Global Information Assurance Certification Paper

A Secure Windows 2000 Infrastructure for GIAC Enterprises

GCNT Practical Assignment
Version 3.0

Author: Harpal Parmar

Date: May 5, 2002

Table of Contents

Introduction

GIAC Enterprises was founded by three university students who saw a need for fortune cookie manufacturers to have the ability to automate the generation of new fortunes for their cookies. They have become quite successful in this field, having eight of the world's leading fortune cookie manufacturers as clients. The three developers started off in their garage developing the software themselves. They did so on individual workstations running on a peer to peer network. They have recently received funding to go online, with verbal agreements from their clients to purchase new fortunes from GIAC online.

Historically, GIAC Enterprises developed software to print fortune cookies, including a database of fortunes which was included with the install cd. They are now in a position where their existing customers are demanding new fortunes for their cookies. GIAC Enterprises has begun an aggressive sales and marketing campaign to sell the software, which has the distinct advantage over its competition, giving them the ability to download new fortunes for a fee from the GIAC internet site. They hired an external contractor to set up the web delivery system which is already in place. They have acquired and built office space on one floor of a five story professional building in Maui. GIAC was fortunate as the office space they moved into used to house an e-business which sold insults over the internet for a fee. They went under. The office space however was ideal, as it contained a climate controlled, physically secure computer room equipped with a fire suppression system as well as a UPS. GIAC also purchased all of the computers that belonged to the previous tenant at a fraction of what they were actually worth.

GIAC Enterprises has hired several employees in anticipation of their growth. GIAC consists of the following departments:

Research & Development

This department consists of sixteen people. There are ten developers who build and improve upon our software, and six people whose job it is to come up with innovative new fortunes which we can sell to our clients. Ironically, three of these people were the biggest clients of the e-insult business and were greatly saddened when they went under. The three original developers of the software are in this group, and they also double as the executive team – the CEO, CIO and CFO.

Sales & Marketing

This department consists of nine people. There are six Account Reps who take care of the existing client base, as well as look aggressively for new customers. There are three people who man the helpdesk, which takes calls from the clients. These people will troubleshoot any issues with the clients, and also train them on the use of the software.

Finance & Human Resources

This department consists of four people. There are three Accounting types who look after the Accounts Payable and Accounts Receivable as well as payroll, and one person who looks after HR functions.

Information Systems

This department consists of three people. Together they look after the entire IT infrastructure of the company.

Despite the different departments, GIAC is a small startup with a fairly flat structure.

Network Design

All of the equipment on the network from the routers and firewalls all the way down to the workstations were purchased from the previous tenant. All of the servers on the GIAC Enterprises network reside in the secure computer room. The previous tenant standardized all of their servers. The servers consist of Dell Power Edge 2500's. They have dual 1 GHz processors and 1Gig of RAM. They also all have four 36 GB disks in a Raid 5 configuration. While this may be overkill for some of our servers, we won't worry too much about it since we bought them for practically nothing.

All Windows based machines on the network are running Norton Antivirus Corporate Edition. The machines on the internal network have the updates pushed to them from two Norton Management servers. The machines in the DMZs get their updates from the Norton Update sites on the internet.

All of the disks in the computers purchased from the previous tenant were wiped clean. We have decided on Windows 2000 as our platform for both servers and workstations. We will build all the machines from scratch, and will patch them all up to the current patch levels.

All servers on the DMZs have been hardened in accordance with the Windows 2000 Guides available from the NSA.

Going forward, the HFNetchk utility will be run on a weekly basis to ensure that all servers are up to date on patches. HFNetchk is a valuable tool for the Windows Administrator as it saves time by scanning remote machines for patch levels and listing the patches the system is missing. HFNetchk is a Microsoft utility available for free at:

> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp

HFNetchk checks for currency of patches for the following products:

Windows NT 4.0
Windows 2000
All system services, including Internet Information Server 4.0 and 5.0
SQL Server 7.0 and 2000 (including Microsoft Data Engine)
Internet Explorer 5.01 and later
(Microsoft Corporation, Microsoft's HFNETCHK Patch Status Utility)

The workstation patches will be applied via Group Policy.

The network is shown in Figure 1 below:

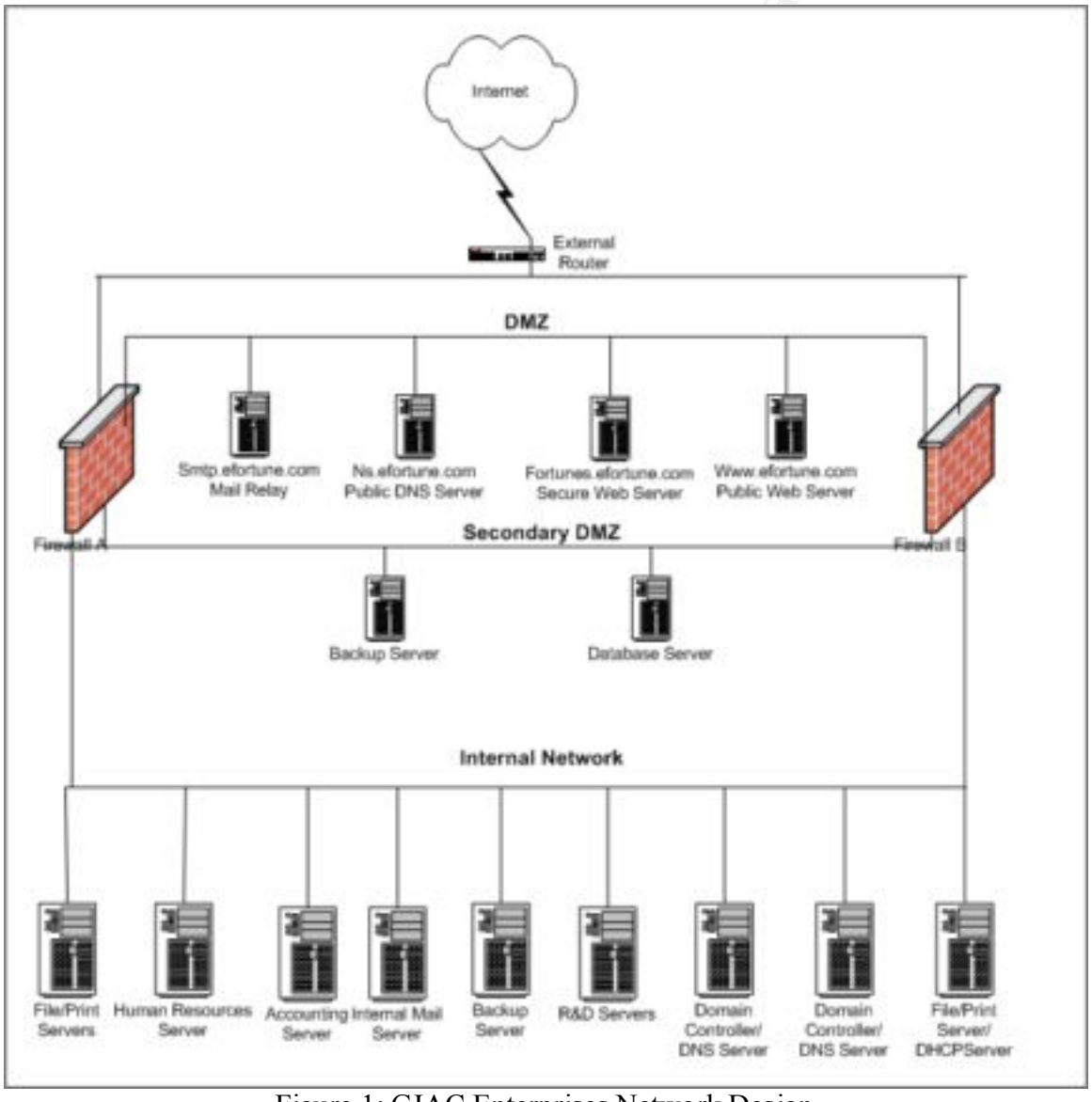


Figure 1: GIAC Enterprises Network Design

External Router

The external router is a Cisco 2600 series router. The router serves as an interface to our internet connection which is currently a T1. There was talk of having a redundant internet link but, due to financial constraints, this plan was put on the backburner for the time being. The router itself was configured by the IT group and secured according to the NSA's Router Security Configuration Guide available at:

http://nsa2.www.conxion.com/cisco/download.htm

Firewalls

There are currently two redundant, load balancing Checkpoint stateful inspection firewalls. They are running Checkpoint VPN 1 version 4.1 with strong encryption. Although not shown in the network diagram, there is a management server which controls the two firewalls. It is located on a protected interface on the firewalls, with access allowed only from the Network Administrators workstations. There is also a heartbeat line between the two firewalls to replicate the state information. The firewalls currently reside on two hardened Sun Ultra 60s. The firewalls block anything that is not explicitly allowed.

DMZ

"A Demilitarized Zone (DMZ) is a small isolated network logically positioned between the protected network and the internet. Isolating the DMZ from the Protected Network provides a layer of defense from attacks launched from compromised public servers." (Bartock *et al.*, pg 4) This network is where all of GIAC Enterprises publicly accessible servers reside. GIAC has registered the efortune.com domain, and all publicly accessible servers will be named accordingly.

External Mail Server (smtp.efortune.com)

The external mail server acts as a relay for incoming and outgoing email for GIAC Enterprises. All incoming and outgoing email is scanned for malicious code.
It is set up so it only relays email to and from GIAC Enterprises.

This server was placed in the DMZ because it needs to be accessible from the internet.

External DNS Server (ns.efortune.com)

The external DNS is for public use. Only information which needs to be advertised to the internet is included on this server. It is the primary DNS server for the publicly accessible domain efortune.com.

This server was placed in the DMZ because it needs to be accessible from the internet.

Secure Web Server (fortunes.efortune.com)

The secure web which allows clients to get new fortunes via the software they have purchased is running IIS 5.0. It has already been setup by a local firm specializing in e-business and security, and is currently in production. The necessary security precautions have been taken during the building of the server. A security audit was performed on the entire delivery system by an accredited third party auditing firm.

The web server utilizes digital certificates to allow for external communications with the clients. The firewalls only allow communications from the existing client's NAT'd ip address space to port 443 for SSL encrypted http sessions. This is done to limit the exposure of the server to the hacker population out on the internet. The certificates are couriered to the client along with the install cd of the software. The software then allows the client to log onto the website and view or download new fortunes into their local database for printing and further processing. The secure web server communicates with a database server which resides in the Secondary DMZ.

This server was placed in the DMZ because it needs to be accessible from the internet.

Public Web Server (www.efortune.com)

The public web server is running IIS 5.0 and has been setup by the same local firm that built the secure web server. It was also audited by the same third party that audited the secure web server. This server's primary function is to provide information about our software to the general fortune cookie community out on the internet. There is contact information for the Sales and Marketing department for anybody interested in a demo or purchase of our software.

This server was placed in the DMZ because it needs to be accessible from the internet.

Secondary DMZ

GIAC Enterprises has another DMZ network. This network has no direct access to or from the internet. This DMZ houses a database server and a backup server. The database server is where the online fortunes actually reside. The secure web server (fortunes.efortune.com) does lookups of the fortunes on this database. The firewalls block all access to and from this server except for the sqlnet port (1521/tcp), as the server is running an Oracle database. The R&D department updates this database with new fortunes as required.

This server was placed in the Secondary DMZ because it needs to be more protected from internet threats than the web servers. If the web server gets hacked, the attacker would not have wide open access to the database where our fortunes reside.

Internal Network

The internal network consists of all of the servers and workstations that are not accessible from the internet. Since GIAC Enterprises is a small company, we will have only one physical network. We will control the security mainly through Active Directory (AD) and Group Policy. Once again, all the systems are running Windows 2000 and HFNetchk is used to ensure that patches are up to date.

DHCP Server

The DHCP server is responsible for assigning IP addresses dynamically to the workstations on the internal network. We will bundle this service on top of one of the general file servers. We will use the DHCP server to disable Netbios over TCP/IP for all of our machines. Windows 2000 doesn't require the use of Netbios, providing it is running in native mode.

This server was placed on the internal network because it serves the internal users and should be protected from the internet.

Domain Controllers

The Domain Controllers (DCs) will also act as DNS servers for the internal network. This internal DNS server is for the internal corp.giac.com domain. The DNS servers only contain information about the internal network, and are not accessible from the internet. DNS will be Active Directory integrated, providing multi master replication and allowing us to add security.

There are two Domain Controllers/DNS servers for corp.giac.com. This is done to address the need for redundancy. We will use the dcpromo utility to make them domain controllers. We will configure them with the Active Directory database and log files on two separate partitions. Since our environment doesn't require compatibility with non Windows 2000 servers, we will not select the "Permissions compatible with pre-Windows 2000 servers". We will also set these servers to run in native mode for the same reason.

These servers were placed on the internal network because they serve the internal users and should be protected from the internet.

Internal Mail Server

The internal mail server is running Exchange 2000. This server provides email services for the internal users. It is configured to forward all outgoing mail to the external mail server, which forwards it to its ultimate destination. The server is running Norton Antivirus for Exchange, and scans the messages for any malicious code.

This server was placed on the internal network because it serves the internal users and should be protected from the internet.

File/Print Servers

These servers provide general file and printer sharing capabilities to the internal users. They are shared by the various departments.

These servers were placed on the internal network because they serve the internal users and should be protected from the internet.

Backup Server

This server handles all the backups for the internal network. It is running Veritas Netbackup, and is configured to do differential backups nightly and full backups on the weekend of all the servers.

This server was placed on the internal network because it serves the internal users and should be protected from the internet.

R&D Servers

These servers are for use by the R&D department. They are used to store data, applications, the repository and to compile code.

These servers were placed on the internal network because they serve the internal users and should be protected from the internet.

Human Resources and Accounting Servers

These servers are for the exclusive use of the Finance & Human Resources departments. They house the Accounting and HR databases. The department employees maintain these databases through a client/server application developed by a popular vendor. The application encrypts and authenticates all data that traverses the network.

These servers were placed on the internal network because they serve the internal users and should be protected from the internet.

Active Directory Design

In today's computer environments, there are many resources scattered over the network. It can be difficult to manage the relationships and security of various workstations, users and groups, printers, file shares and many others. A directory service offers the location where to store these various properties of network objects. It defines the structure of what information is stored and how this information is stored. It also defines the rules for requesting information from the database and what you can do with the answers to these

requests, as well as adding new information to the database. Utilizing a directory service will provide us with a consistent method in which to store and access information about distributed network resources. As an example, you may want to know which printers are available to you on the network, so you would query the directory service for this information and it would return to you a list of printers. Some examples of directory services in use today include NIS in UNIX, Novell's NDS and IBM's Lotus Notes.

