Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

GIAC ENTERPRISES

GCWN Practical Assignment

Version 3.1

Prepared by:

Robert K. Alley
1/17/05 11:00 AM

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GCWN Practical Assignment
Securing Windows

Version 3.1	GIAC Enterprises

Table of Contents:

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents: (cont.)

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GCWN Practical Assignment
Securing Windows

Version 3.1	GIAC Enterprises

Description of GIAC Enterprises: **10 Points**	GIAC is a company that designs, manufactures, and distributes medical equipment to hospitals, fire departments, and the emergency medical community. They maintain an inventory that can be shipped immediately to any location throughout the United States. The main manufacturing facility, which also houses the corporate headquarters, is located near Columbus, Ohio. The other manufacturing facilities are located in Fargo, North Dakota and near Tucson, Arizona. All locations are located near an airport and an interstate highway. This gives them easy access to ship by air or interstate to the East Coast, West Coast and Central US. There are plans to expand into the international market sometime in the future. They currently have an Internet presence and have the name GIAC.COM registered. All Regional locations have their own local information systems support staff that takes care of everything from users, to software, to GPOs. Further, they have the following departments: Finance, Human Resources, Sales, Engineering, Quality, Research and Development, Marketing, and Production Control. Research and Development is located at the Columbus Ohio facility and due to the proprietary nature of the designs is located in a self-contained area. Marketing and Sales are also based out of the corporate office. There are 200 employees at the Corporate Office. This includes temporary employees and CO-OP Students in both the office and manufacturing sides of the business. The other two locations have about 50 employees each. The Sales force has the capability to be mobile and must keep an updated copy of the product information database on their laptop computers. The R&D department, while physically isolated from the rest of the facility, must still maintain a connection to the local area network and to the Internet. The Web Server is located at the Columbus facility. There is also a SQL server located in Columbus.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram:
10 Points

Network History

The network was updated company-wide to eliminate possible Y2K issues in 1999. At the time of the Y2K upgrade, workstation computers were purchased that would run Windows 2000. All workstation were upgraded to Windows 2000 Professional and all network servers were migrated to Windows 2000-Advanced Server early in the year 2000. The SQL server was upgraded to SQL Server 2000 during the year 2000.

There were no firewalls configured prior to 2001. The first ISA server was configured in early 2001, the second in late 2001.

The Research and Development segment of the network was totally isolated and separate from the rest of the network until the department needed access to company email and to the Internet.

The main company server (GIACCORP1) and the Terminal server were upgraded in the first quarter of 2002.

Network Overview (current)

This is a brief look at the networks at each location. A detailed description of the services each server performs follows in the next section.

Columbus

Topology-

- 100 Mbps Ethernet with either Category 5 and Category 5E wiring

Infrastructure-

- Hewlett Packard 4000M and 2424M Switches
- 3Com NICs (3c905)
- Intel NIC (built into mainboard)
- Cisco 3620 (To Remote Sites) (1 four port serial card) (1 fast Ethernet card)
- Cisco 3620 (To Internet) (1 four port serial card) (1 fast Ethernet card)
- Windows 2000 Server (GIACCORP1)
  - Pentium IV, 1.1 GHz
  - 512 MB Memory
  - 40 GB Hard Disk (Hardware RAID 1 mirrored)
  - Promise Technologies Mirroring IDE Controller
- Windows 2000 Server (GIACCORP2)
  - Pentium II, 550 MHz
  - 384 MB Memory
  - (2)10 GB Hard Disk (Hardware RAID 1 mirrored)
  - Promise Technologies Mirroring IDE Controller

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (1)

- Windows 2000 Server (Exchange 2000)
  - Pentium II, 550 MHz
  - 384 MB Memory
  - 10 GB Hard Disk (Hardware RAID 1 mirrored)
  - Promise Technologies Mirroring IDE Controller
- Windows 2000 Server (IIS and SMTP agent)
  - Pentium II, 550 MHz
  - 384 MB Memory
  - 10 GB Hard Disk (Hardware RAID 1 mirrored)
  - Promise Technologies Mirroring IDE Controller
- Windows 2000 Server (Terminal Services)
  - Pentium IV, 1.1 GHz
  - 2048 MB Memory
  - 40 GB Hard Disk (Hardware RAID 1 mirrored)
  - Promise Technologies Mirroring IDE Controller
- Windows 2000 Server (SQL 2000)
  - Pentium II, 650 MHz
  - 384 MB Memory
  - (2)10 GB Hard Disk (Hardware RAID 1 mirrored)
  - Promise Technologies Mirroring IDE Controller
- Windows 2000 ISA Server (External Firewall)
  - Pentium III, 800 MHz
  - 512 MB Memory
  - 20 GB Hard Disk (Software RAID 1 mirrored)
- Windows 2000 ISA Server (Internal Firewall)
  - Pentium III, 800 MHz
  - 512 MB Memory
  - 20 GB Hard Disk (Software RAID 1 mirrored)

Fargo:

Topology-

- 100 Mbps Ethernet with Category 5 and Category 5E wiring

Infrastructure-

- Hewlett Packard 4000M
- Intel NIC
- Intel NIC (built into mainboard)
- Cisco 3620 (To Corp) (1 four port serial card) (1 fast Ethernet card)

(continued on next page)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (2)	(Fargo continued)
	• Windows 2000 Server (DC)
	  • Pentium II, 550 MHz
	  • 384 MB Memory
	  • 8 GB Hard Disk (mirrored)
	
	• Windows 2000 Server (DC) (Email?)
	  • Pentium II, 550 MHz
	  • 384 MB Memory
	  • 8 GB Hard Disk (mirrored)
	
	Tucson:
	
	Topology-
	• 100 Mbps Ethernet with Category 5 and Category 5E wiring
	Infrastructure-
	• Hewlett Packard 4000M
	• Intel NIC
	• Intel NIC (built into mainboard)
	• Cisco 3620 (To Corp) (1 four port serial card) (1 fast Ethernet card)
	• Windows 2000 Server (DC)
	  • Pentium II, 550 MHz
	  • 384 MB Memory
	  • 8 GB Hard Disk (mirrored)
	• Windows 2000 Server (DC) (Email?)
	  • Pentium II, 550 MHz
	  • 384 MB Memory
	  • 8 GB Hard Disk (mirrored)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (3)

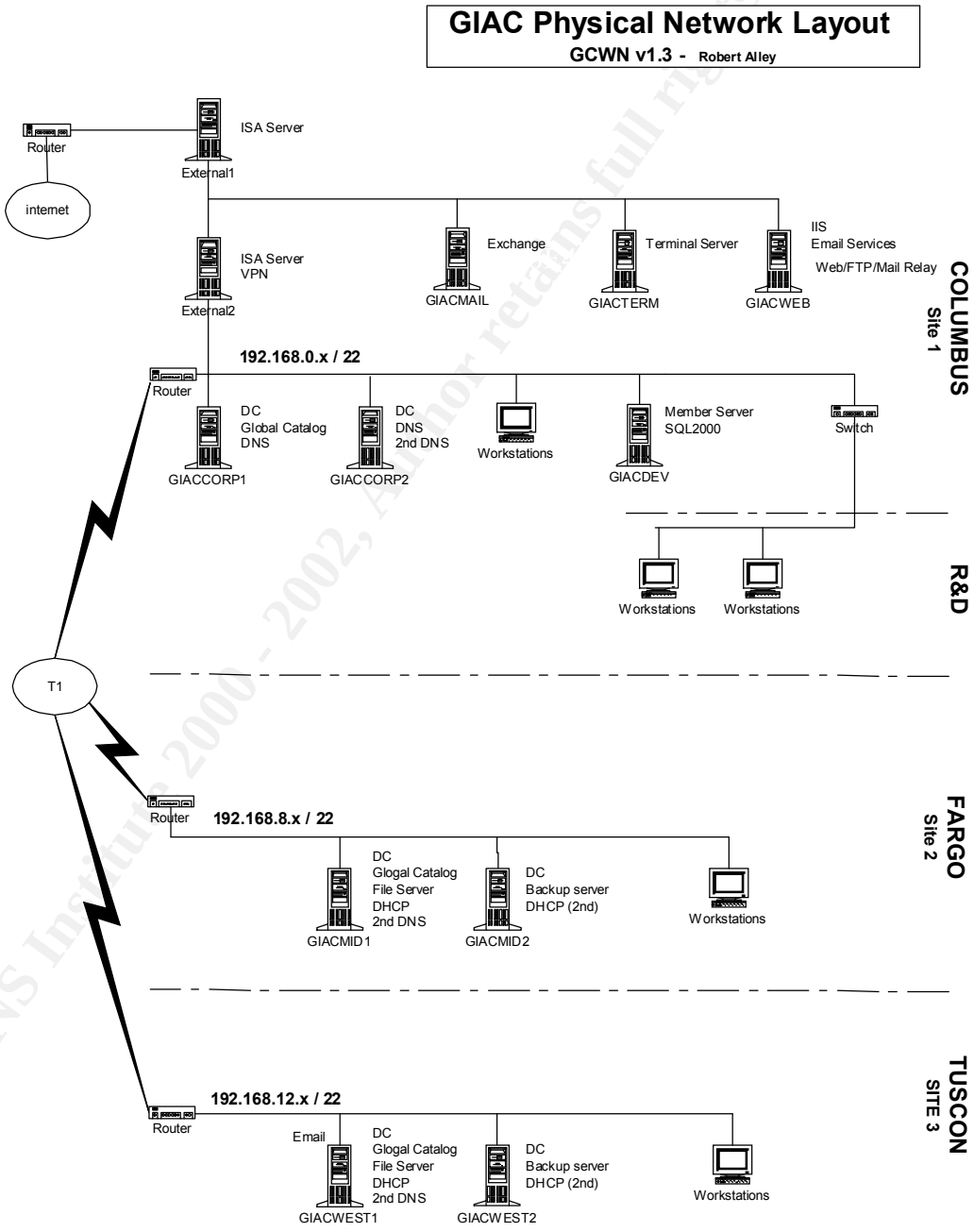


Figure 2a

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (4)

Network Specifics

This is a more detailed view of what roles the various computers play in the overall network. A comprehensive look at each service follows in the next section.

Columbus	
GIACCORP 1 Windows 2000 Server (w/SP2) Domain Controller Global Catalog Server PDC Emulator Relative ID Master (RID) DNS DHCP Custom security template applied	**GIACCORP 2** Windows 2000 Server (w/SP2) Domain Controller Infrastructure Master DHCP (secondary) Custom security template applied
GIACDEV Windows 2000 Server (w/SP2) SQL 2000 Custom security template applied	**GIACMAIL** Windows 2000 Server (w/SP2) Exchange 2000 Custom security template applied
GIACWEB Windows 2000 Server (w/SP2) Internet Information Server Custom security template applied	**GIACTERM** Windows 2000 Server (w/SP2) Custom security template applied
EXTERNAL1/EXTERNAL2 Windows 2000 Server (w/SP2) ISA Server Custom security template applied	
Fargo	
GIACMID1 Windows 2000 Server (w/SP2) Domain Controller Global Catalog Server (Planned) DHCP (Primary) Custom security template applied	**GIACMID2** Windows 2000 Server (w/SP2) Domain Controller DHCP (secondary) Custom security template applied
Tucson	
GIACWEST1 Windows 2000 Server (w/SP2) Domain Controller Global Catalog Server (Planned) DHCP (Primary) Custom security template applied	**GIACWEST2** Windows 2000 Server (w/SP2) Domain Controller DHCP (secondary) Custom security template applied

Table 2a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (5)	**Active Directory Services** GIACCORP1 was the first domain controller created and serves four(4) FMSO (Flexible Single Master Operation) roles. These are: Schema Master: Domain Naming Master Relative ID Master (RID) PDC Emulator As **Schema Master**, GIACCORP1 is responsible for updating and then propagating Active Directory schema changes out to the other Domain Controllers. There can be only one Schema Master per forest. The Domain Naming Master role allows this server to add and remove domains from the Active Directory namespace. There can be only one Domain Naming Master. With the role of **Relative ID Master** or **RID**, this server issues a pool of numbers to each Domain Controller within the domain so that they can issue unique Security IDs (SID) to newly created objects. It is also responsible for performing the move of an object from the current Domain to a new Domain when an object is moved. There is one RID Master per Domain Responding to requests from NT4 PDCs, Maintaining the time for the Active Directory Domain, and resolving failed logon attempts are the responsibility of the **PDC Emulator**. There is one PDC Emulator per Domain. The role of Infrastructure Master was moved to GIACCORP2. With the role of **Infrastructure Master**, GIACCORP2 has duty of updating the SID and Distinguished Name information of objects in Active Directory. When the Infrastructure Master role is on the same machine as a Global Catalog server, it does not recognize changes to the objects in Active Directory and no updates are sent out to other Domain Controllers. Therefore this role was moved to GIACCORP2. GIACCORP1 is currently the only **Global Catalog** server in the domain. GIACMID1, and GIACWEST1 will take on the function of Global Catalog servers when the company expands into global markets. The reasoning behind this is that in a single domain, all Domain Controllers contain the same information and queries into Active Directory do not require a Global Catalog server to resolve Universal Group membership. When the tree expands and contains multiple domains, having a Global Catalog Server in each site has the advantage of keeping these queries on the local network where they will be faster and will not use up the bandwidth of the WAN connection.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (6)

DNS Services

GIACCORP1 is the main DNS server for the company. It has one (1) forward lookup zone defined, one (1) reverse look up zone, is Active Directory integrated, allows for dynamic updates, and is set up as a forwarder to the DNS Server of the ISP. With an Active Directory integrated zone all Domain Controllers will have a copy of the zone information and there will be no need for primary or secondary DNS servers.

The reverse lookup zone is simply a method of resolving DNS names from IP addresses. With Dynamic Update enabled, the forward and reverse lookup information can be updated by the DHCP server or the workstation.

All DNS requests that cannot be resolved by the servers in each site are sent to GIACCORP1. If the DNS cache at GIACCORP1 does not contain the requested record, then it forwards the request to the DNS server at the ISP.

1 forward lookup zone	ad.giac.com
1 reverse lookup zone	in-addr.arpa
other	Active Directory integrated Dynamic updates

The forward lookup zone is for the ad.giac.com namespace.

From a security standpoint, all internal zones transfers are secured by the use of Active Directory Integrated Zones, and Secure Dynamic Updates from the client computers.

DHCP Services

There are three (3) scopes created for use in the GIAC network and they are located in the respective locations of the company.

Columbus

GIACCORP1 is configured as the main DHCP server on the Columbus network. It is configured with a scope that contains all 1024 Class C addresses from the address range of 192.168.0.0/22 (4 Class C address ranges super-netted together). 30% of the addresses are excluded from use. These are 307 addresses from the upper end of the range. The reasoning behind this is that these addresses are defined and enabled on the secondary DHCP Server (GIACCORP2) in the event that DHCP services are unavailable from GIACCORP1. The range of addresses from 192.168.0.1 through 192.168.0.63 are set aside for manually assigned addresses and are setup as reserved in the scopes of both DHCP servers.

GIACCORP2 is configured as the secondary DHCP server. It is configured with a scope of all 1024 Class C addresses from the 192.168.0.0/22. 70% of the addresses are excluded from use. These addresses are in the lower range of the 1024 addresses

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (7)	and are issued by the GIACCORP1 DHCP server. The remaining 30% of the addresses that are issued by GIACCORP2 and are enough to cover the Columbus site in the event that the DHCP services of GIACCORP1 are unavailable. Both DHCP servers are configured to dynamically update DNS. This keeps the DNS records current. **Fargo** GIACMID1 and GIACMID2 are configured the same as their counterparts in the Columbus network. The address range of 192.168.4.0/22 is in use as the super-netted segment thereby giving this segment 1024 IP addresses to use. **Tucson** GIACWEST1 and GIACWEST2 are configured the same as their counterparts in the Columbus network. The address range of 192.168.8.0/22 is in use as the super-netted segment thereby giving it 1024 IP addresses to use as with the other segments. **SNMP Services** Due to the relatively small size of the network, SNMP services are not in use. **SMTP Service** (Email) Email is handled through a two-step process for incoming mail and a one step for outgoing. The Exchange Server does not receive incoming mail directly. The External ISA server actually re-directs the mail to a message screener running on the Web server. The message screener is an option component of the ISA Server, which checks the mail against a set of rules to see if it should be forwarded. If the mail passes all the checks, it is then sent on to the Exchange server to be delivered to the internal user. (see additional security section for description of this process) Outgoing mail is sent to the Exchange server where it is sent on to the appropriate destinations. **Web Services** The IIS server is not directly accessed from the outside world. The external ISA server "publishes" or in better terms, accepts port 80 (http) and port 443 (SSL) web requests and redirects them to the web server located on the Perimeter (DMZ) network. This has the effect of protecting the web server from attacks on other all

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram (Cont.) (8)	ports other than 80 and 443. (see additional security section) **WINS Services** WINS is not in use. **Terminal Services** Mobile and remote users can access resources by using the GIACTERM server. It is located in the Perimeter (DMZ) Network. The external firewall is set to allow the MS-WBT-Server protocol (TCP 3389 and UDP 3389) to pass through. The internal firewall is configured to allow GIACTERM access to internal resources DNS (UDP 53), SQL Server (TCP 1433), others may be needed depending on future growth NetBIOS (TCP 137,139), Kerberos Password (TCP 464), Secure LDAP (TCP 636), Kerboros Sec (TCP 88). **IPSEC** Is only used by the Research and Development team. (see additional security) **Backups** A differential backup scheme is used for the facilities. Backups are performed on the following schedule: Sunday: Full Monday: Diff Tuesday: Diff Wednesday: Diff Thursday: Diff Friday: Diff There are two sets of tapes used for the daily backups (M-F), and these are alternated every other week. A total of 10 tapes are used for the dailys. The Sunday tape is considered to be the weekly tape, and the last Sunday of each month is pulled from use and stored at an offsite location. The other weekly tapes are stored onsite in a fireproof data safe, and are re-used in subsequent months. The fiscal year ends with the calendar year, so the last tape of the year is used as the yearly tape and the first tape after all financial transactions are complete is saved as the fiscal tape. Additional copies are made of the yearly and fiscal tapes and one set is stored locally while the other is stored off-site.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Active Directory (AD) Design and Diagram
---
30 Points

Domain and OU Design

GIAC has a single Active Directory Domain. This design was chosen for the following reasons:

- Simplicity (Easier to manage)
  - Only Global Groups and Domain Local groups are needed. Universal groups are only needed when multiple domains are used.
  - Global Groups can be added to Universal groups later when the company expands into other parts of the world and begins using multiple domains.
  - When membership in a Universal Group changes, the changes must be replicated to other Domains. This eliminates the need for Universal Groups for now.
  - A single domain level group policy for software installation is all that will be needed.
- Only one Account Policy is needed
  - The company is currently limited to one continent and is within the boundaries of one government.
  - Passwords, Kerberos settings, and account lockout policies will be the same throughout the current organization.
- Placing each location into a separate domain may reduce replication traffic, but the use of sites and the speed of the T1 link will handle any current and planned traffic.
- When the company expands into Europe, South America, and Asia it will then look at creating separate Domains for those regions.

There are seven (9) Organizational Units (OU) created (see figure 3a).
The Columbus location has the most complex structure. It has a parent OU (EAST) and 3 child OUs (Corp, Mfg, Dev). Fargo and Tucson each have a parent OU (Mid and West) and a Mfg child OU. There is a separate OU to address the needs of the sales/mobile people.

Columbus	Fargo	Tucson	Other

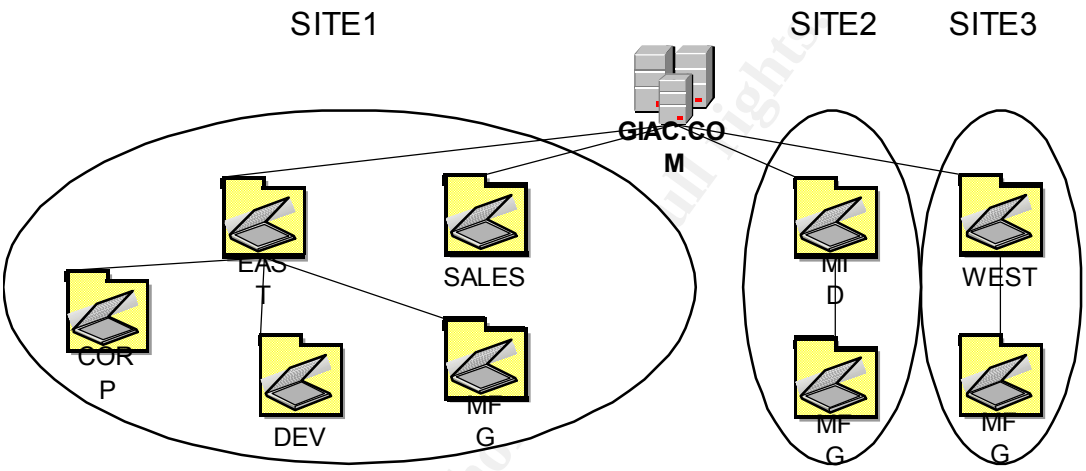
• East
  • Corp
  • Mfg
  • Dev
	• Mid
	  • Mfg
		• West
		  • Mfg
			• Sales

(Fig 3a) Organizational Unit listing

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Active Directory (AD) Design and Diagram (cont.) (2)



(Fig 3b) OU Design for GIAC.COM

Domain and OU Design Specifics

Columbus

East:

- This is the container for the eastern division of the company. It is the Parent OU for the corporate offices, the Research and development division, and for the manufacturing floor.
- One of the purposes of this container is to allow for GPO settings that affect all of the Eastern Division. Any GPO settings that are set at this level will flow through inheritance into the child OUs (Corp, Dev, and Mfg)
- Another purpose is for delegation of authority. Network administrators for the entire Eastern location can be assigned at this point. Their authority will flow through inheritance into the child OUs.

Corp:

- The main purpose for this container is for GPO assignment. It is used for software deployment and system/user settings that are specific to the corporate office area.

Dev:

- All of the resources for the Research and Development department are in this container. It is used for R&D specific GPO settings

Mfg:

- This is the container for the manufacturing floor and is used to contain the resources relating to production.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Active Directory (AD) Design and Diagram (cont.) (3)	• It allows the software GPO from the parent GPO (East) to be blocked so that the software applications are not installed. • The GPO for this OU assigns new software applications and very restrictive desktop settings **Fargo** Mid: • This is the container for the mid-US division of the company. It is the Parent OU for Fargo and contains one child OU. • It is use for the assignment of software, and to delegate administrative control Mfg: • This is the container for the manufacturing floor and is used to contain the resources relating to production. • It allows the software GPO from the parent GPO (East) to be blocked so that the software applications are not installed. • The GPO for this OU assigns new software applications and very restrictive desktop settings **Tucson** West: • This is the container or the western division of the company. It is the Parent OU for Tucson and contains one child OU. • It is used for the assignment of software and to delegate administrative control. Mfg: • This is the container for the manufacturing floor and is used to contain the resources relating to production. • It allows the software GPO from the parent GPO (East) to be blocked so that the software applications are not installed. • The GPO for this OU assigns new software applications and very restrictive desktop settings **Corporate-Wide** Sales: • The mobile users have some specific requirements due to the use of laptops. This OU is used to address the issues that are specific to mobile users.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

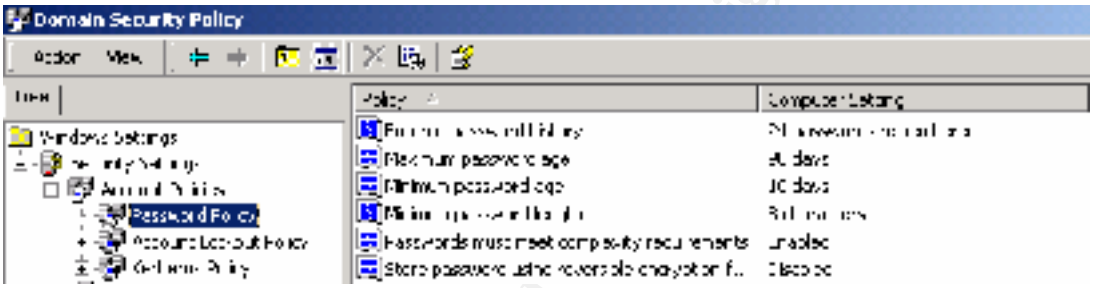
Group Policy and Security: 50 Points Total

Basic Group Policy

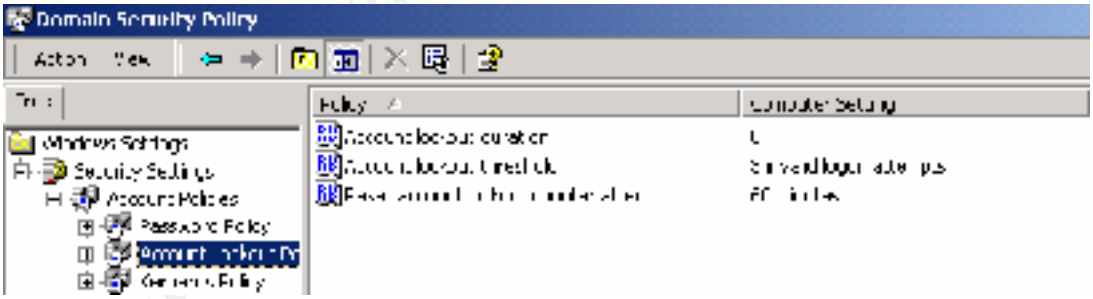
---

20 Points

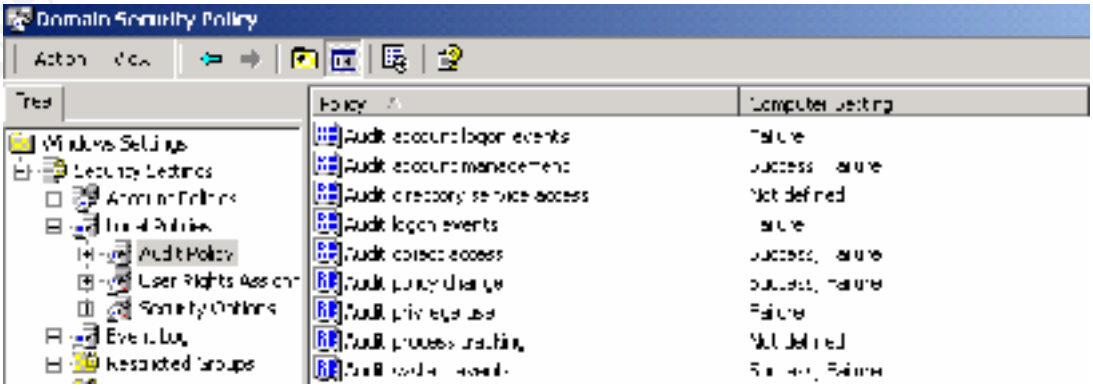
Default Domain Policy



In the Default Domain Policy, the **Password Policy** settings are configured to be strict. A setting of ninety days (90) is used for the Maximum Password Age to help reduce the chance that people would write their password down due to it changing frequently.



The **Account Lockout Policy** is set so that the account will have to be reactivated by a member of the systems support staff. Automatic reset of the accounts has effectively been disabled.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (2)

The **Audit Policy** is set to monitor important events but not overwhelm the staff.

Audit Account Logon Events:
Set to log when there is a failure logging into a user account.

Audit Account Management:
Set to log both successful and failed attempts to change user account info.

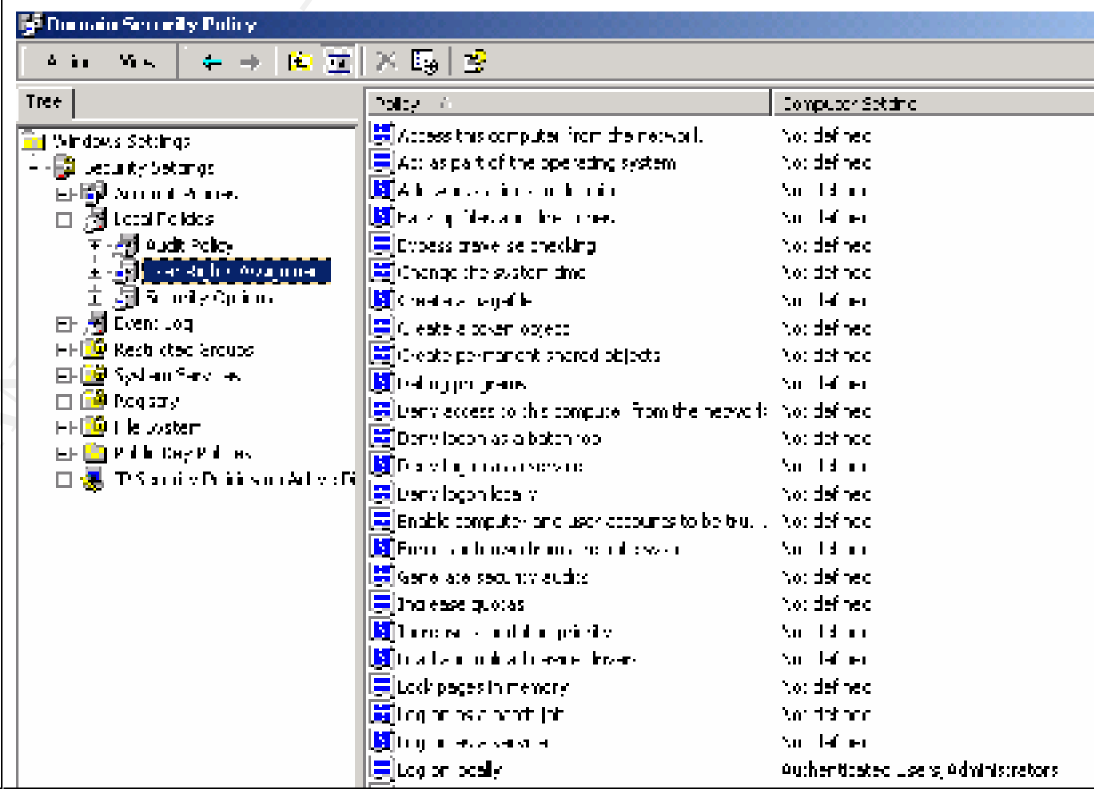
Audit Logon Events:
Failure of service accounts and major application accounts is recorded with this setting. It is set for failures.

Audit Object Access:
Used to track access to Active Directory Objects. The object must have auditing turned on for the objects that access it.

Audit Policy Change:
This setting will produce log records when changes are made to policies, and other settings. Most notably to user accounts and security settings.

Audit privilege Use:
Will log events such as changes to the system time.

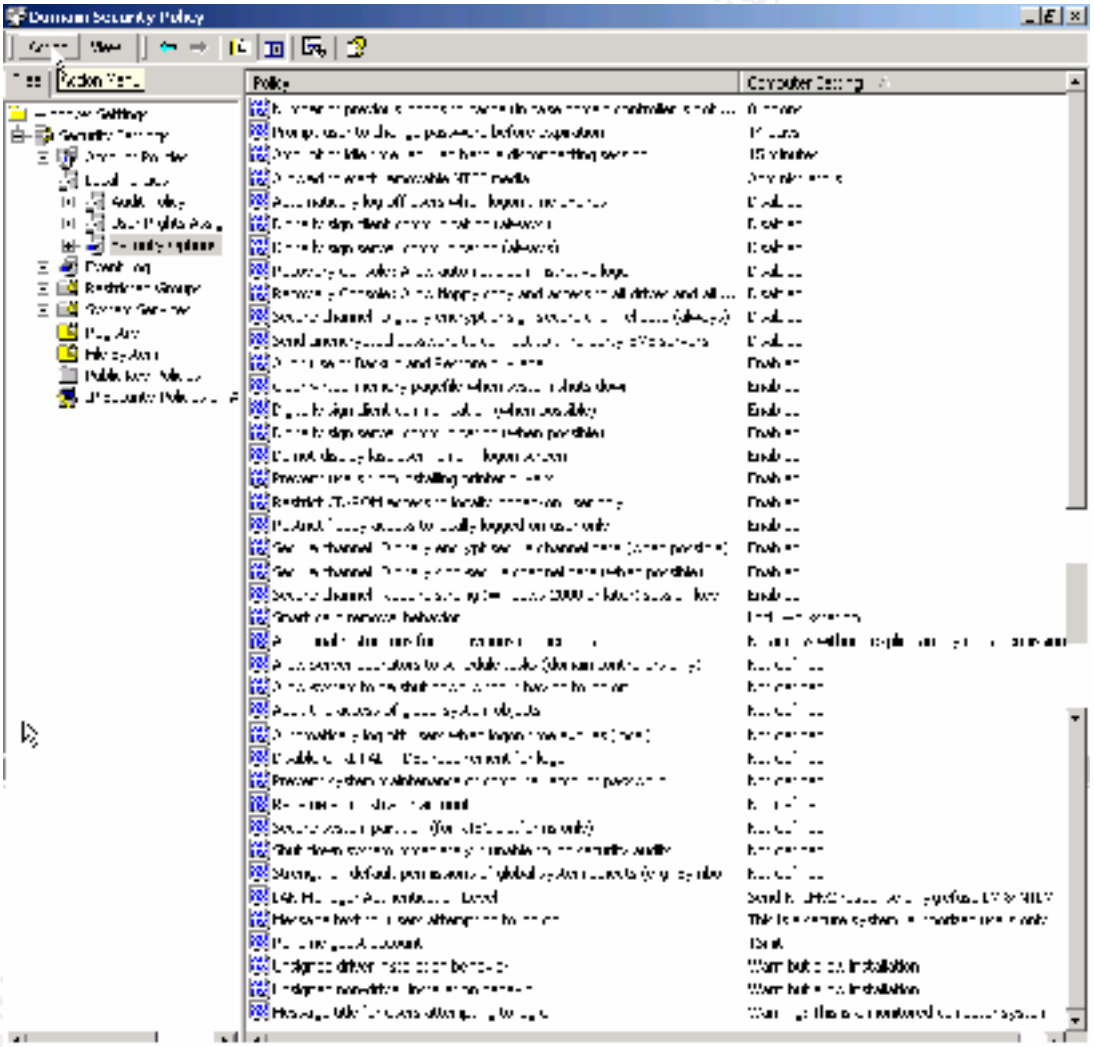
Audit System Events:
Tracks start up and shutdown of the computer, and other events that affect the whole system. Failure of these events will be tracked.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (3)

The only setting changed in User Rights Assignments is who is allowed to log on locally. It is set to allow only administrators and authenticated users.



In the area of Security Options, several items are changed from the default.

Number of previous logons to cache:

Set to 0. This forces authentication to a Domain Controller for access. If not set, a computer could be disconnected from the network after a user account has been disabled, and the user will still be able to logon.

Prompt user to change password before expiration:

Set to 14 days as courtesy to the user.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (4)	Amount of idle time before disconnecting session: Set to 15 minutes Allowed to eject removable NTFS media: Administrators only Automatically log off users when logon time expires: Disabled Digitally sign client communications (always): Disabled. This setting may cause communications problems, so it is disabled. Digitally Sign server communications (always): Disabled. Same as above. Recovery Console: allow Automatic administrative logon: This is set to Disabled to force the use of a password to enter the Recovery Console. Recovery Console: Allow floppy copy and access to all drives and…: Disabled. This option would allow someone to copy files from non-W2000 system directories when they are in the Recovery Console. Secure Channel: Digitally encrypt or sign secure channel data (always): Disabled. This option would force all computers to connect to Domain Controllers with a secure channel. Send unencrypted password to third-party SMB servers: Disabled. This is to prevent non-Microsoft servers from receiving an unencrypted password. Audit use of Backup and Restore privilege: Enabled to track which users are backing up data that can be restored elsewhere. Clear virtual memory pagefile when the system shuts down: Enabled to prevent information from being retrieved from the pagefile if the harddisk is stolen. Digitally sign client communication (when possible): Enabled. This will allow secure communications when both sides support it, but still allow a connection when they don't. Digitally sign server communications (when possible): Enabled. Same as above. Do not display last user name in logon screen: Enabled. Although a determined individual could get logon names another way, this is less it could be done. Prevent users from installing print drivers: Enabled to prevent possible loading of Trojans Restrict CD-ROM access to locally logged-on user only: Enabled. Prevents sharing of the CD-ROM drive.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (5)

Restrict floppy access to locally logged-on user only:
Enabled. Prevents sharing of the floppy drive.

Secure Channel: Digitally encrypt secure channel data (when possible):
Enabled. To enhance secure communications when possible.

Secure Channel: Digitally sign secure channel data (when possible):
Enabled. Same as above.

Secure Channel: Require strong (Windows 2000 or later) session key:
Enabled. Same as above.

Smart Card removal behavior:
It is set to Lock Workstation, so that the key has to be present and in the reader for the computer to be used.

Additional restrictions for anonymous connections:
"No access without explicit anonymous permissions" is the option chosen. This option is to prevent the "null" user account from gaining access to information.

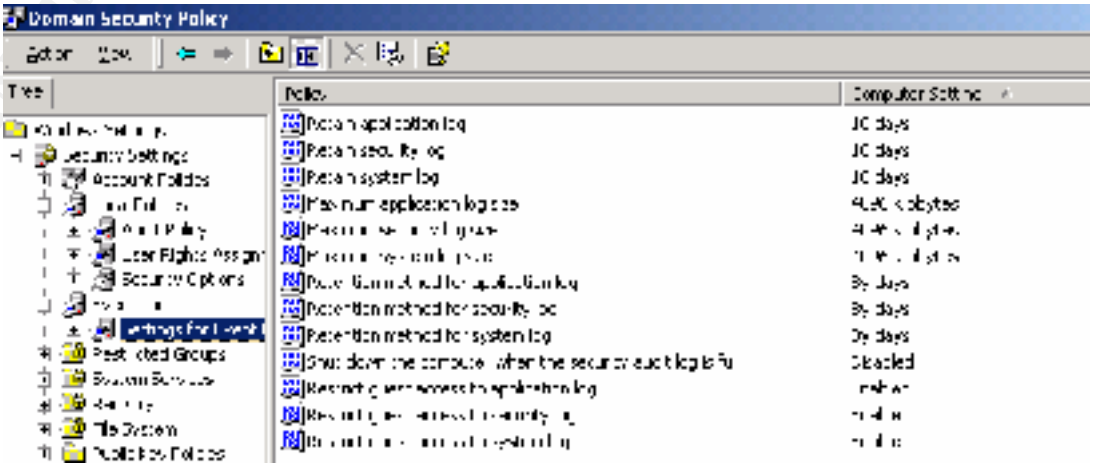
LAN Manager Authentication level:
This option is set to "Send NTLMv2 response only\refuse LM & NTLM" to ensure the higher level of protection from NTLMv2 is used.

Message text for users attempting to log in:
This is set to a message that informs the users that they are on a secure system, and that it is for authorized access only.

Rename guest account:
Any generic name that follows the naming rules.

Unsigned driver installation behavior/ Unsigned non-driver installation behavior:
Warn but allow a installation

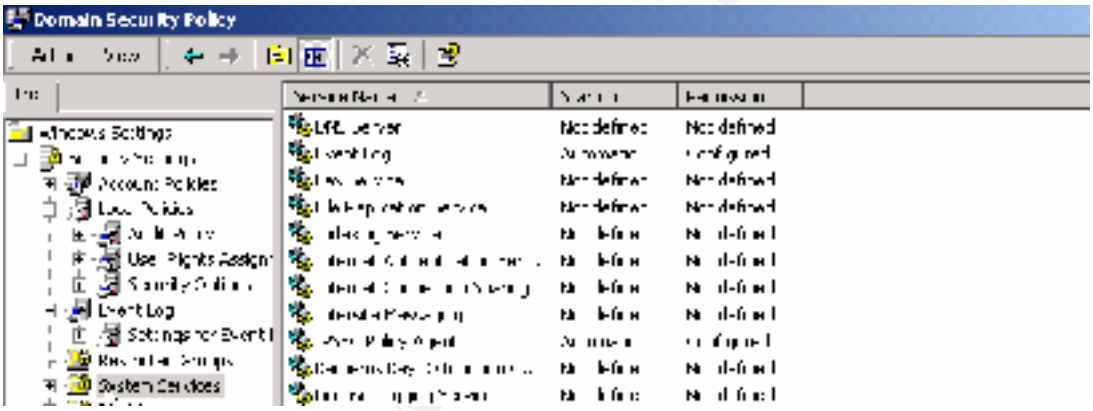
Message title for users attempting to log on:
A warning that they are login onto a secured or monitored system.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (6)

The Event Log settings are configured for each machine to have four (4) Megabytes of disk space and to overwrite on a ten (10) day schedule. The ten (10) day schedule is to allow more than a one (1) week overlap.

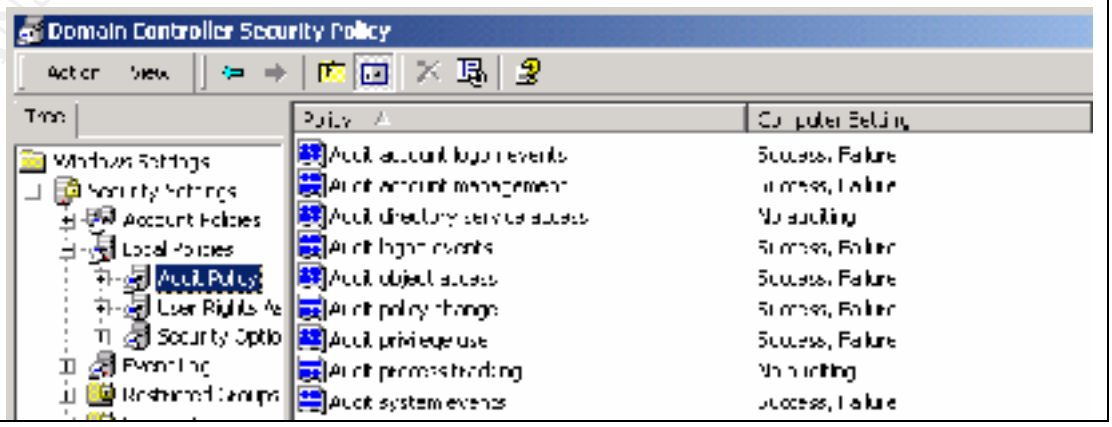


The only System Services that are configured are the Event Log and the IPSEC Policy Agent. Both are configured to start automatically when the system starts. This is to ensure that logging and IP security cannot be inadvertently turned off.

An additional GPO is assigned to the domain for items not covered in the Default Domain Policy. (see Additional Group Policy below)

Group Policy for Domain Controllers

Very few changes are made to the Group Policy for Domain Controllers over what is set for the Domain Policy. One thing to note is that by replicating the settings here, it is ensured that changes to the Domain Policy does not affect the security of the Domain Controllers. Listed below are the differences from Domain Policy.

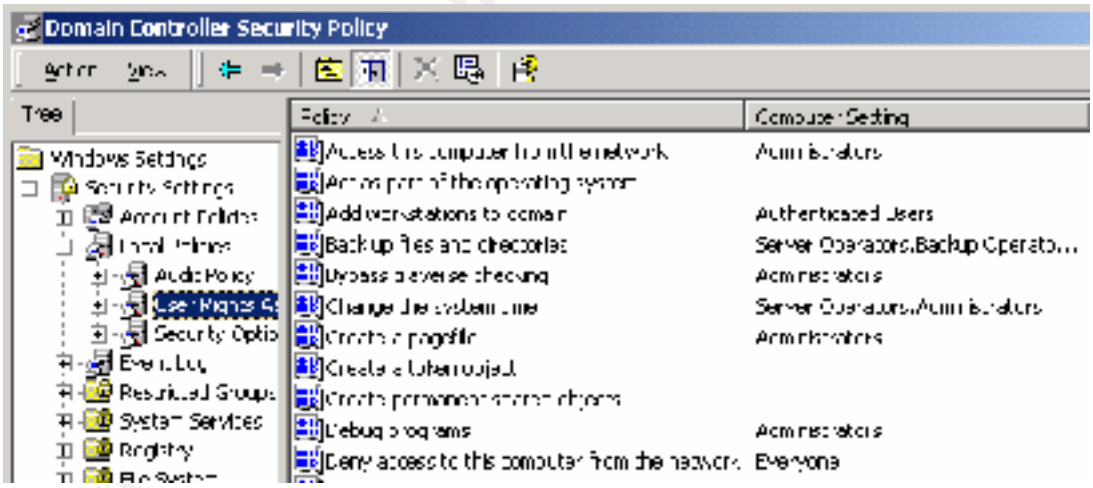


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (7)

The Audit Policy is different in that Audit Account Logon Events, Audit Logon Events, and Audit Privileged Use are now all set for Success and Failure. The reasoning for this is that these settings:

Audit Account Logon Events:
Will allow the tracking of successful logons to the servers.
Audit Logon Events:
The successful logon of services on the system. This may identify services that have accidentally or maliciously been turned on.
Audit Privileged Use:
The successful change of the system time is one example of what will now be tracked on the server.

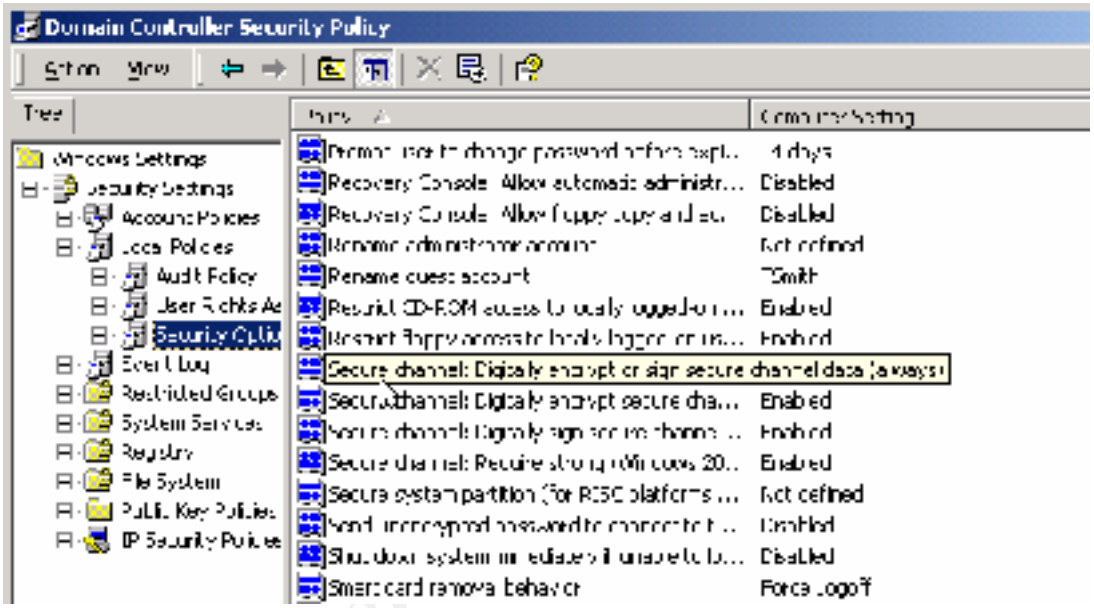


Multiple options are set in the User Rights Assignment page. The "basicdc.inf" security template is applied by default to "new" domain controllers and makes these configuration settings at the time of installation. An upgraded NT4 domain controller, on the other hand, does not have this template applied. This template was modified to include GIAC settings and is imported into the Domain Controller GPO so that it will be applied to all Domain Controllers. If a Domain Controller's settings get changed, they will be changed back when the GPO refreshes. There is only one setting changed from the default.

Access this computer from the network:
Set to Administrators. This option is set to allow only administrators to attach to the Domain Controllers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Basic Group Policy (Cont.) (8)



In the Security Options page the main things of additional concern are: renaming the guest account, and smart card removal behavior. All other setting are set the same as those of the Domain Group Policy.

Rename guest account:

The guest account is renamed to a name that matches the current naming scheme, but is disabled and never used.

Smart card removal behavior:

Is set to "Force Logoff". The domain setting is to lock the computer, but the Domain Controllers are set to log the user off.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Group Policy:
---
20 Points

Additional Group Policy for the Domain:

There is an additional Group Policy assigned to the domain. This GPO has the software that will be assigned and published. It also contains the specific user and computer settings that are needed.
Listed below are the settings that are changed from the standard configuration.

Turn off Autoplay	Yes	This is to prevent CDs with malicious programs from automatically loading
Delete cached copies of roaming profiles	Yes	
Run logon scripts synchronously	No	This option will force the logon scripts to complete in the order in which they were intended
Run startup scripts visible	No	This is an "out of sight, out of mind" item, the users dos not need to see this happen
Run shutdown scripts visible	No	Same as above.
Don't display the Getting Started welcome screen at logon	Yes	This is a general cleanup item to keep users from being bothered with it.
Turn off background refresh of group policy	No	GPOs should continue to be updated on the default schedule of 90 min. (plus 0 to 30 min)
Scripts policy processing	Yes	To force scripts to be run
Security policy processing	Yes	To ensure security policy
IP Security policy processing	Yes	To ensure that IPSEC policies are enforced
Prohibit use of Internet Connection Sharing on DNS Domain Network	Yes	To prevent PCs from sharing the connection of one PC
Web based printing	No	Precaution to remove unneeded functionality and possible security problems
Prohibit new task creation	Yes	This option is turned off to stop someone from scheduling a malicious program to run

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Group Policy: (Cont.) (2)

Do not keep history of recently opened documents	Yes	This is to make it harder for someone to visit an unattended machine and locate documents.
Clear history of recently opened documents	Yes	Same as above.
Remove user name from Start menu	Yes	Forces the user to enter a username at logon and reduces the ease at which someone can get user names
Hide "my network places" icon on desktop	No	Not a total deterrent, but it makes it harder for some user to browse the network
Password protect the screen saver	Yes	To secure the workstation when the user is absent
Screen saver timeout	10 min	Same as above
Prevent access to registry editing tools	Yes	Disables use of regedit and regedt32
Run legacy logon scripts hidden	Yes	Out of sight, out of mind
No "Computers near me" in My Network Places	Yes	Makes it harder to see other local computer in same workgroup or Domain
No "Entire network" in My Network Places	Yes	Cuts down on casual browsing of local network objects

Group Policy per OU:

East

At this time East Container does not have any additional GPOs assigned.

Corp

An additional GPO is assigned that controls (desktop settings, software…)

Dev

The GPO assigned to DEV is set with IPSEC policies enabled and is more security conscious.

Mfg

The GPO for the Manufacturing OU within the East OU currently blocks the inheritance of the additional Domain GPO and assigns restrictive computer settings as well as a different set of software application.

Mid

At this time Mid Container does not have any additional GPOs assigned.

Mfg

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Group Policy: (Cont.) (3)	The GPO for the Manufacturing OU within the Mid OU currently blocks the inheritance of the additional Domain GPO and assigns restrictive computer settings as well as a different set of software application. **West** At this time West Container does not have any additional GPOs assigned. Mfg The GPO for the Manufacturing OU within the West OU currently blocks the inheritance of the additional Domain GPO and assigns restrictive computer settings as well as a different set of software application. Sales The Sales OU is set up to address the needs of the mobile sales people. It has settings that are specific to offline files and bandwidth specific settings.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Security:
---
10 Points

Roaming Profiles
R&D OU

Groups:

Global groups are used in a Microsoft Network as the first repository for users. From here, the Global Groups are then placed into Domain Local Groups, nested within other Global Groups, or placed into Universal Groups. Microsoft suggests the following method: AGDLP and AGUDLP

A - Add users
G - Assign Users to Global Groups
U - Place Global Groups into Universal Groups
DL - Place Global Groups or Universal Groups into Domain Local Groups
P - Assign Permissions to the Domain Local Groups

Universal Groups can only be used in Native Mode Windows 2000 Domain. Therefore AGUDLP can be used only in Native Mode, while AGDLP can be used in Mixed and Native Modes.
Permissions can be assigned to Domain Local Groups or to Organizational Units (OUs). OUs can be thought of as "logical groupings" of users and other resources. Permissions can be assigned to the Organizational Unit object and these permissions flow to all the objects (users, computers, etc) in the OU. The Domain Local Groups, on the other hand, are used when you only want to assign permissions to a subset of the users, users from other OUs, Global Groups, or users and groups from other domains.
Listed below are the groups created for use in the GIAC network.

Global Groups: (General)

Eng_Col_G	Eng_Far_G	Eng_Tus_G
Finance_Col_G	Finance_Far_G	Finance_Tus_G
HR_Col_G	HR_Far_G	HR_Tus_G
Mfg_Col_G	Mfg_Far_G	Mfg_Tus_G
Prod_Col_G	Prod_Far_G	Prod_Tus_G
QA_Col_G	QA_Far_G	QA_Tus_G
Users_Col_G	Users_Far_G	Users_Tus_G
Mktg_Col_G	Sales_Col_G	Research_Col_G

As can be seen, similar Global Groups for each department are created at each location. Marketing, Sales, and Research are the exception since they are located only in Columbus.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Security: (Cont.) (2)

Global Groups: (additional)

Eng_Users_Col_G	Eng_Users_Far_G	Eng_Users_Tus_G
QA_Users_Col_G	QA_Users_Far_G	QA_Users_Tus_G

These groups are to accommodate the Users who need "read" access to data but not the ability to change it.

Global Groups: (Admin)

Admin_Col_G	Admin_Far_G	AdminTus_G
Admin_Dev_G		

The above listed Global Groups are for administrators in each location.

Administrative groups for the Domain Admins, and Enterprise Admins are already built into Windows 2000. The built-in groups are used whenever possible and new groups are only created when necessary. The built-in groups for Backup Operators, Server Operators, and Print Operators are used.

Domain Local Groups: (General)

Eng_Col_DL	Eng_Far_DL	Eng_Tus_DL
Finance_Col_DL	Finance_Far_DL	Finance_Tus_DL
HR_Col_DL	HR_Far_DL	HR_Tus_DL
Mfg_Col_DL	Mfg_Far_DL	Mfg_Tus_DL
Prod_Col_DL	Prod_Far_DL	Prod_Tus_DL
QA_Col_DL	QA_Far_DL	QA_Tus_DL
Users_Col_DL	Users_Far_DL	Users_Tus_DL
Mktg_Col_DL	Sales_Col_DL	Research_Col_DL

As can be seen, similar Global Groups are created at each location. Marketing, Sales, and Research are located only in Columbus.

Domain Local Groups: (additional)

Eng_Users_Col_DL	Eng_Users_Far_DL	Eng_Users_Tus_DL
QA_Users_Col_DL	QA_Users_Far_DL	QA_Users_Tus_DL

These groups are to accommodate the Users who need "read" access to data but not the ability to change it.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

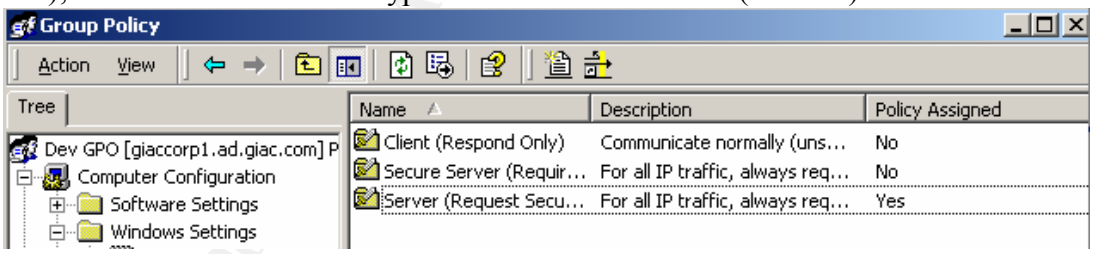
Additional Security: (Cont.) (3)

Domain Local Groups: (Admin)
Admin_Col_DL Admin_Far_DL AdminTus_DL
Admin_Dev_DL

Additional Organizational Units:

Dev: (Research and Development)

The Research and Development users and computers are placed into a separate OU to support the use of an additional Group Policy Object (GPO). This GPO applies to both the users and the computers and mainly focuses on the use of IPSEC to secure communications between the R&D department and the GIACDEV Server. Listed below are the GPO settings that are different. Request Security is set. This causes R&D computers and GIACDEV Server to use IPSEC (they are all in the same Dev OU), but still allows non-encrypted traffic to the firewall (Internal).



Sales: (Mobile Users)

This OU is used to mainly assign settings that are specific to the Sales or Mobile users. These include settings to not push login scripts, startup scripts, shutdown scripts, and logoff scripts to the user. It is set to disallow pushing the "My Documents" folder to the users. It is also set to not do Software installations or updates because of too slow of connection speeds.

Roaming/Mandatory Profiles:

Roaming Profiles are in use by all office users of the network. By using Roaming Profiles, users are able to move to another machine and have the same familiar settings and access that they had on their usual machine. This is convenient when a user's computer becomes unusable due to a failure of the computer or the network connections. It allows the user to stay productive by simply moving to a working computer.

The users on the manufacturing floor use shared accounts that are configured with Mandatory Profiles. The Mandatory Profiles allow a standard configuration to be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Security: (Cont.) (4)	implemented and training to be standardized to that desktop. While a user may be able to make some changes to the desktop settings, those settings will not be retained, and the computer will return to the "standard desktop" the next time it I logged in. **Disable unneeded services** Services that are not being used on a machine should be disabled or removed. Disabling a service will prevent it from being exploited, removing the service will keep it from accidentally or maliciously being turned on. The IIS web service, ftp, and telnet are examples of services that can be disabled on most machines. **Posix / OS/2** Posix and OS/2 compatibility are not required. These subsystems are disabled by editing the registry . http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q320869 **Separate partitions for log and swap** The log and swap files have been moved to a disk partition other than the system partition (usually where the Winnt directory resides). This prevents the system from shutting down due to the harddisk running out of space. **Install into OpSys directory** The operating systems have been installed into the OpSys directory rather than the Winnt directory. This cannot be done from a clean CD install. Either the installation must be done using the winnt.exe program, the winnt32.exe program, or the partition must already contain a winnt directory. This is done because scripted attacks and some utilities look for the winnt directory. (winnt.exe and winnt32.exe can be found in the i386 directory of the Microsoft Windows 2000 installation disk) **Emergency Repair Disk (ERD)** Emergency repair disks have been created and stored in a fireproof data safe in the event that a machine needs to be recovered. Updated disks are made whenever there has been a change made to the disk configuration on a system. To manually create an ERD: Click on Start> Programs> Accessories> System Tools> Backup and then select Tools and "Create an Emergency Repair Disk".

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional Security: (Cont.) (5)

Link on how to create an Emergency Repair Disk:
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q231777

Recovery Console:

The Recovery Console is loaded on all of the servers. When Safe mode and Last Known Good Configuration do not allow a machine to be started properly, the Recovery Console can be used. It can either be loaded and run by using the CDROM drive or it can be placed on the machine as a boot-up option. The boot-up option is what was chosen for GIAC

Listed below is link on how to install the Recovery Console:
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q318752

Message Screener:

The message Screener can be run on the ISA Server or another computer. The Web Server at GIAC was logical choice for this role or the following reasons:

- The Message Screener software requires a computer that is running both IIS and SMTP services.
- The Web Server already existed.
- Microsoft includes an SMTP Virtual Server with Windows 2000.
- The load on the Web Server is low due to the external ISA server acting a reverse proxy/caching server.

The Message Screener installation involves:

- Running the ISA server installation on the Web Server and only installing the Message Screener.
- Running the SMTPCred.exe utility that is in the \isa\i386 directory of the ISA Server installation CD.
  - This will prompt for the Name of the ISA Server, how often to check the ISA Server for updated configuration information, and a logon name/password for access to the ISA server.
- Creating a server publishing rule on the ISA server.
- Configure DCOM to for Message Screener access.

Additional information on setting up the message screener can be found on the ISA Server Installation Disk in *support\docs\smtpfilter*.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A:

Definitions:

Category 5 – Twisted pair (4 pair) wiring used in networks to carry 100 MB data stream

DC – Domain Controller

DHCP – Dynamic Host Configuration Protocol – A service that delivers IP addresses.

Forest – A group of Domains that are part of the same name-space.

GPO – Group Policy Object

ISA – Internet Security and Acceleration. Microsoft Proxy/Firewall

OU- Organizational Unit

RAID - Redundant Array of Inexpensive Drives

RAID 1 – Also known as mirroring. Two synchronized drives are used to hold the data.

SQL – Structured Query Language

Y2K - Year 2000

References:

Cisco:

Cisco 3600 Documentation
http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/index.shtml

Microsoft:

Microsoft Official Curriculum
2150 Designing Security for Windows 2000
1561 Active Directory Design
2154 Active Directory Admin
Windows 2000 Resource Kit

Domain Controller Setup
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q238369

Links on how to create an Emergency Repair Disk
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q231777
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q216337

Global Catalog Setup
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q320824

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References:
(Cont.) (2)

Windows 2000 Deployment guide
http://www.microsoft.com/windows2000/techinfo/reskit/deploymentscenarios/default.asp

SMTP Filter Configuration
\support\docs\smtpfilter.htm (on the ISA Server installation disk)

Transferring FSMO roles
http://search.support.microsoft.com/search/viewDoc.aspx?docID=KC.Q255690

Disabling Posix and OS/2 subsystems
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q320869

Recovery Console installation
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q318752

Windows 2000 Active Directory Roles
http://search.support.microsoft.com/search/viewDoc.aspx?docID=KC.Q197132

Securing connections between two hosts in Windows 2000
http://search.support.microsoft.com/search/viewDoc.aspx?docID=KC.Q301284

Global Catalog requirements for user and computer logon
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q216970

Windows 2000 DNS - Dynamic Updates
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q317590

Windows 2000 - DHCP Dynamic Updates with DNS
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q228803

DHCP Servers with split scopes
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q280473

Designing an ISA server solution
http://www.isaserver.org/pages/articles.asp?art=65

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: July 25th, 2017

Upcoming Training

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