Global Information Assurance Certification Paper

Tomislav Herceg
April 13, 2004

ACTIVE DIRECTORY, GROUP POLICY AND AUDITING SYSTEM DESIGN FOR MERGED WINDOWS 2000 MULTI FOREST ENVIRONMENT

GIAC Certified Windows Security Administrator (GCWN) Practical Assignment
Version 3.2 (revised March 24, 2003)

TABLE OF CONTENTS

ABSTRACT

Two fictions companies SANS Co. and GIAC Enterprise have merged and new Active Directory design is developed. New AD design provides consolidation, interoperability and management of these two companies. Based on defined Active Directory architecture, Group Policy is designed and after that implemented on one web server for test purposes. Finally, overall audit strategy and patch management is developed.

1. INTRODUCTION

This paper represents practical assignment for the GIAC Certified Windows Security Administration program. It consists of three parts that describe the merger of two fictions companies SANS Co. and GIAC Enterprise.

First part contains design of Active Directory domain and network infrastructure in both companies. Network infrastructure and domain design for GIAC Enterprise was taken from Philip M. Cox practical assignment v.3.1 named "Design a Secure Windows 2000 Infrastructure" (http://www.giac.org/practical/Phillip_Cox_GCWN.doc). It also contains domain and network design of SansWGiac, the company which resulted from the fusion, along with the elaboration of major design decisions and benefits on interoperability and overall manageability for new company.

Second part describes Group Policy design and security settings for all domains in new SansWGiac Company and security settings for business critical servers. Certain Group Policy settings will be tested in lab environment. In case of any unusual behavior of GPOs and security settings, problem will be determined and resolved.

Third part discusses the SansWGiac security plan and design of patch management infrastructure. It also describes auditing of network infrastructure and domain servers for checking critical security settings and automatic collection and manipulation of event logs.

2. DOMAIN DESIGN

2.1 SANS COMPANY BASIC FACTS

SANS Co. is company for sea food catering founded in 1990 in Zagreb, Croatia. The company hosts its Web site for catering orders and distribution of their fish specialties to its customers.

SANS Company have offices on 4 locations: main office in Zagreb and 3 regional offices in Rijeka, Split and Dubrovnik. It has 88 employees organized in 5 departments. In main office there are Finance & Human Resource department, Sales & Marketing department and Information Technology department.

Having in mind that SANS Company's core business is sea food catering; Sea Food Research department and Purchase department are established in regional offices situated in cities on Adriatic coast (Istra and Dalmacija). Such organization simplifies the process of sea food supply from local fishermen and also enables application of new methods for sea food cultivation and protection of sea flora and fauna. Information Technology department in every regional office is established to provide IT support to company's employees.

Sans Company department descriptions:

Finance & Human Resource department has 17 employees. The department deals with financial and administrative tasks and human resource management. This department also includes company's management board of 5 employees.

Sales & Marketing department has 25 employees. The largest department in SANS Company deals with phone sale, direct sale and Web sale. Since the majority of sale is performed through Web, the department has 8 web designers and application developers. Marketing department with its mission to provide continual benefits to the customer emphasizes on the ecological growth of sea food and also works closely with local population. SANS company's headquarters also supports this cooperation through its Sea Food Research department.

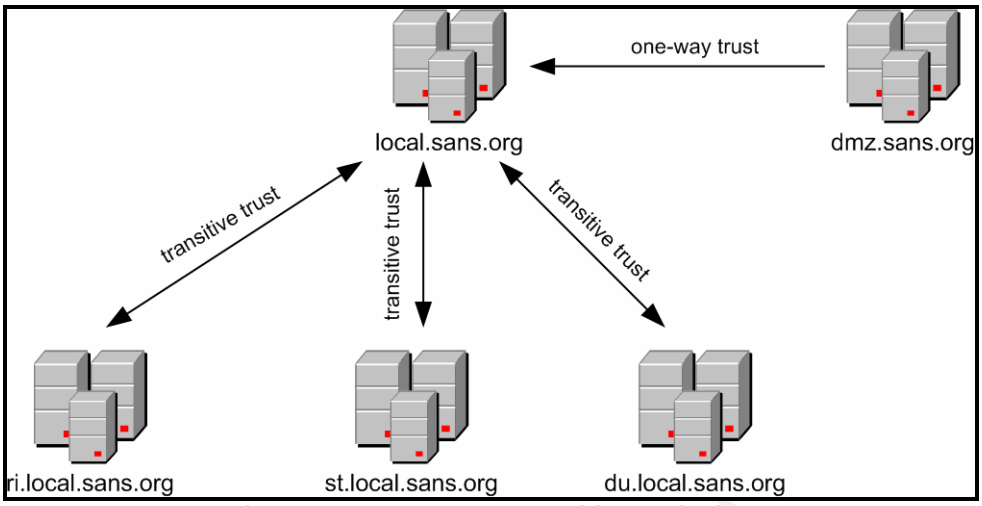
Information Technology department with its 16 employees provides IT support to employees and maintains and implements network services such as web site, firewall, antivirus and antispam protection, e-mail systems and database systems. 10 employees are situated on main location while in each regional office there are 2 employees.

Sea Food Research department has 12 employees. The department deals with research and improvement of sea food growth. It also develops procedures for protection of sea environment and works closely with local fishermen. Each regional Sea Food Research department has 4 employees.

Purchase department has 18 employees and deals with the procurement of fresh and ecologically bred sea food. Its primary resource is local fishermen's catch. Due to its good relationship with local population and fishermen cooperates with Sea Food Research department. The department is established only in regional offices on account of easier development of business relationships and supply with necessary sea products. Each regional Purchase department has 6 employees.

2.2 SANS COMPANY-WIDE ACTIVE DIRECTORY DESIGN

SANS company AD design consists of 2 forests. One forest has internal DNS namespace *local.sans.org* with 4 domains. Second forest with internal DNS namespace *dmz.sans.org* has only one domain.



Picture 1: Sans Company-wide AD design

2.3 SANS COMPANY CORPORATE AD DESIGN

Forest local.sans.org has one root domain *local.sans.org* and three child domains *ri.local.sans.org*, *st.local.sans.org* and *du.local.sans.org*. Root domain *local.sans.org* is located in Zagreb and represents main office while child domains are located in Rijeka - *ri.local.sans.org*, Split - *st.local.sans.org* and Dubrovnik - *du.local.sans.org* and represent regional offices. Two-way transitive trust is established between root domain and child domains.

Root domain *local.sans.org* represents corporate domain which contains all corporate servers, DMZ application servers (external web site, front-end Exchange server and external SQL server) and user workstations. Corporate domain is based on MS Windows 2000 operating system and operates in native mode. All servers are MS Windows 2000 servers with service pack 4 and latest critical security updates installed. User workstations and portable computers are MS Windows 2000 Professional with service pack 4 and all released patches and fixes. Mail exchange system is MS Exchange 2000 with service pack 3 and post-SP3 patches. Database system is MS SQL Server 2000 with service pack 3a.

Child domains hold their own DNS and mail servers in order to increase availability of DNS and mail services and, on the other hand, reduce dependence on servers located in main location. Mail servers in regional offices are Exchange 2000 servers also and placed in the same SANS Exchange organization as all other Exchange servers.

Forest dms.sans.org has one DMZ domain with one-way trust relationship established with SANS domain. This relationship enables IT staff from SANS domain to administer servers in DMZ domain. In case of security intrusion on external DMZ servers, separate DMZ forest limits security threats to servers and user workstations in corporate domain.

2.4 SANS COMPANY DMZ DESIGN

DMZ domain is based on Windows 2003 network infrastructure. All servers in domain are Windows 2003 Standard Server with latest critical security patches installed. DMZ domain operates in Windows 2003 forest functional level. It contains two hardware based firewall systems, external and internal. External hardware based firewall system protects DMZ domain from Internet while internal protects corporate network from DMZ network and thus, from Internet. DMZ domain has two ISA 2000 proxy/application firewall servers and two SMTP relay servers. ISA 2000 and SMTP relay are configured in network load balancing mode thus providing high availability of hosted network services.

Main reason for choosing Windows 2003 operating system over Windows 2000 is improved network load balancing services (NLB) with bi-directional affinity support and larger number of virtual NLB IP addresses.[1] It is also represents referent installation of Windows 2003 infrastructure which provides hands-on experience with new and improved directory and network services thus simplifying the migration process of corporate domain to Windows 2003 Active Directory in the future.

Bi-directional affinity support for NLB enables that IP packets pass through ISA server using same NLB node. Lack of that formerly emphasized support would result in ISA server discarding all IP packets that pass through using different NLB nodes. Large number of virtual NLB IP addresses allows configuration of different virtual IP addresses on both network interfaces. In NLB configuration of ISA server this means that one IP address is configured on external interface (external interface is one connected to external firewall system) and second IP address on internal interface (internal interface is one connected to internal firewall system). Same NLB configuration with two virtual IP addresses is also used for SMTP relay servers in DMZ network.

Antivirus and antispam software installed on SMTP relay servers safeguards corporate network from virus/worm infected email messages. DMZ domain has external DNS server authoritative for *sans.org* zone, domain controller, SUS server for patch management within domain boundaries and content distribution point for synchronization of corporate SUS servers.

From external user's point of view web site is hosted on ISA server through which public web pages and OWA are published. All application servers are moved into safe and secure corporate network behind firewall systems thus reducing the number of network ports for front-end Exchange system opened on internal firewall (front-end Exchange server should by design be placed in corporate domain). It also simplifies the implementation of communication between web site server and SQL server database containing data necessary for SANS Co. public web site.

One-way trust between DMZ domain and SANS domain is established using IPsec AH transport mode thus fine-tuning network traffic control on internal firewall system. Allowed IPsec ports opened on internal firewall allows network communication from

[1] What's New in Clustering for Windows Server 2003 - For Server Clusters and Network Load Balancing, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering/newclust.mspx

DC in DMZ domain towards 2 DCs in SANS domain. IPSec AH transport mode for authentication method use certificates issued by two issuing CA. One CA in corporate network issued certificates for DCs inside corporate network while the other CA in DMZ domain issued certificate for its DC. Both issuing CAs are verified by third party trusted CA e.g. VeriSign

2.5 SANS COMPANY DNS DESIGN

Corporate DNS domain infrastructure contains 8 DNS servers. Two DNS servers are located on each location. DNS servers are authoritative for their DNS domain namespaces i.e. dczg01 and dczg2 are authoritative for *local.sans.org* zone, dcdu01 and dcdu02 for *du.local.sans.org* zone, dcst01 and dcst02 for *st.local.sans.org* and, finally, dcri01 and dcri02 for *ri.local.sans.org zone*. DNS zones on authoritative DNS servers are Active Directory Integrated and configured to allow only secure dynamic update.

In order to speed up name resolution DNS server on each location hosts DNS zones from all other DNS servers as secondary zones. In other words, DNS servers for du.local.sans.org in Dubrovnik host secondary zones *local.sans.org*, *ri.local.sans.org* and *st.local.sans.org*. All regional DNS servers also host *_msdcs.local.sans.org* zone as secondary zone because Active Directory uses a special set of locator records, forest-wide locator records, to help replication partners to find each other and to help clients to find global catalog servers. Active Directory stores all forest-wide locator records in the zone _msdcs.local.sans.org and that information must be widely available throughout the zone. [2] All secondary zone transfer is restricted to name servers defined in zone properties.

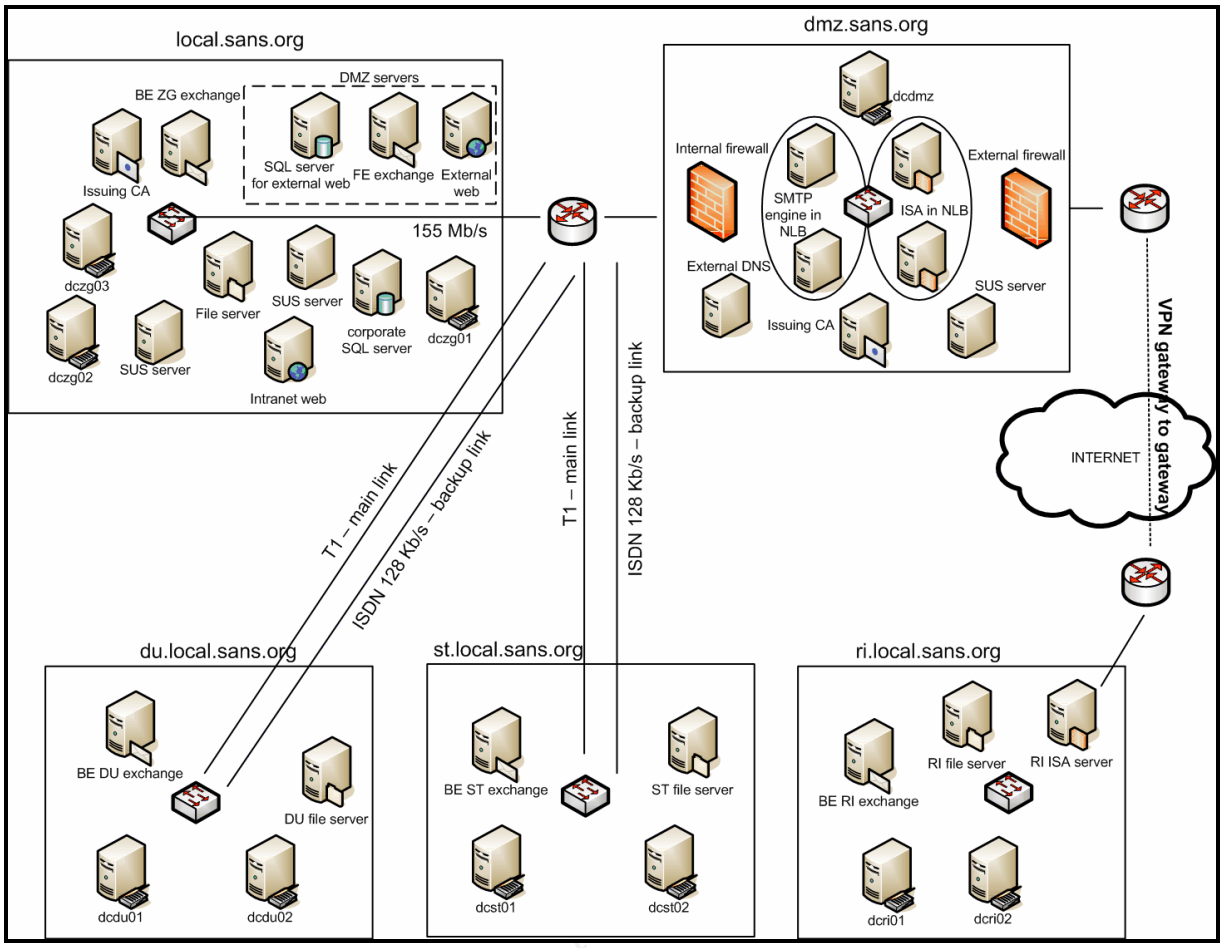
DNS service for DMZ domain is configured on dcdmz domain controller. It is authoritative for dmz.sans.org zone. DNS zone dmz.sans.org is configured as Active Directory Integrated zone. Dcdmz server also hosts as secondary zones all DNS zones in the local.sans.org forest.

Name resolution for external IP addresses is performed through forwarders so that regional DNS servers (dcdu01, dcdu02, dcst01, dcst02, dcri01 and dcri02) forward DNS queries toward DNS servers in main location (dczg01 and dczg02) which in return do forwarding to external DNS server in DMZ.

