Global Information Assurance Certification Paper

Jeff Wankel

Securing Windows 2000 Practical

Version 3.1

Secure Active Directory Design for GIAC Enterprises

Table of Contents

Table of Figures

OVERVIEW OF GIAC ENTERPRISES

GIAC Enterprises is a financial software company. GIAC develops accounting and financial software for mid-tier manufacturing companies. With the recent economic downturn, GIAC Enterprises must continue to evolve its software by adding further integration with customer's ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management) software. Therefore, it is imperative that the software development department maintain a high level of security to protect the company's assets.

The headquarters is located in Chicago, Illinois. The main functions of the company are located at this facility. These functions include accounting, sales and marketing, human resources, professional services, product development and product support. An office located in Miami, Florida is home to a sales team and a professional services group.

Due to customer support requirements, highly available Internet connectivity is a must. Therefore, both sites have two T3 connections to the Internet from different providers with redundant routers, firewalls and VPN (Virtual Private Network) devices. Public web servers allowing access to the support knowledge base and software patches are located on DMZ (De-Militarized Zone) segments off the firewalls.

NETWORK DESIGN AND DIAGRAM

The physical network design for GIAC Enterprises encompasses two sites and several subnets. In Chicago, there is a main corporate subnet where most of the users and servers are located. An enclave contains the software development department. A DMZ containing publicly accessible server is located off the redundant firewalls. This configuration protects the development department from internal users and internal segments from external and DMZ segments.

In Miami, a primary subnet contains the site's servers and users. Publicly accessible servers are located in a DMZ network off of redundant firewalls.

Figure 1 shows the physical network design.

Hardware

All servers have a pair of Intel Pro100 Secure Server NICs running in load-balance configuration. This allows the server to utilize IPSec for encryption of traffic without a significant performance hit to the CPU. Client workstations utilize Intel Pro100 Secure NICs. The IPSec policy will be discussed later in the document.

For fault tolerant disk storage, all servers utilize four hot-pluggable SCSI 9GB hard disks in a RAID-5 configuration with one disk configured as a hot spare.

Software

Unless otherwise noted, all servers are running Microsoft Windows 2000 with service pack 2, IE 6.0, and all hot fixes and security patches. Client workstations are running Windows 2000 with service pack 2, Internet Explorer 6.0, Office XP and all security hot fixes and patches.

Individual Servers

Chisrv01
This server is a domain controller for the giac.com domain and the Flexible Single Master Operation (FSMO) for schema master, domain naming master, RID master, PDC emulator, infrastructure daemon. It serves as an active directory integrated DNS server and an Enterprise Certificate Authority (CA). This server runs Backup Exec from Veritas and attaches to an external tape backup system. It serves as a secondary backup server in case chisrv02 is busy or malfunctioning.

Chisrv02
This machine serves as a domain controller for the giac.com and is the Global Catalog server. It is running an Active Directory integrated DNS server. The server is also the DHCP server for the Chicago user subnet. This server is attached to an external tape backup system and runs Veritas Backup Exec. All servers in Chicago are backed up by this server.

Chisrv03
As a print and file server for Chicago users, this machine is loaded with 6 36GB SCSI hard drives in a RAID 5 array with one drive as a hot spare. Department directories for sales, support, professional services, IS and helpdesk are located on this machine. An automated copy script is run every hour to copy the changed files on the sales and professional services directories to miasrv01. This server houses half of the printers in Chicago.

Chisrv04
Also serving as a print and file server for Chicago users, this machine is loaded with 6 18GB SCSI hard drives in a RAID 5 array with one drive as a hot spare. This machine contains the Chicago user directories. This server contains the other half of the printers in Chicago.

Chisrv05
This server handles file shares for the HR and finance departments. It contains 6 36GB SCSI hard drives configured in a RAID 5 array with a hot spare.

ChiApp01
This server is an application server for the accounting and finance department. This machine is loaded with 8 9GB SCSI hard drives in a two RAID 5 arrays with one drive in each as a hot spare. This application server communicates with databases in the SQL Server cluster.

Chidev01
This server houses the files of the software development department. It is located behind a pair of redundant firewalls that limit access to the server and its users.

Chimail01
This server is running Microsoft Exchange 2000 and houses all mailboxes for the Chicago users. Mail for Miami users is routed via the VPN to the Miami Exchange 2000 server.

Chimail02
This server is running Symantec Norton Anti-Virus for Gateways that performs virus scanning and mail control for inbound SMTP traffic. Inbound mail is scanned for viruses and checked against inbound mail standards. Mail that passes the checks is routed to chimail01 for delivery to user mailboxes. This server is located on the DMZ segment of the network and is a member of the giac.net domain.

Chisql01
This machine is running Windows 2000 Advanced Server and Microsoft SQL Server 2000. It is configured in a cluster with chisql02. It is the primary database server for the support knowledge base that is accessed from web servers located in the DMZ. It is the standby database server for the accounting and financial applications. The knowledge base is replicated with the database cluster located in Miami.

Chisql02
This machine is running Windows 2000 Advanced Server and Microsoft SQL Server 2000. It is configured in a cluster with chisql01. This is the primary database server for the accounting and financial applications. It is the standby database server for the support knowledge base.

Chiwww01
This server is using Windows 2000 Advanced Server and IIS 5.0. The latest security patches for IIS have been applied. This machine is a member of the giac.net domain. This server is a member of a Windows Load Balancing Service (WLBS) pair with chiwww02. This provides for a highly available web farm for access to the support web site.

Chiwww02
This server is using Windows 2000 Advanced Server and IIS 5.0. The latest security patches for IIS have been applied. This machine is a member of the giac.net domain.

