Securing a Windows 2000 Infrastructure

GIAC Enterprises

By
Mike Leeper

Securing Windows
GCWN Practical Assignment
Version 3.0 – Option 1

Introduction

The purpose of this paper is to discuss the design and implementation of a secure Windows 2000 network for GIAC Enterprises, a fictitious E-business that deals in the online sale of fortune cookie sayings.

Although outside parties, such as customers, vendors and partners are dealt with in daily activities, this discussion focuses primarily with securing the internal network used by GIAC employees.

This paper will include the following information:

1) **GIAC Enterprises network design and diagram.**

   This is a diagram showing the physical network of GIAC Enterprises. It will display the location and role of the key servers on the network, as well as any relevant information about the hardware and software configurations.

2) **Active Directory design and diagram.**

   This is a diagram showing the logical Active Directory structure of GIAC Enterprises. It includes all domains, Organizational Units, and trust relationships within this Windows 2000 network. It will also include an explanation of the roles and/or purpose of each of the key logical objects within the tree/forest.

3) **Group Policy and Security.**

   This is a definition of Group Policy security settings for GIAC Enterprises. These definitions will include an explanation of why Group Policy was applied, as it was to the domain and the unique policies applied to the domain controllers.

GIAC Enterprises Overview

GIAC Enterprises is a medium-sized company comprised of 1500 employees located in four geographic locations. The headquarters for GIAC Enterprises is located in Des Moines, Iowa with branch offices in New York, New York, Los Angeles, California, and Dallas, Texas. These branch offices are strategically located for sales and distribution purposes. The main location, Des Moines, houses all Finance, Customer Service, and Resource and Development personnel, as well as the main Human Resources and Information Services departments. The Sales and Distribution personnel are distributed evenly between the main office and each of the remote offices. Each of the branch offices houses 150 employees comprised from the Human Resources, Sales, and Distribution departments. Each of the remote sites also houses 2 Information Services/ Help Desk personnel to support desktop and onsite server problems. Global network support and design is handled from the Des Moines site.

Network Design

GIAC Enterprises is a moderately sized network consisting of an internal corporate network, a DMZ (demilitarized zone) housing the external web servers, and three remote office networks. The remote offices are connected to the home office via 512kb (fractional T1's). There are ISDN connection devices at each remote site for connection fault tolerance to the home office. These are enabled in the event the main fractional T1 connections are broken. This will provide minimal connectivity for the remote business units and provide connection for domain controller synchronization. GIAC Enterprises also has a full T1 connection to the Internet to support it's E-business and internal user activities. Again, there is an ISDN connection device to provide connection to the Internet Service Provider. This connection would be enabled in the event that the main T1 connection should fail. This provides minimal connectivity for external customers and provides fault tolerant connectivity for a main business function.

The internal networks, both remote and home office, operate on switched 100mb full duplex ethernet. The corporate server backbone is supported by switched gigabit full duplex ethernet. Wherever possible, networking and server components are configured for redundancy and fault tolerance. All network devices (firewalls, switches, routers) are kept at current versions of firmware and are configured with strong passwords whenever possible.

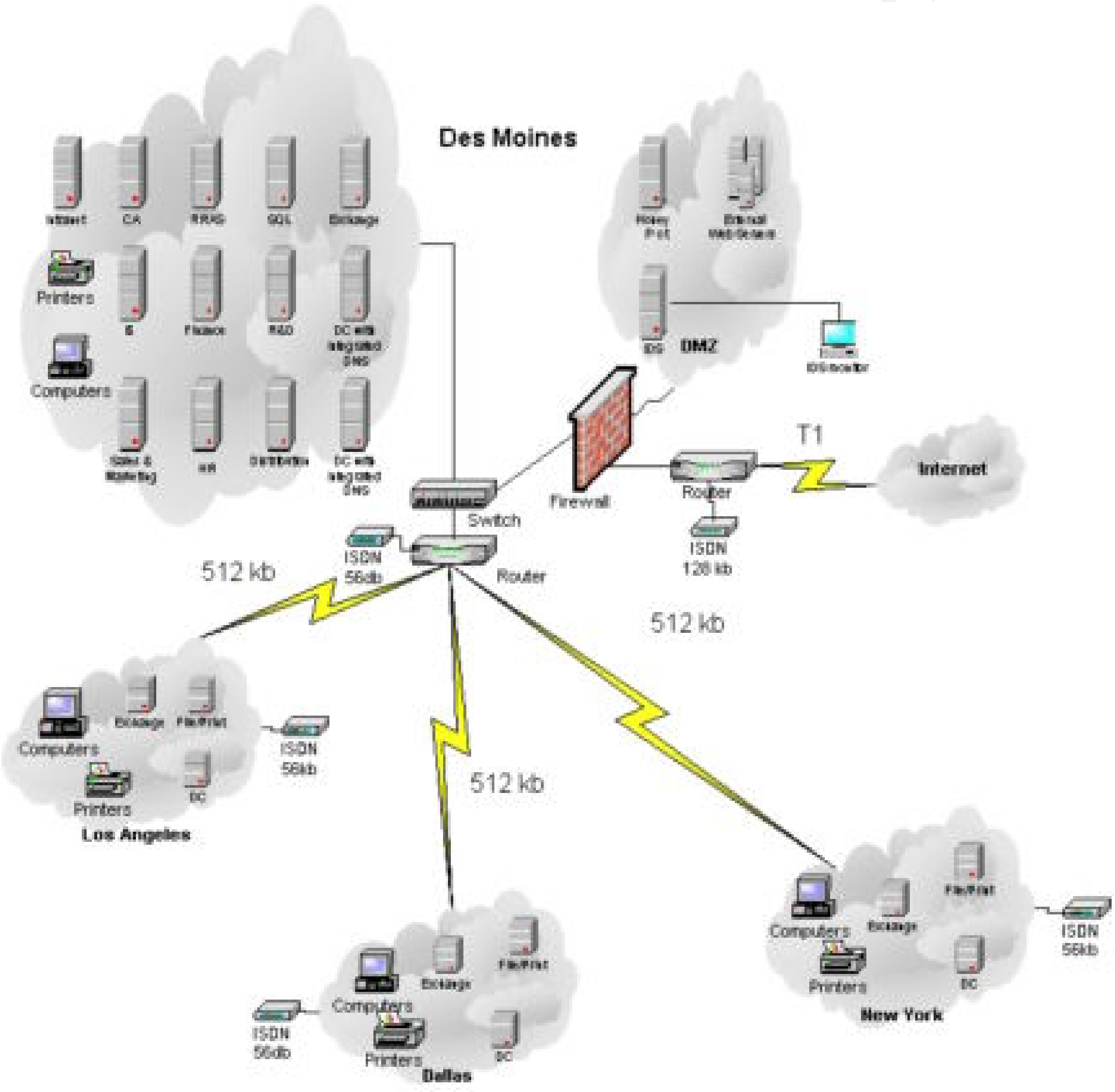
GIAC Enterprises' internal network is protected from Internet traffic by the use of an external firewall. This device allows Internet users to only connect to applications, via port 80, running on the external web servers. There is no direct communication allowed to, or from, the internal network. Very minimal communication is allowed via the firewall from the external web servers and the SQL server database on the internal network. All communications to the Internet are done via a proxy server.

