Global Information Assurance Certification Paper

A Secure Windows 2000 Infrastructure Design

Securing Windows GCNT Practical Assignment
Version 3.0, Option 1

Mary A. Anthes
September 26, 2001

INTRODUCTION

GIAC Enterprises is an e-business that deals in the online sale of fortune cookie sayings. The small startup company has all its staff located in one location but has field sales personnel in various worldwide locations who need access to the GIAC Enterprises corporate network. The company deals with numerous external customers, suppliers and partners but this discussion will focus primarily on the internal GIAC Enterprises network.

The company's IT department is responsible for all system and network administration. Because the company is relatively new, GIAC Enterprises has been able to start from scratch with a complete Windows 2000 network, including all servers and workstations. This simplifies administration, but does require constant vigilance by the administrators for security vulnerabilities and issues with Windows 2000 and associated products: Exchange 2000, IIS 5.0, Office 2000/XP and SQL Server 2000.

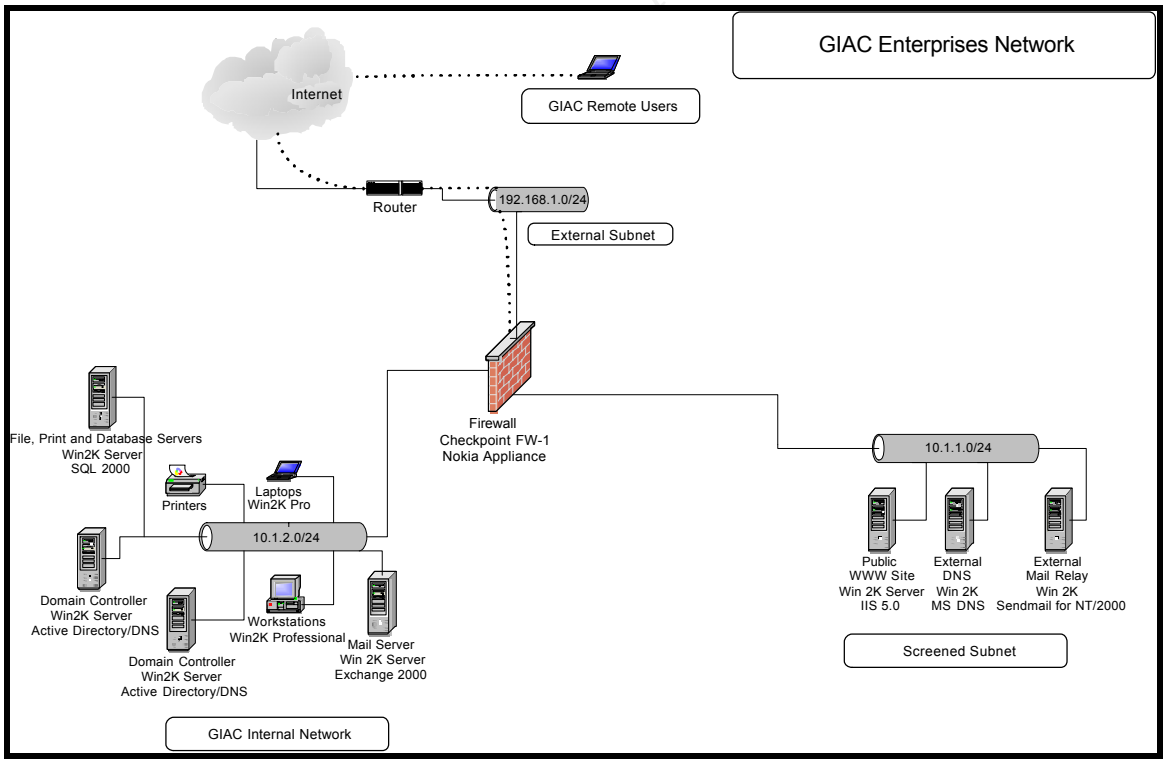
There are four departments at GIAC Enterprises. Research and Development is the heart of the business where the fortunes are developed and new research is ongoing. This department has greater access needs than the other departments, so they have some administrative rights to their own servers. Sales and Marketing, which includes the field sales people, is responsible for customer relations and expanding the GIAC business. Finance and Human Resources provide financial and administrative support. IT is responsible for supporting the enterprise's technology needs, including WAN connectivity, VPN solutions for remote users, internal systems and internet systems (public websites, name servers, etc.).

NETWORK DESIGN

The GIAC Enterprises network is relatively simple. A Cisco 3620 router connects to the company's ISP over a full T1 connection. This T1 connection provides both public internet access to GIAC's web, mail and name servers and internet access for the internal network. The router is connected to the GIAC firewall (Checkpoint Firewall-1 on the Nokia platform). The firewall also provides VPN access for the remote field sales staff in addition to GIAC employees at home or out of town.

The firewall has three interfaces: the external interface, which connects to the 3620 router; a screened subnet, which has all the publicly available servers (web, mail, DNS); and the internal network, which has all the GIAC Enterprises corporate systems and workstations. GIAC chose this standard design in order to segregate and protect their internal network from the internet.

The diagram shows the entire GIAC Enterprises network.



Internet-Accessible Screened Subnet

The firewall allows traffic only to the appropriate ports on the web, mail and name servers. The servers serve only one function, i.e. mail, so that as few ports and services are open to the internet as possible on any one system. The GIAC IT staff either manages

the systems at the console or uses Terminal Server, included in Windows 2000 Server. All the systems run Windows 2000 Server, Service Pack 2, with the latest hotfixes applied. The systems have been hardened; unnecessary services have been disabled and file system permissions have been tightened. GIAC has one web server, running IIS 5.0, a mail relay server running Sendmail for NT/2000, and two name servers that use Microsoft DNS. Sendmail for NT/2000 was chosen for this mail server because its only function is to relay SMTP mail to and from the internal Exchange server. The two DNS systems are for redundancy. One is authoritative for the giacenterprises.com domain and the other provides backup. These are the name servers that are officially registered and used by the internet to locate GIAC Enterprises servers; they contain no information about anything on the internal GIAC network. All of the servers are configured with RAID level 5, hot swappable drives and dual power supplies for maximum reliability.

Internal GIAC Enterprises Network

The internal network contains two Windows 2000 domain controllers, an Exchange 2000 server for email, calendaring and group folders, file and print servers for each department, and an intranet server. The domain controllers also serve as name servers for the internal network. Because GIAC is an all-Windows 2000 shop, they have no need to run WINS. The IT staff is responsible for managing all the servers, except those used by the Research and Development group. The nature of the work in that department requires that those users have administrative access to their resources. All of the servers managed by IT are located in a restricted-access data center. The servers run Windows 2000 Server, Service Pack 2 and the latest hotfixes. These systems are configured with RAID level 5, hot swappable drives and dual power supplies.