This server is a member of a WLBS pair with chiwww01. This provides for a highly available web farm for access to the support web site.

Chiwww03
This server is running IIS 5.0 in addition to Windows 2000 Server. The latest security patches for IIS have been applied. This machine is the intranet server and is a member of the giac.net domain. Availability of this server is not a pressing concern, so it is not configured as part of WLBS farm.

Chidmz01
This machine is a domain controller for the giac.net domain. It is also the Flexible Single Master Operation (FSMO) for schema master, domain naming master, RID master, PDC emulator, infrastructure daemon. It is also an Active Directory integrated DNS.

Miasrv01
This machine serves as a domain controller and Global Catalog server for the giac.com. It is running an Active Directory integrated DNS server. As the file and print server for Miami users, this machine is loaded with 6 18GB SCSI hard drives in a RAID 5 array with one drive as a hot spare. An automated copy script is run every hour to copy the changed files on the sales and professional services directories to Chisrv03. This server is attached to an external tape backup system and runs Veritas Backup Exec. All servers in Miami are backed up by this server.

Miamail01
This server is running Microsoft Exchange 2000 and houses all mailboxes for the Miami users.

Miasql01
This machine is running Windows 2000 Advanced Server and Microsoft SQL Server 2000. It is configured in a cluster with miasql02. It the primary database server for the support knowledge base that is accessed from web servers located in the DMZ. The knowledge base is replicated with the database cluster located in Chicago.

Miasql02
This machine is running Windows 2000 Advanced Server and Microsoft SQL Server 2000. It is configured in a cluster with miasql01. This is the standby database server for the support knowledge base.

Miawww01
This server is running IIS 5.0 in addition to Windows 2000 Advanced Server. The latest security patches for IIS have been applied. This machine is a member of the giac.net domain. This server is a member of a WLBS cluster with miawww02.

Miawww02
This server is running IIS 5.0 in addition to Windows 2000 Advanced Server. The latest security patches for IIS have been applied. This server is a member of a WLBS cluster with miawww01.

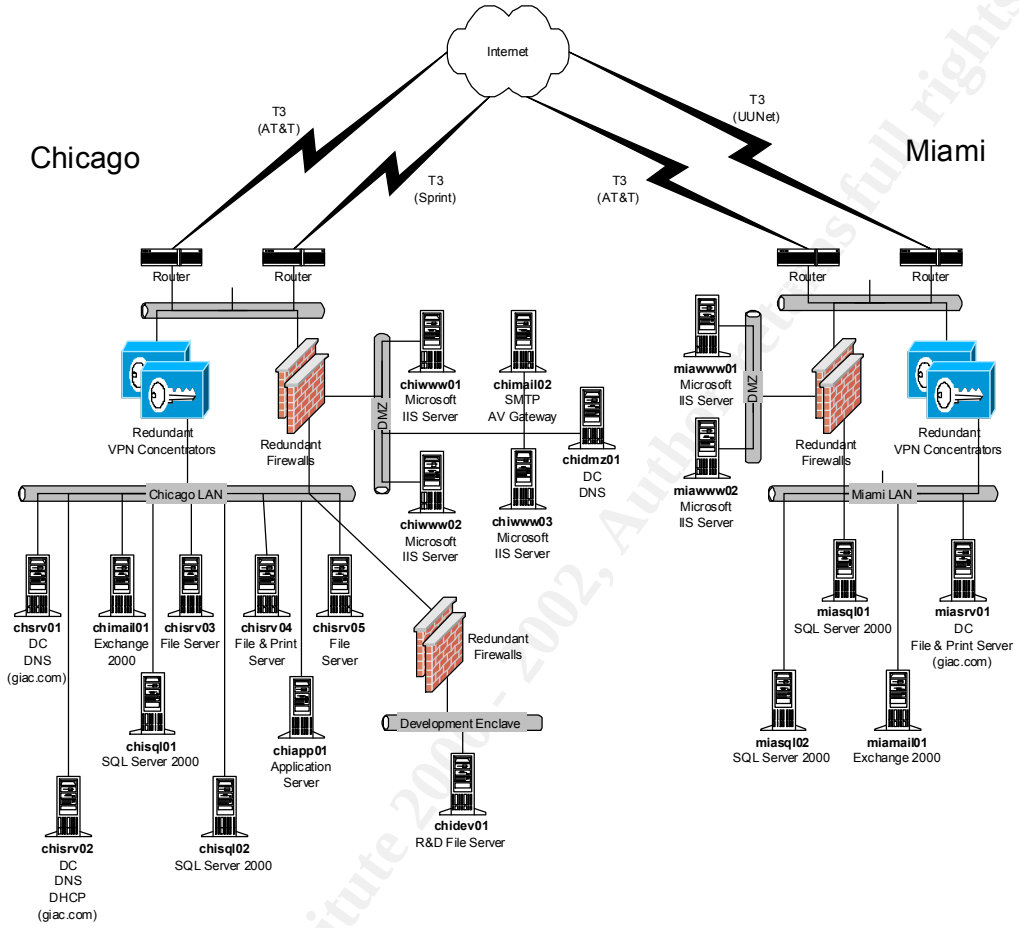

Figure 1 - GIAC Enterprises Physical Network Design

ACTIVE DIRECTORY DESIGN

The Active Directory design for GIAC Enterprises includes two domains, each in a forest, and several OUs within the domains. This two domain design was created to segregate the internal servers and users from the publicly available resources. The giac.com domain will be the main user domain and giac.net will include the publicly accessible servers. Each domain and OU will be discussed below.

