A Secure Network Infrastructure for GIAC Enterprises

GCWN 3.1

Option 1 – Design a Secure Windows 2000 Infrastructure

By

Tyler Lehman

May 2003

Abstract

This document details the creation of a secure network and active directory infrastructure for the fictitious company GIAC Enterprises. GIAC Enterprises has its home office in Houston, Texas, and a branch facility in Washington, D.C. The company makes diapers out of recycled paper obtained from Congress. In the current report, the physical network is discussed as well as antivirus, backup, PKI, and computer configurations. A single domain was selected for GIAC Enterprises, and the design of the active directory is discussed, including the Domain, Sites, and Organizational Units. Group policy is elaborated in depth, with an emphasis on the basic policies for the domain and domain controllers as well as examples of settings to secure other types of systems in the enterprise. Finally, some attention is focused on other security factors such as employee training and physical security of facilities.

Table of Contents

Description of GIAC Enterprises

GIAC Enterprises deals in the manufacture and online sales of biodegradable diapers made from recycled congressional paper. The main offices, production, and shipping are located in Houston, Texas; the supply of paper comes from Congress in Washington, D.C., and is handled by a branch office located in Washington.

The Washington, D.C., office consists of a warehousing facility, supply coordinators, and congressional lobbyists. GIAC Enterprises contracts the shipping of paper from Washington to Houston.

Houston was selected as the base of operations because of its rail and shipping channels, lower-cost facilities, and highly skilled paper shredders. Once the paper reaches Houston it is shredded and processed into diapers at small plants that GIAC Enterprises contracts with.

The main Houston offices house the research and development teams, the sales division, and the human resources department. The research and development teams design more effective diapers and monitor upcoming legislation to create computer models to estimate future supplies of paper; they also study the effects on legislation on the demand for recycled congressional biodegradable diapers. The sales department's main focus in on the web sales and the design of packaging for the diapers. The human resources department controls all employee records. Accounting is outsourced to a private firm.

Some security concerns for GIAC Enterprises include:

- Restricting users from one department from logging on to a computer of another department.
- Delegating parts of administration such as creating accounts for new users to the members of human resources charged with that duty.
- Making sure data is stored in a secure manner on laptops that could be stolen.
- Protecting data through antivirus prevention and backup strategies.

Network Design and Diagram

Network Overview of GIAC Enterprises

There are two main offices in GIAC enterprises: corporate headquarters in Houston, Texas, and a branch office in Washington, D.C. (Figure 1). The corporate headquarters located in Houston, Texas, house most of the employees, corporate administration, web operations, and email services. The corporate offices contain two domain controllers, the web servers, email server, certificate server and file/print servers all running sp3 with all updates.

The branch office in Washington has mobile lobbyists who spend time in the office but also a great deal of time in the Capitol: the lobbyists' tasks there include lobbying Congress to relinquish the papers to GIAC Enterprises as well as promoting legislation that favors the use of eco-friendly paper baby-products. These lobbyists carry laptop computers running the Windows 2000 professional sp3 operating system. The rest of the Washington staff receives the recycled congressional paper and prepares it for shipping to Houston. These employees access their email and fill out online shipping reports on Windows 2000 kiosks located throughout the warehouses. The branch office also houses a domain controller (DC) and a file/print server.

Network Hardware: Both Locations

The two locations use 10/100 switched networks with a gigabit backbone for the workstations. The servers connect to gigabit switches that are part of the backbone. The two offices will be connected with AT&T "xDSL Access to Frame Relay Service" with 1.5 Mbps transmission rates, and only the main office will have access to the internet.

There is also a proxy server (PRXh1 uses the basic server configuration with additional memory and hard drives to store cached web content, see table1 below) at the Houston site that will be used to connect to the internet for the employees at both locations. This proxy server helps control the bandwidth used for internet access because it controls which sites may be accessed, and because it caches common sites (so each hit on common sites does not have to go through the network connection).

DNS from the internet to the email and web servers is handled by the Internet Service Provider (ISP). There is no need to have the internal DNS resolved from the internet.

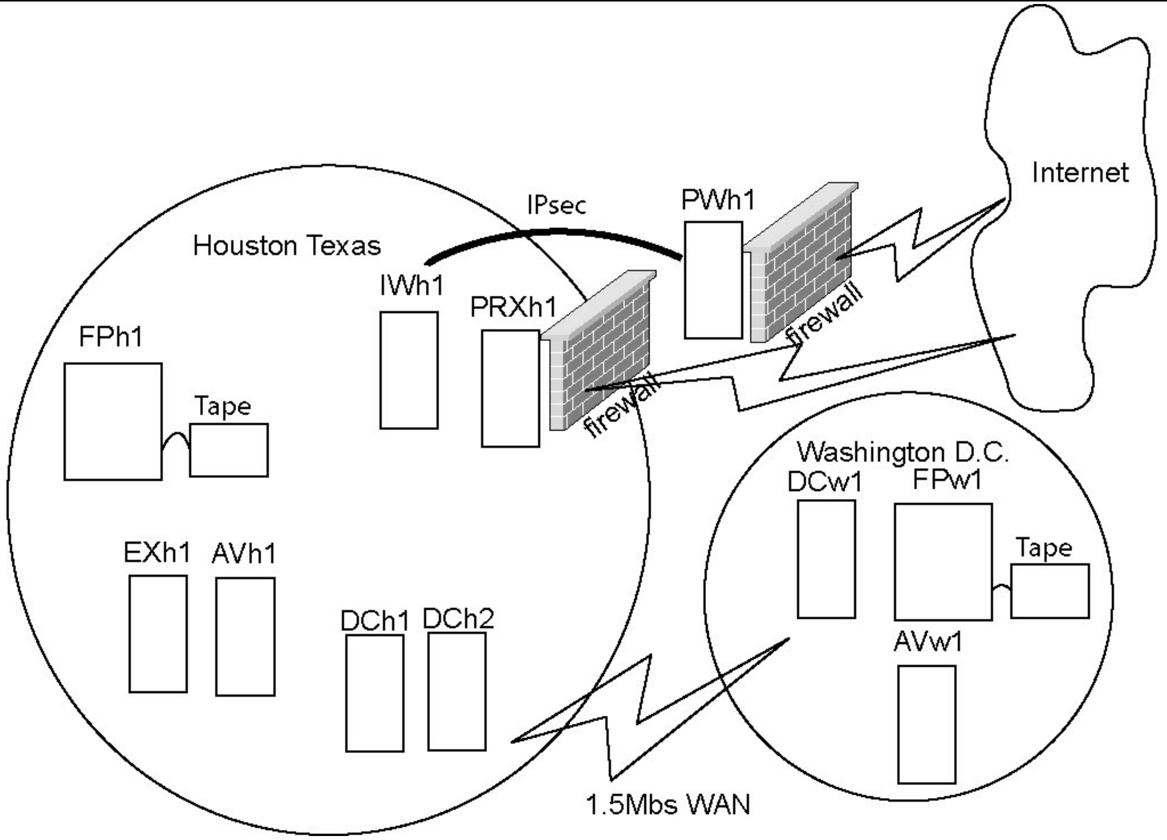

Figure 1 Network Diagram

Figure 1 Legend:

DCh1	First domain controller in Houston
DCh2	Second domain controller in Houston
DCw1	Domain controller in Washington, D.C.
FPh1	File and print server in Houston
FPw1	File and print server in Washington, D.C.
Tape	Tape libraries (in both locations)
EXh1	Exchange mail server in Houston
AVh1	Antivirus server in Houston
AVw1	Antivirus server in Washington, D.C.
IWh1	Internal web server in Houston
PWh1	Public web server in Houston
PRXh1	Proxy server in Houston

Network: Houston, Texas

At the headquarters offices in Houston, Texas, there are two domain controllers (DCh1 and DCh2 both use the basic server configuration, see Table 1 below.) Two DCs are used both for redundancy and to service the larger employee base in Houston.