ACTIVE DIRECTORY DESIGN

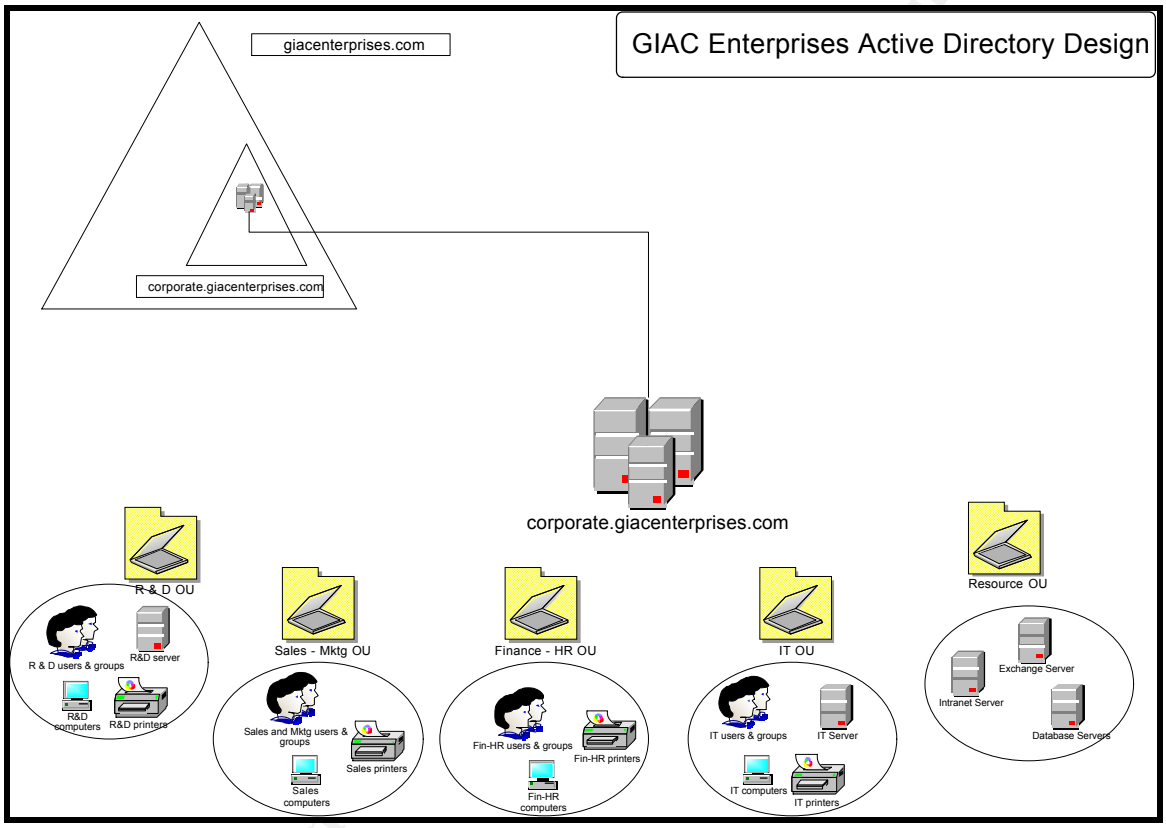
Since GIAC Enterprises is relatively new, the company was able to design a Windows 2000 network without having to consider migration or interoperability issues. The company is small and all staff are located in one location, with the exception of the field salespeople. The IT staff have responsibilities for most of the servers and workstations in the organization. Microsoft and most other experts recommend a single-domain design for most organizations. Since GIAC is small and centrally administered, a single domain design was chosen. However, the Active Directory was designed with an 'empty root' in order to facilitate future growth and reorganization, mergers or acquisitions. Because most staff are located in one place, there is no need to configure more than one site at this time.

The diagram below illustrates the root domain, giacenterprises.com, and its child domain, corporate.giacenterprises.com, which contains all the resources for the company. It is important to note here that the systems on the screened subnet, the public web server, mail relay server and external name servers, are NOT part of giacenterprises.com or any Windows 2000 domain. Since there are only four servers now, it is relatively easy to manage them individually. The security risk of making those systems part of Active Directory outweighed any ease of administration. If those systems were part of giacenterprises.com, directory information and NetBIOS would have to pass through the firewall and into the screened subnet, where it would be at greater risk for compromise because those systems are available to the internet. However, the systems in that subnet could be made into an entirely separate Active Directory forest at some point and a one-way trust established with the giacenterprises.com domain for easier remote management. When there are more systems in that screened subnet, it may make sense to establish a domain for them so they can take advantage of the centralized administration and use group policies to enforce security settings.

Each of the four departments (Research and Development, Sales and Marketing, Finance and HR, IT) has a corresponding Organizational Unit (OU). In addition, there is a Resource OU that holds the servers for some departments and resources that the entire company needs to access, like Exchange and the company intranet. Organizational Units are generally created for management reasons; they make it easier to delegate administration, to apply group policies and to manage all the objects in the domain. The delegation of administration is less relevant for GIAC Enterprises at this point, but it may become more important in the future. However, some groups, like Research and Development, need to have more privileges and control because of the kind of work they do. A larger need for creating the OUs in this network is to apply group policy, which will be discussed in more detail in the next section. One concern with group policies is that if there are too many of them or they are inappropriately deployed, they will slow down the logon process for users. Creating OUs and assigning group policies by OU will help avoid this. If we have a group policy that will only apply to the Finance and HR group, for example, we can link that policy to the Finance and HR OU. That policy will not even be

processed by users in another group who are not part of the Finance and HR OU.

GIAC IT staff will use the built-in Windows 2000 methods for deploying software, updates and service packs to the workstations. The OU structure will help with this as well. The network administrators can create installation packages which they can then deploy through group policy based on OU. Organizational Units were designed to be somewhat fluid. Users and computers can be easily moved from OU to OU, which makes administration easier.



