Global Information Assurance Certification Paper

Security Recipe
GCWN Practical Assignment Version 3.1
Garrett Dietrick, GSEC, MCSE NT 4.0
October 29, 2002

Introduction / Abstract

GIAC Enterprises has been an established pizza restaurant for the past 12 years making and serving pizza throughout North America. GIAC Enterprises has provided a statement to our consulting group to design and implement a secure Windows 2000 network, based on their concerns around data privacy, confidentiality, and integrity.

GIAC Enterprises is headquartered in Hungryopolis, a large metropolitan city, and employs approximately 3000 workers at 250 restaurants in North America. GIAC Enterprise's main mission is to provide the best tasting pizza in the shortest amount of time. GIAC Enterprises sells their pizza in three diverse fashions:

1. Restaurant
2. Phone Delivery
3. Web Order Form

GIAC Enterprises purchases ingredients from a few selected companies. All the materials are sent to a warehouse, where they are distributed to the pizza shops according to sales and necessity. Currently managers at each pizza shop call Headquarters once a week to report their sales and order any materials that are needed.

There are 3 buildings that make up the geographical layout of GIAC Enterprise's headquarters:

1. Sales, Marketing, Accounting, and Human Resources account for approximately 300 employees in the main building.

2. Information Technology and the warehouse have approximately 60 employees (30 in IT and 30 in the warehouse).

3. Research and Development have recently (a year ago) acquired a new building, in which there are 40 employees.

There are two buildings located in Canada:

1. Sales, Human Resources, and Information Technology are located in one building employing 80 people.

2. The warehouse is the other building that has 20 employees. This location is for product distribution throughout Canada.

Background

Since GIAC Enterprise's pizza sales have been exorbitant they have decided to implement a new network in which will provide a secure and more stable environment. Currently GIAC Enterprises has a Windows NT environment with Windows 95 desktops. There is a connection to the internet, which does not have a firewall, demilitarized zone or Intrusion detection systems. GIAC Enterprise's has dealt with virus's in the past couple of years (E.g., I love you, Nimda, Code Red) which really have set back the company financially until now. The owners of GIAC Enterprises would like to start branch offices in new markets, but would like to have the network in place prior to establishing new business. GIAC Enterprises feel that they have stumbled upon a new pizza recipe through their research and development that will revolutionize pizza as it is today. This is also another reason they are interested in implementing a more secure and robust network.

Assumptions

GIAC Enterprise's has decided to lease equipment from Compaq (E.g., servers, workstations. The network equipment, routers and switches, will be purchased from Cisco Systems that the IP and Firewall team will implement in the next phase of the project.

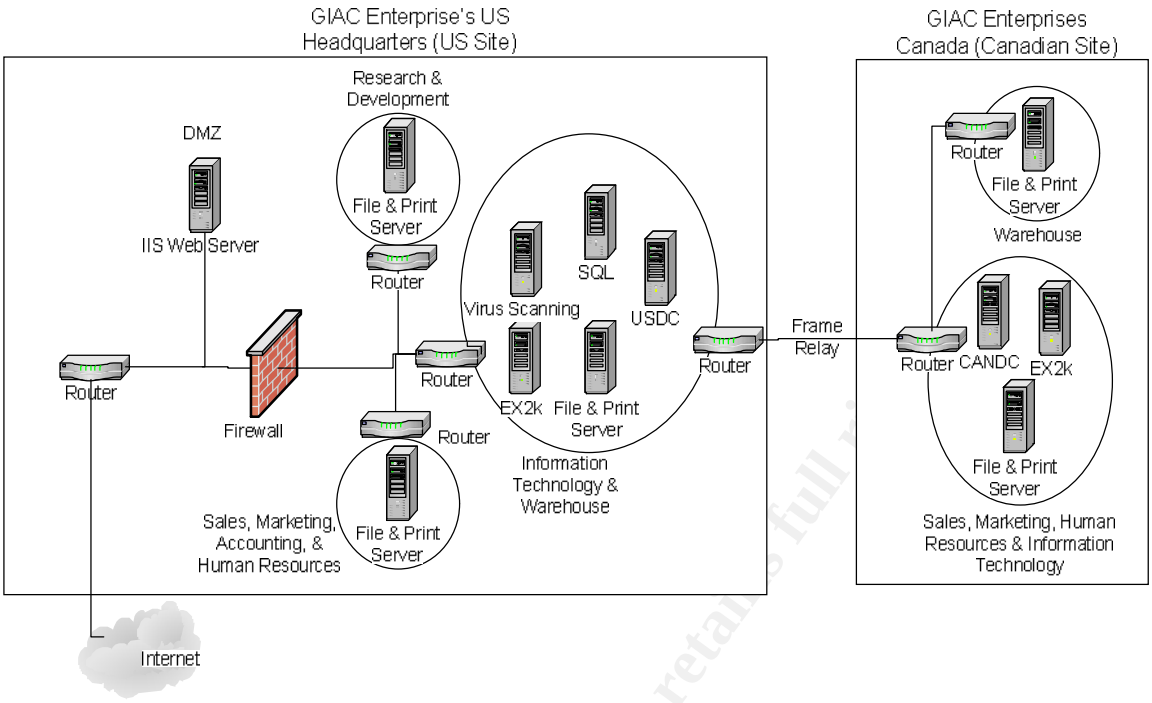
GIAC Enterprises has contracted us to upgrade their existing Windows NT network to Windows 2000 Active Directory, and update their client workstations from Windows 95 to Windows XP.

The messaging team has been approved to architect and implement Exchange 2000 with virus scanning functionality, which they would like consultation on, specifically on how to transmit secure email to and from the regional offices.

GIAC Enterprises has developed a web form for the public to order pizza online. In addition to this web form GIAC has created an intranet site for managers to fulfill on their sales and purchasing. They have asked for our group to review and assess their site security and provide recommendations.

Proposed Architecture

The network diagram provided below has been approved by GIAC Enterprise and they have asked to start as soon as possible.



