Global Information Assurance Certification Paper

GIAC Enterprises Windows 2000 Layout

by
Mike McCabe
GIAC GCNT v3.0 Option #1

Introduction

GIAC Enterprises is a young startup company with offices in Ann Arbor, Michigan. They produce fortune cookie sayings for sale across the Internet. A plan will be presented that will both allow GIAC Enterprises to perform e-commerce across the Internet in a safe manner and still perform needed activities in-house.

GIAC Enterprises consists of a number of groups of people including:

- Research and Development
- Sales and Marketing
- Finance and Human Resources
- Corporate Management
- Information Systems

Each of these groups has different needs and requirements to successfully perform their functions. Research and Development need access to high speed file and print services to allow them to develop better sayings for sale in the future. Sales and Marketing need to be able to access the network remotely while on the road as well as being able to print high gloss marketing brochures. Finance and Human Resources need to be able to manage the employee work force and balance the books each and every month. Corporate Management needs to be able to direct the workforce on a daily basis through various methods like email and web interfaces. Information Systems needs to be able to manage the computer systems and user accounts which allows everybody else in the corporation to perform their activities.

During the development of this network and security plan a few assumptions have been made. First, the assumption that since GIAC Enterprises is a small size company that approvals for the addition and deletion of user accounts is managed by the Human Resources department but performed by the Information Systems Department. It is further assumed that the users in Corporate Management don't have any special rights above and beyond those of normal users, except in the form of access to internal web sites for the updating of information being presented to the employees. Another assumption is that there is no distinction between Information Systems Users except between the Help Desk Operators and everybody else in Information Systems. The last assumption is that the external sales force all have another means of connecting to the Internet when on the road and therefore connect back to the corporate office network via VPN and not dial-up.

Purpose

The purpose of this document is to depict the design of a Network and Windows 2000 Active Directory Domain and associated Organizational Unit Structure, and to show how to secure them using Group Policy Objects. We will start out with the Network design and explain why the components need to be placed where they are being placed. Then the design of the Active Directory will be discussed in detail along with the needed Organization Unit layout. Finally we will elucidate the Group Policy Object design needed to make the GIAC Enterprise Network and Windows 2000 AD design secure.

Network Design

The diagram on the following page (Figure #1) shows the proposed network design for GIAC Enterprises offices in Ann Arbor, Michigan. Starting at the top is shown the Internet Firewall which is in place to block all access to the internal networks except the traffic that we want to allow. The firewall will be setup in such a way as to allow access to the public web server by anonymous users on the Internet. It will allow this access via Port 80 or 443 so that SSL can be used for secure transactions with users on the Internet. It will also allow VPN connections between the external sales force and the internal network through the use of the Remote Access Server.

The Remote Access Server will be setup to allow for PPTP (Point to Point Tunneling Protocol) connections. The high encryption package will be installed on the Remote Access Server so that the highest encryption can be utilized for the best security during remote access by the sales force.

The public web server will be configured to run IIS 5.0. A Verisign digital certificate shall be purchased to allow for trusted SSL communications with external users. There will be no access allowed from the public web server to the internal network except for communications directly back to the database server for external user account information. It must be noted that in no way will any critical information like credit card numbers be stored on the external web server. It is also further noted that any new accounts that are setup by the external users are placed into a separate area of the database server awaiting approval of credit card information. In no way will the external web server be able to have access to the critical information on the database server.

The internal firewall will be setup in such a way as to protect the internal network resources from being corrupted by the Demilitarized Zone systems. The internal firewall will allow for communications between the Remote Access Server and the Radius Server for authentication of the external sales force. It will also be configured to allow for access to the public areas of the database server from the public web server. The only other access that will be allowed is between the Remote Access Server and the internal web servers where the external sales force does all their work. No other access will be allowed through the internal firewall.