The OU structure of the corporate.giacenterprises.com domain and the objects placed in each OU is summarized below:

Resources OU	**Res & Dev OU**	**Finance–HR OU**	**Sales-Mktg OU**	**IT OU**
File servers	R&D users	Fin-HR users	Sales-Mktg users	IT users
Exchange 2000	R&D groups	Fin-HR groups	Sales-Mktg groups	IT groups
Database server	R&D computers	Fin-HR computers	Sales-Mktg computers	IT computers
	R&D printers	Fin-HR printers	Sales-Mktg printers	IT printers
	R&D servers			IT servers

The Research and Development needs to manage its own servers, so those servers have been added to that OU so that administration of those resources can be delegated to R&D. IT will manage all the servers in the Resources OU.

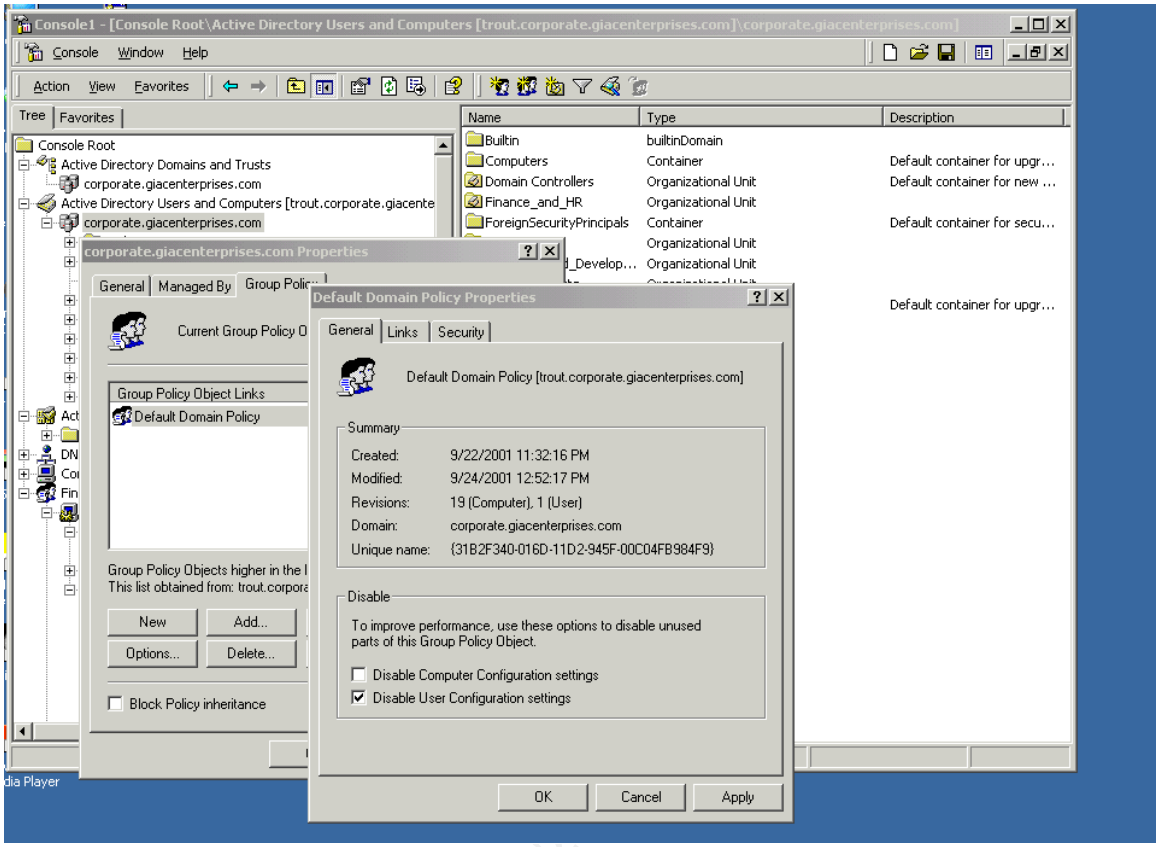
GROUP POLICY and SECURITY DESIGN

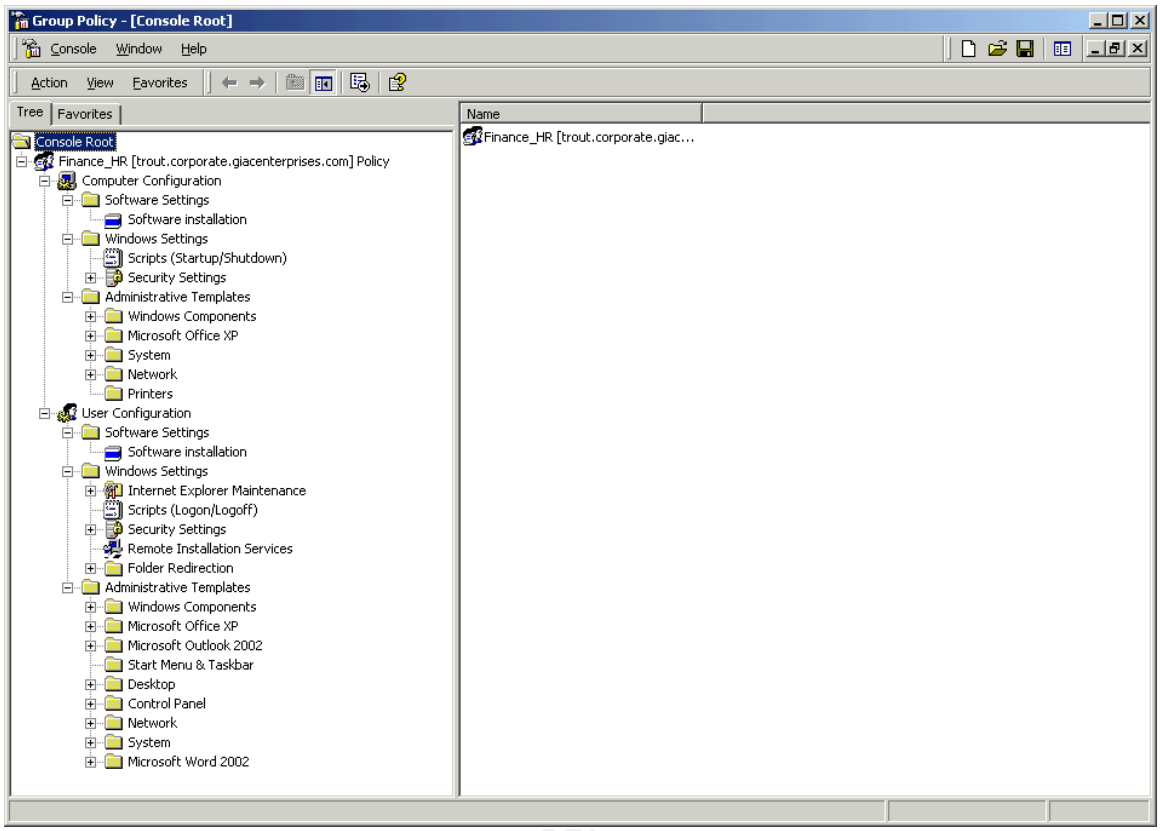
Group policy is one of the best reasons to adopt Windows 2000 and Active Directory. Group policy is designed to centrally enforce security, user desktop and application settings across Active Directory domains. Some of this functionality was available in Windows NT 4.0 with system policies, but it is greatly enhanced with group policies. In fact, group policies have been called 'system policy on steroids.' (see 'The Definitive Guide to Windows 2000 Group Policy,' an e-book available at fullarmor.com, free registration required)