2.6 SANS COMPANY NETWORK DESIGN

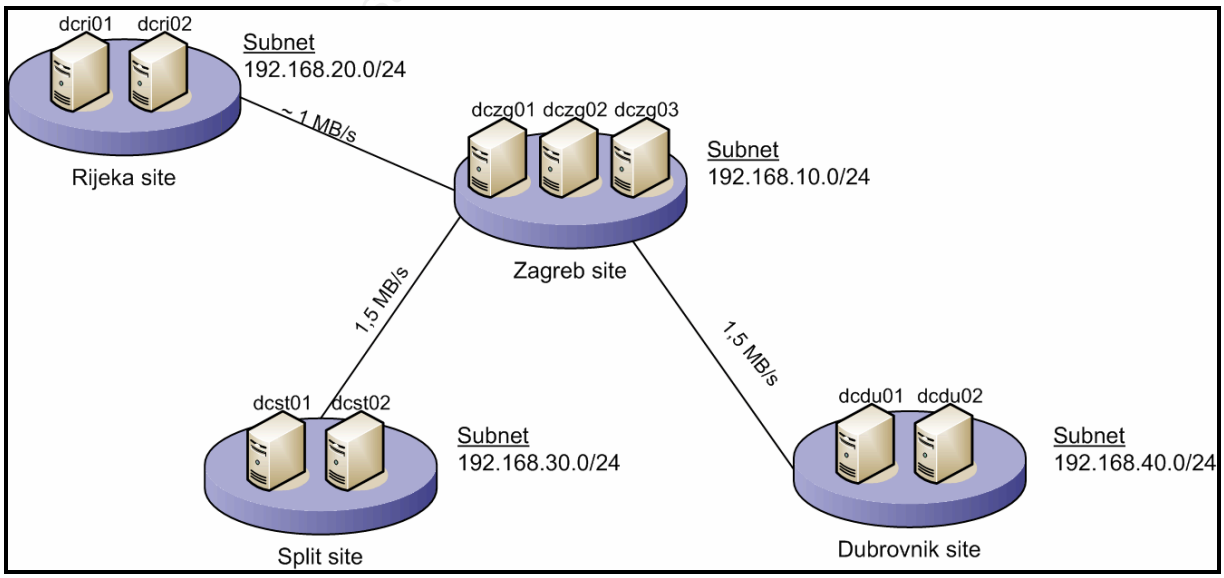
SANS company network infrastructure is made of 5 different subnets (one subnet is DMZ – not showed in site schema). Regional locations in Split and Dubrovnik are connected with main office in Zagreb through T1 link as primary link and ISDN link as backup. Rijeka is connected with Zagreb through gateway to gateway VPN using ISA server in DMZ zone and ISA server in Rijeka. VPN is L2TP/IPSec based. DMZ network subnet is connected by 155 Mb/s link to network subnet in Zagreb.

[2] Best Practice Active Directory Design for Managing Windows Networks, http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/bpaddsgn.mspx



Picture 2: Sans Company network design

Hub and spoke site topology of local.sans.org forest follows network design. Site topology is made of 4 sites, each site represents remote location. Site link connect all remote sites to central Zagreb site. Replication between regional sites and central site is scheduled every hour because changes to schema and configuration NC are not that frequent. DMZ forest has only one site without any site link connections.



Picture 3: Sans Company site design

2.7 SANS COMPANY ORGANIZATION UNIT DESIGN

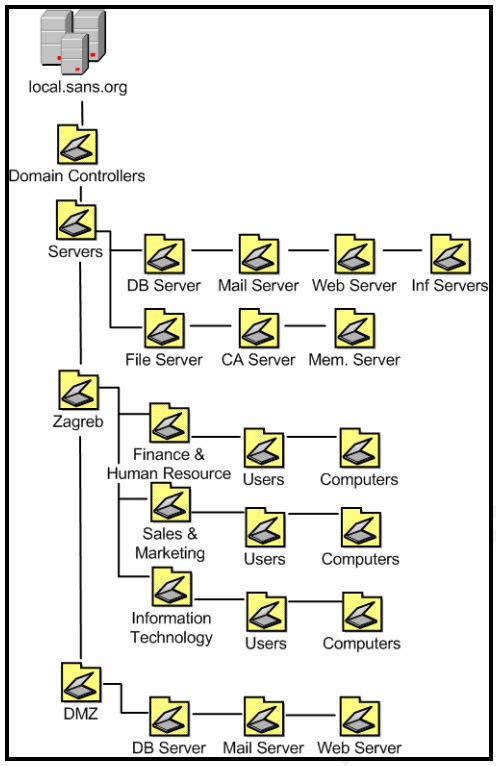
Organizational unit design is based on group policy application and company's organizational structure.

Local.sans.org domain contains 3 top level OUs: Servers, Zagreb and DMZ. Top level organizational units are created in order to ensure the application and propagation of the same security settings to sublevels organizational units.

Domain Controllers organizational unit (default OU) contains domain controllers.

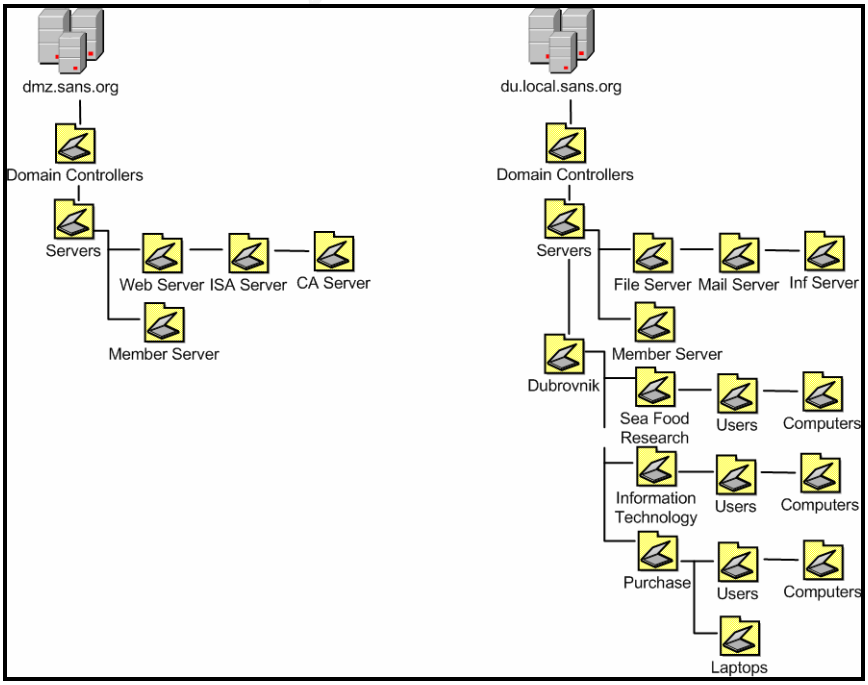
Organizational unit Zagreb contains following OUs:

- Finance & Human Resources OU – sub organizational units Users and Computers contain user and computer accounts for Finance & Human Resource department. Finance & Human Resource department is located only in central office in Zagreb.
- Sales & Marketing OU – sub organizational units Users and Computers contain user and computer accounts for Sales & Marketing department. It is located only in central office.
- Information Technology OU – sub organizational units Users and Computers contain user and computer accounts for IT department but only for IT staff located in central office.
- Servers OU contains following low-level organizational unit:
    - DB server OU – contains database servers
    - Mail server OU – contains back-end Exchange 2000 servers in its domain
    - Web server OU – contains internal web servers used for intranet web site, SUS servers and test web servers
    - Inf server OU – contains servers that hosts infrastructural services e.g. DHCP, WINS
    - File servers OU – contains file and print servers
    - CA server OU – contains issuing CA server
    - Member server OU contains all other servers used for various purposes but do not belong to any previously mentioned categories
- DMZ OU contains the following organizational units:
    - DB server OU – contains database servers that hold databases for external web servers
    - Mail server OU – contains front-end Exchange 2000 servers
    - Web server OU – contains all external web servers published thought ISA server as SANS public web site



Picture 4: local.sans.org domain organizational unit design

Regional domains ri.local.sans.org, st.local.sans.org and du.local.sans.org hold the same organizational structure. The only difference is in ri.local.sans.org which in Servers OU contains also ISA server organizational unit. This OU contains ISA server used for establishing gateway to gateway VPN connections with central location in Zagreb.



Picture 5: DMZ and Dubrovnik regional office organizational unit design

Regional domains contain the following organizational units:

- Domain controllers (default OU) – contains all domain controllers
- Servers OU contains following organizational units:
    - File server OU – contains file and print servers
    - Mail server OU – contains back-end mail servers
    - Inf server OU – contains servers that host network infrastructure services e.g. DHCP, WINS
    - Member servers OU – contains all other servers used for various services but cannot be placed to any previously mentioned OU
    - ISA server OU – only in ri.local.sans.org and as mentioned contains ISA server for establishing gateway to gateway VPN connections between Rijeka and Zagreb
- Regional_name (e.g. Dubrovnik OU) OU contains following sub organizational units:
    - Sea Food Research OU – sub organizational units Users and Computers contains user and computer accounts for Sea Food Research department. Sea Food Research departments are located only in regional offices.
    - Purchase OU – sub organizational units Users, Computers and Laptops contain user and computer accounts for Purchase department. Purchase department is located only in regional domains because regional offices are situated in cities on Adriatic coast thus simplifying sea food procurement and business cooperation with local fishermen
    - Information Technology OU – sub organizational units Users and Computers contain user and computer accounts for IT department but only for IT stuff located in regional offices

DMZ domain contains the following organizational units:

- Domain controllers OU – contains domain controllers in DMZ domain
- Servers OU with the following organizational units:
    - Web server – contains SUS server
    - ISA server – contains ISA servers
    - CA server – contains issuing CA servers
    - Member server – contains SMTP relay servers and external DNS server

2.8 GIAC ENTERPRISE BASIC FACTS

GIAC Enterprise was founded in 1996 on Hvar island, Croatia. Company's core business is production of vine brand "Hvar's sunrise". GIAC Enterprise offices are situated on two locations. Research and Development department as central part of GIAC Enterprise is located on Hvar island where core production takes place i.e. development of viniculture methods, grape breeding and vine production. Sales & Marketing, Finance & Human Resource and IT department are located in Zagreb. Some basic facts about GIAC Enterprise infrastructure are presented in next few sections. Detailed description of GIAC Enterprise departments including Active Directory design, organizational units structure and network design are described in Philip M. Cox practical assignment v3.1 with title "Design a Secure Windows 2000 Infrastructure" (http://www.giac.org/practical/Phillip_Cox_GCWN.doc).

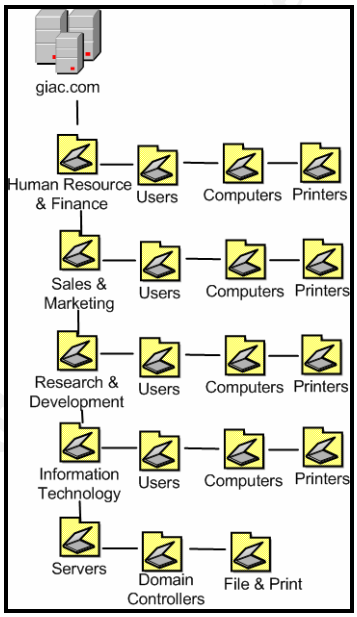
2.9 GIAC ENTERPRISE ACTIVE DIRECTORY AND OU DESIGN

GIAC Enterprise is relatively small company with one forest i.e. one domain giac.com. Windows 2000 with latest service pack is primary operating system used throughout domain. Domain operates in Windows 2000 native mode.

Giac.com domain contains 4 basic organizational units which describe organizational structure of company, i.e.:

- Human Resource and Finance
- Sales and Marketing
- Research and Development
- Information Technology
- Servers (additional OU that hosts all corporate servers)

Each department organizational unit is then divided into Users, Computers and Printers organizational units. Organizational unit Servers is divided into Domain Controllers and File & Print organizational units.

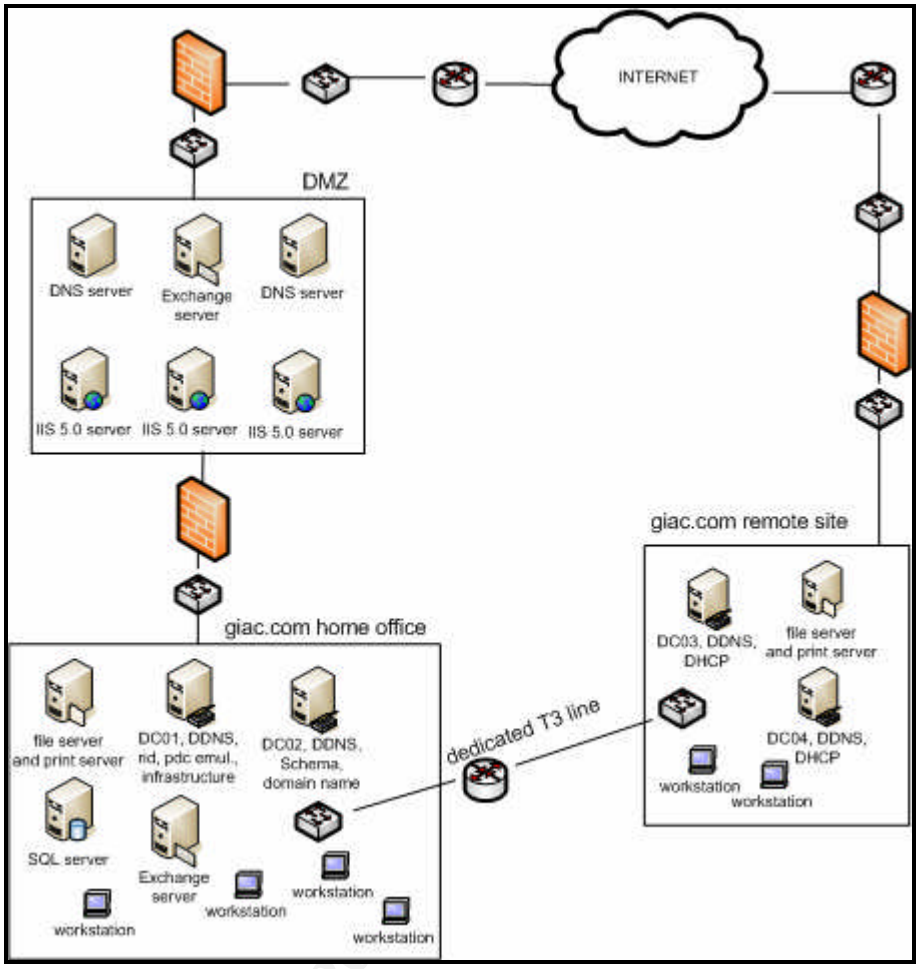


Pictures 6: Giac.com domain organizational unit design

Exchange 2000 is used as mail exchange system and SQL 2000 as database server.

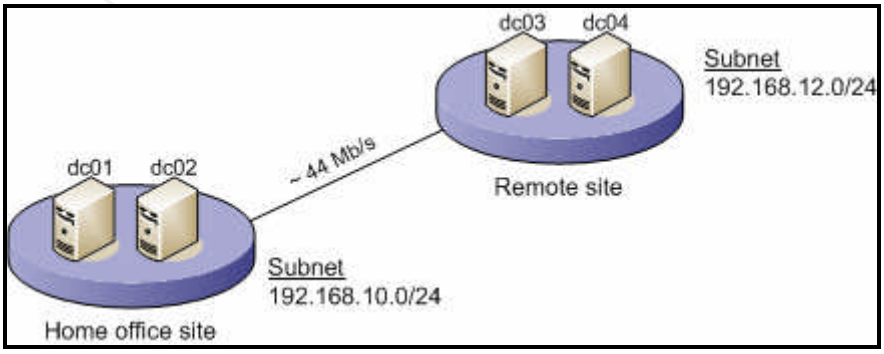
DMZ is not designed as separate forest or workgroup; actually servers are installed as stand-alone and each placed in separate workgroup. DMZ contains three web servers with IIS 5.0, two external DNS servers and one Exchange 2000 server.

2.10 GIAC ENTERPRISE NETWORK DESIGN



Picture 7: Giac.com Company network design

GIAC Enterprise' network is made of two different subnets. Each location (Zagreb, Hvar) has its own subnet including DMZ network. Locations are connected with dedicated T3 link. All traffic between these two locations is encrypted using hardware based encryption devices. Both locations have separate T1 links for Internet. Separate AD site is created for each subnet. Replication between sites is scheduled every fifteen minutes.