In the proposed diagram there are two domain controller servers, five file and print servers, two Exchange 2000 servers, one Internet Information Server, one SMTP virus scanning server and one SQL server. Each server will be installed with Windows 2000 and have a specific role within the physical site. There are 5 physical sites (three in the US and 2 in Canada) and 2 logical sites, one in the US and one in Canada.

All the Windows 2000 servers contain the following:

- Windows 2000 with sp3 and the latest hotfixes
- Participate with the Active Directory
- Mirrored drives Raid 0 for the Operating system (OS)
- RAID 5 drives for files and applications
- NTFS Partitions for file security
- DAT drives for backup and recovery
- Stored in locked environmentally safe closets / rooms
- Guest account has been renamed and disabled
- Administrator account has been renamed and disabled
- Uninterruptible Power Supply (UPS) in event of power failure or disruption
- Install only applications / programs that are specific to the server (i.e., Exchange, SQL, and IIS). The more applications and programs that are installed can cause room for more down time and / or authorized access.
- Disable all non-essential services (e.g., messenger service and telnet) that will not affect the performance of the main application or service running on that specific server

- Page file is located on two partitions (depending on the amount of memory on the server) mirrored. This would enable the page file to be located off the mirrored drives for the Operating system. Page files should be at least the same size plus 50 megabytes as the amount of memory in the server. However, this does have some dependencies on what is running on the server.
- Enabled Crash dump files for review in case a server crashes.
- Virus scanning software, with automatic update features enabled and reviewed on a weekly basis for compliance.

There are five file and print servers throughout GIAC Enterprises which serve the same role. The purpose of these servers is to provide a place to save and share files and offer printing capabilities to users. The rational for five file and print servers are that there are 5 physical sites, connected by either a WAN or a LAN, which has the possibility of failing. Users in their specific location would not have to worry about losing access to their work files while having the file and print server local. However this is not the case for Exchange 2000 services.

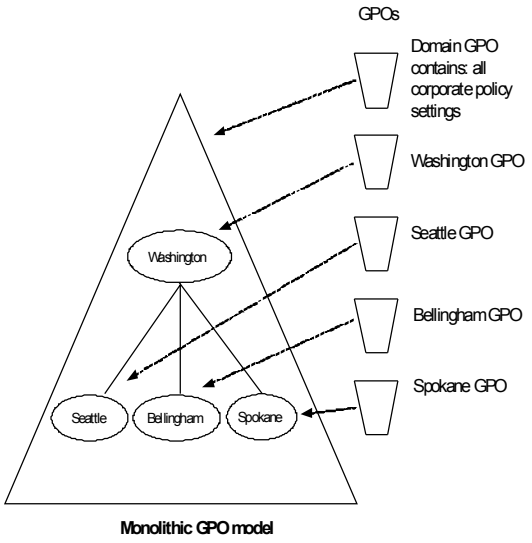
There are two Exchange 2000 servers. One Exchange server is located at each site. The main purpose of the Exchange server is to provide email messaging services, but it can also provide news groups, calendaring, journaling, etc. There will encrypted communications between the two sites. The XP Outlook client will be installed on all workstations to access the Exchange 2000 server.

The Internet Information Server (IIS) is located at US headquarters in the IT and warehouse building within the Demilitarized Zone (DMZ). GIAC Enterprises is using the IIS server for managers to update accounting with their sales and order supplies from the warehouse through the use of web forms. Each pizza shop will have a Windows XP workstation which will dial into US headquarters via a 1-800 number into the DMZ RRAS server farm. This will give managers access to the web form. The IIS server also hosts the site for customers to order pizzas from their local pizza shop.

Active Directory Structure

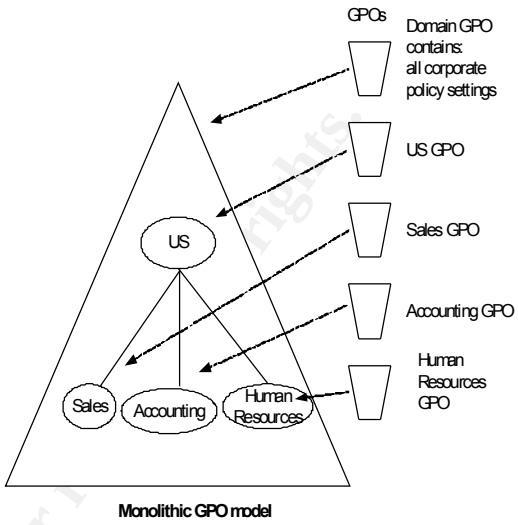
After all the servers were converted over to Windows 2000, the Active Directory (AD) was implemented. GIAC Enterprises asked that the AD be setup in a manner that it would be flexible and easy to administer, leaving room to expand in the future. The Active Directory was built with one domain and two sites for the current time, with room to add more sites if necessary. The AD was architected by geographic location first and then by functional layout. Thus, there are two sites based on geographical layout and then departmental OU's based on Functionality. Microsoft provides examples of GPO design, one of them being "Monolithic", which is fitting for how GIAC Enterprises Group Policy will be administered. Below, on the left, is Microsoft's example of a Monolithic design.

(Microsoft, Windows 2000 Group Policy, http://www.microsoft.com/windows2000/docs/grouppolwp.doc) On the right is how GIAC Enterprises GPO will be managed.



Monolithic GPO Design Model

The objective of this design is to create Group Policy objects based on a monolithic design—an approach that reduces the number of Group Policy objects that apply to a user and/or computer but may not be optimal for delegation.



This diagram represents a portion of GIAC Enterprises GPO design, modeled after Microsoft's Monolithic design model.

The OU Structure was built with departmental boundaries being established (e.g., Accounting, Sales, IT, etc.). The purpose the AD was designed this way was primary for the ease of administering each department within their respective site. There are 3 levels of OU structure:

- Site (US, and Canada)
- Departments
- A level of OU's representing each class of object (e.g., Users, Desktops, Servers, etc.)