By default when Active Directory is installed, two group policy objects (GPOs) are created: the Default Domain Policy and Default Domain Controller Policy. The Default Domain Policy applies to the entire domain. However, it can be overridden by OU policies. The order of precedence for applying GPOs is: NT 4 system policies, local GPOs, site, GPOs, domain GPOs and OU GPOs. Since GIAC Enterprises does not have NT 4 systems, there will not be any system policies. The corporate.giacenterprises.com is a single-site domain, therefore there will not be any site-based GPOs. The OU GPO will be processed last, which means its settings will override any settings in any domain GPOs. The Default Domain Controller Policy is applied only to the domain controllers. In this case, there are two domain controllers for corporate.giacenterprises.com. We will look at the key settings for both of these GPOs, in addition to settings for the group policies for some individual OUs.

Default Domain Policy

In this policy, we will define some settings that need to be applied to every user in the domain. Group policies are divided into two sections: Computer Configuration and User Configuration. For the domain-wide policy, we are only interested in the Computer Configuration settings. The User Configuration settings will be handled in the OU GPOs. We will disable the User Configuration settings so they will not have to be processed when the user logs on.





All of the settings below are found under the Computer Configuration option.

We will use the default domain policy to establish password requirements for the domain.

Windows Settings | Security Settings | Account Policies | Password Policy	
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	2 days
Minimum password length	7 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

The effect of these settings is that users must change their passwords every 90 days and they cannot reuse any of the last eight passwords they had. To prevent someone from quickly changing their password nine times, which would allow them to keep using the same password, we set the minimum password age to two days. We also enable the password length and complexity requirements, which will force users to choose a password that is at least seven characters long and uses a mix of letters, numerals and symbols. Storing passwords using reversible encryption is only necessary if Digest authentication is being used. (Cox, Windows 2000 Security Handbook, p. 284) We will leave it disabled, which is the default.

Windows Settings | Security Settings | Account Policies | Account Lockout Policy	
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Resent account lockout counter after	30 minutes

The lockout policy settings dictate how many failed logon attempts are allowed before the account is locked. The duration of 30 minutes means that once the account is locked, the user must wait 30 minutes before they can log on. Five tries to get a password right seems reasonable; if it is set much lower, it will result in more calls to have passwords reset or accounts unlocked. Higher values mean that intruders have more attempts to guess the password. A lockout duration of 30 minutes should dissuade most hackers trying to guess the password, but still allow the legitimate user to get back to work in a reasonable amount of time.

The third option under Account Policies is Kerberos Policy. We will leave these settings at the default options, as recommended. (Cox, Windows 2000 Security Handbook, p. 286, and Opitz, Guide to Windows 2000 Kerberos Settings, p. 5)

We will also set up some auditing policies for the domain.

Windows Settings | Security Settings | Local Policies | Audit Policy	
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not defined
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	Not defined
Audit system events	Success, Failure

By choosing these settings we will log all logon successes and failure and any changes to the accounts on the system. We have enabled auditing on object (files, registry keys) access failures, but we would also need to enable that on the particular object to log any events. This should be done carefully as it can fill up an event log very quickly. We are also logging changes in security policy (for example, changes in user rights) and system events like shutdowns.

The Event Log settings are closely related to the audit policies.

Windows Settings | Security Settings | Event Log | Settings for Event Logs * not all settings shown	
Maximum application log size	2 MB

Maximum security log size	5 MB
Maximum system log size	2 MB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled

The log retention policies will be set as follows:

- Security Log events will be retained for 21 days. If the log fills before that, the oldest events will be overwritten.
- System Log events will be retained for 14 days. If the log fills before that, the oldest events will be overwritten.
- Application Log events will be overwritten as needed.

For critical systems like servers, a method of reviewing and archiving logs on a weekly basis will be established so critical events are not missed. For workstations, if the logs fill up, they will just be overwritten.

There are numerous policy settings in the User Rights Assignment (Windows Settings | Security Settings | Local Policies | User Rights Assignment) category. Some of the key settings will be explained here.

Access this computer from the network	Administrators, Users

This allows users to connect to the computer over the network.

Back up files and directories	Administrators, Backup Operators, Server Operators

Only administrators, backup operators and server operators will be able to back up files. User files will be kept on file servers for centralized backups. They will not need to back up their own files.

Change the system time	Administrators

System times will be set in log on scripts. There is no need for users to set the time on their workstations. It is important that the time in the domain be synchronized for Kerberos security and in the case of an intrusion or attempted intrusion, the logs across different systems can be correlated.

Force shutdown from a remote system	Administrators

Only administrators should be allowed to remotely shut down any of the systems.

Manage auditing and security log	Administrators

This setting allows users with this right to view and clear the event log. We only want administrators to have that right.

Restore files and directories	Administrators, Backup Operators, Server Operators

Since file storage and back up is centrally managed at GIAC Enterprises, there is no need for users to restore files.

A number of policy settings are available under Security Options (Windows Settings | Security Settings | Local Policies | Security Options). The key settings for our GIAC Enterprises security policy will be discussed below.

Additional restrictions for anonymous connections	No access without explicit anonymous permissions

The default setting, no restrictions, would allow anonymous users to list account names, network shares and have the same access as the "Everyone" group. In some environments, anonymous connections must be allowed for some applications and interoperability. (Haney, "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set," p. 36) However, this is not the case for GIAC Enterprises.

Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (when possible)	Enabled

These settings make it possible to digitally sign packets for the authentication of SMB communications. We have chosen the 'when possible' setting to allow unsigned communication when possible but it is not required.