The most common protocol used to query and edit directory services is the Lightweight Directory Access Protocol (LDAP). LDAP runs on tcp port 389 by default, and is the *de facto* standard. It is defined in RFC 2251, available at:

http://www.ietf.org/rfc/rfc2251.txt.

Active Directory is Microsoft's implementation of a directory service. It is a structured database of objects which is replicated throughout various parts of an organization. It can be used to manage various objects on the network. AD contains information about numerous things including Distributed File System shared folders, trust relationships, computer properties, groups, organizational units, printers and a great deal more. You can even define your own custom object, which can potentially help address the unique needs of an organization.

The structure of the AD database is defined by the Schema. The Schema defines objects and their attributes which can be stored in AD. AD includes uniquely named objects which represent network resources such as computers or users. These leaf objects can be located inside Container objects in order to better organize AD. This can be done in a hierarchical manner to make it easier to understand. An Organizational Unit (OU) is a common Container.

Active Directory can be broken down into three main sections known as "Naming Contexts": The Schema Naming Context, The Configuration Naming Context and the Domain Naming context.

Schema Naming Context

The Schema Naming Context is the section that defines the structure of the AD database, and this schema information is replicated throughout an organization. The Schema can be modified if required. For example, we may want to add additional attributes to an object. We may want to include Cell Numbers for the IT Department in the Global Catalog. Global Catalog is a part of the Active Directory database which is replicated between joined domains via special DCs called Global Catalog Servers. Each site requires at least one GC server, and since bandwidth is not an issue as our domain resides on the same LAN, each Domain Controller, with the exception of the one running Infrastructure Master FSMO role, will also act as a Global Catalog server. Adding attributes to the Global Catalog involves modifying the Schema.

The Schema can be modified using ADSI scripts or by using the Schema Manager snap-in in the Microsoft Management Console (MMC). It is important to note that changes to the schema are permanent, you can not reverse them. In order to make the changes, there are a few steps which must be taken. First we must enable Schema Modifications on the FSMO Schema master.

FSMO stands for Flexible Single Master Operation, and there are certain services which run in FSMO mode. These services are not well suited for the multi-master replication of AD. A Domain Controller which runs a FSMO service is referred to as the FSMO Master of that service. There are five FSMO masters, all of which will by default be assigned to the first Domain Controller in the first domain.

1) The PDC Emulator Master operates as a Windows NT Primary Domain Controller for backwards compatibility. It will perform the functions of a PDC (e.g. process password changes, replicate to the Backup Domain Controllers (BDC)). If a user attempts a logon with an incorrect password at another DC, it will then be passed to the PDC Emulator for authentication.

2) The RID master is responsible for allocating Relative Identifiers (RID) to each Domain Controller in the domain. When a DC creates a computer object, group or user, it has to assign a unique identifier for each object. The RID is part of this unique identifier, and the DC requests a pool of RIDs from the RID master which it then assigns to the objects.

3) The Infrastructure Master is responsible for updating inter-domain references. Objects in one domain can be referenced in another domain. If the object gets modified or moved in another domain, the Infrastructure Master updates the reference so it knows the modifications made, or the new location of the object.

4) The Schema Master is the only system which can modify the AD Schema. Therefore, if we want to modify the Schema, we need to have access to the Schema Master.

5) The Domain Naming Master is the system which controls whether a domain can be added or removed from the forest.

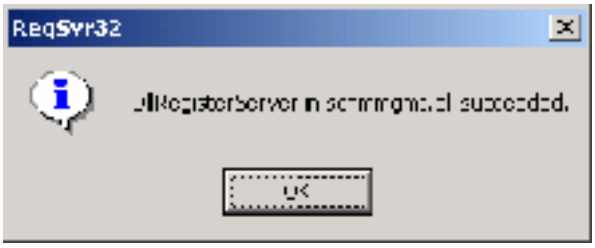
There can be only one Schema Master and one Domain Naming Master in a forest. There can be only one RID Master, one PDC Emulator Master and one Infrastructure Master in a domain.

At GIAC, we will assign the RID Master and PDC Emulator Master roles to the same Domain Controller, and the Infrastructure Master Role to another DC. The Schema Master and Domain Naming Master need to be strongly secured in both a physical sense and an electronic sense. We will ensure both of these roles are assigned to the same DC.

Before we can install the Schema Manager snap-in, we need to register the DLL. This can be done by opening a command prompt and executing the following command:

regsvr32.exe schmmgmt.dll

Once we execute this command, we see the following message:



In order to modify the Schema, you must be a member of the Schema Admins group. By default, the Administrator is a member of the Schema Admins group. We can add the Active Directory Schema snap-in in the MMC, and then make our modifications utilizing this snap-in.

Since the changes to the Schema are irreversible, we will remove all users in the Schema Admins group to prevent any unauthorized or accidental attempts to modify the schema. Since the schema is rarely modified, we will temporarily add the Administrator account to the Schema Admins group only while making the modification, and remove it once the change is complete. We will also audit changes to the Schema Admins group. This will alert us to any unauthorized attempts to modify the schema.

We can enable Schema Modification on the FSMO Schema Master by right clicking on the Schema Manager snap-in and selecting Operations Master. There is a check box called "The Schema may be modified on this Domain Controller" which, when selected, will enable this functionality.

Configuration Naming Context

"The Configuration Naming Context holds information about sites, subnets, replication transports, trusts, and configuration data for the File Replication Service, the Active Directory Service, and other services." (Fossen, pg. 48) The replication of AD revolves around sites, which are typically a set of computers on a LAN or on subnets connected via a high speed link.

Sites reflect the physical structure of the network, as opposed to domains which reflect more the logical structure. A site may have multiple domains and a domain may be in multiple sites.

We can define site information like subnets and inter site transports. This information is used by AD to determine the best way to use the available network resources. For

example, when a user logs onto a domain, AD will search for a DC in the same site. Since systems in the site are connected via fast network connections, authenticating to a DC on the same site improves the efficiency resulting in a faster logon process than if we were authenticating to a remote DC.

Replication of AD within a site, or Intrasite Replication, is set up by default by the Knowledge Consistency Checker service. The KCC will set up the replication to occur automatically and frequently. The first Domain Controller installed will set up a site called Default First Site. Any additional DCs will be automatically added to the same site as the original DC, but can be removed manually later.

This site information can be viewed and modified using the Active Directory Sites and Services snap-in in the MMC. At GIAC Enterprises, we will have only one Site. We will rename the Default First Site to "Maui".

If we had more than one site, we would set up Intersite Replication which has to be set up manually through the use of Intersite Transports. These Intersite Transports are what Domain Controllers in different sites use to replicate AD. There are two types of Intersite Transports, IP and SMTP. The IP transports make use of RPC over IP, and are typically used when there is a fast and reliable link between sites. The SMTP transports utilize email to replicate AD, and are typically used when reliable links are not available, or as a backup to IP transports. SMTP transports are only available if the sites are in different domains. SMTP transports also require that the IIS SMTP service is installed on the DCs, and they must also have access to Windows 2000 Enterprise Certifications Authority to request a Domain Controller certificate. This is necessary since the SMTP data is encrypted.

Domain Naming Context

The Domain Naming Context contains the information about Domains and Organizational Units. This includes things like users, groups, computer accounts and group memberships.

Although it is not a requirement, Windows 2000 domains should be named following the DNS naming conventions in order to make things simpler. Naming our domain to follow the DNS standards will make it easier to map to email addresses and DNS zones of authority.

When designing our physical network, we have tried to keep things as simple as possible. We want to continue following this path when we plan our Active Directory design. Domains are replication boundaries, so a valid reason for creating multiple domains is to control replication traffic. Our environment at GIAC Enterprises is a small one, hence we will keep it simple and have only one domain. This follows recommendations put forth by Microsoft:

> *"keep in mind that for many organizations, a structure consisting of one domain that is simultaneously one forest consisting of one tree is not only possible, but may be the optimal way to organize your network. Always begin with the simplest structure and add complexity only when you can justify doing so."*
> (Microsoft Corporation, Active Directory Whitepaper, pg. 24)

The first Windows 2000 domain to be installed becomes the root domain. This domain cannot be removed, or joined to any other domain. The root domain sets the Schema and Configuration Naming Contexts, which will be replicated to all other domains that join the forest. This domain also will be the only one in the forest to have the built in Schema Admins group, and the Enterprise Admin Group. The Enterprise Admins group is added to the local Administrators group of every computer belonging to any domain that joins the root domain.

A tree consists of multiple domains that share a parent-child relationship. An example of a tree would be cisco.com and sanjose.cisco.com where cisco.com is the parent, and sanjose.cisco.com is the child. The Schema, Configuration Naming Context and Global Catalog are replicated throughout the tree, but the Domain Naming Context information is only shared among DCs in the same domain.

A forest is multiple domains where there is no parent-child relationship. They still replicate the Schema, Configuration Naming Context and Global Catalog, and must have a Windows 2000 root domain. The first domain installed in the forest will be the windows 2000 root domain.

GIAC Enterprises will consist of one domain, corp.giac.com. This will be the Windows 2000 root domain. It will be installed as a new forest, and will define the Schema and Configuration Naming Context for itself and any domains that join it in the future, whether they are joining the forest or a tree.

GIAC Enterprises is small, with no immediate plans of branching out and requiring multiple domains. However, if this does happen, we want Maui to be Headquarters. We would want corp.giac.com to be the root domain, as we would likely want some degree of administrative control over the other offices.

Organizational Units

Organizational Units (OUs) are container objects in which we can place other objects. The objects we can place in an OU are users, groups, computers, printers, and shared folders. We can also have nested OUs, provided they are from the same domain. We will avoid having many levels of nested OUs as this will slow down the processing of Group Policy.

An OU's main function revolves around security and delegation of authority. OUs should be designed around the differing needs throughout the organization with respect to security and delegation. The Group Policies we will create are going to be applied to the

OUs we create now. We will keep this in mind when designing our Active Directory structure.
There are some default objects created in AD, namely the Builtin, Computers and Users folders. Once we build our OUs, we will move the objects from these default folders into the OUs we create. If we want to delegate control to an OU in the future, it will be nice to have objects organized into their own OU, as the Delegation of Control wizard cannot be used on the Builtin folder.

We've decided to organize the Active Directory structure as outlined in Figure 2 below:

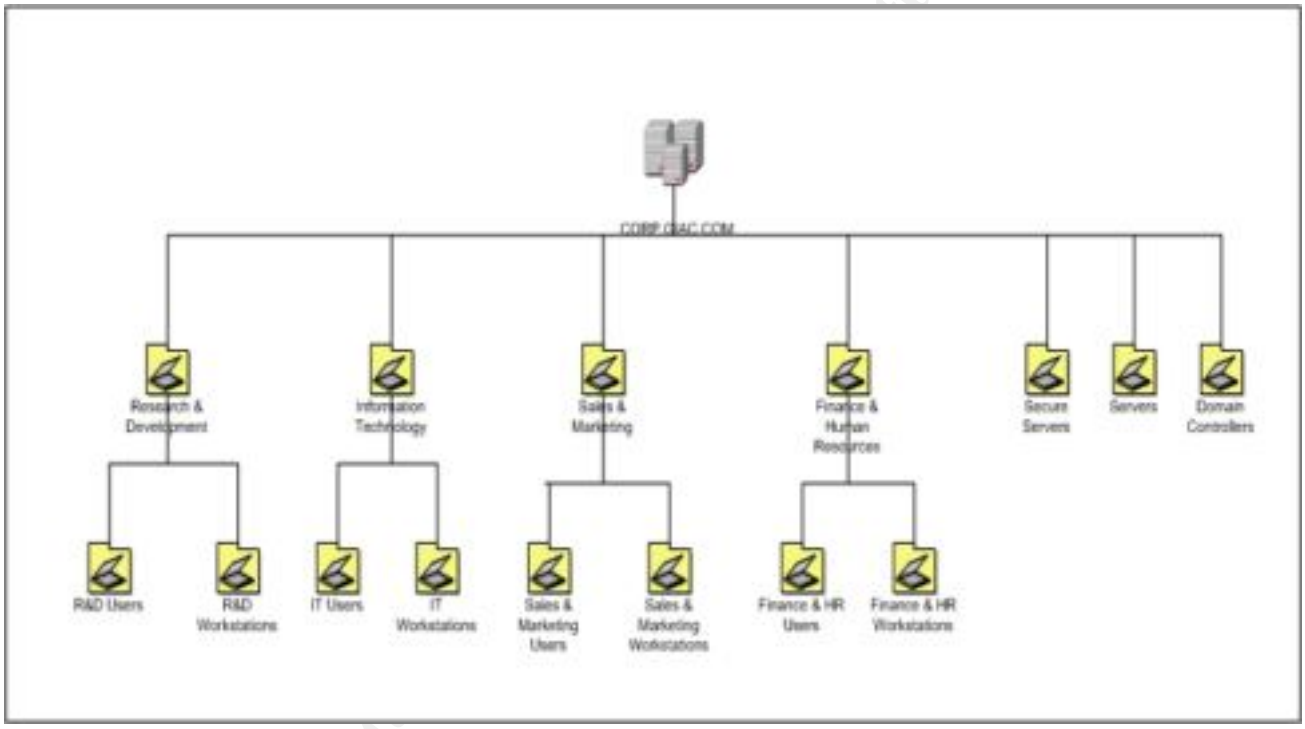


Figure 2: Corp.giac.com Active Directory Design

The domain of corp.giac.com consists of several Organizational Units and some nested OUs. The default domain policy will be applied across the entire domain, and Group Policies will be applied as indicated below.

In order to satisfy the differing security requirements for the different types of servers, we broke them down into the following OUs:

Domain Controllers

This OU contains the two Domain Controllers on our network. There will be a Group Policy applied to this organizational unit based on the settings recommended by the NSA. The domain controllers are in their own OU because they need to have different audit and security features. The Domain Controllers should be better protected than most servers. If an attacker were to gain control of a Domain Controller, and modify some Active

Directory settings, this change would be propagated to all the other Domain Controllers. For example, an attacker might change the permissions on a share which contained sensitive information, allowing everyone access to it.

Servers

This OU contains general purpose servers including the R&D servers, general file and print servers which are shared by the various departments, email servers and backup servers. These servers have different audit and security needs than the Domain Controllers.

Secure Servers

This OU contains the HR and Accounting servers. These have special similar security requirements.

We've decided to have an OU for each department. Although these departments don't all have differing security requirements, we've done this to make the management of Group Policy a little easier.

In each group, Research & Development, Sales & Marketing, IT and Finance & Human Resources, there are nested OUs. These OUs represent the Users in the various departments, and the Workstations in the various departments. The policies will be applied to the User OU and the Workstations OU. The reason we do this is because although the same group policy will be applied to both OUs, we will apply only the Computer Configuration settings to the Workstations OU, and the User Configuration settings only to the Users OU. This should also help performance, since we are only applying the portions of the policy that are needed.