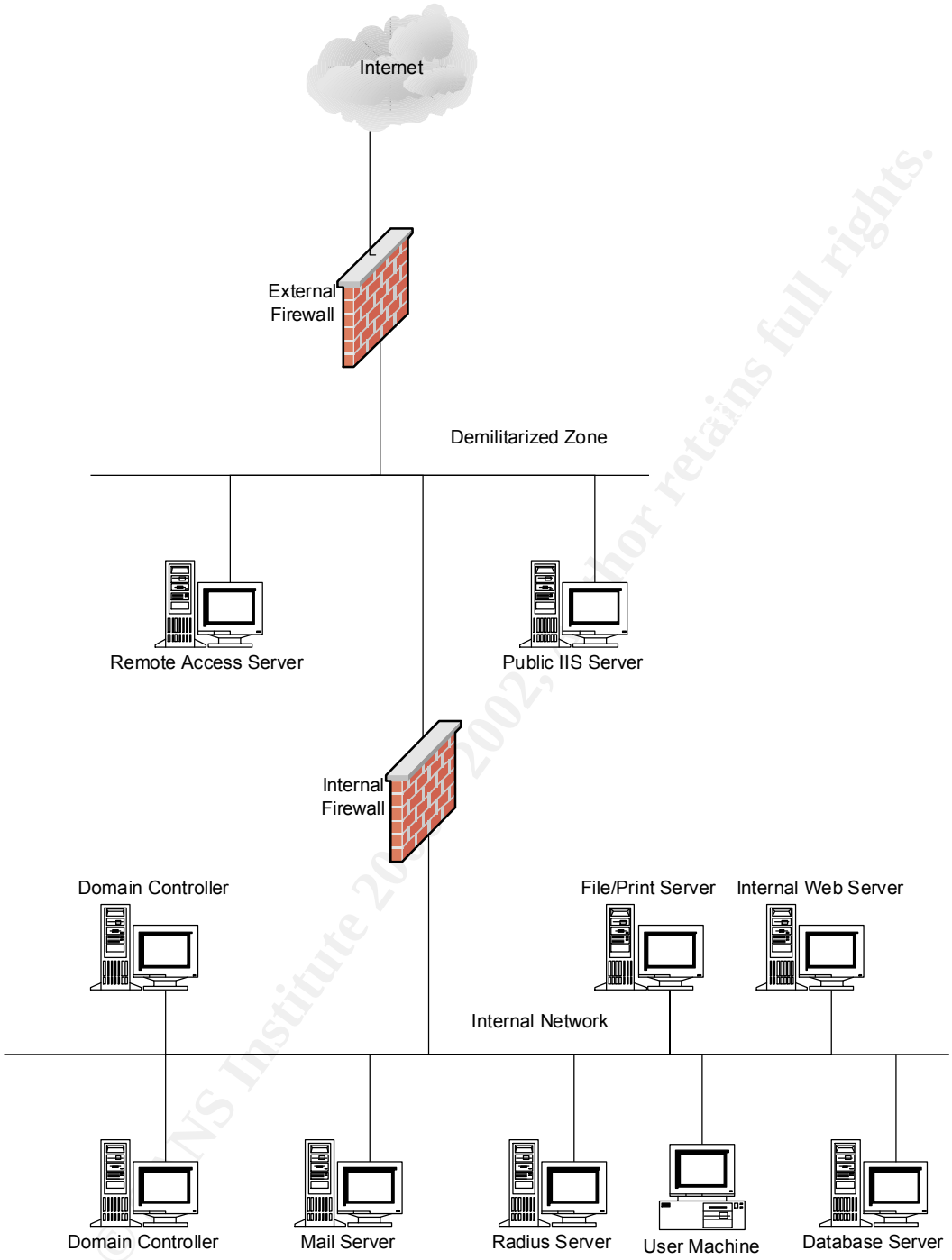

Figure #1

On the internal network there exist a number of servers. Two domain controllers are the mainstay of the Active Directory control for the entire corporations' network. A mail server running Microsoft Exchange does all internal and external mail. The radius server performs authentication and authorization for the external sales force and their VPN access through the remote access server. The File/Print server contains all users home directories and queue management for all printers within the corporate network. The

internal web server is used by all departments for everything from database manipulation to employee information dispersal. The database server contains a database of all employee information, all order and other financial information as well as a database of all external users.

Active Directory Setup

The diagram in Figure #2 shows the proposed layout of the Active Directory Structure including the domain GIAC and the various Organizational Units. The premise behind the design is to both deal with the current security and performance requirements of GIAC Enterprises and to setup for the future growth of the company. One domain has been designed into the structure. If in the future GIAC Enterprises decides to branch out and have remote locations it will be necessary to create more domains and add them to the forest that is already in place.

The design incorporates different Organizational Units for select groups of servers and elements within the GIAC Enterprises corporate structure. On the server side we have separated out the domain controllers from the web servers and kept these devices separate from the file/print, database and other servers. This was done to allow for separate control of the various types of servers. Organizationally we have created place holders for the various organizations within GIAC Enterprises. These consist of the following units:

- Research and Development – Users and Workstations
- Sales and Marketing – Sales Users, Marketing Users and Workstations
- Corporate Management – Users and Workstations
- Information Systems – Users, Help Desk Users and Workstations
- Finance and Human Resources – Human Resources Users, Finance Users and Workstations

The single domain model employed in the design is sufficient for the current needs of GIAC Enterprises. Group policies will be developed to be applied across the domain for things like Internet Access and general user permissions and rights. These will be supplemented by the individual group policies applied at the organizational unit level for each grouping of users and workstations.

In order to separately control the different kinds of servers it was necessary to break out the servers into different organizational units. The domain controllers have their own separate unit because they need to be configured with different audit and security features than a normal server. The web servers have a separate unit so that they can be grouped together and managed as a unit with group policy. The rest of the servers have been grouped separately from the workstations so they can be managed as a group.