Between the corporate intranet and the internet there is a DMZ bounded by two firewalls: the first filters most incoming traffic but lets in traffic to the public web server (PWh1 uses the basic server configuration plus an additional NIC: one for support to the internet, the other to receive updates from the internal network). PWh1 is a standalone server that has been hardened with security templates discussed later and whose content comes from an internal web server (discussed later). The firewall blocks all connections to ports on the web server that are not necessary for web function.

The second firewall filters inbound web traffic through the proxy server and forwards email to a spam filter and then on to the internal exchange server (Exh1 uses the basic server configuration with additional memory and hard drives to store mailboxes). Inside the second firewall is the internal web server (IWh1 is configured like the public web server, but with additional hard drive space to hold added web sites): it contains a working copy of the website and runs the internal intranet. Changes to the website are published through the inner firewall to the public web server over an IPsec encrypted channel on a daily basis. The connection is only enabled when an update occurs and can only be initiated from the internal web server: the connection is only established when the update and maintenance scripts are in use. This connection will be used to upload changes to the website and to gather log information on a scheduled basis.

IDS (intrusion detection system) equipment, in conjunction with firewall logs, can be used to monitor traffic behind the first and second firewalls to monitor attempts to compromise the web server or attempts to access the internal intranet. Host-based IDS such as Tripwire will be implemented on the servers with very strict settings on the web server. If the web server is compromised it can be rebuilt quickly with new fixes, or a new server can be installed in its place while the compromised server is analyzed.

There is also a file and print server in the Houston offices to service the operations in Houston (FPh1 uses the basic server configuration with an additional disk array of twelve disks and an additional NIC).

Employees in Houston have Windows 2000 professional workstations (all use the basic workstation configuration) at their desks; the computers are not shared by employees.

Network: Washington, D.C.

At the branch office in Washington, D.C., there is one domain controller (DCw1 uses the basic server configuration, see Table 1 below) that replicates with the DCs in Houston over a virtual private network shown in the diagram. Placing a DC in Washington serves two purposes; it provides additional redundancy for the active directory by having copies in both Houston and Washington, as well as an increase in performance by reducing traffic between the two cities during working hours. Washington also has a file and print server (FPw1 is configured like FPh1, but with only 6 drives), as much of the data storage and printing needs for the Washington operations are not shared with those in Houston. Also it would not be feasible have all file sharing and printing going across the Wide Area Network (WAN) to Houston.

The lobbyists all work on laptop computers (basic laptop configuration, see Table 1 below) that fit into docking stations when in the office; however, they are out of the office at different times of the day to meet members of Congress and always take their laptops with them. All lobbyists use smart cards to logon to their laptops, which are equipped with PCMCIA card readers.

The warehouse workers do all of their computer tasks at kiosk computers that they logon to with their smart cards. One computer can be shared by several employees, and employees can log on to various kiosks throughout the warehouse.

Computer Configurations: Both Locations

All workstations will be set up with images created for their task: e.g., workstations in the sales department will have an image for sales, while workstations in research and development will have an R&D image. This makes it easy to rollout new systems and to replace failed machines. The individual employees store their data on file servers that are backed up every night. The basic configurations of the computer in GIAC Enterprises are shown in Table 1.

All computers in GIAC Enterprises are formatted with the NT file system (NTFS). NTFS is the heart of file security, as it allows one to set permissions down to the file level. NTFS makes it possible to set permissions on almost every aspect of the operating system. NTFS also facilitates the use of file compression and the encrypted file system (EFS)

Table 1 Basic Computer Configurations

Basic Servers	• Dual processors • 2GB RAM • High-speed SCSI drives, of which two are RAID 1 (mirrored) drives for the operating system; other drives as needed are in a RAID 5 (stripe set with parity) configuration • Dual 10/100/1000 NICs w/IPsec • Redundant power supplies and fans
Basic Workstations	• Single processor • 512 MB RAM • IDE hard drive • Single 10/100 NIC • Card reader keyboard
Basic Laptops	• Single processor • 512 MB ram • IDE hard drive • Single 10/100NIC • PCMCIA card reader

Updates, Smart Fixes, and Service Packs: Both Locations

Updates and hot fixes will be tested in a test lab that is made with several machines running VMware to create virtual machines for the test environment. After being tested, the patches are installed on the servers during off-hours and will be scheduled to not overlap with the tape backup schedule that is discussed on the next page. The workstations will use the automatic update program to receive approved critical updates and hot fixes from one of GIAC Enterprises' own update servers. Other tested updates will be offered by way of group policy.

All computers will be at the latest service pack with all tested critical updates applied. Systems will also be audited with hfnetchk to make sure updates have been installed.

Security Templates

All new servers have security templates applied to them to enforce basic security. These configure the setting of such things as the password policies on the local accounts and, most importantly, can set permissions on any file or part of the registry. All of these are local policies and can be overridden with group policy; however, policies can be created and applied to different machines so that they all have the same settings. The process of using a security template entails loading it into a database, then applying the database to the computer. This ‘tattoos’ the system and can not be undone, although the setting can be changed by applying a different template. The tools used to edit and apply security templates are the security configuration and analysis snap-in and secedit.exe. The snap-in works with the Microsoft management console (MMC) and is a GUI interface to work with security templates. Secedit is a command line tool to work with the templates. Note that secedit can not be run against a remote machine: it must be run locally or from a terminal server. However, it can be called by a script run on the remote machine; this can be done to reapply a template every night to the external web server.

Security templates have been designed by many groups to harden computers that perform many different roles. Microsoft makes template such as Basic Server, Secure Server, Secure DC. Templates are also made by many other entities, such as the National Security Agency (NSA), the Center for Internet Security (CIS), and the SysAdmin, Audit, Network, Security Institute (SANS). These templates can also be edited and used to harden machines.

Antivirus: Both Locations

All of the computers also are loaded with Symantec antivirus corporate edition to prevent viruses. There is a computer in each location that is designated as a Symantec antivirus server. The master server in Houston (AVh1) gets its antivirus update from Symantec, while all computers in Houston get their updates and are monitored by the one in Houston. Since the server in Houston is designated as the master server, the secondary server (AVw1) in Washington also gets its updates from Houston, while all of the workstations in Washington connect to the server in Washington for their updates and are monitored by the one in Washington. Virus updates for the antivirus servers are downloaded every night, while workstations will check every ten minutes to see if there are updates on the server. Real-time scanning for viruses is on all the time, and a full scan is done once a week. If a new virus is discovered, the updates can be downloaded to the server manually and will be distributed to the workstations quickly. A virus sweep can be initiated from the antivirus servers at any time for all computers in the domain. Also, Symantec antivirus for mail servers is loaded on the exchange server to scan all email for viruses.