Disable CTRL+ALT+DEL requirement for logon	Disabled

If this setting is enabled, the user does not have to press the Ctrl-Alt-Del keys to get the logon box. The Ctrl-Alt-Del sequence establishes a secure path for logging on and should not be disabled. (Haney, "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set," p. 40)

LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM

NTLMv2 authentication is far more secure than LanManager (LM) or NT LanManager (NTLM). Since GIAC Enterprises is a Windows 2000 shop, this setting can be enabled without making any changes to the workstations or servers. For Windows 9x clients, the Directory Services Client needs to be installed to use NTLMv2. For Windows NT 4.0, Service Pack 4 or higher needs to be installed to use NTLMv2.

Message text for users attempting to log on	This is a private system. All use is monitored and logged. By logging on to this system, you consent to all corporate policies.
Message title for users attempting to log on	Authorized Users Only

These settings enable a message box which appears before.

Rename administrator account	Rename to something other than 'administrator'

Even though this may not stop an experienced hacker, renaming the administrator account will stop attacks that target the administrator account by name. The account description should be changed as well.

Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) sessions key	Enabled

"When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted." (Windows 2000 Server Resource Kit: Supplement 1 Group Policy Reference) However, not all information on that channel is encrypted. These settings will encrypt all data on the channel. All the secure channel options can be enabled because GIAC Enterprises is a single forest and there are no issues with trusted or trusting domains. If there were trusts that had to be considered, then all domain controllers in all the trusted domains would have to have these options enabled as well.

Default Domain Controller Policy

The default domain controller policy will only apply to the two domain controllers in the corporate.giacenterprises.com domain. We will use many of the same settings from the default domain policy in this policy.

Password and account lockout policies will be identical to the default domain policy.

Windows Settings | Security Settings | Account Policies | Password Policy	
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	2 days
Minimum password length	7 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Windows Settings | Security Settings | Account Policies | Account Lockout Policy	
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Resent account lockout counter after	30 minutes

Auditing policies and Event Log settings will be modified somewhat from the default domain controller policy because of the sensitive information on the domain controllers and the need to control access to those servers.

Windows Settings | Security Settings | Local Policies | Audit Policy	
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	Not defined
Audit system events	Success, Failure

These settings are identical to the default domain policy settings, except for the addition of logging access to objects in Active Directory. This is similar to 'audit object access' but applies only to Active Directory objects.

The Event Log settings are closely related to the audit policies. Again the settings are identical to the default domain policy settings. The only change is the increase of the security log to 10 MB because of the critical information stored on the domain controllers.

Windows Settings | Security Settings | Event Log | Settings for Event Logs * not all settings shown	
Maximum application log size	2 MB
Maximum security log size	10 MB
Maximum system log size	2 MB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled

The log retention policies will be set as follows:

- Security Log events will be retained for 21 days. If the log fills before that, the oldest events will be overwritten.
- System Log events will be retained for 14 days. If the log fills before that, the oldest events will be overwritten.
- Application Log events will be overwritten as needed.

A method of reviewing and archiving logs on a weekly basis will be established so critical events are not missed.

There are numerous policy settings in the User Rights Assignment (Windows Settings | Security Settings | Local Policies | User Rights Assignment) category. Some of the key settings will be explained here. In particular, we will note settings where the default did

not meet the GIAC Enterprises needs and was changed.

Access this computer from the network	Administrators, Authenticated Users

This allows authenticated users and administrators to connect to the computer over the network. The default setting includes the 'Everyone' group, but there is no need to allow that for the domain controllers.

Add workstations to a domain	Administrators

By default this setting includes Authenticated Users and Administrators. At GIAC Enterprises, only the IT staff will be adding workstations to the domain, so we have removed the Authenticated Users group.

Bypass traverse checking	Administrators, Authenticated Users

This right allows to traverse directories even though they may not have permissions to that directory. The default setting included the Everyone group, which has been removed.

Log on locally	Administrators, Server Operators, Backup Operators

By default, users are NOT allowed to log on locally to a domain controller. We will leave the defaults but this is an important setting and should be double-checked.

A number of policy settings are available under Security Options (Windows Settings | Security Settings | Local Policies | Security Options). Most of these settings will be the same as in the default domain policy. The settings that are different are discussed.

Do not display last user name in logon screen	Enabled

Even though the domain controllers are in a secured data center, we will use this setting to remove the user name from the logon screen. Since IT staff will be logging on to these servers as administrators, it is important to keep that user name from appearing on the screen.

Shut down system immediately if unable to log security audits	Enabled

This setting can be dangerous on a critical system like a domain controller, as the system could be DOS-ed by someone writing garbage information into the security log. However, we have enabled it because we need to know immediately if the security log is full so that we do not lose information.

Organizational Unit Group Policies

The GIAC Enterprises network administrators utilize GPOs based on the departmental

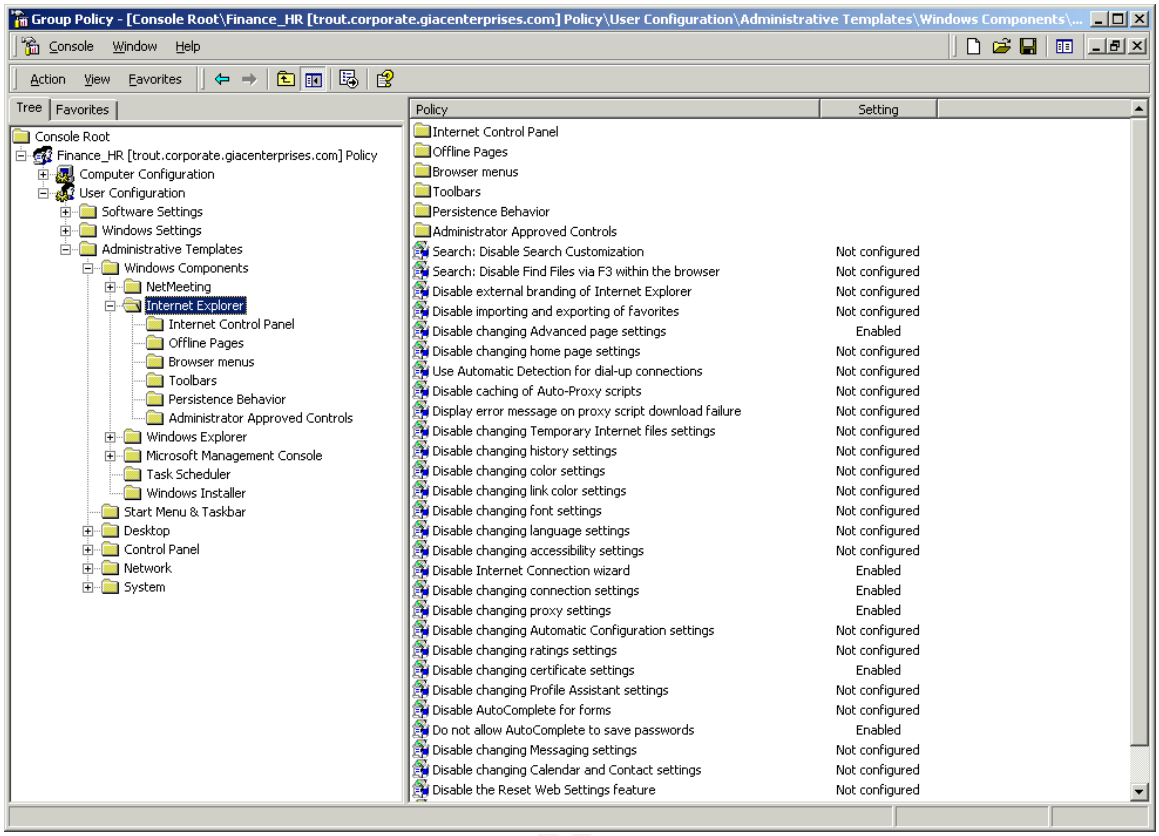
OU to enforce other pieces of the company security policy. There are probably hundreds of settings dealing with user desktops, applications and security that can be modified. We will take the Finance-HR GPO as one example; the Sales-Marketing GPO is similar. The IT and Research and Development groups do not have additional GPOs as they need to have less restrictions to do their jobs. In addition, we will look at a GPO that is applied to the field sales group. These users are part of the Sales – Marketing OU but have some different needs as they connect remotely via VPN to GIAC Enterprises.