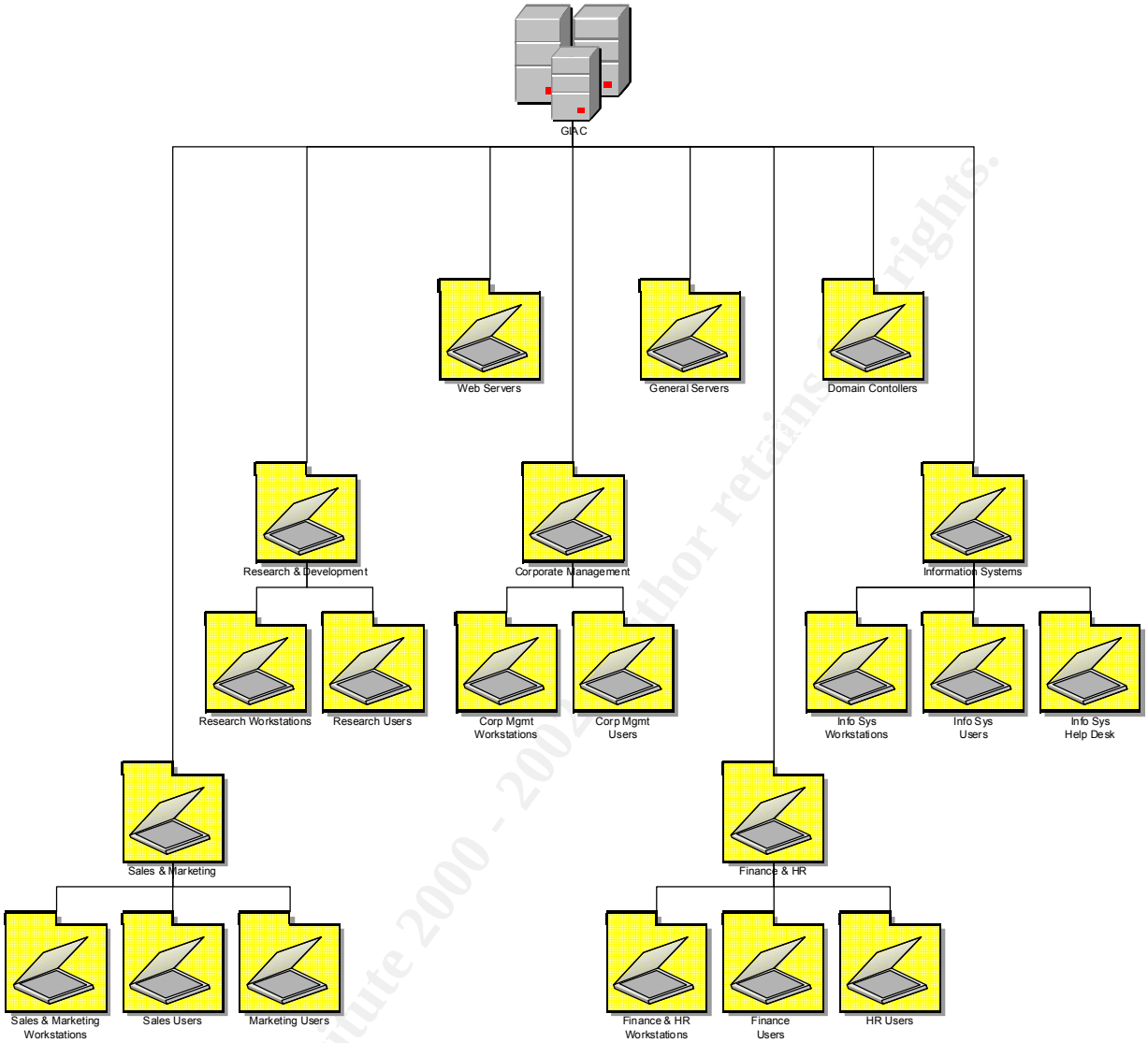

Figure #2

Each organization in GIAC Enterprises is separated out and given a place holder organizational unit. These placeholders are simply there to make the management of the group policies a bit easier. The placeholders will have no group policies actually applied to them. The group policies for user and computer configurations will be applied at the next level below the placeholders where the user and workstation organizational units exist.

Starting at the left side of the diagram in Figure #2 the Sales and Marketing organization structure is depicted. It is broken up into three different organizational units consisting of a workstation unit, a sales users unit and a marketing users unit. The workstation unit exists to allow for group policy to be set specifically for sales and marketing workstations. The breakup of the sales and marketing users into two different organizational units was done to make grouping of the users that have rights to dial-up the network easier to manage.

The next grouping is for the Research and Development organization. This group is split into two separate organizational units. First is the workstations unit where any group policies that are specific for the research and development workstations can go. Second is a users organizational unit where any specific group policies relating to research and development users can go.

The next group is for corporate management. This group like the research and development group is separated into two organization units, one for workstations and one for the users. The reasoning behind this separation is the same as for the research and development workstations and users.

The next group on the diagram still working our way from left to right is the Finance and Human Resources group. This group is split into three organizational units, one for workstations, one for Finance users and one for Human Resources users. The breakup of finance and human resources users is to allow for easier grouping of the human resources users which will have rights to edit active directory information on individual users. The finance users don't have this ability because they are not responsible for the management of non computer related information in the active directory. Finance however does need access to the financial information that human resources doesn't need so splitting these groups up makes sense.

The last group is the Information Systems group which is split into three organizational units. The first unit is for workstations and will basically get the standard workstation policies for the domain. The second and third units are for general users and help desk users. The help desk users have a limited scope on what they are allowed to change within the active directory. They are basically limited to being able to change or set passwords, enable and disable accounts and unlock accounts. The general users group in Information Systems has the ability to create, modify and delete accounts, add users to global and/or local groups, create global and local groups and basically do everything that the help desk can do as well.

The last discussion of the active directory setup is on performance. It was felt that the importance of putting in the place holders for each organizational unit was much more beneficial than any performance issue that they raised. It is not expected that these place holders will have any group policies applied at their level and so will not figure into the security settings each time a computer is booted or logged into. The separation of workstations and users should improve performance because group policies for workstations will have their user configuration sections turned off and the group policies for users will have their computer configuration sections turned off.

From a security standpoint, having the groups separated by the same organizational model allows for future self control by the organizations as GIAC Enterprises gets bigger. It will be much easier down the road to give users in each organization control over their organizational units if they are originally setup to allow for it at the beginning. For now the security and centralization of having the Information Systems department being the

only users that have full control over the active directory and the information inside of it, except for personal information which is controlled by Human Resources, allows us to provide for exceptional control over group policy.

Group Policy Setup

In the following pages we will go over the proposed group policy setup. The group policies for each Domain and Organizational Unit will be discussed as needed to show any changes from the base domain policy. Because of the basic layout of our Organizational Unit structure there is very little overlap between computer policies and user policies.

Domain Policy:

The domain level group policy is the place where issues like password aging, length, number of attempts and complexity are dealt with. These have been dealt with in our domain level group policy as well as account lockout policy, a legal warning message before logon, auditing, event log issues and some miscellaneous other issues with programs like windows explorer and internet explorer. Some user policies are also dealt with at the domain level including the setting up of a screen saver policy that will be applied domain wide.

To set the policies in the following tables you must bring up the domain group policy editor by performing the following procedure:

1. Start up a copy of the Microsoft Management Console that has the Active Directory Users and Computers Snap-In.
2. Double click on the Active Directory Users and Computers Snap-In. This will expand to show your domain.
3. Right click on the domain name and select properties from the pop-up window.
4. At the top of the dialog that gets displayed click on the tab for Group Policy.
5. Highlight the default domain policy line in the window that appears.
6. Click on the edit button to get to the group policy editor.
7. Expand Computer Configuration by clicking on the + sign to the left of the title.

Password:

The first set of policies we will deal with is the ones controlling password policy. To get to the section of group policies open up the Computer Configuration->Windows Settings->Security Settings->Account Policies->Password Policy. The first password policy is history. The enforce password history setting will be set to 24. This means that the last 24 passwords will be retained for each user by the system and the system will not allow any of these 24 passwords to be used again.

Another policy that gets set with this group is the password age; both minimum and maximum. The maximum age controls how long a password is good for, in our case it is set to 90 days. This was selected as a compromise to try and get people to come up with good passwords while giving them the chance to get accustomed to the password so they won't write it down on a sticky note and paste it on their monitor. The minimum age is set to 1 day. This is to stop people from effectively defeating the 24 password history rule. If this was shorter then people could just simply run through their last 24 passwords until their favorite password came up again.

The next policy that will be set is the one controlling the minimum password length. In our group policy we have set this to be 8 characters. This is a compromise between keeping this number large which makes for better passwords and keeping it short so that users can easily come up with good passwords.

The next policy that is set in this group is the one that enables the complexity requirements for passwords. With this set, enabled passwords must have at least 3 of the 4 types of characters in them (Uppercase Alpha, Lowercase Alpha, Numeric and Special Characters). It will also not allow any part of your username to be in the password.

The last policy in this group that we will set is the "Store password using reversible encryption for all users in the domain". This policy is set to disabled so that there is no possibility that a hacker could get a list of reversible passwords.

You set a policy simply by double clicking on it in the right hand pane of the console. Set the following policies as shown in the following table:

Policy	Setting
Enforce Password History	24
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the Domain	Disabled

Account Lockout:

To get to the next set of policies open up the group using Computer Configuration-> Windows Settings->Security Settings->Account Policies->Account Lockout Policy. In order to protect our systems from repeated attempts to guess passwords by hackers we need to slow them down some. This is what account lockout is meant to do. There are a few items we can set for this group of policies including the duration, a threshold and a counter reset timing feature.

The duration is how long to lockout the account before the system will unlock it and allow another attempt at logon. In our policy we selected 30 minutes. This number was a compromise between generating a significant number of help desk calls from people getting themselves locked out and slowing down somebody that is actually trying to attack us.

The threshold was chosen to be 5 invalid attempts. This was chosen to be just beyond what a normal person might do in trying to remember their password, but short enough to catch the hacker that's trying to guess a password.

The counter reset policy item will be set to 30 minutes. This was chosen to make sure that any hacker attempting to guess passwords would have to wait at least 30 minutes between attempts.

So for account lockout policy set the following policies as shown in the table:

Policy	Setting
Account Lockout Duration	30 minutes
Account Lockout Threshold	5 invalid logon attempts
Reset Account Lockout counter after	30 minutes

Audit Policy:

The next set of policies that need setting are in Computer Configuration->Windows Settings->Security Settings->Local Policies->Audit Policy. These settings deal with what gets audited and written to the event logs (the policies of which we will set later).

The first auditing policy is "Audit Account logon events". This policy will be set to log both success and failure because we absolutely want to be able to determine who has had access to our computers and when. Also the failure of these events will help us determine if an attacker is attempting access.

The next auditing policy is "Audit Account Management". This policy will be set to log both success and failure. This policy logs an event when somebody changes an account, adds an account or deletes and account. We want to track this so that accounts do not get setup with special privileges without us knowing about the change.

The next auditing policy is "Audit logon events". This policy will be set to log only failures. In addition to the account logon events set above, this policy will log the failure of somebody trying to access the local system. This policy is important because it shows us locally based attacks on the system. The difference between the account logon events and this one is basically the account logon events shows the success or failure at the domain controller whereas this event shows the success or failure of local logon events.

The next policy in auditing that we want to set is "Audit policy changes". This policy will be set to log both success and failure. We absolutely want to see if somebody changes an audit, user rights or trust policy on a system, by logging both success and failure we see both attempts to and successful changes that are made.

The last policy that we will look into is the policy to audit privilege use. This policy we will set to log failures only. This event will basically show us any failure on the use of a user right by the user or system. This allows us to track if somebody is trying to attack the systems through the use of a non-granted user right.