Picture 8: Giac.com site design

2.11 SANS & GIAC MERGER INTO NEW SANSWGIAC COMPANY

SANS company decided to buy GIAC Enterprise in order to expand its catering with quality vine, increase sales and strengthen its market position. IT project team is formed during the merger of these companies. Team consists of 4 employees from IT department of GIAC Enterprise, 5 IT employees from SANS Company including project leader chosen due to large experience and maintenance of complex IT infrastructure. Its task is the integration of Active Directory and network infrastructure.

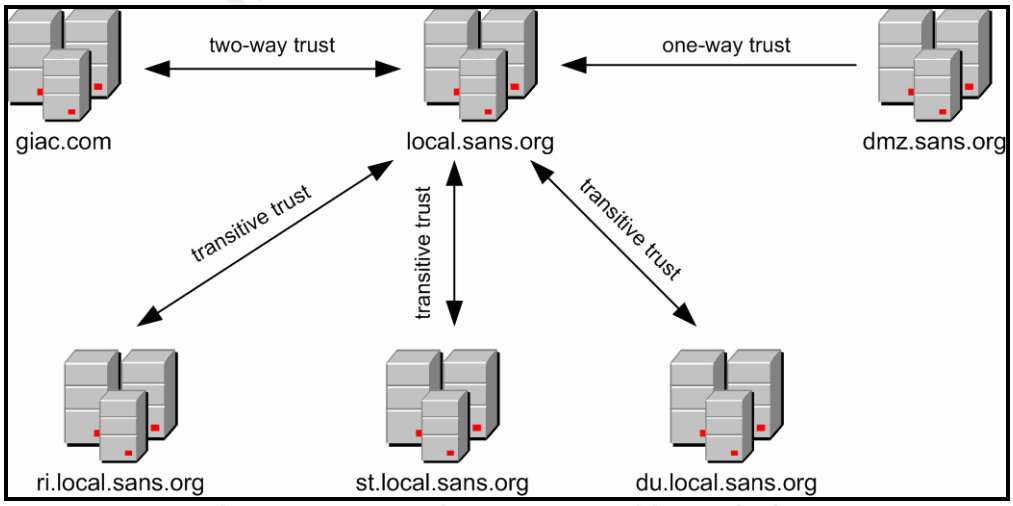
The following goals are defined before the merger:

- merger must be transparent to internal users (both SANS and GIAC's employees are able to perform its daily business)
- merger must be transparent to external users (customers are able to submit queries, orders)
- consolidation of servers and network resources
- reduction of IT costs of new SansWGiac company

The process of integration will be carefully planned, tested, performed and finally documented thoroughly. Detailed checklists and backup/restore procedures will be defined for each phase of integration. Test environment will be built for testing purposes and it will represent two different domains with all their specifics crucial for integration. All procedures that require certain downtime, e.g. moving servers from GIAC Enterprise DMZ to SANS Company DMZ will be performed by night.

2.12 SANSWGIAC ACTIVE DIRECTORY DESIGN

SansWGiac Company will contain 3 forests. First two forests will be local.sans.org and dmz.sans.org. Third forest will be giac.com. Two-way trust will be established between giac.com forest and local.sans.org forest. Active directory design of SANS company and its trust relationships will not change. GIAC Enterprise' DMZ zone will cease to exist and all servers from giac.com DMZ will migrate to DMZ organizational unit in local.sans.org domain.



Picture 9: SansWGiac Company wide AD design

All SQL server databases will be moved to newly created SQL server cluster and GIAC Enterprise SQL server will be uninstalled. With new clustered SQL server all databases will be consolidated and hosted on more reliable system providing high available SQL service for SansWGiac employees.

New clustered file server will be implemented in local.sans.org domain for sharing files and documents essential for new SansWGiac company. Also on that file server will be placed all documents required for inter-company department collaboration. That way we do not need to create additional trusts between SANS Company child domains and giac.com forest and therefore we reduced administrative tasks necessary for maintaining large number of trusts.

Implementation of access control rights will follow best practices design recommended by Microsoft. Global groups will be created in root domains for controlling access to shared resources. User accounts that require access to shared resources in different domains will then be added into these global groups. Global groups will then be added into Universal groups and Universal groups will be added into Domain local groups in domains where required resources are located. Groups will be created only in root domains due to Sea Food Research department's need for access to SQL databases and regional IT and Purchase department only need access to documents and files shared on clustered file server common for all SansWGiac company employees.

One central installation of MS Identity Integration Server 2003 will be used for Exchange free/busy information, GAL and Public Folder synchronization between two companies. MIIS 2003 will be located in local.sans.org domain.

2.13 SANSWGIAC DMZ DESIGN

DMZ zone of GIAC Enterprise will cease to exist and all web severs will be moved to DMZ organizational unit of local.sans.org domain. The transition will be simple because servers are stand-alone, each in its own workgroup. DNS zone giac.com will be transferred to external DNS server in dmz.sans.org and DNS server will be uninstalled. Web server transfer will be performed by night due to required reboot when adding servers to domain.

Existing mailboxes on Exchange server in GIAC Enterprise's DMZ will be migrated to FE Exchange server in local.sans.org. Mailbox migration will not be a problem because Exchange server in GIAC Enterprise is not in Exchange organization (i.e. it is member of its own workgroup and thus not bind to giac.org domain) and total number of mailboxes to migrate is small.

Web server migration and termination of Exchange server from GIAC Enterprise DMZ will allow the implementation of one unique DMZ design of SansWGiac that enables administration using domain accounts and reduces administration overhead from managing two different DMZ concepts. It will also enable creation and application of standardized GPOs on all servers in DMZ; simplify communication between GIAC enterprise web server and SQL server databases for external web,

consolidation of web sites into single SansWGiac' corporate web site and reduce number of servers in DMZ.

Termination of GIAC Enterprise's DMZ zone will simplify network infrastructure, reduce number of used network devices (switches, routers and two hardware based firewalls) and administrative overhead for maintaining large number of servers.

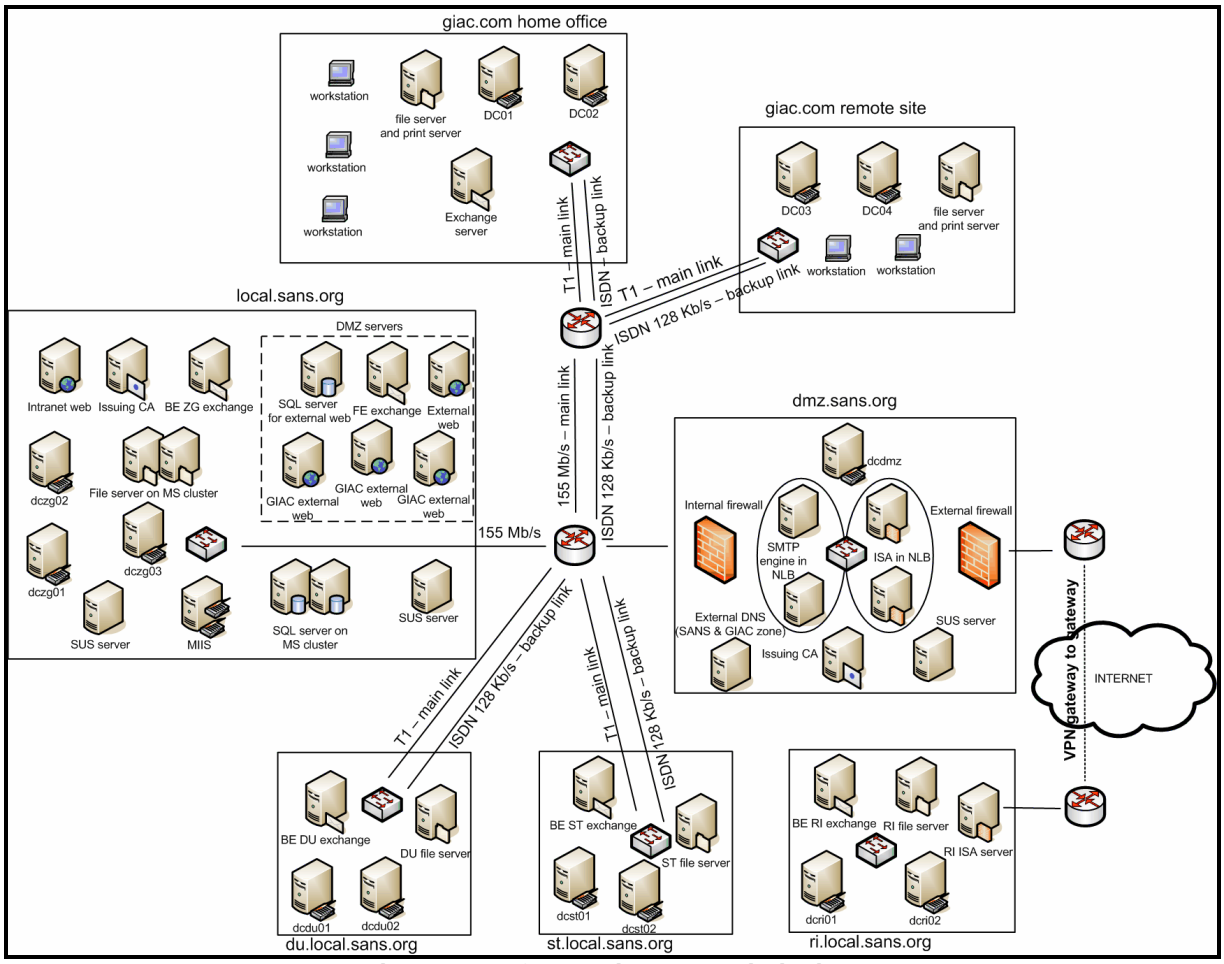
2.14 SANSWGIAC DNS DESIGN

DNS infrastructure design will stay the same except that each DNS server will host as secondary zones all authoritative zones from other domains in SansWGiac Company. DNS servers in GIAC Enterprise will be configured as forwarders pointing to DNS servers in Zagreb (dczg01 and dczg02) which in return are configured as forwarders toward external DNS server in SansWGiac DMZ zone.

2.15 SANSWGIAC NETWORK DESIGN

SansWGiac Company will contain 7 different subnets (one subnet is for DMZ). Each location will be separate subnet. Site design will not change. T3 dedicated link between giac.com home office and giac.com remote location will be replaced by T1 link as primary link and ISDN link as backup. This way link redundancy will be increased but link costs will stay on same level. T1 link with ISDN link as backup link will be established between giac.com central office and local.sans.org.

Internet access through T1 dedicated links for giac.com home office and remote office will be replaced with Internet access through unique ISA server proxy/firewall system.



Picture 10: SansWGiac network design

2.16 SANSWGIAC ORGANIZATION UNIT DESIGN

Organizational unit design of GIAC Enterprise will be changed according to design of SANS Company. SANS Company organizational unit design will not change.

Design changes will standardize organizational unit structure throughout domains of new SansWGiac Company and also enable the following:

- standardized Group Policy design
- simplified Group Policy administration
- improved testing and implementation of Group Policy
- application of existing and widely used security templates

Organizational unit scheme of GIAC Enterprise will be modified as follows: Domain controllers will be transferred to default Domain Controllers OU, sub organizational unit Domain Controllers from Servers OU will be removed. Servers OU will be extended with additional organizational units according to services that host each server. Printers OU from all organizational units will be removed and all print servers will be transferred to File server organizational unit. This will reduce number of GPO because previous analysis showed no need for separate GPOs for each Printers OU in different organizational units. Top level organizational unit GIAC is introduced as parent organizational unit for GIAC Enterprise's departmental organizational units.

After the last design modification is performed GIAC Enterprise domain will contain the following organizational units:

- Domain controllers OU – contains all domain controllers
- Servers OU - contains the following organizational units:
    - File server OU - holds file and print servers
    - Mail server OU – contains Exchange mail servers
    - Inf server OU – holds network infrastructure servers e.g. DHCP, WINS
    - DB server OU – contains database servers
    - Member servers OU – contains all other server types
- GIAC organizational unit contains the following OUs:
    - Research & Development OU – sub organizational units Users and Computers contain user and computer accounts for Research & Development department.
    - Information Technology OU – sub organizational units Users and Computers contain user and computer accounts for IT department of GIAC Enterprise domain.
    - Sales & Marketing OU - sub organizational units Users and Computers contain user and computer accounts for Sales & Marketing department.
    - Human Resource & Finance OU - sub organizational units Users and Computers contain user and computer accounts for Human Resource & Finance department

3. SECURITY POLICY AND TUTORIAL

3.1 GROUP POLICY DESIGN

Organizational unit design and organizational unit redesign in GIAC Enterprise depends on Group Policy design. GPO in SansWGiac company applies on organizational units (except default domain policy that applies on domain) thus OU design is basics for Group Policy design.

For security enforcement throughout SansWGiac company IT staff prepared GPOs with home-defined security settings and administrative templates. Home made security and administrative templates are based on predefined security templates, best practices and recommendation from Windows 2000 Hardening Guide, Securing Windows 2000 Server Guide and NSA-SNAC (National Security Agency-Systems and Network Attack Centre) Windows 2000 Security Guides. Security settings of Windows 2003 in DMZ zone are based on Windows 2003 Server Security Guides. Each security template is carefully tested in testing environment then exported by Group Policy Management Console (GPMC) and copied across multiple forest and domains. GPMC is installed on Windows XP management computer because GPMC works only on Windows XP/2K3 operating system.

All domains in SansWGiac company hold the same Group Policy design. Each domain has standardized settings for Account Policies which are approved by management and defined in Default Domain Policy. Event Log settings and System service settings are also standardized across SansWGiac Company following best

practices guides and latest security bulletins e.g. messenger service is configured as disabled according to MS03-043 security bulletin and evaluation of messenger service usability in production environment over possible security threats performed by IT staff. Default Domain Controllers Policy is applied on Domain controllers default organizational unit. Details about Default Domain Policy security settings are provided in Group Policy testing section of this paper.

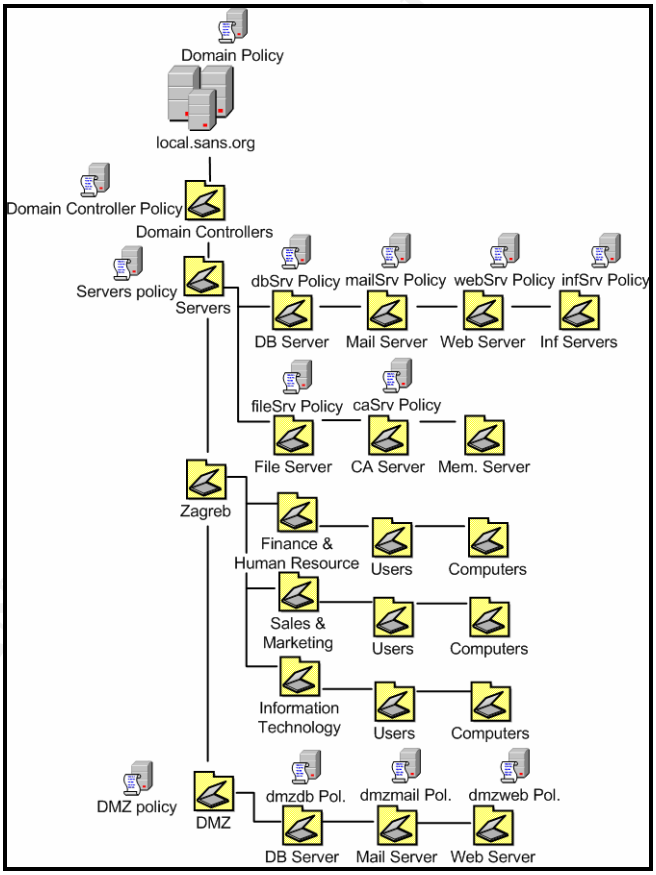
Each domain holds Servers organizational unit with its sub OUs for different server types. Servers Policy applies to organizational unit Servers, while depending on hosted service type different policies apply on sub organizational units e.g. fileSrv Policy is defined for File server OU. Such OU and GPO design enables propagation of common security settings defined in Servers Policy to all sub level organizational units. Server specific settings are defined and customized using specific server policy links to that server's organization unit.