First Level of OU

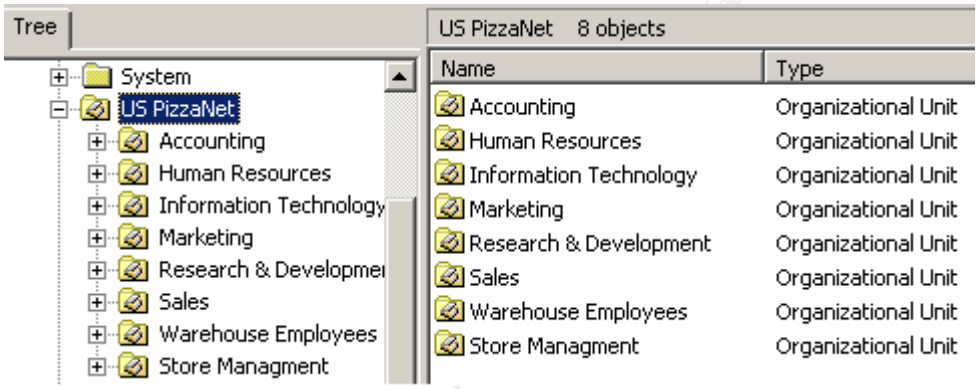
The two sites, (e.g. US and Canada) have several Organizational Unit's (OU), which are segregated at the department level. The sites act as the first level of OU structure. This will allow for policy to be segregated at the site level is necessary.

Second Level of OU

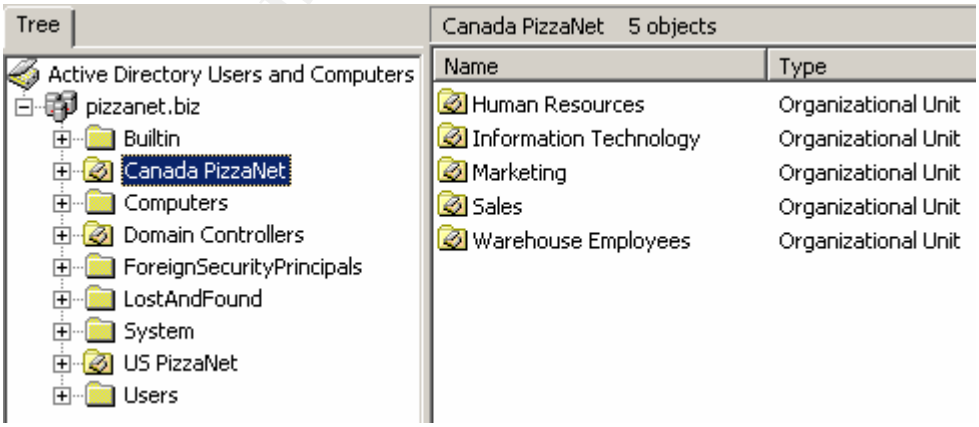
The second level OU structure was established at the department level since GIAC Enterprises felt this would give them the flexibility to administer and the ability to maintain an organized AD.

Attached below are two screen shots of the Active Directory structure that GIAC Enterprises was looking for as the second level of OU structure.

This design allows for room for additional departments. The US site includes 8 departments as shown below in the right pane.



The Canadian Site has only five, second level OU's / Departments. Three departments were consolidated into US accountability after the merge (e.g. Accounting, Research & Development, and Store Managment).



While having an OU structure for each department might seem difficult and time consuming to administer, it will create for a clean and orderly company. This will

also allow for flexibility in applying Group Policy (GPO) at the departmental level, which is discussed later.

Third Level OU Structure

At the third level of OU structure exists the actual objects within the Active Directory. These objects consist of the following:

- Administrator Accounts
- Desktops
- GPO (Group Policy Objects)
- Groups
- Laptops
- Servers
- Users

Administrator Account OU's were created for user accounts that can perform administrative duties within the specific department. Administrators within a department (e.g., Human Resources) should only use their administrative accounts when performing administrative duties. This OU is used to contain / house the Administrator accounts.

Desktop OU's were created to maintain a listing of all the desktops that are within the departments. There is a distinction between desktops and laptops based on those administering desktops, and will differ from laptops (e.g., Remote access / dial up etc.).

GPO OU's contain all the Group Policy Objects that pertain to the particular Department. Each department will have differing group policies (Group Policy will be covered more in another section).

Group OU's will contain Domain Distribution Groups. These groups are a collective group of accounts that have something in common, which will form a group.

Laptop OU's were created primarily to allow for a separate grouping of users to force policy amongst laptop user vs. desktop users. This also allows departments to segregate laptop users vs. desktop users for purposes of inventory and ease of administration.

Server OU's provide a logical grouping of the servers that are maintained for that department (e.g., the Accounting server).

User OU's contain a list of all the users for a specific department. Users will be placed in their respective departments. When a new user starts with the company they will be added to the department that they are joining. As well as

users that are leaving a department for whatever reason (i.e., laid off, quit, or terminated) their id's will remain in the department they worked in, disabled however for a period of ninety days, where they will be deleted from the system.

Third level OU's are the last level of OU structure. OU structure will be limited to this level (i.e. there will not be in organizational units below the third level); however, there can be more third level OU's created if necessary. The main reasons for having three levels of OU include:

- Ease of Administration
- Looks and feel (Aesthetics)
- Delegation

However, there is another important reason why the OU's are structured the way they are, that being security.

GIAC Enterprises wanted to ensure that they had the ability to establish administrative controls over their organization. By establishing departmental OU's GIAC Enterprises will have the capability to ensure that policies are administered to the appropriate departments. What this provides is a flexible security model. GIAC Enterprises will be able to administer one set of computers in one OU that is different in another OU (e.g. the US/Sales/Users can have different policies administered to them than say the CAN/Sales/Users). This model makes it possible to delegate at a specific level, but also allows for administration to delegate from a central location such as the domain level.