One of the many benefits of group policies is that they can be created and modified without being linked to an OU. The policy does not go into effect until it is linked. Multiple GPOs can apply to an OU (or domain or site) and the same GPO can be linked to multiple OUs, domains or sites. However, care needs to be taken that the GPO processing will not slow down user logon time and that the settings do not conflict or otherwise combine to have an unintended effect.

Finance-HR GPO

For this GPO, we will concentrate on the User Configuration settings. The default domain and default domain controller policies will still be in effect for the Computer Configuration settings. This GPO is linked to the Finance-HR Organizational Unit. There is a global group, called Finance_HR Users, which contains all the user accounts for the staff in these departments. That group has been given "Read" and "Apply Group Policy" rights to this GPO. Without those rights, the policy will not be applied to the user.

Under User Configuration | Administrative Templates | Windows Components | Internet Explorer, we can control many settings for Internet Explorer. This is important because of hostile code that may be in ActiveX controls or JavaScript. We also want to try and restrict what the users can download on their systems.



A summary of all the Internet Explorer settings that have been configured follows:

User Configuration | Administrative Templates | Windows Components | Internet Explorer	
Disable changing Advanced page settings	Enabled
Disable changing certificate settings	Enabled
Do not allow AutoComplete to save passwords	Enabled
User Configuration | Administrative Templates | Windows Components | Internet Explorer | Internet Control Panel	
Disable the Security page	Enabled
Disable the Content page	Enabled
Disable the Connections page	Enabled
Disable the Programs page	Enabled
Disable the Advanced page	Enabled
User Configuration | Administrative Templates | Windows Components | Internet Explorer | Browser menus	
Disable save this program to disk option	Enabled

These settings restrict the user from seeing any tabs in Tools | Internet Options except for the General tab. We can use the Internet Explorer Administration Kit (http://www.microsoft.com/windows/ieak/default.asp) to build a customized version of IE for our users, configure the security and program settings, distribute it and then use a

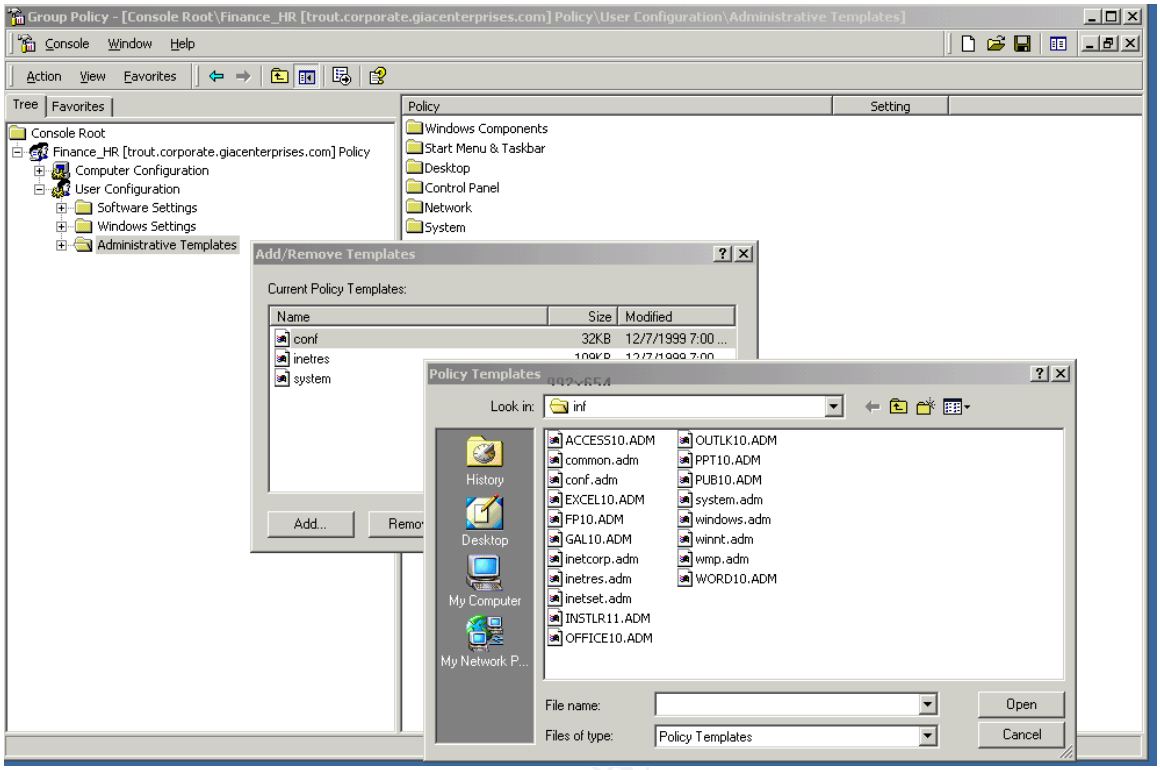
GPO like this to ensure that no changes are made. We also can prevent the user from saving programs to their computer from the Internet.