So for auditing options set the following policies as shown in the table:

Policy	Setting
Audit Account logon events	Success, Failure
Audit Account management	Success, Failure
Audit logon events	Failure
Audit policy changes	Success, Failure
Audit privilege use	Failure

Security Options:

The next set of policies that need setting are in Computer Configuration->Windows Settings->Security Settings->Local Policies->Security Options. These settings deal with the logon process, password expiration notification, administrator and guest account naming and software installation behavior.

The first policy we will set is "Additional restrictions for anonymous connections". This policy is a means to place restrictions on the use of anonymous accounts like the Everyone account. We will set this to "Do not allow enumeration of SAM accounts and shares, this will block anonymous access to being able to list the usernames and shares that are available thereby stopping a hacker from using anonymous access to gather this critical information.

Normally with Windows 2000 when you logon after hitting Ctrl-Alt-Delete you are prompted with a username/password dialog box that has the username already filled in for you of the last user to logon to the system. The policy "Do not display last username in logon screen" removes this feature so that windows will not supply this information. We want to do this to remove the possibility of somebody just walking up to a system and getting a valid username right from the computer itself.

The next two policies are set for legal reasons. The policies "Message text for users attempting to log on" and "Message title for users attempting to log on" pretty much work together to create a dialog box that appears before the user is prompted for their username and password. An example message is shown below:

The computer system (including all software, electronic mail, and the network) you have accessed is for the sole use of Company-authorized users (including contractors, consultants, and Company employees) in their conduct of company-related business. Anything created, obtained or retained on the system is the property of the company.

All persons accessing the system without, or in excess of, their authority or otherwise inappropriately using the system are subject to disciplinary action, including termination, and/or criminal prosecution.

The company regularly monitors the system for maintenance and to investigate the activities of individuals suspected of improper usage. Anyone using the system herby consents to such monitoring. Any suspected misuse should be immediately reported to the local Corporate Security representative.

System users are accountable for the use and security of their passwords.

The next policy that will be set in this section of the group policy is the one dealing with notification to the user about password expiration. This policy is set to 14 days to give the user plenty of time to change their password before expiration.

The next policy deals with whether to allow or prevent users the ability to install printer drivers on their local machines. Since at GIAC Enterprises we have built our print management around a server, there is no local print devices and so this feature is not needed. Therefore, we will set this policy to enable which will prevent users from installing the print drivers.

The next two policies deal with renaming the built-in accounts for the administrator and the guest. It is a good idea to rename these accounts because all hackers in the world know these names just as well as you do. It opens the system up for a known attack. For our group policy we decided to name them smithj and jonesj.

The last policy in this section of the group policy is one that controls how unsigned non-driver software installation will proceed. The default for this policy is to allow the installation with no notification of the user. We will change this policy to have it warn the user that the software they are installing is not signed but will allow the user to still install it.

So for security options set the following policies as shown in the table:

Policy	**Setting**
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares
Do not display last user name in logon screen	Enabled
Message text for users attempting to log on	See text above

Policy (cont)	Setting (cont)
Message title for users attempting to log on	Important Notice
Prompt user to change password before expiration	14 days
Prevent users from installing printer drivers	Enabled
Rename administrator account	Smithj
Rename guest account	Jonesj
Unsigned non-driver installation behavior	Warn but allow installation

Event Logs:

The next section of policies we will look at all deal with the event logs. Since this is the domain group policy these settings will be the default for the entire domain. We will later update these policies for specific servers like the domain controllers.

The three event logs (application, security and system) all have the same policy controls that can be applied to them. These controls include the maximum size, the restriction of guest access and the retention of data method to use. In our case we will set the three logs the same so the discussion will only cover one log. For maximum length, a size of 10MB was selected. It was felt that 30MB on each system was not much disk space to give up for logging in this era of 20+ gigabyte hard drives.

The next policy dealt with guest access of the logs. We have elected to restrict this access so that the log files cannot be used against us by a hacker. With restricting guest access only an administrator on the system can view the logs.

The last part of this policy group is the retention of the log data. The retention can be set to rollover on a daily basis, on an as needed basis or to never rollover. The basic problem with the daily and never rollover options is that if the log exceeds the size of the log file set above then it just stops logging. It was felt that this was unacceptable. It would be better to have lost old information than to have lost new information. Therefore the retention policy on each log is set to "as needed".

The following table gives a summarization of the event log settings:

Policy	Setting
Maximum application log size	10240 KB
Maximum security log size	10240 KB
Maximum system log size	10240 KB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retention method for application log	As Needed
Retention method for security log	As Needed
Retention method for system log	As Needed

Internet Explorer:

The next group of policies is in a different location from the above policies so go to Computer Configuration->Administrative Templates->Windows Components. From here you will see the next two sections we will be adjusting.

First will be Internet Explorer policies. Since we want to be secure in our use of the Internet it becomes necessary to lock down some of the security features of Internet Explorer. This area of group policy is where we can accomplish this. The first policy we want to change is "Security Zones: Do not allow users to change policy". This will block users from being able to change the zone policy in their local browsers. We want to do this so that users cannot setup their systems to trust the Internet at a higher level. The default level in Internet Explorer for the Internet zone is a Medium level. Medium level makes Internet Explorer prompt before downloading any potentially unsafe content and any unsigned ActiveX controls will not be downloaded.

The next policy we will set for Internet Explorer will block the users' ability to add, modify or delete sites. This policy stops the user from being able to add an Internet site to the list of trusted sites or marking a site as an internal site.

The last policy for Internet Explorer that we will set is the one which makes Internet Explorer itself stop looking for new versions. We want to do this so we can control the version of Internet Explorer that our users are employing. If we don't do this then we will end up with people that don't upgrade and those that upgrade to beta software leaving us as administrators with a multitude of versions to deal with.