Group Policy Objects

While the Active Directory was being established and architected, Group Policy Object's architected. In, Windows 2000 Active Directory Design and Deployment, Gary L. Olsen states, "Policy may be applied at the site, the domain, or an OU container, and it affects computer and users in that container and in containers below it by inheritance". (Olsen, Chapter 5) There can be an overriding policy / base policy set at the site level which encompasses the base level of policies for GIAC Enterprises. Gary L. Olsen goes on to say that, "Users and computers inherit any policy set at an upper-level container if there are no conflicts. If there is a conflict, the last writer wins, so the lower-level containers override policy set at higher-level containers". (Olsen, chapter 5) What this enables is for administrators of departmental OU's to decide if there are any more specific policies that need to be implemented for their specific department.

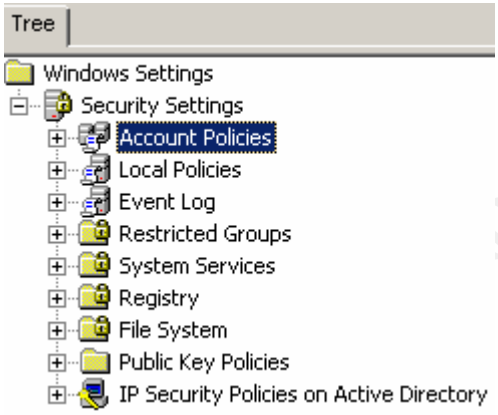
GIAC Enterprises mentioned that they just read an article from Information Week with an interview with Jason Fossen, an independent security consultant and also an instructor for SANS. Information week asks Jason, "What are the most important security enhancements (From going from Windows NT to Windows

2000)? Jason responds by stating, “Group Policy is a good example of how Windows 2000 security can be managed across an enterprise. Group Policy lets an administrator define a template of NT File System permissions, registry values, start up-shut-down scripts, and other settings and apply this template to thousands of systems automatically”. (Levitt, http://www.informationweek.com/834/prwinsec.htm) Group Policy is the foundation of Windows 2000 security.

As asked by GIAC Enterprises, the team developed the Default Domain Policy and the Default Domain Controller policies based on industry standards and input from GIAC Enterprises.

Default Domain Policy

The Default Domain Policy is the base policies used for GIAC Enterprises. The Default Domain Policy can be found at Start / Programs / Administrative Tools / Domain Security Policy. There is a security setting node which contains child nodes to administer. The child nodes consist of:



Account Policies:

- Password Policy
  - Enforcing Password history to remember 20 passwords or 5 years worth. This is to ensure that users will not reuse passwords to make it easier for password crackers to obtain unauthorized access.
  - Maximum Password age is setup for a 90 day period. Users are forced to change their password at least every 90 days, or immediately if compromised in any way.
  - Minimum Password Age is set at 1 day. This is set at one day so that users cannot run through 20 passwords to get back to their original password over a one day period. However, if a user’s

password is compromised the user will be asked to call the administrator to make the user change the password.
- Minimum password length is set to 8 characters.
- Password must meet complexity requirements is set to enable.

Note: The MCSE Training Kit "Microsoft Windows 2000 Professional" states, "If enabled (Password complexity), all passwords must meet or exceed the specified minimum password length; must comply with the password history settings; must contain capitals, numerals or punctuation; and cannot contain the user's account or full name". (Microsoft, p398). This is also the exact same statement Windows 2000 provides when a user does provide a complex password.

The statement is inaccurate in two fashions; one does not need to provide any capital letters in their password and a complex password must contain three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (A through Z)
- Base 10 digits (0-9)
- Non-alphanumeric characters (e.g.,!, $, #, %)

- Account Lockout Policy
  - Account Lockout Duration is set to 0. Account is locked out until an administrator unlocks it.
  - Account Lockout Threshold is set to 3 invalid logon attempts. This will not allow hacking tools to continuously attempt to login as a user without locking them out.
  - Reset Lockout Counter after 60 minutes. Again, this amount of time would hopefully thwart attempts to gain access to a user account.
- Kerberos Policy
  - Enforce User Logon Restrictions is Enabled. Since, Windows XP will be the client utilized at GIAC Enterprises, they will use Kerberos authentication. By enforcing user logon restriction, the Key Distribution Center (Service) will validate every session ticket to the server that is being queried for service.
  - Maximum Lifetime for Service Ticket is set for 600 minutes (ten hours) that a specified ticket is valid for a service, whereas the ticket would have to be renewed.
  - Maximum Lifetime for User Ticket is set at 10 hours before a new ticket request is asked for or provided.
  - Maximum Lifetime for User Ticket Renewal is set for 7 days.
  - Maximum tolerance for computer clock synchronization is set for 5 minutes. This will allow for some flexibility in computer / server

clocks to ensure that the timestamps are within a 5 minute time period of one another.