All desktops, laptops, and servers on the GIAC Enterprise network are configured using Windows 2000 products. The desktops and laptops utilize Windows 2000 Professional and drives are configured with the NTFS file system. The HR and Research and Development areas utilize the Encrypted File System for added protection of sensitive data. These units are also configured with Smart Card readers, which is a requirement for authentication to the GIAC Enterprise network. All servers are configured with Windows 2000 Server with the exception of the external web servers. These servers are configured with Windows 2000 Advanced Server, which supports network load balancing and clustering. All servers are configured to use RAID 1 or RAID 5 or a combination of these RAID technologies. This provides adequate disk fault tolerance for data protection. Nightly backups are performed on all servers and the tapes are rotated on a scheduled basis. Tapes, which are encrypted and password protected, are stored in an offsite storage vault. All Windows 2000 computers are kept at the most current service packs (currently Service Pack 2) and the most current firmware via hardware manufacturer, as well as any applicable hotfixes. All systems are configured for high encryption level (128 bit). All servers are monitored for performance and hardware issues and problems. Server administrators are alerted when an error condition exists.

All desktops, laptops, and servers are configured and protected by the latest anti-virus software. Signature/definition files are kept current via the anti-virus vendors automatic update feature. Updates are checked several times a day and updates are automatically downloaded. The administrators are notified and updates are tested. If testing goes well, the updates are then allowed to flow out to all other servers, desktops, and laptops on the GIAC Enterprise network. Antivirus software is provided to GIAC Enterprise employees for their home systems to reduce the threat of infected files being brought into the company via diskette/CD. Administrators are notified of virus detection on the network

Critical systems, especially those that are more exposed to attack, such as the external web servers, are "hardened". Unnecessary services are removed, NTFS permissions are tightened on appropriate objects, and host-based packet filtering is employed where applicable.

Activity in the DMZ is highly monitored. The use of an Intruder Detection System and the deployment of a "honey pot" server help to alert administrators to any possible hacker activity. The "honey pot" server has Microsoft IIS installed but is left partially patched with all ports opened to draw attention of would be hackers. This server is highly audited for <u>any</u> activity.



GIAC Enterprises Network Diagram

Active Directory Design

Among the advantages of implementing Windows 2000 Active Directory on the GIAC Enterprise network, were the features and functionality it allows. It makes user administration, security policy administration, Exchange administration, and a host of other things much easier, efficient, and less time consuming for the GIAC system administrators. These features include:

•AD provides a single storage mechanism for all domain security policy and account information. This was important to the GIAC Enterprise system administrators, such that a centralized, manageable security policy and settings could be applied to the internal corporate network and the different remote sites.

•AD provides a hierarchical namespace for all user, group, and computer account information. This allows these entities to be grouped by Organizational Units (OUs). Business units can seamlessly share resources though separated by physical sites/networks.

•Administrator rights can be delegated to the level of OUs for creating and managing user, group, and computer account information. In addition, rights can be granted to individual properties of objects. System Administrators, located at each of the different sites are given rights to manage the users and systems that they are responsible for and not given excessive rights to the global network.

•AD's use of multi-master replication techniques allows domain controllers to act as peers. This allows updates to be made to any domain controller, not just the primary domain controller (PDC). This was very important for the network design of GIAC Enterprises and the criticality of their remote offices. Authentication traffic was not only greatly reduced but communication channels between domain controllers were made more secure through the use of stronger encryption methods. Since domain controllers are peers, only changes are replicated out to the other domain controllers.

•AD uses a new domain model that supports a hierarchical tree of domains. This simplifies trust management among domains because trust is automatic and transitive throughout the domain tree. Though GIAC Enterprises uses a single domain model, this was important to the GIAC system administrators as well. With the acquisition of new companies, the support of a hierarchical tree eases the creation/migration of this company into the existing tree/forest structure.

•The adoption of Internet standard security protocols, including Kerberos V5 and Transport Layer Security (TLS), improve authentication of users and computers.

•Credential mapping of public-key certificates to user accounts allows strong client authentication to PKI-enabled applications. Highly important with GIAC's issuance of Smart Card technology.

•Smart card support for interactive logon. Very important for GIAC Enterprise security requirements. Integrated Smart Card technologies help to ensure that only the intended user is access corporate resources.

•The inclusion of a certificate server that integrates the issuance of X.509 V3 certificates into the GIAC operating environment. Combined with AD, this provides a scalable and seamless foundation for GIAC Enterprises PKI structure.

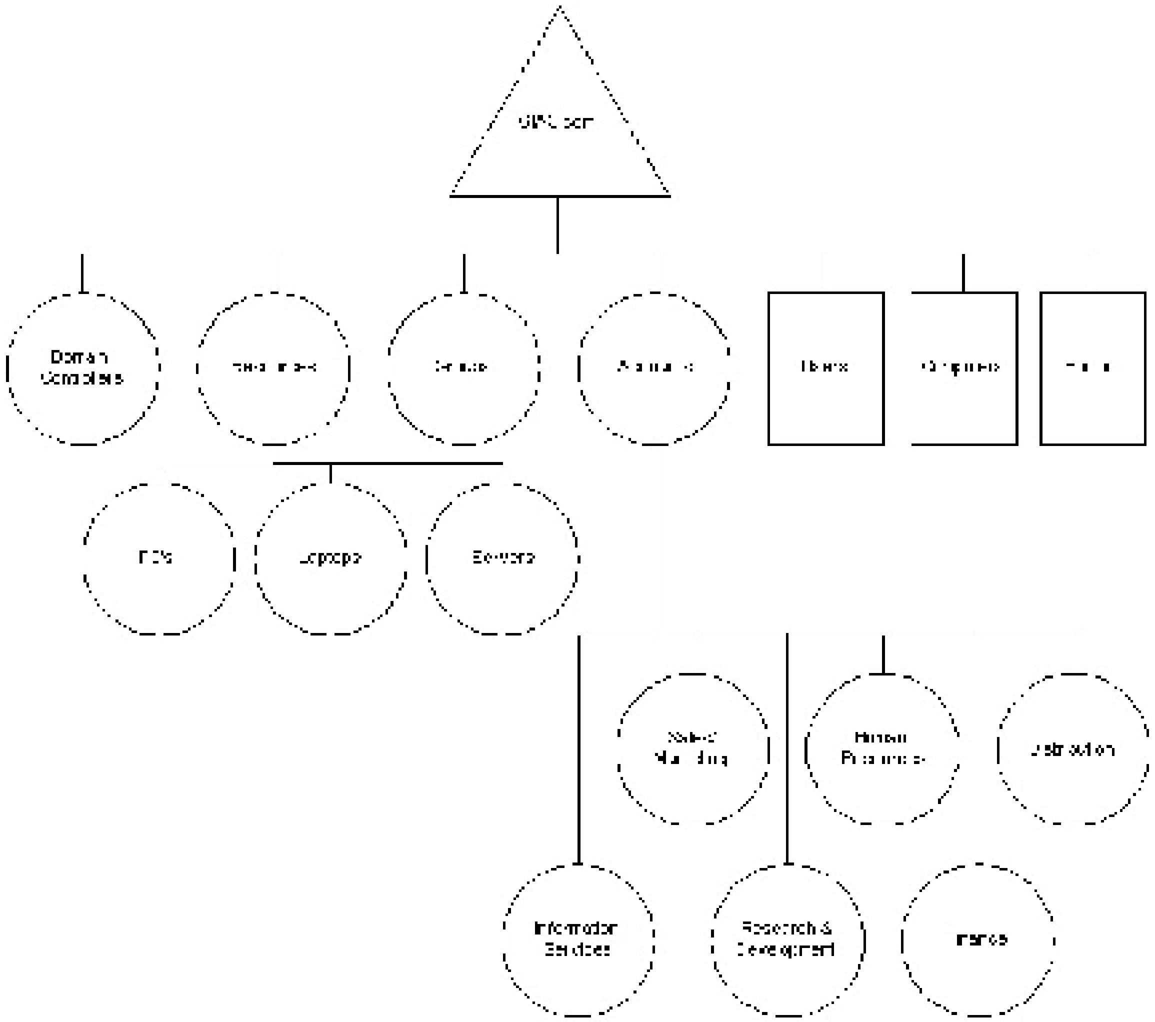
•Simplified administrative dialog boxes to manage the private- and public-key pairs and certificates.