We could potentially exclude a certain user or group from having a Group Policy applied to it if we had the need to. In order to have a Group Policy applied to his desktop, a user must have at least the Read and Apply Group Policy permissions. We could assign Deny Read and Deny Apply Group Policy to users or groups we want to make exempt from the Group Policy.

There will be two different Group Policies applied to the workstations:

General Group Policy

The General Group Policy will be applied to the Users and Workstations OUs for the IT department and the R&D department. Employees of these two groups have similar requirements. For example they both need the ability to install software on their local machines, whereas someone in the Finance&HR group does not.

Secure Group Policy

This group policy will be applied to the Users and Workstations OUs for the Sales&Marketing department and the Finance&HR department. Employees of these two groups have similar security requirements, which are more stringent than what is required for IT and R&D. The Secure Group Policy settings will be more stringent than the General Group Policy to address these requirements.

The design we have chosen for Active Directory addresses our immediate needs, and paves the way for any future growth. In the near future, we will look at delegating control over the users in the R&D group to someone in the R&D department. This will allow them to manage their own user accounts and groups, which will reduce the strain placed on the IT department.

Group Policy

Group Policy in Windows 2000 stems from the Security Configuration Editor and System Policy from Windows NT 4.0. We can utilize Group Policy to control various computer and user settings across our network, which gives us greater control over the activities of our users and enhanced security. There are many settings which can be used to do everything from changing NTFS permissions and auditing to changing registry values. We can set user rights, password policies, IPSEC and PKI policies, set which services may run, and assign startup and shutdown scripts. We can use Group Policy to set workstations to automatically install programs, which can be very useful when a patch comes out to address a serious security vulnerability.

Another useful function is the management of users' desktops. We can set various aspects of this including disabling some components of Control Panel, such as add/remove programs. This setting is useful as it helps prevent users from installing software which may contain malicious code. We can also use Group Policy to enable password protected screen savers which lock the screen on every computer in our organization after a certain period of inactivity. The settings described above are only the tip of the iceberg, there are many things we can do with Group Policy as we will see. In short, Group Policy will be a great tool to help us enforce our corporate policies and standards throughout our organization.

The Group Policy settings can be viewed and modified from the Group Policy Editor, a Microsoft Management Console snap-in. Group Policy is divided into two major categories, Computer Configuration and User Configuration. These sections consist of various settings we can modify, which will be applied when a computer is powered up or when a user logs in. They can also be applied at a configurable scheduled interval.

We can also manually refresh the policies using the command line secedit tool. The refreshpolicy option can be used to reapply the GPO security settings. It can be used to reapply the Computer settings or the User settings. The syntax of the command is as follows:

secedit /refreshpolicy {machine_policy | user_policy}[/enforce]

The enforce option will refresh the security settings even if the Group Policy Objects have not changed.

The secedit tool is a command line version of the Security Configuration and Analysis snap-in, therefore we can also use it to audit the security settings on machines. We can use the analyze option to do this. We can even put this into a batchfile and have it run periodically so we know if any of the settings are not compliant with our security policy. The syntax is as follows:

secedit /analyze [/DB *filename*] [/CFG *filename*] [/log *logpath*] [/verbose] [/quiet]

Group Policy Objects are created and then can be linked to Sites, Domains or Organizational Units. At GIAC Enterprises, we will create GPOs and link them to multiple OUs as described in the Active Directory Design section above. Any changes made to the GPOs will be received automatically by the OUs linked to it. Doing it this way reduces administration.

Security templates can be utilized to initially configure the security settings of a Group Policy Object. These templates determine the security setting options available and what their default settings are. These templates are available from vendors, and it is easier to start with one of these templates and modify them to fit our environment, than to create our own. We will make use of the templates that the National Security Agency has available for download, and customize them to suit our environment. These templates are available at:

http://nsa2.www.conxion.com/win2k/download.htm

The order in which Group Policies are applied is important as they are applied cumulatively, that is, a GPO applied to the domain will overwrite a setting defined in a GPO applied to a site. Subsequently a GPO applied to an OU will overwrite a setting defined in a GPO applied to a domain. The GPOs are applied in the following order:

- Local GPO
- Site GPO
- Domain GPO
- Organizational Unit GPO
- Child Organizational Unit GPO

This order can be modified by utilizing the Block Inheritance or No Override options. The Block Inheritance option disables a child container from having the GPOs of higher level Containers applied to it. You can only block all GPOs from being inherited, it is not granular. The No Override option prevents lower level containers from overriding the GPO. If there is a No Override option set on an OU, and there is a Block Inheritance option set on a child OU, the No Override option prevails.

These options should not be used unless absolutely necessary, as it will make troubleshooting of GPOs difficult. That being said, we will utilize the No Override option on our Default Domain Policy. Since this policy is domain wide, we need to enforce it as such. We do not want the OUs to have the ability to override this policy as it contains important settings such as Password Policies, Account Lockout Policies, etc.

Much of the Group Policy design is based upon the recommendations put forth by the NSA, specifically "Guide to Securing Microsoft Windows 2000 Active Directory", "Guide to Securing Microsoft Windows 2000 Group Policy" and "Guide to Securing Windows 2000 Group Policy: Security Configuration Toolset". These guides are available at:

http://nsa2.www.conxion.com/win2k/download.htm.

We have decided to use the available NSA security templates in our Group Policies. We will utilize the following templates. These templates are described in the NSA's "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset" (Table 1). As previously stated, we will customize them to suit our environment and needs.

Template Name	Platform	Description
W2k_dc.inf	Windows 2000 Server/Advanced Server Domain Controller	Enhanced security settings For Windows 2000 Domain Controllers
W2k_workstation.inf	Windows 20000 Professional	Enhanced security settings For Windows 2000 Workstations
W2k_server.inf	Windows 2000 Server/Advanced Server	Enhanced security settings for Windows 2000 Member or Standalone server
W2k_domain_policy.inf	Windows 2000 Domain	Enhanced Account Policy settings To be applied in a domain-level Group Policy Object

Table 1: NSA Enhanced Security Configuration Files
(Haney, NSA Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset, pg 19)

We will take a staged approach, applying security templates one at a time and testing to ensure there were no ill effects as a result of the changes before we proceed with more changes. Most security settings can be restored by using the default "setup security.inf" file. This is the template applied with a default install of the OS and is stored in %SystemRoot%\security\templates. Note that any settings that are specified as "Not Defined" in the template will not reverse changes made by the NSA templates. We will copy the NSA templates and rename them (e.g. GIAC-DomainPolicy.inf) before we modify or apply them. We will also make backups of all of our systems before proceeding.

The modifications to the templates will be done utilizing the Security Templates snap-in in the Microsoft Management Console.

Default Domain Policy

The Default Domain GPO will be used to set some important domain wide settings. This helps us to enforce our corporate security policy throughout our domain.

Properly set Account Policies are an integral component of controlling security. Below are some of the important domain wide settings we will enforce.

We will begin by copying the NSA's w2k_domain_policy.inf to GIAC-DomainPolicy.inf. We can then begin to customize it to meet our requirements.

Password Policy

Passwords are an integral part of security as they are in many cases the only thing preventing an attacker from gaining access to a system. Therefore protecting passwords becomes very important. One method of protecting passwords is changing them frequently. If an attacker did get her hands on the encrypted password hash, we want to make it difficult for her to decrypt those hashes. Windows 2000 provides some important mechanisms to enforce our passwords through Group Policy. Below are some of the settings we want to enforce domain wide.

Enforce Password History

This setting determines the number of password changes that have to occur for a given user account before a password can be reused. This helps prevent a user from reusing their favorite passwords. Reusing the same password defeats the purpose of requiring password changes in the first place. The default value in the NSA template is 24, which is an acceptable value in our environment.

Maximum Password Age

This setting determines the maximum number of days an account may have the same password. This setting forces the users to change passwords frequently. If an attacker did manage to get the password, if it is changed frequently, the damage may be reduced. The default value in the NSA template is 90, which is an acceptable value in our environment.

Minimum Password Age

This setting determines the minimum number of days an account must have the same password. This setting helps to discourage users from reusing their favorite passwords. By default, a user can change his password as often as he likes, there is no limit. This setting, in conjunction with the "Enforce Password History" setting, will make it much more difficult for the user. If the user can change the password as often as he likes, there

is nothing to stop him from cycling through a bunch of passwords if he really wants to reuse his favorite password. If he has to wait one day between password changes, he will have to change the password every day for 24 days before he would be allowed to arrive at the same password. This would likely cause most users not to bother with it, and just use a new password. The default value in the NSA template is 1 day, which is an acceptable value in our environment.

Minimum Password Length

This setting determines the minimum amount of characters the password must contain. This setting can be used to prevent the use of blank passwords and shorter passwords. Since each additional character increases the possible combinations exponentially, a longer password will be harder to crack. The default value in the NSA template is 12. This value makes for a very long password for the users to remember. The users have expressed some concern about this, so although having 12 characters in the password is nice from a security standpoint, we must find a balance between security and functionality. Therefore, we will modify this setting to 8 characters.

Passwords Must Meet Complexity Requirements

This setting enforces strong password requirements. By utilizing the passfilt.dll dynamic link library, we can force a user to choose a password which has a minimum level of complexity to it. Each additional component increases the possible combinations that an attacker will have to try and guess exponentially. This helps to defend against brute force and dictionary password guessing attacks. The following is a description of what passfilt.dll requires to meet password complexity:

> *The default password filter (passfilt.dll) included with Windows 2000 requires that a password:*
>
> *- Does not contain all or part of the user's account name*
> *- Is at least six characters in length*
> *- Contains characters from three of the following four categories:*
> *- English upper case characters (A..Z)*
> *- English lower case characters (a..z)*
> *- Base 10 digits (0..9)*
> *- Nonalphanumeric (For example, !,$#,%)*
>
> *Complexity requirements are enforced upon password change or creation.*
(Microsoft Corporation, Resource Kit Supplement:1 Group Policy Reference)

The default value in the NSA template is enabled, which is the value we will use in our environment.

Store password using reversible encryption for all users in the domain

This setting allows you to store passwords on the system using encryption which is reversible. This option is available to support applications which use the password for authentication. Enabling this option would result in security essentially equivalent to storing the password in clear text. The default value in the NSA template is disabled, which is the value we will use in our environment.

Account Lockout Policy

The Account Lockout Policy allows us to counter brute force and dictionary attacks by making it difficult for an attacker to repeatedly attempt to logon. After a configurable amount of failed logon attempts, we can disable the account for a period of time. If an attacker must wait fifteen minutes before attempting to try the next password, she is less likely to continue trying.

Account Lockout Duration

This setting determines how long an account will be locked out after the "Account lockout threshold" has been reached. This setting helps us to counter brute force and dictionary attacks. The default value in the NSA template is 15 minutes, which is an acceptable value in our environment.

Account lockout threshold

This setting determines the number of failed logon attempts that cause an account to be locked out. The account remains locked until the "Account Lockout Duration" has expired or an Administrator manually unlocks it. This setting also helps us counter brute force and dictionary attacks. The default value in the NSA template is three attempts, which is an acceptable value in our environment.

Reset account lockout counter after

This setting determines the length of time in minutes after a failed logon attempt, that the bad logon counter is reset to zero. The default value in the NSA template is 15 minutes, which is an acceptable value in our environment.

Audit Policy

Auditing is an important component of security. It alerts us to conditions which may be suspicious, and possibly indicative of a security breach. We need to monitor attempts to access the system, or to exceed authority. We can loosely look at it as a low level form of Intrusion Detection. Unfortunately there is no auditing turned on in Windows2000 by default. Once turned on, the information is logged to the Security section of the event viewer. Auditing policy is not defined in the NSA's template, so we will modify the following Audit Policy settings in our GIAC-DomainPolicy.inf template.

Audit account logon events

This setting allows us to audit logon events on remote machines, where the local computer was used to authenticate the logon. This setting allows us to know who is attempting to logon to our machines, and if it was successful or failed. These logs could be used to trace when a user logged on and from where in case of a security breach. Since we need to know who has attempted to access our systems, we will modify this setting to "Success, Failure".

Audit account management

This setting audits modifications to accounts. It tracks when accounts are created, deleted or modified, enabled or disabled, or if the password has changed. This can be useful for alerting us to any suspicious activity. For example, an attacker may create herself a "backdoor" account to gain access to the system at a later date. It can also help us determine if someone who is unauthorized to modify accounts, is in fact trying to modify an account. We will set this to audit "Success, Failure".

Audit logon events

This setting tracks users who have logged on or off, or made a network connection to the local computer. "Audit account logon events" audits logon events on remote machines, whereas this setting audits access on the local machine. This is useful for the same reasons as "Audit account logon events" We will set this to "Failure", as logging successful and failed logons will result in a large amount of data being logged. This will help us determine attempts to break into the system.

Audit policy change

This setting determines if we audit changes in the user rights policies, audit policies themselves, and trust policies. Monitoring changes in the policies themselves will alert us to attempts at changes in privilege. We will set this to "Success, Failure".

Audit privilege use

This setting allows us to audit the use of privileges assigned to accounts by the Administrator. Since auditing "Success" would result in a lot of log entries, we will set this to "Failure". This will alert us to an unprivileged user attempting to exercise a privilege he is not authorized to do. It is worth noting that there are some user rights that don't get audited even if "Audit privilege use" is enabled.

> *By default, audits are not generated for use of the following user rights even if success or failure auditing is specified for audit privilege use:*
>
> *- Bypass traverse checking*
> *- Debug programs*

- *Create a token object*
- *Replace process level token*
- *Generate Security Audits*
- *Backup files and directories*
- *Restore files and directories*

(Microsoft Corporation, Resource Kit Supplement:1 Group Policy Reference)

Once we have enabled these audit policies, we can use NTLast to capture failed logon attempts on remote machines. There are many options available with this tool. For example you can retrieve successful logons, failed logons, interactive or remote logons. You can retrieve events before or after a particular date. This process can be automated through the use of a batch file, which can then be run periodically. This handy tool is available from Foundstone at:

http://www.foundstone.com/knowledge/forensics.html

Best of all, this tool is free.

Security Options

There are a few key attributes that we will set at the domain level:

Additional restrictions for anonymous connections

This setting determines whether anonymous users can perform various activities, such as seeing the domain accounts and network shares. This activity is allowed by default in Windows 2000 for convenience sake. We want to give an attacker as little information as possible, therefore this setting will be set to "No access without explicit anonymous permissions". This removes "Everyone" and "Network" from the anonymous user's token which prevents anonymous or null users from accessing information about network resources and enforces the use of valid accounts.