OUs for each department are created under top level organizational unit named by region or domain where it is located (e.g. Zagreb OU). Default Domain Policy complies with security requirements for all departments thus there is no need for separate Group Polices. Also sensitive data from all departments is stored on file or database servers protected by server specific GPOs. Organizational units for departments (HR, Sales, IT etc.) and its top level OU (Zagreb OU, Rijeka OU, etc.) are created for potential software packages distribution through Group Policies. That way GPO created on top-level organizational unit (e.g. Zagreb OU) can be used for common software packages distribution to all sub-level department organizational units. Any department specific or customized software packages can be distributed through GPO created for that department. Exception to this rule are GPOs for Laptops organization unit in Purchase OU created in each regional domain because of higher security requirements for mobile users.

Root domain local.sans.org contains the following GPOs:

- Default Domain policy
  - security template SWG.inf
  - link to local.sans.org domain
- Default Domain Controllers policy
  - security template SWGdc.inf
  - link to Domain Controllers OU
- Servers Policy
  - security template SWGSrv.inf
  - link to Servers OU
- dbSrv Policy
  - security template dbSrv.inf
  - link to DB server OU
- mailSrv Policy
  - security template mailSrv.inf
  - link to Mail Server OU
- webSrv Policy
  - security template webSrv.inf
  - link to Web Server OU
- infSrv Policy
  - security template infSrv.inf

    - link to Inf Server OU
- fileSrv Policy
    - security template fileSrv.inf
    - link to File Server OU
- caSrv Policy
    - security template caSrv.inf
    - link to CA server OU
- DMZ Policy
    - security template IntSWGDMZ.inf
    - link to DMZ OU
- dmzdb Policy
    - security template IntSWGDMZdb.inf
    - link to DB Server OU
- dmzmail Policy
    - security template IntSWGDMZowa.inf
    - link to Mail Server OU
- dmzweb Policy
    - security template IntSWGDMZweb.inf
    - link to Web Server OU

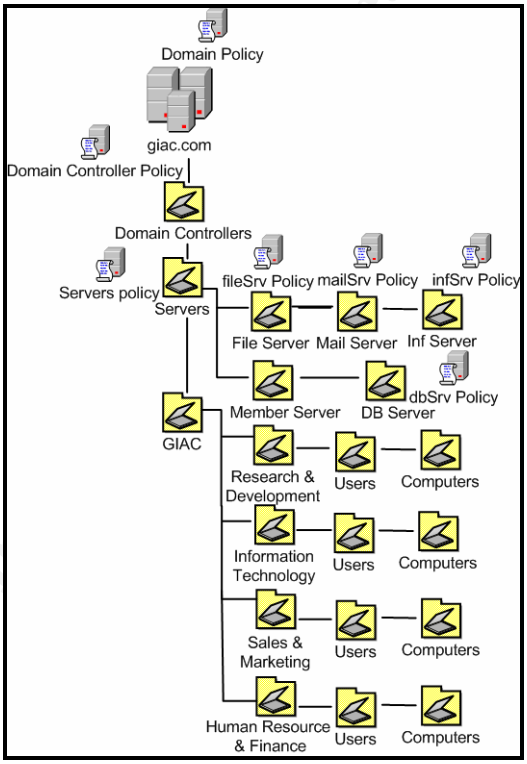


Picture 11: Group Policy design for local.sans.org domain

Root domain giac.com contains the following GPOs:

- Default Domain policy
    - security template SWG.inf
    - link to giac.com domain

- Default Domain Controller Policy
  - security template SWGdc.inf
  - link to Domain Controllers OU
- Servers Policy
  - security template SWGSrv.inf
  - link to Servers OU
- fileSrv Policy
  - security template fileSrv.inf
  - link to File server OU
- mailSrv Policy
  - security template mailSrv.inf
  - link to Mail Server OU
- infSrv Policy
  - security template infSrv.inf
  - link to Inf Server OU
- dbSrv Policy
  - security template dbSrv.inf
  - link to DB Server OU

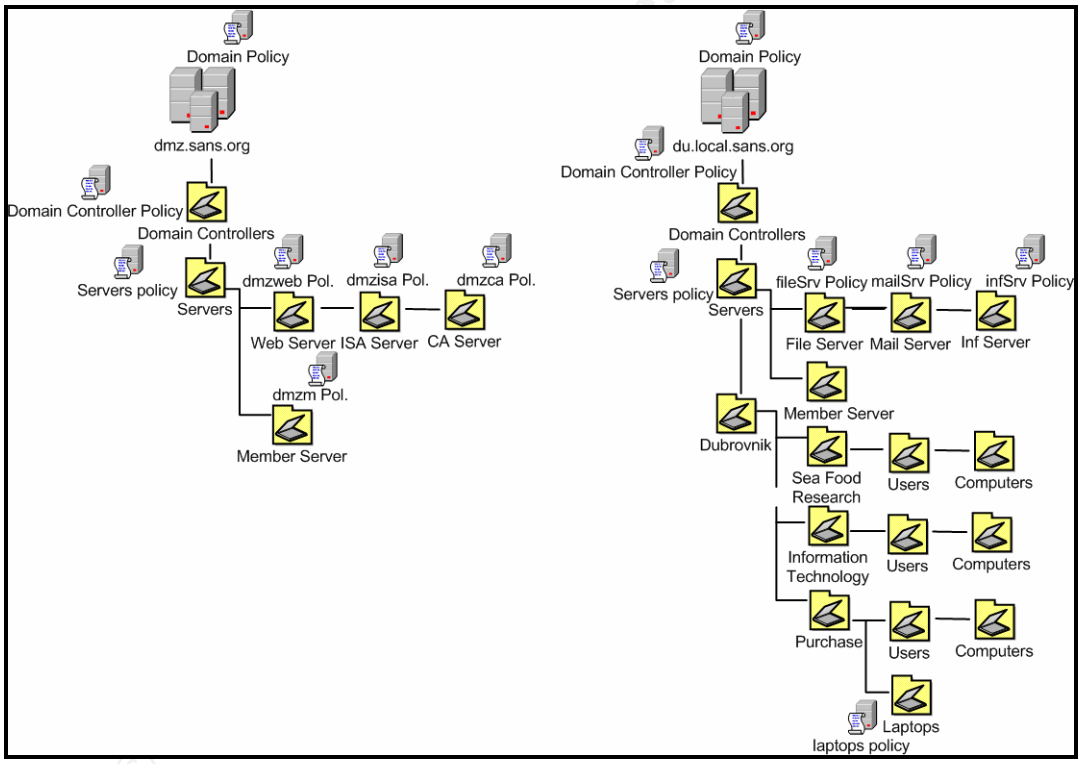


Picture 12: Group Policy design for giac.com domain

Regional domains (ri.local.sans.org, st.local.sans.org, du.local.sans.org) contain the following Group Policy objects:

- Default Domain policy
  - security template SWG.inf
  - link to ri.local.sans.org, st.local.sans.org and du.local.sans.org domain
- Default Domain Controller Policy
  - security template SWGdc.inf
  - link to Domain Controllers OU

- Servers Policy
  - security template SWGSrv.inf
  - link to Servers OU
- fileSrv Policy
  - security template fileSrv.inf
  - link to File server OU
- mailSrv Policy
  - security template mailSrv.inf
  - link to Mail Server OU
- infSrv Policy
  - security template infSrv.inf
  - link to Inf Server OU
- dbSrv Policy
  - security template dbSrv.inf
  - link to DB Server OU
- isaSrv Policy
  - security template isaSrv.inf
  - link to ISA Server OU



Picture 13: Group Policy design for dmz.sans.org and du.local.sans.org domain

Root domain dmz.sans.org holds the following Group Policy objects:

- Default Domain policy
  - security template ExtSWGDMZ.inf
  - link to local.sans.org domain
- Default Domain Controller Policy
  - security template ExtSWGDMZdc.inf
  - link to Domain Controllers OU
- Servers Policy

    - security template ExtSWGDMZSrv.inf
    - link to Servers OU
- dmzweb Policy
    - security template ExtSWGDMZweb.inf
    - link to Web Server OU
- dmzisa Policy
    - security template ExtSWGDMZisa.inf
    - link to ISA Server OU
- dmzcaPolicy
    - security template ExtSWGDMZca.inf
    - link to CA Server OU
- dmzm Policy
    - security template ExtSWGDMZsmtp.inf
    - link to Member Server OU

Root domain local.sans.org holds 13 GPOs; each regional domain holds 7 GPOs except ri.local.sans.org domain which holds 8 GPOs. Dmz.sans.org domain holds 7 GPOs same as giac.org. In total 42 GPOs and 21 different security templates are defined. Most of security templates used in dmz.sans.org and DMZ OU of local.sans.org domain are incremental (11). Number of GPOs is large, but it is much better and efficient to spend some time to customize and fine tune all relevant security settings for specific services and apply them to servers through GPOs, then to have small number of GPO but tune every server separately through local security policies. Thus SansWGiac Company has many GPOs fine-tuned with custom security templates that have security registry settings like TCP/IP stack hardening.

3.2 GROUP POLICY TESTING

Test environment is implemented for Group Policy evaluation. It consists of three servers:

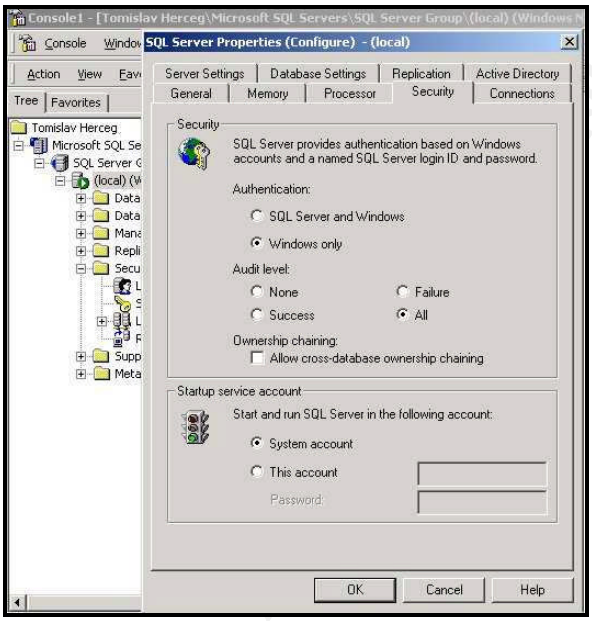
- domain controller DCZG01 for local.sans.org domain
- SQL server DMZSQL for hosting database using in external SansWGiac company web site
- web server DMZIIS (IIS 5.0) as external SanswGiac company web site server (http://www.sanswgiac.com)

All of them are Windows 2000 Standard Edition severs with service pack 4 and latest security patches installed.

Computer accounts for dmzsql and dmziis servers are placed in their respective organization units DB server OU and Web server OU. Both OU are located in organization unit DMZ in local.sans.org domain as described in Group Policy design.

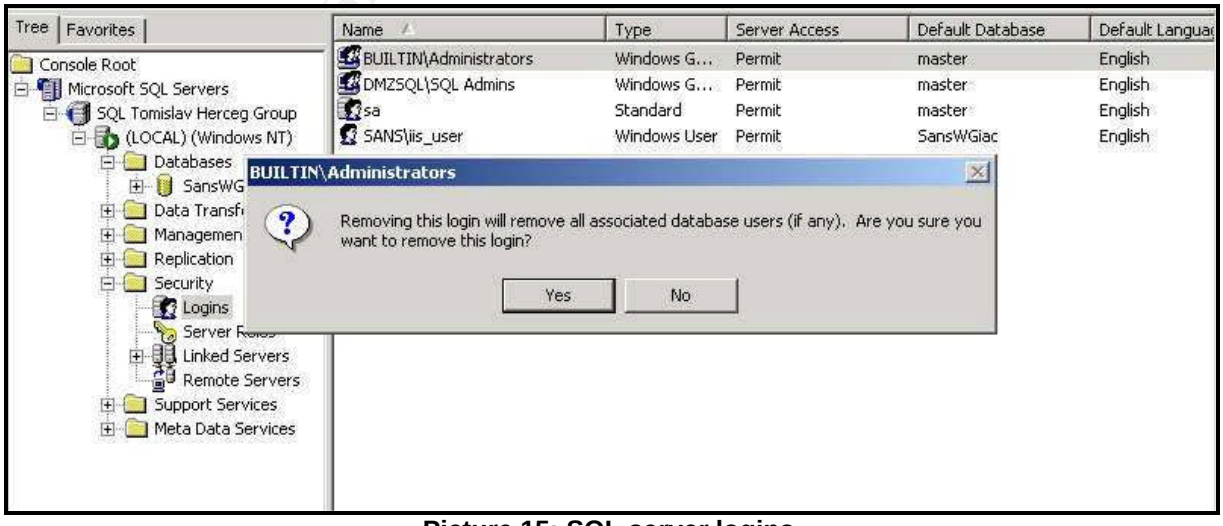
Microsoft SQL server 2000 Enterprise Edition with service pack 3a is installed on dmzsql server without additional security updates for SQL server. SQL server programs files and database files are installed on default location. Only Server Components with SQL server component are installed. For SQL server management Tools are installed Enterprise Manager, Profiler, Query Analyzer and DTC Client Support and Client Connectivity component. Services SQLserverAgent and MSSQLServerADHelper are stopped and set to manual startup type.

Both test databases, Pubs and Northwind, installed by default are deleted. New database SansWGiac is created. Database SansWGiac contains one table and one stored procedure. Product table holds all types of fishes offered by SansWGiac catering. Stored procedure get_all_products contains select statement for displaying all products from Product table. SQL server service runs under System account. Authentication level is set to Windows only as SQL server security best practices recommends. Audit level is set to All.



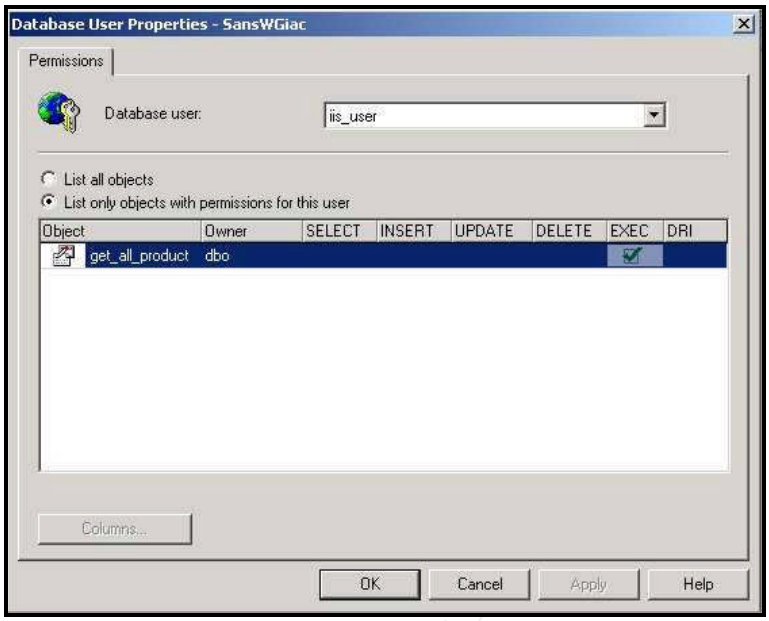
Picture 14: SQL server security settings

For SQL server logins we removed BULTIN\Administrators group and created SQL Admins local group that contains only designed SQL admins in SansWGiac Company. We also have default sa account (SQL system administrator account) for which we created complicated and long passphrase. Domain user account iis_user is created for web site access to SansWGiac database. User iis_user is member of Domain Guest security group.