•Integrated encryption technology. Simplifying the using encryption within GIAC Enterprises, both internally and externally.

•The inclusion of the encrypting file system (EFS) to support the transparent encryption and decryption of user files and folders. Greatly enhances GIAC Enterprise security by encrypting files or folders to prevent unauthorized access to said data. Used extensively on GIAC issued laptop computers and in the Human Resource and Research & Development areas.

•The inclusion of the Internet Protocol Security Protocol (IPSec). Integrating IPSec into AD greatly simplifies administering IPSec because AD provides centralized management of GIAC Enterprises network security policy.

•Virtual private network (VPN) solutions that are integrated into AD provide unified account access and management.



GIAC Enterprises Active Directory Structure

GIAC Enterprises Active Directory Overview

The domain design for GIAC Enterprises is a single domain, within a single forest for ease of administration.

Sites

GIAC Enterprises chose to create separate physical sites for the remote locations with less than optimum connectivity to the home office. Those sites, with 512 Kbps WAN links back to the home office, were created and are managed in separate physical sites. By creating separate physical sites and locating a domain controller, that function as a global catalog server and secondary DNS in those sites, users at those locations will experience minimal latencies in terms of authentication and in object searches.

Also the creation of these separate physical sites will allow support staff to control the times and amounts of replication traffic across these WAN connections. When you create a separate physical site the replication traffic that must occur is compressed. If domain controllers were placed at these locations and left in the default physical site, support staff would have minimal control over replication traffic and would not have the compression capabilities.

Organizational Units

Organizational Units enable administrators to structure network objects in a way that is logical and straightforward to administrators and users alike. (For instance, all objects can be structured in an OU hierarchy that mimics the organizational diagram.) This is the way GIAC Enterprises' Active Directory was structured. GIAC Enterprises chose to use the current container model, which separates business units into separate containers/Organizational Units. Since their technical support staff is familiar with this structure and business functions are well structured and well defined, this worked out well for GIAC Enterprise administration.

Organizational Units also provide a simple way for administrators to assign, to specific users and groups, the permissions to create and change attributes on the objects stored in one or more Organizational Units, and to assign differentiated rules or policies to network objects – based on their position in the OU hierarchy. Several Organizational Units were created to provide for separate GIAC Enterprise administrative functions and instrumented to protect data structures. Group Policies were created and are applied to these OUs to provide for each business units unique security needs. Each of the top level Organizational Units are administered by a different individual, or individuals, within Information Services. The OU structure was created to follow the unique responsibilities within the Information Services for the different business units. These Organizational Units provide inheritance of access rights, enabling GIAC Administrators to restrict to members of an OU the access to resources specific to their particular business unit.

This was particularly important for the protection of data within the Human Resources and Research & Development departments. These departments require the utmost control of who has access to data within these divisions. The Organizational Unit structure, group membership and security settings, make this possible.

Group Policy and Security

While not exclusively a security capability, Group Policy extends and takes advantage of the Active Directory service. Group Policy settings are contained in Group Policy Objects (GPOs), which are in turn associated with the Active Directory containers: sites, domains, and OUs. Group Policy allows you to uniformly enforce defined security policies throughout the corporate infrastructure by creating domain-level GPOs that define the most critical security-related settings. These settings will then be enforced on each and every computer in the domain.

GIAC Enterprises is an entirely Windows 2000 based network. No backward compatibility is needed. Servers and desktops are configured to use NTLMv2 response authentication level only. Eliminating the vulnerability to password cracker tools used by hackers. NTLMv2 adds additional security features:

- **Unique session keys per connection** – Captured session keys are made useless after a connection is completed.[1]
- **Session keys are protected by a key exchange** – Unless a key pair is obtained, a session key cannot be used.[1]
- **Unique keys are generated for the encryption of session data and its integrity** – The key used for encryption of data from the client to the server is different than the one used for encryption of data from the server to the client.[1]

[1] "Designing Microsoft Windows 2000 Network Security, Chapter 3 Designing Authentication for a Microsoft Windows 2000 Network", pg. 85, Microsoft Corporation, 2001.

Since the highest level of security is essential to GIAC Enterprises, these features are a requirement to stay ahead of the competition. To maintain the highest level of security on the internal network, GIAC Enterprises applied the High Security templates (Hisecdc.inf and Hisecws.inf) to all of its Windows 2000-based computers. Hisecws.inf security template was applied to all client computers and Hisecdc.inf is applied to all Windows 2000 servers, both Domain Controllers and file and print servers. The Hisecws.inf security template was first imported into a Group Policy Object and applied to the PC's and the Laptops Organizational Units containing computer accounts. The Hisecdc.inf security template was first imported into a Group Policy Object and applied to the Domain Controllers OU and the Servers OU containing only computer accounts. Since these security templates are computer configuration settings, there was no benefit to applying them to Organizational Units that contain no computers.

Since the servers located in the corporate DMZ are stand-alone servers (not part of the domain), the Hisecdc.inf security templates were applied and are maintained manually. A DMZ domain will be implemented if the number of servers within the DMZ grows and becomes harder to manage manually.

Because users authenticate to the network through the use of Smart Cards, security settings are left at higher standards in the Default Domain Policy. Normally, these higher settings would cause administrative overhead. By use of private/public keys, Smart Cards alleviate the administrative overhead and provide a much more secure authentication mechanism than "user name & passwords".