There are other Windows settings that we can control as well:

User Configuration | Administrative Templates | Start Menu & Taskbar	
Disable and remove links to Windows Update	Enabled
User Configuration | Administrative Templates | Control Panel | Add/Remove Programs	
Hide Add/Remove Windows Components page	Enabled
Hide the "Add a program from CD-ROM or floppy disk" option	Enabled
Hide the "Add programs from Microsoft" option	Enabled
User Configuration | Administrative Templates | Control Panel | Display	
Activate screen saver	Enabled
Password protect the screen saver	Enabled
Screen Saver timeout	Enabled
User Configuration | Administrative Templates | Control Panel | System	
Disable registry editing tools	Enabled

These settings restrict the user from loading programs from CDROM or disk, at least through the Control Panel. It also prohibits access to Windows Update, both from the Control Panel Add/Remove Programs applet and on the Start Bar. We have also password protected the screen saver, which will activate after 15 minutes of idle time. Finally, we have restricted the user from editing the registry through regedit.exe and regedt32.exe.

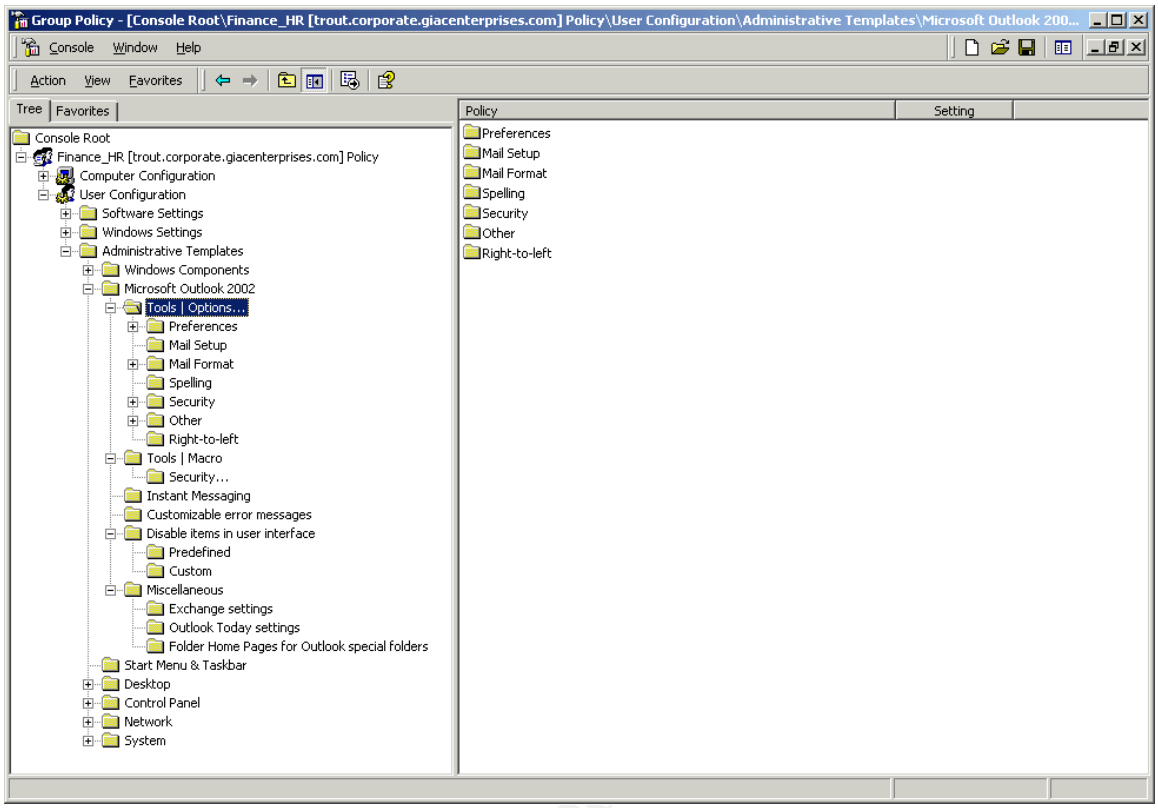
Microsoft makes additional templates available for other applications as well. There are a number of settings in the Microsoft Office programs that have security implications. Many of these can be controlled through the templates available in the Office Resource Kit. The templates are available at http://www.microsoft.com/office/ork/xp/appndx/appa18.htm. The policy templates (ADM files) can then be added to the Administrative Templates folders in the GPO by right-clicking the folder and selecting 'Add/Remove Templates …'



The files available from the Office XP Resource Kit are:

Access10.adm	MS Access	Office10.adm	Shared by Office components
Excel10.adm	MS Excel	Outlk10.adm	MS Outlook
FP10.adm	MS FrontPage	Ppt10.adm	MS Powerpoint
GAL10.adm	Clip Organizer	Pub10.adm	MS Publisher
Instlr11.adm	Windows Installer 1.1	Word10.adm	MS Word

We will just look at some of the options in the Outlk10.adm file, since Outlook has a number of security issues and needs to be managed carefully to avoid introducing viruses or worms.



The settings we will make are summarized:

User Configuration | Administrative Templates | Microsoft Outlook 2002 | Tools - Options | Security	
Prevent users from customizing attachment security settings	Enabled
Allow access to e-mail attachments	Enabled (In addition to enabling this setting, the allowed extensions must be listed: for example, DOC, XLS, TXT)
User Configuration | Administrative Templates | Microsoft Outlook 2002 | Miscellaneous	
Prevent users from adding HTTP e-mail accounts	Enabled

Users are prevented from changing the security settings on attachments and are restricted in the types of attachments they can receive. In addition, users are restricted from adding HTTP email accounts to their Outlook clients; they cannot get their Hotmail, for example, in their Outlook client. It must be noted that while these restrictions are nice to have, they will not be enough to protect the company network from all viruses and worms entering via email. Antivirus protection must be installed on the mail server and possibly content filtering software as well to block malicious files.

Field Sales GPO

GIAC Enterprises has a number of sales staff who live and work all over the world. These staff do work onsite, but do all their work via VPN connections and company-provided laptops. Because these users are out on the internet, using a variety of ISPs, GIAC has little control over the network environment these systems are in. We can use group policies to try and minimize the risk to these laptops as well as the GIAC Enterprises network, since they do connect to the network. Group policies alone will not protect these systems. They will also need regularly updated antivirus protection and personal firewall software, like Zone Alarm or BlackIce.