Automatically log off users when logon time expires

A user may be granted access to network resources only during a certain time period. We have a consultant working with the developers from time to time. We want him to do his work during office hours so he can't bill for overtime. We also want to enforce this option to prevent someone from accessing the HR and Finance user accounts after hours as they have access to sensitive information. This setting will help us enforce our corporate policies, security and otherwise.

We will set this to enabled, which will disconnect any active SMB sessions when a user's logon hours expire. This will prevent a user from accessing network resources when they are not allowed to.

Do not display last user name in logon screen

When a user logs onto a Windows 2000 machine, the username of the last person who was successful in logging on is displayed in the username field. We don't want to give out any information about usernames to a malicious user. Some of our employees sit in open cubicles which makes them more susceptible to attempts to gain access after hours. We will set this to enabled, to prevent the last username from being displayed.

LAN Manager Authentication Level

The following is Microsoft's description of LAN Manager Authentication Level and the different options for the setting:

> *Determines which challenge/response authentication protocol is used for network logons. The choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers as follows:*
>
> - ***Send LM & NTLM responses**: Clients use LM and NTLM authentication, and never use NTLMv2 session security; DCs accept LM, NTLM, and NTLMv2 authentication.*
> - ***Send LM & NTLM - use NTLMv2 session security if negotiated:** Clients use LM and NTLM authentication, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.*
> - ***Send NTLM response only:** Clients use NTLM authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.*
> - ***Send NTLMv2 response only:** Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.*
> - ***Send NTLMv2 response only\refuse LM:** Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM (accept only NTLM and NTLMv2 authentication).*
> - ***Send NTLMv2 response only\refuse LM & NTLM:** Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM and NTLM (accept only NTLMv2 authentication).*
>
> *The default setting for servers is **Send LM & NTLM responses**.*

(Microsoft Corporation, Resource Kit Supplement:1 Group Policy Reference)

We will set this to Send NTLMv2 response only\refuse LM, as LM password hashes are much easier to crack. . This will help prevent the use of less secure authentication methods on our network. This setting may affect some processes in Windows 2000, therefore we will test this setting as much as possible before implementing it in our

environment. However, there may be issues that do not crop up in our test environment so we will have to deal with them as they come up after we change the setting in the production environment. Changing this setting will also introduce some connectivity issues with older clients, but since all of our systems are Windows 2000 this particular issue will not affect us.

Message text for users attempting to log on

This setting specifies the warning banner that will appear when a user attempts to logon. There have been legal cases where a hacker has gained access to a system which did not display a warning. In some cases the system actually said something like "Welcome to System", and the hacker's defense was that he didn't know he was not supposed to be on the system. Unfortunately the judge agreed. Further information on a specific case is available at:

> http://www.attrition.org/security/advisory/auscert/AA-93.03.Suggested.Login.Banner

Since no system is completely secure, security breaches will be something we are forced to deal with. To prevent a similar situation from happening to us, we will display a legal disclaimer when anyone logs on.

We have decided to use Lance Spitzner's recommended warning banner, as follows:

> *"WARNING: You must have prior authorization to access this system. All activity may be logged and monitored. By accessing this system you fully consent to all monitoring.Unauthorized access or use will be prosecuted to the fullest extent of the law. You have been warned"* (Spitzner)

Message title for users attempting to log on

This setting determines the message in the title bar of the window in which our warning banner is displayed. We will set it to read "Attention!".

Prompt user to change password before expiration

We want to change the passwords frequently for the reasons mentioned above in the Password Policy section. This setting determines when the system will warn the user that their password is expiring soon, and giving them the option of changing it now or at a later time. We want to warn the user well in advance to avoid forcing them to change the password at a moments notice. If we warn the user in advance, they are more likely to come up with a password that they will remember. Yellow post-its on monitors don't make for good security. We will set this to 14 days so that users will have plenty of time to think up of a good password that they can remember.

Rename administrator account

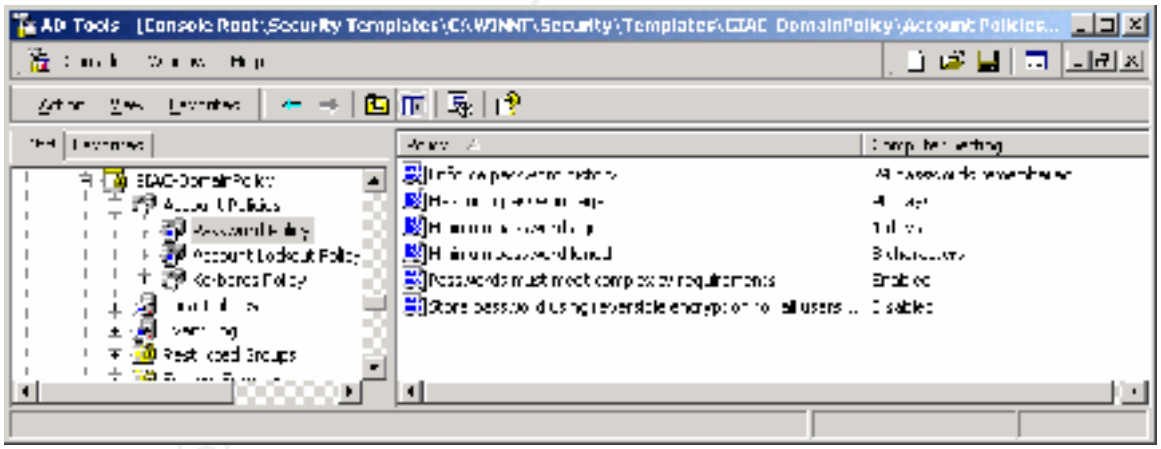
A hacker will target specific default accounts when trying to gain access to a system. Well known accounts such as root, Administrator, Admin, guest etc. are frequent targets. To help limit the potential compromise of these accounts, the accounts should be renamed. The Administrator and guest accounts also have a default description in Windows 2000. Renaming these accounts is not enough, as the description will be an obvious indication to the hacker of what the account actually is.
This setting is disabled in the NSA template. We will set it to rename the administrator account to "bobby", and change the description of the account.

When I made this change on my Domain Controller, I could not access the domain via the MMC snap-ins. I had to logout and login as "bobby" since it went ahead and renamed the account. I was able to function normally after that.

Rename guest account

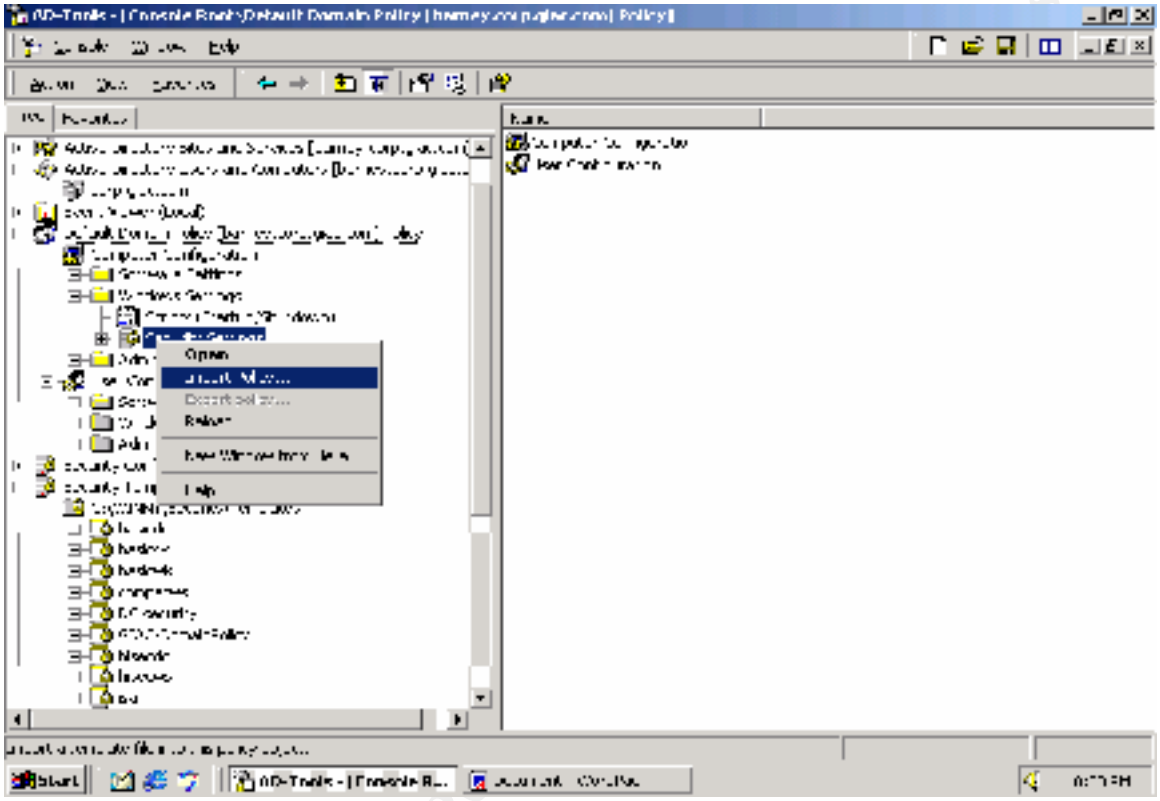
Like the Administrator account, the guest account is frequently targeted by hackers. For these same reasons, we will rename the guest account to "zack" and change the description.

We can use the "Security Templates" snap-in to make the modifications to our GIAC-DomainPolicy.inf template. See Appendix A: GIAC-DomainPolicy Template.

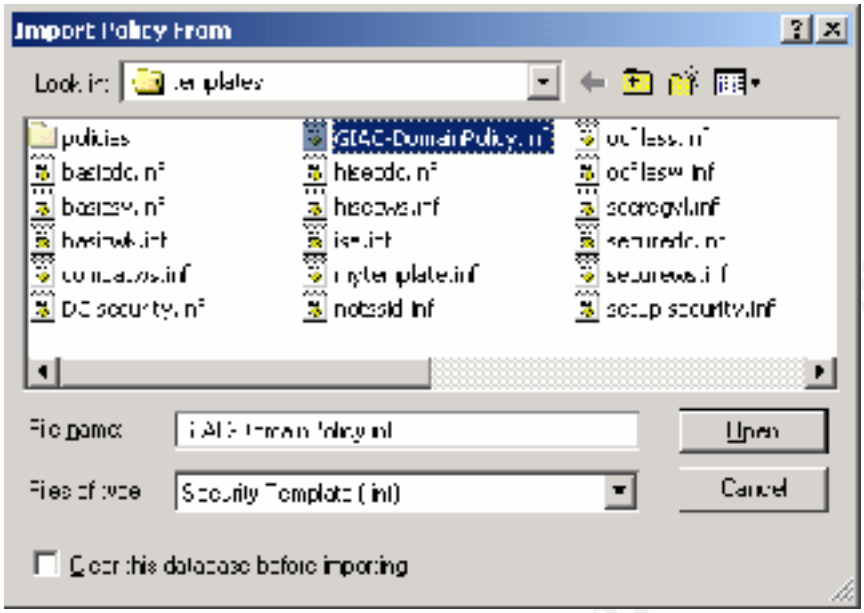


Once we have modified the template, we can import it into the Default Domain Policy.

- In the Group Policy snap in, go to Computer Configuration->Windows Settings ->Security Settings.
- Right click on Security Settings and select “Import Policy”.

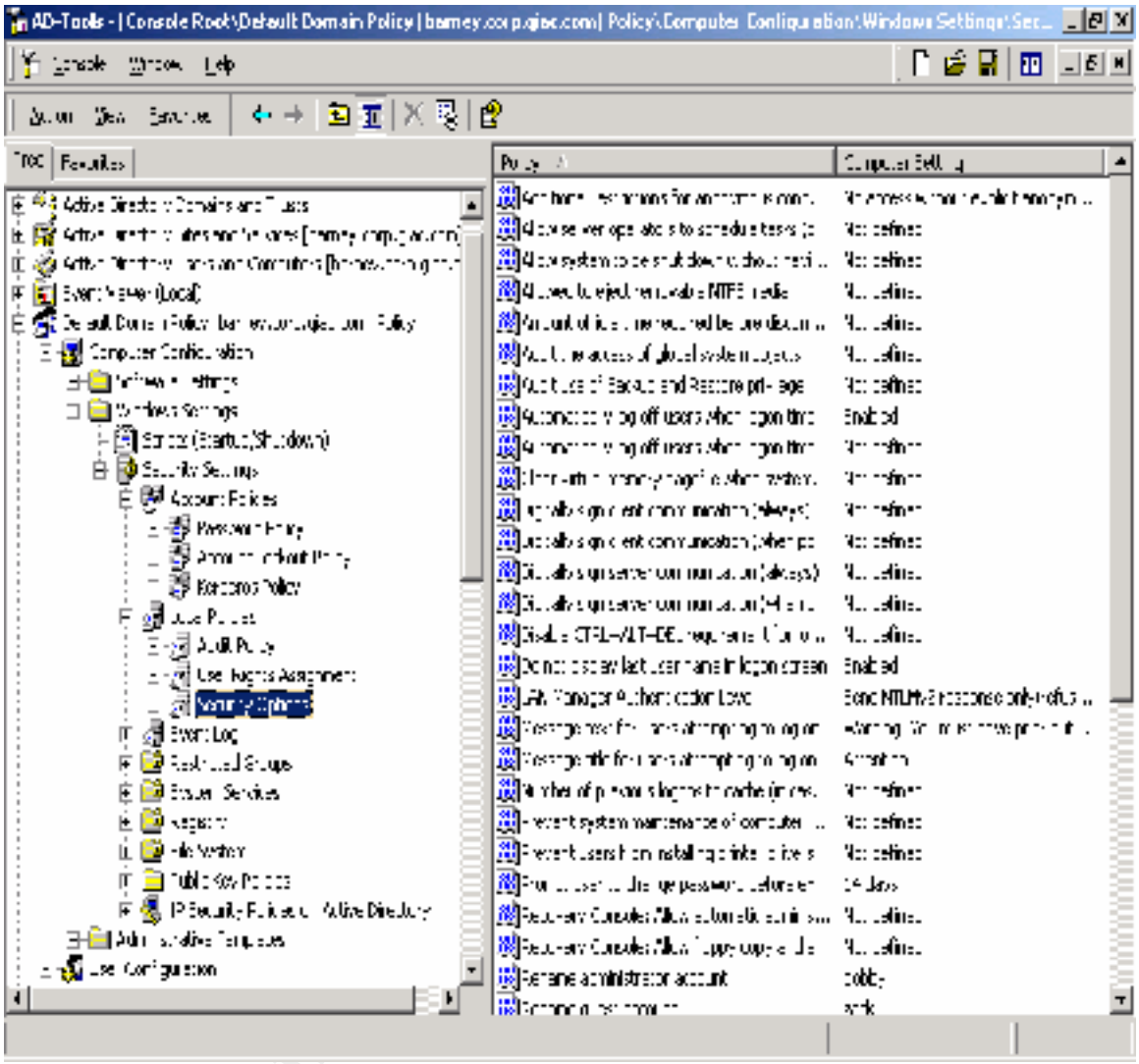


- The “Import Policy From” window will display all the inf files in %SystemRoot%\security\templates. Select the GIAC-DomainPolicy.inf template.