IIS

All of the servers running IIS 5.0 have the Hisecweb.inf security templates applied manually as well. These additional security settings harden the overall strength of the Web servers by setting Startup and Permissions on native System Services. This template disables services that are not needed and/or desirable on IIS 5.0 based web servers. Additional hardening of these Web servers was done by:

- Changing all of the default account names. This prevents hackers from attempting to connect to the Web servers using the default account names included with Windows 2000.

- Ensuring that the Web servers are not members of the same forest as the private network. All external Web servers are stand-alone servers to prevent Active Directory, on the private side, from becoming compromised.

• Separating available content into different folders by type. Security was then applied according to file type (i.e. Scripts, Exe's, Static Web Pages, etc.).

• Removing all sample applications from the Web server. All sample application files were removed which will prevent them from being used as a tool by hackers.

•Disabling unnecessary services. All unnecessary services were disabled either by the Hisecweb.inf security template or manually. This helps in the prevention of attacks.

• Configuring IPSec to block commonly attacked ports. This policy drops any connection attempts to ports listed in the IPSec filter.

• Enabling IIS logging. Logging is enabled on the external Web servers to help determine whether the servers have been or are under attack.

• Implementing Secure Socket Layer (SSL) protocol to protect secure areas of the Web servers. SSL encrypts all data being transferred between GIAC and it's customers.

• Disabling the use of parent paths. This prevents hackers from gaining access to data not normally considered accessible.

• All the external Web servers in GIAC's DMZ are configured to be part of an NLBS cluster. This not only offers a fault tolerant, load-balanced solution, it also helps in the prevention of attacks. If a server in the NLBS cluster is considered unavailable (perhaps because of an attack), incoming traffic is then redirected to the remaining servers in the cluster.

Through the use of security templates, the practice of the above hardening techniques, insertion of an un-patched Honey Pot server, the use of an Intruder Detection System, and the constant auditing/monitoring of the Web servers/DMZ, help to make the GIAC Enterprises Web infrastructure secure.

Default Domain Policy settings

Account Policies

- Password Policy

- **Enforce password history** –Determines the number of unique passwords that must be used before the user can reuse old passwords. (Default Domain Policy setting is 1)

- **Maximum password age —**Determines the number of days that a password can be used until it expires. A value of 0 specifies that passwords in your environment never expire. (Default Domain Policy setting is 42).

- **Minimum password age —**Determines the number of days that a password must be used until it can be changed. A value of 0 specifies that passwords can be changed immediately. (Default Domain Policy setting is 0).

- **Minimum password length —**Determines the lowest number of characters that users' passwords must contain. Since a value of 0 specifies that users aren't required to have passwords the default setting of 0 is changed to 8. (Default Domain Policy setting is 8).

- **Passwords must meet complexity requirements —** Determines whether to use a password filter (PASSFILG.DLL). This is a global requirement for user passwords to meet more stringent complexity requirements. (Default Domain Policy setting is set to ENABLED)

- **Store passwords using reversible encryption —**The Default Domain Policy setting is DISABLED. Not used by GIAC.

- **User must log on to change the password —** Determines whether users have to log on before they can change their passwords. When this policy is enabled, users have to logon before changing their passwords. When a user's password is expired, this creates an interesting predicament because the user can 't log on to change the password and an administrator has to reset it. Even though this is an administrative problem, this setting is left as DISABLED because of the use of Smart Cards for authentication. (Default Domain Policy setting is DISABLED).

-Account Lockout Policy

- **Account lockout threshold** —Determines how many failed logon attempts it takes to lock out a user's account. A value of 0 specifies that accounts never get locked out. This was a global requirement of all accounts network-wide. (Default Domain Policy is set to 5).

- **Account lockout duration** —Determines how long an account remains locked out before automatically being unlocked. A value of 0 specifies that an account remains locked out until an administrator unlocks it. This was a global requirement of all accounts network-wide. (Default Domain Policy is set to 0).

- **Reset account lockout counter after** —Determines how many minutes must pass before the failed logon count is reset to 0. If an account lockout threshold is defined, the value must be less than or equal to the account lockout duration. This was a global requirement of all accounts network-wide. (Default Domain Policy is set to 30).

-Kerberos Policy

These default settings were defined for the first domain controller in the domain during installation and are considered more than secure, they are left as global default for the GIAC domain.

- **Enforce user logon restrictions** —Determines whether validation of a session ticket occurs against the user rights policy of the target computer. This is to be left ENABLED in all environments. (Default Domain Policy is set to ENABLED).

- **Maximum lifetime for service ticket** —Determines the number of minutes that a session ticket can be used to access a service. The value must be greater than 10 and less than or equal to the Maximum Lifetime for a User Ticket setting. (Default Domain Policy is set to 60).

- **Maximum lifetime for user ticket** —Determines the number of hours that a user's ticket-granting ticket can be used. (Default Domain Policy is set to 10).

• **Maximum lifetime for user ticket renewal** —Determines the number of days that a ticket-granting ticket can be renewed for. (Default Domain Policy is set to 7).

• **Maximum tolerance for computer clock synchronization**—Determines the maximum clock skew in minutes that Kerberos allows to function properly. (Default Domain Policy is set to 5).

Local Policies

-Security Options

The only domain level settings under Security Options are:

• **Automatically log off user when logon time expires (local)**—Determines whether to automatically log off users when their logon time for local connections expires. This setting is set to ENABLED globally because it applies to both workstations and servers. (Default Domain Controller Policy is set to ENABLED).

• **Message text for users attempting to log on-** Set to "This system is the property of GIAC Enterprises and is for authorized use only. Unauthorized use is a violation of federal law. All data, software, transactions, and electronic communications are subject to monitoring."

• **Message title for users attempting to logon** —Set to "Legal Notice"

Default Domain Controller Policy settings

These are the settings that are uniquely applied to the Domain Controllers within the Domain Controllers OU. These are setting that are not being applied from the Default Domain Policy or default settings. All client and server communication settings are set to be digitally signed and encrypted to ensure authenticity.

Local Policies

Audit Policy

Since all Domain Controllers are audited the same, these settings are configured as global policies for all Domain Controllers.

• **Audit account logon events** —Determines whether to audit the logon and logoff events of another computer on which the local computer is used to validate the account. (Default Domain Controller Policy is set to "Success" and "Failure").

• **Audit account management** —Determines whether to audit all account-management operations on a computer. (Default Domain Controller Policy is set to "Success" and "Failure").

• **Audit directory service access** —Determines whether to audit user access of an AD object that has an SACL defined on it. (Default Domain Controller Policy is set to "Success" and "Failure").

•**Audit logon events** —Determines whether to audit every logon, logoff, and network connection event on a computer. (Default Domain Controller Policy is set to "Success" and "Failure").

• **Audit object access** —Determines whether to audit every object access that has an SACL defined on it. (Default Domain Controller Policy is set to "Success" and "Failure").

• **Audit policy change** —Determines whether to audit every change of policy, including user rights assignment policies, audit policies, and trust policies. (Default Domain Controller Policy is set to "Success" and "Failure").

• **Audit privilege use** —Determines whether to audit the use of a user right. (Default Domain Controller Policy is set to "Success" and "Failure").