The single domain model was chosen to simplify network management and security. This allows users to logon to the network from either site and maintain their OU specific security settings. Should all the domain controllers in a site become unavailable, users can authenticate to the domain controller in the other site.

Although there are two physical sites, there are redundant Internet connections of 45Mbps and VPN concentrators at each site. Microsoft recommends a minimum link speed of 9.6kbps for 20,000 users.[1] GIAC Enterprise's links far exceed this minimum for GIAC's 250 users; therefore the company can utilize a single primary domain.

Active Directory integrated DNS servers are utilized throughout the giac.com and giac.net domains. The domain namespaces of giac.com and giac.net are publicly registered on the Internet.

giac.com

All servers in the giac.com domain are placed into one of two OUs based on their role – Domain Controller or Server. The one exception being the Development OU server. This is because servers are shared by multiple departments. As the company grows, creating a Servers sub-OU for each OU department will be evaluated.

Each department has a distinct OU for its users and computers. This design was utilized to provide different levels of security to each department, to deploy software to individual departments via group policy and to delegate user management. For example, the users in the helpdesk OU can reset passwords for users in the sales, services, support and HR OUs. The remaining OUs require someone in the IS OU to reset passwords.

The default Domain Controllers OU will contain the domain controllers within the giac.com domain. This is where the domain-wide password and account settings are applied.

The Development OU contains the software developers. This department is the crown jewel of GIAC Enterprises and has modified security setting configured in the group policy. It is further segregated into a server OU and user OU.

The Finance OU contains the finance and accounting users. These users run the GIAC Enterprises software in production.

[1] "Best Practices Active Directory Design for Managing Networks"

Sales and marketing users at GIAC are placed into the Sales OU. These are mobile users who often work remotely. A Miami Users OU contains the users located in the Miami office. This is primarily for site specific settings that need to be applied.

The HR domain contains the human resources users.

The Services OU contains the professional services staff at GIAC. These are the individuals who assist GIAC Enterprises customers with the implementation and customization of the financial software. These users are mobile and often work remotely. They are considered power users and have a group policy that loosens some of the security restrictions. A Miami Users OU contains the users located in the Miami office. This is primarily for site specific settings that need to be applied.

The customer support staff at GIAC Enterprises is represented by the Support OU. This department provides customer tech support for GIAC Enterprises customers. They have a security settings that are more lenient that the company standard to allow them to troubleshoot customer's problems.

The IS OU contains the information services group at GIAC Enterprises. This department is responsible for the computers, networks and security at GIAC Enterprises. These users have a unique security policy and software requirements. The helpdesk staff is further segregated into a helpdesk OU.

giac.net

The second domain utilized by GIAC Enterprises is giac.net. This domain encompasses all Windows 2000 servers located on the DMZ networks off the firewalls in Chicago and Miami. OUs are utilized to further segregate the security of the machines based on the role of the server.

The default Domain Controllers OU will contain the domain controllers within the giac.net domain.

The Web Server OU contains all web servers. This allows the web server specific settings to be centrally applied to all servers.

The Intranet Servers OU is a child OU of the Web Servers OU. The creation of the sub-OU allows the web server settings to be inherited by these machines and allows specific settings necessary for the intranet servers is to be set by this OU's group policy.

The Mail Server OU contains the publicly accessible SMTP servers on the DMZ. The primary benefit of this OU is the ability of group policy to apply specific settings to the mail servers.