Backup: Both Locations

There are also two AIT 3 tape libraries with barcode readers. The one in Houston holds 40 tapes and has 4 drives, while the one in Washington holds 10 tapes with one drive. All backups are handled by Veritas Backupexec backup software. In Houston the drives are used in a RAID configuration to reduce the backup times (with the tape drives set in a RAID configuration data can be written to all of the drives at once, allowing for faster backups.) In both branches a full backup of all servers is done every Friday night, and differential backups are performed every week night. Every week the previous week's full backup is taken off-site. Monthly backups are kept in an off-site safe for 1 year.

Auditing: Both Locations

Auditing of the event logs will be done with the help of Microsoft Operations Manager (MOM). There will be a MOM installation at both sites.

Active Directory (AD) Design and Diagram

The GIAC Enterprise will consist of one domain: GIAC.net (see Figure 2 below). The GIAC.net name will be used for the internal network, and GIAC.com will be the name of its internet web presence. GIAC.net will consist of two sites to reduce traffic between Washington and Houston for performance reasons. The headquarters site will consist of the users and resources in the Houston area, while the branch site will consist of the users and resources in the Washington area.

There are 7 machine OUs: the Domain Controllers OU, the Servers OU and one for each type of User (R&D, Sales, etc., see Figure 2 below). There is also a Users OU and under the Users OU there will be 5 sub OU's that will control the 5 major types of employees so that group policy can be applied to the groups as described in the next sections.

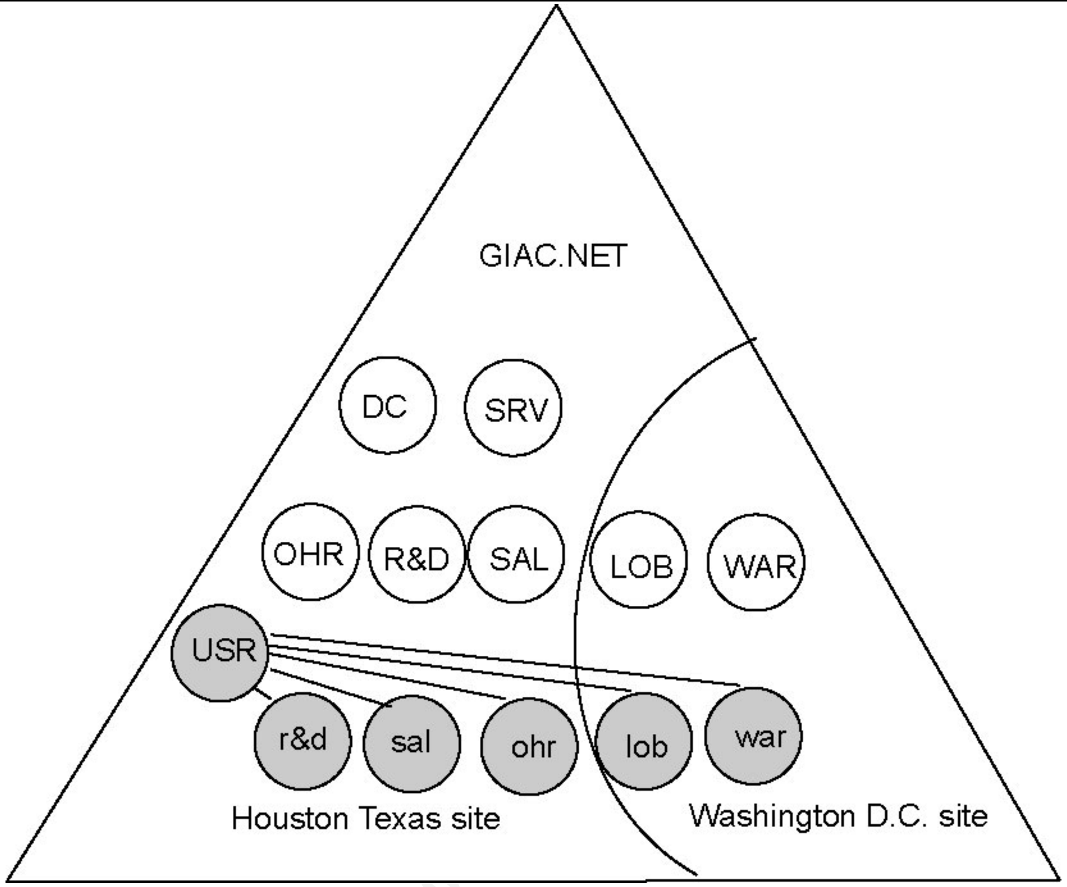

Figure 2 Diagram of Active Directory

Figure 2 Legend:

DC	Domain Controllers OU
SRV	Servers OU
OHR	Office of Human Resources OU
R&D	Research & Development OU
SAL	Sales OU
LOB	Lobbyists OU
WAR	Warehouse OU
USR	Users OU
r&d	research & development users OU
sal	sales users OU
ohr	office of human resources users OU
lob	lobbyists users OU
war	warehouse users OU

All white circles indicate OUs containing machines: grey circles represent OUs containing users. All OUs are at the same hierarchy unless connected by lines to show sub OUs (i.e., the only sub-OUs are those under the Users OU).

Domain

The placement of Flexible Single-Master (FSMO) roles follows the guidelines from Microsoft ("FSMO Placement and Optimization"). Because of the single domain model implemented at GIAC Enterprises, deciding the placement of the roles is simplified. DCh1 will be the PDC emulator, RID master, and Infrastructure master, while DCh2 will be the Schema master and Domain master. By only using one domain, placement of the global catalog is not critical, since all of the active directory is replicated between all DCs. This also greatly simplifies trust relationships as all users are all in the same domain and can be controlled with group policy and NTFS permissions.

For the internal domain, all DNS is handled by all of the domain controllers, which are all running an AD integrated DNS. Also, all network configuration for the workstations will be done with DHCP; this allows for easy management and organization of IP addresses and network configurations.

In the domain, we use Public Key Infrastructure (PKI). GIAC Enterprises employs an off-line root Certificate Authority, and the domain controllers are Issuing Certificate Authorities. Parts of the domain use smartcards for authentication: smartcards are physical devices that hold individual's private keys. PKI also allows the use of IPsec VPNs, an encrypted file system, and secure e-mail.

Sites

Two sites mimic the physical locations of the offices. There are two DCs in Houston and one in Washington: all active directory replication is handled by the Knowledge Consistency Checker (KCC). Placing a domain controller in each site reduces traffic between sites because all authentication occurs in the local site. With Windows2000 replication can occur reliably at relatively low data transfer rates, but to make sure that replication traffic does not interfere with user traffic replication can be set to occur only in the off-peak hours. Fossen states that the RPC replication of AD is much improved over NT4: "AD replication over slow links works quite well" (Fossen, Track 5 - Securing Windows, 5.1 Windows2000/XP Active Directory, p.88). Fossen then gives examples with rates of 19.2 Kbs and 250Kbs as being stable and notes even the ability to do replication over 9600 bps connections (p. 88).

Organizational Units (OUs)

There are two main types of OUs in GIAC.net: the machine OUs and the user OUs.

Machine OUs

The machine OUs include the Domain Controllers OU and the Servers OU, along with OUs for the *computer accounts* of each type of worker (such as research and development, sales, lobbyist, etc.).

The Domain Controllers OU is used to configure all of the domain controllers; it is created by default when the active directory is made. Group policy applied to the Domain Controllers OU is discussed in the Basic Group Policy section.

