Global Information Assurance Certification Paper

Design a Secure Windows 2000 Infrastructure

Practical Assignment Version 3.1 Option 1

Gary Newcomb
10/30/2002

Table of Contents

1. INTRODUCTION 5

1.1. Description of GIAC Enterprises 5

2. NETWORK DESIGN AND DIAGRAM 8

2.1. Site Design 8
2.1.1. Sites 9
2.1.2. Site Links 9
2.1.3. Site Link Bridges 9
2.1.4. Subnets 9
2.1.5. KCC 9

2.2. Infrastructure Location 9
2.2.1. Domain Controller 9
2.2.2. Global Catalog 9
2.2.3. Domain Name Master 10
2.2.4. Schema Master 10
2.2.5. RID Master 10
2.2.6. Infrastructure Master 10
2.2.7. PDC Emulator 10
2.2.8. Exchange Infrastructure 10
2.2.9. DNS 10
2.2.10. Other servers 10
2.2.11. Server hardware specifications 11

3. ACTIVE DIRECTORY DESIGN AND DIAGRAM 13

3.1. Forest/Domain Design 13

3.2. OU Design 13

3.3. DNS Design 17
3.3.1. Zones 18
3.3.2. Root Hints 18
3.3.3. Forwarders 18

4. GROUP POLICY AND SECURITY 19

4.1. Default Domain Policy 19
4.1.1. Computer Configuration/Windows Settings/Security Settings 19
4.1.1.1. Account Policies/Password Policy 19
4.1.1.2. Account Policies/Account Lockout Policy 20
4.1.1.3. Local Policies/User Rights Assignments 21
4.1.1.4. Local Policies/Security Options 21
4.1.2. User Configuration/Windows Settings/Scripts 22

4.2. Default Domain Controller Policy 23
4.2.1. Computer Configuration/Windows Settings/Security Settings 23
4.2.1.1. Local Policies/Audit Policy 23
4.2.1.2. Local Policies/User Rights Assignments 24
4.2.1.3. Local Policies/Security Options 24
4.2.1.4. Event logs/Settings for Event Logs 28
4.2.1.5. Services 29
4.2.2. Computer Configuration/Administrative Templates/ 30
4.2.2.1. System/Group Policy 30

5. ADDITIONAL GROUP POLICY 31

5.1. Resources/Office/Workstations OU 31
5.1.1. Computer Configuration/Windows Settings/Security Settings 31
5.1.1.1. Local Policies/Audit Policy 31
5.1.1.2. Local Policies/Security Options 32
5.1.1.3. Event logs/Settings for Event Logs 32

5.2. Resources/Office/ Servers OU 32
5.2.1. Computer Configuration 33
5.2.1.1. Local Policies/Audit Policy 33
5.2.1.2. Windows Settings/Security Settings/Local Policies/Security Options 33
5.2.1.3. Windows Settings/Security Settings/Event logs/Settings for Event Logs 33
5.2.1.4. Windows Settings/Security Settings/Services 33
5.2.1.5. Administrative Templates/System/Group Policy 34

5.3. User Accounts/ Contractors User Configuration/Administrative Templates 34
5.3.1. Windows Components/Internet Explorer 34
5.3.1.1. Offline Pages 35
5.3.1.2. Browser menus 35
5.3.2. Windows Explorer 35
5.3.3. Microsoft Management Console 35
5.3.4. Task Scheduler 36
5.3.4.1. Windows Installer 36
5.3.5. Start Menu & Taskbar 36
5.3.6. Desktop 36
5.3.7. Control Panel 37
5.3.7.1. Add/Remove Programs 37
5.3.7.2. Display 37
5.3.8. Network 37
5.3.8.1.1. Offline Files 37
5.3.8.2. Network Connections 37
5.3.9. System 38
5.3.9.1. User Profiles 38
5.3.9.2. Scripts 38

6. ADDITIONAL SECURITY 38

6.1. Domain Controller settings 38

6.2. Member Server settings 39

6.3. Internet Web servers 39

7. CONCLUSION.....42

8. REFERENCES.....44

1. Introduction

1.1. Description of GIAC Enterprises

This paper will discuss the design and implementation of a secure Windows 2000 infrastructure for a fictional company called GIAC Enterprises. Section 1 will discus GIAC Enterprises' business model, organizational structure, the physical layout of GIAC Enterprises' network, and its' information technology infrastructure. Section II will discuss the network design for GIAC. Section III will discuss the Active Directory design for GIAC. Section IV will discuss how Group Polices applied at the domain and domain controller organization unit will be utilized to enhance security at GIAC. Section V will discuss additional Group Polices to be applied at the server, workstation and user organizational unit level. Finally section VI will discuss additional security measures the domain controllers, member servers, and the Internet web servers.

GIAC Enterprises is a startup company providing online fortunes via it's; web site, Prophecy.com. The web site provides the public with fortunes of all types, from traditional horoscopes personalized for an individual to more exotic fortunes based on Yi Ching. GIAC is based in New York City, NY with an office in Boston, MA

GIAC Enterprises is a small but growing firm with 100 employees in NYC and 25 additional employees in Boston. GIAC Enterprises has six major departments, Research and Development, Sales and Marketing, Finance, Human Resources, Legal, and Information Technology. The R&D department is located in the Boston office. The Sales department will use contract employees for telemarketing purposes. The Marketing department will use contractors to maintain and update the Prophecy.com website. Other department may use contractors for temporary clerical help.

GIAC Enterprises' two offices are each connected to the Internet via a T1 circuit and to each other via virtual private network (VPN) over the Internet. The internal network at each office is protected by a firewall between it and the Internet. The NYC office infrastructure consists of two domain controllers, one file and print server, two clustered Exchange servers, and one misc. server that will host DHCP services. The Boston office consists of two domain controllers, one file and print server which will also provide DHCP services for the client workstations and two servers dedicated to the R&D department. The R&D servers are isolated on their own virtual network.

GIAC Enterprises' has a web farm and application servers located at major ISP's datacenter. This is a co-location arrangement; GIAC administers the servers but not the network. The benefits to GIAC include reduced cost for large pipes to the Internet, the ability to quickly increase the minimum and maximum bandwidth available, load balancing for the web servers, intrusion detection, and firewall services without additional capital and manpower expenditures. GIAC also avoids the

expense of building its' own DMZ to host the Internet facing web servers. Since GIAC is relatively small, acquiring staff to duplicate the services provided by the ISP would be very expensive. GIAC can access daily reports via a web site at the ISP on web server traffic and attempts at unauthorized access.

The web servers are not integrated into the Active Directory structure of the firm. GIAC will administer the remote servers with W2K Terminal Services connecting via a VPN. Security for these servers will be discussed in the additional security section of this document.

As GIAC is a startup it will buy all new hardware for its servers and workstation. All the servers will run Windows 2000 Server and the workstations will use Windows 2000 Professional. All servers and workstations will have Service Pack 3 loaded. GIAC will use the hot fix utility Hfnetchk to determine what patches must be applied to servers and workstations. All servers will be located in secure rooms with emergency power and air conditioning services.

Given the fiercely competitive nature of the online fortune market security is of paramount concern to GIAC Enterprises. GIAC's security policy requires that

- Access to the servers and workstations is limited to legitimate users.
- Each user or support person has the minimum level of access required to perform their duties.
- Access to domain resources and critical events are tracked.
- The configuration of the servers and workstation is consistent across the organization.
- That user account settings are configured for maximum protection from unauthorized persons.
- All superfluous services are disabled to minimize vulnerabilities.
- The desktop environment of contractors at GIAC is managed and standardized.

GIAC requires that all servers and workstations names are standardized. Name standards for servers and workstations are detailed below.

Servers

- The first 4 characters denote the domain of which the server or workstation is a member.
- The next 3 characters indicate the location of the server. The location is not too granular such that a server move would imply a server rename, but granular enough such that a server's location can be determined from its name. E.g. NYC
- The next 2 characters indicate the function i.e.: domain controller, application server etc. It may contain any combination of numbers or characters. E.g. DC for domain controller.
- The next 2 characters are used to ensure uniqueness. i.e.: 99

- The final character is optional and used to denote special applications like a cluster.