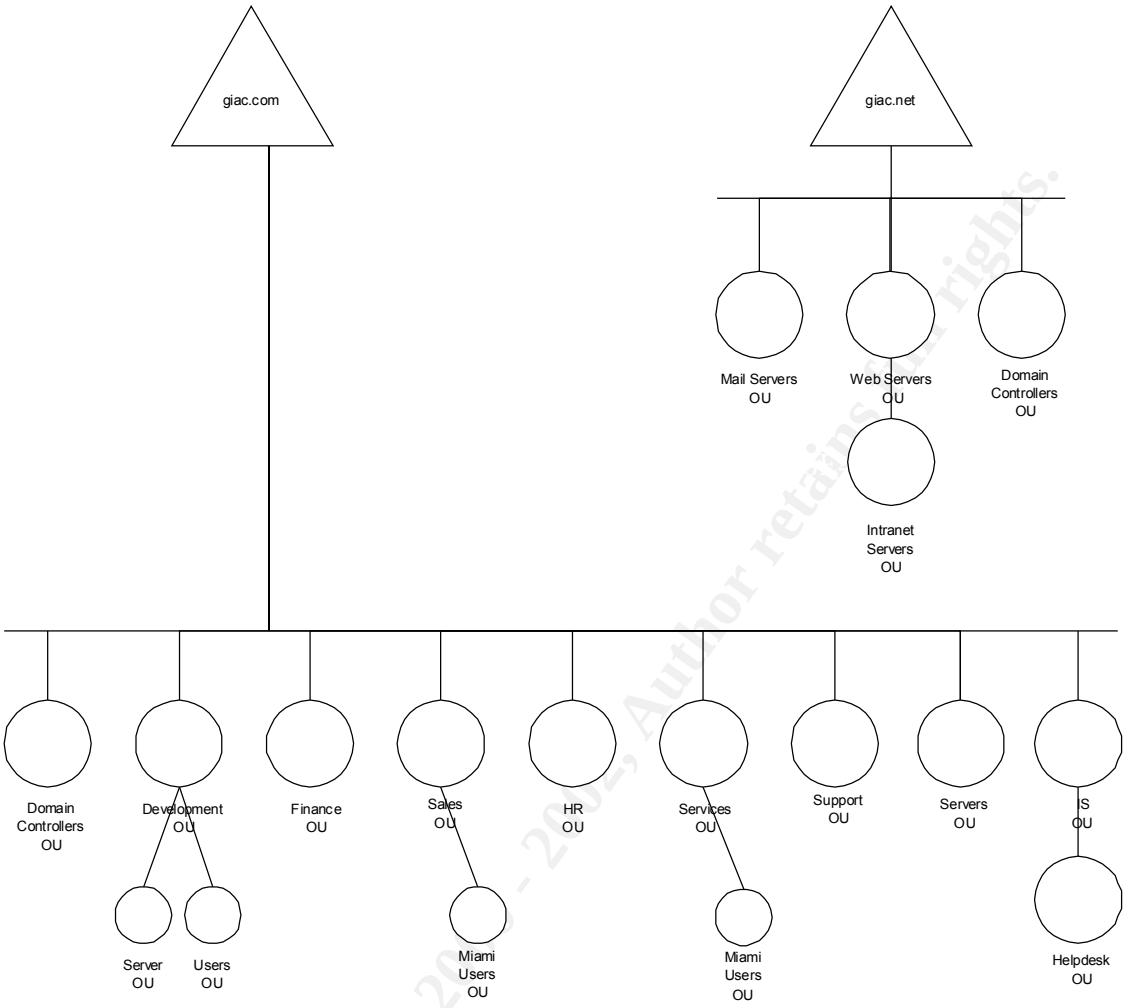

Figure 2 - GIAC Enterprises Active Directory Design

GROUP POLICY AND SECURITY

Group Policy is a key piece of Active Directory. With Group Policy, settings can be applied to all users and machines in a domain or to a very selected group of users or machines placed in an OU. The default installation of Active Directory includes two group policies which will be covered below. Each OU inherits the group policy of its parent domain and OUs (unless explicitly overridden).

Basic Group Policy

Each Active Directory domain contains a Default Domain Policy. This group policy is applied to all machines in the domain (unless explicitly overridden). The domain controllers in each domain have a Default Domain Controller Policy applied. Both of these default policies will be covered for each domain. Because of the inheritance of Group Policy settings, domain-wide settings can be made in the Default Domain Policy and only modifications or additional settings can be made at the OU level.

Default Domain Policy for giac.com

The Default Group Policy for giac.com will be applied to all users and computers within the domain. This policy is configured to set a general overall security level for all domain users and computers. Where necessary, individual OUs will be used to modify Group Policy settings. The Default Domain Policy will limit access to network settings, Internet Explorer security settings and Microsoft Netmeeting. A default IPSec policy, computer certificate auto enrollment and event log settings will also be defined. Non-default settings for the policy will be covered here.

Computer Configuration
- Windows Settings
  - Security Settings
    - Local Policies
      - Audit Policy
        - ***Audit Account Logon Events*** – Success, Failure
        - ***Audit Account Management*** – Success, Failure
        - ***Audit Logon Events*** – Success, Failure
        - ***Audit Object Access*** – Failure
        - ***Audit Policy Change*** – Success, Failure
        - ***Audit Privilege Use*** – Failure
        - ***Audit Process Tracking*** – Failure
        - ***Audit System Events*** – Success, Failure

          The audit policy settings are configured to allow third party log analysis tools to have sufficient data to analyze and correlate should an intrusion occur.

Security Options

Additional Restrictions for anonymous connections – *No Access without explicit anonymous permissions*

This setting is used to limit anonymous NetBIOS connections to the machine to enumerate SAM accounts and shares.

Message text for users attempting to log on – *Unauthorized access to GIAC Enterprises resources is prohibited. GIAC Enterprises reserves the right to monitor and log all communications and activities conducted on the GIAC Enterprises's computing resources.*

This setting provides a legal notice banner to users logging on to the domain.

Message title for users attempting to log on – *Unauthorized Access Prohibited*

This setting provides the title for the legal banner box.

Recovery Console: Allow automatic administrative logon – *Disabled*

Rename administrator account – *sysadmin*

This setting provides an additional layer of obscurity to unauthorized access to the administrator account. It is set to deter casual password guessing, not determined attacks.

Rename guest account – *giac_guest*

This setting provides an additional layer of obscurity to unauthorized access to the guest account. Although the guest account is disabled, this is an additional step in case it is accidentally reactivated. It is set to deter casual password guessing, not determined attacks.

Event Log

Settings for Event Logs

Maximum application log size - *16384 kilobytes*

Maximum security log size - *16384 kilobytes*

Maximum system log size - *16384 kilobytes*

Restrict guest access to application log - *Enabled*

Restrict guest access to security log - *Enabled*

Restrict guest access to system log - *Enabled*

Retention method for application log – *Do not overwrite events*

Retention method for security log - *Do not overwrite events*

Retention method for system log - *Do not overwrite events*

Shut down the computer when the security audit log is full - *Disabled*

The event log policy settings are configured to store a sufficient number of event log entries prior to the logs being copied off and backed up. Systems have sufficient

disk space, so the logs are allowed to grow and the workstation log backup routine is run less frequently.

Public Key Policies
Automatic Certificate Request Setting
Computer – *Obtain a computer certificate.*
IPSec – *Obtain a computer IPSec certificate to be used for computer identification.*
The public key policy is configured to auto-enroll computers with computer and IPSec certificates. This allows all computers to transparently utilize IPSec encryption and authentication for inter-machine communications.

IP Security Policies on Active Directory
Client (Respond Only) – *Applied*
This setting is configured as a default so that clients will respond to IPSec if requested by a server.