The Servers OU is for the servers, such as the antivirus servers and file and print servers. This controls settings that need to be more strict than that of the regular users' computers, like restricting who can logon locally so that only the users with administrative purposes can logon.

The other machine OUs (Research & Development; Sales; Human Resources, etc.) are used to configure the different machine types. Using Remote Installation Services, images and programs that are needed by the R&D teams can be assigned to the computers of the R&D OU using Group Policy Objects (GPOs), while images and programs that are needed by the Sales teams can be assigned to the computers of the Sales OU. Also GPOs can be used to prevent users from other groups such as Sales from being able to log in to the Human Resources machines. Some examples will be given later in the section Selected Additional Group Policies.

In the Warehouse OU (*not* the warehouse users OU), both machine properties and a mandatory set of user policies will be set on the kiosk machines using a technique called loopback processing of group policy. In this way, whenever someone logs on the user's environment will be the same, with a more restricted user interface.

User OUs

The user OUs include a general user OU (GIAC Users), with sub OUs for the *user accounts* of each type of users. The GIAC Users OU also has security groups defined that are used for such things as allowing access for users to certain computers. The process will be discussed a little later.

In the user OUs, GPOs can also be used to modify the user environment, from such things as adding items to the desktop or favorites, to redirecting folders to locations on the network.

Security Groups

All users will be added to security groups that will be given permissions to logon to various computers. Some examples of general ones will be listed here with a brief description of their main use.

- HR users: are all of the normal users that logon to the machines in the office of human resources OU. They will be given logon rights through group policy, and in this way only human resources people can logon to the computers in the human resources department
- HR computer administrators: these would be users that would add new computers to the OHR OU.

- HR user administrators: are users that are to be given the right to add new users when they are hired to work for GIAC Enterprises. The group is delegated the add user right in the various users OUs.
- HR user maintenance: contains users that are to be given the right to edit some of the user information in Active Directory, including such things as phone numbers and addresses.
- Sales users: works the same way for the sales department as the HR users group works for human resources.
- Sales computer administrators: these would be users that would add new computers to the Sales OU.

There would also be similar groups made for all of the other departments. In addition, a restricted users group would be created and through group policy be denied access to logon to any of the computers; it would contain accounts such as guest, or anyone that was to be terminated, or other sensitive accounts that should not be allowed to logon to the computers in GIAC Enterprises.

Security Templates

Security templates discussed earlier can also be imported into GPOs to configure many computers with the same template. This is the easiest way to configure Access Control Lists (ACLs) on a large number of sensitive files and registry settings in a uniform and timely manner.

Group Policy and Security

Basic Group Policy

In this section I will discuss specific group policy settings for the Default Domain Policy that is applied to the whole domain, and for the Default Domain Controller Policy that is applied to the Domain Controllers OU.

Default Domain Policy

The Default Domain Policy GPO is used for general domain-wide policies. The Default Domain Policy is primarily for setting up the account policies such as policies that pertain to password enforcement, length, complexity, and lockout information. The account policies are only set at the Default Domain policy level and cannot be overridden at a lower level OU.

A quick discussion about password practices at GIAC Enterprises: although complex passwords are good, the length of the password is probably the best way to ensure password integrity. There will be a continuing emphasis on how employees choose a password, i.e., pass phrases are a good way to make long, complex passwords that are easy to remember. Also, all administrators will be given two accounts: one that has administrator rights set high enough for them to do their administrative tasks, and a second for email, browsing the web, etc. This will help reduce the risk of a virus being initiated under an administrator's rights. The auditing tool L0phtCrack will be used on a regular basis to see if a basic level of password strength is maintained.

(For the GPOs listed below, the solid bulleted items are the policy and the setting and are taken directly from the Windows2000 group policy; the open bulleted ones in italics are the reasons that they were configured. This section does not include all settings that are available.)

Windows Settings: Security Settings: Account Policies: Password Policy

- Enforce password history 24 passwords remembered
  - *This is set to 24 which increases security because no one can just recycle a couple of passwords. In this way people will have to make more unique passwords and it should make it less likely that the user will be able to use the same couple of passwords that they use for other things such as web sites.*
- Maximum password age 90 days
  - *This requires passwords to be changed once a quarter. This is important because the password should change by the time someone would be able to crack it.*
- Minimum password age 1 days
  - *This makes it very unlikely that someone could cycle through 24 passwords so that they could always use the same one.*

- Minimum password length 8 characters
  - *Passwords longer than 14 characters are desirable in that the results of a cracked lanman will result in the wrong password. However, with at least 8 characters and complexity filters, passwords can be slow to crack. Password selection education will be used to educate employees on the importance of selecting a good password with emphasis on using techniques such as a passphrase to make long and complex passwords .*
- Passwords must meet complexity requirements Enabled
  - *Requires password to contain characters from 3 of the 4 groups (uppercase, lowercase, numeric, and non alpha-numeric.) This helps to create passwords that are not as vulnerable to a dictionary attack.*
- Store password using reversible encryption for all users in the domain Disabled
  - *We will not have anything that needs reversible encryption, so this is disabled.*

Windows Settings: Security Settings: Account Policies: Account Lockout Policy

- Account lockout threshold 5 invalid logon attempts
  - *This prevents a script from going through a dictionary of passwords trying to crack passwords.*
- Reset account lockout counter after 10 minutes
  - *This says that making the 5 invalid attempts in a 10 minute time frame locks the account.*
- Account lockout duration 15 minutes
  - *To reduce calls to the help desk, the lockout duration is set to 15 minutes. This means that 15 minutes after the last invalid logon attempt the lockout will be removed. This time period gives the employee time to take a break and see if they can remember the password, and then they can try it again after 15 minutes. This is sufficient to thwart dictionary attacks because such attacks could only test up to 20 passwords an hour.*

Windows Settings: Security Settings: Account Policies: Kerberos Policy

The default setting for Kerberos should be fine in the GIAC.net environment

- Enforce user logon restrictions Enabled
- Maximum lifetime for service ticket 600 minutes
- Maximum lifetime for user ticket 10 hours

- Maximum lifetime for user ticket renewal 7 days
- Maximum tolerance for computer clock synchronization 5 minutes

Windows Settings: Security Settings: Local Policy: Security options

- Automatically log off users when logon time expires Disabled
    - *There will not be time restrictions on when users can work.*
- Smart card removal behavior Lock Workstation
    - *Smartcards will be used in some locations, and this sets the default behavior when they are removed.*
- Accounts: Rename administrator account newname
    - *The administrator account should be renamed to something that is not a common name for an administrator, as 'root' or 'sa' is; it could be a name in the same format as a common user. It is also possible to lock the administrator account from invalid network logon attempts as discussed in the section Additional Security Settings.*
- Accounts: Rename guest account Not defined
    - *We did not define a new name, but 'guest' should be disabled and a long password (~30 characters) should assigned to prevent its use if it was enabled. The main window for resetting the password holds 56 characters, but it is possible to enter passwords of up to 127 characters (Fossen, Track 5 – Securing Windows, 5.2 Windows 2000/XP Group Policy and DNS, p. 82).*

Domain Controller Policy

In this section the domain controller policy is detailed and additional settings are described for securing the domain controllers. First, however, a few comments on the physical security of the servers: all servers are in a locked room with all keys numbered and tracked. The boot order has been set in the BIOS to boot from the hard drive first. This helps in two ways: it makes it harder for some one to reboot the system and boot from a floppy or CD; second, and more likely, if a disk was inadvertently left in the drive and the computer is restarted for service it would not hang because it could not find a boot disk. The items detailed in this section implement additional settings and further secure the domain controllers.