Local Policies

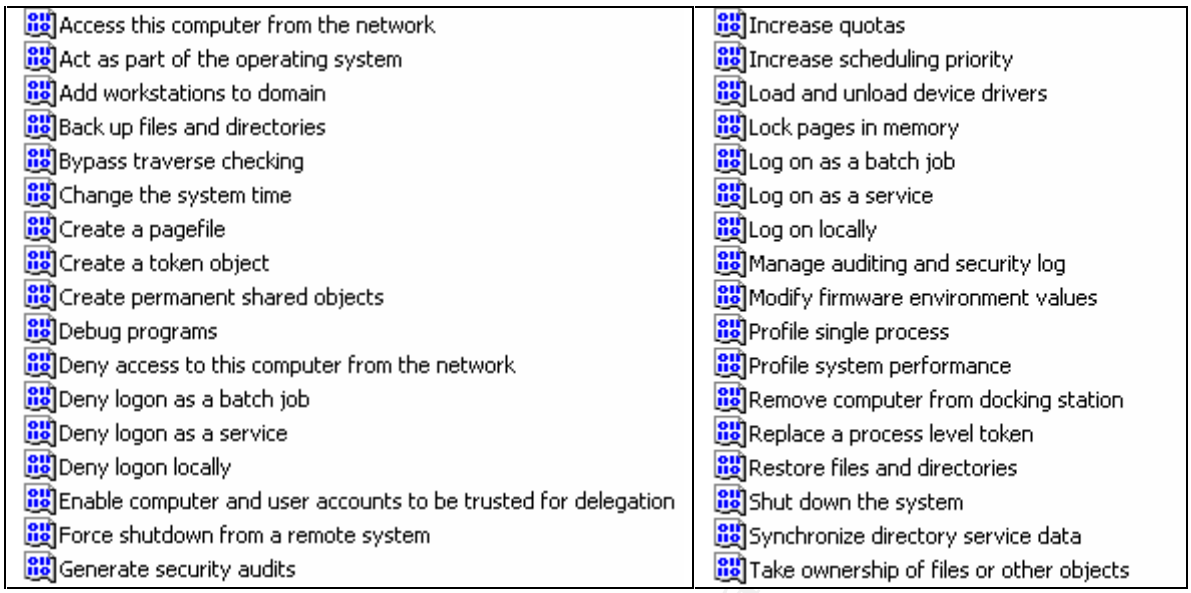
- Audit Policy
  - Audit Account Logon Events – is enabled only on logon failures to log when a possible breech or attempted breech occurred.
  - Audit Account Management – events are being logged on successful and failed attempts. This log should be reviewed to ensure that the appropriate people are managing the accounts. This log would provide management information on whether the appropriate people have been given access to make changes on accounts.
  - Audit Directory Service Access- Logging will only take place on the failure of someone trying to modify or access the directory with unauthorized access.
  - Audit Object Access – is enabled only on objects that are identified by GIAC Enterprises. Two examples of items that might be audited include, but are not limited to, file-level and printer-level objects.
  - Audit Policy Change – will be audited on success and failures due to the fact that Audit Policy change should be limited to very few changes. Successful policy change should go through an organized group of individuals at GIAC Enterprises, (i.e., change management, or problem management).
  - Audit Privilege Use is set to failure. This audit log provides information on each action a user performs utilizing a specific user right and will take note of it in a failed attempt to perform an action the user does not have access to perform.
  - Audit System Events are set to failure. The audit log captures when an administrator would reboot or restart the server or makes adjustments to system security.

The recommendation was to have the Audit logs be centrally stored and analyzed or have a tool that would centrally review all events deemed important (Errors and Warnings) summarized for later analysis.

GIAC Enterprises also felt that escalation procedures should be documented and communicated to ensure that procedures were in place in instances of breach of policy or unauthorized access. Audit logs are taken for granted at most companies. They are generally a good source of information for accumulating events and facts to determine system issues.

- User Rights Assignment

This policy section determines which users and groups have access to perform the following actions:



Access to these settings is very important and should be reviewed and evaluated periodically to ensure that the appropriate users / groups have the appropriate rights / access.

- Security Options

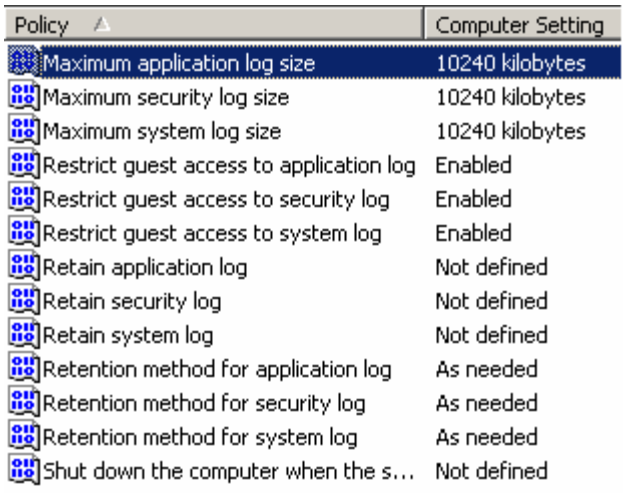
There are many security options to configure, for purpose of GIAC Enterprises, the key options will be discussed. The settings were taken from the security template hisecws.inf (located in C:\WINNT\security\templates), with several modifications.

- Interactive Logon: Do not display last user name is enabled. This policy setting should be set for all computing devices if possible especially servers, because of the users whom administrate them.
- Interactive Logon: Number of previous logons to cache is set to 3.
- Disconnect clients when logon hours expire is set to enable both locally and remotely. This setting will primary be used for contractor accounts, however there will be other accounts (e.g., training and restrictive accounts) where logon hours will be established and maintained by this policy.
- Prevent users from installing print drivers is enabled.

- Event Log

The Event logs are another very good source of obtaining information concerning application, security, and system issues. These log files should also be centrally managed and reviewed periodically (i.e. daily, weekly) to ensure that system

stability and integrity are maintained. Attached is a screen shot of the Event log settings.



Policy	Computer Setting
Maximum application log size	10240 kilobytes
Maximum security log size	10240 kilobytes
Maximum system log size	10240 kilobytes
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed
Shut down the computer when the s...	Not defined

Event logs will be set at 10 megabytes apiece. In the event that more than 10 megabyte are needed (If the event log file exceeds 10 megabytes during the day (i.e. prior to the log files being back up to tape) they will be adjusted to allocate more space).

Guest access will be restricted to mitigate against unauthorized users obtaining critical information about the system and its resources.

Retention of the log files will not be defined, however it will delete logs as needed to make room for more recent log information. Again, in the case that more than 10 megabytes of data are being produced, this could change to allow for a larger log file with a specified length of time (e.g. days).

Additionally, a history of event logs should be maintained for a duration of time long enough to review, assist with troubleshooting, and to provide a record of past events, which could assist in security / legal investigations. This history should be maintained for a years time (e.g. Tape Media).