Administrative Templates
Windows Components
NetMeeting
Disable Remote Desktop Sharing – *Enabled*
Remote desktop sharing could allow remote access to a user's desktop. Therefore, this application is disabled.

System
Logon
Run Startup Scripts Visible – *Disabled*
Run Shutdown Scripts Visible – *Disabled*
By running scripts hidden, users do not have the ability to cancel them.

Network
Network and Dial-Up Connections
Prohibit configuration of connection sharing – *Enabled*
Connection sharing is a feature that is not necessary in this environment and is disabled.

User Configuration
Windows Settings
Internet Explorer Maintenance
Connection
Automatic Browser Configuration
Automatically detect configuration settings – *Disabled*

Browser settings are explicitly configured via group policy and this setting is disabled to prevent unexpected connection settings.

Proxy Settings

Enable Proxy Settings – *Enabled*

Address of Proxy – *gw.giac.com port 3128*

These settings define the HTTP proxy for all domain users in Chicago. Miami users will have a different proxy set via an OU Group Policy setting.

Administrative Templates

Windows Components

NetMeeting

Disable Whiteboard – *Enabled*

Disable Chat – *Enabled*

Disable Netmeeting 2.x Whiteboard – *Enabled*

Prevent Sending Files – *Enabled*

Prevent Receiving Files – *Enabled*

Prevent Automatic acceptance of calls – *Enabled*

These settings could allow files to be downloaded to the users' machines. Therefore, these are disabled as they are a potential security risk and are unnecessary.

Application Sharing

Disable Application Sharing – *Enabled*

Application offers potential remote access to users' machines, so it is disabled as a preventative measure.

Internet Explorer

Disable Internet Connection Wizard – *Enabled*

Disable Changing connection settings – *Enabled*

Disable Changing proxy settings – *Enabled*

Disable Changing Automatic Configuration settings – *Enabled*

Disable Changing Certificate settings – *Enabled*

Do not allow AutoComplete to save Passwords – *Enabled*

Internet Explorer configuration is to limit user's ability to modify settings. This results in enhanced security due to misconfiguration and fewer helpdesk calls.

Network

Network and Dial-Up Connections

Prohibit enabling/disabling a LAN connection - *Enabled*

Prohibit access to properties of a LAN connection - *Enabled*

Prohibit access to the Network Connection Wizard – *Enabled*

Prohibit connection of connection sharing - *Enabled*

Prohibit TCP/IP advanced configuration - *Enabled*

Users are prohibited from changing network connections and settings. This leads to fewer helpdesk calls due to user exploration.

Default Domain Controller Policy for giac.com

The Default Domain Controller Policy for giac.com will be applied to all domain controllers within the domain. General domain policy setting applied via the Default Domain Policy apply to all machines and are inherited by the domain controllers OU and only additional modified settings are applied. Only non-default settings for the policy will be covered here.

Computer Configuration

Windows Settings

Security Settings

Account Policies

Password Policies

Enforce Password History – *13 Passwords*

Maximum Password Age – *45 days*

Minimum Password Age – *5 days*

Password Must Meet Complexity Requirements – *Enabled*

Store Passwords Using Reversible Encryption – *Disabled*

These settings provide a password policy that requires complex passwords, expires passwords every 45 days and maintains 13 unique passwords.

Account Lockout Policy

Account Lockout Duration – *60 minutes*

Account Lockout Threshold – *5 Invalid Login Attempts*

Reset Account Lockout Counter after – *60 minutes*

The account lockout policy is set to lock the account after 5 failed attempts and maintain the lock for 60 minutes. The lockout counter resets after 60 minutes. This policy will thwart brute force password cracking attempts, but not require a helpdesk call to unlock accounts.

Local Policies

Audit Policy

Audit Directory Services Access – *Failure*

This setting will log failed directory access attempts which can by used by third party log analysis and intrusion detection tools to spot intrusion attempts.

Default Domain Policy for giac.net

The Default Group Policy for giac.net will primarily be utilized to lockdown the computers in the domain. Since the machines in the giac.net domain are publicly accessible machines, there are no user workstations and a very limited number of user accounts. Where necessary, individual OUs will be used to modify Group Policy settings, such as web servers. Non-default settings for the policy will be covered here.

Computer Configuration
Windows Settings
Scripts
Startup Scripts – startup-giac.net.vbs
This setting will run the startup-giac.net.vbs script at startup of the giac.net servers. This script sets registry settings outlined under additional security.
Security Settings
Local Policies
Audit Policy
Audit Account Logon Events – Success, Failure
Audit Account Management – Success, Failure
Audit Logon Events – Success, Failure
Audit Object Access – Failure
Audit Policy Change – Success, Failure
Audit Privilege Use – Failure
Audit Process Tracking – Failure
Audit System Events – Success, Failure
The audit policy settings are configured to allow third party log analysis tools to have sufficient data to analyze and correlate should an intrusion occur.
Event Log
Settings for Event Logs
Maximum application log size - *16384 kilobytes*
Maximum security log size - *16384 kilobytes*
Maximum system log size - *16384 kilobytes*
Restrict guest access to application log - *Enabled*
Restrict guest access to security log - *Enabled*
Restrict guest access to system log - *Enabled*
Retention method for application log – *Do not overwrite events*
Retention method for security log - *Do not overwrite events*
Retention method for system log - *Do not overwrite events*
Shut down the computer when the security audit log is full - *Disabled*
The event log policy settings are configured to store a sufficient number of event log entries prior to the logs being copied off and backed up. Since the systems have sufficient disk space, this prevents logs from being filled up and new log messages being missed. A routine is run to

manually copy off the Windows log files from the machines on a regular basis.