Picture 15: SQL server logins

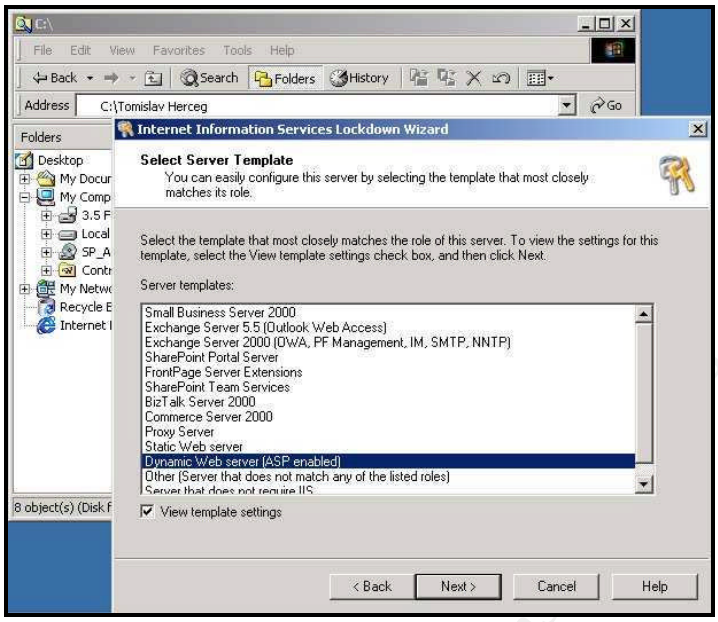
Iis_user has only access to database SansWGiac and is placed in Public database role. The only permission granted to iis_user is to execute get_all_products stored procedure.



Picture 16: IIS_user database permissions

On web server IIS 5.0 with Common Files, Internet Information Service Snap-in and World Wide Web server is installed. Folder InetPub is left on root of C disk. New folder IISlogs is created on root of C disk and the location of log file directory is changed to C:\IISLogs on Default web site properties > Extended Logging Properties > General properties tab. Folder IISlogs is shared with share name IISLogs and share permissions are set to Full control for Everyone. NTFS permissions for IISLogs share are set to Full control for local Administrators group, Full control to System group and Read & Execute permissions to Scriptoman domain user account. Domain user account Scriptoman is account used for running scheduled VBScript that copies IIS log files to shared folder on management server as described in auditing system design. User account Scriptoman has long passphrase because it is used rarely. User Scriptoman is member of Domain Users security group only.

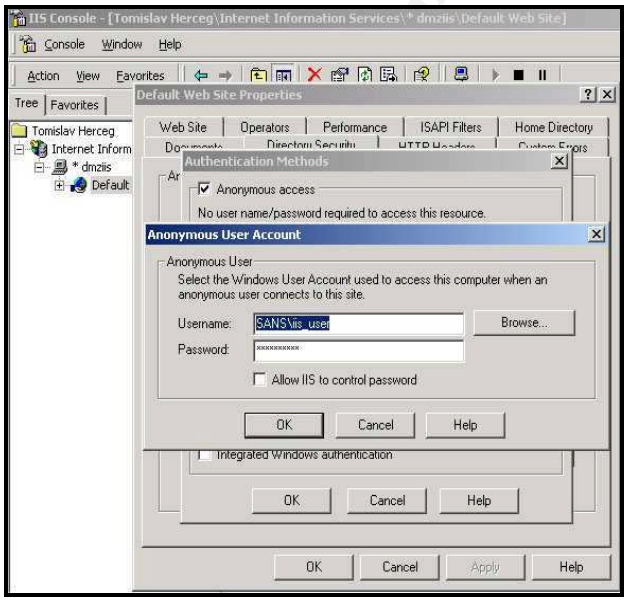
IISLockdown tool 2.1 with dynamic web server (ASP enabled) template is used for additional web server protection. After IISLockdown tool implementation, folders scripts and iissamples in InetPub folder are deleted by default. URL Scan tool is not installed because web servers are published trough ISA server that has URL Scan installed.



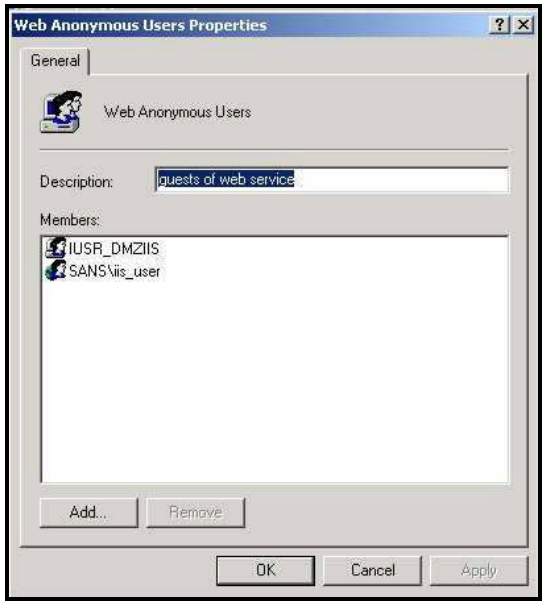
Picture 17: IISLockdown tool template

Every user that through browser accesses web server is treated as anonymous and its access is controlled through default local user account created during IIS installation. Local user account for anonymous access to web pages has format IUSR_server_name e.g. IUSR_DMZIIS and is member of Guest local group. IISLockdown tool created additional local Web Anonymous Users group and put IUSR_DMZIIS user in it.

Because IUSR_DMZIIS user is local and cannot be used for network access to SQL server that uses windows only authentication, user account for anonymous access to web site is changed to domain account iis_user. Also user account iis_user is member of local Guest and Web Anonymous Users group. Thus iis_user account has all required NTFS permissions defined for IUSR_DMZIIS user.



Picture 18: Change account for IIS anonymous user account



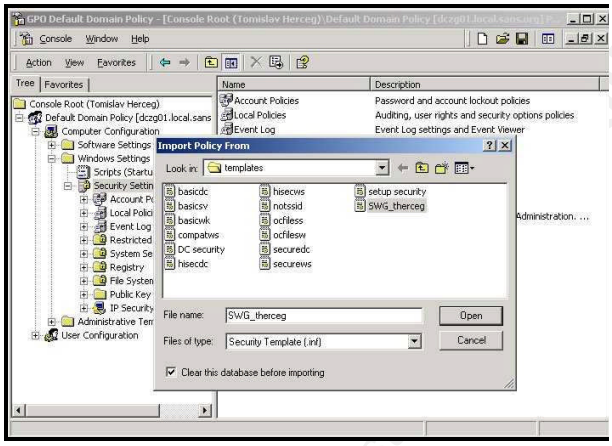
Picture 19: Add iis_user to local web anonymous users group

Domain controller DCZG01 is installed and configured without any special configuration settings and changes.

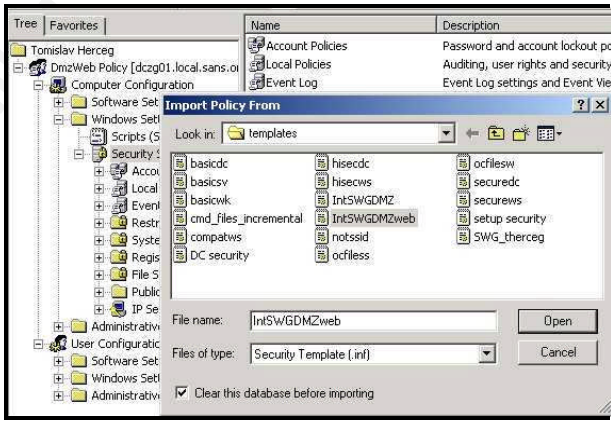
3.3 APPLYING GROUP POLICY

SansWGiac IT staff is subscribed to security list and bulletin e.g. Microsoft Security Bulletin and @RISK: The Consensus Security Vulnerability Alert and one of its tasks is constant evaluation of new vulnerabilities. Group Policy is updated using incremental and tested security templates based on this evaluation and level of threats. Refresh of that new Group Policy is set to default refresh mechanisms of Group Policy, i.e. refresh for computer/user GPO is every 90 minutes with offset of up to 30 minutes. Security templates created for Group Policy are imported in respective GPOs using Group Policy MMC snap-in. Secedit.exe command line tool in logon script for Group Policy refresh will be used in case of emergency.

Two GPOs, DMZ Policy and DMZWeb Policy are created for Group Policy testing. Default Domain Policy is updated with SWC_therceg.inf security template. Default Domain Controller Policy is left with default settings.

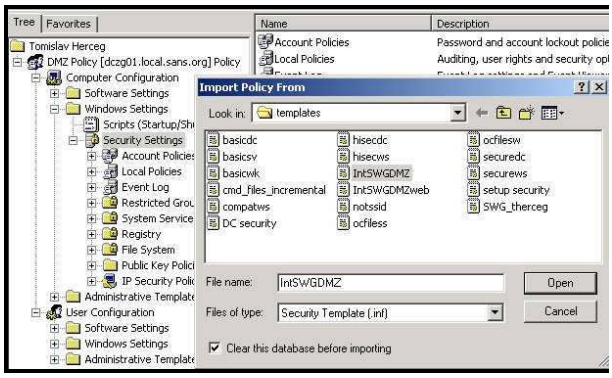


Picture 20: Import security template to Default Domain Policy

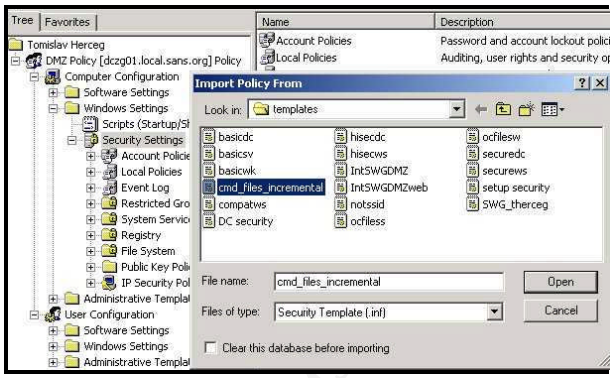


Picture 21: Import security template to DmzWeb Policy

DMZ Policy is linked to DMZ organization unit and updated with IntSWGDMZ.inf security policy and cmd_files_incremental.inf incremental security template that sets NTFS permission only to local Administrators group for number of command line tools such as cmd.exe or tftp.exe.

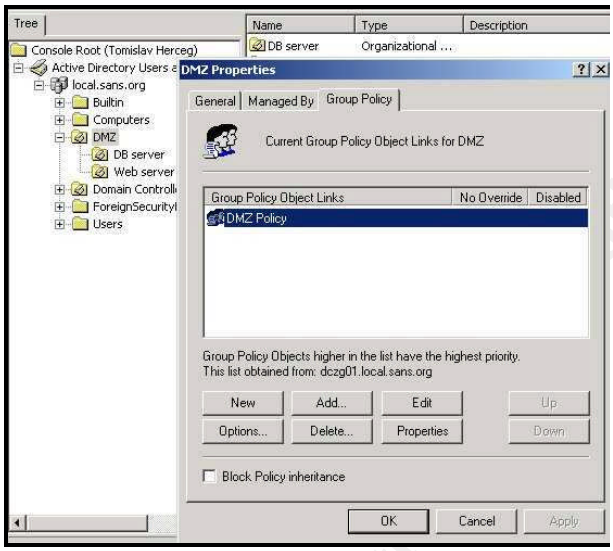


Picture 22: Import security template to DMZ Policy

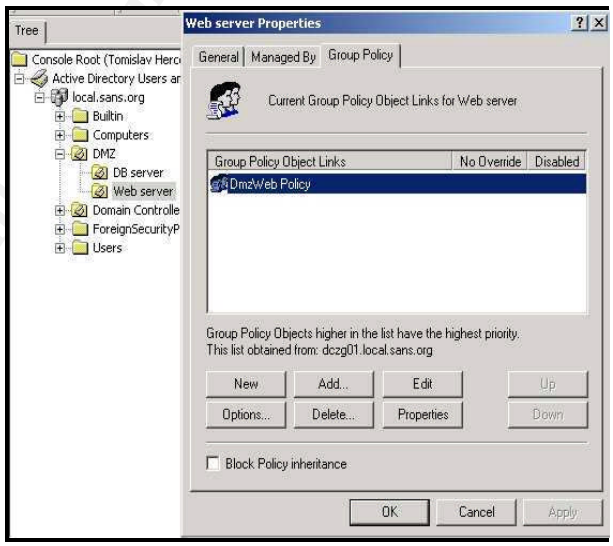


Picture 23: Import incremental security template to DMZ Policy

DmzWeb Policy is linked to Web server OU (OU inside DMZ OU) and updated with IntSWGDMZweb.inf security template based on modify version of secureintranetwebserver.inf. All security templates (except cmd_ files_incremental.inf and InzSWGDMZweb.inf) are showed on the following page.



Picture 24: DMZ Policy link to DMZ OU



Picture 25: DmzWeb Policy link to Web server OU

```
; Security Configuration Template for Security Configuration Editor
;
; Date: 08.04.2004
; Template Name:      SWG_therceg.INF
; Template for GCWN practical assignment based on
; MSS Domain.inf (Securing Windows 2000 Server Guide) and
; w2k_domain_policy.inf (NSA/SNAC W2K Security Guide)

[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1

[System Access]
;-----------------------------------------------------------
;Account Policies - Password Policy
;-----------------------------------------------------------
MinimumPasswordAge = 1
```

```
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24

;-------------------------------------------------------------
;Account Policies - Lockout Policy
;-------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = 30
ForceLogoffWhenHourExpire = 1

;-------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
MaximumLogSize = 179200
AuditLogRetentionPeriod = 2
[Security Log]
MaximumLogSize = 179200
AuditLogRetentionPeriod = 2
[Application Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0

;-------------------------------------------------------------
;             Local Policies\Audit Policy
;-------------------------------------------------------------
[Event Audit]
AuditLogonEvents = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditAccountLogon = 3

;-------------------------------------------------------------
;Account Policies - Kerberos Policy
;-------------------------------------------------------------
[Kerberos Policy]
MaxTicketAge = 8
MaxRenewAge = 10
MaxServiceAge = 480
MaxClockSkew = 5
TicketValidateClient = 1

[Profile Description]
Description=Local.sans.org baseline domain template

[Registry Values]
[Service General Setting]
Messenger,4,"D:(A;OICI;GA;;;WD)"
wuauserv,2,"D:(A;OICI;GA;;;WD)"
```

SWG_therceg.inf security template

```
; Security Configuration Template for Security Configuration Editor
;
; Date: 08.04.2004
; Template Name:       IntSWGDMZ.INF
; Template for GCWN practical assignment use
; TCP/IP hardening and other security registry setting described in
; Stefan Norberg book "Securing Windows NT/2000 Servers for the Internet"
```

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1

;-------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
MaximumLogSize = 307200
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 307200
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 3145728
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

;-------------------------------------------------------------------------
;             Local Policies\Audit Policy
;-------------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 2
AuditAccountLogon = 3

[Profile Description]
Description=Baseline template for servers in DMZ OU


[Service General Setting]
Alerter,4,"D:(A;OICI;GA;;;WD)"
ClipSrv,4,"D:(A;OICI;GA;;;WD)"
Browser,4,"D:(A;OICI;GA;;;WD)"
Dfs,4,"D:(A;OICI;GA;;;WD)"
TrkWks,4,"D:(A;OICI;GA;;;WD)"
TrkSvr,4,"D:(A;OICI;GA;;;WD)"
SharedAccess,4,"D:(A;OICI;GA;;;WD)"
mnmsrvc,4,"D:(A;OICI;GA;;;WD)"
Spooler,3,"D:(A;OICI;GA;;;WD)"
TlntSvr,4,"D:(A;OICI;GA;;;WD)"
seclogon,3,"D:(A;OICI;GA;;;WD)"
RemoteAccess,4,"D:(A;OICI;GA;;;WD)"
RasMan,4,"D:(A;OICI;GA;;;WD)"
RasAuto,4,"D:(A;OICI;GA;;;WD)"
[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
```