• **Audit process tracking** —Determines whether to audit tracking information for application processes. (Default Domain Controller Policy is set to "No Auditing"). This setting is left alone because of the huge amount of information that is generated and is mostly useless from a security perspective.

•**Audit system events** —Determines whether to audit events that might affect the system's security or its security log. (Default Domain Controller Policy is set to "Success" and "Failure").

-Security Options

Almost all of these settings are set by importing the Hisecdc.inf security template into the Default Domain Controller GPO and apply to all Domain Controllers.

• **Additional restrictions for anonymous connections** — Determines what, if any, additional restrictions should be placed on anonymous connections. Helps to ensure that only authenticated access is allowed on the network. (Default Domain Controller Policy is set to "No Access without Explicit Anonymous Permissions").

• **Allow server operators to schedule tasks (domain controllers only)**—Determines whether server operators can schedule AT jobs. (Default Domain Controller Policy is set to DISABLED).

• **Allow system to be shut down without having to log on** — Determines whether computers can be shut down from the Windows Logon dialog box. (Default Domain Controller Policy is set to DISABLED).

• **Allowed to eject removable NTFS media** —Determines which users are allowed to eject removable NT file system (NTFS) media. (Default Domain Controller Policy is set to "Administrators").

• **Amount of idle time required before disconnecting a session** —A value between 0 and 0xFFFFFFFF that determines the amount of idle time before an SMB session is disconnected because of inactivity. (Default Domain Controller Policy is set to 15 Minutes).

•**Audit the access of global system objects** —Determines whether global system objects with SACLs defined are audited. (Default Domain Controller Policy is set to DISABLED).

• **Audit use of Backup and Restore privilege** —Determines whether to audit every use of the backup and restore privileges. (Default Domain Controller Policy is set to DISABLED).

• **Automatically log off users when logon time expires** —Determines whether to log off users automatically when their logon time for SMB connections expires. (Default Domain Controller Policy is set to ENABLED).

• **Automatically log off user when logon time expires (local)**—Determines whether to automatically log off users when their logon time for local connections expires. (Default Domain Controller Policy is set to ENABLED).

• **Clear virtual memory pagefile when system shuts down** —Determines whether to automatically clear the pagefile when the system shuts down. (Default Domain Controller Policy is set to ENABLED).

• **Digitally sign client communications (always)**—Determines whether SMB client communications are always digitally signed. (Default Domain Controller Policy is set to ENABLED).

• **Digitally sign client communications (when possible)**—Determines whether SMB client communications are digitally signed when possible. (Default Domain Controller Policy is set to ENABLED).

• **Digitally sign server communications (always)**—Determines whether SMB server communications are always digitally signed. (Default Domain Controller Policy is set to ENABLED).

• **Digitally sign server communications (when possible)**—Determines whether SMB server communications are digitally signed when possible. (Default Domain Controller Policy is set to ENABLED).

• **Disable CTRL+ALT+DEL requirement for logon** —Determines whether the CRTL+ALT+DEL key combination is required before a user logs on. (Default Domain Controller Policy is set to DISABLED).

•**Do not display last user name in logon screen** —Determines whether the name of the last successfully logged-on user is displayed in the Windows Logon dialog box. If the policy is enabled, the last user name isn't displayed. (Default Domain Controller Policy is set to ENABLED).

•**LAN Manager Authentication Level** —Determines which versions of the LAN Manager authentication protocol are accepted. (Default Domain Controller Policy is set to "Send NTLMv2 Response Only / Refuse LM & NTLM"). Since GIAC is an entirely Windows 2000 environment, this make for much more secure authentication.

• **Number of previous logons to cache (in case domain controller is not available)**—Determines how many cached successful logons the computer keeps in case a domain controller isn't available. I recommend setting this value to between 3 and (Default Domain Controller Policy is set to 10).

• **Prevent system maintenance of computer account password** —Determines whether a computer account password is updated every week. If this policy is enabled, the password isn't updated. (Default Domain Controller Policy is set to DISABLED).

• **Prevent users from installing printer drivers** —Determines whether regular users can install print drivers. If enabled, this policy prevents users from installing print drivers. (Default Domain Controller Policy is set to ENABLED).

•**Prompt user to change password before expiration** —Determines how far in advance users should be advised that their password is about to expire. (Default Domain Controller Policy is set to 14 days).

• **Recovery console: Allow automatic administrative logon; Recovery console: Allow floppy copy and access to all drives and all folders** —Determine how easy it is to gain access to a system and its drives and folders from the Win2K recovery console. (Default Domain Controller Policy is set to DISABLED on both).

• **Rename administrator account; Rename guest account** —Determine whether the administrator and/or guest account is renamed. (Default Domain Controller Policy is set to ENABLED). This ensures that the default Administrator and Guest account names are no longer public knowledge.

• **Restrict CD-ROM access to locally logged-on user; Restrict floppy access to locally logged-on user** —Determine whether CD-ROM and/or floppy devices are accessible to only the locally logged-on user. If enabled, these policies allow access to the specified devices only by the locally logged-on user. Even when enabled, if there isn't an interactive user, the media is accessible over the network. (Default Domain Controller Policy is set to ENABLED).

• **Secure channel: Digitally encrypt or sign secure channel data (always)**—Determines whether secure channel communications are always digitally signed or encrypted (but not necessarily both). (Default Domain Controller Policy is set to ENABLED).

• **Secure channel: Digitally encrypt secure channel data (when possible)**—Determines whether secure channel communications are encrypted when possible. (Default Domain Controller Policy is set to ENABLED).

• **Secure channel: Digitally sign secure channel data (when possible)**—Determines whether secure channel communications are digitally signed when possible. (Default Domain Controller Policy is set to ENABLED).

• **Secure channel: Require strong (Windows 2000 or later) session key** —Determines whether all secure channel communications require strong session key encryption. (Default Domain Controller Policy is set to ENABLED). Since GIAC is an entirely Windows 2000 environment, this is enabled to enhance security.

• **Send unencrypted password to connect to third-party SMB servers** —Determines whether clear-text passwords can be sent to third-party SMB servers that don 't support password encryption during authentication. If this policy is enabled, clear-text passwords are allowed. (Default Domain Controller Policy is set to DISABLED).
• **Shut down system immediately if unable to log security audits** —Determines whether the system should shut down if security events cannot be logged. If enabled, this policy causes the system to stop whenever a security event cannot be logged. (Default Domain Controller Policy is set to DISABLED).

• **Smart card removal behavior** —Determines what should occur when a smart card is removed from the system. (Default Domain Controller Policy is set to "Force Logoff").

- **Strengthen default permissions of global system objects (such as Symbolic links)**—Determines the strength of the default ACLs for global system objects. If enabled, this policy modifies the default access to prevent non-administrator users from modifying objects that they didn't create. (Default Domain Controller Policy is set to ENABLED).

- **Unsigned driver installation behavior** —Determines what should happen when a device driver that isn't digitally signed is installed on the computer. (Default Domain Controller Policy is set to "Do Not Allow Installation").