Local Policies

Security Options

Additional Restrictions for anonymous connections – *No Access without explicit anonymous permissions*

This setting is used to limit anonymous NetBIOS connections to the machine to enumerate SAM accounts and shares.

Message text for users attempting to log on – *Unauthorized access to GIAC Enterprises resources is prohibited. GIAC Enterprises reserves the right to monitor and log all communications and activities conducted on the GIAC Enterprises's computing resources.*

This setting provides a legal notice banner to users logging on to the domain.

Message title for users attempting to log on – *Unauthorized Access Prohibited*

This setting provides the title for the legal banner box.

Recovery Console: Allow automatic administrative logon – *Disabled*

This setting requires administrative user and password to access the recovery console.

Rename administrator account – *dmzadmin*

This setting provides an additional layer of obscurity to unauthorized access to the administrator account. It is set to deter casual password guessing, not determined attacks.

Rename guest account – *giacdmz_guest*

This setting provides an additional layer of obscurity to unauthorized access to the guest account. Although the guest account is disabled, this is an additional step in case it is accidentally reactivated. It is set to deter casual password guessing, not determined attacks.

Administrative Templates

Windows Components

NetMeeting

Disable Remote Desktop Sharing – *Enabled*

Remote desktop sharing could allow remote access to a user's desktop. Therefore, this application is disabled.

System

Logon

Run Startup Scripts Visible – *Disabled*

Run Shutdown Scripts Visible – *Disabled*

By running scripts hidden, users do not have the ability to cancel them.

Network
Network and Dial-Up Connections
Prohibit configuration of connection sharing – *Enabled*
Connection sharing is a feature that is not necessary in this environment and is disabled.

User Configuration
Windows Settings
Internet Explorer Maintenance
Connection
Automatic Browser Configuration
Automatically detect configuration settings – *Disabled*
Browser settings are explicitly configured via group policy and this setting is disabled to prevent unexpected connection settings.

Proxy Settings
Enable Proxy Settings – *Enabled*
Address of Proxy – *gw-dmz.giac.com port 3128*
These settings define the HTTP proxy for all machines in the domain.

Administrative Templates
Windows Components
NetMeeting
Disable Whiteboard – *Enabled*
Disable Chat – *Enabled*
Disable Netmeeting 2.x Whiteboard – *Enabled*
Prevent Sending Files – *Enabled*
Prevent Receiving Files – *Enabled*
Prevent Automatic acceptance of calls – *Enabled*
These settings could allow files to be downloaded to the users' machines. Therefore, these are disabled as they are a potential security risk and are unnecessary.

Application Sharing
Disable Application Sharing – *Enabled*
Application sharing is prohibited by GIAC Enterprises security policy.

Internet Explorer
Disable Internet Connection Wizard – *Enabled*
Disable Changing connection settings – *Enabled*

Disable Changing proxy settings – *Enabled*
Disable Changing Automatic Configuration settings – *Enabled*
Disable Changing Certificate settings – *Enabled*
Do not allow AutoComplete to save Passwords – *Enabled*

Internet Explorer configuration is to limit the user's ability to modify settings. This results in enhanced security due to reduced configuration errors and fewer helpdesk calls.

Network
Network and Dial-Up Connections
Prohibit enabling/disabling a LAN connection - *Enabled*
Prohibit access to properties of a LAN connection - *Enabled*
Prohibit access to the Network Connection Wizard – *Enabled*
Prohibit connection of connection sharing - *Enabled*
Prohibit TCP/IP advanced configuration - *Enabled*

Users are prohibited from changing network connections and settings. This leads to fewer helpdesk calls due to user exploration.

Default Domain Controller Policy for giac.net

The Default Domain Controller Policy for giac.net will be applied to all domain controllers within the domain. General domain policy setting applied via the Default Domain Policy apply to all machines and are inherited by the domain controllers OU and only additional modified settings are applied. Only non-default settings for the policy will be covered here.

Computer Configuration
Windows Settings
Security Settings
Account Policies
Password Policies
Enforce Password History – *24 Passwords*
Maximum Password Age – *30 days*
Minimum Password Age – *5 days*
Password Must Meet Complexity Requirements – *Enabled*
Store Passwords Using Reversible Encryption – *Disabled*

These settings provide a password policy that requires complex passwords, expires passwords every 30 days and maintains 24 unique passwords.

Account Lockout Policy
Account Lockout Duration – *120 minutes*
Account Lockout Threshold – *5 Invalid Login Attempts*
Reset Account Lockout Counter after – *120 minutes*

The account lockout policy is set to lock the account after 5 failed attempts and maintain the lock for 120 minutes. The

lockout counter resets after 120 minutes. This policy will thwart brute force password cracking attempts, but not require a helpdesk call to unlock accounts.

Local Policies
Audit Policy
Audit Directory Services Access – *Failure*
This setting will log failed directory access attempts which can by used by third party log analysis and intrusion detection tools to spot intrusion attempts.

Additional Group Policy

Group policy can be applied to individual OUs. These additional group policies are used to apply security settings that are different from the default policies.

Web Servers OU

Additionally in the Web Servers OU, group policy is used to control system services and apply additional file ACLs.

Additional group policy settings are applied to this OU. These settings are based on locking down servers that are available for public access.