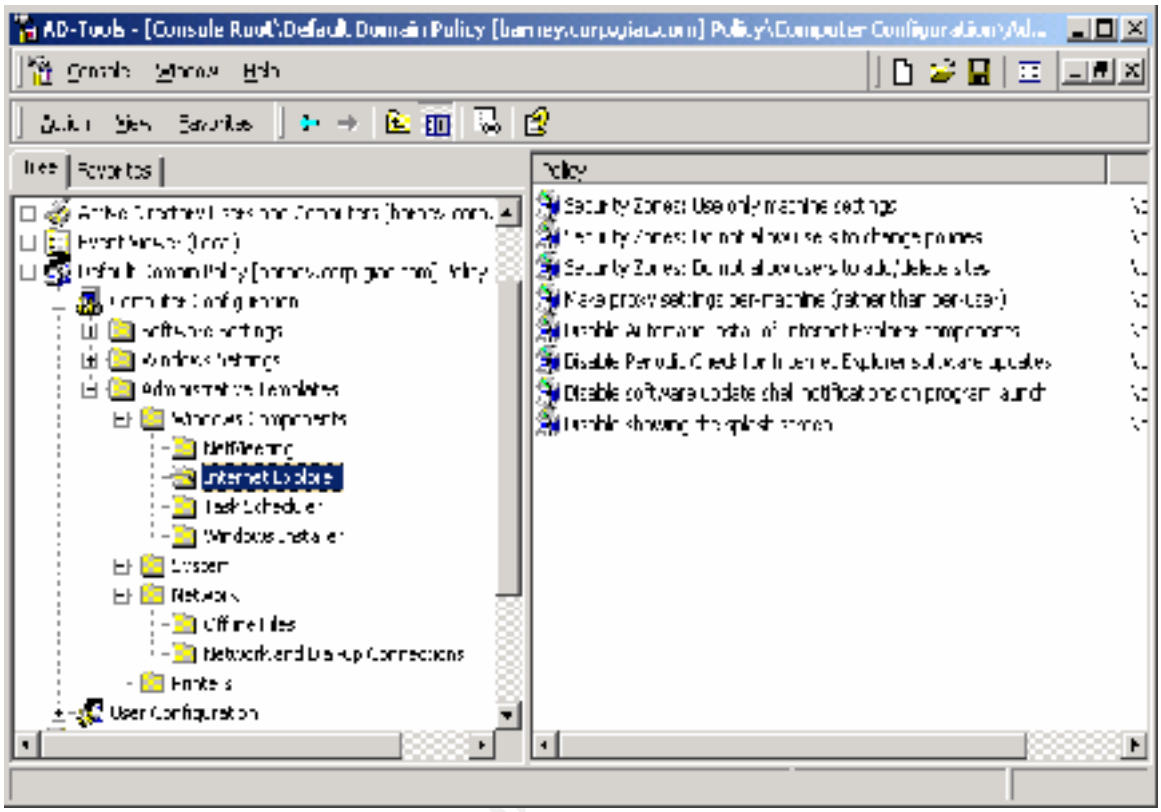


- Click “Open”

We can see below that the settings from the GIAC-DomainPolicy.inf template have been imported into the Security Settings section of Default Domain Policy.



We will now configure some of the key system settings in the Default Domain Policy. This is done in the Administrative Templates section of the policy:



Internet Explorer

Security Zones: Do not allow users to change policies

Internet Security zones are an important security feature of Internet Explorer. They allow us to choose the level of security we wish to apply in our browsers. If these settings are improperly set, several security holes are potentially opened up, putting not only a single PC at risk, but our entire network. As an example, we want to set the "Download unsigned Active X controls" to disabled. Active X gives open access to your system, which could result in serious damage if the Active X code is malicious. The only real security is that you trust the entity that created the Active X code. If you allow unsigned code to be executed, you cannot verify the source, thereby bypassing the security offered within Active X.

We will set this to enabled in order to prevent users from changing acceptable security zone settings established by the IT Department.

Security Zones: Do not allow users to add/delete sites

A security zone groups web sites which have common security levels together. You can add or remove websites to the Trusted or Restricted zones. The sites in these zones have the same security levels applied to them. For example, you may trust Microsoft.com and allow it to have more access to your system than you would a hacker site. If a user has access to change these settings, they can compromise the security of the system.
We will set this to enabled. This will prevent users from adding or removing sites from security zones.

Disable Automatic Install of Internet Explorer components

We will set this to enabled. This will prevent IE from downloading components when users browse to a web site that needs that component. This will help prevent unauthorized and possibly malicious software from being installed, allowing the IT department to have more control over the environment.

Disable Periodic check for Internet Explorer software updates

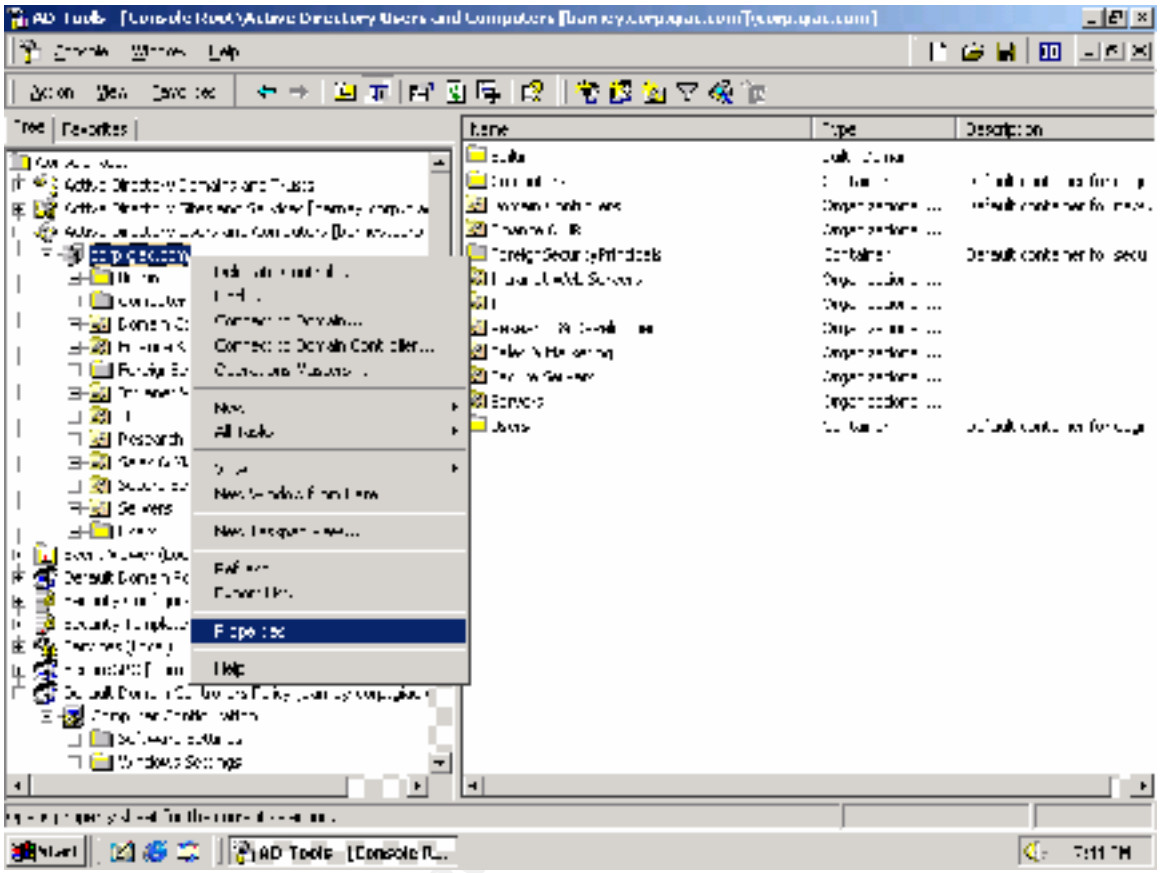
Internet Explorer checks every 30 days for new versions of IE, and notifies the user. This puts version control in the hands of the end user, rather than in the hands of the IT department where it belongs. New versions may have security or compatibility issues which need to be tested before they are rolled out into production.

By enabling this setting, we will prevent IE from checking to see whether the latest available browser is running, and notifying the user when a new version is available. This decision should be made by the IT Department, not by the user.

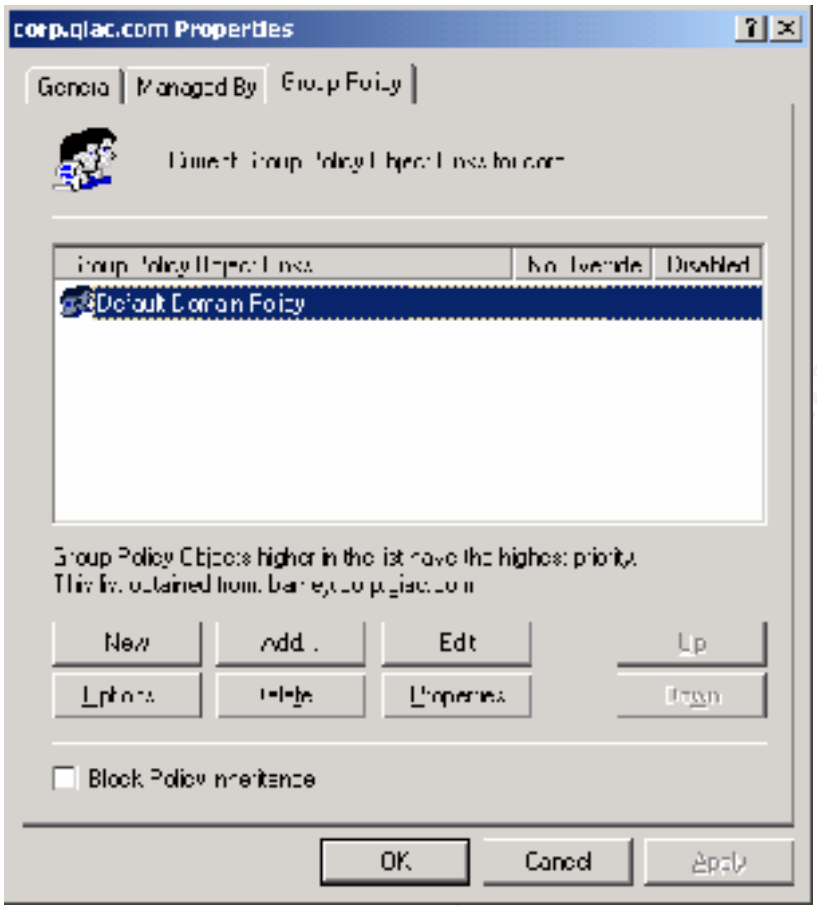
Now that we have modified our settings, we will double check that the settings have been applied. Logging on to a workstation on the domain verified that our warning banner setting has propagated out to the desktop. When we pressed CTRL-ALT-DEL to log on, the username field was blank. Going into the Local Security Policy on the workstation verified some of the other settings.

Now that we have our Domain Policy defined, we want to set the No Override option to enforce our policy regardless of what is set in the OUs.

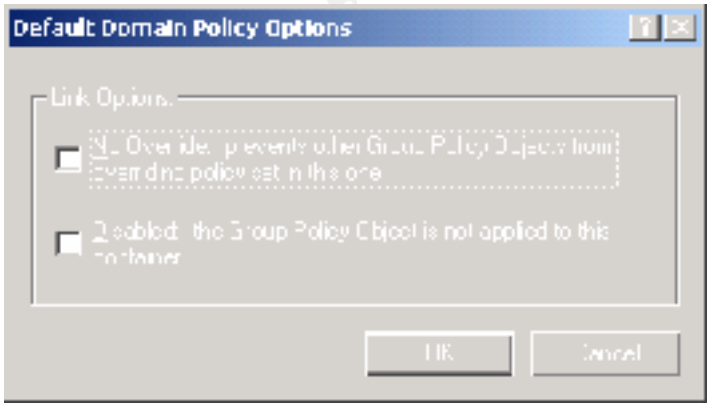
This is easily accomplished by right clicking on our domain in the Active Directory Users and Computers snap-in and selecting Properties.



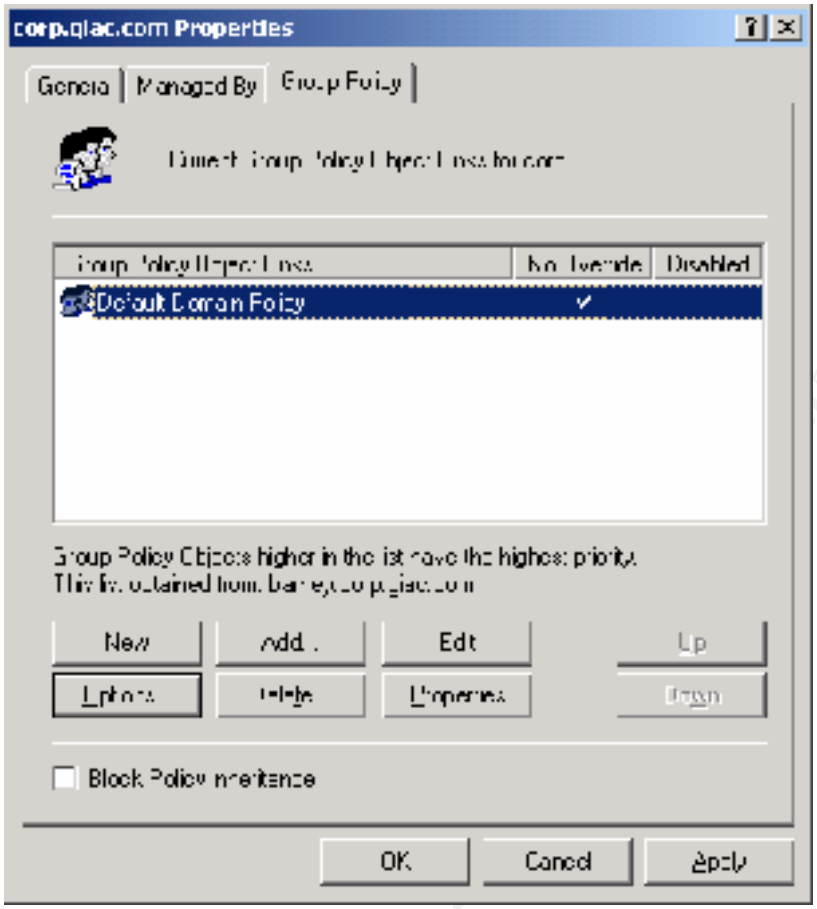
This brings up the corp.giac.com Properties window. We select the Group Policy tab and we can select Add to add the Default Domain Policy GPO to our domain.