To enforce this GPO, we will create a group called Field_Sales and place it in the Sales – Marketing OU. This group will have "Read" and "Apply Policy" rights to the GPO, but the rest of the Sales and Marketing staff will not since we only want this policy to apply to the remote users.

GIAC IT staff is responsible for installing software on these laptops, just like the systems in the office. We will disable IE's automatic installation of IE components and periodic checks for IE updates.

Computer Configuration | Administrative Templates | Windows Components | Internet Explorer	
Disable automatic install of Internet Explorer components	Enabled
Disable periodic check for Internet Explorer software updates	Enabled

We will use some of the same settings as the GPOs for Finance and HR for restricting the Tools | Internet Options menu in Internet Explorer. The users will only see the 'General' page and will not be able to save programs to disk from the browser.

User Configuration | Administrative Templates | Windows Components | Internet Explorer	
Disable changing Advanced page settings	Enabled
Disable changing certificate settings	Enabled
Do not allow AutoComplete to save passwords	Enabled
User Configuration | Administrative Templates | Windows Components | Internet Explorer | Internet Control Panel	
Disable the Security page	Enabled
Disable the Content page	Enabled
Disable the Connections page	Enabled
Disable the Programs page	Enabled
Disable the Advanced page	Enabled

Since IT staff is responsible for installing software to these systems, we will restrict their

ability to install programs from CD, disk or the internet. We will also disable 'Windows Update.'

User Configuration | Administrative Templates | Windows Components | Internet Explorer | Browser menus	
Disable save this program to disk option	Enabled
User Configuration | Administrative Templates | Start Menu & Taskbar	
Disable and remove links to Windows Update	Enabled
User Configuration | Administrative Templates | Control Panel | Add/Remove Programs	
Hide Add/Remove Windows Components page	Enabled
Hide the "Add a program from CD-ROM or floppy disk" option	Enabled
Hide the "Add programs from Microsoft" option	Enabled

We want to ensure that the remote users cannot make unauthorized changes to their network and remote access settings.

User Configuration | Administrative Templates | Network | Network and Dial-up Connections	
Prohibit deletion of RAS connections	Enabled
Prohibit access to the Network Connection wizard	Enabled

There are many more settings in this folder, but many of them will not affect non-administrators anyway since they are already restricted in their access to network and dialup configurations.

Since these users connect over a variety of connections (DSL, cable modem, dialup), we need to enable the "Slow link detection" setting. If a slow link is detected, some aspects of group policy are not applied. We have set the slow link setting to be 128 K or less. This setting and other related settings are configured in 'Computer Configuration | Administrative Templates | System | Group Policy.' In addition, we need to configure slow link detection for User Configuration settings, 'User Configuration | Administrative Templates | System | Group Policy.' See Microsoft Knowledge base articles Q227260 and Q227369 for more information about which settings can be adjusted for slow links.

We can use the Office Resource Kit templates for this GPO as well to secure Outlook.

User Configuration | Administrative Templates | Microsoft Outlook 2002 | Tools - Options | Security	
Prevent users from customizing attachment security settings	Enabled
Allow access to e-mail attachments	Enabled (In addition to enabling this setting, the allowed extensions must be listed: for example, DOC, XLS, TXT)

User Configuration | Administrative Templates | Microsoft Outlook 2002 | Miscellaneous	
Prevent users from adding HTTP e-mail accounts	Enabled

Users are prevented from changing the security settings on attachments and are restricted in the types of attachments they can receive. In addition, users are restricted from adding HTTP email accounts to their Outlook clients; they cannot get their Hotmail, for example, in their Outlook client.

One thing that cannot be enforced with group policies is the use of the encrypting file system (EFS). Since laptops are at a great risk of being stolen, we would like to utilize EFS for additional data security. We cannot configure it with group policy, but we can set up encrypted folders when the computer is being configured so that the contents placed in these folders will be encrypted.

CONCLUSIONS

We have noted a few cases in the discussion of the group policies where we cannot use group policies to secure the network. We cannot force the use of the encrypting file system. We can set prohibit users from changing our designated security levels for Internet Explorer and Outlook and we can even specify the types of email attachments users can open (.doc, .xls, etc)

To further secure the GIAC Enterprises network, we have to utilize other features of Windows 2000 or third-party products. One thing that would be nice to do with group policies is to reset some of the file type associations, like .vbs, so that they will not automatically run, but would open in notepad, for example. There does not appear to be a way to set this in group policy, but we can script a registry change that will enforce this setting on workstations. In addition, we will need to purchase antivirus software for the mail servers, file servers and workstations and keep it updated.

It would also be nice to force the administrator accounts to have longer passwords and to change them more frequently. However, this setting is controlled by the domain policy and we do not want to force those settings on all users. So we will have to rely on the administrators themselves to make these changes.

REFERENCES

Cox, Philip. "Hardening Windows 2000." (version 1.0, 20 Mar 2001). URL: http://www.systemexperts.com/tutors/HardenW2K101.pdf (24 Sept 2001).

Cox, Philip and Tom Sheldon. Windows 2000 Security Handbook. Berkeley, CA: Osborne/McGraw-Hill, 2001.

Haney, Julie M. "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." (version 1.0, May 17, 2001) URL: http://nsa2.www.conxion.com/win2k/download.htm (24 Sept 2001)
* Part of the National Security Agency's Windows 2000 Security guides

Mar-Elia, Darren and Sean Daily. "The Definitive Guide to Windows 2000 Group Policy." URL: http://www.fullarmor.com/ebook/read (26 July 2001). Note: Registration is required but access to the e-book is free.

Lowe-Norris, Alistair G. Windows 2000 Active Directory. Sebastopol, CA: O'Reilly, 2000.

MCSE Training Kit: Microsoft Windows 2000 Active Directory Services. Redmond: Microsoft Press, 2000.

Minasi, Mark, Christa Anderson, Brian M. Smith, and Doug Toombs. Mastering Windows 2000 Server. 3rd ed. San Francisco: Sybex, 2001.

Opitz, David. "Guide to Windows 2000 Kerberos Settings." (version 1.1, updated June 27, 2001) URL: http://nsa2.www.conxion.com/win2k/download.htm (24 Sept 2001)
* Part of the National Security Agency's Windows 2000 Security guides

Securing Windows 2000 Step by Step: A consensus document by security professionals from dozens of user organizations. Preliminary Edition. Version 1.0c. SANS Institute, May 20, 2001.

Windows 2000 Server Resource Kit, Supplement 1. Redmond: Microsoft Press, 2001.