Computer Configuration
Windows Settings
Security Settings
System Services
Alerter - *Disabled*, *Administrators – Full Control*
Clipbook Server - *Disabled*, *Administrators – Full Control*
Computer Browser - *Disabled*, *Administrators – Full Control*
DHCP Client - *Disabled*, *Administrators – Full Control*
Distributed File System - *Disabled*, *Administrators – Full Control*
Distributed Link Tracking Client - *Disabled*, *Administrators – Full Control*
License Logging Service - *Disabled*, *Administrators – Full Control*
Logical Disk Manager Administrative Services - *Disabled*, *Administrators – Full Control*
Messenger - *Disabled*, *Administrators – Full Control*
Network DDE - *Disabled, Administrators – Full Control*
Network DDE DSDM - *Disabled*, *Administrators – Full Control*
Print Spooler - *Disabled*, *Administrators – Full Control*
Remote Registry Service - *Disabled, Administrators – Full Control*
RunAS Service - *Disabled*, *Administrators – Full Control*
Task Scheduler - *Disabled*, *Administrators – Full Control*
TCP/IP NetBIOS Helper - *Disabled*, *Administrators – Full Control*

Telephony - *Disabled*, *Administrators – Full Control*
These services are unnecessary and are therefore disabled. [2]

File System

%systemdrive%\tools\arp.exe – *Administrator – Full Control*
%systemdrive%\sbin\at.exe – *Administrator – Full Control*
%systemdrive%\sbin\atsvc.exe – *Administrator – Full Control*
%systemdrive%\sbin\cacls.exe – *Administrator – Full Control*
%systemdrive%\sbin\cmd.exe – *Administrator – Full Control*
%systemdrive%\sbin\cscript.exe – *Administrator – Full Control*
%systemdrive%\sbin\debug.exe – *Administrator – Full Control*
%systemdrive%\sbin\edit.com – *Administrator – Full Control*
%systemdrive%\sbin\edlin.exe – *Administrator – Full Control*
%systemdrive%\sbin\finger.exe – *Administrator – Full Control*
%systemdrive%\sbin\ftp.exe – *Administrator – Full Control*
%systemdrive%\sbin\ipconfig.exe – *Administrator – Full Control*
%systemdrive%\sbin\nbtstat.exe – *Administrator – Full Control*
%systemdrive%\sbin\net.exe – *Administrator – Full Control*
%systemdrive%\sbin\netstat.exe – *Administrator – Full Control*
%systemdrive%\sbin\nslookup.exe – *Administrator – Full Control*
%systemdrive%\sbin\ping.exe – *Administrator – Full Control*
%systemdrive%\sbin\posix.exe – *Administrator – Full Control*
%systemdrive%\sbin\qbasic.exe – *Administrator – Full Control*
%systemdrive%\sbin\rcp.exe – *Administrator – Full Control*
%systemdrive%\sbin\rdisk.exe – *Administrator – Full Control*
%systemdrive%\sbin\regedit.exe – *Administrator – Full Control*
%systemdrive%\sbin\regedt32.exe – *Administrator – Full Control*
%systemdrive%\sbin\rexec.exe – *Administrator – Full Control*
%systemdrive%\sbin\route.exe – *Administrator – Full Control*
%systemdrive%\sbin\rsh.exe – *Administrator – Full Control*
%systemdrive%\sbin\runonce.exe – *Administrator – Full Control*
%systemdrive%\sbin\secfixup.exe – *Administrator – Full Control*
%systemdrive%\sbin\syskey.exe – *Administrator – Full Control*
%systemdrive%\sbin\telnet.exe – *Administrator – Full Control*
%systemdrive%\sbin\tracert.exe – *Administrator – Full Control*
%systemdrive%\sbin\wscript.exe – *Administrator – Full Control*
%systemdrive%\sbin\xcopy.exe – *Administrator – Full Control*
These system files can be exploited during an intrusion attempt, therefore they are moved to the %systemdrive%\sbin directory from the WINNT directory and NTFS access control lists (ACL) applied to limit access to administrators. [3]
d:\website\html_files – *Administrator – Full Control*

[2] Walker, p.8

[3] Dodds, et al.

System – Full Control
Authenticated Users - Read
Anonymous – Read

d:\website\image_files - *Administrator – Full Control*
System – Full Control
Authenticated Users - Read
Anonymous – Read

d:\website\asp_files - *Administrator – Full Control*
System – Full Control
Authenticated Users - Execute (special access)
Anonymous – Execute (special access)

d:\website\include_files – *Administrator – Full Control*
System – Full Control
Authenticated Users - Execute (special access)
Anonymous – Execute (special access)

These NTFS ACL permissions set the default security settings on the web site directories. The website is located on a distinct partition and the directories have been renamed to provide additional security. [4]

Development OU

The Development group is the major asset of GIAC Enterprises. Therefore, some additional security is implemented on their OU. Local security options are defined to further authenticate and secure communications to the server, control smart card behavior, and the action to take when the security log is full.

Computer Configuration
Windows Settings
Security Settings
Local Policies
Security Options

Clear virtual memory pagefile when system shuts down – *Enabled*
This setting clears the virtual pagefile at shutdown to prevent someone from potentially gaining data from the pagefile. [5]

Digitally sign client communications (always) – *Enabled*
This setting enables mutual authentication and message authentication for SMB traffic. This prevents a man-in-the-middle attacks and active message attacks. [5]

Digitally sign server communications (always) – *Enabled*

[4] Walker, p.13
[5] Dodds, et al

This setting enables mutual authentication and message authentication for SMB traffic. This prevents a man-in-the-middle attacks and active message attacks. [6]

Do not display last user name in logon screen – *Enabled*

This setting prevents someone from obtaining half of the username password combination by looking at the last username in the logon prompt. [6]