We can then click the Options button to set the No Override option.



Once we've done that, we see that the Default Domain Policy is linked to corp.giac.com domain, and has the No Override option set.



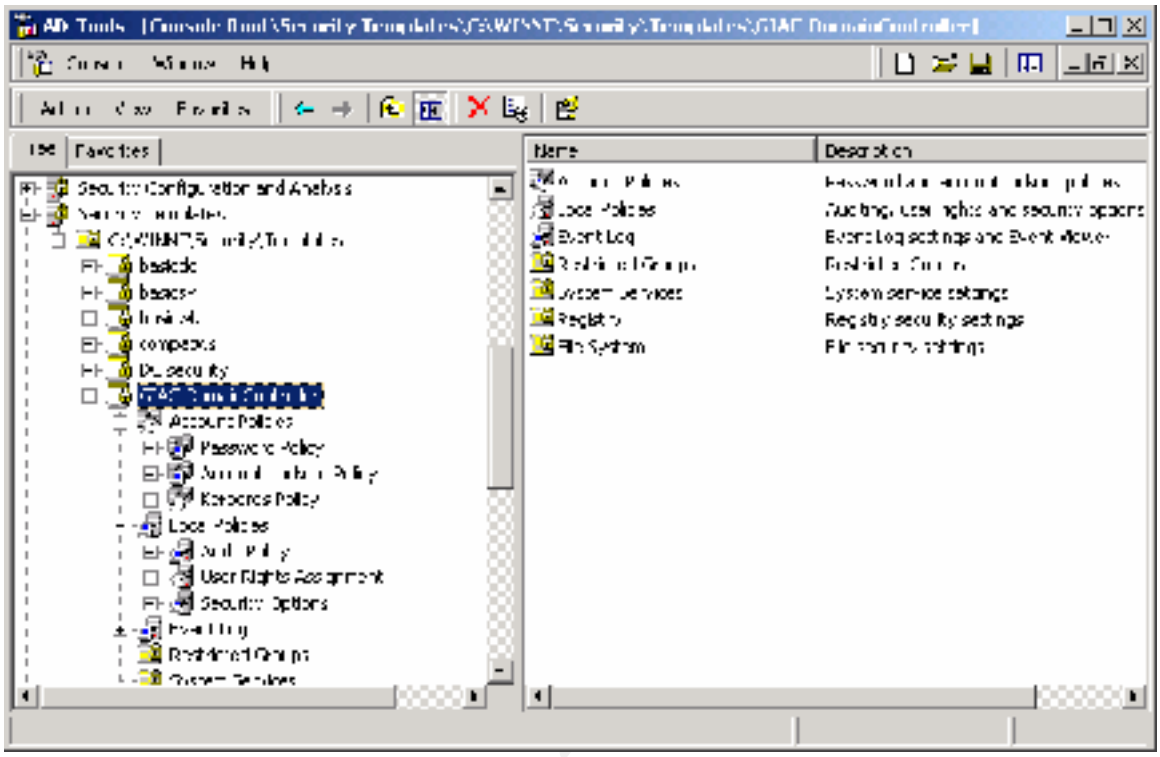
Default Domain Controller Policy

Next we will look at the Default Domain Controller Policy. This policy will apply to all of our Domain Controllers. Security is very important in our environment, especially for our servers.

Once again, we will use an NSA security template as a baseline for our security. Since we trust the NSA, we are confident that we are getting a secure Domain Controller if we apply the w2k_dc.inf template. Therefore we will utilize the w2k_dc.inf, and modify any settings we need to for our environment. The w2k_dc.inf template makes several changes to the Account Policies, Local Policies, Event Log, Registry and File System permissions. It will not be feasible to go over every setting, so instead we'll focus on the changes we will make.

We will begin by copying w2k_dc.inf. We will rename the copied file to GIAC-DomainController.inf before we begin customizing it. Since the Default Domain Policy applies to all Organizational Units across the domain, those settings will also be applied to the Domain Controllers.

Once we've done this, we can modify the various setting by utilizing the Security Templates snap-in.



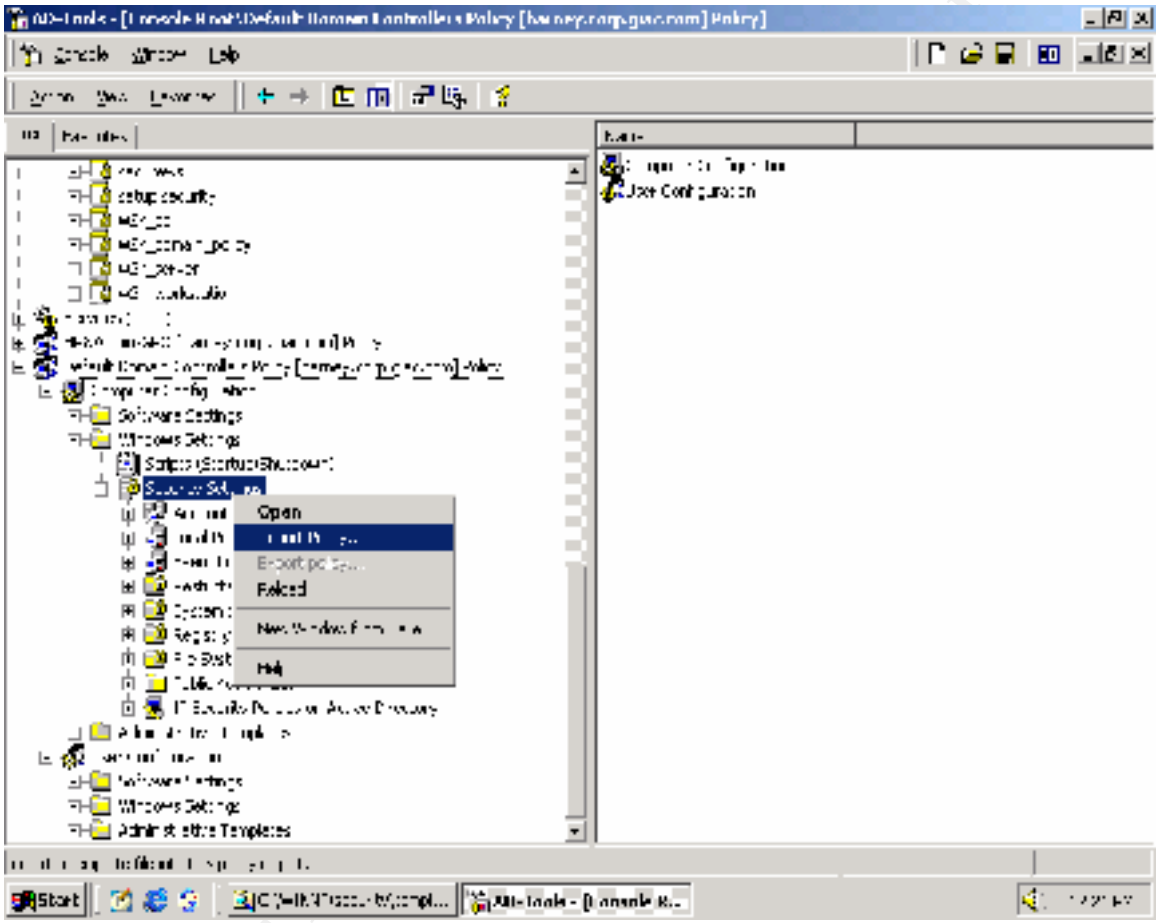
Clear virtual memory pagefile

The "Clear virtual memory pagefile when system shuts down" in "Security Options" is set to enabled in the NSA template. Having this option enabled left us with shutdowns that took in the neighborhood of 10 minutes. Since our Domain Controllers are in a physically secure location, we have decided to disable this option in order to improve upon performance.

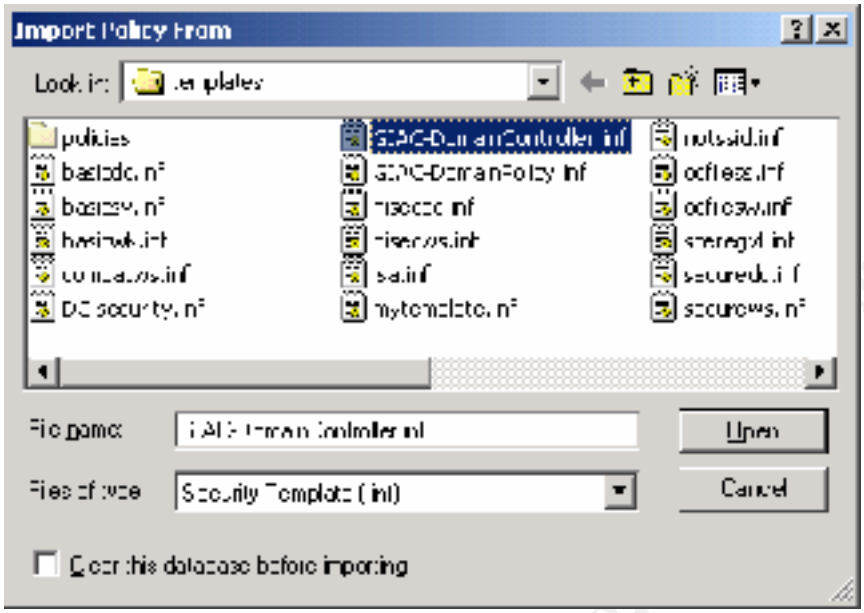
Once we have modified the template, we can import it into the Default Domain Controllers Policy.

- In the Default Domain Controllers Policy Group Policy snap in, go to Computer Configuration->Windows Settings ->Security Settings.

- Right click on Security Settings and select “Import Policy”.



- The “Import Policy From” window will display all the inf files in %SystemRoot%\security\templates. Select the GIAC-DomainController.inf template.

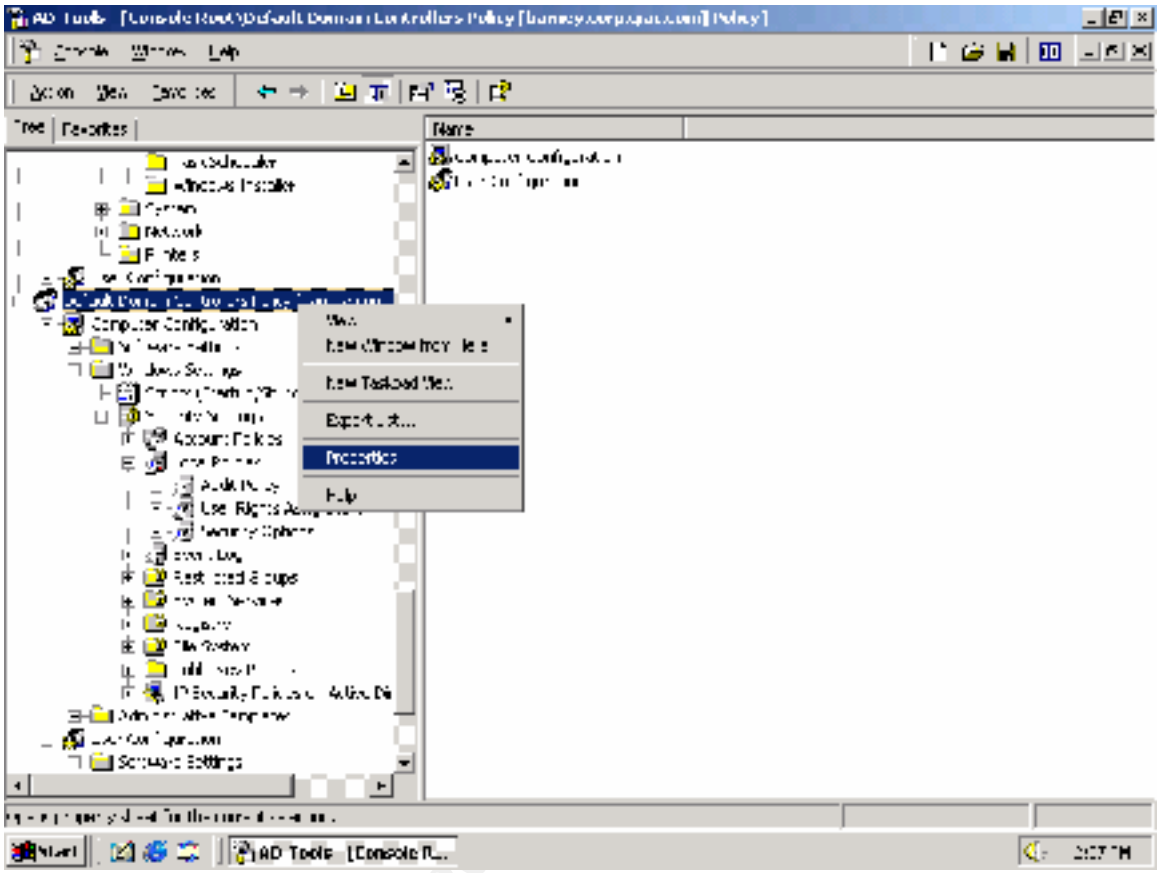


- Click “Open”

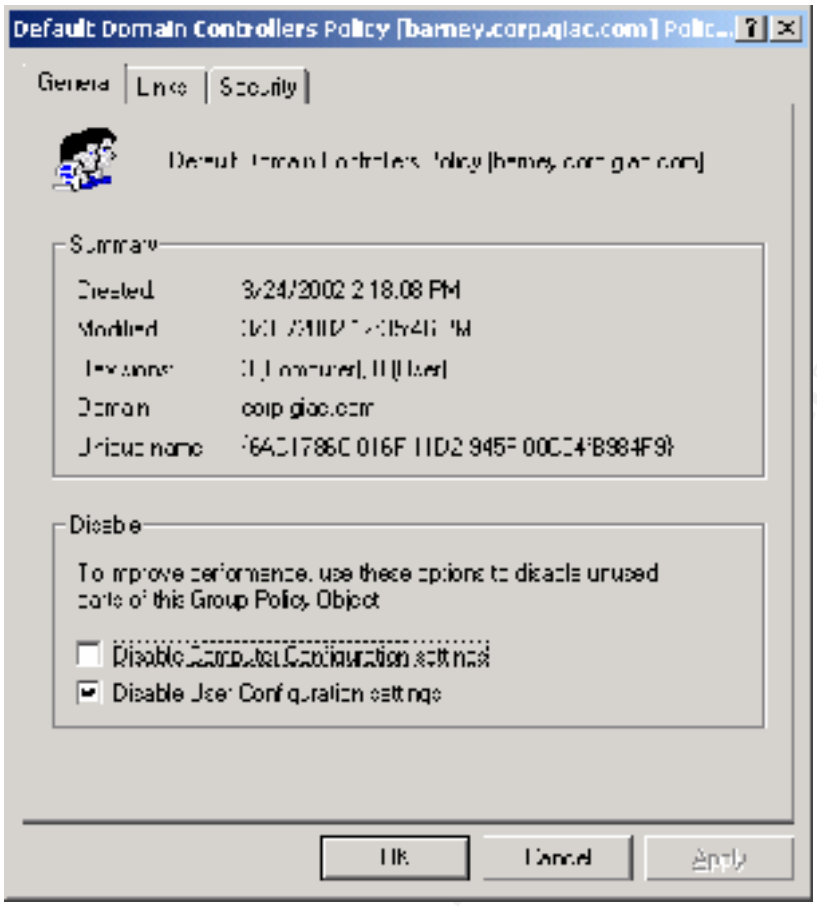
- The settings from the GIAC-DomainController.inf template have been imported into the Security Settings section of Default Domain Policy.