Default Domain Controller Policy

The Default Domain Controller (DC) Policies are similar in nature to the Default Domain Policies, however, the main difference is that the default domain controller polices should be more restrictive based on the users accessing the servers and logging done for the DC's.

GIAC Enterprises has established a restrictive domain security policy, so within this section concentrating on Default Domain Controllers settings will only be

explained if differences are acknowledged between the two. Otherwise assume that the settings are the same as the default domain policies mentioned above.

The Default Domain Policy is the base policies used for GIAC Enterprises Domain Controllers. The Default Domain Controller Policy can be found at Start / Programs / Administrative Tools / Domain Controller Security Policy.

Account Policies:

- Password Policy
    - Maximum Password age is setup for a 30 day period. Administrators are forced to change their password at least every 30 days, or immediately if compromised in any way. Due to the nature of the administrative rights a user has access to their account passwords should be change regularly to ensure that an administrative account is not accessible.
    - Minimum Password Age is set at 10 days. This is set at one day so that users cannot run through 20 passwords to get back to their original password in a ten day period. However, if an administrator's password is compromised the administrator will be asked to have the password changed.
    - Minimum password length is set to 8 characters.

- Account Lockout Policy
    - The Account Lockout Policies are the same as Domain Policies.
    - Administrators will have two accounts. One account will be for their job responsibilities that do not require administrative access, and another account that will provide them with the functionality that they necessitate to get their job done as an administrator.

- Kerberos Policy
    - Same as the Domain Policies Section.

Local Policies

- Audit Policy
    - Audit Directory Service Access - Will log both success and failures to modify directory access. This log gathers information on success or failure to access a directory object that has its own System Access Control Lists (SACL).
    - Audit System Events are set for success and failure attempts to restart / reboot the Domain Controllers. This log also captures

events that pertain to changing or modifying system security and the system security log.

- User Rights Assignment
  - Same as the Domain Policies section.

- Security Options
  - This section is very similar to the Domain Policies section however, instead of using the hisecws.inf template; the hisecdc.inf template was used instead. This template is used to provide a highly secure domain controller.

- Event Log
  - The maximum log size for the application, security, and system log files is set at 50 megabytes. This is to ensure that when events are written to the log files that they should not be overwritten. GIAC Enterprises want to have the ability to go back and review event logs as far back as one year. Backup media will be archived off-site for a period of 2 years, which will meet GIAC Enterprises expectations of maintaining the log files for a year.
  - Guest access is restricted to the application, security, and the system logs, just as it was in the Domain Policies.
  - The retention method for the application, security and the system log files is on an "As Need" basis. When the log files reach 50 megabytes

Additional Group Policies

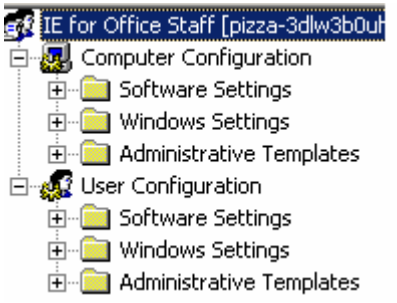
The Default Domain and Domain Controller Policies encompass many of the security policies that pertain to GIAC Enterprises' network; however, there are other security policies that contribute to the policies mentioned above. Two examples include Internet Explorer and Desktop security settings.

Internet Explorer Security Settings

Internet Explorer (IE) was configured to be administered through Group Policy. GIAC Enterprises wanted their internet browser (IE) to be locked down considerably, but not to a point that it became useless. We worked with them and have made agreements on the particular settings. One item that GIAC Enterprises mentioned was that they would like to harden the IE settings for the computers because they have had problems in the past with employees viewing inappropriate

To create a group policy, right click on the domain Pizzanet.biz, and select properties. Within the properties section select the Group Policy Tab at the top of the screen. Notice that the Default Domain Policy resides within this

container. Click on the “New” button. This will bring up a line to give the group policy a name. The name of this one will be IE for Office Staff. Next highlight it and select edit. This will bring up a Microsoft Management Console (MMC), Group Policy, which is called IE for Office Staff. Shown below is a screen shot of IE for Office Staff.



Notice that there are two sections: one Computer Configuration and one User Configuration. While there are going to be many commonalities between the two configuration methods, there are differences as well.

Computer Configuration:

The configuration settings are noted below.

- Security Zones: The first three settings are concerning Security Zones. They are enabled to ensure that any user logging onto that specific computer will have the same security zone settings. It also limits any user logging onto that computer, the ability to change policies or add / remove sites within the policy.

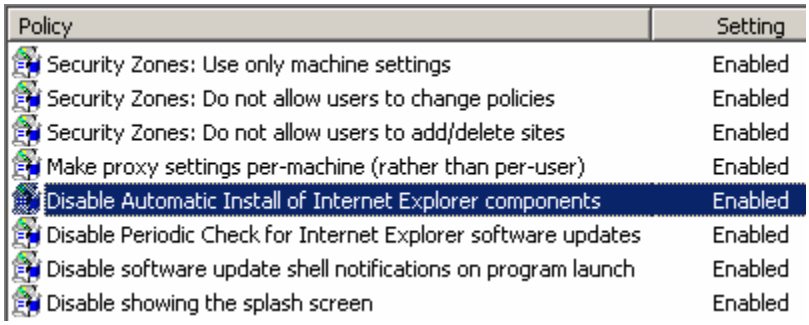
- Proxy settings are set per computer, so that it does not matter who logs onto that computer, these settings will take affect.

- Disable Automatic Install of Internet Explorer components is enabled. GIAC Enterprises understands that there is going to be many calls coming in due to the fact that many site want to install components. The idea is to find out what these components are (i.e. plug-ins, flashes, pdf’s, etc.) and publish them to the users if their job responsibilities call for it.