```
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\NoNameReleaseOnDemand=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxportsExhausted=4,5
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenedRetried=4,80
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen=4,100
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\AutoShareServer=4,0
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisabled8dot3NameCreation=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1
MACHINE\Software\Microsoft\OLE\EnableDCOM=1,N
MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
```

IntSWGDMZ.inf security template

3.4 TEST OF POLICY SECURITY SETTINGS

To evaluate how policy security settings are applied two tests are conducted:

A. domain user that is only member of web server's local User group tried to logon locally on web server
B. lifetime settings are examined using Kerberos Tray tool (Kerbtray.exe)[3].

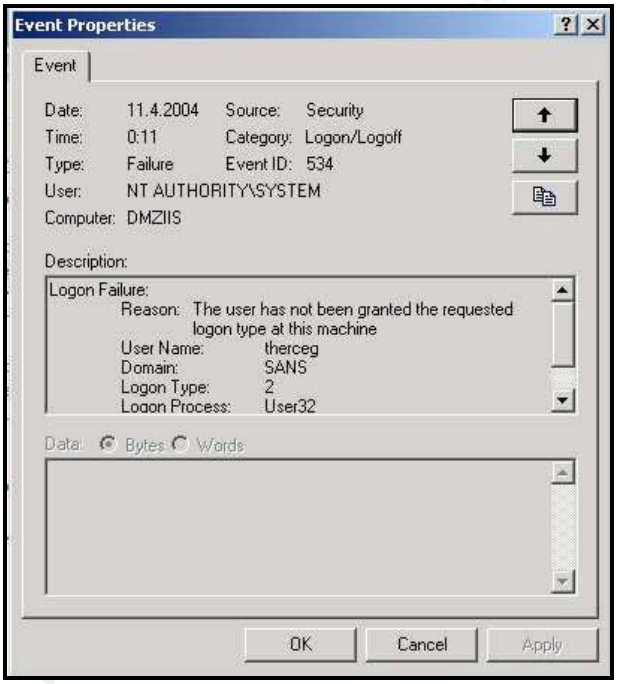
Test A: Logon locally on web server

Logon locally security settings are defined in DmzWeb policy and allow logon locally only to Account Operators, Administrators, Backup Operators, Print Operators and Servers Operators. When user that is not a member of one of these groups tries to logon locally he gets warning logon message "The local policy of this system does

[3] The Windows 2000 Server Resource Kit: Supplement 1, http://www.microsoft.com/windows2000/techinfo/reskit/default.asp

not permit you to logon interactive". Corresponding logon/logoff event are created also.

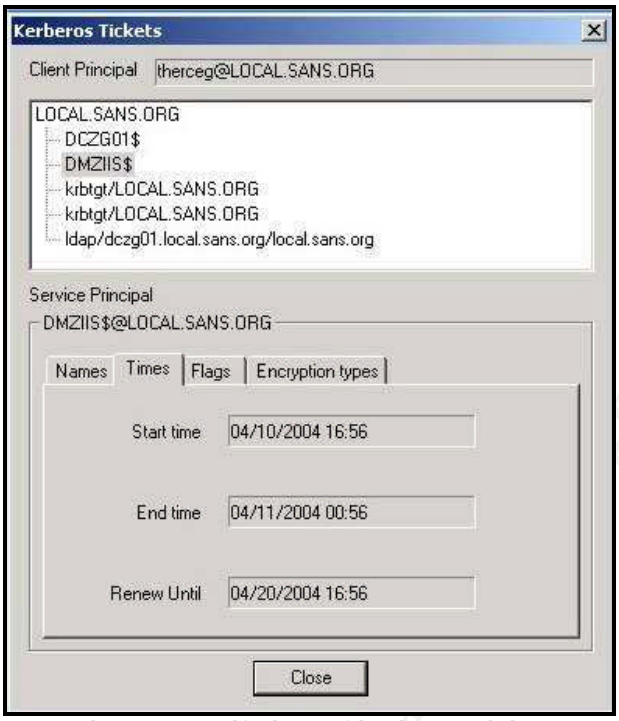
Picture 26: Local logon failed on web server



Picture 27: Security event for failed local logon

Test B: Kerberos ticket lifetime setting

Kerberos tickets are created and cached on local computer when user successfully logs on computer. Using Kerberos Tray tool for examining one of tickets, on Times tab we can see lifetime of that ticket. On enclosed pictures "Lifetime of kerberos ticket" you can see Kerberos ticket start time is 16:56 (04:56 p.m.) on 04/10/2004 and end time is 00:56 (00:56 a.m.) on 04/11/2004. That means that maximum lifetime for that ticket is 8 hours which is exactly the same as Maximum lifetime for user ticket defined in Kerberos settings in Default Domain Policy. Same thing goes for Renew until time value which is 16:56 (04:56 p.m.) on 04/20/2004 as defined in Maximum lifetime for user ticket renewal and set to 10 days.



Picture 28: Lifetime of kerberos ticket

3.5 SYSTEM FUNCTIONALITY TEST

To evaluate if applied policy security settings will cause any problems and affect system functionality, two tests are performed:

A. browse default page on SansWGiac web site and perform queries against SQL server database
B. run scheduled task with VBScript that copies IIS logs files from shared folder on web server to shared folder on management server (in this case on SQL server).

Test A: Browsing SansWGaic web site

Default.asp page is created in root folder of Default web site for testing purposes. VBScript is used as script language for default.asp. VBscript on default.asp through ADO connects to SansWGiac database and executes get_all_product stored procedure. For connection to SQL server and SansWGiac database script uses trusted connection e.g. through windows authentication accesses SQL server with account defined for IIS anonymous access which is iis_user domain account. SQL server is not installed on the same server as web server.

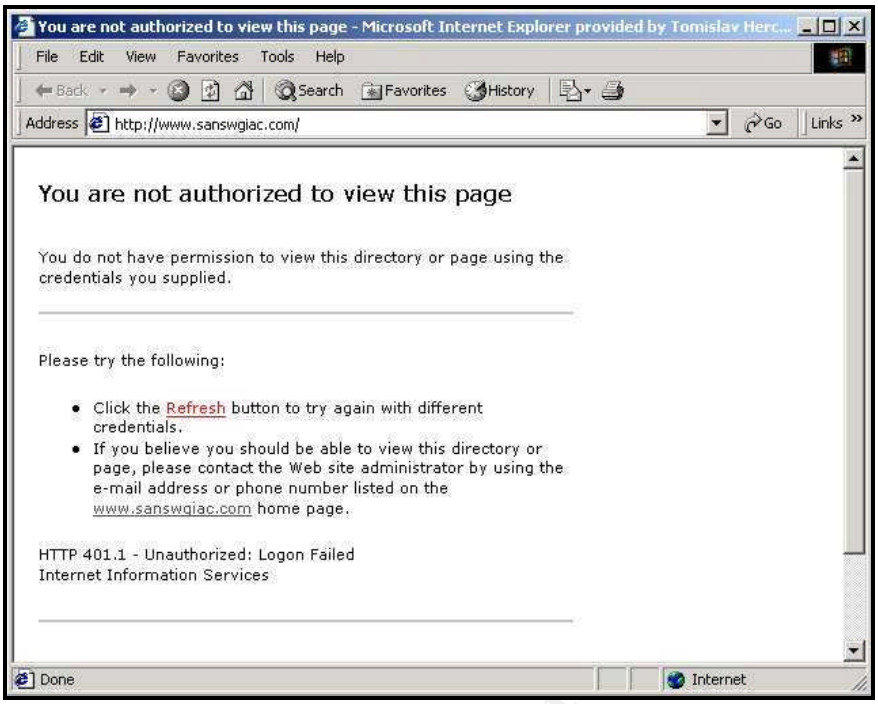
```
<%@ LANGUAGE="VBSCRIPT" %>
<HTML>
<HEAD>
<META HTTP-EQUIV="Content-Type" content="text/html; charset=iso-8859-1">
<TITLE>Welcome to SansWGiac company</TITLE>
</HEAD>
<BODY>
<h1>Get you sea food catering at SansWGiac company</h1>
<%
Set objconn=CreateObject("ADODB.Connection")
Set objrs=CreateObject("ADODB.Recordset")
objconn.ConnectionString="Provider=SQLOLEDB;Data Source=dmzsql;Initial Catalog=SansWGiac;" &_
"Trusted_Connection=Yes"
objconn.Open
strSQL = "exec get_all_product"
objrs.Open strSQL, objConn
Do Until objrs.EOF
name = (objrs(0))
Response.Write("" & name & "")
%>
<P>
<%
objrs.MoveNext
Loop
%>
<a href="https://www.sanswgiac.com/orders">Order now (Secure site)</a>
</BODY>
</HTML>
```

Default.asp script

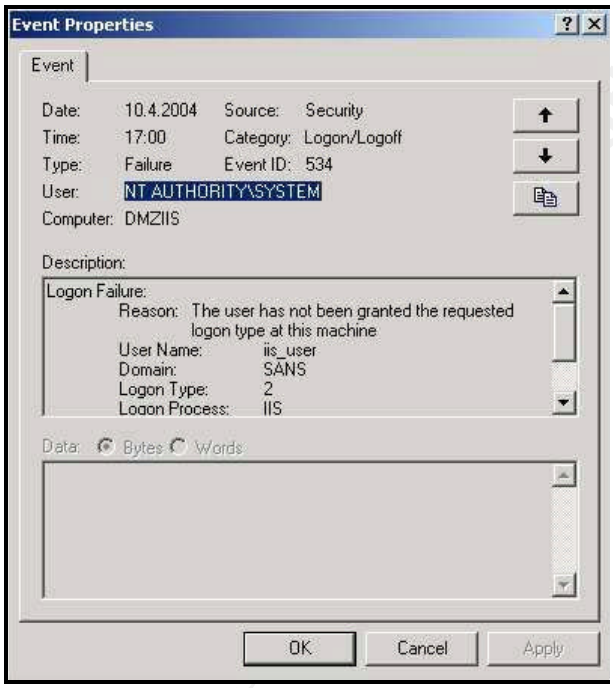
First time we tried to access to default web page we got "HTTP 401.1 - Unauthorized: Logon Failed" error. Also on web server respective event log entries with ID 534 for logon type 2 (Interactive logon) and logon type 4 (Batch logon) are generated for user iis_user. In IIS log sc_status was "401 5" (without quotes).

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2004-04-10 12:21:33
#Fields: date time c-ip cs-username cs-method cs-uri-stem cs-uri-query sc-status sc-win32-status time-taken cs(User-Agent) cs(Cookie) cs(Referer)
2004-04-10 12:21:33 192.168.1.2 - GET / - 401 5 640 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) -
2004-04-10 12:21:49 192.168.1.2 - GET / - 401 5 15 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:21:50 192.168.1.2 - GET / - 401 5 15 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:21:51 192.168.1.2 - GET / - 401 5 47 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:21:53 192.168.1.2 - GET / - 401 5 16 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:21:54 192.168.1.2 - GET / - 401 5 31 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:21:55 192.168.1.2 - GET / - 401 5 31 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:21:57 192.168.1.2 - GET / - 401 5 32 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:22:03 192.168.1.2 - GET / - 401 5 16 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:22:04 192.168.1.2 - GET / - 401 5 62 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:22:05 192.168.1.2 - GET / - 401 5 47 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:22:07 192.168.1.2 - GET / - 401 5 93 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:22:08 192.168.1.2 - GET / - 401 5 31 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:25:16 192.168.1.2 - GET / - 401 5 47 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
2004-04-10 12:25:16 192.168.1.2 - GET / - 401 5 15 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) - -
```

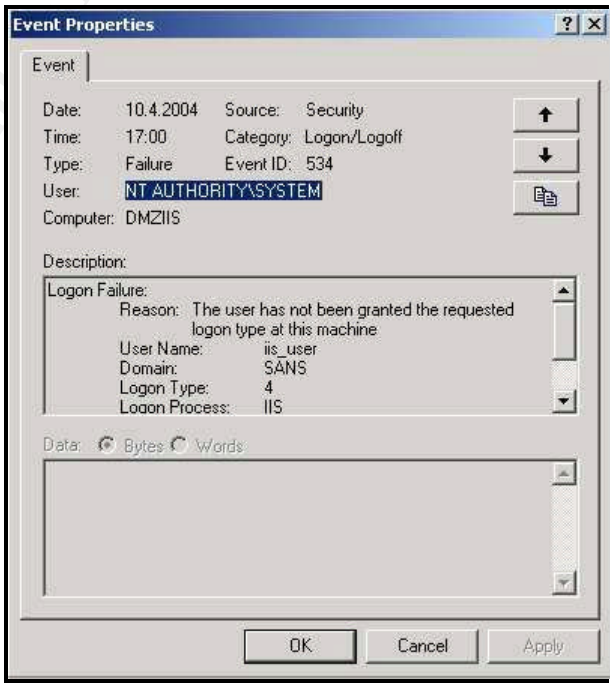
IIS logs with error code 401- Access Denied.



Picture 29: Error when access default web page



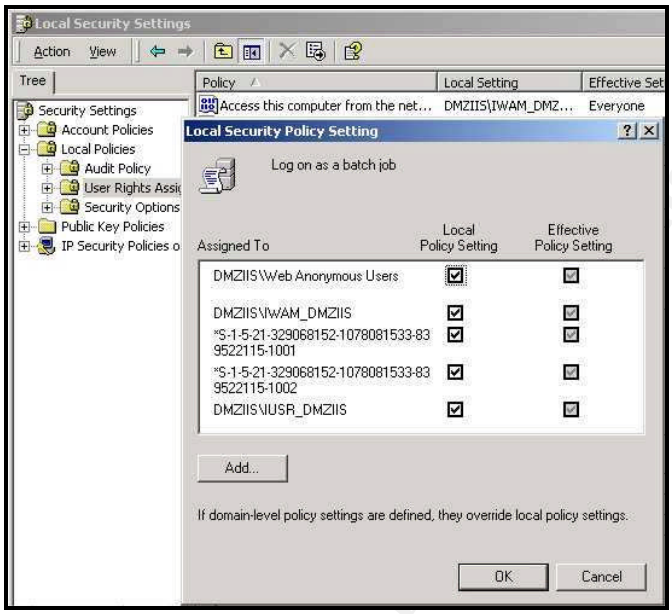
Picture 30: Browsing error event entry for logon type 2



Picture 31: Browsing error event entry for logon type 4

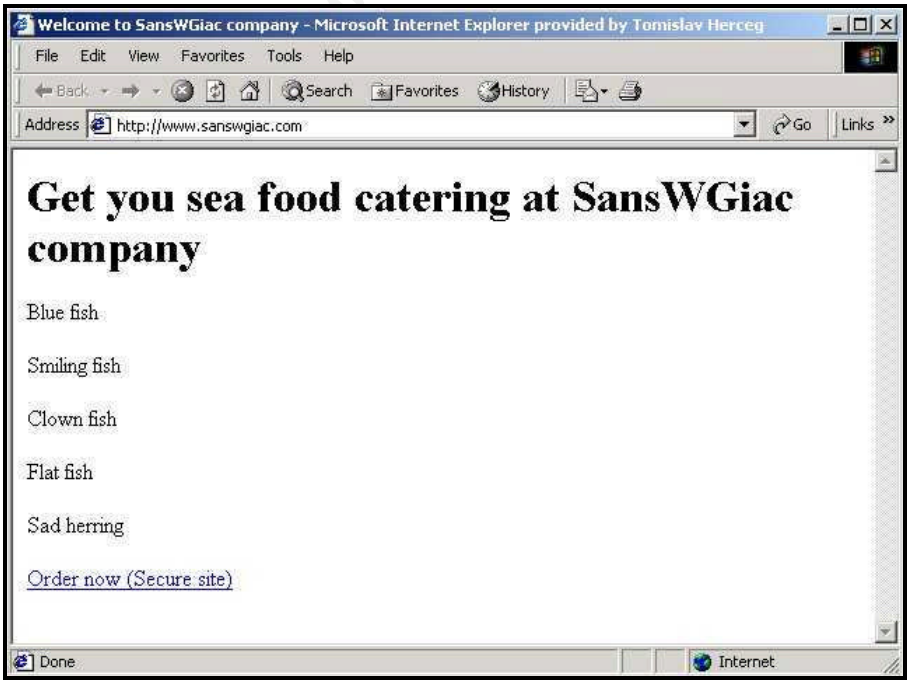
In order to ensure minimal set of rights for web site access and performance of necessary operations we granted rights one by one and tested assigned rights. The goal was to give iis_user minimal set of user rights required for web site operations and verify if it is really necessary for anonymous IIS user (i.e. iis_user) to have interactive logon rights.