LAN Manager Authentication Level – *Send NTLMv2 response only\refuse LM & NTLM*

This setting forces workstations to use the stronger NTLMv2 authentication and session security and refuses the weaker LM & NTLM security. [6]

Secure Channel: Digitally encrypt or sign secure channel data (always) – *Enabled*

This setting digitally signs and encrypts communication with the domain controllers via the secure channel. [6]

Secure Channel: Require Strong (Windows 2000 or later) Session key – *Enabled*

This setting requires strong session keys for secure channel communications. [6]

Send Unencrypted Password to Connect to Third-Party SMB Servers – *Enabled*

This setting prevents the Windows password from being sent clear text to third party SMB server. [6]

Shut down immediately if unable to log security audits – *Enabled*

This setting forces the machine to shutdown if the security log is full. This prevents someone from covering up their tracks by overwriting the security event log. [6]

Smart card removal behavior – *Lock Workstation*

Since the development OU uses smart cards for logon, when the smart card is removed the workstation is locked. [6]

Unsigned driver installation behavior – *Do Not Allow Installation*

This setting requires that all drivers installed on the computers to be digitally signed. This prevents a Trojan from being installed with an unsigned driver. [6]

[6] Dodds, et al

Additional Security

Although Active Directory and Group Policy provide a very high level of security and control, there are some areas of security that require settings outside of Group Policy or additional products to fulfill. SYN flood attack protection and host intrusion detection are two areas that settings outside Group Policy are utilized.

SYN Flood Attack protection

Several registry settings are available to mitigate TCP SYN Flood attacks, modify default TCP/IP stack behavior and otherwise harden the stack on a Windows 2000 machine.[7] These registry settings are grouped into the startup-giac.net.vbs script (appendix A) and are applied to all machines in the giac.net domain at startup.

The first four registry settings apply to TCP SYN flood protection. The first setting controls the machines response to a SYN flood attack. The next three setting help define thresholds for a SYN attack.

A setting of 2 for this key is the best protection against a SYN attack. It slows down SYN-ACK responses and connection responses timeout quickly when under attack.
Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: Reg_DWORD
Value: SynAttackProtect = 2

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: Reg_DWORD
Value: TcpMaxHalfOpen = 100 (default)

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: Reg_DWORD
Value: TcpMaxHalfOpenedRetried = 80 (default)

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: Reg_DWORD
Value: TcpMaxPortsExhausted = 5 (default)

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: Reg_DWORD
Value: TcpMaxConnectResponseRetransmissions = 2

[7] Norberg, p. 67-71

This registry setting prevents machines from attempting to switch gateways if the default appears to be down.
Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: REG_DWORD
Value: *Enabled*eadGWDetect = 0

This setting changes the default TCP Keep-Alive timer from 2 hours to 5 minutes. This can clean-up dead TCP sessions quicker to free up resources. (pg 70)
Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: REG_DWORD
Value: KeepAliveTime = 300,000

IP source routing is disabled on all servers via the following registry key. This prevents attackers from specifying an alternate route for IP traffic.
Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\
Type: REG_DWORD
Value: DisableIPSourceRouting = 2

Host Intrusion Detection System

Host intrusion detection is one area where additional software is required to fulfill the requirements. At GIAC Enterprises, Cisco Host Intrusion Detection System (HIDS) is used to protect the servers from abnormal access. The Cisco HIDS software operates by placing a shim between the applications and the operating system. The software has a "signature" list that identifies abnormal system calls and accesses. Once the software is placed in protection mode, invalid system calls are blocked before they reach the OS and are logged.[8] The Web Server Edition is installed on all IIS servers and the Windows OS Edition is installed on all servers in the organization.

[8] "Cisco IDS Host Sensor Data Sheet".

REFERENCES

Norberg, Stefan; Securing Windows NT/2000 Servers for the Internet United States of America: O'Reilly & Associates, Inc., 2001

Walker, William E., IV; "Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0" (Version 1.3.1), March 4, 2002. URL: http://nsa1.www.conxion.com/win2k/guides/w2k-14.pdf

Cisco Systems. "Cisco IDS Host Sensor Data Sheet". December 19, 2001 URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/wdsi_ds.htm.

Dodds, Tom; Kerby, Warren; Howard, Michael; "Data Security and Data Availability for End Systems" 2000. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpent/sec3/datavail.asp

Microsoft Corporation. "Best Practices Active Directory Design for Managing Networks" 2001. URL: http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp?frame=true

APPENDIX A

startup-giac.net.vbs

```
'#####################################################
'# Filename: startup-giac.net.vbs
'#
'# Purpose: Startup script for giac.net domain
'#
'# Function: Set registry settings to harden IP stack
'#
'#####################################################

Set Sh = CreateObject("WScript.Shell")
key = "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\"
Sh.RegWrite key & "SynAttackProtect", 2, "REG_DWORD"
Sh.RegWrite key & "TcpMaxHalfOpen", 100, "REG_DWORD"
Sh.RegWrite key & "TcpMaxHalfOpenedRetried", 80, "REG_DWORD"
Sh.RegWrite key & "TcpMaxPortsExhausted", 5, "REG_DWORD"
Sh.RegWrite key & "TcpMaxConnectResponseRetransmissions", 2, "REG_DWORD"
Sh.RegWrite key & "KeepAliveTime", 300000, "REG_DWORD"
Sh.RegWrite key & "EnableDeadGWDetect", 0, "REG_DWORD"
Sh.RegWrite key & "DeadGWDetectDefault", 1, "REG_DWORD"

key = "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters\"
Sh.RegWrite key & "DisableIPSourceRouting", 2, "REG_DWORD"

'### End of Script
```