(For the GPOs listed below, the solid bulleted items are the policy and the setting; the open bulleted ones in italics are the reasons that they were configured. This section does not include all settings that are available.)

Windows Settings: Security Settings: Account Policies

The account policies can only be set at the default domain policy level so they are not configured in the Domain Controller Policy. And if different account policies are necessary, that in and of itself would be a reason to create a new domain.

Windows Settings: Security Settings: Local Policy: Audit Policy

- Audit account logon events Success, Failure
  - *Auditing for Failure can show if someone is trying to guess a password, but without auditing for Success you can't see if they were able to guess the correct one (this is related to Kerberos authentication).*
- Audit account management Success, Failure
  - *This is useful to track accounts and to monitor if someone is moved into a new group, or tries to move themself into a new group or create new users.*
- Audit logon events Success, Failure
  - *Auditing for Failure can show if someone is trying to guess a password, but without auditing for Success you can't see if they were able to guess the correct one.*
- Audit object access Failure
  - *There is not much need to measure Success because most normal activity results in successful access.*
- Audit policy change Success, Failure
  - *Shows when policies are changed and can aid in trouble-shooting if a change causes something not to work.*

- Audit privilege use Failure
- Audit system events Success, Failure

Windows Settings: Security Settings: Local Policy: User Rights Assignments

In this section, the GPOs restrict the listed user groups' access to the different rights that can be exercised on the domain controllers. In many cases this removes ones that were there by default. In some cases, None indicates that all user groups are removed. Note that in this sub-section only, italics also indicate the groups.

- Access this computer from the network *Users,Administrators*
  - *This allows only these two groups to access the domain controller from the network.*
- Act as part of the operating system *MOM@GIAC.net*
  - *The Microsoft Operations Manager (MOM) requires an account that runs as part of the operating system.*
- Add workstations to domain *Administrators,Account Operators*
- Adjust memory quotas for a process *Administrators*
- Allow logon through Terminal Services *Administrators*
- Back up files and directories *Administrators,Server Operators,Backup Operators*
- Bypass traverse checking *Everyone*
- Change the system time *Administrators,Server Operators*
- Create a pagefile *Administrators*
- Create a token object *MOM@GIAC.net*
- Create permanent shared objects *None*
- Debug programs *Administrators*
- Deny access to this computer from the network *Restricted Users*
- Deny logon as a batch job *None*
- Deny logon as a service *None*
- Deny logon locally *Restricted Users*
  - *The deny logon GPOs take precedence over the logon (see below), so if a user is a member of more than one group and one group is denied logon, the user cannot logon.*

- Deny logon through Terminal Services *Restricted Users*
    - *The restricted users group was created so someone could be denied all access by their account being added to the group: and these few setting immediately above will not allow them to logon locally, from the network or through terminal services*
- Enable computer and user accounts to be trusted for delegation *Administrators*
- Force shutdown from a remote system *Administrators,Server Operators*
- Generate security audits *None*
- Increase scheduling priority *Administrators*
- Load and unload device drivers *Administrators*
- Lock pages in memory *None*
- Log on as a batch job *MOM@GIAC.net,SYSTEM,backupexec@GIAC.net*
- Log on as a service *MOM@GIAC.net, ,Databaseadmin@giac.net*
- Log on locally *Server Operators,Print Operators, TsInternetUser@GIAC.net,Backup Operators,Administrators,Account Operators*
    - *This keeps regular users from being able to logon locally to the domain controllers, although users should not have physical access to the domain controllers anyway.*
- Manage auditing and security log *Administrators*
- Modify firmware environment values *Administrators*
- Profile single process *Administrators*
- Profile system performance *Administrators*
- Remove computer from docking station *Administrators*
- Replace a process level token *None*
- Restore files and directories *Administrators,Server Operators,Backup Operators*
- Shut down the system *Server Operators,Print Operators,Backup Operators,Administrators,Account Operators*
- Synchronize directory service data *None*
- Take ownership of files or other objects *Administrators*

Windows Settings: Security Settings: Local Policy: Security Options

- Audit: Shut down system immediately if unable to log security audits Disabled
    - *In the case of GIAC Enterprises this was disabled because a denial of service attack could occur by someone intentionally filling the logs. Also we use large log file sizes so it would be harder for someone to hide their activity by cycling the log, i.e., filling the log until it overwrites any unauthorized activity that they were doing.*
- Devices: Prevent users from installing printer drivers Enabled
    - *In this way no printers will be added except by an administrator. However, only administrators will be able to log on to the servers directly, as set forth earlier in the User Rights Assignments section of the GPO.*
- Devices: Restrict CD-ROM access to locally logged-on user only Enabled
- Devices: Restrict floppy access to locally logged-on user only Enabled
    - *The above two GPOs, Restrict CD-Rom and Restrict floppy use, make it so no one can connect to them across the network.*
- Devices: Unsigned driver installation behavior Warn but allow installation
    - *Since some software used may not be signed, the setting of 'Warn but allow installation' will allow administrators to load drivers that they have tested.*
- Domain controller: Refuse machine account password changes Disabled
    - *The machine account password should be changed on a regular basis.*
- Domain member: Maximum machine account password age 30 days
    - *Causes all machines to create new account password. Since machines are like users and have accounts in Windows 2000, a cracked machine password could also be a security risk.*
- Domain member: Require strong (Windows 2000 or later) session key Enabled
- Interactive logon: Do not display last user name Not defined

- Interactive logon: Do not require CTRL+ALT+DEL Disabled
    - *It is important that the stop command like this is used so that someone cannot be running a program that looks like a logon screen to capture passwords.*
- Interactive logon: Message text for users attempting to log on

  This system is for the use of GIAC Ent. authorized users only. Individuals using this computer system with authority, without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
    - *This is a message that comes from CERT Advisory CA-1992-19 (as quoted by Witter) and suits the needs of GIAC Enterprises.*
- Interactive logon: Message title for users attempting to log on
  Warning: This is a monitored computer system!
- Interactive logon: Number of previous logons to cache (in case domain controller is not available) 0
    - *Although not used for domain controllers, this is set for the case of a machine that is added to the Domain Controllers OU but has not been promoted to a DC yet.*
- Interactive logon: Prompt user to change password before expiration 7 days
- Interactive logon: Require Domain Controller authentication to unlock workstation Not defined
- Interactive logon: Smart card removal behavior Not defined
- Microsoft network client: Digitally sign communications (always) Not defined
- Microsoft network client: Digitally sign communications (if server agrees) Not defined
- Microsoft network client: Send unencrypted password to third-party SMB servers Disabled
    - *Password should never be sent unencrypted.*