- **Unsigned non-driver installation behavior** —Determines what should happen when a non-device driver that isn't digitally signed is installed on the computer. (Default Domain Controller Policy is set to "Silently Succeed").

Event Log

Settings for Event Logs

Almost all of these settings are set by importing the Hisecdc.inf security template into the Default Domain Controller GPO and apply to all Domain Controllers

- **Maximum application log size; Maximum security log size; Maximum system log size** —Determine the size in kilobytes (Kb) of the event logs. (Default Domain Controller Policy is set to: 512kb for Application and System logs; 10240 kb for Security log).

- **Restrict guest access to application log: Restrict guest access to security log; Restrict guest access to system log** —Determine whether guest access is allowed to the logs. If these policies are enabled, guests cannot access the logs. (Default Domain Controller Policy is set to ENABLED for each log type).

- **Retention method for application log; Retention method for security log; Retention method for system log** —Determine the wrapping mechanism for each of the specified audit logs. (Default Domain Controller Policy is set to "Overwrite Events As Needed).

- **Shut down the computer when the security audit log is full** —Superseded by Shut Down System Immediately if Unable to Log Security Audits and shouldn't be used. (Default Domain Controller Policy is set to DISABLED).

Default Member Server Policy settings

These are the settings that are uniquely applied to the member servers within the Servers OU. These are setting that are not being applied from the Default Domain Policy or default settings. Almost all of these settings are set by importing the Hisecdc.inf security template into the Default Member Server GPO and apply to all servers. All client and server communication settings are set to be digitally signed and encrypted to ensure authenticity.

Local Policies

Audit Policy

- **Audit account logon events** —Determines whether to audit the logon and logoff events of another computer on which the local computer is used to validate the account. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit account management** —Determines whether to audit all account-management operations on a computer. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit directory service access** —Determines whether to audit user access of an AD object that has an SACL defined on it. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit logon events** —Determines whether to audit every logon, logoff, and network connection event on a computer. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit object access** —Determines whether to audit every object access that has an SACL defined on it. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit policy change** —Determines whether to audit every change of policy, including user rights assignment policies, audit policies, and trust policies. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit privilege use** —Determines whether to audit the use of a user right. (Default Member Server Policy is set to "Success" and "Failure").

- **Audit process tracking** —Determines whether to audit tracking information for application processes. (Default Member Server Policy is set to "No Auditing"). This setting is left alone because of the huge amount of information that is generated and is mostly useless from a security perspective.

- **Audit system events** —Determines whether to audit events that might affect the system's security or its security log. (Default Member Server Policy is set to "Success" and "Failure").

-Security Options

- **Additional restrictions for anonymous connections** —Determines what, if any, additional restrictions should be placed on anonymous connections. Helps to ensure that only authenticated access is allowed on the server. (Default Member Server Policy is set to "No Access without Explicit Anonymous Permissions").

- **Allow system to be shut down without having to log on** —Determines whether computers can be shut down from the Windows Logon dialog box. (Default Member Server Policy is set to DISABLED).

- **Allowed to eject removable NTFS media** —Determines which users are allowed to eject removable NT file system (NTFS) media. (Default Member Server Policy is set to "Administrators").
- **Amount of idle time required before disconnecting a session** —A value between 0 and 0xFFFFFFFF that determines the amount of idle time before an SMB session is disconnected because of inactivity. (Default Member Server Policy is set to 15 Minutes).

- **Audit the access of global system objects** —Determines whether global system objects with SACLs defined are audited. (Default Member Server Policy is set to DISABLED).

• **Audit use of Backup and Restore privilege** —Determines whether to audit every use of the backup and restore privileges. (Default Member Server Policy is set to DISABLED).

• **Automatically log off users when logon time expires** — Determines whether to log off users automatically when their logon time for SMB connections expires. (Default Member Server Policy is set to ENABLED).

• **Automatically log off user when logon time expires (local)**—Determines whether to automatically log off users when their logon time for local connections expires. (Default Member Server Policy is set to ENABLED).

• **Clear virtual memory pagefile when system shuts down** —Determines whether to automatically clear the pagefile when the system shuts down. (Default Member Server Policy is set to ENABLED).

• **Digitally sign client communications (always)**—Determines whether SMB client communications are always digitally signed. (Default Member Server Policy is set to ENABLED).

• **Digitally sign client communications (when possible)**— Determines whether SMB client communications are digitally signed when possible. (Default Member Server Policy is set to ENABLED).

• **Digitally sign server communications (always)**— Determines whether SMB server communications are always digitally signed. (Default Member Server Policy is set to ENABLED).

• **Digitally sign server communications (when possible)**— Determines whether SMB server communications are digitally signed when possible. (Default Member Server Policy is set to ENABLED).

• **Disable CTRL+ALT+DEL requirement for logon** — Determines whether the CRTL+ALT+DEL key combination is required before a user logs on. (Default Member Server Policy is set to DISABLED).

•**Do not display last user name in logon screen** —Determines whether the name of the last successfully logged-on user is displayed in the Windows Logon dialog box. If the policy is enabled, the last user name isn't displayed. (Default Member Server Policy is set to ENABLED).

•**LAN Manager Authentication Level** —Determines which versions of the LAN Manager authentication protocol are accepted. (Default Member Server Policy is set to "Send NTLMv2 Response Only / Refuse LM & NTLM"). Since GIAC is an entirely Windows 2000 environment, this make for much more secure authentication.

• **Number of previous logons to cache (in case domain controller is not available)**—Determines how many cached successful logons the computer keeps in case a domain controller isn't available. (Default Member Server Policy is set to 10).

• **Prevent system maintenance of computer account password** —Determines whether a computer account password is updated every week. If this policy is enabled, the password isn't updated. (Default Member Server Policy is set to DISABLED).

• **Prevent users from installing printer drivers** —Determines whether regular users can install print drivers. If enabled, this policy prevents users from installing print drivers. This helps to prevent installation of drivers that may contain security holes. (Default Member Server Policy is set to ENABLED).

•**Prompt user to change password before expiration** —Determines how far in advance users should be advised that their password is about to expire. (Default Member Server Policy is set to 14 days).

• **Recovery console: Allow automatic administrative logon; Recovery console: Allow floppy copy and access to all drives and all folders** —Determine how easy it is to gain access to a system and its drives and folders from the Win2K recovery console. (Default Member Server Policy is set to DISABLED on both).

• **Rename administrator account; Rename guest account** —Determine whether the administrator and/or guest account is renamed. (Default Member Server Policy is set to ENABLED). This ensures that the default Administrator and Guest account names are no longer public knowledge.

- **Restrict CD-ROM access to locally logged-on user; Restrict floppy access to locally logged-on user** —Determine whether CD-ROM and/or floppy devices are accessible to only the locally logged-on user. If enabled, these policies allow access to the specified devices only by the locally logged-on user. Even when enabled, if there isn't an interactive user, the media is accessible over the network. (Default Member Server Policy is set to ENABLED).

- **Secure channel: Digitally encrypt or sign secure channel data (always)**—Determines whether secure channel communications are always digitally signed or encrypted (but not necessarily both). (Default Member Server Policy is set to ENABLED).