Since the Default Domain Controller GPO only specifies Computer Configuration settings, we will disable the User Configuration settings in the GPO. Since we are not using this portion of the GPO, we can disable it, and this will improve performance.

This can be done by right clicking on the Group Policy snap in for Default Domain Controllers Policy and selecting Properties:



We disable the user configuration settings by checking the "Disable User Configuration Settings" checkbox.



Servers

Next we will look at the Server OU. We will create a ServerGPO and link it to the Server OU. This policy will apply to all of our general servers. This includes the R&D servers, file servers, print servers, email server and backup server.

Once again, we will use an NSA security template as a baseline for our security. Since we trust the NSA, we are confident that we are getting a secure server if we apply the w2k_server.inf template. Therefore we will utilize the w2k_server.inf, and modify any settings we need to for our environment. The w2k_server.inf template makes several changes to the Account Policies, Local Policies, Event Log, Registry and File System permissions.

The procedure for configuring and applying the template is very similar to what we did above for the Default Domain Controller Policy. We will call our template GIAC-Server.inf. We will modify the Clear virtual memory pagefile setting as we did above.

Secure Servers

Next we will look at the Secure Server OU. We will create a SecureServerGPO and link it to the SecureServer OU. This policy will apply to all of our special needs servers. This OU consists of the Accounting and HR servers. Since they contain confidential information, we want to be more vigilant about these servers.

The servers were built with minimal installs of the OS. The employees in the Finance & HR group run a package purchased from a well-known vendor to store and maintain employee data. Due to the confidential nature of the data they handle, we want to protect these servers more vigilantly than one of our general servers. The workstations in the Finance & HR department are configured with static ip addresses. The ip addresses are all in the 10.10.99.x range. Although the network is using a class B mask, the machines have been addressed in what appears to be a class C network to uniquely identify them so the filtering rules on servers and firewalls can be made simpler.

Once again, we will use an NSA security template as a baseline for our security. Since we trust the NSA, we are confident that we are getting a secure server if we apply the w2k_server.inf template. Therefore we will utilize the w2k_server.inf, and modify any settings we need to for our environment. The w2k_server.inf template makes several changes to the Account Policies, Local Policies, Event Log, Registry and File System permissions.

The procedure for configuring and applying the template is very similar to what we did above for the ServerGPO. We will call our template GIAC-SecureServer.inf.

We will also make the following modifications to the SecureServerGPO.

Any unnecessary services pose a risk to our servers. The services may be prone to known as well as unknown vulnerabilities. Known vulnerabilities are something the manufacturer is aware of, and generally has put out a patch to address. Unknown vulnerabilities are vulnerabilities in a service which have yet to be discovered. Keeping in mind that all known vulnerabilities were once unknown (or unaddressed at least), it is to our advantage to minimize our exposure to these vulnerabilities by shutting down any unnecessary services. If we are not running the service, we are not susceptible to known or unknown vulnerabilities associated with these services.

Therefore, we will disable the following unnecessary services

Computer Browser
DHCP Client
DHCP Server
DNS Server
Fax Service
IIS Admin Service
Internet Authentication Service

Internet Connection Sharing
Intersite Messaging
Messenger
NetMeeting Remote Desktop Sharing
Print Spooler
Protected Storage
Remote Registry Service
Routing and Remote Access
RunAs Service
Simple Mail Transport Protocol (SMTP)
TCP/IP NetBIOS Helper Service
Telephony
Telnet
Terminal Services
Windows Internet Name Service (WINS)
World Wide Web Publishing Service

We will also utilize the IPSEC filtering capabilities to limit access to these servers. Since the Accounting and HR applications already encrypt and authenticate the data as it traverses the network, we will not need to worry about encryption or authentication within the IPSEC policy. We will set up the IPSEC policy to allow connections from the Finance & HR workstations.

SecureGPO

The Finance & Human Resources and the Sales & Marketing departments have different security needs than the R&D and IT departments. As we explained above, we will have a General GPO and a SecureGPO which will be applied to different OUs as needed.

We will use the NSA's w2k_workstation.inf template as a starting point. This template features enhanced security settings for Windows 2000 Workstations. Since we trust the NSA, we are confident we are getting a reasonably secure workstation if we apply the w2k_workstation.inf template. Therefore we will utilize the w2k_workstation.inf, and modify any settings we need to for our environment. The w2k_workstation.inf template makes several changes to the Account Policies, Local Policies, Event Log, Registry and File System permissions. It will not be feasible to go over every setting, so once again we will focus on the changes we will make.

We will begin by copying w2k_workstation.inf. We rename the copied file to GIAC-SecureWorkstation.inf. Since the Default Domain Policy applies to all Organizational Units across the domain, those settings will also be applied to the Finance&HR. Again we will outline the changes made to the template, as opposed to analyzing each setting.

Computer Configuration

Automatically log off users when logon time expires

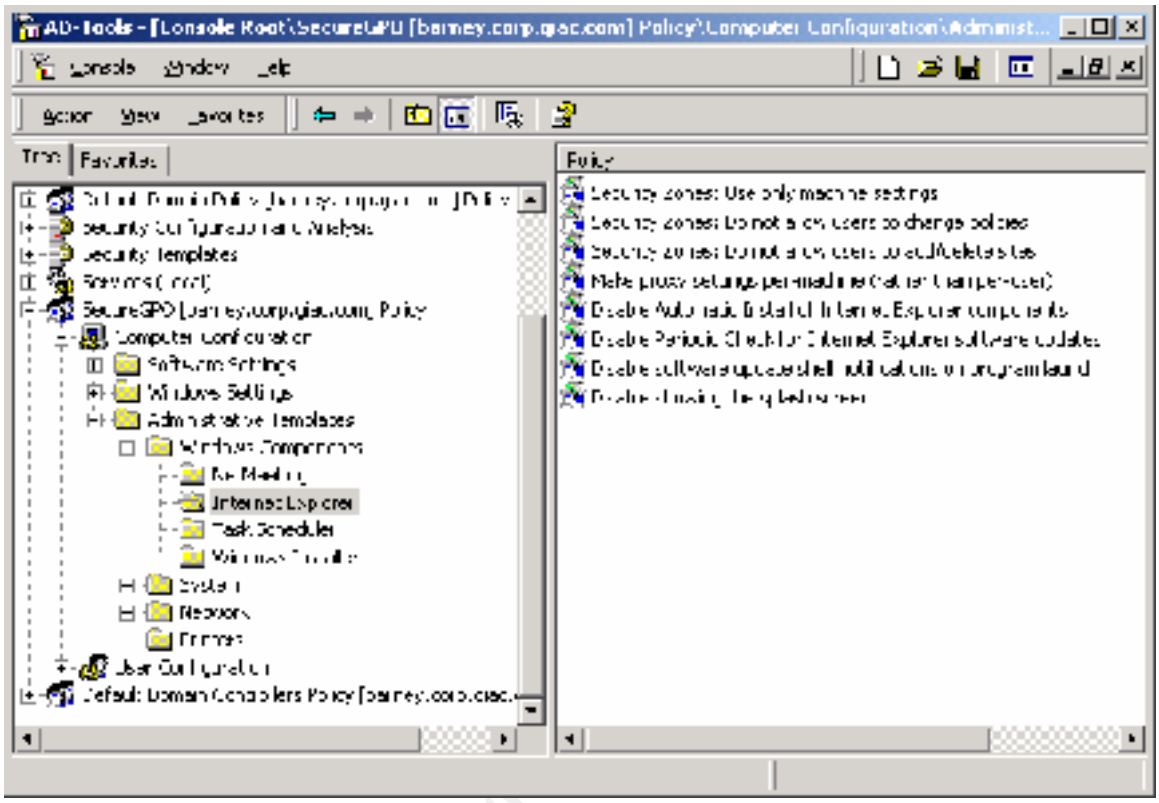
This setting will be enabled. This causes client sessions to be forcibly disconnected when a user's logon hours expire. Though this is set in the Default Domain Policy, we will set it here as well just to be as through as possible.

Next we will disable some system services which don't need to be running. Not all of these services are running by default, but to be thorough we will disable them. The following services will be disabled:

- DHCP Server
- DNS Server
- Fax Service
- IIS Admin Service
- Internet Connection Sharing
- Intersite Messaging
- Net Meeting Remote Desktop Sharing
- Runas Service
- TCP/IP Netbios Helper Service
- Telnet
- Terminal Services
- WINS

We can now import this template into the SecureGPO in the same way we did for the Domain Controllers.

We will now continue customizing the settings for the SecureGPO. We can continue in the Computer Configuration by customizing the settings under Administrative Templates.



Netmeeting

Prevent Sharing

The sharing function of Netmeeting allows a user to share out applications or the desktop to remote users. This is beneficial to employees in our Accounting department as they have been having "virtual" meetings with vendors as we look for a new payroll system. Many of the vendors reside out of state. We do want to prevent our users from sharing anything out themselves, while still being able to view applications shared by others. We will enable this option to prevent our employees from sharing out applications or their desktop.

Windows Installer

Disable Windows Installer

Windows installer is Microsoft's answer to InstallSheild. Files that utilize the .msi extension are Windows installer programs. We do not want members of the HR & Finance department to be able to install programs on their systems. Allowing this could introduce malicious code to the network, and it takes version control out of the hands of the IT department.

We will disable the Windows Installer and set it to "Always". This will help prevent users from installing software on their machines. Any software installed on machines in the Finance & HR department must be authorized by the IT Department.

It is important to note that this setting only applies to Windows installer programs. Employees are still able to install programs through other means. Some of these other methods are addressed in the Control Panel section below.

Disable Patching

We will disable patching. This helps restrict users from installing patches using the Windows Installer. Patches, like any other executable, can be used to introduce malicious code. Patch levels should be tested and approved by the IT Department.

System

Disable Autoplay

We will enable this setting for CDROM drives. This prevents the CDROM drive from automatically reading a cd when you insert it. This will help prevent the introduction of malicious code to the system or the disclosure of sensitive information (e.g. Password hashes) by someone who gains physical access to it. There have been cases where this feature is used to bypass password protected screen savers, which poses all kinds of security risks.

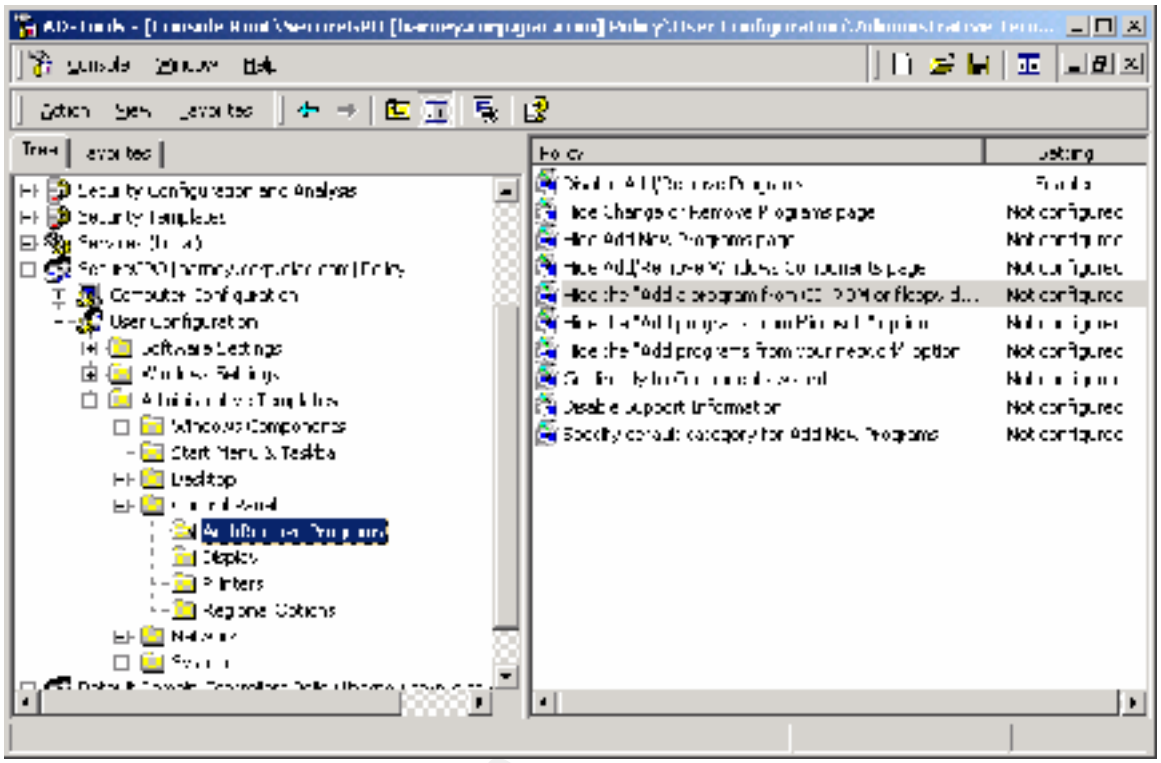
Network and Dialup Connections

Prohibit configuration of connection sharing

The connection sharing feature is used to share a connection to a remote network amongst computers on a LAN. This is undesirable as it may be used to bypass security features of our firewall. This can open the door to hackers as there is no firewall protection on the PC itself. Once the PC is compromised, our entire network is in jeopardy. Therefore, we will enable this setting. This prevents users from being able to configure the Internet Connection Sharing feature of a dial-up connection.

User Configuration

The user configuration section of the GPO will also be modified.



All of our configuration changes will be done in the Administrative Templates section.