Problem is resolved after, in Local security settings, we assigned Log on as batch job user right to local Web anonymous User group (iis_user is member of this group). So conclusion is that account for anonymous access to web site do not need Interactive logon user right, only Log on as batch job right.

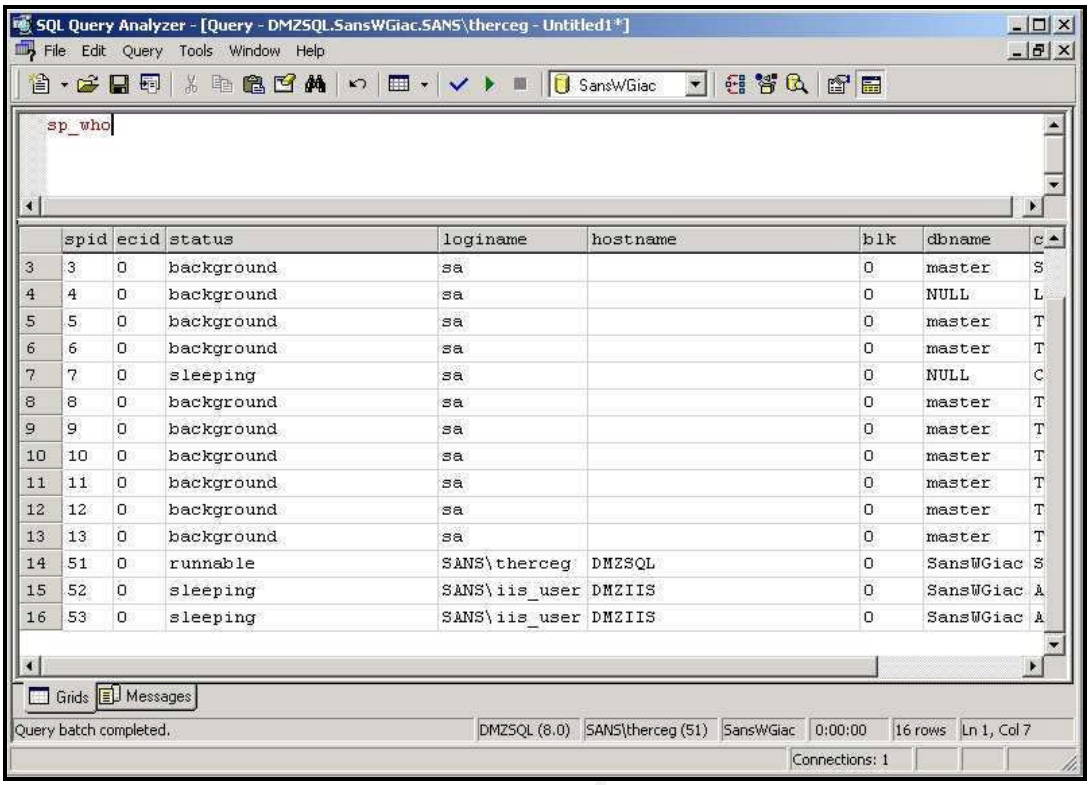


Picture 32: Resolution to browsing problem

Also when we checked information about current SQL server users and processes (using system stored procedure sp_who) on SansWGiac database, SANS\iis_user is displayed which means that connection to database is established to provide data for default web page.



Picture 33: Default page of www.sanswgiac.com web site



	spid	ecid	status	loginame	hostname	blk	dbname	c
3	3	0	background	sa		0	master	S
4	4	0	background	sa		0	NULL	L
5	5	0	background	sa		0	master	T
6	6	0	background	sa		0	master	T
7	7	0	sleeping	sa		0	NULL	C
8	8	0	background	sa		0	master	T
9	9	0	background	sa		0	master	T
10	10	0	background	sa		0	master	T
11	11	0	background	sa		0	master	T
12	12	0	background	sa		0	master	T
13	13	0	background	sa		0	master	T
14	51	0	runnable	SANS\therceg	DMZSQL	0	SansWGiac	S
15	52	0	sleeping	SANS\iis_user	DMZIIS	0	SansWGiac	A
16	53	0	sleeping	SANS\iis_user	DMZIIS	0	SansWGiac	A

Picture 34: IIS_user connection to SQL server

Test B: Gathering IIS logs on management share folder

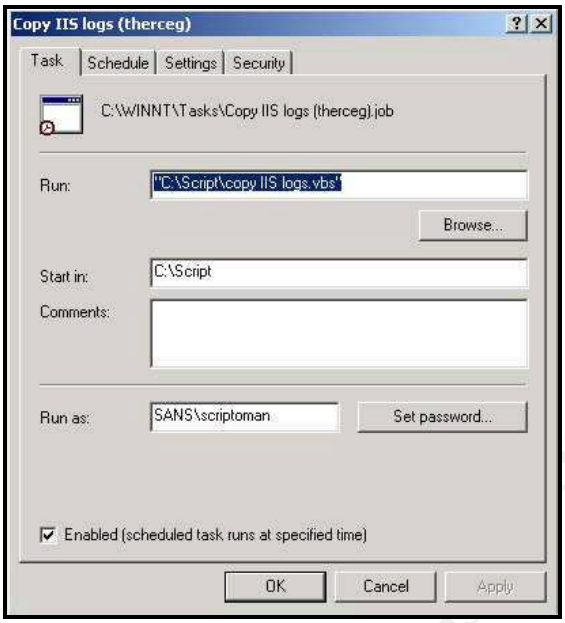
Folder CopyIISLogs is created on management server (in this case on SQL server). It is shared with share name CopyIISLogs and assigned share permissions are Full control for Everyone. NTFS permission for CopyIISLogs share are set to Full control for local Administrators group and System group and Modify permissions for Scriptoman domain user account. Source folder with IIS logs (IISLogs on dmziis server) and set share and NTFS permission are described at the beginning of Group Policy test evaluation in section regarding IIS installation and implementation.

```
'============================================================
'
' AUTHOR: Tomislav Herceg
' DATE  : 9.4.2004
'============================================================
Dim objFSO, objFile
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFolder = objFSO.GetFolder("\\dmziis\IISLogs\W3SVC1")
Set colFiles = objFolder.Files

For Each Files In colFiles
        Set objLogFile = objFSO.GetFile("" & files.path & "")
        objLogFile.Copy ("\\dmzsql\CopyIISLogs\")
Next
```

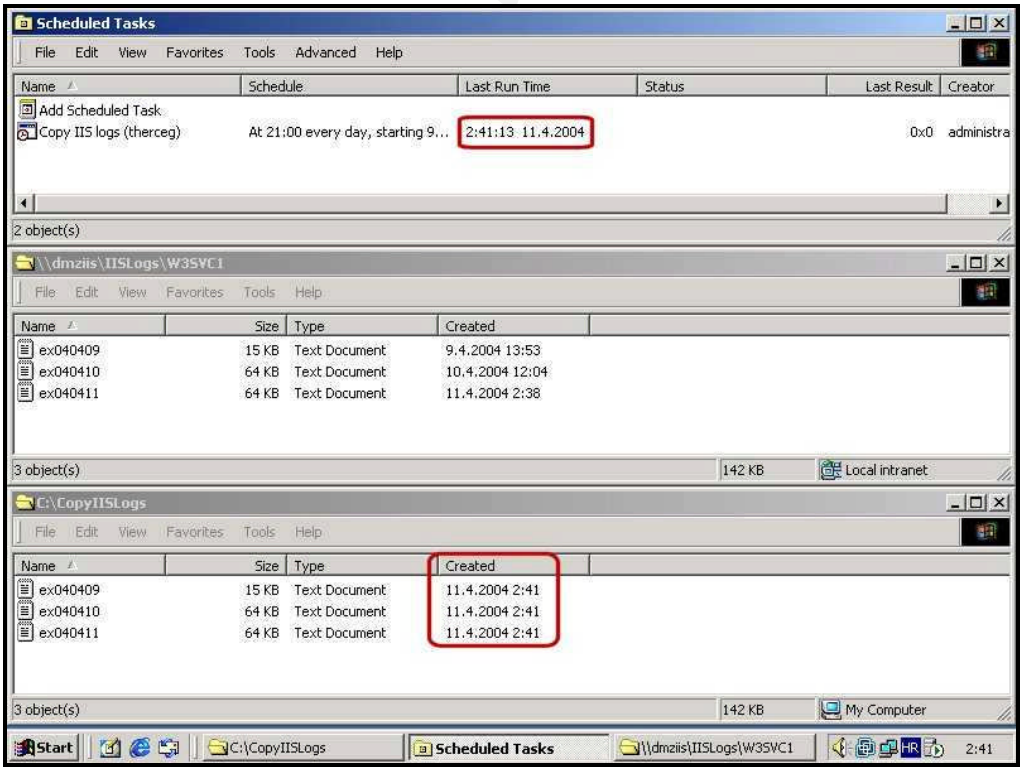
VBScript for IIS logs copy

Task with VBScript is scheduled to run every day at 09:00 p.m. under security context of Scriptoman user. Scriptoman was added to local Administrators group on the server where task is scheduled (dmzsql server).



Picture 35: Copy IIS Logs task general properties

When we manually started the task, VBscript successfully copied IIS log files from dmziis server (shared folder IISLogs) to dmzsql server (shared folder CopyIISLogs). As shown in following picture task "Copy IIS logs (therceg)" started at 02:41:13 on 11.04.2004 and all IIS logs files were copied to CopyIISLogs folder at the same time when task was started.



Picture 36: Copy IIS logs to management server

3.6 EVALUATION OF GROUP POLICY

Group Policy design of SansWGiac Company is based on outspread organizational units structure that enables definition of specific and fine-tuned GPOs but it also brings out large number of created GPOs (42) and security templates (21). Such large number of GPOs and security templates represents challenge against maintenance and administration control. Also customization of security templates used in SansWGiac Group Policy design adds additional overhead to maintenance and administration. But benefits gained by creation of specific GPOs and security templates are much bigger than the problem of maintaining and administrating all GPOs.

The problem of maintaining and administering GPO infrastructure can be solved through efficient delegation of GPOs. IT department can form groups responsible for maintaining and updating several GPOs. Definition and fine-tuning of GPOs for specific servers organizational units requires much effort and time only at the beginning (time spend on creation can be reduced by using tested and well known security templates created by Microsoft and other security organization as NSA or SANS). Administration and maintenance of all Group Policy Object should be assigned to junior IT staff members after the implementation of initial Group Policy infrastructure. That way senior IT staff can devote to optimization and future development of Group Policy design and creation of complex security templates in case of any future business or security needs.

Some issues exist regarding certain security settings applied through GPO such as Account lockout threshold value in Account lockout Policy which can be set only in Default Domain Policy. In other words, some applications like Microsoft Exchange client or Windows 2000 DS/DFS client may send credentials more than once per logon attempt and generated many invalid logon attempts and falsely lock user account. In order to reduce helpdesk phone calls Microsoft recommends to increase threshold to 10 and to require more complex passwords (or passphrases).[4]

If we increase account lockout threshold it could present security issue because the same Default Domain policy applies to servers in DMZ organizational unit which require more restrictive security policies then other servers and workstations in the same domain. Transferring servers from DMZ OU to DMZ domain which has more restrictive account policy is not a solution since it threatens the whole DMZ design. Real solution for servers in DMZ is the definition of more restrictive policy through Audit Policy, User Rights Assignment and Security Options and establishment of efficient auditing system as defined in auditing part of this paper.

For now no other departmental Group Policy exists because Default Domain Policy is tested and evaluated as efficient. If in any case it becomes inefficient, departmental organization unit structure is design with potential GPOs in mind so implementation of any new Group Policy should not be any problem.

[4] Resnick, Mike & Vasil, Joe, Microsoft Windows 2000 Server and Windows Server 2003: Password and Account Lockout Features, Support WebCasts, 2003., http://support.microsoft.com/default.aspx?kbid=813500

4. AUDIT

Auditing system design is a necessity in order to provide proactive and efficient monitoring of complex SansWGiac's Active Directory infrastructure and critical security settings defined by Group Policy design. It has to be totally automated with invention system of collecting, analyzing and storing of all security relevant logs thus allowing fast and efficient forensic analysis in case of any security intrusion. It is also necessary to implement some type of real time monitoring system with performance log tracking, detection of potential bottlenecks and historical data.

Audit policy has to be defined before actual auditing system implementation. It will define what will be monitored, how long it will be monitored and also resources necessary for auditing system implementation. Audit policy has to be verified and approved by management board and all requirements for auditing system have to be defined based on such approved policy.

Audit policy and all implementation details of auditing system will be defined as part of SansWGiac corporate security policy.

4.1 AUDIT POLICY

Audit policy objective is based on STRIDE threat model[5]. STRIDE is acronym made of first letters of words that denote different types of threats, i.e.:

- Spoofing – attacker access to the system using fake user identity or IP address
- Tampering – unauthorized data change
- Repudiation - ability of users to deny that they performed specific actions
- Information disclosure – unwanted disclosure of confidential information
- Denial of service – making a system or application unavailable
- Elevation of privilege – user try to take higher privileges then he already have

After STRIDE threat model analysis following audit policy objectives are defined:[6,7]

- To detected unauthorized tempering with sensitive security principals like Domain Admins or Enterprise Admins.
- To detected unauthorized change of system security policy.
- To detected unauthorized change of server auditing system.
- To detected and record every unauthorized access to system resources.
- To detected and record every suspicion system activity that might affect security.

[5] Improving Web Application Security: Threats and Countermeasures, Chapter 2 - Threats and Countermeasures, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/threatcounter.asp

[6] Heong, Willie Lui Tien, The Design and Implementation of a Windows 2000 Multi-Forest Infrastructure, GCWN Practical Assigment, 2003., http://www.giac.org/practical/GCWN/Willie_Lui_GCWN.pdf

[7] Hynes, Byron, Windows Auditing Enhancements and MACS, PowerPoint Presentation, Microsoft IT Forum 2003, Copenhagen

4.2 AUDITING SYSTEM

SansWGiac auditing system is designed based on audit policy objectives. SansWGiac auditing system consists of the three servers:

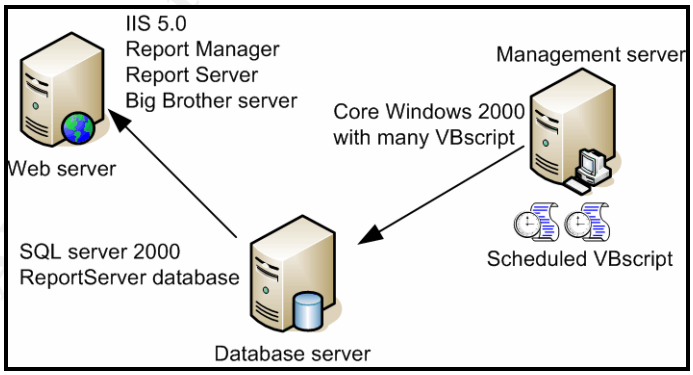
- Web server (IIS 5.0)
- Database server (SQL server 2000)
- Management server

All three servers are Windows 2000 machines with service pack 4 installed. On database server SQL server 2000 with service pack 3a is installed. Management server hosts no additional OS components. On web servers .Net framework is installed due to requirements of SQL server Reporting Services.

Report generating (weekly, monthly and yearly) is based on SQL server Reporting Services. It is made of 3 main components:

- Report Manager - application layer
- Report Server - server layer
- ReportServer database - data layer

Report Manager and Report Server are installed on web server while ReportServer database is installed on database server. Weekly reports are generated every Sunday at 6:00 p.m. and stored in folder Week Report on web server. Week report folder contains subfolders numbered by weeks in which reports are stored for specific week. Monthly reports are generated every first Monday in month and stored in Month Report on web server. Month report folder also has subfolders numbered by months in which specific reports are stored. Yearly report is generated by the end of each year. This data is additionally processed using Microsoft Excel Pivot tables and possible security improvements are suggested based on data analysis. This report is send to management board.



Picture 37: Auditing system architecture

Folders Week Report and Month Report are copied on daily basis to shared folder on file server which is daily backup on tapes.

Actual implementation of log collection and monitoring of system and Active Directory modifications is based on VBScripts placed on management server. VBScripts use Windows Management Instrumentation (WMI) infrastructure and Active Directory Services Interface (ADSI) as scripting interface to Active Directory infrastructure. VBScripts are executed using Task Scheduler.

VBScripts for log collection are executed during night or weekend when network traffic is low. All event logs are deleted from servers after have been successfully stored in database. The deletions of event logs are taken down in VBScript log on management server.

VBScripts for collecting security and system event logs are executed according to the following schedule:

- VBScript for domain controllers is executed daily at 9:00 p.m. In addition, Directory Service, DNS server and File Replication Service logs are gathered from domain controllers.
- VBScript for workstations is executed every Saturday at 12:00 a.m. for gathering all logs necessary for week reports.
- VBScript for corporate servers (mail server, file server and infrastructure servers) is executed daily at 10:00 p.m.
- VBScript for servers in DMZ organizational unit is executed daily at 11:00 p.m.
- VBScript for servers in DMZ zone is executed daily at 8:00 p.m.

VBScripts for collecting application event logs are executed according to the following schedule:

- VBScript for domain controllers is scheduled every Saturday at 12:00 p.m.
- VBScript for infrastructure and mail servers is scheduled at 10:00 p.m.
- VBScript for other servers (database servers, file servers) is scheduled every Saturday 1:00 p.m.
- VBScript for DMZ servers is scheduled every Saturday at 2:00 p.m.

Application logs from workstation are not regularly collected and are overwritten as needed.

Group Policy design defines event log maximum size large enough to keep all logs. Retention methods for system and security logs are defined as Do not overwrite events (clear log manually).

All event logs are stored on database server. New database for storing logs is created by the beginning of year. Database consists of several tables defined by months for specific server type. Thus for storing event logs from domain controllers there are 12 different tables in database. This way the queries for report generation are speed up.

Alert VBScripts scheduled on management server are executed every 30 minutes and analyze stored event logs for event IDs such as ID 529 (user attempt to log on with invalid username or password), ID 531 (user account is disabled), ID 539 (user account locked out) and send alerts by email or SMS messages to responsible IT members. Different alert script is defined for each server and service type.

Alert email messages are sent using SMTP mail servers (SMTP engine on Exchange server inside corporate network and SMTP relay engines in DMZ). In order to prevent unauthorized relying on all SMTP servers are defined IP addresses for relaying messages. GPRS modem[8] is implemented for sending alerts by SMS messages.

[8] http://www.gsm-modem.de/gprs-module.html

GPRS modem consists of standard GPRS cell-phone card and serial cable connected to management server. When alert is generated, VBScript with at command creates SMS message and sends is through GPRS modem.

Standard SQL server backup is used for backing up event log database. For performance reasons database backups up on disk and then on tape using Windows backup. Backup is performed on daily bases and two last copies of database kept, e.g. on Monday there are backups from Saturday and Sunday. Every last Friday in month database is backuped on tape which is then stored and kept for 3 years in fireproofed safe.

Logs stored in textual files, e.g. IIS logs, SQL server logs, SMTP logs and ISA server logs, are also gathered using VBScripts.

VBScripts for collecting .txt logs are executed according to the following schedule:

- VBScript for web servers (IIS) is scheduled daily at 9:00 p.m.
- VBScript for database servers is scheduled every Saturday at 11:00 a.m.
- VBScript for mail servers is scheduled daily at 10:00 p.m.

Textual log files are copied to shared folder on management server using VBScripts. After successful copying log files are processed with specific VBScripts that analyze log files searching for signature of possible hacker attack by using Log Parser COM architecture[9] (LogParser.dll). If possible hacker attack is detected then VBScript send alert e-mail or SMS messages to responsible IT members. When analysis is finished log files are transferred to database using SQL Output format from Log Parsers tool. Textual log files are later moved to shared folder on file server and then backuped up on tape. Tape containing backups from last month of the year is stored and kept for 3 years in fireproof safe.

Web servers in DMZ hold additional VBScript that analyses logs every 5 minutes and almost in real time can detect every attempt of hacker attack and send alerts to responsible IT stuff via email.

VBScripts based on WMI infrastructure especially on WMI Event Scripting are used for monitoring unauthorized configuration changes in Active Directory. For example, VBScript are created as WMI temporary event consumers that monitor changes in value "Schema Update Allowed" defined in registry key HKLM\System\CurrentControlSet\Services\NTDS\Parameters. If value is change from 0 to 1 then VBScript send alert by e-mail or SMS messages. VBScript is runs on management server as all other VBScript.

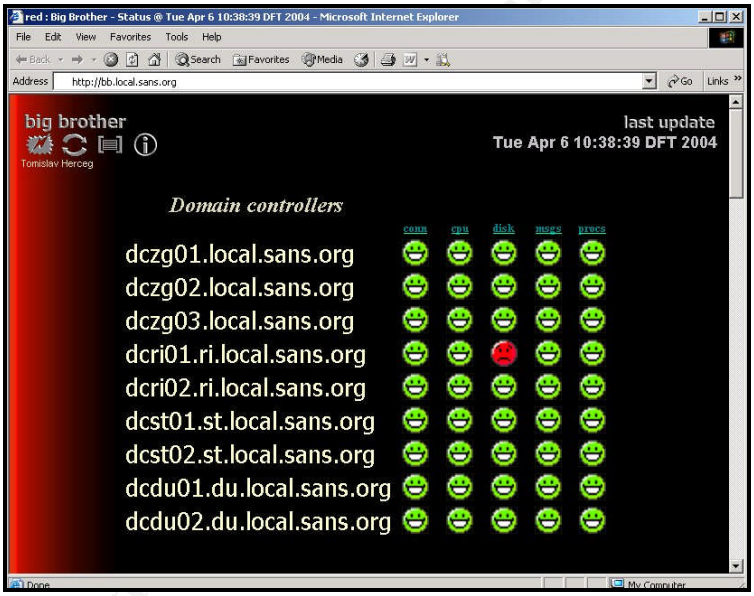
Auditing system with accompanying VBScripts is designed as self healing system. In addition we have another set of VBScripts (so called older brother VBScript - ObVBScript) used to monitor production VBScript, e.g. scripts that collect and parse logs. When ObVBScript detects that production VBScript does not work it tries to fix the problem. If problem remains responsible IT staff is notified by e-mail or SMS messages. Every second week IT people manually check every VBScript logs.

[9] Log Parser Tool Ver. 2.1 from IIS 6.0 Resource Guide Tools, http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en

Big Brother monitoring system[10] is used for real time monitoring and tracking of all critical network services. Big Brother's design is based on client server architecture. Server side of the system is installed on web server while client side is installed locally as service on servers that want to be monitored.

Client software supports monitoring disk space, CPU usage, event log messages and can check that important processes or services are up and running. Also Big Brother System support monitoring of ftp, http, https, smtp, pop3, dns, telnet, imap, nntp, and ssh services without client software installation. Monitoring of other required services can be easily added.

Server side of Big Brother supports also alert notification which in case of Windows NT/2K server is limited to email messages. In order to provide notification by SMS VBScript that checks Big Brother's notification mailbox, generates SMS message in case of new notification email and sends it through GPRS modem. In addition, Big Brother system support reporting and access to historical status information.



Picture 38: Big Brother web page

Server status monitored by Big Brother is displayed in web or WAP page. Different colors are used for presenting different system status of monitored servers where red color indicates potential problem with monitored service while green color indicates that service is up and running. Background color of web page with monitored servers is also changed depending on different server status. Web page can be customized according to ones needs and requirements. Data collection and verification of service status is set to every 5 minutes.

Intrusion Detection System (IDS) called RealSecure Server Sensor for ISA Server[11] is implemented on ISA servers in DMZ domain. Host-based IDS for monitoring sensitive accounts and groups is installed on all domain controllers.

[10] http://bb4.com/features.html
[11] http://www.iss.net/isaserver/

Every six months IT stuff will schedule independent vulnerability assessment and penetration testing with previous approval from management.

4.3 PATCH MANAGEMENT SYSTEM

SansWGiac company's patch management system consists of two separate systems. Microsoft Software Update Services (SUS) is implemented in forest local.sans.org and, on the other hand, Update Expert in forest giac.com. Both systems are kept after merger because the migration and integration of patch management system is planned after release of new SUS 2.0 services (now named WUS – Windows Update Services).

Considering new improvements and functionalities of new WUS (support for various version of Windows, Office, Exchange and SQL Server, better logging capabilities and reporting, frequency and time schedule when managed systems should check for approved updates, etc.)[12] that draws it near to Update Expert, all patch management will be migrated to WUS. During migration, current infrastructure of SUS servers will be kept and, in addition, two new SUS servers will be added to giac.com forest (one server for update of workstation and one for server update). Thus the whole patch management system will be standardized eliminating administration overhead of maintaining two different products and what is most important costs of licensing Update Expert will be eliminated.

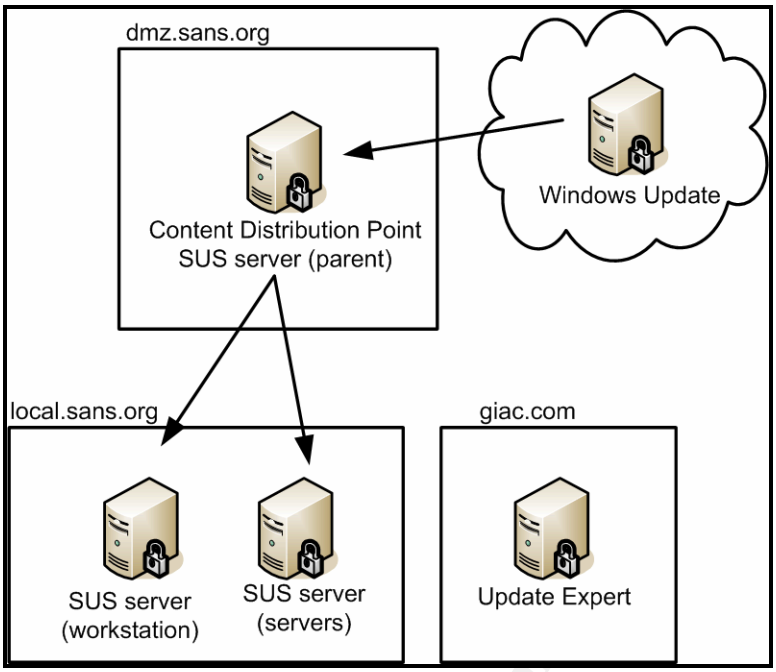
SANS Company SUS server architecture is based on scale-out model and consists of 3 servers. One server is located in dmz.sans.org forest (DmzSus) while others are located in local.sans.org forest (SansSusW and SansSusS). DmzSus server in DMZ is updated from Windows Update web site and used as Content Distribution Point for SansSusW and SansSusS servers. Also DmzSus server is used as primary SUS server for servers placed in dmz.sans.org forest. In order to reduce downtime of servers in DMZ zone only installation of security patches rated as critical is approved. Security patches rated as important are installed only if IT stuff determines that vulnerability is likely to affect particular server's configuration.

As current version of SUS service does not support definition of different sets of approved security patches, in local.sans.org forest two SUS servers are installed:

- SansSusW server - only for workstation update
- SansSusS server - only for servers update

This way on SansSusW server we can approve all security patches and schedule installation on workstations every morning at 06:00 a.m. (if new patch exists) no matter of their rating. On the other hand, on SansSusS server we approve only security patches rated as critical or important and schedule installation on servers in controlled manner (usually during night in 02:00 a.m.). This way we provide timely installation and application of security patches on workstations and servers and also ensure high server uptime.

[12] http://download.microsoft.com/download/3/d/e/3de7e695-109a-494f-b43a-5cb8f7f98293/WinUS_Datasheet.doc



Picture 39: Patch management system in SansWGiac Company

All Automatic Updates client (in dmz.sans.or and local.sans.org forest) are configured with Auto download and scheduled install behavior.

5. REFERENCES

Best Practice Active Directory Deployment for Managing Windows Networks, http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/depovg/bpaddply.mspx

Best Practice Active Directory Design for Managing Windows Networks, http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/bpaddsgn.mspx

Borge, Stein, Managing Enterprise Systems with the Windows Script Host, Apress, 2002, ISBN: 1-89311-567-4

Cox, M. Philip, Design a secure Windows 2000 Infrastructure, GCWN Practical Assignment, 2002., http://www.giac.org/practical/Phillip_Cox_GCWN.doc

Cox, Philip, Hardening Windows 2000 ver. 1.3, System Experts, 2002, http://www.systemexperts.com/win2k/hardenW2K13.pdf

Cribben, Mark & Sayers, Dave, Deploying Active Directory and MMS in Multi-Forest Scenarios: Mergers, Acquisitions, Grass-Roots Deployments and Autonomous Organizations (Part 1&2), PowerPoint Presentation, Microsoft IT forum 2002, Copenhagen

Deploying Microsoft Software Update Services, http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx

Design Considerations for Delegation of Administration in Active Directory, http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/addeladm.mspx

Fossen, Jason, DNS & Group Policy, The SANS Institute, 2003.

Galkine, Alexei, AD Design, Group Policy and Audit for SANS Co. and GIAC Enterprise merge, GCWN Practical Assignment, 2003., http://www.giac.org/practical/GCWN/Alexei_Galkine_GCWN.pdf

Garden, Jay; Design, Secure and Audit the Combined SANS Co & GIAC Windows 2000 Network, GCWN Practical Assignment, 2003., http://www.giac.org/practical/GCWN/Jay_Garden_GCWN.pdf

Heong, Willie Lui Tien, The Design and Implementation of a Windows 2000 Multi-Forest Infrastructure, GCWN Practical Assigment, 2003., http://www.giac.org/practical/GCWN/Willie_Lui_GCWN.pdf

Hynes, Byron, Windows Auditing Enhancements and MACS, PowerPoint Presentation, Microsoft IT Forum 2003, Copenhagen

Improving Web Application Security: Threats and Countermeasures, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/threatcounter.asp

Lissoir, Alain, Understanding WMI Scripting, Digital Press, 2003, ISBN: 1-55558-266-4

Microsoft Solution for Securing Windows 2000 Server, http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/default.mspx

Microsoft SQL Server 2000 Reporting Services Deployment Guide, http://www.microsoft.com/technet/prodtechnol/sql/2000/deploy/rsdepgd.mspx

Microsoft Windows 2000 Security Hardening Guide, http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

MSA Enterprise Design for DNS, http://www.microsoft.com/resources/documentation/msa/2/all/solution/en-us/msa20rak/vmhtm76.mspx

MSDN Library, Building and Configuring More Secure Web Sites, 2002., http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/openhack.asp

Multiple Forest Considerations, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/mtfstwp.mspx

Norberg, Stefan, Securing Windows NT/2000 Servers for the Internet, O'Reilly, 2001, ISBN: 1-56592-768-0

NSA/SNAC Operating Systems Guides - Microsoft Windows 2000 Guides, http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/w2k_securityguides.zip

Planning and Implementing Federated Forests in Windows Server2003, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/fedffin2.mspx

Resnick, Mike & Vasil, Joe, Microsoft Windows 2000 Server and Windows Server 2003: Password and Account Lockout Features, Support WebCasts, 2003., http://support.microsoft.com/default.aspx?kbid=813500

Riley, Steve, Improving Trust In Your Infrastructure With IPSec, PowerPoint Presentation, TechNet Technical Traning CD 24, 2003.

Riley, Steve, ISA Server Internals and Infrastructure Design, PowerPoint Presentation, Microsoft IT Forum 2003, Copenhagen

Smith, Randy Franklin, Application-layer Filtering: Moving Security up the Network stack, Security Watch, A quarterly Publication produced by Windows & .NET magazine, August 2003.

The Windows 2000 Server Resource Kit: Supplement 1, http://www.microsoft.com/windows2000/techinfo/reskit/default.asp

What's New in Clustering for Windows Server 2003 - For Server Clusters and Network Load Balancing, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering/newclust.mspx

Windows Server 2003 Security Guide, http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

Windows Update Services - Beta Version Datasheet, http://download.microsoft.com/download/3/d/e/3de7e695-109a-494f-b43a-5cb8f7f98293/WinUS_Datasheet.doc