Windows Installer:

The next policy area we will discuss is located at Computer Configuration->Administrative Templates->Windows Components->Windows Installer. This section deals with the installation of software on the system. We would like to restrict the ability of users to add software to their systems that has not been approved by management and certified by Information Systems personnel. In order to do this we will disable the Windows Installer task. Set the policy called "Disable Windows Installer" to enabled.

Connection Sharing:

The last policy in this area is located under Computer Configuration->Administrative Templates->Network->Network and Dial-Up Connections. The policy we are going to set is "Prohibit configuration of connection sharing". The reason we want to prohibit the users from enabling or configuring connection sharing is because, we don't want our users to be creating multiple routes for the network. With this option set, the user will not be able to have a dial-in modem that allows access to our network. They will not be

able to dial-up an Internet Service Provider and have somebody hack the connection and gain access to our internal network through that connection.

In the following table is a summary of the policy changes to make in this area:

Location	Policy	Setting
Windows Components->Internet Explorer	Security Zones: Do not allow users to change policy	Enabled
Windows Components->Internet Explorer	Security Zones: Do not allow users to add/delete sites	Enabled
Windows Components->Internet Explorer	Disable periodic check for Internet Explorer software	Enabled
Windows Components->Windows Installer	Disable Windows Installer	Enabled
Network->Network and Dial-up Connections	Prohibit configuration of connection sharing	Enabled

Screen Saver:

The next set of policies that will be set for the entire domain deal with User Configuration instead of Computer Configuration. This will be the only place where both computer and user configurations are used in the same group policy.

In order to get to the next group go to User Configuration->Administrative Templates->Control Panel->Display. Here you will find some policies that deal with the screen saver and other things that display with the display icon from the control panel including background selection, wallpaper selection, resolution setting and others. We want to make sure that everybody at GIAC Enterprises has a password locked screen saver in place so that every computer will lock after a period of 15 minutes. To do this we need to set 3 policies in this area. The first policy we want to set is "Password protect the screen saver". We want to enable this policy so that users will be forced to enter their password to re-access the system.

The next policy we want to set is "Screen saver timeout". We want to enable this and set its timeout to 900 seconds so we force an inactive computer to go to its screen saver after 15 minutes of inactivity.

The last policy we will set in this area is "Screen saver executable name". We will set this to ss3dfo.scr which is the screen saver that shows the Windows 2000 flag flowing in a simulated breeze. This screen saver is automatically installed on all Windows 2000 systems and so should be available on all our systems.

The following table summarizes the screen saver policy settings:

Policy	Setting
Password protect the screen saver	Enabled
Screen saver timeout	Enabled – 900 seconds
Screen saver executable filename	Ss3dfo.scr

Domain Controller:

This completes the design of the default domain group policy. We will now begin talking about the design of a group policy for the domain controllers for the GIAC Enterprises network. In order to get to the group policy for the domain controllers you must follow the below procedure:

1. Start up a copy of the Microsoft Management Console and open the Active Directory Users and Computers snap-in.
2. Highlight the domain name and double click to show the organization units that are below the domain as shown in Figure #2.
3. Find the entry for domain controllers and right click on it. From the pop-up menu that appears select properties.
4. A dialog box will appear with tabbed entries across the top. The rightmost one should be labeled Group Policy. Select it.
5. You should now see a line that says "Default Domain Controllers Policy". Select it and click on the button labeled "Edit".

The main things that will be set different in the domain controller group policy will be the audit and event logging strategy. Domain controllers need to log more information about the use of the systems than regular computers do. Therefore, the audit policies will be expanded to include the auditing of both success and failure for the following items:

- Account Logon Events
- Account Management
- Directory Service Access
- Logon Events
- Object Access
- Policy Changes
- Privilege Usage
- System Events

To select these go to Computer Configuration->Windows Settings->Security Settings->Local Policies->Audit Policy. From here set the policies shown in the table to the settings show in the table:

Policy	Setting
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	Success, Failure
Audit system events	Success, Failure

The next area we need to change is the event logging policies. Whereas 10MB files were plenty for a standard computer it is no where near enough in size for a domain controller which logs all logon and logoff events as well as all domain access attempts.

To set the event log policies we need to go to Computer Configuration->Windows Settings->Security Settings->Event Log->Settings for event log. We will set these policies as shown in the following table:

Policy	Setting
Maximum application log size	30912 KB
Maximum security log size	30912 KB
Maximum system log size	30912 KB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed
Shut down the computer when the security audit log is full	Disabled

This will assure that we have plenty of log space for each of the audit logs. Each one is set to restrict guest access so that not just anybody can read the logs. Each one is set to overwrite data as needed, which means that we will get the full benefit of the 30MB for each log file, without the possibility of the systems not logging new data, which can happen if we chose the method of either manually or by days for retention method.

Other Servers:

The next group policies that will be set are for the two organizational units that control the other servers. For these other servers, group policies will be implemented that control

the audit and event logging policies. To create these policies perform the following procedure:

1. Start the MMC console that has Active Directory Users and Computers as a snap-in.
2. Open up the Active Directory Users and Computers snap-in and double click on the domain name.
3. Right click on the General Servers or Web Servers organizational units and select properties from the menu that pops up.
4. Select the Group Policy Tab from the top of the dialog box.
5. Click on the "New" button and name the new group policy either General Servers or Web Servers depending on which you are setting up.
6. Click on the "Edit" button to edit the group policy.

The first area we will change is the auditing settings. These will vary slightly from the ones set in the domain policy. The basic differences can be found in the fact that we will audit both success and failure of logon events, both the success and failure of system access events and the success and failure of object access events. These changes can be seen in the following table:

Policy	Setting
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit system events	Success, Failure

The next area we need to change is the event logging policies. Whereas 10MB files were plenty for a run of the mill computer and 30MB was the right number for the domain controllers. For the general and web server systems 20MB is a more appropriate number because we are logging slightly more than the average server, especially the log hungry IIS servers, but we are not logging as much as a standard domain controller.

To set the event log policies we need to go to Computer Configuration->Windows Settings->Security Settings->Event Log->Settings for event log. We will set these policies as shown in the following table:

Policy	Setting
Maximum application log size	20480 KB
Maximum security log size	20480 KB
Maximum system log size	20480 KB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	As needed

Retention method for security log	As needed
Retention method for system log	As needed
Shut down the computer when the security audit log is full	Disabled

Users Policy:

The next group policy we will be looking into will be the group policy for the users organizational units. There are many of these organizational units including sales users, marketing users, research users, corporate management users, human resource users, help desk users and finance users. We have left off the information systems users because they will have the default domain group policy applied which does not restrict users as much as the following group policy will. In order to get started perform the following procedure to get to where we are editing the group policy for a users organizational unit:

1. Start the MMC console that has Active Directory Users and Computers as a snap-in.
2. Open up the Active Directory Users and Computers snap-in and double click on the domain name.
3. Double click on the Organizational Unit Placeholder of where you want to set the group policy (like Sales & Marketing or Finance and Human Resources).
4. This will open up the organizational unit placeholder. From here select the users organizational unit you want to work with and right click on it. Select properties from the menu that pops up.
5. Select the Group Policy Tab from the top of the dialog box.
6. Click on the "New" button and name the new group policy. We recommend either something like "Sales Users" or "Users: Sales".
7. Click on the "Edit" button to edit the group policy.

The policies we will set using group policy for the general user population will involve restricting use of certain elements of Internet Explorer, Windows Installer and Microsoft Management Console. First we will go over the changes to be made to Internet Explorer. The first change we want to make is to make it so the general user cannot make changes to the security settings or advanced settings that get set in the Internet Explorer Control Panel. To do this we need to go to User Configuration->Administrative Templates->Windows Components->Internet Explorer->Internet Control Panel. From here we will simply disable the appropriate policies which will remove the tabs from the users Internet Explorer Control Panels. See the following table for a summary:

Policy	**Setting**
Disable the Security Page	Enabled
Disable the Advanced Page	Enabled

The next policies we want to change for Internet Explorer are in User Configuration->Administrative Templates->Windows Components->Internet Explorer. Here we will

block the users ability to auto complete forms, including the blocking of password saving by the user. We do this for security reasons. Having the user store in the clear, passwords to various web sites locally on the machine in an accessible location is not an acceptable practice. The following table summarizes these policy settings:

Policy	Setting
Disable AutoComplete for forms	Enabled
Do not allow AutoComplete to save passwords	Enabled

The next policies we will set involve the Windows Installer. You can get to these policies using User Configuration->Administrative Templates->Windows Components->Windows Installer. There is only one policy we need to modify in this area and that is to disable the ability of the general user to load new software from removable media. The following table summarizes the policy settings for Windows Installer:

Policy	Setting
Disable media source for any install	Enabled

The next policies we want to set involve the Microsoft Management Console. For normal users we want to restrict access to various snap-ins' like Active Directory Users and Computers and Active Directory Domains and Trusts. In order to accomplish this we need to go to User Configuration->Administrative Templates->Windows Components->Microsoft Management Console. Here we will first set the policy that enables the restricted list of snap-ins by enabling the "Restrict users to the explicitly permitted list of snap-ins". After setting this policy we need to double click to go to the "Restricted/Permitted snap-ins" folder to set the snap-ins that we are going to allow. The following table lists the policies we need to set for the Microsoft Management Console:

Policy	Setting
Restrict users to the explicitly permitted list of snap-ins	Enabled
Computer Management	Enabled
Disk Management	Enabled
Disk Defragmenter	Enabled
Fax Service	Enabled
Local Users and Groups	Enabled
Performance Logs and Alerts	Enabled
Services	Enabled
Shared Folders	Enabled
System Information	Enabled
Telephony	Enabled

The last policy we need to set for general users is the one that will remove the add/remove programs icon from the control panel and anywhere else its possible to add and/or remove programs. To do this we need to be at User Configuration-

>Administrative Templates->Control Panel->Add/Remove Programs. We simply need to enable the policy for "Disable Add/Remove Programs". The following table summarizes this policy setting:

Policy	Setting
Disable Add/Remove Programs	Enabled

Other Miscellaneous Configuration

There are a few things that will need to be setup for GIAC Enterprises that are not covered by group policy. The first one is Active Directory permissions. The Information Systems users (not help desk users) will be the only group that can edit any property of the active directory entry for a user. It will be necessary to have the Human Resources users grouped in such a way as to allow for only specific fields to be editable. The help desk users will also need to be grouped in such a way that only the fields they should be able to edit can be edited by the group.

In the sales users organizational unit the user accounts will all need to be setup with dial-in permission so that the sales force can get access to the internal network while they are on the road. The finance users will also need to be given permissions to access the database servers in such a way that they can process the financial books.

Other miscellaneous tasks that will need to be accomplished include the configuration and setup for the Routing and Remote Access Server, the configuration of the public Internet Information Server including the lock down of the web services to prevent hackers from breaking the server. Also, the configuration of the Internet Authentication Server will need to be accomplished to allow the sales force to login remotely. The database servers will need to be setup to allow for Active Directory permissions and authentication use so that access to the company's data is secure. And, just like the public web servers the internal web servers should be locked down tight as well.

Conclusion

In conclusion if GIAC Enterprises follows through with the plan in this document they will end up with a secure environment that allows them to both perform their e-commerce across the Internet, and still be secure from hackers whether they be on the inside or outside.

In this document we have explored a number of different aspects of the design required to secure the GIAC Enterprises network including the network design itself. The network design consisted of a relatively flat network on the inside to allow for the most flexibility. It included two firewalls for protection of the perimeter. This two firewall design allows us to have a De-Militarized zone where we can put our limited public resources for supporting the e-commerce that is GIAC Enterprises life blood. Traffic through the outside firewall can be severely restricted to just the public web server and the remote

access server. The inside firewall can then be structured and designed such that access by the public web server and remote access server is restricted to just the database server and internet authentication servers respectively. In the future it might be necessary to break up the internal network into separate smaller networks connected together by routers but at this stage of GIAC Enterprises growth it is not deemed necessary.

The next thing this document explored was the design for an Active Directory layout, including a proposed organizational unit layout. The single domain model was chosen because GIAC Enterprises does not have multiple locations to be concerned with. This automatically leads us to a single domain model. The organizational structure was chosen to allow for the further expansion of the model as GIAC Enterprises grows. The model used included some placeholder organizational units for the major groups within GIAC Enterprises. These groups were Sales and Marketing, Research and Development, Corporate Management, Finance and Human Resources and Information Systems. In all cases for these groups a workstation organizational unit was created as a holder for that departments' workstations. In the case of Research and Development and Corporate Management only one other organizational unit was created to hold the users for that department. In the case of Sales and Marketing it was necessary to split the sales and marketing users into two separate groups due to the requirement of the sales force to be able to login remotely across the Internet. In the case of the Finance and Human Resources departments it was necessary to separate them due to the requirement that Human Resources be able to edit fields within the active directory. In the case of the Information Systems department it was required that the help desk users be separated from the rest of Information Systems so they would not have the unrestricted accounts that the rest of the Information Systems users had.

The next topic to be addressed by this document was the layout of the group policies for the domain, the domain controllers and the users. A fairly restrictive policy set was selected so that normal users could not change their systems by adding or removing software. The domain was setup to be relatively secure and to provide a template for the workstations in the domain. The domain level of group policy specified the password policy, account lockout policy, audit policy and event log policies for the domain. It also set some miscellaneous policies for things like renaming the administrator and guest accounts, setup a login message warning about usage of the system for things other than the business of GIAC Enterprises, and setup so there is no last name displayed at logon so hackers can't guess usernames. It also set policies to prevent users from loading printer drivers and setup to warn users 14 days in advance of their password expiring. Using the domain group policy we also setup Internet Explorer so that the security levels could not be changed. We disabled Windows Installer and stopped anybody from creating a backdoor into the network by turning on connection sharing. We set a domain wide policy for a screen saver to activate on everybody's desktop after 15 minutes of inactivity, and for it to lock the screen, thereby requiring the user to re-enter their password.

The group policy continued in the setting of separate policies for domain controllers and the other servers. This consisted mostly of changing the audit and event log policies

since the domain policy was very restrictive to begin with. We then setup a user policy that should be applied to every group except the information systems users organizational unit. This policy went even further to restrict the ability of Internet Explorer to do auto-complete functions including the saving of passwords that users might use online. We disabled the Windows Installer from being started from removable media like CD-ROMS and floppy disks. The next item that was restricted was the users ability to load any snap-ins that were not explicitly defined into the Microsoft Management Console. The last thing that we did with the policy for users was to remove the ability of a normal user to use the Add/Remove program system via the control panel.

The last section of this document talked about some of the other security configurations that would need to be completed to truly have a secure environment. This included discussions about grouping the various users into groups to allow them to have different permissions into things like file systems, printers and most of all the Active Directory.

If GIAC Enterprises follows the security template and layout as described in this paper we feel they will have a very usable but highly secure environment with which to work with. The concept of having a small organization with this high level of security is not usual in the industry but we feel that if GIAC Enterprises starts off with a high level of security that it will be much more capable of maintaining it as the company grows.

References

"Windows 2000 Group Policy." URL:http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp, (December 10, 2001)

"Introduction to Windows 2000 Group Policy." URL:http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.asp, (December 11, 2001)

"Microsoft Windows 2000 Advanced Server Documentation.", URL:http://www.microsoft.com/windows2000/en/advanced/help/ (Active directory->Concepts->Planning for Active Directory->Planning organizational unit structure.) (December 14, 2001)

"Windows NT 5.0 Group Policy." URL:http://pot-pourri.fltr.ucl.ac.be/wint40/win2000/groupe_policy/GroupPolicyNT5.htm, (December 15, 2001)

Fossen, Jason. "Securing Windows." GIAC training course from San Diego SANS Conference October 2001.

Microsoft Inc. Designing a Secure Microsoft Windows 2000 Network. Microsoft Training and Certification Course Number 2150A, Ikon Training facility Troy, Michigan November 2001.

Last Updated: May 26th, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**