- Microsoft network server: Amount of idle time required before suspending session 15 minutes
- Microsoft network server: Digitally sign communications (always) Not defined
- Microsoft network server: Digitally sign communications (if client agrees) Not defined
- Microsoft network server: Disconnect clients when logon hours expire Not defined
- Network access: Allow anonymous SID/Name translation Not defined
- Network access: Do not allow anonymous enumeration of SAM accounts Not defined
- Network access: Do not allow anonymous enumeration of SAM accounts and shares Enabled
    - *This prevents NULL users from getting a list of usernames or shares, including hidden shares.*
- Network access: Do not allow storage of credentials or .NET Passports for network authentication Not defined
- Network security: Do not store LAN Manager hash value on next password change Not defined
- Network security: LAN Manager authentication level Send NTLMv2 response only\refuse LM
    - *This prevents the LM hash values from being captured in transit by a network sniffer by refusing LM for authentication and forces the use of the more secure NTLMv2. NTLMv2 is also better than the older NTLMv1 in that it salts encryption with a random number.*
- Recovery console: Allow automatic administrative logon Disabled
- Recovery console: Allow floppy copy and access to all drives and all folders Disabled
    - *The previous two items make sure that administrators have to use the recovery console password if they boot into the recovery mode, and limits the access that they can use if in the recovery console.*
- Shutdown: Allow system to be shut down without having to log on Disabled
    - *This would prevent someone who cannot log on to the server from shutting down the server. (The physical security of the system should prevent this also.)*

- Shutdown: Clear virtual memory pagefile Not defined
- System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) Enabled

Windows Settings: Security Settings: Event log

- Maximum application log size 51200 kilobytes
- Maximum security log size 51200 kilobytes
- Maximum system log size 51200 kilobytes
    - *Using a large log size makes sure that all events are recorded, and later in this section the retention method is set to overwrite as needed, which keeps the most recent events in the log. Due to the size the log should contain at least one day of logs. Since there is a tape backup every night, all logs should be able to be reconstructed.*
- Prevent local guests group from accessing application log Enabled
- Prevent local guests group from accessing security log Enabled
- Prevent local guests group from accessing system log Enabled
    - *These three settings explicitly prevent guest group from accessing any of the logs.*
- Retain application log Not defined
- Retain security log Not defined
- Retain system log Not defined
- Retention method for application log As needed
- Retention method for security log As needed
- Retention method for system log As needed

Selected Additional Group Policies

In this section I will discuses some additional settings that are configured in some of the other group policies. In the Lobbyist Group Policy section I will detail how the laptops will be additionally configured for security. In the Warehouse Group Policy section I will discuss some of the GPOs specific to computer settings, as well as some of those specific to users.

Group policies are independent from the OUs to which they are applied so there will be some group policies that are applied to multiple OUs. The local settings on the servers are basically like those of the domain controllers, so a server local Policy would be made and applied to the Servers OU. In most cases the OUs for the different machine groups are similar so they can all share the same policy for those parts, and then a more specific policy one can be created for each OU that has just the things needed for that OU.

General Machine Group Policies

This group policy has the user part disabled so it just has settings for the machines and is applied to all of the machine OUs such as R&D, Sales, etc. It sets most of the security settings for the machines.

(For the GPOs listed below, the solid bulleted items are the policy and the setting; the open bulleted ones in italics are the reasons that they were configured. This section does not include all settings that are available.)

Windows Settings: Security Settings: Local Policy: Audit Policy

• Audit account logon events	Success, Failure
• Audit account management	Success, Failure
• Audit logon events	Success, Failure
• Audit object access	Failure
• Audit policy change	Success, Failure
• Audit privilege use	Failure
• Audit process tracking	Not defined
• Audit system events	Success, Failure

Windows Settings: Security Settings: Local Policy: User Rights Assignments

The user rights settings here help protect the systems from network-born attacks.

• Access this computer from the network	Administrators
• Force shutdown from a remote system	Administrators
• Take ownership of files or other objects	Administrators

- Deny access to this computer from the network *Restricted Users*
- Deny logon locally *Restricted Users*
  - *The deny logon GPOs take precedence over the logon (see below), so if a user is a member of more than one group and one group is denied logon, the user cannot logon. The restricted users group was created so someone could be denied all access by just adding their account to the group, and these few settings immediately above will not allow them to logon locally or from the network.*

Windows Settings: Security Settings: Local Policy: Security Options

- Accounts: Rename administrator account Not defined
  - *This is already defined in the Default Domain policy*
- Accounts: Rename guest account Not defined
  - *A new name is not defined, but guest should be disabled and a long password (~30 characters) should be assigned to prevent its use if it was enabled.*
- Audit: Shut down system immediately if unable to log security audits Not defined
  - *In the case of GIAC Enterprises this was not defined because a denial of service attack could occur by someone intentionally filling the logs. Also we use large log file sizes so it would be harder for someone to hide their activity by cycling the log, i.e., filling the log until it overwrites any unauthorized activity that they were doing.*
- Devices: Prevent users from installing printer drivers Disabled
  - *Users will need to be able to add printers in particular if they need to connect to someone else's printer while out of the office. This is enabled for the domain controllers and servers where adding un-tested printers could be a risk.*
- Devices: Restrict CD-ROM access to locally logged-on user only Enabled
- Devices: Restrict floppy access to locally logged-on user only Enabled
  - *The Restrict CD-Rom and Restrict floppy use makes it so no one can connect to them across the network. This is still a safe thing to do for all of the computers.*

- Devices: Unsigned driver installation behavior
  Warn but allow installation
  - *Since some software used may not be signed, the setting of 'Warn but allow installation' will allow administrators to load drivers that they have tested.*
- Domain member: Maximum machine account password age
  30 days
  - *Causes all machines to create new account passwords. Since machines are like users and have accounts in Windows 2000, a cracked machine password could also be a security risk.*
- Domain member: Require strong (Windows 2000 or later) session key
  Enabled
- Interactive logon: Do not display last user name Enabled
  - *The username will not be seen by the next person to use the computer, which makes it harder to start guessing a username and password combination.*
- Interactive logon: Do not require CTRL+ALT+DEL Disabled
  - *It is important that a stop command like this is used so that someone cannot be running a program that looks like a logon screen to capture passwords.*
- Interactive logon: Message text for users attempting to log on

  This system is for the use of GIAC Ent. authorized users only. Individuals using this computer system with authority, without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
  - *This is a message that comes from CERT Advisory CA-1992-19 (as quoted by Witter) and suits the needs of GIAC Enterprises.*
- Interactive logon: Message title for users attempting to log on
  Warning: This is a monitored computer system!

- Interactive logon: Number of previous logons to cache (in case domain controller is not available) 1
    - *While away from the office it is important to have the ability to logon to the system using the cached domain account.*
- Interactive logon: Prompt user to change password before expiration 7 days
- Interactive logon: Smart card removal behavior Lock System
    - *When the user pulls the smartcard from the machine, the system will lock on a laptop used by one person; this is the most convenient.*
- Microsoft network client: Send unencrypted password to third-party SMB servers Disabled
    - *Passwords should never be sent unencrypted.*
- Network access: Allow anonymous SID/Name translation Disabled
    - If enabled this could allow someone to find the name of well known SIDs such as that of the administrator, even if the name was changed.
- Network access: Do not allow anonymous enumeration of SAM accounts and shares Enabled
    - *This prevents NUL users from getting a list of usernames or shares, including hidden shares. This can be a problem for some older programs, such as older versions of Veritas Backup Exec. It may be necessary to move down to not allowing anonymous access only to the SAM accounts if a new software that is needed uses NUL users to find shares.*
- Network security: Do not store LAN Manager hash value on next password change Enabled
    - *The LM hash is easier to crack. If someone could extract the SAM database, the presence of the LM hash requires only the crack of two 7 digit passwords.*
- Network security: LAN Manager authentication level Send NTLMv2 response only\refuse LM
    - *This prevents the LM hash values from being captured in transit by a network sniffer by refusing LM for authentication and forces the use of the more secure NTLMv2. NTLMv2 is also better than the older NTLMv1 in that it salts encryption with a random number.*
- Recovery console: Allow automatic administrative logon Disabled