- **Secure channel: Digitally encrypt secure channel data (when possible)**—Determines whether secure channel communications are encrypted when possible. (Default Member Server Policy is set to ENABLED).

- **Secure channel: Digitally sign secure channel data (when possible)**—Determines whether secure channel communications are digitally signed when possible. (Default Member Server Policy is set to ENABLED).

- **Secure channel: Require strong (Windows 2000 or later) session key** —Determines whether all secure channel communications require strong session key encryption. (Default Member Server Policy is set to ENABLED). Since GIAC is an entirely Windows 2000 environment, this is enabled to enhance security.

- **Send unencrypted password to connect to third-party SMB servers** —Determines whether clear-text passwords can be sent to third-party SMB servers that don 't support password encryption during authentication. If this policy is enabled, clear-text passwords are allowed. (Default Member Server Policy is set to DISABLED).

- **Shut down system immediately if unable to log security audits** —Determines whether the system should shut down if security events cannot be logged. If enabled, this policy causes the system to stop whenever a security event cannot be logged. (Default Member Server Policy is set to DISABLED).

- **Smart card removal behavior** —Determines what should occur when a smart card is removed from the system. (Default Member Server Policy is set to "Force Logoff").

- **Strengthen default permissions of global system objects (such as Symbolic links)**—Determines the strength of the default ACLs for global system objects. If enabled, this policy modifies the default access to prevent non-administrator users from modifying objects that they didn't create. (Default Member Server Policy is set to ENABLED).

- **Unsigned driver installation behavior** —Determines what should happen when a device driver that isn't digitally signed is installed on the computer. This helps to prevent installation of drivers that may contain security holes. (Default Member Server Policy is set to "Do Not Allow Installation").

- **Unsigned non-driver installation behavior** —Determines what should happen when a non-device driver that isn't digitally signed is installed on the computer. (Default Member Server Policy is set to "Silently Succeed").

Event Log Settings

- **Maximum application log size; Maximum security log size; Maximum system log size** —Determine the size in kilobytes (Kb) of the event logs. (Default Member Server Policy is set to: 512kb for Application and System logs; 10240 kb for Security log).

- **Restrict guest access to application log: Restrict guest access to security log; Restrict guest access to system log** —Determine whether guest access is allowed to the logs. If these policies are enabled, guests cannot access the logs. (Default Member Server Policy is set to ENABLED for each log type).

- **Retention method for application log; Retention method for security log; Retention method for system log** — Determine the wrapping mechanism for each of the specified audit logs. (Default Member Server Policy is set to "Overwrite Events As Needed).

- **Shut down the computer when the security audit log is full** —Superseded by Shut Down System Immediately if Unable to Log Security Audits and shouldn't be used. (Default Member Server Policy is set to DISABLED).

Default Workstation Policy settings

These are the settings that are uniquely applied to the workstations and laptops within the PCs OU and the Laptops OU. These are setting that are not being applied from the Default Domain Policy or default settings. Most of these settings are imported from the Hisecws.inf security template into the Default Workstation GPO. All client and server communication settings are set to be digitally signed and encrypted to ensure authenticity.

Local Policies

Audit Policy

- **Audit account logon events** —Determines whether to audit the logon and logoff events of another computer on which the local computer is used to validate the account. (Default Workstation Policy is set to "Success" and "Failure").

- **Audit account management** —Determines whether to audit all account-management operations on a computer. (Default Workstation Policy is set to "Success" and "Failure").

- **Audit directory service access** —Determines whether to audit user access of an AD object that has an SACL defined on it. (Default Workstation Policy is set to "No Auditing").

- **Audit logon events** —Determines whether to audit every logon, logoff, and network connection event on a computer. (Default Workstation Policy is set to "Success" and "Failure").

- **Audit object access** —Determines whether to audit every object access that has an SACL defined on it. (Default Workstation Policy is set to "Success" and "Failure").

- **Audit policy change** —Determines whether to audit every change of policy, including user rights assignment policies, audit policies, and trust policies. (Default Workstation Policy is set to "Success" and "Failure").

- **Audit privilege use** —Determines whether to audit the use of a user right. (Default Workstation Policy is set to "Success" and "Failure").

- **Audit process tracking** —Determines whether to audit tracking information for application processes. (Default Workstation Policy is set to "No Auditing"). This setting is left alone because of the huge amount of information that is generated and is mostly useless from a security perspective.

- **Audit system events** —Determines whether to audit events that might affect the system's security or its security log. (Default Workstation Policy is set to "Success" and "Failure").

-Security Options

- **Additional restrictions for anonymous connections** — Determines what, if any, additional restrictions should be placed on anonymous connections. To help ensure that only authenticated users have access to the network. (Default Workstation Policy is set to "No Access without Explicit Anonymous Permissions").

- **Allowed to eject removable NTFS media** —Determines which users are allowed to eject removable NT file system (NTFS) media. (Default Workstation Policy is set to "Administrators").

- **Amount of idle time required before disconnecting a session** —A value between 0 and 0xFFFFFFFF that determines the amount of idle time before an SMB session is disconnected because of inactivity. (Default Workstation Policy is set to 15 Minutes).

- **Audit the access of global system objects** —Determines whether global system objects with SACLs defined are audited. (Default Workstation Policy is set to DISABLED).

- **Audit use of Backup and Restore privilege** —Determines whether to audit every use of the backup and restore privileges. (Default Workstation Policy is set to DISABLED).

- **Automatically log off user when logon time expires (local)**—Determines whether to automatically log off users when their logon time for local connections expires. (Default Workstation Policy is set to ENABLED).

• **Clear virtual memory pagefile when system shuts down** —Determines whether to automatically clear the pagefile when the system shuts down. (Default Workstation Policy is set to ENABLED).

• **Digitally sign client communications (always)**—Determines whether SMB client communications are always digitally signed. (Default Workstation Policy is set to ENABLED).

• **Digitally sign client communications (when possible)**—Determines whether SMB client communications are digitally signed when possible. (Default Workstation Policy is set to ENABLED).

• **Digitally sign server communications (always)**—Determines whether SMB server communications are always digitally signed. (Default Workstation Policy is set to ENABLED).

• **Digitally sign server communications (when possible)**—Determines whether SMB server communications are digitally signed when possible. (Default Workstation Policy is set to ENABLED).

• **Disable CTRL+ALT+DEL requirement for logon** —Determines whether the CRTL+ALT+DEL key combination is required before a user logs on. (Default Workstation Policy is set to DISABLED).

•**Do not display last user name in logon screen** —Determines whether the name of the last successfully logged-on user is displayed in the Windows Logon dialog box. If the policy is enabled, the last user name isn't displayed. (Default Workstation Policy is set to ENABLED).

•**LAN Manager Authentication Level** —Determines which versions of the LAN Manager authentication protocol are accepted. (Default Workstation Policy is set to "Send NTLMv2 Response Only / Refuse LM & NTLM"). Since GIAC is an entirely Windows 2000 environment, this make for much more secure authentication.