- Disable Periodic Check for Internet Explorer Software update is enabled. The reasoning for this is the same as above. GIAC Enterprises IT staff wishes to test all applications / service packs / hot fixes etc. prior to being published to the appropriate groups.

- Disable software update shell notifications on program launch is enabled for the same reasons noted directly above.

- Disable showing the splash screen is enabled. Preference / aesthetics



Policy	Setting
Security Zones: Use only machine settings	Enabled
Security Zones: Do not allow users to change policies	Enabled
Security Zones: Do not allow users to add/delete sites	Enabled
Make proxy settings per-machine (rather than per-user)	Enabled
Disable Automatic Install of Internet Explorer components	Enabled
Disable Periodic Check for Internet Explorer software updates	Enabled
Disable software update shell notifications on program launch	Enabled
Disable showing the splash screen	Enabled

User Configuration:

IE can be configured in a couple of areas under User Configuration. The first area is under Windows Settings / Internet Explorer Maintenance and the other area is Administrative Templates / Windows Components / Internet Explorer.

Internet Explorer Maintenance

Browser User Interface

- Browser Title can be adjusted for aesthetics.
- Animated Bitmaps – can adjust the icon in the upper-left hand pane of the browser, again just aesthetics.
- Custom Logo - Personalizing IE with GIAC Enterprises. What GIAC Enterprises did was use a pizza for their IE logo.
- Browser Toolbar buttons – can be modified, not necessary, again, just for looks.

Connection

- Connection Settings – need to be configured to automatically detect the internet connection (e.g. LAN).
- Automatic Browser Configuration is also set to automatically detect configuration settings.
- Proxy Settings are enabled. Within this section there is a list of Exceptions (Not to use the proxy server for local access (i.e., intranet)). Within this section, GIAC opted to place their intranet site.
- User Agent String – This configuration setting allows for the customizing of what the sites visited by GIAC Enterprises sees in their logging. This has been customized to say “Eat Pizza at GIAC”

URLs

- There are three sections under URL’s: Favorites & Links, Important URLs, and Channels. All three of these settings are primarily used for quick links / ease of use. GIAC Enterprises included some of the Manufacturing companies websites within the Favorites, but other than that they decided not to do much with these settings.

Security

- Security Zones and Content Ratings settings are configured here. Security Zones were mentioned above in the Computer Configuration section limiting what access users have to access and modify the Security Settings. GIAC Enterprises decided to have the security settings set at the template level of Medium for the Internet Zone, which increases user interaction because the user will be prompted before downloading etc.

  There are other zones within this section, such as: Local intranet (Medium low), Trusted sites (Medium low), Restricted sites (High), and My computer (Medium low).

  Content Ratings are the second section of Security Zones and Content Ratings settings tab. Since there were issues in the past with inappropriate internet usage, GIAC Enterprises wanted the settings to be set in a way that GIAC Enterprise employees would find it difficult to access many of the sites that are deem inappropriate.

- Authenticode Settings are also configured under the Security tab. These settings configure what software credentials and publishers are trustworthy. The advice that was give was to prompt users whenever they receive a new plug-in or flash. Reasoning behind this is that on a rare occasion a hacker has been known to fake credentials to act like they are from a trustworthy company (e.g. Microsoft) and potentially cause distress to many Network Administrators.

Programs

- Is the last container in the Internet Explorer Maintenance folder. This is where a company can configure to use other contact lists, or email clients as the defaults for IE. In the case of GIAC Enterprises nothing here had to be modified.

Under Administrative Templates is the last area that can configure IE settings. The settings within this section are enabled, disabled, or not configured. For purposes of this document, GIAC Enterprises asked that we only list the settings we configured.

There are six folders under the Internet Explorer folder in this section, they are as follows:

- Internet Control Panel
- Offline Pages
- Browser menus
- Toolbars
- Persistence Behavior
- Administrator Approved Controls

Internet Control Panel

- The settings under this section were not configured. The folder is to configure whether or not users are able to view and configure Internet options. This functionality is disabled in the Browser menus.

Browser Menus

- Tools menu: Disable Internet Options … menu option is set to enable. To note, users can still view and make changes on the Internet Options icon in the Control Panel.

Under the main folder Internet Explorer are some settings that can be configured. The following were configured.

- Disable external branding of Internet Explorer is enabled.
- Disable changing Temporary Internet files settings is enabled.
- Disable changing history settings is enabled.
- Do not allow AutoComplete to save passwords is enabled

Desktop Group Policy

GIAC Enterprises wanted to lock down the desktops to a degree, but also make it possible to work. In the Group Policy MMC, in the User configuration node exists a folder called Administrative Templates, which contains the following sub-folders: Start Menu & Taskbar, and Desktop. While, there are other folders under Administrative Templates these folders will be where the Desktops settings will primarily be configured.

Start Menu & Taskbar

Settings located in the Start Menu & Taskbar that GIAC has configured include:

- Remove user's folders from the Start Menu is enabled
- Disable and remove links to Windows Update is enabled
- Remove Documents menu from the Start menu is enabled
- Remove Run menu from the Start menu enabled
- Add Logoff to the Start menu is enabled

Desktop

The Settings in the Desktop node include two folders, (Active Desktop and Active Directory) and other settings that deal with desktop look and feel. Although, look and feel really seems a big part in these settings, what really is happening is that GIAC is limited the options users have to either accidentally create issues or intentionally cause issues.

The Active Desktop folder, nothing is configured in this folder or the Active Directory folder. Included below are the settings that make the desktop a more secure place to compute.

- Hide all icons on the desktop is enabled.
- Do not add shares of recently opened documents to My Network Places, is enabled.
- Prohibit user from changing My Documents path is enabled. What this will do is ensures GIAC Enterprises that users are saving files in the proper directories.
- Disable adding, dragging, dropping and closing the Taskbar's toolbars is set to enable. The main reason for this is that GIAC had issues in the past with users dragging and dropping items in the wrong folders and losing them. This posed more help desk calls and time searching for directories or objects that were misplaced.
- Disable Desktop toolbars is enabled.