Workstations

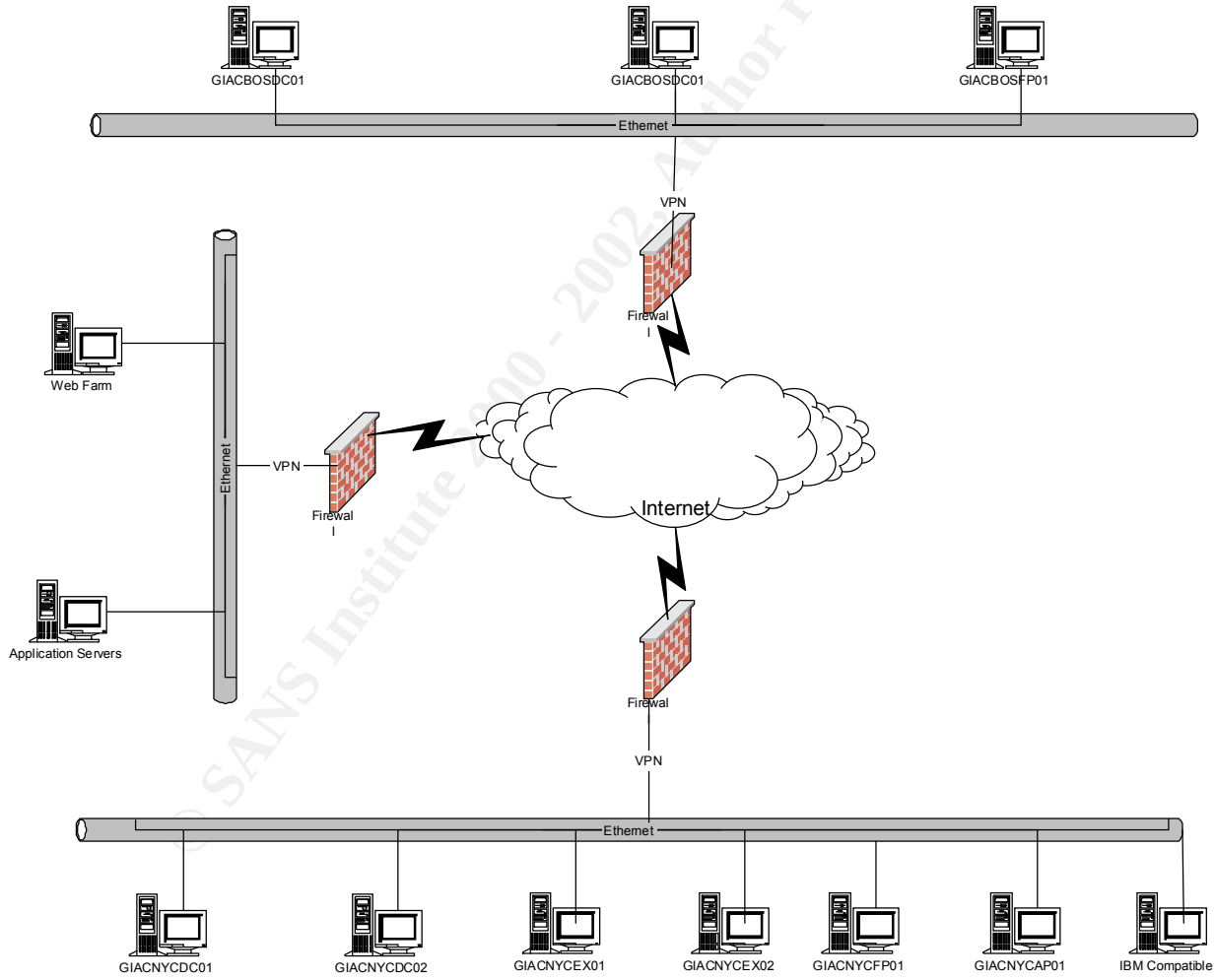
- The first 4 characters denote the domain of which the server or workstation is a member.
- The next 3 characters indicate the location of the workstation. E.g. NYC
- The next 2 characters indicate the function i.e.: WS for workstation.
- The final 3 characters are used to ensure uniqueness for a workstaion. E.g. 001
- The final 2 characters are used to ensure uniqueness for a server. E.g. 01

2. Network Design and Diagram

Section 2 will discuss GIAC Enterprises' network design. GIAC's networks will be protected from the Internet by firewalls. GIAC will use VPNs to connect the two office locations. GIAC will also use a VPN to connect to and manage its' web servers located at its' ISP datacenter. Each GIAC office will have a T1 connection to the Internet. Discussion of GIAC's firewall, VPN, routers and Ethernet switches is beyond the scope of this document.

2.1. Site Design

The diagram below shows the network configuration for GIAC Enterprises.



2.1.1. Sites

Sites will be defined by groups of subnets linked by a local area network. GIAC Enterprises will consist of two sites, one site for each office. Each office will be contained in one building.

2.1.2. Site Links

Site links will be used between sites linked by a wide area network. GIAC Enterprises will have a site link between the NYC and Boston office. GIAC Enterprises will use IP for the site link protocol with replication scheduled every thirty minutes.

2.1.3. Site Link Bridges

Active Directory automatically enables site link bridging. GIAC Enterprises has a small, simple network so this default behavior will not be modified. On a large and complex network use Microsoft Knowledge Base article **Q244368** to determine if site bridging should be disabled.

2.1.4. Subnets

GIAC Enterprises will create a subnet object for each network subnet and assign it location name. When a client searches for a local resource, Active Directory will show resources on the client's subnet. Subnet objects will follow the standard below.

Description – the description of the subnet, e.g. NYC HQ 5th floor East subnet
Site – the AD site where the subnet is located, e.g. NYC HQ
Location – the specific location of the subnet, e.g. NYC HQ/5th floor East

2.1.5. KCC

Due to its' small size GIAC Enterprises will use the Knowledge Consistency Checker to optimize the site link topology. In very large Active Directory implementations the KCC should be disabled.

2.2. Infrastructure Location

See Microsoft Knowledge Base article FSMO Placement and Optimization on Windows 2000 Domain Controllers (Q223346) for information on assigning FSMO roles. The specific roles for each server are discussed below.

2.2.1. Domain Controller

To ensure redundancy GIAC Enterprises will have two domain controllers at both of its' sites. The NYC HQ site will use two Dell PE 2650 servers. The Boston office will use Dell PE 1650 servers.

2.2.2. Global Catalog

All domain controllers will be global catalog servers.

2.2.3. Domain Name Master

The domain name master server will reside at the NYC HQ location. Server giacnycdc01 will fill this role.

2.2.4. Schema Master

The schema master will reside at the NYC HQ location. Server giacnycdc01 will fill this role.

2.2.5. RID Master

The RID master will reside at the NYC HQ location. Server giacnycdc02 will fill this role.

2.2.6. Infrastructure Master

The infrastructure master will reside at the NYC HQ location. Server giacnycdc02 will fill this role. Since this is a single domain/forest and all domain controllers are also global catalog servers this role is redundant. Also as giacnycdc02 is a global catalog server nothing would ever be updated in any case.

2.2.7. PDC Emulator

The PDC emulator will reside at the NYC HQ location. Server giacnycdc02 will fill this role.

2.2.8. Exchange Infrastructure

GIAC Enterprises will have one Exchange server located with the majority of the users at the NYC HQ site.

2.2.9. DNS

All domain controllers will run DNS services.

2.2.10. Other servers

GIAC Enterprises will have one file and print server at each site. The NYC HQ site will have an additional server that will provide DHCP, Symantec System Center, and other misc. services

Table 2.1 Server Roles

Location	Server Name	DC	Schema Master	Domain Master	RID	PDC	Infrastructure Master	GC	DNS	Dhcp
New York	giacnycdc01	X	X	X				X	X	
	giacnycdc02	X			X	X	X	X	X	
	giacnycfp01									X
	giacnycia01									X

Boston	giacbosdc01	X						X	X	
	giacbosdc02	X						X	X	
	giacbosdfp1									X

2.2.11. Server hardware specifications

This section will discuss the hardware specifications for GIAC servers.

Table 2.2 Domain Controller hardware specifications

Model:	Dell 2650	**CPU:**	2 x Xeon/1.8 or higher
RAM:	1 Gb	**Disks:**	PERC3 SCSI controller 5 x 36 Gb 2 disks RAID 1 3 disks RAID 5
NICs:	Dual, teamed NICs for failover.	**Remote Management:**	Dell Remote Access Card (DRAC)
Power:	Redundant	**Fans:**	Redundant
OS:	Server SP3 and hot fixes identified by Hfnetchk	**Other:**	SYSVOL/OS (C:) (16Gb mirror) AD Logs (D:) (16Gb mirror) AD Database (E:) (72Gb RAID 5) CD-ROM (Z:)

Table 2.3 File and Print server hardware specifications

Model:	Dell 2600	**CPU:**	2 x Xeon/1.8 or higher
RAM:	1 Gb	**Disks:**	PERC3 SCSI controller 2 x 36 Gb 4 x 72 Gb 2 disks RAID 1 3 disks RAID 5
NICs:	Dual, teamed NICs for failover.	**Remote Management:**	Dell Remote Access Card (DRAC)
Power:	Redundant	**Fans:**	Redundant

OS:	Server SP3 and hot fixes identified by Hfnetchk	**Other:**	SYSVOL/OS (C:) (16Gb mirror) Paging file and printer workspace (D:) (16Gb mirror) User Data (E:) (216 Gb RAID 5) CD-ROM (Z:)

Table 2.4 Misc. application server hardware specifications

Model:	Dell 2650	**CPU:**	2 x Xeon/1.8 or higher
RAM:	1 Gb	**Disks:**	PERC3 SCSI controller 2 x 36 Gb 2 disks RAID 1
NICs:	Dual, teamed NICs for failover.	**Remote Management:**	Dell Remote Access Card (DRAC)
Power:	Redundant	**Fans:**	Redundant
OS:	Server SP3 and hot fixes identified by Hfnetchk	**Other:**	SYSVOL/OS (C:) (16Gb mirror) Programs (D:) (16Gb mirror) CD-ROM (Z:)

Table 2.4 Exchange server hardware specifications

Model:	Dell 2600	**CPU:**	2 x Xeon/1.8 or higher
RAM:	2 Gb	**Disks:**	PERC3 SCSI controller 2 x 18 Gb 2 x 18 Gb 4 x 72 Gb 2 disks RAID 1 3 disks RAID 5
NICs:	Dual, teamed NICs for failover.	**Remote Management:**	Dell Remote Access Card (DRAC)
Power:	Redundant	**Fans:**	Redundant

OS:	Server SP3 and hot fixes identified by Hfnetchk	**Other:**	SYSVOL/OS (C:) (16Gb mirror) Logs (D:) (16Gb mirror) Data (E) CD-ROM (Z:)