Internet Explorer – Internet Control Panel

Disable the Security page

The Security tab in the Internet Options dialog box in IE contains user defined sites and security levels. In the Secure GPO, we do not want to allow the users to make any adjustments or changes to the settings defined by the IT Department. Therefore, we will set this to enabled. This removes the security tab from the interface in the Internet Options dialog box.

Disable the Connections page

The Internet Connections tab in the Internet Options dialog box in IE contains various dialup, VPN and proxy settings. There is also a setup button which invokes the internet connection wizard. Modifying these settings could potentially be used to bypass the firewall. Users should have no need to stray from the IT Department designated settings. We will set this to enabled, which removes the Connections tab from the interface in the Internet Options dialog box.

Disable the Advanced page

It is important that the IT Department set the Internet settings standards for the corporation. The Advanced tab in the Internet Options dialog box allows you to set various options relating to security, multimedia, printing, browsing, java and http. We do not want users to have the potential to intentionally or unintentionally modify these settings. For example, we don't want users to uncheck the "Check for publishers certificate revocation" setting, as the certificate is used to validate the source. If the certificate is no longer valid, using it to authenticate the signer is foolish.

We will set this to enabled, which will remove the Advanced tab from the interface in the Internet Options dialog box altogether.

Microsoft Management Console

Restrict users to the explicitly permitted use of snap-ins

Microsoft Management Console is used to administer the settings of Windows 2000 system. This is not something the user should be normally doing. Enabling this setting will allow us to restrict the MMC snap-ins a user can see. This will prevent the user from having access to snap-ins which control administrative functions, such as adding, deleting or modifying a user or a group.

We will set this to enabled, and restrict user access to the following snap-ins:

- Disk Manager
- Disk Defragmenter
- Event Viewer
- Performance Logs and Alerts
- Shared Folders
- System Information

Start Menu & Task Bar

Disable and remove links to Windows Update

As mentioned previously, the IT Department should set the standards for version control on the desktop. Allowing access to the Windows Update website would put this control in the users' hands. We can utilize this setting to block access to the Windows Update website, and to remove the hyperlink from the start menu. It will also remove the hyperlink from the Tools menu in IE.

We will set this to enabled to prevent users from getting updates and patches for various Windows components and software. This will keep things standardized, as the IT Department will decide which software and patches are installed.

Control Panel – Add/Remove Programs

Disable Add/Remove Programs

For the reasons mentioned previously, we want to restrict the users' ability to install software on the systems. This setting will help us achieve that goal by removing the Add/Remove Programs icon from Control Panel.

By enabling this option, we will restrict users from modifying components of Windows 2000, as well as various other programs. Users may still be able to install or uninstall programs through other methods, but it is better to limit their options as much as we can.

Control Panel – Display

Hide Screen Saver Tab

The screen saver plays an extremely important role in the general security of our company. Enabling a password protected screen saver severely reduces the chances of someone coming up to a system that is logged in and having full access to the network. Users tend to be forgetful, and will leave their systems unattended without locking the screen. We can set the screen saver to kick in after 15 minutes of inactivity, and have it password protected. This will reduce chances of a malicious user or stranger from abusing the system.

Beyond this, we do not want the user to have the ability to modify the screen saver section (i.e. remove the password protection, or disable the screen saver), and by enabling this setting, we will remove the screen saver tab entirely.

Activate Screen Saver

This setting works in conjunction with a couple of other settings, namely the "Screensaver executable name" and the "Screen saver timeout". If the Screensaver executable name is set, which we will do below, and the Screen saver timeout is also set, which we also do below, the desktop screen saver will run. We will set this to enabled.

As mentioned previously, we want to have a password protected screen saver to run after 15 minutes of inactivity. This is done to minimize the chances of the computer being left unlocked. At GIAC Enterprises, users are asked to make a habit of locking their computers when they leave their offices, however this does not always happen. This setting will help to enforce the locking of workstations while they are unattended.

Screen Saver executable name

We have decided to make the logon.scr screen saver the corporate standard. This setting specifies the screen saver used for the users desktop to which this Group Policy is applied.

Password protect the screen saver

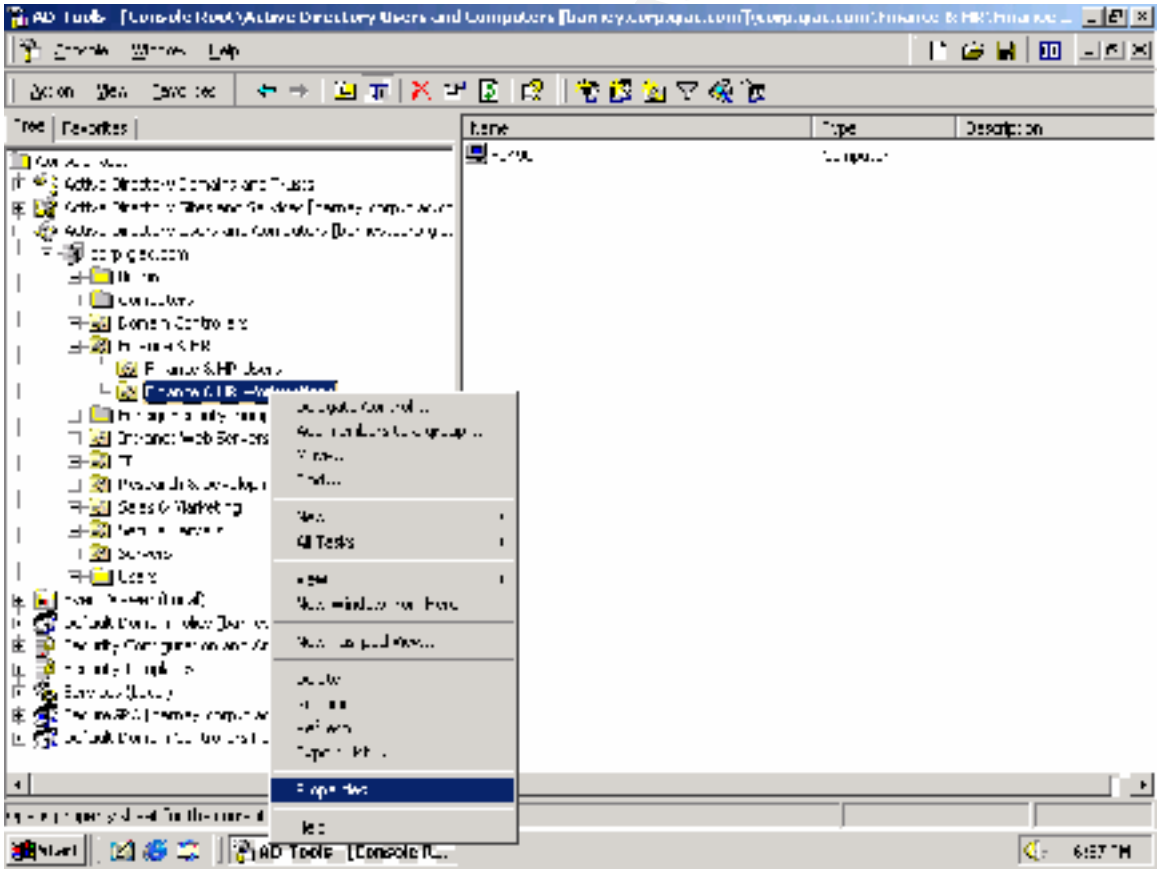
By enabling this setting, we will password protect any screen savers that run on the systems to which this Group Policy is applied.

Screen Saver timeout

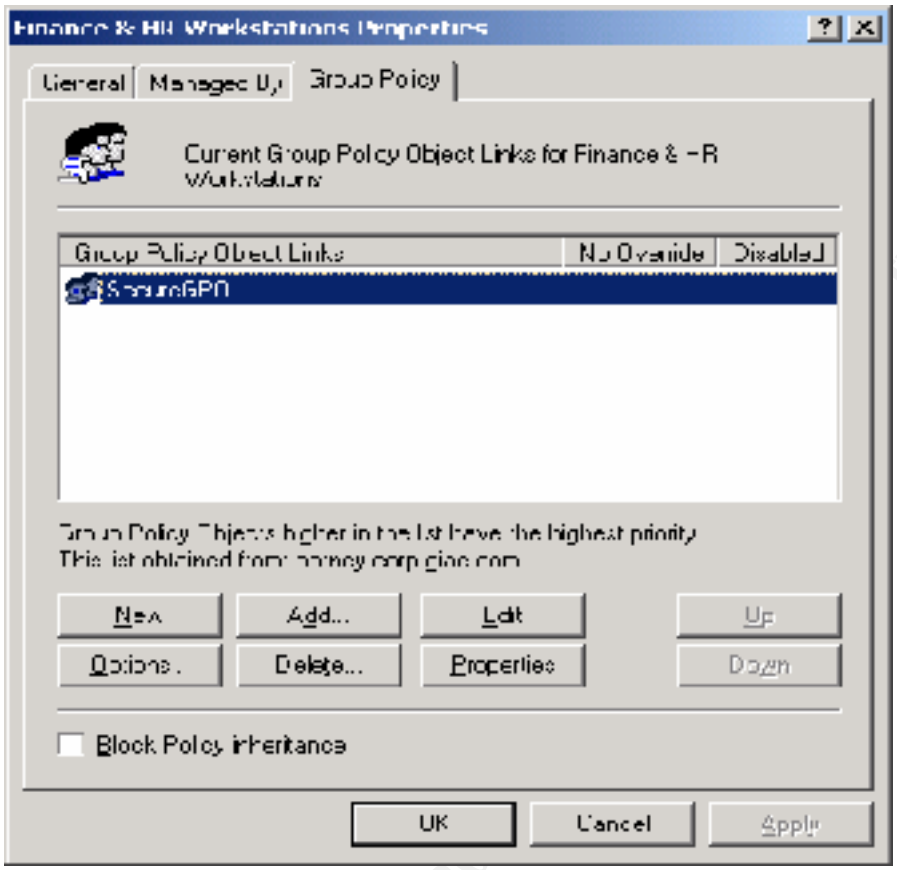
Working in conjunction with the Password protect the screen saver, the Screen Saver timeout setting will add an important level of security to our environment. We will set this to enabled with a timeout of 900 seconds (15 minutes). This will mean the password protected screen saver will launch after 15 minutes of user inactivity.

We now have our SecureGPO configured. We can now easily link it to the Finance&HR Users and Workstations OUs.

We do this by going to the OU we wish to apply the GPO to in the Active directory Users and Computers for our domain. We can right click the Finance & HR Workstation OU and select Properties.



This brings up the Finance & HR Workstations Properties. Here we can click add and select the GPO.



The Group Policy is now linked to the OU.

We can also apply this policy in a similar manner to the Sales & Marketing Users and Workstations. We have created one policy, and linked it to more than one OU.

General GPO

For the IT and R&D groups, we need a security policy that is a little less strict. These groups need more flexibility and special needs, the ability to install their own software as an example.

For this GPO we will apply the NSA's w2k_workstation.inf template so we get a basic level of security on the workstations. We will rename the w2k_workstation.inf template to GIAC-GeneralWorkstation.inf.

Once again, the default domain policy still applies. We will modify the settings for the Control Panel Display options to the same values as we did in the SecureGPO. We can apply the policy in the same manner as we did for the SecureGPO.

Conclusion

GIAC Enterprises will be more secure now than they would have been had we not utilized Active Directory and Group Policy. These two components of Windows 2000 allow us to centrally manage the security of our organization. Through the use of Active Directory and Group Policy, we have been able to effectively enforce our Corporate Security Policy across our network. Active Directory and Group Policy are granular enough that we can easily meet the differing security needs of our various users.

We have been able to maintain our security without significantly impacting performance for our users. One of the major complaints about security has been that it impacts users, but with Windows 2000 we have shown we have the flexibility to implement security without impacting all of the users.

The plan we have set forth for GIAC Enterprises meets the existing security and functionality needs of the company. It also has the flexibility to grow and change along with the company.

References

"Active Directory White Paper". Microsoft Windows 2000. October 12, 1999. Microsoft Corporation: May 5, 2002 <http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adarch.asp>

Antoine, Vanessa *et al.* "Router Security Configuration Guide". Systems and Network Attack Center. Vers. 1.0j. November 21, 2001. National Security Agency: May 5, 2002. <http://nsa2.www.conxion.com/cisco/download.htm>

Bartock, Paul Jr. *et al.* "Microsoft Windows 2000 Network Architecture Guide". Systems and Network Attack Center. Vers. 1.0. April 19, 2001. National Security Agency: May 5, 2002. <http://nsa2.www.conxion.com/win2k/guides/w2k-1.pdf>

Fossen, Jason *et al.* Windows 2000:Active Directory and Group Policy. Vers. 5.1.3. Sans Institute, 2001.

Haney, Julie M. "Guide to Securing Windows 2000 Group Policy". Systems and Network Attack Center. Vers. 1.1. September 13, 2001. National Security Agency: May 5, 2002. <*http://nsa2.www.conxion.com/win2k/guides/w2k-2.pdf*>

Haney, Julie M. "Guide to Securing Windows 2000 Group Policy: Security Configuration Toolset". Systems and Network Attack Center. Vers. 1.1. January 22, 2002. National Security Agency: May 5, 2002. <http://nsa2.www.conxion.com/win2k/guides/w2k-3.pdf>

Lee, I. "A Research Guide for Students" March 24, 2002: May 5, 2002 <http://www.aresearchguide.com/9parenth.html.>

"Microsoft's HFNETCHK Patch Status Utility" Microsoft Technet. 2002. Microsoft Corporation: May 5, 2002 <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp>

"Resource Kit Supplement:1 Group Policy Reference". Windows 2000 Resource Kits. 2001. Microsoft Corporation: May 5, 2002. <http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp>

Rice, David C. "Group Policy Reference" Systems and Network Attack Center. Vers. 1.0.8. March 2, 2001. National Security Agency: May 5, 2002. <http://nsa2.www.conxion.com/win2k/guides/w2k-4.pdf>

Sanderson, Mark J. and Rice, David C. "Guide to Securing Microsoft Windows 2000 Active Directory". Systems and Network Attack Center. Vers. 1.0. December 2000. National Security Agency: May 5, 2002. <http://nsa2.www.conxion.com/win2k/guides/w2k-5.pdf>

Spitzner, Lance. "Armoring Solaris". August 19, 2001: May 5, 2002 <http://www.enteract.com/~lspitz/example.html#A>

"Step-by-Step Guide to Using the Security Configuration Tool Set". Microsoft Technet. 2002. Microsoft Corporation: May 5, 2002. <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/seconfig.asp>

Wahl, M. *et al*. "Lightweight Directory Access Protocol (v3) RFC 2251". Network Working Group. Vers. 3. December 1997. Internet Engineering Task Force.: May 5, 2002. <http://www.ietf.org/rfc/rfc2251.txt>