• **Number of previous logons to cache (in case domain controller is not available)**—Determines how many cached successful logons the computer keeps in case a domain controller isn't available. I recommend setting this value to between 3 and (Default Workstation Policy is set to 10).

• **Prevent system maintenance of computer account password** —Determines whether a computer account password is updated every week. If this policy is enabled, the password isn't updated. (Default Workstation Policy is set to DISABLED).

• **Prevent users from installing printer drivers** —Determines whether regular users can install print drivers. If enabled, this policy prevents users from installing print drivers. This helps to prevent installation of drivers that may contain security holes. (Default Workstation Policy is set to ENABLED).

•**Prompt user to change password before expiration** —Determines how far in advance users should be advised that their password is about to expire. (Default Workstation Policy is set to 14 days).

• **Recovery console: Allow automatic administrative logon; Recovery console: Allow floppy copy and access to all drives and all folders** —Determine how easy it is to gain access to a system and its drives and folders from the Win2K recovery console. (Default Workstation Policy is set to DISABLED on both).

• **Restrict CD-ROM access to locally logged-on user; Restrict floppy access to locally logged-on user** —Determine whether CD-ROM and/or floppy devices are accessible to only the locally logged-on user. If enabled, these policies allow access to the specified devices only by the locally logged-on user. Even when enabled, if there isn't an interactive user, the media is accessible over the network. (Default Workstation Policy is set to DISABLED for both).

• **Secure channel: Digitally encrypt or sign secure channel data (always)**—Determines whether secure channel communications are always digitally signed or encrypted (but not necessarily both). (Default Workstation Policy is set to ENABLED).

- **Secure channel: Digitally encrypt secure channel data (when possible)**—Determines whether secure channel communications are encrypted when possible. (Default Workstation Policy is set to ENABLED).

- **Secure channel: Digitally sign secure channel data (when possible)**—Determines whether secure channel communications are digitally signed when possible. (Default Workstation Policy is set to ENABLED).

- **Secure channel: Require strong (Windows 2000 or later) session key** —Determines whether all secure channel communications require strong session key encryption. (Default Workstation Policy is set to ENABLED). Since GIAC is an entirely Windows 2000 environment, this is enabled to enhance security.

- **Send unencrypted password to connect to third-party SMB servers** —Determines whether clear-text passwords can be sent to third-party SMB servers that don 't support password encryption during authentication. If this policy is enabled, clear-text passwords are allowed. (Default Workstation Policy is set to DISABLED).

- **Shut down system immediately if unable to log security audits** —Determines whether the system should shut down if security events cannot be logged. If enabled, this policy causes the system to stop whenever a security event cannot be logged. (Default Workstation Policy is set to DISABLED). This was found not to be beneficial.

- **Smart card removal behavior** —Determines what should occur when a smart card is removed from the system. (Default Workstation Policy is set to "Lock Workstation").

- **Strengthen default permissions of global system objects (such as Symbolic links)**—Determines the strength of the default ACLs for global system objects. If enabled, this policy modifies the default access to prevent non-administrator users from modifying objects that they didn't create. (Default Workstation Policy is set to ENABLED).

- **Unsigned driver installation behavior** —Determines what should happen when a device driver that isn't digitally signed is installed on the computer. This helps to prevent installation of drivers that may contain security holes. (Default Workstation Policy is set to "Do Not Allow Installation").

- **Unsigned non-driver installation behavior** —Determines what should happen when a non-device driver that isn't digitally signed is installed on the computer. (Default Workstation Policy is set to "Silently Succeed").

Event Log

Settings for Event Logs

- **Maximum application log size; Maximum security log size; Maximum system log size** —Determine the size in kilobytes (Kb) of the event logs. (Default Workstation Policy is set to: 512kb for Application and System logs; 10240 kb for Security log).

- **Restrict guest access to application log: Restrict guest access to security log; Restrict guest access to system log** —Determine whether guest access is allowed to the logs. If these policies are enabled, guests cannot access the logs. (Default Workstation Policy is set to ENABLED for each log type).

- **Retention method for application log; Retention method for security log; Retention method for system log** —Determine the wrapping mechanism for each of the specified audit logs. (Default Workstation Policy is set to "Overwrite Events As Needed).

- **Shut down the computer when the security audit log is full** —Superseded by Shut Down System Immediately if Unable to Log Security Audits and shouldn't be used. (Default Workstation Policy is set to DISABLED).

Security Groups

Windows 2000 allows you to organize users and other domain objects into groups for easy administration of access permissions. Security groups let you assign the same security permissions to large numbers of users in one operation. This ensures consistent security permissions across all members of a group. Using security groups to assign permissions means that the access control on resources remains fairly static and easy to control and audit. When users need access, you can add them to the appropriate security groups as needed (and remove them when they no longer need access), and the Access Control Lists on resources change less frequently. Windows 2000 supports four types of security groups, which are differentiated by their scope:

- **Universal groups** - grant access to similar groups of accounts defined in multiple domains. Since GIAC Enterprises uses a single domain within a single forest model, it uses only the two built-in groups, Enterprise Administrators and Domain Administrators. There are only 3 members in the Enterprise Administrators group. This reduces the chance of Schema and structural changes being made. All Enterprise and Domain Administrators are located in the Des Moines office.

- **Global groups** - combine users who share a common access profile. GIAC uses these types of groups in grouping user accounts according to business units. These groups are then made members of Domain Local groups to grant rights to resources. Delegated administrative authority is tightly configured/restricted around business unit boundaries.

- **Domain local groups** - grant access to resources in a domain. GIAC uses these types of groups as well as Local groups to grant access to resources.

- **Computer local groups** -grant access on local computers without granting access across an entire domain. GIAC uses these types of groups as well as Domain Local groups to grant access to resources.

Awareness and Training

Continued awareness of security issues and events is an important part of network security. Regular security event notification from such groups as the SANS Institute helps to keep GIAC administrators ahead of the game. Patch availability and Hotfix notifications from Microsoft Security plays an important role as well keeping GIAC administrators alerted of weaknesses in OS and application code/configurations. Regular scans of the network using tools, such as Microsoft's HFNETCHK utility, helps to ensure the integrity of all the Windows 2000 computers.

User training is an important aspect in GIAC Enterprises' business and security is no exception. Users are trained on the importance of their role and are informed as to what to do or who to call when a security event occurs. They are trained on the use of Smart Cards and the importance/consequences of unauthorized use.

Overall security is only as strong as the weakest link and GIAC Enterprises has taken great strides to ensure its complete integrity.

References

1) Schultz, E. Eugene, Windows NT/2000 Network Security, MacMillan Technical Publishing, 2000.

2) McLean, Ian, Windows 2000 Security Little Black Book, Coriolis Technology Press, 2000.

3) Komar, Brian, Designing Microsoft Windows 2000 Network Security, Microsoft Press, 2001

4) Fossen, Jason, Securing Windows 2000, GIAC training course, Great Lakes SANS, 2001.

5) Windows 2000 Group Policy, URL: http://www.microsoft.com/windows2000/docs/grouppolwp.doc