- Recovery console: Allow floppy copy and access to all drives and all folders Disabled
  - *The previous two items make sure that administrators have to use the recovery console password if they boot in to the recovery mode, and limits the access that they can use if in the recovery console.*
- Shutdown: Allow system to be shut down without having to log on Enabled
  - *It is not as critical if a users computers is rebooted (compared to a domain controller or server).*
- Shutdown: Clear virtual memory pagefile Enabled
  - *The virtual memory page file could be analyzed and unencrypted data could be extracted.*
- System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) Enabled

Windows Settings: Security Settings: Event log

- Maximum application log size 5120 kilobytes
- Maximum security log size 5120 kilobytes
- Maximum system log size 5120 kilobytes
  - *Logs should be kept so that they can be queried in the event of problems.*
- Prevent local guests group from accessing application log Enabled
- Prevent local guests group from accessing security log Enabled
- Prevent local guests group from accessing system log Enabled
  - *These three settings explicitly prevent guest group from accessing any of the logs*.
- Retain application log Not defined
- Retain security log Not defined
- Retain system log Not defined
- Retention method for application log As needed
- Retention method for security log As needed
- Retention method for system log As needed

Windows Settings: Security Settings: System Services

Here are the settings for the Systems Services node of the group policy, which facilitates the disabling of services for all of the machines to which the GPO is applied. All services of the machines can be controlled through the System

Services node; however, the list below (Bower et al., p. 62) is a partial list to show the ones that will be disabled.

- Alerter Disabled
- ClipBook Disabled
  - *The ClipBook service is used to transfer clipboard information to a remote computer. The service runs under a higher privilege so it could be vulnerable to exploit, and the ability to have remote access to the clipboard on these machines is not necessary*
- Distributed File System Disabled
- Messenger Disabled
  - *The messenger service lets messages be sent and received; this is not necessary for the function of these machines and has been abused in the past for advertising.*
- NetMeeting Remote Desktop Sharing Disabled
  - *This can allow remote access to the desktop as if logged on locally. This feature is not needed in the GIAC environment and could pose a security risk.*
- Network DDE Disabled
- Network DDE DSDM Disabled
- Print Spooler Disabled
  - *The print spooler is only necessary if the computer were going to share a printer with others.*
- Remote Registry Service Disabled
  - *This could allow others to edit the registry from a remote location.*
- Routing and Remote Access Disabled
  - *Routing and Remote Access services necessary only if someone needs to dial in to this machine and create a VPN; disabling this GPO does not prevent the user of the machine from creating a VPN to another machine.*
- RunAs Service Disabled
- SNMP Service Disabled
- SNMP Trap Service Disabled
  - *The two Simple Network Management Protocol services can release a lot of information about the machine.*
- TCP/IP NetBIOS Helper Service Disabled
  - *Not needed in a native mode domain.*

- Telnet Disabled
  - *Telnet allows a remote connection to the computer but is not encrypted and so is a security risk.*
- World Wide Web Publishing Service Disabled
  - *GIAC has no need for the laptops to run a web server, so this will make sure it is off.*

General User Group Policies

This group policy has the machine portion disabled, so it just has settings for the users and is applied to all of the user OUs such as R&D, Sales, etc. It sets most of the security settings for the machines and can also be used to configure the user interface, which includes such items as company websites, Internet Explorer proxy settings, desktop settings, and a password-protected screen saver that should be set to start after ten minutes). Almost any thing related to the windows user interface can be configured in these group policies. The main security-related item that we will set is folder redirection. Two GPOs will be created, one for Houston and one for Washington: each will configure folder redirection to the file server in their own location. The Houston user group policy can be applied to the users sub-OUs that are based in Houston (sales, research & development, and office of human resources), and the Washington users group policy can be applied to the users sub-OUs that are based in Washington (lobbyist & warehouse).

User Settings: Windows Settings: Folder Redirection

In the user settings part of each group policy, the Application Data and My Documents should be redirected to network shares on the file and print server. This allows for a quick logon since the data is not stored in a roaming profile that has to be loaded, and the data is accessible at whichever computer that the user goes to. This also puts the data on the file server so it is backed up. If something happens to a computer, the computer can be replaced and the data is still available. If a file is lost, it can be retrieved from a tape backup.

Group Policy for the Lobbyist OU

First, however, a few comments about other security used for the lobbyists' laptops: all users will logon to their systems using smartcards. This makes authentication a two-step authentication: since the user employs a physical object (smartcard) and a piece of knowledge (password), the logon is much more secure. Without the smartcard, knowledge of the password is of no use; likewise, a smartcard without a password provides no access. The smart card doubles as the employee ID and key to the Washington office. The laptops will also use the Encrypted File System (EFS) for storing data on the laptops. Each user is also given a security cable and instructed on its use.

This section uses some of the GPO settings to show specific ways that group policy can further secure the computers of the lobbyists. Local Policies are be configured in the same manner as described in the last section (General Machine Group Policies), so now only ones specifically needed for the laptop users in the lobbyists' OU are detailed.

(For the GPOs listed below, the solid bulleted items are the policy and the setting; the open bulleted ones in italics are the reasons that they were configured. This section does not include all settings that are available.)

Windows Settings: Security Settings: Local Policy:

All of these are set in the General Machine Group Policies and do not need to be changed.

Windows Settings: Security Settings: Event log

All of these are also set in the General Machine Group Policies and do not need to be changed.

Windows Settings: Security Settings: Restricted Groups

- Administrators and Power Users Added
    - *These groups are added to Restricted Groups and set to only contain the proper groups ("How to Restrict Group Membership"). The Administrators group contains the domain and local Washington administrators, and Power Users can be set to None to ensure that no one is added to that group. This will reset the users with access to these groups every time the GPO is re-applied. Setting up restricted groups in this way makes it possible to add a group of users as laptop administrators to each machine, through group policy, without going to every machine. This also would remove anyone who was able to get elevated privileges from the restricted groups. For the administrators in the lobbyist OU, the lobbyist administrators group can be added which will allow the designated users to administer the machine. None of the users needs the elevated privileges of Power User, so the restriction will also keep that group empty.*

Windows Settings: Security Settings: System Services

All of these are also set in the General Machine Group Policies and do not need to be changed.

Warehouse Group Policy

The warehouse workers have a different working environment. They use machines that are located around the warehouse; they insert their smartcard to logon. All of their personal files are automatically redirected to network storage. The kiosk does not store their profiles locally since many different people may logon to the same machine. The smartcard is set to log them off when removed so that the next person can connect.

Only some of the settings will be discussed in this section to show specific ways that group policy can further secure the computers of the warehouse OU. Local Policies could be configured in the same manner as described in the last sections; only ones specifically needed for the warehouse users in the warehouse OU are detailed. In particular, some GPOs that affect the desktop environment will be discussed in this section.

First the general machine group policy is applied, then the warehouse group policy. By doing it in this way the warehouse group policy will further modify the policies from the default domain and general machine policies. The warehouse policies apply machine policies to the computers as well as the user portion of group policy using a process called loopback processing. This allows the macine to first load the machine policy as usual then to act as a user and load a user policy.

(For the GPOs listed below (most of which are specific to computer settings, although some are specific to users), the solid bulleted items are the policy and the setting; the open bulleted ones in italics are the reasons that they were configured. This section does not include all settings that are available.)

Windows Settings: Security Settings: Local Policy: Audit Policy

Auditing can be configured in the same way as in the lobbyist policy detailed in the audit policy settings of the general machine group policy section.

Windows Settings: Security Settings: Local Policy: User Rights Assignments

User rights can be configured in the same way as in the lobbyist policy detailed in the user rights policy settings of the general machine group policy section.

Windows Settings: Security Settings: Local Policy:

Most of these are set in the General Machine Group Policies and do not need to be changed.

Windows Settings: Security Settings: Local Policy: Security Options

- Devices: Prevent users from installing printer drivers Enabled
    - *The users will use a mandatory profile in which the printers are pre-configured so the end user does not need to add printers.*
- Interactive logon: Number of previous logons to cache (in case domain controller is not available) 0
    - *Because warehouse workers use smart cards to logon, and because several users share a kiosk, there is no reason to cache the logons.*
- Interactive logon: Smart card removal behavior Logoff System
    - *When the user pulls the smartcard from the machine, the system will log off. The users have their smartcard attached to their body on a retractable cable or lanyard. Then the card is inserted into*

the computer and the PIN is entered; they are then logged on to a mandatory profile. When they are ready to move on, they simply remove the smartcard: the computer logs off and is ready for the next user.

Windows Settings: Security Settings: Event log

All of these are also set in the General Machine Group Policies and do not need to be changed

Windows Settings: Security Settings: Restricted Groups

- Administrators and Power Users Added
    - *These groups are added to Restricted Groups and set to only contain the proper groups ("How to Restrict Group Membership"). The Administrators group contains the domain and local Washington administrators, and Power Users can be set to 'none' to ensure that no one is added to that group. This will reset the users with access to these groups every time the GPO is re-applied. Setting up restricted groups in this way makes it possible to add a group of users as laptop administrators to each machine through group policy without going to every machine. This also would remove anyone who was able to get elevated privileges from the restricted groups. In here the warehouse administrators are added to the administrators group. None of the users needs the elevated privileges of Power User, so the restriction will also keep that group empty.*

Windows Settings: Security Settings: System Services

All of these are also set in the General Machine Group Policies and do not need to be changed.

Administrative Templates: System: Group Policy

- User Group Policy loopback processing mode Merge
    - *This is the very important tool for securing the kiosk workstation; it allows the computer the computer to run a user GPO. In merge mode the user's own GPO settings are merged with those in the loopback GPO. If there are conflicting settings, the loopback setting are always used. Another option would be to use the replace setting, in that case the only user setting would be the one in the loop back GPO.*

User Settings: Windows Settings: Folder Redirection

In the user settings part of the group policy applied to the warehouse users OU, the Application Data and My Documents should be redirected to network shares on the file and print server in Washington. This allows for a quick logon since the data is not stored in a roaming profile that has to be loaded, and the data is accessible at whichever kiosk that the user goes to.

In the loopback portion on user settings, other things can be set which become mandatory sittings on all of the kiosk computers.

User Settings: Administrative Templates: Start Menu and Task Bars

• Remove Run menu from Start Menu	Enabled
• Remove Logoff on the Start Menu	Enabled
• Remove and prevent access to the Shut Down command	Enabled
• Prevent changes to Taskbar and Start Menu Settings	Enabled
• Remove and disable the Turn Off Computer button	Enabled

User Settings: Administrative Templates: Control Panel

• Prohibit access to the Control Panel	Enabled

Additional Security

A few other things that can be done to increase the security of the servers or the enterprise as a whole will be discussed now.

- It is particularly important to **disable all services** that are not needed for a system to do its job. All of the servers will have only the services that are needed to do their specific tasks; in many cases this is done by setting local policy with security templates customized for the individual type of server. For other computers the same thing can be done with group policy, which makes disabling unnecessary services easier to do on many computers simultaneously.
- The administrator account can not be locked out in Windows 2000, so it is possible to attempt to guess the password an unlimited number of times. **The administrator account can be locked with passprop.exe**, a program that can be found on the NT4 resource kit, as illustrated in (Shawgo p. 32-33). Passprop.exe only locks the account as seen from the network: an administrator can still logon locally. This is most useful for the local administrator account, which does not need to be used for logon in a domain environment. However it is also useful for the domain administrator account, as the users with administrator rights should use an account that has been given only the rights needed to do their administrative jobs, while they should use a second regular user account for things like checking email and other non-administrative tasks. The actual administrator account should only need to be used occasionally.
- **Regular training on password practices at GIAC enterprises will be implemented**. Although complex passwords are good, the length of password is probably the best way to ensure password integrity. There will be a continuing emphasis on how employees choose a password; for example, using passphrases is a good way to make long complex passwords that are easy to remember.
- **Training on the use of smartcards is also important**. Users must always have their smart card with them and they must be trained to remove the card whenever they leave a machine. This is particularly important for laptop users where the temptation to leave the card in the system could give a card to someone who steals a computer. But as the card is also used for the employee ID and entry into the building, it is not as likely to be left behind.
- For Windows2000 Professional, the local administrator is the default Encrypted File System (EFS) recovery agent. Removing the local administrator from the role of EFS recovery agent and **adding a domain administrator as an EFS recovery agent** prevents encrypted data on a stolen laptop from being accessed in the event that the local

administrator password is cracked. **Laptop users also are trained in the use of EFS for corporate data**.

- Physical security includes **a locked server room with access control**. The servers are also under video surveillance with motion detection. This keeps a record of anyone using the servers.
- There are written **Disaster Recovery Plans** so administrators on duty will know exactly what to do in the case of a failure. These plans also specify who to call and where backup media is stored. The disaster recovery plan also describes the physical security of backup media, which includes such things as how media will be secured while on-site and when media will be taken to an off-site secure location.
- **Background checks should be done when hiring employees in sensitive positions**. Some employees such as administrators in the organization can have access to sensitive data; therefore it is important to perform background checks before these people are hired. The check can find prospective employees with questionable backgrounds, and can act as a deterrent to having unscrupulous people apply in the first place.

References

Bower, Ben; Dean Farrington; and Chris Weber. Securing Windows2000 Professional: Using the Gold Standard Security Template, Version 1.5. SANS Institute, 2002.

Fossen, Jason. Track 5 - Securing Windows, 5.1 Windows2000/XP Active Directory. SANS Institute, 2002.

Fossen, Jason. Track 5 - Securing Windows, 5.2 Windows2000/XP Group Policy and DNS. SANS Institute, 2002.

"FSMO Placement and Optimization on Windows 2000 Domain Controllers: Microsoft Knowledge Base Article 223346." Microsoft TechNet. 20 December 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B223346 (27 March 2003).

"How to Restrict Group Membership By Using Group Policy in Windows 2000: Microsoft Knowledge Base Article 320045." Microsoft TechNet. 26 October 2002. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320045 (27 March 2003).

Shawgo, Jeff (ed.) The SANS Institute: Windows 2000 Security Step by Step. A Survival Guide for Windows 2000 Security: A consensus document by security professionals, Version 1.5. SANS Institute, 2001.

Witter, Franklin. "Legal Aspects of Collecting and Preserving Computer Forensic Evidence." The SANS Institute. 20 April 2001. URL:http://www.sans.org/rr/incident/evidence.php (27 March 2003).