Keeping a clean, yet workable environment on the desktop prevents users from misusing settings and policies that they do not need to configure.

Additional Security Measures:

While Group Policies provide security to GIAC Enterprises there are other security measures to implement to mitigate the loss of availability, integrity, and confidentiality. While most of the security measures are technical, there are certainly some process techniques that will provide a more secure environment. The following security measures are added in addition to the Group policies mentioned above.

- GIAC Enterprises wishes to have a formal documented process for creating groups and assigning rights and privileges to those groups. They have decided to do this to eliminate cluster and create process to an area that has not had much attention in their network prior to the migration. Along with a process of creating groups and assigning rights and permissions. It will be assigned to the local groups and not to individual accounts. Accounts will then be placed into groups.
- Service accounts will be assigned the lowest level of access necessary to perform the service they provide (e.g., firewall services do not need to be logged in as the Domain Administrator).
- Each user is assigned a unique account (e.g., user ID) by CSS ISS, to enable access to the Company network. (The procedure for issuing user accounts will be the same as the current ones in the Windows NT environment.)
- Disable the "AutoPlay" functionality on floppy disk / CD-ROM drives. Leaving this function enabled could allow programs to launch automatically upon startup of the computer, which could override the controls initiated by the operating system.

- To prevent unauthorized / unintended access to company resources, workstations and servers should be locked / logged off from when they are unattended or not in use. If a user forgets to lock or log off group policy sets the client machines screen savers to initiate after a 15 minute period.
- DNS and DHCP services should be run from different servers if DHCP is going to be used to perform registration of DNS records on behalf of its clients. If combined on one server, the DNS updates will not be encrypted when transmitted, once configured.
- The Directory Services Restore Mode Administrators password, along with all other service account passwords, is secured. This password is used to restore the Active Directory database from a backup and to protect access to the Active Directory database file stored on the server. This password (unlike group and user passwords) is stored in the server's local Security Accounts Manager (SAM) data store.
- A cost-benefit analysis should be performed to determine if the native tools for administering Windows and Exchange 2000 will provide the desired results (e.g., an appropriate level of granularity for security administration). If not, a third party administration tool should be procured. While MMC provides a nice and easy to use interface, there are other tools out there that might provide better services. Some tools to consider include tools like NetIQ's suite for example.
- Domain controllers are only used for managing the master security database and not for other purposes, such as hosting applications or databases.
- A formal Delegation Model should be established and communicated. (Delegation will occur at the level of each Organizational Unit and will include setting up user accounts and resetting passwords, for example.)
- GIAC Enterprises has had a procedure that they will continue in their new environment which includes signed authorization forms, and appropriate competency requirements (e.g., education / experience) are established and adhered to before delegating authority to anyone with a privileged account (e.g., for resetting passwords at an Organizational Unit level).
- Centralized administration of delegated users exists to maintain a complete listing of all user IDs that have been granted administrative privileges.

  This listing is periodically reviewed for appropriateness of the individuals included. Additionally, defined escalation procedures exist to immediately terminate any unauthorized access and report this to the appropriate individuals.
- Delegation is administered through the "least access required" principle, which provides only the access required to complete authorized tasks. Providing only the necessary amount of system access will enhance the overall control environment.
- A policy on permission "inheritance" was established (if and when to use it) and incorporated into the process for assigning permissions to ensure that unauthorized access was not invoked.

- A methodology is in place outlining the ownership, granting, and reviewing of rights, permissions, and shares. (The user who creates an object is the object's owner, while the Administrator account owns objects created during the installation.)

  Additionally, GIAC Enterprises performed an examination of the rights and permissions in the NT environment, prior to migrating them to Windows 2000 (i.e., unnecessary rights and permissions will be removed during the migration) in order to clean up from their unorganized environment.
- File sharing will be controlled at the file and directory level not at the share level. The default permissions on a share in Windows 2000 are granted to the "Everyone" group with Full Control. GIAC did this in their Windows NT environment so this is not much of a change for them.

XP additional security

- Remote Desktop will only allow the assigned owner access to the computer remotely. It is important to set the settings of this feature correctly; opening permissions to everyone could be potentially disastrous.
- Another tool similar in function is remote assistance which will be set to allow others (i.e. helpdesk and administrators access to the client computer after asking for permission.
- A personal firewall feature that is integrated with Windows XP should be configured and part of the standard desktop. GIAC Enterprises is not impressed with this functionality as it is. They are considering some third-party applications such as Norton Personal firewall, BlackIce, and ZoneAlarm.

The security settings mentioned above are by no means the all inclusive solution for a secure system, however they are meant to provide security by means of defense in depth. Each and every layer of security that GIAC Enterprises decides to utilize persuades hackers from making attempts at obtaining unauthorized access or performing Denial of Service (DOS) attacks.

GIAC Enterprises has made some great strides in security coming from their NT 4.0 network to Windows 2000 and by implementing the Active Directory. While you can use a recipe to build a pizza from scratch by having the main ingredients, (e.g. flower, egg, tomatoes, group policy, etc.) there is always room for more toppings (i.e. security).

Works Cited

Microsoft. MCSE Training Kit: Microsoft Windows 2000 Professional. Redmond: Microsoft Press, 2000.

Levitt, Jason. "Windows 2000 Security Represents A Quantum Leap." InformationWeek. 23 April 2001. URL: http://www.informationweek.com/834/prwinsec.htm

Microsoft. "Windows 2000 Group Policy." Microsoft Windows 2000 Server. 2000. URL: http://www.microsoft.com/windows2000/docs/grouppolwp.doc

Olsen, L. Gary. Windows 2000 Active Directory Design and Deployment. New Riders Publishing, 2001.

Last Updated: July 27th, 2017

Upcoming Training

SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC505: Securing Windows and PowerShell Automation	SEC505 - 201709,	Sep 18, 2017 - Nov 13, 2017	vLive
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced