerability assessment are also used to verify the quality of the infrastructure.

[8] Microsoft Baseline Security Analyzer, http://www.microsoft.com/technet/security/tools/mbsahome.mspx
[9] Microsoft Port Reporter 1.0, http://support.microsoft.com/?id=837243
[10] eEye Retina Network Security Scanner, http://www.eeye.com/html/Products/Retina/index.html
[11] Sanctum Inc. AppScan Audit Edition, http://www.sanctuminc.com/solutions/appscanaud/index.html

Although not required, a second level of security assurance is provided through the hiring of external consultants. The results of the internal audit and the external audit are then compared for consistencies and recommendations are derived from the gaps identified.

Security issues that are easily addressed are fixed as quickly as possible. Those that required significant investment are mitigated via various risk management solution and documented for reference and review in the operation audit.

Operation Audit:

The system and process applied needs to be effective throughout the Active Directory infrastructure life cycle. This phase encompasses not only the compliance factor but also the exception factor through near real-time event monitoring. In order to perform near real-time event monitoring, a system is created to extract, gather and consolidate log data from the critical servers such as domain controllers, internal file and printer servers, and HR servers.

Existing solution such as ELM Enterprise Manager, which was deployed in GIAC enterprise, will be scaled up to meets the need of SANS Co. as well. In addition, customized scripts are created to extract additional information such as patch and configuration levels and redirect them to ELM Enterprise Manager. Off-site storage of the collected data is also employed to meet retention requirement.

Data extracted includes:

- Change and use of privileged accounts
- Change to Group Policy Objects
- Change in permissions
- Change to system file and registry
- Change to system accounts
- Change to Active Directory setup
- System performance
- Change to software installed base
- Logon violations
- Applications servers logs

Customized rules, based on site installation, are created to query the database and determine the following through artificial intelligence analytics:

- Exception to baseline configurations and flag them for daily review
- Track system changes and update baseline template
- Identified abnormal activity and provide near real-time notification

Issues identified through follow-up of the near real-time notification and daily

review are tracked and managed through a separate problem management process.

On an annual basis, compliance review is conducted again by the internal information security staffs and separately by independent external consultants. The review should encompass configurations, patch level, design modifications, network vulnerability assessment, and problem management processes. This periodic check is required to validate that any system changes are fully documented, tracked and that the security assurance level is maintained as per originally designed. Gaps identified in the review are addressed via quick and easy solution, risk mitigation techniques and documented for reference in future audit. Tools that can be deployed can be the same as those listed under the implementation audit.

Risks and Considerations

Log from personal computer systems is not collected as the cost of gathering and storing such data is more than what the business could afford. However, events logs are still captured on the local machine and are automatically overwritten as needed. These machines are capable of storing log entries for approximately 2 weeks under normal usage. This is sufficient data for most investigation, given the turnaround time, in the event of a security breach.

There is a risk that excessive logging might affect the performance of the network. Therefore, care must be taken in the configuration of what data to capture so as it will not overwhelm the available network bandwidth. Testing is required to measure the impact to network performance and refinement be made after significant infrastructure changes.

Additionally, there is also a possibility that logging devices might outgrow existing disk space either at the client or at the centralized collector. Threshold must be set based on disk space usage and monitored periodically. It is recommended that such local storage threshold is set at 80% capacity over a period of at least week.

References

1) Clark, Dana. “SANS Co. / GIAC Enterprises Secure AD Integration”. GIAC Certified Windows Security Administrator (GCWN #261). November 30, 2003 URL: http://www.giac.org/practical/GCWN/Dana_Clark_GCWN.pdf (April 28, 2004)

2) eEye Digital Security. “Retina Network Security Scanner”. 2004. URL: http://www.eeye.com/html/Products/Retina/index.html (April 28, 2004)

3) Fossen, Jason. SANS Institute. “Active Directory”. GCWN Course material version 1.5. February 19, 2003.

4) Fossen, Jason. SANS Institute. “DNS and Group Policy”. GCWN Course material version 1.5. February 20, 2003.

5) Fossen, Jason. SANS Institute. “Securing Internet Information Server”. GCWN Course material version 16.1. February 20, 2003.

6) Hogwash. June 27, 2001. URL: http://sourceforge.net/projects/hogwash/ (April 28, 2004)

7) IBM. “Tivoli Configuration Manager 4.2.1”. 2004. URL: http://www-306.ibm.com/software/tivoli/products/config-mgr/enhancements-4-2.html (April 28, 2004)

8) Microsoft. “IIS 5.0 Baseline Security Checklist”. 2001. URL: http://www.microsoft.com/technet/security/chklist/iis5cl.mspx (April 28, 2004)

9) Microsoft. “lislockd.exe lockdown tool 2.1”. October 10, 2002. URL: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC (April 28, 2004)

10) Microsoft. “Microsoft Baseline Security Analyzer V1.2”. February 20, 2004. URL: http://www.microsoft.com/technet/security/tools/mbsahome.mspx (April 28, 2004)

11) Microsoft. “Port Reporter 1.0”. April 22, 2004. URL: http://support.microsoft.com/?id=837243 (April 28, 2004)

12) National Institute of Standards and Technology. “Advanced Encryption Standard”. February 28, 2001. URL: http://csrc.nist.gov/CryptoToolkit/aes/ (April 28, 2004)

13) National Security Agency. “Security Recommendation Guides”. November 24, 2003. URL: http://nsa1.www.conxion.com/ (April 28, 2004)

14) Sanctum Inc. “AppScan Audit Edition””. 2004. URL: http://www.sanctuminc.com/solutions/appscanaud/index.html (April 28, 2004)

15) TNT Software. “ELM Enterprise Manager 3.1”. 2004. URL: http://www.tntsoftware.com/Products/EEM/ (April 28, 2004)

16) Zeltser, Lenny. “Designing a Secure Windows 2000 Infrastructure”. GIAC Certified Windows Security Administrator (GCWN #178). May 3, 2002 URL: http://www.giac.org/practical/Lenny_Zeltser_GCWN.doc (April 28, 2004)