3. Active Directory Design and Diagram

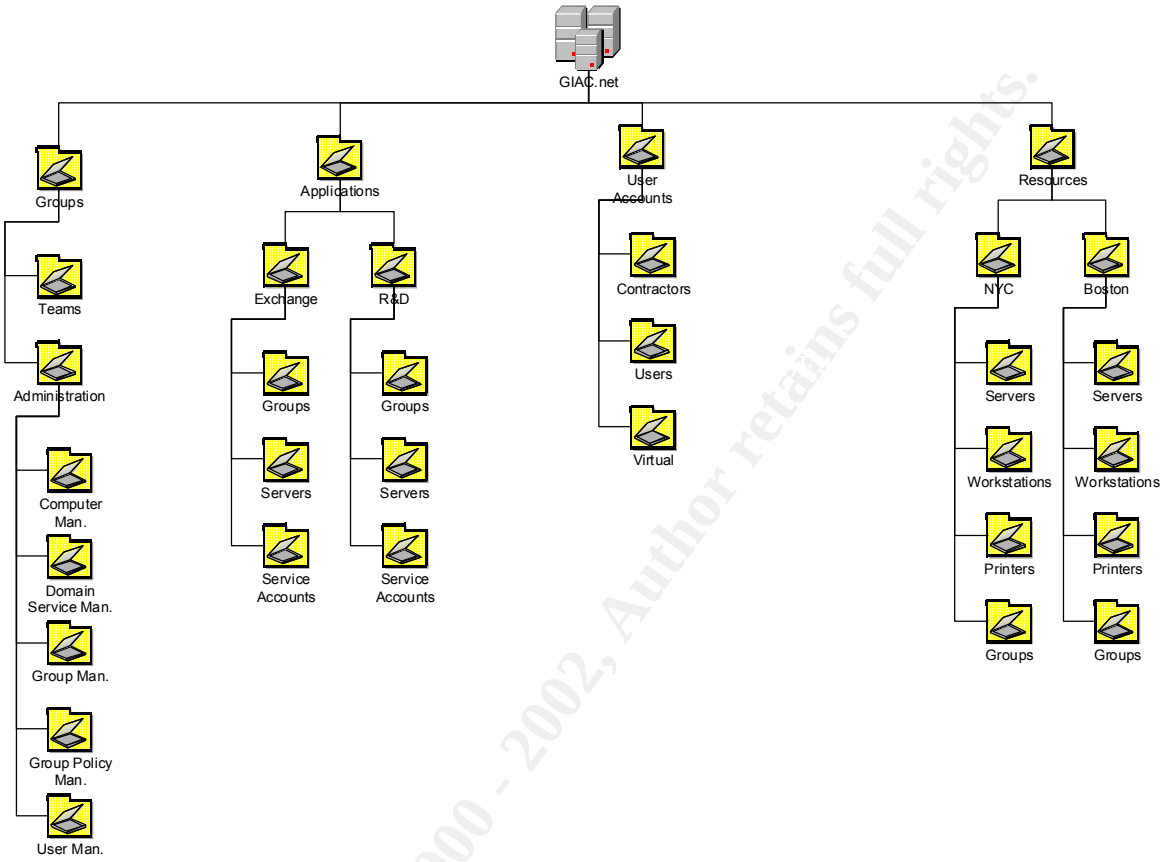
Section 3 of the document will discuss the design of GIAC Enterprises' Active Directory infrastructure. Active Directory organizational units and groups will play an important role in GIAC security objective of granting domain members and administrators the appropriate level of access for their role.

3.1. Forest/Domain Design

GIAC Enterprises is a small organization so it will utilize a one forest and one domain design. This will minimize the expense of deploying domain controllers and managing the Active Directory infrastructure. This strategy does mean that the ability to secure access to the Active Directory schema is not as robust. However, given the escalation of privileges exploit documented in Microsoft Security Bulletin MS02-001 "Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data" an empty placeholder/root domain is not justified. The GIAC Enterprises' domain name will be GIAC.net.

3.2. OU Design

In addition to the standard Active Directory organization units and containers, GIAC Enterprises will use the organization units diagramed below.



User accounts will reside in subordinate organizational units of the User Accounts OU. GIAC employees' accounts will live in the User Accounts/User OU; temporary employees' accounts will live in the User Accounts/Contractors OU. Temporary employees will include telemarketers, clerical workers, web developers, and others hired for special projects. This will facilitate customizing group polices for the different types of users

The Applications organizational unit will have two subordinate organizational units, the Exchange and R&D organizational units. This reflects the departmental structure at GIAC Enterprises and will allow those teams to administer their own servers, applications and groups without setting up separate domains for the departments. Servers that provide services to a specific location will be placed under Resources/*Office*/Servers organizational units. If the servers provide a specific application to the enterprise or don't service a specific location they will fall under the Applications/*App*./Servers OU.

Groups will be contained in the Groups/Administration/*Specific Role* organizational units, Applications/*App*./Groups and Resources/*Office*/Groups organizational units. Table 3.1 will provide more detailed information on the role and

contents of each OU, then the specifics of why GIAC is using multiple organizational units for groups will be discussed.

Table 3.1: Organizational Unit Design

OU Structure	Description/Example
Applications	e.g. Enterprise Systems, Infrastructure etc
Exchange	All Exchange objects
Servers	All Exchange server objects
Groups	All Exchange related group objects
Service Accounts	All Exchange service accounts
R&D	All R&D objects
Servers	All R&D server objects
Groups	All R&D related group objects
Service Accounts	All R&D service accounts
Groups	All team and administration group objects
Teams	All team groups
Administration	All administration groups
Computer Man.	Manages computers
Domain Services Man.	Manages domain services
Group Man.	Manages specific groups
Group Policy Man.	Manages group polices
User Man.	Manages user objects
Resources	All objects not managed by a dedicated team
Office	All offices will have this structure
Servers	All servers for a office (i.e. File & Print)
Workstations	All workstations for a office
Printers	All printer objects in an office
Groups	All group objects in an office
User Accounts	All users
Contractor	All contractors
Users	All associates
Virtual	All virtual users (using a portal, for example)

As stated previously multiple organizational units will contain groups. The Resources/*Office*/Groups will contain groups for each location that will be utilized to grant access to files and directories. Other groups will contain all users for a particular location or a subset of users at a location, such as a department. These groups will be used in the login script referenced in the Default Domain group policy.

The Groups organizational unit will have two subordinate organizational units, the Teams and Administration organizational units. These organizational units will contain all team and administration groups. Team groups will have individual as members while the Administration groups will have Team and other Administration OU groups as members. Teams are formed around function, such as Security or Site Support and have specific roles. Some of the groups are detailed in the table below.

Table 3.2: Groups by OU

Groups OU		
	Teams OU	
		Helpdesk
		Security
		NY Site Support
		Boston Site Support
Administration OU		
	Computer Management OU	
		Manage Computers All (this group is a members of the other Manage Computers groups)
		Manage Computers NYC
		Manage Computers Boston
		Modify Computers All (this group is a member of the other Modify Computers groups)
		Modify Computers NYC
		Modify Computers Boston
	User Management OU	
		Modify Users
		Modify Contractors
		Modify Virtual Users
		Modify All Users (this group is a member of the other Modify Users groups)
		Manage Users
		Manage Contractors
		Manage Virtual Users
		Manage Users All (this group is a member of the other Manage User groups)

The groups in the various Administrative organizational units will be assigned specific permissions to particular Active Directory objects. Active Directory has a very granular security model and we can take advantage of that feature to customize our delegation model. The table below shows what permissions will be assigned to the Manage/Modify User/Contractors/Virtual Users groups.

Table 3.3: Permissions for Manage/Modify User/Contractors/Virtual Users group

OU	Change User Objects (unlock accounts, change passwords)	Create/Delete User Objects
Users	Modify Users	Manage Users
Contractors	Modify Contractors	Manage Contractors
Virtual Users	Modify Virtual Users	Manage Virtual Users
All Users	Modify All Users	Manage All Users

Each group has a different role or set of permissions, the Modify Users/Contractors/Virtual Users group has the ability to unlock accounts and change passwords. The Modify All Users will be a member of all the other Modify/*User Object* groups in the User Management OU. Now a Team group can be added to any of these groups and it will inherit the assigned permissions.

For example the Helpdesk group from the Groups/Teams OU will be a member of the Modify All Users groups. This will allow the Helpdesk team to change passwords and unlock accounts for all users in the User Accounts OU and subordinate organizational units. The Security team will be member of the Manage All Users group, this allows them to create and delete all user accounts in the User Accounts OU and subordinate organizational units.

This structure allows us to create a delegation model where a set of permissions are assigned to a group which in turn has other groups/teams as members. If GIAC decides that a group/team should have different permissions or role the group/team can be deleted or added as a member in the appropriate group. This delegation model works best in a native mode domain where a global group can be nested in another global group. It is possible to partially implement this design in a mix mode domain using global groups in the Administration OU and domain local groups in the Team OU. However, it is not possible to create the Manage/Modify All groups as the Manage/Modify specific user/computer cannot be members of another global group.

3.3. DNS Design

This section of the document will discuss the design of the DNS infrastructure for GIAC Enterprises. Following guidelines in Microsoft Knowledge Base article DNS Namespace Planning (Q254680) the internal name space will not match the external name space. The internal name space will be the same as the domain name GIAC.net. The internal name space will not be visible to the Internet. Access to the internal DNS servers will be blocked except for responses to queries initiated by GIAC.net DNS servers.

3.3.1. Zones

The GIAC.net domain will run in native mode. The GIAC.net zone will be AD integrated. This reduces administrative overhead as AD will handle DNS replication. If a root or placeholder domain exists secondary copies of each domain zone should be placed on the other domains' DNS servers.

3.3.2. Root Hints

GIAC.net will leave the root domain hints but queries for non-GIAC.net resources will be forwarded to their ISP's DNS servers.

3.3.3. Forwarders

GIAC.net will forward any requests it is not able to resolve to GIAC Enterprises' ISP. Additionally the 'Do not use recursion' option will be enabled. This means that the GIAC DNS servers will rely only on the external DNS for resolution of other domains. If the ISPs' DNS cannot resolve the query the GIAC DNS will not query the roots hint servers to resolve the name. This has several advantages, traffic to and from the Internet is reduced, demands on the GIAC DNS's is reduced as the ISP's DNS server does the Internet related host lookups, no GIAC servers are directly exposed to the Internet and GIAC does not need to create an external own DMZ to host Internet facing servers.

4. Group Policy and Security

Section 4 will discuss the design of group polices for GIAC Enterprises. Polices will be assigned at the domain or OU level. The following sections are organized by domain or OU and then by Computer or User Configuration within the group policy. The sections are organized as they appear in the Group Policy MMC. The strategy for group policies at GIAC at the domain level is to minimize the number of policy settings and only apply polices that are universal. More specific and detailed group policies will be applied at the domain controller, server, workstation, and Contractor organization unit level. Hopefully this will result in simpler polices that are easier to support and troubleshoot.

GIAC will use Microsoft Corporations' Security Operations Guide for Windows 2000 Server as a guide to determining how to configure its' group polices. The SOG is a best practice document from Microsoft and uses the role played by a server as the basis for determining how to configure security via group policy. There are two broadly defined roles, that of domain controller and member server. Within the member server role there are several additional categories including, application server, file and print server, infrastructure server, and IIS server. The SOG is useful because GIAC's servers also fall into the same categories or roles and it contains specific suggestions for policy settings for the domain controllers and member servers.

The group policies implemented by GIACs will help limit access to workstations and servers to legitimate users; capture data that can be analyzed to detect and track unauthorized access; ensure the consistent configuration of servers and workstations; configure user account settings for maximum protection from unauthorized persons; minimize the number of services running on a server or domain controller; and manage the contractor's desktop environment.

4.1. Default Domain Policy

This section will discuss policies implemented at the domain level for all users and computers. The Password and Account Lockout policies must be set at the domain level. Any password or account lockout policies set at an OU level will not apply to a user unless they logon locally to that computer. The Default Domain group policies will be used to configure user setting for maximum protection from unauthorized persons.

4.1.1. Computer Configuration/Windows Settings/Security Settings

4.1.1.1. Account Policies/Password Policy

Password policies should bolster security but policies that are too stringent run the risk that users will write their passwords down or store them in another insecure manner.

GIAC Enterprises' password polices are at a medium level of security. This policy will configure user account settings to that the users have maximum protection from unauthorized persons by enforcing password history, setting a maximum and minimum password age, a minimum password length and require complex passwords.

Enforce password history: GIAC will set the password history to 12, Microsoft recommends a setting of 24 remembered password. A password history of 24 is appropriate for an organization which requires a high level of security. That level of security is not required at GIAC.

Maximum password age: While Microsoft recommends a maximum password age of 42 days GIAC will require password changes after 60 days. If the users are required to change their passwords too frequently security could actually be degraded as they resort to recording their passwords on paper or in other insecure methods.

Minimum password age: GIAC will set the minimum password age to 2 days; this matches the recommended setting from Microsoft. Preventing the users from changing their password too quickly makes it more difficult for them to recycle their old password.

Minimum password length: GIAC will set the minimum password length to 8 characters; this matches the recommended setting from Microsoft. A longer password significantly increases the level of security for the domain. The combination of longer and complex passwords is very powerful tool for enhancing security.

Password must meet complexity requirements: GIAC will enable this policy; this matches the recommended setting from Microsoft. The password must have a minimum of 6 characters, must contain a mix of upper and lower case letters, numbers, and non-alpha characters. This is a very important policy setting because increasing the complexity of the password significantly enhances the strength of the password and increases the difficulty of cracking it.

Store passwords in reverse encryption for all users in the domain: GIAC will disable this policy; this matches the recommended setting from Microsoft. This setting is used for applications that require the user password, it should disabled unless absolutely necessary.

4.1.1.2. Account Policies/Account Lockout Policy

GIAC Enterprises' Account Lockout Polices meets the recommended setting from Microsoft. These policies are designed to thwart brute force attacks on user's passwords and assist in meeting GIAC security objective of maximum protection for user accounts. GIAC will not require a users' whose account has been locked out due to a misspelled account name or password to be unlocked by an administrator but after 5 attempts to login to the domain the account will remain locked out for 30 minutes.

Account lockout duration (in minutes): GIAC will set this policy to 30 minutes; this matches the recommended setting from Microsoft. The user account will remain locked for 30 minutes or until an administrator unlocks it.

Account lockout threshold: GIAC will set this policy to 5 attempts; this matches the recommended setting from Microsoft. The user has 5 attempts to logon before the account is locked out.

Reset account lockout counter after (x minutes): GIAC will set this policy to 30 minutes; this matches the recommended setting from Microsoft. The counter which tracks invalid login attempts is not reset for 30 minutes.

4.1.1.3. Local Policies/User Rights Assignments

User Rights Assignment polices for the domain policy will be left at the default settings.

4.1.1.4. Local Policies/Security Options

This section discusses settings for the Security Options policies. This policy strengthens security for user accounts by limiting anonymous access and clearly stating that unauthorized access to this network is not permitted. GIAC will minimize the number of security options set at the domain level; additional security options will be configured at the domain controller, server, and workstation or user OU level. This will eliminate any overlap between group policies and will preclude the need to utilize the block inheritance or no override options. Security Options that are highlighted in bold were identified by Jason Fossen, in the SANS Institute course Securing Windows, as being especially important (Fossen, 135-136).

Additional restrictions for anonymous connections: Use this setting to prevent Null Users access to network resources. Microsoft recommends a setting of "No access without explicit anonymous permissions". GIAC will follow Microsoft's recommended setting.

Use care when setting this option, consult Microsoft Knowledge Base article "How to Use the Restrict Anonymous Registry Value in Windows 2000 (Q246261)". When this option was set to "No access without explicit anonymous permissions" in a mixed mode domain; Exchange 2000 stopped working.

Automatically log off users when logon time expires (local): Use this setting to force users to logoff if they are restricted to using the network to certain hours. By default this policy setting is disabled. GIAC will not restricting any users' ability to work on the network and will leave the policy setting at the default.

Message text for users attempting to log on: Use this policy setting to notify users that they are accessing a private computer network and unauthorized use is prohibited. The text for this policy setting is below.

"This is a GIAC Corporation computer. Use of this computer is restricted to official business. This computer is subject to monitoring to monitoring at any time. By using this computer you are consenting to being monitored. Any evidence of unauthorized access, use or modification will be used for criminal prosecution." (This text is derived from SANS and CERT guidelines).

Message title for users attempting to log on: A title for the logon message text. The title will be "GIAC Enterprises".

4.1.2. User Configuration/Windows Settings/Scripts

It is possible to have a script run when a computer starts up or shuts down or have it run when a user logs on or off. GIAC will assign a logon script to the users. Using a group policy to assign script is a powerful tool and simplifies user administration as each user profile does not have to be edited to assign a logon script.

Logon Script

The logon script for domain users will be assigned using this group policy setting. Users will be members of groups based on their location. Drives will be mapped based on group membership. This give administrator's maximum flexibility as individual profiles do not refer to a specific logon script or home directory. It also allows different locations or groups of users to have different network shares mapped. The login script will use a MS Resource kit utility ifmember.exe to test for group membership and provide customized drive mappings based on location and/or department. Typically this includes a home area for the user, a shared data area for teams to have common access to files, and a share for any applications that can or need to be run from the network. This simple script is shown below.

```
%LOGONSERVER%\netlogon\ifmember "nycusers"
IF %ERRORLEVEL% EQU 0 GOTO BOS
net use M: \\giacnycfp01\%username%$      /PERSISTENT:NO
net use N: \\ giacnycfp01\apps            /PERSISTENT:NO
net use O: \\ giacnycfp01\shareddata      /PERSISTENT:NO
GOTO END
:BOS
%LOGONSERVER%\netlogon\ifmember "bosusers"
IF %ERRORLEVEL% EQU 0 GOTO END
net use M: \\giacnbosp01\%username%$      /PERSISTENT:NO
net use N: \\ giacbosfp01\apps            /PERSISTENT:NO
net use O: \\ giacbosfp01\shareddata      /PERSISTENT:NO
GOTO END
:END
```

4.2. Default Domain Controller Policy

The Default Domain Controller group policies will address GIAC's security requirements by securing communication between the servers and clients; configuring audit settings and event logs so GIAC can track access and log critical events; standardizing the configuration of the domain controllers; and minimizing the number of services running on a domain controller.

As with the Default Domain group policies GIAC will use the group policy settings in the Security Operations Guide for Windows 2000 Server by Microsoft Corporation as a guide for configuring its' group policy settings. These policies will be applied at the Domain Controller OU. No policies will be configured in the User Configuration section so that section of the group policy will be disabled. Disabling the user configuration portion of the policy will make the processing of the group policy faster.

4.2.1. Computer Configuration/Windows Settings/Security Settings

4.2.1.1. Local Policies/Audit Policy

GIAC Enterprises' Audit Policy settings will match Microsoft's recommended settings. Auditing is an important tool to detect and track unauthorized access. It will also log any unauthorized behavior and track user access. The Audit Policy settings are described below.

Audit Account Logon events: GIAC will set this policy to Success/Failure; this matches the Microsoft recommended setting. All successful or failed logins to the domain from another computer that the domain controller validates are captured in this log.

Audit Account Management: GIAC will set this policy to Success/Failure; this matches the Microsoft recommended setting. All successful or failed changes to any domain account are captured.

Audit Directory Service Access: GIAC will set this policy to Failure; this matches the Microsoft recommended setting. All failed attempts to access any AD object with a system access control list.

Audit Logon Events: GIAC will set this policy to Success/Failure; this matches the Microsoft recommended setting. All successful or failed logons, logoffs, or network connections to a domain controller are captured. A successful or failed logon to a domain member workstation would not be captured via this audit setting.

Audit Object Access: GIAC will set this policy to Success/Failure; this matches the Microsoft recommended setting. All failed attempts of a user to access any object with a system access control list, for example a printer or file folder will be captured.

Audit Policy Change: GIAC will set this policy to Success/Failure; this matches the Microsoft recommended setting. All successful or failed changes to user rights, audit policies, and trust policies. This is a useful for detecting unauthorized changes to groups and polices.

Audit Privilege Use: GIAC will set this policy to Failure; this matches the Microsoft recommended setting. This will log failed attempts of a user exercising a right.

Audit Process Tracking: GIAC will set this policy to No Auditing; this matches the Microsoft recommended setting. This policy setting captures things like process exit, program activation. It could generate large volumes of data so it is set to no auditing.

Audit System Events: GIAC will set this policy to Success/Failure; this matches the Microsoft recommended setting. This policy setting will record the shutdown or startup of the domain controllers and events regarding system security or the security log.

4.2.1.2. Local Policies/User Rights Assignments

If the GIAC policy setting did not change from the default setting it is not discussed below. GIAC will allow the workstation support staff at each site to add workstations to the domain. This is an example of using group policy to limit the level of access for users of the domain.

Add workstations to domain: Administrators and site support groups
By default users are allowed to add 10 workstations to the domain. They will not be allowed to do this on the GIAC domain to prevent unauthorized machines from accessing the domain.

4.2.1.3. Local Policies/Security Options

These policy settings will set the appropriate level of access for users on the domain controllers; secure communication on the domain thereby preventing unauthorized access to the servers or workstations; and ensuring that the domain controllers have a standard configuration. If the GIAC policy setting did not change from the default setting of the local computer group policy or it is not different from the Default Domain Group Policy it is not discussed below. In most instances GIAC Enterprises' will follow the recommended settings for Security Options from Microsoft. Where there is a divergence an explanation will be provided. Security Options that are highlighted in bold were identified by Jason Fossen as being especially important (Fossen, 135-136).

Allow server operators to schedule tasks: GIAC will disable this policy; this matches the Microsoft recommended setting. Only administrators will be able to schedule tasks on the domain controllers

Allow system to be shutdown without having to log on: GIAC will disable this policy; this matches the Microsoft recommended setting. The server cannot be shutdown without logging on first.

Allowed to eject removable NTFS media: Set to Administrators; this matches the Microsoft recommended setting. Only administrators will be allowed to eject removable NTFS media.

Amount of idle time required before disconnecting session: GIAC will set this policy to 15 minutes; this matches the Microsoft recommended setting. If a SMB session is inactive longer than 15 minutes it will be disconnected. If the client becomes active again the sessions is revived.

Audit the access of global system objects: GIAC will disable this policy; this matches the Microsoft recommended setting. If enabled then when system devices are created they are assigned a default system access list.

Audit the use of Backup and Restore privilege: GIAC will disable this policy; this matches the Microsoft recommended setting. Use of backup and restore will not be logged. This will reduce the size of the security log.

Clear virtual memory page file when system shuts down: GIAC will enable this policy; this matches the Microsoft recommended setting. This will prevent possible access to sensitive information in the page file.

Digitally sign client communications (always): GIAC will enable this policy; this matches the Microsoft recommended setting. This policy setting requires that all secure channel traffic must be signed. This prevents communication between the server and client being intercepted and spoofed. Requiring a digital signature will impose a performance penalty.

Digitally sign client communications (when possible): GIAC will enable this policy; this matches the Microsoft recommended setting. This policy setting requires that a client sign secure channel traffic if the SMB server requires it.

Digitally sign server communications (always): GIAC will enable this policy; this matches the Microsoft recommended setting. This policy setting requires that all secure channel traffic must be signed.

Digitally sign server communications (when possible): GIAC will enable this policy; this matches the Microsoft recommended setting.

Disable CRTL+ALT+DEL requirement for logon: GIAC will disable this policy; this matches the Microsoft recommended setting. This policy prevents attacks aimed at intercepting a user's password.

Do not display last user name in logon screen: GIAC will enable this policy; this matches the Microsoft recommended setting. This will make it more difficult to someone to break into the domain controller.

Guest account status: GIAC will disable this policy. While Microsoft does not have a recommendation for this setting, disabling this account will enhance security as this is a well known account and is a frequent target of hackers.

LAN Manager Authentication Level: This policy will be is set to NTLMv2 response only, refuse LM and NTLM; this matches the Microsoft recommended setting. The GIAC domain will run in native mode and all the clients will use Windows 2000 Professional so maintaining compatibility with pre Windows 2000 clients is not an issue.

Number of previous logons to cache (in case domain controller is not available): This policy will be is set to 0; this matches the Microsoft recommended setting. No credentials will be cached on the server; an administrator must login to the domain to access the domain controller.

Prevent system maintenance of computer account password: GIAC will disable this policy; this matches the Microsoft recommended setting. This policy ensures that a new computer account password will be generated each week.

Prevent users from installing printer drivers: GIAC will enable this policy; this matches the Microsoft recommended setting. This policy prevents users from installing a printer on the domain controller.

Recovery Console: Allow automatic administrative logon: GIAC will disable this policy; this matches the Microsoft recommended setting. If enabled this policy would not require the Administrator password to run the Recovery Console.

Recovery Console: Allow floppy copy and access to drives and folders: GIAC will disable this policy; this matches the Microsoft recommended setting. If enabled this policy would allow someone to use the SET command in the Recovery Console. That person could then enable access to all files, allow copies to a floppy, use wildcards with commands, and turn off prompting when overwriting a file.

Rename administrator account: Renaming this account enhances security by making it more difficult for someone to use it to illegally access the domain. Microsoft does not have a recommendation for this setting. GIAC will rename the administrator account to)(#Admin~^ .

Rename guest account: This policy will be undefined. Microsoft does not have a recommendation for this setting. As with the administrator account renaming this account makes it more difficult for someone to use it to illegally access the domain but as the account is disabled GIAC will set this policy to not needed.

Restrict CD-ROM access to locally logged-on user only: GIAC will enable this policy; this matches the Microsoft recommended setting. When this setting is enabled, only the user logged on locally can access the CD-ROM. The CD-ROM can still be shared but it will be unavailable to network users when someone is logged on locally.

Restrict floppy access to locally logged-on user only: GIAC will enable this policy; this matches the Microsoft recommended setting. As with the CD-ROM network access to the floppy is denied while a user is logged on locally.

Secure channel: Digitally encrypt or sign secure channel data (always): GIAC will enable this policy; this matches the Microsoft recommended setting. Requiring digital encryption and signature does impose a performance penalty.

Secure channel: Digitally encrypt channel data (when possible): GIAC will enable this policy. The Microsoft recommended setting is enabled.

Secure channel: Digitally sign channel data (when possible): GIAC will enable this policy. The Microsoft recommended setting is enabled.

Secure channel: Require strong (Windows 2000 or later) session key: GIAC will enable this policy; this matches the Microsoft recommended setting This policy requires that all outgoing secure channel traffic use a strong encryption key otherwise the key strength is negotiated.

Send unencrypted password to connect to third-party SMB servers: GIAC will disable this policy; this matches the Microsoft recommended setting. If enabled the SMB redirector can send passwords in clear text to a non Microsoft SMB server.

Shut down system immediately if unable to log security audits: GIAC will disable this policy. The Microsoft recommended setting is enabled. GIAC is allowing log files to be overwritten as needed and will archive the logs on a daily basis so this setting is superfluous.

Smart card removal behavior: GIAC will set this policy to lock the workstation; this matches the Microsoft recommended setting. If a smart card is used for user validation and is removed the server is locked.

Strengthen default permissions of global system objects: GIAC will enable this policy. The Microsoft recommended setting is enabled. This policy setting allows reading shared objects but not modifying those they did not create.

Unsigned driver installation behavior: GIAC will set this policy to Do not allow installation; this matches the Microsoft recommended setting. This policy setting will not allow unsigned drivers to be installed.

Unsigned non-driver installation behavior: This policy setting will be Warn but allow installation; this matches the Microsoft recommended setting. This policy setting will allow the installation of non-certified non-driver software on the server.

4.2.1.4. Event logs/Settings for Event Logs

These policies will address security requirement to capture critical events. GIAC Enterprises' will use Microsoft Resource Kit utilities and scheduled batch commands to consolidate event logs for analysis and archival purposes. In most instances GIAC Enterprises' will match the recommended settings from Microsoft. The exception is the retention method for the log files. GIAC will archive logs on a daily basis and will allow them to be overwritten as needed. GIAC also increased the size of the event logs to ensure that the logs will not be overwritten too quickly due to audit policy settings. Properties for the DNS, Directory Services, and File Replication Service event logs cannot be set via group policy and must be set manually or by a script for the domain controllers.

Maximum application log size: GIAC will set this policy to set to 100 Mb so that events will not be overwritten before they are archived. This exceeds the Microsoft recommended size of 10 Mb's.

Maximum security log size: GIAC will set this policy to 100 Mb. This exceeds the Microsoft recommended size of 10 Mb's.

Maximum system log size: GIAC will set this policy to 100 Mb. This exceeds the Microsoft recommended size of 10 Mb's.

Restrict guest access to application log: GIAC will enable this policy; this matches Microsoft's recommendation.

Restrict guest access to security log: GIAC will enable this policy; this matches Microsoft's recommendation. While the guest account is disabled denying guest access to the logs is an additional layer of defense.

Restrict guest access to system log: GIAC will enable this policy; this matches Microsoft's recommendation.

Retention method for application log: GIAC will set this policy to as needed. The Microsoft recommended setting is do not overwrite events but this required an administrator to manually clear the logs files. This is could be automated but GIAC will allow the logs to overwrite as needed while archiving the logs on a daily basis.

Retention method for security log: GIAC will set this policy to as needed. The Microsoft recommended setting is to not overwrite events.

Retention method for system log: GIAC will set this policy to as needed. The Microsoft recommended setting is to not overwrite events.

4.2.1.5. Services

These policy settings address the security requirement to minimize the risks created by unneeded services on a server. By default Windows 2000 installs numerous services configured to run at startup. Any unneeded service is a potential security risk and should be disabled. The services listed below will be disabled if installed. GIAC will not install IIS on the domain controllers. Some of these services may need to be enabled if extra functionality is desired or required.

Alerter – used to send administrative alerts.
Application Management – used by IntelliMirror to install applications on computer.
ClipBook – shares clipboard data to remote computers, does not prevent use of local clipboard.
Computer Browser – maintains list of computers on network.
Distributed Link Tracking Server – stores information so files can be tracked across volumes in a domain.
Distributed Transaction Coordinator – coordinates transactions across multiple computers.
Fax Service – allows the sending and receiving of faxes.
IIS Admin Service – enables administration of IIS.
Indexing Service – creates indexes of files for faster lookups.
Internet Connection Sharing – allows multiple computers to share Internet access.
Intersite Messaging - enables mail replication between sites.
IPSEC Policy Agent (IPSEC Service) – manages IP security.
License Logging Service – tracks client access licenses.
Messenger – enables sending and receiving messages from and to users and computers.
NetMeeting Remote Desktop Sharing – allows others to access computer via MS NetMeeting.
Network DDE – enables dynamic data exchange on the same or different computers.
Network DDE DSDM – used by Network DDE to manage shared DDE exchanges.
NTLM Security Support Provider – allows users to logon via NTLM authentication.
Performance Logs and Alerts – collects performance data from local or remote computers.
Print Spooler – enables printing locally and remotely.
QoS Admission Control (RSVP) – provides services for QoS applications.
Remote Access Auto Connection Manager– if there is no network connection this service offers dial up or VPN connectivity.
Remote Access Connection Manager – creates and manages dial-up and VPN connections.
Removable Storage – manages automated devices for cd's and tapes.
Routing and Remote Access – enables local and wide area routing services.
RunAs Service – logged on user can run tool or program with different permissions.
Simple Mail Transport Protocol (SMTP) – email transport.
Smart Card – enables smart card support for server.
Smart Card Helper – supports non Plug and Play smart card readers.

Task Scheduler – runs tasks at scheduled time.
Telephony – works with applications that need Telephony API support.
Telnet – enables telnet access to computer.
Terminal Services enables telnet access to the computer. This service will be enabled to allow for remote administration of the server.
Uninterruptible Power Supply – enables communication with to a UPS connected to server serial port.
Utility Manager – allows an administrator to configure accessibility tools.
Windows Installer – installs software.
Windows Management Instrumentation – reduces TCO by supplying system management information.
World Wide Web Publishing Service – enables web services.

Microsoft also recommends that the services listed below be configured for a manual startup.

Logical Disk Manager Administrative Service – services disk management requests such as adding a new drive or configuring a partition.
COM+ Event System – enables system to notify administrators of events.
Network Connections – enables configuration of network connections.
Remote Procedure Call (RPC) Locator – used by 3rd party code to find RPC servers.
Windows Management Instrumentation Driver Extensions – provides information on what drivers have supplied WMI information.

4.2.2. Computer Configuration/Administrative Templates/

4.2.2.1. System/Group Policy

These policy settings determine how group policies are applied. Group policies will always be applied although an administrator could logon to a domain controller and get a desktop before the group polices were completely applied. While this not acceptable behavior for a workstation, only administrators will logon to the domain controllers and it is desirable to minimize the time it takes them to logon.

Disable background refresh of Group Policy: This policy will be disabled. Group policy changes will be not updated until the user logs off.

Apply Group Policy for computers asynchronously during startup: This policy will be enabled. This could result in the desktop loading before the group polices are finished but will allow for faster logon to the domain controller.

Apply Group Policy for users asynchronously during logon: This policy will be enabled. As with the previous policy setting this could result in the desktop loading before the group polices are finished but will allow for a faster logon.

5. Additional Group Policy

GIAC Enterprises will have separate group policies for the workstations and servers so it can maintain maximum flexibility in its group policy implementation. There will be one group policy object which will be linked to multiple Resource/*Office*/Workstation or Server organizational units. Many of the policy settings for domain controller, servers, and workstations will be the same, however, using different polices will make it simpler to troubleshoot the group policies. It will also make administration of group policies less complicated by allowing GIAC to avoid using the filtering, no override, and block inheritance features of group policies. The following sections will highlight the differences between the workstation, server and domain controller group policy settings.

In addition, GIAC will define a group policy for the User Accounts/Contractors organization unit. The Contractor group policy will limit what temporary employees can access and change on their computers. This will allow GIAC to lower the total cost of ownership for the computer used by contractors. The next section will discuss the workstation OU.

5.1. Resources/*Office*/Workstations OU

The group polices applied at the workstation OUs will help GIAC meet the requirements of its' security policy by configuring audit settings and event logs so GIAC can tracking access and log critical events; and by standardizing the configuration of the workstations. No changes to User Configuration policies will be made at the Workstation OU level so that section of the group policy will be disabled. Disabling the User section of the group policy will speed up the processing of the GPO.

5.1.1. Computer Configuration/Windows Settings/Security Settings

There will be a workstation OU for each GIAC Enterprises office. One group policy object will be created and linked to the workstation OU of each office. The Security Operations Guide for Windows 2000 Server by Microsoft does not address workstation security. GIAC will use the secure workstation template (securews.inf) from Microsoft as a guide to configuring workstation security.

5.1.1.1. Local Policies/Audit Policy

These policies differ from the domain controller policies in the following respects.

Audit Directory Service Access: This policy is not applicable at the workstation level.

Audit Logon Events: GIAC will set this policy to Failure; this matches the Microsoft recommended setting. All successful or failed logons, logoffs, using a local not domain account, or network connections to a workstation are captured.

Audit Object Access: GIAC will set this policy to no auditing; this matches the Microsoft recommended setting.

Audit System Events: GIAC will set this policy to no auditing; this matches the Microsoft recommended setting.

5.1.1.2. Local Policies/Security Options

These policies differ from the domain controller policies in the following respects.

Administrator account status: This policy will not be defined. This policy setting is not defined in the template. The administrator account will not be disabled to allow site support to access the workstation locally if necessary.

Guest account status: GIAC will disable this policy. This will disable the local guest account on the workstation and enhance security on the workstation; this matches the recommended setting from Microsoft.

Number of previous logons to cache (in case domain controller is not available): GIAC will set this policy to 10. This will allow the user to logon to the workstation and work if a domain controller is not available to validate their logon.

Rename administrator account: This policy will not be defined. In order to make desktop support simpler the administrator account will not be renamed. This policy setting is not defined in the template.

Rename guest account: This policy will not be defined. As the account is disabled GIAC will set this policy to not needed. This policy setting is not defined in the template.

5.1.1.3. Event logs/Settings for Event Logs

While workstation logs are not as critical as server event logs but they are useful for troubleshooting purposes. These policies differ from the domain controller policies in the following respects. GIAC will allow them to be overwritten as needed, they will not be archived and the logs will not be as large as the domain controller logs.

Maximum application log size: GIAC will set this policy to 10 Mb.

Maximum security log size: GIAC will set this policy to 10 Mb.

Maximum system log size: GIAC will set this policy to 10 Mb.

5.2. Resources/*Office*/ Servers OU

The Servers OU group policies will address GIAC's security requirements by securing communication between the servers and clients; by configuring audit settings

and event logs so GIAC can track access and log critical events; by standardizing the configuration of the member servers; and by minimizing the number of services running on a member server.

There will be a server OU for each GIAC office. A single group policy object will be created and linked to the server OU of each office. Many of the policy settings for domain controller and servers will be the same. The following sections will highlight the differences. No changes will be made to the User Configuration settings so that section of the group policy will be disabled.

5.2.1. Computer Configuration

5.2.1.1. Local Policies/Audit Policy

Server audit policies are the same as the domain controller policies. Audit policy settings were discussed in the domain controller group policy section and will not be rehashed here.

5.2.1.2. Windows Settings/Security Settings/Local Policies/Security Options

Server audit policies are the same as the domain controller policies. Security policy settings were discussed in the domain controller group policy section and will not be rehashed here.

5.2.1.3. Windows Settings/Security Settings/Event logs/Settings for Event Logs

Server event log policies are the same as the domain controller policies. These policy settings were discussed in the domain controller group policy section and will not be rehashed here.

5.2.1.4. Windows Settings/Security Settings/Services

Member server settings for services are the same as the domain controller services with the following exceptions. These services will be disabled on member servers.

Distributed File System
RPC Locator

The following services will be enabled and set to start automatically on some member servers. The role a server plays will determine which additional services will be enabled.

DHCP Server will run on the file/print and application servers.
IIS Admin will run on the file/print servers.

Print Spooler will run on the file/print servers.
World Wide Web Publishing service will run on the file/print servers. This service will be installed to allow GIAC to use Internet Printing on its intranet. This allows the users to use a web interface to manage print jobs and install printers.

5.2.1.5. Administrative Templates/System/Group Policy

These policy settings determine how group policies are applied. Group Policy settings for domain member servers will be the same as domain controllers.

5.3. User Accounts/ Contractors User Configuration/Administrative Templates

The Contractors OU group policies will address GIAC's security requirements by configuring desktop and application setting via group policy. Contractors are temporary workers hired for telemarketing, clerical tasks, maintaining GIAC external web site, or other special projects. GIAC will implement user policies to customize the desktop and applications for contractors. This will allow GIAC to control what they can see and do on the network and reduce the cost of supporting the contractors. There are no computers in the Contractors OU so policies will only be applied on User Configuration section of the GPO. The computer section of the GPO will be disabled to reduce the time required to process the policies.

These policy settings are derived from the 'Multi-User Desktop Scenario' from the Microsoft whitepaper "Implementing Common Desktop Management Scenarios". This whitepaper discusses six scenarios for managing different types of users. The degree to which the user can control or manage the computer depends on the role they play in the organization. The settings for the 'Multi-User Desktop Scenario' are most appropriate model. Contractors will be allowed to customize the desktop to a limited extent but cannot modify hardware or network connections.

5.3.1. Windows Components/Internet Explorer

This policy will lock down Internet Explorer so the contractors cannot change the default GIAC settings.

Search: Disable Search Customization	Enabled
Search: Disable Find Files via F3 within the browser	Enabled
Disable external branding of Internet Explorer	Enabled
Disable importing and exporting of favorites	Enabled
Disable changing Advanced page settings	Enabled
Disable changing home page settings	Enabled
Use Automatic Detection for dial-up connections	Enabled
Disable changing Temporary Internet files settings	Enabled
Disable changing history settings	Enabled
Disable changing color settings	Enabled

Disable changing link color settings	Enabled
Disable changing font settings	Enabled
Disable changing language settings	Enabled
Disable changing accessibility settings	Enabled
Disable Internet Connection wizard	Enabled
Disable changing connection settings	Enabled
Disable changing proxy settings	Enabled
Disable changing Automatic Configuration settings	Enabled
Disable changing ratings settings	Enabled
Disable changing certificate settings	Enabled
Disable changing Profile Assistant settings	Enabled
Disable AutoComplete for forms	Enabled
Do not allow AutoComplete to save passwords	Enabled
Disable the Reset Web Settings feature	Enabled
Disable changing default browser check	Enabled

5.3.1.1. Offline Pages

Disable adding channels	Enabled
Disable removing channels	Enabled
Disable adding schedules for offline pages	Enabled
Disable editing schedules for offline pages	Enabled
Disable removing schedules for offline pages	Enabled
Disable offline page hit logging	Enabled
Disable all scheduled offline pages	Enabled
Disable channel user interface completely	Enabled
Disable downloading of site subscription content	Enabled
Disable editing and creating of schedule groups	Enabled
Subscription Limits	Enabled

5.3.1.2. Browser menus

Help menu: Remove 'Tip of the Day' menu option	Enabled
Help menu: Remove 'For Netscape Users' menu option	Enabled
Help menu: Remove 'Send Feedback' menu option	Enabled
Disable Save this program to disk option	Enabled

5.3.2. Windows Explorer

This policy will limit what the user can manage, run and see on the workstation and the network.

Hides the Manage item on the Windows Explorer context menu	Enabled
Allow only per user or approved shell extensions	Enabled
No Entire Network in My Network Places	Enabled
Do not request alternate credentials	Enabled

5.3.3. Microsoft Management Console

This policy restricts contractors to approved MMC's and limits their privilege level.

Restrict the user from entering author mode	Enabled
Restrict users to the explicitly permitted list of snap-ins	Enabled

5.3.4. Task Scheduler

This policy stops the contractors from modifying any scheduled tasks.

Hide Property Pages	Enabled
Prevent Task Run or End	Enabled
Disable Drag-and-Drop	Enabled
Disable New Task Creation	Enabled
Disable Task Deletion	Enabled
Disable Advanced Menu	Enabled
Prohibit Browse	Enabled

5.3.4.1. Windows Installer

This policy will not allow any program to be installed from a cd or floppy.

Prevent removable media source for any install	Enabled

5.3.5. Start Menu & Taskbar

This policy locks down the Start Menu and Taskbar so the contractors only see the programs GIAC chooses to display. It limits access to the network and the command prompt.

Remove links and access to Windows Update	Enabled
Remove programs on Settings menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Add Logoff to the Start Menu	Enabled
Remove Drag-and-drop context menus on the Start Menu	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Remove access to the context menus for the taskbar	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled

5.3.6. Desktop

This policy restricts the extent that the contractors can customize the desktop.

Do not add shares of recently opened documents to My Network Places	Enabled
Prohibit user from changing My Documents path	Enabled
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled
Prohibit adjusting desktop toolbars	Enabled
Don't save settings at exit	Enabled

5.3.7. Control Panel

These policies allow GIAC to control what the contractors can access via the control panel.

Show only specified control panel applets	Enabled

5.3.7.1. Add/Remove Programs

These policies restrict the user's ability to add or delete programs on the computer by hiding those menu options in the control panel.

Hide Add/Remove Windows Components page	Enabled
Hide the Add a program from CD-ROM or floppy disk option	Enabled
Hide the Add programs from Microsoft option	Enabled
Specify default category for Add New Programs	Enabled

5.3.7.2. Display

These policies hide display options so the users cannot customize the desktop.

Hide Desktop tab	Enabled
Hide Settings tab	Enabled
Screen saver executable name	Enabled
Screen Saver timeout	Enabled

5.3.8. Network

This policy allows GIAC to control how the contractors can set offline folder settings and prevents them from making changes to the network configuration.

5.3.8.1.1. Offline Files

Prohibit user configuration of Offline Files	Enabled
Remove Make Available Offline	Enabled
Prevent use of Offline Files Folder	Enabled

5.3.8.2. Network Connections

Ability to rename LAN or RAS connections available to all users	Disabled
Prohibit access to properties of components of a LAN connection	Enabled
Prohibit access to properties of components of a remote access connection	Enabled
Prohibit TCP/IP advanced configuration	Enabled
Prohibit access to the Advanced Settings item on the Advanced menu	Enabled
Prohibit adding and removing components for a LAN or RAS connection	Enabled
Prohibit access to properties of a LAN connection	Enabled
Prohibit Enabling/Disabling components of a LAN connection	Enabled
Ability to change properties of an all user remote access connection	Disabled
Prohibit changing properties of a private remote access connection	Enabled
Prohibit deletion of remote access connections	Enabled
Ability to delete all user remote access connections	Disabled

Prohibit connecting and disconnecting a remote access connection	Enabled
Ability to Enable/Disable a LAN connection	Disabled
Prohibit access to the New Connection Wizard	Enabled
Prohibit renaming private remote access connections	Enabled
Prohibit access to the Dial-up Preferences item on the Advanced menu	Enabled
Prohibit viewing of status for an active connection	Enabled

5.3.9. System

This policy suppress the configuration/welcome screen for new users, lock the contractors out of the registry, does not allow cd's to automatically start when loaded, and ensures that logon scripts must complete before the desktop appears.

Don't display the Getting Started welcome screen at logon	Enabled
Prevent access to registry editing tools	Enabled
Turn off Autoplay	Enabled

5.3.9.1. User Profiles

Limit profile size	Enabled

5.3.9.2. Scripts

Run logon scripts synchronously	Enabled

6. Additional Security

GIAC Enterprises will use the hfnetchk.exe tool from Microsoft on a monthly basis to detect any missing patches on the servers. Section 6.1 will outline additional configuration steps for domain controllers and member servers.

6.1. Domain Controller settings

The following options will be enabled to enhance security for GIAC.net DNS servers.

- DNS zones will be Active Directory integrated. This has several beneficial effects, the primary/secondary role is eliminated and records can be updated on any DNS server. Zone transfers are more efficient as only changes are replicated. Security is enhanced as specific permissions can be assigned to DNS records.

- Zone transfers will be disabled. The GIAC.net zone is Active Directory integrated and there are no non-AD secondary zones so zone transfers are not necessary. This enhances security by not permitting anyone to transfer the contents of an entire zone.

- DNS activity will be logged. There are eleven activities which can be logged to assist in troubleshooting or detecting unauthorized access. If they are all enabled the log file could be overwritten too quickly as the default size is only four mb's. GIAC will enable logging for updates and the number of query messages

received. This will allow administrators to see who is submitting and querying data. Additional activities will be logged as needed. GIAC will use an automated process to centralize the DNS log files.

- The Secure Cache against Pollution will be enabled. This will prevent anyone from incorrect information on Internet or Intranet destinations. The DNS server will discard any information it did not specifically request.

- All access to internal DNS servers will be block at the firewall. Not advertising internal resources to the Internet will help keep unauthorized users out.

- The DNS servers will require secure updates. The DNS servers at GIAC will allow dynamic updates but requiring secure updates requires Kerberos authentication reducing the risk of bogus entries in the DNS.

- The DNS records of critical systems will be protected by using ACL's in AD Users and Computers.

- The directory service, file replication and DNS event logs properties are not set via group policy. These should be configured to match the other event logs. This can be implemented via an administrative template.

- All of the domain controllers will use an authoritative time source on the internal network. This time source will be a router which synchs its' time with an authoritative time source on the Internet. See Microsoft Knowledge Base Article "How to Configure an Authoritative Time Server in Windows 2000 (Q216734)".

- Set the timeout values for the Terminal Server Service. If an administrator is disconnected from a server the terminal session will not be terminated unless the server is specifically configured to terminate inactive sessions after X minutes of inactivity. GIAC will set the timeout value to 15 minutes.

6.2. Member Server settings

- Set the timeout values for the Terminal Server Service. Use the same value as for the domain controllers.

6.3. Internet Web servers

GIAC Enterprises Internet web servers will be standalone servers. They will be configured as follows.

Table 6.1 Web server hardware specifications

Model:	Dell 2650	**CPU:**	2 x Xeon/1.8 or higher
RAM:	1 Gb	**Disks:**	PERC3 SCSI controller 2 x 36 Gb 2 x 72 Gb 2 disks RAID 1 2 disks RAID 1
NICs:	Dual, teamed NICs for failover.	**Remote Management:**	Dell Remote Access Card (DRAC)
Power:	Redundant	**Fans:**	Redundant
OS:	Server SP3 and hot fixes identified by Hfnetchk	**Other:**	SYSVOL/OS (C:) (16Gb mirror) Paging and log files (D:) (16Gb mirror) Web sites (E:) (72GB mirror) CD-ROM (Z:)

IIS 5 will be installed with default settings as part of the operating system installation. GIAC will move the Inetpub directory to the E: drive on the server. This will limit the impact of directory traversal exploits. GIAC will then use the "Secure Internet Information Services 5 Checklist" and the IIS Lockdown tool from Microsoft to configure the Internet web servers. This checklist includes the Hisecweb template, which makes the following configuration changes. GIAC will make one change to the template to allow remote administration of the server. The terminal services service will not be disabled.

Account Polices (Password, Account Lockout polices)
Enforce password history: Set to 24.
Maximum password age: Set to 42.
Minimum password age: Set to 2.
Minimum password length: Set to 8.
Password must meet complexity requirements: Set to enabled.
Store passwords in reverse encryption for all users in the domain: Set to disabled.
Account lockout duration (in minutes): Set to 30 minutes.
Account lockout threshold: Set to 5 attempts.
Reset account lockout counter after (x minutes): Set to zero.

Audit Policies
Audit Account Logon events: This policy will be set to Success/Failure.
Audit Account Management: This policy will be set to Success/Failure.

Audit Logon Events: This policy will be set to Success/Failure.
Audit Object Access: This policy will be set to Failure.
Audit Policy Change: This policy will be set to Success/Failure.
Audit Privilege Use: This policy will be set to Failure.
Audit Process Tracking: This policy will be set to No Auditing.
Audit System Events: This policy will be set to Success/Failure.

Security Options
Allow system to be shutdown without logging on: Set to disabled
Allowed to format and eject removable media: Set to Administrators.
Audit the use of backup and restore priviledge: Set to enabled.
Clear virtual memory pagefile: Set to enabled.
Digitally sign communications (if client agrees): Set to enabled.
Digitally sign communications (if server agrees): Set to enabled
Digitally encrypt secure channel data (when possible): Set to enabled.
Digitally sign secure channel data (when possible): Set to enabled.
Disable machine account password changes: Set to disabled.
Disconnect clients when logon hours expire: Set to enabled.
Do not allow anonymous enumeration of SAM accounts and shares: Set to enabled.
Do not display last user name in logon screen: Set to enabled.
Do not require CRTL+ALT+DEL: Set to disabled.
LAN Manager Authentication Level: Set to send LM & NTLM – use NTLMv2 if session security negotiated.
Message title for users attempting to log on: Same as domain.
Message text for users attempting to log on: Same as domain.
Prevent users from installing printer drivers: Set to enabled.
Restrict CD-ROM access to locally logged-on user only: Set to enabled.
Restrict floppy access to locally logged-on user only: Set to enabled.
Send unencrypted password to connect to third-party SMB servers: Set to disabled.
Strengthen default permissions of internal system object: Set to enabled.
Unsigned driver installation behavior: Set to Do not allow installation.

The event logs are set as follows:
Maximum application log size: Not defined.
Maximum security log size: This policy will be set to 10 Mb.
Maximum system log size: Not defined.
Restrict guest access to application log: Set to Enabled.
Restrict guest access to security log: Set to Enabled.
Restrict guest access to system log: Set to Enabled.
Retention method for application log: Not defined.
Retention method for security log: Set to as needed.
Retention method for system log: Not defined.

The following system services are disabled.
Alerter
ClipBook

Computer Browser
DHCP client
Fax Service
Internet Connection Sharing
Irmon
Messenger
NetMeeting Remote Desktop Sharing
Print Spooler
Remote Access Auto Con. Manager
Remote Access Connection Manager \
Remote Registry
Task Schedular
Telephony
Terminal Services This service will be enabled to allow remote administration of server.

Using the latest IIS Lockdown utility from Microsoft GIAC will select as its template the dynamic web server. GIAC will disable all IIS services except the web server. It will disable all script mapping except Active Server Pages. It will remove the virtual directories for IIS Samples, Scripts, MSADC, and IIS Help virtual directories and disable WebDav. It will also set file permissions to limit access to system utilities to administrators and deny anonymous users write rights to the web content directory. GIAC will install UrlScan to eliminate bogus request to the web servers.

7. Conclusion

Group polices are a very powerful tool for implementing security in your domain. Designing your group polices requires a balance between optimizing security, retaining compatibility with legacy clients and applications and the needs of your clients. Great care should be exercised in creating your policies and they should be thoroughly tested before they are placed into production. Document polices in detail to avoid conflicts or redundancies. Good documentation will also make troubleshooting any issues with group policy much easier.

This document has described and provided a network diagram for GIAC Enterprises. It has discussed how GIAC Enterprises would implement Active Directory and how it would leverage global groups to delegate administration. Group polices have been created at the domain, domain controller, server, workstation, and Contractor OU levels to help GIAC attain its' security objectives. The Default Domain group policies were used to configure user account settings for maximum protection from unauthorized users. The Default Domain Controller, Server OU, and Workstation OU group policies were used to limit access to servers and workstations to legitimate users by securing communications between servers and workstations; to limit the level of access to servers to the appropriate persons; by configuring audit and event log settings so GIAC can track access and critical events; to ensure that the configuration of servers and workstations was consistent; and to minimize the number of services on the servers. The Contractors

OU group polices were used to mange the desktop environment of temporary employees. Finally additional security measures for computers in the domain and internet facing web servers were discussed.

8. References

CERT. "Setting up a logon banner on Windows NT 4.0", March 17, 1999. http://www.cert.org/security-improvement/implementations/i034.01.html

Fossen, Jason. 5.1 Windows 2000/XP: Active Directory and Group Policy. SANS Institute, 2002.

Microsoft Corporation. "Configuring Account Policies in Active Directory (Q255550)", Feb. 24, 2000. http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q255550&&FR=1

Microsoft Corporation. "FSMO Placement and Optimization on windows 2000 Domain Controllers (Q223346)", May 22, 2002. http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q223346&ID=KB;EN-US;Q223346

Microsoft Corporation. "Group Policy Application Rules for Domain Controllers (Q259576)." April 11, 2000. http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q259576&&FR=1

Microsoft Corporation. "How to Configure an Authoritative Time Server in Windows 2000 (Q216734)", March 12th, 2002. http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q216734

Microsoft Corporation. "IIS 5.0 Baseline Security Checklist", 2001. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/deploy/depovg/securiis.asp

Microsoft Corporation. Implementing Common Desktop Management Scenarios. Redmond: Microsoft Corporation, 2000. http://www.microsoft.com/windowsxp/pro/techinfo/administration/scenarios/default.asp

Microsoft Corporation. Prescriptive Guidance: Security Operations Guide for Windows 2000 Server. 2002. 51 – 77. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp

Microsoft Corporation. "Microsoft Security Bulleting MS 02-001 Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data V1.1" (April 24, 2002. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-001.asp.

Microsoft Corporation. Windows 2000 Group Policy Whitepaper. Redmond: Microsoft Corporation, 2000. http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp

Microsoft Corporation. Microsoft Windows 2000 Server Resource Kit. Redmond: Microsoft Press, 2000.

Minasi, Mark, Anderson, Christa, Smith, Brian, and Toombs, Doug. Mastering Windows 2000 Server, Fourth Edition. San Francisco: Sybex, 2002.

Sanderson, Mark J. and Rice, David C. Guide to Securing Microsoft Windows 2000Ò Active Directory ver. 1, National Security Agency. December, 2000.

The Center for Internet Security. Level One Benchmark Windows 2000 Operating System. 2001

Last Updated: May 23rd, 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**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**